servicenow

Sicherheitsmanagement Zürich

Zuletzt aktualisiert: 17.12.2025

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Materialien wurden für Sie mit einer Übersetzungssoftware übersetzt. Es wurden angemessene Anstrengungen unternommen, um Ihnen eine akkurate Übersetzung zu liefern. Jedoch können menschliche Übersetzer nicht durch automatisierte Übersetzungstechnologien ersetzt werden. Die Übersetzungen werden ungeprüft bereitgestellt. Es wird keinerlei Gewährleistung, weder ausdrücklich noch implizit, für die Genauigkeit, Zuverlässigkeit und Richtigkeit von Übersetzungen in andere Sprachen übernommen. Manche Inhalte wurden aufgrund der Beschränkungen der Übersetzungssoftware möglicherweise nicht präzise übersetzt. Die Ausgangssprache dieser Dokumente ist Englisch. Jegliche Diskrepanzen oder Unterschiede, die bei der Übersetzung entstehen, sind nicht verbindlich und haben keine Rechtswirkung für die Einhaltung oder Durchsetzung von Rechten.

Einige Beispiele und Grafiken, die hier dargestellt sind, dienen nur der Veranschaulichung.®ine echte Zuordnung oder Verbindung zu ServiceNow-Produkten oder -Services ist nicht beabsichtigt und sollte nicht abgeleitet werden.

ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken
sind Marken und/oder eingetragene Marken von ServiceNow, Inc., in den USA und/oder anderen Ländern. Andere Unternehmens- und
Produktnamen können Marken der jeweiligen Unternehmen sein,
denen sie zugeordnet sind.

Bitte lesen Sie die Nutzungsbedingungen für die ServiceNow-Website unter www.servicenow.com/terms-of-use.html

Automatische Übersetzung

Firmensitz
2225 Lawson Lane
Santa Clara, CA 95054
USA
(408) 501-8550

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhaltsverzeichnis

Security Operations **5**

Security Operations erkunden 7

Now Assist für Security Incident Response 14

Untersuchen 16

Konfigurieren 20

Verwenden Now Assist Zum Schließen von Security Incidents 27

Verwenden Sie agentische Workflows 40

Now Assist für Vulnerability Response 56

Untersuchen 57

Konfigurieren 60

Generative KI-Kompetenzen verwenden 63

Verwenden Sie agentische Workflows 73

Referenz 79

Angriffsoberflächenverwaltungsanwendungen 83

Vulnerability Response 85

Application Vulnerability Response 912

Container Vulnerability Response 1129

Konfigurations-Compliance 1212

Vulnerability Response Arbeitsbereiche 1494

Software-Stückliste 1701

Enterprise Security Case Management-Anwendungen 1743

Security Incident Response 1744

Threat Intelligence 3264

Sicherheitsstatus-Überwachung 3509

Untersuchen 3511

Verwenden Sie den Arbeitsbereich 3527

Verwenden Sie Minderungssteuerungen 3550

Referenz 3575

Cybersicherheits-Dashboard 3588

Aktivieren Sie Benchmark-Punktzahlen 3607

Legen Sie Ziele fest 3608

Integration von Sicherheitssimulationen und -Schulungen für Security Operations 3608

Risiko- und Compliance-Dashboard für GRC: Metrics 3611

Threat Intelligence-Sicherheitszentrum 3621

Untersuchen 3623

Konfigurieren 3630

Integrieren 3633

Verwalten 3722

Referenz 3768

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden....3776
Data Loss Prevention Incident Response....4017
Untersuchen....4019
Konfigurieren....4022
Verwalten....4023
Incidents verwalten....4081
Eingehende Integration....4104
Integrieren....4107
Security Operations Allgemeine Funktionalität....4180
Erstellen und definieren Sie Filtergruppen in Security Operations....4183
Transformation freigegebener Daten....4185
Security Operations E-Mail-Verarbeitung....4188
Security Operations Feldzuordnung....4199
Security Operations Feldwerttransformationen....4204
Security Operations Ergänzungsdatenzuordnung....4205
Security Operations Anwenderdefinierte Eskalation....4208
Erstellen Sie domänengetrennte Eigenschaftsüberschreibungen....4209
Erstellen Sie eine Betriebssystemgruppe....4210
Richten Sie Sicherheits-Tag-Gruppen und -Tags ein....4212
Sicherheitsanmerkungen....4216
Mit Security Support Common installierte Komponenten....4218
Modulzugriff nach Rolle für Security Operations-Anwendungen....4219
[store-future: BEGIN review]
[End]
Security Operations durchsuchen....4927
Referenzen zur Integration mit Security Operations....4927
Security Operations Workflow-Auslöser....5030
Orchestration für Security Operations....5032
Security Operations Szenarien und Beispiele....5033
[store-future: BEGIN review]
Reduzieren Sie die Zeit für die Bedrohungsanalyse durch Automatisierung....5033
[store-future: BEGIN review]
[End]
Priorisieren Sie wichtige Schwachstellen....5039
[store-future: BEGIN review]
[End]
[End]
Security Operations Und ServiceNow Store....5042
Laden Sie eine Anwendung aus dem herunter ServiceNow Store Zum ersten Mal....5042
Installieren Sie ein Security Operations Integration....5048
Aktualisieren Sie eine Anwendung, die zuvor aus dem heruntergeladen wurde ServiceNow Store....5052
Führen Sie ein Upgrade Ihrer Instanz auf das nächste Familien-Release durch....5053

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations

ServiceNow® Security Operations Anwendungen importieren Incident-Daten aus Ihren Sicherheitstools in eine strukturierte Antwort-Engine, die intelligente Workflows, Automatisierung, Datenvisualisierungen und eine enge Verbindung mit IHR verwendet, um Bedrohungen basierend auf den Auswirkungen, die sie für Ihre Organisation darstellen, zu priorisieren und zu lösen.

Klicken Sie auf eine dieser Kacheln, um zu beginnen.

Security Operations-Anwendungen und ihre Arbeitsbereiche

Erfahren Sie, wie Security Operations Anwendungen können Ihnen helfen, Ihre Sicherheitslage zu verbessern.

Now Assist für Security Incident Response

Erfahren Sie, wie Now Assist for Security Incident Response unterstützt ServiceNow® Kompetenzen der generativen KI (GenAI) im Security Incident Response-Arbeitsbereich und in der Core-UI (UI16).

Now Assist für Vulnerability Response

Erfahren Sie, wie Now Assist für Vulnerability Response Unterstützt ServiceNow® Kompetenzen der generativen KI (GenAI) im Vulnerability Response-Arbeitsbereich und in der Core-UI (UI16).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

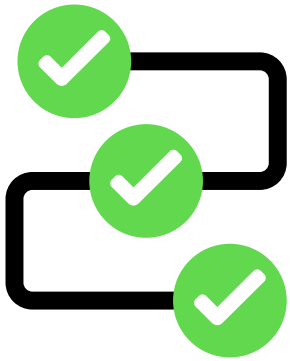
Angriffsoberflächenverwaltungsanwendungen

Erfahren Sie mehr über die Anwendungen in Vulnerability Response, mit denen Sie Schwachstellen auf Ihrer gesamten Cyberangriffsoberfläche identifizieren und beheben können.

Enterprise Security Case Management-Anwendungen

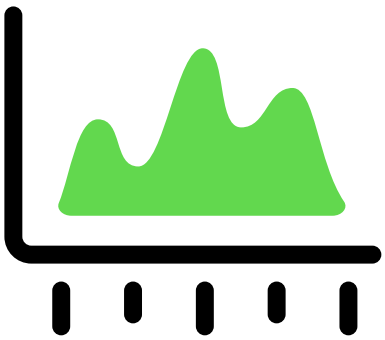
Erfahren Sie mehr über die Anwendungen in Security Incident Response, mit denen Sie kritische Security Incidents analysieren, isolieren und beheben können, während sie sich entwickeln.

Anwendungen zur Sicherheitsstatus-Steuerung



Erfahren Sie mehr über die Anwendungen, mit denen Sie Einblicke in Ihre allgemeine Sicherheitslage erhalten.

Cybersicherheits-Dashboard

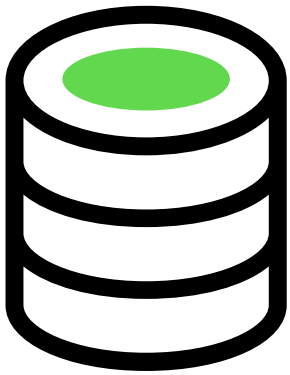


Erfahren Sie, wie das Cybersicherheits-Dashboard Daten aus den verschiedenen SecOps-Produkten in einem einheitlichen Dashboard konsolidiert.

Threat Intelligence-Sicherheitszentrum

Erfahren Sie, wie Threat Intelligence-Sicherheitszentrum Die Plattform (TISC) bietet Technologielösungen für die Zusammenfassung und Verwaltung von Threat Intelligence.

Reaktion auf Incident zur Vermeidung von Datenverlust

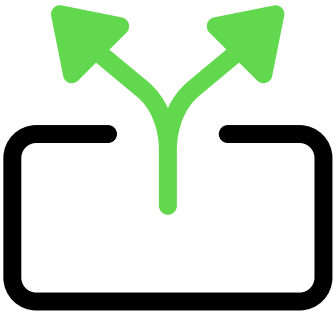


Erfahren Sie, wie Sie vertrauliche Informationen für Ihre Kunden verwalten und Ihre Datenverlustkanäle identifizieren und schützen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gemeinsam genutzte Security Operations-Anwendungen



Erfahren Sie mehr über Funktionen und Module, die allgemeine Funktionen in allen bereitstellen Security Operations.

Security Operations-Szenarien und -Beispiele

Erfahren Sie mehr darüber, wie Sie erhalten Security Operations Anwendungen aus dem ServiceNow® Store Und Szenarien für Anwendungen, die Sie während der Verwendung der -Produkte verwenden können.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Security Operations erkunden

Schützen Sie Ihre Assets und die Unternehmensumgebung mit ServiceNow Security Operations-Anwendungen und die Leistung von ServiceNow AI Platform®. Verbinden Sie Ihre Sicherheits- und IT-Teams, um Sie bei der Priorisierung und Lösung von Bedrohungen basierend auf den Auswirkungen zu unterstützen, die sie auf Ihre Organisation haben.

Security Operations – Übersicht

Die Security Operations die suite von Anwendungen hilft Ihnen, Ihre Assets zu schützen, indem Sie Ihre allgemeine Sicherheitslage verbessern. Zum Beispiel durch die Integration von Anwendungen wie Security Incident Response, Vulnerability Response, Und Sicherheitsstatus-Überwachung Mit Ihren vorhandenen Sicherheitstools können Analysten, Manager und IT-Teams des Security Operations Center (SOC):

- Reagieren Sie auf sich schnell entwickelnde Cyber- und Sicherheitsbedrohungen
- Schwachstellen identifizieren, priorisieren und beheben
- Zeigen Sie Ihren vollständigen Asset-Bestand an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

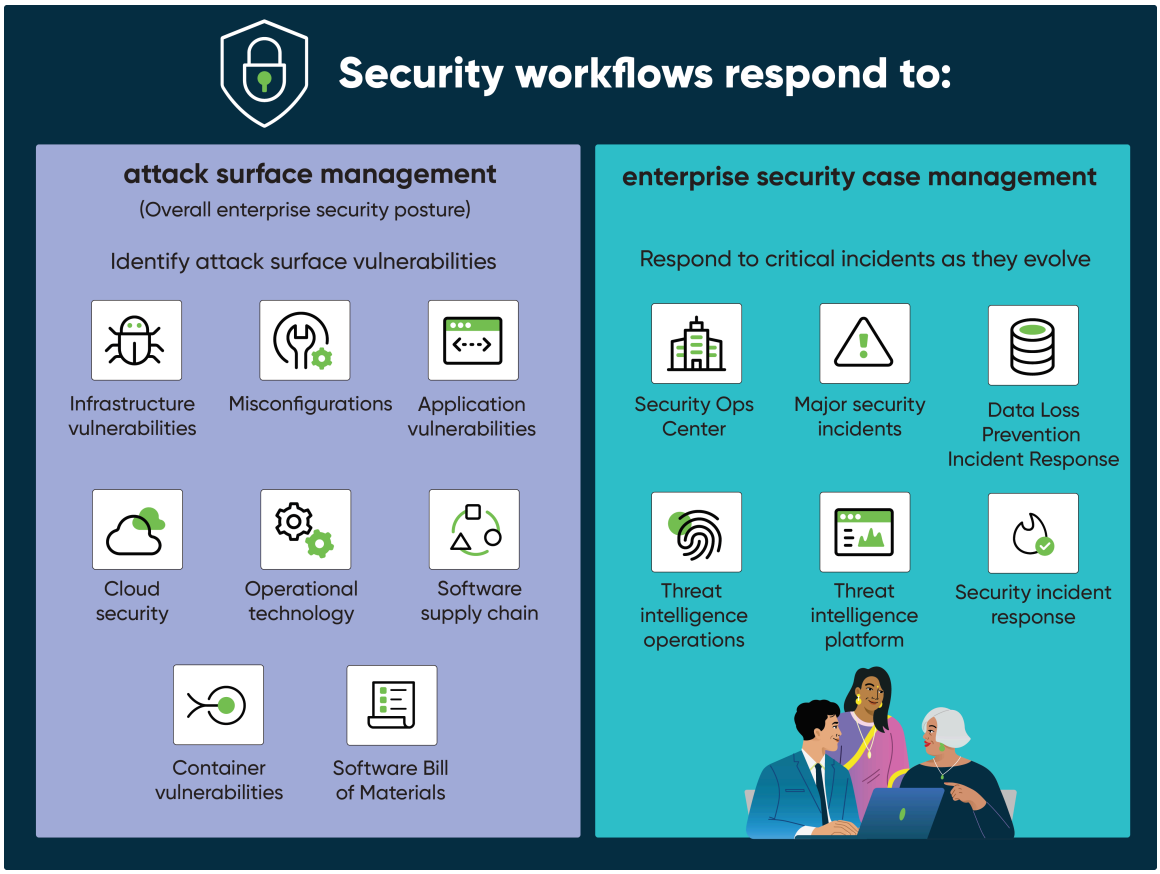
- Bestimmen Sie die Gesamtabdeckung des Sicherheitstools
- Lösen Sie Security Incidents schneller mit intelligenten Workflows und ServiceNow Generative KI-Kompetenzen (GenAI). Weitere Informationen finden Sie unter Now Assist für Security Incident Response.

Security Operations Anwendungen für Workflows

Die Security Operations Anwendungen fallen in zwei allgemeine Kategorien für Security Operations Workflows:

- Angriffsoberflächenmanagement: Anwendungen und Tools, mit denen Sie Schwachstellen antizipieren, verstehen und schließen können.
- Management von Sicherheitsfällen für Unternehmen: Anwendungen und Tools, mit denen Sie schnell auf kritische Incidents reagieren können.

Sicherheits-Workflows



Die beiden Kategorien von Security Operations-Anwendungen und die Anwendungsfälle, mit denen Sie in Ihrer Unternehmensumgebung umgehen können.

Vorteile von Security Operations Anwendungen

Anzeigen Security Operations Anwendungen und Daten mit Anwenderoberflächen der nächsten Generation (Arbeitsbereiche). Mit Arbeitsbereichen können Sicherheitsanalysten, Security Operation Center (SOC)-Manager und Korrekturspezialisten in Ihrer Organisation die folgenden Arten von Workflows von einem zentralen Standort aus überwachen und verwalten:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Lebenszyklus von Security Incidents von der ersten Analyse bis zur Eindämmung, Beseitigung und Wiederherstellung.
- Die Schwachstellen, die ihnen am wichtigsten sind, damit sie strategisch entscheiden können, welche Schwachstellen sie an IT-Teams senden, um sie zu beheben.
- Wichtige Einblicke und wichtige Anwendungsfälle für die Abdeckung von Sicherheitstools und Asset-Hygiene, die importierte Informationen zu Ihren Assets melden und überwachen.

Angriffsoberflächenverwaltungsanwendungen

Anwendungen, mit denen Sie Bedrohungen antizipieren und Schwachstellen identifizieren können

Anwendung	Beschreibung	Anwender
Sicherheitsstatus-Überwachung	Erhalten Sie Einblicke in die Bereitstellung von Sicherheitstools und die Abdeckung Ihrer Assets basierend auf einem Asset-Bestand und importierten Daten. Service Graph Connectors und ServiceNow-Produkte wie Hardware Asset Management (HAM) und ITOM Discovery werden für Datenimporte unterstützt. Audits basierend auf Richtlinien helfen Ihnen, die Behebung von Kombinationen mit hohem Risiko wie Internetrisiko und bekannten Schwachstellen zu priorisieren. Erstellen Sie anwenderdefinierte Richtlinien und Einblicke, um die Compliance von Assets mit den Konfigurationsstandards Ihrer internen Sicherheitstools zu überwachen.	• CISO • Informationssicherheitsanalyst • Security Operations-Manager • IT Operations-Ingenieur • Serviceverantwortlicher (Persona des Korrekturbesitzers)
Vulnerability Response	Schwachstellen-Scanner und Bewertungstools von Drittparteien helfen Ihnen, die Risiken zu identifizieren, die Schwachstellen für die	• CISO • Informationssicherheitsanalyst • Security Operations-Manager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen, mit denen Sie Bedrohungen antizipieren und Schwachstellen identifizieren können (Fortsetzung)

Anwendung	Beschreibung	Anwender
	folgenden Arten von Assets darstellen: • Infrastruktur (Host) • Behälter • Anwendungen • Software-Stückliste Schwachstellen, die von diesen Tools identifiziert werden, gelten als Risiken für die Sicherheits- und IT-Teams, die für die Wartung und Sicherung der Assets einer Organisation verantwortlich sind.	• IT Operations-Ingenieur • Serviceverantwortlicher (Persona des Korrekturbesitzers)
Konfigurations-Compliance	Überprüfen Sie Ihre Compliance mit Sicherheits- oder Unternehmensrichtlinien. Identifizieren, priorisieren und korrigieren Sie nicht konforme Konfigurationselemente mit Testergebnissen, die aus SCA-Integrationen von Drittanbietern (Secure Configuration Assessment) gewonnen wurden.	• CISO • Informationssicherheitsanalyst • Security Operations-Manager • IT Operations-Ingenieur • Serviceverantwortlicher (Persona des Korrekturbesitzers)

Enterprise Security Case Management-Anwendungen

Anwendungen, mit denen Sie auf kritische Sicherheitsverletzungen und Incidents reagieren können

Anwendung	Beschreibung	Anwender
Security Incident Response	Vereinfachen Sie den Prozess der Identifizierung kritischer Incidents, indem Sie leistungsstarke Workflow- und Automatisierungstools anwenden, die die Korrektur beschleunigen.	• CISO • Informationssicherheitsanalyst • Security Operations-Manager • Threat Intelligence-Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen, mit denen Sie auf kritische Sicherheitsverletzungen und Incidents reagieren können (Fortsetzung)

Anwendung	Beschreibung	Anwender
	Integrieren Sie Ihre vorhandenen SIEM-Tools (Security Information and Event Manager) mit Security Incident Response Und Security Operations-Anwendungen, um Bedrohungsdaten aus verschiedenen Quellen zu importieren und automatisch priorisierte Security Incidents zu erstellen.	
Management schwerwiegender Sicherheits-Incidents	Die Funktionen zum Management schwerwiegender Security Incidents funktionieren mit den vorhandenen Security Incident Response-Produktfunktionen. Dies umfasst die Fähigkeit eines Sicherheitsanalysten, einen Standard-Security Incident zu einem schwerwiegenden Security Incident zu eskalieren, sodass die neuen Produktfunktionen zur Unterstützung des Korrekturprozesses verfügbar sind. Verfolgen Sie den Fortschritt schwerwiegender Security Incidents (MSI) von der Discovery bis zur Analyse. Schlagen Sie Lösungen vor, heraufstufen und verknüpfen Sie Security Incidents und den Abschluss.	• CISO • Informationssicherheitsanalyst • Security Operations-Manager • IT Operations-Ingenieur • Serviceverantwortlicher (Persona des Korrekturbesitzers) • Allgemeiner rat
Reaktion auf Incident zur Vermeidung von Datenverlust	Mit der Data Loss Prevention Incident Response (DLP IR) können Sie den Korrekturworkflow von DLP-Incidents aus mehreren Quellen überprüfen und verwalten, z. B. Endpunkt, Netzwerk, E-Mail und Cloud. Mit der DLP-Anwendung können Sie Ihre Datenverlustkanäle	• CISO • Informationssicherheitsanalyst • Security Operations-Manager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen, mit denen Sie auf kritische Sicherheitsverletzungen und Incidents reagieren können (Fortsetzung)

Anwendung	Beschreibung	Anwender
	identifizieren, reagieren und schützen.	
Threat Intelligence	Ermöglicht es Incident-Response-Teams, Bedrohungssuchen, -Suchen und -Korrelation zu automatisieren. Die Integration mit MITRE ATT&CK ermöglicht es Ihnen, die Erkennung und Minderungsabdeckung zu messen und zu verstehen, und hilft bei der Bedrohungssuche.	• CISO • Informationssicherheitsanalyst • Security Operations-Manager • Threat Intelligence-Analyst
Threat Intelligence-Sicherheitszentrum (TISC)	Aggregieren, kuratieren und verwalten Sie Threat Intelligence aus mehreren Quellen, und führen Sie das Threat Intelligence-Fallmanagement durch. Verfolgen Sie Kampagnen, operationalisieren Sie Threat Intelligence, und reagieren Sie auf umsetzbare Intelligenz.	• CISO • Informationssicherheitsanalyst • Security Operations-Manager • Threat Intelligence-Analyst

Empfehlungen für weitere Themen

Wählen Sie eine Kachel aus, um mit zu beginnen Security Operations Arbeitsbereiche.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsbereich für Security Incident Response

Erfahren Sie mehr über den Security Incident Response-Arbeitsbereich

Arbeitsbereich des Schwachstellenmanagers

Erfahren Sie mehr über den Vulnerability Manager-Arbeitsbereich

Arbeitsbereich Für Sicherheitsstatus-Steuerung

Erfahren Sie mehr über den Arbeitsbereich für die Sicherheitsstatus-Steuerung

Arbeitsbereich der Schwachstellenbewertung

Erfahren Sie mehr über den Arbeitsbereich „Schwachstellenbewertung“

Arbeitsbereich für IT-Korrekturen

Erfahren Sie mehr über den Arbeitsbereich „IT-Korrektur“

Software-Stücklisten-Arbeitsbereich

Erfahren Sie mehr über den Arbeitsbereich „Software-Stückliste“

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsbereich des Threat Intelligence Security Center (TISC)	Arbeitsbereich für Incident Response zur Verhinderung von Datenverlust (DLP)	Arbeitsbereich für Management schwerwiegender Security Incidents (MSIM)
Erfahren Sie mehr über den TISC-Arbeitsbereich	Erfahren Sie mehr über den DLP-Arbeitsbereich	Erfahren Sie mehr über den MSIM-Arbeitsbereich

Problembehandlung und Hilfe

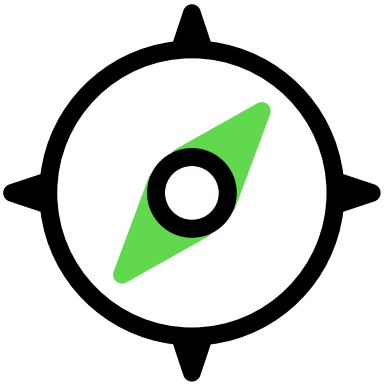
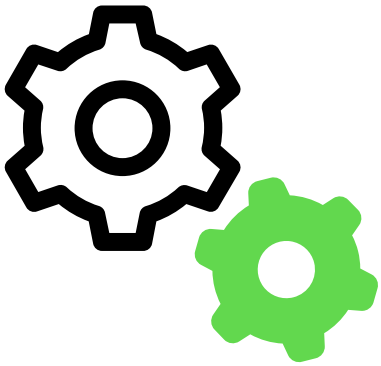
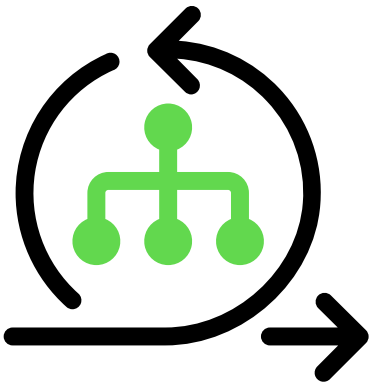
- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Now Assist für Security Incident Response

Sicherheitsanalysten können intelligente Workflows und verwenden ServiceNow Kompetenzen der generativen KI, die ihnen bei der Lösung von Security Incidents helfen. Sicherheitsmanager können den Kontext von Security Incidents und Abschlussnotizen schnell in einem präzisen, leicht lesbaren Format überprüfen. Zeigen Sie Analysedaten nach Incident an, und lesen Sie empfohlene Korrekturschritte Mit Now Assist für Security Incident Response Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Konfigurieren	Verwenden
		
Erfahren Sie mehr über Now Assist für Security Incident Response	Erfahren Sie, wie Sie die Kompetenzen für konfigurieren und aktivieren Now Assist für Security Incident Response	Erfahren Sie, wie Sie mit generativer KI und Details zusammenfassen und Abschlussnotizen für Security Incidents generieren Now Assist für Security Incident Response

Wichtig:

- Nicht alle Modellanbieter sind für Kunden mit landesinternen SKUs verfügbar, und einige Now Assist-Produkte/-Funktionen sind derzeit für Kunden im Land nicht verfügbar. Weitere Informationen finden Sie unter KB1584492 artikel in der Now Support Knowledge Base. Überprüfen Sie in zukünftigen Releases auf Updates der Modellanbieter-Verfügbarkeit.
- Einige Now Assist Produkte/Funktionen sind derzeit für Kunden in den mit FedRAMP, NSC DOD IL5 oder Australia IRAP geschützten Rechenzentren, selbst gehosteten Kunden oder anderen eingeschränkten Umgebungen nicht verfügbar. Weitere Informationen finden Sie im Now Support Knowledge Base-Artikel KB0743854 . Überprüfen Sie auf Verfügbarkeitsaktualisierungen in zukünftigen Releases.
- Einige Now Assist Produkte/Funktionen sind derzeit nur für Kunden in einigen Regionen verfügbar. Überprüfen Sie auf Verfügbarkeitsaktualisierungen in zukünftigen Releases.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

KI-Beschränkungen

Diese Anwendung nutzt künstliche Intelligenz (KI) und maschinelles Lernen, zwei sich schnell entwickelnde Studienbereiche, in denen Vorhersagen auf Grundlage von Datenmustern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erstellt werden. Daher liefert diese Anwendung möglicherweise nicht immer präzise, vollständige und angemessene Informationen. Darüber hinaus besteht keine Garantie dafür, dass diese Anwendung für Ihren Anwendungsfall vollständig trainiert oder getestet wurde. Um diese Probleme zu mindern, liegt es in Ihrer Verantwortung, Ihre Verwendung dieser Anwendung auf Richtigkeit, Schaden und Angemessenheit für Ihren Anwendungsfall zu testen und zu bewerten, menschliche Aufsicht über die Ausgabe zu übernehmen und zu Entscheidungszwecken nicht ausschließlich KI-generierte Ausgaben zu verwenden. Dies ist besonders wichtig, wenn Sie diese Anwendung in Bereichen mit weitreichenden Auswirkungen wie Gesundheitswesen, Finanzen, Recht, Beschäftigung, Sicherheit und Infrastruktur einsetzen möchten. Sie stimmen zu, sich an zu halten Richtlinie zur zulässigen Nutzung von KI von ServiceNow , Die von ServiceNow aktualisiert werden kann.

Datenverarbeitung

Bei dieser Anwendung müssen die Daten einzelner ServiceNow-Kundeninstanzen in eine zentrale ServiceNow-Umgebung übertragen werden, die sich in einer anderen Rechenzentrumsregion befinden kann als die, in der sich Ihre Instanz befindet, und möglicherweise an einen externen Cloud-Anbieter, z. B. Microsoft Azure. Diese Daten werden gemäß den internen Richtlinien und Verfahren von ServiceNow gehandhabt, einschließlich unserer Richtlinien, die über unser CORE-Compliance-Portal verfügbar sind.

Datenerfassung

ServiceNow sammelt und verwendet die Eingaben, Ausgaben und Ausgabenbearbeitungen dieser Anwendung, um ServiceNow-Technologien wie ServiceNow-Modelle und KI-Produkte zu entwickeln und zu verbessern. Darüber hinaus erfasst diese Anwendung Daten aus Security Incidents, Incidents, Change-Anforderungen, Probleme und angreifbare Elemente . Kunden können der Datenerfassung für die Zukunft jederzeit widersprechen, wie auf der Now Assist Abwählseite beschrieben.

Weitere Informationen finden Sie unter Now Assist-Dokumentation .

Now Assist für Security Incident Response erkunden

Ihre Sicherheitsanalysten können intelligente Workflows und verwenden ServiceNow Kompetenzen der generativen KI, die ihnen helfen, Security Incidents im Flow ihrer Arbeit mit zu selektieren, zu untersuchen und zu schließen Now Assist für Security Incident Response Anwendung.

Now Assist für Security Incident Response – Übersicht

Mit Kompetenzen für generative KI und agentischen Workflows haben Ihre Sicherheitsanalysten die Möglichkeit:

- Fassen Sie Security Incident-Details zusammen, und überprüfen Sie den Kontext schnell in einem präzisen, leicht lesbaren Format.
- Generieren Sie empfohlene nächste Schritte für einen Security Incident.
- Generieren Sie Analysedaten nach dem Incident.
- Generieren Sie Abschlussnotizen.
- Korrelationseinblicke generieren

Sicherheitsanalysten können Ergebnisse, Incident-Details und Abschlussnotizen mit anderen Analysten, Managern und wichtigen Stakeholdern teilen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Assist für Security Incident Response Anwender

Anwender

Anwender	Beschreibung
Sicherheitsanalysten und -Manager	Zeigen Sie eine Vorschau der Security Incident-Details an, sehen Sie sich deren potenzielle Auswirkungen an, und zeigen Sie die wichtigsten Korrekturaktionen an, die bereits mit Security Incident-Zusammenfassungen mithilfe generativer KI durchgeführt wurden. Zusammenfassungen und empfohlene nächste Schritte (Aktionen) Geben Sie Analysten und Managern einen Vorsprung bei ihren Untersuchungen und helfen Sie beim Schließen von Security Incidents. Generieren Sie mithilfe generativer KI automatisch einen Entwurf von Abschlussnotizen. Abschlussnotizen für Security Incidents werden schnell basierend auf Nachbesserungs- und Eindämmungsaktivitäten erstellt, zusätzlich zu anderen relevanten Details, die sich auf ihren Abschluss beziehen.

Now Assist für Security Incident Response – Vorteile

Now Assist für Security Incident Response Funktionen

Leistung	Funktion	Anwender
Beschleunigen Sie die Selektierung von Security Incidents mit langen Aktivitätenströmen, indem Sie Arbeitsnotizen und kontextbezogene Informationen schnell in einem präzisen, leicht lesbaren Format überprüfen.	Generieren Sie Zusammenfassungen für Security Incidents, die die folgenden Informationen enthalten: • Problem • Details • Beobachtungen • Schlüsselaktionen ausgeführt • Abschlussdetails	• Sicherheitsanalysten • Sicherheitsmanager
Generiert automatisch einen Entwurf von Abschlussnotizen für einen Security Incident, wenn er zum Abschluss bereit ist. Analysten können jeden Inhalt ändern, der von der KI-Kompetenz generiert wird, indem sie ihn bearbeiten, entfernen oder eigene Notizen hinzufügen, bevor sie den Security Incident schließen.	Generieren Sie Security Incident-Abschlussnotizen	• Sicherheitsanalysten • Sicherheitsmanager
Generieren Sie auf Anforderung empfohlene nächste Schritte innerhalb des Workflows, um Ihnen beim Schließen eines Security Incidents zu helfen.	Generieren Sie empfohlene Aktionen für Security Incidents	• Sicherheitsanalysten • Sicherheitsmanager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Assist für Security Incident Response Funktionen (Fortsetzung)

Leistung	Funktion	Anwender
Generieren Sie eine Analyse nach dem Incident, die eine Ursachenanalyse, eine Auswirkungsbewertung und gelernte Lektionen im Workflow zum Schließen eines Security Incidents umfasst.	Generieren Sie eine Analyse nach dem Incident	• Sicherheitsanalysten • Sicherheitsmanager
Verbinden Sie aktuelle Incidents mit vergangenen Ereignissen, die dieselben betroffenen Anwender, Konfigurationselemente (Configuration Items, CIs) oder erkennbaren Elemente betreffen.	Korrelationseinblicke generieren	• Sicherheitsanalysten • Sicherheitsmanager
Erfahren Sie schnell mehr über die Details eines Security Incidents, indem Sie auf Zusammenfassungen und Abschlussnotizen von zugreifen Now Assist Bereich.	Greifen Sie über auf die Zusammenfassung der generativen KI und die Abschlussnotizen zu Now Assist Bereich. Geben Sie Anforderungen ein, um grundlegende Informationen zu Security Incidents im Bereich zu erhalten.	• Sicherheitsanalysten • Sicherheitsmanager
Passen Sie die Kompetenzen der generativen KI für Zusammenfassungen und Abschlussnotizen an Ihre Anforderungen an.	Kopieren Sie eine Kompetenz, und ändern Sie die Felder der zugehörigen Tabelle, definieren Sie die Verfügbarkeit der Kompetenz, und wählen Sie aus, wo die Kompetenz angezeigt wird.	Administrator

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Now Assist für Security Incident Response finden Sie unter:

- Now Assist für Security Incident Response konfigurieren
- Fassen Sie einen Security Incident mit zusammen Now Assist für Security Incident Response
- Generieren Sie Abschlussnotizen für einen Security Incident mit Now Assist für Security Incident Response
- Generieren Sie Korrelationseinblicke in Now Assist Bereich mit Now Assist für Security Incident Response
- Generieren Sie empfohlene Aktionen für einen Security Incident mit Now Assist für Security Incident Response
- Generieren Sie mit eine Analyse nach dem Incident für einen Security Incident Now Assist für Security Incident Response
- Eingaben und Auslöser für Now Assist für Security Incident Response

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergänzende Informationen für Now Assist für Security Incident Response

Verschaffen Sie sich einen schnellen Überblick über wichtige Informationen im Zusammenhang mit der Anwendung Now Assist für Security Incident Response.

Unterstützte Versionen

Version 2.0.1 von Now Assist für Security Incident Response Unterstützt:

- veraltet UI (UI16): Security Incident Response Kernanwendung, v13.6.4
- Arbeitsbereich für Security Incident Response(SIR-Arbeitsbereich), v1.7.0
- Now Assist für ServiceNow AI Platform® V6.0.1

Unterstützte Anwenderoberflächen

Die Now Assist für Security Incident Response Enthält die Kompetenzen der generativen KI, die in der folgenden Tabelle aufgeführt sind.

Now Assist für Security Incident Response Unterstützte Schnittstellen und Kompetenzen

Schnittstelle	Features
Security Incident Response	• Zusammenfassung des Security Incidents. • Generierung der empfohlenen nächsten Schritte für einen Security Incident. • Generierung von Analysen nach Incident, die Ursachenanalyse, Auswirkungsbewertung und gelernte Lektionen umfassen. • Now Assist Bereich. • Generierung von Abschlussnotizen. • Korrelationseinblicke aus der Now AssistBereich.
Veraltet UI16	• Zusammenfassung des Security Incidents • Generierung der empfohlenen nächsten Schritte für einen Security Incident. • Generierung von Analysen nach Incident, die Ursachenanalyse, Auswirkungsbewertung und gelernte Lektionen umfassen. • Now Assist Bereich. • Generierung von Abschlussnotizen. • Korrelationseinblicke aus der Now AssistBereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Assist für Security Incident Response konfigurieren

Die Now Assist für Security Incident Response Die Anwendung wird in unterstützt Arbeitsbereich für Security Incident Response Und in veraltet Core-UI (UI16). Sie können das geführte Setup in verwenden Now Assist-Administrator Zu konfigurierende Konsole Now Assist für Security Incident Response.

Konfiguration – Übersicht

Durch Freigeben von Daten für ServiceNow® KI-Entwicklungsprogramm stellen Sie relevante Daten bereit, um die Genauigkeit der Vorhersage und die Anwender-Experience zu verbessern, Produkte an Ihre Geschäftsanforderungen anzupassen und Halluzinationen für aktivierte zu reduzieren Now Assist Kompetenzen.

Sie können eine deaktivieren ServiceNow Instanz aus der Datenfreigabe von Now Assist-Administrator Konsole, wenn Sie nicht teilnehmen möchten. Weitere Informationen finden Sie unter Opt out of data sharing for Now Assist . Wiederholen Sie den Abwählvorgang für alle Instanzen, die verwenden Now Assist Funktionalität.

Verwenden Sie die Now Assist-Administrator-Konsole, um Now Assist für Security Incident Response zu konfigurieren. Diese Konsole enthält alles, was Sie für die Installation der Anwendungen und die Konfiguration der Kompetenzen für generative KI benötigen. Weitere Informationen finden Sie unter Configuring Now Assist Admin features .

In der folgenden Tabelle sind die Funktionen und Kompetenzen aufgeführt, auf die Sie über die Now Assist-Administrator-Konsole zugreifen können.

Now Assist für Security Incident Response Funktionen und Kompetenzen in Now Assist-Administrator Konsole

Now Assist-Technologieprodukt	Security Incident-Kompetenzen
Now Assist für Security Incident Response	Zusammenfassung des Security Incidents **Hinweis:** Die Incident-Zusammenfassung unterstützt Security Incidents in einem anderen Status als **Entwurf** .
	Generierung von Lösungshinweisen.
	Empfohlene Aktionen für Security Incident Die Kompetenz „empfohlene Aktionen für Security Incidents“ unterstützt Security Incidents in einem anderen Status als **Geschlossen** Und **Abgebrochen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Assist für Security Incident Response Funktionen und Kompetenzen in Now Assist-Administrator Konsole (Fortsetzung)

Now Assist-Technologieprodukt	Security Incident-Kompetenzen
	Hinweis: Die Anwendung KI-Suche muss aktiviert sein, damit die Kompetenz empfohlene Aktionen für Security Incidents funktioniert. Um zu überprüfen, ob die KI-Suche in Ihrer Instanz aktiviert ist, navigieren Sie zu **Alle** > **KI-Suche** > **Status der KI-Suche**an. Wenden Sie sich an den Support, wenn auf der Seite angegeben wird, dass die KI-Suche nicht aktiviert ist. Korrelationseinblicke unterstützen Security Incidents in allen status.
	Generierung der Analyse nach dem Incident

1. Install Now Assist plugins .

   Installieren Sie Now Assist für Security Incident Response Anwendung (sn_sec_gen_ai) und Security Incident Response Kernanwendungen [sn_si].

2. Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Security Incident Response

   Konfigurieren und überprüfen Sie die Details für eine Kompetenz. Sie aktivieren eine Kompetenz über Geführtes Setup.

Verwenden Geführtes Setup Zu implementieren Now Assist für Security Incident Response

Geführtes Setup Stellt eine Sequenz von Aufgaben bereit, die Ihnen bei der Konfiguration helfen Now Assist für Security Incident Response Auf Ihrem ServiceNow Instanz. Um zu öffnen Geführtes Setup Für Now Assist für Security Incident Response, Navigieren Sie zu **Alle** > **Now Assist Admin** > **Features**an.

Weitere Informationen finden Sie unter Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Security Incident Response.

Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Security Incident Response

Konfigurieren und überprüfen Sie die Details für eine Kompetenz in Geführtes Setup. Sie können eine Kompetenz über aktivieren Geführtes Setup.

Vorbereitungen

Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Now Assist Admin** > **Features**an.
2. Mit **Technologie** Wählen Sie im Navigationsbereich aus **Security Operations** Aus der Liste.
   Diese Security Incident-Kompetenzen werden auf der Security Incident-Karte angezeigt:
   - Empfohlene Aktionen für Security Incident

     Die Anwendung KI-Suche muss aktiviert sein, damit die Kompetenz empfohlene Aktionen für Security Incidents funktioniert. Um zu überprüfen, ob die KI-Suche in Ihrer Instanz aktiviert ist, navigieren Sie zu **Alle** > **KI-Suche** > **Status der KI-Suche**an. Wenden Sie sich an den Support, wenn auf der Seite angegeben wird, dass die KI-Suche nicht aktiviert ist.
   - Analyse nach Incident
   - Generierung von Korrelationseinblicken
   - Security Incident-Zusammenfassung
   - Lösungshinweise generieren
3. Wählen Sie Aus **Zeigen Sie Details an** .
   Sie können die Kompetenzen, die in der Anwendung enthalten sind, nicht bearbeiten. Um die Standardeinstellungen zu bearbeiten, müssen Sie eine Kopie erstellen. Weitere Informationen zum Anpassen einer Kompetenz finden Sie unter Now Assist für Security Incident Response-Kompetenzen anpassen.
4. Wählen Sie Aus **Kompetenz aktivieren** Für die gewünschte Kompetenz.
5. Führen Sie die Schritte aus, um eine Kompetenz mit zu konfigurieren und zu aktivieren Geführtes Setup.

   Hinweis:
   Einige Kompetenzen erfordern nicht alle unten aufgeführten Konfigurationsschritte. Wählen Sie die einzigen Aufgaben aus, die im linken Bereich angezeigt werden, und befolgen Sie die Anweisungen. Nachdem Sie die Aufgaben abgeschlossen haben, aktivieren Sie die Kompetenz.

   a. Wählen Sie im Navigationsbereich aus **Wählen Sie Eingabe** Zum Konfigurieren der Eingaben oder Auslöser für die ausgewählte Kompetenz.

      Einige oder alle der folgenden Elemente Eingabevorlagen für die Kompetenz werden aufgelistet: **In Arbeit** , **Überprüfen** , Und **Geschlossen** . Die **In Arbeit** Vorlage ist ausgewählt.

      Möglicherweise möchten Sie diese Eingabevorlagen in ihren Standardeinstellungen belassen, bis Sie sich mit den Kompetenzen für vertraut gemacht haben Now Assist für Security Operations Arbeit.

      Jedoch Für einige der Kompetenzen Sie können bestimmte zugehörige Tabellenfelder ändern, den Prompt für einen Security Incident testen, die Verfügbarkeit der Kompetenz definieren und auswählen, wo die Kompetenz angezeigt wird.

      Wenn Sie Felder ändern möchten, wählen Sie nur die unterstützten Optionen aus den Listen aus, die als Teil Ihrer Eingabedaten bereitgestellt werden.

      Wenn Sie die Eingaben oder Auslöser für eine Kompetenz ändern, bestimmen Sie, wie und wann eine Kompetenz verwendet wird. Sie können die Eingabedatenquelle einer Kompetenz nicht ändern. Die Datenquelle enthält die Tabellen und Felder, auf denen die Fähigkeit basiert. Sie können jedoch eine Kompetenz kopieren und anpassen. Weitere Informationen finden Sie unter Now Assist für Security Incident Response-Kompetenzen anpassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie Aus **Speichern und fortfahren** Um zum nächsten Schritt in zu wechseln Geführtes Setup.
7. **Wahlweise:** Testen Sie die Eingabeaufforderung für einen Security Incident-Datensatz.
8. Wählen Sie Aus **Speichern und fortfahren** Um zum nächsten Schritt in zu wechseln Geführtes Setup.
9. **Wahlweise:** Wählen Sie eine der folgenden Optionen aus, um die Verfügbarkeit zu definieren.
10. Wählen Sie Aus **Speichern und fortfahren** Um zum nächsten Schritt in zu wechseln Geführtes Setup.
11. Wählen Sie Aus **Wählen Sie Anzeige aus** Um zu bestimmen, wo Sie die Kompetenz anzeigen möchten.
12. Wählen Sie **Speichern und fortfahren**, um mit dem nächsten Schritt fortzufahren.
13. **Wahlweise:** Fügen Sie Rollen hinzu, oder entfernen Sie sie.

    (Optional) Standardmäßig werden die Rollen sn_si.Analyst und sn_si.Manager hinzugefügt und können die Ergebnisse der automatisierten Kompetenzgenerierung anzeigen. Sie können Rollen nur hinzufügen oder entfernen, wenn Sie es sind Now Assist für Security Incident Response-Kompetenzen anpassen.
14. Überprüfen Sie Ihre Auswahlmöglichkeiten, und wählen Sie aus **Aktivieren** Um die Konfiguration für die Kompetenz abzuschließen.
15. Wählen Sie Aus **Zurück zu Security Incident** .
    Die Kompetenz wird im Abschnitt aktive Kompetenzen angezeigt.

Now Assist für Security Incident Response-Kompetenzen anpassen

Passen Sie einige der Eingabefelder einer generativen KI-Kompetenz an die Anforderungen Ihrer Umgebung an.

Vorbereitungen

Erforderliche Rollen: administrator

Prozedur

1. Navigieren Sie zu **Alle** > **Now Assist Admin** > **Features** Registerkarte von Now Assist-Administrator Konsole.
2. Mit **Technologie** Wählen Sie im Navigationsbereich aus **Security Operations** Aus der Liste.
   Diese Security Incident-Kompetenzen werden angezeigt:
   - Empfohlene Aktionen für Security Incident
   - Analyse nach Incident
   - Generierung von Korrelationseinblicken
   - Security Incident-Zusammenfassung
   - Lösungshinweise generieren
3. Erstellen Sie eine Kopie einer Kompetenz, und passen Sie die Eingabefelder an.

   a. Wählen Sie auf der Funktionskarte Security Incident die Option aus **Zeigen Sie Details an** .

   b. Suchen Sie im Abschnitt aktive Kompetenzen die Kompetenz, die Sie kopieren möchten, und wählen Sie das Symbol weitere Aktionen ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie Aus **Erstellen Sie eine Kopie** .

d. Bestätigen Sie Ihre Auswahl im Modal.
Das geführte Setup wird angezeigt.

e. In **Allgemeine Details** Geben Sie einen eindeutigen Namen und eine Beschreibung für die Kompetenz ein.

f. Fahren Sie mit dem nächsten Schritt fort, indem Sie auswählen **Speichern und fortfahren** .

g. Wählen Sie Aus **Wählen Sie Eingabe** .

Wenn **Wählen Sie Eingabe** Ist ausgewählt, werden diese Eingabevorlagen für die Kompetenz aufgelistet: In Arbeit, Überprüfung und Geschlossen. Die Vorlage in Arbeit ist ausgewählt.

Sie können einige der Basiseingabetabellenfelder, die Bedingungen und die zugehörigen Listen für die Vorlagen konfigurieren. Wählen Sie nur aus den zugehörigen Tabellen aus, die in den Listen für Ihre Eingabedaten unterstützt werden.

Sie können die Basiseingabetabelle [sn_si_Incident] nicht ändern oder eine neue Datenquelle für Ihre Kopie der Kompetenz „Security Incident-Zusammenfassung“ hinzufügen.

h. Ändern Sie die bearbeitbaren Felder in der Vorlage „in Arbeit“ mit dem Bedingungsgenerator und den Filterbedingungen.

i. Fahren Sie mit dem nächsten Schritt in fort Geführtes Setup Für die Vorlage in Arbeit durch Auswahl von **Speichern und fortfahren** .

- **Passen Sie die Eingabeaufforderung an** : Bearbeiten Sie den Prompt, indem Sie die vordefinierten Abschnitte neu anordnen oder entfernen. Sie können den Prompt anhand eines Security Incident-Datensatzes für jede Eingabevorlagenkonfiguration überprüfen und testen.
- **Definieren Sie die Verfügbarkeit** :

Option	Beschreibung
Kompetenz ist immer verfügbar	Die Kompetenz ist für Anwender immer verfügbar.
Verfügbarkeit von Kompetenzen anpassen	Die Kompetenz ist nur verfügbar, wenn die Bedingungen erfüllt sind (Standard). Verwenden Sie den Bedingungsgenerator, um Ihre Bedingungen festzulegen.

- **Wählen Sie Anzeige aus** :

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Produktintern	Zusammenfassung von Security Incidents in allen Sicherheitsprodukten anzeigen. Now Assist Kompetenzen werden in Formularen und Arbeitsbereichen angezeigt.
Anwenderrollen	Wählen Sie das Erweiterungssymbol ( )
Now Assist-Bereich	Now Assist Kompetenzen sind in verfügbar Now Assist Bereich. **Hinweis:** Wenn diese Option nicht angezeigt wird, müssen Sie den Bereich Now Assist aktivieren. Weitere Informationen finden Sie unter Turn on the Now Assist panel .

j. Wählen Sie Aus **Speichern Sie die Vorlage** Um Ihre Änderungen an der Vorlage in Arbeit zu speichern.

k. Wählen Sie die Vorlage Überprüfen aus.

l. Ändern Sie die bearbeitbaren Felder in den Vorlagen „Überprüfen“ und „Geschlossen“ mit Filterbedingungen, wie in den vorherigen Schritten beschrieben.

m. Wählen Sie Aus **Speichern und fortfahren** Um mit dem nächsten Schritt in fortzufahren Geführtes Setup.

n. Wählen Sie Aus **Speichern Sie die Vorlage** Um Ihre Änderungen an einer Vorlage zu speichern.

o. Wählen Sie Aus **Überprüfen und aktivieren** Um Ihre Kompetenz zu überprüfen und zusätzliche Änderungen vorzunehmen.

4. Wählen Sie **Aktivieren**.
   Ihre Kompetenz wird auf der Seite „Security Incident“ im Abschnitt alle verfügbaren Security Incident-Kompetenzen angezeigt.
5. Wählen Sie Aus **Kompetenz aktivieren** .

Eingaben und Auslöser für Now Assist für Security Incident Response

Sie können einige der Eingaben oder Auslöser für eine generative KI-Kompetenz konfigurieren. Mit Eingaben oder Auslösern können Sie bestimmen, wie und wann eine Kompetenz verwendet wird.

Eingaben und Auslöser

Eingaben identifizieren die für eine Kompetenz verwendeten Daten. Eingaben umfassen die Tabelle und Felder, die zum Generieren einer Security Incident-Zusammenfassung verwendet werden. Ein Auslöser initiiert eine Aktion. Auslöser bestimmen beispielsweise, wann das System eine Zusammenfassung generiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Eingaben und Auslöser ändern, aber Sie können die Datenquelle einer Kompetenz nicht ändern. Die Datenquelle enthält die Tabellen und Felder, auf denen die Fähigkeit basiert.

Kompetenz „Security Incident-Zusammenfassung“

Eingaben für die Kompetenz „Security Incident-Zusammenfassung“ identifizieren die Tabelle und die Felder, die bei der Generierung einer Security Incident-Zusammenfassung verwendet werden. In der folgenden Tabelle sind die Eingaben für die Kompetenz „Security Incident-Zusammenfassung“ auf der Seite „Eingabe auswählen“ in aufgeführt Now Assist-Administrator Konsole.

Eingabe	Beschreibung
Datenquelle	Tabelle „Security Incident“ [sn_si_Incident].
Eingabefelder	• Kurzbeschreibung • Beschreibung • Status • Priorität • Arbeitsnotizen • Zusätzliche Anmerkungen
Zugehörige Eingabetabellen	• Betroffene CIs: Konfigurationselement • Betroffene Anwender: Anwender • Security Incident Response Aufgabe: Kurzbeschreibung • Status: Beliebiger anderer Status als **Abgebrochen** . • Zugeordnete erkennbare Elemente: Das Ergebnis erkennbarer Elemente ist böswillig oder verdächtig.

Kompetenz „Lösungshinweise generieren“

Eingaben für die Kompetenz „Lösungsnotizen generieren“ identifizieren die Tabelle und Felder, die verwendet werden, wenn die Lösungshinweise für einen Security Incident generiert werden. In der folgenden Tabelle sind die Eingaben für die Kompetenz „Generierung von Lösungshinweisen“ auf der Seite „Eingabe auswählen“ in aufgeführt Now Assist-Administrator Konsole.

Eingabe	Beschreibung
Datenquelle	Tabelle „Security Incident“ [sn_si_Incident].
Eingabefelder	• Kurzbeschreibung • Beschreibung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabe	Beschreibung
	• Arbeitsnotizen • Zusätzliche Anmerkungen

Kompetenz zur Generierung empfohlener Aktionen für Security Incidents

Eingabe	Beschreibung
Datenquelle	Tabelle „Security Incident“ [sn_si_Incident].

Kompetenz zur Generierung von Analysen nach Incidents

Eingabe	Beschreibung
Datenquelle	Tabelle „Security Incident“ [sn_si_Incident].

Kompetenz zur Generierung von Korrelationseinblicken

Ihre Korrelationseinblicke für einen Security Incident können Datensätze aus den folgenden Tabellen enthalten, Sie müssen jedoch über die Berechtigung zum Zugriff auf diese Tabellen und Datensätze verfügen.

Eingabe	Beschreibung
Datenquelle	Tabelle „Security Incident“ [sn_si_Incident]. Tabelle „Konfigurationselement“ [cmdb_ci]. Incident-Tabelle [Incident]. Tabelle „Change-Anforderung“ [Change_Request]. Tabelle „Problem“ [Problem]. Tabelle für angreifbares Element [sn_vul_vulnerable_item]. Ordnen Sie die Tabelle des erkennbaren Elements [sn_ti_observable] zu.

Verwenden Now Assist für Security Incident Response Zum Schließen von Security Incidents

Sicherheitsanalysten können Security Incidents mithilfe der von unterstützten generativen KI-Kompetenzen schnell aus ihrem Arbeitsfluss schließen Now Assist für Security Incident Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über Now Assist für Security Incident Response

Mit Kompetenzen der generativen KI mit Now Assist für Security Incident Response, Ihre Sicherheitsanalysten haben die Möglichkeit:

- Fassen Sie Security Incident-Details zusammen, und überprüfen Sie den Kontext schnell in einem präzisen, leicht lesbaren Format.
- Generieren Sie Abschlussnotizen (Lösungshinweise).
- Generieren Sie empfohlene Aktionen für einen Security Incident
- Generieren Sie Analysedaten nach Incident
- Generieren Sie Korrelationseinblicke, um die Incident-Untersuchung zu beschleunigen.

Sicherheitsmanager und -Analysten können Zusammenfassungen und Abschlussnotizen von Security Incidents an den folgenden Standorten anfordern:

- Security Incident-Datensätze
- Security Incident Response Arbeitsbereich
- Die Now Assist Bereich.

Hinweis:
Die empfohlenen Aktionen für Security Incidents und die Analysekompetenzen nach dem Incident sind nicht über verfügbar Now Assist Bereich.

Sicherheitsmanager und -Analysten können von den folgenden Standorten empfohlene nächste Schritte und Analysedaten nach Incident generieren:

- Security Incident-Datensätze
- Security Incident Response Arbeitsbereich

Sicherheitsmanager und -Analysten können Korrekturaufgaben aus generierten empfohlenen Aktionen nur aus Security Incidents in erstellen Security Incident Response Arbeitsbereich.

1. Fassen Sie einen Security Incident mit zusammen Now Assist für Security Incident Response

   Generieren Sie eine Zusammenfassung für einen Security Incident, die das zugrunde liegende Problem, Incident-Details, Daten zu zugehörigen Listen (erkennbare Elemente) und bereits ergriffene Schlüsselaktionen enthält.

2. Generieren Sie empfohlene Aktionen für einen Security Incident mit Now Assist für Security Incident Response
3. Generieren Sie mit eine Analyse nach dem Incident für einen Security Incident Now Assist für Security Incident Response
4. Generieren Sie Korrelationseinblicke in Now Assist Bereich mit Now Assist für Security Incident Response
5. Generieren Sie Abschlussnotizen für einen Security Incident mit Now Assist für Security Incident Response

   Generieren Sie automatisch die Abschlussnotizen für einen Security Incident.

6. Generative KI-Kompetenzen in anfordern Now Assist Bereich für Now Assist für Security Incident Response

   Generieren Sie Zusammenfassungen und Abschlussnotizen aus dem Now Assist Bereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die empfohlenen Aktionen für Security Incidents und die Analysekompetenzen nach dem Incident sind nicht über verfügbar Now Assist Bereich.

7. Now Assist für Security Incident Response-Kompetenzen anpassen

   Passen Sie die Eingabefelder einer Kompetenz an die Anforderungen Ihrer Umgebung an.

Fassen Sie einen Security Incident mit zusammen Now Assist für Security Incident Response

Verstehen Sie den Kontext eines Security Incidents mit der generativen KI-Kompetenz „Zusammenfassung von Security Incidents“.

Vorbereitungen

Sie können einen Security Incident in zusammenfassen veraltet Core-UI (UI16) und im Arbeitsbereich für Security Incident Response. Die Felder, die für die Eingabedaten verwendet werden, um einen Incident mithilfe generativer KI zusammenzufassen, müssen mindestens 50 Wörter enthalten. Weitere Informationen zu den Eingabefeldern finden Sie unter Eingaben und Auslöser für Now Assist für Security Incident Response.

Erforderliche Rollen: sn_si.Analyst, sn_si.Manager oder sn_si.Basic

Prozedur

1. In veraltet Core-UI, navigieren Sie zu **Alle** > **Security Incident** > **Incidents** Und öffnen Sie einen Security Incident, der Ihnen zugewiesen ist.
2. Alternativ navigieren Sie zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** Und öffnen Sie einen Security Incident, der Ihnen zugewiesen ist.
3. Auf der **Übersicht** Wählen Sie die Registerkarte aus **Zusammenfassen** .
   - Die generierte Zusammenfassung wird in einem Banner oben im Security Incident-Datensatz in angezeigt veraltet Core-UI16.
   - Die generierte Zusammenfassung wird auf angezeigt **Übersicht** Registerkarte in Arbeitsbereich für Security Incident Response.
4. **Wahlweise:** Wählen Sie aus den folgenden Optionen aus, nachdem die Zusammenfassung generiert wurde.

   (Optional) Von KI generierte Zusammenfassungen verfehlen möglicherweise wichtige Details. Möglicherweise möchten Sie die Zusammenfassung auf Richtigkeit und Vollständigkeit überprüfen, bevor Sie fortfahren.

Generieren Sie Abschlussnotizen für einen Security Incident mit Now Assist für Security Incident Response

Generiert automatisch einen Entwurf der Abschlussnotizen für einen Security Incident, wenn Sie ihn schließen. Der Entwurf kann bearbeitet werden und wird vor dem Schließen des Security Incident überprüft. Er kann nach Bedarf verwendet oder geändert werden. Abschlussnotizen enthalten Informationen zur Lösung eines Security Incidents für andere Analysten, Manager und wichtige Stakeholder.

Vorbereitungen

Erforderliche Rollen: sn_si.Analyst, sn_si.Manager oder sn_si.Basic

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

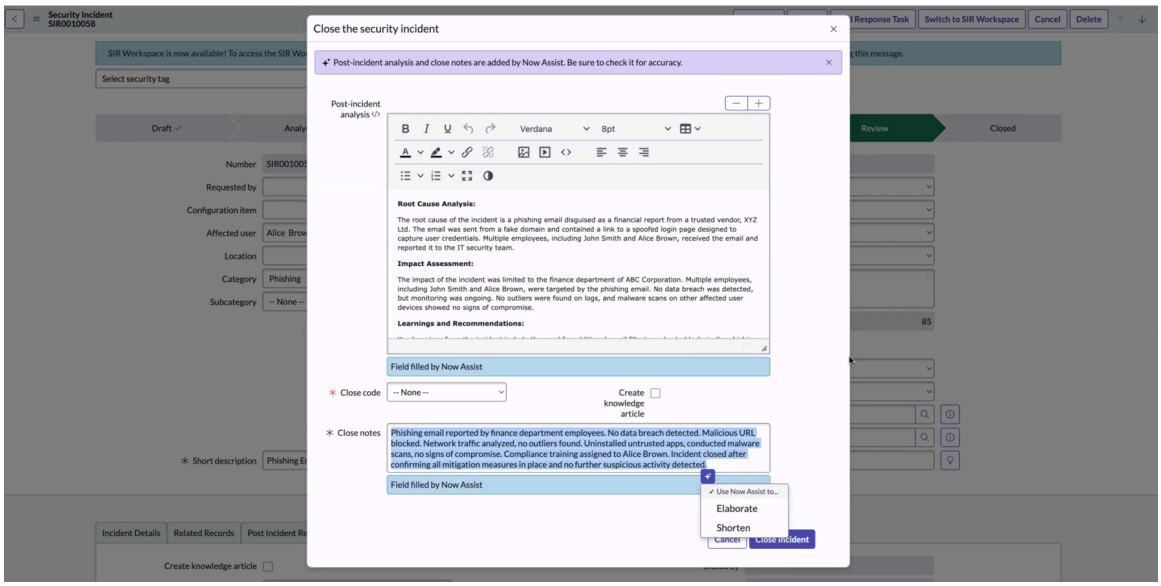
Hinweis:

Wenn die Felder „Abschlusscode“ oder „Abschlussnotizen“ für einen Security Incident bereits aktualisiert wurden, ändert Now Assist diese Felder unabhängig vom aktuellen Status des Incident nicht. Damit Now Assist diese Felder aktualisieren kann, stellen Sie sicher, dass sowohl die Felder „Abschlusscode“ als auch „Abschlussnotizen“ leer bleiben.

Prozedur

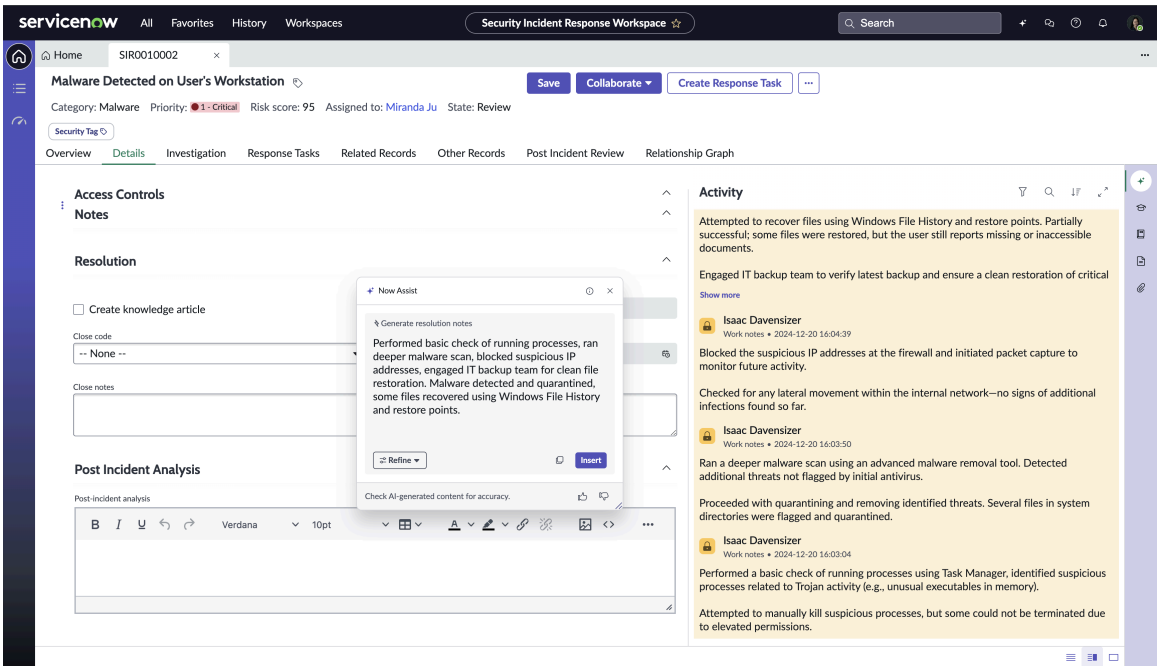
1. In veraltet Core-UI, navigieren Sie zu **Alle** > **Security Incident** > **Incidents** Und öffnen Sie einen Security Incident, der Ihnen zugewiesen ist.
2. Alternativ navigieren Sie zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** Und öffnen Sie einen Security Incident, der Ihnen zugewiesen ist.
3. Schließen Sie den Security Incident.

Der folgende Screenshot zeigt die Lösungshinweise, die für das Schließen des Security Incident in Core UI16 generiert wurden.

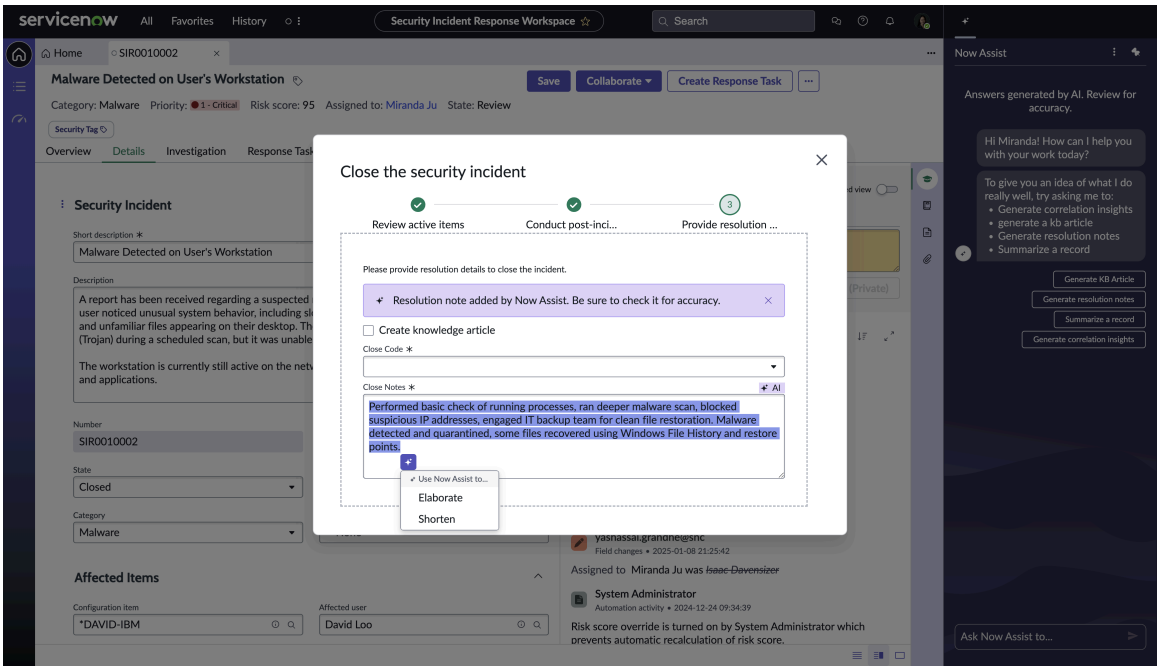


Automatisch generierte Lösungshinweise aus dem Security Incident Response-Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Bearbeiten Sie die Lösungshinweise, die über das Now Assist-Kontextmenü im Security Incident Response-Arbeitsbereich generiert wurden.



Automatische Übersetzung

Generieren Sie empfohlene Aktionen für einen Security Incident mit Now Assist für Security Incident Response

Generieren Sie automatisch die nächsten Schritte, die Ihre Analysten ausführen können, um ihnen beim Schließen eines Security Incidents im Security Incident Response-Arbeitsbereich zu helfen. Die empfohlenen Schritte basieren auf vorhandenen Security Incidents und Wissensartikeln.

Vorbereitungen

Empfohlene nächste Schritte funktionieren für aktive Security Incidents in einem anderen status als **Geschlossen** Oder **Abgebrochen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anwendung KI-Suche muss aktiviert sein, damit die Kompetenz empfohlene Aktionen für Security Incidents funktioniert. Um zu überprüfen, ob die KI-Suche in Ihrer Instanz aktiviert ist, navigieren Sie zu **Alle** > **KI-Suche** > **Status der KI-Suche**an. Wenden Sie sich an den Support, wenn auf der Seite angegeben wird, dass die KI-Suche nicht aktiviert ist.

Erforderliche Rollen: sn_si.Analyst, sn_si.Manager oder sn_si.Basic

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** Und öffnen Sie einen Security Incident, der Ihnen zugewiesen ist.
2. Wählen Sie aus **Empfohlene Aktionen** Symbol ( ) In der kontextbezogenen Sidebar.

3. Wählen Sie Aus **Rufen Sie Empfehlungen ab** .
4. Wählen Sie im modalen Dialogfeld „KI-generierte Inhalte überprüfen“ die Option aus **Ich bestätige** . Generierte empfohlene Aktionen werden auf Karten angezeigt. Oben werden bis zu vier Referenzen für die Aktionen angezeigt. Diese Referenzen können eine beliebige Kombination von Wissensartikeln (KB) oder Security Incidents (SIR#) sein.
5. Wählen Sie auf einer Karte eine aus.
6. **Wahlweise:** Wählen Sie im Bereich empfohlene Aktionen das Aktualisierungssymbol aus, um die empfohlenen Aktionen erneut zu generieren.

   Die empfohlenen Aktionen bleiben eine Stunde lang im Cache. Sie können die empfohlenen Schritte aktualisieren, wenn:

   - Sie glauben, dass sich die Informationen im Zusammenhang mit dem Security Incident seit dem letzten Generieren der Aktionen geändert haben.
   - Sie verlassen die Seite, melden sich ab, melden sich erneut an und kehren innerhalb einer Stunde zum Security Incident zurück.

   Sie müssen die Aktionen ab Schritt 3 erneut generieren, um sie nach einer Stunde anzuzeigen.
7. Wählen Sie Aus **Erstellen Sie eine Antwortaufgabe** Auf einer Karte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Arbeitsbereich wird eine neue Registerkarte geöffnet. Die **Kurzbeschreibung** Und **Beschreibung** Felder werden automatisch aus den Details auf der von Ihnen ausgewählten Karte „empfohlene Aktion“ ausgefüllt.

8. Bearbeiten Sie das Formular nach Bedarf, und wählen Sie aus **Speichern** Zum Erstellen der Antwortaufgabe.
   Bis Sie den Wert in der Systemeigenschaft ändern, bleiben die beiden Optionen für alle empfohlenen Aktionen, die Sie generieren, erhalten **Zeigen Sie Details an** Und **Erstellen Sie eine Antwortaufgabe** .

9. **Wahlweise:** Erstellen Sie eine Antwortaufgabe aus den empfohlenen Aktionen.
   Standardmäßig bietet Ihnen der Workflow die Möglichkeit, die empfohlenen Aktionen in Arbeitsnotizen von den Karten zu speichern. Wenn Sie die Möglichkeit haben möchten, eine Antwortaufgabe aus einer Aktionskarte zu erstellen, anstatt sie in Arbeitsnotizen zu speichern, müssen Sie das Feld Wert für ändern **Empfohlene SecOps-Aktion** [Systemeigenschaft sn_sec_ra.card_action_config].

   a. Navigieren Sie als Anwender mit der Rolle „Security Incident Manager“ [sn_si.Manager] zu sys_properties.LIST.

   b. Suchen Sie die Systemeigenschaft SecOps Recommended Action [sn_sec_ra.card_action_config], und öffnen Sie den Datensatz.

   c. Ändern Sie den Wert von Freigeben_zu_Arbeit_Notizen Bis Create_Task .

   d. Speichern Sie den Datensatz.

   e. Kehren Sie zum Security Incident-Datensatz zurück, und aktualisieren Sie die Seite.
      Die Aktionskarten bieten Ihnen die Optionen für **Zeigen Sie Details an** Und **Erstellen Sie eine Antwortaufgabe** .

Generieren Sie mit eine Analyse nach dem Incident für einen Security Incident Now Assist für Security Incident Response

Generieren Sie automatisch eine Analyse nach dem Incident für einen Security Incident, die eine Ursachenanalyse, eine Auswirkungsbewertung sowie Informationen zu Lerninhalten und Empfehlungen enthält.

Vorbereitungen

Sie müssen die Kompetenz „Analyse nach Incident“ aktiviert haben, wenn Sie eine Analyse nach Incident automatisch von generieren möchten Now Assist für Security Incident Response.

Wenn die Abschlussnotizen bereits vor dem Schließen des Security Incident manuell ausgefüllt wurden, wird dieser Inhalt nicht von überschrieben Now Assist für Security Incident Response Wenn Analysten das Feld Status auf festlegen **Geschlossen** .

Erforderliche Rollen: sn_si.Analyst, sn_si.Manager oder sn_si.Basic

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** Und öffnen Sie einen Security Incident, der Ihnen zugewiesen ist.

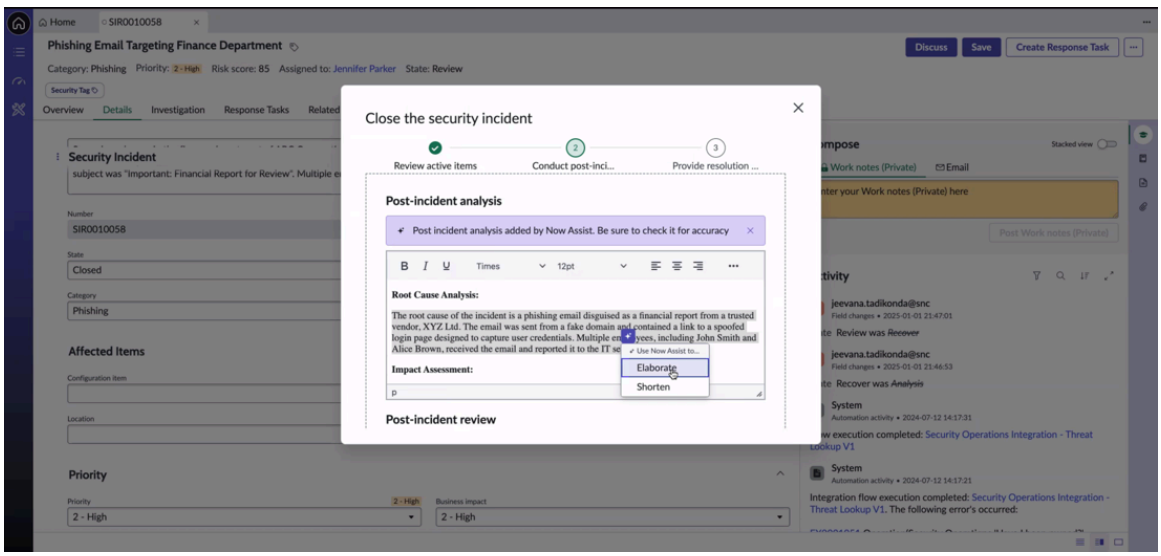
2. Auf der **Details** Wählen Sie die Registerkarte aus **Geschlossen** Im Feld Status, um den Security Incident zu schließen.
   Das Modal Security Incident schließen wird geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Wählen Sie Aus **Überprüfen Sie aktive Aufgaben** Dient zum Überprüfen aller aktiven Korrekturaufgaben, die diesem Incident zugeordnet sind.
   Eine neue Registerkarte mit Datensätzen zur Überprüfung wird geöffnet. Verwenden Sie diese Option, um sicherzustellen, dass Sie bereit sind, den Security Incident zu schließen, da diese Aktion alle zugehörigen Workflows und Aktivitäten abbricht und den Incident für alle zugehörigen Korrekturaufgaben schließt.
4. Um die Analyse nach dem Incident zu generieren, wählen Sie aus **Als Nächstes** .
   Die Analyse nach dem Incident wird im Modal mit drei Abschnitten angezeigt. Beachten Sie das Now Assist-Symbol ( ) Gibt an, dass der Inhalt von generiert wird Now Assist für Security Incident Response.
   - Ursachenanalyse
   - Auswirkungsbewertung
   - Erkenntnisse und Empfehlungen

   Hinweis:
   Sie können das Now Assist-Kontextmenü für alle Analyseoptionen nach Incident verwenden und die Ursachenanalyse/Auswirkungsbewertung/Lerninhalte und Empfehlungen ausarbeiten oder kürzen und den Text ersetzen. **Ausarbeiten** Hilft Ihnen, dem vorhandenen Text weitere Informationen hinzuzufügen. **Kürzen** Macht den ausgewählten Text prägnanter.

Der folgende Screenshot zeigt, wie das Now Assist-Kontextmenü verwendet wird, um den gewünschten Text für die Analyse nach Incident auszuarbeiten oder zu kürzen und zu ersetzen.



5. Überprüfen Sie den Bericht, um die Richtigkeit zu überprüfen, und nehmen Sie die erforderlichen Änderungen vor.
6. **Wahlweise:** Wählen Sie Aus **Nehmen Sie eine Bewertung vor** Und **Konfigurieren/Vorschau des Berichts** Dient zum Durchführen der Überprüfung nach dem Incident.
   Alle Änderungen, die Sie an der Überprüfung nach dem Incident vornehmen, werden eine Stunde lang beibehalten, wenn Sie diese Seite verlassen, um die Bewertung durchzuführen oder eine andere Aktion auszuführen. Nach einer Stunde müssen Sie den Status auf setzen **Geschlossen** Erneut für den Incident, um die Analyse nach dem Incident und Abschlussnotizen neu zu generieren.
7. Wählen Sie Aus **Als Nächstes** Um die Lösungshinweise zu generieren.
   Die Lösungshinweise werden im Feld Abschlussnotizen angezeigt.
8. Wählen Sie einen aus der Liste für den Abschlusscode aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wählen Sie Aus **Schließen Sie Den Incident** .
   Die Analyse nach dem Incident wird im Feld Analyse nach dem Incident auf der Registerkarte Details und auf der Registerkarte Übersicht zu Security Incidents im Security Incident Response Workspace gespeichert.

Korrelationseinblicke mit erkunden Now Assist für Security Incident Response

Sie können Korrelationseinblicke generieren, um zu vermeiden, dass Ihre Untersuchung betroffener Anwender, Konfigurationselemente und erkennbarer Elemente dupliziert wird, und Ihnen helfen, den Security Incident, an dem Sie arbeiten, schneller zu lösen. Sie wählen die Kriterien aus einem Security Incident aus, auf dem Sie die Korrelationseinblicke basieren möchten.

Korrelationseinblicke werden aus dem Security Incident Response-Arbeitsbereich generiert

Beginnend mit v 3.0.0 von Now Assist für Security Incident Response, Generieren und zeigen Sie Korrelationseinblicke an, und zeigen Sie die Ergebnisse in an Arbeitsbereich für Security Incident Response.

- Wenn Sie zuvor ein Konfigurationselement (Configuration Item, CI) oder einen betroffenen Anwender ausgewählt haben, auf dem Ihre Einblicke basieren sollen, hat die Suche den primären betroffenen Anwender oder das primäre CI zurückgegeben, das einem Security Incident zugeordnet ist. Beginnend mit V3.0.0 Der Service Desk-Mitarbeiter fragt Sie, mit welchem CI oder welchem betroffenen Anwender Sie den Security Incident aus den zugehörigen Listen korrelieren möchten.
- Sie können Korrelationseinblicke aus generieren **Untersuchung** Registerkarte für einen Security Incident in einem beliebigen Status in Arbeitsbereich für Security Incident Response.
- Sie können Einblicke für mehrere Elemente gleichzeitig für generieren **Zugeordnete Erkennbare Elemente** , **Konfigurationselemente** , Und **Betroffene Anwender** .
- Ergebnisse werden in einem Dialogfeld ohne Modus angezeigt, das Sie ändern und verschieben können.
- Ihr Zeitbereich für die Suche nach Korrelation beträgt 30 Tage.

Hinweis:
Nachdem Sie ein erkennbares Element generiert haben, das einem Security Incident zugeordnet ist, werden die Einblicke für dieses erkennbare Element gespeichert, bis Sie es mit einem anderen Zeitbereich erneut generieren. Ihre Einblicke für Ihren neuen Zeitbereich werden angezeigt.

Die Kompetenz zur Generierung von Korrelationseinblicken muss aktiviert sein, bevor Sie sehen können **Generieren Sie Korrelationseinblicke** Option in Arbeitsbereich für Security Incident Response. Weitere Informationen finden Sie unter Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Security Incident Response.

Korrelationseinblicke werden aus generiert Now Assist Bereich in Arbeitsbereich für Security Incident Response Und in UI (UI16)

Die Kompetenz zur Generierung von Korrelationseinblicken muss aktiviert sein, bevor Sie sehen können **Generieren Sie Korrelationseinblicke** Option in Now Assist Bereich.

Wenn Sie nicht sehen Now Assist Bereich müssen Sie ihn aktivieren. Weitere Informationen finden Sie unter Turn on the Now Assist panel .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können Korrelationseinblicke aus einem Security Incident-Datensatz in jedem Status in generieren Arbeitsbereich für Security Incident Response Oder in veraltet UI (UI16).
- Standardmäßig suchen Korrelationseinblicke nach übereinstimmenden Datensätzen aus den letzten 30 Tagen.
- Sie können Werte für suchen und überprüfen **Konfigurationselement** , **Betroffener Anwender** , Und **Erkennbare Elemente** Filter für Korrelationseinblicke in **Details** Registerkarte in Arbeitsbereich für Security Incident Response, Oder in den zugehörigen Listen Konfigurationselemente, Betroffene Anwender und erkennbare Elemente in veraltet UI (UI16).
- Ihre Suchkriterien und -Ergebnisse bleiben im angezeigt Now Assist Bereich, bis Sie die Konversation zurücksetzen. Um Ihre Konversation zurückzusetzen, wählen Sie aus Now Assist Symbol „weitere Optionen“ ( ) Im Bereich und wählen Sie aus **Konversation Zurücksetzen** .
- Sie müssen Zugriff auf die folgenden Tabellen haben, um diese Datensätze in den generierten Korrelationseinblicken anzuzeigen:
  - Tabelle „Konfigurationselement“ [cmdb_ci].
  - Incident-Tabelle [Incident].
  - Tabelle „Change-Anforderung“ [Change_Request].
  - Tabelle „Problem“ [Problem].
  - Tabelle für angreifbares Element [sn_vul_vulnerable_item].
  - Ordnen Sie die Tabelle des erkennbaren Elements [sn_ti_observable] zu.
- Ihre Ergebnisse für Korrelationseinblicke basieren auf den Tabellen, auf die Sie Zugriff haben. Wenn Sie beispielsweise angreifbare Elemente (VIT) in Ihren Ergebnissen von Korrelationseinblicken anzeigen möchten, müssen Sie über verfügen Vulnerability Response Anwendung installiert und die Lesezugriffsrolle (sn_vul.read_all).

Informationen zu den Schritten zum Generieren von Korrelationseinblicken finden Sie unter Generieren Sie Korrelationseinblicke in Now Assist Bereich mit Now Assist für Security Incident Response.

Generieren Sie Korrelationseinblicke aus dem Arbeitsbereich für Security Incident Response Mit Now Assist für Security Incident Response

Generieren und zeigen Sie Korrelationseinblicke in der an Arbeitsbereich für Security Incident Response Damit Sie vergangene Ereignisse mit dem Security Incident verknüpfen können, an dem Sie arbeiten.

Vorbereitungen

Erforderliche Rollen: sn_si.Analyst, sn_si.Manager oder sn_si.Basic

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** Und öffnen Sie einen Security Incident, der Ihnen zugewiesen ist.
2. Wählen Sie aus **Untersuchung** Registerkarte im Security Incident-Datensatz.
3. Wählen Sie mindestens einen Filter aus, auf dem Sie Ihre Korrelationseinblicke basieren möchten.

   Sie können mehr als ein erkennbares Element auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Zugeordnete Erkennbare Elemente** : Datensätze, die durch gemeinsam genutzte erkennbare Elemente verknüpft sind, die potenzielle laufende Angriffe oder die wiederholte Verwendung schädlicher Infrastruktur vermuten lassen. Beispiele können IP-Adressen, URLs oder Datei-Hashes sein.
- **Konfigurationselemente** (CI): Datensätze mit denselben CIs, damit Sie potenzielle Schwachstellen in bestimmten Systemen identifizieren können. Ein Beispiel sind Laptops von Anwendern.
- **Betroffene Anwender** : Frühere Incidents, die dieselben Anwender haben, damit Sie Muster wie häufige Phishing-Versuche oder mehrere nicht autorisierte Zugriffsversuche erkennen können. Ein Beispiel ist der Name eines bestimmten Anwenders.

Eine Liste übereinstimmender Elemente wird angezeigt.

4. Wählen Sie die Elemente aus der Liste aus, für die Sie Einblicke generieren möchten.
5. Wählen Sie Aus **Generieren Sie Einblicke** .
   Ein Dialogfeld wird geöffnet. Nach einigen Minuten werden Ihre Korrelationseinblicke angezeigt. In diesem Dialogfeld stehen Ihnen die folgenden Optionen zur Verfügung:
   - Einblicke aktualisieren ( ): Sie können die Elemente in der Liste ändern, nachdem Ihre ersten Einblicke generiert wurden, und Ihre Ergebnisse aktualisieren.
   - Erweitern Sie ( ) – Ändern Sie die Größe des Dialogfelds, und ziehen Sie es auf der Seite herum.

   Sie haben die folgenden Optionen für jeden Korrelationseinblick-Eintrag im Dialogfeld.

   - **Ändern Sie den Zeitbereich** – Wählen Sie einen Zeitbereich aus, um das Dialogfeld mit übereinstimmenden Einblicken neu zu laden. Ihre Ergebnisse für diesen Eintrag werden automatisch neu generiert, wenn Sie einen neuen Zeitbereich auswählen. Der Zeitbereich für jeden Eintrag wird neben dem Einblick angezeigt, z. B. 35.35.35.35. (100 Tage) .
   - Zuletzt generiert: Das Datum, an dem der Einblick zuletzt generiert wurde.
   - Inhalt bewerten – ( ) Und ( ).
   - Kopieren – ( ) Kopieren Sie den Einblick in die Zwischenablage.
   - **In Arbeitsnotizen freigeben** – Bearbeiten Sie den Inhalt, und veröffentlichen Sie ihn in den Arbeitsnotizen zum Security Incident.

   Korrelationseinblicke werden für erkennbare Elemente gespeichert, wenn Sie sie basierend auf dem Standardsuchzeitraum (30 Tage) zum ersten Mal generieren. Diese Einblicke werden gespeichert, bis Sie Einblicke für die erkennbaren Elemente mit einem anderen Suchzeitraum erneut generieren. Ändern Sie das 30-Tage-Limit für die Abfrage, indem Sie die folgenden Schritte ausführen:

   a. Navigieren Sie als Anwender mit der Rolle „Security Incident Manager“ [sn_si.Manager] zu sys_properties.LIST.

   b. Suchen Sie die Systemeigenschaft Korrelation-Suchzeitraum [sn_sec_gen_ai.correlation_Lookback_period], und öffnen Sie den Datensatz.

   c. Geben Sie eine Zahl in ein **Wert** Feld bis zu 360.

   d. Speichern Sie den Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Kehren Sie zum Security Incident-Datensatz zurück, und aktualisieren Sie die Seite.

f. Generieren Sie Korrelationseinblicke. Ihre Ergebnisse basieren auf Ihrem neuen Suchzeitraum.

Generieren Sie Korrelationseinblicke in Now Assist Bereich mit Now Assist für Security Incident Response

Generieren Sie Korrelationseinblicke aus dem Now Assist Bereich, mit dem Sie vergangene Ereignisse mit dem Security Incident verknüpfen können, an dem Sie arbeiten.

Vorbereitungen

Erforderliche Rollen: sn_si.Analyst, sn_si.Manager oder sn_si.Basic

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** Und öffnen Sie einen Security Incident, der Ihnen zugewiesen ist.
2. Alternativ dazu in veraltet UI (UI16), suchen Sie einen Security Incident in der Tabelle „Security Incidents“ [sn_si_Incident], und öffnen Sie ihn.
3. Wählen Sie aus Now Assist Symbol ( ) Im oberen Header, um zu öffnen Now Assist Bereich.
4. Wählen Sie Aus **Generieren Sie Korrelationseinblicke** .

   Korrelationseinblicke werden generiert, wenn mindestens einer der folgenden Werte abgeglichen werden kann. Die folgenden Filter, auf denen Ihre Einblicke basieren sollen, werden in angezeigt Now Assist Bereich. Nur die Filter, die Übereinstimmungen mit anderen Security Incidents aufweisen, werden angezeigt.

   Hinweis:
   Wenn Sie keinen Security Incident-Datensatz geöffnet haben, werden Sie aufgefordert, die Nummer für einen Security Incident-Datensatz einzugeben, nachdem Sie ausgewählt haben **Generieren Sie Korrelationseinblicke** .

   - **Konfigurationselement** (CI): Datensätze mit demselben CI, damit Sie potenzielle Schwachstellen in bestimmten Systemen identifizieren können. Ein Beispiel ist der Laptop eines Anwenders.
   - **Betroffener Anwender** : Frühere Incidents, die denselben Anwender haben, damit Sie Muster wie häufige Phishing-Versuche oder mehrere nicht autorisierte Zugriffsversuche erkennen können. Ein Beispiel ist der Name eines bestimmten Anwenders.
   - **Erkennbare Elemente** : Datensätze, die durch gemeinsam genutzte erkennbare Elemente verknüpft sind, die potenzielle laufende Angriffe oder die wiederholte Verwendung schädlicher Infrastruktur vermuten lassen. Beispiele können IP-Adressen, URLs oder Datei-Hashes sein. Sie müssen einen genauen Wert für ein erkennbares Element eingeben, z. B. einen vollständigen Datei-Hash.

   Wenn für einen dieser Filter keine übereinstimmenden Daten vorhanden sind, werden keine angezeigt. Sie werden aufgefordert, dem Security Incident, mit dem Sie arbeiten, einen dieser Werte hinzuzufügen, zu speichern, Ihre Konversation im Bereich zurückzusetzen und es erneut zu versuchen.

5. Setzen Sie Ihre Konversation zurück, indem Sie auswählen Now Assist Symbol für Menü „weitere Optionen“ ( ) Im Bereich und wählen Sie aus **Konversation Zurücksetzen** .
6. Wählen Sie einen Filter aus.

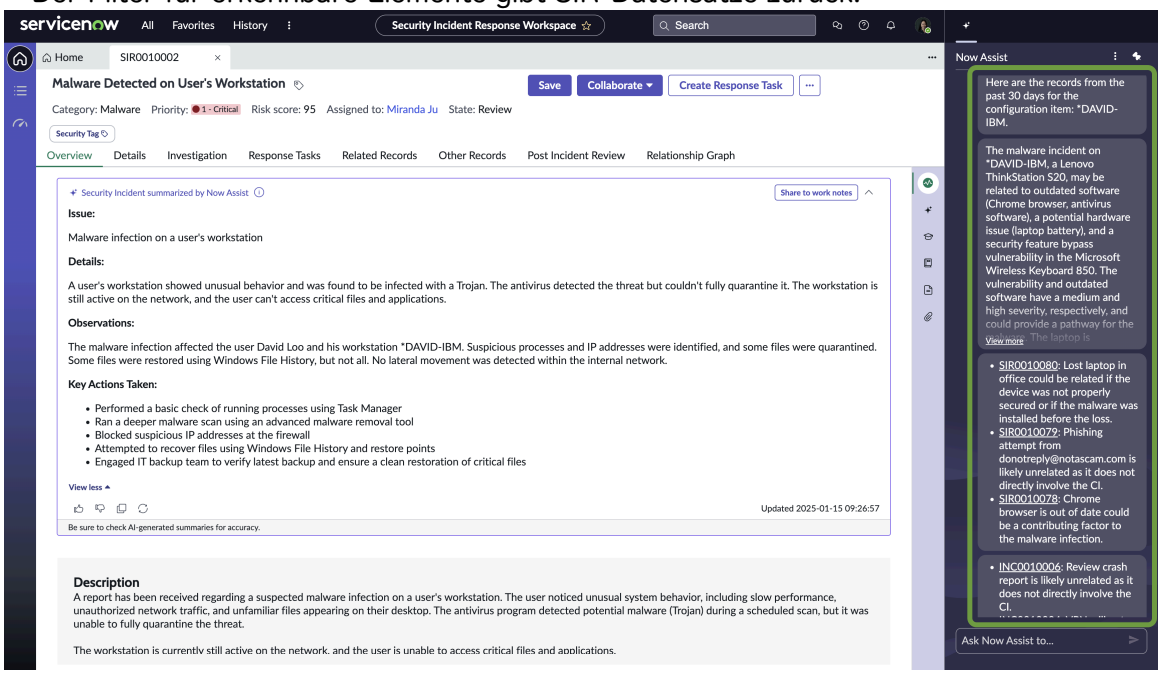
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übereinstimmende Ergebnisse werden in angezeigt Now Assist Bereich.

Im folgenden Beispiel: **Konfigurationselement** Wurde angefordert. Die Suche hat eine allgemeine Zusammenfassung zurückgegeben und Links zu Datensätzen mit einem übereinstimmenden Konfigurationselement enthält.

Die Ergebnisse sind nach Datensatztyp gruppiert: Security Incident-Datensatz (SIR), Incident (INC), Change Request (CHG), Problem (PRB) und angreifbares Element (VIT).

- Der Filter „Betroffene Anwender“ gibt Folgendes zurück: SIR-, INC- und CHG-Datensätze.
- Das Konfigurationsfilterelement gibt Folgendes zurück: SIR-, INC-, CHG-, PRB- und VIT-Datensätze.
- Der Filter für erkennbare Elemente gibt SIR-Datensätze zurück.



7. **Wahlweise:** Ändern Sie das 30-Tage-Limit für die Abfrage, indem Sie die folgenden Schritte ausführen:
   a. Navigieren Sie als Anwender mit der Rolle „Security Incident Manager“ [sn_si.Manager] zu sys_properties.LIST.
   b. Suchen Sie die Systemeigenschaft Korrelation-Suchzeitraum [sn_sec_gen_ai.correlation_Lookback_period], und öffnen Sie den Datensatz.
   c. Geben Sie eine Zahl in ein **Wert** Feld bis zu 360.
   d. Speichern Sie den Datensatz.
   e. Kehren Sie zum Security Incident-Datensatz zurück, und aktualisieren Sie die Seite.

Generative KI-Kompetenzen in anfordern Now Assist Bereich für Now Assist für Security Incident Response

Fordern Sie eine Security Incident-Zusammenfassung oder Abschlussnotizen von an Now Assist Bereich.

Vorbereitungen

Siehe Now Assist panel Zum Aktivieren von Now Assist Bereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rollen: si_Analyst, si_Manager oder sn_si.Basic

Prozedur

1. Melden Sie sich bei einer Instanz an, in der Now Assist für Security Incident Response Anwendung ist installiert.
2. In veraltet Core-UI, navigieren Sie zu **Alle** > **Security Incident** > **Incidents** Und öffnen Sie einen Security Incident, der Ihnen zugewiesen ist.
3. Alternativ navigieren Sie zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response** Und öffnen Sie einen Security Incident, der Ihnen zugewiesen ist.
4. Wählen Sie das Now Assist-Symbol ( ) Im oberen Banner.

Verwenden von agentischen KI-Workflows in Now Assist Für Security Incident Response

Verwenden Sie Security Incident Response KI-Agents , um Ihre Aufgaben autonom auszuführen.

Verfügbare agentische Workflows für KI-Agents für Security Incident Response

Name des Agentischen Workflows	Beschreibung	Verfügbare KI-Agents
Security Incident schließen	Dieser agentische Workflow hilft Sicherheitsanalysten, einen Security Incident in natürlicher Sprache zu schließen Now Assist Bereich.	Security Incident-Nachbearbeitungsgenerator
Analysieren von Metriken für Security Operations	Dieser agentische Workflow hilft Managern des Security Operations Center (SOC), die Leistung ihrer Sicherheitsanalysten zu analysieren. Metriken werden für die Antwort auf Security Incidents generiert (SIR) Datensätze für Fallvolumen, durchschnittliche Zeit bis zur Zuweisung (MTTA) und durchschnittliche Zeit bis zur Lösung (MTTR).	• KI-Agent für das Abrufen von Security Incidents • KI-Agent für die Analyse von Sicherheitsmetriken
Security Incident-Lösung	Dieser agentische Workflow hilft Sicherheitsanalysten, einen Lösungspfad für Security Incidents zu identifizieren. Dieser Workflow unterstützt die Sicherheitsanalysten auch beim Schließen eines Security Incidents mit natürlicher Sprache in Now Assist Bereich.	• KI-Agent für die Lösung von Security Incidents • KI-Agent zur Verwaltung von Exchange Online-Integrationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare agentische Workflows für KI-Agents für Security Incident Response (Fortsetzung)

Name des Agentischen Workflows	Beschreibung	Verfügbare KI-Agents
		• KI-Agent für das Generieren von Security Incident-Abschlüssen • KI-Agent für die Analyse erkennbarer Elemente • KI-Agent zur Verwaltung von Security-Incident-Aktivitäten
SIR-Schichtübergabebericht generieren	Dieser agentische Workflow fügt dem Schichtübergabebericht Details zu einem Security Incident hinzu. Der Service Desk-Mitarbeiter füllt die verschiedenen Abschnitte der Schichtübergabe mit dem entsprechenden Inhalt aus, indem er die relevanten Details aus dem Security Incident identifiziert.	Security Incident-Schichtübergabe – KI-Agent

Wichtig:
Standardmäßig sind alle agentischen Workflows und KI-Agent-Datensätze schreibgeschützt.

Um einen agentischen Workflow zu ändern, müssen Sie zuerst Duplicate an agentic workflow , Und fahren Sie dann mit den folgenden Schritten fort:

- Aktivieren Sie den Workflow.
- Aktivieren Sie alle KI-Agents im Workflow.
- Bei Bedarf können Sie einen Auslöser hinzufügen, um den Workflow automatisch aufzurufen.

Suchen Sie nach einem KI-Agenten?

- Möglicherweise sind KI-Agenten mit installiert Now Assist Anwendung, die nicht in Agenten-Workflows verwendet wird. Informationen zum Anzeigen aller in Ihrer Instanz verfügbaren Agenten finden Sie unter Suchen Sie KI-Agenten .
- Um Agenten zu finden, die möglicherweise nicht auf Ihrer Instanz installiert sind, besuchen Sie die KI-Agent-Marketplace Auf ServiceNow Store.

Security Incident Response KI-Agent-Sammlung – Agentischen Workflow zum Schließen von Security Incidents

Mit dem agentischen Workflow „Security Incident schließen“ können Sicherheitsanalysten einen Security Incident schließen.

Übersicht über den agentischen Security Incident-Workflow schließen

Brechen Sie mit dem agentischen Workflow „Security Incident schließen“ die zugehörigen Antwortaufgaben ab, generieren Sie Lösungshinweise, Abschlussnotizen, Abschlusscode

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und Post Incident Analysis (PIA) während des Abschlusses eines Security Incident, geben Sie Feedback, und passen Sie Inhalte in natürlicher Spracheaus dem an Now Assist Bereich.

Wenn Sie diesen agentischen Workflow ändern möchten, können Sie dies Duplikat Passen Sie die Einstellungen an Ihre spezifischen Anforderungen an, und aktivieren Sie stattdessen die duplizierte Version des agentischen Workflows.

Service Desk-Mitarbeiter, der im agentischen Workflow „Security Incident schließen“ verwendet wird

Der Experte für Security Incident-Nachbearbeitungsgenerator wird im agentischen Workflow „Security Incident schließen“ verwendet.

[store-future: BEGIN review]

Tools, die dem agentischen Workflow zum Schließen von Security Incidents zugeordnet sind

Die folgenden Tools sind einem KI-Agent zugeordnet, der im agentischen Workflow „Security Incident schließen“ verwendet wird.

Tools, die dem Schließen von Security Incidents zugeordnet sind

Tooltyp	Ausführungsmodus	Name	Beschreibung
Skripte	Autonom	Ruft Security Incident-Details ab	Tool zum Abrufen der Security Incident-Details von der Security Incident-Nummer.
Skripte	Autonom	Ruft Abschlusscodewerte ab	Tool zum Abrufen verfügbarer Abschlusscodewerte für den Security Incident.
Skripte	Autonom	Schließt den Security Incident als falsch positiv	Tool, das verwendet wird, wenn der Incident als falsch positiv geschlossen wird.
Skripte	Autonom	Aktualisiert den Security Incident	Tool zum Aktualisieren eines Felds des Security Incidents.
Subflow	Autonom	Generiert Abschlussnotizen	Tool zum Generieren von Abschlussnotizen für den Security Incident.
Subflow	Autonom	Generiert eine Analyse nach dem Incident	Tool zum Generieren einer Analyse nach dem Incident für den Security Incident.

[End]

[store-future: BEGIN review]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auslöser für den agentischen Workflow „Security Incident schließen“

Für diesen agentischen Workflow sind keine Auslöser vorhanden. Bei Bedarf können Sie einen Auslöser hinzufügen, um den agentischen Workflow automatisch aufzurufen.

[End]

Schließen Sie einen Security Incident

Chatten Sie mit einem KI-Agent in Now Assist Bereich, mit dem Sie einen Security Incident schließen können.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst oder sn_si.Manager

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie den Security Incident, den Sie mit dem KI-Agent schließen möchten.
3. Wählen Sie Now Assist ( )-Symbol.
   Die Now Assist Bereich wird angezeigt.
4. Schließen Sie den Security Incident mit einer der folgenden Optionen.

Security Incident Response KI-Agent-Sammlung – Agentischen Workflow zum Lösen von Security Incidents

Chatten Sie mit einem KI-Agent in Now Assist Bereich, mit dem Sie einen Lösungsplan für einen Security Incident erstellen und ihn lösen können.

Übersicht über den agentischen Workflow für Security Incidents lösen

Verwenden Sie den agentischen Workflow Security Incident lösen, um die Incident-Details abzurufen, Wissensartikel und ähnliche geschlossene Security Incidents abzurufen, einen Lösungsplan zu erhalten und den Security Incident zu lösen.

Wenn Sie diesen agentischen Workflow ändern möchten, können Sie dies Duplikat Passen Sie die Einstellungen an Ihre spezifischen Anforderungen an, und aktivieren Sie stattdessen die duplizierte Version des agentischen Workflows.

Service Desk-Mitarbeiter, die im agentischen Workflow „Security Incident lösen“ verwendet werden

Der agentische Workflow Security Incident lösen enthält die folgenden Service Desk-Mitarbeiter:

- KI-Agent für die Lösung von Security Incidents
- KI-Agent zur Verwaltung von Exchange Online-Integrationen
- KI-Agent für das Generieren von Security Incident-Abschlüssen
- KI-Agent für die Analyse erkennbarer Elemente
- KI-Agent zur Verwaltung von Security-Incident-Aktivitäten

[store-future: BEGIN review]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tools, die dem KI-Agent des Generators „Plan für Security Incidents lösen“ zugeordnet sind

Alle Tools sind vom Skripttyp.

Tools, die dem KI-Agent des Generators „Plan für Security Incidents lösen“ zugeordnet sind

Name	Ausführungsmodus	Beschreibung
Security Incident-Details abrufen	Autonom	Ruft die Security Incident-Details aus der Security Incident-Nummer ab.
Rufen Sie Wissen und ähnliche Incidents ab	Autonom	Ruft relevante Wissensartikel und ähnliche geschlossene Security Incidents mit einer Suchabfrage ab.

[End]

[store-future: BEGIN review]

Tools, die dem KI-Agent des Security Incident-Nachbearbeitungsgenerators zugeordnet sind

Tools, die dem Nachbearbeitungsgenerator für Security Incidents zugeordnet sind

Tooltyp	Ausführungsmodus	Name	Beschreibung
Skripte	Autonom	Ruft Security Incident-Details ab	Ruft die Security Incident-Details aus der Security Incident-Nummer ab.
Skripte	Autonom	Ruft Abschlusscodewerte ab	Tool zum Abrufen verfügbarer Abschlusscodewerte für den Security Incident.
Skripte	Autonom	Schließt den Security Incident als falsch positiv	Tool, das verwendet wird, wenn der Incident als falsch positiv geschlossen wird.
Skripte	Autonom	Aktualisiert den Security Incident	Aktualisiert ein Feld des Security Incidents.
Subflow	Autonom	Generiert Abschlussnotizen	Generiert Abschlussnotizen für den Security Incident.
Subflow	Autonom	Generiert eine Analyse nach Incident	Generiert eine Analyse nach dem Incident für den Security Incident.

[End]

[store-future: BEGIN review]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tools, die dem KI-Agent der Analyse erkennbarer Elemente für Security Incidents zugeordnet sind

Alle Tools sind vom Skripttyp.

Tools, die dem KI-Agent der Analyse erkennbarer Elemente für Security Incidents zugeordnet sind

Name	Ausführungsmodus	Beschreibung
Ruft die Ergebnisse der Fähigkeitsausführung ab	Autonom	Ruft die Bedrohungssuche ab und stellt Ergebnisse zur Ergänzung erkennbarer Elemente bereit.
Bedrohungssuche ausführen	Autonom	Führt eine Bedrohungssuche für erkennbare Elemente durch.
Ergänzung erkennbarer Elemente ausführen	Autonom	Ruft zusätzlichen Kontext im Zusammenhang mit den erkennbaren Elementen ab.
Erkennbares Element abrufen, das dem Security Incident zugeordnet ist	Autonom	Ruft erkennbare Elemente ab, die einem Security Incident zugeordnet sind.

[End]

[store-future: BEGIN review]

Tools, die dem KI-Agent des Security Incident Core Activities-Handlers zugeordnet sind

Alle Tools sind vom Skripttyp.

Tools, die dem KI-Agent des Security Incident Core Activities Handlers zugeordnet sind

Name	Ausführungsmodus	Beschreibung
Incident-Status aktualisieren	Autonom	Aktualisiert das Statusfeld eines Security Incidents.
E-Mail senden	Autonom	Sendet E-Mails.
Zugehörigen Datensatz erstellen	Autonom	Erstellt Incidents, Probleme, Change-Anforderungen oder Antwortaufgaben. Die Eingabeparameter „Short_description“, „description“, „Security_Incident_sys_ID“ sind zum Aufrufen dieses Tools obligatorisch.

[End]

[store-future: BEGIN review]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auslöser für den agentischen Workflow „Security Incident lösen“

Für diesen Anwendungsfall sind keine Auslöser vorhanden. Bei Bedarf können Sie einen Auslöser hinzufügen, um den Anwendungsfall automatisch aufzurufen.

[End]

Lösen Sie einen Security Incident

Chatten Sie mit einem KI-Agent in Now Assist Bereich zum Lösen eines Incident.

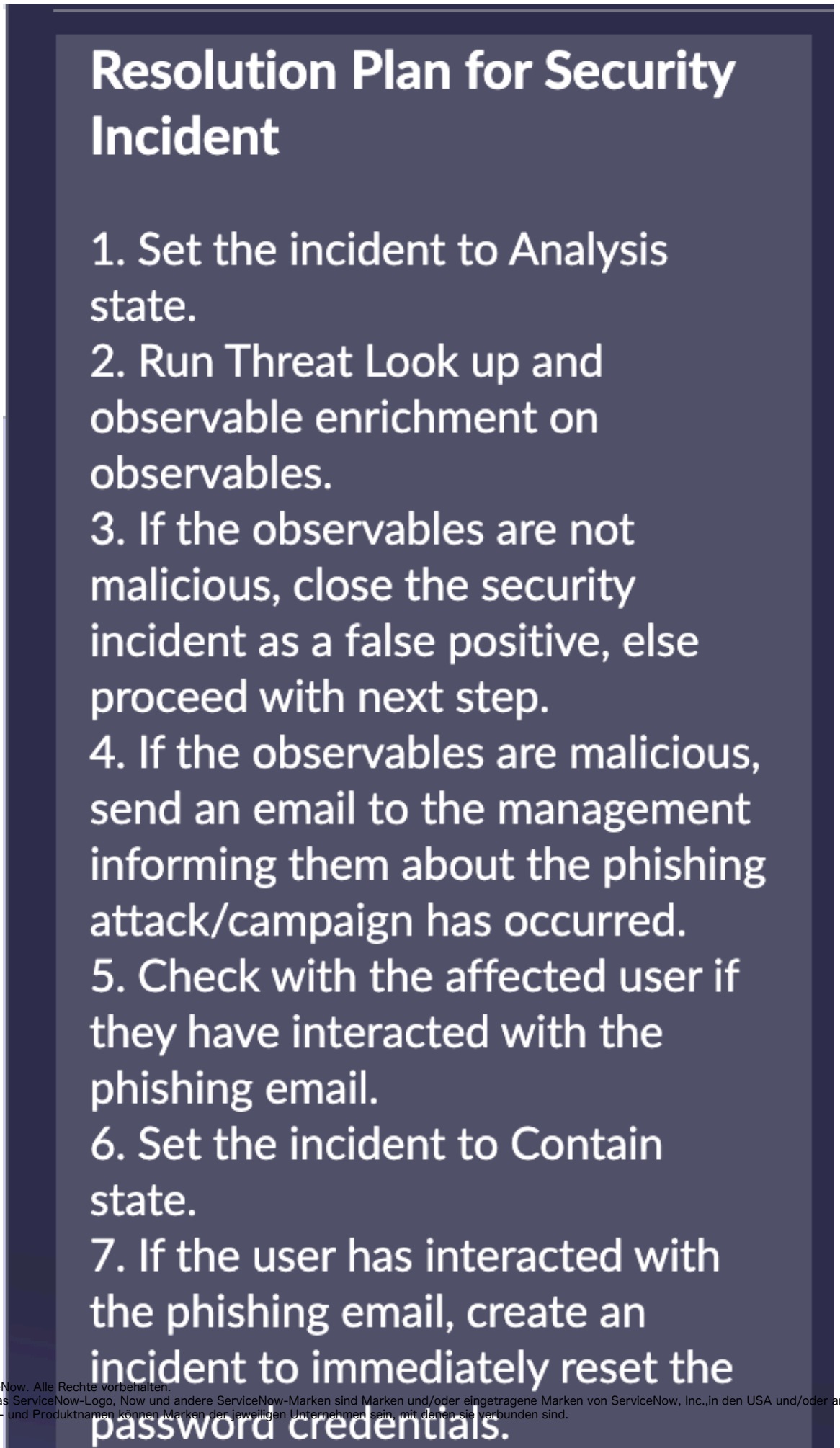
Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie den Security Incident, den Sie mit dem KI-Agent lösen möchten.
3. Wählen Sie aus Now Assist( )-Symbol.
   Der agentische Workflow „Security Incident lösen“ ist bei Bedarf verfügbar. Sie können eine Abfrage in natürlicher Sprache eingeben, um einen Security Incident mithilfe dieses agentischen Workflows zu lösen.
4. Auf der Now Assist Bitten Sie den Service Desk-Mitarbeiter, den Security Incident durch Betreten zu lösen Lösen Sie diesen Incident , Lösen Sie diesen Security Incident , Oder Lösen Sie den Security Incident: SIR0012345 .
   Die Now Assist Der Bereich enthält alle Aktionen, die Sie für den Security Incident ausführen können.
5. Wählen Sie Aus **Lösen Sie Security Incident** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der KI-Agent analysiert den Security Incident und stellt eine Zusammenfassung des Incident und seines aktuellen Status bereit. Darüber hinaus stellt der KI-Agent mithilfe der Incident-Details, Wissensartikel und ähnlicher geschlossener Security Incidents einen Lösungsplan bereit.

6. Geben Sie positive Antworten ein, z. B. `Sieht gut aus` Oder `Ok` Wenn Sie dem Lösungsplan zustimmen. Um eine positive Antwort zu erhalten, untersucht der KI-Agent jeden Schritt im Lösungsplan und unterstützt den Analysten (den Anwender mit der Rolle „sn_si.Analyst“) bei der Lösung. Für jeden Schritt stellt der KI-Agent Feedback bereit und fordert den Analyst auf, einzugreifen. Wenn der KI-Agent beispielsweise den für eine Phishing-E-Mail generierten Incident identifiziert, erfolgt der folgende agentische Workflow:

Agentic-Workflow zur Lösung eines Phishing-E-Mail-Incidents

Aufgaben zum Lösen eines Security Incidents	Beschreibung
Aktualisieren Sie den Status des Security Incidents	Der KI-Agent aktualisiert den Status des Security Incidents. Wenn der Status des Security Incidents beispielsweise Entwurf ist, aktualisiert der KI-Agent ihn auf Analyse.
Bedrohungssuche und Ergänzung erkennbarer Elemente für erkennbares Element ausführen	Der KI-Agent initiiert einen Prozess zur Bedrohungssuche und Ergänzung erkennbarer Elemente. Wenn der Analyst mit einer positiven Eingabe bestätigt, stellt der KI-Agent die Zusammenfassung der Analyse und Ergänzung erkennbarer Elemente bereit.
Senden Sie für schädliche erkennbare Elemente eine E-Mail an die Verwaltung	Der Analyst kann den KI-Agent bitten, eine E-Mail an das Management zu senden. Der KI-Agent stellt einen E-Mail-Entwurf bereit und fragt nach den Empfängern der E-Mail. **Hinweis:** Der Analyst kann die gesendete E-Mail in überprüfen **Andere Datensätze** Registerkarte.
Überprüfen Sie mit dem betroffenen Anwender, ob er mit der Phishing-E-Mail interagiert hat	Der Analyst überprüft manuell mit dem betroffenen Anwender, ob er mit der Phishing-E-Mail interagiert hat.
Wenn der Anwender mit der Phishing-E-Mail interagiert hat, setzen Sie seine Anmeldeinformationen für das Passwort zurück	Wenn der betroffene Anwender mit der Phishing-E-Mail interagiert hat, kann der Analyst den KI-Agent bitten, einen Incident zu erstellen, um das Anwenderpasswort zurückzusetzen. Der KI-Agent stellt eine Zusammenfassung für den Incident bereit und erstellt einen Incident, wenn der Analyst die Zusammenfassung genehmigt.
Blockieren Sie den Absender/die E-Mail/die URL im E-Mail-Gateway	Der KI-Agent fordert den Analysten auf, dass Absender/E-Mail/URL im E-Mail-Gateway blockiert werden. Der Analyst kann den KI-Agent bitten, eine Antwortaufgabe zum Blockieren von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgaben zum Lösen eines Security Incidents	Beschreibung
	Absender/E-Mail/URL im E-Mail-Gateway zu erstellen. Der KI-Agent stellt die Informationen für die Antwortaufgaben bereit und erstellt eine Antwortaufgabe, nachdem der Analyst sie genehmigt hat. **Hinweis:** Der Analyst kann die Antwortaufgabe abschließen und die Antwortaufgabe als markieren **Abgeschlossen** Auf der **Antwortaufgaben** Registerkarte. Der Analyst bestätigt dem KI-Agent, dass die Antwortaufgabe abgeschlossen ist.
Suchen und löschen Sie die Phishing-E-Mail aus allen Anwendereingängen	Der KI-Agent informiert den Analysten, die Phishing-E-Mail aus allen Anwendereingängen zu löschen. Der Analyst löscht die Phishing-E-Mail und bestätigt dem KI-Agent.
Registrieren Sie den betroffenen Anwender für ein obligatorisches Phishing-Training	Wenn der betroffene Anwender mit der Phishing-E-Mail interagiert hat, informiert der KI-Agent den Analysten, den betroffenen Anwender für das obligatorische Phishing-Training zu registrieren.
Führen Sie das Audit des Security Incidents durch	Der KI-Agent führt das Audit des Security Incidents durch und stellt die Zusammenfassung bereit.
Security Incident schließen	Der KI-Agent schließt den Incident. Weitere Informationen finden Sie unter Schließen Sie einen Security Incident.

Security Incident Response KI-Agent-Sammlung für den agentischen Workflow „Sicherheitsvorgangsmetriken analysieren“

Der agentische Workflow „Metriken für Sicherheitsvorgänge analysieren“ hilft Managern von Sicherheitsvorgängen, die Leistung ihrer Sicherheitsteams zu analysieren.

Übersicht über den agentischen Workflow „Metriken für Sicherheitsvorgänge analysieren“

Manager des Security Operations Center (SOC) können Metriken für das Gesamtfallvolumen, die durchschnittliche Zeit bis zur Zuweisung (MTTA) und die durchschnittliche Zeit bis zur Lösung (MTTR) für die Reaktion auf Security Incidents (SIR) Datensätze, um ihnen Einblicke in die Leistung ihrer Sicherheitsanalysten zu geben. Sie können auch Empfehlungen zur Verbesserung der Metriken einholen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agents, die im agentischen Workflow „Metriken für Sicherheitsvorgänge analysieren“ verwendet werden

- KI-Agent für das Abrufen von Security Incidents
- KI-Agent für die Analyse von Sicherheitsmetriken

Tools, die dem agentischen Workflow „Metriken für Sicherheitsvorgänge analysieren“ zugeordnet sind

Die folgenden Tools sind den KI-Agents zugeordnet, die im agentischen Workflow „Metriken für Sicherheitsvorgänge analysieren“ verwendet werden.

Tooltyp	Ausführungsmodus	Name	Beschreibung
Skript	Autonom	Suchen Sie nach Security Incidents	Dieses Tool ruft das Skript mit der richtigen Eingabe aus der Abfrage des Anwenders auf, um die Security Incidents aus der Datenbank abzurufen.
Skript	Autonom	Analyse	Stellt weitere Analysen für einen angegebenen Metriktyp bereit, Analyst , Gruppe , Startdatum , Enddatum , Zu SOC-Leistung.
Skript	Autonom	Berechnung	Berechnet Leistungsmetriken für SOC-Manager, z. B. Mean Time to Resolve (MTTR) und Mean Time to Assignment (MTTA).
Skript	Autonom	Empfehlen	Empfiehlt Verwaltungsaktionen, die basierend auf einer Analyse einer Metrik ausgeführt werden können.

Auslöser für den agentischen Workflow „Metriken für Sicherheitsvorgänge analysieren“

Für diesen Anwendungsfall sind keine Auslöser vorhanden. Bei Bedarf können Sie einen Auslöser hinzufügen, um den Anwendungsfall automatisch aufzurufen.

Analysieren Sie den agentischen Workflow für Sicherheitsvorgangsmetriken

Chatten Sie mit einem KI-Agent von Now Assist Bereich, der Ihnen hilft, Einblicke in die Effizienz Ihrer Sicherheitsanalysten bei der Lösung von Security Incidents zu erhalten.

Vorbereitungen
Sie müssen aktivieren Now Assist Kompetenz zur Analyse von Sicherheitsvorgangsmetriken, bevor Sie die KI-Agents mit dem agentischen Workflow „Sicherheitsvorgangsmetriken

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

analysieren“ verwenden können. Weitere Informationen finden Sie unter Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Security Incident Response.

Erforderliche Rolle: sn_si.Manager

Prozedur

1. Wählen Sie aus Now Assist Symbol ( ) Von beliebiger Stelle in Ihrer Instanz.
   Die Now Assist Bereich wird angezeigt.
2. Wählen Sie Aus **Analysieren Sie Security Operations-Metriken** In Now Assist Bereich.
3. Wählen Sie bei der Eingabeaufforderung aus **Analysieren Sie Security Incident-Metriken** .

   Der agentische Workflow-Fall „Metriken für Sicherheitsvorgänge analysieren“ ist bei Bedarf. Sie können jede Abfrage in natürlicher Sprache eingeben. Sie können jedoch die in der folgenden Tabelle beschriebenen Eingabeaufforderungen und Schritte verwenden, um sich mit den verfügbaren Metrikdaten und den Möglichkeiten vertraut zu machen.

Ihre Anforderung oder Antwort	Beschreibung
Geben Sie einen Namen für eine Ihrer Sicherheitsanalystengruppen ein, und fordern Sie Metriken an, z. B.: ○ **Analysieren Sie Metriken für Sicherheitsvorgänge für das L1-Analystenteam.** ○ **Sicherheitsmetriken für das L1-Analystenteam für die letzten sechs Monate.** ○ **Wie hat das L1-Analystenteam letzten Monat abgeschnitten?**	Geben Sie ein Team anhand des Namens und einen Zeitraum an.
Beenden Sie die Sitzung , Oder **Anhalten** .	Beenden Sie die Konversation.

   Möglicherweise bevorzugen Sie die Security Incident Response Der Arbeitsbereich wird auf einer anderen Registerkarte geöffnet, damit Sie auf Zuweisungsgruppen, Daten und andere Informationen für Ihre Eingabeaufforderungen verweisen können.

   Ihre Konversation wird gespeichert, bis Sie einen neuen Chat starten. Um einen neuen Chat zu starten, wählen Sie das Symbol „neuer Chat“ ( ).

   Ihre Anforderung wird wiederholt und in hervorgehobenem Text mit weiteren Informationen angezeigt.

   Nach einigen Minuten werden Sie aufgefordert, weitere Informationen zu einem bestimmten Analysten oder einer Analystengruppe bereitzustellen.
4. Geben Sie einen Zuweisungsgruppennamen ein, z. B. **L1-Analystenteam** .
5. Geben Sie an der Eingabeaufforderung einen Zeitbereich ein, z. B. **Die letzten sechs Monate** .
   Die Ergebnisse für Mean Time to Resolve (MTTR), Mean Time to Assignment (MTTA) und die Gesamtzahl der Security Incidents, die Ihr Team bearbeitet hat, werden angezeigt. Klicken Sie auf den Link, um weitere Informationen zu erhalten. Eine neue Registerkarte wird mit einer Liste in UI16 geöffnet.
6. Erweitern Sie **Quellen** Listen Sie auf, und wählen Sie aus **Security Incident-Liste** Link.
   Eine Liste der Security Incidents, die der L1-Analystengruppe zugewiesen sind, wird auf einer neuen Registerkarte in UI 16 angezeigt. Oben in der Liste der von Ihnen angeforderte Datumsbereich (**6 Monate**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

) Wird im folgenden Format angezeigt: Geöffnet > = 2024-09-23 > Geöffnet < = 2025 23-03-23 . Sie werden aufgefordert, eine detailliertere Analyse für MTTR, MTTA oder Fallvolumen anzuzeigen.

In dieser Liste können Sie einen Link auswählen, um einzelne Security Incidents zur Überprüfung zu öffnen. Sie können eine Datensatznummer aus der Liste im Chat eingeben, die der KI-Agent zusammenfassen soll.

7. Kehren Sie zum Chat zurück, und geben Sie Ihre Anforderung für eine Leistungsmetrik in natürlicher Sprache ein, z. B. Ja, tauchen Sie tiefer in MTTR ein.
   Für Ihre Anforderung werden weitere Informationen bereitgestellt, die eine Zusammenfassung und Daten enthalten, die in Abschnitten für Felder zum Security Incident organisiert sind.
   - Kategorieanalyse: Aufgliederung nach Kategorie. Beispiele Nicht Autorisierter Zugriff , Nicht Gepatchte Schwachstelle , Falsch Positiv , Und so weiter.
   - Prioritätsanalyse – Aufgliederung nach Schweregrad: Kritisch, hoch, Mittel.
   - Teamanalyse: Aufgliederung von MTTR nach einzelnen Teammitgliedern.
   - Ausreißer-Analyse: Aufgliederung von Security Incidents mit ungewöhnlich hohen, niedrigen oder anderen eindeutigen Werten.
8. Geben Sie bei der Aufforderung eine positive Antwort auf die Anforderung von Verbesserungsvorschlägen ein.
   Ihre Vorschläge werden angezeigt. Basierend auf den Ergebnissen der Bewertung möchten Sie möglicherweise weitere Informationen zu bestimmten Arten von Security Incidents suchen.
9. Fordern Sie bei der Aufforderung beispielsweise alle Security Incidents in der Phishing-Kategorie, die sich im Status befinden, in natürlicher Sprache an **Analyse** .
10. Wählen Sie aus **Zeigen Sie Ergebnisse an** Link.
    Eine Liste der Security Incidents, die Ihrer Anforderung entsprechen, wird auf einer neuen Registerkarte in UI16 bereitgestellt.

    In dieser Liste können Sie einzelne Incidents öffnen und Zusammenfassungen vom KI-Agent anfordern.
11. **Wahlweise:** Ändern Sie die Systemeigenschaften für die Quellfelder, die für die Metrikanalyse verwendet werden, und den Wert für den Ausreißfaktor.
    - sn_sec_gen_ai.aia_metric_Analysis_dimensions: Der KI-Agent teilt die Analyse bei der Analyse von MTTR- und MTTA-Metriken basierend auf den folgenden Feldern auf: **Kategorie** , **Priorität** , **CLOSE_Code** , **Assigned_to** , **Alert_Sensor** . Benutzer mit den Rollen sn_si.Manager und sn_si.admin können diese Liste ändern.
    - sn_sec_gen_ai.aia_metric_Analysis_Outlier_factor: Diese Eigenschaft bestimmt den Ausreißer-Faktor für MTTR und MTTA. Der Standardausreißer ist 2. Standardmäßig ist ein Datensatz ein Ausreißer, wenn seine MTTR das 2-fache der durchschnittlichen Zeit überschreitet, die eine Zuweisungsgruppe benötigt, um Security Incidents für den von Ihnen angeforderten Zeitraum zu lösen. Benutzer mit den Rollen sn_si.Manager und sn_si.admin können diesen Wert ändern.

SIR-Schichtübergabebericht generieren

Chatten Sie mit einem KI-Agent in Now Assist Bereich, um den agentischen Workflow SIR-Schichtübergabebericht generieren zu verwenden, mit dem Sie einem Schichtübergabebericht die Details eines Security Incidents hinzufügen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über den SIR-Schichtübergabebericht generieren

Verwenden Sie den agentischen Workflow SIR-Schichtübergabebericht generieren, um dem Schichtübergabebericht Details zum Security Incident hinzuzufügen. Der Service Desk-Mitarbeiter füllt die verschiedenen Abschnitte der Schichtübergabe mit dem entsprechenden Inhalt aus, indem er die relevanten Details aus dem Security Incident identifiziert.

Der KI-Agent identifiziert, ob der Analyst Zugriff auf einen Schichtübergabedatensatz hat, generiert Inhalte aus den Security Incident-Details für jeden Abschnitt des Schichtübergabeberichts. Der Analyst kann Feedback zum Inhalt geben, und der KI-Agent generiert den aktualisierten Inhalt und speichert den Inhalt im Schichtübergabebericht, wenn der Analyst genehmigt.

Wenn Sie diesen agentischen Workflow ändern möchten, können Sie dies Duplikat Passen Sie die Einstellungen an Ihre spezifischen Anforderungen an, und aktivieren Sie stattdessen die duplizierte Version des agentischen Workflows.

Service Desk-Mitarbeiter, die in der Übersicht „SIR-Schichtübergabebericht generieren“ verwendet werden

Der agentische Workflow SIR-Schichtübergabebericht generieren enthält die folgenden Service Desk-Mitarbeiter: Security Incident Shift Handover KI Agent.

Fügen Sie dem Schichtübergabebericht Security Incident hinzu

Chatten Sie mit einem KI-Agent in Now Assist Bereich zum Hinzufügen von Security Incident-Details zu einem Schichtübergabebericht.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie den Security Incident, den Sie einem Schichtübergabebericht mit dem KI-Agent hinzufügen möchten.
3. Wählen Sie aus Now Assist( )-Symbol.
   Der agentische Workflow „SIR-Schichtübergabebericht generieren“ ist bei Bedarf verfügbar. Sie können eine Abfrage in natürlicher Sprache eingeben, um einem Schichtübergabebericht einen Security Incident hinzuzufügen.
4. Auf der Now Assist Bitten Sie den Service Desk-Mitarbeiter, einem Schichtübergabebericht einen Security Incident hinzuzufügen Fügen Sie diesen Security Incident der Schichtübergabe hinzu , Oder Fügen Sie diesen Incident der Schichtübergabe hinzu: SIR0012345 Und drücken Sie die Eingabetaste.
   Die Now Assist Bereich löst den Workflow „Security Incident für Schichtübergabe hinzufügen“ aus. Dieser Workflow ruft Details zum Security Incident ab.

   Der KI-Agent findet den Datensatz der Schichtübergabe in Bearbeitung, auf den der Analyst Zugriff hat, und fügt ihm die Security Incident-Details hinzu. Wenn mehrere laufende Schichtübergabedatensätze vorhanden sind, auf die der Analyst Zugriff hat, listet der KI-Agent die fünf häufigsten Schichtübergabedatensätze auf, die der Analyst auswählen kann.

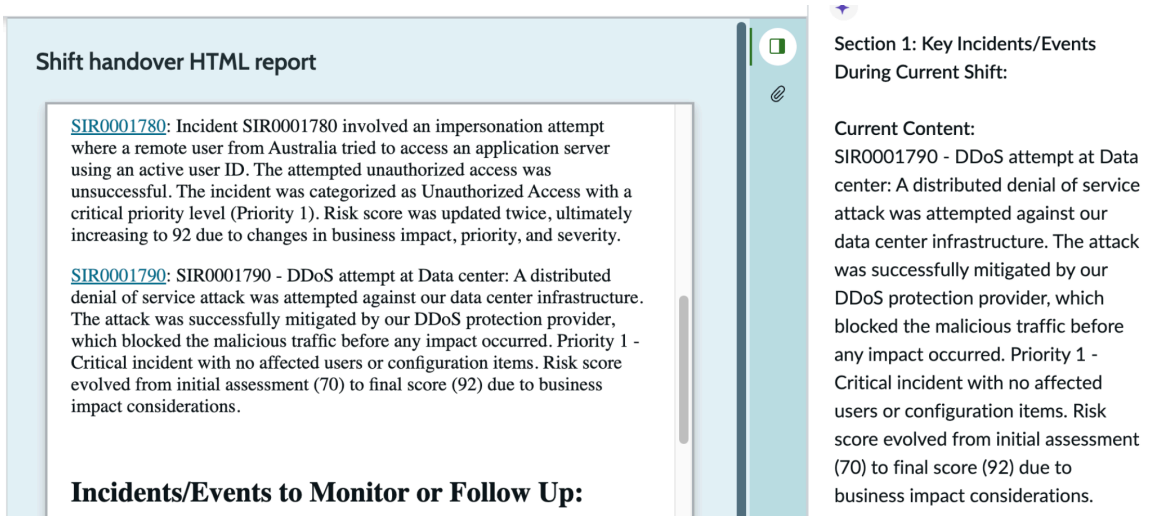
   Wenn keine Schichtübergabedatensätze im Status „Fortschritt“ vorhanden sind und der Gruppe des Anwenders zugewiesen sind oder keine Schichtübergabedatensätze

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vorhanden sind, wird eine Benachrichtigung angezeigt, die angibt, dass keine aktiven Schichtübergabedatensätze für den Anwender vorhanden sind.

5. Geben Sie die Datensatznummer der Schichtübergabe an, und drücken Sie die Eingabetaste.
   Der KI-Agent validiert den Schichtübergabedatensatz, um festzustellen, ob der Datensatz gültig und in Bearbeitung ist. Der angemeldete Analyst hat Zugriff auf den Schichtübergabedatensatz. Bei einer erfolgreichen Validierung generiert der KI-Agent den Inhalt für den Schichtübergabedatensatz und stellt ihn zur Genehmigung bereit.
6. Geben Sie positive Antworten ein, z. B. `Sieht gut aus` , `Genehmigt` , Oder `Ok` Wenn Sie dem Inhalt zustimmen.
   Der KI-Agent speichert den genehmigten Inhalt im entsprechenden Abschnitt des Schichtübergabeberichts.

   Für jeden Abschnitt des Schichtübergabeberichts stellt der KI-Agent den Inhalt bereit und fordert Feedback vom Analysten an. Bei Bedarf können Sie überspringen, um jeden Abschnitt zu aktualisieren.



Ergebnisse
Der KI-Agent zeigt die Zusammenfassung aller aktualisierten und übersprungenen Abschnitte an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Shift Handover Report Update Complete

Security incident SIR0051335 has been successfully added to shift handover report SHR0001013.

Summary of Processing:

Sections Saved (7 total):

1. ✅ Key Incidents/Events During Current Shift
2. ✅ Incidents/Events to Monitor or Follow Up
3. ✅ System/Infrastructure Updates
4. ✅ Outstanding Action Items
5. ✅ Shift Notes/Comments
6. ✅ Next Steps for Incoming Shift
7. ✅ References

Sections Skipped: None

All sections have been successfully

Automatische Übersetzung

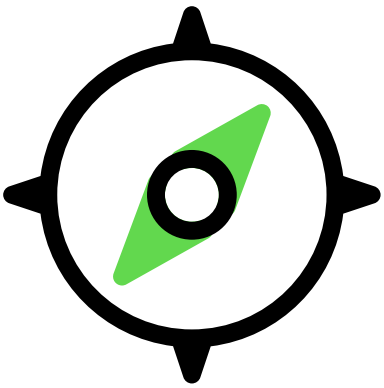
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Assist für Vulnerability Response

Verwenden Sie Now Assist für Vulnerability Response Anwendung, mit der Ihre Schwachstellenmanager und Analysten Ihr potenzielles Risiko kritischer Schwachstellen bewerten und Einblicke in die Compliance Ihrer Servicelevel-Vereinbarung (SLA) für angreifbare Elemente erhalten können.

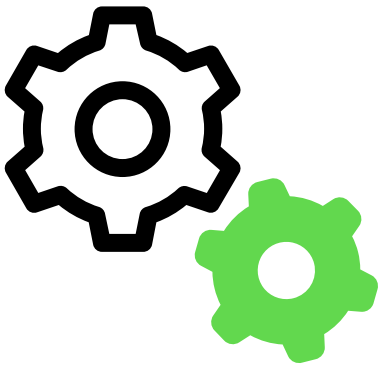
Erste Schritte

Untersuchen



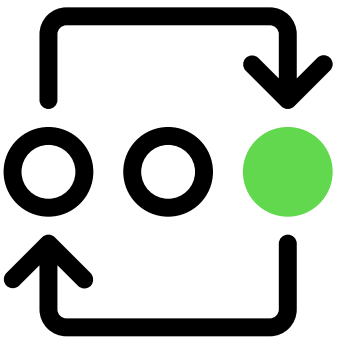
Erfahren Sie mehr über Now Assist für Vulnerability Response

Konfigurieren



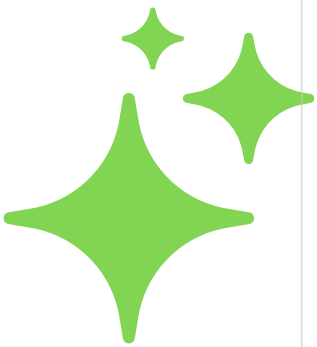
Erfahren Sie, wie Sie generative KI-Kompetenzen und agentische Workflows für konfigurieren und aktivieren Now Assist für Vulnerability Response

Verwenden



Erfahren Sie, wie Sie verwenden Now Assist für Vulnerability Response

KI-Agent-Sammlung



Rufen Sie Informationen zu den KI-Agents und agentischen Workflows für ab Now Assist für Vulnerability Response

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

- Nicht alle Modellanbieter sind für Kunden mit landesinternen SKUs verfügbar, und einige Now Assist-Produkte/-Funktionen sind derzeit für Kunden im Land nicht verfügbar. Weitere Informationen finden Sie unter KB1584492 artikel in der Now Support Knowledge Base. Überprüfen Sie in zukünftigen Releases auf Updates der Modellanbieter-Verfügbarkeit.
- Einige Now Assist Produkte/Funktionen sind derzeit für Kunden in den mit FedRAMP, NSC DOD IL5 oder Australia IRAP geschützten Rechenzentren, selbst gehosteten Kunden oder anderen eingeschränkten Umgebungen nicht verfügbar. Weitere Informationen finden Sie im Now Support Knowledge Base-Artikel KB0743854 . Überprüfen Sie auf Verfügbarkeitsaktualisierungen in zukünftigen Releases.
- Einige Now Assist Produkte/Funktionen sind derzeit nur für Kunden in einigen Regionen verfügbar. Überprüfen Sie auf Verfügbarkeitsaktualisierungen in zukünftigen Releases.

Hilfreiche Ressourcen

Einige ServiceNow Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Datenverarbeitung

Bei dieser Anwendung müssen die Daten einzelner ServiceNow-Kundeninstanzen in eine zentrale ServiceNow-Umgebung übertragen werden, die sich in einer anderen Rechenzentrumsregion befinden kann als die, in der sich Ihre Instanz befindet, und möglicherweise an einen externen Cloud-Anbieter, z. B. Microsoft Azure. Diese Daten werden gemäß den internen Richtlinien und Verfahren von ServiceNow gehandhabt, einschließlich unserer Richtlinien, die über unser CORE-Compliance-Portal verfügbar sind.

Datenerfassung

ServiceNow sammelt und verwendet die Eingaben, Ausgaben und Ausgabenbearbeitungen dieser Anwendung, um ServiceNow-Technologien wie ServiceNow-Modelle und KI-Produkte zu entwickeln und zu verbessern. Darüber hinaus erfasst diese Anwendung Die Schwachstellendaten, die Sie importieren, sowie Informationen zu den Konfigurationselementen in Ihrer CMDB. Kunden können der Datenerfassung für die Zukunft jederzeit widersprechen, wie auf der Now Assist Abwählseite beschrieben.

Weitere Informationen finden Sie unter Now Assist Dokumentation an.

Now Assist für Vulnerability Response erkunden

Erhalten Sie Informationen darüber, wie Ihre Schwachstellenmanager und Analysten verwenden können Now Assist Kompetenzen Und KI-Agents mit Now Assist für Vulnerability Response.

Now Assist für Vulnerability Response – Übersicht

Mit Now Assist Kompetenzen, die mit bereitgestellt werden Now Assist für Vulnerability Response Anwendung haben Ihre Schwachstellenmanager und Analysten die Möglichkeit, doppelte angreifbare Elemente zu identifizieren, zu überprüfen und zu schließen, die aus Ihren Schwachstellen-Scannern importiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Manager und Analysten haben auch die Möglichkeit, klare Anleitungen für die Lösung angreifbarer Elemente zu erhalten, einschließlich der Bereitstellung bevorzugter potenzieller Lösungen, die von Drittanbietern importiert werden Now Assist Kompetenzen.

Mit KI-Agents und agentischen Workflows, die mit bereitgestellt werden Now Assist für Vulnerability Response Anwendung, haben Ihre Schwachstellenmanager und Analysten die Möglichkeit, das potenzielle Risiko Ihrer Umgebung für aktuelle, bekannte Schwachstellen zu bestimmen und anzuzeigen, wie gut Ihre Korrekturziele Ihren Servicelevel-Vereinbarungen (Service Level Agreements, SLAs) entsprechen.

Now Assist für Vulnerability Response – Anwender

Anwender

Anwender	Beschreibung
Schwachstellenmanager und Analysten	Bestimmen Sie Ihr Risiko für Schwachstellen in Ihrer Umgebung und ihre potenziellen Auswirkungen auf Ihre Konfigurationselemente (Configuration Items, CIs) und Business-Services.
Schwachstellenmanager und Analysten	Erhalten Sie Einblicke, wie gut Sie Ihre Korrekturziele für Schwachstellen gemäß Ihren Service Level Agreements (SLAs) erreichen.
Schwachstellenmanager und Analysten	Stellen Sie Analysten Schritte zur Korrektur angreifbarer Elemente (Vits) bereit, die ihnen zugewiesen sind, mit Überwachungsthemen und Korrekturmaßnahmen.
Schwachstellenmanager und Analysten	Erhalten Sie klare Korrekturunterstützung für die Lösung von Korrekturaufgaben, die potenzielle, bevorzugte Lösungen enthalten, falls verfügbar.
Schwachstellenmanager und Analysten	Identifizieren und überprüfen Sie doppelte angreifbare Elemente, die von Ihren Schwachstellen-Scannern importiert werden. Identifizieren Sie das primäre angreifbare Element, das einem Konfigurationselement zugeordnet ist.

Now Assist für Vulnerability Response – Vorteile

Now Assist für Vulnerability Response Funktionen

Leistung	Funktion	Anwender
Identifizieren Sie das primäre (zuerst gefundene) angreifbare Element für ein Konfigurationselement, und entfernen Sie doppelte angreifbare Host-Elemente (Vits).	Deduplizierungskompetenz für angreifbare Elemente	Schwachstellenmanager und Analysten
Erhalten Sie Anleitungen zur Lösung von Korrekturaufgaben, die verfügbare potenzielle, bevorzugte Lösungen von Drittanbietern enthalten.	Empfehlen Sie die bevorzugte Lösung für die VIT-Kompetenz	Schwachstellenmanager und Analysten
• Identifizieren Sie Assets mit Common Vulnerabilities and Exposures (CVEs). • Bestimmen Sie die Anzahl der aktiven Schwachstellen-Elemente (Vits), die CVEs entsprechen.	Bewerten Sie den agentischen Workflow des Schwachstellenrisikos	Schwachstellenmanager und Analysten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Assist für Vulnerability Response Funktionen (Fortsetzung)

Leistung	Funktion	Anwender
• Identifizieren Sie Business-Services mit bekannten Schwachstellen. • Erstellen Sie Überwachungsthemen für die Korrektur angreifbarer Elemente (VIT) basierend auf den bereitgestellten Informationen. Der KI-Agent kann eine Korrekturmaßnahme für die aktiven Vits erstellen, die dem Überwachungsthema zugeordnet sind.		
Erhalten Sie Einblicke in den Fortschritt Ihrer Compliance-Zusammenfassung für Service Level Agreements (SLA) in den letzten 30 Tagen. Zeigen Sie Gruppen und Asset-Typen an, die SLAs nicht eingehalten haben, damit Sie Ziele nachverfolgen und anpassen können.	Analysieren Sie den agentischen Workflow zur Schwachstellenkorrektur	Schwachstellenmanager und Analysten
Rufen Sie relevanten Kontext und Details für die Ihnen zugewiesenen angreifbaren Elemente ab. Analysieren, planen und erstellen Sie Schritte für die Korrektur.	Schritte zur Problemlösung	Schwachstellenanalysten

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Now Assist für Vulnerability Response finden Sie unter:

- Now Assist für Vulnerability Response konfigurieren
- Mit agentischen Workflows in Now Assist Für Vulnerability Response

Ergänzende Informationen für Now Assist für Vulnerability Response

Verschaffen Sie sich einen schnellen Überblick über wichtige Informationen im Zusammenhang mit der Anwendung Now Assist für Vulnerability Response.

Unterstützte Versionen und erforderliche Anwendungen

Die folgenden Anwendungen sind erforderlich:

Anwendung	Version
Now Assist für Vulnerability Response	1.0.4
Now Assist Für Plattform [sn_genai_Platform]	9.1.0
Vulnerability Response Integration mit CISA [sn_vul_cisa]	1.5.1
Vulnerability Response [sn_vul]	26.2.1
Vulnerability Response Lizenzierung und Nutzung [sn_vul_Lizenzierung] (installiert mit [sn_vul])	2.7.1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung	Version
Vulnerability Response Allgemeiner Arbeitsbereich [sn_vul_cmn_WS] (installiert mit [sn_vul])	1.7.0
Vulnerability Response-Integrations-Framework [sn_vul_int_fw]	1.1.2
Schwachstellenlösungsmanagement [sn_vul_Solution]	10.4.3

Unterstützte Anwenderoberflächen

Now Assist für Vulnerability Response Enthält die Kompetenzen der generativen KI, die in der folgenden Tabelle aufgeführt sind.

Unterstützte Now Assist for Vulnerability Response-Schnittstellen

Schnittstelle	Features
Arbeitsbereich des Schwachstellenmanagers	Now Assist Kompetenzen: • Deduplizierung angreifbarer Host-Elemente (Vits). • Unterstützung bei der Nachbesserung, die die Bereitstellung potenzieller, bevorzugter Lösungen von Drittparteien umfasst. KI-Agents: Schwachstellenmanager und Analysten können bewerten, ob Ihre Konfigurationselemente (Configuration Items, CIs) und Ihre Business-Services Schwachstellen ausgesetzt sind. Überprüfen Sie auf neue bekannte ausnutzbare Schwachstellen der Cybersicherheits- und Infrastruktursicherheitsbehörde (CISA), und bewerten Sie ihre potenziellen Auswirkungen auf Ihre Umgebung. Schwachstellenmanager und Analysten können Einblicke in Ihre Compliance-Metriken erhalten, um zu verstehen, wie effektiv Ihre Organisation Korrekturziele für Schwachstellen basierend auf Service-Level-Vereinbarungen (SLAs) erfüllt.
UI6	Links in den Antworten in Now Assist Bereich öffnen Sie neue Registerkarten in Ihrem Browser.

Now Assist für Vulnerability Response konfigurieren

Die Now Assist für Vulnerability Response Die Anwendung wird in unterstützt Now Assist Bereich und bei Bedarf verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration – Übersicht

Durch Freigeben von Daten für ServiceNow® KI-Entwicklungsprogramm stellen Sie relevante Daten bereit, um die Genauigkeit der Vorhersage und die Anwender-Experience zu verbessern, Produkte an Ihre Geschäftsanforderungen anzupassen und Halluzinationen für aktivierte zu reduzieren Now Assist Kompetenzen.

Sie können eine deaktivieren ServiceNow Instanz aus der Datenfreigabe von Now Assist-Administrator Konsole, wenn Sie nicht teilnehmen möchten. Weitere Informationen finden Sie unter Opt out of data sharing for Now Assist . Wiederholen Sie den Abwählvorgang für alle Instanzen, die verwenden Now Assist Funktionalität.

Verwenden Sie vor v1.0.4 KI-Agenten-Studio Zum Konfigurieren Now Assist für Vulnerability Response.

Verwenden Sie ab v1.0.4 Now Assist-Administrator Zu konfigurierende Konsole Now Assist für Vulnerability Response. Diese Konsole enthält alles, was Sie für die Installation der Anwendungen und die Konfiguration der Kompetenzen für generative KI benötigen. Weitere Informationen finden Sie unter Configuring Now Assist Admin features .

Die Now Assist Bereich muss aktiviert sein. Weitere Informationen finden Sie unter Turn on the Now Assist panel .

- Install Now Assist plugins .

  Installieren Sie Now Assist für Vulnerability Response Anwendung (sn_vul_ai).

- Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Vulnerability Response

  Konfigurieren und überprüfen Sie die Details für eine Kompetenz in Geführtes Setup. Sie können eine Kompetenz über aktivieren Geführtes Setup.

- Aktivieren Sie einen agentischen Workflow für Now Assist für Vulnerability Response

  Die Now Assist für Vulnerability Response KI-Agents, die in der Anwendung enthalten sind, werden standardmäßig aktiviert. Sie müssen die agentischen Workflows über aktivieren KI-Agenten-Studio Zu verwenden Now Assist für Vulnerability Response. Weitere Informationen finden Sie unter Aktivieren Sie einen agentischen Workflow für Now Assist für Vulnerability Response.

  Konfigurieren und aktivieren Sie einen agentischen Workflow über Geführtes Setup.

Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Vulnerability Response

Konfigurieren und überprüfen Sie die Details für eine Kompetenz in Geführtes Setup. Sie können eine Kompetenz über aktivieren Geführtes Setup.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Now Assist Admin** > **Kompetenzen**an.
2. Mit **Technologie** Wählen Sie im Navigationsbereich aus **Security Operations** Aus der Liste.
   Die Now Assist Die Seite Kompetenzen für Security Operations wird angezeigt. Diese Now Assist für Vulnerability Response Kompetenzen werden für unterstützt Now Assist für Vulnerability Response:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Empfohlene bevorzugte Lösung für VIT
- Deduplizierung angreifbarer Elemente

3. Wählen Sie Aus **Kompetenz aktivieren** Für die gewünschte Kompetenz.
4. Führen Sie die Schritte aus, um eine Kompetenz mit zu konfigurieren und zu aktivieren Geführtes Setup.

Hinweis:
Einige Kompetenzen erfordern nicht alle unten aufgeführten Konfigurationsschritte. Wählen Sie die einzigen Aufgaben aus, die im linken Bereich angezeigt werden, und befolgen Sie die Anweisungen. Nachdem Sie die Aufgaben abgeschlossen haben, aktivieren Sie die Kompetenz.

5. Wählen Sie auf der Seite „Allgemeine Details“ die Option aus **Speichern und fortfahren** .
Diese Seite ist schreibgeschützt.
6. **Wahlweise:** Wählen Sie eine der folgenden Optionen aus, um die Verfügbarkeit zu definieren.
7. Wählen Sie Aus **Speichern und fortfahren** .
8. Definieren Sie den Zugriff.

Hinweis:

- Für die Deduplizierungskompetenz für angreifbare Elemente wird die Rolle sn_vul_ai.run_vi_dedup_job angezeigt. Diese Rolle ist erforderlich, um die Deduplizierungsaufträge aus dem Arbeitsbereich auszuführen.
- Für die Kompetenz „bevorzugte Lösung für VIT empfehlen“ wird die Rolle sn_vul_ai.run_suggest_solution angezeigt. Diese Rolle ist erforderlich, um die empfohlene Lösungsfunktion für angreifbare Elemente auszuführen.
- Die Rolle „sn_vul_ai.read_Suggest_Solution_Job“ ist erforderlich, um die geplante Aufgabe für Korrekturaufgaben auszuführen, die Tabelle „Lösungsauftrag empfehlen“ [sn_vul_ai_Suggest_Solution_Job] anzuzeigen und den Ausführungsstatus anzuzeigen.

Sie können diese Rollen bearbeiten, aber Sie möchten sie möglicherweise als Standardeinstellungen für diesen Schritt belassen.

9. Wählen Sie Aus **Speichern und fortfahren** .
10. Legen Sie fest, wo Sie die Kompetenz anzeigen möchten und wer sie im Arbeitsbereich anzeigen kann.
11. Wählen Sie Aus **Speichern und fortfahren** .
12. Überprüfen Sie Ihre Auswahlmöglichkeiten, und wählen Sie aus **Aktivieren** Um die Konfiguration für die Kompetenz abzuschließen.
13. Wählen Sie Aus **Kehren Sie zu Security Operations zurück** Um zur Seite „Now Assist-Kompetenzen für Security Operations“ zurückzukehren.
Sie sind jetzt zur Überprüfung bereit Verwenden Now Assist für Vulnerability Response Zur Korrektur angreifbarer Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie einen agentischen Workflow für Now Assist für Vulnerability Response

Sie müssen die agentischen Workflows im KI Agent Studio aktivieren. Die Now Assist für Vulnerability Response KI-Agents, die in der Anwendung enthalten sind und in den agentischen Workflows verwendet werden, werden standardmäßig aktiviert.

Vorbereitungen

Die Now Assist Bereich muss aktiviert sein. Weitere Informationen finden Sie unter Turn on the Now Assist panel .

Erforderliche Rolle: aia-admin

Prozedur

1. Navigieren zu **Alle** > **KI-Agenten-Studio** > **Übersicht**an.
2. Wählen Sie die Karte für den agentischen Workflow aus, den Sie konfigurieren und aktivieren möchten.
   - **Anwendungsfall Bewerten Sie das Schwachstellenrisiko**
   - **Anwendungsfall Analysieren Sie den Schwachstellen-Korrekturstatus**

   Wenn Sie diesen agentischen Workflow ändern möchten, können Sie dies Duplikat Passen Sie die Einstellungen an Ihre spezifischen Anforderungen an, und aktivieren Sie das Duplikat.

   Das geführte Setup wird angezeigt. Die Seite „Beschreiben und verbinden“ ist schreibgeschützt.
3. Wählen Sie **Fortsetzen**.
4. Wählen Sie für Auslöser definieren die Option aus **Fahren Sie Fort** .

   Die Seite „Auslöser definieren“ ist schreibgeschützt.
5. Wählen Sie aus **Anzeige** Schalten Sie für die Seite „Anzeige auswählen“ ein/aus, damit die Konversation mit dem KI-Agent in angezeigt wird Now Assist Bereich.
6. Wählen Sie das Pfeilsymbol aus, um den Abschnitt zu erweitern.
   Die Rollen sn_vul.Vulnerability_admin und sn_vul.Vulnerability_Analyst werden angezeigt. Diese Rollen werden für die agentischen Workflows in unterstützt Now Assist für Vulnerability Response Anwendung.
7. Wählen Sie aus, um den agentischen Workflow zu aktivieren **Speichern und testen** .
   Sie können die agentischen Workflows jetzt bei Bedarf aufrufen.
8. **Wahlweise:** Wählen Sie Aus **Anwendungsfall** (Agentischer Workflow) und geben Sie die Informationen ein, die Sie testen und auswählen möchten **Test starten** .

Verwenden Now Assist für Vulnerability Response Zur Korrektur angreifbarer Elemente

Schwachstellenmanager und Analysten können Korrekturaufgaben innerhalb ihres Arbeitsflusses mit den von unterstützten Kompetenzen für generative KI lösen Now Assist für Vulnerability Response.

Übersicht über Now Assist für Vulnerability Response Kompetenzen

Mit Kompetenzen der generativen KI mit Now Assist für Vulnerability Response, Haben Ihre Schwachstellenmanager und Analysten die Möglichkeit:

Identifizieren und schließen Sie doppelte angreifbare Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Deduplizierung wird nur für aktive angreifbare Host-Elemente (VIT) unterstützt

Zeigen Sie empfohlene bevorzugte Schwachstellenlösungen für angreifbare Elemente an.

Hinweis:

- Sie müssen installieren und aktivieren Vulnerability Solution Management[sn_vul_Solution] zum Importieren und Anzeigen bevorzugter und verfügbarer Schwachstellenlösungen. Diese Anwendung stellt aktuelle Lösungen mit geplanten Importen bereit. Vulnerability Solution Management Ist auf verfügbar ServiceNow® Store.
- Diese generative KI-Kompetenz unterstützt nur aktive angreifbare Host-Elemente (Vits). Vits müssen sich im befinden **Öffnen** , **Wird Untersucht** , **Warten Auf Implementierung** , Oder **Wird Überprüft** status.
- Aktuelle Lösungen, die Schwachstellen am effektivsten beheben, auch als Lösungen der höchsten Ersetzung bezeichnet, müssen verfügbar sein, damit Sie sie von Drittanbietern importieren können. Siehe Vulnerability Solution Management Weitere Informationen zu finden Vulnerability Solution Management Und unterstützte Integrationen für weitere Informationen.
- Die **Konfigurationselement** Das Feld in einer VIT muss mit einem Wert aus der Tabelle „Konfigurationselement“ [cmdb_ci] ausgefüllt werden.
- Die **Schwachstelle** Feld in einer VIT muss ausgefüllt werden.

- Identifizieren Sie doppelte angreifbare Elemente mit Now Assist für Vulnerability Response

  Identifizieren und gruppieren Sie doppelte angreifbare Elemente (Vits), die aus mehreren Scannern erstellt wurden. Identifizieren Sie das primäre angreifbare Element, und entfernen (schließen) Sie Duplikate.

- Schlagen Sie bevorzugte Schwachstellenlösungen mit vor Now Assist für Vulnerability Response

  Identifizieren Sie die am besten geeignete bevorzugte Lösung für ein bestimmtes angreifbares Element (VIT).

Identifizieren Sie doppelte angreifbare Elemente mit Now Assist für Vulnerability Response

Erstellen oder führen Sie einen Auftrag aus, um die primären (zuerst gefundenen) angreifbaren Elemente für Konfigurationselemente zusammen mit doppelten angreifbaren Elementen zu identifizieren, die von Ihren Schwachstellen-Scannern importiert werden.

Vorbereitungen

Siehe Verwenden Now Assist für Vulnerability Response Zur Korrektur angreifbarer Elemente Um weitere Informationen zu den Anforderungen für zu erhalten Now Assist Kompetenz. Siehe Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Vulnerability Response Um weitere Informationen zur Aktivierung zu erhalten.

Erforderliche Rollen:

Hinweis:
sn_vul.Vulnerability_admin und sn_vul.Vulnerability_Analyst erben die folgenden Rollen, wenn Sie installieren Now Assist für Vulnerability Response Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Deduplizierungsmodul für angreifbare Elemente im Arbeitsbereich anzeigen – sn_vul_ai.now_assist_user
- Deduplizierungsauftragskonfigurationen erstellen – sn_vul_ai.configure_VI_dedup
- Deduplizierungsaufträge ausführen – sn_vul_ai.run_vi_dedup_job
- Überprüfen Sie doppelte Auftragsdatensätze – sn_vul_ai.Review_duplicate_VI

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Wählen Sie aus Now Assist ✦ Symbol im Navigationsbereich.
   Die **Alle Auftragskonfigurationen** , **Alle Aufträge** , Und **Alle doppelten Überprüfungen** Registerkarten werden im angezeigt Now Assist Seite. Sie müssen einen Deduplizierungsauftrag als ersten Schritt für die Deduplizierung angreifbarer Elemente (Vits) erstellen.

   Hinweis:
   Sie müssen über die Rolle sn_vul_ai.configure_VI_dedup verfügen, um Aufträge zu erstellen.

3. Um einen Auftrag zu erstellen, wählen Sie aus **Neu** Und füllen Sie die Felder aus.

Feld	Beschreibung
Titel	Eindeutiger Name, der Ihnen hilft, diesen Auftrag von anderen Jobs zu identifizieren.
E-Mail-Benachrichtigung	Aktivieren Sie das Kontrollkästchen, um E-Mail-Benachrichtigungen zu erhalten, wenn dieser Auftrag abgeschlossen ist. Wenn diese Option ausgewählt ist, können Sie die folgenden Informationen in einer E-Mail anzeigen: ○ Doppelte angreifbare Elemente gefunden ○ Gesamtzahl der verarbeiteten angreifbaren Elemente ○ Betroffene Konfigurationselemente ○ Wählen Sie aus **Überprüfen Sie Duplikate** Link zum Anzeigen der Liste der Duplikate im Arbeitsbereich. Alternativ können Sie im oberen Banner das Symbol Benachrichtigungen anzeigen (Gell) auswählen, um Nachrichten mit den doppelten angreifbaren Elementen anzuzeigen, die für abgeschlossene Aufträge gefunden wurden.
Bedingungen festlegen	**a.** Wählen Sie aus **Legen Sie Bedingungen fest** Link zum Filtern der angreifbaren Elemente, die Sie auf Duplikate überprüfen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Ein Beispiel könnte sein: **[Konfigurationselement] [enthält] [serverbasierte VIS]** . Die **Legen Sie Bedingungen fest** Der Link wird aktualisiert und zeigt eine Anzahl mit Ihren übereinstimmenden Ergebnissen an. Möglicherweise möchten Sie Ihren Auftrag basierend auf Ihren zurückgegebenen Ergebnissen umbenennen. Sie können auswählen **Zeigen Sie übereinstimmende Ergebnisse an** Link, um angreifbare Elemente anzuzeigen, die Ihre Bedingungen erfüllen, und weitere Details wie eine Zusammenfassung, Konfigurationselemente und Risikobewertungen im Bedingungsmodal anzuzeigen. **b.** Wenn Sie mit den Ergebnissen zufrieden sind, wählen Sie aus **Speichern** .

4. Nachdem Sie den Auftrag gespeichert haben, die **Auftrag ausführen** Die Schaltfläche wird im Datensatz angezeigt und aktiviert.

Sie sind bereit, einen Auftrag auszuführen.

Hinweis:
Sie müssen über die Rolle sn_vul_ai.run_vi_dedup_job verfügen, um sie anzuzeigen **Auftrag ausführen** Schaltfläche und Aufträge initiieren.

a. Navigieren Sie zum Ausführen eines Auftrags zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Now Assist** > **Alle Auftragskonfigurationen**an.

b. Suchen Sie den gewünschten Auftrag, wählen Sie den Datensatz in der Spalte Nummer aus, um ihn zu öffnen, und wählen Sie aus **Auftrag Ausführen** .
Es wird eine Meldung angezeigt, dass der Auftrag im Hintergrund ausgeführt wird. Um weitere Informationen zum Status Ihres Jobs zu erhalten, wählen Sie aus **Zeigen Sie den Fortschritt an** Link.

Nachdem Sie Auftrag ausführen ausgewählt haben, wird der Auftrag zum Überprüfen der Deduplizierung angreifbarer Elemente initiiert und im Hintergrund ausgeführt.

Es gibt einen weiteren Auftrag, der alle 30 Minuten ausgeführt wird, um sicherzustellen, dass die aktiven Aufträge abgeschlossen wurden.

Nachdem Ihr Auftrag erfolgreich abgeschlossen wurde, können Sie die von Ihrem Auftrag gefundenen doppelten Vits überprüfen, bewerten und schließen.

Hinweis:
Sie müssen über die Rolle sn_vul_ai.Review_duplicate_VI verfügen, um doppelte Vits zu überprüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Überprüfen Sie doppelte Vits.

a. Um abgeschlossene Aufträge und die Listen doppelter angreifbarer Elemente zu überprüfen, navigieren Sie zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Now Assist** > **Alle Aufträge**an.

b. Öffnen Sie einen Datensatz (**AUFTRAG NR.**) Und wählen Sie aus **Doppelte Angreifbare Elementüberprüfungen** Zugehörige Liste.

c. **Wahlweise:** Wählen Sie die Links aus, um das angreifbare Element zu öffnen (**VIT-NUMMER**) Datensätze zur Überprüfung, bevor Sie bestimmen, ob die Vits im Datensatz Duplikate sind.

d. Wählen Sie für einen Side-by-Side-Vergleich der doppelten VIT-Datensätze ein (**DUP-NR.**) Datensatz, um ihn zu öffnen.

- Auftragsnummer und Status (**Muss Überprüft Werden**) Wird angezeigt.
- Die Felder „Konfidenz“ und „Grund“ enthalten weitere Informationen. In der Spalte Grund werden die Gründe für generative KI und Now LLM-Service angezeigt, warum diese Vits als Duplikate gelten.
- Informationen zum primären VIT und zur doppelten VIT sind im Abschnitt „Details zu angreifbaren Elementen“ nebeneinander zu finden.
- Datum der ersten Suche für das primäre und die doppelten Vits. Ein primärer VIT hat normalerweise das früheste Datum der ersten Entdeckung.
- Wählen Sie die Informationen aus ⓘ Symbol in den Feldern Details zu primären angreifbaren Elementen und Duplikat, wenn Sie die VIT-Datensätze auf dieser Seite öffnen möchten.

e. Wählen Sie eine aus.

Option	Beschreibung
Als nicht Duplikat markieren	Dies sind zwei unterschiedliche angreifbare Elemente, die mindestens zwei eindeutige Schwachstellen darstellen. Diese beiden angreifbaren Elemente werden in den zukünftig erstellten Aufträgen nicht als Duplikate betrachtet. Der Status geht von über **Muss Überprüft Werden** Bis **Kein Duplikat** Für **DUP-NR.** Datensatz.
Duplikat bestätigen	Ihre Überprüfung zeigt an, dass diese beiden Vits Duplikate sind. Der VIT-Datensatz, der im doppelten Datensatz mit der Bezeichnung angezeigt wird Duplikat Übergeht zu **Geschlossen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Eine Arbeitsnotiz mit Abschlussnotizen wird dem geschlossenen VIT-Datensatz hinzugefügt. Alle zugehörigen Erkennungen im geschlossenen VIT werden in den primären VIT-Datensatz verschoben. Arbeitsnotizen werden dem primären VIT hinzugefügt, um anzuzeigen, dass ein Duplikat geschlossen und seine Erkennungen verknüpft wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Hinweis: Die Systemeigenschaft sn_vul_ai.duplicate_VI_Confidence_threshold automatisiert den Deduplizierungsworkflow für angreifbare Elemente. Diese Systemeigenschaft ist standardmäßig aktiviert, hat jedoch keinen Schwellenwert für eine Konfidenzpunktzahl. Ohne Wert für den Schwellenwert schließt der automatisierte Workflow keine Duplikate. **Hinweis:** Konfidenzpunktzahlen von 100 für Vits werden nicht von berechnet Now Assist Kompetenz. Diese Punktzahl wird durch Abgleich mit deterministischer Logik berechnet. Wenn Sie einen Schwellenwert eingeben, werden alle Duplikate, deren Vertrauenspunktzahlen größer als der von Ihnen angegebene Wert sind, automatisch geschlossen, und ihre Erkennungen werden in das primäre angreifbare Element zusammengefasst. Möglicherweise möchten Sie diese Systemeigenschaft in ihrer Standardeinstellung ohne Schwellenwert belassen, bis Sie mit dem Workflow vertraut sind und einige Zeit haben, um einen genauen Wert festzulegen. In der Standardeinstellung können Sie die Kontrolle über die Bedingungen behalten, unter denen Ihre doppelten Vits überprüft, markiert und verarbeitet werden. Sie müssen über die Rolle sn_vul_ai.configure_VI_dedup oder sn_vul_ai.Review_duplicate_VI verfügen, um diese Systemeigenschaft zu ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. **Wahlweise:** Alternativ können Sie doppelte Elemente aus dem überprüfen **Alle doppelten Überprüfungen** Listenregisterkarte aus einem **DUP-NR.** Datensatz.
Mit dieser Liste können Sie eine Massenbearbeitung der doppelten Datensätze und der zugehörigen VIT-Datensätze durchführen.

Schlagen Sie bevorzugte Schwachstellenlösungen mit vor Now Assist für Vulnerability Response

Verwenden Sie generative KI-Argumentation mit Now Assist für Vulnerability Response(Now Assist Mit VR), damit Ihre Analysten potenzielle bevorzugte Lösungen von Drittanbietern für die Schwachstellen in Ihren Assets finden können.

Vorbereitungen

Siehe Verwenden Now Assist für Vulnerability Response Zur Korrektur angreifbarer Elemente Um weitere Informationen zu den Anforderungen für zu erhalten Now Assist Kompetenz. Siehe Konfigurieren und aktivieren Sie eine Kompetenz für Now Assist für Vulnerability Response Um weitere Informationen zur Aktivierung zu erhalten.

Erforderliche Rollen:

Hinweis:
sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst und sn_vul.Remediation_owner erben die folgenden Rollen, wenn Sie installieren Now Assist für Vulnerability Response Anwendung.

- sn_vul_ai.run_suggest_solution: Erforderlich, um die Funktion „empfohlene Lösung“ für angreifbare Elemente auszuführen.
- sn_vul_ai.read_Suggest_Solution_Job: Erforderlich, um die geplante Aufgabe für Korrekturaufgaben auszuführen und die Tabelle „Lösungsauftrag empfehlen“ [sn_vul_ai_Suggest_Solution_Job] und den Ausführungsstatus anzuzeigen.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Öffnen Sie einen Datensatz für angreifbare Host-Elemente (VIT), und wählen Sie aus **Details** Registerkarte.
3. Zu verwenden Now Assist Mit VR-Begründung wählen Sie aus, um die Lösungen zu finden, die Ihren Schwachstellen am besten entsprechen **Lösung empfehlen** .
4. Alternativ öffnen Sie eine Korrekturaufgabe (RT), die Ihnen zugewiesen ist, und wählen Sie aus **Lösung empfehlen** .

   In den folgenden Tabellen werden die Nachrichten und Benachrichtigungen beschrieben, die angezeigt werden und wo nach der Auswahl Daten ausgefüllt werden **Lösung empfehlen** In VIT- und Korrekturaufgabendatensätzen.

   Hinweis:
   Now Assist Mit VR werden keine Schwachstellenlösungen generiert. Lösungen werden aus Drittpartei-Integrationen importiert. Damit Sie sehen können **Lösung empfehlen** Schaltfläche in VIT- und Korrekturaufgabendatensätzen muss mindestens eine Lösung der höchsten verfügbaren Ersatzlösung für die mit dieser VIT verknüpfte Schwachstelle vorhanden sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensätze für angreifbare Elemente (VIT)

Nachricht oder Benachrichtigung	Beschreibung
Now Assist für VR hat eine potenzielle Lösung gefunden, mit der Sie diese Schwachstelle beheben können. Weitere Informationen finden Sie im Abschnitt „Korrektur“ und im Aktivitätenstrom auf der Registerkarte „Details“.	Informationen für eine bevorzugte Lösung werden auf der Registerkarte Details eines VIT in den Feldern bevorzugte Lösung und Zusammenfassung im Abschnitt „Korrektur“ ausgefüllt. Arbeitsnotizen werden in den Aktivitätenstrom eingegeben. Überprüfen Sie die Lösungen auf Richtigkeit. **Hinweis:** Wenn eine VIT über eine Lösung verfügt, die von bereitgestellt wurde Now Assist Für VR kann sich die Lösung ändern, wenn Sie weitere Lösungen importieren und den Auftrag erneut ausführen (auswählen **Lösung empfehlen**).
Mit Now Assist für VR wurde basierend auf den folgenden Gründen eine Lösung für diese Schwachstelle gefunden.	Details im Aktivitätenstrom in Vits dazu, warum diese Lösung bestimmt wurde Now Assist Damit VR eine bevorzugte Lösung ist. Begründung wird nur in Vits angezeigt. Bevorzugte Lösungen, die von der Kompetenz gefunden werden, werden in Korrekturaufgaben auf der Registerkarte „Lösungen“ zusammengefasst. Überprüfen Sie die Lösungen auf Richtigkeit.
Es wurde keine Lösung gefunden. Weitere Informationen finden Sie im Abschnitt „Korrektur“ und im Aktivitätenstrom auf der Registerkarte „Details“.	Zusammenfassung im Aktivitätenstrom auf der Registerkarte „Details“ in Vits darüber, warum keine Lösung gefunden wurde. Begründung wird nur in Vits angezeigt.

Datensätze der Korrekturaufgabe (RT)

Nachricht oder Benachrichtigung	Beschreibung
Verwenden Sie Now Assist für VR, um potenzielle bevorzugte Lösungen für die angreifbaren Elemente in dieser Korrekturaufgabe zu finden. Ihre Leistung kann beeinträchtigt werden, wenn die Korrekturaufgabe eine große Anzahl von Vits aufweist.	○ Die RT muss mindestens eine VIT haben. Der Standardwert für die maximale Anzahl von Vits in einer RT ist 1.000. Möglicherweise möchten Sie diesen Wert in seiner Standardeinstellung beibehalten. **Hinweis:** Sie können den Höchstwert mit der Systemeigenschaft sn_vul_ai.max_vits_allowed_for_Suggest_Solution ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachricht oder Benachrichtigung	Beschreibung
	○ Überprüft alle Vits in der Korrekturaufgabe, Lösungen werden jedoch nur für Vits in der Korrekturaufgabe empfohlen, die sich im status „aktiv“ befinden, Lösungen mit der höchsten Ersatzlösung aufweisen und noch keine Lösung haben. **Hinweis:** Wenn Sie den Auftrag erneut ausführen (wählen Sie aus **Lösung empfehlen**) Für eine Korrekturaufgabe wertet der Auftrag standardmäßig nur Vits ohne Lösungen aus (Wahr). Um Vits mit Lösungen auszuwerten, müssen Sie die Systemeigenschaft sn_vul_ai.exclude_vits_with_Solution in ändern Falsch . ○ Stellt eine Zusammenfassung für die bevorzugte Lösung im Aktivitätenstrom auf der Registerkarte „Details“ der Korrekturaufgabe bereit. ○ Bevorzugte Lösungen, die von der Kompetenz gefunden werden, werden in Korrekturaufgaben auf der Registerkarte „Lösungen“ zusammengefasst. ○ Führt einen Rolldown der Lösungsinformationen für übereinstimmende Vits in der Korrekturaufgabe durch. Lösungsinformationen werden in den Feldern bevorzugte Lösung und Zusammenfassung und im Aktivitätenstrom auf den Registerkarten Details ausgefüllt. ○ Wenn ein Hintergrundauftrag in Bearbeitung ist und Lösungen für diesen Datensatz bewertet werden, wird **Lösung empfehlen** Schaltfläche ist in der Korrekturaufgabe nicht sichtbar. Sie können die Schaltfläche anzeigen, nachdem der Auftrag abgeschlossen wurde. Überprüfen Sie die Lösungen auf Richtigkeit.
Derzeit werden Lösungen für Vits erfasst. Wählen Sie diesen Link aus, um den Fortschritt nachzuverfolgen.	Sehen Sie sich den Auftragsstatus und eine Zusammenfassung an, die die folgenden Informationen enthält:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachricht oder Benachrichtigung	Beschreibung
	○ Gesamtanzahl der Vits in Korrekturaufgabe: n ○ Anzahl der verarbeiteten Vits: n ○ Vits mit Lösungen: n Vits Wenn nicht genügend Informationen vorhanden sind, um eine Lösung sicher vorzuschlagen, werden keine Lösungen für Vits bereitgestellt. Die Zusammenfassung wird auch im Aktivitätenstrom bereitgestellt, nachdem der Auftrag abgeschlossen wurde.
Lösungen werden für Vits nicht bereitgestellt, wenn nicht genügend Informationen vorhanden sind, um eine Lösung sicher vorzuschlagen.	Für bestimmte Vits wurden keine Lösungen gefunden, da nicht genügend Informationen vorhanden sind oder keine Lösungen der höchsten Ersatzlösung bereitgestellt wurden Now Assist Um eine Lösung zu bestimmen. ○ Die Felder bevorzugte Lösung und Zusammenfassung bleiben im VIT leer. ○ Arbeitsnotizen werden in den Aktivitätenstrom der VIT- und Korrekturaufgabe eingegeben. ○ Begründung wird nur in Vits angezeigt.

Mit agentischen Workflows in Now Assist Für Vulnerability Response

Verwenden Sie Vulnerability Response KI-Agents , um Ihre Aufgaben autonom auszuführen.

Verfügbare agentische Workflows für KI-Agents für Vulnerability Response

Name des Agentischen Workflows	Beschreibung	Verfügbare KI-Agents
Schwachstellenrisiko bewerten	• Bestimmen Sie, ob Ihre Konfigurationselemente (CIs) und Business-Services bekannten Schwachstellen ausgesetzt sind. • Bestimmen Sie die potenziellen Auswirkungen, die eine bestimmte Schwachstelle in Ihrer Umgebung haben kann. • Überprüfen Sie CIs auf neue ausnutzbare Schwachstellen der	• KI-Agent für CISA-Schwachstellenanalyse • KI-Agent zur Analyse des Schwachstellenrisikos • KI-Agent für das Erstellen von Überwachungsthemen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare agentische Workflows für KI-Agents für Vulnerability Response (Fortsetzung)

Name des Agentischen Workflows	Beschreibung	Verfügbare KI-Agents
	Cybersicherheits- und Infrastruktursicherheitsbehörde (CISA) (Zero-Day). • Erstellen Sie Überwachungsthemen im Vulnerability Manager-Arbeitsbereich, um angreifbare Elemente zu beheben.	
Status der Schwachstellenkorrektur analysieren	• Erhalten Sie Einblicke in Ihre Compliance-Metriken und -Statistiken, um herauszufinden, wie gut Sie Korrekturzieldaten für Datensätze von angreifbaren Elementen (VIT) einhalten. • Zeigen Sie Ihre monatlichen VIT-Datensatzkorrektursummen an, und identifizieren Sie verpasste Ziele. • Aufgliederung der Korrekturdaten für Vits nach **Schweregrad** , **Zuweisungsgruppe** , **Konfigurationselement** , Und **Schwachstelle** Für Ihre monatlichen Compliance-Überprüfungen von Servicelevel-Vereinbarungen (Service Level Agreement, SLA).	KI-Agent für Compliance-Analysen bei Korrekturen

Wichtig:
Standardmäßig sind alle agentischen Workflows und KI-Agent-Datensätze schreibgeschützt.

Um einen agentischen Workflow zu ändern, müssen Sie zuerst Duplicate an agentic workflow , Und fahren Sie dann mit den folgenden Schritten fort:

- Aktivieren Sie den agentischen Workflow. Die Now Assist für Vulnerability Response KI-Agents, die in der Anwendung enthalten sind, werden standardmäßig aktiviert.
- Bei Bedarf können Sie einen Auslöser hinzufügen, um den agentischen Workflow automatisch aufzurufen.

Suchen Sie nach einem KI-Agenten?

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

- Möglicherweise sind KI-Agenten mit installiert Now Assist Anwendung, die nicht in Agenten-Workflows verwendet wird. Informationen zum Anzeigen aller in Ihrer Instanz verfügbaren Agenten finden Sie unter Suchen Sie KI-Agenten .
- Um Agenten zu finden, die möglicherweise nicht auf Ihrer Instanz installiert sind, besuchen Sie die KI-Agent-Marketplace Auf ServiceNow Store.

- Bewerten Sie den agentischen Workflow des Schwachstellenrisikos.

  Chatten Sie mit einem KI-Agent von Now Assist Bereich, mit dem Sie bewerten können, ob Ihre Konfigurationselemente und Ihre Business-Services Schwachstellen ausgesetzt sind.

- Analysieren Sie den agentischen Workflow zur Schwachstellenkorrektur.

  Chatten Sie mit einem KI-Agent von Now Assist Bereich, der Ihnen hilft, Einblicke in Ihre Compliance-Metriken zur Lösung angreifbarer Elemente zu erhalten.

Bewerten Sie den agentischen Workflow des Schwachstellenrisikos

Chatten Sie mit einem KI-Agent von Now Assist Bereich, mit dem Sie das potenzielle Risiko Ihrer Konfigurationselemente und Ihrer Business-Services für Schwachstellen bewerten können.

Vorbereitungen

Die Now Assist Bereich muss aktiviert sein. Weitere Informationen finden Sie unter Turn on the Now Assist panel .

Erforderliche Rollen: sn_vul.Vulnerability_admin oder sn_vul.Vulnerability_Analyst

Prozedur

1. Wählen Sie aus Now Assist Symbol ( ) Von beliebiger Stelle in Ihrer Instanz.
   Die Now Assist Bereich wird angezeigt.

   Der agentische Workflow „Schwachstellenrisiko bewerten“ ist bei Bedarf verfügbar. Sie können jede Abfrage in natürlicher Sprache eingeben. Sie können jedoch die in der folgenden Tabelle beschriebenen Eingabeaufforderungen und Schritte verwenden, um sich mit den verfügbaren Schwachstellendaten und den Möglichkeiten vertraut zu machen. Die folgenden Schritte zeigen Ihnen, wie Sie aktuelle Schwachstellendaten anfordern, ein Überwachungsthema basierend auf den zurückgegebenen Ergebnissen erstellen und die Gesamtauswirkung einer Schwachstelle auf Ihre Umgebung bestimmen.

Ihre Anforderung oder Antwort	Beschreibung
Was sind die letzten CISA-Schwachstellen?	**Zuletzt** In Ihrer Frage bezieht sich auf neue Schwachstellen, die in den letzten sieben Tagen aufgetaucht sind. Sieben Tage (eine Woche) sind der Standardzeitraum für den agentischen Workflow. Wenn Sie für einen bestimmten Zeitraum von sieben Tagen nach neuen Schwachstellen suchen möchten, geben Sie eine Anforderung mit einem Wert ein, der in der Vergangenheit liegt, z. B. **Was sind die letzten Schwachstellen in den letzten 30 Tagen?**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihre Anforderung oder Antwort	Beschreibung
Ja, erstellen Sie ein Überwachungsthema für die Schwachstelle CVE-2018-9065.	Wenn Sie gefragt werden, ob Sie ein Überwachungsthema erstellen möchten, ziehen Sie es möglicherweise vor, in Ihrer Antwort spezifisch zu sein. Bestätigen Sie beispielsweise die Anforderung, und geben Sie eine bestimmte Schwachstelle im folgenden Format ein: **CVE-2018-9065** .
Können Sie mir eine detaillierte Auswirkungsanalyse für die CVE-2018-9065-Schwachstelle geben?	Die Analyse potenzieller Auswirkungen von Schwachstellen wird nur für betroffene Business-Services und Konfigurationselementklassen unterstützt.
Ausgabe für die vorherige Frage anzeigen.	Fordern Sie den Service Desk-Mitarbeiter auf, Ihre vorherige Frage zu überprüfen, wenn Sie keine Antwort erhalten.
Beenden Sie die Sitzung , Oder **Anhalten** .	Beenden Sie die Konversation.

Ihre Konversation wird gespeichert, bis Sie einen neuen Chat starten. Wenn die Konversation unerwartet beendet wird, starten Sie einen neuen Chat. Um einen neuen Chat zu starten, wählen Sie das Symbol „neuer Chat“ ( ).

2. Geben Sie eine Anforderung in natürlicher Sprache ein, um zu sehen, ob Sie aktuellen Schwachstellen ausgesetzt sind, z. B. **Was sind die letzten CISA-Schwachstellen?**

   Da in Ihrem Eintrag kein Bereich angegeben ist, sammelt der Service Desk-Mitarbeiter standardmäßig Daten zu ausnutzbaren Schwachstellen der Cybersicherheits- und Infrastruktursicherheitsbehörde (CISA) zu Ihren Assets und gibt Informationen aus den letzten sieben Tagen zurück.

   Die Common Vulnerabilities and Exposures (CVE)-Schwachstellen, die sich auf Ihre Assets auswirken und denen angreifbare Elemente in Ihrer Umgebung zugeordnet sind, werden aufgelistet.

   Möglicherweise gibt der Service Desk-Mitarbeiter auch Aliasse zurück, die CVEs entsprechen. Aliasse werden gemeldet, wenn Sie Scanner von Drittanbietern zum Importieren Ihrer Schwachstellendaten verwenden. Beispiel: CVE-2018-8627 (Alias: TEN-119686, TEN-119596) mit Schweregrad „Mittel“ hat 4 angreifbare Elemente (Vits). Diese Antwort gibt an, dass die Schwachstelle vom Tenable-Scannerprodukt (TEN) erkannt und importiert wurde.

3. **Wahlweise:** Wählen Sie den Link bekannte ausnutzbare CISA-Schwachstellen aus, um Informationen zu allen zurückgegebenen CVEs zu erhalten.
   Die Liste wird in einer neuen Registerkarte in UI16 geöffnet.

4. Kehren Sie zum Chat zurück, und geben Sie an der Eingabeaufforderung eine Anforderung für den Service Desk-Mitarbeiter ein, ein Überwachungsthema für ein CVE zu erstellen, z. B. **Ja, erstellen Sie ein Überwachungsthema für die Schwachstelle CVE-2018-9065.**
   Der Service Desk-Mitarbeiter schlägt einen Namen für Ihr Überwachungsthema vor und bittet um eine Bestätigung. Sie können den Namen ändern.

5. Geben Sie Ein **OK** .

6. Wählen Sie den Link aus, um das Überwachungsthema im Vulnerability Manager-Arbeitsbereich anzuzeigen und weitere Details sowie die angreifbaren Elemente anzuzeigen, die dem CVE zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Liste wird in einer neuen Registerkarte in UI16 geöffnet. Nach der Überprüfung der Daten können Sie sich entscheiden, weitere Informationen zu den Auswirkungen des CVE auf Ihre anderen Assets zu erhalten.

7. Kehren Sie zu zurück Now Assist Bereich, geben Sie ein, und fordern Sie den Service Desk-Mitarbeiter eine detaillierte Auswirkungsanalyse an, z. B. **Können Sie mir eine detaillierte Auswirkungsanalyse für die CVE-2018-9065-Schwachstelle geben?**
   Diese Anforderung gibt Informationen zu Ihren Konfigurationselementen und Business-Services zurück, die von diesem CVE betroffen sind. Sie bietet eine Aufgliederung der Relevanz, eine Liste der betroffenen Business-Services und eine Liste der Klassen betroffener Konfigurationselemente. Es gibt auch einen Link für detailliertere Informationen.

8. **Wahlweise:** Fordern Sie eine Gesamtbewertung des Schwachstellenrisikos für einen bestimmten Business-Service an.
   Informationen zum Business-Service enthalten zugeordnete angreifbare Elemente, Relevanz (Risiko) und die Konfigurationselemente nach Klasse werden aufgelistet.

Analysieren Sie den agentischen Workflow zur Schwachstellenkorrektur

Chatten Sie mit einem KI-Agent von Now Assist Bereich, der Ihnen hilft, Einblicke in Ihre monatlichen Compliance-Metriken für Korrekturen für angreifbare Elemente zu erhalten.

Vorbereitungen

Die Now Assist Bereich muss aktiviert sein. Weitere Informationen finden Sie unter Turn on the Now Assist panel .

Erforderliche Rollen: sn_vul.Vulnerability_admin oder sn_vul.Vulnerability_Analyst admin

Prozedur

1. Wählen Sie aus Now Assist Symbol ( ).
   Die Now Assist Bereich wird angezeigt.

   Der agentische Workflow „Schwachstellen-Korrekturstatus analysieren“ ist bei Bedarf. Sie können jede Abfrage in natürlicher Sprache eingeben. Sie können jedoch die in der folgenden Tabelle beschriebenen Eingabeaufforderungen und Schritte verwenden, um sich mit den verfügbaren Daten und den Möglichkeiten vertraut zu machen.

   Diese Schritte geben Ihnen Einblicke in Ihre Compliance-Metriken, um herauszufinden, wie gut Ihre Teams ihre monatlichen Korrekturzieldaten für Datensätze angreifbarer Elemente einhalten, wie in Ihrer Servicelevel-Vereinbarung (SLA) gemeldet.

Ihre Anforderung oder Antwort	Beschreibung
Wie lautet meine Compliance für die Nachbesserung für den Monat Oktober 2024?	Standardmäßig basiert die Suche auf der Zuweisungsgruppe. Wenn Sie keinen Monat angeben, sucht der KI-Agent nach dem aktuellen Monat und beginnt dann, monatlich rückwärts zu gehen. Alternativ können Sie den Service Desk-Mitarbeiter um eine Aufgliederung nach Konfigurationselementklasse oder Schwachstelle bitten. Geben Sie beispielsweise ein **Wie hoch ist meine**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihre Anforderung oder Antwort	Beschreibung
	Compliance für den Monat Oktober 2024 für Windows-Server?
Welche Asset-Typen haben die am häufigsten verpassten SLAs berücksichtigt?	Die Ergebnisse werden basierend auf den Daten für den Monat Ihrer ursprünglichen Anforderung nach Asset-Typ organisiert.
Welche Zuweisungsgruppe hatte die wenigsten verpassten kritischen SLAs?	Rufen Sie die Zuweisungsgruppe ab, die die meisten oder wenigsten verpassten SLAs basierend auf dem Schweregrad des angreifbaren Elements (VIT) hatte: Kritisch , Hoch , Mittel , Und Niedrig . Darüber hinaus können Sie den KI-Service Desk-Mitarbeiter bitten, verpasste SLAs nach VIT-Kategorie zu suchen.
Ausgabe für die vorherige Frage anzeigen.	Fordern Sie den Service Desk-Mitarbeiter auf, Ihre vorherige Frage zu überprüfen, wenn Sie keine Antwort erhalten.
Beenden Sie die Sitzung , Oder **Anhalten** .	Beenden Sie die Konversation.

Ihre Konversation wird gespeichert, bis Sie einen neuen Chat starten. Wenn die Konversation unerwartet beendet wird, starten Sie einen neuen Chat. Um einen neuen Chat zu starten, wählen Sie das Symbol „neuer Chat“ ( ).

2. Geben Sie eine Anforderung in natürlicher Sprache ein, um Ihre Korrekturmetriken für einen bestimmten Monat und ein bestimmtes Jahr anzuzeigen, z. B. Wie lautet meine Compliance für die Nachbesserung für den Monat Oktober 2024?

   Die Ergebnisse sind in Abschnitte organisiert.

   - Zusammenfassung: Gesamtzahl der Datensätze mit SLA-Korrekturzielen für den von Ihnen angeforderten Monat und das von Ihnen angeforderten Jahr und die Prozentsummen für verpasste und erfüllte Zieldaten.
   - Aufgliederung nach Schweregrad: Angreifbare Elemente, bei denen Korrekturziele nicht eingehalten wurden, werden nach Schweregrad „Kritisch“, „hoch“, „Mittel“ und „Niedrig“ aufgegliedert.
   - Aufgliederung nach Zuweisungsgruppen: Prozentsatz der Gesamtdatensätze mit verpassten Zielen, aufgeschlüsselt nach Zuweisungsgruppen.
   - Weitere Informationen: Link „Compliance zur Korrektur für Oktober 2024“ – weitere Informationen zu den Daten anzeigen. In UI16 wird eine neue Registerkarte geöffnet.

3. Sie können spezifischere Informationen zu verpassten SLAs anfordern, z. B. Welche Asset-Typen haben die am häufigsten verpassten SLAs berücksichtigt?
   Die Ergebnisse werden für die Daten für den Monat Ihrer ursprünglichen Anforderung nach Asset-Typ organisiert, z. B. Windows Server, Datenbank, Linux Server, und so weiter.

4. Sie können spezifischere Informationen über die Produktivität Ihrer Teams in diesem Monat anfordern, z. B. Welche Zuweisungsgruppe hatte die wenigsten verpassten kritischen SLAs?
   Die Zuweisungsgruppe mit der geringsten Anzahl von wird zurückgegeben Kritisch Vits, die das SLA verpasst haben.

5. Sie können diese Ergebnisse beispielsweise mit einem anderen Monat vergleichen: Wie schneiden diese Daten im Vergleich zu November 2024 ab?
   Die Ergebnisse sind in Abschnitte organisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vergleichszusammenfassung: Gesamtzahl der Datensätze mit SLA-Korrekturzielen für den Zeitraum, den Sie zuerst angefordert haben (**Oktober 2024**) Im Vergleich zu Ihrer letzten Anforderung (**November 2024**).
- Aufgliederung nach Schweregrad: Angreifbare Elemente, bei denen Korrekturziele nicht eingehalten wurden, werden nach Schweregrad aufgeschlüsselt: Kritisch , Hoch , Mittel , Und Niedrig .
- Beobachtungen: Analyse von Daten und Einblicke in Datentrends basierend auf dem Vergleich.
- Weitere Informationen: Link „Compliance zur Korrektur für November 2024“ – weitere Informationen zu den für den Vergleich verwendeten Daten anzeigen. In UI16 wird eine neue Registerkarte geöffnet.

Now Assist für Vulnerability Response Referenzinformationen

Informationen zur Sammlung von Tools, Agents und KI-Agents für Now Assist für Vulnerability Response.

Referenzen

Zeigen Sie Übersichten für die folgenden agentischen Workflows an.

- Vulnerability Response KI-Agent-Sammlung für den agentischen Workflow „Schwachstellenrisiko bewerten“
- Vulnerability Response KI-Agent-Sammlung für den agentischen Workflow „Schwachstellen-Korrekturstatus analysieren“

Vulnerability Response KI-Agent-Sammlung für den agentischen Workflow „Schwachstellenrisiko bewerten“

Die Tools und KI-Agents für den agentischen Workflow Schwachstellenrisiko bewerten.

Übersicht über den Agentic-Workflow

Die folgenden agentischen Workflows sind in der Anwendung Now Assist für Vulnerability Response enthalten:

- Bewerten Sie den agentischen Workflow des Schwachstellenrisikos
- Analysieren Sie den Workflow zur Schwachstellenkorrektur

Wenn Sie diesen agentischen Workflow ändern möchten, können Sie dies Duplikat
Passen Sie die Einstellungen an Ihre spezifischen Anforderungen an, und aktivieren Sie die duplizierte Version des agentischen Workflows.

Bewerten Sie das Schwachstellenrisiko – Übersicht über den agentischen Workflow

Verwenden Sie den agentischen Workflow Schwachstellenrisiko bewerten aus der Now Assist Bereich, der Ihnen hilft:

- Bestimmen Sie, ob Ihre Konfigurationselemente (CIs) und Business-Services bekannten Schwachstellen ausgesetzt sind.
- Bestimmen Sie die potenziellen Auswirkungen, die eine bestimmte Schwachstelle in Ihrer Umgebung haben kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überprüfen Sie CIs auf neue ausnutzbare Schwachstellen der Cybersicherheits- und Infrastruktursicherheitsbehörde (CISA) (Zero-Day).
- Erstellen Sie Überwachungsthemen im Vulnerability Manager-Arbeitsbereich, um angreifbare Elemente zu beheben.
- Passen Sie Inhalte in natürlicher Sprache an.

Service Desk-Mitarbeiter, die im agentischen Workflow „Schwachstellenrisiko bewerten“ verwendet werden

- Ausführung Der Vulnerability Response-Aktion
- CISA – Analyse bekannter ausgenutzter Schwachstellen
- Ratgeber Für Bewertung Des Schwachstellenrisikos

[store-future: BEGIN review]

Tools, die dem agentischen Workflow „Vulnerability Response: Impact and Exposure Assessment“ zugeordnet sind

Die folgenden Tools sind KI-Agents zugeordnet, die im agentischen Workflow „Vulnerability Response: Impact and Exposure Assessment“ verwendet werden.

Tools, die dem agentischen Workflow „Vulnerability Response: Impact and Exposure Assessment“ zugeordnet sind

Tooltyp	Ausführungsmodus	Name	Beschreibung
Skripte	Autonom	Rufen Sie weitere Informationen zu einer Schwachstelle ab	Das Tool für CISA – Analyzer-Agent für bekannte ausgenutzte Schwachstellen ruft weitere Informationen zu einer Schwachstelle mithilfe der ID der Schwachstellen-ID ab.
Skripte	Autonom	Suchen Sie nach aktuellen CISA-KEVs	Tool für CISA – Analyse bekannter ausgenutzter Schwachstellen – Agent überprüft basierend auf der Anzahl der von Ihnen eingegebenen Tage auf aktuelle CISA-Schwachstellen und den Katalog bekannter ausgenutzter Schwachstellen (KEV).
Skripte	Autonom	Business-Service-Schwachstellenzusammenfassung	Tool for Vulnerability Exposure Assessment Advisor Agent identifiziert die betroffenen Konfigurationselemente (CI) und ihre jeweiligen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tools, die dem agentischen Workflow „Vulnerability Response: Impact and Exposure Assessment“ zugeordnet sind (Fortsetzung)

Tooltyp	Ausführungsmodus	Name	Beschreibung
			Schwachstellen. Außerdem werden die aktiven angreifbaren Elemente (VIT) und die VIT-Kategorisierungen identifiziert.
Skripte	Autonom	CI-Schwachstellenanalyse	Tool for Vulnerability Exposure Assessment Advisor-Mitarbeiter identifiziert Schwachstellen, die sich auf ein Konfigurationselement auswirken.
Skripte	Autonom	CVE-Auswirkungsanalyse	Das Tool für die Bewertung des Schwachstellenrisikos analysiert die Auswirkungen der CVE-ID (Common Vulnerability Exposure ID) eines Common Vulnerability Exposure, indem die Anzahl der betroffenen Vits und Business-Services sowie ihre jeweilige Relevanz berücksichtigt werden.
Skripte	Autonom	Überwachungsthema erstellen	Tool für Vulnerability Response Action Executor Agent, das basierend auf gesammelten Informationen zu Schwachstellen und Konfigurationselementen ein Überwachungsthema erstellt.

[End]

[store-future: BEGIN review]

Auslöser für den agentischen Workflow „Vulnerability Response: Impact and Exposure Assessment“

Für diesen agentischen Workflow sind keine Auslöser vorhanden. Bei Bedarf können Sie einen Auslöser hinzufügen, um den agentischen Workflow automatisch aufzurufen.

[End]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response KI-Agent-Sammlung für den agentischen Workflow „Schwachstellen-Korrekturstatus analysieren“

Die Tools und KI-Agents für den agentischen Workflow Schwachstellen-Korrekturstatus analysieren.

Analysieren Sie die Übersicht über den agentischen Workflow zur Schwachstellenkorrektur

Verwenden Sie den agentischen Workflow Schwachstellen-Korrekturstatus analysieren aus der Now Assist Bereich, der Ihnen hilft:

- Erhalten Sie Einblicke in Ihre Compliance-Metriken und -Statistiken, um herauszufinden, wie gut Sie Korrekturzieldaten für Datensätze von angreifbaren Elementen (VIT) einhalten.
- Zeigen Sie Ihre monatlichen VIT-Datensatzkorrektursummen an, und identifizieren Sie verpasste Ziele.
- Aufgliederung der Korrekturdaten für Vits nach **Schweregrad** , **Zuweisungsgruppe** , **Konfigurationselement** Und **Schwachstelle** Für Ihre monatlichen Compliance-Überprüfungen von Servicelevel-Vereinbarungen (Service Level Agreement, SLA).

Wenn Sie diesen agentischen Workflow ändern möchten, können Sie dies Duplikat Passen Sie die Einstellungen an Ihre spezifischen Anforderungen an, und aktivieren Sie die duplizierte Version des agentischen Workflows.

Agent, der im agentischen Workflow „Schwachstellen-Korrekturstatus analysieren“ verwendet wird

Der Anbieter von Compliance-Einblicken für Korrekturmaßnahmen wird vom agentischen Workflow „Schwachstellen-Korrekturstatus analysieren“ verwendet.

[store-future: BEGIN review]

Tools, die dem Anwendungsfall „Vulnerability Response: Korrekturziele“ zugeordnet sind

Die folgenden Tools sind einem KI-Agent zugeordnet, der im agentischen Workflow „Vulnerability Response: Korrekturziele“ verwendet wird.

Tools, die dem agentischen Workflow „Vulnerability Response: Korrekturziele“ zugeordnet sind

Tooltyp	Ausführungsmodus	Name	Beschreibung
Skripte	Autonom	Rufen Sie Statistiken Zur Korrektur-Compliance Ab	Tool für Compliance-Einblicke in Korrekturmaßnahmen – der Service Desk-Mitarbeiter erfasst Compliance-Statistiken für Korrekturen nach Monat, Schweregrad, Zuweisungsgruppe, Schwachstelle und Konfigurationselement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[End]

[store-future: BEGIN review]

Auslöser für den agentischen Workflow „Vulnerability Response: Korrekturziele“

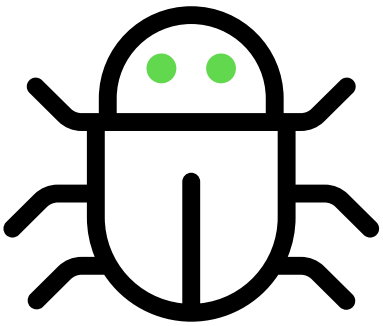
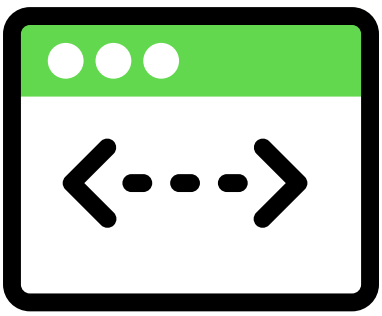
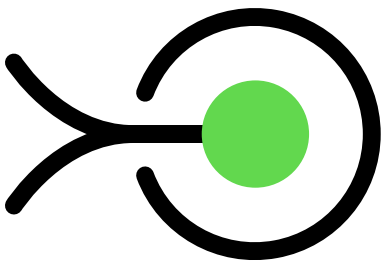
Für diesen agentischen Workflow sind keine Auslöser vorhanden. Bei Bedarf können Sie einen Auslöser hinzufügen, um den agentischen Workflow automatisch aufzurufen.

[End]

Angriffsoberflächenverwaltungsanwendungen

Die Vulnerability Response Und andere Anwendungen, aus denen das Angriffsoberflächenmanagement besteht, helfen Ihnen, Ihre angreifbaren Assets zu priorisieren und Kontext hinzuzufügen, damit Sie feststellen können, wann geschäftskritische Systeme bedroht sind. Mit der CMDB können Ihre Sicherheitsteams auch systemübergreifende Abhängigkeiten leicht identifizieren und schnell die Geschäftsauswirkungen von Changes oder Ausfallzeiten bewerten.

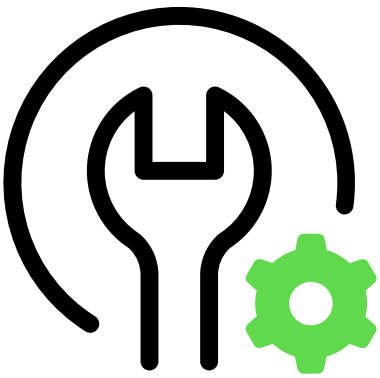
Vulnerability Response Anwendungen

Vulnerability Response	Application Vulnerability Response	Container Vulnerability Response
		
Erfahren Sie mehr über die Anwendung Vulnerability Response	Erfahren Sie mehr über die Anwendung Application Vulnerability Response	Erfahren Sie mehr über die Anwendung Container Vulnerability Response

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Anwendungen (Fortsetzung)

Konfigurations-Compliance



Erfahren Sie mehr über die Anwendung Configuration Compliance

Software-Stückliste

Erfahren Sie mehr über die Anwendungen „Software Bill of Materials“

Vulnerability Response Arbeitsbereiche

Arbeitsbereich des Schwachstellenmanagers

Erfahren Sie mehr über den Vulnerability Manager-Arbeitsbereich

Arbeitsbereich für IT-Korrekturen

Erfahren Sie mehr über den Arbeitsbereich „IT-Korrektur“

Arbeitsbereich der Schwachstellenbewertung

Erfahren Sie mehr über den Arbeitsbereich „Schwachstellenbewertung“

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community

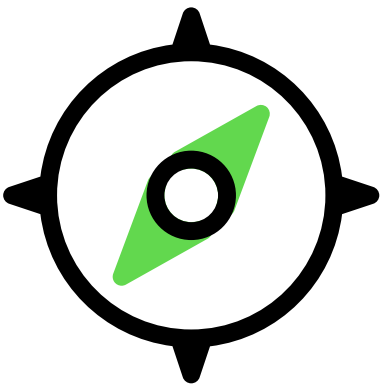
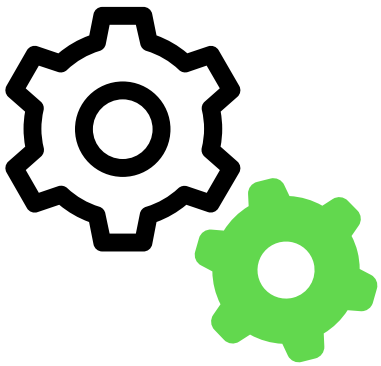
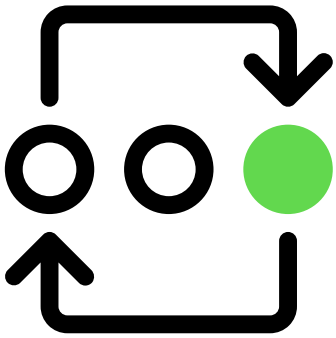
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Vulnerability Response

Die National Vulnerability Database (NVD) und andere Quellen erfassen Informationen zu bekannten Schwachstellen. Diese Schwachstellen können Schwachstellen in Software, Betriebssystemen, die Malware ausnutzen kann, und andere Angriffe umfassen. Die ServiceNow® Vulnerability Response Die Anwendung unterstützt Sie bei der Nachverfolgung, Priorisierung und Behebung dieser Schwachstellen.

Vulnerability Response

Untersuchen	Einrichten und konfigurieren	Integrieren
		
Erfahren Sie mehr über die Funktionen von Vulnerability Response	Installieren und richten Sie Ihre Vulnerability Response-Anwendung ein	Erweitern Sie Vulnerability Response durch Integration mit anderen Anwendungen

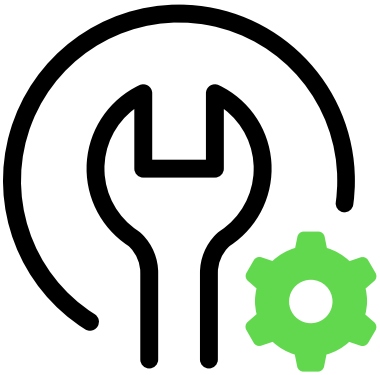
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response (Fortsetzung)

Verwenden Sie die Vulnerability Response-Arbeitsbereiche

Erfahren Sie, wie Sie Vits in den Arbeitsbereichen „Schwachstellenmanager“, „IT-Korrektur“ und „Schwachstellenbewertung“ überwachen, verwalten und beheben.

Beheben

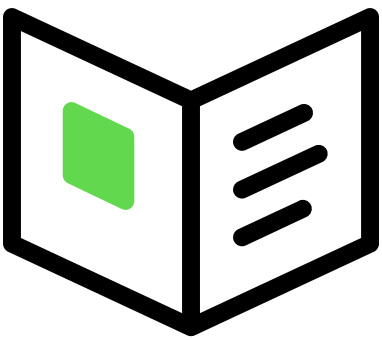


Verwenden Sie die Funktionen von Vulnerability Response, um Ihre Schwachstellen zu beheben und Ihre Assets zu schützen

Analytics Und Reporting

Überwachen Sie den Korrekturfortschritt

Referenz



Erhalten Sie weitere Details zu Vulnerability Response-Versionshinweisen, Komponenten und Referenzinformationen zu Feldern, Tabellen und Eigenschaften

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Erkunden Sie Vulnerability Response Anwendung

Die ServiceNow® Vulnerability Response Die Anwendung importiert und gruppiert angreifbare Elemente automatisch gemäß Regeln, mit denen Sie Schwachstellen schnell beheben können. Schwachstellendaten werden aus externen Quellen abgerufen, z. B. aus der National Vulnerability Database (NVD) und Integrationen von Drittparteien, und mit von entwickelten Anwendungen verarbeitet ServiceNow®.

Sehen Sie sich einen Überblick über die Reaktion auf Schwachstellen an, die angreifbare Elemente, Korrekturaufgaben und ihre Lebenszyklen definiert.

Übersicht über die typische Schwachstellenantwort in einem Unternehmen im Vergleich zur Schwachstellenantwort mit ServiceNow und definiert angreifbare Elemente, Schwachstellengruppen und ihre Lebenszyklen.

Vulnerability Response Und Ihre Unternehmensumgebung

In einer Enterprise-Umgebung verwenden Organisationen normalerweise Schwachstellen-Scanner und Bewertungstools, um die Risiken zu identifizieren und zu verwalten, die Schwachstellen für ihre Assets darstellen. Schwachstellen, die von diesen Tools identifiziert werden, gelten als Risiken für die Sicherheits- und IT-Teams, die für die Wartung und Sicherung der Assets einer Organisation verantwortlich sind. Einige Risiken können die folgenden Arten identifizierter Schwachstellen umfassen, sind aber nicht darauf beschränkt:

- Abhängigkeit von veralteter Software oder falsch konfigurierten Systemen
- Ungesicherte Netzwerkprotokolle
- Abhängigkeit von fehlerhaften Softwarebibliotheken von Drittanbietern
- Schlechte oder inkonsistente Systemadministrationshygiene
- Baseline-Systembilder, die nicht gehärtet sind

Da diese potenziellen Risiken exponiert sind, stehen Sicherheits- und IT-Teams häufig vor Herausforderungen bei der Verarbeitung und Verarbeitung des Volumens von Schwachstelleninformationen, die aus ihren Scan- und Bewertungstools generiert werden. Insbesondere finden sich diese Teams überfordert, wenn sie ein hohes Volumen identifizierter Schwachstellen verwalten und umsetzbare Reaktionsmaßnahmen entwickeln, um die potenziellen Risiken ihrer Organisation zu mindern.

Sie können diese Herausforderungen für Ihre eigene Sicherheitslage identifizieren, indem Sie die folgenden Fragen stellen:

- Welche identifizierten Schwachstellen sollten zuerst überprüft werden?
- Was bedeuten diese identifizierten Schwachstellen für unsere Organisation?
- Wer sollte für identifizierte Risiken verantwortlich sein und besitzen?
- Wer sollte handlungsfähig sein und an der Lösung/Minderung dieser Risiken arbeiten?

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wie können wir identifizierte Schwachstellen mit den vorhandenen Ressourcen effektiv mindern?
- Was sind die potenziellen unbeabsichtigten Ergebnisse der Reduzierung der identifizierten Schwachstellen?
- Welchen Prozess verfolgen wir, um Schwachstellen zu beheben, die von uns unternommenen Schritte nachzuverfolgen und sicherzustellen, dass unsere Aktionen funktioniert haben?
- Woher wissen wir, ob wir Fortschritte bei der Reduzierung unserer Gesamtrisikosituation machen?

Vulnerability Response, Security Operations Und ServiceNow AI Platform®

Die Vulnerability Response Anwendung ist Teil von Security Operations suite. Zusammen helfen diese Anwendungen Ihnen, Ihre Assets zu schützen, indem sie Ihre allgemeine Sicherheitslage verbessern.

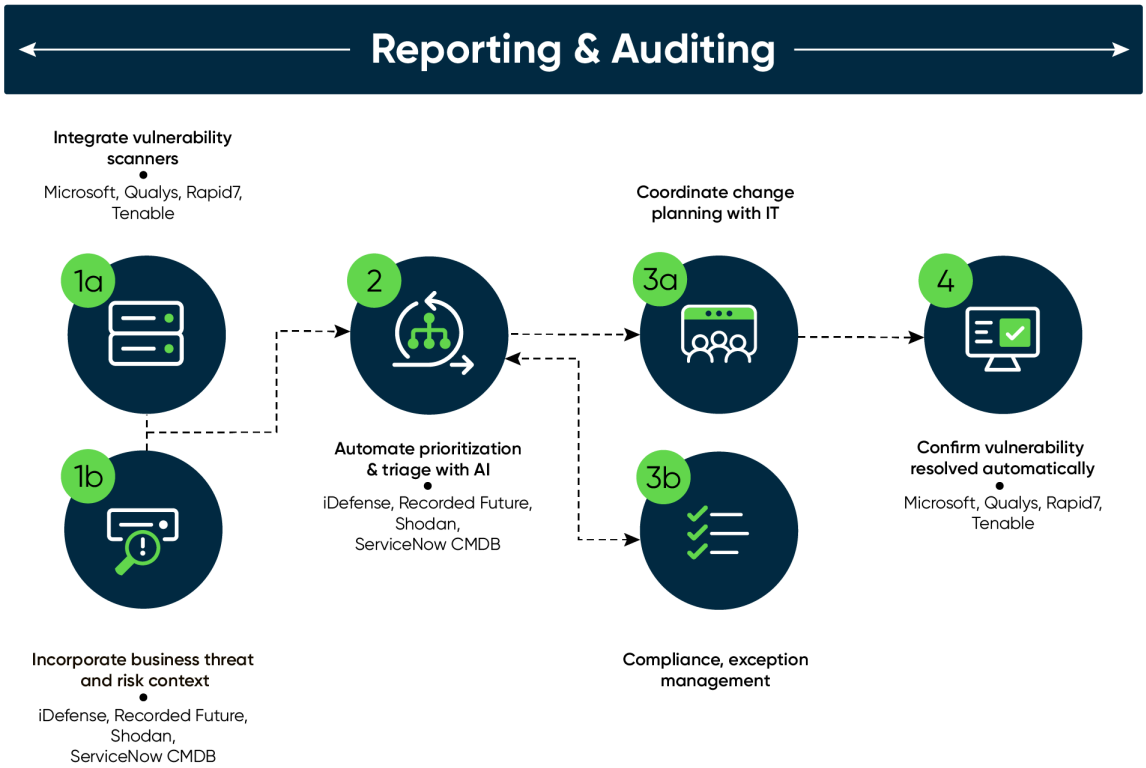
Die ServiceNow Vulnerability Response Die Anwendung hat zwei primäre Ziele:

- Helfen Sie den Sicherheitsteams, die bei der Verarbeitung großer Mengen von Schwachstellendaten gefordert werden.
- Helfen Sie den Betriebsteams, die mit der Behebung von Schwachstellen beauftragt sind.

Auf diese Weise können Sie verwenden Vulnerability Response Anwendung zur Automatisierung des Informationsflusses, von der Integration über die Untersuchung und dann bis zur Lösung.

Der Schwachstellenverwaltungsprozess in ServiceNow AI Platform®Kann Prozesse, Daten, Berichterstellung und Automatisierung mit umfassen CMDB.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Integrieren Sie Scanner von Drittparteien und ServiceNow® Anwendungen mit Vulnerability Response Anwendung zum Erfassen bekannter Schwachstellendaten.
- Verbessern Sie Ihre erfassten Schwachstellendaten mit Exploit, Threat Intelligence, Risiko und Geschäftskontext. Verwenden Sie diese Daten, um Sie bei Patch- und Korrekturstrategien zu unterstützen.
- Importierte Schwachstellen aus dem NVD und Erkennungsdaten aus Drittparteiprodukten werden mit den Assets in Ihrer CMDB abgeglichen. Die Selektierung kann Folgendes umfassen: Erstellen von Korrekturaufgaben, die aus mehreren angreifbaren Elementen bestehen, d. h. Ihre Assets, die festgestellte Schwachstellen aufweisen, Gruppieren dieser Aufgaben nach Kategorie, Priorisierung und Zuweisung an Teams.
- Nutzen Sie ein koordiniertes Change- und Ausnahmemanagement, um Schwachstellen zu beheben, die möglicherweise zusätzliche manuelle Eingriffe, mehr Zeit bis zur Lösung oder umfassende Forschung erfordern.
- Bestätigen Sie, dass Schwachstellen durch Erkennungen aus Ihren Scannerprodukten automatisch behoben und aktualisiert werden.

Wer verwenden könnte Vulnerability Response In Ihrer Organisation

Vulnerability Response Anwender lassen sich in der Regel in zwei Personae einteilen.

Schwachstellenanalyst

Die Persona des Schwachstellenanalysten befindet sich normalerweise in Sicherheit, Risk and Compliance oder Management. Diese Benutzer überwachen Schwachstellen und bestimmen, wann die Korrekturprozesse initiiert werden sollen.

Wichtig:
Der Schwachstellenanalyst verwendet hauptsächlich Arbeitsbereich des Schwachstellenmanagers Dient zum Überwachen und Erstellen von Korrekturaufgaben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verantwortlicher für Korrektur

Die Persona „Korrekturbesitzer“ ist normalerweise Teil von IT Operations, DevOps/Engineering oder einem Serviceverantwortlichen. Diese Anwender führen die Korrekturaufgaben aus, die zum Beheben von Schwachstellen erforderlich sind. Sie können Ausnahmen oder Change-Anforderungen übermitteln, wenn kontrollierte Prozesse für die Wartung oder Entfernung von Assets erforderlich sind.

Wichtig:
Der Korrekturbesitzer bearbeitet hauptsächlich Korrekturaufgaben aus innerhalb von Arbeitsbereich für IT-Korrekturen.

Application Vulnerability Response

Die Application Vulnerability Response(AVR)-Funktion von ServiceNow® Vulnerability Response Die Anwendung importiert angreifbare Anwendungselemente (AVITs) und ermöglicht es Ihnen gemäß Regeln, Anwendungsschwachstellen zu beheben. Sie ist als separates Abonnement verfügbar. Für Application Vulnerability Response Dokumentation siehe Application Vulnerability Response erkunden.

Verfügbare Versionen

Für ein Glossar von Begriffen und weiteren Verweisen, einschließlich Links, Problembehandlung, Wissensartikeln sowie Felddaten in den Formularen und Datensätzen in Vulnerability Response, Siehe Vulnerability Response Referenzinformationen.

Freigabeversion	Release-Hinweise
Vulnerability Response V23.0	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Vulnerability Response Anwendungen Und CSDM Tabellen

Die Vulnerability Response, Application Vulnerability Response, Integrationen von Schwachstellen von Drittparteien und Software Bill of Materials Anwendungen verwalten (Daten mittragen zu) CSDM Tabellen. Diese Anwendungen verwenden auch Daten aus CSDM Tabellen, die andere Anwendungen generieren. Mehrere ServiceNow Produkte profitieren daher von diesen und fügen ihnen einen Mehrwert hinzu Security Operations Anwendungen. Weitere Informationen finden Sie unter Vulnerability Response Anwendungen Und CSDM Tabellen.

Installation von Vulnerability Response Und unterstützte Anwendungen

Die Vulnerability Response Die Anwendung ist über verfügbar ServiceNow Store. Die Anwendung unterstützt andere ServiceNow Anwendungen und Integrationen von Drittparteien, die Sie auch aus herunterladen ServiceNow Store. Weitere Optionen sind auch verfügbar, um das grundlegende Setup zu erweitern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgaben für das Standard-Setup

Die Vulnerability Response Anwendung ist als erster Schritt erforderlich. Weitere Informationen zur Installation finden Sie unter Implementierungsprüfliste für Vulnerability Response Anwendung Und Installieren Sie Vulnerability Response Anwendung.

- Nachdem die Installation abgeschlossen ist, können Sie Konfigurieren Sie Vulnerability Response mit dem Setup-Assistenten .

  Weisen Sie mit dem Setup-Assistenten Anwender und Gruppen für den Zugriff auf die Anwendung zu, erstellen oder bearbeiten Sie Zuweisungsregeln, Regeln für Korrekturaufgaben und Zieldaten, richten Sie Risikorechner ein.

- Sie können auch eine oder mehrere unterstützte Drittanbieterintegrationen über den Setup-Assistenten auswählen, installieren und konfigurieren. Diese Integrationen rufen Schwachstellendaten von externen Systemen und Lieferanten ab. Weitere Informationen zur Funktionsweise von Integrationen und den von unterstützten Integrationen Vulnerability Response, Siehe Vulnerability Response-Integrationen.
- Führen Sie vor der Implementierung von Drittpartei-Integrationen die geplante NVD-Integration und CWE-Aufgabe als Teil Ihres ersten Setups von aus Vulnerability Response.

  Siehe Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken Und Konfigurieren und führen Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen aus Weitere Informationen zum Installieren, Konfigurieren und Anzeigen der NVD- und CWE-Bibliotheken.

- Wählen Sie gegebenenfalls eine Analytics-Anwendung aus. Die Anwendung Performance Analytics Content Pack für Vulnerability Response enthält Berichte, die alle Phasen des Schwachstellenmanagement-Lebenszyklus abdecken.

  [Optional] Installieren und konfigurieren Sie Performance Analytics for Vulnerability Response[PA] Anwendung Anwendung.

- Wählen Sie gegebenenfalls eine Lösungsanwendung aus. Das Lösungsmanagement hilft Ihnen, die Schwachstellen in Ihrer Umgebung mit den Lösungen zu korrelieren, die sie beheben könnten. [Optional] Anwendung Solution Management for Vulnerability Response installieren.

  Hinweis:

  - Wenn Vulnerability Solution Management Anwendung ist aktiviert, die Integration der Microsoft Security Response Center-Lösung Und Red Hat Solution Integration Können im Setup-Assistenten bearbeitet werden.

  - Vulnerability Solution Management Erfordert ein separates Abonnement. Weitere Informationen finden Sie unter Vulnerability Solution Management.

- [Optional] Installieren Sie die ServiceNow Agent-App und Vulnerability Response Mobile-App Für Mobile Experience für Vulnerability Response.

Andere Setup-Aufgaben, die Sie ausführen können

Diese zusätzlichen Setup-Aufgaben ergänzen Ihre Basiskonfiguration und unterstützen die Korrektur mit Optionen für Berichterstellung, E-Mail-Benachrichtigungen, native Integrationskonfiguration und die Arbeit mit angreifbaren Elementen. Die meisten dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgaben werden außerhalb des Setup-Assistenten ausgeführt. Weitere Informationen finden Sie unter Zusätzlich Vulnerability Response Setup- und Konfigurationsaufgaben.

Erweiterte Aufgaben außerhalb des Standard-Setups

Diese optionalen Konfigurationsaufgaben werden außerhalb des Setup-Assistenten ausgeführt und erfordern Codierung oder erweiterte Funktionen ServiceNow Fachwissen und werden nicht als Teil der Basiskonfiguration betrachtet. Weitere Informationen finden Sie unter Erweitert Vulnerability Response Konfigurationsaufgaben.

Vulnerability Response Personas und granulare Rollen

Bevor Sie Schwachstellen erfolgreich mit beheben können Vulnerability Response Anwendung müssen Sie Ihren Anwendern und Gruppen im Setup-Assistenten Personas und Rollen zuweisen.

Einer der ersten Konfigurationsschritte, die für erforderlich sind Vulnerability Response Die Anwendung dient zum Zuweisen von Rollen an Anwender und Gruppen. Rollen definieren, was Anwender und Gruppen in sehen und tun können Vulnerability Response, Performance Analytics for Vulnerability Response, Und alle Drittpartei-Integrationen mit Vulnerability Response.

Sie weisen vorhandenen Anwendern und Gruppen im Setup-Assistenten Persona-Rollen zu. Weitere Informationen finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.

Hinweis:

Wenn Sie ein Upgrade-Kunde sind, können Sie weiterhin Ihre vorhandenen Rollen für verwenden Vulnerability Response Anwendung. Der Zugriff für Anwender und Gruppen, die mit den Berechtigungen „sn_vul.Vulnerability_read“ und „sn_vul.Vulnerability_write“ vor v10.3 zugewiesen wurden, hat sich nicht geändert.

Um jedoch mehr Kontrolle darüber zu erhalten, was Anwender und Gruppen im tun und sehen können Vulnerability Response Anwendung auf Aufgabenebene. Sie können granulare Rollen verwenden. Weitere Informationen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Wenn Sie bereits Rollen mit dem Setup-Assistenten zugewiesen haben und granulare Rollenzuweisungen für alle Anwender und Gruppen über das Modul „Anwenderverwaltung“ verwalten möchten, finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response Weitere Informationen finden Sie unter .

Persona-Rollen und granulare Rollen beginnen

Schlüsselbegriffe.

Rolle

Rollen definieren, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung.

Gruppe

Eine Reihe von Anwendern, die bestimmte Rollen und einen gemeinsamen Zweck teilen.

Persona-Rolle

Eine vorkonfigurierte Rolle in der Anwendung, die aus mehreren granularen Rollen besteht. Die Persona-Rollen in Setup-Assistent, Schwachstellenadministrator, Schwachstellenanalyst, Korrekturbesitzer, Konfigurationselementmanager, und Exception Manager sind so konzipiert, dass sie den allgemeinen Stellenbezeichnungen für Manager, Analysten und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Serviceverantwortliche in einer IT-Organisation oder Schwachstellen-Korrekturgruppe entsprechen.

Geerbte Rollen

Ein Begriff, der Rollen beschreibt, die Anwender automatisch erwerben, wenn ihnen andere Rollen zugewiesen werden. Beispielsweise erben alle Anwender oder Gruppen, die mit der Persona sn_vul.Remediation_owner zugewiesen sind, auch die granularen Rollen sn_vul.read_assigned,sn_vul.write_assigned.

Zugriffssteuerungsliste (ACL)

Zugriffssteuerungslisten schränken den Zugriff auf Daten ein, indem sie von Anwendern verlangen, eine Reihe von Anforderungen zu erfüllen, bevor sie mit ihnen interagieren können.

Beginnt ab Vulnerability Response V16.5, um zu schützen, dass Berichte zugänglich gemacht werden, legen Sie fest **Alle ACLs „Report_View“** Als `active=true`. Diese ACL stellt sicher, dass die geschützten Daten nur autorisierten Anwendern zur Verfügung stehen.

Im Setup-Assistenten weisen Sie Gruppen und Anwender Persona-Rollen zu.

Hinweis:
Im Setup-Assistenten ist die Systemadministratorrolle (admin) für die Aufgaben im ersten Abschnitt erforderlich, die Rollen zuweisen und Integrationen installieren. Nachdem Sie im Setup-Assistenten Persona-Rollen zugewiesen und Integrationen installiert haben, können Sie einen Anwender oder eine Gruppe mit der Rolle sn_vul.Vulnerability_admin zuweisen, um alle verbleibenden Aufgaben im Setup-Assistenten abzuschließen und zu verwalten Vulnerability Response Anwendung.

Die folgenden Tabellenlisten Vulnerability Response Mit der Anwendung installierte Persona-Rollen.

Persona-Rollen für Vulnerability Response	Beschreibung
Weisen Sie Benutzern oder Gruppen sn_vul.Vulnerability_admin – Schwachstellenadministrator zu.	Benutzer mit dieser Rolle haben vollständigen Zugriff auf die Anwendung Vulnerability Response (VR) und ihre Datensätze. Benutzer mit dieser Rolle konfigurieren alle VR-Anwendungen und -Regeln und installieren Drittanbieterintegrationen.
Weisen Sie Benutzern und Gruppen sn_vul.Vulnerability_Analyst – Schwachstellenanalyst zu.	Benutzer und Gruppen mit dieser Rolle zeigen alle Datensätze für die VI-Korrektur an und aktualisieren sie.
Weisen Sie Anwendern und Gruppen sn_vul.Remediation_owner – Korrekturbesitzer zu.	Benutzer und Gruppen mit dieser Rolle beheben Schwachstellen, die ihnen oder einer Gruppe zugewiesen sind, der sie angehören. Gruppen oder Anwender mit dieser Rolle zeigen die ihnen oder einer Gruppe, der sie angehören, zugewiesenen Datensätze an und aktualisieren sie.
Weisen Sie Anwendern und Gruppen sn_vul.ci_Manager zu.	Benutzer und Gruppen mit dieser Rolle verwalten die Neuklassifizierung nicht abgeglichener Konfigurationselemente (CIs), die nicht in der Configuration Management Database (CMDB) gefunden werden.
Weisen Sie bestimmten Bereichen in der Anwendung Lesezugriff nach Aufgabe zu.	Weisen Sie beispielsweise sn_vul.read_all zu, damit ein Anwender alle VR-Datensätze anzeigen kann. Um Lesezugriff zum Anzeigen von Regeln für Korrekturaufgaben zu erhalten, weisen Sie

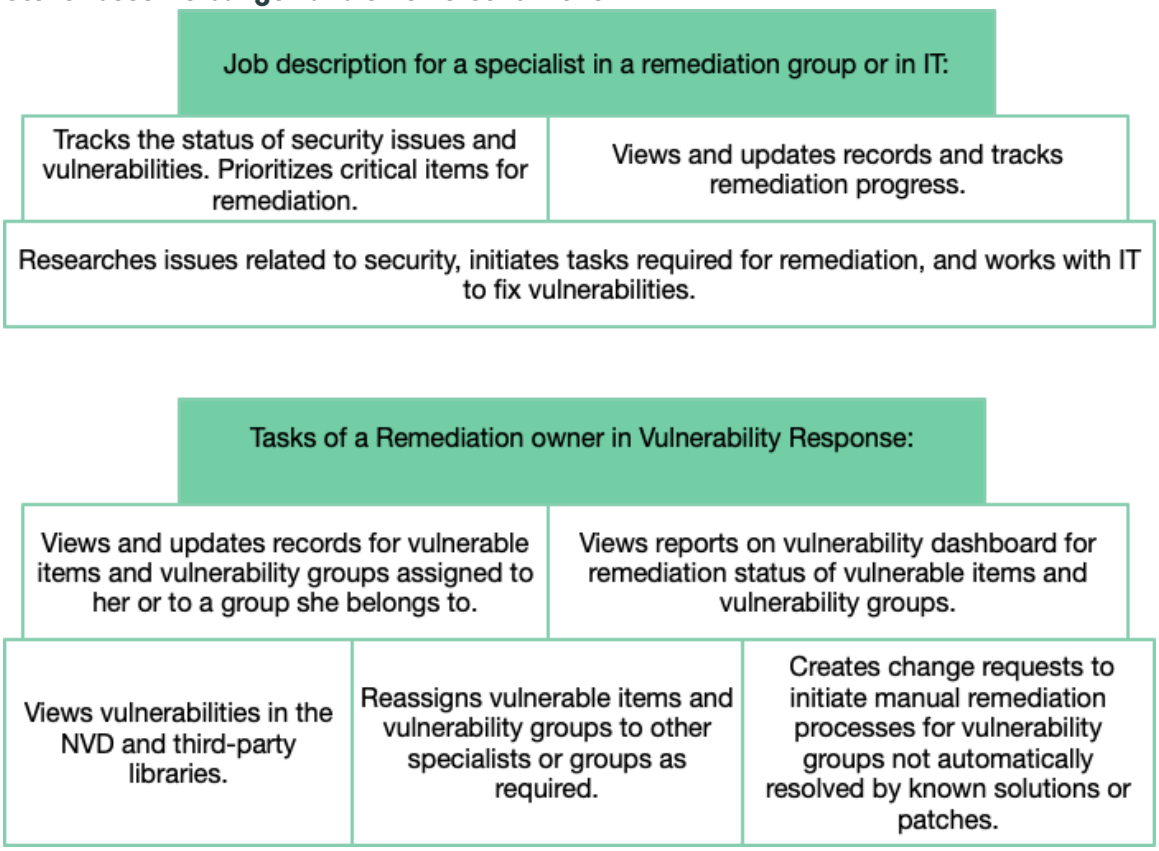
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persona-Rollen für Vulnerability Response	Beschreibung
	sn_vul.read_Group_rules zu. Benutzer und Gruppen mit dieser Rolle aktualisieren keine Datensätze.

Granulare Rollen und Persona-Rollen

Eine Möglichkeit, über Persona-Rollen nachzudenken, besteht darin, zu berücksichtigen, wie sich ihre Beschreibungen auf Stellenbeschreibungen für verschiedene Positionen IN DER IT- oder Schwachstellenbeseitigung in Ihrer Organisation beziehen können. Die folgende Abbildung zeigt eine mögliche Stellenbeschreibung für einen Korrekturspezialisten in DER IT UND wie sich die diesem Auftrag zugeordneten Aufgaben auf die Aufgaben einer Korrekturbesitzer-Persona-Rolle in beziehen Vulnerability Response Anwendung.

Stellenbeschreibungen und eine Persona-Rolle



Sowohl die Auftragsbeschreibung als auch die Persona-Rolle des Korrekturbesitzers können als eine Reihe von Korrekturaufgaben definiert werden. Im vorherigen Bild sitzen eine Stellenbeschreibung und eine Persona-Rolle in grünen Blöcken neben den Aufgaben, die sie beschreiben. In diesem Beispiel entsprechen einige der typischen Stellenanforderungen für einen Spezialisten in einer Korrekturgruppe direkt den Aufgaben, aus denen die Persona des Korrekturbesitzers in besteht Vulnerability Response: Überprüfen und aktualisieren Sie Datensätze, verfolgen Sie den Korrekturstatus von Schwachstellen, priorisieren Sie Elemente für die Korrektur, und wenden Sie Korrekturen und Patches damit an.

Manchmal entsprechen die Aufträge in Ihrer Organisation jedoch nicht direkt den Aufgaben, die eine der fünf Persona-Rollen im ausmachen Vulnerability Response Anwendung. Aus verschiedenen Gründen, z. B. zum Schutz vertraulicher Daten oder zur Einhaltung von Vorschriften, müssen Sie den breiten Zugriff beschränken, den einige der Persona-Rollen Ihren Anwendern und Gruppen gewähren. Oder umgekehrt müssen Sie Anwendern und Gruppen mehr Zugriff gewähren, damit sie ihre Aufgaben ausführen können. Mit granularen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen können Sie Rollen einfach anpassen und den Zugriff von Anwendern und Gruppen steuern Vulnerability Response, Performance Analytics for Vulnerability Response, Und Drittpartei-Integrationen.

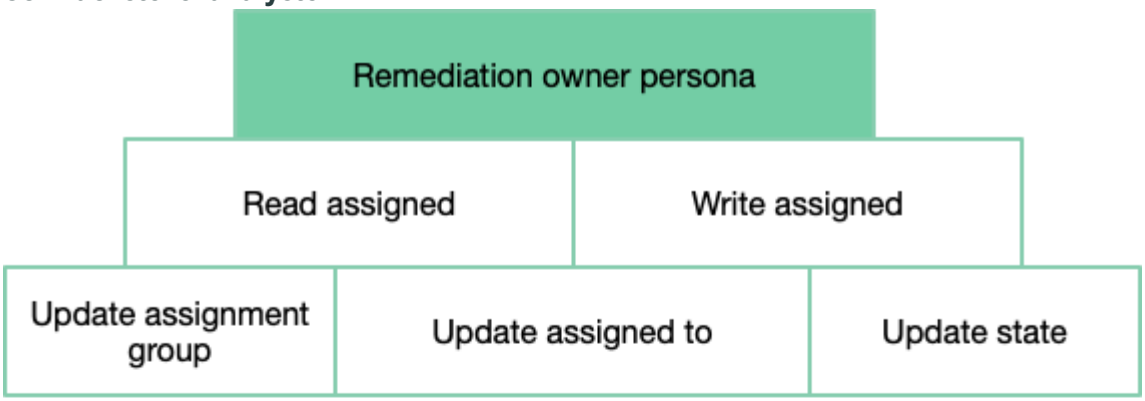
Die granularen Rollen definieren die Aufgaben

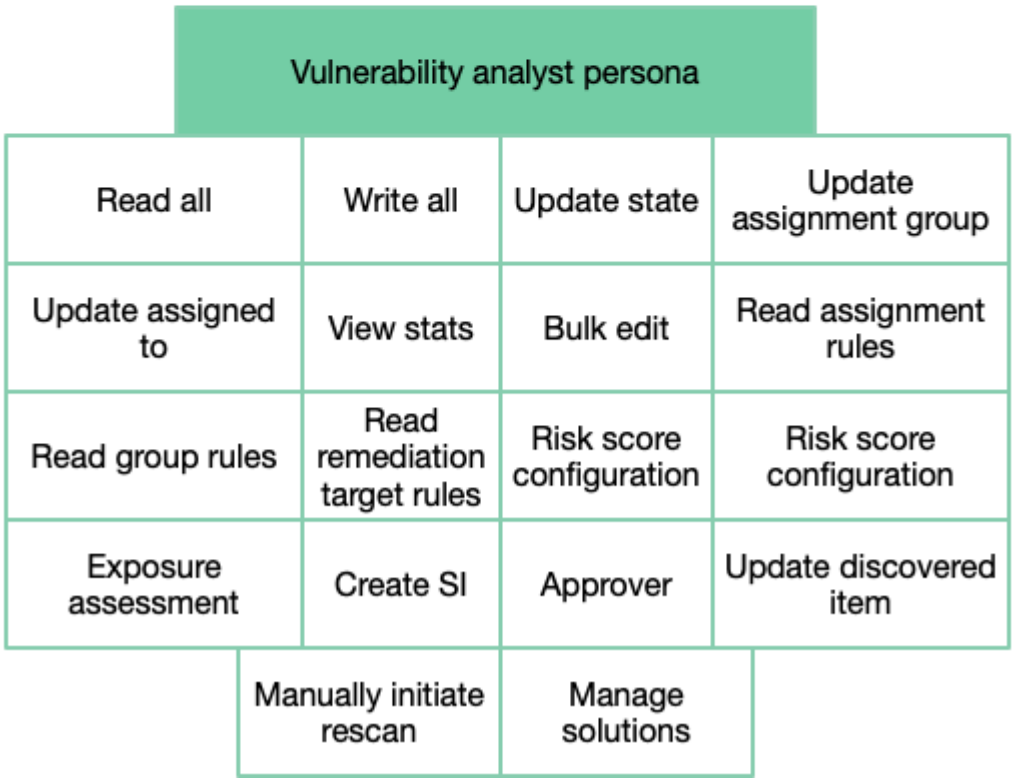
Die Namen für die granularen Rollen in Vulnerability Response Beschreiben Sie normalerweise, was Anwender in tun und sehen können Vulnerability Response Anwendung. Im vorherigen Bild haben beispielsweise Anwender und Gruppen, denen die Persona des Korrekturbesitzers zugewiesen ist, die granularen Rollen sn_vul.read_assigned und sn_vul.write_assigned. Diese granularen Rollen ermöglichen es Anwendern oder Gruppen, angreifbare Elemente und Datensätze für Korrekturaufgaben anzuzeigen und zu aktualisieren, die ihnen zugewiesen sind. Um Beschreibungen bestimmter granularer Rollen anzuzeigen, navigieren Sie als Anwender mit der Systemadministratorrolle zu **Anwenderadministration** > **Rollen** Und suchen Sie die gewünschte Rolle. Rollen, die automatisch geerbt werden, wenn eine Rolle zugewiesen wird, werden aufgelistet. Wenn eine Rolle von anderen Rollenzuweisungen abhängt, werden auch alle erforderlichen Rollen aufgelistet.

In der folgenden Abbildung werden die granularen Rollen sowohl der Rolle des Korrekturbesitzers als auch der Persona des Schwachstellenanalysten dargestellt. Beachten Sie, dass die Persona des Korrekturbesitzers die Berechtigungen „read_all“ und „write_all“ der Persona des Schwachstellenanalysten nicht enthält. Die granularen Rollen read_all und write_all sind erforderlich, damit Anwender und Gruppen alle Datensätze für angreifbare Elemente und Korrekturaufgaben lesen und bearbeiten können. Um diese Rollen anzupassen, fügen Sie einfach granulare Rollen hinzu oder entfernen Sie sie, um den Zugriff zu erweitern oder zu beschränken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Granulare Rollen und die Personas des Korrekturbesitzers und Schwachstellenanalysten





Wenn Ihre Anwender und Gruppen mehr Zugriff haben sollen, als die Persona-Rollen zulassen, können Sie Anwendern und Gruppen feinere Rollen hinzufügen. Umgekehrt können Sie granulare Rollen entfernen, wenn Sie den Zugriff für bestimmte Anwender und Gruppen auf Aufgabenebene beschränken möchten.

Hinweis:
Zum Zuweisen und Bearbeiten granularer Rollen im Modul „Anwenderverwaltung“ ist die Systemadministratorrolle erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Granulare Rollen mit Skripting-Zugriff

Die folgenden Rollen bieten Skriptzugriff auf die aufgeführten Tabellen:

Rolle	Tabelle	Anwendung
sn_vul.Manage_Auto_close_stale_VI	sn_vul_cmn_Auto_close_rule	Vulnerability Response
sn_vul.App_Manage_Auto_close_rule		Vulnerability Response
sn_vul_Container.Manage_Auto_close_stale_VI		Container Vulnerability Response
sn_vul_Container.Manage_assignment_rules	sn_vul_assignment_rule	Container Vulnerability Response
sn_vul.App_Manage_assignment_rules		Application Vulnerability Response
sn_vul.Manage_assignment_rules		Vulnerability Response
sn_vul_agile.write	sn_vul_agile_Tool	Vulnerability Response
sn_vul_int_fw.configure_Integrations	sn_vul_int_fw_Integration	Vulnerability Response

Granulare Rollen im Modul „Anwenderverwaltung“

Ein Beispiel für die Verwaltung granularer Rollen für einen Anwender oder eine Gruppe finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Informationen zum Zuweisen von Persona-Rollen finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.

Vulnerability Response Übersicht über Zuweisungsregeln

Definieren Sie die Kriterien, nach denen angreifbare Elemente (Vits) automatisch einer Zuweisungsgruppe zur Korrektur zugewiesen werden.

Eine standardmäßige Zuweisungsregel, **Der CI-Supportgruppe zuweisen** , Ist im Basissystem enthalten, das angreifbare Elemente dem zuweist **CI-Supportgruppe** . Die Regel „CI-Supportgruppe zuweisen“ weist jeder Supportgruppe, die für das Konfigurationselement (CI) festgelegt ist, das der VIT zugeordnet ist, eine VIT zu.

Hinweis:
Die Zuweisungsregeln bewerten manuell erstellte Zuweisungen nicht neu.

Zuweisungstyp, ob **Manuell** Oder **Regel** Ist über das VIT-Formular und die Listenansicht verfügbar. Jede VIT, die ursprünglich von einer Regel zugewiesen wurde, anschließend aber manuell neu zugewiesen wurde, enthält einen Verweis auf die ursprüngliche Regel.

Verwenden Sie Zuweisungsregel- und Zuweisungstypinformationen, um Fälle zu identifizieren, in denen die Zuweisungsregeln keine richtige Übereinstimmung für den beabsichtigten Empfänger gefunden haben. Sie können die Informationen auch verwenden, um zu identifizieren, welche Regeln die meisten Neuzuweisungen hatten.

Die durch Zuweisungsregeln festgelegten Zuweisungsgruppen werden von verwendet **Regeln Für Korrekturaufgaben** Zum Zuweisen von Besitzern zu Korrekturaufgaben (VULs).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Zu erstellen Rapid7 InsightVM Asset-Tags, die zur Verwendung im Bedingungsfilter für Zuweisungsregeln verfügbar sind, müssen Sie ausführen Rapid7 InsightVM Integration der Asset-Liste vor der anderen Rapid7 InsightVM Integrationen.

Die Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird in diesem Datensatz oder Formular nicht unterstützt.

Angreifbare Elemente werden automatisch zugewiesen

Es gibt drei verschiedene Möglichkeiten, angreifbare Elemente mit zuzuweisen **Zuweisen mit** :

- Anwender Gruppe: Mit dieser Option können Sie eine der vorhandenen auswählen ServiceNow AI Platform® Anwendergruppen.
- Anwender Gruppenfeld: Mit dieser Option können Sie ein beliebiges Zuweisungsgruppenfeld auswählen, das in der Tabelle „cmdb_ci“ verfügbar ist. Standardmäßig werden die folgenden drei Gruppenfelder angezeigt:
  - Keine: Gibt keinen Standardwert für dieses Pflichtfeld an
  - Konfigurationselement: Genehmigungsgruppe
  - Konfigurationselement: Zuweisungsgruppe
  - Konfigurationselement: Supportgruppe
- Skript: Mit dieser Option können Sie die Bedingungen mithilfe eines Skripts definieren. Diese Option erfordert Codierung oder erweitert ServiceNow Fachwissen.Weitere Informationen zur Verwendung des Skripteditors zum Definieren komplexer Bedingungen finden Sie unter KB0965240 KB-artikel.

Führen Sie zuerst Regeln mit hoher Priorität aus (Elemente, die eine besondere Behandlung erfordern, bei denen das Risiko kritisch ist oder eine VIT von der Compliance mit behördlichen Vorschriften behandelt werden sollte). Führen Sie als Nächstes Ihre allgemeinen Regeln aus, bei denen keine spezielle Behandlung erforderlich ist und Sie wissen, wer dafür verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um Vits der Gruppe zuzuweisen, die ermittelt, welcher Zuweisungsgruppe sie angehören soll. Diese Gruppe kann eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel würde zuletzt ausgeführt.

Bewertungsprozess für Zuweisungsregel

Zuweisungsregeln werden verwendet, um eine VIT auszuwerten und zuzuweisen, wenn eine neue VIT geöffnet wird, d. h. importiert, manuell erstellt oder erneut geöffnet wird. Wenn Sie Zuweisungsregeln nicht manuell erneut anwenden, nachdem sich die VIT oder ihre Statusänderungen geändert haben, wird ein VI einmal ausgewertet.

Der folgende Prozess wird für jede neue, aktualisierte oder erneut geöffnete VIT verwendet:

- Für jede Schwachstellenzuweisungsregel wird die VIT mit dem Zuweisungsfilter verglichen, wobei zuerst die Regel der niedrigsten Reihenfolge gilt.
- Wenn die Bedingung erfüllt ist, wird der VIT eine Zuweisungsgruppe zugewiesen. Die Suche wird beendet.
- Wenn die Bedingungen keine Übereinstimmung zwischen allen anderen Regeln finden, wird die VIT der Standardzuweisungsgruppe zugewiesen, wenn eine Standardregel vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sobald das angreifbare Element zugewiesen wurde, verwendet die entsprechende Regel für Korrekturaufgaben die Zuweisung als eines ihrer Kriterien für die Platzierung der angreifbaren Elemente in eine Korrekturaufgabe. Siehe Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben und Filtern in Vulnerability Response, um weitere Informationen zu erhalten.

Hinweis:
Die Standardregel ist die Regel mit dem höchsten Wert für die Ausführungsreihenfolge. Eine endgültige Regel, die eine gute Ausweichmöglichkeit ist, ist Aktiv=wahr . Wenn keine Standardregel vorhanden ist, bleibt die VIT nicht zugewiesen, wenn die Korrekturaufgabenregel die Zuweisung vornimmt.

Zuweisungsregeln werden erneut angewendet

Wenn Sie eine Zuweisungsregel ändern, verwenden Sie **Änderungen Anwenden** Schaltfläche auf der Listenseite „Zuweisungsregeln“, um alle geänderten Regeln für alle aktiven offenen AES erneut auszuführen, mit Ausnahme der manuell zugewiesenen.

Hinweis:

Wenn *`Reapply all vulnerability assignment rules`*Die geplante Aufgabe wurde nicht vor der ersten Verwendung ausgeführt **Änderungen Anwenden** , Dann werden alle Zuweisungsregeln für alle offenen Vits ausgeführt, mit Ausnahme der manuell zugewiesenen Vits. Danach alle nachfolgenden Verwendungen von **Änderungen Anwenden** Führen Sie nur die geänderten Regeln und alle abhängigen Regeln erneut aus. Änderungen an einer Regel können dazu führen, dass eine VIT mit einer anderen unveränderten Regel übereinstimmt. Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.

Die geplante Aufgabe [*`Reapply all vulnerability assignment rules`*] Ist standardmäßig inaktiv. Wenn diese Option aktiviert ist, werden alle Regeln auf alle offenen Vits angewendet, mit Ausnahme der manuell zugewiesenen. Es kann ausgeführt werden **Täglich** , **Wöchentlich** , **Monatlich** , **Regelmäßig** , **Einmal** , Oder **Bei Bedarf** . Je nachdem, wie viele aktive VIS Sie in Ihrer Umgebung haben, denken Sie daran, die festzulegen **Ausführen** Feld entsprechend nach der ersten Ausführung, um Leistungsauswirkungen zu vermeiden.

Upgrade-Kunden sollten sich auf beziehen Vulnerability Response Release-Hinweise für Informationen zu den Auswirkungen dieser Funktion auf vorhandene Vits.

Wichtig:
Als Schwachstellenadministrator und -Analyst können Sie die neuesten Zuweisungen für ausgewählte angreifbare Elemente in abrufen Arbeitsbereich des Schwachstellenmanagers. Diese Methode ist effizienter als die Ausführung der Zuweisungsregeln für alle angreifbaren Elemente in der klassischen Anwenderoberfläche, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Arbeitsbereich des Schwachstellenmanagers.

Wenn sich eine Zuweisungsgruppe in einer Zuweisungsregel ändert, können die angreifbaren Elemente automatisch neu ausgewertet und neu gruppiert werden, indem die Systemeigenschaft sn_vul.rerun_Task_rules und die Business-Regel Link zu Korrekturaufgaben aktiviert werden.

So aktivieren Sie die Systemeigenschaft:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Öffnen Sie die Systemeigenschaft sn_vul.rerun_Task_rules.
3. In **Wert** Feld, legen Sie den Wert auf „wahr“ fest.

Wenn die Systemeigenschaft auf „wahr“ festgelegt ist und die Zuweisungsregeln erneut angewendet werden, wird die Verknüpfung der angreifbaren Elemente mit den Korrekturaufgaben aufgehoben, bei denen die Bedingung nicht mehr erfüllt ist.

Hinweis:
Standardmäßig ist die Systemeigenschaft sn_vul.rerun_Task_rules auf „falsch“ festgelegt.

Um die Neugruppierung angreifbarer Elemente zu automatisieren, müssen Sie die Business-Regel „Korrekturaufgaben verknüpfen“ aktivieren.

So aktivieren Sie die Business-Regel:

1. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**an.
2. Öffnen Sie die Business-Regel „Link zu Korrekturaufgaben“.
3. Wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren der Business-Regel.

Die Business-Regel gruppiert die angreifbaren Elemente neu, indem sie in die relevante Gruppe verschoben oder eine Gruppe erstellt wird, wenn sie nicht unter einer vorhandenen Gruppe gruppiert werden können.

Hinweis:

- Die angreifbaren Elemente werden aus den Gruppen entfernt, ohne die Gruppen zu löschen.
- Nur die Elemente werden entfernt, die mithilfe von Regeln für Korrekturaufgaben oder Korrekturmaßnahmen erstellt werden.
- Die Neugruppierung erfolgt automatisch nur, wenn sich die Zuweisungsgruppe als Teil einer Zuweisungsregel ändert, nicht, wenn sie manuell geändert wird.
- Zuweisungsregeln gelten nicht für Vits im Status „zurückgestellt“. Wenn eine VIT zurückgestellt wird, müssen Sie sie bei Bedarf manuell zuweisen.

Die Neugruppierung in Arbeitsbereichen wird für Korrekturaufgaben durchgeführt, die aus einer Korrekturmaßnahme erstellt werden.

Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben

Konfigurieren Sie Korrekturaufgaben (VULs), damit Analysten und Korrekturspezialisten angreifbare Elemente (VI) organisieren und massenweise analysieren können. Die Kriterien, nach denen Korrekturaufgaben erstellt werden, sind so konfiguriert, dass Sie angreifbare Elemente nicht manuell zu Korrekturaufgaben zuweisen müssen. Mit Korrekturaufgaben können Sie den Fortschritt überwachen und den Korrekturprozess effizienter steuern.

Nachverfolgung der Anzahl der Zurückstellungen für angreifbare Elemente und Korrekturaufgaben

Verfolgen Sie, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Container-Element oder eine Korrekturaufgabe zurückgestellt wird. Eine geplante Aufgabe, **Legen Sie die Anzahl der Zurückstellungen fest** , Wird täglich ausgeführt, um die Anzahl der Datensätze, die mehrmals zurückgestellt werden, in der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte „Anzahl der Zurückstellungen“ zu buchen. Datensätze werden in den Modulen „mehrere Zurückstellungen“ für VR, AVR und CVR angezeigt.

Angreifbare Elemente werden automatisch aktualisiert

Hinweis:
Die Aktualisierungsautomatisierung für angreifbare Elemente gilt nur für Korrekturaufgaben, die mit dem Bedingungsfilter oder der Filtergruppe erstellt wurden. Automatisierung gilt nicht für VIS, die manuell hinzugefügt oder mithilfe von Regeln für Korrekturaufgaben gruppiert wurden.

Wenn **Zugehörige angreifbare Elemente automatisch aktualisieren** Das Kontrollkästchen ist aktiviert, neue VIS, die den Filterkriterien der Korrekturaufgabe entsprechen, werden der Aufgabe automatisch hinzugefügt. Angreifbare Elemente in der Korrekturaufgabe, die nicht mehr den Filterkriterien entsprechen, werden automatisch aus der Aufgabe entfernt.

Standardmäßig, wenn die Korrekturaufgabe den verlässt **Öffnen** status: Das Kontrollkästchen ist deaktiviert. Wenn angreifbare Elemente unabhängig vom Status weiterhin zur Korrekturaufgabe hinzugefügt werden sollen, deaktivieren Sie *`Set auto refresh vulnerable items`*Business-Regel.

Sie können das Kontrollkästchen im Status „wird untersucht“ erneut manuell aktivieren. **Zugehörige angreifbare Elemente automatisch aktualisieren** Ist nicht deaktiviert, wenn die Korrekturaufgabe in verschoben wird **Warten Auf Implementierung** status. Sobald sich der Status „Warten auf Implementierung“ befindet, können der vorhandenen Aufgabe keine neuen angreifbaren Elemente hinzugefügt oder vorhandene angreifbare Elemente entfernt werden.

Hinweis:
Wenn eine Korrekturaufgabe manuell erstellt wird und VIS mithilfe von hinzugefügt werden **Bedingung** Filter oder **Filtergruppe** , Das Kontrollkästchen ist deaktiviert. Sie haben die Möglichkeit, das Kontrollkästchen auszuwählen oder nicht.

Angreifbare Elemente werden manuell aktualisiert

Für manuell erstellte Korrekturaufgaben mit **Filtergruppe** Oder **Bedingung** Filtern, wenn Sie auf klicken **Aktualisieren** Zugehöriger Link zu zugeordneten angreifbaren Elementen auf der **Korrekturaufgabe** Seite werden alle angreifbaren Elemente hinzugefügt, die den Filterkriterien entsprechen. Elemente, die den Kriterien nicht mehr entsprechen, werden entfernt. Diese Aktion ermöglicht eine sofortige Aktualisierung der Liste der angreifbaren Elemente und wird unabhängig davon verwendet, ob **Zugehörige angreifbare Elemente automatisch aktualisieren** Kontrollkästchen ist aktiviert oder nicht.

Manuell erstellte Korrekturaufgaben mit **Bedingung** Oder **Filtergruppe** Filtertypen werden einmal pro Stunde aktualisiert.

Regeln für Korrekturaufgaben verstehen

Mit Regeln für Korrekturaufgaben können Sie definieren, wie angreifbare Elemente automatisch gruppiert und zugewiesen werden. Eine Standardregel, **Schwachstelle** , Ist im Basissystem enthalten, das angreifbare Elemente basierend auf ihren Schwachstellen sammelt. Sie können jedoch nach jedem anderen Satz von Werten in Spalten gruppieren, auf die über das VI zugegriffen werden kann Diese Werte können Support-Gruppe für Konfigurationselemente (Configuration Item, CI), Schwachstellenschweregrad usw. enthalten.

Sie können eine beliebige Anzahl von Bedingungen erstellen. Sobald Sie eine Auswahl für „Gruppieren nach“ festgelegt haben, wird eine weitere Zeile angezeigt. Sie können bis zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

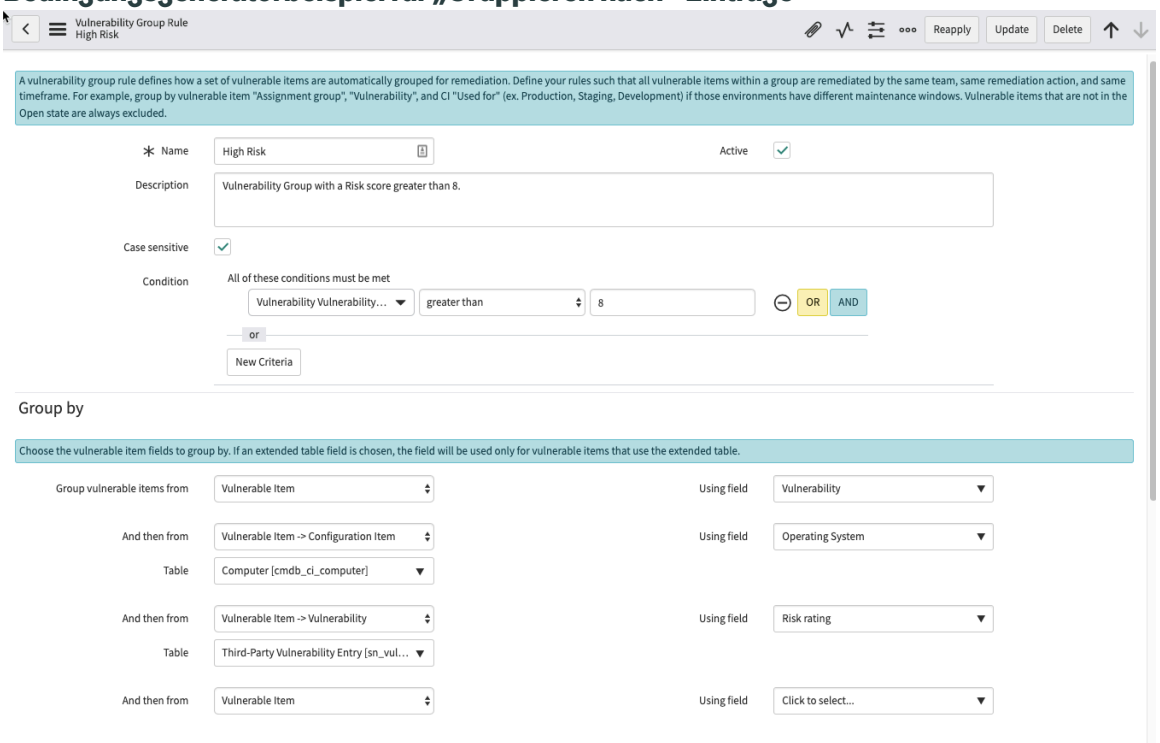
sechs haben **Gruppieren nach** Auswahlen. Sie können auch die Gruppenzuweisung automatisieren. Siehe Erstellen oder bearbeiten Vulnerability Response Regeln für Korrekturaufgaben und Filtern in Vulnerability Response, um weitere Informationen zu erhalten.

Hinweis:
Zu erstellen Rapid7 InsightVM Asset-Tags, die zur Verwendung im Bedingungsfilter für Regeln für Korrekturaufgaben verfügbar sind, müssen Sie ausführen Rapid7 InsightVM Integration der Asset-Liste vor der anderen Rapid7 InsightVM Integrationen.

Sie können Ihre angreifbaren Elemente beispielsweise nach der Kostenstelle des angreifbaren CI oder nach dem Angriffsvektor der Schwachstelle gruppieren. Sie können eine Aufgabenregel für Schwachstellen mit niedrigem Schweregrad oder CIs mit niedrigem Risiko haben. Sie können eine weitere Aufgabenregel für kritische Server und Schwachstellen mit Exploits haben – angreifbare Elemente, die das Unternehmen einem höheren Risiko aussetzen.

Für angreifbare Elemente, die das Unternehmen einem höheren Risiko aussetzen, kann ein anderer Satz von Regeln verwendet werden. Der Name der Korrekturaufgabe wird an die Regel der Korrekturaufgabe angehängt **Gruppieren nach** Werte für die Kurzbeschreibung des neuen Datensatzes. Siehe Erstellen Sie manuell eine Korrekturaufgabe in Vulnerability Response Für weitere Informationen zu verfügbaren Feldern.

Bedingungsgeneratorbeispiel für „Gruppieren nach“-Einträge



Wenn ein neues angreifbares Element erstellt, importiert oder erneut geöffnet wird, nachdem es geschlossen wurde, werden die Schwachstellen-Regeln dafür ausgewertet. Ein VI wird nur einmal automatisch ausgewertet, es sei denn, es wird nach dem Schließen erneut geöffnet, oder die Regeln werden manuell erneut angewendet.

Der folgende Prozess wird für jedes neue oder erneut geöffnete VI verwendet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für jede Regel für Korrekturaufgaben wird das VI mit dem Regelfilter für Korrekturaufgaben verglichen.

- Für jede Regel, bei der die Regelbedingung für Korrekturaufgaben erfüllt ist, ruft die Regel die Daten aus dem ab **Gruppieren nach** Auswahlen im VI Erstellt einen Gruppennamen und ein Feld. In diesem Fall **Hohes Risiko: QID-32342:** *`Zusammenfassung von QID-3242`* (Name: Schwachstellen-ID: Schwachstellen-Zusammenfassung).

  Hinweis:
  Das Feld „Kurzbeschreibung“ ist auf 160 Zeichen beschränkt. Längere Schwachstellenzusammenfassungen werden gekürzt.

  Die Regel überprüft, ob eine Übereinstimmung vorhanden ist **Öffnen** Korrekturaufgabe, die derselben Zuweisungsgruppe wie das VI zugewiesen ist

  - Wenn die Aufgabe gefunden wird, wird das VI der vorhandenen Aufgabe in hinzugefügt **Öffnen** status.
  - Wenn keine Aufgabe in **Öffnen** status wurde gefunden, die Regel erstellt einen **Hohes Risiko: QID-32342** Aufgabe, weist sie derselben Zuweisungsgruppe wie das VI zu und platziert das VI in der Korrekturaufgabe.

Es kann mehr als eine Regel für Korrekturaufgaben definiert werden, um verschiedene Arten von Schwachstellen zu gruppieren. Da jede Schwachstelle mit den Regelbedingungen für Korrekturaufgaben verglichen wird, bevor sie in eine Korrekturaufgabe eingefügt wird, können zu viele Regeln Auswirkungen auf die Leistung haben.

Standardmäßig verwenden Regeln für Korrekturaufgaben die vom festgelegte Zuweisungsgruppe **Zuweisungsregeln** Für das angreifbare Element beim Gruppieren der Elemente und weist die Korrekturaufgabe zu, um die angreifbaren Elemente abzugleichen.

Als Teil der Standardaufgabenregel wird die Zuweisung dieser Korrekturaufgaben durch die Regeln in gesteuert **Zuweisungsregeln** Modul. Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

Wenn eine Aufgabenregel aus der Formular- oder Listenansicht gelöscht wird, haben Sie die Möglichkeit, alle zu löschen **Öffnen** Von dieser Regel erstellte Aufgaben. Aufgaben nicht in **Öffnen** Sind ausgeschlossen.

Regeln für Korrekturaufgaben werden erneut angewendet

Wenn Sie eine Korrekturaufgabenregel ändern möchten, verwenden Sie **Erneut Anwenden** Schaltfläche auf der Seite mit der Regel für Korrekturaufgaben, um die geänderte Regel für alle aktiven erneut auszuführen **Öffnen** Von dieser Regel erstellte Korrekturaufgaben. Korrekturaufgaben werden automatisch basierend auf der geänderten Regel gelöscht und neu erstellt.

Wichtig:
Als Schwachstellenadministrator und -Analyst können Sie die Regeln für Korrekturaufgaben für ausgewählte angreifbare Elemente in auswerten Arbeitsbereich des Schwachstellenmanagers. Diese Methode ist effizienter als die erneute Anwendung der Regeln für Korrekturaufgaben in der klassischen Anwenderoberfläche, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Arbeitsbereich des Schwachstellenmanagers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Korrekturzielregeln

Korrekturzielregeln definieren den erwarteten Zeitrahmen für die Korrektur angreifbarer Elemente (VI), ähnlich wie SLAs einen Zeitrahmen für die Behebung der Schwachstelle selbst bieten. Wenn ein Asset beispielsweise PCI-Daten (Kreditkartendaten) enthält, muss die Schwachstelle für dieses Element gemäß PCI DSS innerhalb von 30 Tagen behoben werden.

Schwachstellenmanager können Korrekturzielregeln erstellen, indem sie Folgendes definieren:

- Das Nachbesserungsziel
- Das Erinnerungsziel
- Die Erinnerung und Benachrichtigungsempfänger – Wer soll benachrichtigt werden, wenn die angreifbaren Elemente (VIS) das Erinnerungsziel oder das Korrekturziel überschritten und nicht behoben wurden.

Analysten und Manager von Schwachstellen können das Korrekturzieldatum im Formular für Schwachstellen-Elemente und in Listenansichten anzeigen, solange sich die angreifbaren Elemente nicht in befinden **Zurückgestellt** , **Gelöst** , Oder **Geschlossen** status. Korrekturzielregeln werden beim Import ausgeführt und erneut ausgeführt, wenn ein VI erneut geöffnet wird.

Die **Korrekturzieldatum** Ist in der VI-Listenansicht wie folgt farbcodiert:

- Angreifbare Elemente, die ihr Benachrichtigungsdatum nicht erreicht haben, werden grün angezeigt.
- Angreifbare Elemente, die sich dem Korrekturzieldatum nähern, werden orange angezeigt.
- Angreifbare Elemente, die das Korrekturzieldatum überschritten haben, werden rot angezeigt.

Eine Zusammenfassungs-E-Mail pro Korrekturzielregel wird gesendet, wenn ein oder mehrere VIS sich dem Korrekturzieldatum nähern oder das Korrekturzieldatum überschritten ist.

Korrekturzielregeln können deaktiviert oder gelöscht werden

Wenn eine Regel deaktiviert ist, werden die aktuellen Korrekturzieldaten für die VIS gelöscht, auf die sie angewendet wurde. Wenn ein VI eine aktive Regel erfüllt, wird diese Regel angewendet, andernfalls hat das VI keine Regel oder kein Zieldatum, und sein Status ist **Kein Ziel** .

Wenn Regeln gelöscht werden, wird **Korrekturziel** Datum und zugehörige Felder für geschlossene, zurückgestellte oder gelöste VIS werden beibehalten. Die **Korrekturziel** Datum und zugehörige Felder für nicht geschlossene VIS werden gelöscht, und alle abhängigen Regeln werden erneut angewendet.

Korrekturzielregel-Szenario

Wenn mehrere Korrekturzielregeln auf dasselbe angreifbare Element angewendet werden, wird die restriktivste Regel angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Korrekturziele werden aus berechnet **Zuletzt Geöffnet** Datum plus Anzahl der Tage (gemessen in 24-Stunden-Schritten).

Ab V17.1 werden Korrekturziele aus berechnet **Ziel von (Datum)** . Der Standardwert bleibt erhalten **Datum der letzten Öffnung** .

Beispiel: Wenn ein angreifbares Element die Bedingung für zwei Korrekturzielregeln erfüllt:

Szenario: Angreifbares Element zuletzt geöffnet am 01/2018 um 10:00:00.

- Korrekturzielregel 1: Zuletzt geöffnet am 03/07/2018; Korrekturziel ist 15 Tage seit dem letzten Öffnen; berechnetes Korrekturzieldatum ist 03/16/2018 10:00:00.
- Korrekturzielregel 2: Zuletzt geöffnet am 03/10/2018; Korrekturziel ist 10 Tage seit dem letzten Öffnen; berechnetes Korrekturzieldatum ist 03/11/2018 10:00:00.

In diesem Szenario gilt die Korrekturzielregel 2 für das angreifbare Element, da es das restriktivere Datum hat. 10 Tage seit der ersten Identifizierung des angreifbaren Elements im Vergleich zu 15 Tagen.

Hinweis:
Sobald die Korrekturzielregel definiert ist, werden die Korrekturzieldaten von berechnet `Evaluate remediation targets` Geplante Aufgabe.

Über die geplante Aufgabe „Korrekturziele auswerten“

`Evaluate remediation targets` Wird einmal täglich um 16:00 Uhr ausgeführt.

Es wird durch alle aktiven Schwachstellenregeln iteriert, beginnend mit diesen Regeln mit dem frühesten Korrekturzieldatum. Es werden alle angreifbaren Elemente untersucht, die:

- Befinden sich nicht in **Geschlossen** , **Zurückgestellt** , Oder **Gelöst** status.
- Hat kein Korrekturzieldatum.
- Haben ein Korrekturzieldatum, das nach dem Datum in der Korrekturzielregel liegt.

`Evaluate remediation targets` Fügt ein Korrekturzieldatum hinzu, wenn eines nicht vorhanden ist oder wenn eine Regel zu einem früheren Datum als dem im Datensatz führt, aktualisiert sie das vorhandene Zieldatum. Schließlich wird aktualisiert **Korrekturziel** Und **Korrekturstatus** Felder im Formular „Angreifbares Element“.

Sobald `Evaluate remediation targets`Wird ausgeführt, verfügbare Benachrichtigungen werden gesendet.

`Evaluate remediation targets` Löscht die Korrekturfelder im VI und stoppt das Senden von Benachrichtigungen.

Die `sn_sec_cmn.evaluate_targetmissed_records`Wenn diese Eigenschaft aktiviert ist, wird verhindert `Remediation Target Rules`Geplante Aufgabe aus der Bewertung verpasster VIS. Diese Eigenschaft ist standardmäßig aktiviert.

Korrekturzielregeln werden erneut angewendet

Wenn Sie eine Korrekturzielregel ändern, verwenden Sie **Änderungen Anwenden** Schaltfläche auf der Listenseite „Korrekturzielregeln“, um alle geänderten Regeln für alle aktiven offenen VIS außer denen in erneut auszuführen **Geschlossen** , **Zurückgestellt** Oder **Gelöst** status. Je nachdem, wie viele VIS Sie haben, kann dies einige Zeit dauern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn die geplante Aufgabe *Evaluate remediation targets*Wird ausgeführt, Sie können keinen Prozess zum erneuten Anwenden initiieren. Wenn jedoch bereits ein Prozess zur erneuten Anwendung ausgeführt wird und die geplante Aufgabe ausgelöst wurde, werden sie parallel ausgeführt.

Prozesse in erneut anwenden Vulnerability Response Und Application Vulnerability Response Sind unabhängig und können parallel ausgeführt werden.

Wichtig:

Als Schwachstellenadministrator und -Analyst können Sie das neueste Korrekturzieldatum für ausgewählte angreifbare Elemente in abrufen Arbeitsbereich des Schwachstellenmanagers. Diese Methode ist effizienter als die Ausführung der Korrekturzielregeln für alle angreifbaren Elemente in klassisch UI, die ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Arbeitsbereich des Schwachstellenmanagers.

Zugehörige Informationen

Erstellen oder bearbeiten Vulnerability Response Korrekturzielregeln

Zeigen Sie den Korrekturzielstatus von an Vulnerability Response Angreifbares Element

Erstellen oder bearbeiten Sie Benachrichtigungen zu Korrekturzielen

Schwachstellenklassifizierungsgruppen und -Regeln

Klassifizierungsgruppen automatisieren die Klassifizierung von Werten einer Tabelle basierend auf den in der Gruppe definierten Klassifizierungsregeln. Die Bedingung für jede Regel wird in der Reihenfolge ausgewertet, und die erste Übereinstimmungsregel wird verwendet.

Das Vulnerability Response-Basissystem enthält die folgenden zwei Klassifizierungsgruppen, die erkannte Elemente bzw. Schwachstellen klassifizieren:

- Klassifizierung erkannter Elemente
- Klassifizierung von Schwachstelleneinträgen

Immer wenn Schwachstellen und erkannte Elemente importiert werden, werden die Schwachstellen-Klassifizierungsregeln in den jeweiligen Gruppen ausgeführt. Basierend auf den in der Regel festgelegten Bedingungen werden die Datensätze der relevanten Klassifizierungsgruppe klassifiziert. Sie können diese Regeln erstellen, bearbeiten, löschen oder erneut auf eine vorhandene Schwachstelle anwenden.

Hinweis:

- Für eine ausgewählte Tabelle kann nur eine aktive Klassifizierungsgruppe vorhanden sein.
- Sobald Sie eine Gruppe erstellt haben, können Sie sie nicht löschen.

Weitere Informationen finden Sie unter Erstellen und bearbeiten Sie eine Klassifizierungsregel, Wenden Sie eine Regel auf eine vorhandene Schwachstelle an und Deaktivieren oder löschen Sie eine Klassifizierungsregel.

Lösungen für maschinelles Lernen für Vulnerability Response

Empfehlungen für die Zuweisung von Schwachstellen Verwendet ServiceNow® Predictive Intelligence Und maschinelles Lernen, um Zuweisungsgruppen für angreifbare Elemente (VIS) und Korrekturaufgaben (VULs oder RTS) zu empfehlen. Sie können die Zeit reduzieren, die Sie für die Identifizierung der Besitzer für nicht zugewiesene oder falsch zugewiesene

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellenergebnisse aufwenden. Außerdem können Sie eine vom System generierte Konfidenzpunktzahl anzeigen, die bewertet, ob die empfohlene Zuweisungsgruppe geeignet ist, die Schwachstelle zu beheben.

Die Predictive Intelligence-Fähigkeiten werden in verwendet Vulnerability Response Um bessere Arbeitserfahrungen zu bieten, indem ein Lösungsdefinitionsmodell erstellt und trainiert wird, das die Zuweisungsgruppe basierend auf vorhandenen Daten vorhersagen kann.

Weitere Informationen hierzu finden Sie unter Predictive Intelligence .

Empfehlungen für die Zuweisung von Schwachstellen

Mit Empfehlungen für die Zuweisung von Schwachstellen Anwendung (com.snc.Vulnerability.Recom), kann das System Empfehlungen in zuweisen Vulnerability Response Verwenden ServiceNow Predictive Intelligence. Dieses Plugin erfordert:

- Vulnerability Response(`Com.snc.Vulnerability`)
- Predictive Intelligence(`com.glide.platform_ml`)

Weitere Informationen hierzu finden Sie unter Predictive Intelligence .

Vertrauensbewertungen

Verwenden Sie Empfehlungen für die Zuweisung von Schwachstellen Anwendung zum Generieren der Konfidenzpunktzahl, die das Konfidenzniveau der empfohlenen Zuweisungsgruppen für die ausgewählten RTS oder VIS meldet. Die Konfidenzpunktzahl bewertet, ob das System zuversichtlich ist, dass die empfohlene Zuweisungsgruppe zur Behebung der Schwachstelle geeignet ist. Es werden bis zu 10 Empfehlungen angezeigt. Diese Empfehlungen basieren auf der höchsten Wahrscheinlichkeit für erfolgreiche Zuweisungen. Die erste Empfehlung in der Liste bedeutet, dass das System die höchste Sicherheit hat, dass es die richtige Zuweisungsgruppe ist.

Beispielsweise schlägt die Konfidenzpunktzahl auf einer Skala von 0 bis 100 für jede Zuweisungsgruppe die Wahrscheinlichkeit vor, dass ein VI oder RT zu dieser bestimmten Gruppe gehört.

Zugehörige Informationen

Predictive Intelligence

Klassifizierungslösung erstellen und trainieren

Eine Ähnlichkeitslösung erstellen und trainieren

Clustering-Lösung erstellen und trainieren

Erweiterte Einstellungen für ML-Lösungen konfigurieren

CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Integrationen von Schwachstellen von Drittparteien

Wenn Daten aus einer Drittpartei-Integration importiert werden, Vulnerability Response Verwendet automatisch Hostdaten, um nach Übereinstimmungen in zu suchen Configuration Management Database (CMDB). Dies geschieht mit **CI-Suchregeln** . Diese Regeln werden verwendet, um Konfigurationselemente (Configuration Items, CIs) zu identifizieren und dem Datensatz für angreifbare Elemente hinzuzufügen, um die Korrektur zu erleichtern.

Navigieren Sie ab Version 19.0 zu **Security Operations** > **CMDB** > **Suchregeln** Um die Liste in Ihrer Instanz zu suchen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Assets importiert werden, wird zuerst eine Suche für durchgeführt **Erkannte Elemente** Listen Sie mithilfe von Drittpartei-IDs auf, um Übereinstimmungen mit Konfigurationselementen (Configuration Item, CIs) aus vorherigen Importen zu finden. Wenn eine Host-ID-Übereinstimmung gefunden wird, wird sie als verwendet **Konfigurationselement** Feld im Datensatz des angreifbaren Elements.

Sie können mit sehen, wie importierte Assets CIs zugeordnet werden **Erkannte Elemente** Liste. Wenn keine Übereinstimmung gefunden wird oder das Feld „Host-ID“ leer ist, verwenden die Regeln die anderen Hostinformationen, um zu versuchen, das CI korrekt zu identifizieren. Wenn immer noch keine Übereinstimmung gefunden wird, wird ein Platzhalter-CI erstellt und als festgelegt **Nicht abgeglichenes CI** . Siehe Nicht abgeglichene CIs Um weitere Informationen zur Behandlung dieser CIs zu erhalten.

CI-Suchregeln können domänengetrennt sein und quellspezifisch sind. Jede Quelle kann mehrere Bereitstellungen haben.

Hinweis:
CI-Suchregeln werden von allen Bereitstellungen der Integration der Schwachstellenquelle freigegeben. Wenn eine Regel gelöscht oder geändert wird, wirken sich die Löschung oder Änderungen auf alle Bereitstellungen der Schwachstellenintegration aus.

Beim Versuch einer Übereinstimmung besteht der erste Schritt in einer Lieferanten-ID-Suche nach einer genauen Übereinstimmung für Quelle, Source_instance und Lieferanten-ID. Dann werden Suchregeln in der Reihenfolge von der niedrigsten bis zur höchsten ausgeführt und beendet, wenn eine Regel nur ein einzelnes CI als Übereinstimmung zurückgibt. Wenn eine Regel so erstellt wird, dass sie mehr als ein CI zurückgibt, wird nur die erste Übereinstimmung verwendet.

Hinweis:
Um einen Abgleich bei Netzwerkelementen auf niedriger Ebene zu vermeiden, wenn ein übereinstimmendes CI einer von ist `Dscy_switchport` , `cmdb_ci_Network_Adapter` , `cmdb_ci_nic` , Oder `cmdb_ci_ip_address` , Das übergeordnete CI wird zurückgegeben.

Eine Systemeigenschaft zum Ausschließen von CI-Klassen ist verfügbar. Diese Eigenschaft ist mit Upgrade nicht verfügbar. Siehe Ignorieren Sie CI-Klassen Für Upgrade-Informationen und Anweisungen zum Festlegen der Eigenschaft.

Um das Auffinden übereinstimmender Probleme zu erleichtern, wird die CI-Suchregel, die zum Auffinden verwendet wird, dem Datensatz „erkanntes Element“ in hinzugefügt **CI-Übereinstimmungsregel** Feld. Suchregeln werden nach den niedrigsten Werten ausgewertet **Reihenfolge** Wert zuerst.

Die CI-Suchregeln werden mit den entsprechenden Integrations-Plugins geliefert.

Einige von Qualys CI-Suchregeln sind:

- QUALYS-HOST-ID
- FQDN
- NetBIOS
- DNS
- IP

Einige von Rapid7 CI-Suchregeln sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MAC-Adresse
- FQDN
- HostName
- IP

Einige der CI-Suchregeln für Tenable.io sind:

- FQDN
- NETBIOS
- HOSTNAME
- MAC-Adresse
- DNS

Hinweis:
Die CI-Suchregeln Tenable.io priorisieren und füllen die nicht leeren Netzwerkschnittstellenwerte (FDQN, IPV4 und MacAddress) gegenüber den regulären FDQN-, IPV4- und MacAddress-Werten für ein erkanntes Element aus. Wenn diese Netzwerkschnittstellenwerte leer sind, werden die regulären FDQN-, IPV4- und MacAddress-Werte für ein erkanntes Element ausgefüllt.

Einige der CIs Tenable.sc-Suchregeln sind:

- MAC-Adresse
- FQDN
- NETBIOS

Hinweis:
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Iterieren und Durchführen des Abgleichs innerhalb von verwendet wird CMDB Kann zu längeren Verarbeitungszeiten führen. Um eine potenzielle Verschlechterung der Ressourcen oder Leistungskomplikationen zu vermeiden, testen Sie alle anwenderdefinierten CI-Suchregeln oder Änderungen an vordefinierten **CI-Suchregeln** . Siehe Schritte zur Verhinderung doppelter oder verwaister Datensätze nach der Ausführung Vulnerability Response CI-Suchregeln Weitere Informationen zum verhindern doppelter verwaister Datensätze, zum Löschen von Daten und zum Bereinigen von Daten.

Hinweis:
Informationen zum CI-Abgleich finden Sie unter KB0998706 .

Aktualisierte CI-Suchregeln werden erneut angewendet

Wenn Sie eine CI-Suchregel ändern, klicken Sie auf **Änderungen Anwenden** Auf der Listenseite „CI-Suchregeln“, um alle Regeln für die erkannten Elemente erneut auszuführen, die:

- Wurden mit den aktualisierten Regeln abgeglichen
- Werden von keiner Regel abgeglichen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn sich das Konfigurationselement (Configuration Item, CI) nach erneuter Anwendung der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Die betroffenen Erkennungen und angreifbaren Elemente werden ebenfalls aktualisiert. Weitere Informationen finden Sie unter Wenden Sie CI-Suchregeln erneut auf ausgewählte erkannte Elemente an .

Nicht klassifizierte Hardware

Wenn ein Asset keine Übereinstimmung in findet Configuration Management Database (CMDB) Nach CI-Suchregeln wird das Asset als nicht klassifizierte Hardware bezeichnet.

Wenn Daten aus importiert werden ServiceNow Erstellte Integrationen, Vulnerability Response Verwendet automatisch Hostdaten, um nach Übereinstimmungen in zu suchen CMDB. Die CI-Suchregeln werden verwendet, um Konfigurationselemente (Configuration Items, CIs) zu identifizieren und dem Datensatz für angreifbare Elemente hinzuzufügen, um die Korrektur zu erleichtern. Wenn die Assets nicht in gefunden werden CMDB, Führt die Identification and Reconciliation Engine (IRE) eigene Identifizierungsregeln aus, die für die Hardwareklasse und alle untergeordneten Elemente definiert sind, und erstellt ein CI unter einer nicht klassifizierten Hardwareklasse. Wenn Discovery Findet dieses Asset, anstatt die vorhandene nicht klassifizierte Hardware neu zu klassifizieren, wird ein CI erstellt. Dies liegt daran, dass die Identifizierungsregel vom Namen des Hardware-CI abhängt.

Wenn die Identification and Reconciliation Engine (IRE) aktiviert ist, wird die Option „Neu klassifizieren“ aus erkannten Elementen nicht unterstützt.

Die folgenden Extrakte zeigen die IRE-Nutzlast zum Erstellen von CI in nicht klassifizierter Hardware über Vulnerability Response Und Discovery Entsprechend.

```
"className": "cmdb_ci_unclassed_hardware",

"values": {
      "name": "asset01.company.com",//from NetBios,
      "mac_address": "1a:5e:2c:0e:42:f3",
      "fqdn": "asset01.company.com",
      "ip_address": "133.10.3.123"
   }

"settings": {
      "updateWithoutSwitch": true
   }
```

```
"className": "cmdb_ci_cmdb_ci_win_server"

"values": {
      "name": "asset01",
      "mac_address": "1a:5e:2c:0e:42:f3",
      "fqdn": "asset01.company.com",
      "ip_address": "133.10.3.123",
      "os_domain": "company"
   }

"settings": {
      "updateWithoutSwitch": false
   }
```

In diesem Fall wird das vorhandene nicht klassifizierte Hardware-CI nicht für den Windows-Server neu klassifiziert, und stattdessen wird ein neues CI unter Windows-Server erstellt. Der Grund für die Identifizierungsregel hängt vom Namen des Hardware-CI ab. Wenn Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Nutzlasten bemerken, der Name in der Nutzlast von Vulnerability Response Ist entweder mit FQDN/NETBIOS identisch, aber es ist nur der Hostname für die Nutzlast von Discovery.

Zugehörige Informationen

Klassifizieren Sie nicht klassifizierte Hardware erneut

Nicht abgeglichene CIs

Konfigurationselemente (CIs) werden automatisch mit CIs in abgeglichen Configuration Management Database (CMDB) Wenn sie importiert werden. Standardmäßig berechnet der geplante Job **Security Operations** > **CMDB** > **Erkannte Elemente** Modul listet diese Konfigurationselemente ohne Übereinstimmung auf.

Wenn Sie der Meinung sind, dass ein nicht übereinstimmendes CI zu einer vorhandenen Klasse in der CMDB gehört, Überprüfen Sie Ihre CI-Suchregeln . Andernfalls sollten Sie berücksichtigen Konfigurationselement wird erneut klassifiziert .

Hinweis:
Der Standardfilter für diese Liste ist auf festgelegt **Nicht Abgeglichen** . Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Wenn die Identification and Reconciliation Engine (IRE) aktiviert ist, wird die Option „Neu klassifizieren“ aus erkannten Elementen nicht unterstützt.

Zugehörige Informationen

Zeigen Sie nicht abgeglichene Konfigurationselemente an, und klassifizieren Sie sie erneut

Nicht übereinstimmende erkannte Elemente abstimmen

Schritte zur Verhinderung doppelter oder verwaister Datensätze nach der Ausführung Vulnerability Response CI-Suchregeln

Deduplizierung vorhandener Konfigurationselemente

CIs für werden erstellt Vulnerability Response Verwenden der Identifizierungs- und Abgleichsmodul

Sie können Konfigurationselemente (Configuration Items, CIs) in erstellen Configuration Management Database (CMDB) Mit der Ire-API (Identification and Reconciliation Engine). Wenn Sie die IRE-API zum Erstellen von CIs verwenden, können Sie verhindern, dass doppelte CIs erstellt werden, und Sie können CI-Attribute abgleichen, indem Sie zulassen, dass nur autorisierende Datenquellen in schreiben CMDB.

Eine CI-Klasse (Tabelle) ist der ursprüngliche Tabellenname in der Instanzdatenbank. CMDB Enthält Basissystemklassen, die Daten zu CIs speichern.

IRE für die CI-Erstellung verwenden

Vor Vulnerability Response V12.2, Wenn ein übereinstimmendes CI weder in der Liste erkannter Elemente noch gefunden wird CMDB, Wird ein CI in der nicht abgeglichenen CI-Klasse (`sn_sec_cmn_Unmatched_ci`). Weitere Informationen finden Sie unter Nicht abgeglichene CIs .

Ab v24.0.6 von Vulnerability Response, Wenn IRE auf Ausnahmen stößt, die die Erstellung von CIs verhindern, werden die Besonderheiten dieser Ausnahmen im Feld „zusätzliche Informationen“ aufgezeichnet. Durch die Untersuchung der Details in diesem Feld können Sie die Ursache bestimmen und die erforderlichen Korrekturen implementieren, um sicherzustellen, dass das CI erfolgreich erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beginnend mit Vulnerability Response Wenn bei Anwendung der CI-Suchregeln keine Übereinstimmung gefunden wird, werden die Asset-Informationen an IRE gesendet, und ein CI wird in einem der erstellt `Nicht Klassifizierte Hardware` Und `Unvollständiges IP-identifiziertes Gerät` Klassen. Beginnt ab Vulnerability Response V18.0, eine neue Klasse, `Cloud-Ressource` Ist ebenfalls enthalten. Weitere Informationen zum Konfigurieren der Kategorisierung nicht übereinstimmender Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert.

CMDB CI-Klassen

Hinweis:
Um die neuen Klassen zu verwenden, aktivieren Sie CMDB CI-Klassenmodelle-Plugin. Andernfalls werden CIs in der nicht abgeglichenen CI-Klasse erstellt.

Wenn der Host, den Sie von einem Scanner einer Drittpartei importiert haben, nicht in der Liste erkannter Elemente oder gefunden werden kann CMDB, Ist es Erstellt In einer der folgenden neuen Elemente CMDB CI-Klassen.

CMDB CI-Klassen

CMDB CI-Klasse	Beschreibung
Unvollständiges IP-identifiziertes Gerät (`cmdb_ci_Inclusive_ip`)	Das CI wird in dieser Tabelle erstellt, wenn in den vom Scanner empfangenen Hostinformationen nur die IP-Adresse verfügbar ist.
Nicht Klassifizierte Hardware (`cmdb_ci_Unclassed_Hardware`)	CI wird in dieser Tabelle erstellt, wenn in den vom Scanner empfangenen Hostinformationen eine der folgenden Informationen verfügbar ist: • Hostname • IP-Adresse • DNS • NETBIOS • MAC-Adresse **Hinweis:** Wenn die MAC-Adresse verfügbar ist, wird der Netzwerkadaptereintrag erstellt und mit dem nicht klassifizierten Hardware-CI verknüpft. Wenn sowohl die IP- als auch die MAC-Adresse verfügbar sind, wird auch das IP-Adressen-CI erstellt und mit dem nicht klassifizierten Hardware-CI verknüpft.
Cloud-Ressource (`cmdb_ci_CMP_resource`)	CI wird in dieser Tabelle erstellt, wenn `Cloud Resource ID`Ist in den Hostinformationen verfügbar, die vom Scanner empfangen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CMDB CI-Klassen (Fortsetzung)

CMDB CI-Klasse	Beschreibung
	Hinweis: Wenn der Asset-Typ einer Scannerintegration ist `Hybrid` Und `sn_sec_cmn.unmatched_cloud_resource_enabled`Syst ist „falsch“, die CIs werden in erstellt `Nicht Klassifizierte Hardware` Klasse, aber nicht in `Cloud-Ressource` Klasse.

Wenn die Identification and Reconciliation Engine (IRE) aktiviert ist, wird die Option „Neu klassifizieren“ aus erkannten Elementen nicht unterstützt.

Das System verwendet automatisch eine nicht abgeglichene CI-Klasse, wenn einer der folgenden Fälle eintritt:

- Die CMDB CI-Klassen-Plugin ist nicht aktiviert.
- IRE löst beim Erstellen eines CI eine Ausnahme aus.

Weitere Informationen finden Sie unter Nicht abgeglichene CIs .

Zugehörige Informationen

Store-App „CMDB CI Class Models“

Identification and Reconciliation Engine (IRE)

CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert

Beginnend mit Vulnerability Response V20.0 können Sie die nicht abgeglichenen Cloud-Assets aus kategorisieren Qualys, Rapid7 und Tenable-Scanner in `Nicht Klassifizierte Hardware` Mithilfe von `sn_sec_cmn.unmatched_cloud_resource_enabled`Systemeigenschaft.

Diese Systemeigenschaft mit `Falsch` Als Standardwert wird mit dem Basissystem geliefert. Klassifiziert die nicht abgeglichenen Cloud-Assets in ein `Nicht klassifizierte Hardware` (`cmdb_ci_unclassed_hardware`) Oder `Cloud-Ressource` (`cmdb_ci_cmp_resource`)-Klasse für die Integrationen, die sowohl Infrastruktur- als auch Cloud-Assets enthalten.

Beginnend mit Vulnerability Response V20.0, die Spalte Asset-Typ wird in den Drittpartei-Integrationen (`sn_sec_int_Integration`) Tabelle zur Identifizierung der Integrationen, die sowohl Infrastruktur- als auch Cloud-Assets unterstützen. Die Spalte „Asset-Typ“ hat den Wert, `Hybrid` Für die Scanner, die sowohl Infrastruktur- als auch Cloud-Assets enthalten. Beispiel: Qualys, Rapid7 und Tenable-Integrationen haben den Wert als `Hybrid` In der Spalte Asset-Typ.

- Für die Neuinstallation von Vulnerability Response V20.0 und höher werden alle nicht abgeglichenen Cloud-Assets kategorisiert in:
  - `Nicht Klassifizierte Hardware` Klasse standardmäßig.
  - `Cloud-Ressourcen` Klasse, wenn Sie ändern `sn_sec_cmn.unmatched_cloud_resource_enabled`Systemeigenschaft zu `Wahr` .
- Für Upgrades auf Vulnerability Response V20.0:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Assets in vorhanden sind `Cloud-Ressource` Klasse, die `sn_sec_cmn.Unmatched_Cloud_resource_enabled` Die Systemeigenschaft ist auf „wahr“ festgelegt, damit die nicht abgeglichenen Cloud-Assets weiterhin zu hinzugefügt werden `Cloud-Ressource` (`cmdb_ci_cmp_resource`) Klasse.
- Andernfalls wird `sn_sec_cmn.Unmatched_Cloud_resource_enabled` Die Systemeigenschaft ist auf „falsch“ festgelegt, sodass die nicht abgeglichenen Cloud-Assets kategorisiert werden `Nicht Klassifizierte Hardware` Klasse.

Hinweis:
Wenn Sie den Wert von ändern `sn_sec_cmn.unmatched_cloud_resource_enabled`Systemeigenschaft: Stellen Sie sicher, dass nicht übereinstimmende Konfigurationselemente in der zuvor angestrebten CI-Klasse gelöscht werden, und wenden Sie die Suchregeln erneut an. Weitere Informationen zum Löschen vorhandener CIs und zum erneuten Anwenden von CI-Suchregeln, damit die neuen CIs in der richtigen Klasse erstellt werden, finden Sie unter KB1533376 .

Erkannte Elemente

Assets werden automatisch mit Konfigurationselementen (CIs) in abgeglichen Configuration Management Database (CMDB) Wenn sie mit importiert werden **CI-Suchregeln** . Erkannte Elemente geben Ihnen Einblick, wie die Asset-Identifizierung CIs in zugeordnet wird CMDB.

Erkannte Elemente werden berücksichtigt **Übereinstimmend** , **Nicht Abgeglichen** , Oder **Neu Klassifiziert** . Identifizierte CIs befinden sich in **Übereinstimmend** status.

Um das Auffinden potenzieller Übereinstimmungsprobleme zu erleichtern, wird die CI-Suchregel, die dem CI entspricht, in angezeigt **CI-Übereinstimmungsregel** Feld.

Standardmäßig berechnet der geplante Job **Security Operations** > **CMDB** > **Erkannte Elemente** Modul listet nicht übereinstimmende Konfigurationselemente auf. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Eine Beschreibung der Felder in erkannten Elementen finden Sie unter Formularfelder „erkannte Elemente“. Weitere Informationen zum Abgleichen nicht abgeglichener erkannter Elemente und zum erneuten Anwenden von CI-Suchregeln auf ausgewählte erkannte Elemente finden Sie unter Nicht übereinstimmende erkannte Elemente abstimmen Und Wenden Sie CI-Suchregeln erneut auf ausgewählte erkannte Elemente an Entsprechend.

CI-Änderungen für erkannte Elemente

Wenn sich ein Konfigurationselement (CI) für ein erkanntes Element (DI) ändert, werden die betroffenen Erkennungen und angreifbaren Elemente (VIS) aktualisiert. Die Risikopunktzahl, Zuweisungsregeln, Gruppenregeln und Korrekturzielregel werden neu bewertet.

Ab v24.0.6 von Vulnerability Response, Sie können die Aktualisierungen eines CI in der Tabelle „erkanntes Element“ anzeigen. Informationen, einschließlich des vorherigen CI, des aktualisierten CI und des Anwenders, der die Änderungen vorgenommen hat, werden in der zugehörigen Liste Audit-Verlauf dokumentiert.

Wenn ein VI mit derselben Schwachstelle und demselben CI vorhanden ist, werden die Erkennungen mit dem vorhandenen VI aktualisiert, und das aktuelle VI wird mit dem Substatus als geschlossen Ungültiges CI . Arbeitsnotizen werden aus den folgenden Gründen hinzugefügt:

- Wenn Erkennungen von einem VI in ein anderes verschoben werden.
- Wenn ein doppeltes VI geschlossen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie das CI für das vorhandene VI nicht aktualisieren möchten, legen Sie die Eigenschaft fest `sn_sec_cmn.Update_on_ci_Change` Bis `Falsch` . Wenn sich dann ein CI ändert, wird ein neues VI erstellt, und das vorhandene wird als geschlossen `Ungültiges CI` .

Der Standardwert der Eigenschaft `sn_sec_cmn.Update_on_ci_Change` Ist `Wahr` .

Erkannte Elemente werden neu bewertet

Wenn neue Daten für ein erkanntes Element empfangen werden, wird das erkannte Element nicht sofort neu ausgewertet. Beim Empfang neuer Daten wird die *`reevaluate_ci`*Option ist auf festgelegt *`true`*Standardmäßig.

Die geplante Aufgabe *`Re-apply CI Lookup Rules on the Changed Discovered items`*Wertet alle erkannten Elemente aus, deren Quelldaten vom Scanner geändert werden. Es verarbeitet die erkannten Elemente erneut und aktualisiert die angreifbaren Elemente im Zusammenhang mit dem erkannten Element, dessen Quelldaten geändert werden. Der Wert dieser geplanten Aufgabe ist *`On Demand`*Standardmäßig.

Hinweis:
Sie können diese geplante Aufgabe auch täglich ausführen. Weitere Informationen zum Initiieren dieses Auftrags, zur Auftragshäufigkeit und zum Anzeigen der Anzahl der von ihm verarbeiteten Datensätze finden Sie unter KB1695110 Vulnerability Response: Wenden Sie CI-Suchregeln erneut auf die geänderten erkannten Elemente an .

Vulnerability Response status der Korrekturaufgabe und der angreifbaren Elemente

Mit Vulnerability Response Anwendung können Sie das Statusmodell verwenden, um den Status einer Korrekturaufgabe jederzeit anzuzeigen. Wenn Sie wissen, wie sich die einzelnen Status zueinander beziehen und sich gegenseitig auswirken, können Sie bestimmen, wann und wie Sie Ihre angreifbaren Elemente (VIS) beheben können.

status der Korrekturaufgabe

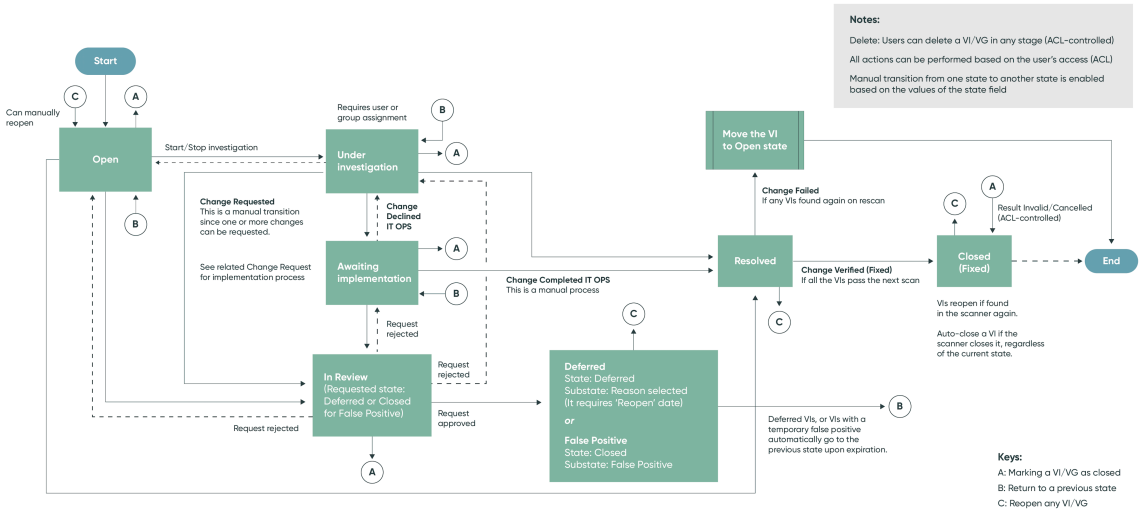
Komplexe Anwendungsfälle können manchmal dazu führen, dass sich ein angreifbares Element in einem anderen Status befindet als seine Korrekturaufgabe. Das Verständnis der Funktionsweise von status hilft bei der Erklärung dieses Verhaltens und kann beim Erstellen von Korrekturaufgaben und beim Erstellen oder Bearbeiten von Regeln für Korrekturaufgaben helfen.

Hinweis:
Ab v23.0 von Vulnerability Response, **Statusgenehmigung Des Angreifbaren Elements** Der Workflow ist veraltet und wird durch den Flow „Genehmigung des Schwachstellenstatus“ im Flow Designer ersetzt.

Korrekturaufgaben haben viele mögliche status, wie im folgenden Diagramm dargestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response-Status-Flow



Hinweis:
Jedes Aufgabenformular enthält **Folgen** Und **Aktualisieren** Schaltflächen, die Standard für sind ServiceNow Aufgaben.

Weitere Informationen zu status und Aktionen von Korrekturaufgaben, die Sie für einen entsprechenden Status ausführen können, finden Sie unter Vulnerability Response status der Korrekturaufgabe.

Weitere Informationen zu Erkennungen, Korrekturaufgaben und status angreifbarer Elemente finden Sie unter Erkennungen, Korrekturaufgaben und status angreifbarer Elemente.

Weitere Informationen zu Korrekturaufgaben und VI-status finden Sie unter Korrekturaufgaben und status angreifbarer Elemente.

Weitere Informationen zum Status der Korrekturaufgabe für VIS in mehreren Gruppen finden Sie unter Status der Korrekturaufgabe für angreifbare Elemente (Vits) in mehreren Gruppen.

Berechnung und Anzeige des Alters angreifbarer Elemente

Das Alter der angreifbaren Elemente (VIS) wird in angezeigt Vulnerability Response Anwendung mit mehr Details.

Das Alter angreifbarer Elemente (VI) wird im Format Tage/Stunden/Minuten in der Spalte Alter in der Listenansicht angreifbare Elemente und in den Feldern Alter und Alter geschlossen in VI-Datensätzen (VIT) angezeigt. Das in signifikanteren Ziffern angezeigte Alter kann Ihnen helfen, die folgenden Aktivitäten genauer auszuführen:

- Konfigurieren Sie Regeln im Modul „Regeln automatisch löschen“, um bestimmte VI-Datensätze nach Tagen/Stunden/Minuten anzuvisieren und zu löschen. Das Entfernen von Datensätzen mit größerer Genauigkeit kann Ihre Leistung steigern, insbesondere wenn Sie eine große Anzahl von VI-Datensätzen in Ihrer Instanz haben.
- Zeigen Sie Berichte mit spezifischeren Details in Performance Analytics für an Vulnerability Response Anwendung.
- Erstellen Sie Filter, die nur die gewünschten VIS identifizieren.
- Schneiden Sie Listenansichten so aus, dass nur die gewünschten VIS angezeigt werden.
- Dot-Walking einfacher.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine geplante Aufgabe berechnete das Alter und aktualisiert alle aktiven AES. In Instanzen mit einer großen Anzahl von VI-Datensätzen kann dieser Prozess langsam sein und sich negativ auf die Leistung auswirken. Das VI-Alter wird bei Bedarf effizienter berechnet und mit deutlicheren Stellen mit einer erweiterten Altersspalte angezeigt. Die Spalte „erweitertes Alter“ wird automatisch hinzugefügt, wenn Sie installieren oder aktualisieren Vulnerability Response Anwendung.

Hinweis:
Wenn Sie ein Upgrade durchführen und das VI-Alter nicht in der Listenansicht angreifbare Elemente und in den Feldern Alter und Alter geschlossen in aktiven VI-Datensätzen (VIT) im Format Tage/Stunden/Minuten (9 Tage, 18 Stunden, 29 Minuten) angezeigt wird, ist die Spalte Alter in Ihrer Instanz nicht aktuell. Weitere Informationen zur Lösung dieses Problems nach einem Upgrade finden Sie unter KB0749231 .

Die Spalte und die Felder „Alter“ können nicht bearbeitet werden. Ein Schwachstellenmanager mit der Berechtigung „sn_vul.Vulnerability_read“ oder die Schwachstellenadministrator-Persona kann diesen Wert anzeigen, und IT-Korrekturbesitzer mit der Rolle „sn_vul.Remediation_owner“ können ihn in Datensätzen anzeigen, die ihnen zugewiesen sind.

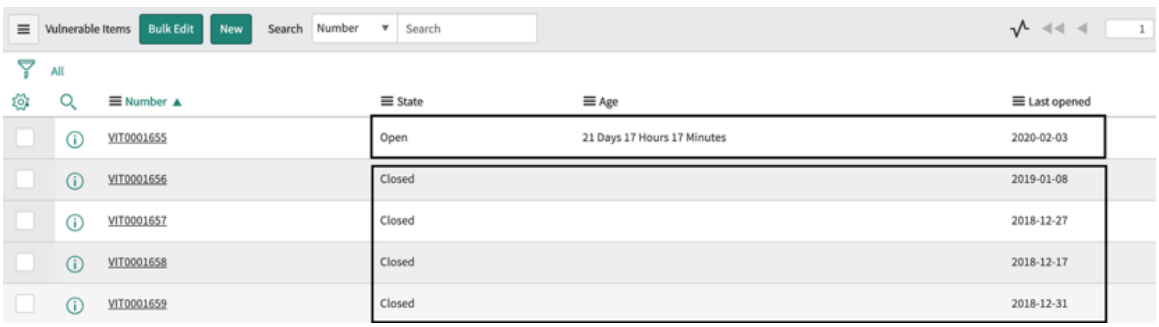
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

VI-Alter wird wie in den folgenden Bildern angezeigt.

Liste der angreifbaren Elemente

Wie in der folgenden Abbildung gezeigt, wird in der Listenansicht angreifbare Elemente das Alter in der Spalte Alter in Tagen/Stunden/Minuten (21 Tage 17 Stunden 17 Minuten) nur für aktive VIS angezeigt. Aktive VIS sind VIS in einem anderen status als „Geschlossen“. Dieser Alterswert stellt die Anzahl der Tage dar, die das VI aktiv war.

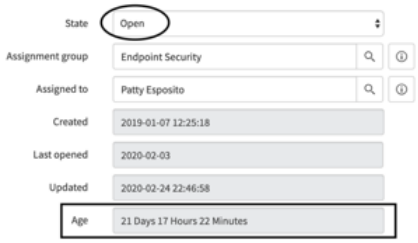
Das Alter wird für VIS im Status „Geschlossen“ nicht angezeigt. Für VIS, die zuvor den Status „Geschlossen“ hatten und dann erneut geöffnet wurden, stellt der Wert die Anzahl der Tage dar, an denen das VI seit dem Datum der letzten Öffnung aktiv war.



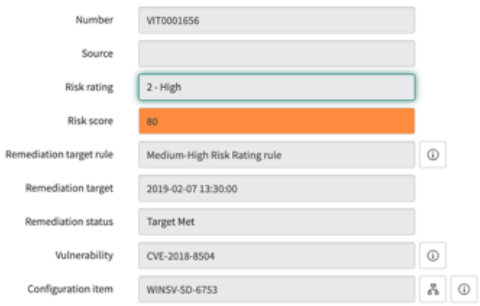
Alter der VI-Datensätze

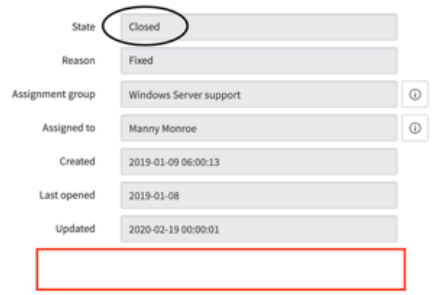
In den VI-Datensätzen ist der Wert der Spalte Alter in der Listenansicht für aktive VIS im Feld Alter sichtbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



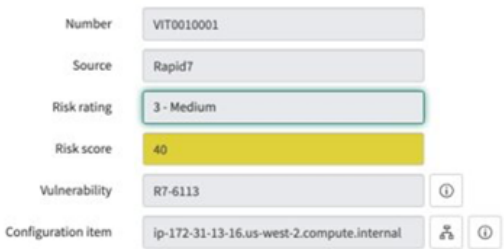
Der Wert der Spalte Alter wird für VI-Datensätze im Status „Geschlossen“ nicht angezeigt.

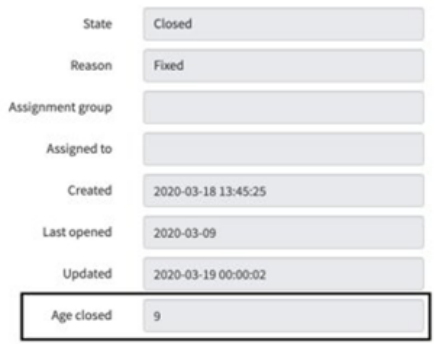




Alter in der Liste angreifbarer Elemente und in VI-Datensätzen, wenn ein VI aktualisiert wird

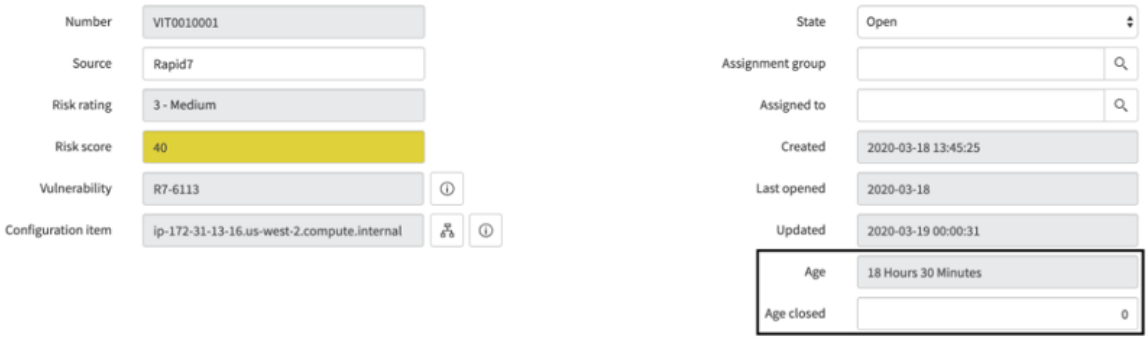
Wenn sich ein VI im Status „Geschlossen“ befindet, wird das Feld Alter nicht angezeigt. Wenn das VI in „Geschlossen“ übergeht, wird der Wert in der Anzahl der Tage ab der Spalte „Alter“ im Feld „Geschlossen“ (9) angezeigt, wie in der folgenden Abbildung dargestellt. Dieser Wert stellt die Anzahl der Tage dar, die das VI aktiv war, bevor es in „Geschlossen“ übergegangen ist Im folgenden Bild war dieses VI beispielsweise 9 Tage, 18 Stunden und 29 Minuten aktiv, aber nur die Anzahl der Tage (9) wird im geschlossenen Datensatz angezeigt.





Wenn dieses VI erneut geöffnet wird und der VI-Status zurück in „Offen“ wechselt, wird das Feld Alter geschlossen auf 0 zurückgesetzt. Da das VI wieder aktiv ist, wird das Alter in Tagen/Stunden/Minuten in der Listenansicht in der Spalte Alter und im Feld Alter in der VIT angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Weitere Informationen zum Anpassen der Berechnungen für Alter und Alter geschlossen finden Sie unter KB1703270 artikel.

Entfernen von Zuweisungen aus angreifbaren Elementen und Korrekturaufgaben

Sie können löschen **Zugewiesen an** Und **Zuweisungsgruppe** Felder in angreifbaren Elementen direkt aus den Datensätzen für angreifbare Elemente und Korrekturaufgaben, die Sie bestimmen, dass sie Ihnen oder Ihren Gruppen möglicherweise falsch zugewiesen sind.

Übersicht über den Workflow

Korrekturbesitzer und Schwachstellenanalysten können löschen **Zugewiesen an** Und **Zuweisungsgruppe** Felder und aktualisieren Sie Datensätze für die Neuzuweisung mit **Zuweisung Aufheben** UI-Aktion.

Anwendungsfall

Wenn Sie feststellen, dass Datensätze nicht in Ihrem Korrekturbereich liegen, oder wenn Sie der Meinung sind, dass sie Ihnen oder Ihren Gruppen falsch zugewiesen wurden, können Sie sich selbst oder Ihre Gruppen aus dem entfernen **Zugewiesen an** Und **Zuweisungsgruppe** Felder in Datensätzen für angreifbare Elemente und Korrekturaufgaben.

UI-Aktion „Zuweisung aufheben“ und Menü „weitere Optionen“

Sie können **Zuweisung Aufheben** Die folgenden Datensätze mit einer UI-Aktion oder aus dem Menü „weitere Optionen“ ( ) In einem anderen Status als „Geschlossen“ oder „gelöst“:

- Korrekturaufgaben (VULs, AVULs und CVULs) sowohl in der klassischen Umgebung als auch in den Arbeitsbereichen.

  Wenn eine Korrekturaufgabe mit dieser Funktion aktualisiert wird, wird **Zugewiesen an** Und **Zuweisungsgruppe** Felder in allen zugehörigen Vits, die dieselben Zuweisungsgruppen haben, werden ebenfalls gelöscht.

  Hinweis:
  Wenn eine VIT, AVIT oder CVIT in einer Korrekturaufgabe eine andere Zuweisungsgruppe als die Korrekturaufgabe hat, wird die Zuweisung nicht aufgehoben. In den meisten Fällen wurden diese angreifbaren Elemente manuell zugewiesen.

- Angreifbare Elemente (Vits, AVITs und CVITs) in der klassischen Umgebung und den Arbeitsbereichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Datensätze, für die Sie Zuweisungen mit der UI-Aktion oder manuell aktualisieren, werden im Modul „nicht zugewiesen“ unter den jeweiligen Produktmodulen angezeigt.

Für die Schritte zum Löschen von **Zugewiesen an** Und **Zuweisungsgruppe** Felder in Datensätzen mit *Unassigned*UI-Aktion, siehe Entfernen Sie Zuweisungen aus angreifbaren Elementen und Korrekturaufgaben Weitere Informationen finden Sie unter .

Systemeigenschaft und Benachrichtigungen

Wenn Sie auswählen **Zuweisung Aufheben** In einem Datensatz ist standardmäßig die *sn_vul.unassign_vr.approval_required*Und die Systemeigenschaft löst den Genehmigungs-Flow aus und erstellt einen Statusänderungsgenehmigungsdatensatz im Status „Überprüfen“, und die Genehmigungsanforderung wird für den Genehmiger ausgelöst, der in angezeigt wird **Meine Genehmigungen** Liste.

Hinweis:
Als Schwachstellenadministrator [sn_vul.Vulnerability_admin] können Sie festlegen *sn_vul.unassign_vr.approval_required*Systemeigenschaft zu **Falsch** Zum Deaktivieren des Genehmigungsprozesses.

- Wenn die Anforderung genehmigt wird, *sn_vul.default_assignment_group*Löscht **Zugewiesen an** Und **Zuweisungsgruppe** Felder und füllt aus **Zuweisungstyp** Feld mit **Nicht Zugewiesen** . Als Schwachstellenadministrator können Sie den Wert in ändern *sn_vul.default_assignment_group*Systemeigenschaft, damit die Zuweisungsfelder gelöscht werden und dann eine bestimmte Gruppe zugewiesen wird. Beispiel: Wenn ein Anwender auf klickt **Zuweisung Aufheben** Für einen Datensatz, der zur Überprüfung an eine bestimmte Gruppe weitergeleitet werden soll, können Sie im Feld Wert der Systemeigenschaft eine System-ID für die Gruppe Ihrer Wahl hinzufügen.

  Hinweis:
  Wenn Sie diesen Wert ändern, werden Benachrichtigungen für alle Vits, AVITs und angezeigt CVITs Nicht zugewiesene werden an die von Ihnen angegebene Gruppe gesendet.

- Wenn Ihre Anforderung abgelehnt wird, wird der Grund in angezeigt **Notizen** Registerkarte.

Alternativ, wenn *sn_vul.default_assignment_group*Ist nicht für eine bestimmte Gruppe konfiguriert. Standardmäßig werden Anwender, die Sie der Anwendergruppe „Benachrichtigung aufheben“ hinzufügen, benachrichtigt, wenn die Zuweisung von Datensätzen aufgehoben wird. Die *sn_vul.default_assignment_group*Die Systemeigenschaft bestimmt die Benachrichtigungen an diese Gruppe.

Der Zuweisungstyp, unabhängig davon **Manuell** , **Regel** , Oder **Nicht Zugewiesen** , Ist in den VIT-Datensätzen und der Listenansicht verfügbar. Die **Nicht Zugewiesen** Der Zuweisungstyp wird in Datensätzen nach angezeigt **Zugewiesen an** Und **Zuweisungsgruppe** Felder werden von der Systemeigenschaft gelöscht.

Siehe Genehmigen oder lehnen Sie eine Anforderung zum Aufheben der Zuweisung in ab Vulnerability Response Weitere Informationen zum Genehmigen von Anforderungen.

Überwachen Sie Ihre Zuweisungsregeln mit der geplanten Aufgabe für diese Funktion

Eine tägliche geplante Aufgabe zählt die Datensätze beim Übergang zu **Nicht Zugewiesen** Zuweisungstyp. Mit dieser Anzahl können Schwachstellenanalysten alle Zuweisungsregeln

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

überwachen und anpassen, die möglicherweise nicht gut funktionieren, basierend auf Zuweisungsregeln, die eine höhere Anzahl nicht zugewiesener VIS aufweisen.

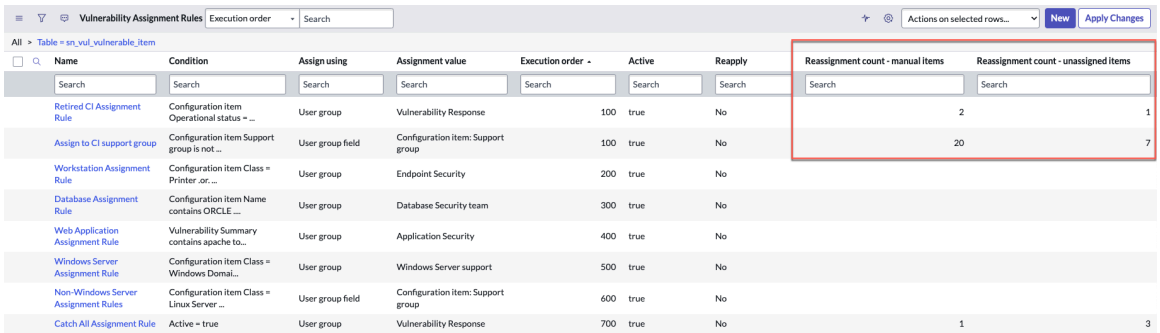
Die *`Reassignment count for assignment rules`*Die geplante Aufgabe wird täglich ausgeführt und veröffentlicht die Gesamtzahl der VIS, die von dieser Funktion für eine bestimmte Zuweisungsregel nicht zugewiesen werden.

Die von diesem Auftrag gesammelten Anzahlen gelten für die angreifbaren Elemente und die eindeutigen Zuweisungsregeln für Vulnerability Response Und Application Vulnerability Response. Anzahlen werden nach Zuweisungsregel in jeder Zuweisungsregelliste für jedes Modul angezeigt.

Der Auftrag zählt auch alle Datensätze, die manuell nicht zugewiesen wurden. Sowohl die manuellen Anzahlen als auch die von dieser Funktion gesammelten Anzahlen werden in der Liste „Schwachstellenzuweisungsregeln“ in zwei Spalten angezeigt: *`Reassignment count - manual items`*Und *`Reassignment count - unassigned items`*.

1. Navigieren Sie als Schwachstellenadministrator zu , um diese Anzahlen anzuzeigen **Vulnerability Response** > **Administration** > **Zuweisungsregeln**an.
2. Klicken Sie auf das Zahnradsymbol oben rechts in der Liste, und wählen Sie aus *`Reassignment count - manual items`*, Und *`Reassignment count - unassigned items`*Zur Anzeige.
3. Jedes VI, das ursprünglich von einer Regel zugewiesen wurde, anschließend jedoch automatisch oder manuell neu zugewiesen wurde, enthält einen Verweis auf die ursprüngliche Regel in der Listenansicht.

Das folgende Beispiel zeigt die Anzahl der Neuzuweisungen für zwei Zuweisungsregeln.



Vulnerability Response Rechner und Regeln für Schwachstellenrechner

Schwachstellenrechner automatisieren die Berechnung der Anfangswerte für die Felder in angreifbaren Elementen. Die Bedingung für jeden Rechner wird in der Reihenfolge ausgewertet, und der erste übereinstimmende Rechner wird verwendet.

Schwachstellen-Rechner

Die Vulnerability Response Das Basissystem enthält zwei Schwachstellenrechner, die die Basis festlegen **Risikopunktzahl** Für das angreifbare Element.

- **Standardrisikorechner**
- **Schwachstellenschweregrad**

Schwachstellenrechner können erstellt werden, um die Auswirkungen angreifbarer Elemente basierend auf beliebigen Kriterien mithilfe von Bedingungsfiltern zu priorisieren und zu bewerten. Unabhängig davon, ob es sich um die Geschäftsauswirkung der Schwachstelle,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Klasse des Konfigurationselements (Configuration Item, CI) oder das Alter des angreifbaren Elements handelt, können Sie zusätzliche Schwachstellenrechner erstellen, um andere Felder für angreifbare Elemente festzulegen. Oder Sie können die vorhandenen Schwachstellenrechner anpassen. Ein Rechner kann geschrieben werden, um einen beliebigen Satz von Prioritäten widerzuspiegeln. Siehe Erstellen Sie einen Vulnerability Response Rechner und Filtern in Vulnerability Response, um weitere Informationen zu erhalten.

Darüber hinaus können Sie Attribute in Configuration_item [cmdb_ci] in der Configuration Management Database (CMDB) verwenden, um Logik für Ihre Vulnerability Response-Risikorechner zu erstellen. Wenn Sie beispielsweise feststellen, dass CIs, die in Ihrer Organisation nach außen gerichtet sind, angreifbarer sind und möglicherweise sofortige Nachbesserungen erfordern, können Sie Attribute wie zuweisen `Internet Facing`Für diese CIs. Dieses Attribut und andere sind in den Versionshinweisen des Common Service Data Model aufgeführt . Für aktuelle Informationen und Anleitungen zum CMDB, Siehe die folgenden Themen:

- Konzeptionelles Modell des allgemeinen Servicedatenmodells
- CMDB-Schemamodell
- Vulnerability Response: Berechnung der Risikopunktzahl (KB1169927)

Jeder Rechner enthält eine Liste von Rechnerregeln mit einer Bedingung, die bestimmt, wann sie angewendet werden sollen. Wenn der Rechner ausgeführt wird, wird die Bedingung für jede Rechnerregel in der Reihenfolge ausgewertet, und die erste übereinstimmende Rechnerregel wird verwendet.

Die **Schwachstellenschweregrad** Der Rechner berechnet **Risikopunktzahl** Für angreifbare Elemente mit dem normalisierten Schwachstellenschweregrad.

Hinweis:

- Nur ein Rechner pro Zielfeld (**Risikopunktzahl**) Kann gleichzeitig aktiv sein. **Schwachstellenschweregrad** Ist standardmäßig deaktiviert.
- Immer wenn die Risikopunktzahl für eine VIT aktualisiert wird, wird die aktualisiert **Notizen** Abschnitt wird mit den folgenden Details aktualisiert:
  - Rechnergruppenname
  - Rechnername: Je nachdem, ob die Rechnerregel auf einer Vorlage oder einem Skript basiert, wird der Name mit den Details in Klammern angehängt. Um die Basis der Rechnerregel zu ändern oder anzuzeigen, klicken Sie auf eine beliebige Regel, und wählen Sie aus **Erweiterte Ansicht** Kontrollkästchen. Von **Werttyp** Wählen Sie im Dropdown-Feld die erforderliche Option aus. Wenn Vorlage ausgewählt ist, wird die Risikopunktzahl gemäß der in der Regel angegebenen Bedingung aktualisiert. Wenn Skript ausgewählt ist, können Sie das vorhandene Skript entweder hinzufügen oder aktualisieren.

    Die Systemeigenschaft `sn_sec_cmn.risk_score_changes_add_worknotes`Hilft beim Ausfüllen des Abschnitts „Arbeitsnotizen“. Ab v25.0.3 von Vulnerability Response, Die Systemeigenschaft ist standardmäßig inaktiv. Wenn Sie sie aktivieren, können Sie nur alle Änderungen im Zusammenhang mit der Risikopunktzahl anzeigen.

Alle aktivierten Schwachstellenrechner legen die ausgewählten Felder jedes Mal fest, wenn ein angreifbares Element erstellt wird, wenn sich ein zugehöriges CI oder eine Schwachstelle ändert oder wenn sich ändert **Berechnen Sie Die Risikopunktzahl** Zugehöriger Link in einem angreifbaren Element wird verwendet. Beispielsweise wird die Risikopunktzahl für Datensätze angreifbarer Elemente automatisch aktualisiert, wenn der Schweregradwert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für eine importierte Schwachstelle aktualisiert wird. Nachdem ein Schwachstellenimport eine Schwachstellenpunktzahl aktualisiert hat, wird die Kennzeichnung „Neu berechnen“ für diese Schwachstelle aktiviert. Die Risikopunktzahlen für die angreifbaren Elemente, für die die Kennzeichnung „Neuberechnung“ aktiviert ist (wahr), werden neu berechnet.

Wenn Sie in einem vorhandenen angreifbaren Element auf klicken **Berechnen Sie Die Risikopunktzahl** Zugehöriger Link und einer der Rechner ist aktiviert, der **Risikopunktzahl** Feld im angreifbaren Element wird aktualisiert.

Hinweis:

- Die **Berechnen Sie Die Risikopunktzahl** Der zugehörige Link ist nur sichtbar, wenn mindestens ein Schwachstellenrechner aktiviert ist.
- Sie können die Risikopunktzahl für ein angreifbares Element in aktualisieren Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen Indem Sie auswählen **Berechnen Sie Die Risikopunktzahl** Schaltfläche in der Datensatzansicht.
- Immer wenn sich die Risikopunktzahl für eine VIT ändert, werden die folgenden Details im Abschnitt „Notizen“ der VIT dokumentiert:
  - Rechnergruppenname
  - Rechnername
  - Feldwerte mit ihrer Gewichtung und ihrem Beitrag zur Risikopunktzahl
  - Endgültige Risikopunktzahl

Regeln des Schwachstellen-Rechners

Der Basissystemrechner **Standardrisikorechner** Enthält die Regel **Standardrisikoregel** , Eine spezialisierte Schwachstellenrechnerregel, die als bezeichnet wird **Risikoregel** . Wird berechnet **Risikopunktzahl** Basierend auf mehreren Werten:

- Schwachstellenschweregrad
- Exploit-Informationen
- Relevanz
- Externes Risiko des CI mit der Schwachstelle
- EPSS-Punktzahlen

Sie können die Werte anpassen, die in verwendet werden sollen **Standardrisikoregel** Und wie viel Gewichtung jeder dieser Werte gegeben werden soll. Gewichtungen werden verwendet, um anzupassen, wie viel jedes Element beim Festlegen der Basis zählt **Risikopunktzahl** .

Sie können die Kriterien für die Standardrisikoregel anpassen. Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel für Vulnerability Response-Risikorechner.

Ein Beispiel dafür, wie Risikopunktzahlen für Risikoregelrechner bestimmt werden, finden Sie unter Beispiel zur Berechnung der Risikopunktzahl für Vulnerability Response.

Zuweisen eines Gewichtungsprozentsatzes

Sie können den Gewichtungsprozentsatz (0–100) auch auf der Feldwertebene zuweisen. Sie können beispielsweise jeder Schweregradstufe einen Gewichtungsprozentsatz zuweisen (keine zu Kritisch).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Schweregradgewichtung für die Risikoregel 50 beträgt und die folgenden Gewichtungswerte für die Schweregradstufe zugewiesen werden:

Schwachstellenschweregrad	Risikopunktzahl
Kritisch	100
Hoch	50
Mittel	20
Keine	0

Wenn der Schweregrad „Kritisch“ ist, beträgt die entsprechende Gewichtung 50. Wenn der Schweregrad hoch ist, beträgt die äquivalente Gewichtung 25, und wenn der Schweregrad Mittel ist, beträgt die äquivalente Gewichtung 10. Wenn der Schweregrad „keine“ ist, ist die entsprechende Gewichtung 0. Weitere Informationen finden Sie unter Beispiel zur Berechnung der Risikopunktzahl für Vulnerability Response.

Regeleinstellungen für Schwachstellenrechner

Jede Regel hat einen **Reihenfolge** Einstellung. Die erste, die den Bedingungen entspricht, aktualisiert jedoch **Risikopunktzahl** Feld im angreifbaren Element. Weitere Informationen zu Einstellungen für Schwachstellenrechner-Regeln finden Sie unter Erstellen Sie einen Vulnerability Response Rechner. Nicht geskriptete Rechnerregeln verursachen normalerweise weniger Auswirkungen auf die Leistung als geskriptete Rechnerregeln.

Das Basissystem **Schwachstellenschweregrad** Der Rechner enthält Rechnerregeln, die jedem Schweregrad (keine bis Kritisch) einen Wert (0–100) für zuweisen **Risikopunktzahl** Basierend auf Schweregrad. **Unbekannter Schweregrad** Wird automatisch eine Risikopunktzahl von 100 zugewiesen. Diese Werte können angepasst werden und z. B. **Standardrisikorechner** , Neue Rechnerregeln oder neue Risikoregeln können erstellt werden.

Gewichtungen Der Schwachstellenrisikopunktzahl

Allen Schwachstellen wird eine Risikopunktzahl und eine Bewertung basierend auf Faktoren wie Schweregrad, Relevanz, Ausnutzungsinformationen usw. zugewiesen. Die Business-Regel `Update Risk Rating from Risk Score`ln der Tabelle „angreifbare Elemente“ ist für die Berechnung der Risikobewertung verantwortlich. Wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Elemente ausgefüllt.

Wert (Risikobewertung)	Gewichtung (Risikopunktzahl)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

- Die Risikobewertungstypen werden in der Basistabelle als vr_Risk_Rating geliefert. Diese Typen werden als Teil der Business-Regel in jeder Tabelle übergeben, in der die Risikobewertung berechnet wird.
- Das Skript wird geändert, sodass Sie die Einträge in den Tabellenwerten für Risikopunktzahlgewichtungen für die Berechnung der Risikobewertung abfragen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, stellen Sie sicher, dass Sie die Bezeichnungen für die neue Risikobewertung hinzufügen und auch die zugehörigen Skripts und Business-Regeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.
- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle mit Risikopunktzahlgewichtungen zugreifen, indem Sie sn_sec_cmn_Risk_Score_weight im Filternavigator eingeben.

Darüber hinaus wird die Risikopunktzahl automatisch neu berechnet, wenn die zugehörigen Common Vulnerabilities and Exposures (CVEs) oder Drittpartei-Einträge (TPEs) für die Schwachstellen-Elemente (VIS) mit einer bekannten CVE-Exploit-Schwachstelle (KEV) verknüpft sind.

Tenable-Schwachstellenintegration und Tenable-Risikoregel

Die Tenable-Risikoregel ist mit verfügbar Tenable Vulnerability Integration. Die Vulnerability Priority Rating (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit einem neuen Standardrisikorechner in verwendet wird Vulnerability Response. Die Tenable-Risikoregel wird mit installiert Vulnerability Response Integration with Tenable Anwendung als Teil des Standardrisikorechners in den Schwachstellenrechnern von Vulnerability Response.

Diese Risikoregel ist standardmäßig deaktiviert. Weitere Informationen finden Sie unter Konfigurieren Sie die Tenable-Schwachstellenintegration mit dem Setup-Assistenten.

Vulnerability Response Erkennungen angreifbarer Elemente aus Drittpartei-Integrationen

Zeigen Sie alle Informationen an, die von Drittpartei-Scans in erfasst werden ServiceNow AI Platform® Instanz. Zeigen Sie die zurückgegebenen Ergebnisse der Scans zu Erkennungs- und VI-Datensätzen (angreifbare Elemente) in Ihrer Instanz an, da diese Ergebnisse auf den Scannern angezeigt werden.

Übersicht

Die Vulnerability Response Die Anwendung unterstützt Integrationen von Drittparteien, die Daten angreifbarer Elemente aus Ihrer Unternehmensumgebung abrufen. Detaillierte Daten zu Erkennungen, d. h. einzelne, eindeutige Vorkommen von Schwachstellen, die von den Scannern Ihrer Drittanbieterintegrationen gemeldet werden, werden importiert und sowohl in den Erkennungs- als auch in den Datensätzen für angreifbare Elemente in angezeigt ServiceNow AI Platform Instanz.

Drittpartei-Integrationen rufen Erkennungsdaten für angreifbare Elemente ab. Erkennungen sind eindeutige Vorkommen von Schwachstellen, wie von den Scannern gemeldet. Erkennungsdaten werden mit angreifbaren Elementen gekoppelt, und der VI-Status wird basierend auf dem Status der Erkennungen aktualisiert. Wenn kein VI gefunden wird, wird ein neues erstellt. Erkennungen werden nur durch Daten geöffnet oder geschlossen, die direkt von einem Scanner gefunden werden.

In vorherigen Versionen von Vulnerability Response, Erkennungen angreifbarer Elemente, die Beziehung zwischen einem CI (Asset) in Ihrer Umgebung und einer importierten Schwachstelle von einem Scanner einer Drittpartei, hat ein eindeutiges angreifbares Element in erstellt ServiceNow AI Platform Instanz.

Die Granularität der vom Scanner bereitgestellten Originaldaten wird beibehalten. Bei Erkennungen werden die Erkennungsdaten mit angreifbaren Elementen gekoppelt. Wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

während einer Erfassung kein angreifbares Element gefunden wird, wird ein neues VI erstellt.

Ab Version 21.1.2 von Vulnerability Response, Eine Systemeigenschaft *sn_vul.show_last_open_detection*Wird im Basissystem bereitgestellt. Standardmäßig ist der Wert dieser Eigenschaft auf „falsch“ festgelegt, und das aktuelle Verhalten der Zusammenfassung der Werte aus der ersten Erkennung zum VI bleibt unverändert. Wenn dieser Wert jedoch auf „wahr“ festgelegt ist, wird ein VI nach einer Erfassung automatisch mit der letzten offenen Erkennung aktualisiert. Die Felder wie IP-Adresse, SSL, Port, Protokoll, NetBIOS, und Nachweise werden für die VI-Erkennungen aktualisiert. Bei Bedarf können Sie die Erkennungsfelder anpassen, die aktualisiert werden sollen, indem Sie ändern DetectionBase Skript.

Um die Werte für die letzte offene Erkennung anzuzeigen, navigieren Sie zu **Letzte Offene Erkennung** Registerkarte in der VI-Formularansicht. Um alle im letzten Jahr geöffneten VIS mit den letzten offenen Erkennungswerten zu aktualisieren, können Sie die geplante Aufgabe ausführen *Update Last Open Detection Value To VITs*Bei Bedarf. Diese geplante Aufgabe wird auch im Basissystem bereitgestellt.

Hinweis:
Wenn sich ein Konfigurationselement (Configuration Item, CI) an einem erkannten Element ändert, werden die entsprechenden Aktualisierungen auch in den Erkennungen berücksichtigt. Daher können die Erkennungen von einem VI in ein anderes VI verschoben werden Basierend auf dieser Änderung und dem Wert von *sn_vul.show_last_open_detection*Eigenschaft, werden die Werte der Erkennungen für die Quell- und Ziel-VIS zusammengefasst.

Unterstützte Versionen von Vulnerability Response

Weitere Informationen zum Installieren oder Aktualisieren von Vulnerability Response Anwendung, siehe Vulnerability Response installieren.

Unterstützte Integrationen von Drittparteien

Eine unterstützte Integration von Drittparteien mit Ihrem Vulnerability Response Anwendung ist für die Erkennung angreifbarer Elemente erforderlich. Die folgenden Drittpartei-Integrationen werden von unterstützt Vulnerability Response Anwendung für Erkennungen angreifbarer Elemente:

- Qualys-Host-Erkennungsintegration
- Rapid7 Data Warehouse:
  - Integration Angreifbarer Elemente
  - Integration Der Lösung Angreifbarer Elemente
- #Integration der Rapid7-Lösung für angreifbare Elemente (InsightVM)
  - Insight VM-Integration
  - Integration angreifbarer Elemente: API
- Tenable Vulnerability Integration
- Microsoft Defender Vulnerability Management

Diese Drittpartei-Integrationen sind mit einem separaten Abonnement von verfügbar ServiceNow Store. Weitere Informationen zu diesen Integrationen finden Sie unter Vulnerability Response-Integrationen Und Security Operations Und ServiceNow Store Weitere Informationen zum Abrufen der Berechtigung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Überprüfen, ob Ihr Drittpartei-Scanner für den Import konfiguriert ist, finden Sie unter Installieren und konfigurieren Sie die Anwendung Rapid7 Integration for Security Operations Und Qualys Vulnerability Integration installieren.

Schlüsselbegriffe für Erkennungen angreifbarer Elemente

Schwachstelle

Daten zu Schwachstellen in Software, Betriebssystemen und Assets, die aus internen und externen Quellen importiert wurden. Diese Daten werden importiert und mit vorhandenen Assets (Konfigurationselemente, CIs) verglichen, die in der CMDB aufgeführt sind.

Angreifbares Element

Ein angreifbares Element wird erstellt oder aktualisiert, wenn eine importierte Schwachstelle mit einem CI in der CMDB übereinstimmt.

Erkennung

Ein einzelnes, eindeutiges Vorkommen einer Schwachstelle, wie von einem Scanner gemeldet, der als Erkennung angreifbarer Elemente bezeichnet wird ServiceNow AI Platform Umgebung. Eine Erkennung enthält angereicherte Daten zu einer Schwachstelle und alle entsprechenden angreifbaren Elemente. Diese Daten werden im Erkennungsdatensatz (VID#) und in der Listenansicht angreifbarer Elemente angezeigt, die die folgenden Details enthält:

- Zuerst gefunden (Daten)
- Zuletzt gefunden (Datum)
- DNS-Name
- Net BIOSName
- IP-Adresse
- Port
- Protokoll
- Nachweis
- SSL
- Anzahl Ermittlungen

Hinweis:
Das Hinzufügen einer Business-Regel in der Erkennungstabelle wirkt sich auf die Leistung der Erfassung aus.

Erkennungsschlüssel

Eine Kombination von Feldern mit Hash, die eine Möglichkeit zum Identifizieren und Verknüpfen einer Erkennung mit einem angreifbaren Element bot. Erkennungsschlüssel sind integrationsspezifisch.

Erkennungsschlüsselkonfigurationen

Scanner	Schwachste	Port	Protokoll	Asset-ID	Nachweis	NIC
Qualys-IDs	Ja	Ja	Ja	Ja	Nein	NA
Tenable	Ja	Ja	Ja	Ja	Nein	NA
Rapid7	Ja	Ja	Ja	Ja	Ja (Groß-/ Kleinschreibung	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennungsschlüsselkonfigurationen (Fortsetzung)

Scanner	Schwachste	Port	Protokoll	Asset-ID	Nachweis	NIC
					wird nicht beachtet)	

Hinweis:

- Wenn der Erkennungsschlüssel nicht angegeben ist, oder für Versionen vor Vulnerability Response14.0. Der Erkennungsschlüssel ist eine Kombination aus Schwachstelleneintrag, Port, Protokoll, Asset-ID und Nachweis.
- Ab v19.0 von Vulnerability Response, Für wird eine neue Erkennungsschlüssel-NIC hinzugefügt Rapid7 InsightVM, Der standardmäßig aktiviert ist. Vorhandene Erkennungen ohne NIC werden mit der ersten eingehenden NIC in der Nutzlast von aktualisiert Rapid7. Der Erkennungsschlüssel wird neu berechnet und in der Erkennung einschließlich NIC neu ausgefüllt. Neue Erkennungen werden erstellt, wenn ähnliche Erkennungen mit unterschiedlichen NIC-Werten erkannt werden. Diese Daten werden nicht in der Tabelle „angreifbare Elemente“ zusammengefasst. Der NIC-Wert wird in einer neuen Spalte in der Tabelle „sn_vul_Detection_key_config“ und „sn_vul_Detection“ gespeichert.

De-dup

Der von verwendete Prozess Vulnerability Response Anwendung der Reduzierung einzelner Erkennungen in einem einzelnen VI, wenn die Daten bestimmte hartcodierte Kriterien erfüllen.

Externe VI-ID

Der im Feld externe ID der VI-Tabelle gespeicherte Wert. Dieser Wert ist ein Hash, der aus der Kombination von Schlüsseln in einem VI besteht und darstellt, was es innerhalb der Anwendung einzigartig macht. Er besteht aus einem CI und einem Eintrag für angreifbare Elemente.

Öffnen Sie gelöste angreifbare Elemente erneut

Angreifbare Elemente auf festgelegt **Gelöst** In Ihrem ServiceNow AI Platform Instanz, aber nicht auf übergegangen **Geschlossen/Behoben** Durch die nachfolgenden Integrationsausführungen werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Geschlossene VIS mit einem Substatus von **Behoben** Oder **Veraltet** Werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die VIS mit der neuen Schwachstelle abgeglichen werden können.

Gemäß der Skripteinbindung *`DetectionBase`*, Methode *`_shouldReOpenVI()`*, Wenn die VIT früher war **Geschlossen** Mit Substatus **Behoben** , **Veraltet** , Oder **CI außer Betrieb genommen** , Wird erneut geöffnet, und die Erkennung wird der vorhandenen VIT zugeordnet.

Angenommen, das Datum der Schließung eines VIT liegt nach dem Datum Last_found einer Erkennung. Sie sollten davon ausgehen, dass diese VIT-Datensätze geschlossen bleiben. Wenn jedoch eine zuvor geschlossene VIT erneut geöffnet wird, bedeutet dies, dass die VIT durch eine frühere Erkennung geschlossen wurde und die Schwachstelle bei einem späteren Scan erneut gefunden wurde. Wenn eine neue Erkennung gefunden wird, die der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

geschlossenen VIT entspricht, die dieselbe Schwachstelle im Konfigurationselement der VIT aufweist, wird die VIT erneut geöffnet.

Für Rapid7 Erkennungen ist jetzt auf der Rapid7-Konfigurationsseite in Ihrer Instanz eine Option verfügbar, um gelöste VIS nach Alter erneut zu öffnen. Wenn diese Option aktiviert ist, werden VIS auf festgelegt **Gelöst** Aber dann nicht zu übergegangen **Geschlossen/ Behoben** Durch nachfolgende Scans gehen zurück zu **Öffnen** Nach der von Ihnen eingegebenen Anzahl von Tagen.

Für Qualys Erkennungen, wenn der Scanner weiterhin VIS findet, die auf festgelegt wurden **Gelöst** Aber dann nicht zu übergegangen **Geschlossen/Behoben** Durch nachfolgende Scans werden diese VIS zurück zu verschoben **Öffnen** Wenn das Datum der letzten Suche nach dem Datum der Lösung liegt.

Zeigen Sie Erkennungsdaten an

Sie zeigen die aus Erkennungen angreifbarer Elemente importierten Daten im VI-Datensatz an. Weitere Informationen finden Sie unter Anzeigen Vulnerability Response Erkennungsdaten für angreifbare Elemente und Verifizieren Vulnerability Response Erkennungsdaten für angreifbare Elemente in VINTRUN-Datensätzen (Integrationsausführung).

Vulnerability Solution Management

Korrelieren Sie die Schwachstellen in Ihrer Umgebung automatisch mit dem Lösungen, mit denen sie behoben werden könnten. Identifizieren Sie die Korrekturmaßnahmen, die für Ihre Schwachstellen gelten, und priorisieren Sie sie durch die größte Reduzierung des Schwachstellenrisikos.

Vulnerability Solution Management

Sicherheits- und IT-Teams verbringen häufig eine beträchtliche Zeit mit der Erforschung von Schwachstellenergebnissen, um die effektivsten Behandlungen für ihre Umgebung zu identifizieren. Angesichts des Umfangs und der Komplexität von Schwachstellen in großen Organisationen ist die Umsetzung von Schwachstellenergebnissen in Korrekturaufgaben ein manueller, langwieriger und fehleranfälliger Prozess.

Mit Vulnerability Solution Management, Sie können Ihre Schwachstellen-Ergebnisse automatisch mit den Lösungen korrelieren, die sie beheben. Identifizieren Sie die Software-Patches, Konfigurationsupdates und andere Steuerungen, die die größten Auswirkungen für Ihr Unternehmen ohne manuellen Aufwand haben.

Vulnerability Solution Management-Anforderungen

Vulnerability Solution Management Ist eine Funktion, die in verfügbar ist Vulnerability Response Anwendung. Vulnerability Solution Management Erforderlich Ein separates Abonnement.

Weitere Informationen zum Abrufen von Berechtigungen für Anwendungen aus dem ServiceNow Store, Siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung. Siehe Anwendung Solution Management for Vulnerability Response installieren Weitere Informationen zur Installation der Anwendung, nachdem Sie sie auf Ihre Instanz heruntergeladen haben.

Nach der Installation Vulnerability Solution Management Bietet Ihnen Zugriff auf Microsoft Security Response Center Und Red Hat Lösungsdaten aus innerhalb Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Sie können beide Lösungsanwendungen über den Setup-Assistenten konfigurieren. Weitere Informationen finden Sie unter Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management Mit dem Setup-Assistenten.

Siehe Integration der Microsoft Security Response Center-Lösung Und Red Hat Solution Integration Für weitere Informationen zu den importierten Lösungen .

Verfügbare Versionen

Für die aktuelle Version von Vulnerability Solution Management, Stellen Sie sicher, dass Sie die aktuelle Version von haben Vulnerability Response Installiert.

Release-Version von Vulnerability Solution Management	Kompatible Versionen von Vulnerability Response	Release-Hinweise
Vulnerability Solution Management V10.3	Vulnerability Response V18.0	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Über Lösungen und Ersatz

Ein ersetztes Update ist ein vollständiger Ersatz eines oder mehrerer früherer Releases. Beispielsweise kann ein Hotfix-Update durch ein Service Pack ersetzt werden. Lösungen beziehen sich auf Schwachstellen. Lösungen können sich auch auf andere Lösungen in einer Ersatzkette beziehen. Lösungen beheben Schwachstellen in vorherigen Lösungen und sind kumulativ. Vulnerability Solution Management Ordnet Schwachstellen aus vorherigen Lösungen automatisch Ersatzlösungen zu. Wenn eine ältere Schwachstelle gefunden wird, kann eine höhere Ersatzlösung sie beheben, aber die höchste Ersatzlösung wird bevorzugt, da sie die kumulativste ist.

Potenzielle vs. Bevorzugte Lösungen

Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben könnte. Schwachstellen haben oft viele potenzielle Lösungen. Eine bevorzugte Lösung ist die einzelne Lösung, die zum Beheben einer Schwachstelle oder eines angreifbaren Elements (VI) dient. Sie kommuniziert die Absicht und ermöglicht detailliertere Bereitstellungsmetriken.

Bevorzugte Lösungen

Vulnerability Solution Management Legt automatisch die effektivste Lösung fest (**Bevorzugte Lösung**) Für die erkannte Schwachstelle basierend auf der höchsten Ersatzlösung, wenn nur eine höchste Ersatzlösung vorhanden ist. Wenn für die Schwachstelle mehr als eine höchste Ersetzung vorhanden ist, wird kein Wert festgelegt. In Vulnerability Response, A **Bevorzugte Lösung** Ist Microsoft Security Response Center Oder Red Hat Lösung mit der höchsten Ersatzlösung, die aus den Lösungen abgeleitet ist, die der Schwachstelle zugeordnet sind.

Bevorzugte Lösung Werte können für das angreifbare Element oder die Schwachstelle festgelegt werden. Wenn diese Option direkt auf der Schwachstelle festgelegt ist,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

übernehmen alle angreifbaren Elemente, die der Schwachstelle zugeordnet sind, diese Lösung. Ändern Sie **Bevorzugte Lösung** Werte für mehrere angreifbare Elemente, die die Massenbearbeitungsfunktion verwenden. Bei Massenbearbeitung wird nur der verwendet **Bevorzugte Lösung** Für das angreifbare Element wird aktualisiert, indem festgelegt wird **Bevorzugte Lösung** Auf der Ebene des Schwachstelleneintrags würde festlegen **Bevorzugte Lösung** Für alle neuen VIS in Zukunft. Massenbearbeitung gilt nur für aktuelle angreifbare Elemente.

Hinweis:
Wenn mehrere höchste Ersatzlösungen für eine Schwachstelle vorhanden sind, **Bevorzugte Lösung** Werte auf der Schwachstellenebene werden gelöscht, da diese Lösung vom betroffenen Asset abhängt. Wenn mehrere höchste Ersatzlösungen für eine Schwachstelle vorhanden sind, legen Sie einen fest **Bevorzugte Lösung** Für das angreifbare Element. Mit können Sie eine andere Lösung festlegen **Suchen** Liste in **Angreifbares Element** Formular.

Alle bevorzugten Lösungen für die angreifbaren Elemente in Korrekturaufgaben befinden sich in einer zugehörigen Liste auf der **Korrekturaufgabe** Datensatz.

Nicht alle Lösungsimporte führen zu vollständigen Datenaktualisierungen. Der Ersetzungsprozess wird aktualisiert, wenn:

- Ein angreifbares Element wird erstellt.
- Die Daten für ein aktives VI wurden geändert

Hinweis:
Beginnend mit v22.0 von Vulnerability Response, Die Lösungen befinden sich in den obigen beiden Fällen nicht in der Warteschlange.

- Für einen Drittparteieintrag mit dem CVE wird eine neue Zuordnung erstellt.
- Neue Lösungsdaten wurden seit dem letzten Import veröffentlicht. Eine vorhandene Lösung wird aktualisiert.

Ab v24.0.6 von Vulnerability Response, Sie können die Lösung zusätzlich zu Lieferantenlösungen aus Scannern erfassen. Die Korrekturdaten von Scannern wie Tenable, Qualys, Und Microsoft TVM wird verwendet, um die Lösungen zu erstellen. Diese Scannerlösungen werden mit den folgenden Integrationen importiert:

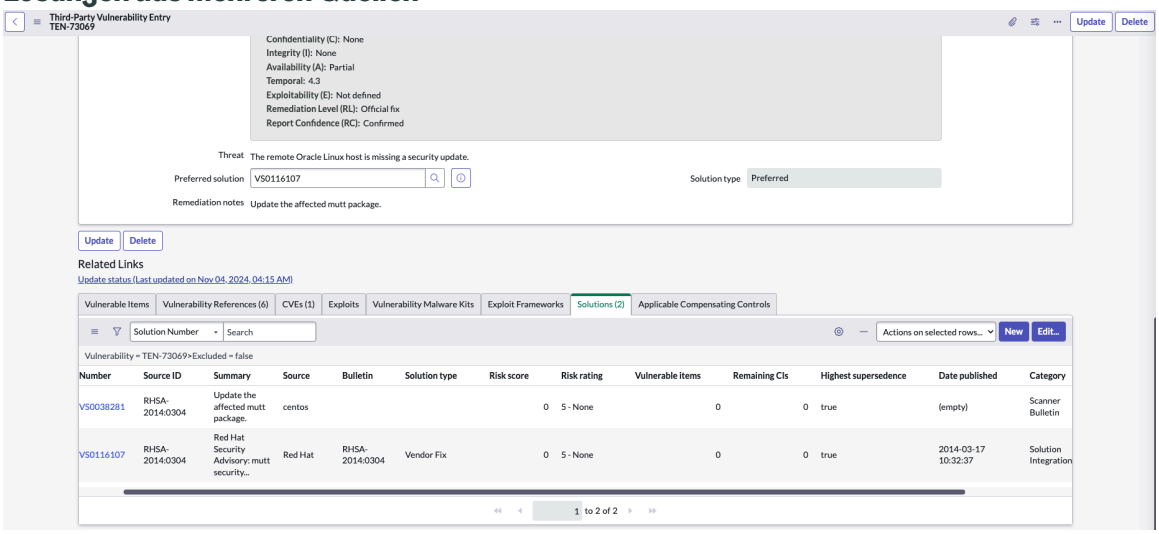
- Tenable.sc Plugin-Integration
- Tenable.io Plugin-Integration
- Qualys Knowledge Base (Auffüllen)
- Integration von Microsoft TVM-Computer-Schwachstellen (vollständiger Import)
- Integration von Microsoft TVM-Computer-Schwachstellen (Delta-Import)

Wenn die Schwachstellenintegrationen ausgeführt werden, wird eine Nutzlast von Korrekturinformationen erstellt, bevor Drittparteieinträge verarbeitet werden. Für Tenable und Qualys, Die Korrekturdaten werden auf der Ebene der Schwachstellen oder Drittpartei empfangen. Umgekehrt werden für Microsoft TVM Lösungen auf Erkennungsebene erstellt, wodurch eine direkte Auffüllung bevorzugter Lösungen für die angreifbaren Elemente ermöglicht wird, ohne dass eine weitere Verarbeitung erforderlich ist. Diese Lösungen werden basierend auf diesen Korrekturinformationen erstellt und nach Bedarf verarbeitet. Bei der Verarbeitung wird die bevorzugte Lösung für die Schwachstellen ausgefüllt und auf die angreifbaren Elemente zurückgesetzt. Die bevorzugte Lösung wird in der folgenden Reihenfolge ausgefüllt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Manuelle Auswahl: Wenn Sie eine Lösung manuell auswählen, wird sie nicht überschrieben.
- Lieferantenlösungen (Microsoft-, RedHat-, CVRF- und CSAF-Importe): Wenn Sie eine Lösung nicht manuell auswählen, wird die Lieferantenlösung automatisch ausgewählt.
- Neueste Lösungen (falls aktiviert): Wenn für eine Schwachstelle mehrere Lösungen mit höherem Ersatz verfügbar sind, wird die verwendet **Bevorzugte Lösung** Feld bleibt leer. In solchen Fällen, wenn Sie die Eigenschaft aktivieren `sn_vul.latest_solutions`, Die neueste höhere Ersatzlieferantenlösung wird als bevorzugte Lösung ausgefüllt.
- Scanner-Bulletin-Lösungen (falls aktiviert): Wenn Sie eine Lösung nicht manuell auswählen oder Lieferantenlösungen nicht verfügbar sind, wird die **Bevorzugte Lösung** Feld wird mit den Scannerlösungen ausgefüllt, die bereitgestellt werden, dass eine einzelne Scannerlösung vorhanden ist. Sie müssen die Eigenschaft aktivieren `sn_vul.populate_scanner_solutions`Zum Ausfüllen der Scannerlösungen.

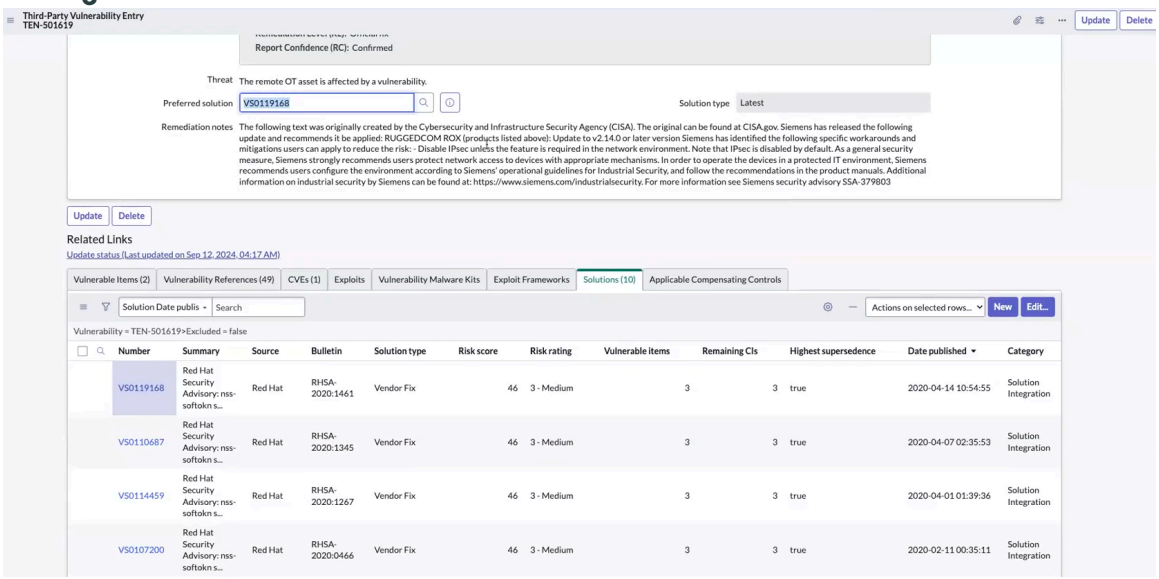
Lösungen aus mehreren Quellen



Dieses Beispiel veranschaulicht die Auswahl einer Lösung, wenn mehrere Lösungen aus verschiedenen Quellen verfügbar sind. In diesem Fall gibt es zwei Lösungen für eine Schwachstelle – eine von einem Lieferanten und eine andere von einem Scanner. Da die Lösung VS0116107 von einem Lieferanten erhalten wird, d. h. Redhat, der eine höhere Einstellung hat, wird sie als bevorzugte Lösung ausgewählt.

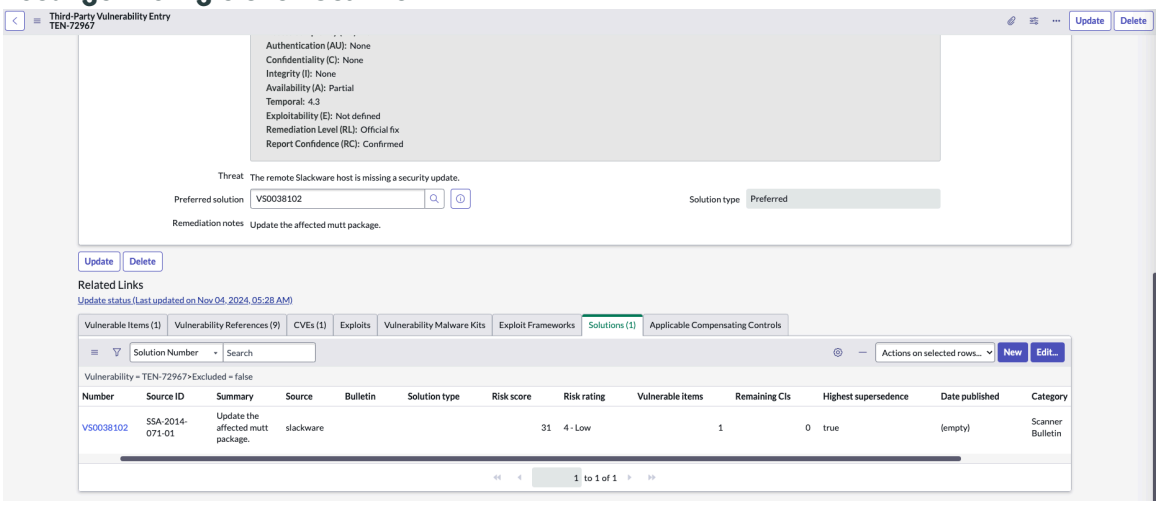
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lösungen desselben Lieferanten



Dieses Beispiel veranschaulicht die Auswahl einer Lösung, wenn mehrere Lösungen vom selben Lieferanten verfügbar sind, d. h. in diesem Fall „Redhat“. Wenn *sn_vul.latest_solutions*Die Eigenschaft ist aktiviert, und für eine bestimmte Schwachstelle sind keine anderen Lieferantenlösungen verfügbar. Diese Lösungen werden verarbeitet, wobei bevorzugte Lösungen für die Schwachstellen und anschließend für angreifbare Elemente ausgefüllt werden. Wenn Sie die Eigenschaft aktivieren *sn_vul.latest_solutions*, Die neueste Lösung wird als bevorzugte Lösung ausgewählt.

Lösungen vom gleichen Scanner



Dieses Beispiel veranschaulicht die Auswahl einer Lösung, wenn nur eine Scannerlösung über die Scanner verfügbar ist. Wenn *sn_vul.populate_scanner_solutions*Eigenschaft ist aktiviert, die Lösungen werden verarbeitet, wobei die bevorzugten Lösungen für die Schwachstellen und anschließend für die angreifbaren Elemente ausgefüllt werden. Wenn mehrere Scannerlösungen vorhanden sind, die **Bevorzugte Lösung** Feld ist aufgrund von Mehrdeutigkeit leer.

Verbesserung des Lösungsmanagements und der Leistungsoptimierung

Lösungen werden aus verschiedenen Integrationen erhalten, einschließlich Microsoft und Redhat. Erstere stellt monatliche Updates bereit und richtet eine Kette von Abhängigkeiten ein, um die bevorzugte Lösung für Schwachstellen nachzuverfolgen. Andere Integrationen folgen diesem Update-Format jedoch nicht und müssen keine Abhängigkeitskette für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sie einrichten. Zuvor wurde eine Verarbeitungslogik verwendet, bei der ein Diagramm erstellt wurde, um Vorrang zu erhalten und die am häufigsten ersetzenden Lösungen zu identifizieren. Diese Lösungen wurden als bevorzugte Lösung für die Schwachstellen vorgeschlagen. Da die Erstellung des Diagramms jedoch zeitaufwändig ist, sind die anderen Integrationen von diesem Prozess ausgeschlossen. Zur Verbesserung der Leistung ab v22.0 von Vulnerability Response, Die Methode `utility.processNonGraphSolutions()` Wird in aufgerufen `Process Vulnerability Solutions Metrics Queue`Geplante Aufgabe. Diese Methode verarbeitet Lösungen aus anderen Integrationen als Microsoft.

Zweitens werden die Lösungen mithilfe der geplanten Aufgabe aus verschiedenen Quellen in die Warteschlange gestellt `Process Vulnerability Solutions Metrics Queue`. Diese geplante Aufgabe umfasst das Rollup von Lösungen aus NVD-Einträgen zu Drittpartei-Einträgen, das Ausfüllen bevorzugter Lösungen zu Schwachstellen und das Aktualisieren der Korrekturstatusmetriken für die Lösungen. In den folgenden Szenarien müssen nur die Korrekturstatusmetriken aktualisiert werden:

- Wenn sich die bevorzugte Lösung für die Schwachstellen ändert
- Wenn die Vits erstellt oder gelöscht werden
- Wenn ein VIT-Import abgeschlossen ist

Obwohl die Lösungen in der Warteschlange stehen, um nur die Korrekturstatusmetriken zu aktualisieren, versuchen sie dennoch, Lösungen von NVD-Einträgen zu Drittparteieinträgen zusammenzufassen und die bevorzugten Lösungen auszufüllen. Um diesen Prozess zu optimieren, finden Sie in der Tabelle „Schwachstellenlösung“ die Spalte **Status aktualisieren** Wird eingeführt. Wenn die Korrekturstatusmetriken für Lösungen aktualisiert werden müssen, ohne dass ein Rollup oder eine Auffüllung bevorzugter Lösungen erforderlich ist, werden die Lösungen nicht mehr in die Warteschlange gestellt. Stattdessen wird **Status aktualisieren** Spalte wird direkt als „wahr“ aktualisiert. Dieser Ansatz ermöglicht die Verarbeitung von Fällen, in denen nur die Korrekturstatusmetriken aktualisiert werden müssen, was zu Zeit- und Ressourceneinsparungen führt. Sobald die Verarbeitung der Lösungen in der Warteschlange abgeschlossen ist, werden in der geplanten Aufgabe Lösungen identifiziert, die mit dem Aktualisierungsstatus „wahr“ gekennzeichnet sind. Anschließend werden sie durch diese Lösungen iteriert, berechnet die Anzahl und aktualisiert die Korrekturstatusmetriken entsprechend. Dieser Schritt spielt eine wichtige Rolle bei der Verbesserung der Leistung der geplanten Aufgabe, da die Anzahl der Lösungen, die in die Warteschlange gestellt werden müssen, reduziert wird. Um Korrekturstatusmetriken anzuzeigen, navigieren Sie zur Tabelle Schwachstellenlösung [sn_vul_Solution], und wählen Sie eine Schwachstellenlösung aus. Wählen Sie dann aus **Korrekturstatus** Registerkarte. Die Registerkarte enthält die folgenden Felder:

Korrekturstatusmetriken

Feld	Beschreibung
Bevorzugte Lösungsziele: Korrekturstatus für VIS, für die dies die bevorzugte Lösung ist	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Verbleibende CIs	Anzahl der CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturstatusmetriken (Fortsetzung)

Feld	Beschreibung
VIs insgesamt	Anzahl der aktiven und geschlossenen angreifbaren Elemente, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
CIs insgesamt	Anzahl der CIs, die mindestens einem aktiven und geschlossenen angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Behobene AEs in Prozent	Prozent abgeschlossen für Korrektur angreifbarer Elemente (VI). Gilt für VIS, für die diese Lösung bevorzugt wird. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Behobene CIs in Prozent	Prozent abgeschlossen für CI-Korrektur. Gilt für VIS, für die diese Lösung bevorzugt wird. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Bevorzugte Lösungsziele (enthält zurückgestellte): Korrekturstatus für VIS, einschließlich zurückgestellte, für die dies die bevorzugte Lösung ist	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung zur Korrektur bevorzugt wird.
Verbleibende CIs	Anzahl der CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
VIs insgesamt	Anzahl der aktiven und geschlossenen angreifbaren Elemente, für die diese Lösung zur Korrektur bevorzugt wird.
CIs insgesamt	Anzahl der CIs, die mindestens einem aktiven und geschlossenen angreifbaren Element zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird.
Behobene AEs in Prozent	Prozent abgeschlossen für Korrektur angreifbarer Elemente (VI). Gilt für VIS, für die diese Lösung bevorzugt wird.
Behobene CIs in Prozent	Prozent abgeschlossen für CI-Korrektur. Gilt für VIS, für die diese Lösung bevorzugt wird.
Potenzielle Lösungsziele: Korrekturstatus für alle VIS mit einer Schwachstelle im Zusammenhang mit dieser Lösung	
Angreifbare Elemente	Anzahl der aktiven (nicht geschlossenen) angreifbaren Elemente, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Verbleibende CIs	Anzahl der CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung eine potenzielle Lösung zur Korrektur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturstatusmetriken (Fortsetzung)

Feld	Beschreibung
	darstellt. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Potenzielle Lösungsziele (enthält zurückgestellte): Korrekturstatus für alle VIS, einschließlich zurückgestellte, mit einer Schwachstelle im Zusammenhang mit dieser Lösung	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt.
Verbleibende CIs	Anzahl der CIs, die mindestens einem aktiven angreifbaren Element zugeordnet sind, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt.

Drittens muss die Verfügbarkeit einer bevorzugten Lösung für Schwachstellen und Vits sichergestellt werden, um die Schwachstellen zu beheben. In Situationen, in denen für eine Schwachstelle mehrere höhere Ersatzlösungen vorhanden sind, wird eine bevorzugte Lösung aufgrund von Mehrdeutigkeiten nicht ausgefüllt. Um dieses Szenario zu beheben, wird ein Ansatz implementiert, bei dem die Verarbeitungslogik ausgeführt und die bevorzugte Lösung ausgefüllt wird, wenn sie verfügbar ist. In Fällen, in denen nur eine höhere Ersatzlösung vorhanden ist, wird sie als bevorzugte Lösung ausgefüllt. Wenn mehrere höhere Ersatzlösungen vorhanden sind, bleibt das Feld bevorzugte Lösung leer. Das Ziel besteht jedoch darin, die höchste Ersatzlösung, die als neueste veröffentlicht wird, als bevorzugte Lösung auszufüllen. Um dies zu erreichen, eine Systemeigenschaft *sn_vul.latest_solutions*Wird eingeführt. Standardmäßig ist diese Eigenschaft auf „false“ gesetzt. Wenn Sie die Fähigkeit aktivieren möchten, die neuesten Lösungen als bevorzugte Lösung auszufüllen, wenn keine bevorzugte Lösung verfügbar ist, können Sie diese Eigenschaft aktivieren. Nach der Aktivierung wird die aktiviert **Lösungstyp** Spalte wird in der Tabelle „Schwachstellen“ mit den folgenden Optionen aktualisiert:

- Bevorzugt: Wenn die bevorzugte Lösung ausgefüllt ist
- Aktuell: Wenn keine bevorzugte Lösung verfügbar ist, wird basierend auf dem Veröffentlichungsdatum die neueste Lösung aus dem Satz der höchsten Ersatzlösungen ausgewählt. Das Feld, das als aktuelle Lösung ausgewählt werden soll, kann mit angepasst werden *sn_vul.latest_solutions*Systemeigenschaft. Standardmäßig ist der Wert auf „Veröffentlichungsdatum“ festgelegt, kann jedoch in „zuletzt geändert“ geändert werden, um die Lösung basierend auf der Spalte „zuletzt geändert“ in den Lösungen auszuwählen.
- Manuell: Wenn der bevorzugte Lösungstyp manuell aktualisiert wird. Der Vorrang für diesen Lösungstyp ist der höchste.

In bestimmten Szenarien kann sich die bevorzugte Lösung für ein angreifbares Element (VIT) von der bevorzugten Lösung für die entsprechende Schwachstelle unterscheiden. Dies tritt auf, wenn die bevorzugte Lösung manuell in einer VIT und nicht in der Schwachstelle aktualisiert wird. In solchen Fällen die **Lösungstyp** Feld ist in der VIT ausgeblendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Was Vulnerability Solution Management Tut

- Ordnet während automatisch neue angreifbare Elemente (Vits) und Korrekturaufgaben Lösungen zu Integration der Microsoft Security Response Center-Lösung Und Red Hat Solution Integration Importieren.

  MSRC Lösungen sind dem neuesten Bulletin zugeordnet, in dem die Lösung angezeigt wird.

- Ordnet angreifbare Elemente und Korrekturaufgaben automatisch Lösungen zu, wenn Schwachstellendatensätze manuell Lösungen zugeordnet werden.

  Hinweis:
  Angreifbare Elemente, die manuell einer anderen Lösung zugewiesen wurden, werden nicht automatisch mit Lösungsänderungen auf Schwachstellenebene aktualisiert.

- MSRC: Erstellt Ersatzketten während des Imports, die Sie in der zugehörigen Liste der Lösung anzeigen können.
- Gibt an, ob eine Lösung eine Lösung mit dem höchsten Ersatzwert ist oder nicht.
- Listet die Lösung auf **Risikopunktzahl** Zugeordnet zu jeder Lösung, um Ihnen die größten Möglichkeiten zur Risikominderung zu bieten.

- Verwaltet **Korrekturstatus** Für Lösungen in **Drittanbieter-Schwachstelleneinträge** , **Korrekturaufgaben** , Und **Schwachstellenlösung** Datensätze, damit Sie den Korrekturfortschritt nachverfolgen können.

  Enthält:

  - Anzahl der angreifbaren Elemente nach Prozentsatz der Korrektur für die VIS mit bevorzugten Lösungen mit und ohne diese VIS im Status zurückgestellt.
  - Anzahl der Konfigurationselemente (Configuration Item, CI) nach Prozentsatz der Korrektur für die VIS mit bevorzugten Lösungen mit und ohne diese VIS im Status „Zurückgestellt“.
  - Anzahl der angreifbaren Elemente nach Prozentsatz der Korrektur für die VIS mit potenziellen Lösungen mit und ohne diese VIS im Status „zurückgestellt“.
  - Anzahl der Konfigurationselemente nach Prozentsatz der Korrektur für die VIS mit bevorzugten Lösungen mit und ohne diese VIS im Status zurückgestellt.

Was Sie damit tun können Vulnerability Solution Management

- Erstellen, aktualisieren, anzeigen oder löschen Sie Lösungen, die Schwachstellen zugeordnet sind, damit Sie Schwachstellen-Lösungen nachverfolgen können, die nicht von Inhalten von Drittanbietern abgedeckt werden. Die Lösungsintegration mit dem Rapid7 Data Warehouse wird nicht unterstützt.
- Ordnen Sie Schwachstellen von Drittparteien und NVD-Einträge einem Lösungsdatensatz zu.
- Entfernen Sie angreifbare Elemente und Korrekturaufgaben, und ordnen Sie sie erneut einer Lösung zu.
- Zeigen Sie an **Bevorzugte Lösung** Gilt für eine bestimmte Schwachstelle in den Formularen „Schwachstelle“ und „angreifbare Elemente“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie ein an **Bevorzugte Lösungen** Zugehörige Liste in Korrekturaufgabenformularen, die alle Lösungen auflisten, die von mindestens einem aktiven VI innerhalb dieser Gruppe bevorzugt wurden.
- Zeigen Sie an **Korrekturstatus** Details zu einer Lösung, die die mit der Bereitstellung von verbundene Risikominderung anzeigen **Bevorzugte Lösung** Auf Schwachstellen, angreifbaren Elementen, Korrekturaufgaben und Lösungsformularen.
- Zeigen Sie Schwachstellen, die für eine bestimmte Lösung gelten, im Lösungsformular an.
- MSRC: Zeigen Sie die Ersatzlösungen für eine bestimmte Lösung für eine Schwachstelle an, um das neueste bereitzustellende Update oder ein früheres, fokussierteres, effizienteres Update zu finden.
- Zeigen Sie Listen von Lösungen an, die nach verschiedenen Merkmalen sortiert sind.
  - Alle: Lösungen sortiert nach Veröffentlichungsdatum und Nummer.
  - MSRC: Höchste Ersetzung: Lösungen mit aktiven, nicht zurückgestellten angreifbaren Elementen. Sortiert nach **Höchste Ersatzleistung** , **Veröffentlichungsdatum** , Und **Nummer** .
  - Mit angreifbaren Elementen: Lösungen mit aktiven, nicht zurückgestellten angreifbaren Elementen. Sortiert nach **Höchste Ersatzleistung** Oder **Bevorzugt** , **Risikopunktzahl** , Und **Nummer** . Wenn bereitgestellt, bieten die obersten Einträge in der Liste die größte Risikominderung für die Assets in Ihrer Umgebung.

Risikopunktzahl und Risikobewertung des Lösungsdatensatzes

Hinweis:
Der Lösungsdatensatz **Risikopunktzahl** Und **Risikobewertung** Unterscheiden sich von den Feldern, die für Schwachstellen, angreifbare Elemente und Korrekturaufgaben verwendet werden.

Der Lösungsdatensatz **Risikopunktzahl** Ist eine gewichtete Berechnung basierend auf dem angreifbaren Element **Risikopunktzahl** Und eine Anzahl der aktiven angreifbaren Elemente mit dieser Lösung als ihre **Potenzielle Lösung** . Die Lösung **Risikopunktzahl** Bietet eine Schätzung der Risikoreduzierung, die die Lösung voraussichtlich erreichen wird.

Der Lösungsdatensatz **Risikopunktzahl** Wird wie folgt berechnet:

- Zunächst werden 85 % des höchsten oder Maximums verwendet **Risikopunktzahl** Eines aktiven angreifbaren Elements mit dieser potenziellen Lösung.
- Der Lösungsdatensatz **Risikopunktzahl** Dann tabellariert die Gesamtzahl der angreifbaren Elemente mit dieser potenziellen Lösung. Für jeden Bereich der Anzahl der angreifbaren Elemente werden einige Punkte hinzugefügt und insgesamt erreicht.
  - 0–09 angreifbare Elemente fügen keine Punkte hinzu
  - 10–99 angreifbare Elemente fügen 5 Punkte hinzu
  - 100–999 angreifbare Elemente fügen 10 Punkte hinzu
  - 1000 und mehr angreifbare Elemente fügen 15 Punkte hinzu

  Zum Beispiel für ein angreifbares Element **Risikopunktzahl** Von 80, der Lösungsdatensatz **Risikopunktzahl** Würde bei 68 beginnen. Wenn bei dieser potenziellen Lösung insgesamt 200 aktive angreifbare Elemente vorhanden sind, dann die endgültige Lösung **Risikopunktzahl** Wäre 78.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Lösungsdatensatz **Risikobewertung** Trennt den Lösungsdatensatz **Risikopunktzahl** In Bereiche von kritisch bis keine. Lösung **Risikobewertung** Bewertet die Risikominderung für die angreifbaren Elemente, die diese Lösung korrigiert.

Bis zu VR v16.1 trennten Risikobewertungen die resultierende Lösung **Risikopunktzahl** In die folgenden Bereiche:

- 1 – Kritisch (Lösung Über 90 **Risikopunktzahl**)
- 2 – hoch (Lösungsdatensatz 70-89 **Risikopunktzahl**)
- 3 – Mittel (Lösungsdatensatz 30-69 **Risikopunktzahl**)
- 4 – Niedrig (Lösungsdatensatz 1-29 **Risikopunktzahl**)
- 5 – keine (0 Lösungsdatensatz **Risikopunktzahl**)

Ab VR v16.1 trennen Risikobewertungen die resultierende Lösung **Risikopunktzahl** In die folgenden Bereiche für das Lösungsmanagement:

- 1 – Kritisch (Lösung Über 90 **Risikopunktzahl**)
- 2 – hoch (Lösungsdatensatz 70-89 **Risikopunktzahl**)
- 3 – Mittel (Lösungsdatensatz 40-69 **Risikopunktzahl**)
- 4 – Niedrig (Lösungsdatensatz 1-39 **Risikopunktzahl**)
- 5 – keine (0 Lösungsdatensatz **Risikopunktzahl**)

Anwendungsfälle

Zeigen Sie den Fortschritt der Statusbereitstellung eines aktuellen Patch-Zyklus mithilfe des Moduls mit dem höchsten Ersatz, sortiert nach Datum, an.

Zeigen Sie Lösungen mit dem höchsten Wert mithilfe des Moduls mit angreifbaren Elementen an, sortiert nach Risikopunktzahl.

Lösungslisten kommunizieren wichtige Lösungsdetails, Risikopunktzahlen und Bereitstellungsmetriken. Verwenden **Risikopunktzahl** Und aktive VI-Anzahlen für die Priorisierung. Sehen Sie, welche Lösungen im aktuellen Patch-Zyklus nicht vorankommen, möglicherweise ein Hinweis auf eine verpasste Bereitstellungsvoraussetzung.

Hinweis:
Hinzufügen **%VIS korrigiert(percent_nd_pref_VIS_Remediated)** Von **Personalisieren Sie Listenspalten** Menü für den Korrekturfortschritt im Formular „Schwachstellenlösungen“.

Integration der Microsoft Security Response Center-Lösung

Überprüfen und implementieren Sie vorgeschlagene Korrekturlösungen, die von bereitgestellt werden Integration der Microsoft Security Response Center-Lösung.

Integration der Microsoft Security Response Center-Lösung Ist in enthalten Vulnerability Solution Management Funktion von Vulnerability Response, Verfügbar durch separates Abonnement. Siehe Vulnerability Solution Management Um weitere Informationen dazu zu erhalten Vulnerability Response Umfasst Lösungen.

Microsoft Security Response Center Untersucht Berichte über Sicherheitsschwachstellen, die sich auf Microsoft-Produkte und -Services auswirken, und stellt Lösungsinformationen bereit, um Sicherheitsrisiken zu verwalten. Lösungen sind bekannte Korrekturen, die in importiert wurden Integration der Microsoft Security Response Center-Lösung Von Microsoft Security Response Center Produkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Integration der Microsoft Security Response Center-Lösung Enthält Einstiegspunkte zu Microsoft Security Response Center Produkt, wird als geplante Aufgaben aufgerufen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird. Geplante Aufgaben werden automatisch und in der angegebenen Reihenfolge ausgeführt. Sie können einzelne geplante Aufgaben auch manuell ausführen.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Verfügbare Versionen

Für die aktuelle Version von Vulnerability Solution Management Und Microsoft Security Response Center Lösungen überprüfen Sie, ob Sie über die aktuelle Version von verfügen Vulnerability Response Installiert.

Weitere Informationen zum Installieren und Konfigurieren von Vulnerability Solution Management Und Lösungsintegrationen siehe Anwendung Solution Management for Vulnerability Response installieren Und Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management Mit dem Setup-Assistenten.

Release-Version von Vulnerability Response	Version von Vulnerability Solution Management	Release-Hinweise
Vulnerability Response V15.0	V10.3	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Rollen

Integration der Microsoft Security Response Center-Lösung Aufgaben umfassen die folgenden Rollen.

- sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet): Kann Datensätze lesen, schreiben und löschen.
- sn_vul.Vulnerability_write: Kann Datensätze lesen und schreiben.
- sn_vul.Vulnerability.read: Kann Datensätze lesen.
- sn_vul.Remediation_owner: Kann interne Notizen zu Datensätzen lesen und schreiben, die der Korrekturfachgruppe oder Einzelperson zugewiesen sind. (Enthalten in der Rolle itil.)

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration der Microsoft Security Response Center-Lösung

Um anzuzeigen Integration der Microsoft Security Response Center-Lösung, Navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**an.

Die folgende Integration ist im Basissystem enthalten.

Integration der Microsoft Security Response Center-Lösung

Integration	Beschreibung
Integration der Microsoft Security Response Center-Lösung	Ruft Lösungen und die Zuordnung der National Vulnerability Database (NVD) ab, um Lösungen Schwachstellen, angreifbaren Elementen und Korrekturaufgaben zuzuordnen. **Hinweis:** Die Integration der Microsoft Security Response Center-Lösung Stellt keine Lösungen vor 2016 bereit.

Lösungen

Informationen zum Anzeigen importierter Lösungen in einer Liste finden Sie unter Zeigen Sie eine Lösung an.

Red Hat Solution Integration

Sie können vorgeschlagene Korrekturlösungen überprüfen und implementieren, die von bereitgestellt werden Red Hat Solution Integration In Vulnerability Response Anwendung.

Red Hat Solution Integration Ist in enthalten Vulnerability Solution Management Funktion von Vulnerability Response, Verfügbar durch separates Abonnement. Siehe Vulnerability Solution Management Um weitere Informationen dazu zu erhalten Vulnerability Response Umfasst Lösungen.

Red Hat Solution Integration Untersucht Berichte über Sicherheitsschwachstellen, die sich auf diese auswirken Red Hat Produkte und Services und stellt Lösungsinformationen bereit, um Sicherheitsrisiken zu verwalten. Lösungen, die als Korrekturen bezeichnet werden, werden in importiert Red Hat Solution Integration Von Red Hat.

Ab Version 21,0 von Vulnerability Response, Red HatÜberträgt Nutzlasten im CSAF-Format (Common Security Advisory Framework) anstelle des CVRF-Formats (Common Vulnerability Reporting Framework). CSAF, ein XML-basierter Standard, unterscheidet sich sowohl in Struktur als auch im Format von CVRF. Um diese Änderung zu berücksichtigen, wurde ein neuer CSAF-Parser entwickelt. Dieser Parser interpretiert das CSAF-Format und extrahiert die erforderlichen Felder, um die Tabellen entsprechend auszufüllen.

Hinweis:
Standardmäßig erhalten Sie die Nutzlast im CSAF-Format.

Die folgenden Extrakte zeigen das Integrationsskript zum Analysieren der von empfangenen Nutzlast Red Hat In den Formaten CSAF und CVRF.

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is provided in the event

* The function should return the newly constructed script. */
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
(function(integrationProcessGr){

// Add any logic here to construct your integration script as necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF payload is expected
return new sn_vul.RedHatSolutionIntegration(true);
})(integrationProcessGr);
```

```
/** « This function serves to construct the integration script.

* The integration process record (integrationProcessGr) is provided in the event

* The function should return the newly constructed script. */
(function(integrationProcessGr){

// Add any logic here to construct your integration script as necessary.

// Pass true if CSAF payload is expected. Pass false if CVRF payload is expected
return new sn_vul.RedHatSolutionIntegration(false);
})(integrationProcessGr);
```

Red Hat Solution Integration Enthält Einstiegspunkte zum Red hat-Produkt, die als geplante Aufgabe aufgerufen werden. Die geplante Aufgabe vereinfacht den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird. Wird automatisch ausgeführt. Sie können die geplante Aufgabe auch manuell ausführen.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Verfügbare Versionen

Für die aktuelle Version von Vulnerability Solution Management Und Red Hat Lösungen überprüfen Sie, ob Sie über die aktuelle Version von verfügen Vulnerability Response Installiert.

Weitere Informationen zum Installieren und Konfigurieren von Vulnerability Solution Management Und Lösungsintegrationen siehe Anwendung Solution Management for Vulnerability Response installieren Und Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management Mit dem Setup-Assistenten.

Release-Version von Vulnerability Response	Version von Vulnerability Solution Management	Release-Hinweise
Vulnerability Response V15.0	V10.3	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Rollen

Red Hat Solution Integration Aufgaben umfassen die folgende Rolle:
sn_vul.configure_rhsa_Integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Red Hat Solution Integration

Um anzuzeigen Red Hat Solution Integration, Navigieren Sie zu **Vulnerability Response** > **Administration** > **Integrationen**an.

Die folgende Integration ist im Basissystem enthalten.

Red hat-Integration

Integration	Beschreibung
Red Hat Solution Integration	Ruft Lösungen und die Zuordnung der National Vulnerability Database (NVD) ab, um Lösungen Schwachstellen, angreifbaren Elementen und Korrekturaufgaben zuzuordnen.

Lösungen

Informationen zum Anzeigen importierter Lösungen in einer Liste finden Sie unter Zeigen Sie eine Lösung an.

Rapid7 Lösungsmanagement

Lösungen sind bekannte Korrekturen, die in importiert werden Rapid7 Vulnerability-Integration Entweder von Rapid7 Data Warehouse Oder Rapid7 InsightVM. Rapid7 Data Warehouse importiert sowohl Lösungen als auch Ersatzlösungen. Mit Rapid7 InsightVM, Erhalten Sie Lösungen als Teil der Rapid7-Integration angreifbarer Elemente – API.

Ab Version 21,0 von Vulnerability Response, Es gibt eine Änderung in der Art und Weise, wie Lösungen von erstellt werden Rapid7 InsightVM. Anstatt sich auf zu verlassen **Solution_Summary** , **Solution_fix** , Oder **Solution_type** Felder, Rapid7 InsightVM Erstellt jetzt Lösungen mithilfe der vom Scanner bereitgestellten Solution_ID. Dies bedeutet, dass auch wenn diese Felder leer sind, eine Lösung erstellt wird, solange eine Lösungs-ID verfügbar ist.

Um importierte Lösungen als Liste anzuzeigen, navigieren Sie zu **Rapid7** > **Lösungen**an.

Wenn Vulnerability Solution Management Das Plugin wird aktiviert, dann die neueste Version von Rapid7 Vulnerability-Integration Bietet die folgenden wichtigen Funktionen für Lösungen:

- Die Rapid7 Lösungsmanagement wird in Schwachstellenlösungsmanagement verschoben.
- Eine neue Integration von Rapid7 Predictional Solution Management für das Data Warehouse wird eingeführt. Die Integration ruft die erforderliche Lösung aus dem ab Rapid7 Data Warehouse.
- Die zugehörige Liste von Rapid7 (Lösung) in Drittparteieinträgen (TPE) ist ausgeblendet.
- Die zuvor importierten Daten können im neuen Datenmodell angezeigt werden. Rapid7-Lösungen, Lösungsersatz und Schwachstellenlösungszuordnung werden erneut

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

importiert und die **Importieren seit** Feld ist auf leer festgelegt. Das Feld wird im Lösungsmanagement ausgefüllt.

- Die Erkennungen werden aktualisiert, um das Lösungsfeld auszufüllen. Erkennungen zeigen die Lösungen an, da sie Teil von Vulnerability Solution Management sind.
- Rapid7 Erhält beim Festlegen der bevorzugten Lösung in TPE für eine höhere Präferenz gegenüber anderen Lösungen Rapid7 Data Warehouse.
- Die -Lösungen werden aus Erkennungen für zu angreifbaren Elementen (VI) zusammengefasst Rapid7 InsightVM.

Hinweis:
Wenn Sie den nicht aktiviert haben Vulnerability Solution Management Plugin, dann funktioniert die Anwendung unverändert.

Vulnerability Solution Management

Wenn Sie aktiviert haben Vulnerability Solution Management-Plugin, dann Rapid7 Lösungen für beide Rapid7 Data Warehouse und Rapid7 InsightVM Wird in der Tabelle „Schwachstellenlösungen“ [sn_vul_Solution] ausgefüllt. Wenn Sie jedoch nicht aktiviert haben Vulnerability Solution Management Plugin, dann Rapid7 Vulnerability-Integration Funktioniert unverändert und importiert die Lösungen in die anwenderdefinierte Tabelle [sn_vul_r7_Solution].

Um die Tabelle „Schwachstellenlösungen“ anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Schwachstellenlösungen** Wo Sie die Lösungen verschiedener Lieferanten anzeigen und vergleichen können. Um importierte Lösungen in der anwenderdefinierten Tabelle anzuzeigen, navigieren Sie zu **Alle** > **Rapid7 Vulnerability-Integration** > **Lösungen**an.

Hinweis:
Nach Quelle gruppieren, um Lösungen basierend auf Lieferanten anzuzeigen.

Rapid7 – erforderliche Integration von Solution Management

Wenn Sie aktiviert haben Vulnerability Solution Management Plugin, wird ein Korrekturskript ausgeführt und ändert die Reihenfolge der Integrationen. Die neue erforderliche Rapid7-Lösungsintegration für Rapid7 Data Warehouse ordnet die Lösungen den erforderlichen Lösungen zu. Die Integrationen werden in der folgenden Reihenfolge ausgeführt:

1. Rapid7 Lösungsintegration
2. Rapid7 Erforderliche Lösung
3. Rapid7 Ersetzt Die Lösungsintegration
4. Rapid7 Integration Der Schwachstellenlösungszuordnung
5. Rapid7 VI-Lösungsintegration (ab v19.0 von Vulnerability Response)

Hinweis:
Wenn Sie die Integrationen manuell ausführen, beginnen Sie mit Rapid7 Lösungsintegration#. Ändern Sie die Next Integration Chain in nicht Rapid7 Integration. Die Sequenz wird in der Spalte nächste Integration definiert.

Zugehörige Liste „Rapid7 (Lösungen)“ in TPE

Wenn Sie aktiviert haben Vulnerability Solution Management-Plugin, dann können Sie Folgendes tun:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können die TPEs anzeigen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Drittpartei**an.
- Sie können die zugehörige Liste „Lösungen“ (Rapid7) nicht sehen, die in den älteren Releases verfügbar war.
- Sie können die zugehörigen Rapid7-Lösungen in der zugehörigen Liste Lösungen zusammen mit den Lösungen aus anderen Quellen anzeigen, z. B. RedHat, Microsoft (MSRC) usw.

Wenn Sie den nicht aktiviert haben Vulnerability Solution Management Plugin, dann geschieht Folgendes:

- Die Funktionalität „zugehörige Listen“ bleibt unverändert.
- Sie können die zugehörige Liste Lösungen (Rapid7) anzeigen.
- Die zugehörige Liste „Lösungen“ ist ausgeblendet.

Bevorzugte Lösung für TPE und VIS

Rapid7 Ruft die Lösung aus dem Data Warehouse auf der Ebene des Drittpartei-Eintrags (TPE) und für ab Rapid7 InsightVM Auf Erkennungsebene.

Für ein Rapid7 Data Warehouse wird die Lösung auf folgende Weise verwaltet:

- Die bevorzugte Lösung wird auf der TPE basierend auf der Schwachstellen- und Lösungszuordnung festgelegt.
- Wenn die Schwachstelle von Rapid7 Hat eine einzige höchste Ersatzlösung von Rapid7, Dann wird sie unabhängig von anderen Lösungen von Lieferanten, die an diese Schwachstelle angehängt sind, als bevorzugte Lösung festgelegt.
- In allen anderen Fällen bleibt der Flow der bevorzugten Lösung gleich. #Weitere Informationen zum Standardverhalten bevorzugter Lösungen finden Sie unter Vulnerability Solution Management.

Für Rapid7 InsightVM, Die Lösung wird wie folgt verwaltet:

- Die bevorzugte Lösung wird von Erkennungen zu#VIS zusammengefasst.
- Wenn es eine einzelne Erkennung und Lösung von gibt Rapid7, Wird die Lösung#zu VI zusammengefasst
- Wenn mehrere Erkennungen vorhanden sind und alle dieselbe Lösung von haben Rapid7, Wird die Lösung zu VI zusammengefasst
- Wenn mehrere Erkennungen mehrere Lösungen von haben Rapid7, Wird die neueste Lösung im VI zusammengefasst

Ab v19.0 von Vulnerability Response, Die bevorzugte Lösung, die von Rapid7 Data Warehouse generiert wird, wird von direkt in angreifbare Elemente ausgefüllt Rapid7 Umgehung des Bedarfs für Vulnerability Solution Management. Diese Änderung stellt sicher, dass jegliche Unsicherheit hinsichtlich potenzieller Lösungen für diese angreifbaren Elemente beseitigt wird.

Um diese direkte Belegung über zu erreichen Rapid7, Die folgenden Schritte werden ausgeführt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Eine neue Integration, Rapid7 VI-Lösungsintegration, wird eingerichtet und in den vorhandenen Rapid7 Vulnerability Integration-Workflow integriert.
- Eine neue Tabelle [sn_vul_r7_rapid7_VI_Solution_Import] wird erstellt.
- Eine neue Transformationszuordnung Rapid7 VI-Lösungstransformation wird erstellt.
- Die Skripteinbindung Rapid7AssetsImportProcessor wird geändert, um die Verarbeitung von Lösungen auszuschließen, die von Rapid7 in generiert wurden Vulnerability Solution Management.

Bei der Ausführung der Rapid7 VI-Lösungsintegration werden die unverarbeiteten Daten von abgerufen Rapid7 Wird in der neu erstellten Tabelle gespeichert. Anschließend wird die Rapid7 VI-Lösungstransformation ausgelöst, die diese Daten verarbeitet und die bevorzugte Lösung direkt in die Tabelle „Angreifbares Element“ ausfüllt.

Hinweis:
Die Rapid7 VI-Lösungsintegration füllt die bevorzugte Lösung ausschließlich aus, wenn die Vulnerability Solution Management Plugin wurde installiert.

Ab v22.0 von Vulnerability Response, Die Lösungen von Rapid7 Sind bei der Ausführung der geplanten Aufgabe nicht mehr in der Warteschlange *`Process Vulnerability Solutions Metrics Queue`*. Diese geplante Aufgabe umfasst das Rollup von Lösungen von NVD-Einträgen zu Drittparteieinträgen, die Auffüllung bevorzugter Lösungen zu Schwachstellen und die Aktualisierung der Korrekturstatusmetriken für die Lösungen. In den folgenden Szenarien müssen nur die Korrekturstatusmetriken aktualisiert werden:

- Wenn sich die bevorzugte Lösung für die Schwachstellen ändert
- Wenn die Vits erstellt oder gelöscht werden
- Wenn ein VIT-Import abgeschlossen ist

Obwohl die Lösungen in der Warteschlange stehen, um nur die Korrekturstatusmetriken zu aktualisieren, versuchen sie dennoch, Lösungen von NVD-Einträgen zu Drittparteieinträgen zusammenzufassen und die bevorzugten Lösungen auszufüllen. Um diesen Prozess zu optimieren, finden Sie in der Tabelle „Schwachstellenlösung“ die Spalte **Status aktualisieren** Wird eingeführt. Wenn die Korrekturstatusmetriken für Lösungen aktualisiert werden müssen, ohne dass ein Rollup von Lösungen von NVD-Einträgen zu Drittpartei-Einträgen oder der Auffüllung bevorzugter Lösungen erforderlich ist, werden sie nicht mehr in die Warteschlange gestellt. Stattdessen wird **Status aktualisieren** Spalte wird direkt als „wahr“ aktualisiert. Dieser Ansatz ermöglicht die Verarbeitung von Fällen, in denen nur die Korrekturstatusmetriken aktualisiert werden müssen, was zu Zeit- und Ressourceneinsparungen führt. Sobald die Verarbeitung der Lösungen in der Warteschlange abgeschlossen ist, werden in der geplanten Aufgabe Lösungen identifiziert, die mit dem Aktualisierungsstatus „wahr“ gekennzeichnet sind. Anschließend werden sie durch diese Lösungen iteriert, berechnet die Anzahl und aktualisiert die Korrekturstatusmetriken entsprechend. Dieser Schritt spielt eine wichtige Rolle bei der Verbesserung der Leistung der geplanten Aufgabe, da die Anzahl der Lösungen, die in die Warteschlange gestellt werden müssen, reduziert wird.

Lösungsersatzkette, die aus dem Rapid7 Data Warehouse für eine Schwachstelle importiert wurde

Sie können die Ersatzlösungen für eine Lösung anzeigen, indem Sie eine Schwachstellenlösung auswählen und die zugehörige Liste Ersatzlösungen auswählen. Sie können die vorangehenden Lösungen anzeigen, indem Sie die zugehörige Liste vorherige

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lösungen auswählen. Wenn Sie eine Lösung an den TPE anhängen, wird die Ersatzlösung dieser Lösung an diesen TPE angehängt.

Ändern Sie die maximale Tiefe der Lösungsaustauschkette in einem Diagramm nach Systemeigenschaft

Die in empfangene Lösungsersetzungskette Rapid7 Das Datenmodell ist zu lang, um das Diagramm während der Auffüllung der bevorzugten Lösung zu erstellen. Um die Tiefe der Kette einzuschränken, eine Systemeigenschaft mit dem Namen *`sn_vul.max_recursion_depth`*Mit dem Wert 500 wird erstellt. Wenn die Kettentiefe mehr als 500 beträgt, wird der Rest der Kette ignoriert. Um die maximale Tiefe der Kette zu ändern, navigieren Sie zur Tabelle [sys_properties], und ändern Sie den Wert der Eigenschaft.

Upgrade von wird durchgeführt Rapid7 Anwendung

Wenn Sie ein Upgrade durchführen Rapid7 Vulnerability-Integration Plugin und haben noch nicht aktiviert Vulnerability Solution Management Plugin, dann funktioniert die Anwendung unverändert.

Ob Sie aktivieren Vulnerability Solution Management Plugin vor oder nach dem Upgrade von Rapid7 Anwendung, die **Importieren seit** Feld bleibt für die folgenden Integrationen leer:

- Rapid7#– Integration Der Ersatzlösung
- Integration Der Rapid7-Schwachstellenlösungszuordnung
- Rapid7-Lösungsintegration

Hinweis:
Ab der nächsten Integrationsausführung werden die Daten in die Tabelle „Schwachstellenlösung“ gefüllt.

Für Rapid7 InsightVM, Die Daten werden auf Erkennungsebene empfangen. Wenn Rapid7 InsightVM Die Integration wird ausgeführt. Die Lösungen werden in die Tabelle „Schwachstellenlösung“ importiert.

Generisches Framework zum Erfassen von Daten von einem beliebigen Lösungsanbieter

Ein generisches Framework für die Integration von Solution Intelligence ist verfügbar, um die Erfassung von Daten in verschiedenen Dateiformaten von Lösungsanbietern zu unterstützen. Diese Formate beschleunigen den Informationsaustausch und die Verarbeitung und erleichtern die Freigabe wichtiger sicherheitsbezogener Informationen in einem standardisierten Berichtsformat.

Die unterstützten Dateiformate sind:

Common Vulnerability Reporting Framework (CVRF)

Das Common Vulnerability Reporting Framework (CVRF) ist eine XML-basierte Sprache. Wichtige Lieferanten wie Oracle, Red Hat, Cisco, Und Microsoft Unterstützt das CVRF-Format.

Common Security Advisory Framework (CSAF)

Das Common Security Advisory Framework (CSAF) ist ein Open Source-Standard, der JSON-basierte strukturierte, maschinenlesbare Sicherheitsempfehlungen bereitstellt. Wichtige Lieferanten wie Siemens, Red Hat, Hitachi und Schneider unterstützen das CSAF-Format.

Das von CVRF oder CSAF unterstützte Lösungsmanagement umfasst die folgenden wichtigen Funktionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfiguration über Setup-Assistent
- Unterstützung des Imports von CVRF- oder CSAF-Daten über Dateiimport
- Unterstützung des Imports von CVRF- oder CSAF-Daten über CVRF Oder CSAF URL
- Unterstützung des Imports von CVRF- oder CSAF-Daten über Empfehlungen
- Zuordnung von Lösungen zu zugehörigen Schwachstellen

Das Plugin „Vulnerability Response“ aktualisiert die Metrikstatus der erstellten Lösung.

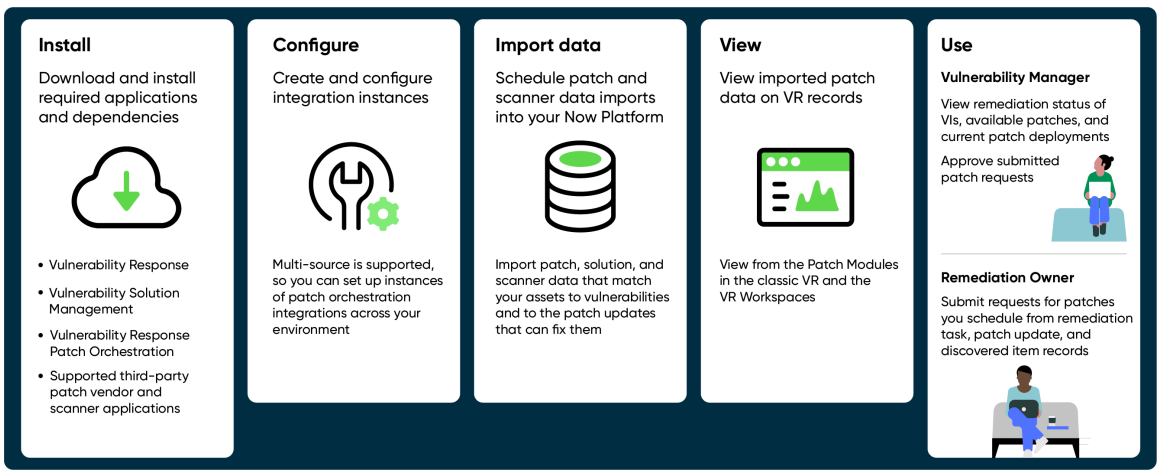
Weitere Informationen zum Konfigurieren der Lösungsanbieter finden Sie unter Konfigurieren Sie Anbieter von Schwachstellen-Lösungen.

Patch-Orchestration mit Vulnerability Response

Mit Patch Orchestration mit können Sie Patches und Patch-Bereitstellungen für kritische Schwachstellen für große Gruppen Ihrer Assets verwalten Vulnerability Response. Vulnerability Response Patch-Orchestration und die Patch-Orchestration-Integrationen sind im verfügbar ServiceNow® Store.

Verstehen der Patch-Orchestration mit Vulnerability Response

Patch-Orchestration mit Vulnerability Response Verwendet Daten aus geplanten Importen von Drittanbieter-Lösungsintegrationen, Patch-Lieferanten und Schwachstellen-Scannern. Diese Daten werden in korreliert Vulnerability Response Anwendung. Diese Datenorganisation ermöglicht Ihnen, die Schritte des Korrekturzyklus für Schwachstellen abzuschließen. Beginnen Sie mit der Identifizierung von Schwachstellen, wenden Sie dann Patches und Updates an, und schließen Sie schließlich angreifbare Elemente mithilfe von Scannerdaten von Drittanbietern, die alle aus Ihrem stammen ServiceNow AI Platform® Instanz.



Patch-Orchestration mit Vulnerability Response Wird sowohl in der klassischen Umgebung als auch in unterstützt Vulnerability Response Arbeitsbereiche.

Informationen zur Patch-Orchestration in den Arbeitsbereichen finden Sie unter Patch-Orchestration mit Vulnerability Response Arbeitsbereiche.

Mit Patch-Orchestration in Vulnerability Response, Schwachstellenmanager und Analysten sowie IT-Korrekturspezialisten können die folgenden Korrekturaufgaben ausführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Weitere Kontextinformationen und Informationen zu den Arten von Patches und Lieferanten, aus denen ihre Lösungen bestehen (Patches).
- Zeigen Sie Schwachstellen- und Lösungsdaten sowie den Fortschritt der Schwachstellenkorrektur aus Datensätzen in an, und überwachen Sie sie Vulnerability Response Arbeitsbereiche oder in der klassischen Umgebung.
- Stellen Sie Patches bereit, die von Drittanbieterlösungen für unterstützt werden Windows, CentOS, macOS, Oracle, Und andere Assets in regelmäßigen, geplanten Intervallen. Sie können Patches außerhalb der Geschäftszeiten planen, um Konflikte mit den Arbeitnehmern zu vermeiden.
- Identifizieren Sie mithilfe importierter Erkennungsdaten, die von Drittanbieterscannern bereitgestellt werden, Assets, die Schwachstellen aufweisen und nicht gepatcht wurden oder nicht erfolgreich durch geplante Patches aktualisiert wurden.
- Initiieren und planen Sie verfügbare Patches für Assets, die Updates aus Patch-Update, Korrekturaufgabe und erkannten Elementdatensätzen in erfordern Vulnerability Response Anwendung.
- Überwachen Sie Patch-Bereitstellungen mit einem optionalen Genehmigungsprozess für Patch-Anforderungen, die von Ihren Korrekturspezialisten übermittelt werden.

Wichtige Begriffe

Konfigurationselement bzw. Configuration Item (CI)

CIs sind die vorhandenen Assets, die in Ihrer#Configuration Management Database (CMDB) aufgeführt sind.

Angreifbares Element (VI)

Eine importierte Schwachstelle, die einem vorhandenen Asset in Ihrer CMDB entspricht. Angreifbare Elemente (Vits) werden gemäß bestimmten Kriterien, die Korrekturaktionen für VIS angeben, in Korrekturaufgaben oder Listen gruppiert.

Instanz

Bezieht sich auf einen eindeutigen Account einer Lösungsanbieteranwendung. Beispielsweise kann jeder Anwenderaccount eine Instanz in der HCL BigFix-Anwendung sein. Dieser Begriff bezieht sich auch auf eine eindeutige, sichere Webadresse für einen ServiceNow AI Platform® Instanz.

Lösung

Im Kontext dieser Integration gibt es zwei Arten von Lösungen, potenziell und bevorzugt. Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben könnte. Schwachstellen haben oft viele potenzielle Lösungen. #Eine bevorzugte Lösung entspricht der effektivsten Lösung für eine bestimmte erkannte Schwachstelle.

Patch

Software-Updates, die Schwachstellen beheben. Patch-Lieferanten verwenden ihre eigenen Namen für Patches. In der Anwendung HCL BigFix werden Patches beispielsweise Fixlets genannt.

Bevorzugter Patch

Bevorzugte Patches sind Software-Updates, die bestimmte Schwachstellen beheben sollen. Patches werden nach der Bereitstellung den angreifbaren Elementen zugeordnet, die sich auf bestimmte Schwachstellen beziehen, und sie werden behoben.

Bereitstellung

Die Bereitstellung für die Zwecke dieser Integration bezieht sich darauf, wenn Sie einen Patch auf einen Computer anwenden, initiieren oder planen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bereitstellung in ServiceNow AI Platform Kann auch auf eine Integration verweisen, die mehrere Quellen unterstützt. Eine einzelne Integration wird als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie mehrere Bereitstellungen eines Drittanbieterscanners oder einer Integration eines Lösungsanbieters in Ihrer Umgebung haben.

Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch-Orchestration-Integration erforderlich sind

- Die Vulnerability Response Anwendung und die Abhängigkeits-Plugins, Security Support Common und Security Support Orchestration.
- Vulnerability Solution Management.
- Vulnerability Response Patch-Orchestration-Anwendung, die in verfügbar ist ServiceNow® Store.
- Eine unterstützte Drittanbieter-Patch-Lieferantenanwendung, z. B. Integration der Patch-Orchestration für Vulnerability Response mit HCL BigFix Oder Integration der Patch-Orchestration von Vulnerability Response mit Microsoft SCCM .
- Unterstützte Scanner-Integrationen von Drittanbietern mit Vulnerability Response.

Erforderliche Rollen

Anwender benötigen Rollen, die für die Patch-Orchestration-Integration spezifisch sind, die Sie verwenden, um Daten anzuzeigen und Patches aus der zu planen Vulnerability Response Anwendung. Weitere Informationen finden Sie in den Konfigurationsinformationen für die von Ihnen verwendeten unterstützten Integrationen.

- Verständnis der Integration der HCL BigFix-Patch-Orchestration mit Vulnerability Response Und Integration der Patch-Orchestration von Vulnerability Response mit Microsoft SCCM .
- In Vulnerability Response Arbeitsbereiche und die klassische Umgebung, die Rolle „sn_vul_Patch_orch.read_Patch“, mit der Anwender Daten anzeigen, aber nicht bearbeiten können, werden mit den Rollen „sn_vul.Remediation_owner“ und „sn_vuln.Vulnerability_Analyst“ geerbt.

  Die Rollen, die Sie zuweisen müssen und die zum Konfigurieren der Verbindungen zu den Patch-Lieferanten und Zeitplanpatches erforderlich sind, sind integrationsspezifisch. Siehe Konfigurieren Sie Vulnerability Response Patch-Orchestration-Integration mit HCL BigFix Und Konfigurieren Sie das Vulnerability Response Patch Orchestration mit MS SCCM, um weitere Informationen zu erhalten .

Es gibt einen Übermittlungs- und Genehmigungsprozess für Patch-Anforderungen, die in den Anwendungen enthalten sind. Standardmäßig ist eine Systemeigenschaft aktiviert [**sn_vul_Patch_orch.Patch_Approval_required**] In der Anwendung Vulnerability Response Patch Orchestration in Ihrem ServiceNow AI Platform Instanz.

Diese Systemeigenschaft ist aktiviert, sodass Patch-Bereitstellungen bei der Planung zur Überprüfung und Genehmigung an Anwender übermittelt werden, die der Genehmigungsgruppe „Patch-Update“ der Ebene 1 zugewiesen sind. Wenn Anwender mit der Rolle „sn_vul_Patch_orch.configure_Patch“ Patches ohne Genehmigung planen sollen, können Sie [. Deaktivieren **sn_vul_Patch_orch.Patch_Approval_required**] Eigenschaft. Möglicherweise möchten Sie Genehmigungen aktivieren lassen, damit geplante Patches nicht mit den normalen Arbeitszeiten in Konflikt stehen. Wenn Sie die Systemeigenschaft „Genehmigung“ deaktivieren, kann jeder Anwender mit der Rolle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„sn_vul_Patch_orch.configure_Patch“ Patches ohne Überprüfung und Genehmigung planen und bereitstellen.

Weitere Informationen zum Deaktivieren dieser Systemeigenschaft finden Sie im Konfigurationsthema für Ihre unterstützte Integration.

- Konfigurieren Sie Vulnerability Response Patch-Orchestration-Integration mit HCL BigFix.
- Konfigurieren Sie die Patch-Orchestration für Vulnerability Response mit Microsoft SCCM-Integration.

Planen Sie Patches von Vulnerability Response Datensätze

Korrekturspezialisten können Patch-Updates planen, um angreifbare Elemente zu lösen und den Korrekturfortschritt zu überwachen – alles aus Datensätzen in Vulnerability Response Anwendung.

Sie können Patches aus den folgenden Datensätzen planen:

- Patch-Update
- Nachbesserungsaufgabe
- Erkanntes Element

Datensätze, in denen ein Rollup aktiver VI durchgeführt wird, werden gezählt Vulnerability Response

Um potenzielle Leistungsprobleme beim Rollup aller Patches für alle Schwachstellen zu vermeiden, ändert die geplante Aufgabe, die Änderungen aufgreift, nur die Anzahl der aktiven VI. Diese Anzahländerungen und zugehörigen Daten werden in den folgenden Datensätzen in zusammengefasst Vulnerability Response Anwendung:

- VIT (angreifbares Element)
- RT (Korrekturaufgabe)
- Schwachstellenlösung
- Patch-Update

Weitere Informationen zum Anzeigen von Patch-Daten und Patch-Daten-Rollups zu Datensätzen und zum Anzeigen von Patches ohne Lösungen finden Sie in den folgenden Themen.

- Patch-Daten- und Status-Rollup für Patch-Orchestration in Vulnerability Response.
- Patch-Daten anzeigen und Patches planen in Vulnerability Response.
- Zeigen Sie Patches ohne Lösungen in an Vulnerability Response.

Massenbearbeitung angreifbarer Elemente mit Patches

Sie können angreifbare Elemente in der klassischen Umgebung, die Patches aus der klassischen Umgebung enthalten, massenbearbeiten. Weitere Informationen zur Funktionsweise der Massenbearbeitung finden Sie unter Bearbeiten Sie angreifbare Elemente in Massenarbeit Vulnerability Response. Die bevorzugten Patches für alle VIS, die für die Massenbearbeitung ausgewählt wurden. Diese Option zum Bearbeiten funktioniert nur, wenn allen ausgewählten VIS bevorzugte Patches zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbesserungen Des Patch-Management-Datenmodells

Das Plugin „Patch-Management-Datenmodell“ – ein eigenständiges, kostenloses Plugin, das das Datenmodell kapselt, das derzeit in der VR Patch Orchestration-Anwendung verwendet wird. Dies umfasst Schlüsseltabellen wie Sammlung, Patch-Update, Patch-Bereitstellung und andere.

Dieses Plugin kann von Patch-Management-Tools verwendet werden, um die Patch-Management-Daten zu erfassen, die von Anwendungen wie ITSM, Vulnerability Response usw. für die vorhandenen Workflows verwendet werden sollen.

Wichtige Erweiterungen:

- Tabellen wie Sammlungsgerät, Patch-Update, Patch-Bereitstellungstabellen im vorhandenen Patch Orchestration-Plugin werden in das neue Datenmodell-Plugin verschoben.
- Die Daten aus der alten Tabelle werden in die neuen Tabellen für die vorhandene VR-Patch-Orchestration-Funktion migriert.

Ausnahmemanagement – Übersicht

Wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Richtlinie nicht einhalten kann, können Sie eine Ausnahme anfordern. Das Ausnahmemanagement umfasst das anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Element (VI) oder eine Korrekturaufgabe (RT), die nicht gemäß der Richtlinie korrigiert werden können.

Einige Schwachstellen haben möglicherweise keinen Patch, eine Korrektur oder eine Lösung. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko akzeptieren, da Sie die Konsequenzen einer Nichtbeseitigung der Schwachstelle bestätigen und zustimmen.

Lebenszyklus einer Ausnahme

Definition einer Ausnahme

Eine Ausnahme ist eine Anforderung zum Zurückstellen der Korrektur eines VI oder RT für einen bestimmten Zeitraum. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Ausnahme wird angefordert

Als Korrekturbesitzer können Sie mit dem Ausnahmeverwaltungsprozess eine Ausnahme für ein VI oder RT beantragen. Nachdem der Ausnahmegenehmiger diese Anforderung genehmigt hat, wechselt das VI oder RT zu einem **Zurückgestellt** status.

Ausnahmeanforderung wird genehmigt

VIS oder RTS, die nicht sofort behoben werden können, werden von Schwachstellenanalysten überprüft, auf Risiko bewertet und für eine Zurückstellung genehmigt, bis sie behoben werden können. Das Genehmigen einer Ausnahmeanforderung kann ein Workflow auf zwei Ebenen sein. Wenn nur der Genehmiger der ersten Ebene vorhanden ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Beginnt ab Vulnerability Response V15.0: Wenn Sie die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht zurück in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für das Ausnahmemanagement und falsch positive Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

  Sobald eine Ausnahmeanforderung für ein VI oder RT genehmigt wurde, können Sie die folgenden Aktionen ausführen:

  - Erneut öffnen
  - Löschen
  - Aktualisieren Sie **Zuweisung an** Oder **Zuweisungsgruppen** Felder
- Ab v23.0 von Vulnerability Response, **Genehmigung Des Ausnahmeregelstatus** Der Workflow ist veraltet und wird im Flow Designer durch die Flow-Ausnahmeregelgenehmigung ersetzt.

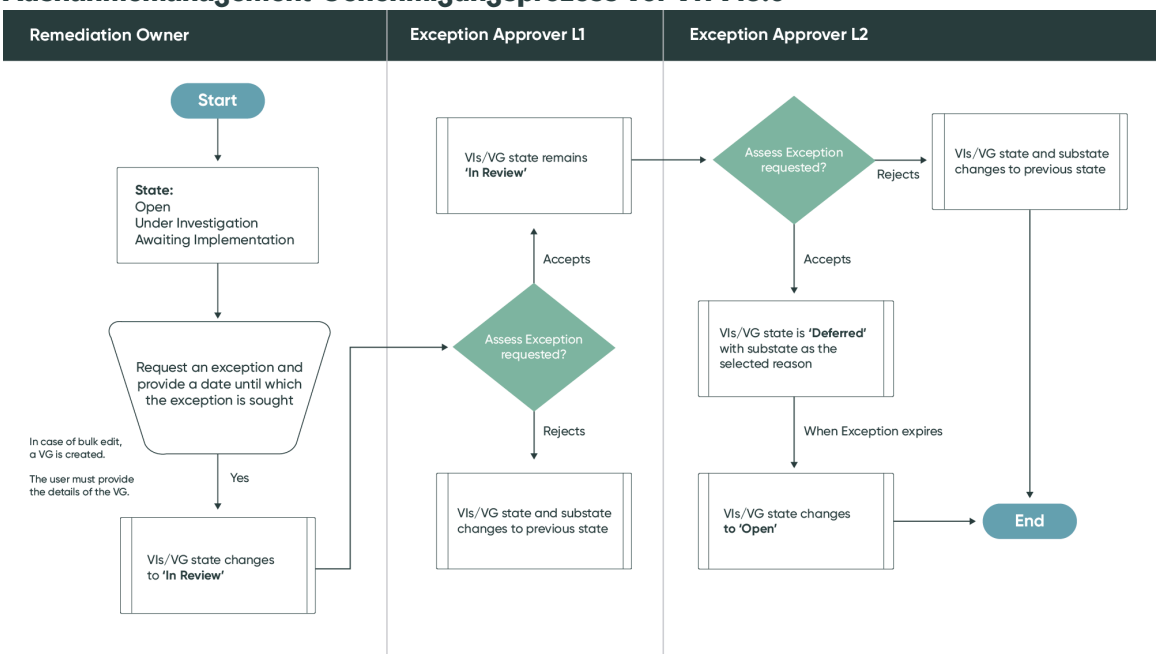
Nachverfolgung einer Ausnahmeanforderung

Nachdem Sie die Ausnahme ausgelöst haben, können Sie ihren Status mithilfe von nachverfolgen **Statusänderungsgenehmigungen** Registerkarte des VI oder RT. Wenn eine Aktion für eine RT ausgeführt wird, können Sie den Status der einzelnen VIS in dieser RT nicht nachverfolgen.

Ablauf einer Ausnahmeanforderung

Wenn eine Ausnahmeanforderung für ein bestimmtes VI oder RT abläuft, wird das betroffene VI oder RT auf zurückgesetzt **Öffnen** status.

Ausnahmemanagement-Genehmigungsprozess Vor VR v15.0



Wenn ein einzelnes VI oder alle VIS in einer RT beim nächsten Scan übergehen, werden die VIS und gegebenenfalls die RT durchgeführt **Status** Feld ändert sich in **Geschlossen** Mit dem Substatus **Behoben** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehrere Zurückstellungen

Verfolgen Sie, wie oft ein Datensatz oder eine Korrekturaufgabe zurückgestellt wird. Eine geplante Aufgabe, `set deferral counts`, Wird täglich ausgeführt, um die Anzahl der Datensätze, die mehrmals zurückgestellt werden, in der Spalte „Anzahl der Zurückstellungen“ im Modul „mehrere Zurückstellungen“ für VR zu buchen. Alle Anzahlen für Datensätze, die einer Korrekturaufgabe zugeordnet sind, werden erfasst und veröffentlicht, wenn eine Korrekturaufgabe mehr als einmal zurückgestellt wird.

Zugehörige Informationen

Fordern Sie Ausnahmen für Korrekturaufgaben und -Datensätze in an Arbeitsbereich des Schwachstellenmanagers

Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen

Fordern Sie eine Ausnahme mit an GRC: Richtlinien- und Compliance-Management In Arbeitsbereich für IT-Korrekturen

Übersicht über Ausnahmeregeln

Ausnahmeregeln für Vulnerability Response Ermöglichen Sie es Ihnen, den Zurückstellungsprozess für angreifbare Elemente (VIS) zu automatisieren. Fordern Sie eine Ausnahme für die angreifbaren Elemente (VIS) an, die nicht sofort behoben oder zurückgestellt werden können, indem Sie die betroffenen Schwachstellen, Konfigurationselemente (Configuration Items, CIs) oder VIS identifizieren. Verschieben Sie die übereinstimmenden VIS basierend auf der Regel, wenn das System sie identifiziert, indem Sie den VI-Zurückstellungsprozess automatisieren.

Verwenden von Ausnahmeregeln in Ihrer Organisation

Verwenden Sie Ausnahmeregeln, um neue und vorhandene VIS automatisch für einen bestimmten Zeitraum zurückzustellen, wenn sie der genehmigten Regelbedingung entsprechen. Die Automatisierung minimiert das Risiko fehlender Servicelevel-Vereinbarungen und erleichtert die Verwaltung mehrerer Elemente, da Sie manuelle Eingriffe vermeiden.

Zurückstellungsregeln unterstützen die Reihenfolge, d. h. die Regel mit der höchsten Priorität wird zuerst ausgeführt. Wenn eine Regel mit hoher Priorität auf ein VI angewendet wird, werden keine nachfolgenden Regeln erneut darauf angewendet, auch wenn die Bedingung mit dem VI übereinstimmt

Hinweis:

- Sie können Regeln nur erstellen, wenn Sie auswählen Vulnerability Response In der Konfiguration „Ausnahmemanagement“. Details finden Sie unter Konfigurieren Sie das Ausnahmemanagement für Vulnerability Response.
- Wenn VIS durch eine Ausnahmeregel zurückgestellt werden, werden sie in die erstellte Zurückstellungskorrekturaufgabe (RT) kopiert. Die VIS sind weiterhin Teil des RTS, dem sie zuvor angehörten.

Der Lebenszyklus einer Ausnahmeregel sieht wie folgt aus:

- Erstellen einer Ausnahmeregel
- Genehmigen einer Ausnahmeregelanforderung
- Ausnahmeregel aktivieren
- Ausnahmeregel wird zurückgestellt
- Ablauf einer Ausnahmeregel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen einer Ausnahmeregel

Sie können eine Ausnahmeregel erstellen, um die VIS, die den definierten Bedingungen für den angegebenen Zeitraum entsprechen, automatisch zurückzustellen. Nachdem Sie eine Ausnahmeregel erstellt haben, übermitteln Sie sie zur Genehmigung.

Genehmigen einer Ausnahmeregelanforderung

Das Genehmigen einer Ausnahmeregelanforderung ist ein zweistufiger Prozess. Wenn nur der Genehmiger der ersten Ebene vorhanden ist, kann die Ausnahmeregel durch eine einzige Genehmigung bewertet und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahmeregelgenehmigung genehmigt werden. Nachdem die Regel genehmigt wurde, wird eine Korrekturaufgabe (RT) erstellt. Weitere Informationen finden Sie unter Antrag auf Ausnahmeregel genehmigen.

Hinweis:

Beginnt ab Vulnerability Response V15.0: Wenn Sie die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht zurück in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für das Ausnahmemanagement und falsch positive Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Nachdem eine Ausnahmeregelanforderung genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Abbrechen
- Löschen

Ausnahmeregel aktivieren

Nachdem eine Ausnahmeregel genehmigt wurde, wird standardmäßig eine Korrekturaufgabe im Status „Zurückgestellt“ erstellt. Ab dem Datum „gültig ab“ wird die Ausnahmeregel für alle erstellten VIS und auch für die VIS ausgeführt, die vom Status „Geschlossen“ in den Status „Offen“ verschoben werden.

Hinweis:

Wenn Sie die Option für vorhandene Daten ausführen aktivieren, wird eine geplante Aufgabe einmal für die vorhandenen Daten am Datum „gültig ab“ ausgeführt.

Ausnahmeregel wird zurückgestellt

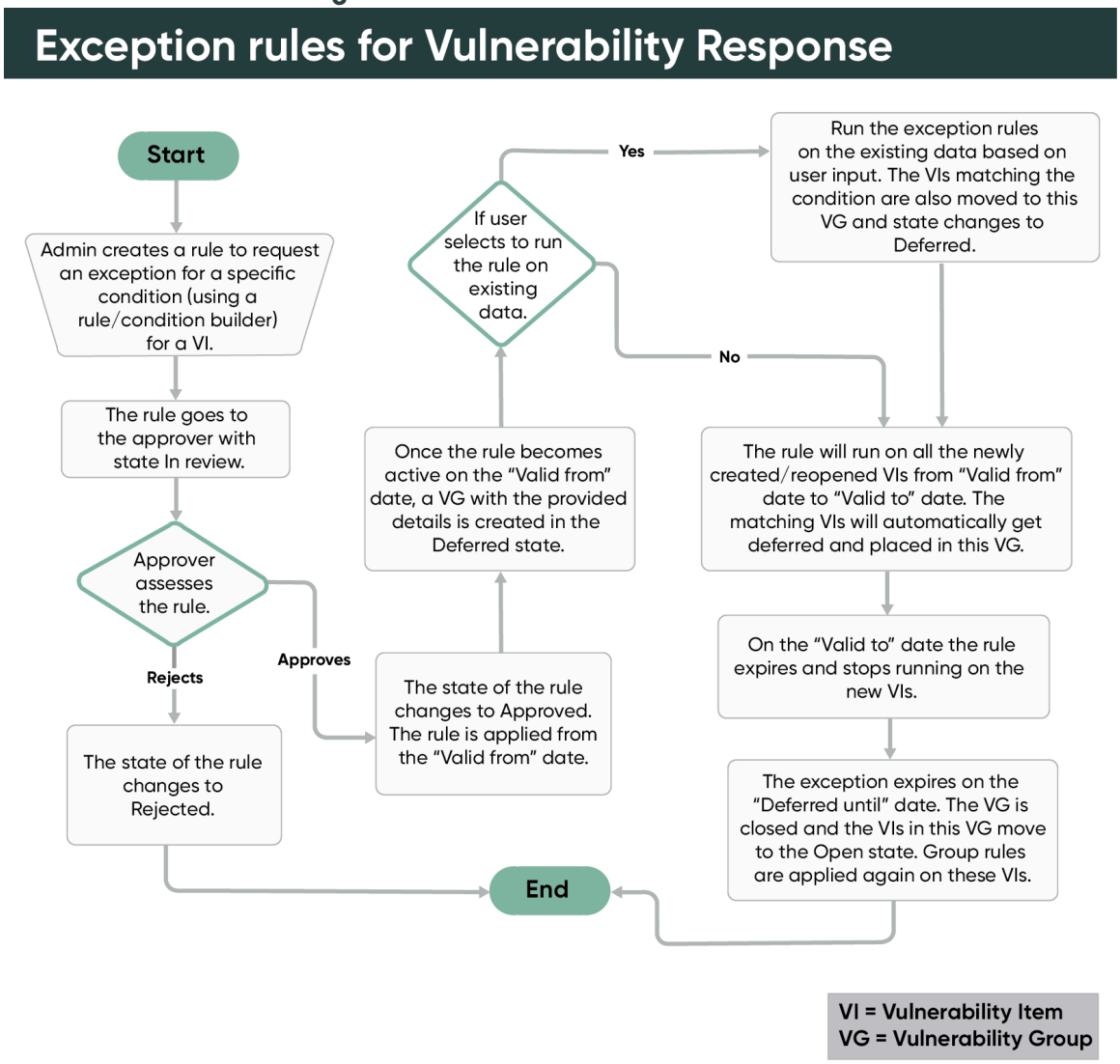
Sie können VIS, die den in dieser Ausnahmeregel definierten Bedingungen entsprechen, bis zum Datum „zurückgestellt bis“ zurückstellen, das für die Regel definiert ist. An diesem Datum wird die Korrekturaufgabe, die Sie für die Ausnahmeregel erstellt haben, geschlossen, und alle VIS in dieser Gruppe werden zurück in den Status Offen versetzt. Gruppenregeln werden erneut auf sie angewendet, um sie dem erforderlichen RTS zuzuweisen.

Ablauf einer Ausnahmeregel

Nach Ablauf der Ausnahmeregel wird sie nicht mehr für neue oder erneut geöffnete VIS ausgeführt. Die zugeordnete RT bleibt bis zum Datum „Zurückgestellt bis“ im Status „Zurückgestellt bis“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow für Ausnahmeregeln vor v15 .0



Übersicht über Ausschlussregeln

Ausschlussregeln bieten eine Möglichkeit, Erkennungen während des Erfassungsprozesses in zu filtern oder auszuschließen, dass sie nicht in angreifbare Elemente (Vits) konvertiert werden Vulnerability Response.

Diese Regeln können für verschiedene Szenarien eingerichtet werden, z. B.:

- Ausgenommen Schwachstellen mit niedrigem Schweregrad oder Risiko, die keine sofortige Korrektur erfordern.
- Verbesserung des Korrekturprozesses durch Priorisierung der kritischsten Vits für Aktionen.
- Reduzieren Sie die Verarbeitungszeit während des Datenimports, indem Sie einen Prozentsatz der Erkennungen aus der VIT-Konvertierung ausschließen.

Während des Prozesses der Datenerfassung gibt es unterschiedliche Ansätze für die Verarbeitung neuer und vorhandener Erkennungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für neue Erkennungen:
  - Wenn eine neue Erkennung die Bedingungen einer Ausschlussregel nicht erfüllt, wird eine Erkennung mit den Vits erstellt.
  - Wenn eine neue Erkennung die Bedingungen einer Ausschlussregel erfüllt, wird die Regel der Erkennung zugeordnet, VIT wird jedoch nicht erstellt. Füllen Sie die Referenz für die übereinstimmende Ausschlussregel im Erkennungsdatensatz aus. Die Spalte „Ausschlussregel“ wird im Erkennungsdatensatz entsprechend mit der Referenz „Ausschlussregel“ ausgefüllt.
- Für vorhandene Erkennungen:
  - Wenn die Erkennung die Bedingungen einer Ausschlussregel nicht erfüllt, wird mit dem normalen Workflow fortgefahren.
  - Wenn eine vorhandene Erkennung den Bedingungen einer Ausschlussregel entspricht, bleibt die dieser Erkennung zugeordnete VIT im aktuellen Status, die Regel wird jedoch der Erkennung zugeordnet. Der Status der VIT wird durch den in definierten Wert gesteuert *sn_vul.close_vit_with_excluded_detections*Eigenschaft. Standardmäßig ist der Wert in dieser Eigenschaft auf „falsch“ festgelegt. Wenn der Wert auf „falsch“ festgelegt ist, werden die Erkennungen unter einer VIT ausgeschlossen, und der Status der Vits bleibt im aktuellen Status. Wenn der Wert jedoch auf „wahr“ festgelegt ist, können die folgenden Szenarien auftreten:
    - Wenn jede Erkennung unter einer VIT ausgeschlossen ist, wird der Status der VIT in „Geschlossen ausgeschlossen“ aktualisiert.

      Hinweis:
      Ab v22.1.2 von Vulnerability Response Ein neuer Substatus namens Ausgeschlossen wurde hinzugefügt.

    - Wenn eine Erkennung als geschlossen markiert ist, während die verbleibenden ausgeschlossen sind, wird die VIT als „Geschlossen behoben“ festgelegt.
    - Wenn die VIT offene Erkennungen hat, bleibt die VIT offen.

Zugehörige Informationen

Erstellen Sie eine Ausschlussregel

Falsch Positiv Übersicht

Ein falsch positives ist eine Bedingung, bei der der Scanner meldet, dass im System eine Schwachstelle vorhanden ist, in Wirklichkeit jedoch keine Schwachstelle vorhanden ist. Es kann mehrere Gründe geben, z. B. falsche Klassifizierung, falsche Logik oder Algorithmus im Scanner. Der Korrekturbesitzer kann angreifbare Elemente (VIS) oder Korrekturaufgaben (RTS) als falsch positiv markieren.

Wichtig:
Sie können die angreifbaren Host-Elemente als falsch positiv markieren Arbeitsbereich des Schwachstellenmanagers. Weitere Informationen zum Markieren der angreifbaren Host-Elemente als falsch positiv im Massenvorgang finden Sie unter Massenbearbeitung für falsch positive Werte im Vulnerability Manager-Arbeitsbereich.

Lebenszyklus eines falsch positiven Elements

Bedeutung von falsch positiv

Der Scanner gibt irgendwann eine Warnung aus, wenn in Wirklichkeit keine Schwachstelle vorhanden ist. Wenn beispielsweise ein Konfigurationselement außer Betrieb genommen wurde, der Scanner jedoch weiterhin ein Problem damit auslöst, markieren Sie es als falsch positiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wird als falsch positiv markiert

Details zum Markieren eines VI oder RT als falsch positiv finden Sie unter Als falsch positiv markieren.

Arbeiten mit falsch positivem

Sobald ein VI oder RT als falsch positiv markiert wurde, wird der Status in „Geschlossen“ aktualisiert, und der Substatus wird in „falsch positiv“ geändert. Die folgenden Aktionen können ausgeführt werden:

- Erneut öffnen
- Löschen
- Aktualisieren Sie das Datum in **Bis** Feld. Dieses Datum wird dann als Ablaufdatum für das falsch positive Datum verwendet.

Hinweis:
Wenn nicht genehmigt, kehrt das VI oder RT in den vorherigen Status zurück.

Genehmigen eines falsch positiven Elements

Der Genehmiger kann die falsch positiven Elemente über seinen Genehmigungs-Workflow genehmigen.

Hinweis:

Wenn Sie ab Vulnerability Response v15.0 die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht zurück in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für das Ausnahmemanagement und falsch positive Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Falsch positiv wird erneut geöffnet

Ein VI oder RT in einem falsch positiven Substatus kann jederzeit erneut geöffnet werden.

Verfolgen eines falsch positiven Werts

Verwenden Sie **Statusänderungsgenehmigungen** Abschnitt zum Nachverfolgen des Status des falsch positiven Elements. Nach der Genehmigung wird der Status des VI oder RT in „Geschlossen“ aktualisiert, und der Grund ist „falsch positiv“.

Ablauf eines falsch positiven Elements

Nur der falsch positive Genehmiger kann ein bis-Datum festlegen, bis zu dem das falsch positive Datum abläuft, damit das VI oder RT abläuft. Außerdem können nur falsch positive Ergebnisse ablaufen, für die der Genehmiger ein bis-Datum angegeben hat. Dieses Datum kann angegeben werden, nachdem der falsch positive Wert genehmigt wurde.

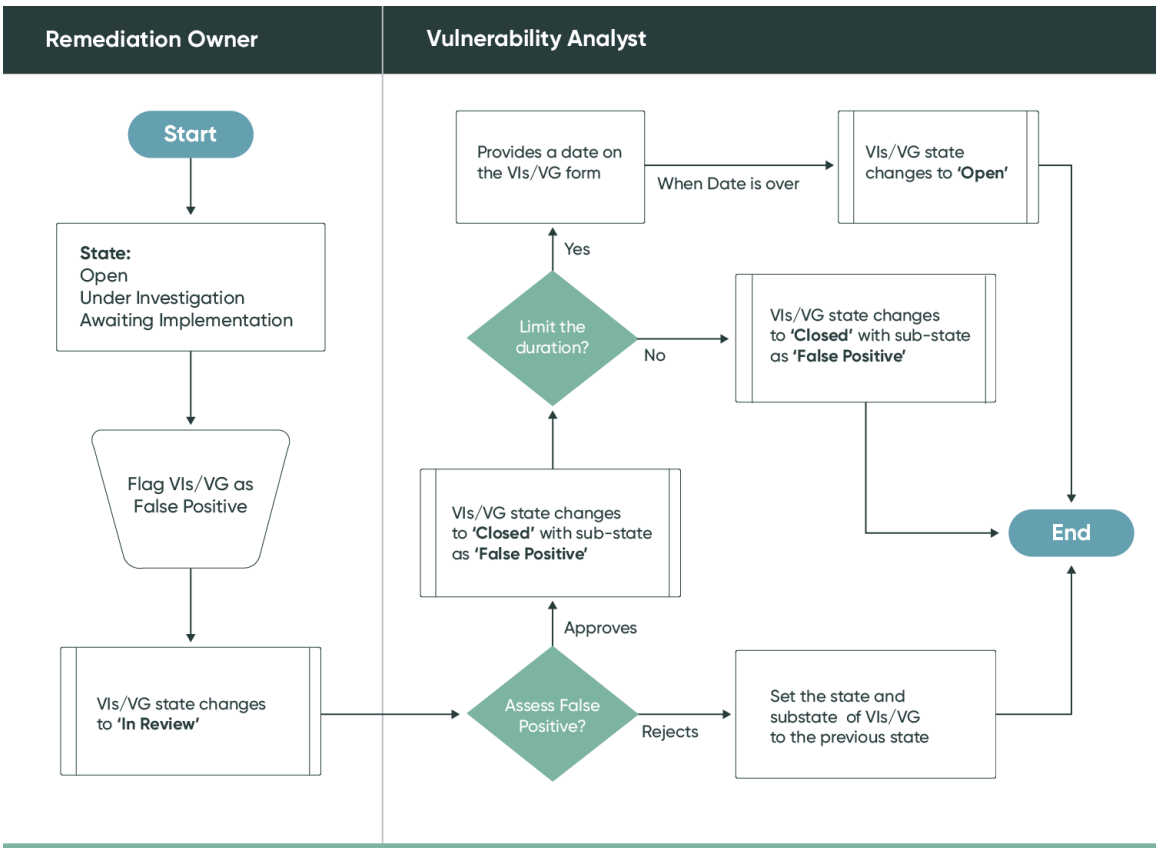
Ein falsch positiver Wert ohne bis-Datum ist ein dauerhaft falsch positiver Wert. Nachdem der falsch positive Wert abgelaufen ist, wird der Status des VI oder VR wieder in Offen verschoben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Ab v21.0 von Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Falsch positiver Genehmigungsprozess vor v15 .0



Der Genehmigungsprozess ist automatisch, wenn alle VIS den nächsten Scan bestehen. Die VIS werden unabhängig vom aktuellen Status automatisch geschlossen. Die VIS oder, falls zutreffend, die RT **Status** Felder ändern sich in **Geschlossen** Mit dem Substatus **Behoben.**

Weitere Informationen finden Sie unter Markieren und genehmigen eines falsch positiven Elements.

Zugehörige Informationen

Fordern Sie ein falsch positives Ergebnis für ein angreifbares Element oder eine Korrekturaufgabe an

Fragebogenunterstützung in Ausnahmemanagement über intelligente Bewertung

Konfigurieren Sie erweiterte Fragebogen als Teil des Ausnahmeverwaltungsprozesses mit intelligenter Bewertung. Dadurch können Korrekturbesitzer detaillierteren Kontext für Ausnahmeanforderungen bereitstellen, und Genehmiger können bedingte Fragen konfigurieren, um Informationen für eine fundierte Entscheidungsfindung zu sammeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rollen

Vorlagenleser Für Intelligente Bewertungen : **sn_vul_cmn.Smart_assessment_template_Manager** (Schwachstellenadministrator und Vorlagenleser) ermöglicht Administratoren das Erstellen und Bearbeiten von Vorlagen.

Akteur der intelligenten Bewertung : **sn_vul_cmn.Smart_assessment_actor** Ermöglicht Ihnen (Korrekturbesitzer und Administratoren) das Ausfüllen der Fragebogen/Bewertungen.

Leser für intelligente Bewertungen : **sn_vul_cmn.Smart_assessment_Reader** Ermöglicht Ihnen (Genehmiger) das Lesen der übermittelten Fragebogenantworten.

Voraussetzung: Die Plugins für intelligente Bewertungen müssen installiert werden, da die intelligente Bewertung eine Abhängigkeit von Vulnerability Response ist.

Sie können jetzt Fragebogen als Teil des Ausnahmeverwaltungsprozesses mit intelligenter Bewertung konfigurieren. Es ermöglicht Schwachstellenadministratoren/Managern, bedingte Fragen zu konfigurieren, um die richtigen Informationen zu sammeln, die für eine fundierte Entscheidungsfindung erforderlich sind, während Korrekturbesitzer detaillierteren Kontext für Ausnahmeanforderungen bereitstellen können. Dies verbessert die Zusammenarbeit zwischen den Teams „Schwachstellenmanagement“ und „Korrektur“, indem der Genehmigungsprozess optimiert und die Klarheit und Vollständigkeit der Begründungen von Ausnahmen sichergestellt wird.

Fragebogen und intelligente Bewertungen sind im Arbeitsbereich sowie in der klassischen Anwenderoberfläche zugänglich, da einige Workflows noch Fragebogen im älteren Stil erfordern, während die neue Bewertung anwenderfreundlicher ist und nur im Arbeitsbereich unterstützt wird.

In **Ausnahmeverwaltungskonfiguration** Auf dem Bildschirm können Sie jetzt die Bewertung für Ausgleichssteuerung, Ausnahme anfordern und falsch positive Datensätze auswählen.

Hinweis:
Wenn Sie das Feld „Bewertung zum anfordern einer Ausnahme“ ausfüllen, ermöglicht das System Ihnen, die Vorlage für intelligente Bewertungen zu berücksichtigen, andernfalls werden die klassischen Fragebogen berücksichtigt.

Sie können die beiden folgenden Optionen verwenden: :

- **Intelligente Bewertung** : Verwalten Sie die Fragebogen im Schwachstellen-Arbeitsbereich.
- **Vorhandener Fragebogen** : Sie können sowohl im Arbeitsbereich als auch im Classic Experience auf den vorhandenen Fragebogen zugreifen.

Die obigen Vorlagen können vom Vorlagenleser für intelligente Bewertungen aufgerufen/bearbeitet werden: **sn_vul_cmn.Smart_assessment_template_Manager** .

Konfigurieren Sie die Bewertungsvorlage

Bewertungsvorlagen enthalten die Fragen, die während des Anforderungsprozesses (z. B. beim anfordern einer Ausnahme) gefragt werden. Die oben genannten vorkonfigurierten Vorlagen werden mit einer intelligenten Bewertung bereitgestellt. Sie können bei Bedarf auch eigene Vorlagen erstellen.

Vorbereitungen
Erforderliche Rolle:

Vorlagenleserrolle : **sn_vul_cmn.Smart_assessment_Reader** Ermöglicht Ihnen (Genehmiger) das Lesen der übermittelten Fragebogenantworten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle Des Vorlagenakteurs : **sn_vul_cmn.Smart_assessment_actor** Ermöglicht Ihnen (Korrekturbesitzer und Administrator) das Ausfüllen der Fragebogen/Bewertungen.

Warum und wann dieser Vorgang ausgeführt wird

Im Vulnerability Response-Arbeitsbereich können Sie die Vorlage mit dem Bewertungsziel VCA auswählen, die für die Ausnahmeanforderung verwendet werden soll (z. B. Ausnahme für Vulnerability Response, falsch positiv für Vulnerability Response). Wenn Sie die Standardvorlage auswählen, werden die Fragen automatisch ausgefüllt. Wenn Sie eine eigene Vorlage erstellen, kann sie geändert werden.

Prozedur

1. Navigieren Sie zu Bewertungsarbeitsbereich.
2. Wählen Sie ein vorhandenes aus **Bewertungsvorlage** Oder wählen Sie eine aus **Neue Vorlage**
3. Geben Sie die folgenden Details ein:
   - **Vorlagenname** : Ein eindeutiger Name für die Vorlage
   - **Bewertungsname** : Der Name, der beim Anzeigen der Bewertung im System angezeigt wird.
   - **Vorlagenkategorien** : Vorlagen werden kategorisiert, um die Verwaltung zu erleichtern. Einige Vorlagenkategorien werden sofort bereitgestellt, z. B. Vorlagen für Vulnerability Response-Fragebogen. Sie können Vorlagen Ihrer Wahl erstellen.
   - **Bewertungsziele** : Gibt die Tabelle an, zu der die Vorlage gehört. Für VR ist dies die VCA-Tabelle (Tabelle „Genehmigung von Schwachstellen-Changes“).

Workflow für intelligente Bewertung

Korrekturbesitzer müssen den Fragebogen ausfüllen, bevor sie zur Genehmigung übermitteln. Genehmiger überprüfen den Fragebogen und treffen Genehmigungs-/Ablehnungsentscheidungen basierend auf den bereitgestellten Informationen.

Vorbereitungen

Erforderliche Rolle: **sn_vul_cmn.Smart_assessment_Reader**

Warum und wann dieser Vorgang ausgeführt wird

Im Folgenden finden Sie den Workflow der Anpassung der intelligenten Bewertung:

- **Anforderung für Ausnahme/falsch positiv** Wenn Sie eine Ausnahme anfordern oder etwas als falsch positiv markieren, überprüft das System, ob ein Fragebogen erforderlich ist.
- Wenn **Fragebogenoption ist aktiviert** , A **Obligatorische Nachricht** Fordert den Anwender auf, den Fragebogen auszufüllen, bevor mit dem Genehmigungsprozess fortgefahren wird.
- **Entwurfsstatus** : Die **Genehmigung Der Statusänderung Der Schwachstelle** (VCA)-Datensatz verbleibt im Entwurfsstatus, bis der Fragebogen übermittelt wurde, und das Schwachstellenelement (VIT) befindet sich im Status „Offen“.
- **Genehmigeransicht** : Sobald Korrekturbesitzer den Fragebogen ausgefüllt und übermittelt haben, werden die Datensätze „Genehmigung der Änderung des Schwachstellenstatus“ (VCA) und „Schwachstellenelement“ (VIT) in den Status „in Überprüfung“ verschoben. Genehmiger können die Fragebogen unter „alle > meine Genehmigungen“ überprüfen. Die VIT wird nach Genehmigung der Datensätze in den Status „zurückgestellt“ verschoben. Sie können den Fragebogen über einen Link anzeigen, der von den Korrekturbesitzern im Header des Datensatzformulars übermittelt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren **Alle** > **Meine Genehmigungen**Zum Anzeigen des Fragebogens.
2. Sobald der Datensatz ist **Genehmigt** , VIT wird in den Status zurückgestellt verschoben.
3. Sie können den Fragebogen über einen Link anzeigen, der von den Korrekturbesitzern im Header des Datensatzformulars übermittelt wurde.

Fragebogen für „falsch positiv“ oder „Ausnahme anfordern“

Wenn der Fragebogen für „falsch positiv“ oder „Ausnahme anfordern“ ausgelöst, aber nicht vollständig ausgefüllt wird.

Wenn der Fragebogen für „falsch positiv“ oder „Ausnahme anfordern“ ausgelöst, aber nicht vollständig ausgefüllt wird, wechselt der VCA-Datensatz in den Status „Entwurf“. Wenn Sie eine Ausnahme aus derselben Kategorie auslösen möchten, werden Sie nach einer Popup-Notiz zu derselben zum vorherigen Fragebogen navigiert. Wenn Sie einen falsch positiven Datensatz anstelle einer vorhandenen Anforderungsausnahme erstellen möchten, überschreibt das System die Genehmigung der Schwachstellenstatus-Änderung (VCA) und erstellt einen neuen falsch positiven Datensatz zur Genehmigung der Schwachstellenstatus-Änderung (VCA).

Wenn der Fragebogen zur Hälfte ausgefüllt ist und dasselbe Schwachstellenelement (VIT)/ oder ein ELEMENT in der klassischen Ansicht geöffnet wird, werden Sie zum Arbeitsbereichsfragebogen navigiert, um die verbleibenden Daten auszufüllen, wenn derselbe Anforderungstyp erneut ausgelöst wird. Wenn der Fragebogen in der klassischen Ansicht selektiv ausgefüllt wird und dasselbe Element im Arbeitsbereich geöffnet wird, wird der Fragebogen der klassischen Ansicht im Arbeitsbereich geöffnet.

Watchdog für Vulnerability Response

Der Watchdog wird verwendet, um Tabellen basierend auf den von Ihnen angegebenen Bedingungen nachzuverfolgen. Sie kann beispielsweise verwendet werden, um Details von Fehlern bei der Integrationsausführung in zu protokollieren Vulnerability Response.

Sie können wählen, ob Sie über diese Fehler benachrichtigt werden möchten. Basierend auf dieser Benachrichtigung können Sie die Fehlerkorrektur planen. Die standardmäßigen Watchdogs sind:

- Integrationsausführung fehlgeschlagen: Wenn der Status der Integrationsausführung auf „Abgeschlossen“ und der Substatus auf „Fehlgeschlagen“ festgelegt ist, werden Anwender und Anwendergruppen benachrichtigt, wenn die Bedingung eine Anzahl größer als 0 zurückgibt, d. h. die Integrationsausführung schlägt fehl.
- Integrationen mit langer Ausführungszeit: Skript zur Überprüfung, ob die Integrationsausführung die festgelegte Zeit überschreitet. Dieser Watchdog warnt Sie proaktiv, wenn der Abschluss der Integrationsausführung verzögert wird.
- Überlappende regelmäßige Ausführungen: Skript zum Überprüfen der wiederkehrenden Integrationsausführungen, die während ihres bevorstehenden Vorkommens weiterhin ausgeführt werden. Generiert einen Link, der die Liste dieser Integrationsausführungen enthält.

Überwachungsprotokoll

Der Watchdog verfügt über ein Beobachtungsprotokoll, das angibt, wie oft die Bedingung erfüllt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersichts-Dashboard

Verwenden Sie das Übersichts-Dashboard, um den Watchdog für die letzten 30 Tage zu überwachen. Sie können mehrere Widgets erstellen, um andere überwachte Watchdog-Themen nachzuverfolgen.

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard ist in der neuen Experience-UI verfügbar.

Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Bericht

Name	Beschreibung
WatchDog-Fehler der letzten 30 Tage	Alle Bedingungen wurden in den letzten 30 Tagen erfüllt.

Weitere Informationen finden Sie unter Konfigurieren Sie Watchdog und Fehlerbehandlung für Erkennungen.

Change-Management für Vulnerability Response

Als IT-Korrekturbesitzer können Sie Change-Anforderungen (CHG) direkt aus Korrekturaufgaben (RT) in erstellen und verwalten Vulnerability Response Anwendung. Change-Anforderungen helfen Ihnen, Change-Aktivitäten für Ihre Assets zu initiieren und nachzuverfolgen, damit Sie Ihre Korrekturaufgaben und die entsprechenden angreifbaren Elemente korrigieren können.

Change-Anforderungen und der Schwachstellen-Workflow

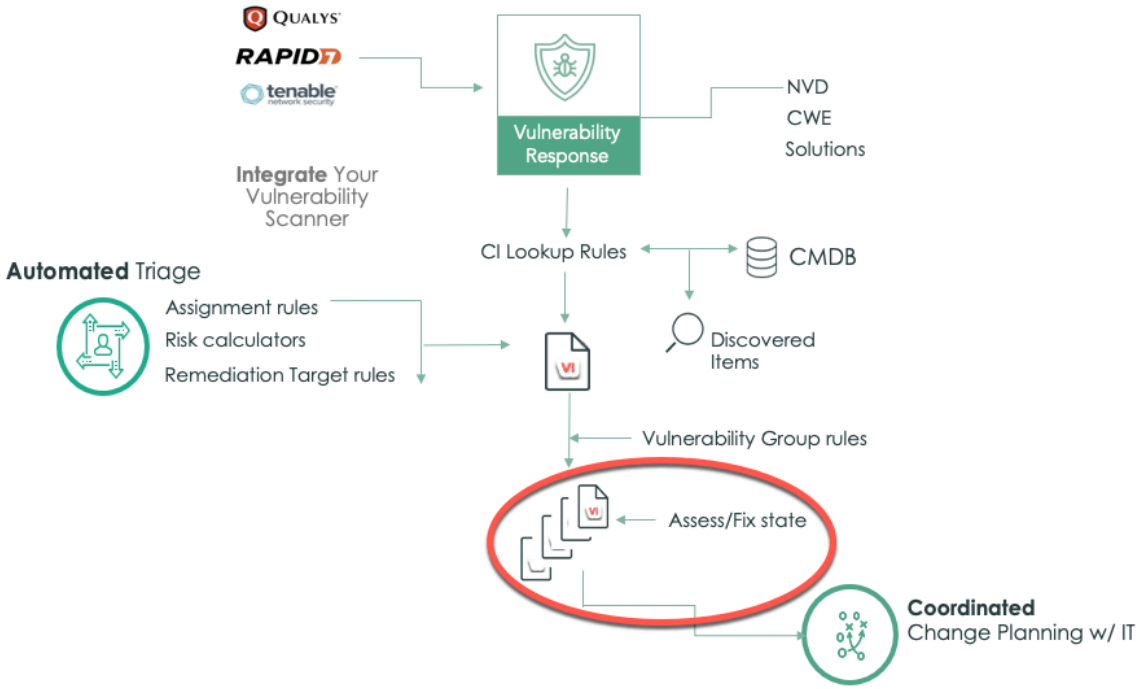
Wenn Sie mit der Vulnerability Response-Anwendung nicht vertraut sind, finden Sie weitere Informationen unter Erkunden Sie Vulnerability Response Anwendung.

Die folgende Abbildung zeigt den Informationsfluss für Vulnerability Response, Von der Integration (Scanner) durch automatisierte Selektierung und in die Untersuchung.

Change-Anforderungen und Change-Management sind Teil des Korrekturprozesses (Status Bewerten/Beheben) in der Vulnerability Response Workflow, der in der folgenden Abbildung angezeigt wird. Während dieser Phase können Sie Change-Anforderungen verwenden, um die Behebung von Schwachstellen zu initiieren und nachzuverfolgen. Sie können Change-Anforderungen direkt aus der Korrekturaufgabe erstellen und verwalten und Untersuchungs- und Korrekturaufgaben auflisten, die Lösungen für betroffene Assets für die Konfigurationselemente (Configuration Items, CI) in Ihrer CMDB enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Change-Anforderungen in Vulnerability Response



Wann Change-Anforderungen in Vulnerability Response verwendet werden sollen

Als IT-Korrekturbesitzer können Sie Change-Anforderungen aus einer Korrekturaufgabe erstellen, wenn ein manueller und kontrollierter Prozess jeglicher Art zum Ändern oder Entfernen unterstützter Konfigurationselemente (CIs) in Ihrer CMDB erforderlich ist. Durch das Erstellen und Verwalten von Change-Anforderungen direkt aus einem Korrekturaufgabendatensatz können Sie Schwachstellen schnell untersuchen und beheben. Die VIS einer gelösten Korrekturaufgaben können während des nächsten geplanten Scans in gescannt und verifiziert werden ServiceNow AI Platform Und zur automatisierten Selektierung von zurückgekehrt Vulnerability Response Workflow. Zu den manuellen Eingriffen, die möglicherweise Change-Anforderungen erfordern, gehören die folgenden Beispiele:

- Ein Software-Patch, eine Korrektur oder eine andere Aufgabe von IT, die für angreifbare Elemente vor der RT-Lösung erforderlich ist.
- Sie bestimmen, dass eine Teilmenge der angreifbaren Elemente in einer Korrekturaufgabe weitere Untersuchungen oder Neuzuweisungen an eine andere Abteilung erfordert.
- Sie bestimmen, dass eine Teilmenge angreifbarer Elemente in einer RT mit einem großen Satz angreifbarer Elemente in eine neue Korrekturaufgabe verschoben werden kann.
- Sie können eine Korrekturaufgabe einer vorhandenen Change-Anforderung zuordnen, um Doppelungen von Korrekturaufgaben zu vermeiden.

Typen von Change-Anforderungen für eine RT

Die Vulnerability Response Die Anwendung verwendet die drei Arten von Service-Changes, die von unterstützt werden ITSM Change-Management Produkt auf Ihrem ServiceNow AI Platform® Instanz – Standard, Notfall und Normal. Die Art des Change, den Sie auswählen, bestimmt, welches Statusmodell aufgerufen wird und welcher Change-Prozess befolgt werden muss. Change-Anforderungen erfassen die detaillierten Informationen zum Change, z. B. den Grund des Change, die Priorität, das Risiko, den Typ des Change und die Change-Kategorie. Siehe Change-Typen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Vulnerability Response IT-Korrekturbesitzer haben die folgenden Optionen, um normale, Standard- und Notfall-Change-Anforderungen direkt aus einer Korrekturaufgabe zu erstellen:

- Sie können Change-Anforderungen erstellen, die vorab ausgefüllte Informationen aus der Korrekturaufgabe enthalten, um den Prozess zu optimieren und Zeit zu sparen.
- Sie können eine Korrekturaufgabe einer vorhandenen Change-Anforderung zuordnen, um zu vermeiden, dass doppelte Change-Anforderungen erstellt werden, die ähnliche Informationen und angreifbare Elemente teilen.
- Mit einer Reihe von Bedingungen können Sie eine Teilmenge angreifbarer Elemente herausfiltern und eine Korrekturaufgabe aufteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue RT verschoben.

Sie können angreifbare Elemente anhand von Werten aus beliebigen Feldern aus einer Korrekturaufgabe filtern und die Change-Anforderung nur auf die Elemente anwenden, die Ihren Filterkriterien entsprechen.

Zugehörige Informationen

Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe

Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu

Teilen Sie eine Korrekturaufgabe auf

Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben

Bewertung des Softwarerisikos mit Software Asset Management (SAM Foundation)

Verwenden Sie ServiceNow® Schwachstelle Anwendung „Risikobewertung“, um die Gesamtanzahl der installierten Software für ein bestimmtes Softwarepaket in Ihren Assets zu bestimmen. Bei Verwendung mit ServiceNow® Software Asset Management (SAM) Foundation-Anwendung, bewerten Sie Ihr Risiko, erstellen Sie angreifbare Elemente, und verwalten Sie die Fehlerkorrektur für die von Ihnen erkannte angreifbare Software.

Wichtig:
Sie können die Risikobewertung nach Common Vulnerabilities and Exposures (CVE) und Software durchführen, um die zusätzlichen Fähigkeiten im Vulnerability Assessment-Arbeitsbereich zu nutzen. Weitere Informationen finden Sie unter Arbeitsbereich für Schwachstellenbewertung kennenlernen.

Ermitteln Sie Ihr Risiko für angreifbare Software, indem Sie Informationen zu angreifbarer Software (Herausgeber, Produkt, Edition und Version) bereitstellen, ohne die CVE-Datenbank (Common Vulnerabilities and Exposures) zu verwenden. Bewerten Sie Fälle von Zero-Day-Schwachstellen (aktueller Tag) für Software für die folgenden Fälle:

- Wenn Produkte noch keine CVE-Daten haben.
- Wenn zwischen dem Zeitpunkt, zu dem eine Schwachstelle öffentlich bekannt wird, und dem die CVE-Daten mit der Schwachstelle im NVD aktualisiert werden.
- Wenn Sie zwischen den geplanten Scans Ihres Schwachstellen-Scanners mehr über die Schwachstelle erfahren.

Mit Schwachstelle Anwendung „Risikobewertung“, wenn Sie den Herausgeber und das Produkt für die angreifbare Software kennen, verwenden Sie die Datensätze, die die installierte Software in Ihrem Netzwerk auflisten, die von erstellt wurde SAM Foundation Anwendung können Sie Ihr Risiko potenziell schädlicher Softwarepakete bei Bedarf bewerten.

Wenn Sie wissen, wie groß Ihr Risiko für diese Art von Schwachstellen ist, können Sie proaktiv reagieren, indem Sie eine rote Warnung implementieren und die Software

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

deinstallieren oder Ihr Security Operations Center (SOC) informieren, nach einem bestimmten Patch zu suchen. Sie können angreifbare Elemente erstellen und dem Korrekturspezialisten Aufgaben für die Nachbesserung weiterer Untersuchungen zuweisen. Zeigen Sie eine Liste der Korrekturaufgaben (VUL) an, um sicherzustellen, dass die gewünschten angreifbaren Elemente erstellt und dem VUL korrekt zugeordnet sind.

Zugehörige Informationen

Konfigurieren Sie Schwachstelle Risikobewertung

Bewerten Sie Ihr Risiko für angreifbare Software

Schwachstellen-Krisenmanagement

Erstellen und verfolgen Sie kritische Schwachstellenereignisse über den Vulnerability Crisis Management (VCM)-Workflow. Erstellen Sie Schwachstellenbewertungsdatensätze, zeichnen Sie Schlüsselattribute der Schwachstelle auf, um das Risiko zu berechnen, führen Sie eine Bewertung durch, um das Gefahrenniveau zu identifizieren, und binden Sie Stakeholder ein, um eine koordinierte und schnelle Reaktion auf Schwachstellen zu erhalten.

Verwalten von Schwachstellen-Krisenereignissen

Schwachstellen-Krisenmanagement ist ein vollständiger Workflow zur Verarbeitung von Schwachstellen-Krisenereignissen mit den folgenden Fähigkeiten.

- Identifizieren Sie angreifbare Konfigurationselemente effizient, indem Sie kritische Schwachstellen mit dem Softwareinstallationsbestand von korrelieren Software Asset Management Und Software Bill of Materials(SBOM) Bestand, vom Scanner gemeldete Schwachstellen und Configuration Management Database (CMDB).
- Konvertieren Sie Bewertungsergebnisse zur Korrektur in angreifbare Elemente.
- Initiieren Sie einen schwerwiegenden Security Incident, um eine schnelle und koordinierte Reaktion auf die Bedrohung sicherzustellen.
- Engagieren Sie sich mit Teams im gesamten Unternehmen, und arbeiten Sie mit ihnen zusammen, um eine einheitliche Reaktion auf Schwachstellen zu ermöglichen.
- Stellen Sie funktionsübergreifende Stakeholder und beteiligte Teams regelmäßige Statusberichte bereit, um Transparenz und Kommunikation während der gesamten Krise zu gewährleisten.

Schwachstellen-Krisenmanagement mit dem Arbeitsbereich für Schwachstellenbewertung

Hinweis:
Ab v1.0.1 von Vulnerability Crisis Management ist die Anwendung als separates Abonnement im Store verfügbar. Sie können über den Arbeitsbereich „Schwachstellenbewertung“ nur dann auf Schwachstellenmanagement zugreifen, wenn Sie über eine feingranulierte Berechtigung verfügen oder die Anwendung aus dem Store installiert haben. Zuvor war Vulnerability Crisis Management im Plugin Vulnerability Emergency Response enthalten. Ab v3.2.2 wurde das Plugin „Vulnerability Emergency Response“ in „Bewertung des Schwachstellenrisikos“ umbenannt.

Bei der Identifizierung einer Schwachstelle von Interesse erstellt der Schwachstellenereignismanager einen Schwachstellenbewertungsdatensatz mit Informationen zur Threat Intelligence-Quelle, den Schwachstellenmerkmalen und den betroffenen Produkten. Diese Informationen werden für weitere Auswirkungs- und Risikoanalysen verwendet.

Nachdem der Datensatz für eine Schwachstelle von Interesse erstellt wurde, wird eine Risikobewertung durchgeführt. Diese Bewertung umfasst die strukturierte Risikobewertung,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Überprüfung des Datensatzes und die Beobachtungen des Analysten, der die Aufgabe ausführt. Die anfängliche Risikopunktzahl für eine Schwachstelle von Interesse wird anhand der Attribute berechnet, die zum Zeitpunkt der Ereigniserstellung verfügbar sind. Die Risikopunktzahl für die Bewertung kann sich ändern, wenn zusätzliche Informationen verfügbar werden. Verwenden Sie die Risikopunktzahl, um die potenziellen Auswirkungen der Ausnutzung zu bestimmen und Antwortprioritäten festzulegen.

Nachdem die Bewertung für eine Schwachstelle von Interesse erstellt und festgestellt wurde, dass sie ein Risiko für die Infrastruktur der Organisation darstellt, können Sie die Bedrohung weiter analysieren, indem Sie die Risikobewertung mit einer detaillierten Risikobewertung mit dem Softwareinstallationsbestand von aktualisieren Software Asset Management, Software Bill of Materials(SBOM) Bestand, vom Scanner gemeldete Schwachstellen und Configuration Management Database (CMDB). Betroffene Konfigurationselemente und Anwendungen werden automatisch durch die Bewertung identifiziert. Zusätzliche betroffene Elemente können manuell hinzugefügt werden.

Sobald die Bewertung abgeschlossen ist, können angreifbare Elemente oder angreifbare Anwendungselemente für die Risikoergebnisse erstellt werden, denen noch kein angreifbares Element zugeordnet ist. Der Risikopunktzahlrechner von angreifbaren Elementen kann genutzt/konfiguriert werden, um die Risikopunktzahl für angreifbare Elemente anzupassen, die mit Schwachstellenbewertungsdatensätzen verknüpft sind. Dem Schwachstellenbewertungsdatensatz können Risikostufe und Ereignispriorität zugewiesen werden. Basierend auf der Ereignispriorität kann der Vulnerability Event Manager die Schwachstellenbewertung vorschlagen, heraufstufen oder mit einem schwerwiegenden Security Incident verknüpfen.

Verwenden Management schwerwiegender Sicherheits-Incidents Um Korrekturaktivitäten nachzuverfolgen und zu verwalten, verknüpfen Sie laufende Security Incidents, erstellen Sie Ad-hoc-Aufgaben, binden Sie betroffene Teams ein, senden Sie Statusberichte, und arbeiten Sie mithilfe von Zusammenarbeitsintegrationen zusammen, die in verfügbar sind Management schwerwiegender Sicherheits-Incidents.

ServiceNow® Software Asset Management Und Software Bill of Materials(SBOM) Bewertung: Verarbeitungslogik

Mit Software Asset Management Daten, die CPEs, die von NVD für das CVE stammen, und dann die Discovery-Modelle werden mit der Zeichenfolgenübereinstimmungslogik abgerufen. Nach dem Abrufen der Discovery-Modelle wird ein Scan nach zugehörigen Installationen ausgeführt, die zugehörigen Konfigurationselemente werden abgerufen, und die Tabelle „Betroffenes Konfigurationselement“ wird ausgefüllt. Sie können weitere Details wie Herausgeber, Produkt, Version und Edition angeben. Basierend auf diesen werden alle übereinstimmenden Discovery-Modelle und die Softwareinstallationen für den Datensatz abgerufen. Anschließend werden die zugehörigen Konfigurationselemente abgerufen, und die Tabelle „Betroffenes Konfigurationselement“ wird neu ausgefüllt.

Für SBOM, Die zugeordnete Software für das CVE aus der zugehörigen Tabelle (m2m) (zwischen CVE und Software) wird abgerufen. Nach dem Abrufen der Softwaredetails werden die zugehörigen SBOM-Komponenten identifiziert, indem das Produkt und die Version aus der SBOM-Komponente mit dem Produkt und der Version der identifizierten Software abgeglichen werden.

Nachdem die zugeordneten Komponenten gefunden wurden, werden die Entitäten abgerufen, die sich auf die Komponenten beziehen. Das Produktmodell aus den Entitäten und das zugehörige CI (falls gefunden) werden abgerufen, und das Konfigurationselement wird in der Tabelle „Betroffenes Konfigurationselement“ gespeichert. Wenn das Konfigurationselement keine angreifbaren Elemente enthält, können Sie es verwenden, um das angreifbare Element zu erstellen. Wenn kein Konfigurationselement gefunden wird, wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

das Produktmodell in der Tabelle „Betroffenes Softwaremodell“ gespeichert und kann zum Erstellen angreifbarer Anwendungselemente verwendet werden.

Weitere Informationen zur Verwendung des Schwachstellen-Krisenmanagement-Workflows finden Sie unter Verwenden des Arbeitsbereichs „Schwachstellenbewertung“ .

Zugehörige Informationen

Schwachstellenbewertung erkunden

Arbeitsbereich für Schwachstellenbewertung kennenlernen

Registerkarte „Bewertung“

Domain Separation und Vulnerability Response

Die Domänentrennung wird in Vulnerability Response unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Standard

- Enthält alle Aspekte von **Standard** Level-Support.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

So funktioniert Domain Separation in Vulnerability Response

Mit der Domänentrennung können Sie VR standardisieren (Vulnerability Response) Verfahren für den gesamten Kundenstamm, den Sie bedienen, mit niedrigeren Betriebskosten und einer höheren Servicequalität.

Separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. stellen sicher, dass Kundendaten getrennt werden und niemals anderen Clients zugänglich gemacht werden.

Unterstützung der Domänentrennung in Vulnerability Response nach Versionsveröffentlichungen

Release	Supportstufe	Notizen
Orlando	Standard	
Paris	Standard	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützung der Domänentrennung in Vulnerability Response nach Versionsveröffentlichungen (Fortsetzung)

Release	Supportstufe	Notizen
Quebec	Standard	
Rom	Standard	
San Diego	Standard	
Tokio	Standard	
Utah	Standard	
Vancouver	Standard	
Waschtondc	Standard	

Domänentrennung für Vulnerability Response Die Anwendung deckt die folgenden Produktfunktionen ab:

- Erfasst die angreifbaren Elemente von Drittanbieterscannern (z. B. Qualys, Rapid 7 oder Tenable) in der richtigen Domäne. Die Daten werden in derselben Domäne erfasst wie der Integrationsanwender, dessen Anmeldeinformationen für die Integration verwendet werden.
- Scannt bestimmte Assets erneut von Vulnerability Response In der Domäne, von der sie angefordert wurde.
- Verwendet den CMDB-CI-Suchprozess, um sicherzustellen, dass die CI-Informationen aus den Scannern mit den CIs in der CMDB der Domäne des Integrationsanwenders übereinstimmen.
- Berechnet Risikopunktzahlen auf Ebene der angreifbaren Elemente gemäß dem Risikopunktzahlrechner, der in derselben Domäne wie der Integrationsanwender definiert ist.
- Korrekturzielregeln werden für angreifbare Elemente gemäß den Korrekturzielregeln ausgeführt, die in derselben Domäne wie der Integrationsanwender definiert sind.
- Regel(n) für Korrekturaufgaben können definiert werden und in derselben Domäne bleiben wie die Domäne des Integrationsanwenders.
- Korrekturaufgaben, die mit den Regeln für Korrekturaufgaben erstellt wurden, bleiben in derselben Domäne wie die Gruppenregeln.
- Der Zurückstellungsworkflow durchläuft den Genehmigungsprozess in derselben Domäne, für die die Zurückstellung angefordert wird.
- Berichte und Dashboards zeigen die status angreifbarer Elemente an, z. B. Alter des angreifbaren Elements, offene angreifbare Elemente nach CI, Schwachstellen nach Auswirkung und Status des Korrekturzieldatums in der Domäne, zu der es gehört.
- Wissen von Drittanbieterscannern oder der National Vulnerability Database (NVD) kann in der globalen Domäne erfasst werden, und Daten können über mehrere Clients hinweg freigegeben werden.

Hinweis:
In allen obigen Fällen gelten die übergreifenden Prinzipien der Sichtbarkeit in getrennten Domänen-Trennung in der NOW Platform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Erstellen und Unterstützen von domänengetrennten Importen finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration Und Erstellen und unterstützen Sie mehrere Domänen im Framework für Hintergrundaufträge.

Anwendungsfälle

Die Vulnerability Response Die Anwendung verwaltet den Lebenszyklus eines Schwachstellenelements von Ende bis Ende Die folgenden Anwendungsfälle sind auf Domänentrennung ausgerichtet:

- **Erfassen** Angreifbare Elemente (Schwachstellen in Asset) aus Ihrer Drittpartei-Integration.
  - Erfasst Daten aus mehreren Instanzen
  - Deduplizieren Sie das angreifbare Element
  - Mit CMDB-CI abgleichen
- **Ergänzung** Von angreifbaren Elementen mit Risikopunktzahlen und Korrekturzieldaten
  - Asset-Ergänzung (CMDB)
  - Ergänzung der Risikopunktzahl und des Korrekturzieldatums
- **Gruppe** Angreifbare Elemente und weisen Sie die Korrekturaufgabe zu
  - Gruppieren Sie die angreifbaren Elemente automatisch
  - Weisen Sie die Korrekturaufgabe automatisch zu
- **Beheben**
  - Korrekturaufgaben
  - Umfassender Korrekturlebenszyklus
  - Zurückstellungs-Workflow
- **Messen** Die Sicherheitslage der Organisation und das Schwachstellenmanagementprogramm
  - Schwachstellentrend, am stärksten angreifbares Asset, Schwachstelle nach Alter
  - Korrekturstatus bis zum Korrekturzieldatum

Setup

Domänentrennung für wird eingerichtet Vulnerability Response Erfordert keine zusätzlichen Schritte. Alle Vulnerability Response Tabellen beziehen die Domänenspalte, nachdem die Instanz domänengetrennt ist. Sie können Importdaten der Schwachstellenintegration an bestimmte Domänen weiterleiten. Weitere Informationen finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration.

Domänengetrennte Daten

Daten können domänengetrennt werden, was bedeutet:

- Angreifbares Element, das von Scannern von Drittparteien erfasst wird, bleibt in derselben Domäne wie die Domäne des Integrationsanwenders und ist von keiner anderen Domäne aus zugänglich.
- Schwachstellen, angreifbare Elemente (Instanzen) oder Assets in einer Domäne können nicht in anderen Domänen angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Risikobewertungsalgorithmus, die Regeln für Korrekturaufgaben und die Korrekturzielregeln können von niemandem außerhalb der Domäne angezeigt werden.
- Schwachstelleninformationen aus dem NVD können in der globalen Domäne vorhanden sein und für alle Kunden freigegeben werden.
- Korrekturaufgaben in einer Domäne können nicht in einer anderen Domäne angezeigt werden.
- In einer Domäne erstellte Zurückstellungs-Workflows sind in einer anderen Domäne nicht sichtbar.
- Alle E-Mail-Benachrichtigungen befinden sich in der Domäne, zu der sie gehören.

Hinweis:

Die in der Instanz verfügbaren geplanten Importvorlagen sind standardmäßig auf „Domäne: Global“ festgelegt. Um Konflikte zu vermeiden, wenn mehrere Domänen in Instanzen vorhanden sind, passen Sie die folgende Praxis an:

- Verteilen Sie die in der Instanz verfügbaren Importvorlagen auf die Anzahl der an der Integration beteiligten Domänen.
- Aktualisieren Sie die Domäne des Importvorlagendatensatzes auf die sys_ID der Zieldomäne.
- Erstellen Sie bei Bedarf Importvorlagen für jede Domäne.
- Stellen Sie sicher, dass jede Domäne über 2 Importvorlagen verfügt.
- sn_vul_sched_Import_Pool: Diese Tabellendatensätze müssen domänengetrennt sein, wenn Domänentrennung in der Instanz vorhanden ist

Wie Schwachstellenanalysten ihre eigenen Anwendungsdaten verwalten

- Analysten erstellen eigene Anwendungsinstallation, Verwaltung von Anwendungen mit mehreren Quellen und CI-Suchregeln.
- Analysten können bestimmte Integrationen ausschließlich für die Verwendung innerhalb der Domäne konfigurieren.
- Analysten können eigene Zurückstellungs- und Change-Management-Workflows erstellen.
- Analysten können eigene Regeln für Korrekturaufgaben und Risikobewertungslogik erstellen, um Schwachstellen genau zu priorisieren, Korrekturaufgaben automatisch zuzuweisen und der richtigen Zuweisungsgruppe zuzuweisen.
- Domänenanwender erstellen ein manuelles Schwachstellenelement und schließen das Element dann.

Geschäftslogik und Prozesse, die vom Instanzbesitzer domänengetrennt werden können

- Vulnerability Response Anwender und Gruppen
- Vulnerability Response-Integrationen
- Vollständige Setup-Konfiguration (Anwender- und Gruppenverwaltung, Anwendungsinstallation, Verwaltung von Anwendungen mit mehreren Quellen, CI-Suchregeln, Regeln für Korrekturaufgaben, Risikorechner, Korrekturzielregeln usw.)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schließen Sie den Korrekturlebenszyklus ab, einschließlich Zurückstellung
- Regelmäßige Aufgaben

Zugehörige Informationen

Domänentrennung für Service Provider

Service-Mapping in Vulnerability Response

Service-Mapping hilft Unternehmen, ein umfassendes Verständnis Ihrer IT-Infrastruktur und der Beziehungen zwischen verschiedenen Komponenten zu erhalten. Es ermöglicht die automatische Erkennung und Zuordnung von Services, Anwendungen und Infrastrukturkomponenten und bietet eine visuelle Darstellung der Abhängigkeiten und Beziehungen.

In Vulnerability Response, Die geplante Aufgabe *`Set related CI services`*Stellt Verbindungen zwischen den betroffenen Business-Services und den Konfigurationselementen (Configuration Items, CIs) her, die den angreifbaren Elementen (Vits) zugeordnet sind. Der Verknüpfungsprozess findet statt, sobald der Integrationsimport abgeschlossen ist, und zwar zu einem festgelegten Zeitpunkt. Um die Leistung dieser geplanten Aufgabe zu verbessern, wurden mehrere Changes implementiert, beginnend mit v21.1.2 von Vulnerability Response. Diese sind:

- Berechnung der Risikopunktzahl: Der Prozess zur Berechnung der Risikopunktzahlen umfasst die Nutzung von *`Set related CI services`*Geplante Aufgabe. Sobald das CI verarbeitet wurde, speichert dieser Auftrag die erforderlichen Daten in der Tabelle „zugehörige Services“ [sn_vul_m2m_ci_Services]. Zuvor in Konfigurations-Compliance, Risikoberechnung, bei der direkt auf zugegriffen wird Configuration Management Database (CMDB) Anwendungsprogrammierschnittstelle (API) *`CIUtils`* Dient zum Abrufen von Services für jedes Testergebnis während des Imports. Der aktuelle Prozess basiert jedoch auf der Ausgabe der geplanten Aufgabe aus der Tabelle „zugehörige Services“ [sn_vul_m2m_ci_Services], um die Risikopunktzahl in zu berechnen Konfigurations-Compliance. Darüber hinaus wurde der Basissystemrechner geändert, um die Tabelle „zugehörige Services“ [sn_vul_m2m_ci_Services] zu verwenden.
- Größe der Services: Der Servicewert in der Systemeigenschaft *`sn_sec_cmn.services_affected_by_CI_max_size`*, Die sich auf bezieht *`Set related CI services`*Die geplante Aufgabe wird von 1000 auf 500 verringert.
- Tiefe der Services: Die Tiefe in der Systemeigenschaft *`sn_sec_cmn.services_affected_by_CI_max_depth`*, Die sich auf bezieht *`Set related CI services`*Die geplante Aufgabe wird von 10 auf 5 reduziert. Der Servicewert wird ebenfalls von 1000 auf 500 verringert.
- Ausschluss von CMDB Klassen: Eine Systemeigenschaft *`sn_sec_cmn.ignoreCIClassForService`*Wurde eingeführt, um die Konfiguration von zu aktivieren CMDB Klassen, für die die Serviceberechnung übersprungen werden soll. Im -Basissystem ist diese Eigenschaft für festgelegt *`cmdb_ci_Unclassed_Hardware`* , *`cmdb_ci_Inclusive_ip`* , *`sn_sec_cmn_Unmatched_ci`* Da diese Klassen von erstellt werden Vulnerability Response Und haben möglicherweise keine Servicezuordnung. Zuvor basierte die Serviceberechnung auf der VIT. Die Logik wurde jedoch geändert, um stattdessen das erkannte Element zu verwenden. Das erkannte Element wird verwendet, um den Service zu berechnen, der dann dem CI in derselben Tabelle zugeordnet wird.
- Geplante Aufgabe für die vollständige Aktualisierung von Services: Eine geplante Aufgabe bei Bedarf *`Full refresh-related CI services for VI`*, Wurde eingeführt, um eine vollständige Aktualisierung der Services durchzuführen. Wenn Sie ein Upgrade auf v21.0 von durchführen Vulnerability Response, *`Set related CI services`*Der Auftrag wird zuerst länger ausgeführt, da die Basistabelle erkannte Elemente anstelle angreifbarer Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwendet. Daher muss der Auftrag alle erkannten Elemente verarbeiten, die innerhalb der letzten 90 Tage gescannt wurden. Wenn Sie häufiger Service-Aktualisierungen benötigen, können Sie darüber hinaus wöchentliche regelmäßige Aktualisierungen planen oder eine vollständige Aktualisierung durchführen. Wenn Sie Aktivitäten ausgeführt haben, die zu Änderungen an den Services geführt haben, die Ihren CIs zugeordnet sind, und Sie möchten Vulnerability Response Um diese Änderungen widerzuspiegeln, können Sie die geplante Aufgabe bei Bedarf ausführen `Full refresh related CI services for VI`. Dieser Auftrag verwendet alle in den letzten 90 Tagen aufgezeichneten erkannten Elemente und aktualisiert die zugehörigen Services entsprechend.

Zugehörige Informationen

Service Mapping

CIUtils - Global

Vulnerability Response – Implementierung

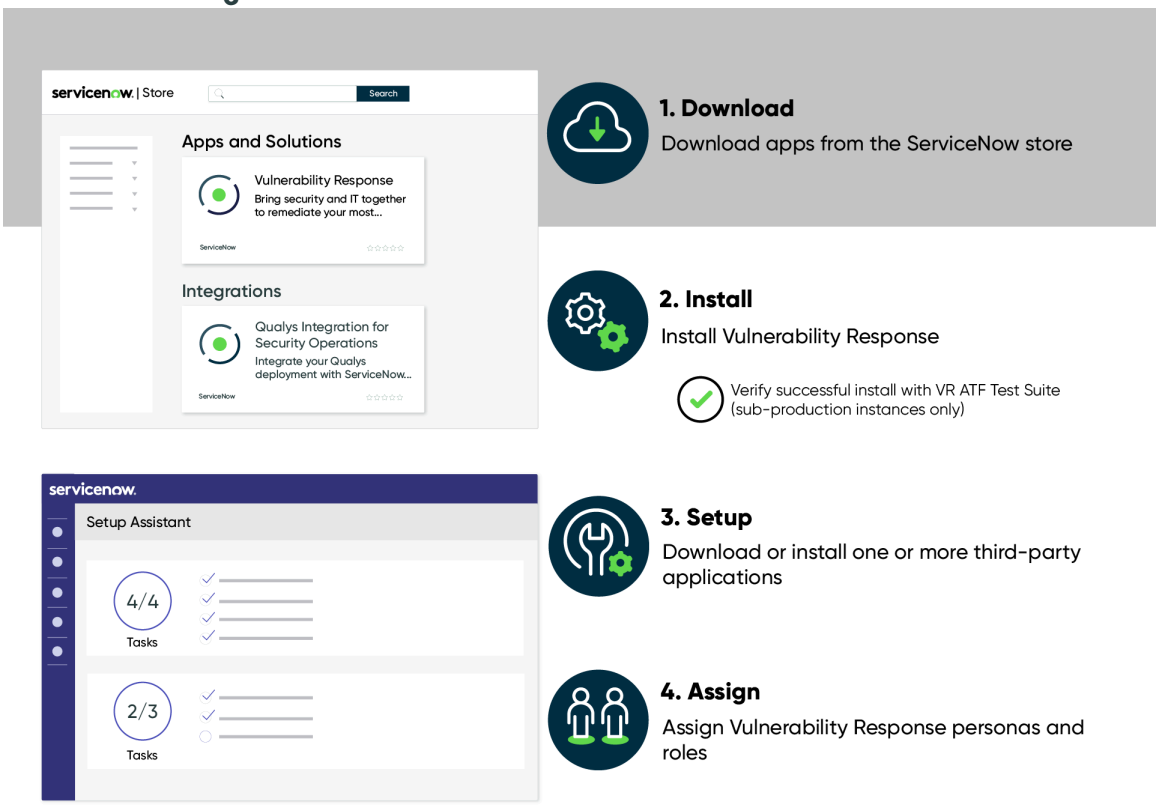
Verwenden Sie die in den folgenden Bildern dargestellten Schritte, um herunterzuladen Vulnerability Response Anwendung aus dem ServiceNow Store, Installieren Sie es auf Ihrem ServiceNow AI Platform® Instanz und konfigurieren Sie sie mit dem Setup-Assistenten.

Ein Installations- und Konfigurationsbeispiel für die Installation des Basissystems, des Vulnerability Response-Anwendung und eine Scanner-Anwendung einer Drittpartei, die Qualys Anwendung, wird in den folgenden Bildern dargestellt. Erforderliche Rollen und obligatorische Aufgaben sowie optionale Schritte werden ebenfalls aufgelistet.

- Weitere Informationen zu den einzelnen Schritten, die in den folgenden Bildern dargestellt sind, sowie eine Prüfliste mit Links zur Begleitdokumentation finden Sie unter Implementierungsprüfliste für Vulnerability Response Anwendung.
- Sie können die in diesem Beispiel dargestellten Konzepte und Schritte auf die Installation und Konfiguration anderer unterstützter Anwendungen für erweitern Vulnerability Response. Eine Liste der Support-Anwendungen finden Sie unter Installation von Vulnerability Response Und unterstützte Anwendungen.
- Zum Herunterladen und Installieren von ist die Administratorrolle erforderlich Vulnerability Response Anwendung und Qualys Für dieses Beispiel verwendete Schwachstellenanwendung.
- Die Administratorrolle weist auch die Persona „Schwachstellenadministrator“ [sn_vul.Vulnerability_admin] und andere zu Vulnerability Response Persona-Rollen für Anwender und Gruppen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Administratoraufgaben



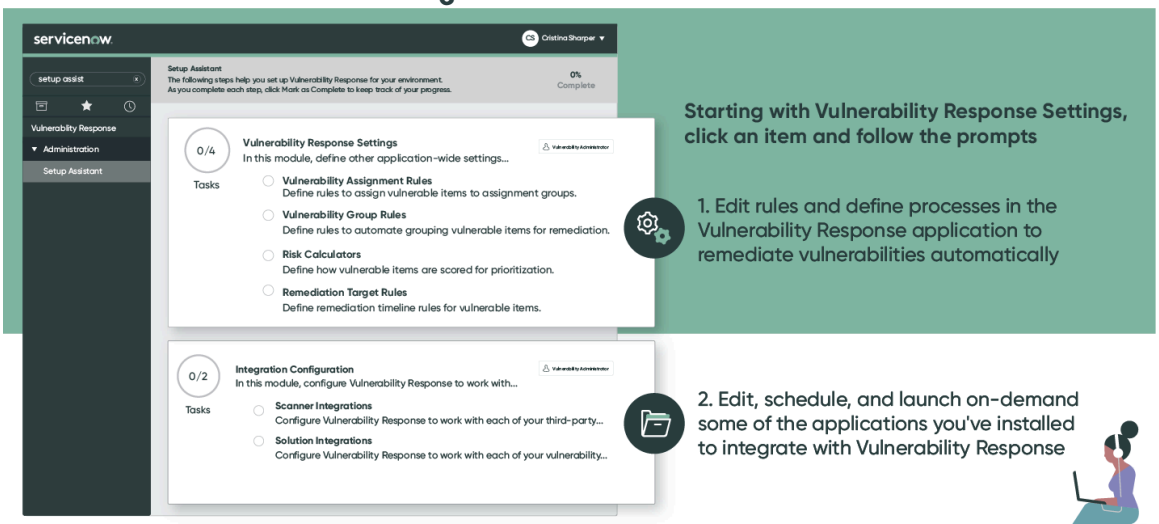
Die Rolle sn_vul.Vulnerability_admin konfiguriert Vulnerability Response Und Qualys Anwendungen im Setup-Assistenten und verifiziert die erwarteten Ergebnisse.

Befolgen Sie die Schritte und Aufforderungen im Setup-Assistenten, beginnend mit dem Abschnitt Einstellungen für Vulnerability Response, um mit der Installation und Konfiguration fortzufahren. Die Überprüfung dieser Einstellungen hilft Ihnen, die Prozesse von zu verstehen und zu verifizieren Vulnerability Response Während Sie mit der Einrichtung Ihrer Umgebung fortfahren.

Erforderliche Rolle: sn_vul.Vulnerability_admin oder alternativ admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellen-Administratoraufgaben



Roles required: sn_vul.vulnerability_admin or admin

Überprüfen Sie die Beschreibungen, Standardeinstellungen und Demodaten, die Sie mit den -Anwendungen installiert haben, in den folgenden Abschnitten:

- Zuweisungsregeln für Schwachstellen: Weisen Sie angreifbare Elemente (VIS) automatisch der entsprechenden Zuweisungsgruppe zu.
- Regeln für Korrekturaufgaben: Gruppieren angreifbare Elemente (VIS) automatisch, wenn sie basierend auf bestimmten Bedingungen importiert werden.
- Risikorechner: Standardrisikorechner ist aktiviert.
- Korrekturzielregeln: Definieren Sie Korrekturzeitlinien für VIS und Korrekturaufgaben (RTS).
- Überprüfen und bearbeiten Sie die Einstellungen für die von Ihnen installierten Drittanbieteranwendungen und installierten Lösungen, und definieren Sie Bedingungen für Ihre Datenimporte. Geben Sie Informationen zu Ihrem Drittpartei-Account ein, und konfigurieren Sie Importeinstellungen, Zeitpläne, Suchregeln für Konfigurationselemente (Configuration Item, CI) und andere Einstellungen.

Weitere Informationen finden Sie unter Implementierungsprüfliste für Vulnerability Response Anwendung.

Für zusätzliche Informationen zum Anpassen oder Implementieren von Vulnerability Response Anwendung, siehe KB1000704 .

Vulnerability Response installieren

Bevor Sie ausführen Vulnerability Response Anwendung in Ihrem ServiceNow AI Platform Instanz müssen Sie die Berechtigung abrufen und die Anwendung aus herunterladen ServiceNow Store, Installieren Sie es auf Ihrem ServiceNow AI Platform Und führen Sie einige Installationsschritte im Setup-Assistenten aus.

Vorbereitungen

Hinweis:

Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

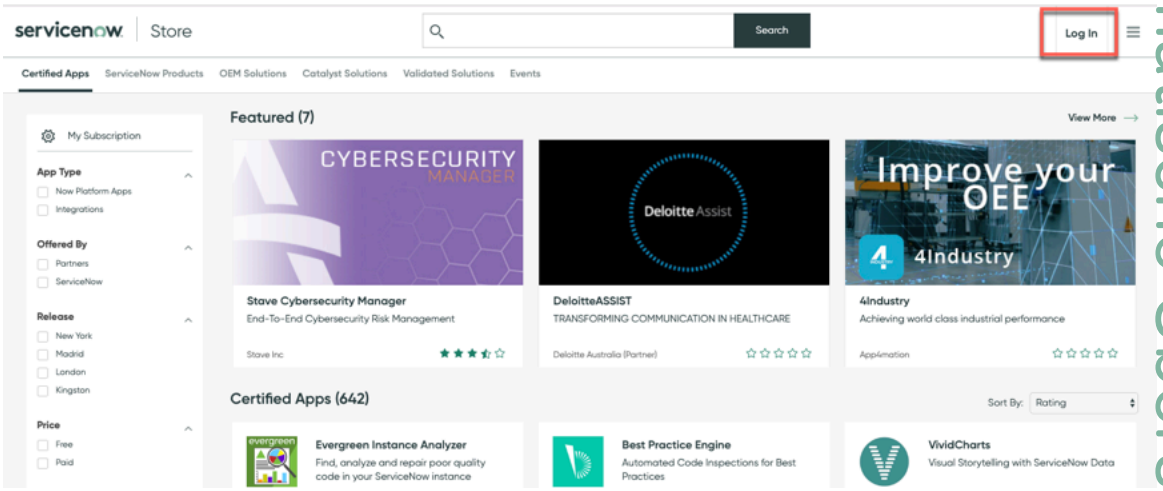
- Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen, die Ihrer Instanz zugewiesen sind.
- Die Administratorrolle ist für die Installation und Zuweisung von Rollen erforderlich.

Erforderliche Rolle: Administrator

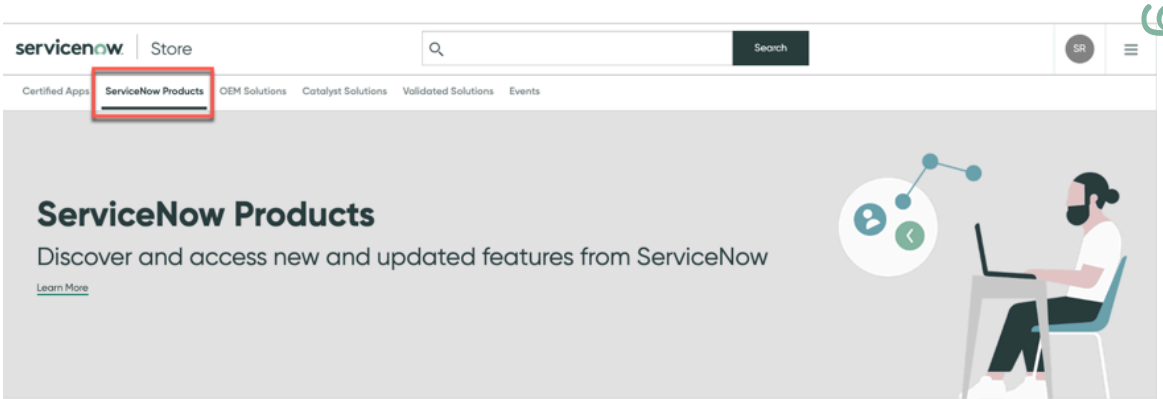
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Prozedur

1. Um die Berechtigung abzurufen und herunterzuladen Vulnerability Response Core-Anwendung navigieren Sie zu ServiceNow Store.
2. Klicken Sie oben rechts auf der Seite auf **Melden Sie Sich An** .



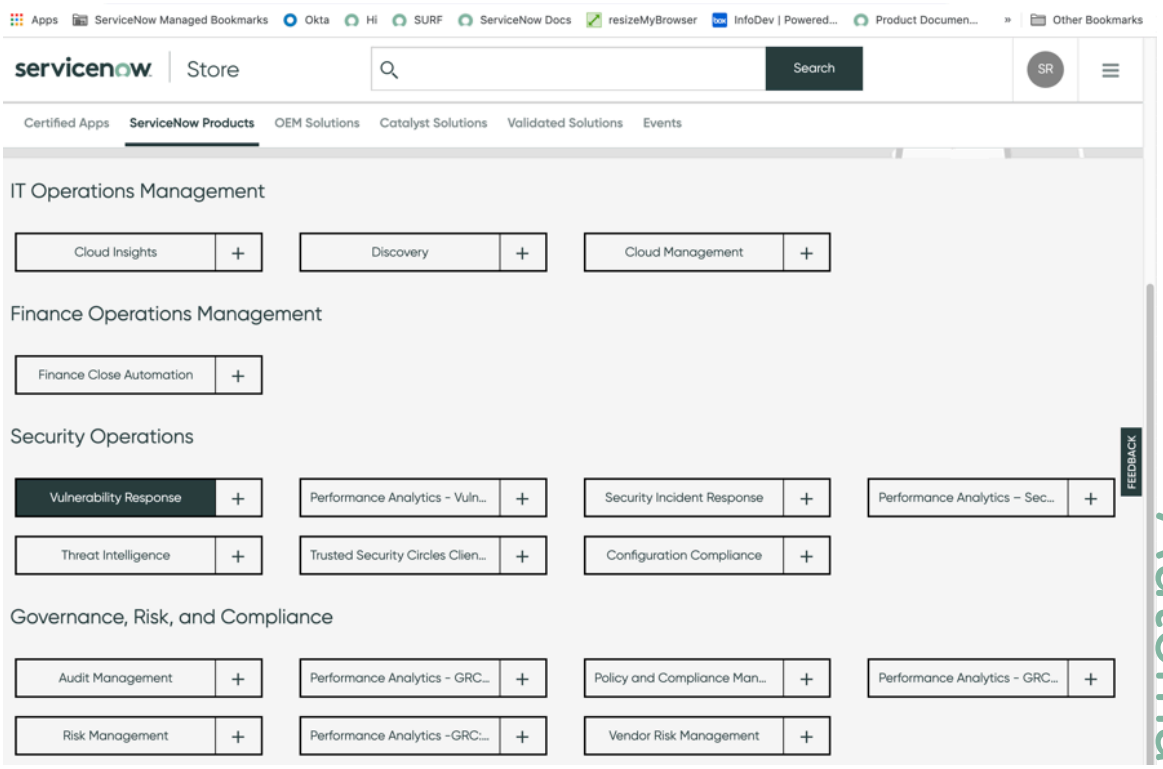
3. Geben Sie im angezeigten Dialogfeld Ihre HI-Anmeldeinformationen ein, und klicken Sie auf **Melden Sie Sich An** .
4. Klicken Sie auf der angezeigten Seite, wenn nicht ausgewählt, auf **ServiceNow-Produkte** Registerkarte.



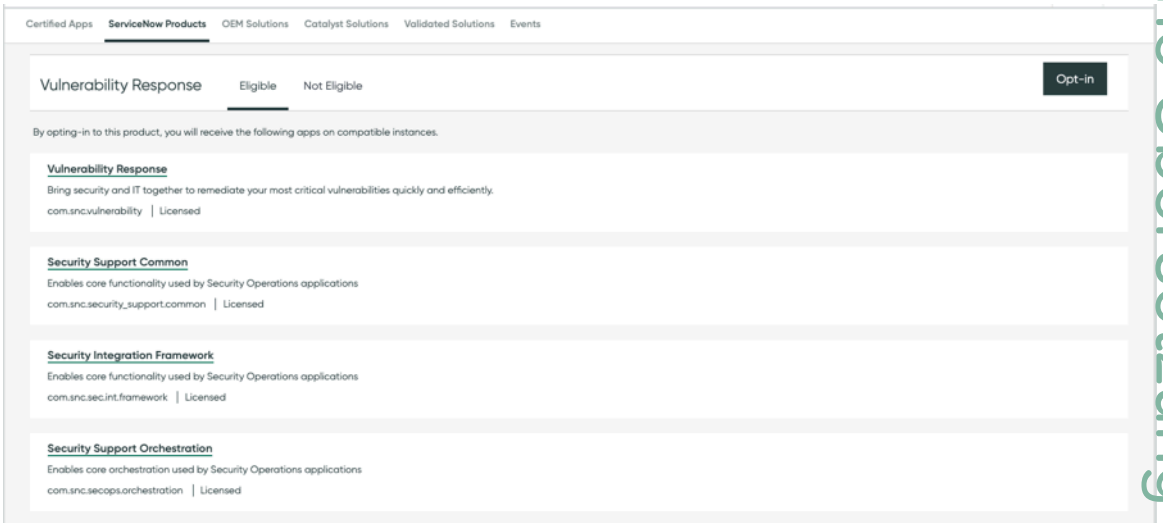
5. Um die zugehörigen Anwendungen anzuzeigen, für die Sie mit berechtigt sind Vulnerability Response Anwendung klicken Sie auf der Produktlistenseite auf **Vulnerability Response** Produkt.

Automatische Übersetzung

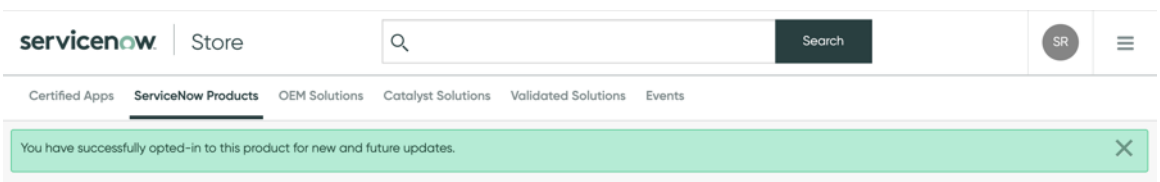
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Auf der Registerkarte „berechtigt“ werden alle Anwendungen aufgelistet, für die Sie berechtigt sind, wenn Sie sich anmelden. Klicken Sie auf einen Link, um weitere Informationen zu einer Anwendung zu erhalten.



6. Um abzurufen Vulnerability Response Core-Anwendung, klicken Sie auf **Aktivieren** .
7. Um den Nutzungsbedingungen zuzustimmen, aktivieren Sie bei der Aufforderung das Kontrollkästchen, und klicken Sie auf **Akzeptieren** .
   Eine Nachricht wird angezeigt, die angibt, dass Sie sich erfolgreich für die Anwendung angemeldet haben.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

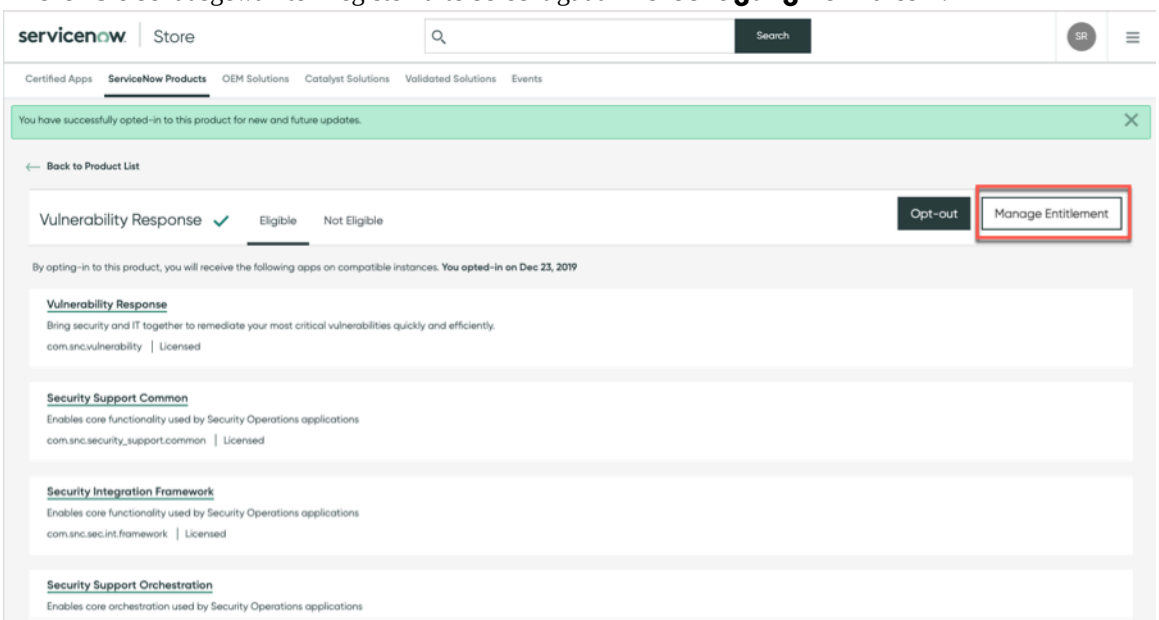
Mit ServiceNow Registerkarte „Produkte“ ausgewählt und angezeigt, ersetzt ein grünes Häkchen das Pluszeichen rechts neben Vulnerability Response Anwendung, wie in der folgenden Abbildung dargestellt.

Nachdem Sie die Nutzungsbedingungen und verwalteten Berechtigungen für eine der Anwendungen in akzeptiert haben **ServiceNow-Produkte** Registerkarte können Sie auf der Seite „Produktliste“ auf das Pluszeichen (+) klicken, um die Berechtigung zu erhalten und sich mit einem einzigen Klick für die anderen Anwendungen auf dieser Seite zu aktivieren.

8. Fahren Sie mit Schritt 10 fort, um die Anwendung auf Ihrem zu installieren ServiceNow AI Platform Instanz.
9. **Wahlweise:** Alternativ können Sie Ihre Berechtigung für verwalten Vulnerability Response Anwendung für andere ServiceNow AI Platform Führen Sie die folgenden Schritte aus.

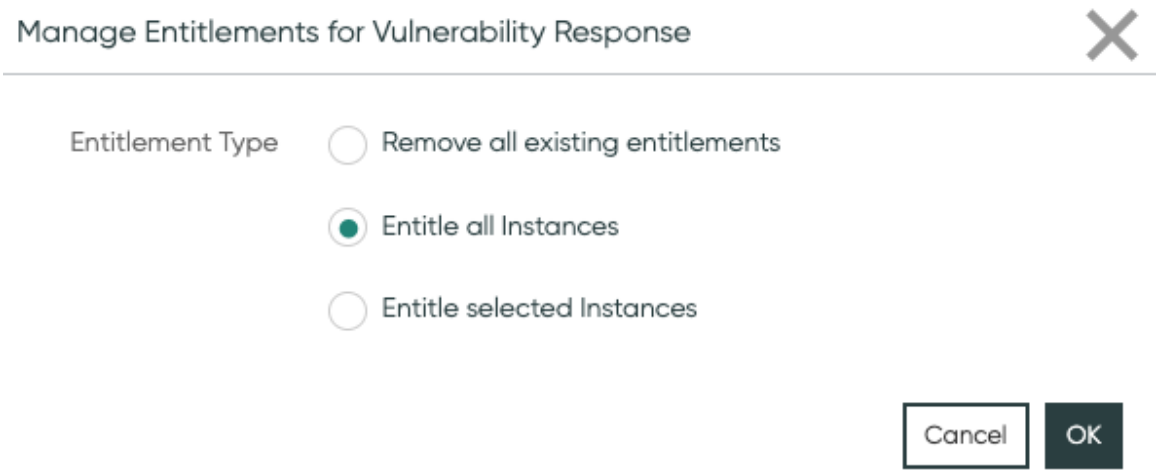
   a. Wenn die Schaltfläche Berechtigung verwalten nicht angezeigt wird, klicken Sie auf Vulnerability Response Anwendung in der Produktliste, um sie anzuzeigen.

   b. Klicken Sie bei ausgewählter Registerkarte berechtigt auf **Berechtigung Verwalten** .



   c. Wählen Sie im angezeigten Dialogfeld Berechtigungen für Vulnerability Response verwalten eine Option aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

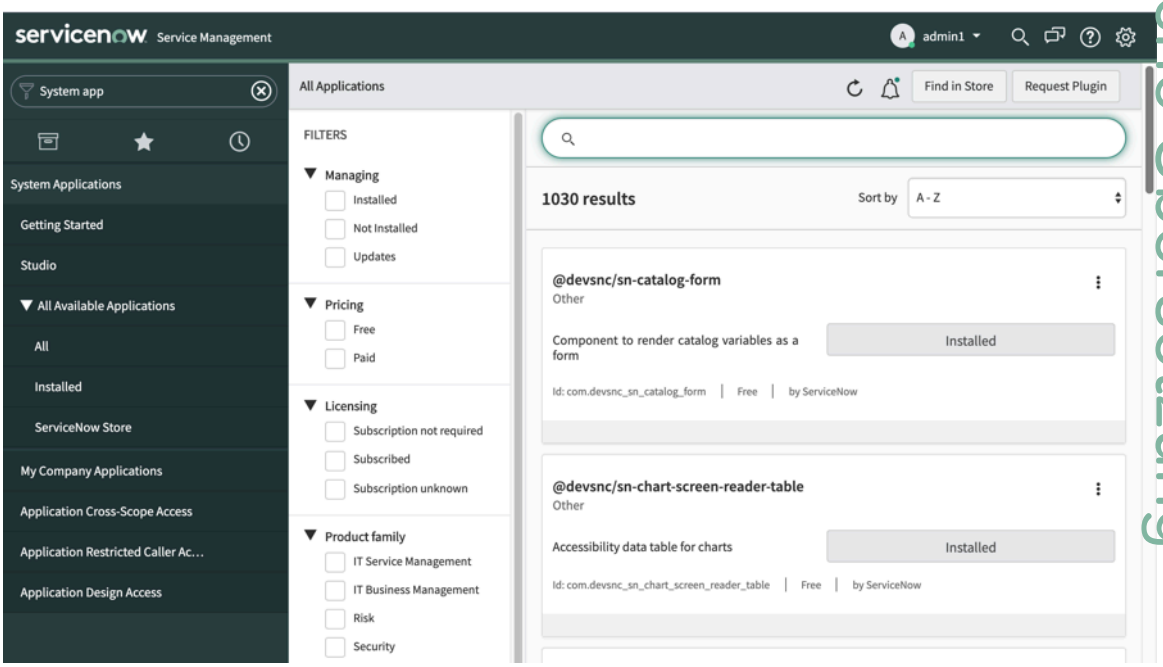


Automatische Übersetzung

d. Klicken Sie Auf **OK** Oder **Abbrechen** Um fortzufahren.
Sie sind bereit, Plugins zu aktivieren und die Anwendung auf Ihrem zu installieren ServiceNow AI Platform Instanz(n).

10. Melden Sie sich bei an ServiceNow AI Platform Instanz, die Sie installieren möchten Vulnerability Response Anwendung auf.

11. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.

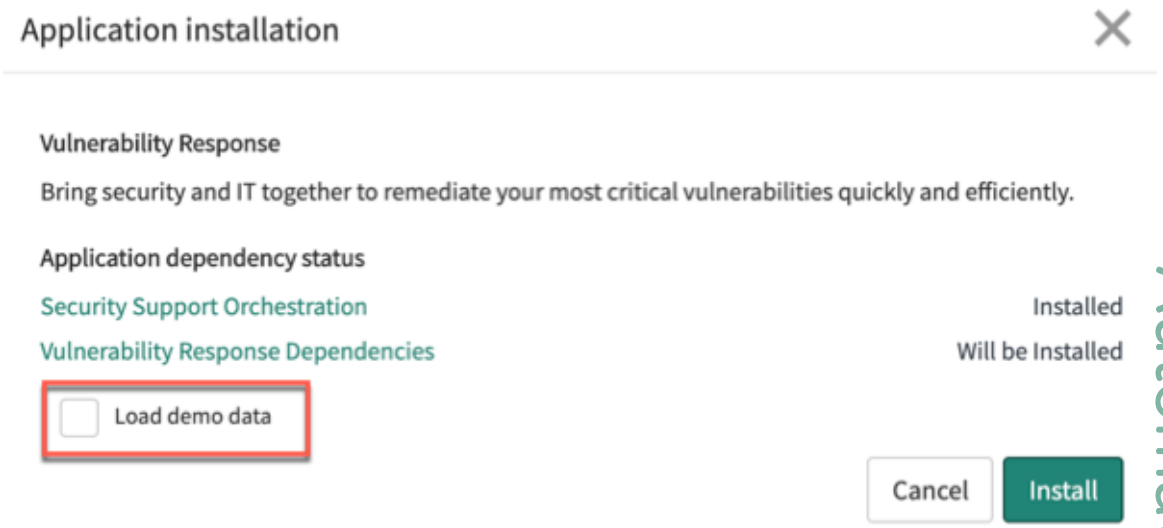


12. Suchen Sie in den aufgeführten Anwendungen die Anwendung Vulnerability Response (sn_vul), wählen Sie eine Version aus der Auswahlliste aus, und klicken Sie auf **Installieren** .
Das Dialogfeld Anwendungsinstallation wird angezeigt. Alle Abhängigkeiten, die installiert werden, werden angezeigt.

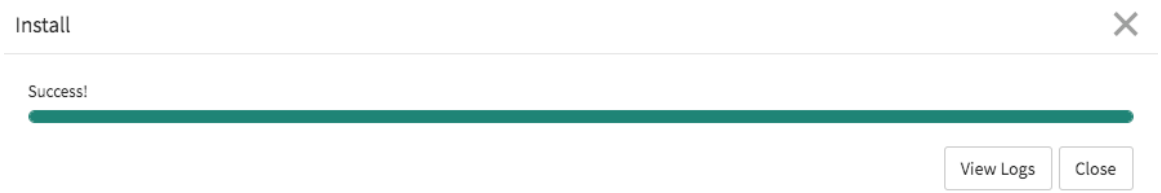
13. Wahlweise: Wenn Sie Demodaten möchten, aktivieren Sie das Kontrollkästchen Demodaten laden, und klicken Sie auf **Installieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie nicht auswählen **Demodaten laden** Kontrollkästchen, Demodaten sind nicht verfügbar, um von zu installieren **Anwendungsmanager** Später. Informationen zur Installation oder Neuinstallation von Demodaten nach der Erstinstallation finden Sie unter Problemumgehung zum Installieren von Demodaten, wenn die Anwendung bereits installiert ist [KB0722909] artikel in Now Support Knowledge Base.

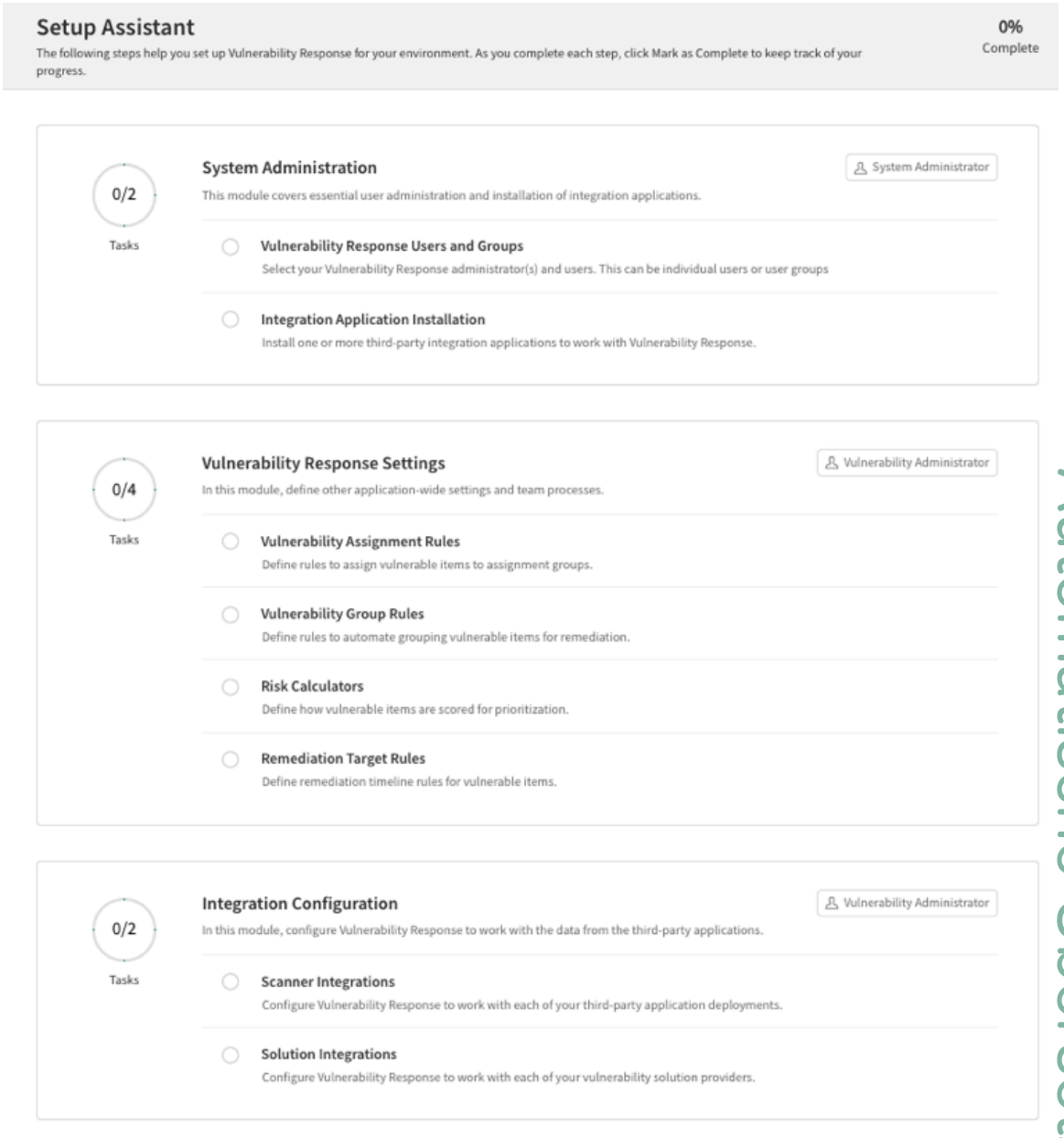


Diese Installation kann einige Zeit dauern. Nachdem die Anwendung erfolgreich installiert wurde, wird im Dialogfeld „Installieren“ eine Nachricht angezeigt.



14. Klicken Sie auf **Schließen**.
15. Nachdem die Installation erfolgreich abgeschlossen wurde, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



16. Befolgen Sie die Anweisungen in den Formularen in den einzelnen Abschnitten.

Nächste Maßnahme

Weitere Informationen zu finden Vulnerability Response Einstellungen, Installation von Anwendungen, Konfiguration, Integrationen, Gruppenregeln, Risikorechner und Korrekturzielregeln finden Sie unter Wird Konfiguriert Vulnerability Response Mit dem Setup-Assistenten.

Mit Vulnerability Response installierte Komponenten

Bei der Aktivierung der Anwendung Vulnerability Response werden mehrere Arten von Komponenten installiert, z. B. Tabellen, Benutzerrollen und regelmäßige Aufgaben.

Zeigen Sie gefilterte Listen für Komponenten an, die mit einer Anwendung installiert wurden

Ab v24.0.6 von Vulnerability Response, Die am häufigsten verwendeten Systemeigenschaften sind jetzt innerhalb von zugänglich Vulnerability Response Anwendung. Um

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

diese Systemeigenschaften anzuzeigen, navigieren Sie zu **Alle**Vulnerability Response**Eigenschaften**an.

Filtern Sie die Tabelle „Anwendungsdateien“ so, dass nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert werden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, sollte installiert werden, damit ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Führen Sie die folgenden Schritte aus, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im Filternavigator ein **sys_metadata.list** Um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) aus, und wählen Sie, **Anwendung** > **ist** Gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**an.
3. Wählen Sie im Bedingungsgenerator aus, um einen zweiten Filter hinzuzufügen **UND** , Und wählen Sie dann aus, **Klasse** > **ist ein** Und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle** , **Geplante Aufgabe** , Oder **Tabelle** .
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die von Ihnen ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

Installierte Rollen

Hinweis:
Rollen, geplante Aufgaben und Tabellen für Application Vulnerability Response Finden Sie in Mit Application Vulnerability Response installierte Komponenten.

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul_prisma.configure_prisma_Integration	Sichert die CRUD- + Report_View-Vorgänge in der Tabelle „sn_vul_prisma_Hosts_Import“ und den Vorgang „Report_View“ in der Tabelle „sn_vul_prisma_Host_attrb“.	
sn_vul.View_Manager_Workspace	Ansichten Arbeitsbereich des Schwachstellenmanagers.	
sn_vul.delete	Löscht Quelldatensätze Und angreifbare Elemente. Vor v23.0 hatte die Administratorrolle die Berechtigung zum Löschen der Quelldatensätze.	• sn_vul_cmn.delete • sn_vul.delete_vulnerable_items
sn_vul_cmn.delete	Löscht Quelldatensätze.	
sn_vulc.Bulk_Edit	Führt einen Massenbearbeitungsvorgang für Testergebnisse aus.	
sn_vul.App_Bulk_Edit	Führt einen Massenbearbeitungsvorgang für angreifbare Anwendungselemente (AVITs) aus.	sn_vul.App_write_all

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul_Container.Container_Bulk_Edit	Führt einen Massenbearbeitungsvorgang für angreifbare Container-Elemente (CVITs) aus.	sn_vul_Container.write_all
sn_vul_cisa.configure_Intelligence_Integration	Konfiguriert Intelligence-Integrationen.	
Schwachstellenmanager und Senior-Analysten [sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)]	Aktualisieren Sie Eigenschaften und Schwachstellenintegrationen. Die Rolle sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) ist für erforderlich Vulnerability Response Administration einschließlich Schwachstellenintegrationen, Regeln für Korrekturaufgaben, Rechner und Korrekturzielregeln und -Aufgaben, Berichte und Konfiguration der Drittpartei-Integration.	• sn_vul.vulnerability_write • sn_vul.ciso_write • sn_sec_cmn.admin • sn_vul_qualys.admin (wenn Qualy Vulnerability Integration installier ist.) • sn_vul_r7.admin (wenn Rapid7 Vulnerability Integration installier ist.) • sn_vul_shodan.admin (wenn die Shodan-Exploit-Integration instal ist.) • sn_vul.configure_nvd_Integration (wenn die NVD-Integrationen installiert sind.) • Treemap_admin (wenn die Performance Analytics-Anwendu installiert ist.)
Patch-Orchestration	Konfiguriert unterstützte Integrationen von Drittanbieter-Patch-Lieferanten. Zeigen Sie Patch-Daten und Patch-Datensätze an, und wenden Sie sie an.	• sn_vul_Patch_orch.configure_Pat Konfigurieren und wenden Sie Patches an. • sn_vul_Patch_orch.read_Patch Kann Patch-Datensätze und -Dat anzeigen. • sn_vul_bigfix.configure_Integratio Konfiguriert die Anwendung BigF Patch Orchestration Integration. Diese Rolle enthält die granularer Rollen sn_vul_bigfix.read_Integrat und connection_admin, die es dem Anwender ermöglichen, eine Verbindung zur BigFix-Konsole herzustellen. • sn_vul_sccm.configure_Integratio Diese Rolle enthält die granularer Rollen sn_vul_sccm.read_Integrat

Automatisierte Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
		und connection_admin, die es dem Anwender ermöglichen, eine Verbindung zur SCCM-Konsole herzustellen. • sn_vul_bigfix.read_Integration Benutzer mit dieser Rolle können die#Datensätze der Vulnerability Response- und der BigFix Patch Orchestration Integration-Anwendung und Patc Orchestration-Daten anzeigen (schreibgeschützt). • sn_vul_sccm.read_Integration Benutzer mit dieser Rolle können die#Datensätze der Vulnerability Response- und der Microsoft SCCM Patch Orchestration Integration-Anwendung und Patc Orchestration-Daten anzeigen (schreibgeschützt).
Schwachstellenanalysten [sn_vul.Vulnerability_write]	Die Rolle sn_vul.Vulnerability_write ist erforderlich, um Korrekturaufgaben und angreifbare Elemente zu verwalten und den Korrekturfortschritt zu überwachen.	• sn_vul.read_all • sn_sc_cmn.write • sn_vul_qualys.user (wenn Qualys Vulnerability Integration installier ist.) • sn_vul_shodan.write (wenn die Shodan-Exploit-Integration instal ist.)
V19.0: Vulnerability Event Manager [sn_vul_Analyst.vul_event_Manager]	Die Rolle sn_vul_Analyst.vul_event_Manager wird verwendet, um die Auswirkungen einer neuen Schwachstelle oder Software zu bewerten oder eine Zero-Day-Schwachstelle hinzuzufügen, um die betroffenen Assets zu identifizieren und angreifbare Elemente (VIS) zu erstellen.	• sn_sec_cmn.read • canvas_user • sn_vul_Analyst.Emergency_Respo • sn_vul.Manage_exposure_assess
Andere [sn_vul.read_all] Die Rolle „sn_vul.Vulnerability_read“ ist veraltet.	Die sn_vul.read_all Die Rolle ist für alle erforderlich, die Einblick in das Schwachstellenmanagement benötigen. Zum Beispiel IT- und Sicherheitsmanager oder jemand, der von Dashboards auf allgemeiner Ebene zu den Elementen, die die	• sn_sec_cmn.read • sn_vul_qualys.read (wenn Qualys Vulnerability Integration installier • sn_vul_shodan.read (wenn die Shodan-Exploit-Integration instal ist.)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Dashboard-Visuals enthalten, detailliert anzeigen möchte. **Wichtig:** Ab v24.0.6 von Vulnerability Response, Die Rolle „sn_vul.read_all“ hat die Berechtigung zum Zugriff auf Arbeitsbereich des Schwachstellenmanagers.	• pa_Viewer (wenn die Performanc Analytics-Anwendung installiert i • sn_vul_Tenable.read_Integration (wenn Tenable Vulnerability Integration installiert ist.) • sn_vul.View_Manager_Workspace
sn_vul.read_assigned	Zeigen Sie angreifbare Elemente an, die Ihnen oder Ihren Zuweisungsgruppen zugewiesen sind, sowohl in der klassischen Anwenderoberfläche als auch in Arbeitsbereich für IT-Korrekturen. **Wichtig:** Ab v24.0.6 von Vulnerability Response, Die Rolle „sn_vul.read_assigned“ hat die Berechtigung zum Zugriff auf Arbeitsbereich für IT-Korrekturen.	sn_vul.View_rem_Workspace
VR-Systemimport-Administrator [sn_vul.vr_Import_admin]	Systemausführung als Anwender. Führt geplante Aufgaben aus. **Hinweis:** Dieser Anwender ist der standardmäßige Ausführungsanwender für jeden Integrationsdatensatz. Nicht ändern.	• import_admin • sn_vul.vulnerability_write
Korrekturbesitzer [sn_vul.Remediation_owner]	Zeigen Sie Berechtigungen für angreifbare Elemente und Korrekturaufgaben an, die Ihnen oder Ihrer Gruppe zugewiesen sind, und aktualisieren Sie sie. Kann alle Schwachstellen und Lösungen anzeigen. Hat Schreibzugriff auf **Feld „interne Notizen“** Im Lösungsdatensatz.	Enthalten in der Rolle itil.
CISOs und Führungskräfte bei Schwachstellen [sn_vul.Vulnerability_ciso]	Zeigen Sie das CISO-Dashboard in Performance Analytics für Vulnerability Response an.	• sn_vul.ciso_read • sn_vul.read_all
Falsch positiver Genehmiger	Genehmigt/lehnt falsch positive Anforderungen ab.	sn_vul.View_Manager_Workspace

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
[sn_vul.false_positive_Approver]		
Ausnahmegenehmiger [sn_vul.Exception_Approver]	Genehmigt/lehnt Ausnahmeanforderungen ab.	sn_vul.View_Manager_Workspace

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
Füllen Sie gespeicherte OOTB-Filter für Host- und App-Modul aus	Migriert Module im Zusammenhang mit dem Host- und App-Modul.
Füllen Sie gespeicherte OOTB-Filter für das CC-Modul aus	Migriert Module im Zusammenhang mit dem CC-Modul.
Füllen Sie gespeicherte OOTB-Filter für das Containermodul aus	Migriert Module im Zusammenhang mit dem Containermodul.
Aktualisieren Sie hostbezogene gespeicherte Filter	Aktualisiert alle Zusammenfassungsdaten im Zusammenhang mit gespeicherten Filtern des Host-Moduls.
Aktualisieren Sie CC-bezogene gespeicherte Filter	Aktualisiert alle Zusammenfassungsdaten im Zusammenhang mit gespeicherten Filtern des CC-Moduls.
Aktualisieren Sie Container-bezogene gespeicherte Filter	Aktualisiert alle Zusammenfassungsdaten im Zusammenhang mit gespeicherten Filtern des Containermoduls.
Aktualisieren Sie App-bezogene gespeicherte Filter	Aktualisiert alle Zusammenfassungsdaten im Zusammenhang mit gespeicherten Filtern des App-Moduls.
Lösen Sie die Zusammenfassungserstellung und -Ausführung für den gespeicherten Filter aus	Erstellt, aktualisiert, führt die Zusammenfassungen im Zusammenhang mit dem gespeicherten Filter aus und aktualisiert sie.
Version 19,0 von Vulnerability Response und v4.0 der Veracode Vulnerability Integration	Die Veracode-CWE-Integration ruft ab Veracode– Spezifische CWE-Daten (Common Weakness Enumeration) für Bedrohungsinformationen und Korrekturempfehlungen. Die Veracode SBOM-Integration erfasst Release-, Version- und Schwachstelleninformationen, die aus stammen VeracodeÜber die Komponenten in Ihren Softwareprojekten. Die Integration generiert SBOMs im CycloneDx-JSON-Format und lädt sie in Ihre Instanz hoch Veracode-Kategorieintegration ruft erweiterte Kategoriedaten von ab Veracode. Die Veracode Mit der DevOps-Integration können DevOps-Anwender Zusammenfassungsdetails für Schwachstellen-Scans von Drittanbietern ohne SecOps-Lizenz anzeigen. JSON-basierte APIs für die folgenden Veracode-Integrationen: Angreifbares Anwendungselement, Scan-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
	Zusammenfassung, Anwendungsliste. Die XML-basierten API-Versionen dieser Integrationen sind veraltet.
Ordnen Sie vorhandene VIS der automatischen Ausnahmeregel zu	Ordnet die automatische Ausnahmeregel automatisch vorhandenen VIS zu.
Angreifbare Erkennungen Automatisch Schließen	Schließt die veralteten angreifbaren Erkennungen automatisch basierend auf der in der Tabelle „sn_vul_Auto_close_config“ definierten Konfiguration.
Version 16.1: Integrationen von HCL BigFix Collection, Fixlet und Aktionen.	Verwalten Sie Patches und Patch-Bereitstellungen für Schwachstellen mit Patches aus dem HCL BigFix-Produkt.
Berechnen Sie zugehörige Anzahlen für alle Lösungen	Standardmäßig inaktiv. Verarbeitet Lösungsdaten einmal pro Nacht anstatt kontinuierlich. Ab v22.0 können Sie diesen Auftrag nur bei Bedarf ausführen. Da diese geplante Aufgabe alle Lösungen verarbeitet, kann sie sich auf die Leistung auswirken. Daher wird empfohlen, diesen Auftrag nur einmal auszuführen, wenn die Lösungsdaten beschädigt sind.
Berechnen Sie die zugehörigen VI-Anzahlen für Schwachstellen- und Korrekturaufgaben	Erfasst manuelle und VI-Importänderungen für den Tag. Gleicht Schwachstellen- und Lösungsbeziehungen ab und berechnet die Gesamtwerte neu. Lösungsdaten werden separat von in die Warteschlange gestellt und verarbeitet **Warteschlange Für Metriken Der Schwachstellenlösung Verarbeiten** Geplante Aufgabe.
Überprüfen Sie Die Mid-Server-Zeitüberschreitung	Pingt den MID-Server an, und Fehler werden nach 30 Sekunden ausgegeben.
V19.0: Überprüfen Sie das potenzielle Schwachstellenrisiko	Verarbeitet die Delta-CVEs, Software und Installationen, um das Risiko zu ermitteln.
Überprüfen Sie den Ausführungsstatus „Warten abgeschlossen“	Markiert eine Integrationsausführung als abgeschlossen, sobald sie als vollständig abgeschlossen verifiziert wurde.
Überprüfen Sie den Ablauf der Zurückstellung für angreifbare Elemente und Gruppen	Sendet Benachrichtigungen, wenn angreifbare Elemente oder Schwachstellen abgelaufen sind (und wenn sie in einer Woche ablaufen). Überprüft, ob eine Ausnahmeregel für ein zurückgestelltes VI gilt, und aktualisiert den **Grund** Und **Bis** Felder gemäß der Ausnahmeregel. Der Status des VI bleibt bis zum letzten Ablaufdatum zurückgestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
Schließen Sie Abbruch-Vits, denen kein CI zugeordnet ist	Schließt automatisch angreifbare Elemente, denen kein Konfigurationselement (Configuration Item, CI) zugeordnet ist und die seit drei Tagen nicht aktualisiert wurden. Der Status ist auf „Geschlossen“/„Abgebrochen“ festgelegt.
Schließen Sie VI beim Löschen des Exp-Datensatzes	Schließt ein VI, wenn es gelöscht wird.
Integration Von Compliance-Ergebnissen	Importiert Testergebnisse zusammen mit Richtlinien, Konfigurationstests (Steuerungen) und Zitaten mit autorisierenden Quellen zur Verarbeitung in der Configuration Compliance-Anwendung.
Integration Der Compliance-Ergebnisse Im Backfill	Teil einer verketteten Integrationsausführung mit Tenable.io Asset-Integration: Importiert Konfigurationsbewertungsdaten für ignorierte Assets, die erkannt werden (importiert durch Asset-Integration).
CR-Statussynchronisierung	Das Skript passt alle vorhandenen Korrekturaufgaben in CHG-Beziehungen zurück, sodass sie synchronisiert werden. Aktiviert die Synchronisierung in Zukunft.
Version 15,0 Integration Von Scan-Anmeldeinformationen	Importiert und speichert vorübergehend sicher Tenable.io Anmeldeinformationen, die für den Zugriff auf den Scanner für erneutes Scannen bei Bedarf verwendet werden.
CWE – umfassende 2000-Integration	Schwachstellenintegration, die Schwachstelleninformationen aus dem von der MITRE Corporation kuratierten CWE-Datensatz (Common Weekness Enumeration) abruft.
V18.0: Veraltete Teilungsaktionsdatensätze löschen	Tägliche Aufgabe zum Bereinigen veralteter Datensätze in Zwischentabellen für geteilte Aufgaben.
Deaktivieren Sie VR-Lösungen, wenn die Anwendung „Lösungen“ nicht aktiv ist	Deaktiviert und blendet aus Vulnerability Solution Management Funktion, wenn Solution Management for Vulnerability Response Anwendung ist nicht installiert.
Bewerten Sie Korrekturziele	Legt Korrekturzieldaten für alle angreifbaren Elemente fest oder aktualisiert sie. Bestimmt den Status von Korrekturzieldaten anhand von Regeln.
• Die Erkennungen für den aktualisierten Schlüssel für Rapid7 werden korrigiert • Die Erkennungen für den aktualisierten Schlüssel für Qualys werden korrigiert • Die Erkennungen für den aktualisierten Schlüssel für Tenable werden korrigiert	Bereinigt Erkennungsdaten automatisch durch eine integrationsspezifische geplante Aufgabe, die nach dem Upgrade auf ausgelöst wird Vulnerability Response.
Version 16.1: Nachbesserungs-Digest generieren	Dieser Auftrag generiert automatisch einen E-Mail-Digest für alle Anwender in der Anwendergruppe „Korrekturbesitzer“. Der Auftrag ist standardmäßig aktiviert.
V19.0: Ausgenutztes CISA-CVE in Risikokonfiguration einfügen	Fügt CISA-CVEs in die Tabelle „Risikokonfiguration“ ein, um das Risiko zu berechnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
V18.0: Fügen Sie klassische Korrekturaufgaben in die einheitliche Korrekturaufgabe ein	Einmalige geplante Aufgabe zum Einfügen aller in der klassischen Anwenderoberfläche erstellten Korrekturaufgaben in die einheitliche Korrekturaufgabe (sn_vul_Remediation_Task).
Integration der Microsoft Security Response Center-Lösung	Vulnerability Solution Management Integration, die Lösungen aus dem abruft Microsoft Security Response Center.
Version 16.1: Microsoft SCCM-Sammlungs-, Patch-Update- und Bereitstellungsintegrationen	Verwalten Sie Patches und Patch-Bereitstellungen für Schwachstellen mit Microsoft SCCM-Patches.
Gedrosselten Integrationsprozess aufnehmen	Erstellt den Integrationsprozess für Shodan Exploit-Integration.
Füllen Sie den Text „betroffene Produkte“ aus	Nach dem Upgrade verarbeitet vorhandene Lösungen, um den Text für betroffene Produkte auszufüllen. Dieser Auftrag wird nur einmal ausgeführt.
Füllen Sie die neue Spalte „CR-Anzahl“ aus	Füllt die neue Spalte „CR-Anzahl“ für Kunden automatisch mit vorhandenen Daten in der Tabelle „Korrekturaufgabe“ [sn_vul_Vulnerability] aus.
Warteschlange Für Metriken Der Schwachstellenlösung Verarbeiten	Verarbeitet die Lösungsdaten in der Warteschlange nach: • Rollup von Lösungen aus NVD-Einträgen zu Drittparteieinträgen • Bevorzugte Lösungen für Schwachstellen und werden ausgefüllt • Aktualisieren der Korrekturstatusmetriken für die Lösungen Darüber hinaus werden auch die Lösungen verarbeitet, die für Aktualisierungsstatus markiert sind. **Hinweis:** Wenn Sie nur verwenden Rapid7, Sie können diese geplante Aufgabe deaktivieren, um die Leistung zu verbessern.
Füllen Sie Datensätze in der Tabelle der Schwachstellen-Lieferantenzuordnung aus Füllen Sie Datensätze in der Tabelle der Schwachstellen-Lieferantenzuordnung für Rapid7-Schwachstellen aus	Fügt Datensätze für vorhandene Schwachstellen in die Zuordnungstabelle für Schwachstellen ein.
Öffnen Sie zurückgestellte Schwachstellengruppen erneut	Öffnet zurückgestellte erneut Korrekturaufgaben Wenn das Aufschubdatum verstrichen ist.
Wenden Sie alle Zuweisungsregeln für Schwachstellen erneut an	Wertet Zuweisungsregeln für alle neu aus **Öffnen** VIS.
Version 16.5: Anzahl der Neuzuweisungen für Zuweisungsregeln	Wird täglich ausgeführt und veröffentlicht die Gesamtzahl der VIS- und Korrekturaufgaben, die von dieser Funktion für eine bestimmte Zuweisungsregel nicht zugewiesen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
Red Hat Solution Integration	Vulnerability Solution Management Integration, die Lösungen aus dem abruft Red Hat Security Advisory.
V17.1: Aktualisieren und beheben Sie doppelte Vits bei Korrekturaufgabe	Sucht doppelte angreifbare Elemente für die Elemente in der Korrekturaufgabe mit „Duplikate VIS automatisch aktualisieren“ als aktiv.
Aktualisieren Sie zugeordnete angreifbare Elemente für regelbasierte Korrekturaufgabe ohne Korrekturaufgabe	Aktualisiert die Korrekturaufgabe mit angreifbaren Elementen, die den Kriterien „Filtergruppe“ und „Bedingungsgruppen“ entsprechen.
Reparieren Sie fehlerhafte angreifbare Elemente, die zuletzt geöffnet und geschlossen wurden	Repariert vorhandene UI-Daten, die durch zuvor behobene Fehler beschädigt wurden.
Rechner erneut ausführen	Wendet die Rechner erneut auf alle angreifbaren Elemente an, die vom Change betroffen sind. Dies löst eine Neuberechnung der kumulativen Risikopunktzahlen von aus Korrekturaufgabe S. **Hinweis:** Das erneute Ausführen von Rechnern kann je nach Umgebung eine lange Zeit dauern.
Wiederholen Sie Abgebrochene Integrationsimportsätze	Wiederholungen abgebrochener Integrationsimportsätze. Versucht 5 Mal erneut, bevor ein Fehler zurückgegeben wird.
Wiederholen Sie Integrationsprozesse	Versucht Integrationsprozesse erneut. Versucht 5 Mal erneut, bevor ein Fehler zurückgegeben wird.
Rollup der Werte angreifbarer Elemente zu Schwachstelle und Gruppe	Berechnet die Risikopunktzahl, die Anzahl der angreifbaren Elemente und den Korrekturzielstatus für Korrekturaufgaben , Mit dem Rollup-Rechner. **Hinweis:** Ab v23.0 von Vulnerability Response, Die geplante Aufgabe wird erweitert, um Hintergrundaufträge mit Multithreading-Fähigkeiten zu erstellen. Dieses Upgrade umfasst die Segmentierung des Auftrags in mehrere kleinere untergeordnete Aufträge, die entweder parallel oder gleichzeitig ausgeführt werden. Diese Änderung ermöglicht die gleichzeitige Verarbeitung mehrerer Datensätze, wodurch die Gesamtaufgabe erheblich beschleunigt wird.
Führen Sie den Schweregradrechner nach der Heraufstufung des vuln-Eintrags aus	Führt den Schweregradrechner aus, nachdem eine zuvor fehlende Schwachstelle mit ihrer Punktzahl und anderen Daten von einem Drittanbieter aktualisiert wurde, z. B. Qualys Cloud Platform, Rapid7 Nexpose.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
	Hinweis: Ab v25.0.3 von Vulnerability Response, Die geplante Aufgabe wird erweitert, um Hintergrundaufträge mit Multithreading-Fähigkeiten zu erstellen. Dieses Upgrade umfasst die Segmentierung des Auftrags in mehrere kleinere untergeordnete Aufträge, die entweder parallel oder gleichzeitig ausgeführt werden. Diese Änderung ermöglicht die gleichzeitige Verarbeitung mehrerer Datensätze, wodurch die Gesamtaufgabe erheblich beschleunigt wird.
V19.0: Risikobewertung für konfigurierte CVEs ausführen	Berechnet das Risiko für alle CVE-Datensätze in der Tabelle „Risikokonfiguration“.
V19.0: Softwarerisiko ausführen	Berechnet das Risiko für alle Softwaredatensätze in der Tabelle „Risikokonfiguration“.
Geplanter Datenquellenprozessor Für Schwachstellen	Überprüft die Importwarteschlange auf zu verarbeitende Einträge und weist basierend auf verfügbaren Ressourcen einen geplanten Importauftrag zu.
Geplante Bereinigung des Anhanges des Schwachstellenintegrationsprozesses	Entfernt Integrations-XML-Anhänge, sobald sie 14 Tage alt sind. Diese Aufbewahrungszeit kann nicht konfiguriert werden.
Zeitüberschreitungsprüfung für geplante Schwachstellenintegration	Bricht Integrationsausführungen ab, die über 60 Minuten dauern.
Legen Sie zugehörige CI-Services für VI fest	Sobald der Integrationsimport abgeschlossen ist, werden die betroffenen Business-Services zum angegebenen Zeitpunkt mit CIs verknüpft, die mit angreifbaren Elementen verbunden sind. Weitere Informationen finden Sie unter Service-Mapping in Vulnerability Response.
Legen Sie die Anzahl der Zurückstellungen fest	Erfasst, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Container-Element oder eine Korrekturaufgabe zurückgestellt wird.
Lösen Sie die nächste Integration aus	Löst die nächste Integration in einer verketteten Integrationsausführung aus.
Vorlagenintegration	Ein einzelner Vorlagendatensatz wird an gesendet Tenable.io Während des erneuten Scans.
Aktualisieren Sie Nicht Gruppierte Angreifbare Elemente	Bestimmt, ob sich ein angreifbares Element in einem r befindet Nachbesserungsaufgabe Und fügt sie hinzu oder entfernt sie aus **Nicht Gruppierte Angreifbare Elemente** Liste. **Hinweis:** Dieser Auftrag wird nach dem Upgrade ausgeführt und kann je nach Datensatz lange dauern.
Aktualisieren Sie Schwachstelle in VG	Aktualisiert **Schwachstelle** Feld in der Tabelle „Korrekturaufgabe“ (sn_vul_Vulnerabilty) nach dem Upgrade. Dieser Auftrag wird einmal ausgelöst und danach inaktiv.
Importvorlage Für Schwachstellen	Engine, die die Importwarteschlange verarbeitet. Einer von 10.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
Update Zum Alter Der Geschlossenen Schwachstellenantwort	Aktualisiert die Spalte „Alter geschlossen“ in der VI-Tabelle.
Anzahl der Vulnerability Response-CI	Berechnet die Anzahl der CIs, die in den letzten 30 Tagen von Drittanbieterscannern gescannt wurden.
Vulnerability Response-Risiko- und Korrekturstatus-Upgrade	Aktualisiert die Risikobewertung für Daten beim Upgrade.
V20.0: Ablauf der Risikominderung überprüfen	Überprüft, ob Ausgleichssteuerungen für ein angreifbares Element und eine Korrekturaufgabe abgelaufen sind. Wenn sie abgelaufen sind, wird die Risikopunktzahl auf die ursprüngliche Risikopunktzahl zurückgesetzt und eine E-Mail-Benachrichtigung gesendet, die angibt, dass die Ausgleichskontrollen abgelaufen sind. Sendet auch eine E-Mail-Benachrichtigung, wenn Ausgleichssteuerungen so festgelegt sind, dass sie innerhalb von 7 Tagen ablaufen.

Installierte Tabellen

Tabelle	Beschreibung
V24.0.6 Prisma-Hosts-Import [sn_vul_prisma_Hosts_Import]	Importsatztabelle für die Hosts.
V24.0.6 Prisma-Host-Attribute [sn_vul_prisma_Host_attrb]	Asset-Attributtabelle für Host-Integration.
V22.0 sn_vul_cmn_Auto_close_rule	Schließt veraltete Erkennungen automatisch basierend auf Filterbedingungen.
sn_vul_cmn_WS_saved_Filter	Speichert die Daten des gespeicherten Filters.
sn_vul_Lizenzierung_usage	Enthält das doppelte Asset, das unvollständige IP-Asset, die Gesamtzahl der Scanner-Assets und die endgültige Nutzung.
sn_vul_m2m_entry_Compensating_Control	Stellt die Zuordnung zwischen Schwachstelleneinträgen und Ausgleichssteuerungen dar.
V21.0 Rapid7-Scan-Engine [sn_vul_r7_Scan_Engine)	Speichern Sie die importierten Scan Engine-Daten für Datensätze, die für die Erkennung von Assets während eines Scans und die Überprüfung auf Schwachstellen verantwortlich sind.
V21.0 Import der Rapid7-Scan-Engine [sn_vul_r7_Scan_Engine_Import]	Wird von der Rapid7 Scan Engine-Integration verwendet, um Importdaten vor der Verarbeitung bereitzustellen.
Version 19.0:	Erweitert die Veracode-Kategorietabelle für CWE-Korrekturempfehlungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_vul_veracode_cwe_Import]	
Version 19.0: [sn_vul_veracode_category_Import]	Speichert importierte Kategoriedaten.
Version 19.0: [sn_vul_veracode_sbom_Import]	Speichert importierte SBOM-Daten, die aus Veracode stammen.
V17.1: Fügen Sie dem VI-Schlüssel einen Nachweis hinzu [sn_vul_Proof_key_Vulnerability]	Rapid7-Schwachstellen, für die der Nachweis im VI-Schlüssel enthalten sein muss. Ab v24.0.6 von Vulnerability Response, Wird die Spalte „Regulärer Ausdruck zum Teilen von Tenable-Vits“ hinzugefügt. Speichert den regulären Ausdruck, der von einem Anwender eingegeben wurde und zum Analysieren des Nachweises aus der Nutzlast verwendet wird.
Bewertete angreifbare Elemente [sn_vul_m2m_exp_SW_VI]	Weist während der Erstellung der Korrekturaufgabe einer Zuweisungsgruppe eine Korrekturaufgabe zu.
Zuweisungsregel [sn_vul_vgr_Assignation_rule]	Weist während der Erstellung der Korrekturaufgabe einer Zuweisungsgruppe eine Korrekturaufgabe zu. Vor v15.0: Weist einen zu Korrekturaufgabe An eine Zuweisungsgruppe während Korrekturaufgabe Erstellung.
Change-Anforderung zuordnen [sn_vul_action_Associate_cr]	Bereitstellungstabelle, die zum Verarbeiten neuer Zuordnungen von Korrekturaufgaben und CHG verwendet wird. Vor v15.0: Bereitstellungstabelle, die zum Verarbeiten neuer VG-CHG-Zuordnungen verwendet wird.
Asynchrone angreifbare Elemente Auftrag [sn_vul_async_VI_Job]	Enthält Hintergrundaufträge, die angreifbare Elemente verarbeiten. Es wird nur ein Auftragstyp unterstützt; wird verwendet, um Schwachstellen in Massenbearbeitung zu bearbeiten.
Auftragstyp Für Asynchrone Angreifbare Elemente [sn_vul_async_VI_Job_type]	Enthält die Typen von Hintergrundaufträgen und verweist auf das relevante Skript. Hat nur einen Prozessor, den **VulnerabilityBulkEditProcessor**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Veraltete Erkennungen automatisch schließen [sn_vul_Auto_close_config]	Speichert die Konfiguration, wie veraltete Erkennungen automatisch geschlossen werden.
Granularität angreifbarer Elemente konfigurieren [sn_vul_action_VI_granularity_config]	Speichert das UI-Formular, das zum Aktivieren oder Deaktivieren von „Port einschließen“ auf der Konfigurationsseite im Modul „VI-Granularität konfigurieren“ verwendet wird.
Change-Anforderung erstellen [sn_vul_action_create_cr]	Wird verwendet, um Change-Anforderungen aus der Korrekturaufgabe zu erstellen.
Angreifbare Elemente erstellen [sn_vul_action_create_VI]	Eine Bereitstellungstabelle, die als Platzhalter für Informationen verwendet wird. In dieser Tabelle werden keine Datensätze gespeichert.
Sammlung [sn_vul_Patch_orch_Collection]	Speichert Sammlungsdaten aus verschiedenen Instanzen.
CWE [sn_vul_cwe]	Katalog der Common Sach and Enumeration (CWE)-Software-Schwachstellen.
Anwendbare CWE-Plattform [sn_vul_cwe_m2m_cwe_Platform]	Enthält die importierten anwendbaren CWE-Plattformdaten.
CWE-Kategorie [sn_vul_cwe_category]	Enthält die importierten CWE-Kategoriedaten.
Häufige CWE-Konsequenz [sn_vul_cwe_consquence]	Enthält die importierten allgemeinen CWE-Konsequenzdaten.
Externe CWE-Referenz [sn_vul_cwe_reference]	Enthält die importierten externen CWE-Referenzdaten.
Beispiel für CWE-Beobachtung [sn_vul_m2m_cwe_cve]	Enthält die importierten CWE-CVE-Daten.
CWE-Plattform [sn_vul_cwe_Platform]	Enthält die importierten CWE-Plattformdaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Externe CWE-Referenz [sn_vul_cwe_reference]	Enthält die importierten CWE-bezogenen externen Referenzdaten.
CWE-Beziehung [sn_vul_m2m_cwe_Relation]	Enthält die importierten CWE-Beziehungsdaten.
CWE-Ansicht [sn_vul_cwe_View]	Enthält die importierten CWE-Ansichtsdaten.
CWE-Schwäche [sn_vul_cwe_schwächness]	Enthält die importierten CWE-Schwachstellendaten.
Version 16.1: Gerätesammlung [sn_vul_Patch_orch_m2m_src_ci_Collection]	Speichert Sammlungsdaten zu erkannten Elementen.
Version 16.1: Geräte-Update [sn_vul_Patch_orch_m2m_src_ci_Update]	Speichert Daten zu den bereitgestellten Patches zusammen mit dem Bereitstellungsstatus, die in erkannten Elementdatensätzen angezeigt werden.
Übereinstimmung Discovery-Modell verwundbare Softw [sn_vul_Discovery_model_Software_match]	Ergänzt den Abgleich von angreifbarer Software zu einem Discovery-Modell.
Konfiguration für Ausnahmeverwaltung [sn_vul_Exception_config]	Speichert die Konfigurationseinstellungen für die Ausnahmeverwaltungsfunktion.
Ausnahmeregel [sn_vul_Auto_Exception_rule]	Enthält den Satz von Regeln, die für das Ausnahmemanagement ausgewertet werden.
Exploit [sn_vul_Exploit]	Enthält die Definitionen von Exploits: Öffentlich verfügbarer Code, der eine Schwachstelle ausnutzt.
Exploit-Framework sn_vul_Exploit_Framework	Enthält die Namen von Exploit-Frameworks: Vollständige Softwarepakete, die viele Exploits ausführen können.
Verfügbar gemachte Discovery-Modelle [sn_vul_m2m_exp_SW_model]	Speichert die Zuordnung zwischen dem Discovery-Modell und Schwachstelle Risikobewertung.
Bewertung des Gefahrenpotenzials	Speichert die Datensätze für die Risikobewertung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_vul_exp_by_SW]	
V19.0: Risikomanifest sn_vul_Analyst_Exposure_Manifest	Manifesttabelle für Delta-Verarbeitung.
Einträge zum Gefahrenpotenzial von Schwachstellen [sn_vul_m2m_entry_exp]	Speichert die Zuordnung zwischen Schwachstelle (sn_vul_entry) und Risikobewertung.
Malware-Kit [sn_vul_Malware_Kit]	Enthält die Details von Malware-Kits: Vorgeschriebene Tools, mit denen ein Exploit oder eine Reihe zugehöriger Exploits ohne zusätzliche Codierungs- oder Konfigurationsarbeiten ausgeführt werden kann
Fehlende Asset-Tabelle [sn_vul_TENABLE_missing_Asset]	Enthält temporäre Asset-IDs für ignorierte Konfigurations-Compliance-Bewertungsdaten mit nicht abgeglichenen Assets.
Update der Microsoft Response Center-Lösung [sn_vul_msrc_Update]	Enthält den Zeitpunkt der letzten Aktualisierung der Lösungsdaten von Microsoft. Wird zum Vergleich mit dem nächtlichen Import verwendet, um die Delta-Daten für den Download zu bestimmen.
Microsoft Security Response Center Lösungsimport [sn_vul_msrc_Solution_Import]	Wird von der Integration der Microsoft Security Response Center-Lösung verwendet, um Importdaten vor der Verarbeitung bereitzustellen.
Integration der Microsoft Security Response Center-Lösung [sn_vul_msrc_Integration]	Erweitert die Tabelle „Schwachstellenintegration“ [sn_vul_Integration] für Integration der Microsoft Security Response Center-Lösung.
Nationale Verwundbarkeit – Datenbankeintrag [sn_vul_nvd_entry]	Dokumentierte Schwachstelle aus der NIST National Vulnerability Database.
NVD-CVSS-Import [sn_vul_nvd_cvss_Import]	Enthält Bereitstellungsdaten, die noch nicht in umgewandelt wurden Vulnerability Response Schema während des NVD-Imports.
Version 16,1 [sn_vul_Patch_orch.Patch_Approval_required]	Wenn Patch-Bereitstellungen über eine Patch-Integration geplant werden, werden Anforderungen zur Überprüfung und Genehmigung an Anwender übermittelt, die der Genehmigungsgruppe „Ebene 1 – Patch-Update“ zugewiesen sind. Diese Eigenschaft ist standardmäßig aktiviert.
Version 16.1: Patch-Bereitstellung [sn_vul_Patch_orch_Deployment]	Speichert Informationen zu bereitgestellten Patches zu Sammlungen und CIs.
Version 16.1: Patch-Update [sn_vul_Patch_orch_Update]	Speichert Informationen zu den Patches, die in verschiedenen Instanzen verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Version 16.1: Potenzieller Patch [sn_vul_Patch_orch_m2m_vuln_Patch]	Speichert Daten zu Patches und Schwachstellen, die die Patches identifizieren, die zur Behebung einer Schwachstelle verwendet werden können.
V19.0: Potenzielles Schwachstellenrisiko sn_vul_Analyst_m2m_POT_exp_SW_model	Risikobewertungstabelle für CVE.
Produktkategorie [sn_vul_Product_category]	Enthält die importierten Produktkategoriedaten.
Red Hat Security Advisory [sn_vul_rhsa_Update]	Vergleicht Red Hat Lösungen für den nächtlichen Auftrag zur Bestimmung der Delta-Daten für den Import.
Red Hat Lösungsimporte [sn_vul_rh_Solution_Import]	Verwendet von Red Hat Solution Integration Dient zum Bereitstellen von Importdaten vor der Verarbeitung.
Red Hat Solution Integration [sn_vul_rh_Integration]	Erweitert die Tabelle „Schwachstellenintegration“ [sn_vul_Integration] für Red Hat Solution Integration.
Zugehörige Business-Services [sn_vul_m2m_ci_Services]	Verknüpft CIs mit Business-Services für die Suche nach betroffenen Services. Enthält eine Kennzeichnung, die angibt, ob sie von Service-Mapping hinzugefügt wurde.
V18.0: Anzahl der Korrekturmaßnahmen [sn_vul_Daily_count_re]	Tägliche Anzahl der Korrekturmaßnahmen. Diese Tabelle wird täglich aktualisiert.
V18.0: Datensatz für Korrekturmaßnahme [sn_vul_Remediation_effort_Record]	Verfolgt den Korrekturfortschritt für Korrekturmaßnahmen (RE). Enthält Verweise auf RES.
Korrekturzielregel [sn_vul_ttr_rule]	Definiert den erwarteten Zeitrahmen für die Korrektur eines angreifbaren Elements. Erweitert Die Anwendungsdatei.
V18.0: Korrekturaufgabe [sn_vul_Remediation_Task]	Speichert alle Korrekturaufgaben für VR-, AVR-, CVR- und Testergebnisgruppen. Besteht aus Informationen im Zusammenhang mit [sn_vul_Vulnerability]-Tabellendatensätzen. Anwender, die keine Datensätze in der Tabellenlistenansicht [sn_vul_Vulnerability] anzeigen können, können diese Datensatzinformationen in der Tabellenlistenansicht [sn_vul_Remediation_Task] anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
	Diese Tabelle ist für Anwender im Vulnerability Manager-Arbeitsbereich oder im IT-Korrekturarbeitsbereich zugänglich
REST-Integration [sn_vul_Rest_Integration]	Erweitert die Tabelle „Schwachstellenintegration“ [sn_vul_Integration] für die REST-basierten Integrationen.
SAM-NVD-Schwachstellenerkennung [sn_vul_sam_config]	Enthält, welche CI und Schwachstellen mit SAM NVD überwacht werden und ob die SAM NVD-Schwachstellenerkennung aktiviert ist oder nicht.
Geplanter Importpool [sn_vul_sched_Import_Pool]	Sammlung von Datensätzen für geplante Importsätze, die verwendet werden, um gleichzeitige Datenquellenimporte zu erleichtern.
Wählen Sie Angreifbares Element Aus [sn_vul_action_select_VI]	Basis-Bereitstellungstabelle, die zur Verarbeitung von aufgeteilten VG, zum Erstellen von CHG und zum Zuordnen von CHG verwendet wird
Setup-Status [sn_vul_Setup_Status]	Nur intern: Wird vom Setup-Assistenten verwendet. Wenn der Setup-Assistent geöffnet wird, wird der Status der abgeschlossenen Schritte angezeigt, und der Prozentsatz in der rechten oberen Ecke stammt aus dieser Tabelle.
Schweregradzuordnung [sn_vul_severity_Map]	Enthält die Zuordnungen vom Quellschweregrad zum normalisierten Schweregrad.
Zuordnung für Lösungsscanner [sn_vul_Solution_Scanner_Mapping]	Ordnet Lieferanten, Scanner und Stichwörter für Ausschluss oder Aufnahme zu.
Teilen Korrekturaufgabe [sn_vul_action_Split_vg]	Bereitstellungstabelle, die zum Teilen verwendet wird Korrekturaufgaben .
Eintrag für Drittpartei-Schwachstelle [sn_vul_third_Party_entry]	Dokumentierte Schwachstelle aus einer Drittparteiquelle.
[sn_vul_Tenable_io_template	Ein Vorlagendatensatz wird an gesendet Tenable.io Und während des erneuten Scans für Elemente importiert, die haben Tenable.io Als Quelle.
Manifest aktualisieren [sn_vul_Update_Manifest]	Liste von Korrekturaufgaben Die aktualisiert wurden und eine Neuberechnung durch den Rollup-Rechner erfordern.
V17.1: Nutzung nach CI-Klassen [sn_vul_Licensing_usage_by_ci_classes]	Enthält die von der CI-Klasse aggregierte Nutzungsanzahl.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Anzahl der VR-Konfigurationselemente [sn_vul_vr_Configuration_item_count]	Enthält den gleitenden kumulativen 90-Tage-Durchschnitt der Konfigurationselemente, die aus Drittpartei-Integrationen importiert wurden.
Zuweisungsregel für Schwachstellen [sn_vul_assignment_rule]	Enthält den Satz von Regeln, die ausgewertet wurden, um die Zuweisungsgruppe für VIS festzulegen.
Schwachstellen-Rechner [sn_vul_Calculator_Group]	Enthält die Regeln des Schwachstellenrechners. Die Reihenfolge des Rechners bestimmt, welcher Rechner zuerst ausgewertet wird, und in jedem Rechner wird höchstens eine Rechnerregel verwendet.
Regel des Schwachstellen-Rechners [sn_vul_Calculator]	Enthält die Regeln für alle Rechner. Für jeden Rechner werden die Rechnerregeln der Reihe nach überprüft. Der erste Rechner, der der Bedingung entspricht, verwendet die Werte innerhalb dieser Regel.
Schwachstellen-CVEs [sn_vul_m2m_entry_cve]	Verknüpft NVD Common Vulnerability Exposures (CVE)-Daten mit angreifbaren Einträgen.
Importwarteschlangeneintrag Schwachstellen-Datenquelle [sn_vul_ds_Import_q_entry]	Warteschlange für Anhänge, bevor sie von einer Datenquelle verarbeitet werden. Wird von Schwachstellenintegrationen verwendet.
Schwachstelleneintrag [sn_vul_entry]	Dokumentierte Schwachstelle.
Schwachstelleneintrags-Scan [sn_vul_entry_Scan]	Speichert die Beziehung zwischen einem Scan und einem Schwachstelleneintrag.
Schwachstellen-Exploit-Framework [sn_vul_m2m_Framework_vul]	Enthält die Beziehung zwischen Exploit-Frameworks und Schwachstellen.
V19.0: Bewertung des Schwachstellenrisikos sn_vul_Analyst_sam_config	Konfigurationstabelle der Risikobewertung für CVE.
Konfiguration der Schwachstellengranularität [sn_vul_granularity_config]	Speichert und verwaltet den Status des ein- oder Ausschlussports für das Modul „VI-Granularität konfigurieren“.
Korrekturaufgaben [sn_vul_Vulnerability]	Sammlung angreifbarer Elemente, die zur Korrektur organisiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Change-Anforderungen für Korrekturaufgaben [sn_vul_m2m_vg_Change_Request]	Speichert die Zuordnung von Korrekturaufgaben und CHG-Anforderungen.
Korrekturaufgabenelemente [sn_vul_m2m_vul_Group_item]	Zuordnung von Korrekturaufgaben und angreifbaren Elementen.
Regeln für Korrekturaufgaben [sn_vul_grouping_rule]	Enthält die Regeln, die die Kriterien definieren, mit denen Gruppen für eine Reihe angreifbarer Elemente automatisch erstellt werden.
Integration von Sicherheitslücken [sn_vul_Integration]	Planbarer Datensatz zum Importieren von Schwachstellendaten aus einer externen Quelle. Erweitert Die Geplante Skriptausführung.
Datenquelle Sicherheitslückenintegration [sn_vul_int_Data_src]	Datenquelle zur Verwendung mit einer Schwachstellenintegration.
Schwachstellenintegrationsprotokoll [sn_vul_Integration_log]	Zeichnet die Ausgabe von Protokollinformationen nach Ausführungen der Schwachstellenintegration auf.
Integrationsprozess für Schwachstellen [sn_vul_Integration_Process]	Einzelnes Prozessvorkommen für eine Schwachstellenintegration.
Warteschlange für Schwachstellenintegration [sn_vul_Integration_Queue]	Stellt die Importanforderungen für eine Integrationsausführung in die Warteschlange, wenn alle Datenquellen verwendet werden.
Ausführung der Schwachstellen-Integration [sn_vul_Integration_Run]	Aufrufe der Schwachstellenintegration. **Hinweis:** Wenn eine Integrationsausführung ausgeführt wird, kann sich im Backlog nur eine Integration im Status „bereit“ befinden.
Statistiken zur Ausführung von Schwachstellenintegrationen [sn_vul_Integration_stats]	Speichert die Aufgliederung jedes Schritts: Z. B. REST-API-Zeit, VI-Erstellungszeit usw. für eine Integrationsausführung
Aufgabe für angreifbares Element [sn_vul_m2m_item_Task]	Angreifbare Elemente, die Problemen, Changes und Security Incidents zugeordnet sind.
Schwachstellen-Malware-Kit [sn_vul_m2m_Malware_Kit_vul]	Enthält die Beziehungen zwischen Schwachstellen und Malware-Kits.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Erforderliche Schwachstellenlösung [sn_vul_m2m_Solution_prerequisite]	Enthält die quellenspezifischen Voraussetzungen für die Anwendung einer Lösung, falls verfügbar.
Grenzwert für Schwachstellenquote [sn_vul_rate_limit]	Definiert ein Quotenlimit, das auf einem Scanner verwendet werden soll.
Verwundbarkeitsreferenz [sn_vul_reference]	Externe Referenzen für bekannte Schwachstellen.
Status der Schwachstellenkorrektur [sn_vul_m2m_ttr_Status]	Status des angreifbaren Elements für die am nächsten angewendete Korrekturzielregel.
Regel zum Schwachstellenrisiko [sn_vul_calc_Risk]	Spezielle Rechnerregel, die mit den Risikopunktzahlrechnern verwendet wird. Nimmt Gewichtungen, die angeben, welche Werte im Zusammenhang mit einem VI zur Berechnung der Risikopunktzahl verwendet werden sollen.
Rechner für Schwachstellen-Rollup [sn_vul_Rollup]	Liste der Schwachstellen-Rollup-Rechner.
Schwachstellen-Scan [sn_vul_Scan]	Schwachstellen-Scan. Enthält, was gescannt werden soll, mit welchem Scanner und eine Zusammenfassung der Scan-Ergebnisse.
Konfigurationselement für Schwachstellen-Scan [sn_vul_m2m_Scan_Configuration_item]	Ordnet CMDB-CIs zu, die in der Warteschlange zum Scannen stehen.
Warteschlangeneintrag für Schwachstellen-Scan [sn_vul_Scan_q_entry]	Scan-Datensatz in Warteschlange zum Scannen oder Verarbeiten. Erleichtert die Anforderungen innerhalb der angegebenen Quotengrenzen.
Quelle des Schwachstellen-Scans [sn_vul_m2m_Scan_Source]	Ordnet Quellen einem Scan-Datensatz zu und gibt an, dass alle Datensätze in der Warteschlange gescannt werden sollen.
Aufgabe des Schwachstellen-Scans [sn_vul_m2m_Scan_Vulnerability]	Ordnet Schwachstellenaufgaben für die Quellen eines Scan-Datensatzes zu.
Schwachstellen-Scanner [sn_vul_Scanner]	Definiert Scanner von Drittparteien, die in Scans verwendet werden sollen.
Grenzwert Für Schwachstellen-Scanner-Rate [sn_cmn_Scanner_rate_limit]	Ordnet einen Scanner einem Quotenlimit zu.
Verwundbare Software [sn_vul_m2m_entry_Software]	Enthält Zuordnungen zwischen Schwachstellen und angreifbarer Software.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

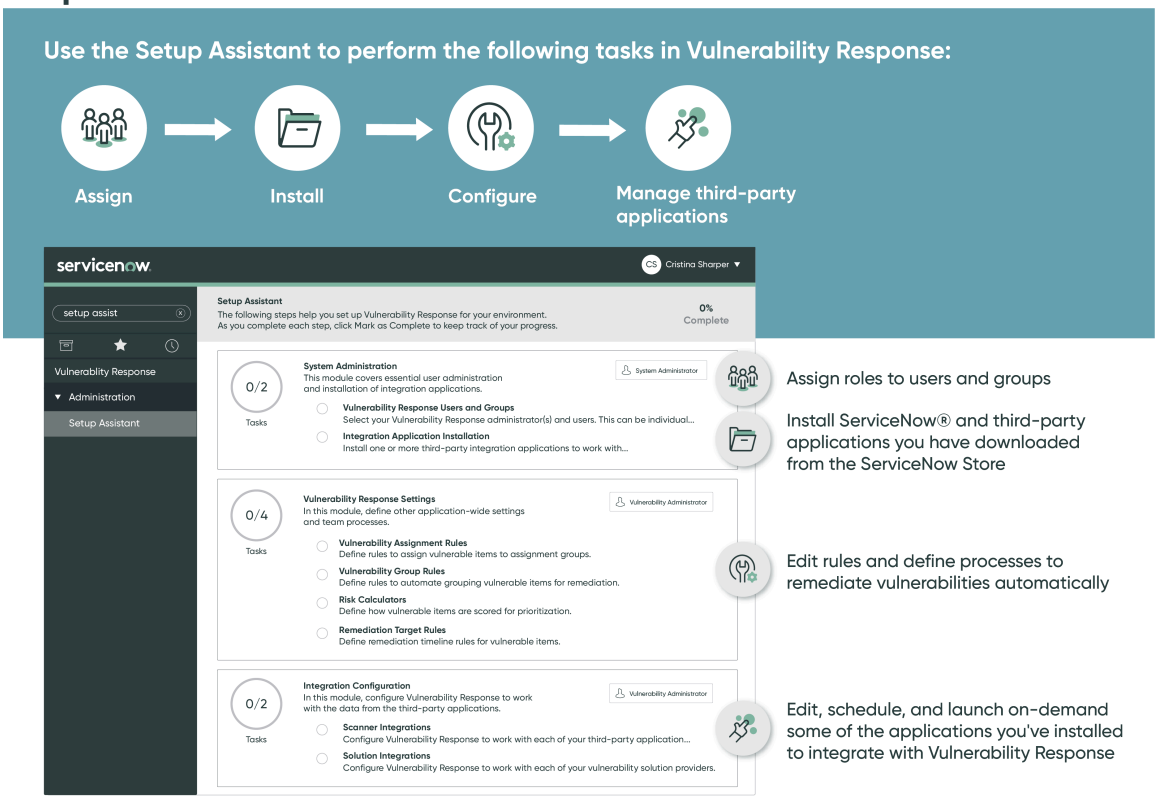
Tabelle	Beschreibung
Schwachstellenlösung [sn_vul_Solution]	Enthält die Beziehungsdaten zwischen der Schwachstelle und den möglichen Lösungen dafür. Ab v24.0.6 von Vulnerability Response, Eine neue Spalte mit dem Titel Scanner-Bulletin wird dieser Tabelle hinzugefügt.
Schwachstellenlösung [sn_vul_m2m_Vulnerability_Solution]	Verknüpft die Tabelle „Schwachstelleneintrag“ (sn_vul_entry) mit der Tabelle „Schwachstellenlösung“ (sn_vul_Solution).
Sicherheitsrisikostatus Change-Genehmigung [sn_vul_Change_Approval]	Verfolgt den Genehmigungsprozess für Schwachstellen.
Ersatzlösung für Schwachstelle [sn_vul_m2m_Solution_supersedence]	Enthält die quellenspezifische Beziehung zwischen Lösungen.
Schwachstellenupdatemanifest [sn_vul_vuln_Update]	Enthält eine Liste von Schwachstellen, deren Rollup-Daten aktualisiert werden müssen, nachdem ihre angreifbaren Elemente aktualisiert wurden oder geschlossen wurden oder sich die Risikopunktzahl geändert hat.
Schwachstellenzuordnung für Lieferanten [Sun_vul_Vulnerability_Vendor_Mapping]	Enthält eine Liste von Schwachstellen und ihren Lieferanten.
Angreifbares Element [sn_vul_vulnerable_item]	Enthält das Auftreten einer Schwachstelle in einem Konfigurationselement.
Erkennung von angreifbarem Element [sn_vul_Detection]	Enthält die Erkennungen angreifbarer Elemente aus Drittpartei-Integrationen.
Software mit Schwachstellen [sn_vul_Software]	Software, die bekanntermaßen bestimmte Schwachstellen aufweist.

Wird Konfiguriert Vulnerability Response Mit dem Setup-Assistenten

Der Setup-Assistent führt Sie durch die Einrichtung Vulnerability Response Und bestimmte Drittpartei-Integrationen für Ihre Umgebung. Der Setup-Assistent bietet fast alles, was Sie zum Installieren und Einrichten Ihrer Umgebung benötigen, damit Sie verwenden können Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setup-Assistent-Funktionalität



Now Platform® roles: admin and vulnerability admin

Die Verwendung des Setup-Assistenten erfordert zwei verschiedene ServiceNow AI Platform® Rollen: administrator und Schwachstellenadministrator.

Weitere Informationen zu den Anweisungen und Hinweismeldungen im Setup-Assistenten finden Sie in den folgenden Abschnitten.

Systemverwaltung: Weisen Sie Anwender und Gruppen zu, und installieren Sie Integrationsanwendungen

Erforderliche Rolle: admin

Eine Liste der Anwender und Integrationen sollte vom Schwachstellenmanager abgerufen werden, bevor mit diesen Aufgaben begonnen wird.

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**an.
2. Im ersten Abschnitt „Systemverwaltung“ weist der -Administrator Anwendern und Gruppen Rollen zu und installiert unterstützte Integrationen.

   Zuweisen Vulnerability Response Personas und Rollen für Anwender und Gruppen im Setup-Assistenten.

   Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.
3. Weisen Sie Rollen im Setup-Assistenten zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Weisen Sie Anwendern oder Gruppen die Rolle „sn_vul.admin“ zu.
- Weisen Sie die Rolle sn_vul.admin für die Verwaltung und Konfiguration von Vulnerability Response zu, einschließlich Schwachstellenintegrationen, Regeln für Korrekturaufgaben, Rechner und Regeln für die Zeit bis zur Korrektur.
- Weisen Sie die Rolle sn_vul_Vulnerability_write für die Erstellung und Aktualisierung von Korrekturaufgaben und angreifbaren Elementen zu.

  Hinweis:
  Alle anderen Anwender erhalten automatisch Schreibzugriff nur auf Korrekturaufgaben, die ihnen zugewiesen sind.

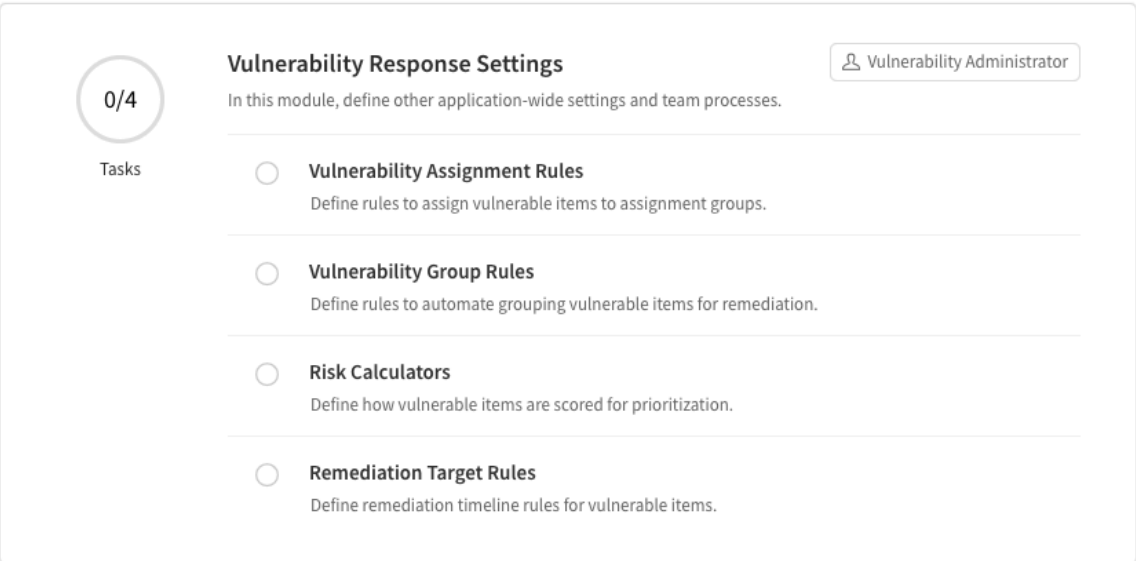
- Weisen Sie die Rolle sn_vul_Vulnerability_read zu, um Korrekturaufgaben, angreifbare Elemente und andere Schwachstelleninformationen anzuzeigen.

  Hinweis:
  Benutzern mit der Rolle „itil“ wird automatisch die Rolle „sn_vul.Remediation_owner“ gewährt, mit der sie Korrekturaufgaben und angreifbare Elemente, Schwachstelleneinträge und Lösungen in anzeigen können Vulnerability Response Anwendung in ihrer Instanz und in der Mobile Agent Anwendung. Es ist keine zusätzliche Zuweisung erforderlich.

4. Installieren Sie Integrationsanwendungen von Drittanbietern.
   - Siehe Installation von Vulnerability Response Und unterstützte Anwendungen Und Vulnerability Response-Integrationen Weitere Informationen zu Anwendungen, die von unterstützt werden Vulnerability Response.
   - Weitere Informationen zur Verwendung des Setup-Assistenten zum Installieren unterstützter Apps finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.

Vulnerability Response-Einstellungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) oder admin



In den Einstellungen für Vulnerability Response definiert der Schwachstellenadministrator anwendungsweite Einstellungen und Regeln für Vulnerability Response. Alternativ kann der Administrator diese Aufgaben ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Erstellen Sie Zuweisungsregeln Für Schwachstellen.

   Erstellen Sie Regeln, die die automatische Zuweisung von Korrekturaufgaben zur Lösung definieren. Mindestens eine Regel ist im Lieferumfang des Basissystems enthalten. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

   Hinweis:

   Die Funktion „erneut anwenden“ erfordert eine Baseline-Anwendung der Regeln. Sobald Ihre Regeln erstellt wurden, aktivieren Sie *`Reapply all vulnerability assignment rules`*Geplante Aufgabe, die nach Belieben ausgeführt werden soll. Andernfalls müssen Sie alle Regeln erneut auf alle offenen VIS anwenden, bevor Sie sie ändern.

   Wenn der Auftrag abgeschlossen ist, legen Sie fest **Ausführen** Feld in der geplanten Aufgabe, das an Ihre Umgebung angepasst ist. Abhängig von der Anzahl der aktiven VIS, die Sie haben, kann die tägliche Bewertung und Aktualisierung dieser VIS keine geringfügigen Auswirkungen auf die Leistung haben. Für größere Umgebungen sollten Sie eine Aktualisierung einmal pro Woche oder sogar einmal pro Monat in Betracht ziehen.

   Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.

2. Erstellen Sie Regeln für Korrekturaufgaben.

   Erstellen Sie Regeln, die die automatische Erstellung von Korrekturaufgaben zur Lösung definieren. Mindestens eine Regel, **Schwachstelle,** Wird mit dem Basissystem geliefert. Sie können die Regeln über das Formular oder die Listenansicht erneut anwenden.

   - Wenn eine Gruppenregel aus der Formular- oder Listenansicht gelöscht wird, haben Sie die Möglichkeit, alle zu löschen **Öffnen** Von dieser Regel erstellte Gruppen. Gruppen nicht in **Öffnen** status sind ausgeschlossen.
   - Siehe CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Integrationen von Schwachstellen von Drittparteien Weitere Informationen zum Erstellen von Regeln für Ihre Umgebung.
   - Siehe Erkunden Sie Vulnerability Response Anwendung Weitere Informationen zur Verwendung von Vulnerability Response Zum Beheben von Schwachstellen.

3. Erstellen und aktivieren Sie Risikorechner.

   Aktivieren Sie Risikorechner, die definieren, wie angreifbare Elemente für die Priorisierung bewertet werden. Mehrere Risikorechner sind im Lieferumfang des Basissystems enthalten. Siehe Vulnerability Response Rechner und Regeln für Schwachstellenrechner Informationen zum Erstellen oder Bearbeiten von Risikorechnern für Ihre Umgebung.

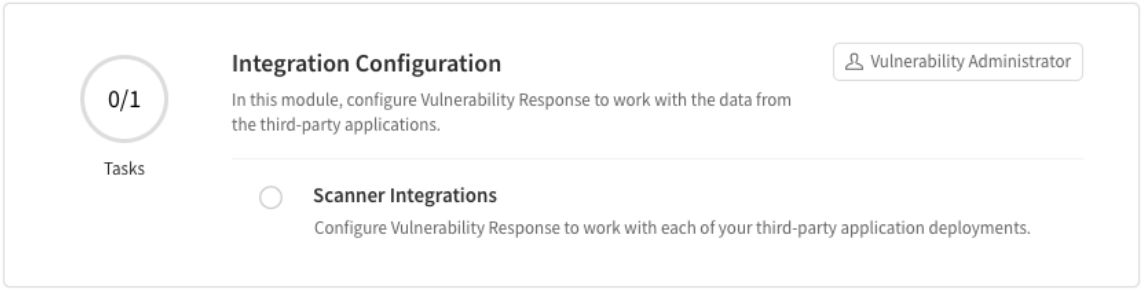
4. Erstellen Sie Korrekturzielregeln.

   Erstellen Sie Korrekturzielregeln für Korrekturkategorien. Mindestens eine Regel ist im Lieferumfang des Basissystems enthalten. Siehe Vulnerability Response Korrekturzielregeln Weitere Informationen zum Erstellen von Regeln für Ihre Umgebung.

Integrationskonfiguration

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) oder admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Konfigurieren, planen, bearbeiten und starten Sie im Abschnitt „Integrationskonfiguration“ die folgenden Integrationen von Schwachstellen-Scannern von Drittanbietern und, falls vorhanden Solution Management for Vulnerability Response Anwendung ist installiert, Lösungsanbieter.

- Siehe Konfigurieren Sie Qualys Vulnerability Integration Mit dem Setup-Assistenten Weitere Informationen zum Konfigurieren von Qualys Vulnerability Integration.
- Konfiguration von Vulnerability Response Integration with Tenable Anwendung wird unterstützt. Siehe Konfigurieren Sie die Tenable-Schwachstellenintegration mit dem Setup-Assistenten.
- Nachdem Sie installiert haben Vulnerability Solution Management Anwendung, die **Lösungsintegrationen** Option wird unten angezeigt **Scanner-Integrationen** . Klicken Sie Auf **Lösungsintegrationen** Konfigurieren Sie Ihre installierten Anbieter von Schwachstellen in diesem Abschnitt des Setup-Assistenten. Die Red Hat Solution Integration Und Integration der Microsoft Security Response Center-Lösung Werden unterstützt.

  Siehe Vulnerability Solution Management Weitere Informationen zu installierten Lösungen. Siehe Anwendung Solution Management for Vulnerability Response installieren Für weitere Informationen zur Installation.

  Siehe Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management Mit dem Setup-Assistenten Weitere Informationen zum Konfigurieren Ihrer installierten Lösungen.
- Wenn eine Integration aus mehreren Quellen besteht, können Sie mehrere Bereitstellungen derselben Drittpartei-Integration haben.
- Die Einstellungen aus Ihrer ursprünglichen Drittpartei-Integration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

  Hinweis:
  Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Erwägen Sie, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

  Daten aus jeder Drittpartei-Integration werden eindeutig identifiziert und sind in einer einzigen Instanz von verfügbar Vulnerability Response.

Hinweis:
Mehrere Schwachstellenintegrationen für Rapid7 InsightVM Sind im Setup-Assistenten nicht verfügbar. Siehe Erstellen Sie domänengetrennte Importe für eine Integration Informationen zum Konfigurieren und Erstellen mehrerer Rapid7 InsightVM Integrationen.

Zusätzliche Aufgaben

Siehe Zusätzlich Vulnerability Response Setup- und Konfigurationsaufgaben Weitere Informationen zu Setup-Aufgaben, die nicht im Setup-Assistenten enthalten sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent

Weisen Sie zu Vulnerability Response Persona-Rollen für Gruppen oder Anwender mit Setup-Assistent.

Vorbereitungen

Wenn Sie bereits Persona-Rollen in zugewiesen haben Vulnerability Response Verwenden Sie den Setup-Assistenten und weitere Informationen zum Bearbeiten und Verwalten Ihrer granularen Rollen und Rollenzuweisungen im Modul „Anwenderverwaltung“, siehe Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Wenn Sie ein Upgrade-Kunde sind, können Sie Ihre vorhandenen Rollen für die Anwendung Vulnerability Response weiterhin verwenden. Zugriff für Anwender und Gruppen, die mit den Berechtigungen sn_vul.Vulnerability_read und sn_vul.Vulnerability_write zugewiesen sind und die in früheren Versionen von verfügbar sind Vulnerability Response Hat sich nicht geändert.

Um jedoch mehr Kontrolle darüber zu erhalten, was Anwender und Gruppen im tun und sehen können Vulnerability Response Anwendung auf Aufgabenebene können Sie Persona und granulare Rollen verwenden.

Wenn Sie die Persona-Rolle sn_vul.Vulnerability_admin noch nicht mit dem Setup-Assistenten zugewiesen haben, führen Sie die folgenden Schritte aus, um sie zuzuweisen. Nach der Zuweisung hat der Schwachstellenadministrator mit dieser Persona-Rolle die Berechtigung, die Aufgaben des Setup-Assistenten nach dem ersten Abschnitt abzuschließen und Regeln und Integrationen von Drittparteien in zu verwalten Vulnerability Response Anwendung.

Eine Übersicht über Persona-Rollen und granulare Rollen finden Sie unter Vulnerability Response Personas und granulare Rollen.

Wenn Sie ein Upgrade-Kunde sind, verwenden Sie die folgende Tabelle als Referenz.

Vorherige Zuweisung	Empfohlene Zuweisung [Anwenderpersona]	Beschreibung
sn_vul.admin	sn_vul.Vulnerability_admin [Schwachstellenadministrator]	Bietet vollständigen Zugriff auf die Anwendung Vulnerability Response (VR). Benutzer mit dieser Rolle konfigurieren VR-Anwendungen und -Regeln und installieren Drittanbieterintegrationen.
sn_Vulnerability_write	sn_vul.Vulnerability_Analyst [Schwachstellenanalyst]	Ermöglicht das Anzeigen und Aktualisieren aller Datensätze für die VIT-Korrektur.
sn_vul.remediation_owner	sn_vul.Remediation_owner [Korrekturbesitzer]	Ermöglicht Anwendern und Gruppen, Schwachstellen zu beheben, die ihnen oder ihrer Gruppe zugewiesen sind, und die zugehörigen Datensätze zu aktualisieren.
sn_vul.admin	sn_vul.ci [CI-Manager]	Ermöglicht die Verwaltung nicht abgeglichener Konfigurationselemente, die in der CMDB nicht gefunden wurden,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorherige Zuweisung	Empfohlene Zuweisung [Anwenderpersona]	Beschreibung
		einschließlich der Aktualisierung erkannter Elemente.
sn_vul.admin	sn_vul.Exception_Approver [Ausnahmegenehmiger]	Ermöglicht die Genehmigung von Ausnahmen, Zurückstellungen und Abschlüssen von Korrekturaufgaben und angreifbaren Elementen.
sn_vul.vulnerability_read	sn_vul.read_all oder sn_vul.read_Group_rules	Gewährt schreibgeschützten Zugriff auf bestimmte Bereiche in der Anwendung. Verwenden Sie sn_vul.read_all, um alle VR-Datensätze anzuzeigen, oder sn_vul.read_Group_rules, um Regeln für Korrekturaufgaben anzuzeigen. Benutzer mit diesen Rollen können Datensätze nicht aktualisieren. **Hinweis:** Mehrere andere Leserollen sind in verfügbar Vulnerability Response Bereich für detaillierteren Zugriff.

Um die granularen Rollen anzuzeigen, die ein Anwender oder Gruppen mit einer Persona-Rolle standardmäßig erbt, navigieren Sie zu **Alle** > **Anwenderadministration** > **Rollen**an. Suchen Sie die gewünschte Rolle, und klicken Sie darauf, um den Datensatz zu öffnen. Auf der Registerkarte enthält Rollen werden alle granularen Rollen der Persona-Rolle sowie alle geerbten Rollen aufgelistet.

Möglicherweise möchten Sie überprüfen, ob alle erforderlichen Anwender und Gruppen erstellt wurden, bevor Sie Rollen im Setup-Assistenten zuweisen. Alternativ können Sie neue Anwender und Gruppen über den Setup-Assistenten hinzufügen, indem Sie auf klicken **Anwenderverwaltungsmodul** Link im Formular, das in der folgenden Abbildung angezeigt wird.

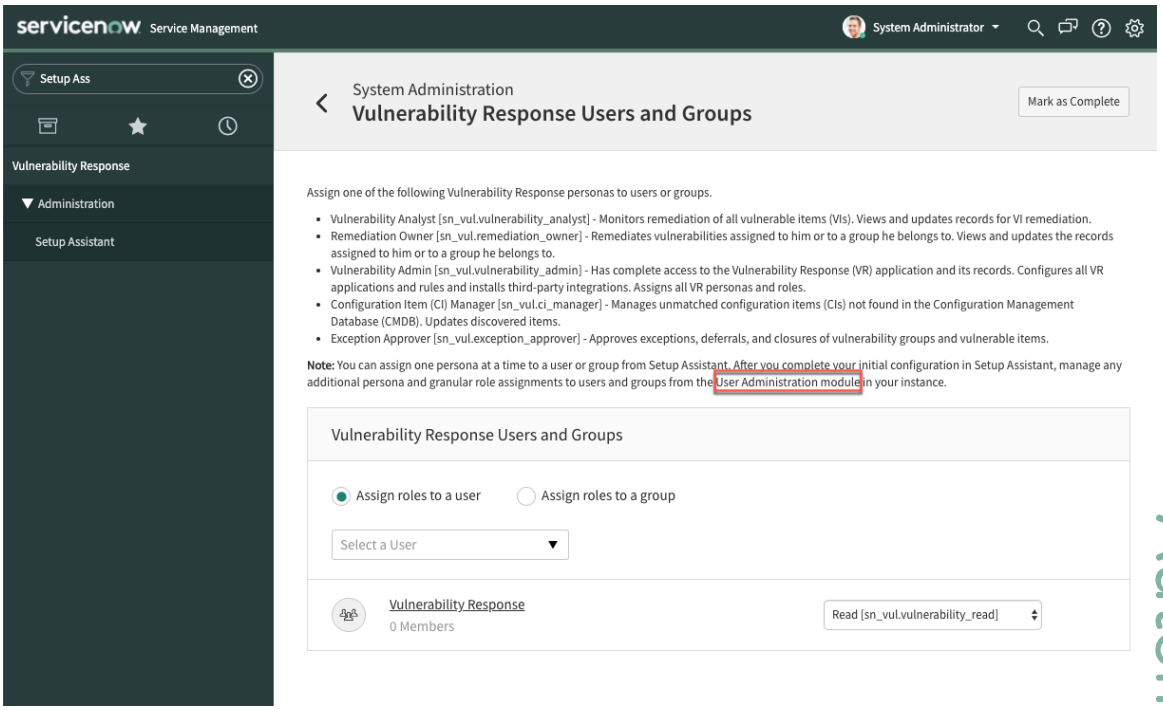
Im folgenden Beispiel, um den Zugriff auf zu beschränken Vulnerability Response Anwendung: Dieses Beispiel zeigt, wie einem Anwender die Schwachstellenadministrator-Persona zugewiesen wird. Normalerweise ziehen Sie es vor, Gruppen andere Persona-Rollen als sn_vul.Vulnerability_admin zuzuweisen.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration Setup-Assistent** .
   Die Seite Setup-Assistent wird angezeigt.
2. Klicken Sie auf Vulnerability Response-Anwender und -Gruppen.
   Die Seite Systemverwaltung Vulnerability Response-Anwender und -Gruppen wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wenn Rollen einem Anwender zuweisen ausgewählt ist, wählen Sie einen vorhandenen Anwender aus der Liste aus.

   Sie können nur einen Anwender oder eine Gruppe mit einer Persona-Rolle zuweisen.

   Nachdem Sie einen Anwender oder eine Gruppe ausgewählt haben, wird auf der rechten Seite des Formulars standardmäßig die Standardpersona Korrekturbesitzer [sn_vul.Remediation_owner] zugewiesen und bleibt in der Liste angezeigt, bis Sie sie ändern.

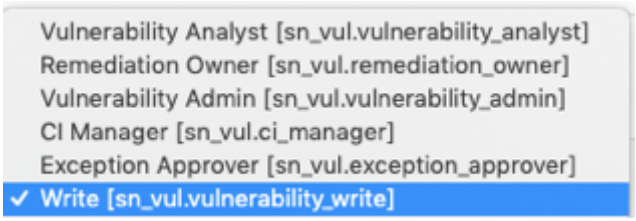
   Hinweis:
   Wenn Sie ein Upgrade auf eine neuere Version von durchführen Vulnerability Response Und Sie haben vor dem Upgrade einem Benutzer oder einer Gruppe zuvor die Rolle sn_vul.Vulnerability_write zugewiesen. Sie wird zusammen mit den neuen Persona-Rollen angezeigt, wie in der folgenden Abbildung dargestellt.

   Wenn Sie ein Upgrade-Kunde sind, können Sie Ihre vorhandenen Rollen für die Vulnerability Response-Anwendung weiterhin verwenden. Der Zugriff für Anwender und Gruppen, die mit den Berechtigungen „sn_vul.Vulnerability_read“ und „sn_vul.Vulnerability_write“ vor v10.3 zugewiesen wurden, hat sich nicht geändert.

   Beachten Sie, dass für vorhandene Anwender oder Gruppen, denen derzeit die Rollen sn_vul.Vulnerability_read oder sn_vul.Vulnerability_write zugewiesen sind, diese Rollen zusammen mit den Persona-Rollen in der Liste angezeigt werden. Sobald Sie eine Persona-Rolle zugewiesen haben, ist die alte Rolle in Zukunft nicht mehr verfügbar. Wie in der folgenden Abbildung gezeigt, wird die Rolle Schreiben [sn_vul.Vulnerability_write] nicht mehr als Option für diesen Anwender oder diese Gruppe angezeigt, nachdem ihm eine der Persona-Rollen zugewiesen wurde.

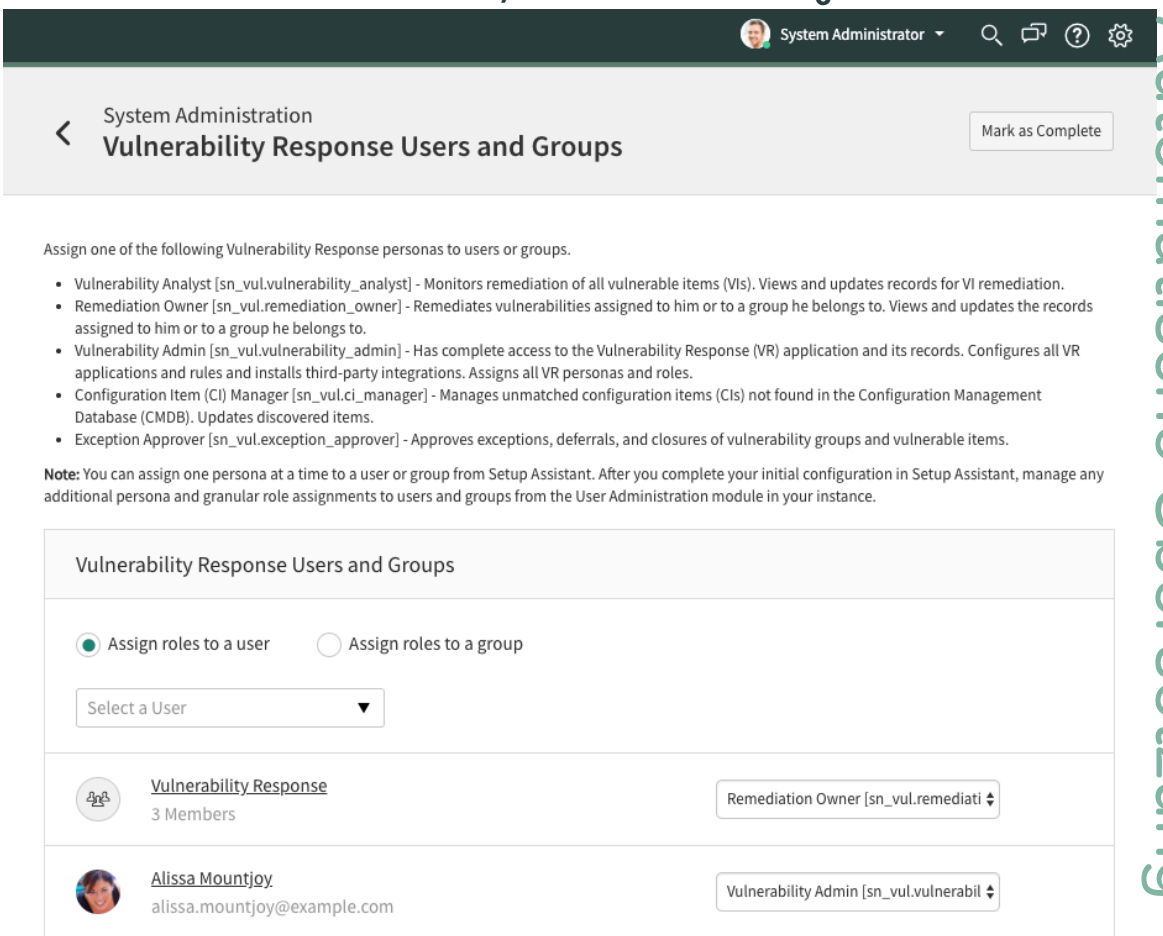
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie in der Liste auf der rechten Seite des Formulars die Option aus **Schwachstellenadministrator [sn_vul.Vulnerability_admin]** .
   Eine Nachricht wird angezeigt, die angibt, dass der Anwender oder die Gruppe erfolgreich der Persona zugewiesen wurde.

Korrekturbesitzer-Persona, die einer Gruppe zugewiesen ist, und Schwachstellenadministrator-Persona, die einem Anwender zugewiesen ist



Automatische Übersetzung

5. Mit den Beschreibungen der oben aufgeführten Persona-Rollen weisen Sie alle Anwender und Gruppen den verbleibenden Persona-Rollen zu: Korrekturbesitzer, Schwachstellenanalyst, CI-Manager und Ausnahmegenehmiger.
   Sie haben die Zuweisung von Persona-Rollen an Anwender und Gruppen mithilfe des Setup-Assistenten erfolgreich abgeschlossen.
6. **Wahlweise:** Führen Sie die folgenden Schritte aus, um die Anwender in einer Gruppe über den Setup-Assistenten zu bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wenn die Gruppe im Formular angezeigt wird, klicken Sie auf den Namen der Gruppe, die Sie bearbeiten möchten.
Der Gruppendatensatz wird angezeigt.

b. Klicken Sie bei ausgewählter Registerkarte Gruppenmitglieder auf **Bearbeiten** .
Das Formular Mitglieder bearbeiten wird angezeigt

c. Verwenden Sie den Slushbucket, um Anwender auszuwählen oder zu entfernen.

d. Klicken Sie Auf **Speichern** Um Ihre Änderungen zu speichern und zum Gruppendatensatz zurückzukehren.

e. Klicken Sie Auf **Aktualisieren** Um zum Setup-Assistenten zurückzukehren.

f. Klicken Sie auf der Seite Setup-Assistent auf **Vulnerability Response-Anwender und -Gruppen** Um mit Ihrer Konfiguration im Setup-Assistenten fortzufahren.

Nächste Maßnahme

Fahren Sie als Systemadministrator mit der Konfiguration von fort Vulnerability Response In Setup-Assistent. Beachten Sie, dass Sie nach Abschluss des ersten Abschnitts von einem Benutzer mit der Rolle „Schwachstellenadministrator-Persona“ die Aufgaben im Setup-Assistenten ausführen können. Weitere Informationen zum Verwalten granularer Rollen und Beispiele finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Verwalten Sie Persona und granulare Rollen für Vulnerability Response

Nachdem Sie Ihre erste Zuweisung von Persona-Rollen mit dem Setup-Assistenten abgeschlossen haben, verwalten Sie zusätzliche granulare Rollenzuweisungen für Anwender oder Gruppen über das Modul „Anwenderverwaltung“ in Ihrer Instanz.

Vorbereitungen

Wenn Sie Ihre Ersteinrichtung und -Konfiguration für noch nicht abgeschlossen haben Vulnerability Response Navigieren Sie mit dem Setup-Assistenten oder Benutzern und Gruppen zugewiesenen Persona-Rollen zu **Vulnerability Response** > **Administration** > **Setup-Assistent**an. Weitere Informationen finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.

Wichtige Begriffe und eine Übersicht über Persona-Rollen finden Sie unter Vulnerability Response Personas und granulare Rollen.

Eine Persona-Rolle ist eine vorkonfigurierte Rolle in der Anwendung, die aus mehreren granularen Rollen besteht. Die Persona-Rollen in Setup-Assistent, Schwachstellenadministrator, Schwachstellenanalyst, Korrekturbesitzer, Konfigurationselementmanager, und Exception Manager sind so konzipiert, dass sie den allgemeinen Stellenbezeichnungen für Manager, Analysten und Serviceverantwortliche in einer IT-Organisation oder Schwachstellen-Korrekturgruppe entsprechen.

Wenn Ihre Anwender und Gruppen mehr Zugriff haben sollen, als eine der Rollen zulässt, können Sie Anwendern und Gruppen feinere Rollen hinzufügen. Umgekehrt können Sie granulare Rollen entfernen, wenn Sie den Zugriff für bestimmte Anwender und Gruppen auf Aufgabenebene beschränken möchten. Außerdem können Sie anwenderdefinierte Rollen erstellen, die Ihren Anforderungen entsprechen.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Um granulare Rollen für Anwender und Gruppen zu verwalten, wählen Sie eine aus, um fortzufahren.

   Die Namen für die granularen Rollen in Vulnerability Response Beschreiben Sie normalerweise, was Anwender tun und sehen können. Um Beschreibungen bestimmter granularer Rollen anzuzeigen, navigieren Sie zu **Alle** > **Anwenderadministration** > **Rollen** Und suchen Sie die gewünschte Rolle. Rollenbeschreibung, Rollen, die automatisch geerbt werden, wenn eine Rolle zugewiesen wird, und alle Rollen, die von anderen Rollen abhängen, werden ebenfalls aufgelistet.

2. Führen Sie die folgenden Schritte aus, um einem Anwender oder einer Gruppe eine granulare Rolle zuzuweisen oder zu entfernen.
   Angenommen, Sie möchten einen IT-Manager mit einer Rolle zuweisen, die diesem Manager ermöglicht, Datensätze anzuzeigen, sie jedoch nicht zu aktualisieren oder zu bearbeiten. Zum Anzeigen von Datensätzen in Vulnerability Response, Performance Analytics for Vulnerability Response, Und weisen Sie diesem Anwender für alle Drittpartei-Integrationen die granulare Rolle sn_vul.read_all zu.

   a. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**an.

   b. Suchen Sie den Anwender, und klicken Sie in der Spalte Name auf den Datensatz, um ihn zu öffnen.
   Der Datensatz des Anwenders wird angezeigt.

   c. Wenn nicht ausgewählt, wählen Sie die Registerkarte Rollen aus.
   Die Rollen, die dem Anwender derzeit zugewiesen sind, werden angezeigt.

   d. Klicken Sie auf **Bearbeiten**.
   Das Formular Mitglieder bearbeiten wird angezeigt.

   e. Geben Sie im Feld Sammlung des Slushbucket den Namen der Rolle ein, wenn Sie ihn kennen, oder geben Sie ein `*sn_vul` Dient zum Anzeigen nur der granularen Rollen, die für Vulnerability Response verfügbar sind.

   f. Suchen und verschieben Sie sn_vul.read_all in die Rollenliste.

   Hinweis:
   Verwenden Sie denselben Prozess, um bestimmte granulare Rollen von Anwendern im Slushbucket zu entfernen, indem Sie die Rolle aus der Liste Rollen in die Liste Sammlung verschieben.

   g. Klicken Sie auf **Speichern**.
   Der Anwenderdatensatz wird mit der neuen granularen Rolle angezeigt.

   h. Klicken Sie Auf **Aktualisieren** Um Ihre Änderungen zu speichern und zur Liste Anwender zurückzukehren.
   Sie haben einem Anwender die Berechtigung zum Lesen, aber nicht zum Aktualisieren von Datensätzen in bereitgestellt Vulnerability Response, Performance Analytics for Vulnerability Response, Und für Integrationen von Drittparteien.

3. Um eine Gruppe so zu bearbeiten, dass nur bestimmte Mitglieder erweiterten Zugriff mit detaillierteren Rollen haben, führen Sie die folgenden Schritte aus.
   Angenommen, Sie möchten bestimmten Anwendern in der Gruppe „Korrekturbesitzer“ (sn_vul.Remediation_owner) gestatten, angreifbare Elemente manuell zu erstellen, Sie möchten diese Berechtigung jedoch nicht auf alle Anwender in der Gruppe erweitern. Die Berechtigung zum

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

manuellen Erstellen angreifbarer Elemente wird von der granularen Rolle „sn_vul.create_vulnerable_items“ gewährt. Um diese Berechtigung nur ausgewählten Anwendern aus dieser Gruppe zu gewähren, führen Sie die folgenden Schritte aus.

a. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**an.

b. Suchen Sie die Korrekturbesitzer-Gruppe, und klicken Sie in der Spalte Name auf die Gruppe, um den Datensatz zu öffnen.
Der Gruppendatensatz wird angezeigt.

c. Wenn nicht ausgewählt, wählen Sie die Registerkarte Gruppenmitglieder aus.
Die aktuellen Mitglieder der Gruppe werden angezeigt.

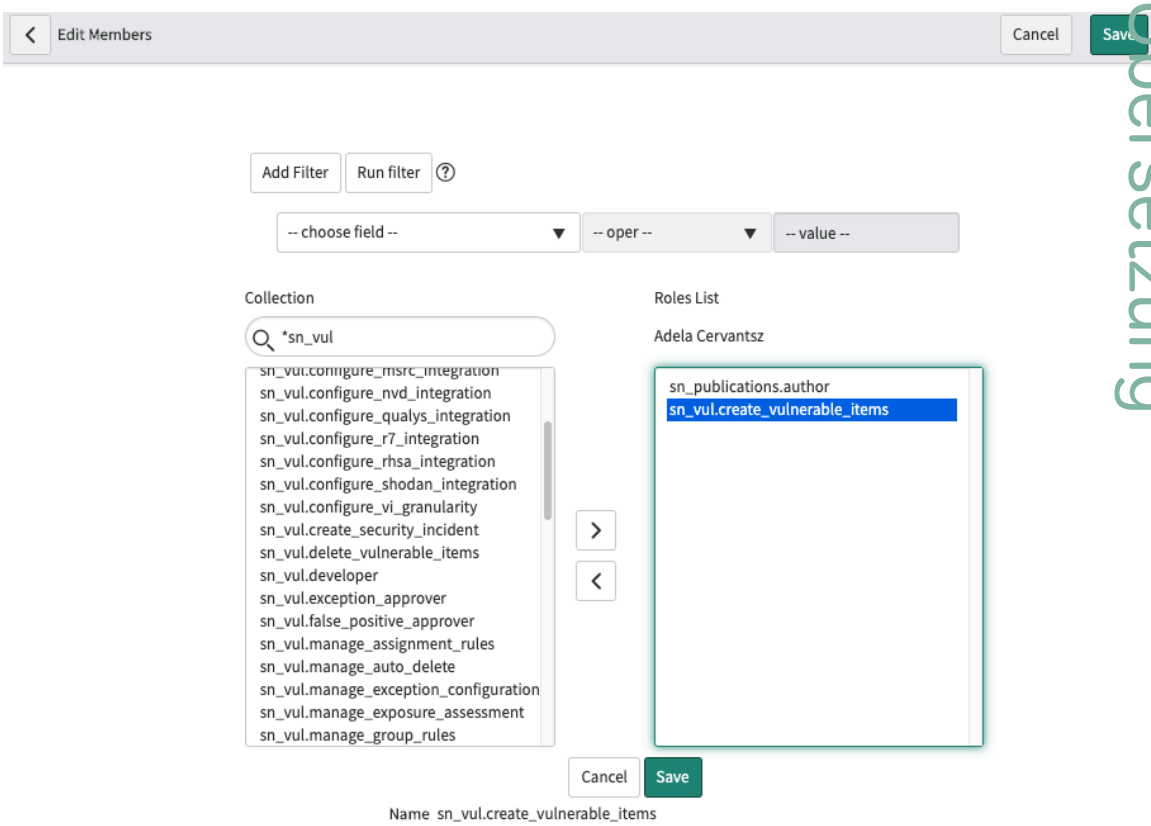
d. Klicken Sie auf einen Namen aus der Liste, der Sie die granulare Rolle zuweisen möchten, und öffnen Sie den Datensatz.

e. Scrollen Sie im Datensatz zur Registerkarte Rollen, und wählen Sie sie aus.
Die dem Anwender zugewiesenen Rollen werden angezeigt.

f. Klicken Sie auf **Bearbeiten**.
Das Formular Mitglieder bearbeiten wird angezeigt.

g. Geben Sie im Feld Sammlung den Namen der Rolle ein, wenn Sie ihn kennen, oder geben Sie ein `*sn_vul` Zum Anzeigen aller granularen Rollen, die für Vulnerability Response verfügbar sind.

h. Suchen und verschieben Sie sn_vul.create_vulnerable_items in die Rollenliste.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Klicken Sie auf **Speichern**.
Der Anwenderdatensatz wird mit der neuen granularen Rolle angezeigt.

j. Klicken Sie auf den zurück-Pfeil, um zurückzukehren, um die Anwender im Datensatz für die Korrekturbesitzergruppe anzuzeigen

k. Klicken Sie auf Namen aus der Liste, der Sie diese granulare Rolle zuweisen möchten, öffnen Sie ihre Datensätze, und verwenden Sie den Slushbucket, um die Rolle zuzuweisen.

l. Nachdem Sie Ihre Änderungen abgeschlossen haben, klicken Sie auf **Aktualisieren** Um Ihre Änderungen zu speichern und zur Gruppenliste zurückzukehren.
Sie haben einigen Anwendern in der Gruppe „Korrekturbesitzer“ (sn_vul.Remediation_owner) die Berechtigung zum manuellen Erstellen angreifbarer Elemente bereitgestellt.

4. Um eine neue Rolle nur mit granularen Rollen zu erstellen, die Sie auswählen, führen Sie die folgenden Schritte aus.
Nehmen Sie in diesem Beispiel an, dass Sie eine Rolle für einen Compliance-Auditor erstellen möchten. Diese Rolle arbeitet eng mit Governance, Risk und Compliance (GRC) zusammen, und der Auftrag erfordert die folgenden Berechtigungen und Aufgaben in Vulnerability Response:
   - Verwaltet Korrekturfristen für angreifbare Elemente und Schwachstellengruppen
   - Genehmigt Ausnahmeanforderungen für die Verlängerung von Fristen oder die Zurückstellung der Korrektur
   - Verwaltet die Bereinigung älterer angreifbarer Elemente mit automatischer Löschung
   - Definieren Sie Risikopunktzahlen
   - Liest alle Datensätze in Vulnerability Response Es ist jedoch nicht zulässig, sie zu bearbeiten.

   a. Navigieren zu **Alle** > **Anwenderadministration** > **Rollen**an.

   b. Klicken Sie in der Liste Rollen auf **Neu** .

   c. Füllen Sie die Felder im Rollendatensatz aus.

      Erstellen Sie einen Namen, wählen Sie die Anwendung aus, die diesen Datensatz enthält, und geben Sie eine Kurzbeschreibung für Ihre neue Rolle ein. Weitere Informationen zu den anderen Feldern im Formular finden Sie unter Erstellen Sie eine Rolle

      Hinweis:
      Wenn Sie einen Namen für Ihre neue Rolle erstellen, bevorzugen Sie möglicherweise einen Namen, der leicht in der Rollenliste erkannt wird und die Funktionalität der Rolle beschreibt. In diesem Beispiel bevorzugen Sie möglicherweise einen Titel wie Compliance-Auditor – GRC-VR.

   d. Klicken Sie auf **Absenden**.
   Die Liste Rollen wird angezeigt.

   e. Suchen Sie Ihre neue Rolle, und klicken Sie darauf, um den Datensatz zu öffnen.

   f. Klicken Sie auf **Bearbeiten**.

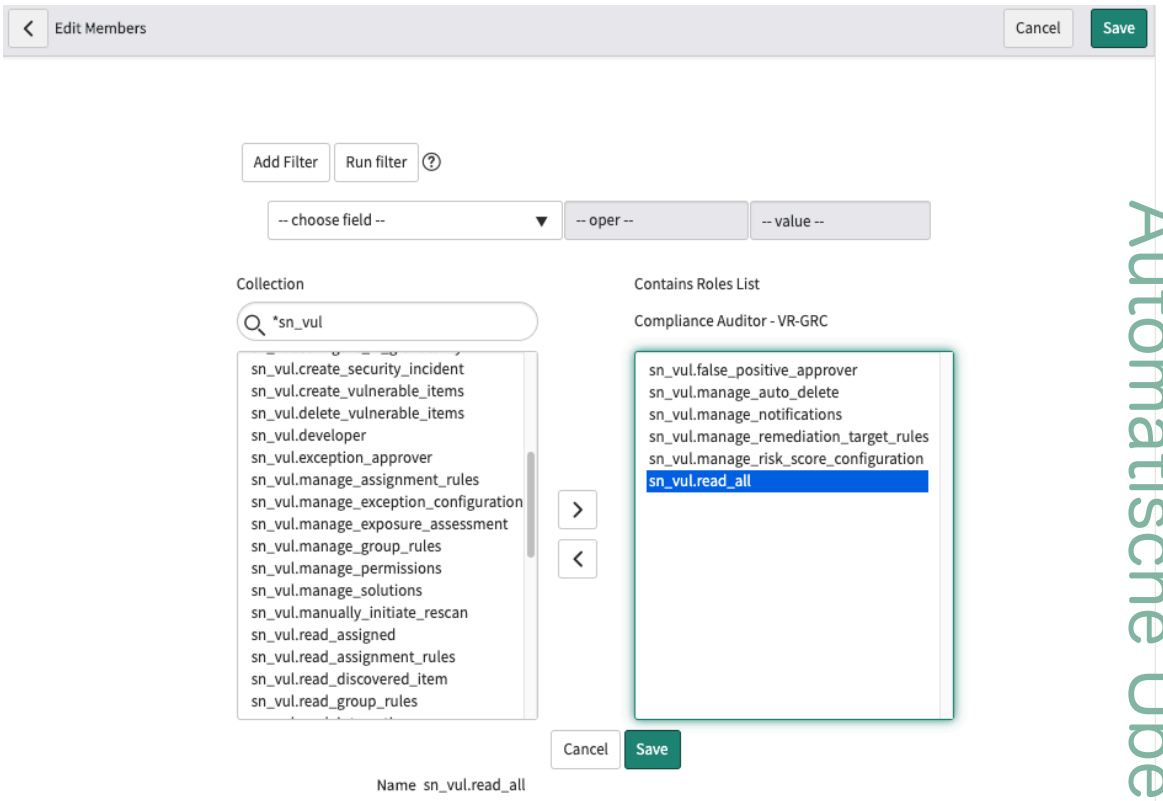
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Formular Mitglieder bearbeiten wird angezeigt.

g. Verwenden Sie den Slushbucket, um Ihrer neuen Rolle granulare Rollen hinzuzufügen.

In diesem Beispiel werden die erforderlichen Rollen für diese neue Rolle in der rechten Spalte in der folgenden Abbildung angezeigt.

Um nur die granularen Rollen für Vulnerability Response anzuzeigen, geben Sie im Feld Sammlung ein `*sn_vul` .



h. Klicken Sie auf **Speichern**.
Der Datensatz für Ihre neue Rolle wird angezeigt. Beginnen Sie mit der Registerkarte enthält Rollen, und bearbeiten Sie die Rolle nach Bedarf.

i. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
Ihre neue Rolle wird in der Liste Rollen angezeigt.

Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent

Installieren Sie die Integrationsanwendungen von Drittparteien, für die Sie eine Berechtigung haben, in Vulnerability Response Mit dem Setup-Assistenten.

Vorbereitungen

Der Setup-Assistent unterstützt die Installation der meisten Integrationsanwendungen von Drittanbietern mit Vulnerability Response, Aber Sie fahren mit der Konfiguration für einige Anwendungen fort, die Sie über Konfigurationsmodule in Ihrer Instanz installieren. Siehe Vulnerability Response-Integrationen Für eine Liste der Anwendungen, die von unterstützt werden Vulnerability Response.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

- Nach der Installation von wird Vulnerability Solution Management Funktion von Vulnerability Response Bietet Ihnen Zugriff auf Integration der Microsoft Security Response Center-Lösung Und Red Hat Solution Integration In Setup-Assistent.
- Vulnerability Solution Management Ist als separates Abonnement verfügbar. Siehe Vulnerability Solution Management Um weitere Informationen dazu zu erhalten Vulnerability Response Umfasst Lösungen.

Bevor Sie Drittanbieteranwendungen über den Setup-Assistenten installieren und aktivieren können, führen Sie die folgenden Aufgaben aus, um eine reibungslose Installation sicherzustellen:

Setup-Aufgaben	Beschreibung
Überprüfen Sie, ob Sie gültig sind ServiceNow Berechtigungen für die Integrationsanwendungen, die Sie installieren möchten.	Navigieren zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz, um Berechtigungen zu verifizieren. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Weitere Informationen zum Abrufen von Berechtigungen für Security Operations Anwendung aus dem ServiceNow Store, Siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung.
(Optional) wenn Sie nicht bereits installiert und aktiviert sind, möchten Sie möglicherweise installieren Vulnerability Response Anwendung vor der Installation der Drittanbieteranwendung.	Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe, Installieren und konfigurieren Sie Vulnerability Response .
Wenn nicht bereits installiert und aktiviert, müssen Sie Schwachstellendaten mit der geplanten Aufgabe „NVD-Integration und CWE“ aktivieren und importieren, bevor Sie eine Scanner-Anwendung einer Drittpartei ausführen, um Daten zu importieren.	Führen Sie die NVD- und CWE-Integrationen als Teil Ihres ersten Setups von aus Vulnerability Response Und vor dem Importieren von Schwachstellendaten in Ihre Instanz mit einem Scanner-Produkt eines Drittanbieters. Weitere Informationen finden Sie unter Verstehen der NVD-Integrationen.
Überprüfen Sie, ob Sie alle Setup-Aufgaben abgeschlossen haben, die für die Drittpartei-Integrationen für erforderlich sind Vulnerability Response.	Überprüfen Sie alle erforderlichen Setup-Aufgaben für jede Integration, die Sie in installieren möchten Vulnerability Response-Integrationen.

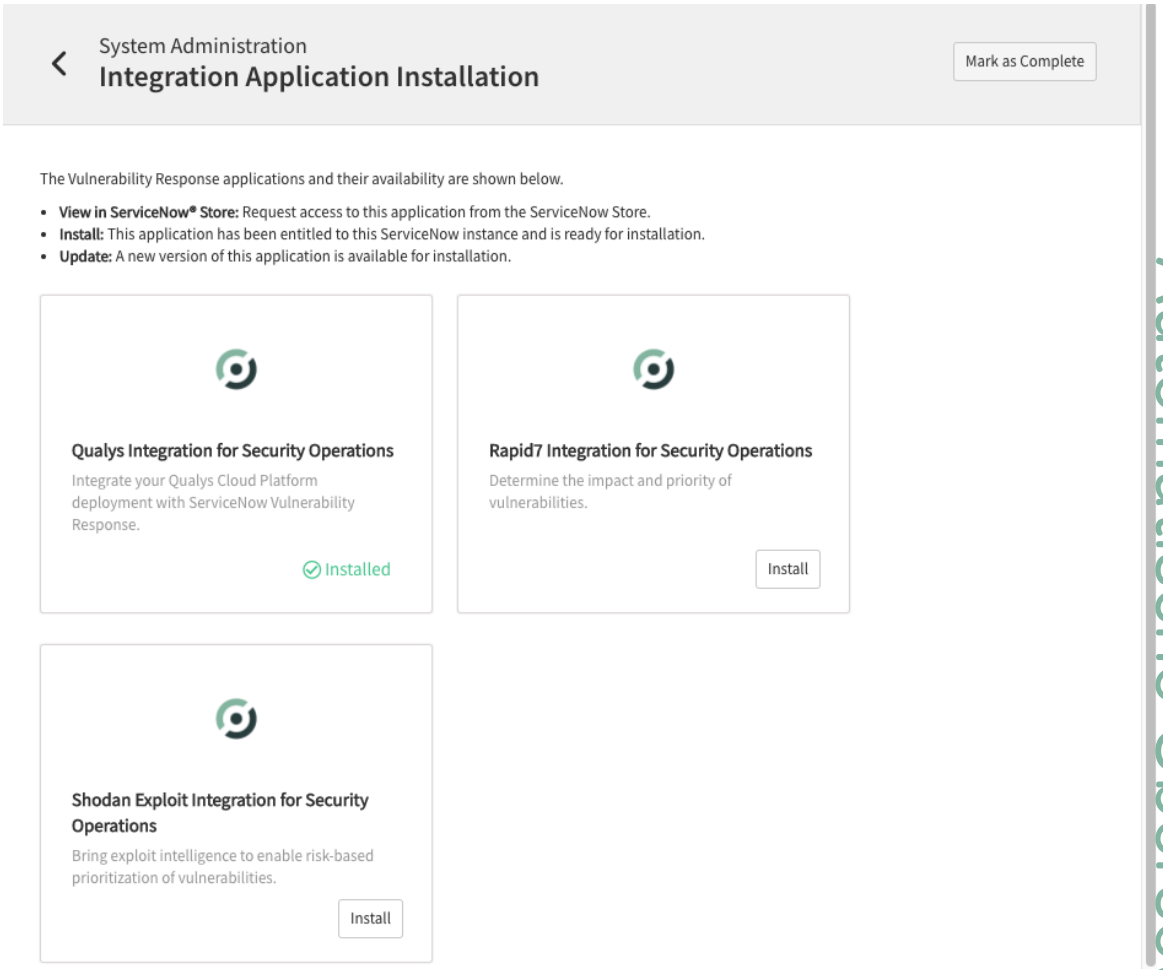
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Systemverwaltung** > **Installation der Integrationsanwendung**an.

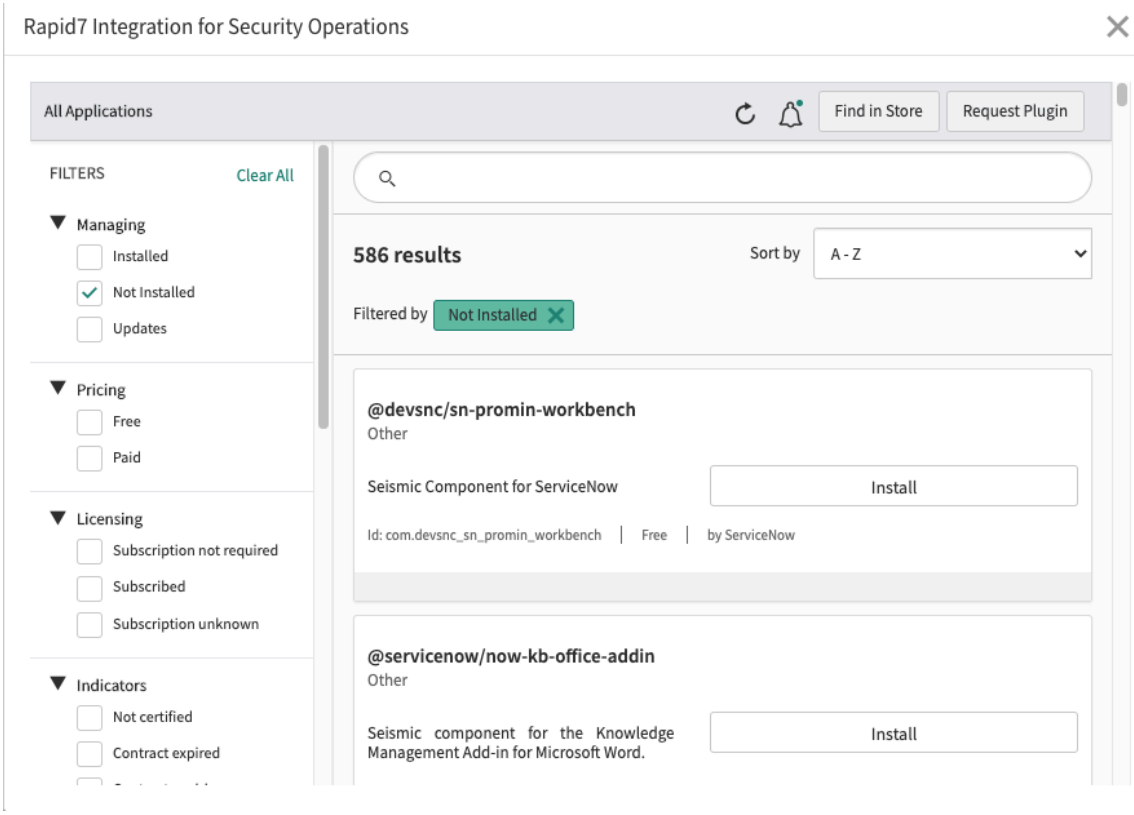
   Nach einigen Minuten werden die Anwendungen angezeigt, für die Sie berechtigt sind und die für die Installation in Ihrer Instanz verfügbar sind.



2. Suchen Sie die Anwendung, die installiert werden soll, und klicken Sie auf **Installieren** Auf der Anwendungskachel.
   Das Dialogfeld alle Anwendungen wird mit dem Namen der Anwendungskachel angezeigt, auf die Sie geklickt haben, z. B. Rapid7 Integration for Security Operations, wie in der folgenden Abbildung dargestellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

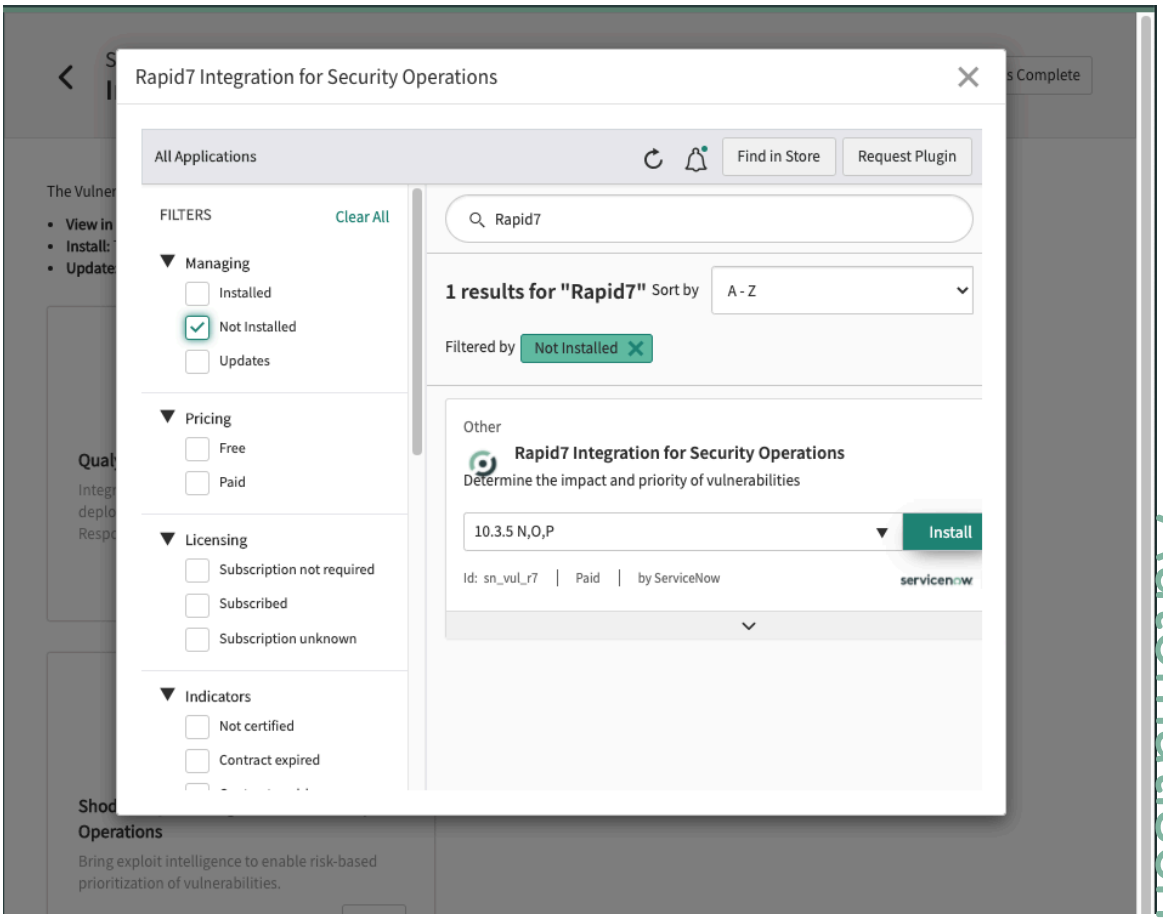


3. Suchen Sie die Anwendung, wählen Sie eine Version aus der Auswahlliste aus, und klicken Sie auf **Installieren** .

   Wenn für die Anwendung ein Update verfügbar ist, wird die **Aktualisieren** Schaltfläche wird angezeigt.

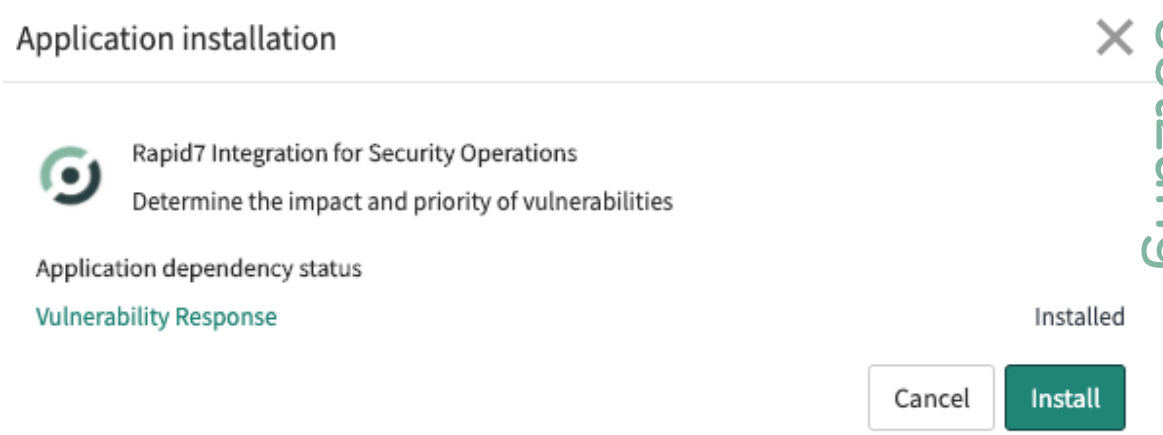
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Im Dialogfeld „Anwendungsinstallation“ wird der Status der Anwendungsabhängigkeit angezeigt. Alle erforderlichen Abhängigkeiten, die noch nicht installiert sind, werden automatisch zusammen mit der Anwendung installiert.

4. Klicken Sie im Dialogfeld „Anwendungsinstallation“ auf **Installieren** .



Das Dialogfeld „Installation“ zeigt an, wann die Installation erfolgreich abgeschlossen wurde.

5. Schließen Sie das Dialogfeld.
Die Seite „alle Anwendungen“ wird angezeigt und zeigt an, dass Ihre Anwendung erfolgreich installiert wurde.

Nach der Installation und Aktivierung können Sie die folgenden Anwendungen und installierten Lösungen direkt im Abschnitt „Integrationskonfiguration“ des Setup-Assistenten konfigurieren, planen und starten :

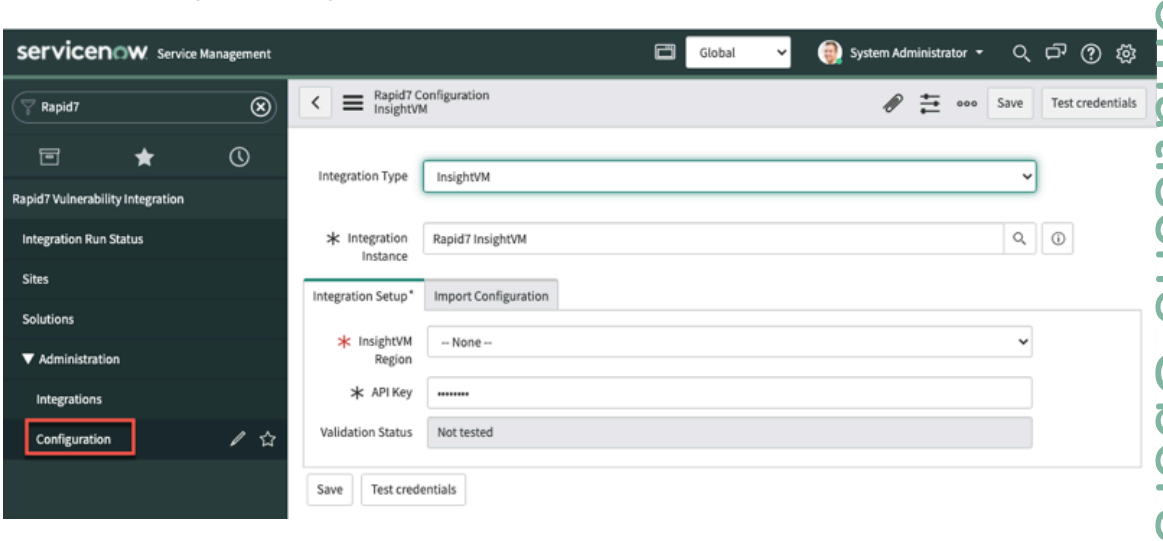
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Qualys Vulnerability Integration
- Die Vulnerability Response Integration with Tenable.
- Die Integration der Microsoft Security Response Center-Lösung
- Die Red Hat Solution Integration
- Integration der Microsoft Security Response Center-Lösung
- Die Microsoft Defender Vulnerability Management Integration

Navigieren Sie für andere Anwendungen, die oben nicht aufgeführt sind, direkt zum Konfigurationsmodul der Anwendung, um mit der Konfiguration fortzufahren und die erforderlichen Anmeldeinformationen von Drittparteien einzugeben. Die folgende Abbildung zeigt beispielsweise den Standort der Konfiguration und des Moduls für Rapid7 Anwendung.

Weitere Informationen zum Konfigurieren bestimmter Anwendungen finden Sie in der Installations- und Konfigurationsproduktdokumentation nach Produktnamen, die für die einzelnen Anwendungen bereitgestellt wird.



Nächste Maßnahme
Fahren Sie mit der Konfiguration Ihrer Anwendung im Setup-Assistenten fort, wenn Ihre Anwendung unterstützt wird.

Wenn Ihre Anwendung für die Konfiguration im Setup-Assistenten nicht unterstützt wird, navigieren Sie direkt zum Konfigurationsmodul der Anwendung, um mit der Konfiguration fortzufahren. Informationen zum Anzeigen unterstützter Anwendungen im Setup-Assistenten finden Sie unter Installation von Vulnerability Response Und unterstützte Anwendungen.

Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken

Wenn nicht bereits installiert, laden Sie die NVD-Integration herunter, führen Sie sie aus, und führen Sie die geplante CWE-Aufgabe als Teil Ihres ersten Setups von Vulnerability Response aus, bevor Sie Schwachstellendaten mit einem Scanner-Produkt einer Drittpartei in Ihre Instanz importieren. Die Vulnerability Response-Integration mit NVD ist im verfügbar ServiceNow Store.

CWE- und NVD-Daten werden erfasst

Importierte Daten aus den NVD- und CWE-Integrationen werden verwendet, um die Schwachstellendaten in Ihrer Instanz anzureichern und zu entscheiden, ob die Korrektur für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Schwachstelle, ein angreifbares Element oder eine Korrekturaufgabe eskaliert werden soll. Nach einem ersten Import können Sie Bibliotheksdatensätze bei Bedarf aktualisieren oder eine geplante Aufgabe konfigurieren, um Datensätze regelmäßig zu aktualisieren. Vulnerability Response Speichert sie unter **Bibliotheken** .

Das Common Vulnerability Scoring System (CVSS), das in NVD- und Drittanbietereinträgen enthalten ist, erfasst die Hauptmerkmale einer Schwachstelle. Vulnerability Response Verwendet CVSS-Daten, um einen normalisierten Wert zu erzeugen, der den Schweregrad der Schwachstelle widerspiegelt. Wenn der Schweregrad berechnet wird, vermittelt die Schwachstelle ein besseres Verständnis des Risikos, das von dieser Schwachstelle für Ihre Organisation ausgeht. Der Schweregrad hilft Ihnen, die Schwachstellenbeseitigung zu bewerten und zu priorisieren.

Wenn dies Ihre erste Installation von ist Vulnerability Response, Oder bevor Daten zum ersten Mal mit einem Scanner-Produkt einer Drittpartei erfasst werden:

1. Führen Sie einen ersten Import von CWE-Daten mit der CWE Comprehensive 2000 Integration durch.

   Weitere Informationen finden Sie unter Konfigurieren und führen Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen aus. Sie führen CWE-Updates durch **Bei Bedarf** Standardmäßig aus dem Integrationsdatensatz, und Sie müssen ihn konfigurieren, wenn er als geplante Aufgabe ausgeführt werden soll.

   Hinweis:
   Planen Sie die Ausführung der CWE-Aktualisierung vor der Aktualisierung der NVD-Datenbank. Der Standardtag für das NVD-Update ist **Wöchentlich** Ein **Montag** .

2. Verifizieren Sie Vulnerability Response Die Anwendung „Integration mit NVD“ wird installiert, und Daten aus der NIST National Vulnerability Database Integration – API (nur CVE) oder der NIST National Vulnerability Database Integration – API (CVE und CPE) wurden erfolgreich importiert.

   Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich. Nach der Installation wird die Integration der NIST National Vulnerability Database Integration – API (nur CVE) standardmäßig aktiviert. Wird täglich ausgeführt. Siehe Verstehen der NVD-Integrationen Und Installieren Sie Vulnerability Response Integration mit der NIST National Vulnerability Database Weitere Informationen finden Sie unter .

3. Drittparteibibliotheken werden als geplante Aufgaben aktualisiert. Weitere Informationen finden Sie in Ihrer Integrationsdokumentation unter Vulnerability Response-Integrationen Weitere Informationen zu Integrationen von Drittparteien.

Importierte Schwachstellendaten und angreifbare Elemente anzeigen

Die folgenden Bibliotheken sind verfügbar:

Bibliotheken	Beschreibung
NVD	Liste der von NVD gefundenen Schwachstellen und enthält Sicherheitsprüflisten, sicherheitsbezogene Softwarefehler, Fehlkonfigurationen, Produktnamen und Auswirkungsmetriken einschließlich Exploits.
CWE	Liste der in der Community entwickelten Softwareschwächungstypen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bibliotheken	Beschreibung
	Jeder CWE-Datensatz enthält auch einen zugehörigen wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über den Bildschirm „Allgemeine Schwachstellenaufzählungen“ eskalieren. Sie dient nur als Referenz.
Drittpartei	Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste zugehöriger Referenzen, angreifbarer Elemente, Exploits und CVEs.

Zugehörige Informationen

Anzeigen Vulnerability Response Schwachstellenbibliotheken

Anwendung Solution Management for Vulnerability Response installieren

Bevor Sie verwenden können Solution Management for Vulnerability Response Funktion von Vulnerability Response In Ihrer Instanz müssen Sie die Installation von abschließen Vulnerability Solution Management Anwendung. Diese Anwendung ist als separates Abonnement in verfügbar ServiceNow Store.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Führen Sie diese Setup-Aufgaben aus, um eine reibungslose Installation zu gewährleisten.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Die Integration der Microsoft Security Response Center-Lösung Und Red Hat Solution Integration Sind die Lösungsanwendungen in verfügbar Solution Management for Vulnerability Response Nach der Installation Vulnerability Solution Management.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Solution Management for Vulnerability Response Erfordert Vulnerability Response Anwendung. Für die aktuelle Version von Vulnerability Solution Management, Stellen Sie sicher, dass Sie die aktuelle Version von haben Vulnerability Response Installiert. Siehe KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema . Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.
Überprüfen Sie, ob Sie über die Berechtigung für die Anwendung verfügen.	Um sicherzustellen, dass Sie die Berechtigung für haben Vulnerability Solution Management Anwendung, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Um die Berechtigung für abzurufen Vulnerability Solution Management Anwendung aus dem ServiceNow Store Und laden Sie es auf Ihren herunter ServiceNow AI Platform Instanz, siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung.
Stellen Sie sicher, dass Ihre NVD-Datensätze für die letzten 10 Jahre auf dem neuesten Stand sind.	Weitere Informationen finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken.
Stellen Sie sicher, dass Ihre Schwachstellen von Drittparteien auf dem neuesten Stand sind.	Siehe Vulnerability Response-Integrationen Informationen zu Integrationen von Schwachstellen von Drittparteien.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow AI Platform Rollen, die Ihrer Instanz zugewiesen sind.	Die folgenden Rollen sind für die Installation und Verifizierung der erwarteten Ergebnisse erforderlich: Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response. • Der Systemadministrator [admin] installiert die Anwendung. Wenn nicht bereits zugewiesen, weist der Administrator die Rolle „Schwachstellenadministrator“ [sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)] zu. • Der Schwachstellenadministrator überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

Erforderliche Rollen: administrator zum Installieren von Vulnerability Solution Management Anwendungs- und Schwachstellenadministrator, um sie zu konfigurieren.

Prozedur

1. Navigieren Sie zum ServiceNow Store.
2. Klicken Sie Auf **Melden Sie sich an** Und geben Sie Ihre HI-Anmeldeinformationen ein.
3. Klicken Sie auf **ServiceNow-Produkte** Registerkarte, um die verfügbaren anzuzeigen ServiceNow Produkte.
4. Klicken Sie auf Plus (**+**) Unterzeichnen Sie neben **Schwachstellenlösungsmanagement** Um alle zugehörigen Anwendungen anzuzeigen, für die Sie berechtigt sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie Auf **Aktivieren** Um zu überprüfen, ob Sie die Berechtigung für haben Vulnerability Solution Management Zur Anwendung.
6. Wenn Sie bereits über eine Berechtigung verfügen, fahren Sie mit Schritt 10 fort, um die Anwendung auf Ihrem zu installieren ServiceNow AI Platform Instanz.
7. Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Akzeptieren** Um den Nutzungsbedingungen bei Aufforderung zuzustimmen.
   Eine Nachricht wird angezeigt, die angibt, dass Sie sich erfolgreich für die Anwendung angemeldet haben.
8. **Wahlweise:** Klicken Sie auf Berechtigung verwalten, wenn Sie Ihre Berechtigung für verwalten möchten Vulnerability Solution Management Auf Sonstiges ServiceNow AI Platform Instanzen.

   Hinweis:
   Wenn **Berechtigung Verwalten** Die Schaltfläche wird nicht angezeigt. Klicken Sie auf **Schwachstellenlösungsmanagement** Anwendung in der Produktliste, um sie anzuzeigen.

   a. Option wählen

   b. Klicken Sie Auf **OK** Oder **Abbrechen** Um fortzufahren.
   Sie sind bereit, Plugins zu aktivieren und die Anwendung auf Ihren Instanzen zu installieren.

9. Melden Sie sich bei an ServiceNow AI Platform Instanz, die Sie installieren möchten Vulnerability Solution Management Anwendung auf.
10. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
11. Suchen Sie nach Vulnerability Solution Management Anwendung (sn_vul_Solution), und klicken Sie auf **Installieren** .
    Im Dialogfeld „Anwendungsinstallation“ wird der Status des Plugins „Anwendungsabhängigkeit“ angezeigt. Alle erforderlichen Abhängigkeiten, die noch nicht installiert sind, werden automatisch zusammen mit der Anwendung installiert.
12. Klicken Sie auf **Installieren**.
    Diese Installation kann einige Zeit dauern. Nachdem die Anwendung und ihre Abhängigkeiten erfolgreich installiert wurden, wird im Dialogfeld „Installieren“ eine Nachricht angezeigt.

    Der Schwachstellenadministrator kann die Anwendung jetzt über den Setup-Assistenten konfigurieren.

13. Klicken Sie auf **Schließen**.

    Die Integration der Microsoft Security Response Center-Lösung Und Red Hat Solution Integration Sind die Lösungsanwendungen in verfügbar Solution Management for Vulnerability Response Nach der Installation Vulnerability Solution Management.

    Zeigen Sie die Schwachstellenlösungen an, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen**an. Weitere Informationen finden Sie unter Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management Mit dem Setup-Assistenten.

Nächste Maßnahme

Nachdem Sie die Anwendung und die verfügbaren Lösungen konfiguriert haben, überprüfen Sie, ob die Tabelle CVEs und Lösungen mit der Schwachstellenlösung [sn_vul_m2m_Vulnerability_Solution] zustimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie Performance Analytics for Vulnerability Response[PA] Anwendung

Bevor Sie verwenden können Performance Analytics for Vulnerability Response Anwendung müssen Sie die Berechtigung erhalten und die Anwendung aus herunterladen ServiceNow Store, Installieren Sie es auf Ihrem ServiceNow AI Platform® Und führen Sie einige Installations- und Konfigurationsschritte aus. Die PA-Anwendung wird nicht als Teil von installiert Vulnerability Response Anwendung. Sie ist als separates Abonnement verfügbar.

Vorbereitungen
Wenn Sie die Anwendung bereits in Ihrer Instanz haben und auf eine neuere Version der Anwendung aktualisieren, fahren Sie mit Schritt 8 in den folgenden Schritten fort, um mit der Aktualisierung und Konfiguration fortzufahren.

Für eine Neuinstallation führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Um zu überprüfen, ob Plugins und Anwendungen installiert und aktiviert sind, navigieren Sie zu **Alle** > **Subscription Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob das Plugin „Vulnerability Response-Abhängigkeiten“ (com.snc.vul_dep) installiert und aktiviert ist.	**Vulnerability Response-Abhängigkeiten** Dieses Plugin enthält alle Abhängigkeits-Plugins, die zur Unterstützung der Anwendung erforderlich sind. Um sicherzustellen, dass das Plugin installiert und aktiviert ist, soll die Anwendung in Ihrer Instanz zu navigieren **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an. Wenn Sie aufgefordert werden, andere Abhängigkeits-Plugins zu aktualisieren, klicken Sie auf die Links in den Dialogfeldern, und befolgen Sie die Anweisungen, um fortzufahren.
Überprüfen Sie, ob ServiceNow Vulnerability Response Anwendung (sn_vul) ist installiert und aktiviert.	**Vulnerability Response** Um sicherzustellen, dass das Plugin installiert und aktiviert ist, soll die Anwendung in Ihrer Instanz zu navigieren **Systemanwendungen** > **Alle**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

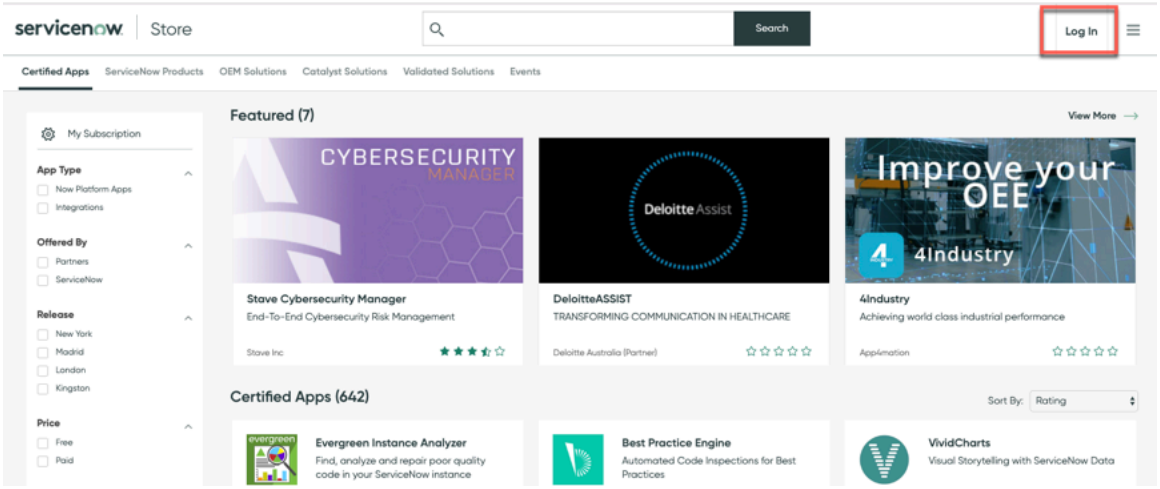
Setupaufgaben	Beschreibung
	verfügbaren Anwendungen > **Alle**an. Wenn Sie aufgefordert werden, andere Abhängigkeits-Plugins zu aktualisieren, klicken Sie auf die Links in den Dialogfeldern, und befolgen Sie die Anweisungen, um fortzufahren. Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich. Wenden Sie sich an ServiceNow, um Einzelheiten zu erfahren.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz. Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Der Performance Analytics-Administrator [PA_admin] oder das System [admin] installiert die Anwendung und überprüft die erwarteten Ergebnisse. • Der Schwachstellenadministrator [sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse mit den PA-Dashboards. • Der Korrekturbesitzer [sn_vul.Remediation_owner] überwacht Change-Management-Aufgaben und liest und aktualisiert zugewiesene Datensätze. Die Rolle „sn_vul.Remediation_owner“ wird ebenfalls automatisch zugewiesen, wenn einem Anwender die Rolle „itil“ zugewiesen wird.
Überprüfen Sie Performance Analytics und Vulnerability Response Anwendungen sind kompatibel.	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Erforderliche Rolle: admin oder pa_admin

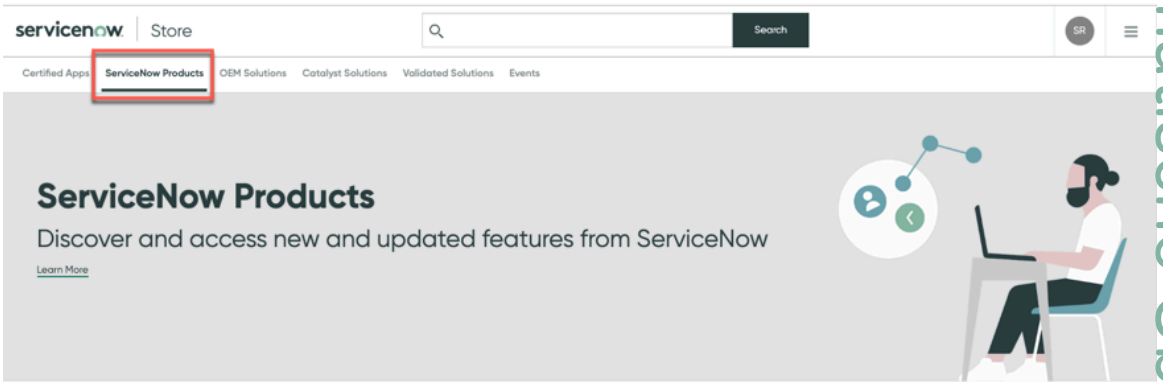
Prozedur

1. Um die Berechtigung zu erhalten und die Anwendung auf Ihren herunterzuladen ServiceNow AI Platform-Instanz navigieren Sie zu ServiceNow Store.
2. Klicken Sie oben rechts auf der Seite auf **Melden Sie sich an** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Geben Sie im angezeigten Dialogfeld Ihre HI-Anmeldeinformationen ein, und klicken Sie auf **Melden Sie Sich An** .
4. Klicken Sie auf der angezeigten Seite, wenn nicht ausgewählt, auf **ServiceNow-Produkte** Registerkarte.

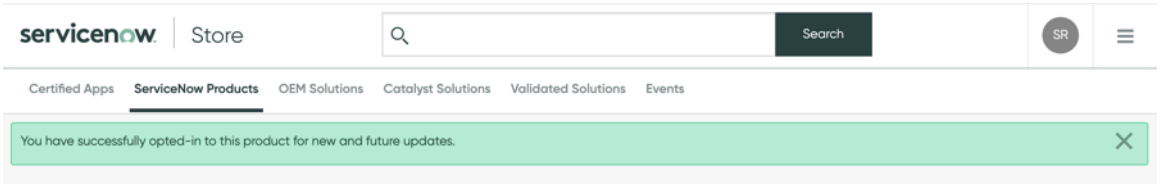


5. Klicken Sie auf der Produktlistenseite auf **Performance Analytics: Vulnerability Response** .

6. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
   Eine Seite mit der Schaltfläche „Aktivieren“ wird angezeigt.
7. Um abzurufen Performance Analytics for Vulnerability Response Anwendung klicken Sie auf **Aktivieren** .
8. Um den Nutzungsbedingungen zuzustimmen, aktivieren Sie bei der Aufforderung das Kontrollkästchen, und klicken Sie auf **Akzeptieren** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

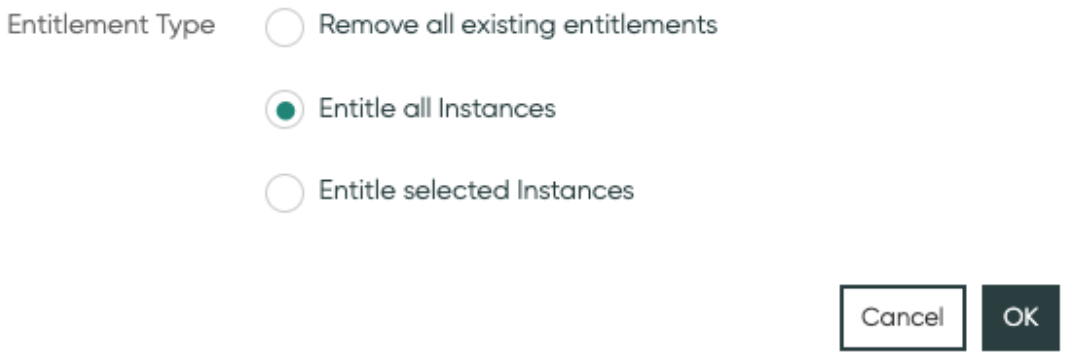


9. **Wahlweise:** Alternativ können Sie Ihre Berechtigung für die Anwendung auf einer anderen verwalten ServiceNow AI Platform Führen Sie die folgenden Schritte aus.

   a. Wenn die Schaltfläche Berechtigung verwalten nicht angezeigt wird, klicken Sie auf Performance Analytics for Vulnerability Response Anwendung in der Produktliste, um sie anzuzeigen.

   b. Klicken Sie bei ausgewählter Registerkarte berechtigt auf **Berechtigung Verwalten** .

   c. Wählen Sie im angezeigten Dialogfeld Berechtigungen für Vulnerability Response verwalten eine Option aus:

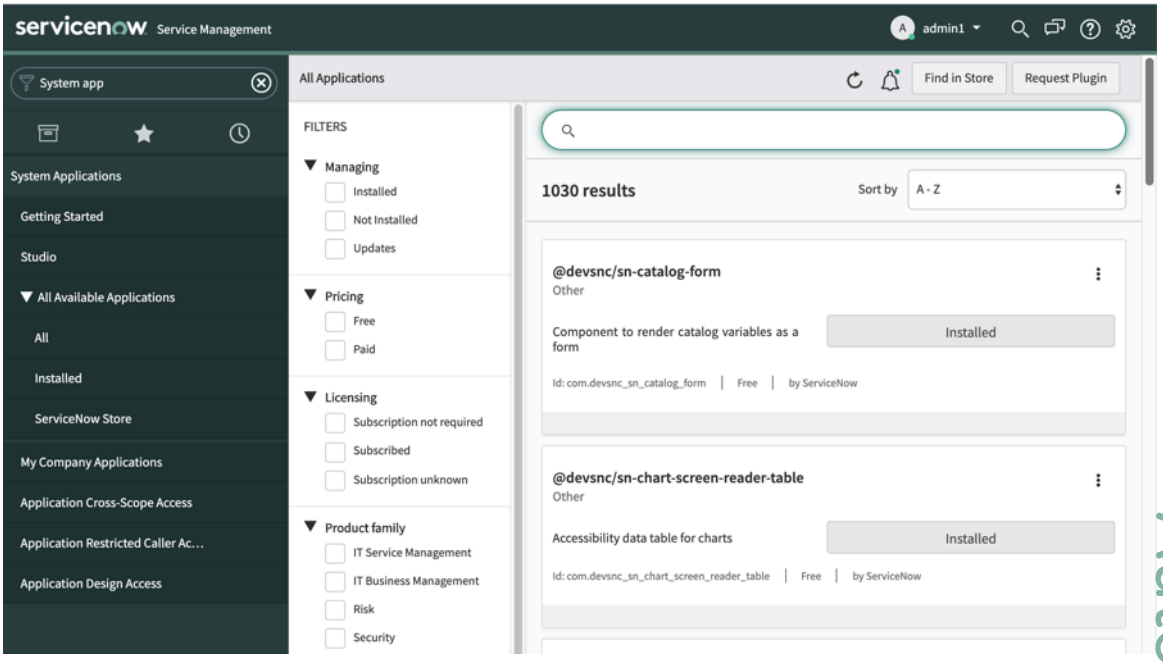


   d. Klicken Sie Auf **OK** Oder **Abbrechen** Um fortzufahren.
   Sie sind bereit, Plugins zu aktivieren und die Anwendung auf Ihrem zu installieren ServiceNow AI Platform Instanz(n).

10. Melden Sie sich bei an ServiceNow AI Platform Instanz, die Sie installieren möchten Vulnerability Response Anwendung auf.
11. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



12. Suchen Sie in den aufgeführten Anwendungen die Anwendung Performance Analytics – Content Pack – Vulnerability Response (sn_vul_Analytics), und klicken Sie auf **Installieren** .

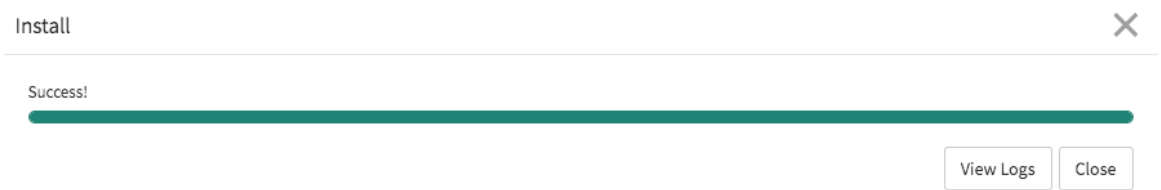
> **Hinweis:**
> Wenn Sie auf eine neue Version aktualisieren, wählen Sie die gewünschte Version aus der Auswahlliste aus.

Und klicken Sie auf **Aktualisieren** .
Das Dialogfeld Anwendungsinstallation wird angezeigt. Alle Abhängigkeiten, die automatisch mit der Anwendung installiert werden, werden ebenfalls angezeigt.

13. **Wahlweise:** Wenn Sie Demodaten möchten, aktivieren Sie das Kontrollkästchen Demodaten laden, und klicken Sie auf **Installieren** .

> **Hinweis:**
> Wenn Sie nicht auswählen **Demodaten laden** Kontrollkästchen, Demodaten sind nicht verfügbar, um von zu installieren **Anwendungsmanager** Später. Informationen zur Installation oder Neuinstallation von Demodaten nach der Erstinstallation finden Sie unter Problemumgehung zum Installieren von Demodaten, wenn die Anwendung bereits installiert ist [KB0722909] artikel in Now Support Knowledge Base.

Diese Installation kann einige Zeit dauern. Nachdem die Anwendung erfolgreich installiert wurde, wird im Dialogfeld „Installieren“ eine Nachricht angezeigt.



14. Klicken Sie auf **Schließen**.

15. **Wahlweise:** Wenn Sie eine große Anzahl aktiver angreifbarer Elemente in Ihrer Umgebung erwarten, sollten Sie möglicherweise die Standardeinstellung für die maximale Anzahl der gesammelten Datensätze ändern, geplante Aufgaben aktivieren und Erfassungszeiten außerhalb der Geschäftszeiten festlegen.

Automatische Übersetzung

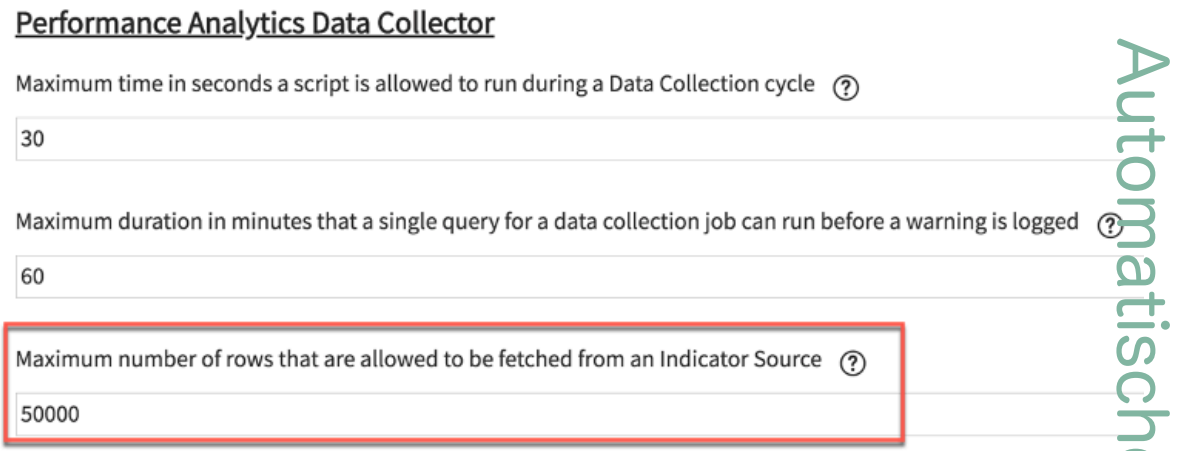
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um diese und andere Einstellungen für die Anwendung nach der Installation zu ändern, gehen Sie wie folgt vor.

a. Navigieren zu **Alle** > **Performance Analytics** > **Administratorkonsole**an.

b. Klicken Sie auf der Kachel „Erweiterte Konfiguration“ auf **Performance Analytics-Eigenschaften** Link.

c. Scrollen Sie auf der Seite Administratorkonsole [Performance Analytics] zum Abschnitt Performance Analytics-Datenerfasser.
Die Standardeinstellung (50.000 Datensätze) wird für die maximale Anzahl von Zeilen angezeigt, die aus einer Indikatorquelle abgerufen werden dürfen.



d. Möglicherweise möchten Sie diese Zahl auf einen Wert erhöhen, der ungefähr 20 % mehr ist als die Gesamtzahl der aktiven angreifbaren Elemente (VIS), die Sie in Ihrer Umgebung erwarten.

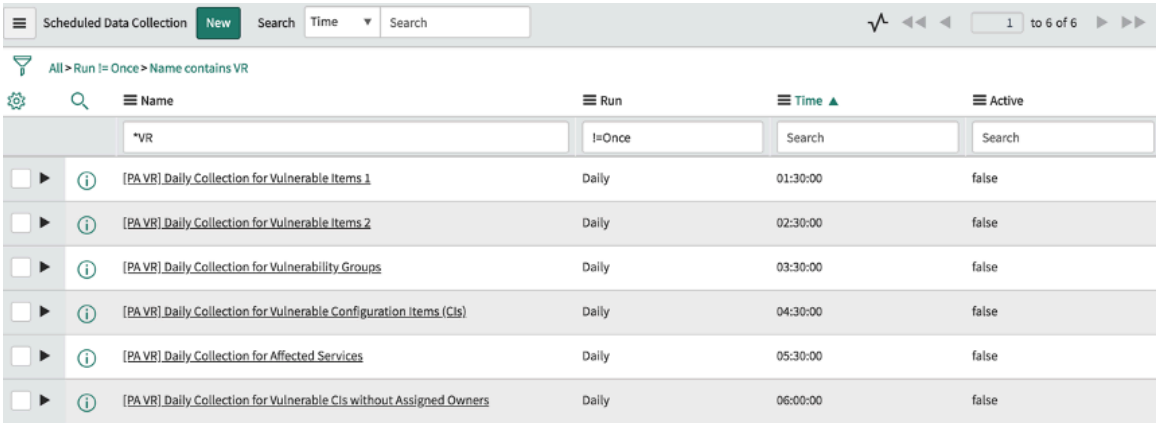
e. Klicken Sie auf **Speichern**.

f. Um geplante Aufgaben zu aktivieren, navigieren Sie zu **Performance Analytics** > **Datenerfasser** > **Aufträge**an.
Die Liste geplante Datensammlung wird angezeigt. In der Spalte aktiv sind die geplanten Aufgaben, die in der Spalte Anwendung für Performance Analytics – Inhaltspaket – Vulnerability Response aufgeführt sind, standardmäßig deaktiviert (Falsch).

Hinweis:
Eine geplante Aufgabe für die Erfassung von Verlaufsdaten wird nicht in der Liste der Aufgaben angezeigt. Bei großen Datensätzen können Sie mit der Erfassung von Daten und Trends im Laufe der Zeit beginnen, indem Sie Ihre täglichen Aufgaben aktivieren, wenn Sie Performance Analytics für einrichten Vulnerability Response Anwendung.

Automatische Übersetzung

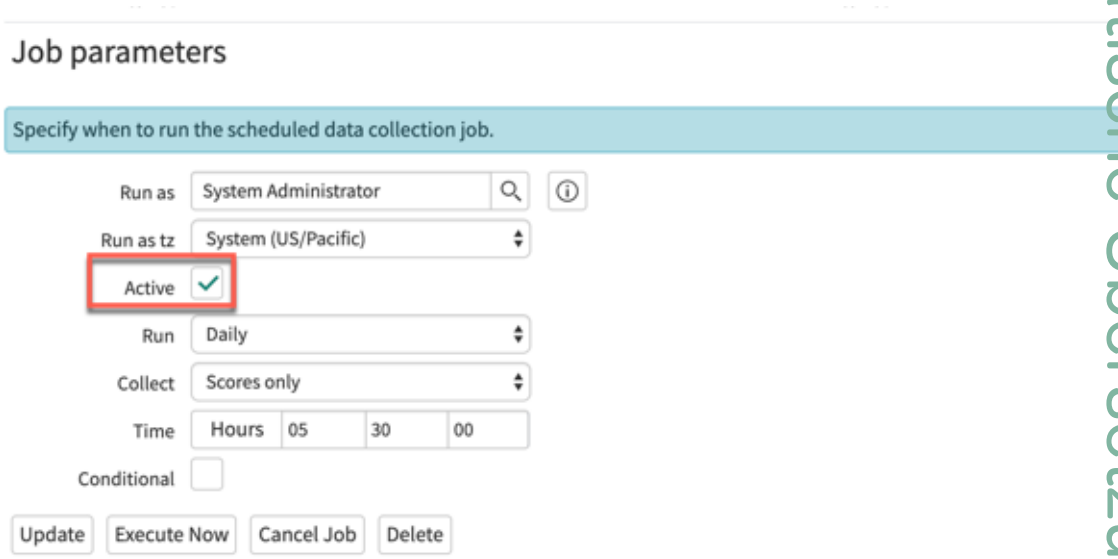
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



g. Klicken Sie in der Spalte Name auf einen Link, um einen PA_VR-Auftragsdatensatz zu öffnen.

h. Wenn Felder nicht bearbeitet werden können, klicken Sie auf **Hier** Link, um sie zu bearbeiten.

i. Klicken Sie im Abschnitt „Auftragsparameter“ auf das Kontrollkästchen aktiv, um einen Auftrag zu planen.
Die Zeitfelder werden angezeigt.



j. Geben Sie die Startzeit für den Auftrag ein.
Wenn Sie ein großes Volumen erwarten, ziehen Sie es möglicherweise vor, Sammlungszeiten außerhalb der Geschäftszeiten festzulegen. Wenn Sie mindestens 10 Millionen aktive VIS in Ihrer Umgebung erwarten, wenden Sie sich an Ihren ServiceNow® Implementierungspartner, um weitere Informationen zum Einrichten Ihrer Datensammlungsumgebung zu erhalten.

Weitere Informationen zu den für die Datensammlung verwendeten Indikatoren finden Sie unter Zeigen Sie an Performance Analytics-Indikatoren für Vulnerability Response[PA].

k. Nachdem Sie alle gewünschten Aufträge aktiviert haben, klicken Sie auf **Aktualisieren** .
Die Liste geplante Datensammlung wird angezeigt. Weitere Informationen finden Sie unter Performance Analytics-Eigenschaften .

Automatische Übersetzung

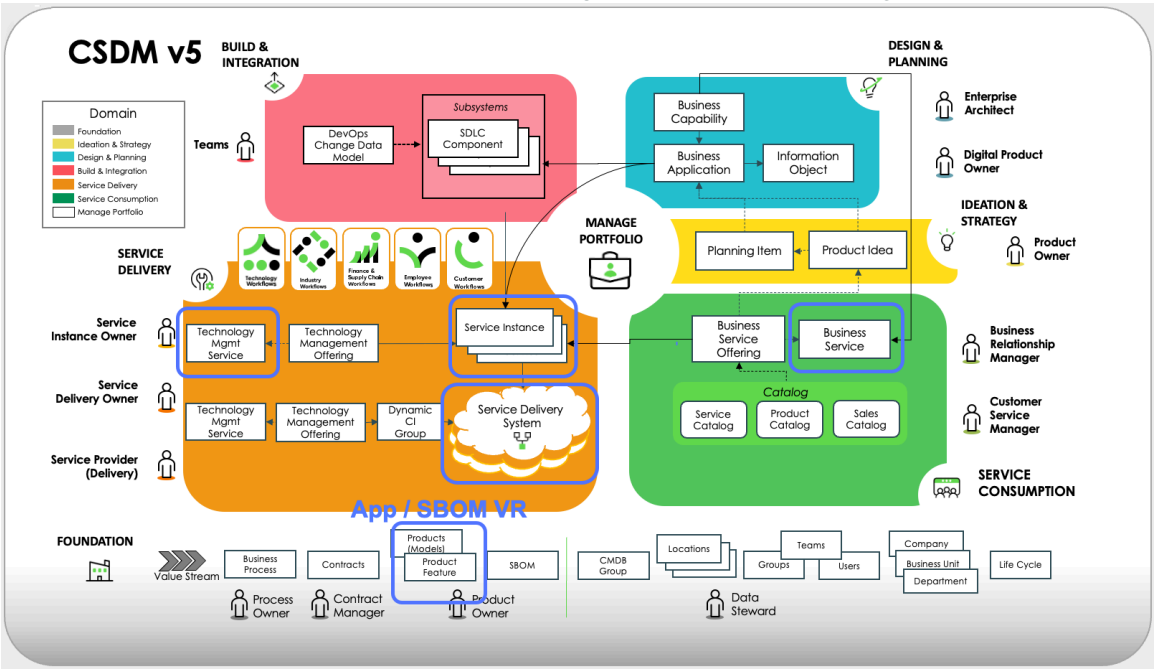
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Navigieren zu **Vulnerability Response** > **Übersicht** Zum Anzeigen des Dashboards.

Vulnerability Response Anwendungen Und CSDM Tabellen

Die Vulnerability Response, Application Vulnerability Response, Integrationen von Schwachstellen von Drittparteien und Software Bill of Materials Anwendungen verwalten (Daten mittragen zu) CSDM Tabellen. Diese Anwendungen verwenden auch Daten aus CSDM Tabellen, die andere Anwendungen generieren. Mehrere ServiceNow Produkte profitieren daher von diesen und fügen ihnen einen Mehrwert hinzu Security Operations Anwendungen.

Die CSDM Daten-Framework und Vulnerability Response Anwendungen



CSDM Tabellen, auf die verwiesen wird Vulnerability Response, Application Vulnerability Response, Integrationen von Schwachstellen von Drittparteien und Software Bill of Materials Anwendungen

Wenn Assets aus Schwachstellen-Scannern von Drittanbietern (Integrationen) importiert werden, werden sie in einbezogen Vulnerability Response Und in bestimmten Tabellen dargestellt:

- Host Vulnerability Response Erkannte Elemente.
- Cloud und Container Vulnerability Response Erkannte Images
- Application Vulnerability Response Erkannte Anwendungen (Produktmodell)

Als Teil von Security Operations CMDB-Konfigurationselement (CI) suchen, wird eine Suche durchgeführt, um einen CI-Datensatz aus importierten Daten mit vorhandenen Datensätzen in der CMDB abzugleichen.

Jeder spezifische CI-Datensatz kann nicht erkennbare Attribute enthalten, z. B. Supportgruppe oder Klassifizierung, die im CI ausgefüllt werden, das als Eingabe für Zuweisungsregeln für angreifbare Elemente verwendet werden kann. Diese Attribute können aus Synchronisierungen des Common Service Data Model (CSDM) basierend auf vorgelagerten technischen Serviceangeboten ausgefüllt werden.

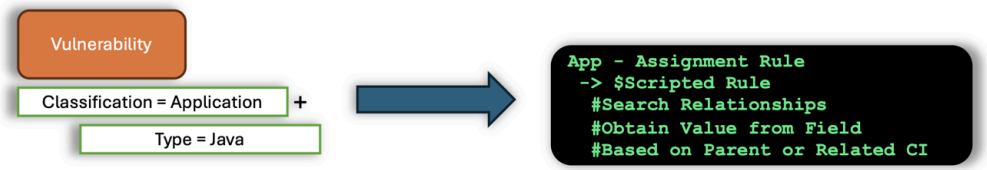
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie zugehörige CSDM-Objekte für nutzen möchten Vulnerability Response, Application Vulnerability Response, Integrationen von Schwachstellen von Drittparteien und Software Bill of Materials Anwendungen müssen Sie geskriptete Regeln verwenden.

Um beispielsweise angreifbare Elemente automatisch zur Korrektur mithilfe von Zuweisungsregeln für angreifbare Elemente zuzuweisen, können Sie eine Regel erstellen, die Klassifizierungswerte für Konfigurationselemente nutzt, wenn sie für importierte Schwachstelleneinträge aktualisiert werden. In diesem Fall benötigen Sie eine geskriptete Regel, um den gewünschten Zielwert aus dem zugehörigen CSDM-Objekt abzufragen.

Unten finden Sie ein Beispiel für eine geskriptete Abfrage, mit der Sie sehen können, ob ein CI Java hat und an einen Schwachstelleneintrag gebunden ist.



Scripted (query)

Vulnerability Response, Application Vulnerability Response, Integrationen von Schwachstellen von Drittparteien und Software Bill of Materials Anwendungen verweisen auf die folgenden Tabellen. Weitere Informationen finden Sie unter CSDM Daten-Framework und Vulnerability Response Anwendungsbild für weitere Informationen.

- Die Tabelle „Produktmodell“ [cmdb_model] (referenziert von Application Vulnerability Response Und Software Bill of Materials).
- Die Tabelle „Anwendungsmodell“ [cmdb_Application_Product_model] (referenziert von Application Vulnerability Response Und Software Bill of Materials).
- Die Tabelle „Konfigurationselement“ [cmdb_ci].
- Die Tabelle „Business-Service“ [cmdb_ci_Service_Business].
- Die Tabelle „Service“ [cmdb_ci_Service].
- Tabelle „CMDB-Gruppe“ [cmdb_Group].
- Tabelle „dynamische CI-Gruppe“ [cmdb_ci_query_based_Service].

CSDM Von verwendete Tabellen Vulnerability Response, Application Vulnerability Response, Integrationen von Schwachstellen von Drittparteien und Software Bill of Materials Anwendungen

1. Tabelle „Produktmodell“ [cmdb_model] (verwendet von Application Vulnerability Response Und Software Bill of Materials).
2. Tabelle „Anwendungsmodell“ [cmdb_Application_Product_model] (verwendet von Application Vulnerability Response Und Software Bill of Materials).
3. Die Tabelle „Konfigurationselement“ [cmdb_ci].
4. Geschäftsanwendung [cmdb_ci_Business_App] (verwendet von Application Vulnerability Response Und Software Bill of Materials).
5. Business-Service [cmdb_ci_Service_Business].
6. Tabelle „Technologiemanagement-Service“ [cmdb_ci_Service_Technical] (früher technischer Service).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn Sie hochladen Software Bill of Materials Dateien, versuchen die SBOM-Anwendungen, alle Produktmodelle und Geschäftsanwendungen abzugleichen, die Sie hochladen, denen, die bereits in Ihrer CMDB vorhanden sind. Sie können Serviceinstanzen verknüpfen (früher Anwendungsservices genannt) Oder Geschäftsanwendungen zu einem Produktmodell.

Produkte, die einen Mehrwert für hinzufügen Vulnerability Response, Application Vulnerability Response, Integrationen von Schwachstellen von Drittparteien und Software Bill of Materials Anwendungen

Mit Vulnerability Response Anwendungen mit den folgenden Elementen ServiceNow Produkte können Ihrer Organisation zugute kommen.

Schwachstellen-Scanner und -Integrationen von Drittparteien

Importierte Schwachstellen aus der National Vulnerability Database (NVD) und Erkennungsdaten von Drittanbieterscannern werden mit den Assets in Ihrer CMDB abgeglichen. Wenn eine importierte Schwachstelle mit einem vorhandenen Asset übereinstimmt, wird ein angreifbares Element erstellt. Angreifbare Elemente werden automatisch in Aufgaben zur Korrektur gruppiert, mit dem Geschäftskontext risikobewertet, priorisiert und den entsprechenden Teams zur Korrektur zugewiesen. Weitere Informationen und eine Liste der Integrationen finden Sie unter Vulnerability Response-Integrationen.

Die CWE Comprehensive 2000- und NVD-Integrationen

Importierte Daten aus den Integrationen der NIST National Vulnerability Database (NVD) und Common Weakness Enumeration (CWE) werden verwendet, um die Schwachstellendaten in Ihrer Instanz zu ergänzen und zu entscheiden, ob die Korrektur für eine Schwachstelle, ein angreifbares Element oder eine Korrekturaufgabe eskaliert werden soll. Siehe Verstehen der NVD-Integrationen und Konfigurieren und führen Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen aus, um weitere Informationen zu erhalten.

Produkte, die von der Integration mit profitieren Software Bill of Materials

Sicherheitsstatus-Überwachung

Sicherheitsstatus-Überwachung Ermöglicht Cybersicherheitsteams, Einblick in ihren gesamten Enterprise-Asset-Bestand zu erhalten und ihre allgemeine Sicherheitslage zu bestimmen. Richtlinien in SSÜ Kann Ihnen helfen, Assets mit Schwachstellen zu erkennen, die Sie mit importieren Vulnerability Response Anwendungen, mit denen Sie Sicherheitstool-Abdeckungslücken finden können.

Governance, Risk und Compliance

Verbinden Sie Sicherheit und IT mit einem integrierten Risikoprogramm, das kontinuierliche Überwachung, Priorisierung und Automatisierung bietet.

DevOps

Schützen Sie Ihre Umgebungen während der Softwareentwicklungszyklen vor potenziell schädlichen Komponenten mit GitHub-Aktionen, die Sie aus Ihrer GitHub-Umgebung initiieren. Laden Sie SBOM-Dateien in hoch ServiceNow AI Platform Aus Ihren GitHub-Repositorys.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen oder bearbeiten Vulnerability Response Zuweisungsregeln

Nachdem Sie Ihre erste Bewertung der Zuweisungsregeln mit dem Setup-Assistenten abgeschlossen haben, können Sie Regeln erstellen, um angreifbare Elemente basierend auf Filterbedingungen automatisch zuzuweisen. Diese Regeln weisen angreifbare Elemente zu, wenn sie importiert oder manuell erstellt werden.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Das Basissystem wird mit einer Schwachstellenzuweisungsregel geliefert. **Der CI-Supportgruppe zuweisen** , Der angreifbare Elemente derselben Zuweisungsgruppe wie die CI-Supportgruppe zuweist. Diese Regel kann mithilfe von Filterbedingungen geändert werden, oder Sie können eine neue Regel erstellen. Mit Zuweisungsregeln definieren Sie die Zuweisungsbedingungen und die Reihenfolge der Ausführung. Sobald ein VI einer Regelbedingung entspricht, wird die Zuweisungssuche beendet.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsregeln**an.
2. Öffnen Sie **Der CI-Supportgruppe zuweisen** Regel oder klicken Sie auf **Neu** .
3. Wenn **Neu** Füllen Sie die Felder im Formular entsprechend aus.

Zuweisungsregel für Schwachstellen

Feld	Beschreibung
Name	Name der Gruppenregel.
Aktiv	Gibt an, ob die Zuweisungsregel aktiv ist.
Ausführungsreihenfolge	Reihenfolge, in der die Regeln ausgewertet werden. Regeln mit hoher Priorität, Elemente, die eine besondere Behandlung erfordern, bei denen das Risiko kritisch ist oder ein VI von regulatorischer Compliance behandelt werden sollte, um zuerst ausgeführt zu werden. Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung gilt R Erfüllt, und Sie wissen, wer für sie verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um der Gruppe VIS zuzuweisen, die ermittelt, welcher Zuweisungsgruppe sie angehören soll. Diese Gruppe kann eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel würde zuletzt ausgeführt.
Beschreibung	Beschreibung der Zuweisungsregel.
Bedingung	
Vorschau	Zeigt an, wie viele Ergebnisse diese Abfrage zurückgibt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bedingungsfelder	Bedingungen, die erfüllt werden müssen. **Hinweis:** Zu erstellen Rapid7 InsightVM Asset-Tags, die zur Verwendung im Bedingungsfilter für Zuweisungsregeln verfügbar sind, müssen Sie ausführen Rapid7 InsightVM Integration der Asset-Liste vor der anderen Rapid7 InsightVM Integrationen. Die Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird in diesem Datensatz oder Formular nicht unterstützt.
Neues Kriterium	Fügt weitere Bedingungsfilterfelder zur Auswahl hinzu.
Zuweisen mit	Um die Zuweisung von Gruppen zu automatisieren, die basierend auf dieser Regel erstellt wurden, wählen Sie eine der verfügbaren Optionen aus. ○ Anwendergruppe: Wählen Sie eine Anwendergruppe aus der Suchtabelle aus. ○ Anwendergruppenfeld: Wählen Sie ein Anwendergruppenfeld aus dem Dropdown-Menü aus. ○ Skript: Erstellen oder bearbeiten Sie ein Skript. **Hinweis:** Das Erstellen oder Bearbeiten eines Skripts erfordert ServiceNow Fachwissen.

4. Klicken Sie auf **Absenden**.
   Neue oder aktualisierte Regeln werden beim nächsten Import ausgewertet.

Hinweis:

Die Funktion „erneut anwenden“ erfordert eine Baseline-Anwendung der Regeln. Sobald Ihre Regeln erstellt wurden und Sie dies noch nicht getan haben, aktivieren Sie `Reapply all vulnerability assignment rules`Geplante Aufgabe, die nach Belieben ausgeführt werden soll. Sie wendet alle Regeln auf alle offenen VIS an, mit Ausnahme der manuell zugewiesenen. Je nachdem, wie viele aktive VIS Sie in Ihrer Umgebung haben, denken Sie daran, die festzulegen **Ausführen** Feld entsprechend nach der ersten Ausführung, um Leistungsauswirkungen zu vermeiden.

Wenn Sie diese geplante Aufgabe nicht ausgeführt haben, wenn Sie versuchen, zu verwenden **Änderungen Anwenden** Schaltfläche im Formular „Zuweisungsregeln“. Sie müssen es dann tun. Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.

Erstellen Sie einen Vulnerability Response Zuweisungsregel mit ML

Verwenden Sie das folgende Skript, um eine Catch-all-Zuweisungsregel für angreifbare Elemente zu erstellen, die ML-Empfehlungen von Predictive Intelligence verwendet, um sie automatisch zur Korrektur zuzuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Empfehlungen für die Schwachstellenzuweisung für Vulnerability Response Die Anwendung muss installiert und aktiviert sein. Diese Anwendung ist auf verfügbar ServiceNow Store.

Eine Klassifizierungslösung muss definiert, aktiv und trainiert sein. Mit diesem Modell können Sie die entsprechende Zuweisungsgruppe für angreifbare Elemente (VI) vorhersagen, wenn Ihre Zuweisungsregeln keine richtige Übereinstimmung für die beabsichtigten Empfänger gefunden haben.

Diese Regel kann Ihnen helfen, die Anzahl der nicht zugewiesenen VIS zu reduzieren, nachdem andere Zuweisungsregeln bereits abgeschlossen wurden.

Siehe Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response installieren und Erstellen und trainieren Sie eine Lösungsdefinition für Vulnerability Response, um weitere Informationen zu erhalten.

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie ziehen es möglicherweise vor, diese Aufgabe nur auszuführen, wenn Sie über erweiterte Codierungserfahrung verfügen oder über fundierte Kenntnisse über verfügen ServiceNow AI Platform, Seine Predictive Intelligence-Funktionen und wie Zuweisungsregeln funktionieren.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsregeln**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Siehe Erstellen oder bearbeiten Vulnerability Response Zuweisungsregeln Um weitere Informationen zu diesen Feldern zu erhalten.
4. Wählen Sie in der Auswahlliste Zuweisen mit die Option aus **Skript** .
5. Kopieren Sie im Editor das folgende Skript, und fügen Sie es ein.

```
  /*
  * Catch-all assignment rule using ML recommendation
  * NOTE: Requires Vulnerability Assignment Recommendations for Vulnerability Response
  * Classification Solution must be active and trained
  */
var vitID = current.sys_id;
getMLAssignmentRecommendation(vitID);

function getMLAssignmentRecommendation(vulnerableItemSysId) {
  var ARU = new sn_vul.AssignmentRecommendationUtils();
  ARU.initialize();

  var viPredictionObj = ARU.getPredictionsForVI(vulnerableItemSysId);
  /*
  *returns object containing array of predictions
  *payload structure:
  *
  {
    "predictions": [
      {
        "sys_id": "b6ed54f3db7b23005daef4eabf9619f3",
        "name": "Windows Server support ",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "confidence_score": "57.54"
        },
        ...
    ],
    "exception": ""
}
*/
var viPredictionArray = viPredictionObj['predictions'];
var topPredictionObj = viPredictionArray.shift();

return topPredictionObj['sys_id'];
}
```

6. Wählen Sie **Absenden**.

Nächste Maßnahme

Überprüfen Vulnerability Response Übersicht über Zuweisungsregeln Für allgemeinere Informationen zu Zuweisungsregeln und *`Reapply all vulnerability assignment rules`*Geplante Aufgabe.

Erstellen Sie einen Vulnerability Response Zuweisungsregel für Service-Support

Verwenden Sie das folgende Skript, um eine Regel zu erstellen, die angreifbare Elemente für die Korrektur basierend auf den Business-Services, die sich auf sie auswirken, zuweist.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie ziehen es möglicherweise vor, diese Aufgabe nur auszuführen, wenn Sie über erweiterte Codierungserfahrung verfügen oder über fundierte Kenntnisse über verfügen ServiceNow AI Platform Und wie Zuweisungsregeln funktionieren.

Mit dieser Regel werden VIS entsprechend der Übereinstimmung mit den in Ihrer CMDB aufgeführten Business-Services zugewiesen. Wenn keine zugehörigen Services, Abteilungen oder Supportgruppen übereinstimmen, werden VIS der Schwachstellenanalystengruppe zugewiesen.

Diese Regel kann Ihnen helfen, die Anzahl der VIS zu reduzieren, die falsch zugewiesen wurden oder nicht zugewiesen bleiben, nachdem andere Zuweisungsregeln bereits abgeschlossen wurden.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsregeln**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Siehe Erstellen oder bearbeiten Vulnerability Response Zuweisungsregeln Um weitere Informationen zu diesen Feldern zu erhalten.
4. Wählen Sie in der Auswahlliste Zuweisen mit die Option aus **Skript** .
5. Kopieren Sie im Editor das folgende Skript, und fügen Sie es ein.

```
/*
Assigns Vulnerable Item based on related Business Service
Assigns to default Vulnerability Analyst group if no related Business Service
*/
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
assignToServiceSupport(current);

function assignToServiceSupport(vitGR) {
   var ci = vitGR.getValue('cmdb_ci');
   var defaultAssignmentGroup = 'Vulnerability Analyst';
   var defaultGR = new GlideRecord('sys_user_group');
   defaultGR.get('name', defaultAssignmentGroup);
   var defaultAssignmentGroupID = defaultGR.sys_id;

   var maxSizeValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_size", 1000);
   var maxDepthValue =
global.SecProperty.getProperty("sn_sec_cmn.services_affected_by_CI_max_depth", 10);
   var customValues = {
      "maxDepth": maxDepthValue,
      "maxSize": maxSizeValue
   };
   var ciu = new global.CIUtils();
   var services = ciu.servicesAffectedByCI(ci, customValues);
   var svc = new GlideRecord("cmdb_ci_service");
   var hasSvc = false;
   if (services && services.length > 0) {
      svc.addQuery("sys_id", "IN", services.join(",")); // returns the service with highest
business criticality. Implement alternate logic here.
      svc.addNotNullQuery("busines_criticality"); // typo intended
      svc.orderBy("busines_criticality");
      svc.setLimit(1);
      svc.query();
      hasSvc = svc.next();
   }
   if (!hasSvc) {
      // If there are no services it should be assigned to a default assignent group
      return defaultAssignmentGroupID;
   } else {
      var serviceAssignmentGroup = hasSvc.getValue('support_group'); //Also consider
managed_by_group, assignment_group, change_control
      return !gs.nil(serviceAssignmentGroup) ? serviceAssignmentGroup :
defaultAssignmentGroupID; //Return the Service assignment group if it is not empty, return
the default assignment group otherwise.
   }
}
```

6. Wählen Sie **Absenden**.

Nächste Maßnahme

Überprüfen Vulnerability Response Übersicht über Zuweisungsregeln Für allgemeinere Informationen zu Zuweisungsregeln und *`Reapply all vulnerability assignment rules`*Geplante Aufgabe.

Erstellen oder bearbeiten Vulnerability Response Regeln für Korrekturaufgaben

Nachdem Sie Ihre erste Bewertung der Regeln für Korrekturaufgaben mit dem Setup-Assistenten abgeschlossen haben, können Sie Regeln erstellen, um angreifbare Elemente automatisch basierend auf Filterbedingungen zu gruppieren. Diese Regeln gruppieren angreifbare Elemente automatisch, wenn sie importiert oder manuell erstellt werden. Verwenden Sie den Filter, um die nach dieser Regel gruppierten angreifbaren Elemente einzuschränken, z. B. die Auswahl aller angreifbaren Elemente mit Exploits.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Das Basissystem wird mit einer Korrekturaufgabenregel geliefert. **Schwachstelle** , Welche angreifbare Elemente nach Schwachstelle und Zuweisungsgruppe gruppiert (aus **Zuweisungsregeln**). Sie können die Regeln über das Formular oder die Listenansicht erneut anwenden. Für einige Beispieleinträge Vulnerability Response Beispiele für Regel für Korrekturaufgaben.

Diese Regel kann wie folgt geändert werden:

Mithilfe von Filterbedingungen und Auswahlmöglichkeiten für Gruppieren.

Standardmäßig werden Korrekturaufgaben verwendet **Zuweisungsregeln** , Falls verfügbar, als Teil ihrer Filterkriterien.

Hinweis:
Wenn keine Zuweisungsregeln vorhanden sind, können Sie mit eine Gruppe auswählen **Anwendergruppe** Feld.

Ab Version 18,0 von Vulnerability Response, **Schwachstelle** Die Regel für Korrekturaufgaben ist in deaktiviert Vulnerability Response Für neue Implementierungen.

Prozedur
1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Regeln für Korrekturaufgaben**an.
2. Öffnen Sie die Regel, oder klicken Sie auf **Neu** .
3. Wenn **Neu** Füllen Sie die Felder im Formular entsprechend aus.

Regel für Korrekturaufgaben

Feld	Beschreibung
Name	Name der Aufgabenregel.
Aktiv	Gibt an, ob die Aufgabe aktiv ist.
Beschreibung	Eine Beschreibung der Regel.
Groß-/ Kleinschreibung beachten	Bestimmt, ob bei einer Bedingung die Groß-/Kleinschreibung beachtet wird oder nicht. **Hinweis:** Beim Standardwert wird die Groß-/Kleinschreibung nicht berücksichtigt.
Bedingung	Optionale Filterbedingungen für die Regel. **Hinweis:** Zu erstellen Rapid7 InsightVM Asset-Tags, die zur Verwendung im Bedingungsfilter für Regeln für Korrekturaufgaben verfügbar sind, müssen Sie ausführen Rapid7 InsightVM Integration der Asset-Liste vor der anderen Rapid7 InsightVM Integrationen. Standardmäßig (**Groß-/Kleinschreibung beachten** Kontrollkästchen deaktiviert) wird bei dem Suchtext, den Sie in den Bedingungsgenerator für Aufgabenregeldatensätze und -Formulare eingeben, die Groß-/Kleinschreibung nicht beachtet. Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	haben die Möglichkeit, Suchvorgänge mit Groß-/Kleinschreibung in Aufgabendatensätzen und -Formularen zu aktivieren.
Gruppieren nach (bis zu sechs Bedingungssätze sind verfügbar)	
Angreifbare Elemente gruppieren aus	Die Tabelle, die die Regel zum Gruppieren von VIS verwendet. Sie können bis zu sechs Filter haben. Die Auswahlmöglichkeiten lauten wie folgt: ○ Angreifbares Element [sn_vul_vulnerable_item] ○ Angreifbares Element → Konfigurationselement [cmdb_ci] ○ Angreifbares Element → Schwachstelle [sn_vul_third_Party_entry] **Hinweis:** Wenn Sie eine erweiterte Tabelle auswählen, wird die **Feld wird verwendet** Wird nur für angreifbare Elemente angewendet, die diese erweiterte Tabelle verwenden.
Mit Feld	Feld in der Tabelle, das die Regel zum Gruppieren von VIS verwendet.
Zuweisung	
Korrekturaufgaben zuweisen nach	Wenn Korrekturaufgaben automatisch zugewiesen werden, wird zusätzlich zu die Zuweisungsauswahl verwendet **Gruppieren Nach** Auswahlmöglichkeiten zum Gruppieren der angreifbaren Elemente. Bei Bedarf werden neue Aufgaben erstellt, um sicherzustellen, dass jedes angreifbare Element in einer Aufgabe mit einem übereinstimmenden Zuweisungsgruppensatz platziert wird. Um die Zuweisung von Aufgaben zu automatisieren, die basierend auf dieser Regel erstellt wurden, wählen Sie eine der verfügbaren Optionen aus. ○ Feld „Gruppieren nach“: Wenn Sie ein Anwendergruppenfeld aus ausgewählt haben **Feld wird verwendet** Werte in **Gruppieren nach** Abschnitt, werden sie im Dropdown-Menü angezeigt. ○ Anwendergruppe: Verwenden Sie die Suchliste, um eine statische Anwendergruppe auszuwählen.

Hinweis:
Wenn Sie Ihre Meinung zu einem der ändern **Gruppieren nach** Einstellungen, die **Löschen Sie die Felder „Gruppieren nach“** Zugehöriger Link setzt zurück **Gruppieren nach** Felder im Formular.

Wenn eine Gruppenregel aus der Formular- oder Listenansicht gelöscht wird, haben Sie die Möglichkeit, alle zu löschen **Öffnen** Von dieser Regel erstellte Gruppen. Gruppen nicht in **Öffnen** status sind ausgeschlossen.

Einige Beispieleinträge finden Sie unter Vulnerability Response Beispiele für Regel für Korrekturaufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie Felder und Gewichtungen für die Risikoregel für Vulnerability Response-Risikorechner

Passen Sie die Parameter und Gewichtungen für die Risikoregel an, damit Sie Risikopunktzahlen generieren können, die die Schwachstellen- und Asset-Daten verwenden, die für Ihre Organisation spezifisch sind. Indem Sie die Felder auswählen, die in der Risikoregel enthalten sind, können Sie ein effektives Risikobewertungs-Framework definieren.

Vorbereitungen

Darüber hinaus können Sie Attribute in Configuration_item [cmdb_ci] in der Configuration Management Database (CMDB) verwenden, um Logik für Ihre Vulnerability Response-Risikorechner zu erstellen. Wenn Sie beispielsweise feststellen, dass CIs, die in Ihrer Organisation nach außen gerichtet sind, angreifbarer sind und möglicherweise sofortige Nachbesserungen erfordern, können Sie Attribute wie zuweisen `Internet Facing`Für diese CIs. Dieses Attribut und andere sind in den Versionshinweisen des Common Service Data Model für das Orlando-Familien-Release aufgeführt. Für aktuelle Informationen und Anleitungen zum CMDB, Siehe die folgenden Themen:

- Konzeptionelles Modell des allgemeinen Servicedatenmodells
- CMDB-Schemamodell

Erforderliche Rolle: sn_vul.manage_Risk_Score_Configuration

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Schwachstellen-Rechner**an.
2. Wählen Sie auf der Seite Schwachstellenrechner die Option aus **Standardrisikorechner** .
3. Navigieren zu **Seite „Schwachstellen-Rechner“** > **Registerkarte „Regeln des Schwachstellenrechners“** > **Standardrisikoregel**an.
4. **Wahlweise:** Legen Sie im Abschnitt „Risikorechnerkriterien“ der Seite „Schwachstellenrisikoregel“ die Gewichtung für jedes Kriterium entsprechend seiner Bedeutung bei der Berechnung der Gesamtrisikopunktzahl fest.
5. Um die Regel zu deaktivieren, müssen Sie löschen **Aktiv** Kontrollkästchen.
6. Um Risikoregelfelder zu den Kriterien des Risikorechners hinzuzufügen, wählen Sie aus **Fügen Sie Kriterien hinzu** .
7. Füllen Sie im Formular die Felder aus.

Formular „Risikoregelfeld“

Feld	Beschreibung
Referenztabelle auswählen	Tabelle, die Sie zum Definieren der Gewichtung der Risikopunktzahl verwenden. Sie können eine dieser Optionen auswählen: ○ **Angreifbares Element** : Fügen Sie Felder hinzu, die direkt vom angreifbaren Element (VI) aus DOT-Walking-fähig sind. ○ **Angreifbares Element: Konfigurationselement** : Fügen Sie Dot-Walk-Felder hinzu, die Teil der Basistabellenerweiterungen sind, z. B.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	die Hardwaretabelle. Diese Felder sind nicht Teil der Basistabelle (cmdb_ci). ○ **Angreifbares Element: Schwachstelle** : Fügen Sie Dot-Walk-Felder hinzu, die Teil der Tabellen sind, die die Basistabelle erweitern, z. B. Drittparteieintrag. Diese Felder sind nicht Teil der Basistabelle „Schwachstelleneintrag“. ○ **Referenztabelle Für Angreifbares Element** : Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) sind, oder Tabellen, die einen Verweis auf das angreifbare Element haben. Diese Felder können nicht direkt vom VI aus per Dot-Walking ausgeführt werden ○ **Konfigurationselement-Referenztabelle** : Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von cmdb_ci sind, oder Tabellen, die einen Verweis auf cmdb_ci haben. Diese Felder können nicht direkt vom VI aus per Dot-Walking ausgeführt werden ○ **Referenztabelle Für Schwachstellen** : Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von sn_vul_entry sind, oder Tabellen, die einen Verweis auf sn_vul_entry haben. Diese Felder können nicht direkt vom VI aus per Dot-Walking ausgeführt werden ○ **Anwenderdefinierte Bedingungen** : Verwenden Sie diese Option, um der Regel Gewichtungen zuzuweisen, indem Sie die Bedingung auswerten. Beispielsweise bestimmt der Filter mit Internetzugriff, ob ein Konfigurationselement (Configuration Item, CI) extern oder intern ist.
Tabelle	Feld, das nur angezeigt wird, wenn eine der folgenden Optionen in der Referenztabelle auswählen ausgewählt ist: ○ **Angreifbares Element -> Konfigurationselement** ○ **Angreifbares Element -> Schwachstelle** ○ **Referenztabelle für angreifbare Elemente** ○ **Referenztabelle für Konfigurationselemente** ○ **Referenztabelle für Schwachstellen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Feld	Feld, das für die Berechnung der Risikopunktzahl für diese Regel verwendet werden soll.
Aggregation	Feld, das nur angezeigt wird, wenn eine Referenztabelle aus der Referenztabelle auswählen ausgewählt wird. Wählen Sie den Mindest- oder Höchstwert aus, der für Berechnungen berücksichtigt werden soll, wenn das Feld aus den zugehörigen Tabellen (m2m) ausgewählt wird.
Gewichtung	Gewichtung dieses Felds innerhalb der Risikoregel. Der Wert muss eine Ganzzahl von 0 bis 100 sein.
Definieren Sie Die Wertgewichtung	Komponente, um jedem Feldwert Gewichtungen zuzuweisen. Für numerische Felder können Feldwerte als Bereich definiert werden (z. B. 1–5). Die Gewichtungen müssen eine Ganzzahl zwischen 0 und 100 sein. **Hinweis:** Dieses Feld wird nicht angezeigt, wenn die Option Anwenderdefinierte Bedingungen in der Referenztabelle auswählen ausgewählt ist.
Bedingungstabelle	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenztabelle auswählen ausgewählt sind. Wählen Sie eine Bedingung aus der Liste aus.
Feldname	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenztabelle auswählen ausgewählt sind. Geben Sie einen Namen für die Risikokriterien ein.
Bedingung	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenztabelle auswählen ausgewählt sind. Zeigen Sie eine Vorschau der Elemente in dieser Tabelle an, die den definierten Bedingungen entsprechen.

8. Wählen Sie **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Aktivieren Sie auf der Seite „Regel“ die Regel, und wenden Sie sie erneut an, um die Risikopunktzahl für die aktiven angreifbaren Elemente neu zu bewerten.

Hinweis:
Ab Version 23,0 von Vulnerability Response, Im Fall von:

- **Standardrisikorechner** Regel: Wenn sich die Risikopunktzahl für ein angreifbares Element (VIT) ändert, werden die folgenden Details im Abschnitt „Notizen“ der VIT dokumentiert:
  - Rechnergruppenname
  - Rechnername
  - Feldwerte mit einer Gewichtung größer als 1 und ihrem Beitrag zur Risikopunktzahl.
  - Endgültige Risikopunktzahl
- **Schwachstellenschweregrad** Risikoregel: Immer wenn die Risikopunktzahl für eine VIT aktualisiert wird, wird die aktualisiert **Notizen** Abschnitt wird mit den folgenden Details aktualisiert:
  - Rechnergruppenname
  - Rechnername: Je nachdem, ob die Rechnerregel auf einer Vorlage oder einem Skript basiert, wird der Name mit den Details in Klammern angehängt. Um die Basis der Rechnerregel zu ändern oder anzuzeigen, wählen Sie eine beliebige Regel aus, und wählen Sie aus **Erweiterte Ansicht** Kontrollkästchen. Von **Werttyp** Wählen Sie im Dropdown-Feld die erforderliche Option aus. Wenn **Vorlage** Ist ausgewählt, wird die Risikopunktzahl gemäß der in der Regel angegebenen Bedingung aktualisiert. Wenn **Skript** Ist ausgewählt, können Sie das vorhandene Skript entweder hinzufügen oder aktualisieren.

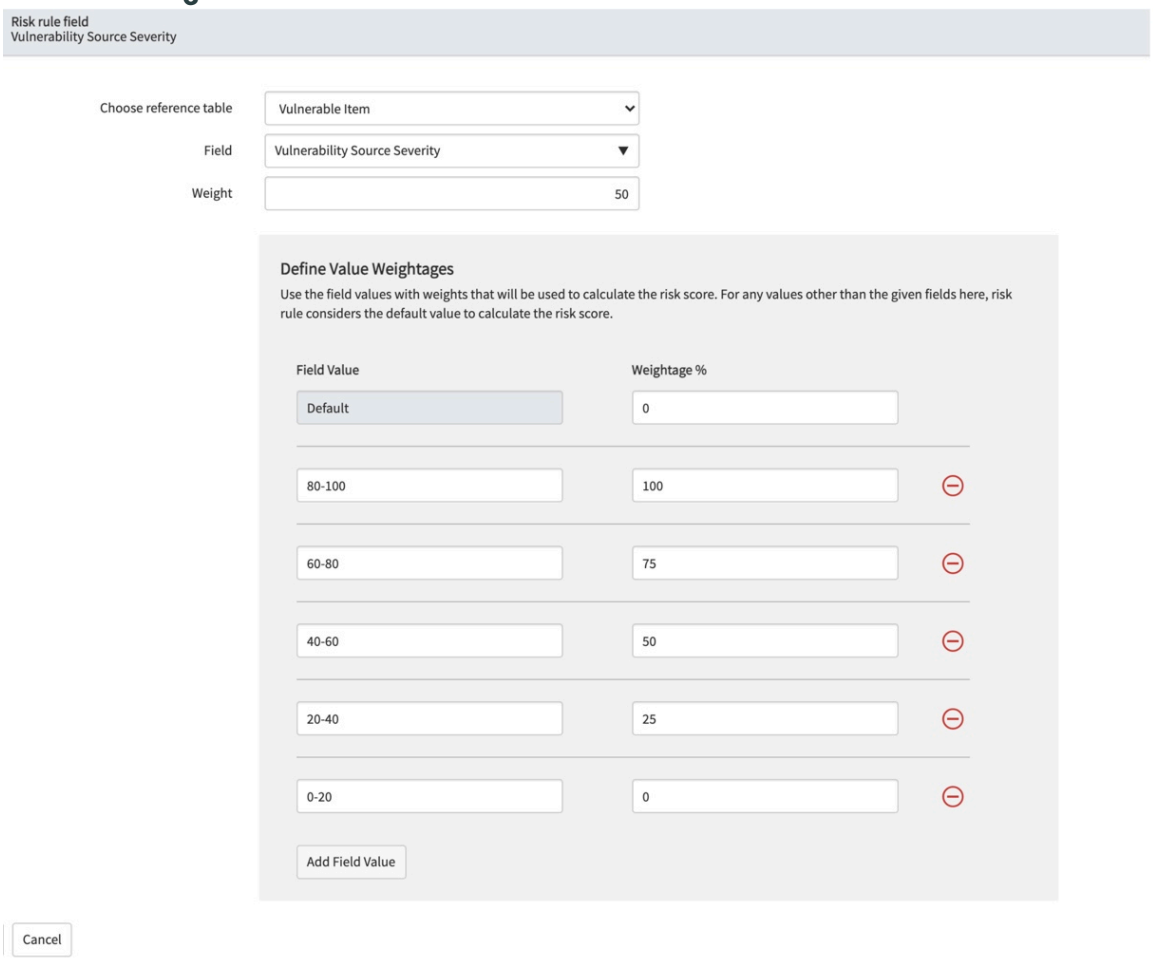
Example:
Beispiel 1: Fügen Sie einen Quellschweregrad als Kriterium für eine Risikoregel hinzu.

Anwendungsfall: Drittpartei-Lieferanten wie Qualys und Tenable geben ihre eigenen Punktzahlen an. Diese Punktzahlen werden in ausgefüllt **Quellenschweregrad** Feld in der Tabelle „sn_vul_entry“. Verwenden Sie dieses Feld für Berechnungen der Risikopunktzahl. Um diese Punktzahl zur Berechnung der Risikopunktzahl zu verwenden, gehen Sie wie folgt vor:

1. Navigieren Sie zur Seite „Risikoregel“.
2. Um die Regel zu deaktivieren, löschen Sie **Aktiv** Kontrollkästchen.
3. Um Risikoregelfelder zu den Kriterien des Risikorechners hinzuzufügen, wählen Sie aus **Fügen Sie Kriterien hinzu** .
4. Wählen Sie in der Liste Referenztabelle auswählen die Option aus **Angreifbares Element** .
5. Wählen Sie in der Feldliste aus **Schwachstelle.Quellenschweregrad** .
6. In **Gewichtung** Feld die relative Wichtigkeit dieses Felds innerhalb der Risikoregel eingeben. Der Wert muss eine Ganzzahl von 0 bis 100 sein.
7. Fügen Sie im Abschnitt „Wertgewichtung definieren“ Feldwerte hinzu, und weisen Sie ihnen eine Gewichtung zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle der angreifbaren Elemente



8. Wählen Sie **Absenden**.

Beispiel 2: Fügen Sie eine Geschäftsrelevanz als Kriterium für eine Risikoregel hinzu.

Anwendungsfall: Nehmen wir an, dass Ihre Organisation über viele Business-Services verfügt. Das Configuration Item (CI) LINUX-SF-6381 wird von den folgenden Services verwendet:

Relevanz der Business-Services

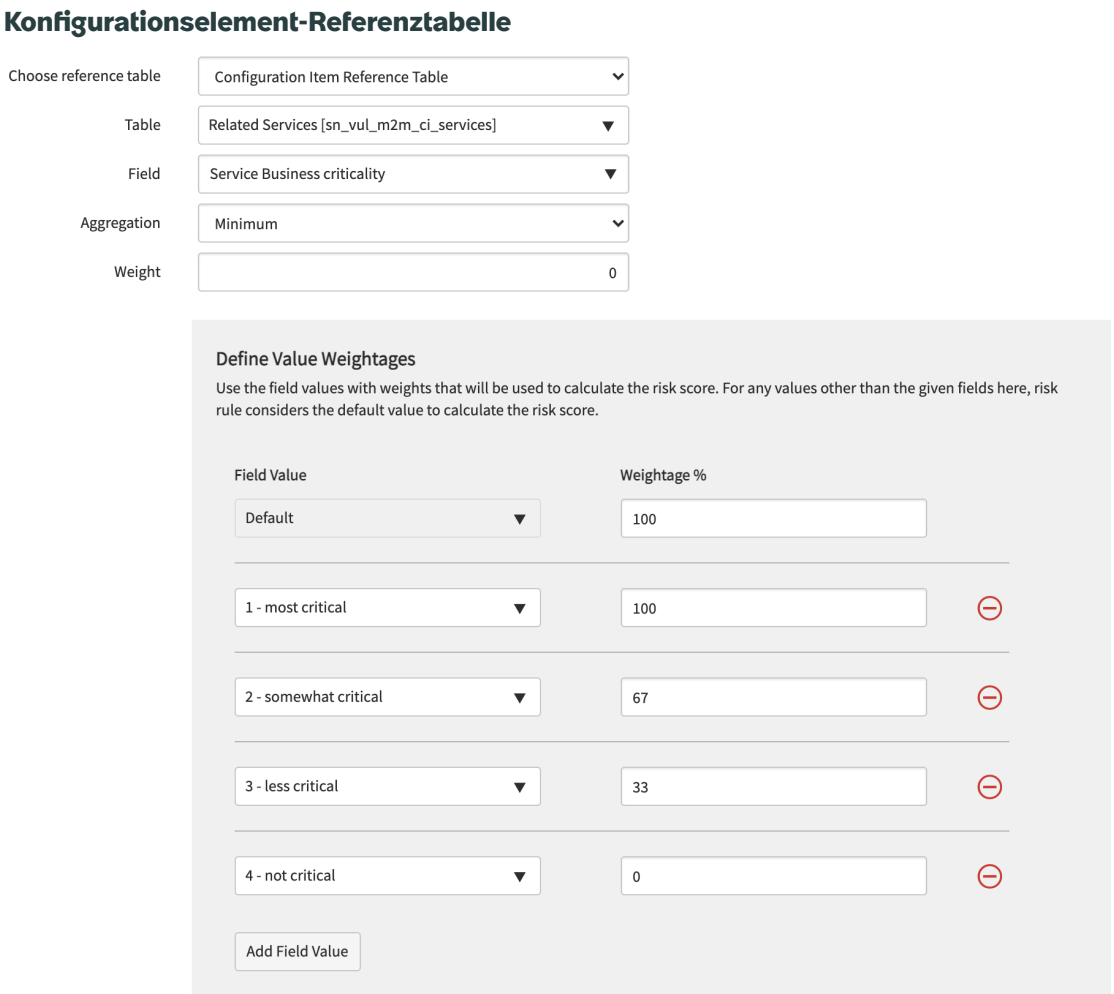
Geschäftsservice	Relevanz
Cloud-Management	1 – Sehr kritisch
E-Commerce	2 – Kritisch
Client-Services	3 – Weniger kritisch
Reise und Ausgaben	4 – Nicht kritisch

Die Zuordnung zwischen CI und Services wird in der Tabelle „zugehörige Services“ [sn_vul_m2m_ci_Services] gespeichert. Wenn eine Schwachstelle im Asset LINUX-SF-6381 gefunden wird, wird ein angreifbares Element (VI) erstellt. Sie können den Wert der Geschäftsrelevanz aus den betroffenen Services verwenden, um die Risikopunktzahl für dieses VI zu berechnen Um den Relevanzwert dieser Services zur Berechnung der Risikopunktzahl zu verwenden, gehen Sie wie folgt vor:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren Sie zur Seite „Risikoregel“.
2. Um die Regel zu deaktivieren, löschen Sie **Aktiv** Kontrollkästchen.
3. Um Risikoregelfelder zu den Kriterien des Risikorechners hinzuzufügen, wählen Sie aus **Fügen Sie Kriterien hinzu** .
4. Wählen Sie in der Liste Referenztabelle auswählen die Option aus **Konfigurationselement-Referenztabelle** .
5. Wählen Sie in der Liste Tabelle die Option aus **Zugehörige Services [sn_vul_m2m_ci_Services]** .
6. Wählen Sie in der Feldliste aus **Service.Geschäftsrelevanz** .
7. In **Zusammenfassung** Feld auswählen **Minimum** Dient zum Abrufen des kritischsten Service für diesen Anwendungsfall (**1: Am kritischsten** Wert) oder Maximum, um den am wenigsten kritischen Service für diesen Anwendungsfall abzurufen (**4: Nicht kritisch** Wert) für diesen Anwendungsfall.
8. In **Gewichtung** Feld die relative Wichtigkeit dieses Felds innerhalb der Risikoregel eingeben. Der Wert muss eine Ganzzahl von 0 bis 100 sein.
9. Fügen Sie im Abschnitt „Wertgewichtungen definieren“ Feldwerte hinzu, und weisen Sie ihnen eine Gewichtung zu.



10. Wählen Sie **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel 3: Fügen Sie dem Risikorechner ein bedingtes Kriterium hinzu.

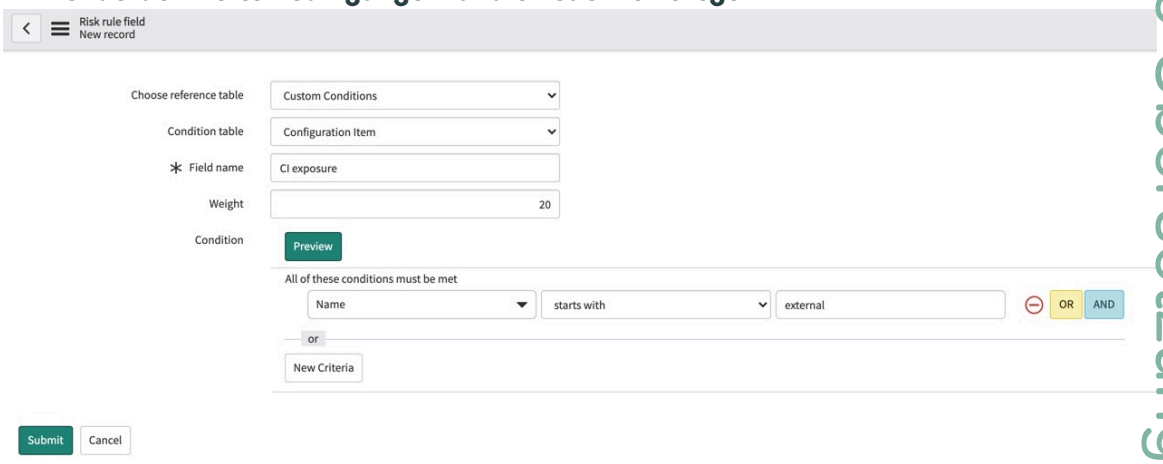
Angenommen, eine Organisation hat mehrere Konfigurationselemente (Configuration Items, CIs), von denen nur einige von einem externen Anwender aufgerufen werden können. Benutzer können Risikopunktzahlgewichtungen für diese nach außen gerichteten CIs hinzufügen.

Hinweis:
Sie können diese CIs anhand ihres Namens identifizieren. Die Namen beginnen mit „extern“.

Gehen Sie wie folgt vor, um der Risikoregel ein bedingtes Kriterium hinzuzufügen:

1. Navigieren Sie zur Seite „Risikoregel“.
2. Um die Regel zu deaktivieren, löschen Sie **Aktiv** Kontrollkästchen.
3. Um Risikoregelfelder zu den Kriterien des Risikorechners hinzuzufügen, wählen Sie aus **Fügen Sie Kriterien hinzu** .
4. Wählen Sie in der Liste Referenztabelle auswählen die Option aus **Anwenderdefinierte Bedingungen** .
5. Wählen Sie in der Liste Bedingungstabelle die Option aus **Konfigurationselement** .
6. In **Feldname** Geben Sie den Namen ein **CI-Risiko** .
7. In **Gewichtung** Feld die relative Wichtigkeit dieses Felds innerhalb der Risikoregel eingeben. Der Wert muss eine Ganzzahl von 0 bis 100 sein.
8. In **Bedingung** Feld auswählen **Name** > **beginnt mit** Und geben Sie den Wert ein **Extern** .

Anwenderdefinierte Bedingungen für die neue Risikoregel



9. Wählen Sie **Absenden**.

Hinweis:
Das Hinzufügen bedingter Kriterien zu Ihrer Risikoregel kann die Leistung beeinträchtigen.

Zugehörige Informationen

Vulnerability Response-Rechner und Regeln für Schwachstellenrechner

Erstellen Sie einen Vulnerability Response-Rechner

Filterung in Vulnerability Response

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Rollup-Rechner

Verwenden Sie nach der ersten Bewertung der Risikorechner im Setup-Assistenten die Schwachstellen-Rollup-Rechner, um zu konfigurieren, wie die kumulative Risikopunktzahl für Korrekturaufgaben und importierte Schwachstellen berechnet wird.

Verwenden Sie die Schwachstellen-Rollup-Rechner, um zu konfigurieren, wie die kumulative Risikopunktzahl für Korrekturaufgaben und importierte Schwachstellen berechnet wird. Die folgenden Rollup-Rechner sind im Lieferumfang des Basissystems enthalten:

- *`Remediation Task Rollup`*: Führt ein Rollup der Risikopunktzahlen für alle angreifbaren Elemente in Korrekturaufgaben durch, um eine Gesamtrisikopunktzahl für die gesamte Gruppe angreifbarer Elemente bereitzustellen.
- *`Patch Update Rollup`*: Führt ein Rollup der Risikopunktzahlen für alle angreifbaren Elemente mit demselben Patch-Update durch, um eine Gesamtrisikopunktzahl für das Patch-Update bereitzustellen.
- *`Organization Risk Score Rollup`*: Führt ein Rollup der Risikopunktzahlen für alle angreifbaren Host-Elemente, angreifbaren Anwendungselemente, angreifbaren Container-Elemente und Konfigurationsprobleme in einer Organisation durch, um eine Gesamtrisikopunktzahl für die gesamte Organisation im einheitlichen Dashboard bereitzustellen.

  Hinweis:
  Beginnend mit v22.0 von Vulnerability Response, Sie können Rollup-Gewichtungen für die Organisationspunktzahl konfigurieren. Außerdem wurden einzelne Rollup-Rechner entfernt.

- *`Vulnerable Item Rollup`*: Führt ein Rollup der Risikopunktzahlen für alle angreifbaren Host-Elemente in einer Organisation durch, um zur Gesamtrisikopunktzahl der gesamten Organisation für ein einheitliches Dashboard beizutragen.
- *`Vulnerability Entry Rollup`*: Führt ein Rollup der Risikopunktzahlen für alle angreifbaren Elemente mit demselben Schwachstelleneintrag durch, um eine Gesamtrisikopunktzahl für den Schwachstelleneintrag bereitzustellen.
- *`Rollup EPSS Scores from NVD to TPEs`*: Führt ein Rollup der EPSS-Punktzahlen für alle angreifbaren Elemente/CVEs durch, die im NVD aufgeführt sind Tabelle Für vorhandene TPEs, um eine Gesamtwahrscheinlichkeit der Ausnutzung der Schwachstelle bereitzustellen.
- *`Remediation Effort Rollup`*: Führt ein Rollup der Risikopunktzahlen für alle Datensätze in einer Korrekturmaßnahme durch, um eine Gesamtrisikopunktzahl für die Korrekturmaßnahme bereitzustellen.

Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Rechner für Schwachstellen-Rollup**an.

Konfigurieren Sie den Rollup-Rechner, um anzugeben, wie viel Gewichtung jedem dieser berechneten Werte beim Festlegen der kumulativen Risikopunktzahl zugewiesen werden soll. Je höher die Gewichtung, desto mehr wird dieser Wert verwendet, um die Rollup-Risikopunktzahl in den Schwachstellen- oder Korrekturaufgaben zu bestimmen.

Hinweis:
Wenn **Zurückgestellte einschließen** Ist ausgewählt, werden alle zurückgestellten angreifbaren Elemente in die Rollup-Berechnung für die Korrekturaufgaben einbezogen. Stellen Sie sicher, dass Sie die Auswirkungen auf die Gesamtberechnung verstehen, bevor Sie diese Option auswählen.

Rollup-Rechner führen die geplante Aufgabe aus, *`Rollup vulnerable item values to vulnerability and groups`*, Alle 15 Minuten, um Änderungen zu übernehmen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und die Details und Risikopunktzahlen für Korrekturaufgaben und Schwachstellen zusammenzufassen. Diese geplanten Aufgaben berechnen auch kumulative Werte für die Anzahl der VIS, die maximale Risikopunktzahl, das Korrekturzieldatum und den Status für Korrekturaufgaben.

Hinweis:
Berechnete Werte für Schwachstelleneinträge enthalten keine Korrekturzieldaten.

Die Risikopunktzahl wird berechnet, wenn:

- Die Risikopunktzahl, das Korrekturziel, der Korrekturstatus oder die Schwachstelle ändert sich für die angreifbaren Elemente.
- Der Status des angreifbaren Elements ändert sich in Offen, zurückgestellt, Geschlossen oder ändert sich von Geschlossen oder zurückgestellt.
- Angreifbare Elemente werden gelöscht.
- Angreifbare Elemente werden der Korrekturaufgabe hinzugefügt oder daraus entfernt.

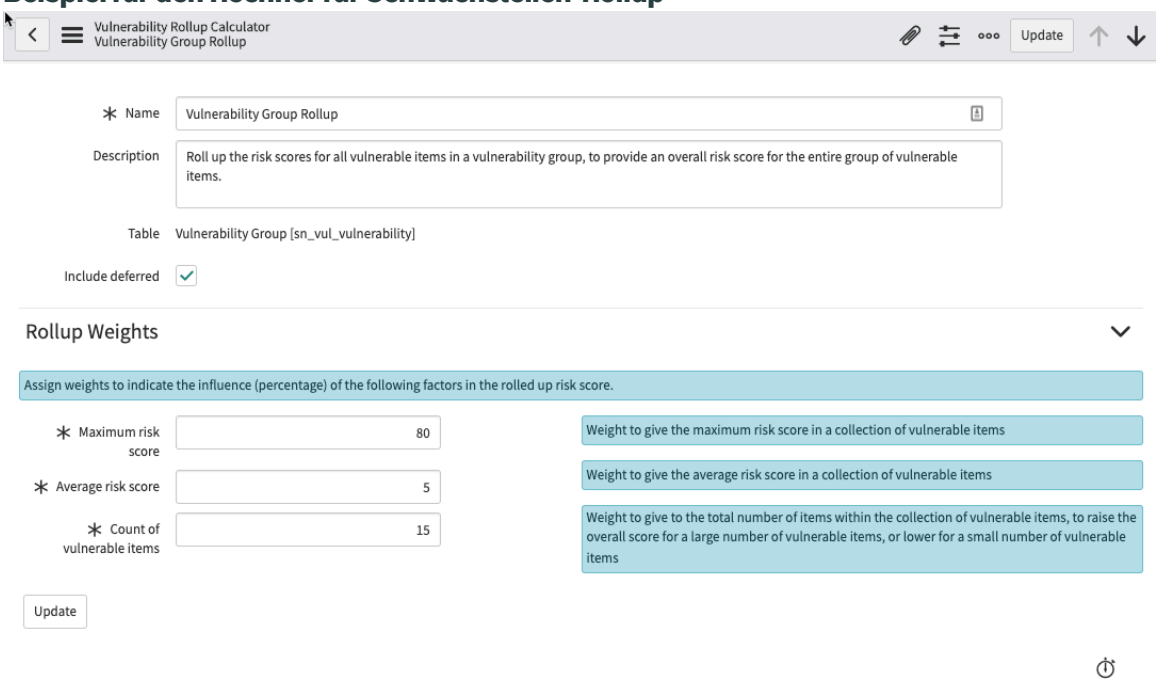
Beispiel für Schwachstellen-Rollup-Rechner: Betrachten Sie eine Korrekturaufgabe VUL324567, die die folgenden angreifbaren Elemente enthält:

- VIT1001 mit Risikopunktzahl von 30
- VIT1002 mit Risikopunktzahl von 40
- VIT1003 mit Risikopunktzahl von 50

Berücksichtigen Sie auch die folgenden Gewichtungen im Schwachstellen-Rollup-Rechner:

- Maximale Risikopunktzahl: 80
- Durchschnittliche Risikopunktzahl: 5
- Anzahl der angreifbaren Elemente: 15

Beispiel für den Rechner für Schwachstellen-Rollup



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Beispiel des Schwachstellen-Rollup-Rechners die Formel zum Bestimmen der Korrekturaufgabe **Risikopunktzahl** lst:

(**Maximale Risikopunktzahl** /100) * 80 + (**Durchschnittliche Risikopunktzahl** /100) * 5 + (Faktor * 15)

Der Faktor wird wie folgt bestimmt:

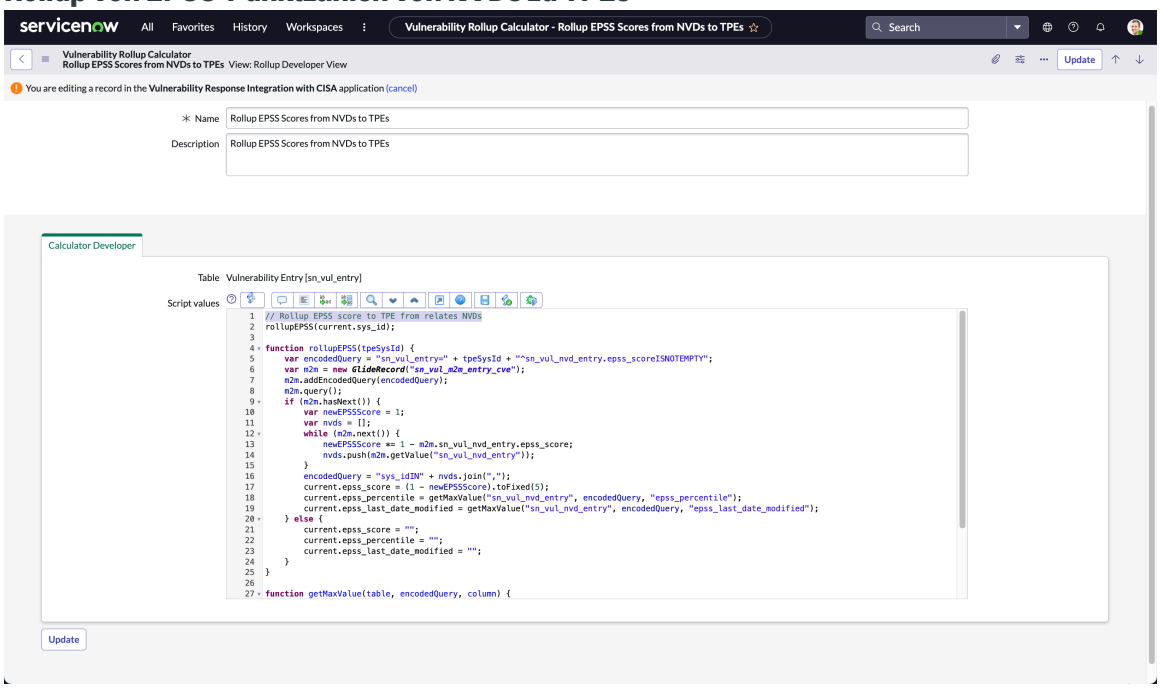
VI-Anzahl	Faktor
< 10	0,2
10-100	0,4
101-1000	0,6
1001-10000	0,8
> 10000	1

Für die Korrekturaufgabe VUL324567:

- Die durchschnittliche Risikopunktzahl beträgt 40
- Die maximale Risikopunktzahl beträgt 50
- 50 (maximale Risikopunktzahl)
- Faktor ist 0,2

Die **Risikopunktzahl** Wäre 45 [(50/100) * 80 + (40/100) * 5 + 0,2 * 15 = 40 + 2 + 3 = 45]

Rollup von EPSS-Punktzahlen von NVDs zu TPEs



EPSS-Rollup-Rechner – Beispiel

Betrachten Sie beispielsweise eine Organisation mit 100 Schwachstellen, von denen jede eine Ausnutzungswahrscheinlichkeit von 5 % aufweist. Die Frage, die für einen Netzwerkverteidiger von großem Interesse ist, könnte lauten: Wie hoch ist die Wahrscheinlichkeit, dass mindestens eine dieser Schwachstellen ausgenutzt wird, und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

was ist daher meine allgemeine Bedrohung? Die Wahrscheinlichkeit, dass mindestens ein Ereignis auftritt, ist einfach die Ergänzung (entgegengesetzt) zu keinen Ereignissen, d. h.:

```
P(at least one exploited vulnerability) = 1 - P(no vulnerabilities are exploited)
```

Wobei die Wahrscheinlichkeit, dass keine Schwachstellen vorhanden sind, das lineare Produkt ist, wenn jede Schwachstelle nicht ausgenutzt wird. Da in diesem Beispiel jede Schwachstelle eine Wahrscheinlichkeit von 5 % hat, dass sie ausgenutzt wird, hat sie eine Wahrscheinlichkeit von 95 %, nicht ausgenutzt zu werden. Und da es 100 davon gibt, können wir dies folgendermaßen schreiben:

```
P(at least one vuln exploited) = 1 - P(no vulns are exploited) = 1 - P(one vuln not
 exploited)^100 = 1 - 0.95^100 = 0.994
```

Was besagt, dass die Wahrscheinlichkeit, dass mindestens eine der Schwachstellen ausgenutzt wird, 99 % beträgt.

Wichtig:
Zum Ändern von `Rollup EPSS Scores from NVD to TPEs`, Sie müssen die Kontextmenüansicht des Formulars zu wechseln **Rollup-Entwickleransicht** Von **Standardansicht** .

[store-future: BEGIN review]

Rollup-Berechnungen der Risikopunktzahl der Organisation

Die Rollup-Funktion für die Risikopunktzahl der Organisation berechnet die Gesamtrisikopunktzahl für eine Organisation im einheitlichen Dashboard. Die Risikopunktzahlen für angreifbare Host-Elemente, angreifbare Anwendungselemente, angreifbare Container-Elemente und Konfigurationsprobleme werden zusammengefasst. Zuvor wurde die maximale Risikopunktzahl durch Mittelung der Punktzahlen für VIT, AVIT, Testergebnisse und CVIT bestimmt. Jedoch ab Version 22 von Vulnerability Response, Die maximale Risikopunktzahl wird jetzt durch Auswahl der höchsten Punktzahl unter den vier festgelegt.

Zur Berechnung der maximalen Risikopunktzahl wird die höchste Punktzahl unter VIT, AVIT, Testergebnissen und CVIT ausgewählt. Wenn Vits beispielsweise die höchste Punktzahl haben, wird diese Punktzahl als maximale Risikopunktzahl betrachtet.

Sobald die Anzahl der VIT-, AVIT-, CVIT- und Testergebnisse ermittelt wurden, werden sie addiert und mithilfe einer Zählmethode normalisiert. Die resultierende Risikopunktzahl wird dann mit der in der Konfiguration angegebenen Anzahlgewichtung multipliziert.

Für die Berechnung der durchschnittlichen Risikopunktzahl wird derselbe Prozess ausgeführt. Die Risikopunktzahlen für AVIT, Konfigurationsprobleme, Testergebnisse und andere Punktzahlen werden zusammengefasst und dann durch die Gesamtanzahl geteilt, um die durchschnittliche Risikopunktzahl zu erhalten. Schließlich werden alle Risikopunktzahlen addiert, um die Risikopunktzahl der Organisation abzuleiten.

[End]

Erstellen oder bearbeiten Vulnerability Response Korrekturzielregeln

Nach der ersten Bewertung der Korrekturzielregeln im Setup-Assistenten können Schwachstellenmanager eine Korrekturzielregel auf Ebene angreifbarer Elemente einrichten, um die Behebung von Schwachstellen mit hohem Risiko rechtzeitig voranzutreiben. Wenn das Korrekturdatum für ein angreifbares Element näher rückt, wird eine Benachrichtigung an die in der Regel angegebenen Anwender oder Gruppen gesendet.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Korrekturzielregeln**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Name der Regel.
Ziel (Tage)	Geben Sie die Anzahl der Tage an, innerhalb derer die angreifbaren Elemente seit dem letzten Öffnen behoben werden sollen.
V17.1: Ziel von (Datum)	Datum, ab dem die Ziel-SLAs berechnet werden. Sie können nur die Felder für Datum oder Datum und Uhrzeit angeben. Der Standardwert ist das Datum der letzten Öffnung. Informationen zum Anpassen der Werte für dieses Feld finden Sie unter KB1642413 .
Aktiv	Standardmäßig ist **Aktiv** Das Kontrollkästchen ist aktiviert, was bedeutet, dass die Korrekturzielregel aktiv ist. Wenn dieses Kontrollkästchen deaktiviert ist, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt wurden.
Benachrichtigen (Tage vor dem Fälligkeitsdatum)	Anzahl der Tage vor der angestrebten Korrekturzeit, bis eine Benachrichtigung gesendet wird. Das mit diesem Wert berechnete Benachrichtigungsdatum wird verwendet, um den Korrekturstatus und die Farbcodierung anzuzeigen. Wenn das Datum vor dem Benachrichtigungsdatum liegt, lautet der Korrekturstatus „in Flug“. Wenn das Benachrichtigungsdatum überschritten und vor dem Korrekturzieldatum liegt, wird der Status als näheres Ziel angezeigt. **Hinweis:** Wenn dieses Feld auf 0 festgelegt ist, wird nur ein festgelegt **Ziel Verfehlt** Benachrichtigung wird gesendet.
Beschreibung	Text, der die Korrekturzielregel beschreibt.
Bedingung	Wählen Sie mit dem Bedingungsfilter die Kriterien für die Anwendung der Regel auf die angreifbaren Elemente aus. Um Auswirkungen auf die Leistung zu vermeiden, testen Sie Ihre Bedingungen im gesamten Produktionsbereich. Mit Tests können Sie bestimmen, wie lange der ist **Bewerten Sie Korrekturziele** Die Ausführung des Auftrags erfordert die Bedingungen und die Größe Ihres Configuration Management Database (CMDB). Die Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird in diesem Datensatz oder Formular nicht unterstützt.
Benachrichtigungen	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Hinweis: Die in der Benachrichtigungs-E-Mail angezeigte Anzahl enthält keine angreifbaren Elemente in **Zurückgestellt** , **Gelöst** , Oder **Geschlossen** status.	
Anwender	Die Personen, die benachrichtigt werden sollen, wenn das ausgewählte angreifbare Element seine angestrebte Korrekturzeit erreicht oder überschritten hat.
Gruppe	Die Gruppe, die benachrichtigt werden soll, wenn das ausgewählte angreifbare Element seine angestrebte Korrekturzeit erreicht oder überschritten hat.
Verlauf aktualisieren	
	Für die anfängliche Erstellung einer Regel nicht verwendet. Anschließend werden Systemarbeitsnotizen hier protokolliert.

4. Klicken Sie auf **Absenden**.
   Diese Regel tritt bei der nächsten Ausführung der geplanten Aufgabe in Kraft. `Evaluate remediation targets`Oder bei Verwendung von **Änderungen Anwenden** Schaltfläche in der Listenansicht „Korrekturzielregeln“. Dasselbe gilt, wenn eine vorhandene Regel aktualisiert wird. Für weitere Informationen zur geplanten Aufgabe und **Änderungen Anwenden** , Siehe Vulnerability Response Korrekturzielregeln.

Konfigurieren Sie installierte Drittanbieterintegrationen mit dem Setup-Assistenten

Konfigurieren Sie Vulnerability Response so, dass sie mit jeder Ihrer installierten Drittanbieteranwendungsbereitstellungen kompatibel ist.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration**an.
2. Wählen Sie Aus **Scanner-Integrationen** Dient zum Konfigurieren installierter Bereitstellungen von Drittanbieteranwendungen.
3. Wenn Solution Management for Vulnerability Response Ist installiert, können Sie auswählen **Lösungsintegrationen** Zum Konfigurieren Ihrer Anbieter von Schwachstellen-Lösungen.

Konfigurieren Sie installierte Lösungsintegrationen für Vulnerability Solution Management Mit dem Setup-Assistenten

Nachdem Sie die Anwendung Schwachstellen-Lösungsmanagement installiert haben, können Sie Ihre Anbieter von Schwachstellen mithilfe des Setup-Assistenten konfigurieren.

Vorbereitungen

Erforderliche Rollen: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) oder admin

Verwenden Sie die folgenden Abschnitte, um die Anweisungen und Hinweismeldungen zu ergänzen, die im Setup-Assistenten für installierte Lösungsintegrationen für bereitgestellt werden Solution Management for Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass Sie bereits installiert haben Vulnerability Solution Management Und die gewünschten Lösungsintegrationen, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.
- Stellen Sie sicher, dass Sie über Anmeldeinformationen für Drittpartei-Accounts verfügen. Sie sind erforderlich, um einige Lösungsintegrationen zu bearbeiten.
- Siehe Anwendung Solution Management for Vulnerability Response installieren Um weitere Informationen zu erhalten, bevor Sie installierte Lösungen konfigurieren.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen**an.

   Die Integration der Microsoft Security Response Center-Lösung Erfordert einen API-Schlüssel und eine URL von Microsoft Security Response Center Um es zu konfigurieren.

   Hinweis:
   Die Eingabe des API-Schlüssels ist für optional MSRC. Um zu erhalten MSRC Schlüssel, benötigen Sie eine Microsoft-ID aus einem live.com, Outlook.com oder Microsoft.com E-Mail-Account, eine bei Microsoft registrierte Telefonnummer oder eine Skype-Anmeldung.

2. Geben Sie die URL ein.
   Die URL im Setup-Assistenten für MSRC ist `https://api.msrc.microsoft.com` .
3. Klicken Sie auf **Fertigstellen**.
4. **Wahlweise:** Sie können Importe bei Bedarf ausführen, indem Sie auf klicken **Jetzt Ausführen** Auf der Konfigurationsseite, nachdem Sie Ihre Anmeldeinformationen eingegeben haben.
5. Die Red Hat Solution Integration Ist auch verfügbar.
   Es ist kein API-Schlüssel erforderlich.
6. Im Setup-Assistenten rechts neben Red Hat Solution Integration, Klicken Sie auf **Bearbeiten** .
7. Überprüfen Sie die URL im Setup-Assistenten für RHSI Ist `https://access.redhat.com/hydra/rest`
8. **Wahlweise:** Sie können Importe bei Bedarf ausführen, indem Sie auf klicken **Jetzt Ausführen** Auf der Konfigurationsseite.
9. Klicken Sie Auf **Beenden** Gefolgt von **Als abgeschlossen markieren** Um die Konfiguration abzuschließen.
   Wenn Sie die Konfiguration abgeschlossen haben, wird im Setup-Assistenten für Lösungsintegrationen ein Häkchen angezeigt.

Konfigurieren Sie die MS TVM Vulnerability Integration mit dem Setup-Assistenten

Konfigurieren Sie Vulnerability Response Integration mit Microsoft Threat and Vulnerability Management (MS TVM), nachdem Sie sie mit dem Setup-Assistenten installiert haben.

Vorbereitungen

Zusätzlich zu den Anweisungen und Hinweismeldungen, die im Setup-Assistenten für bereitgestellt werden Vulnerability Response Führen Sie bei der Integration mit Microsoft Threat and Vulnerability Management die folgenden Aktionen aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vergewissern Sie sich, dass Sie die Anwendung bereits installiert haben, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.
- Siehe Vorbereitung auf die Microsoft Threat and Vulnerability Management Vulnerability Integration Um weitere Informationen zu erhalten, bevor Sie die Integration von Microsoft Threat and Vulnerability Management für konfigurieren Vulnerability Response.
- Stellen Sie sicher, dass Sie über Anmeldeinformationen für MS TVM-Accounts verfügen. Informationen zum Abrufen dieser Anmeldeinformationen finden Sie unter Einrichten Microsoft Azure für die MS TVM-Integration.

Erforderliche Rollen: Systemadministrator (admin) für die Installation, Schwachstellenadministrator (sn_vul.Vulnerability_admin) oder sn_vul.admin (veraltet) und Integration konfigurieren (sn_vul_msft_tvm.configure_Integration) für die Konfiguration

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**an.

   Die Kachel Microsoft Threat and Vulnerability Management wird angezeigt.

   Ms TVM ist eine Integration mit mehreren Quellen, d. h. Sie können mehrere Bereitstellungen derselben Drittpartei-Integration haben. Die Einstellungen aus Ihrer ursprünglichen Drittpartei-Integration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

   Hinweis:
   Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Erwägen Sie, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

   Daten aus jeder Drittpartei-Integration werden eindeutig identifiziert und sind in einer einzigen Instanz von verfügbar Vulnerability Response.

2. Klicken Sie zum Konfigurieren der Microsoft Threat and Vulnerability Management-Integration auf **Bearbeiten** .
3. Füllen Sie im Formular die Felder aus.

Formular „Account-Anmeldeinformationen“

Feld	Beschreibung
Name	Name der Instanz.
TVM-Region	Region in der Nähe Ihres Serverstandorts. Verwenden Sie den Server, der Ihrem Standort am nächsten liegt, um eine optimale Leistung der API zu erzielen.
Authentifizierungstyp	Methode zum Überprüfen der Identität. Die Anwenderauthentifizierung steuert die Sichtbarkeit bestimmter Assets für bestimmte Anwender. Ms TVM exportiert die Gerätegruppen, die für diesen Anwender berechtigt sind. Der Standardwert ist „Anwendung“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Mandanten-ID	Mandantenidentität Ihrer Organisation.
Client-ID	Client-Identität, die nach der Registrierung von MS TVM in Microsoft Azure generiert wird.
Anwendername	Anwender, der Zugriff auf die vollständige Gerätegruppe hat. Dieses Feld wird nur angezeigt, wenn „Anwender“ im Authentifizierungstyp ausgewählt ist.
Passwort	Passwort für den Anwendernamen, der Zugriff auf die vollständige Gerätegruppe hat. Dieses Feld wird nur angezeigt, wenn „Anwender“ im Authentifizierungstyp ausgewählt ist.
Geheimer Clientschlüssel	Geheimer Clientschlüssel, der nach der Registrierung der MS TVM-Anwendung generiert wird. Dieses Feld wird nur angezeigt, wenn Anwendung im Authentifizierungstyp ausgewählt ist.

4. Um Ihre Änderungen zu speichern und zum ersten Integrationsformular zu wechseln, klicken Sie auf **Als Nächstes** .
   Das Formular „Konfiguration importieren von Schwachstellen“ wird angezeigt.
5. Aktivieren oder deaktivieren Sie den Schwachstellenimport, bestimmen Sie das anfängliche Startdatum für die Schwachstellen, die importiert werden sollen, und planen Sie, wann der MS TVM-Schwachstellenimport ausgeführt werden soll.
   Wenn Sie alle Schwachstellen importieren möchten, lassen Sie das anfängliche Startdatum leer.
   a. Um Daten bei Bedarf zu importieren, klicken Sie auf **Schwachstellen Jetzt Importieren** .
   b. Um den Integrationsdatensatz anzuzeigen, klicken Sie auf **Erweiterte Einstellungen** .
6. Um Ihre Änderungen zu speichern und zum ersten Integrationsformular zu wechseln, klicken Sie auf **Als Nächstes** .
   Das Formular „Importkonfiguration für Empfehlungen“ wird angezeigt.
7. Aktivieren oder deaktivieren Sie den Empfehlungsimport, und bestimmen Sie den Zeitplan, wann der Import von MS TVM-Schwachstellen ausgeführt werden soll.
   a. Um Daten bei Bedarf zu importieren, klicken Sie auf **Importieren Sie Jetzt Empfehlungen** .
   b. Um den Integrationsdatensatz anzuzeigen, klicken Sie auf **Erweiterte Einstellungen** .
8. Um Ihre Änderungen zu speichern und zum ersten Integrationsformular zu wechseln, klicken Sie auf **Als Nächstes** .
   Das Formular „Konfiguration für Computer-Import“ wird angezeigt.
9. Aktivieren oder deaktivieren Sie den Computer-Import, bestimmen Sie das anfängliche Startdatum für die Computer, die Sie importieren möchten, und planen Sie, wann der MS TVM-Computer-Import ausgeführt werden soll.
   Wenn Sie alle Computer importieren möchten, lassen Sie das anfängliche Startdatum leer.

Hinweis:
Computer-Tags werden standardmäßig importiert und zum Organisieren und Nachverfolgen der in der MS TVM-Umgebung aufgeführten Computer verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Um die standardmäßigen Suchregeln für Konfigurationselemente (Configuration Item, CI) anzuzeigen, klicken Sie auf **CI-Suchregeln** . CI-Suchregeln definieren, wie Computerdaten aus Drittparteiquellen zur Identifizierung von Konfigurationselementen (Configuration Items, CI) in verwendet werden ServiceNow AI Platform CMDB. Sie haben die Möglichkeit, Suchregeln hinzuzufügen oder die Standard-CI-Suchregeln auf dieser Seite zu ändern. Weitere Informationen finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Integrationen von Schwachstellen von Drittparteien.

b. Um Daten bei Bedarf zu importieren, klicken Sie auf **Importieren Sie Jetzt Computer** .

Hinweis:
Computer mit dem Status „Onboarding in MS TVM“ werden von der ServiceNow-Anwendung abgerufen.

c. Um den Integrationsdatensatz anzuzeigen, klicken Sie auf **Erweiterte Einstellungen** .

10. Um Ihre Änderungen zu speichern und zum ersten Integrationsformular zu wechseln, klicken Sie auf **Als Nächstes** .
Das Formular „Konfiguration importieren von Computerschwachstellen“ wird angezeigt.

11. Aktivieren Sie die folgenden Integrationen, und bestimmen Sie das anfängliche Startdatum für die Schwachstellen, die Sie importieren möchten.

Formular „Konfiguration importieren“ für Computerschwachstellen

Integration	Beschreibung
Delta-Import von Microsoft TVM-Computer-Schwachstellen	Ruft Schwachstellen ab, die während des vollständigen Schwachstellenimports aktualisiert wurden, einschließlich neuer, behobener und aktualisierter Schwachstellen. Sie können Delta-Daten nur für die letzten 14 Tage importieren.
Vollständiger Import von Microsoft TVM-Computer-Schwachstellen	Ruft alle offenen Schwachstellen ab. Aufgrund des hohen Volumens des Datenimports können Sie die wöchentliche Ausführung planen.

Hinweis:

Führen Sie den Computer-Import vor der Integration von Computer-Schwachstellen aus. Andernfalls werden für die fehlenden Computer keine VIS erstellt.

12. Um Ihre Änderungen zu speichern und die Konfiguration im Setup-Assistenten abzuschließen, klicken Sie auf **Beenden** .

Nächste Maßnahme

Wenn Sie die Gruppierung angreifbarer Elemente in der klassischen Umgebung aktivieren möchten, navigieren Sie zu > **Vulnerability Response** > **Administration** > **Regeln für Korrekturaufgaben** > **Microsoft TVM-Empfehlung**an.

Wählen Sie im angezeigten Formular die aus **Aktiv** Option zum Aktivieren. Alternativ wählen Sie aus **Neu** Um eine neue Regel zu erstellen.

Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Qualys Vulnerability Integration Mit dem Setup-Assistenten

Nachdem Sie installiert haben Qualys Anwendung konfigurieren Sie sie mit dem Setup-Assistenten.

Vorbereitungen

Verwenden Sie die folgenden Abschnitte, um die Anweisungen und Hinweismeldungen zu ergänzen, die im Setup-Assistenten für die Konfiguration von bereitgestellt werden Qualys Vulnerability Integration.

- Vergewissern Sie sich, dass Sie die Anwendung bereits installiert haben, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.
- Siehe Vorbereitung für Qualys Vulnerability Integration Um weitere Informationen zu erhalten, bevor Sie konfigurieren Qualys Vulnerability Integration.
- Stellen Sie sicher, dass Sie über Anmeldeinformationen für Drittpartei-Accounts verfügen. Sie sind erforderlich, um einige Drittanbieteranwendungen zu bearbeiten.

Erforderliche Rollen: Systemadministrator (admin) für die Installation, Schwachstellenadministrator (sn_vul.Vulnerability_admin) oder sn_vul.admin (veraltet) für die Konfiguration.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**an.
   Die installierten Integrationen werden angezeigt.
2. Klicken Sie Auf **Bearbeiten** Rechts von Qualys Vulnerability Integration Sie möchten konfigurieren.
3. Geben Sie im Formular „Account-Anmeldeinformationen“ Ihren ein Qualys Cloud Platform Anmeldeinformationen.
   Ihre Anmeldeinformationen sind zum Konfigurieren erforderlich.
4. Verwenden Sie die folgenden Hinweise als Leitfaden, wenn Sie mit der Konfiguration fortfahren.
   - Die **Erweiterte Einstellungen** Link verweist Sie auf Qualys Integrationsdatensatz. Sie können Parameter hinzufügen, die von unterstützt werden Qualys Produkt für Ihre geplanten Abfragen, mit dem Sie die importierten Schwachstellendaten filtern können. Siehe Legen Sie zusätzliche Filterparameter für fest Qualys Importe Weitere Informationen finden Sie unter .
   - Wenn Sie ein Upgrade von einer früheren Version von durchgeführt haben Vulnerability Response Mit einer Version von Qualys Vulnerability Integration Sie haben bereits konfiguriert. Diese Version mit beibehaltenen Konfigurationseinstellungen ist noch verfügbar.

     Unter Importeinstellungen in Host-Erkennungskonfiguration für Qualys Vulnerability Integration, Es gibt eine Option zum Anzeigen behoben Qualys Schwachstellenerkennungsdatensätze. Wenn diese Option aktiviert ist, können Sie angreifbare Elemente aus Erkennungsdatensätzen mit einem festen Status (Status=) erstellen **Behoben**). Weitere Informationen zu Erkennungen angreifbarer Elemente finden Sie unter Vulnerability Response Erkennungen angreifbarer Elemente aus Drittpartei-Integrationen.

     Sie können aktivieren **Nach Netzwerkpartition Suchen** Aktivieren Sie das Kontrollkästchen auf der Seite „Konfiguration der Host-Erkennung“, um den Netzwerkpartition-Bezeichner in die IP-Adressensuche aufzunehmen. Weitere Informationen finden Sie unter Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartition-Bezeichner für Qualys Vulnerability Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Host-Tags werden als Teil von importiert Qualys Integration der Hostliste. Host-Tags werden hauptsächlich zum Filtern verwendet Vulnerability Response Regeln für Zuweisungs- und Korrekturaufgaben. Sie werden im Formular „erkanntes Element“ angezeigt.

Hinweis:
Die Qualys Die Integration der Host-Liste muss ausgeführt werden, bevor Zuweisungs- oder Korrekturaufgabenregeln in erstellt werden Vulnerability Response Damit alle Tags in den Regeln vorhanden sein können und bevor angreifbare Elemente importiert und gruppiert werden.

Qualys **Asset-Tags** Werden im Host-Tags-Modul unter gespeichert Qualys Vulnerability Integration.

- Die Qualys Vulnerability Integration Unterstützt mehrere Quellen. Sie können mehrere Bereitstellungen derselben Drittpartei-Integration haben. Um eine weitere Integration hinzuzufügen, klicken Sie auf der Seite „Scannerintegrationen“ auf **Fügen Sie Die Integration Hinzu** .

  Die Einstellungen aus Ihrer ursprünglichen Drittpartei-Integration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

  Hinweis:
  Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Erwägen Sie, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

  Daten aus jeder Drittpartei-Integration werden eindeutig identifiziert und sind in einer einzigen Instanz von verfügbar Vulnerability Response.

- Sie können Importe bei Bedarf ausführen, indem Sie auf klicken **Jetzt Ausführen** Auf einer Konfigurationsseite.

5. Klicken Sie Auf **Beenden** Um die Konfiguration im Setup-Assistenten abzuschließen.

Konfigurieren Sie die Tenable-Schwachstellenintegration mit dem Setup-Assistenten

Nachdem Sie installiert haben Vulnerability Response Integration with Tenable Anwendung konfigurieren Sie sie mit dem Setup-Assistenten.

Vorbereitungen
Verwenden Sie die folgenden Abschnitte, um die Anweisungen und Hinweismeldungen zu ergänzen, die im Setup-Assistenten für bereitgestellt werden Vulnerability Response Integration with Tenable Integration.

- Vergewissern Sie sich, dass Sie die Anwendung bereits installiert haben, bevor Sie beginnen. Weitere Informationen finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.
- Siehe Vorbereitung auf die Tenable-Schwachstellenintegration Um weitere Informationen zu erhalten, bevor Sie konfigurieren Tenable for Vulnerability Response.
- Stellen Sie sicher, dass Sie über Anmeldeinformationen für Drittpartei-Accounts verfügen. Sie sind erforderlich, um einige Drittanbieteranwendungen zu bearbeiten.

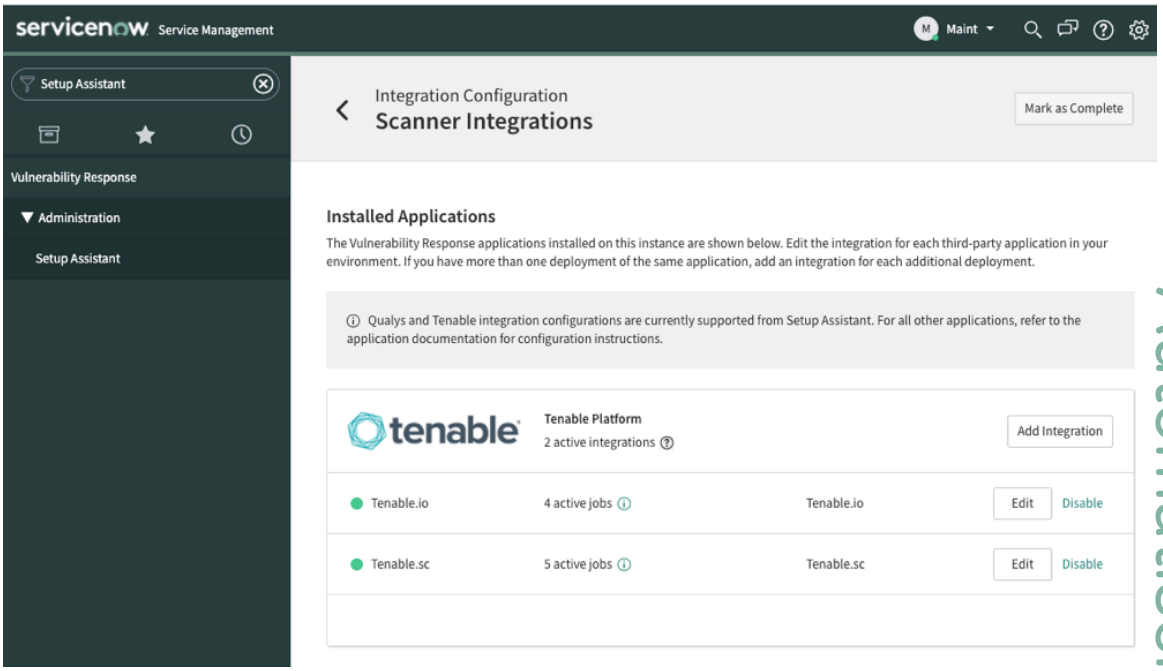
Erforderliche Rollen: Systemadministrator (admin) für die Installation, Schwachstellenadministrator (sn_vul.Vulnerability_admin) oder sn_vul.admin (veraltet) und Integration konfigurieren (sn_vul_Tenable.configure_Integrations) für die Konfiguration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn nicht angezeigt, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**an.

   Die Tenable.io, Tenable.sc, Und Tenable.csIntegrationen werden angezeigt.



   Tenable ist eine Integration mit mehreren Quellen, und Sie können mehrere Bereitstellungen derselben Drittpartei-Integration haben. Die Einstellungen aus Ihrer ursprünglichen Drittpartei-Integration werden als Vorlage für die Einstellungen jeder neuen Integration verwendet.

   Hinweis:
   Wenn Sie die ursprüngliche Schwachstellenintegration löschen, müssen Sie eine andere Integration als Vorlage auswählen. Erwägen Sie, die Integration zu deaktivieren, anstatt sie zu löschen. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

   Daten aus jeder Drittpartei-Integration werden eindeutig identifiziert und sind in einer einzigen Instanz von verfügbar Vulnerability Response.

2. Wählen Sie rechts neben der Tenable-Integration, die Sie konfigurieren möchten, aus **Bearbeiten** .
3. Füllen Sie die Felder im Formular „Account-Anmeldeinformationen“ aus.

   - Tenable.io Erfordert Administratorzugriff mit einem Berechtigungsattribut größer oder gleich 64.

     Hinweis:
     Ab v3.8 von Vulnerability Response Integration with Tenable, Zugriff auf Tenable.io Benötigt keine Administratorrechte mehr. Ein Standardanwender mit einem Berechtigungsattribut von 16 kann auch auf das Produkt zugreifen.

   - Tenable.sc Erfordert Sicherheitsanalysten oder -Manager-Zugriff.
   - Tenable.cs Erfordert ein Token mit Zugriff auf das Tenable CS Platform Generierungstoken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

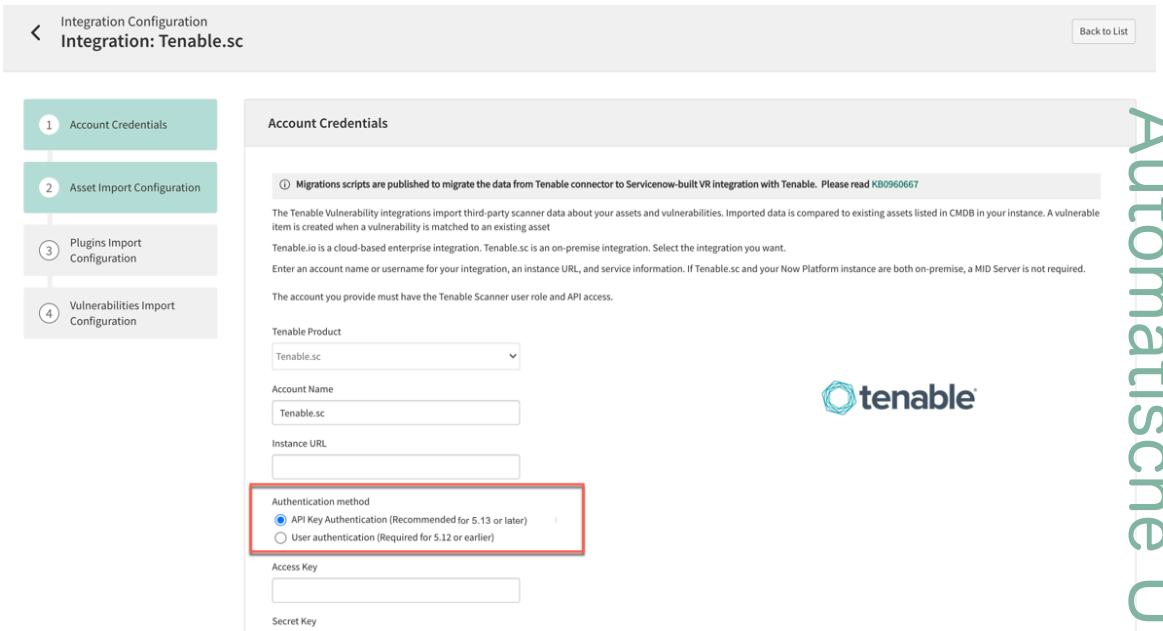
a. Wählen Sie Ihr Tenable-Produkt aus.

b. Geben Sie den Namen Ihres Tenable-Accounts ein.

c. Geben Sie im Feld Instanz-URL die URL für Ihre Tenable-Plattform ein.

d. Wählen Sie eine Authentifizierungsmethode aus (Im Fall von Tenable.cs, Fahren Sie mit Schritt f) fort. .

Basierend auf Ihrer Version von Tenable.sc, Sie haben zwei Optionen für die Authentifizierung:



i. Ab v5.13 von Tenable.sc, Wählen Sie aus **API-Schlüsselauthentifizierung** . Geben Sie Ihre Tenable-Zugriffs- und geheimen Schlüssel ein.

ii. Vor v5.13 wird die Anwenderauthentifizierung von unterstützt ServiceNow AI Platform® Instanz und ist erforderlich. Geben Sie ein ServiceNow AI Platform Anwendername und Passwort.

Nur die API-Schlüsselauthentifizierung wird für unterstützt Tenable.sc. Geben Sie Ihre Tenable-Zugriffs- und geheimen Schlüssel ein.

e. Wahlweise: Wählen Sie einen MID Server aus.

(Optional) Wenn Ihr ServiceNow AI Platform Instanz und Ihr Tenable.sc Anwendung befindet sich nicht am selben Standort. Wählen Sie einen konfigurierten MID-Server aus der Liste aus. Weitere Informationen finden Sie unter MID-Server .

- Ab v15.0 von Vulnerability Response Und v3.0 des Tenable Vulnerability Integration, Sie haben die Möglichkeit, zu aktivieren *Async_request*Parameter wie in beschrieben Datenabrufeinstellungen für die Tenable-Schwachstellenintegration. Wenn Sie synchrone Anrufe tätigen möchten, ist eine Konfiguration mit Tenable erforderlich. Wenden Sie sich an das Tenable-Produkt, um Hilfe zu erhalten. Dieser Parameter gilt nach der Aktivierung für alle Integrationen von Tenable.sc Und es gibt eine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitüberschreitung von 30 Sekunden. Um die Korrekturskripts anzuzeigen, navigieren Sie zu **Systemdefinition** > **Korrekturskripts**an.

- (Optional) Für Bestandskunden ist ein Korrekturskript verfügbar, wenn Sie asynchrone Aufrufe verwenden.

Wenn Ihr ServiceNow AI Platform Instanz und Ihr Tenable.sc Anwendungen sind beide lokal verfügbar. Sie haben jedoch die Möglichkeit, einen konfigurierten MID-Server aus der Liste auszuwählen.

Hinweis:
Gibt an, ob Sie einen verwenden möchten MID-Server Oder nicht, die Integrationen gehen nach fünf Minuten aus, und eine Meldung wird angezeigt, wenn keine Antwort vom Server vorliegt.

Wenn ein Zeitüberschreitungsfehler auftritt, überprüfen Sie im Setup-Assistenten, ob Sie die richtigen Anmeldeinformationen und URL eingegeben haben.

f. Geben Sie das API-Token ein.

Hinweis:
Wenn im Setup-Assistenten ein Fehler für ungültige Anmeldeinformationen angezeigt wird, stellen Sie sicher, dass Sie die richtigen Anmeldeinformationen und URL eingegeben haben.

4. Wählen Sie Aus **Als Nächstes** Um Ihre Änderungen zu speichern und mit dem ersten Integrationsformular fortzufahren.
Im Fall von Tenable.io Und Tenable.sc, Das Formular Asset-Importkonfiguration wird angezeigt. Im Fall von Tenable.cs, Das Formular Container-Asset-Importkonfiguration wird angezeigt.

Hinweis:
Das Formular „Container-Asset-Importkonfiguration“ ist nur sichtbar, wenn Container Vulnerability Response Ist installiert.

5. Aktivieren oder deaktivieren Sie in diesem Formular die Asset-Importintegration, bestimmen Sie das anfängliche Startdatum für die Assets, die Sie importieren möchten, und planen Sie, wann der Import von Tenable-Assets ausgeführt werden soll.

Für Tenable.io

- Die Asset-Integration kann mit verwendet werden Tenable.io Compliance-Ergebnisse und Compliance-Ergebnisse ergänzen die Integration, um sichere Konfigurationsbewertungsdaten zu Ihren Assets in zu importieren Konfigurations-Compliance Anwendung.
- Version 12,2 von Konfigurations-Compliance Anwendung ist in Ihrer Instanz erforderlich, wenn Sie diese sicheren Konfigurationsbewertungsdaten importieren und anzeigen möchten.

  Siehe Konfigurations-Compliance Daten importiert Weitere Informationen darüber, welche Daten mit diesen Integrationen importiert werden und wo sie veröffentlicht werden.

- Die Tenable.io Compliance-Ergebnisse und Compliance-Ergebnisse Backfill-Integrationen sind standardmäßig nicht aktiviert. Wenn Sie sie aktivieren, verwenden Sie möglicherweise die bereitgestellten Standardzeitplaneinstellungen. In den unten aufgeführten Schritten erfahren Sie, wie Sie Integrationen für suchen und aktivieren Tenable Vulnerability Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für initiieren Tenable.io Produkt aus Ihrer Instanz. Die Tenable.io Vorlagenintegration und Tenable.io Die Integration von Scan-Anmeldeinformationen muss aktiviert werden, bevor erneute Scans initiiert werden.

Standardmäßig sind diese Integrationen deaktiviert. Wenn Sie Ihre Anmeldeinformationen für eingeben Tenable.io, Alle Tenable.io Integrationen werden automatisch aktiviert. So aktivieren oder deaktivieren Sie diese Integrationen manuell:

a. Navigieren zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**an.

b. Suchen Sie in der angezeigten Liste nach Tenable.io Gewünschte Integrationsdatensätze.

c. Öffnen Sie jeden Datensatz, und wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren der Integration.

d. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.

e. Kehren Sie zum Setup-Assistenten zurück, um mit Ihrer Konfiguration für fortzufahren Tenable Vulnerability Integration Mit Vulnerability Response.

- Für Tenable.io Integration haben Sie auch die Möglichkeit, den Import von Asset-Tags zu aktivieren und zu deaktivieren. Asset-Tags werden standardmäßig importiert und zum Organisieren und Nachverfolgen der Assets verwendet, die in Ihrer CMDB in aufgeführt sind Tenable.io Umgebung.
- Für beide Tenable.io Und Tenable.sc Produkte, wenn Sie auswählen **Aktivieren Sie Die Suche Nach Netzwerkpartition** Unter Suche nach Netzwerkpartition können Sie einzelne CIs mithilfe der Identification and Reconciliation Engine (IRE) für Ihre Assets mit derselben IP-Adresse erstellen. Siehe Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartition-Bezeichner für Tenable Vulnerability Integration und CIs für werden erstellt Vulnerability Response Verwenden der Identifizierungs- und Abgleichsmodul, um weitere Informationen zu erhalten.
- Wählen Sie für Tenable.io und Tenable.sc oben im Bildschirm neben dem Link Asset-Import die Option aus **CI-Suchregeln** Link zum Anzeigen der standardmäßigen CI-Suchregeln (Configuration Item). CI-Suchregeln definieren, wie Asset-Daten aus Drittparteiquellen zur Identifizierung von Konfigurationselementen (Configuration Items, CI) in verwendet werden ServiceNow AI Platform CMDB. Sie haben die Möglichkeit, Suchregeln hinzuzufügen oder die Standard-CI-Suchregeln auf dieser Seite zu ändern. Weitere Informationen finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Integrationen von Schwachstellen von Drittparteien.
- Wählen Sie Aus **Importieren Sie Jetzt Assets** Dient zum Importieren von Daten bei Bedarf.
- Die **Erweiterte Einstellungen** Link verweist auf den Datensatz „Asset-Integration“. Ab v3.3 können Sie Parameter hinzufügen, die von unterstützt werden Tenable.io Produkt für Ihre geplanten Abfragen, mit dem Sie die Schwachstellendaten filtern können, die Sie mit importieren Tenable.io Assets und die Integrationen von behobenen und offenen Schwachstellen. Siehe Legen Sie zusätzliche Filterparameter für fest Tenable.io Importe Weitere Informationen finden Sie unter .

6. Wählen Sie Aus **Als Nächstes** Um Ihre Änderungen zu speichern und mit dem nächsten Formular fortzufahren.

Hinweis:
Im Fall von Tenable.io Und Tenable.sc. Für Tenable.cs Das Formular „Konfiguration importieren von Host-Schwachstellen“ wird angezeigt. Fahren Sie mit Schritt 9 fort, um eine weitere Tenable-CS-Konfiguration zu erhalten.

Das Formular „Plugins-Importkonfiguration“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Auf der Plugin-Importkonfiguration Formular, aktivieren oder deaktivieren Sie den Import von Plugins (Drittanbieter-Schwachstelleneinträge). Bestimmen Sie das anfängliche Startdatum für die Plugins, die Sie importieren möchten, und planen Sie, wann der Import von Tenable-Plugins ausgeführt werden soll.

   Wenn Sie alle Plugins, Schwachstellen und Assets importieren möchten, lassen Sie das anfängliche Startdatum leer.

   - Wählen Sie Aus **Importieren Sie Jetzt Plugins** Dient zum Importieren von Daten bei Bedarf.
   - Die **Erweiterte Einstellungen** Link verweist auf den Datensatz „Plugins-Integration“.
   - Für den Import von Schwachstellen können Sie Schweregrade für planen und festlegen Tenable.io Für die Schwachstellen, die erfasst werden sollen. Bestimmen Sie ein Datum, damit nur die Schwachstellen importiert werden, die ab einem bestimmten Datum erstellt oder aktualisiert wurden.
   - Für Tenable.sc Integration können Sie einen Abfragefilter und ein Datum bestimmen, sodass nur die Schwachstellen importiert werden, die ab einem bestimmten Datum erstellt oder aktualisiert wurden.

8. Wählen Sie Aus **Als Nächstes** Um Ihre Änderungen zu speichern und mit dem nächsten Formular fortzufahren.
   Das Formular „Konfiguration importieren von Schwachstellen“ wird angezeigt. Aktivieren oder deaktivieren Sie die Integration, und bestimmen Sie das anfängliche Startdatum für die Schwachstellen, die Sie importieren möchten.

   Für Tenable.io Produkt:

   - Importieren Sie nur die Schwachstellen und zugehörigen VIS, die den Bedingungen entsprechen, die Sie mit dem Schweregradfilter ausgewählt haben.
   - Für Tenable.io Asset-Integration, `Last Scan Time`Wird nur für Assets mit Schwachstellen importiert und aktualisiert.
   - Aktivieren Sie **Schwachstellen Behoben** Option zum Anzeigen von VIS für feste Erkennungsdatensätze. Wenn diese Kennzeichnung im Setup-Assistenten aktiviert ist, werden neue VIS für Erkennungen in erstellt **Behoben** status, der in Ihrer Instanz nicht vorhanden ist. Wenn diese Funktion aktiviert ist, kann sie sich negativ auf Ihre Erfassungsleistung auswirken.
   - Die **Erweiterte Einstellungen** Link neben Filter importieren verweist Sie auf den Datensatz „Schwachstellen-Integration“.
   - Wählen Sie aus **Importieren Sie Zeitpläne** Link oben, um zu konfigurieren, wie oft Schwachstellen erfasst werden, und die Integration zu aktivieren.

   Für Tenable.sc Produkt:

   - Importieren Sie nur die Schwachstellen und zugehörigen VIS, die den Bedingungsfiltern entsprechen, die von einer Tenable-Abfrage in der Tenable-Plattform festgelegt werden. Weitere Informationen zu Tenable-Abfragen finden Sie in der Tenable-Dokumentation.

     Der Tenable-Abfragefilter, den Sie im Setup-Assistenten auswählen, gilt auch für Tenable.sc Asset-Integration. Nur die Assets mit den Schwachstellen, die den Bedingungen des Abfragefilters entsprechen, werden importiert.

   - Aktivieren Sie **Schwachstellen Behoben** Option zum Anzeigen von VIS für feste Erkennungsdatensätze. Wenn diese Kennzeichnung im Setup-Assistenten aktiv ist, werden neue VIS für Erkennungen in erstellt **Behoben** status, der in Ihrer Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nicht vorhanden ist. Wenn diese Funktion aktiv ist, kann sie sich negativ auf Ihre Erfassungsleistung auswirken.

- Um den Netzwerkpartition-Bezeichner in die IP-Adressensuche einzubeziehen, wählen Sie aus **Suche nach Netzwerkpartition aktivieren** Kontrollkästchen in **Suche nach Netzwerkpartition** Abschnitt. Weitere Informationen finden Sie unter Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartition-Bezeichner für Tenable Vulnerability Integration.
- Wählen Sie Aus **Importieren Sie Zeitpläne** Oben, um zu konfigurieren, wie oft Schwachstellen erfasst werden, und die Integration zu aktivieren.
- Die **Erweiterte Einstellungen** Link neben Filter importieren verweist Sie auf den Datensatz „Schwachstellen-Integration“.
- Die ServiceNow® Tenable.sc Integration von Scan-Anmeldeinformationen ist aktiviert (Aktiv) Automatisch aus dem Setup-Assistenten in Ihrer Instanz heraus, wenn Sie konfigurieren Tenable.sc Integrationen von Schwachstellen (Tenable.sc Integrationen offener und behobener Schwachstellen).

  Diese Integration importiert und aktualisiert Scanner-Anmeldeinformationen aus dem Tenable.sc Produkt in Ihrer Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationsdaten zu importieren und sicher zu speichern. Navigieren zu **Tenable-Schwachstellen-Integration** > **Integrationen** > **Tenable.sc – Integration von Scan-Anmeldeinformationen** Um weitere Informationen zur Integration von Scan-Anmeldeinformationen anzuzeigen.

9. Wählen Sie Aus **Als Nächstes** Im Schritt „Container-Asset-Importkonfiguration“.
   Das Formular „Konfiguration importieren von Host-Schwachstellen“ wird angezeigt. Aktivieren oder deaktivieren Sie die Integration.
   - Importieren Sie nur die Schwachstellen und zugehörigen VIS, die den Bedingungen entsprechen, die Sie mit dem Schweregradfilter ausgewählt haben.
   - Der Link „Erweiterte Einstellungen“ neben „Filter importieren“ weist Sie auf den Datensatz „Schwachstellen-Integration“.
   - Wählen Sie oben den Link Zeitpläne importieren, um zu konfigurieren, wie oft Schwachstellen erfasst werden, und die Integration zu aktivieren.
   - Wählen Sie oben im Bildschirm neben dem Link „Zeitpläne importieren“ den Link CI-Suchregeln aus, um die standardmäßigen Suchregeln für Konfigurationselemente (Configuration Item, CI) anzuzeigen. CI-Suchregeln definieren, wie Asset-Daten aus Drittparteiquellen zur Identifizierung von Konfigurationselementen (Configuration Items, CI) in verwendet werden ServiceNow AI Platform CMDB. Sie haben die Möglichkeit, Suchregeln hinzuzufügen oder die Standard-CI-Suchregeln auf dieser Seite zu ändern. Weitere Informationen finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response-Schwachstellenintegrationen von Drittanbietern.

10. **Hinweis:**
    Dieser Schritt gilt nur für Tenable.cs Produkt.

    Wählen Sie Weiter, um Ihre Änderungen zu speichern und mit dem nächsten Formular fortzufahren.
    - Importieren Sie nur die Container-Schwachstellen und zugehörigen CVIS, die den Bedingungen entsprechen, die Sie mit dem Schweregradfilter auswählen.
    - Der Link „Erweiterte Einstellungen“ neben „Filter importieren“ weist Sie auf den Datensatz „Schwachstellen-Integration“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wählen Sie oben den Link Zeitpläne importieren, um zu konfigurieren, wie oft Schwachstellen erfasst werden, und die Integration zu aktivieren.
- Die Importkonfiguration für Container-Schwachstellen wird nur angezeigt, wenn Container Vulnerability Response installiert ist.

Das Formular „Konfiguration importieren von Container-Schwachstellen“ wird angezeigt. Aktivieren oder deaktivieren Sie die Integration.

11. Wählen Sie Aus **Beenden** Um Ihre Änderungen zu speichern und die Konfiguration im Setup-Assistenten abzuschließen.

Nächste Maßnahme

(Optional) Navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Schwachstellen-Rechner** > **Standardrisikorechner** > **Tenable-Risikoregel** Zum Aktivieren der Tenable-Risikoregel.

Aktivieren Sie im angezeigten Formular „Schwachstellen-Rechner-Regel“ das Kontrollkästchen aktiv, um es zu aktivieren.

Die Tenable-Risikoregel wird mit installiert Vulnerability Response Integration with Tenable Anwendung als Teil des Standardrisikorechners in den Schwachstellenrechnern von Vulnerability Response. Die Vulnerability Priority Rating (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit dem neuen Standard-Risikorechner verwendet wird. Diese Risikoregel ist standardmäßig deaktiviert. Durch Aktivieren der Tenable-Risikorechnerregel werden die importierten VPR-Werte zur Berechnung der Risikopunktzahl für angreifbare Elemente verwendet. Die Standardgewichtungsverteilung für diesen Risikorechner: VPR = 70 %, Asset = 15 % und Geschäftsrelevanz = 15 %. Das Aktivieren dieser Tenable-Risikorechner-Regel kann sich auf Ihre Leistung der Datenerfassung auswirken.

Siehe Vulnerability Response Rechner und Regeln für Schwachstellenrechner

Schwachstellen-Lösungsanbieter einrichten

Richten Sie Anbieter von Schwachstellen-Lösungen ein, indem Sie der Prüfliste folgen und die Anbieter dann im Setup-Assistenten konfigurieren.

Bereiten Sie die Prüfliste für die Lösungsintegration vor

Verwenden Sie den Setup-Assistenten, um die Implementierung einer Solution Intelligence-Integration für alle Lieferanten vorzubereiten, die das Datenformat Common Vulnerability Reporting Framework (CVRF) oder Common Security Advisory Framework (CSAF) unterstützen.

Vorbereitung der Integration der CVRF-Lösung (Common Vulnerability Reporting Framework)

Verwenden Sie den Setup-Assistenten, um die Implementierung einer Solution Intelligence-Integration für alle Lieferanten vorzubereiten, die das CVRF-Datenformat (Common Vulnerability Reporting Framework) unterstützen.

Bevor Sie beginnen

Zur Integration mit den Lieferanten, die die Lösungen bereitstellen, stellen Sie sicher, dass Sie die Aufgaben in der folgenden Prüfliste ausführen. Sie können die Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren.

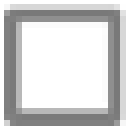
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für Integrationsvorbereitung

Aufgabe	Beschreibung
Abhängige Anwendungen ☐	Überprüfen Sie, ob die folgenden Anwendungen über installiert sind ServiceNow Store: • Schwachstellen-Lösungs-Management: Weitere Informationen zur Installation Vulnerability Solution Management, Siehe Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent Und Anwendung Solution Management for Vulnerability Response installieren. • Vulnerability Response: Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe Vulnerability Response installieren. Diese Integration erfordert Version 16,1 von Vulnerability Response Oder später.
Anmeldeinformationen für Drittpartei-Account ☐	Stellen Sie sicher, dass Sie über Anmeldeinformationen für Drittpartei-Accounts verfügen. Sie sind erforderlich, um einige Lösungsintegrationen zu bearbeiten.
Lieferantenauthentifizierung ☐	Überprüfen Sie, ob Sie die Lieferanten für den Import von Lösungen mit den API's authentifiziert haben. Weitere Informationen zur Authentifizierung von Lieferanten finden Sie unter Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen. Wenn Sie keinen API-basierten Lieferanten konfigurieren möchten, können Sie diesen Schritt überspringen.
Anpassung von Flow und Flow-Aktion ☐	Wenn Sie einen anderen API-basierten Lieferanten als Cisco konfigurieren möchten, müssen Sie die Flow- und Flow-Aktion anpassen, um einen eindeutigen Schlüssel und eine CVRF-URL aus der Antwort einer Empfehlung zu extrahieren. **Hinweis:** Die Veröffentlichung der CVRF-URL ist nicht bei allen Lieferanten Standard. Informationen zum Anpassen des Flows für andere Lieferanten als Cisco finden Sie unter Konfigurieren Sie einen anderen Common Vulnerability Reporting Framework-Lieferanten als Cisco. Sie können diesen Schritt überspringen, wenn sie keine anderen Lieferanten als Cisco konfigurieren möchten. Standardmäßig wurde der Flow für Cisco mit der Anwendung geliefert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für Integrationsvorbereitung (Fortsetzung)

Aufgabe	Beschreibung
Rollen 	Stellen Sie sicher, dass Sie eine Administratorgruppe oder einen Anwender haben, der die Integration verwalten kann. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.Vulnerability_admin) und andere Rollen zu.

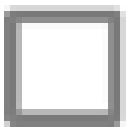
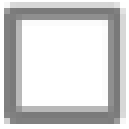
Vorbereitung der Integration der Common Security Advisory Framework (CSAF)-Lösung

Verwenden Sie den Setup-Assistenten, um die Implementierung einer Solution Intelligence-Integration für alle Lieferanten vorzubereiten, die das CSAF-Datenformat (Common Security Advisory Framework) unterstützen.

Bevor Sie beginnen

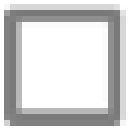
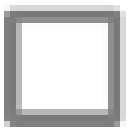
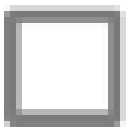
Zur Integration mit den Lieferanten, die die Lösungen bereitstellen, stellen Sie sicher, dass Sie die Aufgaben in der folgenden Prüfliste ausführen. Sie können die Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren.

Prüfliste für Integrationsvorbereitung

Aufgabe	Beschreibung
Abhängige Anwendungen 	Überprüfen Sie, ob die folgenden Anwendungen über installiert sind ServiceNow Store: • Schwachstellen-Lösungs-Management: Weitere Informationen zur Installation Vulnerability Solution Management, Siehe Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent Und Anwendung Solution Management for Vulnerability Response installieren. • Vulnerability Response: Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe Vulnerability Response installieren. Diese Integration erfordert Version 16,1 von Vulnerability Response Oder später.
Anmeldeinformationen für Drittpartei-Account 	Stellen Sie sicher, dass Sie über Anmeldeinformationen für Drittpartei-Accounts verfügen. Sie sind erforderlich, um einige Lösungsintegrationen zu bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für Integrationsvorbereitung (Fortsetzung)

Aufgabe	Beschreibung
Lieferantenauthentifizierung 	Überprüfen Sie, ob Sie die Lieferanten für den Import von Lösungen mit den APIs authentifiziert haben. Weitere Informationen zur Authentifizierung von Lieferanten finden Sie unter Aliasse für Verbindungen und Anmeldeinformationen für das Common Security Advisory Framework (CSAF) konfigurieren. Wenn Sie keinen API-basierten Lieferanten konfigurieren möchten, können Sie diesen Schritt überspringen.
Anpassung von Flow und Flow-Aktion 	Wenn Sie einen anderen API-basierten Lieferanten als konfigurieren möchten Red Hat, Dann müssen Sie den Flow und die Flow-Aktion anpassen, um einen eindeutigen Schlüssel und eine CSAF-URL aus der Antwort einer Empfehlung zu extrahieren. **Hinweis:** Die Veröffentlichung der CSAF-URL ist nicht bei allen Lieferanten Standard. Dient zum Anpassen des Flows für andere Lieferanten als Red Hat, Siehe Konfigurieren Sie einen anderen Anbieter als des allgemeinen Sicherheitsberatungs-Frameworks Red Hat. Sie können diesen Schritt überspringen, wenn sie keine anderen Lieferanten als konfigurieren möchten Red Hat. Standardmäßig der Flow für Red Hat Wurde mit der Anwendung geliefert.
Rollen 	Stellen Sie sicher, dass Sie eine Administratorgruppe oder einen Anwender haben, der die Integration verwalten kann. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.Vulnerability_admin) und andere Rollen zu.

Konfigurieren Sie Anbieter von Schwachstellen-Lösungen

Nachdem Sie die Anwendung Schwachstellen-Lösungsmanagement installiert haben, konfigurieren Sie die Anbieter von Schwachstellen mithilfe des Setup-Assistenten.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin, sn_vul.admin (veraltet) oder admin.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration**an.
2. Klicken Sie Auf **Lösungsintegrationen** .
3. Unter Installierte Lösungen Abschnitt Daten abrufen, indem Sie entweder eine URL, eine API oder einen Import verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um Daten mithilfe einer URL oder API abzurufen, klicken Sie auf **Fügen Sie Die Integration Hinzu** .
- Dient zum Abrufen von Daten durch Hochladen eines Common Vulnerability Response Framework (CVRF) Oder Common Security Advisory Framework (CSAF)-Datei , Klicken Sie auf **Datei Importieren** .

Nächste Maßnahme

Abhängig von Welches Format Sie möchten importieren Daten In , Sie können eine der folgenden Aufgaben ausführen:

- Für CVRF:
  - Informationen zum Importieren einer CVRF-Datei finden Sie unter Importieren Sie Daten des Common Vulnerability Reporting Framework über Dateiimport.
  - Informationen zum Importieren von CVRF-Daten mit den APIs finden Sie unter Importieren Sie CVRF-Daten (Common Vulnerability Reporting Framework) über die CVRF-URL.
  - Informationen zum Importieren von CVRF-Daten über Empfehlungen finden Sie unter Importieren Sie Daten des Common Vulnerability Reporting-Frameworks aus Empfehlungen.
- Für CSAF:
  - Informationen zum Importieren einer CSAF-Datei finden Sie unter Importieren Sie Daten des Common Security Advisory Framework über Dateiimport.
  - Informationen zum Importieren von CSAF-Daten mit den APIs finden Sie unter Importieren Sie CSAF-Daten (Common Security Advisory Framework) über die CSAF-URL.
  - Informationen zum Importieren von CSAF-Daten über Empfehlungen finden Sie unter Importieren Sie Daten des allgemeinen Sicherheitsberatungs-Frameworks aus Empfehlungen.
-

Common Vulnerability Reporting Framework (CVRF)

Das Common Vulnerability Reporting Framework (CVRF) bietet ein standardisiertes Framework für die Erstellung der Dokumentation zu Schwachstellenberichten. Es handelt sich um eine XML-basierte Sprache, die die Freigabe wichtiger sicherheitsbezogener Informationen zwischen verschiedenen Stakeholdern in mehreren Organisationen vereinfacht. Durch die Verwendung des CVRF-Formats können der Informationsaustausch und die Verarbeitung beschleunigt werden.

Importieren Sie Daten des Common Vulnerability Reporting Framework über Dateiimport

Importieren Sie eine CVRF-Datei, um Daten im CVRF-Format anzuzeigen. Der Import ist eine einmalige Aktivität.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) oder admin.

Warum und wann dieser Vorgang ausgeführt wird

Nach dem Import wird ein Warteschlangeneintrag mit einem Anhang erstellt, der analysiert wird, wenn der Eintrag verarbeitet wird. Die Daten werden dann in den entsprechenden Tabellen ausgefüllt. Vor der Analyse der CVRF-Daten wird basierend auf der Konfiguration ein Scanner-Zuordnungsdatensatz erstellt. Anschließend werden die Scanner-Zuordnungsdaten in Lieferantenzuordnungsdaten umgewandelt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Allgemeines Vulnerability Response-Framework**an.
2. Klicken Sie Auf **Datei Importieren** .

> **Hinweis:**
> Sie können jeweils nur eine XML-Datei mit einer maximalen Dateigröße von 1 GB hochladen.

3. In **Name** Geben Sie einen eindeutigen Namen für die Integration ein.
   Der Planer wird mit diesem Namen erstellt.
4. In **Lieferant** Geben Sie den Namen des Lieferanten ein.
   Die **Quelle** Das Feld der Lösungen wird mit dem Lieferantennamen ausgefüllt.
5. Klicken Sie auf **Fertigstellen**.

Ergebnisse

Eine Importwarteschlange wird erstellt. Klicken Sie auf den Link in der Infoleiste, um die Warteschlangeneinträge für den Lieferanten zusammen mit der zugehörigen Liste anzuzeigen. Sie können auch den Status des Auftrags anzeigen.

Nachdem die Daten in das CVRF-Format importiert wurden, werden die Daten wie folgt verarbeitet:

1. Wenn die Warteschlange verarbeitet wird, wird die Datei mit einer dedizierten Datenquelle analysiert.
2. Sobald die Verarbeitung abgeschlossen ist, wird das Anwendungsprotokoll aktualisiert.
3. Sobald die CVRF-XML-Datei analysiert wurde, werden die folgenden Tabellen in ausgefüllt ServiceNow® Vulnerability Response Anwendung.
   - sn_vul_Solution
   - sn_vul_m2m_Vulnerability_Solution
   - sn_vul_nvd_entry
   - sn_vul_Software
   - sn_vul_Product_category

Detaillierte Informationen zu Fehlern oder Ausnahmen finden Sie in den Anwendungsprotokollen.

Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen

Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen, um Lieferanten zu authentifizieren. Bei der Analyse von Beratungsinformationen werden Drittpartei-Lieferanten authentifiziert.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin, sn_vul.admin (veraltet) oder admin

Prozedur

1. OAuth-Authentifizierung erstellen.
   Siehe Erstellen Sie einen Endpunkt für Clients, um auf die Instanz zuzugreifen .
2. Erstellen Sie einen Alias für Verbindungen und Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Siehe Erstellen Sie einen Alias für Verbindungen und Anmeldeinformationen .

3. Erstellen Sie eine Verbindung.
   a. Klicken Sie auf den Namen des neu erstellten Alias für Verbindungen und Anmeldeinformationen.
   b. Unter **Verbindungen** Klicken Sie auf die Registerkarte **Neu** .
   c. Wenn der Authentifizierungstyp OAuth ist, wählen Sie das in Schritt 1 erstellte Anwendungsregistrierungsprofil aus **OAuth-Entitätsprofil** .
   d. Erstellen Sie einen Datensatz in Verbindungen aus der zugehörigen Liste des Datensatzes.
   e. In **Anmeldeinformationen** Feld den in Schritt 3D erstellten Anmeldeinformationsdatensatz auswählen
   f. In **Verbindungs-URL** Geben Sie die URL des Lieferanten ein.
   g. Klicken Sie auf **Absenden**.

Konfigurieren Sie einen anderen Common Vulnerability Reporting Framework-Lieferanten als Cisco

Konfigurieren Sie einen anderen CVRF-Lieferanten (Common Vulnerability Reporting Framework) als Cisco mit API-Unterstützung.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) oder admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Verbindung und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
2. Erstellen Sie einen Datensatz mit dem vom Lieferanten unterstützten Authentifizierungstyp.
   Weitere Informationen zur Authentifizierung eines Lieferanten finden Sie unter Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen.
3. Navigieren zu **Alle** > **Vulnerability Response** > **Flow Designer**an.
4. Duplizieren Sie den Flow mit dem Namen „Advisory Parsing“.

   Hinweis:
   - Wenn eine der Aktionen geändert werden muss, kopieren Sie die Aktion, und verwenden Sie sie im neuen Flow.
   - Aktualisieren Sie die Paginierungsbezogene Logik gemäß dem Lieferanten

5. Wenn die Parameterlogik für den Datumsbereich nicht mit Cisco identisch ist, kopieren Sie die Aktion **Aktualisieren Sie Die Paginierungsparameter** Und nehmen Sie Änderungen nach Bedarf für den Lieferanten vor.
6. Navigieren zu **Alle** > **Vulnerability Response** > **Ergänzungsdatenzuordnungen**an.
7. Erstellen Sie einen Datensatz gemäß Cisco, indem Sie ändern **Eigenschaftsschlüssel** Wert gemäß dem Lieferanten.
   Diese Logik dient zum Zuordnen erforderlicher Felder aus einer beratenden Nutzlast zu einem ServiceNow Tabelle.
8. Ordnen Sie die folgenden API-Tags aus der API-Nutzlast zu.
   Diese Tags müssen Details zugeordnet werden, die in der Tabelle „Ergänzungsdatenzuordnung“ ausgefüllt werden sollen. Standardmäßig wird die Cisco-spezifische Zuordnung geliefert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie müssen einen Datensatz erstellen, wenn Sie mehrere Lieferanten konfigurieren müssen, die Empfehlungen veröffentlichen.

Tag für Advisory-Nutzlast	Spalte aus Tabelle sn_vul_cvrf_Solution_Integration	Beschreibung
CVRF-URL	cvrf_url	Tag-Name, der die CVRF-URL enthält.
Beratungs-ID (eindeutiger Schlüssel für Antwort)	ID	Tag-Name, der einen eindeutigen Bezeichner enthält.
Datum der letzten Änderung	last_modified_date	Tag-Name, der das Datum der letzten Aktualisierung des Datensatzes enthält.
SecurityAdvisoryIntegrationSysId	Integration	Bezieht sich auf die sysId der geplanten Integrationsaufgabe, die die Datensätze der Schwachstellenlösung erstellt.

9. Ändern Sie basierend auf dem Antwortformat die Logik der Analyse, indem Sie die Aktion kopieren **Liste Abrufen** Aus dem Flow „Advisory Analysing“.

Importieren Sie Daten des Common Vulnerability Reporting-Frameworks aus Empfehlungen

Importieren Sie CVRF-Daten aus Empfehlungen, indem Sie die Lieferanten-URL mit dem Importtyp API konfigurieren.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin, sn_vul.admin (veraltet) oder admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn die Integration ausgeführt wird, werden die Ratschläge abgerufen. Die CVRF-URL und die Admitories-ID werden aus der Nutzlast extrahiert. Die REST-API-Aufrufe werden für jede CVRF-URL ausgeführt, und die Daten werden analysiert und in der Tabelle „sn_vul_Solution“ gespeichert.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Allgemeines Vulnerability Response-Framework**an.
2. Klicken Sie Auf **Fügen Sie Die Integration Hinzu** .
3. Füllen Sie im Formular die Felder aus.

Formular „Lösungshinweise importieren“

Feld	Beschreibung
Importtyp	Option zum Auswählen des Importtyps. Wählen Sie Aus **API** .
Name	Eindeutiger Name für die Integration.
Lieferant	Name des Lieferanten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Die **Quelle** Das Feld der Lösungen wird mit dem Lieferantennamen ausgefüllt.
Verbindungsalias	Option zum Auswählen authentifizierter Anmeldeinformationen. **Hinweis:** In der Tabelle „sys_alias“ werden Anmeldeinformationen und die Basis-URL für Empfehlungen gespeichert.
Zeitplan	Häufigkeit, mit der die Daten aktualisiert werden müssen.
Tag	Wochentag, an dem die Daten aktualisiert werden sollen.
Zeit	Uhrzeit der Woche, zu der die Daten aktualisiert werden sollen.
API-Konfiguration	
Flow	Option zum Auswählen des Flows. Der Flow wird ausgelöst, wenn der Planer ausgeführt wird. Der Flow analysiert Ratschläge, extrahiert die CVRF-URL und speichert diese Details in den Aktualisierungstabellen. Sie können den vorhandenen Flow kopieren und nach Bedarf bearbeiten. Sie können beispielsweise Änderungen im Zusammenhang mit der Paginierung vornehmen.
Flow-Aktion	Option zum Auswählen der Flow-Aktion. Flow-Aktionen kümmern sich um die Funktion des Schiebefensters. Sie können die Flow-Aktionen aktualisieren und den Abfrageparameter direkt zur Aktion hinzufügen, indem Sie ziehen.
Zuordnungstabelle	Option zum Auswählen der Zuordnungstabelle. Der Datensatz der Zuordnungstabelle für Ergänzungsdaten wird zum Extrahieren der CVRF-URL und der Advisory-ID aus der Nutzlast von Empfehlungen verwendet.
Hinweise aus Antwort	Option zum Eingeben des Tag-Namens aus der Nutzlast von Empfehlungen, aus denen die Liste der Empfehlungen extrahiert werden kann.
Filterkriterien	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zeitbereichsparameter	Option zum Auswählen des Zeitbereichs für die Anforderung und des Datumsformats für API-Aufrufe. Der Parameter „Start-/Enddatum-Anforderung“ ist der Parametername, der für Start- und Enddatum während API-Aufrufen verwendet wird. Beispiel: Startdatum , Start_date, endDate, end_date.
Datumsformat	Option zum Eingeben des Datumsformats, z. B. Mm/TT/JJJJ. . Das Datumsformat ist das Format, das die API zum Filtern benötigt. Formate, die von GlideDate nicht unterstützt werden, funktionieren nicht.
Anfänglicher Bereich in Tagen	E Geben Sie die Tage an, für die die Daten abgerufen werden müssen, wenn der Planer zum ersten Mal ausgeführt wird. Für nachfolgende Ausführungen wird der Mechanismus des Schiebefensters befolgt. **Hinweis:** Wenn Sie keinen Zeitbereich auswählen möchten, wählen Sie aus **Keine Parameter** .
Scannerzuordnungen	
Scannerquelle	Option zum Auswählen der Quelle des Drittparteieintrags (TPE).
Schwachstellenspalte	Option zum Auswählen des Stichworts.
Stichwörter	Option zum Eingeben des Stichworts für die Suche in der ausgewählten Schwachstellenspalte.

4. Klicken Sie auf **Fertigstellen**.

Importieren Sie CVRF-Daten (Common Vulnerability Reporting Framework) über die CVRF-URL

Importieren Sie CVRF-Daten, indem Sie die Lieferanten-URL im Setup-Assistenten konfigurieren.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin, sn_vul.admin (veraltet) oder admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn die Integration ausgeführt wird, werden Daten aus der URL abgerufen, die analysiert wird. Die Daten werden dann in der Tabelle „sn_vul_Solution“ mit der Quelle als Lieferantenname gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Oracle veröffentlicht direkt die CVRF-URL für die Bereitstellung von Lösungen. Wenn Sie daher die Integration für den Import von Oracle-Daten konfigurieren möchten, stellen Sie sicher, dass Sie über die CVRF-URL für Oracle verfügen, und führen Sie die folgenden Schritte aus.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Allgemeines Vulnerability Response-Framework**an.
2. Klicken Sie Auf **Fügen Sie Die Integration Hinzu** .
3. Füllen Sie im Formular die Felder aus.

CVRF-Formular importieren

Feld	Beschreibung
Importtyp	Typ des Imports. Wählen Sie Aus **URL** .
Name	Eindeutiger Name für die Integration.
Lieferant	Name des Lieferanten. **Hinweis:** Die **Quelle** Das Feld der Lösungen wird mit dem Lieferantennamen ausgefüllt.
URL	URL, von der Sie die Lösungsdaten im CVRF-Format abrufen möchten.
Zeitplan	Häufigkeit, mit der die Daten aktualisiert werden müssen. **Hinweis:** Wenn das Status-Tag von CVRF „ENDGÜLTIG“ anzeigt, wird das Feld automatisch auf festgelegt **Bei Bedarf** Um unnötige Ausführungen zu verhindern.
Tag	Wochentag, an dem die Daten aktualisiert werden sollen.
Zeit	Uhrzeit der Woche, zu der die Daten aktualisiert werden sollen.

4. Klicken Sie auf **Fertigstellen**.

Fehlerbehebung beim Datenimport des Common Vulnerability Reporting Framework

Problembehebungsaktionen können bei der Lösung gängiger Probleme beim Importieren von CVRF-Daten in die Vulnerability Response-Anwendung helfen.

Problem	Aktion
Die Dauer der Integrationsausführung ist lang	Wenn die Integration länger als erwartet ausgeführt wird, gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problem	Aktion
	1. Navigieren Sie zur Tabelle sn_vul_ds_Import_q_entry. 2. Gruppieren nach **Status** Feld. Sie können die Einträge sehen, die sich im status Abgeschlossen, in Bearbeitung oder in der Warteschlange befinden.
Integration beim API-basierten Import fehlgeschlagen	Wenn die Integration beim API-basierten Import fehlschlägt, gehen Sie wie folgt vor: 1. Navigieren Sie zu **Flow Designer** . 2. Öffnen Sie den Flow, der in der Konfiguration ausgewählt wurde. **Hinweis:** Öffnen Sie im Fall von Cisco den Flow „Advisory Parsing“. 3. Klicken Sie Auf **Ausführungen** . 4. Öffnen Sie die neueste Ausführung oder die Ausführung, die debuggiert werden muss. 5. Überprüfen Sie den Flow in jeder Phase.
Integration im API-basierten Import mit einem Zeitüberschreitungsfehler fehlgeschlagen	Wenn die Integration in einem API-basierten Import aufgrund einer Zeitüberschreitung im Flow der beratenden Analyse fehlschlägt, gehen Sie wie folgt vor: 1. Erhöhen Sie die Zeitüberschreitung, indem Sie öffnen sys_properties.LIST . 2. Suchen Sie in der Spalte Name nach `sn_vul.CVRFFlowTimeout (inMiliSeconds)` . **Hinweis:** Die Zeit wird in Millisekunden angegeben. 3. Öffnen Sie den Datensatz, und aktualisieren Sie den Wert mit einer großen Zahl. 4. Speichern Sie den Datensatz, und führen Sie die Integration erneut aus.
Integration mit Fehler „Scannerzuordnung zu Lieferantenzuordnungsdaten wird ausgeführt“ fehlgeschlagen	Überprüfen Sie, ob die Integration während des URL- oder API-basierten Imports mit dem folgenden Fehler fehlschlägt: Die Transformation der Scannerzuordnung zu Lieferantenzuordnungsdaten wird ausgeführt. Daten werden erst ausgefüllt, nachdem die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problem	Aktion
	Transformation abgeschlossen ist. Versuchen Sie, nach einiger Zeit auszuführen. Wenn dieser Fehler auftritt, warten Sie einige Zeit, und führen Sie die Integration erneut aus.
Importwarteschlange wird während des Dateiimports nicht erstellt	Während eines Dateiimports wird die Importwarteschlange manchmal nicht erstellt. Dieser Fehler bedeutet, dass die Transformation, die Scanner-Zuordnungsdaten zu Lieferanten-Zuordnungsdaten zuordnet, ausgeführt wird. Der Warteschlangeneintrag wird erstellt, sobald der Prozess abgeschlossen ist.

Common Security Advisory Framework (CSAF)

Bei Verwendung mit Vulnerability Solution Management, Das Common Security Advisory Framework (CSAF) ermöglicht Automatisierungssicherheitsbenachrichtigungen über ein maschinenlesbares JSON-Format.

Mit CSAF können Sie mit jedem Solution Intelligence-Anbieter integrieren, indem Sie das Lösungsmanagement-Framework verwenden, um die Intelligence-Daten zu importieren. Die CSAF-Sicherheitsbenachrichtigungen können einer der folgenden Typen sein.

- Sicherheitswarnhinweise
- Vulnerability Exploitability Exchange (VEX)
- Security Incident Response
- Informative Beratung

Die CSAF unterstützt nur Dateiimporte, URL-Importe und API-Importe von Sicherheitshinweisen von Lieferanten.

Importieren Sie Daten des Common Security Advisory Framework über Dateiimport

Importieren Sie eine CSAF-Datei, um Daten im CSAF-Format anzuzeigen. Der Import ist eine einmalige Aktivität.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) oder admin

Warum und wann dieser Vorgang ausgeführt wird

Nach dem Import wird ein Warteschlangeneintrag mit einem Anhang erstellt, der analysiert wird, wenn der Eintrag verarbeitet wird. Die Daten werden dann in den entsprechenden Tabellen ausgefüllt. Vor der Analyse der CSAF-Daten wird basierend auf der Konfiguration ein Scanner-Zuordnungsdatensatz erstellt. Anschließend werden die Scanner-Zuordnungsdaten in Lieferantenzuordnungsdaten umgewandelt.

Die Scannerzuordnung gilt nicht für NVD-basierte Schwachstellen (National Vulnerability Database), bei denen es sich um Schwachstellen mit einem Common Vulnerability Entry (CVE) in der NVD-Datenbank handelt.

Wenn Sie nur über eine am höchsten ersetzende Lösung verfügen und ein Rolldown zu den angreifbaren Elementen durchgeführt wird, wird die bevorzugte Lösung ausgefüllt. Wenn in einem NVD-Eintrag mehrere Lieferantenlösungen enthalten sind, wird die bevorzugte Lösung nicht ausgefüllt, da mehr als eine höchste Ersatzlösung vorhanden ist. In diesem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fall müssen Sie manuell eine Lösung auswählen. Bei Schwachstellen von Drittparteien wird die bevorzugte Lösung nur ausgefüllt, wenn Sie die entsprechende Scannerzuordnung hinzufügen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Allgemeines Framework Für Sicherheitswarnhinweise**an.
2. Wählen Sie Aus **Datei Importieren** .

   Hinweis:
   Sie können jeweils nur eine JSON-Datei mit einer maximalen Dateigröße von 15 MB hochladen.

3. In **Name** Geben Sie einen eindeutigen Namen für die Integration ein.
   Der Planer wird mit diesem Namen erstellt.
4. In **Lieferant** Geben Sie den Namen des Lieferanten ein.
   Die **Quelle** Das Feld der Lösungen wird mit dem Lieferantennamen ausgefüllt.
5. Wählen Sie **Fertigstellen** aus.

Ergebnisse

Eine Importwarteschlange wird erstellt. Wählen Sie den Link in der Infoleiste aus, um die Warteschlangeneinträge für den Lieferanten zusammen mit der zugehörigen Liste anzuzeigen. Sie können auch den Status des Auftrags anzeigen.

Nachdem die Daten in das CSAF-Format importiert wurden, werden die Daten wie folgt verarbeitet:

1. Wenn die Warteschlange verarbeitet wird, wird die Datei mit einer dedizierten Datenquelle analysiert.
2. Sobald die Verarbeitung abgeschlossen ist, wird das Anwendungsprotokoll aktualisiert.
3. Sobald die CSAF-JSON-Datei analysiert wurde, werden die folgenden Tabellen in ausgefüllt ServiceNow® Vulnerability Response Anwendung.
   - sn_vul_Solution
   - sn_vul_m2m_Vulnerability_Solution
   - sn_vul_nvd_entry
   - sn_vul_Software
   - sn_vul_Product_category

Detaillierte Informationen zu Fehlern oder Ausnahmen finden Sie in den Anwendungsprotokollen.

Aliasse für Verbindungen und Anmeldeinformationen für das Common Security Advisory Framework (CSAF) konfigurieren

Konfigurieren Sie Aliasse für Verbindungen und Anmeldeinformationen, um Lieferanten zu authentifizieren. Bei der Analyse von Beratungsinformationen werden Drittpartei-Lieferanten authentifiziert.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin, sn_vul.admin (veraltet) oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. OAuth-Authentifizierung erstellen.
   Siehe Erstellen Sie einen Endpunkt für Clients, um auf die Instanz zuzugreifen .
2. Erstellen Sie einen Alias für Verbindungen und Anmeldeinformationen.
   Siehe Erstellen Sie einen Alias für Verbindungen und Anmeldeinformationen .
3. Erstellen Sie eine Verbindung.
   a. Wählen Sie den Namen des neu erstellten Alias für Verbindungen und Anmeldeinformationen aus.
   b. Unter **Verbindungen** Wählen Sie die Registerkarte aus **Neu** .
   c. Wenn der Authentifizierungstyp OAuth ist, wählen Sie das in Schritt 1 erstellte Anwendungsregistrierungsprofil aus **OAuth-Entitätsprofil** .
   d. Erstellen Sie einen Datensatz in Verbindungen aus der zugehörigen Liste des Datensatzes.
   e. In **Anmeldeinformationen** Feld den in Schritt 3D erstellten Anmeldeinformationsdatensatz auswählen
   f. In **Verbindungs-URL** Geben Sie die URL des Lieferanten ein.
   g. Wählen Sie **Absenden**.

Konfigurieren Sie einen anderen Anbieter als des allgemeinen Sicherheitsberatungs-Frameworks Red Hat

Konfigurieren Sie einen anderen Common Security Advisory Framework (CSAF)-Lieferanten als Red Hat Mit API-Unterstützung.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) oder admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Verbindung und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**an.
2. Erstellen Sie einen Datensatz mit dem vom Lieferanten unterstützten Authentifizierungstyp.
   Weitere Informationen zur Authentifizierung eines Lieferanten finden Sie unter Aliasse für Verbindungen und Anmeldeinformationen für das Common Security Advisory Framework (CSAF) konfigurieren.
3. Navigieren zu **Alle** > **Vulnerability Response** > **Flow Designer**an.
4. Duplizieren Sie den Flow mit dem Namen „Advisory Parsing“.

Hinweis:

- Wenn eine der Aktionen geändert werden muss, kopieren Sie die Aktion, und verwenden Sie sie im neuen Flow.
- Überprüfen Sie die Parameter page_index_key und page_size_key gemäß der Lieferanten-API.
- Aktualisieren Sie die Paginierungsbezogene Logik gemäß dem Lieferanten

5. Wenn die Parameterlogik für den Datumsbereich nicht identisch ist Red Hat, Kopieren Sie die Aktion **Aktualisieren Sie Die Paginierungsparameter** Und nehmen Sie Änderungen nach Bedarf für den Lieferanten vor.
6. Navigieren zu **Alle** > **Vulnerability Response** > **Ergänzungsdatenzuordnungen**an.
7. Erstellen Sie einen Datensatz gemäß Red Hat Durch Ändern von **Eigenschaftsschlüssel** Wert gemäß dem Lieferanten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Logik dient zum Zuordnen erforderlicher Felder aus einer beratenden Nutzlast zu einem ServiceNow Tabelle.

8. Ordnen Sie die folgenden API-Tags aus der API-Nutzlast zu.
   Diese Tags müssen Details zugeordnet werden, die in der Tabelle „Ergänzungsdatenzuordnung“ ausgefüllt werden sollen. Standardmäßig ist Red Hat Bestimmte Zuordnung wird geliefert.

   Hinweis:
   Sie müssen einen Datensatz erstellen, wenn Sie mehrere Lieferanten konfigurieren müssen, die Empfehlungen veröffentlichen.

Tag für Advisory-Nutzlast	Spalte aus Tabelle sn_vul_cvrf_Solution_Integration	Beschreibung
CSAF-URL (Ressourcen-URL, die auf CSAF-Nutzlast verweist)	cvrf_url	Tag-Name, der die CSAF-URL enthält.
Beratungs-ID (eindeutiger Schlüssel für Antwort)	ID	Tag-Name, der einen eindeutigen Bezeichner enthält.
Datum der letzten Änderung	last_modified_date	Tag-Name, der das Datum der letzten Aktualisierung des Datensatzes enthält.
Csaf (statischer Wert)	advisory_Format	Hinweisformatwert für CSAF-Nutzlasten. Beachten Sie, dass dies ein statischer Wert ist, der für alle CSAF-Integrationen gilt.
SecurityAdvisoryIntegrationSysId	Integration	Bezieht sich auf die sysId der geplanten Integrationsaufgabe, die die Datensätze der Schwachstellenlösung erstellt.

9. Ändern Sie basierend auf dem Antwortformat die Logik der Analyse, indem Sie die Aktion kopieren **Liste Abrufen** Aus dem Flow „Advisory Analysing“.

Importieren Sie Daten des allgemeinen Sicherheitsberatungs-Frameworks aus Empfehlungen

Importieren Sie CSAF-Daten aus Empfehlungen, indem Sie die Lieferanten-URL mit dem Importtyp API konfigurieren.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin, sn_vul.admin (veraltet) oder admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn die Integration ausgeführt wird, werden die Ratschläge abgerufen. Die CSAF-URL und die Admitories-ID werden aus der Nutzlast extrahiert. Die REST-API-Aufrufe werden für jede CSAF-URL ausgeführt, und die Daten werden analysiert und in der Tabelle „sn_vul_Solution“ gespeichert.

Die Scannerzuordnung gilt nicht für NVD-basierte Schwachstellen (National Vulnerability Database), bei denen es sich um Schwachstellen mit einem Common Vulnerability Entry (CVE) in der NVD-Datenbank handelt.

Wenn Sie nur über eine am höchsten ersetzende Lösung verfügen und ein Rolldown zu den angreifbaren Elementen durchgeführt wird, wird die bevorzugte Lösung ausgefüllt. Wenn in einem NVD-Eintrag mehrere Lieferantenlösungen enthalten sind, wird die bevorzugte Lösung nicht ausgefüllt, da mehr als eine höchste Ersatzlösung vorhanden ist. In diesem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fall müssen Sie manuell eine Lösung auswählen. Bei Schwachstellen von Drittparteien wird die bevorzugte Lösung nur ausgefüllt, wenn Sie die entsprechende Scannerzuordnung hinzufügen.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Allgemeines Framework Für Sicherheitswarnhinweise**an.
2. Wählen Sie Aus **Fügen Sie Die Integration Hinzu** .
3. Füllen Sie im Formular die Felder aus.

Formular „Lösungshinweise importieren“

Feld	Beschreibung
Importtyp	Option zum Auswählen des Importtyps. Wählen Sie Aus **API** .
Name	Eindeutiger Name für die Integration.
Lieferant	Name des Lieferanten. **Hinweis:** Die **Quelle** Das Feld der Lösungen wird mit dem Lieferantennamen ausgefüllt.
Verbindungsalias	Option zum Auswählen authentifizierter Anmeldeinformationen. **Hinweis:** In der Tabelle „sys_alias“ werden Anmeldeinformationen und die Basis-URL für Empfehlungen gespeichert.
Zeitplan	Häufigkeit, mit der die Daten aktualisiert werden müssen.
Tag	Wochentag, an dem die Daten aktualisiert werden sollen.
Zeit	Uhrzeit der Woche, zu der die Daten aktualisiert werden sollen.
API-Konfiguration	
Flow	Option zum Auswählen des Flows. Der Flow wird ausgelöst, wenn der Planer ausgeführt wird. Der Flow analysiert Ratschläge, extrahiert die CSAF-URL und speichert diese Details in den Aktualisierungstabellen. Sie können den vorhandenen Flow kopieren und nach Bedarf bearbeiten. Sie können beispielsweise Änderungen im

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Zusammenhang mit der Paginierung vornehmen.
Flow-Aktion	Option zum Auswählen der Flow-Aktion. Flow-Aktionen kümmern sich um die Funktion des Schiebefensters. Sie können die Flow-Aktionen aktualisieren und den Abfrageparameter direkt zur Aktion hinzufügen, indem Sie ziehen.
Zuordnungstabelle	Option zum Auswählen der Zuordnungstabelle. Der Datensatz der Zuordnungstabelle für Ergänzungsdaten wird zum Extrahieren der CSAF-URL und der Advisory-ID aus der Nutzlast von Empfehlungen verwendet.
Hinweise aus Antwort	Option zum Eingeben des Tag-Namens aus der Nutzlast von Empfehlungen, aus denen die Liste der Empfehlungen extrahiert werden kann.
Filterkriterien	
Zeitbereichsparameter	Option zum Auswählen des Zeitbereichs für die Anforderung und des Datumsformats für API-Aufrufe. Der Parameter „Start-/Enddatum-Anforderung“ ist der Parametername, der für Start- und Enddatum während API-Aufrufen verwendet wird. Beispiel: Startdatum , Start_date, endDate, end_date.
Datumsformat	Option zum Eingeben des Datumsformats, z. B. Mm/TT/JJJJ. . Das Datumsformat ist das Format, das die API zum Filtern benötigt. Formate, die von GlideDate nicht unterstützt werden, funktionieren nicht.
Anfänglicher Bereich in Tagen	E Geben Sie die Tage an, für die die Daten abgerufen werden müssen, wenn der Planer zum ersten Mal ausgeführt wird. Für nachfolgende Ausführungen wird der Mechanismus des Schiebefensters befolgt. **Hinweis:** Wenn Sie keinen Zeitbereich auswählen möchten, wählen Sie aus **Keine Parameter** .
Scannerzuordnungen	
Scannerquelle	Option zum Auswählen der Quelle des Drittparteieintrags (TPE).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schwachstellenspalte	Option zum Auswählen des Stichworts.
Stichwörter	Option zum Eingeben des Stichworts für die Suche in der ausgewählten Schwachstellenspalte.

4. Wählen Sie **Fertigstellen** aus.

Importieren Sie CSAF-Daten (Common Security Advisory Framework) über die CSAF-URL

Importieren Sie CSAF-Daten, indem Sie die Lieferanten-URL im Setup-Assistenten konfigurieren.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin, sn_vul.admin (veraltet) oder admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn die Integration ausgeführt wird, werden Daten aus der URL abgerufen, die analysiert wird. Die Daten werden dann in der Tabelle „sn_vul_Solution“ mit der Quelle als Lieferantenname gespeichert.

Hinweis:
Die URL kann entweder eine direkte CSAF-Nutzlast sein, die die Beratungsdetails enthält, oder eine ressourcenorientierte Feed-URL für Lightweight Information Exchange (ROLIE). In beiden Fällen wird die Nutzlast entsprechend analysiert, und die Lösungsdatensätze werden erstellt. Führen Sie die folgenden Schritte für den CSAF-URL-Import aus.

Sie können auch Schwachstellenlösungen aus CSAF-Aggregatoren oder vertrauenswürdigen Anbietern über einen URL-Import importieren, der ROLIE-Feed unterstützt. Diese Schwachstellen-Lösungen werden basierend auf Common Vulnerabilities and Exposures (CVEs) automatisch dem richtigen Lieferanten und angreifbaren Elementen (Vits) zugeordnet.

Die Scannerzuordnung gilt nicht für NVD-basierte Schwachstellen (National Vulnerability Database), bei denen es sich um Schwachstellen mit einem Common Vulnerability Entry (CVE) in der NVD-Datenbank handelt.

Wenn Sie nur über eine am höchsten ersetzende Lösung verfügen und ein Rolldown zu den angreifbaren Elementen durchgeführt wird, wird die bevorzugte Lösung ausgefüllt. Wenn in einem NVD-Eintrag mehrere Lieferantenlösungen enthalten sind, wird die bevorzugte Lösung nicht ausgefüllt, da mehr als eine höchste Ersatzlösung vorhanden ist. In diesem Fall müssen Sie manuell eine Lösung auswählen. Bei Schwachstellen von Drittparteien wird die bevorzugte Lösung nur ausgefüllt, wenn Sie die entsprechende Scannerzuordnung hinzufügen.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Integrationskonfiguration** > **Lösungsintegrationen** > **Allgemeines Framework Für Sicherheitswarnhinweise**an.
2. Wählen Sie Aus **Fügen Sie Die Integration Hinzu** .
3. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „CSAF importieren“

Feld	Beschreibung
Importtyp	Typ des Imports. Wählen Sie Aus **URL** .
Name	Eindeutiger Name für die Integration.
Einzelner Lieferant	Wählen Sie diese Option aus, wenn Sie CSAF von einem Lieferanten importieren.
Lieferant	Name des Lieferanten. Dieses Feld ist nur verfügbar, wenn Sie auswählen **Einzelner Lieferant** . **Hinweis:** Die **Quelle** Das Feld der Lösungen wird mit dem Lieferantennamen ausgefüllt.
Mehrere Lieferanten	Wählen Sie diese Option aus, wenn Sie CSAF von mehreren Lieferanten importieren.
Aggregator	Ein vertrauenswürdiger Anbieter, dessen Lösung Sie importieren können.
URL	URL, von der Sie die Lösungsdaten im CSAF-Format abrufen möchten.
Zeitplan	Häufigkeit, mit der die Daten aktualisiert werden müssen. **Hinweis:** Wenn das Status-Tag von CSAF „ENDGÜLTIG“ anzeigt, wird das Feld automatisch auf festgelegt **Bei Bedarf** Um unnötige Ausführungen zu verhindern.
Tag	Wochentag, an dem die Daten aktualisiert werden sollen.
Zeit	Uhrzeit der Woche, zu der die Daten aktualisiert werden sollen.
Scanner-Zuordnungen **Hinweis:** Der Abschnitt „Scannerzuordnungen“ ist für CSAF optional.	
Scannerquelle	Option zum Auswählen der Quelle des Drittparteieintrags (TPE).
Schwachstellenspalte	Option zum Auswählen des Stichworts.
Stichwörter	Option zum Eingeben des Stichworts für die Suche in der ausgewählten Schwachstellenspalte.

4. Wählen Sie **Fertigstellen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlerbehebung beim Datenimport des Common Security Advisory Framework

Problembehebungsaktionen können bei der Lösung gängiger Probleme beim Importieren von CSAF-Daten in die Vulnerability Response-Anwendung helfen.

Problem	Aktion
Die Dauer der Integrationsausführung ist lang	Wenn die Integration länger als erwartet ausgeführt wird, gehen Sie wie folgt vor: 1. Navigieren Sie zur Tabelle sn_vul_ds_Import_q_entry. 2. Gruppieren nach **Status** Feld. Sie können die Einträge sehen, die sich im status Abgeschlossen, in Bearbeitung oder in der Warteschlange befinden.
Integration beim API-basierten Import fehlgeschlagen	Wenn die Integration beim API-basierten Import fehlschlägt, gehen Sie wie folgt vor: 1. Navigieren Sie zu **Flow Designer** . 2. Öffnen Sie den Flow, der in der Konfiguration ausgewählt wurde. **Hinweis:** Im Fall von Red Hat, Öffnen Sie den Flow „Advisory Analysing“. 3. Wählen Sie Aus **Ausführungen** . 4. Öffnen Sie die neueste Ausführung oder die Ausführung, die debuggiert werden muss. 5. Überprüfen Sie den Flow in jeder Phase.
Integration im API-basierten Import mit einem Zeitüberschreitungsfehler fehlgeschlagen	Wenn die Integration in einem API-basierten Import aufgrund einer Zeitüberschreitung im Flow der beratenden Analyse fehlschlägt, gehen Sie wie folgt vor: 1. Erhöhen Sie die Zeitüberschreitung, indem Sie öffnen sys_properties.LIST . 2. Suchen Sie in der Spalte Name nach `sn_vul.CVRFFlowTimeout (inMiliSeconds)` . **Hinweis:** Die Zeit wird in Millisekunden angegeben. 3. Öffnen Sie den Datensatz, und aktualisieren Sie den Wert mit einer großen Zahl. 4. Speichern Sie den Datensatz, und führen Sie die Integration erneut aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problem	Aktion
Integration mit Fehler „Scannerzuordnung zu Lieferantenzuordnungsdaten wird ausgeführt“ fehlgeschlagen	Überprüfen Sie, ob die Integration während des URL- oder API-basierten Imports mit dem folgenden Fehler fehlschlägt: Die Transformation der Scannerzuordnung zu Lieferantenzuordnungsdaten wird ausgeführt. Daten werden erst ausgefüllt, nachdem die Transformation abgeschlossen ist. Versuchen Sie, nach einiger Zeit auszuführen. Wenn dieser Fehler auftritt, warten Sie einige Zeit, und führen Sie die Integration erneut aus.
Importwarteschlange wird während des Dateiimports nicht erstellt	Während eines Dateiimports wird die Importwarteschlange manchmal nicht erstellt. Dieser Fehler bedeutet, dass die Transformation, die Scanner-Zuordnungsdaten zu Lieferanten-Zuordnungsdaten zuordnet, ausgeführt wird. Der Warteschlangeneintrag wird erstellt, sobald der Prozess abgeschlossen ist.

Zusätzlich Vulnerability Response Setup- und Konfigurationsaufgaben

Um Sie bei der Korrektur zu unterstützen, können Sie diese zusätzlichen administrativen Setup-Aufgaben als Teil Ihrer Konfiguration außerhalb des Standard-Setups ausführen. Sie führen diese Aufgaben außerhalb des Setup-Assistenten aus.

Sie können die mit bereitgestellten Standardberichte verwenden Vulnerability Response Um Ihre Sicherheitslage zu überwachen. Sie können diese Berichte bearbeiten, wenn sie nicht zu Ihrer Umgebung passen, oder sie als Vorlagen verwenden, um eigene zu erstellen.

Wenn Performance Analytics for Vulnerability Response Die Anwendung ist installiert. Sie können Berichte, reaktionsfähige Dashboards und mehr erstellen. Siehe Erste Schritte mit Berichten Weitere Informationen finden Sie unter .

E-Mail-Benachrichtigungen erhöhen die Produktivität und den reibungslosen Workflow.

Suchen Sie mit der Bewertung des Softwarerisikos nach Herausgeber, Produktname und Versionsnummer in Software Asset Management (SAM Foundation), um Ihr Risiko für angreifbare Software zu bestimmen.

Transparenz in Schwachstellen-Bibliotheken kann Flexibilität bei Gruppierungs- und Korrekturaufgaben bieten.

Konfigurieren Sie das Ausnahmemanagement, damit Sie eine Ausnahme anfordern können, wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Richtlinie nicht einhalten kann.

Weitere zusätzliche Setup-Aufgaben finden Sie in den Themen, die dieser Übersicht folgen.

Schnellstarttests für Vulnerability Response

Überprüfen Sie, ob Vulnerability Response immer noch funktioniert, nachdem Sie eine Konfigurationsänderung vorgenommen haben, z. B. Anwendung eines Upgrades oder Entwickeln einer Anwendung. Kopieren Sie diese Schnellstarttests und passen Sie sie an, um sie bei der Verwendung Ihrer instanzspezifischen Daten zu übergeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder Demoaccounts erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz in nicht-Produktion oder Produktion verwendet wird. Siehe Führen Sie die Test-Suite für Automated Test Framework (ATF) aus Vulnerability Response Weitere Informationen zum Einrichten und Ausführen der Test-Suite für Vulnerability Response.

Vulnerability Response-Schnellstarttests erfordern die Aktivierung der Anwendung Vulnerability Response (sn_vul) und das Laden der Demodaten.

Vulnerability Response-Tests

Test	Beschreibung	Release-Version
VR: Fehlerkorrektur-Zielregel erstellen	Erstellt eine Fehlerkorrektur-Zielregel.	Madrid
VR: Schwachstellengruppenregel erstellen	Erstellt eine Schwachstellengruppenregel.	Madrid
VR: Erstellen eines angreifbaren Elements über das Formular	Ermittelt, ob ein Benutzer ein angreifbares Element erfolgreich aus dem Formular „Angreifbares Element“ erstellen kann.	Madrid
VR: Schwachstellengruppen-Lebenszyklus	Ermittelt, ob ein Benutzer eine Schwachstellengruppe erfolgreich beheben kann.	Madrid
VR: Lebenszyklus von angreifbaren Elementen	Ermittelt, ob ein Benutzer ein angreifbares Element erfolgreich durch seinen Lebenszyklus bewegen kann, und ermittelt zudem, ob ein abgeschlossenes angreifbares Element erneut geöffnet werden kann.	Madrid
VR: Rollup-Rechner	Ermittelt, ob der Rollup-Risiko-Rechner eine Gesamtrisikopunktzahl für eine ganze Gruppe angreifbarer Elemente mit den Punktzahlen für alle angreifbaren Elemente in einer Schwachstellengruppe verfügbar machen kann.	New York
VR: Vulnerability Response-Zuweisungsregeln	Ermittelt, ob mit einem Mustersatz von Zuweisungsregeln angreifbare Elemente automatisch einer Zuweisungsgruppe zur Nachbesserung zugewiesen werden können.	New York
VR: Schwachstellen-Rechner	Testen Sie die Schwachstellen-Rechner.	New York
VR: CI-Suche – Qualys	Erstellt mithilfe der Methode „field_matching“ eine neue Suchregel mit der Bezeichnung	Orlando

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response-Tests (Fortsetzung)

Test	Beschreibung	Release-Version
	„Suche nach Netzwerkadapter“ für Qualys. Ermittelt, ob Konfigurationselemente mit der neuen Suchregel erfolgreich nach Netzwerkadapter und IP-Adresse mit der Tabelle „Erkannte Elemente“ abgeglichen werden.	
VR: Normale Change-Anforderungen und Notfall-Change-Anforderungen erstellen	Ermittelt, ob der Benutzer erfolgreich normale Change-Anforderungen und Notfall-Change-Anforderungen aus einer Schwachstellengruppe erstellen kann.	Orlando
VR: Schwachstellengruppen aufteilen	Ermittelt, ob der Benutzer Schwachstellengruppen erfolgreich aufteilen kann.	Orlando
VR: SG-Status bei Abbruch von CHG aktualisieren	Ermittelt, ob in einer Schwachstellengruppe die Angabe im Feld „Status“ erfolgreich wechselt, wenn eine Change-Anforderung, die der Schwachstellengruppe zugeordnet ist, abgebrochen wird.	Orlando
VR: SG-Status aktualisieren, wenn CHG zur Überprüfung wechselt	Ermittelt, ob in einer Schwachstellengruppe die Angabe im Feld „Status“ erfolgreich wechselt, wenn eine Change-Anforderung, die der Schwachstellengruppe zugeordnet ist, in den Überprüfungsstatus wechselt.	Orlando
VR: CI-Suche – Rapid7	Testen Sie die CI-Suche mithilfe der vorhandenen Rapid7 Vulnerability-Integration-Suchregel **IP-Adresse**.	Orlando
VR: CI-Suche – Qualys	Testen Sie die CI-Suche, indem eine neue Suchregel für Qualys Vulnerability Integration erstellt wird.	Orlando
VR: Ausnahmegenehmigungs-Workflow für VI	Erstellen Sie eine Ausnahmeanforderung, und überprüfen Sie, ob der Genehmigungsprozess funktioniert.	Orlando
VR: Falsch positiver Genehmigungsworkflow für VI	Erstellen Sie eine falsch positive Ausnahmeanforderung, und überprüfen Sie, ob der Genehmigungsprozess funktioniert.	Orlando

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response-Tests (Fortsetzung)

Test	Beschreibung	Release-Version
VR: Application Vulnerability Response (AVR)	Bestimmen Sie, ob Ihre Regeln und Rechner ordnungsgemäß funktionieren. Stellen Sie sicher, dass Updates funktionieren.	Orlando
Korrekturzielregeln: VI-Importtest	Testet die VR-Korrekturzielregeln während des Imports.	Paris
VR: Klassifizierungsregel	Beispiel für eine Klassifizierungsregel, die eine Schwachstelle automatisch klassifiziert.	Tokyo

Zugehörige Informationen

Schnellstarttests

Führen Sie die Test-Suite für Automated Test Framework (ATF) aus Vulnerability Response

Führen Sie die Testsuite Automated Test Framework (ATF) aus, nachdem Sie installiert oder aktualisiert haben Vulnerability Response Anwendung.

Vorbereitungen

Bestätigen Sie eine erfolgreiche Installation und dass Ihre Instanz wie geplant funktioniert.

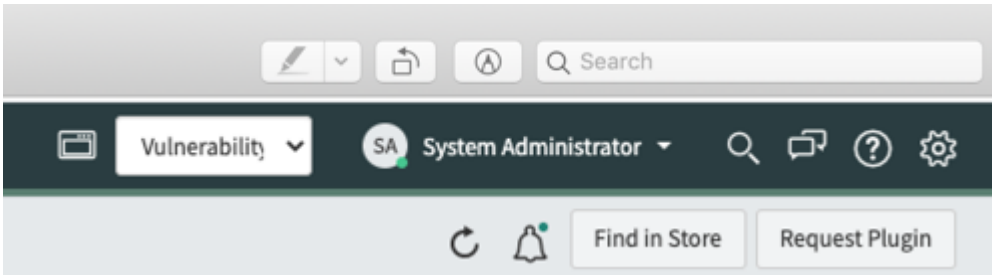
Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder Demoaccounts erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz in nicht-Produktion oder Produktion verwendet wird.

- Überprüfen Sie, ob Sie Demodaten installiert haben, als Sie installiert haben Vulnerability Response. Zum Ausführen von sind Demodaten erforderlich Vulnerability Response Test-Suite.
- Führen Sie die folgenden Schritte aus, um den Test zu aktivieren:

1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Administration** > **Eigenschaften**an.
2. Wenn nicht ausgewählt, wählen Sie aus **Aktivieren Sie die Ausführung der Test-/Test-Suite** Kontrollkästchen.
3. Klicken Sie auf **Speichern**.
4. Wenn der Bereich nicht auf festgelegt ist **Vulnerability Response** Klicken Sie im Header oder im Header nicht der Umfang angezeigt wird, auf das Einstellungssymbol oben auf der Seite im Browserfenster .
5. Klicken Sie im Fenster Systemeinstellungen auf **Entwickler** .
6. Wenn nicht ausgewählt, klicken Sie auf **Anwendungsauswahl im Header anzeigen** Und schließen Sie das Fenster.
7. In der Liste, die neben angezeigt wird Systemadministrator , Klicken Sie auf **Vulnerability Response** Für das Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

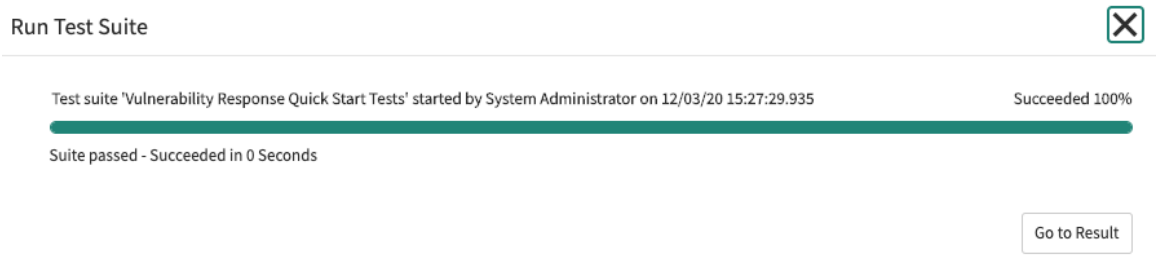
Das Feld wird wie in der folgenden Abbildung angezeigt.



Erforderliche Rolle: admin oder atf_test_admin

Prozedur

1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Suites**an.
2. Suchen Sie in der Test-Suites-Liste nach **Vulnerability Response-Schnellstarttests** .
3. Wählen Sie sie aus, um den Datensatz zu öffnen.
4. Wählen Sie im offenen Datensatz die aus **Aktiv** Kontrollkästchen.
5. Klicken Sie auf **Aktualisieren**.
6. Wenn **Führen Sie Die Test-Suite Aus** Schaltfläche wird nicht angezeigt. Aktualisieren Sie Ihren Bildschirm, öffnen Sie den Datensatz erneut, und klicken Sie auf **Führen Sie Die Test-Suite Aus** Um den Test zu starten.
   Nach einigen Minuten zeigt das Dialogfeld Test-Suite ausführen einen erfolgreichen Test an. Klicken Sie Auf **Wechseln Sie zum Ergebnis**Weitere Informationen finden Sie



unter .

Nächste Maßnahme

Herzlichen Glückwunsch! Sie können mit der Konfiguration von fortfahren Vulnerability Response.

Um weitere Informationen zu automatisierten Tests für zu erhalten Vulnerability Response Und automatisierte Tests, Test-Suites und das Erstellen automatisierter Tests finden Sie unter Automated Test Framework (ATF) .

Empfehlungen für die Zuweisung von Schwachstellen für Vulnerability Response installieren

Installieren Empfehlungen für die Zuweisung von Schwachstellen Damit Sie die Zeit reduzieren können, die Sie für die Identifizierung von Besitzern für nicht zugewiesene oder falsch zugewiesene Schwachstellenergebnisse aufwenden. Diese Anwendung ist als separates Abonnement in verfügbar ServiceNow Store.

Vorbereitungen

Bevor Sie ausführen Empfehlungen für die Zuweisung von Schwachstellen Funktion von Vulnerability Response In Ihrem ServiceNow AI Platform®-Instanz müssen Sie zuerst herunterladen und installieren Empfehlungen für die Zuweisung von Schwachstellen Für Vulnerability Response

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung. Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Weitere Informationen finden Sie unter Aktivieren Sie eine ServiceNow Store-Anwendung .

Erforderliche Rollen: administrator

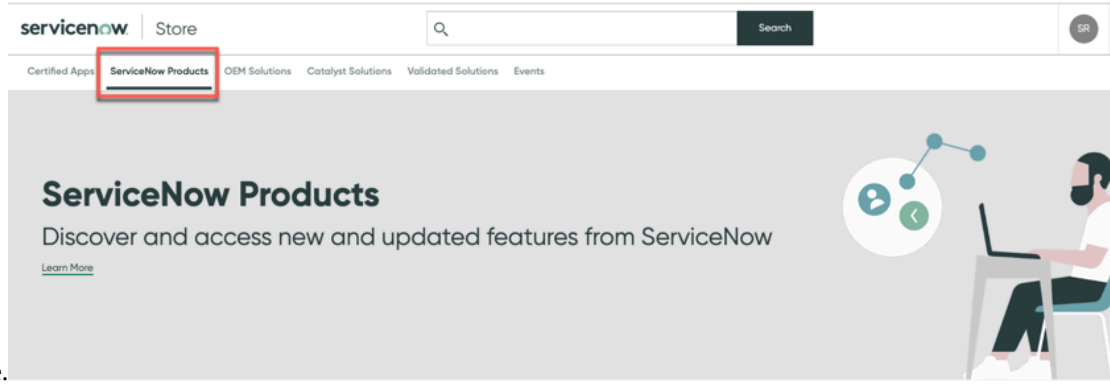
Setupaufgaben	Aktion
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Navigieren zu **Alle** > **Systemanwendungen** > **Alle Anwendungen** > **In Ihrer Instanz installiert**. Vulnerability Response Wird in dieser Liste angezeigt, wenn sie installiert ist. Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren.
Überprüfen Sie, ob Predictive Intelligence Anwendung ist installiert und aktiviert.	Navigieren zu **Systemanwendungen** > **Alle Anwendungen** > **In Ihrer Instanz installiert**. Predictive Intelligence Wird in dieser Liste angezeigt, wenn sie installiert ist. Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Install Predictive Intelligence .
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Überprüfen Sie, ob Sie über diese erforderlichen Rollen für die Installation und Verifizierung der erwarteten Ergebnisse verfügen: • Vulnerability_admin: Erforderlich zum Aktivieren und Konfigurieren Empfehlungen für die Zuweisung von Schwachstellen. Sie können es auch verwenden, um Zuweisungsempfehlungen für angreifbare Elemente und Korrekturaufgaben anzuzeigen und auszuwählen. • ServiceNow administrator: Erforderlich zum Installieren von Anwendungen.

Prozedur

1. Navigieren Sie zum ServiceNow Store.
2. Klicken Sie Auf **Melden Sie Sich An** Und geben Sie Ihre HI-Anmeldeinformationen ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Um die verfügbaren anzuzeigen ServiceNow Produkte klicken Sie auf ServiceNow **Produkte**Registerkarte.



4. Um alle zugehörigen Anwendungen anzuzeigen, für die Sie berechtigt sind Empfehlungen für die Zuweisung von Schwachstellen, Klicken Sie auf Vulnerability Response Produkt.

   Auf der Seite werden alle Anwendungen aufgelistet, für die Sie berechtigt sind, wenn Sie sich anmelden. Um Informationen zu einer Anwendung zu erhalten, klicken Sie auf den Link für die Anwendung.

5. Um sicherzustellen, dass Sie die Berechtigung für haben Empfehlungen für die Zuweisung von Schwachstellen, Klicken Sie auf **Aktivieren** .

6. Um den Nutzungsbedingungen zuzustimmen, aktivieren Sie bei der Aufforderung das Kontrollkästchen, und klicken Sie auf **Akzeptieren** .
   Eine Meldung wird angezeigt, die angibt, dass Sie sich erfolgreich für die Anwendung angemeldet haben.

7. Fahren Sie mit Schritt 10 fort, um die Anwendung auf Ihrem zu installieren ServiceNow AI Platform Instanz.

8. **Wahlweise:** Wenn Sie Ihre Berechtigung für verwalten möchten Empfehlungen für die Zuweisung von Schwachstellen Anwendung für andere ServiceNow AI Platform Instanzen, klicken Sie auf **Berechtigung Verwalten** .

   Hinweis:

   (Optional) Wenn **Berechtigung Verwalten** Die Schaltfläche wird nicht angezeigt. Klicken Sie auf Empfehlungen für die Zuweisung von Schwachstellen Anwendung in der Produktliste, um sie anzuzeigen.

   a. Wählen Sie eine Option.

   b. Klicken Sie Auf **OK** Oder **Abbrechen** Um fortzufahren.
   Sie sind bereit, Plugins zu aktivieren und die Anwendung auf Ihrem zu installieren ServiceNow AI Platform Instanzen.

9. Melden Sie sich bei an ServiceNow AI Platform Instanz, die Sie installieren möchten Empfehlungen für die Zuweisung von Schwachstellen Anwendung auf.

10. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.

11. Suchen Sie in den aufgeführten Anwendungen nach Empfehlungen für die Zuweisung von Schwachstellen Anwendung (sn_vul_Recom), und klicken Sie auf **Installieren** .
    Das Dialogfeld Anwendungsinstallation wird angezeigt, und alle installierten Abhängigkeiten werden angezeigt.

12. **Wahlweise:** Wenn Sie Demodaten möchten, wählen Sie aus **Demodaten laden** Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Installieren** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie nicht auswählen **Demodaten laden** Kontrollkästchen: Demodaten können später nicht vom Anwendungsmanager installiert werden. Informationen zur Installation oder Neuinstallation von Demodaten nach der Erstinstallation finden Sie unter Problemumgehung zum Installieren von Demodaten, wenn die Anwendung bereits installiert ist [KB0722909] artikel in Now Support Knowledge Base.

Diese Installation kann einige Zeit dauern. Nachdem die Anwendung und ihre Abhängigkeiten erfolgreich installiert wurden, wird im Dialogfeld „Installieren“ eine Nachricht angezeigt.

13. Klicken Sie auf **Schließen**.
14. Zum Konfigurieren Empfehlungen für die Zuweisung von Schwachstellen, Siehe Konfigurieren Sie Empfehlungen für die Schwachstellenzuweisung für Vulnerability Response.

Konfigurieren Sie Empfehlungen für die Schwachstellenzuweisung für Vulnerability Response

Aktivieren Empfehlungen für die Zuweisung von Schwachstellen Um die Zeit zu reduzieren, die Sie für die Identifizierung der Besitzer von Schwachstellenergebnissen aufwenden, die nicht oder falsch zugewiesen sind.

Vorbereitungen
Erforderliche Rolle: sn_vul.manage_assignment_Recom_config

Warum und wann dieser Vorgang ausgeführt wird
Diese Anwendung ist standardmäßig nicht aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Zuweisungsempfehlungen**an.
2. Wählen Sie Aus **Aktivieren Sie Zuweisungsempfehlungen** .
   Die **Predictive Intelligence-Lösungsdefinitionsfeld** Wird angezeigt. Der Standardwert ist **Zuweisung Angreifbarer Elemente** .
3. Klicken Sie auf **Speichern**.

Erstellen und trainieren Sie eine Lösungsdefinition für Vulnerability Response

Erstellen und trainieren Sie ein Lösungsdefinitionsmodell für Vulnerability Response Mit Predictive Intelligence. Sie können dieses Modell verwenden, um die Zuweisungsgruppe für ein angreifbares Element (VI) oder eine Korrekturaufgabe (RT) basierend auf vorhandenen Daten vorherzusagen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence** > **Klassifizierung** > **Lösungsdefinitionen**an.
2. Klicken Sie im Formular „Klassifizierungsdefinitionen“ auf **Zuweisung Angreifbarer Elemente** .
   Dies ist die Standardlösungsdefinition.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Die Standardschulungshäufigkeit beträgt 30 Tage. Dies bedeutet, dass das Modell alle 30 Tage automatisch erneut trainiert und dabei den VI-Datensatz verwendet, der der konfigurierten Filterbedingung entspricht.
- Felder aus der Tabelle „Angreifbares Element“ können für Schulungen verwendet werden. Die Standardlösungsdefinition trainiert für zwei VI-Felder: **Schwachstelle.Zusammenfassung** Und **Konfigurationselement.Name** . Sie können die für das Training verwendeten Felder anpassen, je nachdem, welche Felder Ihnen bei der Vorhersage des Besitzes von Schwachstellen in Ihrer Organisation hilfreich sind.

3. Informationen zum Erstellen und Trainieren der Klassifizierungslösung finden Sie unter Erstellen und trainieren Sie eine Klassifizierungslösung .

Hinweis:
Sie können auch eine Ähnlichkeits- oder Clustering-Lösung erstellen und trainieren. Weitere Informationen finden Sie unter:

- Ähnlichkeitslösung erstellen und trainieren .
- Erstellen und trainieren Sie eine Clustering-Lösung .

4. Klicken Sie auf **Update & Retrain (Aktualisieren und neu trainieren)**.

Hinweis:
Informationen zum Konfigurieren erweiterter Einstellungen für ML-Lösungen finden Sie unter Erweiterte Einstellungen für Ihre ML-Lösungen konfigurieren .

Erstellen Sie einen Vulnerability Response Rechner

Ein Schwachstellenrechner ist eine vordefinierte Formel zum Berechnen eines Zielfelds, wenn bestimmte Kriterien erfüllt sind. Rechner, die das angreifbare Element berechnen **Risikopunktzahl** , Kann enthalten **Risikoregeln** .

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Hinweis:
Bei der Ausführung von Schwachstellenrechnern, die Skripts enthalten, kann es zu einer Leistungsverschlechterung kommen.

Ordnen Sie Ihre Regeln so an, dass zuerst die einfachsten Regeln ausgeführt werden und nur Skripts für die Elemente ausgeführt werden, die nicht mit einem Bedingungs- und Vorlagenwert oder einer Risikoregel behandelt werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Schwachstellen-Rechner**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Formular „Schwachstellenrechner“

Feld	Beschreibung
Name	Der Name des Schwachstellenrechners.
Tabelle	Wird automatisch mit dem Namen der Tabelle für angreifbare Elemente ausgefüllt.
Anwendung	Automatisch ausgefüllt mit Vulnerability Response.
Zielfeld	Zu berechnendes Feld.
Beschreibung	Textbeschreibung des Rechners.
Aktiv	Aktivieren oder deaktivieren Sie den Rechner.

4. Klicken Sie mit der rechten Maustaste in den Header zu **Speichern** .
   Die **Regeln Für Schwachstellenrechner** Abschnitt wird angezeigt.
5. Erstellen Sie eine Regel für den Rechner, indem Sie auf klicken **Neu** .

Hinweis:
Für **Neue Risikoregeln** Formular (nur verfügbar, wenn **Zielfeld** Ist **Risikopunktzahl**) Siehe Schritt 10.

6. Füllen Sie die Felder entsprechend aus.

Formular „Schwachstellen-Rechner-Regel“

Feld	Beschreibung
Name	Name der Rechnerregel.
Reihenfolge	Die Reihenfolge, in der der Schwachstellenrechner ausgeführt werden soll. Ein Rechner mit einer Auftragseingabe von 100 wird vor einem Rechner mit einer Auftragseingabe von 200 ausgeführt.
Rechner	Wird automatisch mit dem übergeordneten Rechner ausgefüllt.
Aktiv	Standardmäßig ist **Aktiv** Das Kontrollkästchen ist aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie dieses Kontrollkästchen deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt wurden.
Erweiterte Ansicht	Wenn diese Option ausgewählt ist, können geskriptete Bedingungen und geskriptete Werte aus ausgewählt werden **Bedingungstyp** Und **Werttyp** .

7. Füllen Sie die Felder im aus **Wenn diese Bedingung erfüllt ist** Registerkarte entsprechend.

Registerkarte „wenn diese Bedingung erfüllt ist“

Feld	Beschreibung
Name	Name der Rechnerregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Reihenfolge	Die Reihenfolge, in der der Schwachstellenrechner ausgeführt werden soll. Ein Rechner mit einer Auftragseingabe von 100 wird vor einem Rechner mit einer Auftragseingabe von 200 ausgeführt.
Rechner	Wird automatisch mit dem übergeordneten Rechner ausgefüllt.
Aktiv	Standardmäßig ist **Aktiv** Das Kontrollkästchen ist aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie dieses Kontrollkästchen deaktivieren, gilt diese Regel nicht für angreifbare Elemente, die im System erstellt wurden.
Erweiterte Ansicht	Wenn diese Option ausgewählt ist, wählen Sie unter Skriptbedingungen und geskriptete Werte aus **Bedingungstyp** Und **Werttyp** .
Bedingungstyp	Verfügbar, wenn Sie auswählen **Erweiterte Ansicht** . Zur Auswahl stehen: ○ Filter: Verwendet Filterbedingungen. ○ Filtergruppe: Siehe Erstellen Sie eine neue Filtergruppe Zum Definieren der Rechnerkriterien. ○ Skript: Skriptbedingung, die verwendet wird, um zu bestimmen, wann dieser Rechner angewendet werden soll. **Hinweis:** Bevor Sie Skripts schreiben, um zu bestimmen, wann die Rechner angewendet werden sollen, kehren Sie zu zurück **Schwachstellenrechner** Liste. Erkunden Sie die mit dem Basissystem gelieferten Schwachstellenrechner-Datensätze.
Bedingung	Definiert grundlegende Filterbedingungen, um zu bestimmen, ob der Rechner verwendet werden soll oder nicht. Wählen Sie entweder aus **Filtergruppe** Oder **Skript** Bedingungstypen, blendet dieses Feld aus. Die Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird in diesem Datensatz oder Formular nicht unterstützt.

8. Klicken Sie auf **Legen Sie diese Werte fest** Registerkarte und füllen Sie die Felder im Formular entsprechend aus.

Legen Sie die Registerkarte diese Felder fest

Feld	Beschreibung
Werttyp	Verfügbar, wenn Sie auswählen **Erweiterte Ansicht** . Zur Auswahl stehen: ○ Vorlage: Definieren Sie die Werte, die für jedes Feld festgelegt werden sollen. ○ Skript: Wird verwendet, um die Werte für jedes Feld festzulegen.
Skriptwerte	Verfügbar, wenn Sie ausgewählt haben **Skript** Werttyp. Definiert, auf welche Werte die Berechnungen angewendet werden sollen.
Vorlage	Wählen Sie die Felder und Werte aus, die Sie für den Rechner verwenden möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wählen Sie entweder aus **Skript** Werttyp, blendet dieses Feld aus.

9. Wenn Sie alle Einträge abgeschlossen haben, klicken Sie auf **Übermitteln** .

Hinweis:
Wenn Sie einen vorhandenen Rechner bearbeiten und alle vorhandenen Punktzahlen aktualisieren möchten, können Sie verwenden **Rechner Erneut Anwenden** Schaltfläche. Er durchläuft alle aktiven angreifbaren Elemente (VIS). Wenn dieser Rechner zum Festlegen seines Werts verwendet würde, berechnet er den Wert für diese VIS neu. Da das erneute Anwenden eines Rechners lange dauern kann, wird er von einer geplanten Aufgabe verarbeitet.

10. Für **Neue Risikoregeln** Füllen Sie die Felder entsprechend aus.

Legen Sie jede Gewichtung entsprechend dem Prozentsatz des Ergebnisses fest, der aus diesem Wert stammen soll. Legen Sie für alle Daten, die Ihr Scanner nicht bereitstellt, oder für Daten, die nicht Teil der Risikopunktzahl sein sollten, die Gewichtung auf null fest.

Sie können die Felder hinzufügen, löschen oder aktualisieren. Sie können auch den Gewichtungsprozentsatz für die Feldwerte konfigurieren. Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel für Vulnerability Response-Risikorechner.

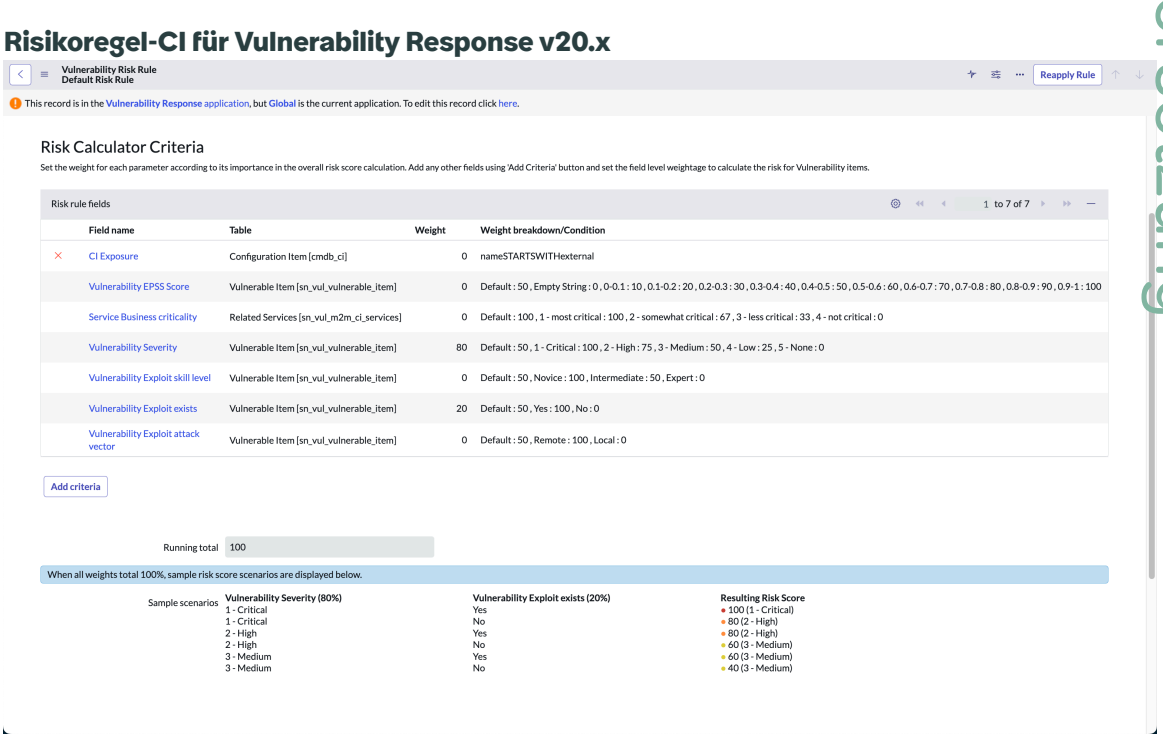
Während Sie die Gewichtungen aktualisieren, zeigen Szenarien die verbleibenden Gewichtungen sowie die erwarteten Gewichtungen an **Risikopunktzahl** Ergebnisse.

Feld	Beschreibung
Name	Name der Rechnerregel.
Reihenfolge	Die Reihenfolge, in der der Schwachstellenrechner ausgeführt werden soll. Ein Rechner mit einer Auftragseingabe von 100 wird vor einem Rechner mit einer Auftragseingabe von 200 ausgeführt.
Rechner	Wird automatisch mit dem übergeordneten Rechner ausgefüllt.
Aktiv	Standardmäßig ist **Aktiv** Das Kontrollkästchen ist aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie dieses Kontrollkästchen deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt wurden.
Bedingung	Definiert grundlegende Filterbedingungen für die Bestimmung, ob der Rechner verwendet werden soll. Wählen Sie entweder aus **Filtergruppe** Oder **Skript** Bedingungstypen, blendet dieses Feld aus.
Gewichtungen	
Schwachstellenschweregrad	Prozentsatz des Ergebnisses, das aus dem Schweregrad stammt.
EPSS-Punktzahl der Schwachstelle	Wahrscheinlichkeit, dass die Schwachstelle ausgenutzt wird. Standardmäßig ist die Gewichtung dieses Kriteriums null. Wenn Sie dies für die Berechnung der Risikopunktzahl verwenden möchten, legen Sie eine entsprechende Gewichtung für diese Kriterien fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Exploit vorhanden	Prozentsatz des Ergebnisses, das aus dem Vorhandensein eines Exploits stammt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, legen Sie die Gewichtung auf null fest.
Exploit-Kompetenzniveau	Prozentsatz des Ergebnisses, das aus dem für den Exploit erforderlichen Kompetenzniveau stammt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, legen Sie die Gewichtung auf null fest.
Exploit-Angriffsvektor	Prozentsatz des Ergebnisses, das von dem Ziel des Angriffs stammt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, legen Sie die Gewichtung auf null fest.
Business-Relevanz des Service	Prozentsatz des Ergebnisses, das aus der Geschäftsrelevanz stammt. Wenn Sie Ihre CIs nicht mit Business-Services verknüpft haben, legen Sie die Gewichtung auf Null fest.
CI-Risiko	Prozentsatz des Ergebnisses, das daraus resultiert, ob das CI mit dem Internet verbunden ist. Wenn die Gewichtung ungleich Null ist, wird ein Bedingungsfilter angezeigt, um zu definieren, welche CI mit Internetzugriff verbunden sind. Legen Sie den Filter fest, um Ihre Konfigurationselemente mit Internetzugriff auszuwählen. Sie können eine Vorschau anzeigen, welche Datensätze mit der Bedingung übereinstimmen.
Laufende Summe	Automatisch berechnete Prozentsätze insgesamt. Wenn dieser Wert 100 erreicht, zeigt die Szenariovorschau Beispiele für Risikopunktzahlen in verschiedenen Szenarien.
Risikopunktzahlszenarien	Wenn alle Gewichtungen 100 % ergeben, werden Szenarien für Risikopunktzahlen angezeigt, die in einigen der möglichen Szenarien eine Vorschau der Risikopunktzahl bieten.

Sie können Kriterien hinzufügen oder entfernen und die Gewichtung jedes Kriteriums mithilfe der eingebetteten Liste anpassen.



11. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Deaktivieren Sie den standardmäßigen Schwachstellenrechner, wenn er nicht verwendet wird

Wenn Sie keine Schwachstellenrechner verwenden, deaktivieren Sie den Standardrechner zusätzlich zu allen anderen, die Sie definiert haben. Schwachstellenrechner werden jedes Mal ausgeführt, wenn ein Datensatz für angreifbare Elemente erstellt oder aktualisiert wird, und können sich auf die Leistung des ersten Imports auswirken.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Schwachstellen-Rechner**an.
2. Öffnen Sie den entsprechenden Rechner.
3. Löschen Sie **Aktiv** Kontrollkästchen zum Deaktivieren des Rechners.
4. Klicken Sie auf **Aktualisieren**.

Erstellen, aktivieren oder ändern Vulnerability Response Regeln automatisch löschen

Sie können die Löschregeln für Schwachstellen-Elemente (VI) und Korrekturaufgaben (RT) erstellen, aktivieren oder ändern. Verwenden Sie die automatische Löschung, um ältere Datensätze aus den VI- und RT-Tabellen zu entfernen.

Vorbereitungen
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Erforderliche Rollen:

- administrator: Ändern Sie die Regeln für das automatische Löschen
- sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet): Zeigen Sie das Modul zum automatischen Löschen an

Warum und wann dieser Vorgang ausgeführt wird
Im Laufe der Zeit wird sich wahrscheinlich eine große Anzahl geschlossener Datensätze in den VI- und DEN ANGREIFBAREN Tabellen in Ihrer Instanz ansammeln. Viele dieser Datensätze wurden möglicherweise länger als 365 Tage geschlossen, wurden jedoch nicht entfernt. Verwenden Sie Regeln zum automatischen Löschen, um viele dieser älteren, geschlossenen Datensätze zu entfernen. Durch das Entfernen dieser Datensätze wird nicht nur die Anzahl der Datensätze in den VI- und ANGREIFBAREN Tabellen erheblich reduziert, sondern auch das Löschen trägt dazu bei, eine hohe Leistung zu gewährleisten.

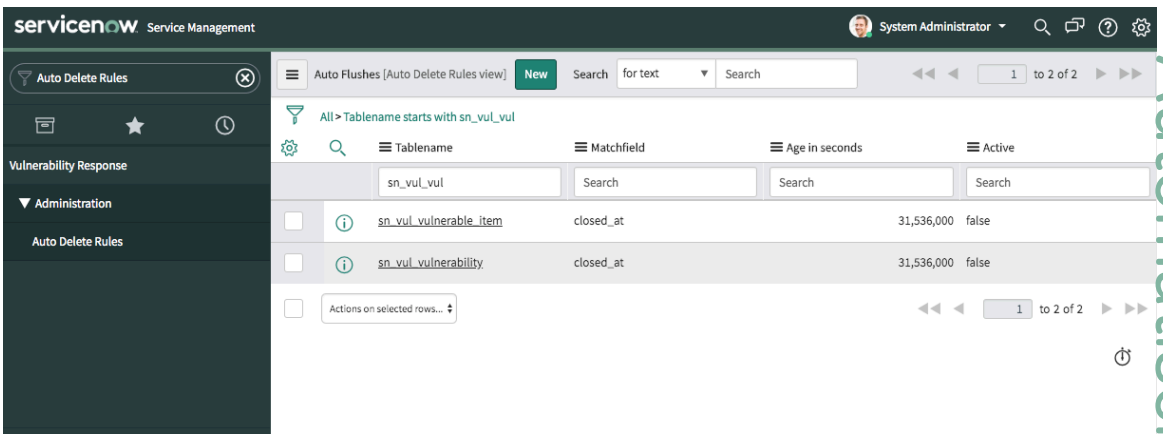
Obwohl Zieldatensätze standardmäßig automatisch gelöscht werden, die seit 365 Tagen geschlossen wurden, wird bei der allerersten Ausführung möglicherweise versucht, zu viele Datensätze in einer einzelnen Transaktion zu bereinigen. Je nach Größe Ihrer Umgebung ziehen Sie es möglicherweise vor, den Löschprozess zu staffeln, um den Umfang der Abfrage zu begrenzen. Sie können beispielsweise Ihre erste Ausführung für geschlossene Datensätze starten, die älter als 450 Tage sind. Nach Abschluss dieser Ausführung können Sie sich in kleineren Schritten (425, 400, 375) nach unten arbeiten, bis Sie die Anzahl der Datensätze reduziert haben, die älter als 365 Tage sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es gibt zwei Regeln, die mit bereitgestellt werden ServiceNow AI Platform® Die automatisch geschlossene Datensätze löschen, die die angegebenen Bedingungen erfüllen, zusammen mit allen Datensätzen, die darauf verweisen. Eine Regel löscht angreifbare Elemente, die andere Regel löscht Korrekturaufgaben. Standardmäßig sind diese Regeln für das automatische Löschen deaktiviert, sodass Sie sie vor dem Löschen von Datensätzen manuell aktivieren müssen. Sie können die beiden vorkonfigurierten Regeln auswählen, die mit Ihrer Instanz bereitgestellt werden, oder eigene Regeln erstellen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Regeln für das automatische Löschen**an.
   Die Listenansicht wird angezeigt.

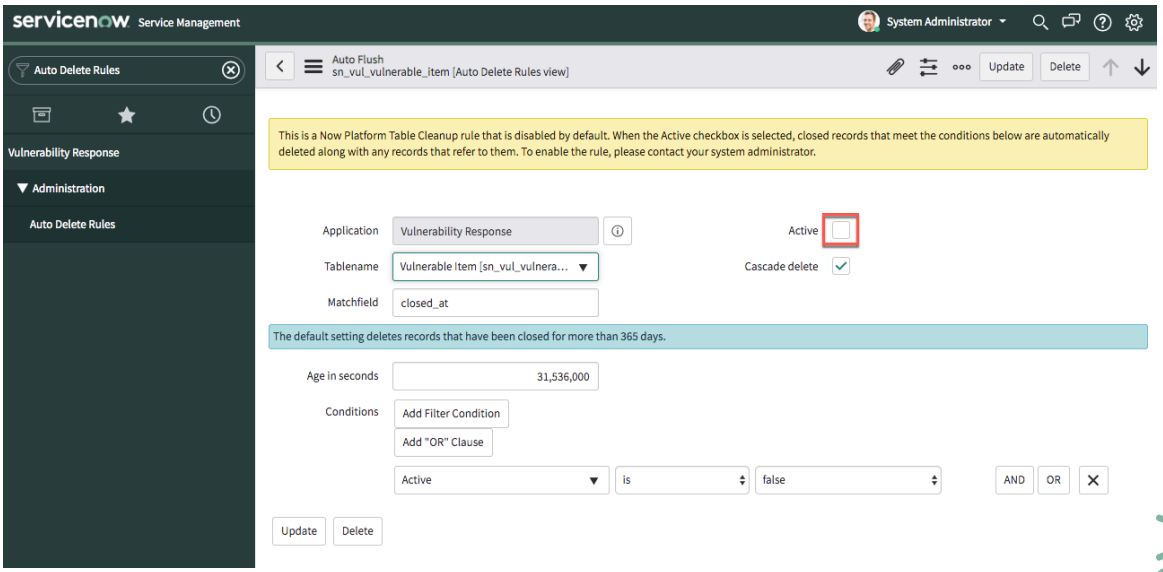


2. Wählen Sie zum Bearbeiten die Löschregel für angreifbare Elemente (sn_vul_vulnerable_item) oder die Regel für Korrekturaufgaben (sn_vul_Vulnerability) aus.
3. Klicken Sie zum Erstellen einer neuen Regel auf **Neu**.
4. Füllen Sie die Felder im Formular entsprechend aus, oder bearbeiten Sie sie.

Feld	Beschreibung
Anwendung	Name der Anwendung, in der Datensätze gelöscht werden. Der Standardwert ist Vulnerability Response.
Tabellenname	Name der Tabelle, für die die Regel angewendet wird.
Feld abgleichen	Feld, für das das System die Dauer überwacht.
Aktiv	Option zum Aktivieren der Regel. Nach der Aktivierung kann der Datensatz gelöscht werden.
Kaskadierendes Löschen	Option zum Löschen aller übereinstimmenden Datensätze sowie aller darauf bezogenen Datensätze. Wenn diese Option nicht ausgewählt ist, werden nur übereinstimmende Datensätze gelöscht, aber nicht die Datensätze, die darauf verweisen.
Alter in Sekunden	Alter des zu löschenden Schwachstellendatensatzes. Sowohl für VI- als auch RT-Regeln beträgt das Alter 365 Tage. Dieses Alter wird in Sekunden angezeigt.
Bedingungen	Filterbedingungen, die die Datensätze in den Tabellen VI und RT (VUL) definieren, für die die Regeln gelten.

5. Wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren einer Regel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sobald die Regel aktiviert ist, wird die stündliche Plattformfunktion **Automatisch leeren** , Löscht die Datensätze aus der Tabelle, für die die Regel aktiviert ist.

Wenn Ihre Umgebung Millionen oder Zehnmillionen von Datensätzen enthält, die Ihren Löschkriterien entsprechen, sollten Sie sich mit beraten ServiceNow Kundensupport vor dem Aktivieren der Regeln zum automatischen Löschen, damit Sie Datensätze mithilfe eines phasenbasierten Prozesses löschen können.

Fügen Sie der Vulnerability Response-Homepage Diagramme zur Bedeutung von Schwachstellen hinzu

Sie können der Übersicht Diagramme zur Definition der Schwachstellenbedeutung und andere Visualisierungen hinzufügen.

Vorbereitungen

- Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.
- Das Plugin „Vulnerability Analytics“ muss aktiviert sein.

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Übersicht**an.
   Einige Berichte werden standardmäßig dem Dashboard hinzugefügt. Weitere Informationen zu diesen Berichten finden Sie unter Wird standardmäßig verwendet Vulnerability Response Dashboards.
2. Klicken Sie in der Nähe des Dashboard-Headers auf das Kartenansichtssymbol + **Fügen Sie Inhalt hinzu** Zum Öffnen des Dialogfelds zum Hinzufügen weiterer Widgets.
3. Aus den Listen in **Widgets Hinzufügen** Dialogfeld auswählen **Berichte** Um mehr anzuzeigen Vulnerability Response Berichte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Position auf dem Bildschirm, an der Sie die Anzeige hinzufügen möchten.
5. Schließen Sie **Fügen Sie Inhalt hinzu** Feld.

Definieren Vulnerability ResponseE-Mail-Benachrichtigungen

Richten Sie E-Mail-Benachrichtigungen ein, um nützliche Informationen zu wichtigen Updates und Aktivitäten wie Genehmigung und Ablehnung falsch positiver Anforderungen zu teilen. Beim Erstellen einer E-Mail-Benachrichtigung wird angegeben, wann sie gesendet werden soll, wer sie erhält und was sie enthält.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **E-Mail-Vorlagen**an.
2. Wählen Sie **Neu**.

   Detaillierte Anweisungen zum Erstellen von E-Mail-Benachrichtigungen finden Sie unter Create an email notification .

Ergebnisse
Wenn ein Empfänger auf die Links in einer E-Mail-Benachrichtigung klickt, werden die Links in geöffnet Arbeitsbereich des Schwachstellenmanagers Oder Arbeitsbereich für IT-Korrekturen Basierend auf ihrer Rolle.

- Links werden in geöffnet Arbeitsbereich des Schwachstellenmanagers Für die Anwender mit den Rollen sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin.
- Links werden in geöffnet Arbeitsbereich für IT-Korrekturen Für die Anwender mit der Rolle sn_vul.Remediation_owner.

Wenn der Empfänger keine der vorherigen Rollen hat, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Definieren Vulnerability Response E-Mail-Vorlagen

Beim Erstellen einer E-Mail-Benachrichtigung wird angegeben, wann sie gesendet werden soll, wer sie erhält und was sie enthält.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **E-Mail-Vorlagen**an.
2. Wählen Sie **Neu**.

   Detaillierte Anweisungen zum Erstellen von E-Mail-Vorlagen finden Sie unter Construct an email message with a template .

Erstellen oder bearbeiten Sie Benachrichtigungen zu Korrekturzielen

Schwachstellenadministratoren können die Korrekturzielbenachrichtigung bearbeiten oder neue hinzufügen, indem sie angeben, wann die Benachrichtigung gesendet werden soll, wer die Benachrichtigung erhält und welchen Inhalt die Benachrichtigung enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Benachrichtigungen**an.
2. Wählen Sie den Benachrichtigungsdatensatz für das Korrekturziel aus, oder wählen Sie aus **Neu** .
3. Füllen Sie die Felder im Formular entsprechend aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Create an email notification .
4. Wählen Sie Aus **Vorschau Der Benachrichtigung Anzeigen** Zum Anzeigen der Nachricht.

Ergebnisse

Ab v21.0 von Vulnerability Response, Wenn ein Empfänger auf die Links in einer E-Mail-Benachrichtigung klickt, werden die Datensätze im geöffnet Arbeitsbereich des Schwachstellenmanagers Oder Arbeitsbereich für IT-Korrekturen Basierend auf ihrer Rolle.

- Links werden in geöffnet Arbeitsbereich des Schwachstellenmanagers Für die Anwender mit den Rollen sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin.
- Links werden in geöffnet Arbeitsbereich für IT-Korrekturen Für Anwender mit Rollen sn_vul.Remediation_owner.

Wenn der Empfänger keine der vorherigen Rollen hat, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Konfigurieren Sie Schwachstelle Risikobewertung

Bewerten Sie mit das Zero-Day-Risiko (aktueller Tag) Ihrer Assets für angreifbare Software Schwachstelle Anwendung „Risikobewertung“.

Wichtig:
Sie können die Risikobewertung nach Common Vulnerabilities and Exposures (CVE) und Software durchführen, um die zusätzlichen Fähigkeiten im Vulnerability Assessment-Arbeitsbereich zu nutzen. Weitere Informationen finden Sie unter Arbeitsbereich für Schwachstellenbewertung kennenlernen.

Erforderliche Rolle: Administrator

Kompatibilitäts- und Systemanforderungen

Die Vulnerability Response Anwendung ist auf verfügbar ServiceNow Store. Die Software Asset Management(SAM) Foundation-Anwendung [com.snc.Asset_Management] wird als Teil von installiert Vulnerability Response Anwendung. Um zu überprüfen, dass SAM Foundation Die Anwendung ist auf Ihrer Instanz installiert. Navigieren Sie zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** Und suchen Sie nach `Com.snc.Asset_Management` . Wenn die Anwendung nicht installiert ist, wählen Sie aus **Installieren** . Weitere Informationen zu SAM Foundation finden Sie unter Software Asset Management Foundation plugin .

Seit Schwachstelle Die Anwendung „Risikobewertung“ erfordert Zugriff auf die Asset-Daten in Ihrem ServiceNow AI Platform® Instanz müssen die Asset-Management-Anwendungen über Daten verfügen, auf die verwiesen werden soll. Die Tabelle „Software-Discovery-Modelle“ [cmdb_sam_SW_Discovery_model] und die Softwareinstallationen [cmdb_sam_SW_install] erfordern Daten.

Die Schwachstelle Anwendung „Risikobewertung“ Auch Funktioniert entweder mit SAM Foundation Oder SAM Pro ServiceNow AI Platform® Anwendungen. Die SAM Pro-Anwendung ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nicht Teil des Core Vulnerability Response Produkt aus dem ServiceNow Store Und erfordert ein separates Abonnement.

Hinweis:
Die SAM Pro-Anwendung ist nur für die Inhaltsbibliothek erforderlich, die bessere Ergebnisse erzielen kann.

Ab v23.0 von Vulnerability Response, Wenn Sie das Pro- oder Enterprise-Abonnement haben, werden Sie zu weitergeleitet **Risikobewertung** Seite in den Arbeitsbereichen basierend auf Ihrer Rolle, wenn Sie auf klicken **Risikobewertung** Link in **Alle** Menü:

Zugriff auf die Risikobewertungsseite in den Arbeitsbereichen

Rolle	Arbeitsbereich
Schwachstellenmanager	Arbeitsbereich des Schwachstellenmanagers
Ereignismanager [sn_vul_Analyst.vul_event_Manager] oder Notfallantwort [sn_vul_Analyst.Emergency_response]	Arbeitsbereich der Schwachstellenbewertung

Um zu vermeiden, zu den Arbeitsbereichen umgeleitet zu werden und auf der Seite „Klassische Risikobewertung“ zu bleiben, legen Sie fest **Linktyp** Bis *Liste der Datensätze* Auf der Registerkarte Linktyp auf der Seite Modul – Risikobewertung. Sie können auf die Seite Modul – Risikobewertung zugreifen, indem Sie auswählen **Modul Bearbeiten** Symbol neben **Risikobewertung** Link in **Alle** Menü.

Mit der Rolle „Schwachstellen schreiben“ [sn_Vulnerability_write] können Sie das Modul „Risikobewertung“ anzeigen und Risikobewertungsdatensätze bei Bedarf für angreifbare Software in Ihrer Instanz mit erstellen und bearbeiten Vulnerability Response Anwendung.

Zugehörige Informationen

Bewerten Sie Ihr Risiko für angreifbare Software

Konfigurieren Sie das Ausnahmemanagement für Vulnerability Response

Wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Richtlinie nicht einhalten kann, können Sie eine Ausnahme anfordern. Das Ausnahmemanagement umfasst das anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Element (VI) oder eine Korrekturaufgabe (RT), die nicht gemäß der Richtlinie korrigiert werden können.

Vorbereitungen

Begrenzen Sie die Dauer einer angeforderten Ausnahme Und fügen Sie der Anforderung „Ausnahme“ oder „falsch positiv“ einen Fragebogen hinzu Mit Vulnerability Response Modul. Standardmäßig wird mit eine Ausnahme angefordert ServiceNow® Vulnerability Response Modul. Sie können auch eine Ausnahme mit anfordern GRC: Richtlinien- und Compliance-Management Integration.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.Manage_Exception_Configuration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Vulnerability Response Ist aktiviert, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ähnlich, wenn GRC: Richtlinien- und Compliance-Management Modul ist installiert. Sie können auswählen GRC: Richtlinien- und Compliance-Management Auf dem Konfigurationsbildschirm. Durch Aktivieren dieser Option können Sie eine Ausnahme anfordern, die das Richtlinien- und Kontrollziel von angibt GRC.

Wenn Sie einen Fragebogen hinzufügen, wird er an die Person gesendet, die die Ausnahme oder falsch positive Anforderung stellt. Sie können entweder den Standardfragebogen verwenden oder einen basierend auf Ihren Anforderungen erstellen.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für die Anforderung der Ausnahme zu verstehen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**an.
2. Wählen Sie im Formular „Konfiguration des Ausnahmemanagements“ aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option aus dem auswählen **Verwalten Sie Ausnahmen mit** Liste.
   Sie können entweder auswählen Vulnerability Response Oder GRC: Richtlinien- und Compliance-Management. Sie müssen aktivieren GRC Zu verwendendes Plugin GRC: Richtlinien- und Compliance-Management Zum anfordern einer Ausnahme. Das Ändern der Konfiguration wirkt sich nicht auf die vorhandenen Daten aus.
3. Wenn Sie ausgewählt haben Vulnerability Response Option: Geben Sie die folgenden Informationen ein:

Einstellungen für das Formular „VR-Ausnahmemanagement“

Feld	Beschreibung
Dauer	Zeitraum, für den eine Ausnahme angefordert werden kann.
Einheit	Zeiteinheit für den angegebenen Zeitraum.
Fragebogen aktivieren, um Ausnahme anzufordern	Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung.
Fragebogen, um Ausnahme anzufordern	Zeigt den von Ihnen ausgewählten Fragebogen an, um eine Ausnahme anzufordern. Die **Ausnahmefragebogen** Wird standardmäßig angezeigt. **Hinweis:** Dieses Feld wird nur angezeigt, wenn Sie auswählen **Aktivieren Sie den Fragebogen, um eine Ausnahme anzufordern** Kontrollkästchen.
Fragebogen für Ausgleichssteuerung	Zeigt den Fragebogen an, den ein Korrekturbesitzer auf Anforderungen zur Risikominderung beantworten muss. Ab v20.0 von Vulnerability Response, Sie können einen Fragebogen für Anforderungen zur Risikominderung festlegen. Die **Fragebogen Zur Ausgleichssteuerung** Ist standardmäßig ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Dieses Feld wird nur angezeigt, wenn Sie auswählen **Aktivieren Sie den Fragebogen, um eine Ausnahme anzufordern** Kontrollkästchen.
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur falsch positiven Anforderung, die ausgelöst wird.
Fragebogen, um falsch positive Meldung zu markieren	Zeigt den von Ihnen ausgewählten Fragebogen an, der als falsch positiv markiert werden soll. Der Fragebogen für falsch positive Anforderung wird standardmäßig angezeigt. **Hinweis:** Dieses Feld wird nur angezeigt, wenn **Aktivieren Sie den Fragebogen, um falsch positiv zu markieren** Das Kontrollkästchen ist aktiviert.

Wenn Sie den vorhandenen Fragebogen angepasst und ein Upgrade auf v20.0 durchgeführt haben, wird dieser anwenderdefinierte Fragebogen für die Anforderung zur Risikominderung anstatt für den Standard angezeigt **Fragebogen Zur Ausgleichssteuerung** .

4. Wenn Sie ausgewählt haben GRC: Richtlinien- und Compliance-Management Option: Geben Sie die folgenden Informationen ein:

Einstellungen für das Formular „VR-Ausnahmemanagement“

Feld	Beschreibung
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur falsch positiven Anforderung, die ausgelöst wird.
Fragebogen, um falsch positive Meldung zu markieren	Zeigt den von Ihnen ausgewählten Fragebogen an, der als falsch positiv markiert werden soll. Der Fragebogen für falsch positive Anforderung wird standardmäßig angezeigt.

5. So konfigurieren Sie Fragebogen basierend auf Bedingungen für Ausnahmen und falsch positive Anforderungen:

   a. Wählen Sie im Abschnitt Konfiguration des VR-Fragebogens die Option aus **Neu** .

   b. Füllen Sie im Formular „Fragebogenkonfiguration – neuer Datensatz“ die Felder aus, und wählen Sie aus **Übermitteln** .
   Weitere Informationen zu den Formularfeldern „Fragebogenkonfiguration“ finden Sie unter Formularfelder „Fragebogenkonfiguration“.
   Der erstellte Fragebogen wird im Abschnitt „Konfiguration des VR-Fragebogens“ des Formulars „Einstellungen für VR-Ausnahmemanagement“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie beispielsweise einen Fragebogen für falsch positive Anforderungen für kritische angreifbare Elemente konfigurieren möchten, wählen Sie aus **Falsch positiv für angreifbare Elemente** Genehmigungsregel, geben Sie die Bedingung als an Risikobewertung ist 1 – Kritisch Und wählen Sie den gewünschten Fragebogen in aus Fragebogenkonfiguration Formular.

6. Wählen Sie **Speichern**.

Fügen Sie einen Ausnahmegenehmiger hinzu

Fügen Sie den Genehmigergruppen Anwender hinzu, damit Sie eine Ausnahme anfordern können.

Vorbereitungen

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.Exception_Approver

Warum und wann dieser Vorgang ausgeführt wird

Bis Zu Vulnerability Response V14.0, ein e Die Ausnahmeanforderung für ein angreifbares Element oder eine Korrekturaufgabe wird mit dem standardmäßigen zweistufigen Genehmigungs-Workflow genehmigt. Die Anforderung muss von zwei Genehmigerebenen genehmigt werden.

Hinweis:
Bis Zu Vulnerability Response V14.0: Wenn kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Jedoch ab Vulnerability Response V15.0: Wenn Sie die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht zurück in Workflow ändern.Informationen zum Konfigurieren von Genehmigungsregeln für das Ausnahmemanagement und falsch positive Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**an.
2. Suchen Sie in der Spalte Name nach **Ausnahme** , Und klicken Sie auf **Ausnahmegenehmiger – Ebene 1**.

Hinweis:
Beginnt ab Vulnerability Response V12.8.1. Sie können die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahme oder falsch positive Anforderung über den Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** Und wählen Sie aus `sn_vul.exception_approver_L1`, `sn_vul.exception_approver_L2`, Oder `sn_vul.false_positive_approver_group`Zum Ändern des Eigenschaftswerts.

3. Klicken Sie im Formular Gruppenausnahmegenehmiger – Ebene 1 auf die zugehörige Liste Gruppenmitglieder.
4. Klicken Sie Auf **Neu** Um eine Liste zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Füllen Sie im Formular die Felder aus.

Anwenderformular

Feld	Beschreibung
Anwender-ID	Eindeutiger Bezeichner für den Benutzer
Vorname	Vorname des Anwenders.
Nachname	Nachname des Anwenders.
Titel	Berufsbezeichnung des Benutzers Geben Sie einen Titel oder eine Stellenbeschreibung ein, oder wählen Sie eine aus der Liste aus.
Abteilung	Abteilung des Anwenders.
Passwort	Passwort, das dem Anwender zugewiesen ist. Dieses Passwort kann dauerhaft oder temporär sein.
Passwort muss zurückgesetzt werden	Option, mit der der Anwender das Passwort zurücksetzen können, um die Sicherheit zu gewährleisten.
Gesperrt	Option zum Sperren des Anwenders aus der Instanz und zum Beenden aller aktiven Sitzungen des Anwenders. Das System verhindert, dass Anwender mit der Administratorrolle sich selbst sperren.
Aktiv	Option zum Aktivieren dieses Anwenders. Nur inaktive Anwender können in diesen Bereichen angezeigt werden: ○ Listen von Anwendern ○ Auswahlliste in Referenzfeldern (Lupensymbol) ○ Liste mit automatischer Vervollständigung, die angezeigt wird, wenn Sie in ein Referenzfeld eingeben
Nur Webservice-Zugang	Option, um diesen Anwender als nicht interaktiven Anwender zu bestimmen.
Interner Integrationsanwender	Option, um diesen Anwender als internen Integrationsanwender zu bestimmen.
E-Mail	E-Mail-Adresse des Anwenders.
Sprache	Bevorzugte Sprache des Anwenders.
Kalenderintegration	Kalender, der zum Verwalten des Arbeitszeitplans verwendet wird. Beispiel: Outlook.
Zeitzone	Zeitzone für den Standort dieses Anwenders.
Datumsformat	Bevorzugtes Format des Anwenders für Daten.
Telefon (geschäftlich)	Geschäftliche Telefonnummer des Anwenders.
Mobiltelefon	Mobiltelefon des Anwenders.
Foto	Foto, das Sie hochladen können, indem Sie auf klicken **Zum Hinzufügen klicken...** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Absenden**.
7. Wiederholen Sie die Schritte 1 bis 5, um einen Ausnahmedämmengenehmiger der Ebene 2 zu erstellen. Der Genehmiger muss zu navigieren **Vulnerability Response** > **Meine Genehmigungen** Und genehmigen Sie Anforderungen.

Hinweis:
Um eine Ausnahme für zu genehmigen GRC: Richtlinien- und Compliance-Management, Siehe Optionales Setup für Richtlinien- und Compliance-Management .

Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement

Beginnend mit Vulnerability Response V15.0: Verwenden Sie den Flow Designer, um Ausnahmeanforderungen für das Ausnahmemanagement, Ausnahmeregeln und die Verwaltung von falsch positiven Werten zu genehmigen. Wenn Sie bereitstellen Vulnerability Response(VR) zum ersten Mal ist der Flow Designer standardmäßig aktiviert.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie ein vorhandener VR-Anwender sind, ist die Standardoption Workflow.
Wenn Sie bereitgestellt haben Vulnerability Response V15.0 oder höher, der Wert der Systemeigenschaft *sn_vul.flow_designer_activation*lst auf „wahr“ festgelegt. Dies bedeutet, dass der Flow Designer standardmäßig aktiviert ist.

Wenn Sie bereits verwenden Vulnerability Response Vor v15.0 ist der Wert dieser Systemeigenschaft auf „falsch“ festgelegt. Sie können den Flow Designer aktivieren, indem Sie den Wert in „wahr“ ändern.

Hinweis:
Sie können den Workflow nicht mehr verwenden, nachdem Sie den Flow Designer aktiviert haben. Einen detaillierten Vergleich zwischen Workflow und Flow Designer finden Sie unter Ausnahmemanagement-Workflow vs. Flow Designer.

Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmemanagement-Workflows konfigurieren.

- Ausnahmeanforderung für Korrekturaufgaben
- Ausnahmeanforderung für angreifbare Elemente
- Ausnahmeregel
- Falsch positiv für Korrekturaufgaben
- Falsch positiv für angreifbare Elemente

Hinweis:
Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den übereinstimmenden Genehmigungs-Workflow. Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**an.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie im Formular die Felder aus.

Formular „Genehmigungsregel“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.
Tabelle	Tabelle, auf die die Regel angewendet wird.
Anwendung	Der Standardwert ist Vulnerability Response.
Regeltyp	Gibt den Regeltyp an. Zum Beispiel Ausnahmeverwaltung, falsch positiv oder Ausnahmeregel.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird.
Beschreibung	Kurzbeschreibung der Genehmigungsregeln.
Genehmigung läuft ab y (Tage) Ab v21.0 von Vulnerability Response	Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann.
Genehmiger benachrichtigen (Tage) Ab v21.0 von Vulnerability Response	Datum, nach dem der Genehmiger benachrichtigt wird, Maßnahmen zu ergreifen.

4. Wählen Sie **Aktualisieren**.
   Auf der Registerkarte „Genehmigungskonfigurationen“ sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren. Weitere Informationen finden Sie unter Erstellen Sie Konfigurationen für eine Genehmigungsregel.

Hinweis:
Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen. Weitere Informationen finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement.

Example:
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Schwachstellen definieren, die in verschiedenen Konfigurationselementen gefunden werden.

Erstellen Sie Konfigurationen für eine Genehmigungsregel

Definieren Sie die Bedingungen, um übereinstimmende angreifbare Elemente, Korrekturaufgaben oder Ausnahmeregeln für eine Genehmigungsebene herauszufiltern.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Im Modul „Genehmigungskonfigurationen“ können Sie mehrere Genehmigungsebenen für verschiedene Konfigurationen konfigurieren. Definieren Sie bedingungsbasierte Regeln, wobei jede Regel mehrere Genehmigungsebenen enthält.

Hinweis:
Verwenden Sie das Modul „Genehmigungsregeln“, um Genehmigungsregeln für die Ausnahmemanagement-Workflows zu konfigurieren. Informationen zum Konfigurieren von Genehmigungsregeln finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**an.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zu **Genehmigungskonfigurationen** Registerkarte.
3. Wählen Sie eine Konfiguration aus.
4. Füllen Sie im Formular die Felder aus.

Formular „Genehmigungskonfiguration“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel.
Reihenfolge	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Auftragseintrag von 100 vor einer Konfiguration mit einem Auftragseintrag von 200 ausgeführt.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungskonfiguration verwendet wird.
Beschreibung	Kurzbeschreibung der Genehmigungskonfigurationsebenen.

5. Legen Sie eine Bedingung für die angreifbaren Elemente oder Korrekturaufgaben auf eine der folgenden Arten fest:

Feld	Beschreibung
Bedingung	Identifiziert die übereinstimmenden angreifbaren Elemente oder Korrekturaufgaben.
Erweiterte Bedingung	Skript, das die Bedingung für die angreifbaren Elemente oder Korrekturaufgaben definiert. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie auswählen **Erweitert** Kontrollkästchen.

6. Wählen Sie **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den übereinstimmenden Genehmigungs-Workflow. Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement.

Example:
Sie können verschiedene Genehmigungspfade definieren für:

- Beispiel 1: Verschiedene Arten von Schwachstellen oder Konfigurationselementen (mit Internetzugriff oder intern).
- Beispiel 2: Zurückstellungs- und Risikoreduzierungsanforderungen, wenn ein Korrekturbesitzer diese Anforderungen gleichzeitig für angreifbare Host-Elemente (Vits) oder Korrekturaufgaben (VUL) stellt.

Die Spalte „Change-Genehmigung“ enthält die Datensätze zur Genehmigung des Zurückstellungsstatus für Change-Genehmigungen. Wenn Sie mit dem Bedingungsgenerator eine Bedingung für die Spalte „Change-Genehmigung“ festlegen, wird der Datensatz für die Zurückstellungsgenehmigung berücksichtigt, nicht jedoch der Datensatz für die Genehmigung der Risikoreduzierung. Um die Bedingung für den Datensatz zur Genehmigung des Risikoreduzierungsstatus festzulegen, verwenden Sie daher **Erweiterte Bedingung** Feld.

Für **Ausnahmeanforderung für angreifbare Elemente** Genehmigungsregel, die **Anforderung einer Risikobewertung von Mittel nach Niedrig** Die Genehmigungskonfiguration ist im Lieferumfang des Basissystems enthalten. Diese Konfiguration ist standardmäßig auf „falsch“ festgelegt. Sie können diese Konfiguration verwenden, um einen Genehmigungspfad für die Risikoreduzierungsanforderungen von Mittel nach Niedrig festzulegen. Sie können das Skript auch in dieser Konfiguration aktualisieren, sodass es für verschiedene Risikobewertungsänderungen in den Risikoreduzierungsanforderungen gilt.

Anforderung einer Risikobewertung von der Konfiguration „Mittel“ nach „Niedrig“:

```
function evaluate() {
   var gr = new GlideRecord("sn_vul_change_approval");
   gr.addQuery("sys_id", approval);
   gr.addQuery("current_value", "3 - Medium");
   gr.addQuery("desired_value", "4 - Low");
   gr.query();
   if (gr.next()) {
      return true;
   }
   return false;
}
evaluate();
```

Legen Sie die vorherige Konfiguration mit der niedrigsten Reihenfolge auf „wahr“ fest, und legen Sie den fest **Standardkonfiguration: Ausnahmeanforderung für VI** Konfiguration auf „wahr“.

Ergebnis: Wenn ein Korrekturbesitzer gleichzeitig eine Zurückstellung und eine Risikominderungsanforderung aus dem IT-Korrekturarbeitsbereich stellt, werden die Genehmigungsanforderungen für die Zurückstellung an die in definierten Genehmiger weitergeleitet **Standardkonfiguration: Ausnahmeanforderung für VI** Und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Genehmigungsanforderungen zur Risikominderung werden an die in definierten Genehmiger weitergeleitet **Anforderung einer Risikobewertung von Mittel nach Niedrig** Konfiguration.

Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement

Definieren Sie die Ebenen der Anwender und Anwendergruppen, die die Ausnahmeanforderungen genehmigen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**an.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zu **Genehmigungskonfigurationen** Registerkarte.
3. Wählen Sie eine Konfiguration aus.
4. Wählen Sie im Abschnitt Genehmigerebenen eine Genehmigerebene aus.
5. Füllen Sie im Formular die Felder aus.

Formular auf Genehmigerebene

Feld	Beschreibung
Name	Name der Genehmigungsebene.
Erforderliche Genehmigung	Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind: ○ Ein Genehmiger erforderlich ○ Alle Anwender müssen genehmigen
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird.
Reihenfolge	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Auftragseintrag von 100 vor einer Konfiguration mit einem Auftragseintrag von 200 ausgeführt.
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel.
Genehmigungskonfiguration	Enthält die Genehmigungskonfigurationen.
Zuweisen mit	Wählen Sie eine Option aus: ○ Anwender und Anwendergruppe ○ Genehmigungstabellenfeld ○ Skript
Gruppen	Genehmigerebenengruppe, die aus mehreren Anwendern besteht. Der Anwender muss über eine der folgenden Rollen verfügen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ sn_vul.Exception_Approver: Für Ausnahmeverwaltung und Ausnahmeregeln ○ sn_vul.false_positive_Approver: Für falsch positiv
Anwender	Bearbeiten Sie die in den Gruppen aufgeführten Anwender.

6. Wählen Sie aus, um die Änderungen zu speichern **Aktualisieren** .

Hinweis:
Vor v15.0 ist der Workflow-Prozess funktionsfähig, wenn Anwender nur in Ausnahmebene 1 vorhanden sind. Ab v15.0 muss jedoch mindestens ein Anwender auf jeder Ebene vorhanden sein.

Vor v15.0 wurde im Workflow das Schwachstellenelement oder die angreifbare Gruppe zurückgestellt, wenn es auf der zweiten Ebene keinen Anwender gab. Ab v15.0 wird die Genehmigungsanforderung jedoch automatisch abgelehnt, wenn auf der zweiten Ebene kein Anwender vorhanden ist.

Example:
Es kann verschiedene Genehmigungsebenen für Schwachstellen für Linux- und Windows-Server geben.

Ausnahmemanagement-Workflow vs. Flow Designer

Beginnend mit Vulnerability Response V15.0, wenn Sie bereitstellen Vulnerability Response(VR) zum ersten Mal ist der Flow Designer für die Genehmigung von Ausnahmeanforderungen im Ausnahmemanagement standardmäßig aktiviert. Wenn Sie ein vorhandener VR-Anwender sind, ist die Standardoption Workflow.

Hinweis:
Beginnend mit Vulnerability Response V19.0, nur Flow Designer wird für neue Kunden unterstützt. Wenn Sie ein vorhandener Anwender sind und ein Upgrade auf durchführen Vulnerability Response V19.0, dann werden sowohl Flow Designer als auch Ausnahmemanagement-Workflow unterstützt.

Workflow versus Flow Designer

Überlegungen	Workflow	Flow Designer
Version	Vor v15.0 von Vulnerability Response.	Ab v15.0 von Vulnerability Response.
Standardoption	Standardoption, wenn Sie ein vorhandener VR-Anwender sind.	Standardoption für neue VR-Anwender ab v15.0.
Festlegen des Genehmigungsprozesses	Das Ausnahmemanagement umfasst Ausnahmen und falsch positive Anforderungen zusammen mit Ausnahmeregeln.	Umfasst das Definieren verschiedener Ebenen und das Hinzufügen verschiedener Genehmiger für verschiedene Anwendungsfälle. Einfacher zu implementieren als der Workflow. Das Ausnahmemanagement umfasst Ausnahmen und falsch positive Anforderungen zusammen mit Ausnahmeregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow versus Flow Designer (Fortsetzung)

Überlegungen	Workflow	Flow Designer
Upgrade auf Flow Designer	Sie können ein Upgrade auf Flow Designer über den Workflow durchführen. Vorhandene Anforderungen können jedoch nur mit dem Workflow genehmigt werden.	Flow Designer ist standardmäßig aktiviert.
Systemeigenschaft *sn_vul.flow_designer_activation*	Wenn Sie den Workflow für das Annahmemanagement vor v15.0 verwendet haben, wird die Systemeigenschaft auf „falsch“ festgelegt. Um den Flow Designer zu aktivieren, legen Sie diese Eigenschaft auf „wahr“ fest. **Hinweis:** Sie können den Workflow nicht mehr verwenden, nachdem Sie den Flow Designer aktiviert haben.	Wenn Sie VR zum ersten Mal für v15.0 oder höher verwenden, wird der Systemeigenschaftswert standardmäßig auf „wahr“ festgelegt.
Genehmigungsregelmodul	Nachdem Sie die Systemeigenschaft auf „wahr“ festgelegt haben, wird der **Aktivieren Sie Modulgenehmigungsregeln** Die geplante Aufgabe wird innerhalb von 24 Stunden ausgeführt. Mit dieser geplanten Aufgabe wird aktiviert **Genehmigungsregeln** Modul. Um dieses Modul sofort zu aktivieren, führen Sie diesen Auftrag manuell aus.	Wenn Sie VR zum ersten Mal aus VR v15.0 bereitgestellt haben, ist dieses Modul standardmäßig verfügbar.
Genehmigungsstufen	Bietet die Option, nur zwei Ebenen von Genehmigern festzulegen.	Bietet mehrere Optionen, z. B. das Festlegen einer beliebigen Anzahl von Konfigurationen, Genehmigerebenen und das dynamische Hinzufügen von Genehmigern für jede Regel.

Fügen Sie einen falsch positiven Genehmiger hinzu

Nur Anwender, die der Gruppe „falsch positive Genehmiger“ hinzugefügt wurden, können falsch positive Ergebnisse für angreifbare Elemente (VIS) und Korrekturaufgaben (VULs) genehmigen. Die Gewährung eines falsch positiven Werts ist ein einstufiger Genehmigungsprozess.

Vorbereitungen

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Hinweis:

Wenn Sie ab Vulnerability Response v15.0 die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht zurück in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für das Ausnahmemanagement und falsch positive Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > > **Anwenderadministration** > **Gruppen**an.
2. In **Name** Spalte, suchen Sie nach **Falsch Positiv** Und klicken Sie auf die Option.
3. Navigieren Sie im Gruppenformular zu **Gruppenmitglieder** > **Neu** (Oder **Bearbeiten**).
4. Erstellen Sie im Anwenderformular einen Datensatz, indem Sie die Anwenderdetails eingeben, und klicken Sie auf **Übermitteln** .
   Alle Rollen werden dem Anwender gewährt. Die ausgewählten Anwender werden der Liste Gruppenmitglieder hinzugefügt. Diese Mitglieder können Anforderungen zum Markieren von VIS oder Korrekturaufgaben als falsch positiv genehmigen. Nach der Genehmigung wird der Status des Datensatzes in „Geschlossen“ aktualisiert und erst am angegebenen Datum erneut geöffnet.

Konfigurieren Sie den Fragebogen für die Risikominderung

Beginnend mit Vulnerability Response V20.0 können Sie den Fragebogen der Risikoreduzierungsanforderung für eine Reihe gefilterter angreifbarer Elemente oder Korrekturaufgaben anpassen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die **Fragebogen für Ausgleichssteuerungen für angreifbare Elemente** Und **Fragebogen für Ausgleichssteuerungen für angreifbare Gruppen** Genehmigungsregeln werden mit dem Basissystem geliefert.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**an.
2. Aktivieren Sie im Formular „Einstellungen für VR-Ausnahmemanagement“ das Kontrollkästchen Fragebogen zum anfordern einer Ausnahme aktivieren.
3. So konfigurieren Sie Fragebogen basierend auf Bedingungen für Risikoreduzierungsanforderungen:
   a. Wählen Sie im Abschnitt Konfiguration des VR-Fragebogens die Option aus **Neu** .
   b. Wählen Sie im Formular „Fragebogenkonfiguration – neuer Datensatz“ die aus **Fragebogen für Ausgleichssteuerungen für angreifbare Gruppen** Oder **Fragebogen für**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgleichssteuerungen für angreifbare Elemente Genehmigungsregel und geben Sie die Bedingung an.

c. Wählen Sie den gewünschten Fragebogen aus, und wählen Sie aus **Übermitteln** .
Weitere Informationen zu den Formularfeldern „Fragebogenkonfiguration“ finden Sie unter Formularfelder „Fragebogenkonfiguration“.
Der erstellte Fragebogen wird im Abschnitt „Konfiguration des VR-Fragebogens“ des Formulars „Einstellungen für VR-Ausnahmemanagement“ angezeigt.

4. Wählen Sie Aus **Speichern** Im Formular „Einstellungen für VR-Ausnahmemanagement“.

Zeigen Sie Vulnerability Response-SLAs für Korrekturaufgaben an

Um sicherzustellen, dass angreifbare Elemente korrekt verarbeitet werden, können Sie eine Servicelevel-Vereinbarung (SLA) für definieren Vulnerability Response Korrekturaufgaben.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird
Die SLA-Definitionen in dieser Liste sind eine Teilmenge der Plattform-SLA-Liste, spezifisch für Vulnerability Response.

Detaillierte Anweisungen hierzu finden Sie unter Create an SLA definition .

Wenn Sie die Zeit nachverfolgen, die zur Korrektur von VIS benötigt wird, ziehen Sie es möglicherweise vor, zu verwenden Vulnerability Response Korrekturzielregeln. Korrekturzielregeln definieren die erwarteten Zeitrahmen für die Korrektur angreifbarer Elemente (VI) speziell im Kontext von Vulnerability Response, während SLAs möglicherweise einen Zeitrahmen für die Behebung der Schwachstelle selbst bieten.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **SLA-Definitionen**an.
2. Klicken Sie auf eine Definition.
Aufgaben-SLAs Werden in den zugehörigen Listen von angezeigt **Korrekturaufgaben** .

Konfigurieren Sie Watchdog

Verwenden Sie die Watchdog-Konfigurationsseite, um neue Watchdogs zu erstellen oder vorhandene Watchdogs mit Bedingungen zu aktualisieren, die Sie angeben möchten. Sie können die Benachrichtigung für jeden Watchdog aktivieren und benachrichtigt werden, wenn die Bedingungen erfüllt sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_cmn.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **WatchDog** > **Konfiguration**an.
2. Wählen Sie den Watchdog aus, den Sie implementieren möchten.
3. Füllen Sie im Formular die Felder aus.

Watchdog-Integrationsformular

Feld	Beschreibung
Name	Name des Watchdogs.
Aktiv	Setzen Sie das Kontrollkästchen auf `true`Zum Aktivieren des Watchdog.
Bedingungstyp	Wählen Sie „Filter“ oder „Skript“ aus.
Erweiterte Bedingung	Dieses Feld wird nur angezeigt, wenn „Skript“ aus dem Bedingungstyp ausgewählt ist.
Tabelle	Wählen Sie die Tabelle aus, um die Watchdog-Bedingung auszuführen.
Bedingung	Bedingung zum Auswerten des Watchdog.
Benachrichtigen	Kontrollkästchen, um die Gruppen oder Anwender zu benachrichtigen, wenn die Watchdog-Bedingung erfüllt ist.
Anwender	Liste der Anwender, die informiert werden sollen, wenn die Watchdog-Bedingung erfüllt ist.
Gruppen	Gruppe, die informiert werden soll, wenn die Watchdog-Bedingung erfüllt ist.
Überwachungsprotokoll	
Watchdog	Verweis auf die Watchdog-Tabelle.
Anzahl	Anzahl der Datensätze, die die Watchdog-Kriterien erfüllen.
Notizen	Zusätzliche Hinweise für die Watchdog-Protokolle.

4. Wählen Sie **Aktualisieren**.

Konfigurieren Sie die maximale Anzahl von Zeilen in der zugehörigen Liste

Steuern Sie die Anzahl der Zeilen, die in zugehörigen Listen angezeigt werden, um die Ladezeit zu verkürzen und die Lesbarkeit und Leistung für Vulnerability Response (VR), Configuration Compliance (CC), Cloud Vulnerability Response (CVR) und Application Vulnerability Response (AVR) zu verbessern. In den zugehörigen Listen werden zugehörige Datensätze angezeigt, z. B. betroffene CIs, Ergebnisse oder Korrekturaufgaben, sodass Sie schnell auf relevante Details zugreifen können, ohne das Formular zu verlassen.

Vorbereitungen

Erforderliche Rolle: sn_vul_cmn.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **sys_properties.LIST**an.
2. Suchen und öffnen Sie die Eigenschaft: *sn_vul_cmn.related_list.set_max_row*
3. Geben Sie im Feld Wert einen der folgenden Werte ein:
   - Positive Ganzzahl: Zeigt diese Anzahl von Zeilen in jeder zugehörigen Liste an.
   - Negative Ganzzahl: Ungültige Eingabe oder ungültiger Wert wird ignoriert.
   - Leer (kein Wert): Zeigt alle Zeilen an.

   Hinweis:
   Das Anzeigen von mehr als 100 Zeilen wirkt sich auf die Leistung aus.
4. Wählen Sie Aus **Aktualisieren** Zum Anwenden der Änderungen.

Ergebnisse

Nachdem Sie die Systemeigenschaft aktualisiert haben, spiegeln die folgenden zugehörigen Listen das konfigurierte Zeilenlimit wider:

In der klassischen UI

- Betroffene CIs
- Bildergebnisse
- Potenziell doppelte Elemente
- Potenzielle Lösungen
- Bevorzugte Lösungen
- Korrekturaufgaben
- Angreifbare Elemente

In der Arbeitsbereich-UI

- Potenzielle Lösungen
- Betroffene CIs
- Betroffene Anwendungen
- Betroffene Docker-Images

Erweitert Vulnerability Response Konfigurationsaufgaben

Die folgenden Setup-Aufgaben erfordern Codierung oder erweitert ServiceNow Fachwissen und werden nicht als Teil der Basiskonfiguration betrachtet.

Sie ziehen es möglicherweise vor, diese Aufgaben nur auszuführen, wenn Sie über erweiterte Codierungserfahrung verfügen oder über Fachkenntnisse in verfügen ServiceNow AI Platform.

Erstellen Sie domänengetrennte Importe für eine Integration

Wenn Sie möchten, dass sich importierte Daten in einer bestimmten Domäne befinden, muss der Anwender, der der Ausführung der Integrationen zugewiesen ist, dieser Domäne angehören.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:
Import_admin und die Rolle „Integration konfigurieren“ für Ihre spezifische Integration, z. B. sn_vul.configure_r7_Integration oder sn_vul_Tenable.configure_Integration.

Warum und wann dieser Vorgang ausgeführt wird

Dieser Satz von Aufgaben erfordert Codierung oder erweitert ServiceNow Fachwissen.

Die Importwarteschlangen enthalten Datenanhänge, die die geplanten Aufgaben (Integrationen) verarbeiten. In einer domänengetrennten Umgebung müssen Sie die geplante Aufgabe mit der richtigen Importwarteschlange abgleichen.

Prozedur

1. Erstellen Sie eine Domäne.
2. Erstellen Sie für jede von Ihnen erstellte Domäne einen Anwender, und weisen Sie den Anwender dieser Domäne zu.

   Stellen Sie sich diesen Anwender als einen vor **Run_as** Platzhalter für die Domäne in Ihrer Schwachstellenintegration. Dies entspricht dem **VR.System** Anwender in der globalen Domäne. Dieser Anwender benötigt Zugriff auf Datenquellen, Transformationszuordnungen und Schwachstellendaten.

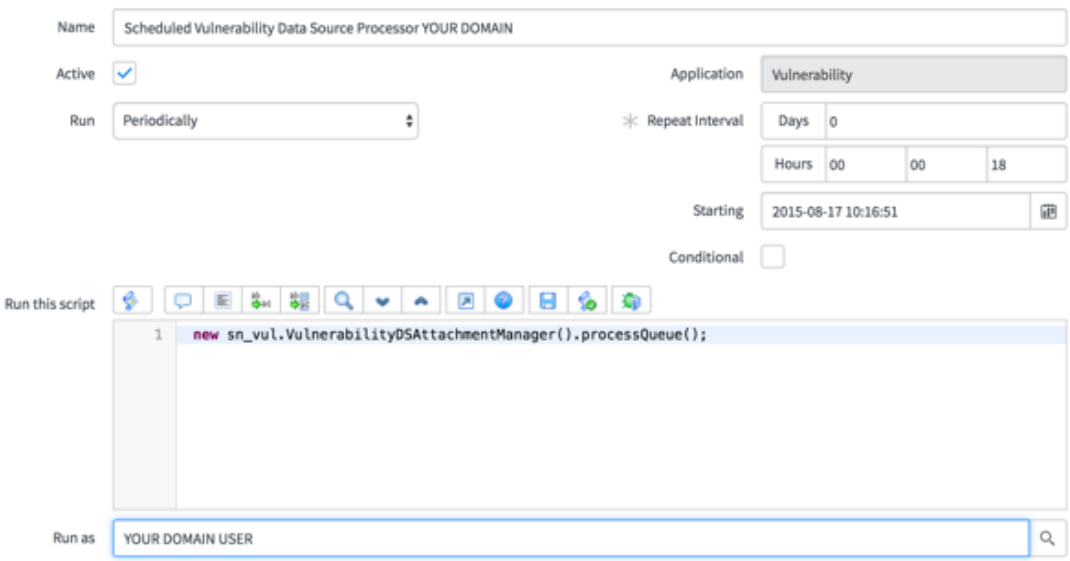
   Hinweis:
   Verwenden Sie diesen Anwender nicht für andere Zwecke.

3. Erstellen Eine geplante Aufgabe in jeder Domäne.
   Weitere Informationen zu zusätzlichen Vorsichtsmaßnahmen und Einstellungen finden Sie unter Zusätzliche Einstellungen für Domänentrennung.

   a. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**an.

   b. Kopieren **Geplanter Datenquellenprozessor Für Schwachstellen** In der Domäne.

   c. Um die geplante Aufgabe zu identifizieren, hängen Sie die Domäne an den Namen an.



   d. In **Ausführen als** Feld ändern **Run_as** Anwender an den Anwender, den Sie in Schritt 2 erstellt haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab v20.1 von Vulnerability Response, Die folgenden Skriptänderungen werden mit dem Basissystem geliefert.

4. **Hinweis:**
   Bearbeiten Sie die folgende UI-Aktion, damit die Integration in ausgeführt wird **Run_as** Anwenderdomäne.

   Bearbeiten Sie **Jetzt Ausführen** UI-Aktion in **Qualys-Host-Erkennungsintegration** Integrationsauftrag Um diesen Codeblock oben in der Datei hinzuzufügen.

   Example

```
//sys id below is of host detection integration
if(current.sys_id == "5d9cf0daff540300c68c9f783894fa4d"){
current.run_as = gs.getUserID
();
}
```

5. **Hinweis:**
   Bearbeiten Sie die folgenden Skripteinbindungen, damit die Integration in ausgeführt wird **Run_as** Anwenderdomäne.

   Bearbeiten Sie **SchwachstellenIntegrationUtils** Skripteinbindungsmethode **AddIntegrationAusführen** Um den hervorgehobenen Code hinzuzufügen

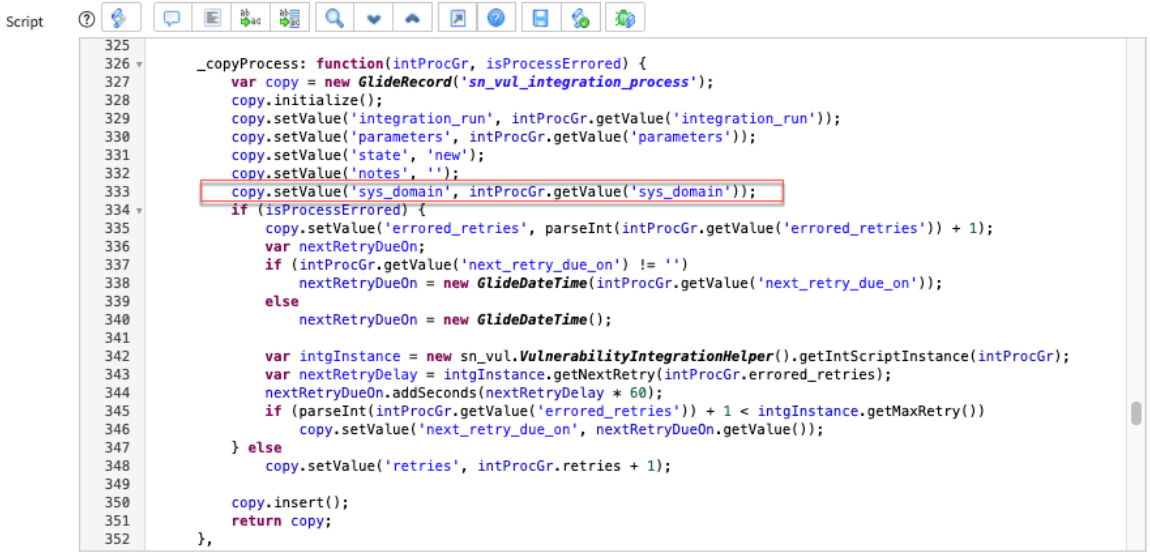
```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

6. Bearbeiten Sie **SchwachstellenIntegrationUtils** Skripteinbindungsmethode, **AddProcessRun** Um den hervorgehobenen Code hinzuzufügen In der folgenden Abbildung .
   AddProcessRun-Code

```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

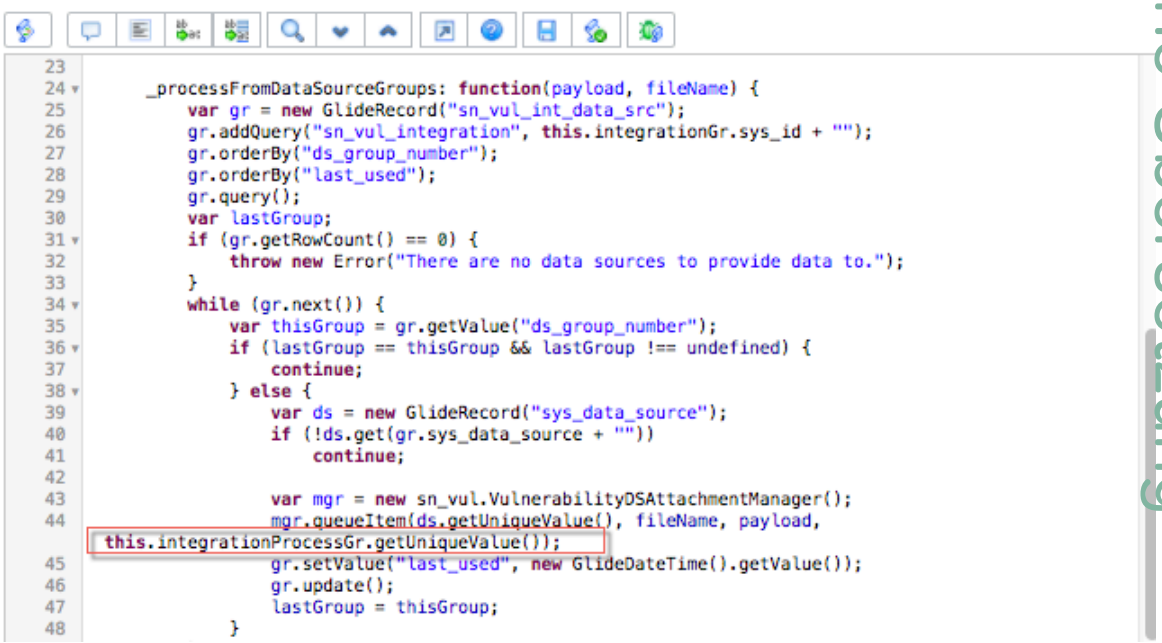

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Bearbeiten Sie **SchwachstellenIntegrationUtils** Skripteinbindungsmethode, **CopyProcess** Um den hervorgehobenen Code in der folgenden Abbildung hinzuzufügen.
   CopyProcess-Code



```
Script
325
326     _copyProcess: function(intProcGr, isProcessErrored) {
327         var copy = new GlideRecord('sn_vul_integration_process');
328         copy.initialize();
329         copy.setValue('integration_run', intProcGr.getValue('integration_run'));
330         copy.setValue('parameters', intProcGr.getValue('parameters'));
331         copy.setValue('state', 'new');
332         copy.setValue('notes', '');
333         copy.setValue('sys_domain', intProcGr.getValue('sys_domain'));
334         if (isProcessErrored) {
335             copy.setValue('errored_retries', parseInt(intProcGr.getValue('errored_retries')) + 1);
336             var nextRetryDueOn;
337             if (intProcGr.getValue('next_retry_due_on') != '')
338                 nextRetryDueOn = new GlideDateTime(intProcGr.getValue('next_retry_due_on'));
339             else
340                 nextRetryDueOn = new GlideDateTime();
341
342             var intgInstance = new sn_vul.VulnerabilityIntegrationHelper().getIntScriptInstance(intProcGr);
343             var nextRetryDelay = intgInstance.getNextRetry(intProcGr.errored_retries);
344             nextRetryDueOn.addSeconds(nextRetryDelay * 60);
345             if (parseInt(intProcGr.getValue('errored_retries')) + 1 < intgInstance.getMaxRetry())
346                 copy.setValue('next_retry_due_on', nextRetryDueOn.getValue());
347         } else
348             copy.setValue('retries', intProcGr.retries + 1);
349
350         copy.insert();
351         return copy;
352     },
```

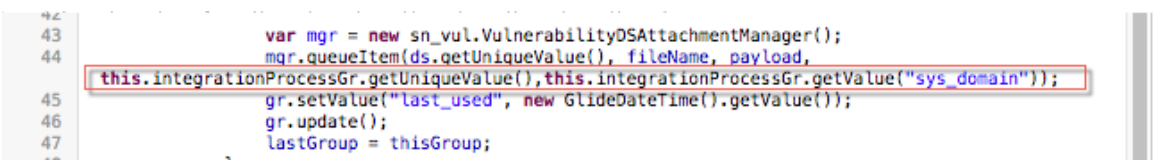
8. Bearbeiten Sie **DataSourceVulnReportRefreshProcessor** Skripteinbindungsmethode **_ProcessFromDataSourceGroups** So ändern Sie diesen ursprünglichen Code:
   Ursprünglicher _processFromDataSourcesGroups-Code



```
23
24      _processFromDataSourceGroups: function(payload, fileName) {
25          var gr = new GlideRecord("sn_vul_int_data_src");
26          gr.addQuery("sn_vul_integration", this.integrationGr.sys_id + "");
27          gr.orderBy("ds_group_number");
28          gr.orderBy("last_used");
29          gr.query();
30          var lastGroup;
31          if (gr.getRowCount() == 0) {
32              throw new Error("There are no data sources to provide data to.");
33          }
34          while (gr.next()) {
35              var thisGroup = gr.getValue("ds_group_number");
36              if (lastGroup == thisGroup && lastGroup !== undefined) {
37                  continue;
38              } else {
39                  var ds = new GlideRecord("sys_data_source");
40                  if (!ds.get(gr.sys_data_source + ""))
41                      continue;
42
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue());
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
48              }
```

An:

_ProcessFromDataSourcesGroups-Code wurde bearbeitet



```
43                  var mgr = new sn_vul.VulnerabilityDSAttachmentManager();
44                  mgr.queueItem(ds.getUniqueValue(), fileName, payload,
    this.integrationProcessGr.getUniqueValue(),this.integrationProcessGr.getValue("sys_domain"));
45                  gr.setValue("last_used", new GlideDateTime().getValue());
46                  gr.update();
47                  lastGroup = thisGroup;
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Bearbeiten Sie **SchwachstellenDSAttachmentManager** Skripteinbindungsmethode, **Warteschlangenelement** Um die folgenden hervorgehobenen Codeblöcke hinzuzufügen Warteschlangenelement

```
queueItem: function(dataSource, attachmentName, reportData, optIntegrationProcess,optDomain) {
    var gr = new GlideRecord(this._QUEUE_TABLE);
    gr.initialize();
    gr.setValue("status", "NEW");
    gr.setValue("data_source", dataSource);
    if (optIntegrationProcess)
        gr.setValue("integration_process", optIntegrationProcess);
    if(optDomain){
            gr.setValue("sys_domain", optDomain);
    }
    var sysId = gr.insert();
```

_GetNext

```
_getNext: function() {
    // First go through the retries, if any
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    var sysDomainUser = gUser.getValue("sys_domain");
    var gr = new GlideRecord(this._QUEUE_TABLE);
    gr.addQuery("status", "RETRY");
    gr.addQuery("sys_domain", sysDomainUser);
    gr.orderBy("queued_on");
    gr.query();
    if (gr.next()) {
        return gr;
    }

    // Then handle the regular queued items
    gr = new GlideRecord(this._QUEUE_TABLE);
    gr.addQuery("status", "QUEUED");
    gr.orderBy("queued_on");
    gr.addQuery("sys_domain", sysDomainUser);
    gr.query();
    if (gr.next()) {
        return gr;
    }
```

Funktion _processQueueEntry

```
_processQueueEntry: function(entry) {
    var schedGrId = this._getScheduledImportSet(entry.data_source);
    if (gs.nil(schedGrId)) {
        return;
    }

    var dataSourceGr = new GlideRecord("sys_data_source");
    if (!dataSourceGr.get(entry.data_source)) {
        gs.warn("Non existent data source - marking as complete");
        entry.setValue("status", "COMPLETE");
        entry.setValue("processing_notes", "Data source does not exist, could not process.");
        entry.update();
        return;
    }

    try {
        this._deleteDataSourceAttachments(entry.data_source);
        if (!this._verifyDataSourceAttachmentsDeleted(entry.data_source)) {
            gs.error("VulnerabilityDSAttachmentManager._processQueueEntry: Attachments not deleted for queue entry " + entry.sys_id);
            throw "Attachments not deleted";
        }
        var attachmentApi = new GlideSysAttachment();
        attachmentApi.copy(this._QUEUE_TABLE, entry.sys_id + "", this._DATA_SOURCE, dataSourceGr.sys_id + "");
        var schedGr = new GlideRecord("scheduled_import_set");
        schedGr.get(schedGrId);
        schedGr.setValue("data_source", entry.data_source);
        schedGr.setValue("run_as", gs.getUserID());
        schedGr.update();
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jetzt sind Sie bereit für domänengetrennte Importe.

Hinweis:
Wenn Sie mehrere Bereitstellungen von haben Vulnerability Response Oder Application Vulnerability Response Integration: Wiederholen Sie diesen Prozess für jede Bereitstellung.

Erstellen und unterstützen Sie mehrere Domänen im Framework für Hintergrundaufträge

Hintergrundaufträge in Vulnerability Response-Produkten sind so konzipiert, dass sie über lange Zeiträume ausgeführt werden, um mehrere Prozesse für Ihre Datensätze auszuführen. Die Hintergrundauftragsprozessoren werden mit dem Basissystem geliefert, das über den Systemanwender ausgeführt wird und Datensätze in der globalen Domäne erstellt.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Domänenadministrator** > **Domänen**an.
2. Erstellen Sie eine Domäne.

   Weitere Informationen zum Erstellen einer Domäne finden Sie unter Create a domain .

   Erstellen Sie für jede erstellte Domäne einen Anwender, und weisen Sie den Anwender der Domäne zu. Angenommen, dieser Anwender ist ein Run_as-Platzhalter für die Domäne. Dies entspricht dem VR.System-Anwender in der globalen Domäne. Dieser Anwender benötigt Zugriff auf Schwachstellendaten.

3. Ändern Sie Run_as der geplanten Aufgaben `Scheduled Background Job Manager`, Und `Close the parent background job`.

   Wenn Sie mehrere Domänen erstellt haben, duplizieren Sie diesen Auftrag, und ändern Sie den Run_as-Anwender entsprechend. Möglicherweise möchten Sie auch eine Kopie der vorangehenden Aufträge mit dem Run_as-Anwender der globalen Domäne behalten In einem inaktiven Modus.

   Zehn Prozessoraufträge (z. B. `Background job processor 10`) Werden mit dem Basissystem geliefert. Ändern Sie die Ausführung ab dieser Aufträge in den domänengetrennten Anwender. Wenn mehrere Domänen vorhanden sind, sind zwei Aufträge pro Domäne ausreichend, diese Aufträge können jedoch bei Bedarf auch dupliziert werden. Behalten Sie zwei Prozessoraufträge mit dem Anwender „Run_as“ in der globalen Domäne bei.

   Ab v20.0 von Vulnerability Response, Die folgenden Skriptänderungen werden mit dem Basissystem geliefert.

4. Ändern Sie die Skripteinbindung `BackgroundJobManager`, Und fügen Sie die folgende Zeile hinzu, wie in der folgenden Abbildung gezeigt.

```
gr.addEncodedQuery("scheduled_job.run_as.sys_domain=" + jobGr.sys_domain + "");
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Löst die erneute Anwendung von Regeln aus der richtigen Domäne bei Bedarf aus.

Erstellen Sie eine Vulnerability Response-CI-Suchregel

Die **CI-Suchregeln** Das Modul enthält Regeln, die verwendet werden, um den übereinstimmenden Datensatz für Hostinformationen zu finden, die während des Imports von Schwachstellen von Drittparteien empfangen werden. Die Hostinformationen werden mit den erkannten Elementen, nicht abgeglichenen Konfigurationselementklassen und abgeglichen Configuration Management Database (CMDB).

Vorbereitungen

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Das Erstellen von CI-Suchregeln erfordert erweiterte Funktionen ServiceNow Und Vulnerability Response Fachwissen. Anstatt eines der vorhandenen zu ändern Suchen Regeln. Erwägen Sie, sie zu kopieren und die Kopie zu ändern. Wenn Sie zufrieden sind, dass die neue Regel das tut, was Sie möchten, deaktivieren Sie die ursprüngliche.

Hinweis:
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **CI-Suchregeln**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „CI-Suchregel“

Feld	Beschreibung
Name	Name der Regel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

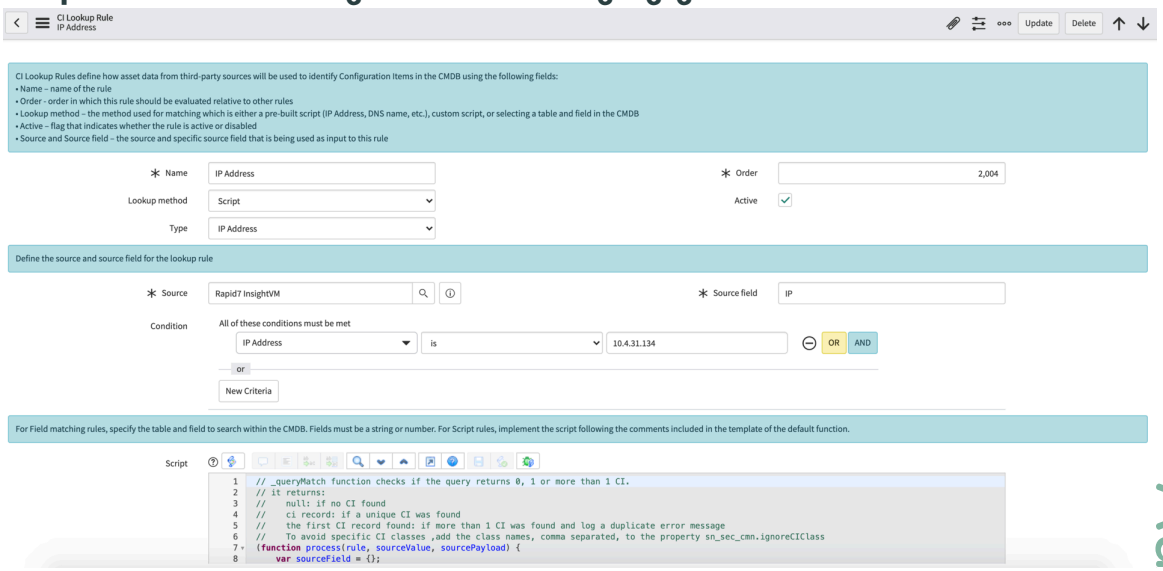
Feld	Beschreibung
Suchmethode	Für den Abgleich verwendete Methode. Die Auswahlmöglichkeiten lauten wie folgt: ○ **Skript** : Vorgefertigtes Skript (IP-Adresse, DNS-Name usw.) oder anwenderdefiniertes Skript. ○ **Feldübereinstimmung** : Suche nach Tabelle oder Feld in der CMDB.
Typ	Mit dem Skript verwendeter Typ **Suchmethode** .
Reihenfolge	Rangfolge für die Regel. Regeln Mit der niedrigsten Reihenfolge werden zuerst ausgewertet.
Aktiv	Kontrollkästchen, um anzugeben, ob die Regel aktiv oder deaktiviert ist.
Quelle	Quelle, die als Eingabe für diese Regel verwendet wird.
Quellenfeld	Quellfeld, das als Eingabe für diese Regel verwendet wird. Wählen Sie ein beliebiges Feld aus, es wird jedoch als behandelt Zeichenfolgenwert.
Bedingung	Bedingung, auf der die CI-Suchregel angewendet wird. Diese Bedingung hängt vom Attribut des Drittanbieterscanners ab. **Hinweis:** Das Asset-Attribut ist Teil der Nutzlast. Sie wird vom Scanner der Drittpartei empfangen. Nutzlastbeispiele finden Sie in der Tabelle „erkannte Elemente“.
Skript	Bearbeitbares Beispielskript, basierend auf **Typ** , Wird angezeigt. Implementieren Sie das anwenderdefinierte Skript gemäß den Kommentaren, die in der Vorlage der Standardfunktion enthalten sind. **Hinweis:** Die Prozessfunktion hat drei Parameter: `rule`, `sourceValue`, Und `sourcePayload`
Tabelle durchsuchen	Tabelle, die in der CMDB gesucht werden soll. Wird mit Feldübereinstimmung verwendet **Suchmethode** .
Feld durchsuchen	Feld, das Informationen enthält, die zum Auffinden eines CI verwendet werden können. Wird mit der Feldübereinstimmung verwendet **Suchmethode** . Dieses Feld kann sich im CI-Datensatz oder in einem zugehörigen Datensatz wie einem Netzwerkadapter befinden.

4. Klicken Sie auf **Absenden**.

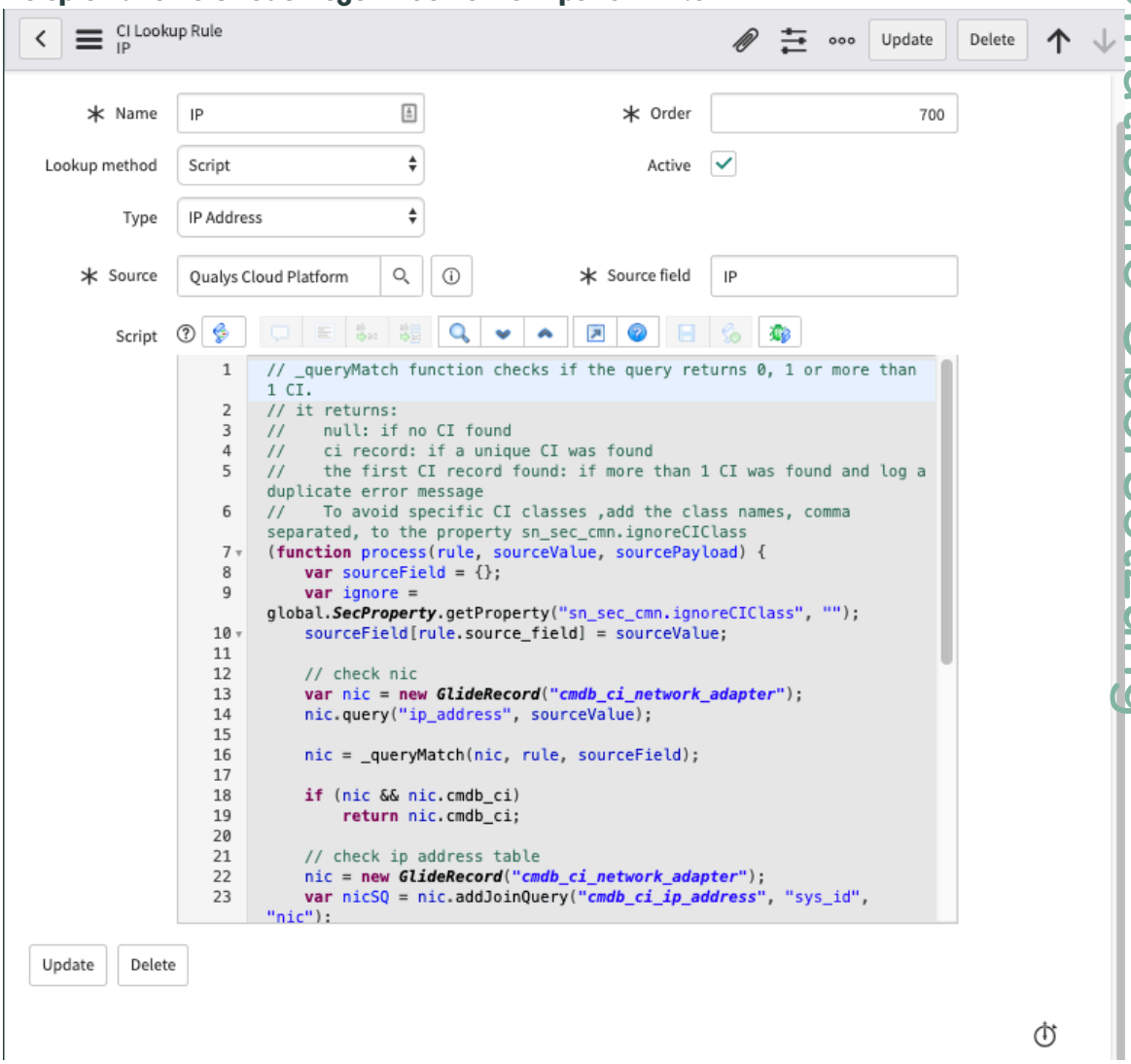
Weitere Informationen zur Implementierung von CI-Suchregeln finden Sie unter . Schritte zur Verhinderung doppelter oder verwaister Datensätze nach der Ausführung Vulnerability Response CI-Suchregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine CI-Suchregel mit einem Bedingungsgenerator für V12.0



Beispiel für eine CI-Suchregel mit einem Skript Vor V12.0



Automatische Übersetzung

Zugehörige Informationen

Vulnerability Response Formularfelder für angreifbare Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ignorieren Sie CI-Klassen

Um einige Konfigurationselementklassen (Configuration Item, CI) zu ignorieren, z. B. Lastenausgleichsmodul [cmdb_ci_lb], legen Sie bei der Ausführung von CI-Suchregeln fest **IgnorierCIClass** [*sn_sec_cmn.ignoreCIClass*] Systemeigenschaft.

Vorbereitungen

Erforderliche Rolle: Administrator

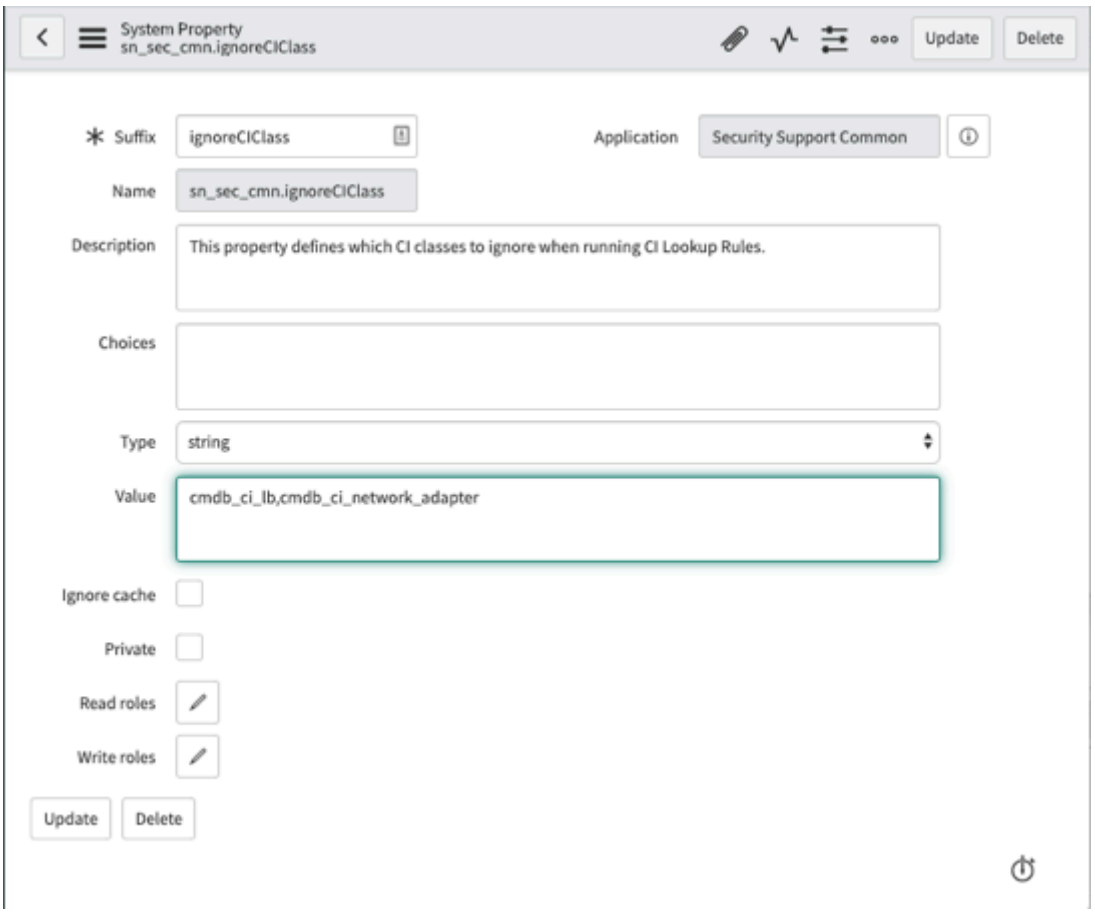
Hinweis:

Die **IgnorierCIClass** Systemeigenschaft ist ab verfügbar Vulnerability Response V9.0, die Eigenschaftsfunktionalität ist jedoch nach einem Upgrade von einer vorherigen Version nicht verfügbar.

Wenn Sie ein Upgrade von einem durchgeführt haben Security Operations Anwendung, vor Version 9,0, siehe KB0788209 Anweisungen zum Aktivieren dieser Funktionalität.

Prozedur

1. Geben Sie Ein `sys_properties.list` In der linken Navigationsleiste.
2. Klicken Sie auf **Eingeben**.
3. In **Suchen** Menü, unter **Name** Geben Sie ein `sn_sec_cmn.ignoreCIClass` .
4. In **Wert** Textfeld: Geben Sie die auszuschließenden CI-Klassen in eine kommagetrennte Liste ein.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Aktualisieren**.
   Diese Liste wird während des nächsten Imports von CI-Suchregeln verwendet. Angreifbare Elemente, die während des Imports erstellt wurden, sind keinem CI des Typs zugeordnet, der in aufgeführt ist **Wert** Feld von sn_sec_cmn.ignoreCIClass Systemeigenschaft.

Filtern Sie außer Betrieb genommene CIs

Filtern Sie außer Betrieb genommene Konfigurationselemente (CIs), während die CI-Suchregeln ausgeführt werden. Um stillgelegte CIs beim Ausführen der Sicherheitsvorgänge-CMDB-CI-Suchregeln zu filtern, legen Sie fest **Filtert heraus dekommissioniertCI** [**sn_sec_cmn.filterAusdekommissionedCI**] Systemeigenschaft auf „wahr“.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Der Standardwert der Systemeigenschaft ist „wahr“. Diese Eigenschaft gilt nur für CI-Suchregeln in Vulnerability Response Und hat keine Auswirkungen auf die Ire-Suchlogik.

Prozedur

1. Geben Sie Ein sys_properties.list In der linken Navigationsleiste.
2. Wählen Sie Aus **Geben Sie Ein** .
3. In **Suchen** Menü, unter **Name** Geben Sie ein sn_sec_cmn.filterAusdekommissionedCI Zum Filtern der stillgelegten CIs.
4. In **Wert** Textfeld: Geben Sie den Wert „wahr“ oder „falsch“ ein.
   Der Standardwert ist „true“.
5. Wählen Sie **Aktualisieren**.
   Dieser Wert wird von CI-Suchregeln während des nächsten Imports verwendet. Die sn_sec_cmn.filterAusdekommissionedCI Die Systemeigenschaft filtert CIs heraus, die die unten aufgeführten Bedingungen erfüllen, während die Suchregeln ausgeführt werden.

```
_isCIDecommissioned: function(gr, filterDecommissionCi) {
      var install_status = false;
      var life_cycle_stage_status = false;
      // check for property
      if (filterDecommissionCi == "true") {
         if (gr.isValidField("install_status"))
            install_status = gr.install_status == 7;
         if (gr.isValidField("life_cycle_stage_status"))
            life_cycle_stage_status = gr.life_cycle_stage_status == "Retired";
      }
      return install_status || life_cycle_stage_status;
```

CIs automatisch heraufstufen

Bearbeiten Sie die JSON-Zeichenfolge in **AutoPromoteFields** [**sn_sec_cmn.autoPromoteFields**] Systemeigenschaft, damit Ihre Suchregeln für Konfigurationselemente (Configuration Item, CI) alle Security Operations-CMDB-CIs automatisch zu übereinstimmenden Einträgen in der Tabelle [cmdb_ci] heraufstufen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Der Systemeigenschaftstyp ist „string“ und erfordert die Eingabe einer JSON-Zeichenfolge. Diese Eigenschaft ist standardmäßig aktiviert und fördert übereinstimmende CIs, während die CI-Suchregeln ausgeführt werden.

Anwenderdefinierte schriftliche Suchskripts können untergeordnete Tabellendatensätze aus dem Skript zurückgeben. Für diese Eigenschaft ist *_autoPromoteCI*Funktion in *CIIdentify Script Include*Verwendet das vom Suchskript zurückgegebene CI und durchläuft automatisch die Beziehungen, um zu gelangen *cmdb_ci*Eingabe und Rückgabe.

Um die Logik der automatischen Heraufstufung zu überschreiben, d. h. um neue CI-Klassen hinzuzufügen oder zu aktualisieren, fügen Sie das JSON-Objekt im Feld Wert in hinzu [**sn_sec_cmn.autoPromoteFields**] Systemeigenschaft.

Prozedur

1. Geben Sie Ein sys_properties.list In der linken Navigationsleiste.
2. Wählen Sie Aus **Geben Sie Ein** .
3. Suchen Sie nach [**sn_sec_cmn.autoPromoteFields**] Systemeigenschaft und wählen Sie den Datensatz aus, um ihn zu öffnen.

   Standardzeichenfolge:

   ```
   {
    "dscy_switchport":"cmdb_ci",
    "cmdb_ci_network_adapter":"cmdb_ci",
    "cmdb_ci_nic":"cmdb_ci",
    "cmdb_ci_ip_address":"nic"
   }
   ```

4. In **Wert** Textfeld: Bearbeiten Sie die Zeichenfolge im Standardpaarungsformat.
5. Wählen Sie **Aktualisieren**.
   Dieser Wert wird von CI-Suchregeln während des nächsten Imports verwendet.

Konfigurieren Sie den Schlüssel für angreifbare Elemente

Konfigurieren Sie die Granularität des angreifbaren Elements (VI T) Geben Sie in ein Vulnerability Response Anwendung zum Definieren, was ein angreifbares Element ausmacht (VI T) In Ihrer Organisation.

Vorbereitungen

Erforderliche Rolle: Administrator

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Schlüsselbegriffe:

Konfigurationselement bzw. Configuration Item (CI)

Ein vorhandenes Asset, das in Ihrer CMDB aufgeführt ist.

Schwachstelle

Ein Datensatz einer bekannten Schwachstelle, die aus dem National Institute of Standards and Technology (NIST), der National Vulnerability Database (NVD), Common Vulnerabilities

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

and Exposures (CWE) oder Integrationen von Drittparteien mit importiert wurde Vulnerability Response.

Angreifbares Element

Ein angreifbares Element wird erstellt, wenn eine importierte Schwachstelle mit einem Konfigurationselement in Ihrer CMDB übereinstimmt.

Erkennung

Ein einzelnes, eindeutiges Vorkommen einer Schwachstelle, wie von den Scannern Ihrer Drittanbieterintegrationen gemeldet. Erkennungen werden importiert und sowohl in den Erkennungs- als auch in den Datensätzen für angreifbare Elemente in Ihrer Instanz angezeigt. Wird auch als Erkennung angreifbarer Elemente bezeichnet.

Standardmäßig ist ein angreifbares Element eine eindeutige Kombination aus einem Konfigurationselement (Configuration Item, CI), einer Schwachstelle und einer Integrationsinstanz. Um angreifbare Elemente mit mehr Granularität zu erstellen, fügen Sie eindeutige Ports hinzu Oder Empfehlungen (nur für Microsoft TVM-Schwachstellen) Aus Erkennungen angreifbarer Elemente. Dies hilft Ihnen, die Behebung von Schwachstellen auf der Ebene zu verwalten, die Ihrer Meinung nach für Ihre Organisation am effektivsten ist.

Wenn Sie angreifbare Elemente mit mehr Granularität erstellen möchten, konfigurieren Sie den Schlüssel für angreifbare Elemente so, dass er den Port enthält Oder-Empfehlung.

- Wenn **Port einschließen** Ist aktiviert, werden angreifbare Elemente von eindeutigen Ports aus Erkennungen angreifbarer Elemente erstellt.
- Wenn **Empfehlung einschließen** Ist aktiviert, wird für jede Empfehlung, die einer Schwachstelle zugeordnet ist, ein separates angreifbares Element erstellt.

Hinweis:
Die **Empfehlung Einschließen** Die Option wird in der UI nur angezeigt, wenn die Microsoft TVM-Integration in Ihrer Umgebung aktiviert ist.

Ab Vulnerability Response V17.1 können Sie Rapid7-Schwachstellen identifizieren und beheben, indem Sie Beweise als VI-Schlüssel hinzufügen. Weitere Informationen finden Sie unter Hinzufügen von Nachweisen zu Schlüsseln für angreifbare Rapid7-Elemente.

Wählen Sie eine Option aus der folgenden Tabelle aus, um die Option „Port einschließen“ zu aktivieren.

Drei Szenarien für die erstmalige Aktivierung der Option „Port einbeziehen“ mit dem VI-Schlüssel

Wenn...	Beschreibung
Mindestens eine der folgenden Bedingungen ist „wahr“: • Sie führen ein Upgrade von einer Version von durch Vulnerability Response Vor v10.0, die die Erkennung angreifbarer Elemente nicht unterstützt hat. • Sie sind ein neuer Kunde und haben keine Vulnerability Response-Daten (Erkennung angreifbarer Elemente oder angreifbarer Elemente) in Ihrem ServiceNow AI Platform® Instanz.	Aktivieren Sie „Port Einschließen“. Nachdem der Einbindungs-Port aktiviert ist, erstellen importierte Erkennungen angreifbare Elemente, die VIS enthalten, die durch einen eindeutigen Port gekennzeichnet sind, beginnend mit dem nächsten Import.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Drei Szenarien für die erstmalige Aktivierung der Option „Port einbeziehen“ mit dem VI-Schlüssel (Fortsetzung)

Wenn...	Beschreibung
• Sie haben bereits Alle Datensätze für angreifbare Elemente und zugehörige Daten wurden gelöscht In Ihrer Instanz sind Sie bereit, alle Ihre Vulnerability Response-Daten zu erstellen, beginnend mit einem neuen Import, um VIS einzubeziehen, die sich durch einen eindeutigen Port unterscheiden.	
Beide Bedingungen sind wahr: • Sie haben v10.0 oder höher von Vulnerability Response Und Sie verfügen in Ihrer Instanz über Vulnerability Response-Daten (Erkennung angreifbarer Elemente oder angreifbarer Elemente), die Sie beibehalten möchten. • Sie möchten mit der Erstellung neuer angreifbarer Elemente beginnen, um VIS einzubeziehen, die nach eindeutigem Port unterschieden werden.	Aktivieren Sie „Port einschließen“. Ihre vorhandenen Erkennungen und die zugehörigen angreifbaren Elemente werden beibehalten. Nachdem der Einbindungs-Port aktiviert ist, erstellen neue Erkennungen neue angreifbare Elemente, die VIS enthalten, die durch einen eindeutigen Port gekennzeichnet sind, beginnend mit dem nächsten Import.
Beide Bedingungen sind wahr: • Sie haben v10.0 oder höher von Vulnerability Response. • Sie verfügen über vorhandene Vulnerability Response-Daten (Erkennungen angreifbarer Elemente oder angreifbarer Elemente), möchten Ihre vorhandenen Daten jedoch nicht beibehalten, da Sie Ihre Schwachstellendaten lieber von einem neuen Import aus erstellen und VIS einschließen möchten, die sich durch einen eindeutigen Port unterscheiden.	1. Löschen Sie alle Datensätze für angreifbare Elemente und zugehörige Daten Aus Ihrer Instanz. 2. Aktivieren Sie „Port einschließen“. Nachdem der Einbindungs-Port aktiviert ist, erstellen neue Erkennungen neue angreifbare Elemente, die VIS enthalten, die durch einen eindeutigen Port gekennzeichnet sind, beginnend mit dem nächsten Import.

Hinweis:

Wenn die Option „Port einschließen“ aktiviert ist, kann für ein Konfigurationselement mehr als ein angreifbares Element erstellt werden. Wenn beispielsweise eine Schwachstelle für zwei Ports in einem Konfigurationselement vorhanden ist, Ports 80 und 443, werden zwei eindeutige VIS erstellt, eines für jeden Port, beginnend mit dem nächsten Import.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Stellen Sie sicher, dass Sie VIS erstellen möchten, um VIS nach eindeutigen Ports einzubeziehen, bevor Sie diese Funktion aktivieren. Sobald Sie den VI-Schlüssel zum Einbeziehen des Ports aktiviert haben, müssen Sie zuerst Ihre Vulnerability Response-Daten löschen, bevor Sie den Einschluss-Port deaktivieren und mit der standardmäßigen VI-Schlüsselgranularität zum Importieren von Schwachstellendaten zurückkehren können, d. h. VIS werden für den Port erstellt, aber nicht durch einen eindeutigen Port unterschieden. Weitere Informationen zum Löschen Ihrer Schwachstellendaten finden Sie unter Löschen Sie alle Datensätze für angreifbare Elemente und zugehörige Daten in Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Konfigurieren Angreifbares Element G Ranularität**an.

   Das Feld zuletzt aktualisiert zeigt das Datum an, an dem der VI-Schlüssel zuletzt konfiguriert wurde.

2. Wählen Sie Aus Die **Port Einschließen** Kontrollkästchen zum Aktivieren.

   Hinweis:
   Wenn Sie die Microsoft TVM-Integration konfiguriert haben **Empfehlung Einschließen** Option ist ebenfalls verfügbar. Dadurch können angreifbare Elemente nach eindeutigen Empfehlungen aus Microsoft TVM-Daten aufgeteilt werden.

3. Wählen Sie **Speichern**.
   Das Bestätigungsdialogfeld wird angezeigt.

   Wenn Sie keine Erkennungsdatensätze für angreifbare Elemente in Ihrer Instanz haben, werden sowohl Erkennungen für angreifbare Elemente als auch angreifbare Elemente ab dem nächsten Import durch einen eindeutigen Port erstellt.

   Wenn in Ihrer Instanz Erkennungen für angreifbare Elemente und angreifbare Elemente vorhanden sind, werden vorhandene Erkennungen und zugehörige angreifbare Elemente beibehalten. Neue Erkennungen erstellen neue Schwachstellen, die VIS enthalten, die durch einen eindeutigen Port gekennzeichnet sind, beginnend mit dem nächsten Import.

Nächste Maßnahme
Überprüfen Sie, ob angreifbare Elemente nach Port in den Datensätzen der Erkennung angreifbarer Elemente und der Datensätze für angreifbare Elemente angezeigt werden. Weitere Informationen finden Sie unter Anzeigen Vulnerability Response Erkennungsdaten für angreifbare Elemente.

Hinzufügen von Nachweisen zu Schlüsseln für angreifbare Rapid7-Elemente

Fügen Sie einen Nachweis als Schlüssel für angreifbare Elemente (VIS) für hinzu Rapid7 VIS. Einschließlich des Nachweises für bestimmte Schwachstellen ermöglicht die Rapid7 Scannerintegration zum Erstellen von VIS für jeden von erhaltenen Nachweis Rapid7.

Ein VI-Schlüssel ist die Kombination aus Schwachstelle, Konfigurationselement (CI) und Integrationsinstanz. Durch die Aufteilung von Erkennungen in verschiedene VIS basierend auf Nachweisen werden mehrere VIS erstellt. Sie können die Schwachstellen den entsprechenden Korrekturbesitzern zuweisen.

Beispielsweise können zwei Erkennungen mit derselben Schwachstelle und demselben CI, aber mit unterschiedlichen Nachweisen vorhanden sein, was zur Erstellung eines VI führt Beginnt ab Vulnerability Response V17.1 können Sie Schwachstellen identifizieren und beheben, indem Sie Beweise als VI-Schlüssel hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können den Nachweis wie folgt als VI-Schlüssel hinzufügen:

Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren** Und wählen Sie die Option zum Einschließen von Nachweisen aus.

Anwendungsfall: Nachweis in VI-Schlüssel für vorhandene VIS einbeziehen oder vorhandene VIS basierend auf Erkennungsnachweis aufteilen

Um VIS basierend auf Nachweisen zu erstellen, können Sie die R7 log4j-Schwachstellen verwenden. Sie können beispielsweise eine der mehreren R7 log4j-Schwachstellen wie verwenden `R7-apache-log4j-Core-cve-2021-44228` , `R7-amazon_linux-cve-2021-44228` , Oder `R7-amazon-linux-ami-2-cve-2021-44228` .

Wenn alle Erkennungen in einem VI denselben Nachweis haben, wird das vorhandene VI so aktualisiert, dass es „Nachweis im VI-Schlüssel (external_ID)“ enthält. Wenn mehrere Erkennungen mit unterschiedlichen Nachweisen vorhanden sind, wird das vorhandene VI geschlossen. Die Erkennungen werden auf die neuen VIS mit „Nachweis im VI-Schlüssel (external_ID)“ aufgeteilt.

Hinweis:

Wenn Sie die Schwachstellen-ID angeben, werden die vorhandenen VIS basierend auf dem Nachweis aufgeteilt. Die neuen Schwachstellen für diese Schwachstellen-ID haben auch einen Nachweis als einer der VI-Schlüssel.

Löschen Sie alle Datensätze für angreifbare Elemente und zugehörige Daten in Vulnerability Response

Entfernen Sie alle Vulnerability Response-Daten (Erkennungen angreifbarer Elemente oder angreifbarer Elemente) und zugehörigen Daten und Datensätze endgültig aus dem aus Vulnerability Response Anwendung in Ihrem ServiceNow AI Platform® Instanz.

Vorbereitungen

Löschen Sie Erkennungsdatensätze für angreifbare Elemente, angreifbare Elemente, Schwachstellengruppen und alle zugehörigen Datensätze in Vulnerability Response Anwendung aus Ihrer Instanz. Verwenden Sie diesen Prozess, um Ihre Instanz zu bereinigen, um Daten mit einem Neustart aus Ihren Drittanbieterintegrationen zu importieren, oder als Voraussetzung, um die Schlüsselkonfiguration für angreifbare Elemente (VIS) auf ihre Standardeinstellung zurückzusetzen. Weitere Informationen zum Konfigurieren des VI-Schlüssels finden Sie unter Konfigurieren Sie den Schlüssel für angreifbare Elemente.

Hinweis:

Mit dieser Aktion werden alle Datensätze angreifbarer Elemente und alle zugehörigen Daten aus Ihrer Instanz gelöscht. Diese Daten können nach dem Löschen nicht abgerufen werden. Außerdem müssen Sie den Datenimport anhalten und Ihre aktiven Drittpartei-Integrationen mit deaktivieren Vulnerability Response.

Das Löschen Ihrer Daten für angreifbare Elemente mit diesem Prozess ist erforderlich, bevor die VI-Schlüsselkonfiguration geändert wird. Durch das Entfernen aller Daten wird sichergestellt, dass alle Ihre Erkennungen für angreifbare Elemente und angreifbare Elemente ab dem nächsten Import zugeordnet und mit den neuesten Daten aktualisiert werden.

Stellen Sie sicher, dass die folgenden Bedingungen gelten, bevor Sie Ihre Daten löschen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie haben v10.0 oder höher von Vulnerability Response Installiert. Weitere Informationen finden Sie unter Vulnerability Response Erkennungen angreifbarer Elemente aus Drittpartei-Integrationen.
- Sie möchten den Include-Port deaktivieren und die VI-Schlüsselkonfiguration auf die Standardeinstellung zurücksetzen.
- Sie haben vorhandene Erkennungen angreifbarer Elemente und angreifbarer Elemente, möchten sie jedoch nicht aktualisieren oder müssen sie beibehalten.
- Sie haben festgelegt, dass Sie alle vorhandenen Vulnerability Response-Daten und zugehörigen Datensätze entfernen möchten, um Ihre Instanz zu bereinigen.

Erforderliche Rolle: sn_vul.Vulnerability_admin

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellen-Integrationen**an.
2. Zeichnen Sie alle angezeigten aktiven Integrationen auf.

   Alle aktiven Integrationen, die mit geplanten Aufgaben aufgeführt sind, werden deaktiviert, bevor alle Ihre angreifbaren Elemente und zugehörigen Daten gelöscht werden, sodass während der Datenentfernung keine neuen Daten importiert werden. Die Aufzeichnung dieser Liste hilft Ihnen, Ihre Integrationen nach Abschluss des Löschvorgangs zu aktivieren.
3. Überprüfen Sie So löschen Sie vorhandene Vulnerability Response-Daten für den erneuten Import artikel in der HI Knowledge Base.
4. Wenn eine Warnmeldung angezeigt wird, die verhindert, dass Sie in die Spalte aktiv schreiben, führen Sie die folgenden Schritte aus, um aktive Integrationen zu deaktivieren.

   a. Klicken Sie in der Spalte Name auf ein Element, um den Datensatz zu öffnen.

   b. Wenn Sie das Kontrollkästchen aktiv nicht bearbeiten können, klicken Sie auf **Hier** Link zum Bearbeiten des Datensatzes.

   c. Klicken Sie auf **Aktiv** Kontrollkästchen, um die Integration zu deaktivieren und die nächste geplante Aufgabe abzubrechen.

   d. Klicken Sie Auf **Aktualisieren** Um Ihre Änderungen zu speichern und zur Liste zurückzukehren.

   e. Stellen Sie sicher, dass Sie alle aktiven Integrationen aus der Integrationsliste deaktiviert haben. Nachdem Sie eine Integration deaktiviert haben, wird sie nicht mehr in der Liste der aktiven Integrationen angezeigt. Um eine Liste inaktiver Integrationen anzuzeigen und alle Integrationen zu suchen, die Sie deaktiviert haben, nachdem Sie alle Ihre Schwachstellendaten gelöscht haben, geben Sie in der Spalte aktiv oben ein `=falsch` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Fahren Sie mit den Schritten im KB-artikel fort, um Ihre vorhandenen Schwachstellendaten zu löschen.
6. Nachdem Sie bestätigt haben, dass alle Daten erfolgreich gelöscht wurden, navigieren Sie zu **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**an.
7. Im Formular:
   - Wenn Sie Daten gelöscht haben, da Sie Ihre Schwachstellendaten so erstellen möchten, dass sie den Port aus einem neuen Import enthalten, aktivieren Sie „Port einschließen“, und klicken Sie auf **Speichern** .
   - Wenn Sie Daten gelöscht haben, da Sie den VI-Schlüssel auf die Standardeinstellung zurücksetzen möchten, deaktivieren Sie „Port einschließen“, und klicken Sie auf **Speichern** .

   Weitere Informationen finden Sie unter Konfigurieren Sie den Schlüssel für angreifbare Elemente.

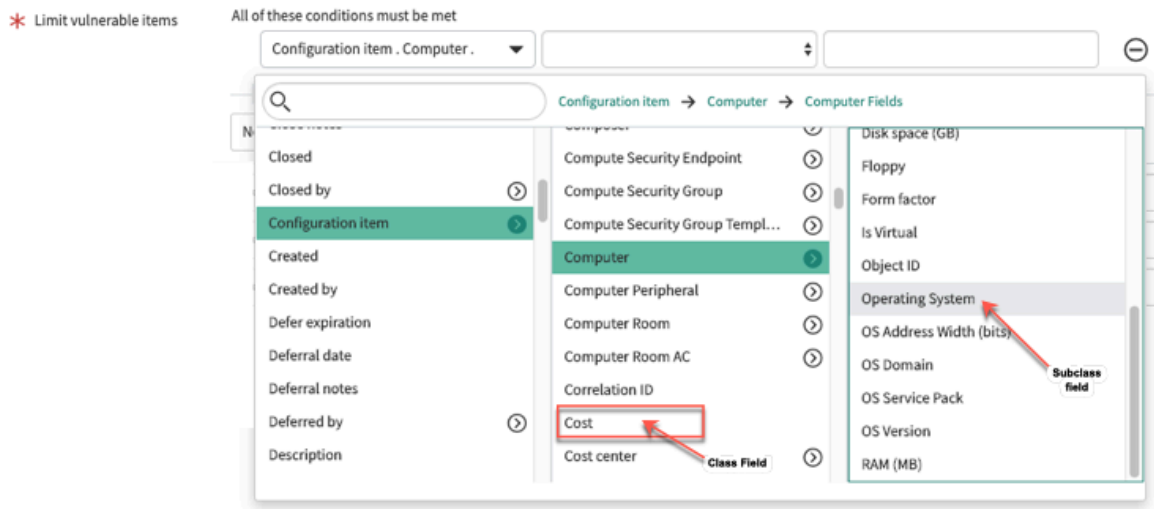
Filtern in Vulnerability Response

Regeln, Rechner und Zuweisungsregeln für Korrekturaufgaben verwenden während des Imports Bedingungen, die mit erstellt wurden **Bedingungsgenerator** . Änderungen an ihren Kriterien können sich auf die Leistung auswirken, da jeder Datensatz mit diesen Filtern ausgewertet wird.

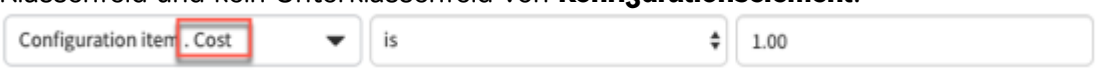
Die mit dem Basissystem gelieferten Regeln und Rechner sind für die Leistung optimiert. Das Bearbeiten oder Erstellen von Regeln oder Rechnern ist vorsichtig und erfordert möglicherweise beides ServiceNow Und Vulnerability Response Fachwissen.

Vermeiden Sie das Filtern basierend auf Unterklassenfeldern

Einige Tabellen unterstützen Erweiterung. Ein Beispiel dafür ist die Tabelle „CMDB-CI“ [cmdb_ci]. Tabellen wie cmdb_ci_Hardware und cmdb_ci_Computer erweitern diese Tabelle. Wenn Sie basierend auf einem Feld filtern, das sich nicht in der übergeordneten Tabelle befindet, kann das Erstellen und Auswerten dieses Filters kostspielig sein.



Zum Beispiel Filtern nach **Konfigurationselement** > **Kosten** Würde die Leistung nicht beeinträchtigen, da **Kosten** Ist ein Klassenfeld und kein Unterklassenfeld von **Konfigurationselement**.



Konfigurationselement > **Computer**, Ist jedoch eine Unterklasse, die einen Dot-Walk zu einem anderen Feld erfordert, in diesem Fall **Betriebssystem**. Dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Prozess kann viele Millisekunden dauern, was sich schnell summiert, wenn Millionen von angreifbaren Elementen importiert werden, und die Leistung beeinträchtigt.

Hinweis:
Die Verwendung der Bedingung [enthält] ist wie eine Platzhaltersuche und kann Auswirkungen auf die Leistung haben. Die Verwendung von [ist] ist, wo immer möglich, effizienter.

Schweregradzuordnung für Vulnerability Response

Vulnerability Response wird mit National Vulnerability Database (NVD) zu normalisierter ServiceNow-Schweregradzuordnung geliefert. Integrationen von ServiceNow-Drittparteien bieten Schweregradzuordnungen bei der Installation. Diese Zuordnungen können angepasst werden, indem die Felder in vorhandenen Zuordnungen geändert werden.

Rapid7 Schwachstellenintegration – Schweregradzuordnung

Normalized_Severity

Berechnen Sie normalized_severity für den Eintrag des dritten Teils anhand des Schweregrads, der aus stammt **sn_vul_nvd_entry** Tabelle. Dies wird mithilfe von Business-Regeln für „normalisierten Schweregrad suchen“ festgelegt **sn_vul_entry** Tabelle.

Source_severity

Daten aus dem **Schweregrad_Punktzahl** Tabelle ist zugeordnet **Source_severity** Tabelle während **Rapid7-Schwachstellenintegration: API** Wird ausgeführt.

Priorität

Dieses Feld ist leer.

Qualys-Schwachstellenintegration – Schweregradzuordnung

Normalized_Severity

Berechnen Sie normalized_severity für den Eintrag des dritten Teils anhand des Schweregrads, der aus stammt **sn_vul_nvd_entry** Tabelle. Dies wird mithilfe von Business-Regeln für „normalisierten Schweregrad suchen“ festgelegt **sn_vul_entry** Tabelle.

Source_severity

Daten aus dem **SCHWEREGRAD_LEVEL** Ist dem zugeordnet **Source_severity** Tabelle während **Qualys Knowledge Base-Integration** Wird ausgeführt.

Priorität

Daten für das Feld Priorität werden von abgerufen **SCHWEREGRADTABELLE** Und zugeordnet zu **Priorität** Tabelle während **Qualys-Host-Erkennungsintegration** Wird mit der Business-Regel ausgeführt, die Qualys-Daten zugeordnet ist.

Hinweis:
Business-Regeln werden im Hintergrund ausgeführt, überprüfen die Priorität für Qualys und ordnen die Priorität entsprechend zu. Um Qualys-Daten zuzuordnen, ist BR verantwortlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Schwachstellenintegration – Schweregradzuordnung

Normalized_Severity

Berechnen Sie normalized_severity für den Eintrag des dritten Teils anhand des Schweregrads, der aus stammt **sn_vul_nvd_entry** Tabelle. Dies wird mithilfe von Business-Regeln für „normalisierten Schweregrad suchen“ festgelegt **sn_vul_entry** Tabelle.

Source_severity

Daten von **Risikofaktor** Tabelle ist zugeordnet **Source_severity** Tabelle während **Tenable.io-Plugin-Integration** Wird ausgeführt.

Priorität

Daten von **Schweregrad_ID** Ist zugeordnet zu **Source_severity** Während **Tenable.io – Integration offener Schwachstellen** Wird ausgeführt.

VPR

Daten von **Punktzahl** Ist zugeordnet zu **Source_Risk_Score** Während **Tenable.io-Plugin-Integration** Wird ausgeführt.

Daten von **Berechnet aus Punktzahl** Ist zugeordnet zu **Source_Risk_Rating** Während **Tenable.io-Plugin-Integration** Wird ausgeführt.

Tenable.sc – Zuordnung des Schweregrads der Schwachstellenintegration

Normalized_Severity

Berechnen **Normalized_severity** Bei Eintrag im dritten Teil mit dem Schweregrad aus der Tabelle „sn_vul_nvd_entry“. Dies wird mithilfe von Business-Regeln für „normalisierten Schweregrad suchen“ festgelegt **sn_vul_entry** Tabelle.

Source_severity

Daten für **Risikofaktor** Tabelle ist zugeordnet **Source_severity** Während **Tenable.io-Plugin-Integration** Wird ausgeführt.

Priorität

Daten von **Schweregrad** Erhalten als **„Schweregrad“: { „ID“: „0“, „Name“: „Info“, „Beschreibung“: „Informativ“ }** Ist zugeordnet zu **Source_severity** Während **Tenable.io – Integration offener Schwachstellen** Wird ausgeführt.

VPR

Daten von **VprScore** Ist zugeordnet zu **Source_Risk_Score** Während **Tenable.io-Plugin-Integration** Wird ausgeführt.

Daten von **Berechnet aus vprScore** Ist zugeordnet zu **Source_Risk_Rating** Während **Tenable.io-Plugin-Integration** Wird ausgeführt.

TVM-Schweregradzuordnung

Normalized_Severity

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechnen Sie normalized_severity für den Eintrag des dritten Teils anhand des Schweregrads, der aus stammt **sn_vul_nvd_entry** Tabelle. Dies wird mithilfe von Business-Regeln für „normalisierten Schweregrad suchen“ festgelegt **sn_vul_entry** Tabelle.

Source_severity

Daten von **Schweregrad** Tabelle ist zugeordnet **Source_severity** Während **Microsoft TVM Vulnerability(CVE)-Integration** Wird ausgeführt.

Priorität

Dieses Feld ist leer.

Erstellen Sie einen Vulnerability Response Schweregradzuordnung

Vulnerability Response Die Schweregradzuordnung wandelt Schweregradfelder der Drittpartei-Quelle in erkennbare Felder in um Vulnerability Response.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Vulnerability Response Wird mit National Vulnerability Database (NVD) zu normalisiert geliefert ServiceNow Schweregradzuordnung. ServiceNow Drittpartei-Integrationen wie Qualys Vulnerability Integration Geben Sie bei der Installation Schweregradzuordnungen an. Diese Zuordnungen können angepasst werden, indem die Felder in vorhandenen Zuordnungen geändert werden.

Das Erstellen oder Bearbeiten einer Schweregradzuordnung ist nur für anwenderdefinierte oder nicht standardmäßige Zuordnungen von Drittparteien in Ihrer Umgebung vorgesehen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Normalisierte Schweregradzuordnung**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feldzuordnung

Feld	Beschreibung
Quelle	Der Name der Quelle für die Schweregradzuordnung.
Quellwert	Der Quellschweregradwert.
Zielwert	Der Wert des Zielschweregrads. Die Auswahlmöglichkeiten lauten wie folgt: ○ 1 – Kritisch ○ 2 – Hoch ○ 3 – Mittel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ 4 – Niedrig ○ 5 – Keine

4. Wiederholen Sie Schritt 3 für jeden Quellenschweregrad.
5. Klicken Sie auf **Absenden**.

Definieren Sie Serviceklassifizierungen für Vulnerability Response Berichterstellung und zugehörige Listen

Konzentrieren Sie sich auf die Berichterstellung und zugehörige Listen in Vulnerability Response Durch Definieren von Serviceklassifizierungen. Darüber hinaus kann die Reduzierung der Anzahl der angeforderten Serviceklassifizierungen die Leistung von verbessern Vulnerability Response Datenerfassung.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis:

Das Bearbeiten von Systemeigenschaften erfordert beides ServiceNow Und Vulnerability Response Fachwissen.

Prozedur

1. Geben Sie Ein `sys_properties_list.do` In der linken Navigationsleiste.
2. Klicken Sie auf **Eingeben**.
3. In **Suchen** Menü, unter **Name** Geben Sie ein `sn_vul.service_classifications` .
4. Öffnen Sie *`sn_vul.service_classifications`*Systemeigenschaft.
5. In **Wert** Textfeld: Geben Sie die kommagetrennte Liste der gewünschten Serviceklassifizierungen ein.

Hinweis:

Wenn diese Einstellung leer ist, werden alle Services aufgelistet.

Beispiele:

Um Business-Services, technische Services und Anwendungsservices anzuzeigen und Serviceangebote, gemeinsam genutzte Services und nicht klassifizierte Services auszuschließen, legen Sie den Wert folgendermaßen fest: **Business-Service, Technischer Service, Anwendungsservice** .

Um Anwendungsservices anzuzeigen, legen Sie den Wert fest auf: **Anwendungsservice** .

6. Klicken Sie auf **Aktualisieren**.
   Die Daten in jedem Bericht und in der zugehörigen Liste der angreifbaren Elemente werden bei der nächsten Ausführung des nächtlichen Performance Analytics-Auftrags nach Serviceklassifizierung gefiltert.

Auditieren Sie ausgewählte Felder in der Tabelle „angreifbare Elemente“

Aktivieren Sie das Auditing für Felder, die Sie in der Tabelle „Angreifbares Element“ [sn_vul_vulnerable_item] angeben. Diese Methode des Audits ist nützlich, wenn Sie Felder auditieren möchten, die Sie standardmäßig nicht auditieren können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

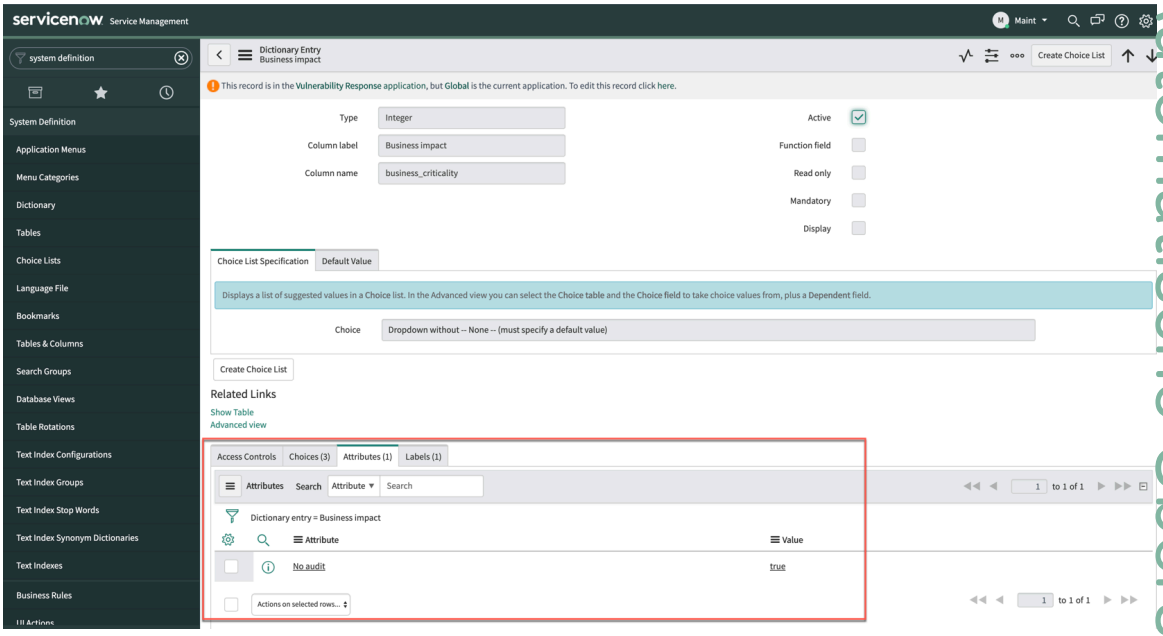
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Tabelle „sn_vul_vulnerable_item“ ist standardmäßig auditierbar. Felder, für die das Attribut „no_Audit“ auf „wahr“ festgelegt ist, können nicht auditiert werden. Weitere Informationen zu Audittabellen finden Sie unter Aktivieren Sie das Auditing für eine Tabelle .

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Systemdefinition** > **Tabellen** Und suchen Sie nach der Tabelle „sn_vul_vulnerable_item“.
   Die Liste der Wörterbucheinträge für die Tabelle wird angezeigt.
2. Um das Auditing für ein Feld zu aktivieren, klicken Sie auf den Namen des Eintrags.
   Die Seite „Wörterbucheintrag“ für diesen Eintrag wird angezeigt.



3. Navigieren zu **Attribute** > **Kein Audit**an.
   Die Seite Wörterbuchattribut wird angezeigt.
4. Klicken Sie auf, um das Attribut „no Audit=true“ zu entfernen **Löschen** .
   Auditing für dieses Feld ist aktiviert.

Automatische Übersetzung

Vulnerability Response Konfiguration des Hintergrundauftrags-Frameworks

Definieren Sie das Framework für Hintergrundaufträge in Ihrem ServiceNow AI Platform® Instanz. Diese Konfigurationsänderungen können Ihnen helfen, die Leistung zu verbessern, indem die Menge der Systemressourcen reduziert wird, die für die Ausführung Ihrer Hintergrundaufträge verwendet werden.

Was können Sie im Hintergrundauftrags-Framework bearbeiten

Mit dem Konfigurationsmodul für Hintergrundaufträge haben Sie die folgenden Einstellungsoptionen im Framework:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können die Anzahl der Hintergrundaufträge definieren, die gleichzeitig für ausgeführt werden Vulnerability Response Prozesse.
- Für lange Aufträge, die im Hintergrund ausgeführt werden und große Datenmengen verarbeiten, können Sie Partitionen erstellen, um Daten in kleineren Blöcken zu verarbeiten.
- Sie können einen Auftrag abbrechen.

Warum sollte das Hintergrundauftrags-Framework konfiguriert werden

Hintergrundaufträge in Ihrem ServiceNow AI Platform® Sind so konzipiert, dass sie über lange Zeiträume ausgeführt werden, um mehrere Prozesse für Ihre Datensätze in auszuführen Vulnerability Response. Diese Aufträge basierten zuvor auf Business-Regeln, die asynchron ausgeführt wurden. Es gibt keine Beschränkung für die Anzahl dieser Aufträge, die im Hintergrund in Ihrer Instanz ausgeführt werden können, sodass die großen Mengen von Datensätzen verarbeitet werden können, die von diesen Aufträgen betroffen sind. Wenn mehrere Aufträge, deren Abschluss lange dauert, gleichzeitig im Hintergrund ausgeführt werden, sind die Systemressourcen betroffen, die für die Ausführung Ihrer geplanten Aufgaben verwendet werden, was sich wiederum negativ auf Ihre Leistung auswirken kann.

Die Konfiguration des Hintergrundauftrags-Frameworks kann Ihnen helfen, Ihre Leistung zu verbessern, indem Sie die Menge reduzieren, die für die Ausführung Ihrer Hintergrundaufträge verwendet wird.

Wichtige Begriffe

Auftragsfähigkeit

Beschreibt die jeweiligen Aufträge. Beispielsweise kann ein bestimmter Auftrag die folgenden Fähigkeiten enthalten:

- Der Auftrag kann parallel mit einem anderen Auftrag desselben Typs ausgeführt werden.
- Der Auftrag kann partitioniert werden.
- Der Auftrag kann während der Ausführung abgebrochen werden.

Gleichzeitigkeit

Bezieht sich auf Aufträge oder Aufträge, die parallel ausgeführt werden.

Partition

Partitionen sind Aufgaben, die aufgeteilt werden können, sodass sie parallel verarbeitet werden können, um eine bessere Leistung zu erzielen. Bezieht sich normalerweise auf Aufträge mit langen Laufzeiten.

Auftragskonfiguration

Bezieht sich auf die Einstellungen für eine bestimmte geplante Aufgabe.

Geplante Aufgabe

Geplante Aufgaben sind automatisierte Aufgaben, die zu einem bestimmten Zeitpunkt oder nach einem wiederkehrenden Zeitplan ausgeführt werden können.

Systemressourcen

Bezieht sich auf die Menge der Systemressourcen, die Sie für eine bestimmte Anzahl von Hintergrundaufgaben und geplanten Aufgaben in Ihrer Umgebung unterstützen müssen.

Systemeigenschaft

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaften speichern Konfigurationsinformationen, die sich selten oder nie ändern. Jedes Mal, wenn Sie eine Systemeigenschaft ändern oder hinzufügen, leert das System den Cache, um alle Knoten im Cluster synchronisiert zu halten. Diese Cache-Leerung wirkt sich auf die Leistung aus.

Business-Regel

Eine Business Rule ist ein serverseitiges Skript, das ausgeführt wird, wenn ein Datensatz angezeigt, eingefügt, aktualisiert oder gelöscht wird oder eine Tabelle abgefragt wird. Geschäftsregeln erfüllen Aufgaben wie das automatische Ändern von Werten in Formularfeldern, wenn bestimmte Bedingungen erfüllt sind, oder das Erstellen von Ereignissen für E-Mail-Benachrichtigungen und Skriptaktionen.

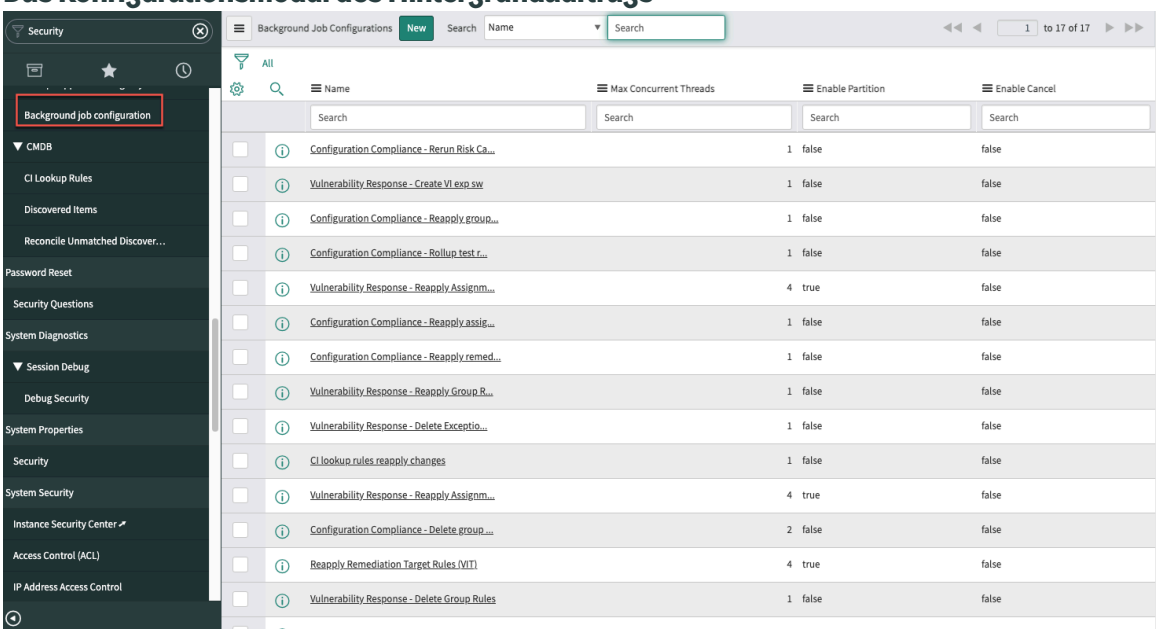
Anwendungsfall zum Definieren des Hintergrundauftrags-Frameworks

Beispielsweise verarbeitet der Hintergrundauftrag, der Korrekturzielregeln für Datensätze angreifbarer Elemente (Vits) und AVITs (Application Vulnerability Response Angreifbare Elemente) anwendet, gleichzeitig große Mengen von Datensätzen mit mehreren Aufgaben.

Abhängig von der Größe des Imports und der Anzahl der Datensätze, die Sie in Ihrer Umgebung haben, kann dieser Auftrag eine große Menge Ihrer verfügbaren Systemressourcen beanspruchen und lange dauern, bis er erfolgreich abgeschlossen ist. Systemwartungsaufträge oder andere geplante Aufgaben werden möglicherweise langsamer ausgeführt.

Das Konfigurationsmodul des Hintergrundauftrags. Aufträge werden nach Name und einer eindeutigen Konfigurations-ID aufgelistet. In diesen Datensätzen können Sie definieren, wie viele Aufgaben Sie für einen bestimmten Hintergrundauftrag gleichzeitig ausführen möchten. Sie können den Auftrag auch so festlegen, dass Partitionen von Daten verarbeitet werden, damit die Aufgaben schneller und einfacher abgeschlossen werden und weniger Systemressourcen verwenden. Sie können einen Auftrag auch abbrechen, wenn Sie feststellen, dass er zu lange ausgeführt wird.

Das Konfigurationsmodul des Hintergrundauftrags



Weitere Informationen zu den erforderlichen Schritten zum Definieren der Hintergrundauftragskonfigurationen finden Sie unter Definieren Sie Hintergrundauftragskonfigurationen in Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie Hintergrundauftragskonfigurationen in Vulnerability Response

Definieren Sie, wie viele Aufgaben Sie für einen bestimmten Hintergrundauftrag gleichzeitig ausführen möchten. Sie können den Auftrag auch so festlegen, dass Partitionen von Daten importiert werden, damit die Aufgaben schneller und einfacher abgeschlossen werden und weniger Systemressourcen verwenden. Sie können einen Auftrag auch abbrechen, wenn Sie feststellen, dass er zu lange ausgeführt wird.

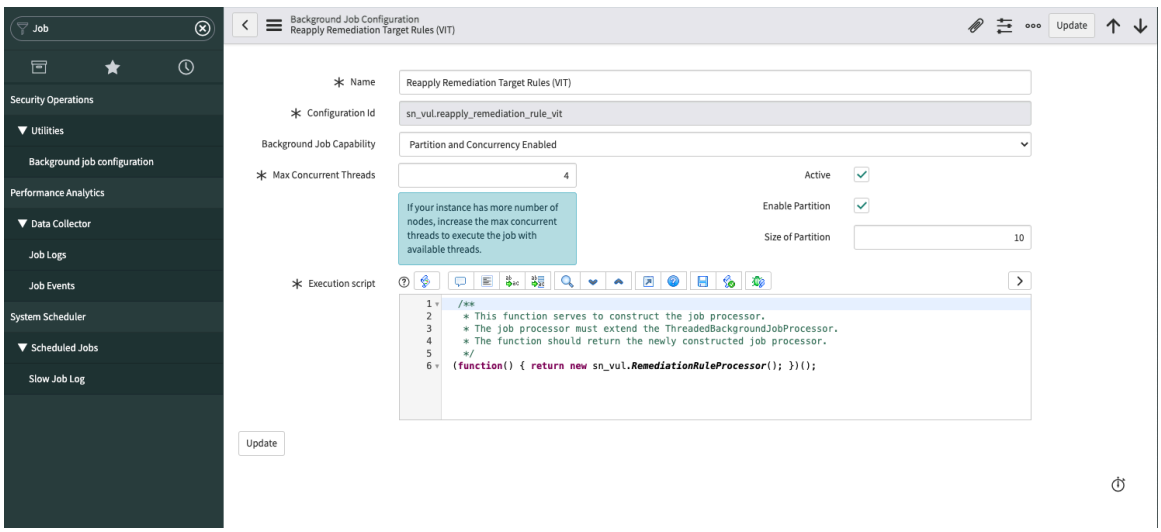
Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder Schwachstellenmanager mit der granularen Rolle sn_sec_cmn.Manage_background_Job

Ein Beispiel finden Sie im Abschnitt unter den Schritten.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Hintergrundauftrags-Konfigurationen**an.
2. Klicken Sie in der Spalte Name auf einen Datensatz, um ihn zu öffnen.
3. Bearbeiten Sie die Felder.



4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
   Im folgenden Beispiel erfahren Sie, wie Sie Ergebnisse für Ihre Konfigurationsänderungen überprüfen.

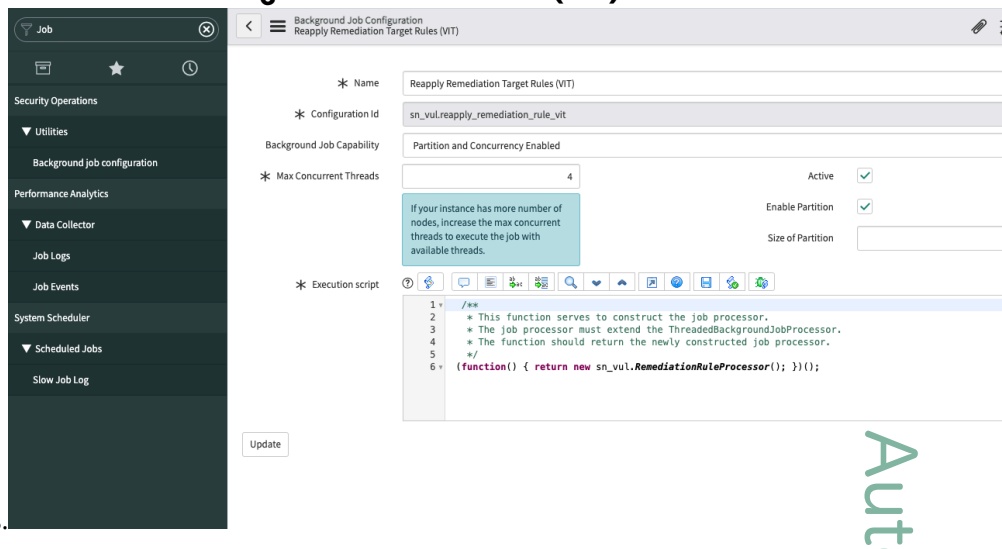
   Es gibt zwei Auftragskonfigurationen für Korrekturzielregeln, die in der Anwendung enthalten sind, eine für angreifbare Elemente und eine für angreifbare Anwendungselemente:

   - Korrekturzielregeln erneut anwenden (VIT)
   - Korrekturzielregeln erneut anwenden (AVIT)

   Angenommen, Sie ändern Ihre Korrekturzielregeln und möchten sie erneut anwenden, ohne die meisten Ihrer verfügbaren Systemverarbeitungsressourcen zu verwenden. Um die Verarbeitungsressourcen zu begrenzen, können Sie die Anzahl der ausgeführten Hintergrundaufträge und die Anzahl der Elemente steuern, die Sie pro Auftrag verarbeiten, im Modul „Hintergrundauftragskonfigurationen“.

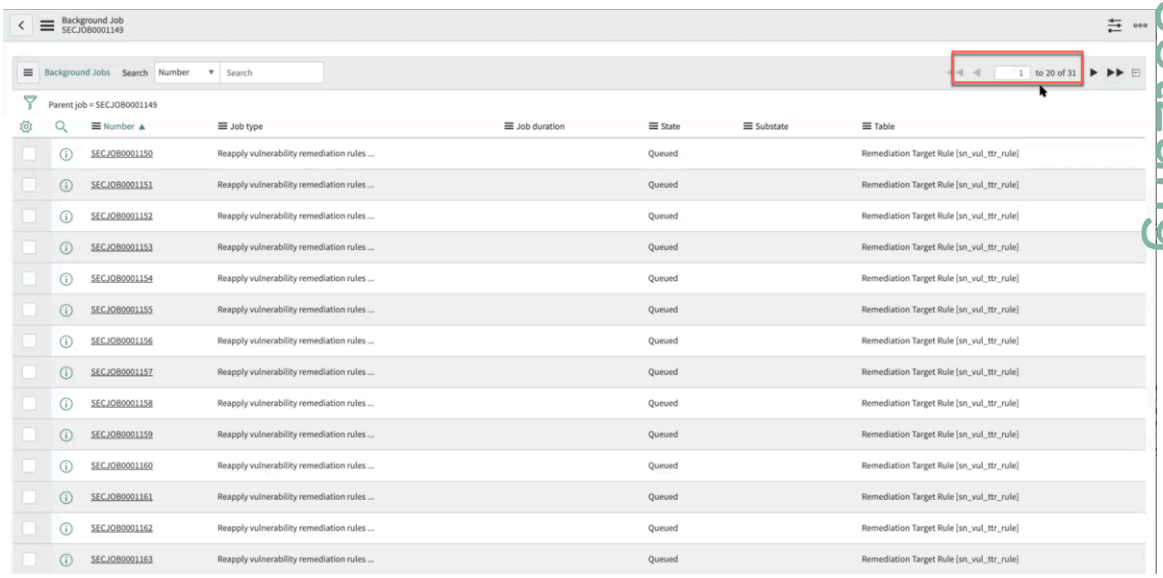
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Um diese Einstellungen zu definieren, navigieren Sie zu **Security Operations** > **Hintergrundauftrags-Konfigurationen** Und klicken Sie auf **Korrekturzielregeln erneut anwenden (VIT)**Zum Öffnen des Konfigurationsauftragsdatensatzes.



Sagen Sie, Sie wissen, dass Sie etwas mehr als 300 VIS haben.

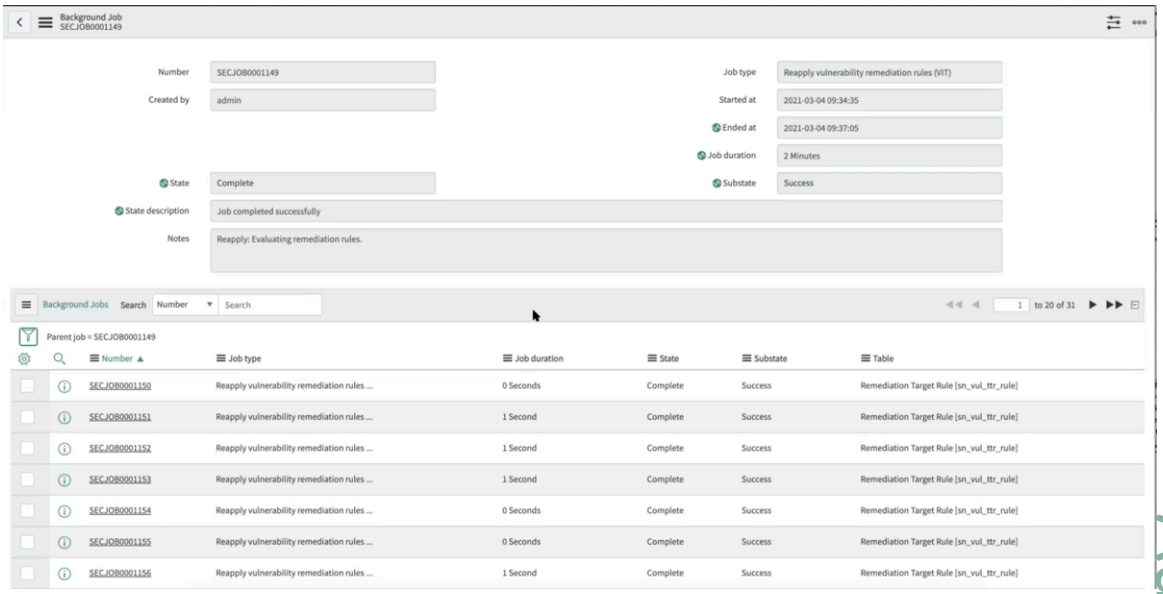
6. Ändern Sie im Datensatz des offenen Konfigurationsauftrags den Wert der Partitionsgröße von **4** Bis **10** .
7. Navigieren zu **Vulnerability Response** > **Korrekturzielregeln**, Suchen Sie die von Ihnen geänderte Regel zur erneuten Anwendung der Schwachstellenkorrektur, wählen Sie den Datensatz aus der Liste aus, und klicken Sie auf **Änderungen Anwenden** Um Ihre Zielregeln für Ihre vorhandenen VIS neu zu bewerten.
   Der Auftrag „Schwachstellen-Korrekturregeln erneut anwenden“ (VIT) befindet sich in der Warteschlange.
8. Klicken Sie auf **Status anzeigen** Link zum Anzeigen des Hintergrundauftragsdatensatzes und zum Überprüfen, ob die Aufträge in der Warteschlange stehen, wie in der folgenden Abbildung gezeigt.
   In diesem Beispiel werden 31 Aufträge erstellt, um Zielregeln für 307 VIS zu verarbeiten (maximal 10 Elemente pro Auftrag). Diese Aufträge sind untergeordnete Aufträge des primären Hintergrundauftrags. Die untergeordneten Aufträge verarbeiten die Datensätze sequenziell.



Wenn alle Aufträge erfolgreich abgeschlossen sind, werden die Felder im Hintergrundauftragsdatensatz aktualisiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Navigieren Sie zu Ihren angreifbaren Elementen, und überprüfen Sie, ob sie Ihre neue Regeländerung widerspiegeln.

Erweiterte parallele Verarbeitung für Hintergrundaufträge in Vulnerability Response

Mit dieser erweiterten Einstellung können Sie unabhängig vom Auftragstyp die Gesamtzahl der Hintergrundaufträge steuern, die parallel verarbeitet werden.

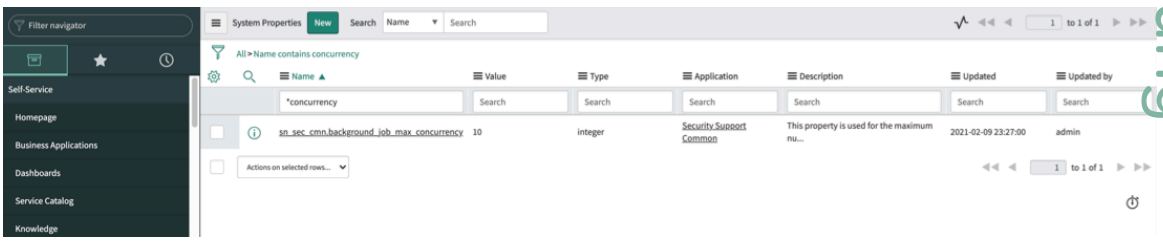
Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder Schwachstellenmanager mit der granularen Rolle sn_sec_cmn.Manage_background_Job

Hinweis:
Dieses Verfahren erfordert fortgeschrittene Programmierkenntnisse.

Prozedur

1. Geben Sie im Filternavigator ein **sys_properties.list** Und suchen Sie `sn_sec_cmn.background_job_max_concurrency`Systemeigenschaft.



2. Klicken Sie darauf, um den Datensatz zu öffnen.

Standardmäßig ist `sn_sec_cmn.background_job_max_concurrency`Die Systemeigenschaft führt maximal 10 Hintergrundaufträge parallel aus.

Wenn Ihre Instanz eine geringe Anzahl von Knoten hat, können Sie diesen Wert in der Systemeigenschaft reduzieren. Angenommen, Sie haben sieben Zuweisungsregeln in Ihrer Gruppenregelliste. Im Auftragskonfigurationsdatensatz „Zuweisungsregeln erneut anwenden“ werden drei Aufträge für die Max. Gleichzeitige Threads festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

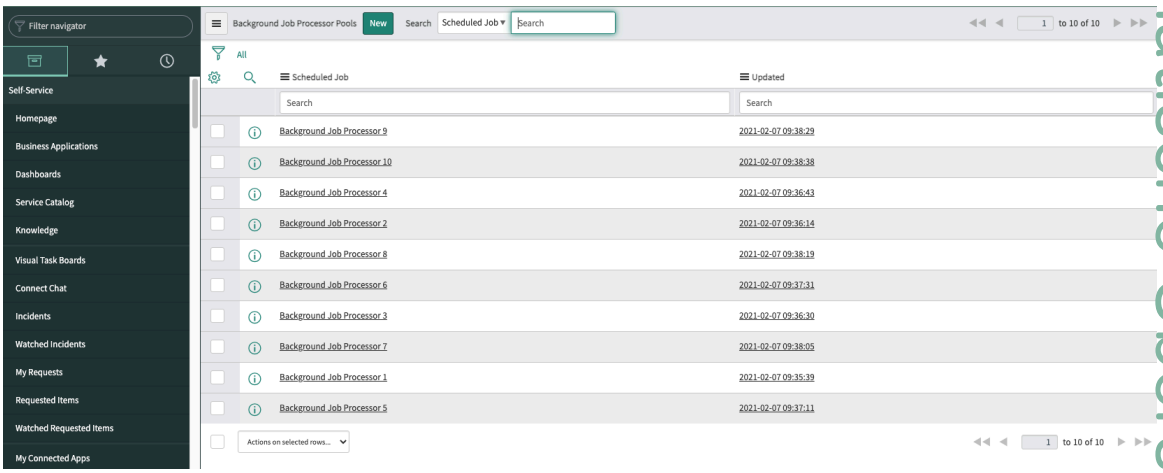
Ihr Gleichzeitigkeitswert für Ihr Framework ist 10, Ihr System ist jedoch eine Instanz mit einem einzelnen Knoten, sodass Sie zwei partitionierte Aufträge aus Ihrem Auftrag „Zuweisungsregeln erneut anwenden“ gleichzeitig verarbeiten können. Wenn Sie die maximale Anzahl gleichzeitiger Threads auf einen Auftragsdatensatz für Zuweisungsregeln festlegen, werden alle Auftragstypen „Zuweisungsregeln erneut anwenden“ sequenziell verarbeitet.

Umgekehrt können Sie diesen Wert erhöhen, wenn Ihre Instanz mehr Knoten hat, Sie müssen jedoch auch weitere geplante Aufgaben hinzufügen, um diese Änderung vorzunehmen.

Um die Anzahl der geplanten Aufgaben zu erhöhen, duplizieren Sie eine geplante Aufgabe so oft wie erforderlich, um den Wert zu erreichen, um den Sie Ihre Systemeigenschaft erhöht haben. Beispiel: Standardmäßig gibt es 10 geplante Aufgaben. Wenn Sie also 20 Aufträge wünschen, müssen Sie einen Auftrag 10 Mal duplizieren.

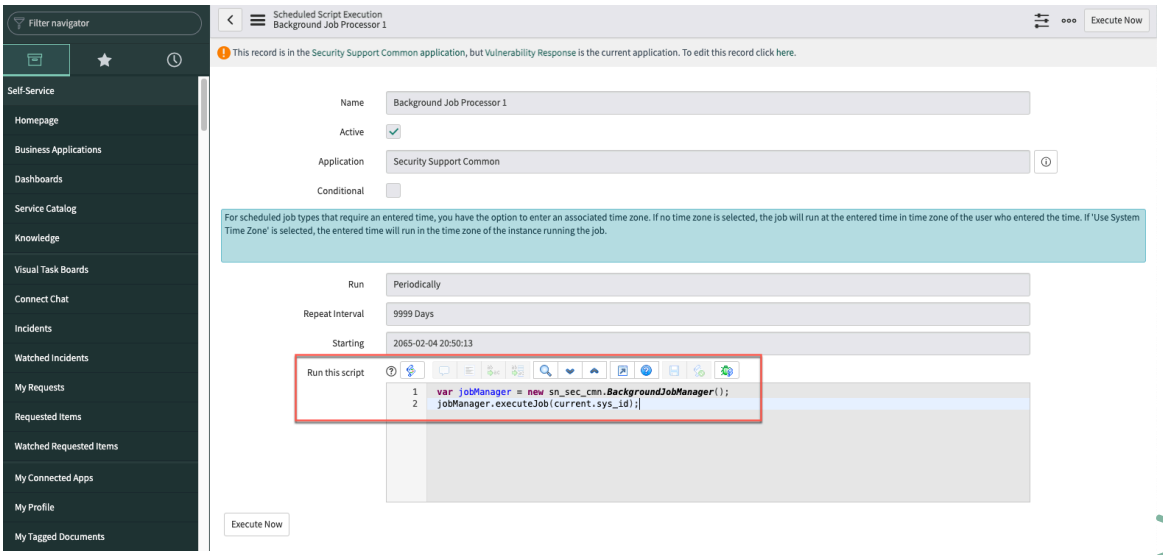
Die zehn geplanten Aufgaben, die in enthalten sind ServiceNow AI Platform® Zur Verarbeitung werden in der Tabelle sn_sec_cmn_background_Job_Processor_Pool angezeigt.

3. Geben Sie im Filternavigator ein **sn_sec_cmn_background_Job_processor_Pool.list**



4. Klicken Sie auf einen Auftrag, um ihn so oft wie erforderlich zu kopieren und zu duplizieren, damit die Anzahl der Aufträge dem Wert entspricht, um den Sie Ihre Systemeigenschaft erhöht haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

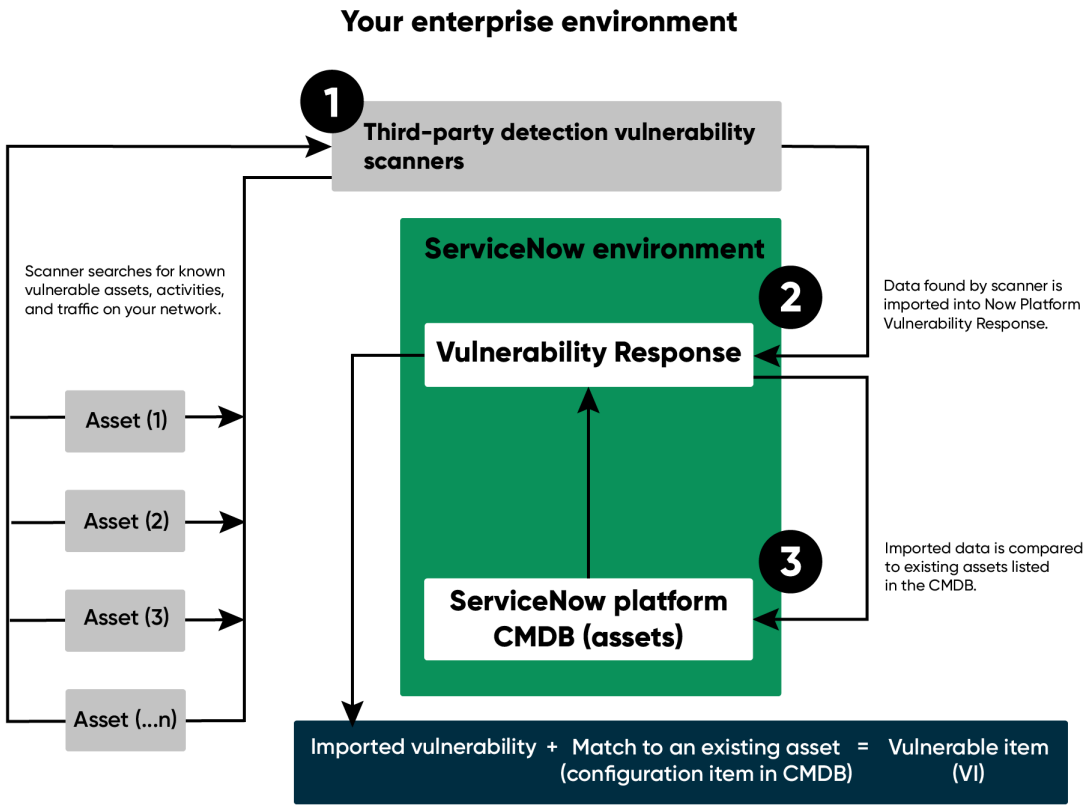


5. Nachdem die geplante Aufgabe definiert wurde, fügen Sie eine Referenz hinzu, indem Sie auf klicken **Neu** In der Liste sn_sec_cmn_background_Job_Processor_Pool für den von Ihnen kopierten Auftrag.

Vulnerability Response-Integrationen

Vulnerability Response Enthält Unterstützung für Integrationen von Drittparteien. In diesem Abschnitt finden Sie einige grundlegende Richtlinien für die Entwicklung eigener Integrationen.

Drittpartei-Integrationen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importierte Schwachstellen aus der National Vulnerability Database (NVD) und Erkennungsdaten von Drittanbieterscannern werden mit den Assets in Ihrer CMDB abgeglichen. Wenn eine importierte Schwachstelle mit einem vorhandenen Asset übereinstimmt, wird ein angreifbares Element erstellt. Angreifbare Elemente werden automatisch in Aufgaben zur Korrektur gruppiert, mit dem Geschäftskontext risikobewertet, priorisiert und den entsprechenden Teams zur Korrektur zugewiesen.

Hinweis:

Drittpartei-Integrationen werden separat behandelt. Wenn mehr als eine Integrationsanwendung von Drittanbietern in Ihrer Umgebung verwendet wird, gibt es keine Deduplizierung angreifbarer Elemente (VIS) über Integrationen hinweg. Beispiel: VI-Deduplizierung zwischen Rapid7 Und Qualys Ist nicht verfügbar.

Allerdings stimmen die Erkennungsanzahl zwischen einem Scanner einer Drittpartei nicht überein (z. B. Qualys) Zu VIS in Ihrem ServiceNow Instanz wird erwartet, da Deduplizierung über IPs, Ports usw. erfolgt.

[store-future: BEGIN review]Die folgende Tabelle enthält eine Liste von Vulnerability Response Von erstellte Infrastrukturintegrationen ServiceNow® Und Partner, um Schwachstellen zu importieren und angreifbare Elemente zu erstellen.
[store-future: BEGIN review]

Vulnerability Response: Infrastrukturintegrationen

Lieferant	Lieferantenprodukt	Integrationszusammenfassung	Store-Link	Schlüsselfunktionen
Tenable	• Tenable.io • Tenable.sc	Ordnen Sie Assets ab, und importieren Sie Schwachstellen von Drittparteien, um angreifbare Elemente zu erstellen. **Hinweis:** Tenable.io Das Starten eines erneuten Scans auf Agent-basierten Computern wird nicht unterstützt.		• Erneutes Scannen der Schwachstelle • Lösungsdaten • Drittparteidefinitionen • Tagging
Rapid7	Rapid7 InsightVM	Ordnen Sie Assets ab, importieren Sie Schwachstellen von Drittparteien, um angreifbare Elemente zu erstellen.		
Qualys	Qualys-VMDR	Ordnen Sie Assets ab, importieren Sie Schwachstellen von Drittparteien, um angreifbare Elemente zu erstellen.		Bei Bedarf erneut scannen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response: Infrastrukturintegrationen (Fortsetzung)

Lieferant	Lieferantenprodukt	Integrationszusammenfassung	Store-Link	Schlüsselfunktionen
CrowdStrike	Crowdstrike Falcon Spotlight	Ordnen Sie Assets ab, und verwenden Sie NVD, um angreifbare Elemente zu erstellen.		• NVD-Definitionen. • Unterstützt Tag-basierte Filterung beim Import.
Microsoft	Microsoft Defender Vulnerability Management	Ordnen Sie Assets ab, und importieren Sie Endpunktschwachstellen, um angreifbare Elemente zu erstellen.		Drittparteidefinitionen.
Microsoft	Microsoft Defender for IoT Microsoft Azure Defender für IoT	Importieren Sie Schwachstellen in ServiceNow Operational Technology Vulnerability Response Und ergreifen Sie risikobasierte Aktionen im Kontext des Produktionsprozesses		
Cisco (Kenna)	Kenna.VM	Ordnen Sie Assets ab, und verwenden Sie NVD, um angreifbare Elemente zu erstellen. Enthält die Kenna-Risikopunktzahl.		• NVD-Definitionen • Lösungsdaten
Tanium	Einhalten	Ordnen Sie Assets ab, und importieren Sie Schwachstellen von Drittparteien, um angreifbare Elemente zu erstellen.		
Orca	Orca-Sicherheit	Ordnen Sie Assets ab, und importieren Sie Schwachstellen von Drittparteien, um angreifbare Elemente zu erstellen.		
Onapsis	Onapsis für SAP Schwachstellen	Ordnen Sie Assets ab, und importieren Sie Schwachstellen von Drittanbietern, um angreifbare Elemente		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response: Infrastrukturintegrationen (Fortsetzung)

Lieferant	Lieferantenprodukt	Integrationszusammenfassung	Store-Link	Schlüsselfunktionen
		für SAP-Assets und -Anwendungen zu erstellen		
Synchronisieren	Synack Red Team	Importieren Sie Schwachstellen aus Synack.		
Assistent	Wiz	Passen Sie Cloud-Assets ab, und importieren Sie Schwachstellen von Drittanbietern, um angreifbare Elemente zu erstellen.		
Schnürarbeit	Schnürarbeit	Importieren Sie Infrastrukturschwachstellen aus Cloud-Asset-Quellen.		Unterstützt Schwachstellenrechner und Filterung nach Schweregrad.
Recorded Future	Attack Surface Intelligence für VR	Externe Angriffe decken Assets und Risiken auf, die in ServiceNow Vulnerability Response importiert wurden. Erstellen Sie angreifbare Elemente aus externen Asset-Erkennungen. Enthält aufgezeichnete zukünftige Bedrohungs- und Schwachstellenanreicherung.		
Mandiant	Management Der Angriffsoberfläche	Importieren Sie Informationen zu Schwachstellen und angreifbaren Elementen aus der Mandiant Attack Surface Management-Plattform.		
IBM	Sicherheitsgarantie	Integrieren Sie die Ergebnisse von IBM Guardium Database-Schwachstellen-Scans mit ServiceNow®.		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response: Infrastrukturintegrationen (Fortsetzung)

Lieferant	Lieferantenprodukt	Integrationszusammenfassung	Store-Link	Schlüsselfunktionen
CyCognito	CyCognito SaaS	Importieren Sie Probleme und Assets aus der Cycognito SaaS-Plattform		
VMware	Carbon Black Cloud	Erfassen Sie Schwachstellendaten und -Kontext aus VMwareCarbon Black Cloud. Erstellen Sie Konfigurationselemente aus Carbon Black Cloud-Endpunkten und Arbeitsauslastung.		
Kern	Schwachstellenverwaltung	Importieren Sie Ergebnisse aus Nucleus Security. Angreifbare Elemente automatisch aktualisieren. Bidirektionale Aktualisierung über Kommentarfeld. Ordnen Sie anwenderdefinierte Felder zu.		
InfoSec Global (ISG)	AgileSec Analytics	Importieren Sie Schwachstellenergebnisse in kryptografischen Assets. Kryptografische Schlüssel, Schlüsselspeicher und Bibliotheken.		
Zählungen	Externes Angriffsoberflächenmanagement	Scannen, erkennen und katalogieren Sie Schwachstellen in Assets mit Internetzugriff.		

[End]
[End]

Automatische Übersetzung

Informationen zu Integrationen von Drittparteien, die von unterstützt werden Application Vulnerability Response Siehe , Integration von Application Vulnerability Response mit anderen Anwendungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Integration von CISA Known Exploit Vulnerability (KEV)
- Verständnis der Integration von Microsoft Threat and Vulnerability Management Vulnerability
- Verständnis der Integration der HCL BigFix-Patch-Orchestration mit Vulnerability Response
- Verstehen von Vulnerability Response Patch-Orchestration-Integration mit Microsoft SCCM
- Verstehen der NVD-Integrationen
- Qualys Vulnerability Integration
- Rapid7 Vulnerability-Integration verstehen
- Shodan Exploit Integration
- Verständnis der Tenable-Schwachstellenintegration
- Integration der Microsoft Security Response Center-Lösung

  Die Integration der Microsoft Security Response Center-Lösung Ist mit verfügbar Vulnerability Solution Management. Für Informationen zur Installation und Konfiguration von Integration der Microsoft Security Response Center-Lösung Und Red Hat Solution Integration, Siehe Anwendung Solution Management for Vulnerability Response installieren. Sie können bei Bedarf konfigurieren, bearbeiten, planen und starten Integration der Microsoft Security Response Center-Lösung Und Red Hat Solution Integration Von innerhalb des Setup-Assistenten aus.

Zusätzliche Hinweise für Integrationen

Wenn mehrere Bereitstellungen für eine Integration unterstützt werden, finden Sie weitere Informationen unter Erstellen Sie domänengetrennte Importe für eine Integration.

- Sie können viele der Integrationsanwendungen im Setup-Assistenten bei Bedarf installieren, konfigurieren, planen und starten.
- Sie können installieren Rapid7 Vulnerability-Integration Anwendung aus Setup-Assistent, die Konfiguration wird für diese Integration jedoch nicht vom Setup-Assistenten unterstützt. Weitere Informationen finden Sie unter Rapid7 Vulnerability-Integration installieren.
- Die Tenable for Vulnerability Response Anwendung nach Tenable wird von Tenable erstellt und verwaltet. Die Dokumentation finden Sie unter Tenable for Vulnerability Response an.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Ab VR v17.1 wurden die folgenden Statusnamen des Integrationsprozesses aktualisiert:

Statusname vor V17.1	Statusname ab V17.1
In Verarbeitung	Wird abgerufen
Warten abgeschlossen	Warten/Bearbeitung läuft

Hinweis:
Sie können die heruntergeladenen und verarbeiteten Anhänge anzeigen. Wenn der Status der Integrationsausführung lautet `Warten abgeschlossen` , Zeigt den Prozentsatz der abgeschlossenen Integration an.

[store-future: BEGIN review]Ab v22.1.2 von Vulnerability Response, Sie können ausschließen, dass Schwachstellen mithilfe von Ausschlussregeln erfasst werden. Außerdem, wenn Sie ausführen Rapid7, Qualys, Tenable for Vulnerability Response, Microsoft Defender Vulnerability Management Integrationen oder manuelle Erfassung von Schwachstellen können Sie die Anzahl der ausgeschlossenen Erkennungen anzeigen. Auf diese Informationen kann in zugegriffen werden **Erkennungen** Registerkarte im Bildschirm „Integrationsausführung“. Weitere Informationen finden Sie unter Übersicht über Ausschlussregeln und Erstellen Sie eine Ausschlussregel.[End]

Vulnerability Response Anwendungen Und CSDM Tabellen

Die Vulnerability Response, Application Vulnerability Response, Integrationen von Schwachstellen von Drittparteien und Software Bill of Materials Anwendungen verwalten (Daten mittragen zu) CSDM Tabellen. Diese Anwendungen verwenden auch Daten aus CSDM Tabellen, die andere Anwendungen generieren. Mehrere ServiceNow Produkte profitieren daher von diesen und fügen ihnen einen Mehrwert hinzu Security Operations Anwendungen. Weitere Informationen finden Sie unter Vulnerability Response Anwendungen Und CSDM Tabellen.

Manuell erstellte Integrationen

Sie können andere Integrationen hinzufügen, die als nicht verfügbar sind ServiceNow Store Anwendungen nach Bedarf. Weitere Informationen finden Sie unter Erstellen Sie manuell eine Schwachstellenintegration.

Verstehen der NVD-Integrationen

Die NVD-Integrationen verwenden Daten, die aus dem Produkt National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) importiert wurden, um die Auswirkung und Priorität von Fehlern in Ihrem Code zu bestimmen. Führen Sie diese Integration als Teil Ihres ersten Setups von aus Vulnerability Response Und vor dem Importieren von Schwachstellendaten in Ihre Instanz mit einem Scanner-Produkt eines Drittanbieters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

NIST NVD erfasst sowohl Common Vulnerabilities and Exposures (CVE) als auch Common Platform Enumeration (CPE)-Daten und stellt diese Daten für bereit ServiceNow AI Platform®. Es lässt sich problemlos in integrieren Vulnerability Response Dient zum Zuordnen von CVE- und CPE-Schwachstellen, um die Daten in Ihrer Instanz zu ergänzen.

Wichtig:
Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Nach der Installation wird die Integration der NIST National Vulnerability Database Integration-API (nur CVE) automatisch als geplante Aufgabe aufgerufen und täglich ausgeführt. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Tipp:
Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response Integration mit NVD v1.2	

Anfänglicher Import von Schwachstellendaten mit den NVD- und CWE-Integrationen

1. Führen Sie einen ersten Import von CWE-Daten mit der CWE Comprehensive 2000 Integration durch.

   Weitere Informationen finden Sie unter Konfigurieren und führen Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen aus. Sie führen CWE-Updates durch **Bei Bedarf** Standardmäßig müssen Sie über den Integrationsdatensatz und konfigurieren.

   Hinweis:
   Planen Sie die Ausführung der CWE-Aktualisierung vor der Aktualisierung der NVD-Datenbank. Der Standardtag für das NVD-Update ist **Wöchentlich** Ein **Montag** .

2. Verifizieren Sie Vulnerability Response Die Integration mit der Anwendung NVD wird installiert, und ein erster Datenimport aus der NIST National Vulnerability Database Integration – API (nur CVE) oder der NIST National Vulnerability Database Integration – API (CVE und CPE) ist erfolgreich.

   Überprüfen Sie für CPEs, ob ein anfänglicher Datenimport aus der NIST National Vulnerability Database Integration – API (nur CPE) erfolgreich ist.

   Zur Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Lizenz erforderlich. Nachdem das Plugin installiert wurde, ist die NIST National

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Database Integration – API (nur CVE) standardmäßig aktiviert. Wird täglich ausgeführt. Weitere Informationen finden Sie unter Installieren Sie Vulnerability Response Integration mit der NIST National Vulnerability Database.

3. Drittparteibibliotheken werden als geplante Aufgaben aktualisiert. Weitere Informationen finden Sie in Ihrer Integrationsdokumentation unter Vulnerability Response-Integrationen Weitere Informationen zu Integrationen von Drittparteien.

Verständnis importierter Schwachstellendaten und angreifbarer Elemente

In Ihrem ServiceNow AI Platform Instanz wird jede importierte Schwachstelle durch einen Schwachstelleneintrag in den Quellbibliotheken von Scannerprodukten von Drittanbietern wie dargestellt Qualys, Zum Beispiel. Die angreifbaren Elemente (VIS), die in Ihrer Instanz importiert und aktualisiert werden, sind Verweise auf Bibliotheken von Drittparteien, z. B. Qualys Bibliothek. Eine Drittparteibibliothek kann wiederum auf den NVD verweisen.

Beispiel: Wenn Sie Schwachstellendaten von Drittparteien aus einem Produkt wie erfassen Qualys, Sie erfassen VIS, die auf eine QID verweisen (Qualys Bezeichner). Im Fall von Qualys, Diese QID wiederum verweist auf ein CVE aus der NVD-Bibliothek. Wenn Sie in einer Korrekturaufgabe oder einem Datensatz für angreifbare Elemente im auf diese QID klicken Vulnerability Response Anwendung und Sie haben die NVD- und CWE-Integrationen ausgeführt, um Daten zu erfassen. Sie zeigen aktuelle, angereicherte Schwachstellendaten an, mit denen Sie die Beziehungen zwischen Ihren VIS und CVEs, CWEs und CPEs sehen können.

Bevor Sie ein Scannerprodukt einer Drittpartei wie ausführen Qualys Die über eine eigene Bibliothek verfügt, müssen Sie mindestens die Integration der NIST National Vulnerability Database Integration – API (nur CVE) (enthält auch CISA-bezogene Details) und CWE-Integration installieren und ausführen, um Schwachstellendaten zu erfassen. Diese NVD- und CWE-Datenimporte bereichern Ihre Vulnerability Response Oder Application Vulnerability Response Daten vor dem Importieren von Daten mit einem Drittparteiprodukt.

Weitere Informationen zum Verwalten von NVD-, CWE- und Drittanbieterbibliotheken und zum Anzeigen dieser Bibliotheken finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken Und Anzeigen Vulnerability Response Schwachstellenbibliotheken.

Nachdem Sie den erfolgreichen NVD-Import verifiziert haben, um Ihre Schwachstellendaten weiter anzureichern, Konfigurieren und führen Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen aus.

Führen Sie die NVD- und CWE-Importe durch, bevor Sie Schwachstellendaten mit einem Drittparteiprodukt importieren. Drittparteibibliotheken werden als geplante Aufgaben aktualisiert. Weitere Informationen finden Sie in Ihrer Integrationsdokumentation unter Vulnerability Response-Integrationen Weitere Informationen zu Integrationen von Drittparteien.

NVD-Integrationen werden gesucht

Um die NVD-Integrationen anzuzeigen, navigieren Sie zu **Vulnerability Response oder Application Vulnerability Response** > **Administration** > **Integrationen**an.

Die folgenden Integrationen sind im Basissystem enthalten.

Hinweis:
Nur die NIST National Vulnerability Database Integration – API (nur CVE) Integration ist standardmäßig aktiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

NVD-Integrationen

Integration	Beschreibung
NIST National Vulnerability Database Integration – API (nur CVE)	Ruft nur NIST NVD-Schwachstellendaten (CVE) ab. Standardmäßig ist diese Integration automatisch auf tägliche Ausführung festgelegt.
NIST National Vulnerability Database Integration-API (nur CPE)	Ruft CPE-Daten von NIST NVD ab. Diese Integration ist standardmäßig inaktiv. Aktivieren Sie diese Integration, wenn Sie CPE-Daten erfassen möchten, die ein formelles Namensformat, eine Methode zum Überprüfen von Namen mit einem System und ein Beschreibungsformat für die Bindung von Text und Tests an einen Namen enthalten. Diese Informationen werden in angreifbarer Software gespeichert. Diese Integration ist auf tägliche Ausführung festgelegt und standardmäßig inaktiv. Informationen zum Aktivieren dieser Integration finden Sie unter NIST National Vulnerability Database – API aktivieren (nur CPE).
NIST National Vulnerability Database Integration-API (nicht zugeordnete CPE)	Ruft CPE-Daten ab, die dem abgerufenen CVE von NIST NVD zugeordnet sind. Diese Integration ist standardmäßig inaktiv. Aktivieren Sie diese Integration, wenn Sie CPE-Daten erfassen möchten, die ein formelles Namensformat, eine Methode zum Überprüfen von Namen mit einem System und ein Beschreibungsformat für die Bindung von Text und Tests an einen Namen enthalten. Diese Informationen werden in einer zugehörigen Liste des NVD-Schwachstelleneintrags gespeichert. Diese Integration ist auf die Ausführung bei Bedarf festgelegt und standardmäßig inaktiv. Informationen zum Aktivieren dieser Integration finden Sie unter Aktivieren Sie die NIST National Vulnerability Database – API (nicht zugeordnete CPE).

Wichtig:
Die Integration „NIST National Vulnerability Database Integration-API (CVE und CPE)“ ist veraltet.

Informationen zu Status der Integrationsausführung finden Sie unter . Zeigen Sie den Status der NVD-Integrationsimportausführung (National Vulnerability Database) an.

Vorbereitung auf die NVD-Integrationen

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die NVD-Integrationen gehen davon aus, dass Sie mit der NIST National Vulnerability Database (NVD) vertraut sind.

Erforderliche Rolle: Administrator

Hinweis:
Nehmen Sie vor dem Ausführen der NVD-Integrationen alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren und führen Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen aus

D ata-Importe aus der CWE bereichern die Schwachstellendaten in Ihrer Instanz weiter. Verwenden Sie CWE-Datensätze (Common Weakness Enumeration), die aus der CWE-Datenbank heruntergeladen wurden, als Referenz, wenn Sie entscheiden, ob eine Schwachstelle eskaliert werden muss. Führen Sie diese Integration als Teil Ihres ersten Setups von aus Vulnerability Response Und vor dem Importieren von Schwachstellendaten in Ihre Instanz mit einem Scanner-Produkt eines Drittanbieters.

Vorbereitungen

Erforderliche Rollen: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Hinweis:

Planen Sie die Ausführung der CWE-Aktualisierung vor der Aktualisierung der NVD-Datenbank. Der Standardtag für das NVD-Update ist **Wöchentlich** Ein **Montag** .

Aktualisieren Sie regelmäßig geplante Datensätze zu allgemeinen Schwachstellen aus der Datenbank „Allgemeine Schwachstellen-Aufzählung“. Sie können bei Bedarf auch das Standardskript aktualisieren oder eigene Skripts schreiben.

Jeder CWE-Datensatz enthält auch einen zugehörigen wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über die Seite „Allgemeine Schwachstellenaufzählungen“ eskalieren.

- Wenn Sie die Administratorrolle innehaben, können Sie der geplanten Aufgabe Repositorys hinzufügen.
- Wenn Sie sn_vul.Vulnerability_read haben, können Sie die geplante Aufgabe ausführen.
- Wenn Sie sn_vul.Vulnerability_write haben, können Sie die Details der geplanten Aufgabe bearbeiten.

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- *sn_sec_cmn.record_threshold_heartbeat*: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- *sn_sec_cmn.maximum_heartbeat_delay*: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**an.
2. Wählen Sie aus **CWE – umfassende 2000-Integration** Geplante Aufgabe.
3. Ändern Sie die Felder nach Bedarf.

Formular „Schwachstellenintegration“

Feld	Beschreibung
Name	Name des geplanten Auftrags.
Aktiv	Gibt an, ob die geplante Aufgabe aktiv ist. Wenn der Auftrag für einen bestimmten Zeitraum nicht ausgeführt werden soll, können Sie die Parameter einrichten, die Sie verwenden möchten, und den Auftrag deaktivieren.
Ausführen	Häufigkeit, mit der der der Auftrag ausgeführt werden soll. Nachfolgende Felder werden basierend auf Ihren Einstellungen in diesem Feld angezeigt oder ausgeblendet. **Hinweis:** Das CWE-Update ist **Bei Bedarf** Standardmäßig. Legen Sie einen geplanten Zeitraum fest, der vor Ihren NVD-Updates liegt. Zur Auswahl stehen: ○ Täglich: Wählen Sie einen aus **Zeit** ○ Wöchentlich: (Häufigste Auswahl) Wählen Sie eine aus **Tag** Und **Zeit** ○ Monatlich: Wählen Sie Aus **Tag** Und **Zeit** ○ Regelmäßig: Wählen Sie eine aus **Wiederholungsintervall** , **Wird Gestartet** Datum und Uhrzeit ○ Einmal: Wählen Sie ein **Wird Gestartet** Datum und Uhrzeit
Tag	Der Tag, an dem die geplante Aufgabe ausgeführt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn Sie ausgewählt haben **Wöchentlich** In **Ausführen** Feld zeigt dieses Feld die Wochentage an. Wenn Sie ausgewählt haben **Monatlich** In **Ausführen** Feld zeigt dieses Feld die Tage des Monats an. **Hinweis:** Planen Sie die Ausführung der CWE-Aktualisierung vor der Aktualisierung der NVD-Datenbank. Der Standardtag für das NVD-Update ist **Wöchentlich** Ein **Montag** .
Zeit	Die Zeit, zu der die geplante Aufgabe beginnen soll. **Hinweis:** Planen Sie die Ausführung der CWE-Aktualisierung vor der Aktualisierung der NVD-Datenbank. Die Standardzeit für das NVD-Update ist 01:00:00
Integrationsskript	Das Skript zum Abrufen von Daten aus den in angegebenen Datenquellen **Datenquellen** Zugehörige Liste.
Quellenintegration	[Schreibgeschützt]
Quelleninstanz	[Schreibgeschützt]
Anwendung	[Schreibgeschützt] der Name der Anwendung, für die Sie die geplante Aufgabe ausführen.
Wiederholungsintervall	Die Anzahl der Tage und Stunden, bevor die geplante Aufgabe erneut ausgeführt wird. Dieses Feld wird angezeigt, wenn **Regelmäßig** Ist in ausgewählt **Ausführen** Liste.
Wird gestartet	Datum und Uhrzeit für den Start der regelmäßigen Aktualisierungen. Dieses Feld wird angezeigt, wenn **Regelmäßig** Ist in ausgewählt **Ausführen** Liste.
Bedingt	Das Kontrollkästchen zum Hinzufügen bedingter Parameter.
Bedingung	Die Bedingungen für die Ausführung des Zeitplanauftrags. Dieses Feld wird angezeigt, wenn **Bedingt** Das Kontrollkästchen ist aktiviert.
Berichtsprozessorstrategie	Die Strategie zum Abrufen von Daten und zur Verarbeitung der geplanten Aufgabe. ○ Dient zum Abrufen von Daten aus den Datenquellen in **Datenquellen** Zugehörige Liste mit dem Skript in **Integrationsskript** Feld auswählen **Datenquellenanhang** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Dient zum Auswählen eines anwenderdefinierten Prozessors in **Berichtsprozessorskript** Wählen Sie das Feld aus **Anwenderdefinierter Berichtsprozessor** .
Berichtsprozessor-Skript	Das Skript, das ausgeführt werden soll, wenn die geplante Aufgabe ausgeführt wird. Dieses Feld wird angezeigt, wenn **Anwenderdefinierter Berichtsprozessor** Ist in ausgewählt **Berichtsprozessorstrategie** Liste.
Prozessorwerksskript	Das Skript zum Erstellen des Berichtsprozessors. Dieses Feld wird angezeigt, wenn **Anwenderdefinierter Berichtsprozessor** Ist in ausgewählt **Berichtsprozessorstrategie** Liste.

4. Klicken Sie mit der rechten Maustaste in den Header zu **Speichern** Ihre Änderungen.
5. Um den Scheduled Job sofort auszuführen, klicken Sie auf **Jetzt ausführen**.
   Sie kehren zur Ansicht Schwachstellenintegrationen zurück.
6. Um den Fortschritt des Imports zu überwachen, wählen Sie aus **CWE – umfassende 2000-Integration** Geplante Aufgabe erneut, und wählen Sie aus **Schwachstellenintegration Wird Ausgeführt** Registerkarte.

   Siehe Anzeigen Vulnerability Response Schwachstellenbibliotheken Um die importierten Einträge anzuzeigen.

Installieren Sie Vulnerability Response Integration mit der NIST National Vulnerability Database

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit das NIST National Vulnerability Database (NVD) ordnungsgemäß in integriert werden kann Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist Anwender dem Schwachstellenmanager in zu Vulnerability Response Oder die App-Sec-Manager-Gruppe in Application Vulnerability Response. Für Informationen zu Gruppenrollen in Vulnerability Response Siehe , Verwalten Sie Persona und granulare Rollen für Vulnerability Response. Für Informationen zu Gruppenrollen in Application Vulnerability Response Siehe Application Vulnerability Response Anwendergruppen und Rollen. • Der Schwachstellenmanager oder App-SEC-Manager überwacht die Konfiguration und verifiziert die erwarteten Ergebnisse.

Erforderliche Rolle: administrator

Hinweis:
Nehmen Sie vor dem Ausführen der NVD-Integrationen alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie die NVD-Integrationen installieren möchten.
2. Navigieren Sie zum ServiceNow Store.
3. In ServiceNow Store, Suchen Sie nach der Anwendung Vulnerability Response Integration mit NVD.
4. Wählen Sie die Anwendungskachel aus.
   Detaillierte Informationen zur Anwendung, die Sie installieren, werden angezeigt.

   Hinweis:
   Erwägen Sie, das zu lesen **Andere Anforderungen** Und **Abhängigkeiten** Abschnitte, falls zutreffend.

5. Wählen Sie Aus **App Anfordern** Und geben Sie ein Now Support Anmeldeinformationen.
6. Wählen Sie Aus **Abrufen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Geben Sie ein **Instanzname** Und **Grund für die Instanz** , Und wählen Sie aus **Validieren Sie Die Instanz** .
8. Wählen Sie Aus **Anforderung** .
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Alle** > **Systemanwendungen** > **Anwendungen** > **Alle**an.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen Sie aus **Installieren** .
    Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Nächste Maßnahme

Änderungen finden Sie nach der Erstinstallation unter Optionale Änderung und Aktivitäten der NVD-Integration.

Aktivieren Sie die NIST National Vulnerability Database – API (nicht zugeordnete CPE)

Um CPE-Daten (Common Platform Enumeration) für abgerufene CVE-Daten (Common Vulnerabilities and Exposures) zu erfassen, können Sie einen vollständigen Datenimport mit einer geplanten Aufgabe bei Bedarf durchführen.

Vorbereitungen

Die Integration von National Institute of Standards and Technology (NIST) National Vulnerability Database Integration (NVD)–API (Unmap CPE) erfasst (CPE) Daten, die ein formelles Namensformat, eine Methode zum Überprüfen von Namen mit einem System und ein Beschreibungsformat zum Binden von Text und Tests an einen Namen enthalten. Diese Informationen werden in einer zugehörigen Liste des NVD-Schwachstelleneintrags gespeichert.

Erforderliche Rolle: sn_vul.Vulnerability_admin oder App-SEC Manager

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **NVD** > **Integrationen**an.
2. Wählen Sie die Integration NIST National Vulnerability Database Integration–API (nicht zugeordnete CPE) aus.
3. Aktivieren Sie die Checkbox **Aktiv**.

   Hinweis:
   Die Integration ist für die Ausführung bei Bedarf vorkonfiguriert. Durch Aktivieren der Integration wird sie automatisch nach der Integration der NIST NVD Integration-API (nur CVE) ausgeführt. Das Ändern anderer Integrationsparameter erfordert beides ServiceNow Und Vulnerability Response Und Kompetenz und kann zu unvollständigen Daten führen.

   a. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**an.
   b. Wählen Sie NIST National Vulnerability Database Integration–API (nicht zugeordnete CPE) Integration aus.
   c. Wählen Sie aus **Integrationsdetails** Registerkarte.
   Unabhängig von **Importieren seit** Feldwert, CPEs für alle abgerufenen CVEs werden abgerufen.
4. Wählen Sie Aus **Jetzt Ausführen** Dient zum Durchführen einer ersten Ausführung der Vollsupport-Integration.
   Nach Abschluss des ersten Imports werden die geplanten Importe von Delta-Daten fortgesetzt.
   Informationen zu Status der Integrationsausführung finden Sie unter Zeigen Sie den Status der NVD-Integrationsimportausführung (National Vulnerability Database) an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

NIST National Vulnerability Database – API aktivieren (nur CPE)

Um CPE-Daten (Common Platform Enumeration) zu erfassen, können Sie einen vollständigen Datenimport mit einer täglichen geplanten Aufgabe durchführen.

Vorbereitungen

Die Integration von National Institute of Standards and Technology (NIST) National Vulnerability Database Integration (NVD)–API (nur CPE) erfasst (CPE) Daten, die ein formelles Namensformat, eine Methode zum Überprüfen von Namen mit einem System und ein Beschreibungsformat zum Binden von Text und Tests an einen Namen enthalten. Diese Informationen werden in einer Tabelle für angreifbare Software gespeichert.

Erforderliche Rolle: sn_vul.Vulnerability_admin oder App-SEC Manager

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **NVD** > **Integrationen**an.
2. Wählen Sie die Integration NIST National Vulnerability Database Integration–API (nur CPE) aus.
3. Aktivieren Sie die Checkbox **Aktiv**.
   - Die Integration ist so vorkonfiguriert, dass sie täglich ausgeführt wird. Das Ändern anderer Integrationsparameter erfordert beides ServiceNow Kompetenz und kann zu unvollständigen Daten führen.
   - Durch die Aktivierung dieser Integration werden automatisch die Integrationen NIST National Vulnerability Database Integration – API (nur CVE) und NIST National Vulnerability Database Integration – API (nicht zugeordnete CPE) aktiviert und das Feld „Ausführen“ auf „bei Bedarf“ festgelegt.
   - Darüber hinaus löst eine erfolgreiche Integrationsausführung der NIST National Vulnerability Database Integration – API (nur CPE) automatisch die NIST National Vulnerability Database Integration – API (nur CVE) aus. Und der erfolgreiche Abschluss der NIST National Vulnerability Database Integration – API (nur CVE) löst automatisch die NIST National Vulnerability Database Integration – API (nicht zugeordnete CPE) aus.

   Hinweis:
   Das Feld Import seit Datum in der Integration der NIST National Vulnerability Database – API (nur CPE) ist standardmäßig leer. Lassen Sie das Feld leer, um Daten der letzten 357 Tage abzurufen.

   Um Verlaufsdaten während des ersten Imports aus dem NVD-Scan abzurufen, legen Sie im Integrationsdatensatz der NIST National Vulnerability Database Integration – API (nur CPE) ein Startdatum fest.

   a. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**an.
   b. Wählen Sie NIST National Vulnerability Database Integration–API (nur CPE) Integration aus.
   c. Wählen Sie aus **Integrationsdetails** Registerkarte.
   d. Legen Sie fest **Importieren seit** Wert des Felds bis zum frühesten Datum, das Sie abrufen möchten. Bei jedem erfolgreichen Import wird dieses Datum auf das Datum und die Uhrzeit des ausgewählten Tages zurückgesetzt.
4. Wählen Sie Aus **Jetzt Ausführen** Dient zum Durchführen einer ersten Ausführung der Vollsupport-Integration.
   Nach Abschluss des ersten Imports werden die geplanten Importe von Delta-Daten fortgesetzt.
   Informationen zu Status der Integrationsausführung finden Sie unter Zeigen Sie den Status der NVD-Integrationsimportausführung (National Vulnerability Database) an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optionale Änderung und Aktivitäten der NVD-Integration

Konfigurieren Sie optionale Änderungen speziell für die NVD-Integrationen.

Hinweis:
Das Ändern anderer NVD-Integrationseinstellungen als der hier aufgeführten erfordert erweiterte Einstellungen ServiceNow Und Vulnerability Response Fachwissen und übersteigt den Umfang der Produktdokumentation.

Führen Sie einen manuellen NVD-Integrationsimport durch

Wenn Ihr anfänglicher Import fehlgeschlagen ist oder Sie nicht auf den geplanten anfänglichen Import warten möchten, können Sie unabhängig von der täglichen oder wöchentlichen geplanten Aufgabe einen vollständigen Datenimport durchführen.

Vorbereitungen

Hinweis:
Die Integrationen NIST National Vulnerability Database Integration – API (nur CPE) und NIST National Vulnerability Database Integration-API (nicht zugeordnete CPE) sind standardmäßig inaktiv. Siehe NIST National Vulnerability Database – API aktivieren (nur CPE) und Aktivieren Sie die NIST National Vulnerability Database – API (nicht zugeordnete CPE), um weitere Informationen zu erhalten.

Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **Administration** > **Integrationen**an.
2. Wählen Sie und Integration aus, z. B. die Integration der NIST National Vulnerability Database Integration – API (nur CVE).
3. Wählen Sie **Jetzt ausführen**.

   Hinweis:
   Wenn die Integration der NIST National Vulnerability Database Integration-API (nicht zugeordnete CPE) aktiviert ist, werden zugehörige CPE-Daten in der zugehörigen Liste „angreifbare Software“ des NVD-Schwachstelleneintrags gespeichert. Weitere Informationen finden Sie unter Vulnerability Response Formularfelder für Schwachstellen.

4. Informationen zu Status der Integrationsausführung finden Sie unter . Zeigen Sie den Status der NVD-Integrationsimportausführung (National Vulnerability Database) an.

Zeigen Sie den Status der NVD-Integrationsimportausführung (National Vulnerability Database) an

Verwenden Sie **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Korrekturentscheidungen zu unterstützen.

Vorbereitungen

So zeigen Sie den Status der Importausführung der NVD-Integration an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vulnerability Response Und die Integrationsanwendung Vulnerability Response mit NVD muss installiert und konfiguriert sein.
- Die NVD-Integrationsimporte müssen ausgeführt werden. Die NIST National Vulnerability Database Integration-API (nur CVE) Integration wird standardmäßig ausgeführt.

Hinweis:
Die Integrationen NIST National Vulnerability Database Integration-API (nur CPE) und NIST National Vulnerability Database Integration-API (nicht zugeordnete CPE) sind standardmäßig inaktiv. Siehe NIST National Vulnerability Database – API aktivieren (nur CPE) und Aktivieren Sie die NIST National Vulnerability Database – API (nicht zugeordnete CPE), um weitere Informationen zu erhalten.

Erforderliche Rolle: sn_vul.Vulnerability_admin oder App-SEC Manager

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter.

Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Der letzte verarbeitete Datensatz, der älter als eine Stunde ist, weist darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es ist eine Zeitüberschreitung aufgetreten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur

1. Wenn Sie das Statusdiagramm der NVD-Integrationsausführung nicht verwenden, Navigieren Sie zu **Alle** > **Vulnerability Response oder Application Vulnerability Response** > **Administration** > **Integrationen**an.
2. Wählen Sie ein aus **Link** Für eine Integration.
3. Wählen Sie aus **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste.
4. Überprüfen Sie, ob alle Importe erfolgreich waren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trouble?

Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:

- Netzwerkunterbrechung.
- Ein Problem bei der Datenübertragung, das zu beschädigten Daten während der Transformation führt.

Wenn eine dieser Bedingungen auftritt, wählen Sie aus **Jetzt Ausführen** , Und führen Sie die Integration erneut aus.

Zugehörige Informationen

Vulnerability Response Formularfelder für Schwachstellen

Fügen Sie CVEs zu Drittparteieinträgen hinzu

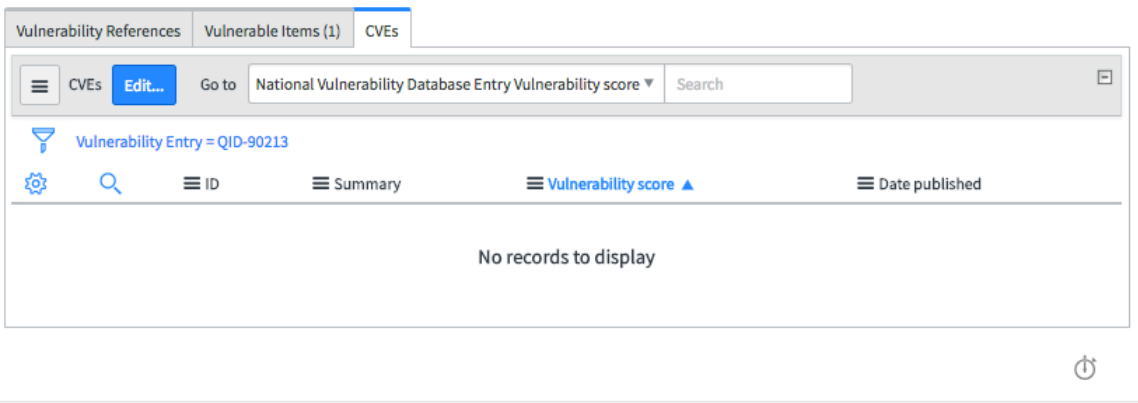
Informationen zu Common Vulnerability and Exposure (CVE) können sich auf eine einzelne Schwachstelle einer Drittpartei beziehen. Sie wird normalerweise während eines Drittanbieterintegrationsimports hinzugefügt, Sie können jedoch mehrere CVEs (Schwachstellen) manuell hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken** > **Drittpartei**an.
2. Öffnen Sie einen Datensatz.
3. Klicken Sie auf **CVEs** Registerkarte „zugehörige Liste“.



4. Klicken Sie auf **Bearbeiten**.
5. Wählen Sie aus, welche CVEs hinzugefügt werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können Bedingungsfilter verwenden, um die CVE-Sammlung zu verfeinern.

6. Klicken Sie auf **Speichern**.

Zugehörige Informationen

Vulnerability Response Formularfelder für Schwachstellen

Anzeigen Vulnerability Response Schwachstellenbibliotheken

Sie können Schwachstellendaten anzeigen, die aus der National Vulnerability Database (NVD), der Common Weakness Enumeration (CWE) oder Drittparteien importiert wurden, um zu entscheiden, ob eine Korrekturaufgabe eskaliert werden soll.

Vorbereitungen

Erforderliche Rolle: sn_vul.Remediation_owner

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken**an.

   Informationen zu bestimmten Feldern finden Sie unter Vulnerability Response Formularfelder für Schwachstellen.

   Die folgenden Bibliotheken sind verfügbar:

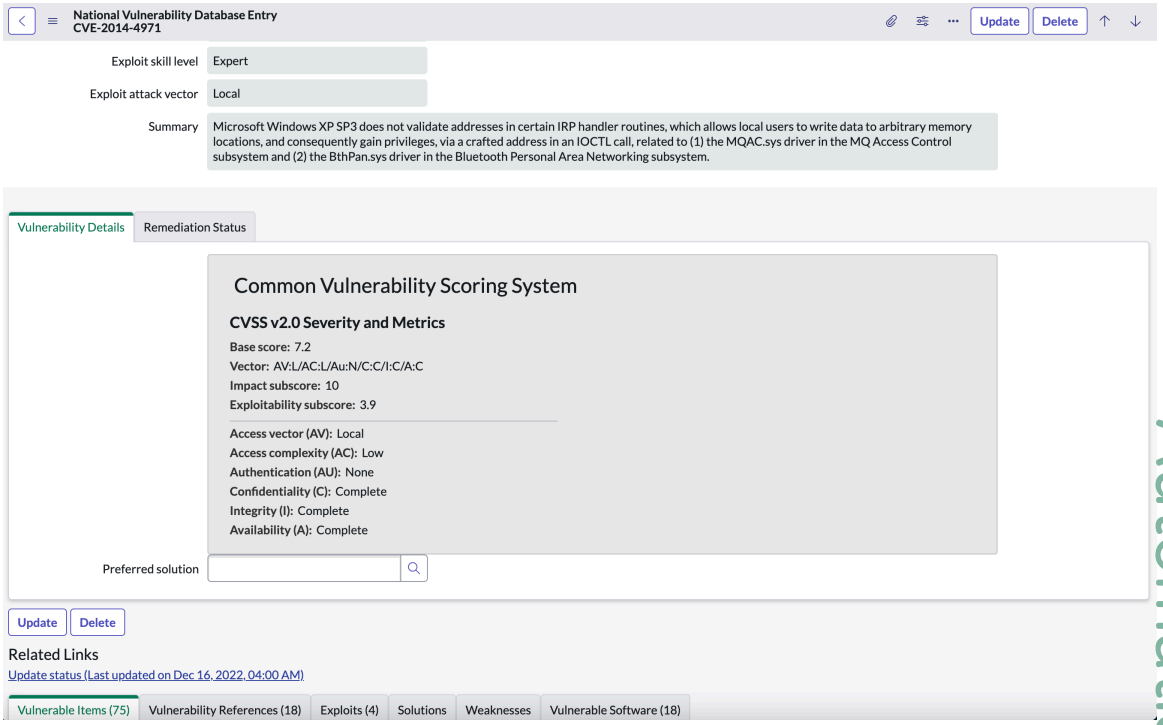
Bibliotheken	Beschreibung
NVD	Liste der von NVD gefundenen Schwachstellen und enthält Sicherheitsprüflisten, sicherheitsbezogene Softwarefehler, Fehlkonfigurationen, Produktnamen und Auswirkungsmetriken einschließlich Exploits.
CWE	Liste der in der Community entwickelten Softwareschwächungstypen. Jeder CWE-Datensatz enthält auch einen zugehörigen wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über den Bildschirm „Allgemeine Schwachstellenaufzählungen“ eskalieren. Sie dient nur als Referenz.
Drittpartei	Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste zugehöriger Referenzen, angreifbarer Elemente, Exploits und CVEs.

2. Wählen Sie eine Bibliothek aus, um Schwachstellen anzuzeigen.
3. Klicken Sie auf einen Link in der Liste, um einen Datensatz zu öffnen.

   Ein CVE-Datensatz in der Bibliothek „nationale Schwachstellen-Datenbankeinträge“. Weitere Informationen finden Sie in **Zugehörige Links** . Nach einem Datenimport können Sie eine Schwachstelle auswählen und ihre Beziehungen zu angreifbaren Elementen, Exploits, möglichen Lösungen, potenziellen Patches und Verweisen auf KB-Artikel in der HI Knowledge Base untersuchen. Wenn Vulnerability Solution Management Ist installiert,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können Sie eine bevorzugte Lösung in NVD-Datensätzen anzeigen, wenn einer verfügbar ist.



Integration von CISA Known Exploit Vulnerability (KEV)

Die Vulnerability Response Durch die Integration in den CISA-Katalog „Known Exploited Vulnerabilities“ (KEVs) werden Daten erfasst, mit denen Sie diese Schwachstellen effektiv priorisieren und beheben können.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

CISA ermöglicht die dringende und priorisierte Behebung aktiv ausgenutzter Schwachstellen für Behörden und Unternehmen.

Über CISA

Cybersecurity & Infrastructure Security Agency (CISA) ist eine US-amerikanische Sicherheitsbehörde für Cybersicherheit und Infrastruktur, die einen Bericht über die am häufigsten ausgenutzten Schwachstellen veröffentlicht. Es lässt sich problemlos in integrieren Vulnerability Response Dient zum Zuordnen von CVE-Schwachstellen (Common Vulnerabilities and Exposures), um die Daten in Ihrer Instanz zu ergänzen. Diese Informationen werden dann in der Tabelle „Drittanbieter-Schwachstelleneinträge“ zusammengefasst. Das früheste Fälligkeitsdatum wird für das Rollup zu den angreifbaren Elementen berücksichtigt.

Hinweis:
Die **CISA ist vorhanden** Kontrollkästchen für von CISA abgerufene CVEs.

Aus der CISA-Integration abgerufene Werte:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- CVE-ID
- Fälligkeitsdatum
- Hinzugefügt am
- Lieferant/Projekt
- Produkt
- Bekannte Ransomware (ab v21.0 von Vulnerability Response, Ein neues Feld **Bekannt für die Verwendung in Ransomware-Kampagnen** Wird aus dem CISA-Katalog „bekannte ausgenutzte Schwachstellen“ (KEVs) erfasst. Dies wird durch die Kennzeichnung von angezeigt **Bekannte Ransomware** Feld in der Datenbanktabelle „nationaler Schwachstelleneintrag“. Die Kennzeichnung wird auf der Ebene Common Vulnerabilities and Exposures (CVE) festgelegt und wird zum Drittparteieintrag (TPE) zusammengefasst.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Geplante Aufgaben

Die CISA-Integration wird automatisch als tägliche geplante Aufgabe aufgerufen. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response v 16.5, v18.0 Vulnerability Response Integration mit CISA v1.0, v1.2	

CISA-Integration anzeigen

Um die CISA-Integration anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Administration** > **Integrationen** > **CISA – Integration von Known Exploit Vulnerability**an.

Die folgenden Integrationen sind im Basissystem enthalten.

Hinweis:
Standardmäßig ist nur die CISA-Integration aktiv.

CISA-Integration

Integration	Beschreibung
Integration von Cybersicherheit und Infrastruktursicherheitsbehörde (CISA)	Ruft CISA-Schwachstellendaten (CVE) ab und ergänzt die vorhandenen Schwachstellendaten. Diese Integration wird automatisch auf die tägliche Ausführung festgelegt.

Informationen zum Anzeigen von Daten in Schwachstellen von Drittparteien finden Sie unter Anzeigen Vulnerability Response Schwachstellenbibliotheken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitung auf die CISA-Integration

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die CISA-Integration für bekannte ausgenutzte Schwachstellen setzt voraus, dass Sie mit der Cybersecurity & Infrastructure Security Agency (CISA) vertraut sind.

Erforderliche Rolle: sn_vul.Vulnerability_admin

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Hinweis:
Nehmen Sie vor der Ausführung der CISA-Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Installieren Sie ServiceNow® Vulnerability Response-Integration mit CISA-Anwendung

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit der bekannte Exploited Vulnerability Advisor der Cybersicherheit & Infrastructure Security Agency (CISA) in integriert werden kann Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.
Überprüfen Sie, ob Vulnerability Response Die Integration mit der NVD-Anwendung wird installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Installieren Sie Vulnerability Response Integration mit der NIST National Vulnerability Database.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist Anwender dem Schwachstellenmanager in zu Vulnerability Response. Für Informationen zu Gruppenrollen in Vulnerability Response Siehe , Verwalten Sie Persona und granulare Rollen für Vulnerability Response. • Der Schwachstellenmanager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich bei der Instanz an, die Sie installieren möchten Vulnerability Response integration with CISA Ein.
2. Navigieren Sie zum ServiceNow Store.
3. In ServiceNow Store, Suchen Sie nach Vulnerability Response integration with CISA Anwendung.
4. Wählen Sie die Anwendungskachel aus.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Erwägen Sie, das zu lesen **Andere Anforderungen** Und **Abhängigkeiten** Abschnitte, falls zutreffend.

5. Wählen Sie Aus **App Anfordern** Und geben Sie ein Now Support Anmeldeinformationen.
6. Wählen Sie Aus **Abrufen** .
7. Geben Sie ein **Instanzname** Und **Grund für die Instanz** , Und wählen Sie aus **Validieren Sie Die Instanz** .
8. Wählen Sie Aus **Anforderung** .
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**an.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen Sie dann aus **Installieren** .
    Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Nächste Maßnahme

Hinweis:
Für ist keine Konfiguration erforderlich CISA Integration.

Verständnis der EPSS-Integration (Exploit Prediction Scoring System)

Übersicht über die EPSS-Integration mit Vulnerability Response.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht über die Integration

Die EPSS-Integration (Exploit Prediction Scoring System) importiert EPSS-Daten im Zusammenhang mit allgemeinen Schwachstellen und Risiken (CVEs) aus First.org, um Schwachstellen zu priorisieren und zu beheben. Weitere Informationen finden Sie unter https://www.first.org . Das Exploit Prediction Scoring System (EPSS) ist eine datengesteuerte Maßnahme zur Schätzung der Wahrscheinlichkeit (Wahrscheinlichkeit), dass eine Software-Schwachstelle im Wildnis ausgenutzt wird. Das EPSS-Modell erzeugt eine Wahrscheinlichkeitspunktzahl zwischen 0 und 1 (0 und 100 %). Je höher die Punktzahl, desto größer ist die Wahrscheinlichkeit, dass eine Schwachstelle ausgenutzt wird.

Datenimporte aus der EPSS-Integration ergänzen die NVD-Daten in Ihrer Instanz weiter. Wenn keine NVD-Datensätze vorhanden sind, wird ein Platzhalter in der CVE-Tabelle erstellt und EPSS-Details in derselben Tabelle hinzugefügt. Führen Sie diese Integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

als Teil Ihres ersten Setups von aus Vulnerability Response Und vor dem Importieren von Schwachstellendaten in Ihre Instanz mit einem Scanner-Produkt eines Drittanbieters.

Wichtig:
Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist VR.System. Ändern Sie diesen Wert nicht.

Anfänglicher Import von Daten mit der EPSS-Integration

1. Führen Sie einen ersten Import von EPSS-Daten mit der EPSS-Integration First.org durch. Weitere Informationen finden Sie unter Konfigurieren Sie eine geplante Aufgabe, und führen Sie sie aus, um CVE-Datensätze mit EPSS-Daten zu aktualisieren.

   Wichtig:
   Sie führen EPSS-Updates durch **Täglich** Standardmäßig aus dem Integrationsdatensatz, und Sie müssen ihn konfigurieren, wenn er als geplante Aufgabe ausgeführt werden soll.

2. Drittparteibibliotheken werden als geplante Aufgaben aktualisiert. Weitere Informationen finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken.

   Wichtig:
   Es wird empfohlen, Integrationen der NIST National Vulnerability Database Integration – API (nur CVE) vor EPSS durchzuführen.

Führen Sie die EPSS-Importe durch, bevor Sie Schwachstellendaten mit einem Drittparteiprodukt importieren. Drittparteibibliotheken werden als geplante Aufgaben aktualisiert. Weitere Informationen zu Integrationen von Drittparteien finden Sie in der Integrationsdokumentation unter Vulnerability Response-Integrationen.

Wichtig:
Die folgende Integration ist im Basissystem enthalten. Die Integration ist standardmäßig aktiv.

Nach der ersten Ausführung werden die Integrationen automatisch in der Reihenfolge von geplanten Aufgaben des Basissystems ausgeführt. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Bei Aktivierung der EPSS-Integration werden die Felder EPSS-Punktzahl, EPSS-Perzentil und EPSS zuletzt geändert der Tabelle „Schwachstelleneinträge“ hinzugefügt. Für vorhandene CVEs werden diese Felder nach erfolgreichem Abschluss des ersten Importauftrags automatisch aktualisiert. Wenn neue CVEs der Tabelle „Schwachstelleneinträge“ nach Abschluss der geplanten EPSS-Aufgabe hinzugefügt werden, geben die neu hinzugefügten CVEs als Quelle EPSS an. Die Punktzahlen werden mithilfe des Basissystems zu vorhandenen TPEs aus CVEs aus der NVD-Tabelle zusammengefasst `Rollup EPSS score from NVD to TPEs calculator`. Sie können den Rechner auch ändern. Weitere Informationen finden Sie unter Vulnerability Response Rollup-Rechner.

Zugehörige Informationen

Erstellen Sie einen Vulnerability Response Rechner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie eine geplante Aufgabe, und führen Sie sie aus, um CVE-Datensätze mit EPSS-Daten zu aktualisieren

Passen Sie die geplante Aufgabe des Basissystems an, um CVE-Datensätze mit EPSS-Daten zu aktualisieren.

Vorbereitungen

Wichtig:
Sie müssen herunterladen und aktivieren Vulnerability Response integration with CISA Plugin (com.snc.Vulnerability.cisa) zum Aktivieren der EPSS-Integration.

Im Folgenden finden Sie die Liste der neuen Felder, die in der NVD-Tabelle zum Speichern von EPSS-Daten hinzugefügt wurden.

- EPSS-Punktzahl
- EPSS-Perzentil
- EPSS – Zuletzt geändert

Hinweis:
Konfigurieren Sie die Listenansicht oder Formularansicht entsprechend der Anforderung, um neu hinzugefügte Felder anzuzeigen.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Datenimporte aus der EPSS-Integration ergänzen die NVD-Daten in Ihrer Instanz weiter. Wenn keine NVD-Datensätze vorhanden sind, wird ein Platzhalter in der CVE-Tabelle erstellt und EPSS-Details in derselben Tabelle hinzugefügt. Führen Sie diese Integration als Teil Ihres ersten Setups von Vulnerability Response aus, und führen Sie den Import von Schwachstellendaten in Ihre Instanz durch.

Hinweis:
Standardmäßig befindet sich die EPSS-Integration First.org in **Aktiv** status. Die geplante Aufgabe des Basissystems ist standardmäßig so konfiguriert, dass sie täglich ausgeführt wird.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**an.
2. Suchen und wählen Sie First.org EPSS-Integration aus.
3. Ändern Sie die Felder nach Bedarf.
4. Klicken Sie mit der rechten Maustaste auf den Header zu **Speichern** Ihre Änderungen.
5. Wählen Sie Aus **Jetzt Ausführen** , Um die geplante Aufgabe sofort auszuführen.
   Sie kehren zur Ansicht Schwachstellenintegrationen zurück.
6. Auswahlvorgang **First.org-EPSS** > **Registerkarte „Ausführungen der Schwachstellenintegration“** Um den Fortschritt des Imports anzuzeigen.
   Nach erfolgreichem Abschluss der geplanten Aufgabe werden die EPSS-Punktzahlen, das Perzentil und die Zeitstempel der letzten geänderten EPSS-Punktzahl in den CVEs aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Weitere Informationen finden Sie unter Fügen Sie die EPSS-Punktzahlbedingung in der Business-Regel des Risikorechners hinzu.
- Siehe Anzeigen Vulnerability Response Schwachstellenbibliotheken Um die importierten Einträge anzuzeigen.

Fügen Sie die EPSS-Punktzahlbedingung in der Business-Regel des Risikorechners hinzu

Ändern Sie die Business-Regel, um dem Risikorechner eine EPSS-Punktzahlbedingung hinzuzufügen.

Vorbereitungen

Hinweis:
Das folgende Verfahren ist erforderlich, damit EPSS-Updates zu Schwachstellen ein Rolldown zu den angreifbaren Elementen durchführen können.

Erforderliche Rolle: sn_vul.manage_Risk_Score_Configuration

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regel**an.
2. Suchen Sie nach **Legen Sie die Kennzeichnung für die Neuberechnung fest** .

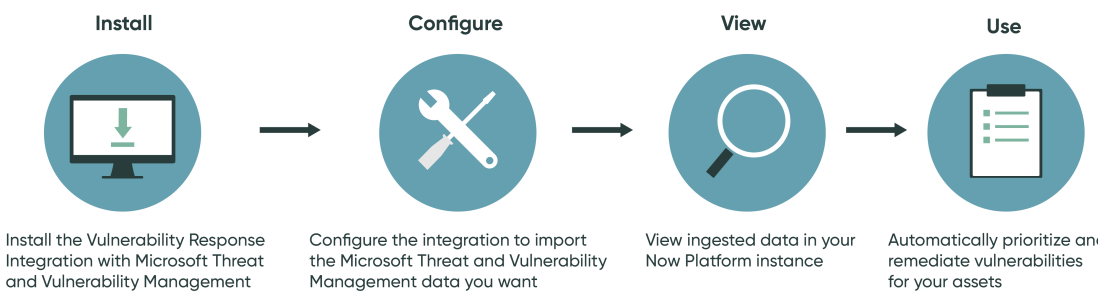
   Hinweis:
   Es gibt zwei `Set recalculate flag`Business-Regeln. Sie können beide verwenden.

3. Navigieren Sie zu **Zeitpunkt der Ausführung** Registerkarte.
4. Wählen Sie Aus **Fügen Sie die Klausel „ODER“ hinzu** Und wählen Sie aus `EPSS-Punktzahl` Von **Wählen Sie das Feld aus** Und `Changes` Von **Wählen Sie den Operator aus** Feld.
5. Wählen Sie **Aktualisieren**.

Verständnis der Integration von Microsoft Threat and Vulnerability Management Vulnerability

Die Vulnerability Response Die Integration mit Microsoft Threat and Vulnerability Management (MS TVM) verwendet Daten, die aus MS TVM importiert wurden, um Sie bei der Priorisierung und Behebung von Schwachstellen für Ihre Assets zu unterstützen. Die Anwendung ist mit einem separaten Abonnement als verfügbar ServiceNow Store.

Sie können die MS TVM Vulnerability-Integration verwenden, um Scannerdaten von Drittanbietern zu Ihren Assets und Schwachstellen zu importieren. Sie können dann Berichte zu Schwachstellen und angreifbaren Elementen im anzeigen Vulnerability Response Dashboards.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response Integration mit MS TVM v2.2	Weitere Informationen zu veröffentlichten Versionen der Vulnerability Response-Anwendung, zur Kompatibilität und zu Schemaänderungen finden Sie unter artikel „Vulnerability Response Compatibility Matrix“ und „Release Schemaänderungen“ [KB0856498] in der HI Knowledge Base .

Domänentrennung und MS TVM

Importieren Sie Schwachstellenintegrationsdaten in eine angegebene Domäne, indem Sie einem Anwender in dieser Domäne zuweisen, der die Integrationen ausführen soll. Informationen zum Erstellen von domänengetrennten Importen für die MS TVM Vulnerability Integration finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration.

Begriffe und wichtige Funktionen der Integrationen

Angreifbare Elemente und Schwachstellen

Ein angreifbares Element wird in erstellt ServiceNow AI Platform Instanz, wenn:

- Eine importierte Schwachstelle von einem Scanner eines Drittanbieters wird mit einem vorhandenen Asset (Konfigurationselement) in Ihrem abgeglichen CMDB). Das MS TVM-Produkt bezieht sich auf diese Übereinstimmungen als Schwachstellen.
- Eine importierte Schwachstelle von einem Scanner eines Drittanbieters wird nicht mit einem vorhandenen Asset in Ihrem abgeglichen CMDB. In diesem Fall wird auch ein nicht abgeglichenes Konfigurationselement (CI) mit einem angreifbaren Element erstellt.

  Verwenden Sie die Identification and Reconciliation Engine (IRE), um CIs in zwei neuen Klassen zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter CIs für werden erstellt Vulnerability Response Verwenden der Identifizierungs- und Abgleichsmodul.

Einträge für Drittpartei-Schwachstellen

Einträge von Drittanbieter-Schwachstellen werden aus Drittanbieterscannern wie MS TVM importiert und in der Tabelle „Drittanbieter-Schwachstelleneinträge“ in aufgeführt ServiceNow AI Platform Instanz. Außerdem werden National Vulnerability Database-Einträge (CVEs) aus MS TVM importiert. Die Exploit-Informationen, die diesen beiden Eintragstypen zugeordnet sind, stammen aus MS TVM. Diese Exploit-Informationen können für die Risikoberechnung verwendet werden.

Hinweis:
Eine Schwachstelle einer Drittpartei wird nur für Schwachstellen abgerufen, denen kein CVE zugewiesen ist. Ms TVM kann einen temporären Namen für die Schwachstelle hinzufügen, z. B. TVM-XXXX-XXXX . Dieser Name wird aktualisiert, nachdem eine CVE-ID zugewiesen wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationselement bzw. Configuration Item (CI)

CIs sind die vorhandenen Assets, die in aufgeführt sind CMDB.

Erkanntes Element

Erkannte Elemente sind die Assets, die aus dem MS TVM-Computer-Import erfasst werden und mit vorhandenen CIs in übereinstimmen CMDB.

Wenn keine Übereinstimmung gefunden wird, wird ein CI in der nicht abgeglichenen CI-Klasse von erstellt CMDB. Aktivieren Sie das Plugin „CMDB CI-Klassenmodelle“. Die Identification and Reconciliation Engine (IRE) erstellt CIs mithilfe neuer Klassen. Weitere Informationen finden Sie unter CIs für werden erstellt Vulnerability Response Verwenden der Identifizierungs- und Abgleichsmodul. Wenn das ursprüngliche, nicht übereinstimmende CI neu klassifiziert wird, werden die erkannten Elementdatensätze aktualisiert, um diesen Status widerzuspiegeln. Erkannte Elemente geben Ihnen Einblick, wie Assets identifiziert und CIs in zugeordnet werden CMDB.

CI-Suchregeln

Wenn Daten aus MS TVM importiert werden, Vulnerability Response Verwendet automatisch Computerdaten (Asset), um nach Übereinstimmungen in zu suchen CMDB. CI-Suchregeln werden verwendet, um CIs zu identifizieren und sie VI-Datensätzen hinzuzufügen, wenn VIS erstellt werden.

Instanz

Eine Instanz bezieht sich auf mehrere Accounts von MS TVM. Jeder Account kann eine Instanz in der MS TVM-Anwendung sein.

Integration

Eine Integration ist eine geplante Aufgabe, die Informationen aus einer Drittparteiquelle abruft, z. B. die Integration der MS TVM-Computer.

Bereitstellung

Wenn eine Integration mehrere Quellen unterstützt, wird eine einzelne Integration als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie mehrere MS TVM-Bereitstellungen in Ihrer Umgebung haben.

Die MS TVM-Integration umfasst auch die folgenden wichtigen Funktionen:

- Sie können die Assets in Ihrer Umgebung identifizieren und die CIs für Ihre vorhandenen erkannten Elemente, angreifbaren Elemente und Erkennungsdatensätze aktualisieren, um Ihnen weitere Details zu Ihren Schwachstellen zu geben.
- Sie können planen, wann die Aufträge für alle MS TVM-Integrationen ausgeführt werden sollen. Sie können geplante Aufgaben auch bei Bedarf ausführen.
- Sie können angreifbare Elemente gruppieren.
- Sie können CI-Suchregeln konfigurieren, um zu definieren, wie die Asset-Daten aus Drittparteiquellen zur Identifizierung von CIs in verwendet werden CMDB.

Erforderliche ServiceNow AI Platform-Rollen

Die Integrationsaufgaben erfordern die folgenden Rollen in Ihrem ServiceNow AI Platform Instanz.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Administrator

Der Systemadministrator verwendet den Setup-Assistenten, um die MS TVM-Anwendung zu installieren. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.Vulnerability_admin) und andere Rollen im Setup-Assistenten zu.

sn_vul.vulnerability_admin

Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der MS TVM-Integrationen im Setup-Assistenten ab. Diese Rolle hat vollständigen Zugriff auf Vulnerability Response Anwendung und ihre Datensätze. Der Schwachstellenadministrator konfiguriert alle Vulnerability Response Anwendungen und Regeln für installierte Drittanbieterintegrationen.

sn_vul_msft_tvm.configure_Integration

Diese Rolle enthält sn_vul_msft_tvm.read_Integration Granulare Rolle. Benutzer mit dieser Rolle können die#Vulnerability Response-Integration mit der Anwendung Microsoft Threat and Vulnerability Management konfigurieren.

sn_vul_msft_tvm.read_Integration

Benutzer mit dieser Rolle können die#Vulnerability Response-Integration nur mit den Datensätzen der Microsoft Threat and Vulnerability Management-Anwendung anzeigen.

Vulnerability Response-Gruppe

Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Anwender, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen sn_vul.read_all und sn_vul.Remediation_owner automatisch.

Ms TVM-Integrationen

Mehrere Quellen werden für alle MS TVM-Integrationen unterstützt. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in hinzufügen und bereitstellen Vulnerability Response. Sie installieren und konfigurieren auch Vulnerability Response Integration mit der MS TVM-Anwendung über den Setup-Assistenten.

Um die MS TVM-Integrationen anzuzeigen, navigieren Sie zu **Microsoft TVM-Schwachstellenintegration** > **Administration** > **Integrationen**. Vulnerability Response Bietet Integrationen mit MS TVM-Endpunkten, um die Daten gemäß den geplanten Zeitintervallen zu importieren. Die folgenden Integrationen sind im Basissystem enthalten.

Ms TVM-Integrationen

Ausführungssequer	Zeitplan	Integration	Beschreibung
1	Täglich	Integration von Microsoft TVM-Empfehlungen	Ruft eine Liste aller umsetzbaren Sicherheitsempfehlungen zum Beheben der Schwachstellen ab.
2	Täglich	Microsoft TVM Vulnerability (CVE)-Integration	Ruft eine Liste der nationalen Schwachstellen-Datenbankeinträge und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ms TVM-Integrationen (Fortsetzung)

Ausführungssequer	Zeitplan	Integration	Beschreibung
			Schwachstelleneinträge von Drittparteien sowie deren Exploit-Informationen ab.
3	Täglich	Integration von Microsoft TVM-Computern	Ruft alle Asset-(Computer-)Daten, einschließlich Computer-Tags, aus Microsoft TVM ab und verarbeitet sie in Ihrer Instanz.
4	Wöchentlich **Hinweis:** Nach der Installation wird diese Integration automatisch nach dem Import des Computers ausgeführt.	Microsoft TVM-Computer – Schwachstellen-Integration (vollständiger Import)	Ruft alle offenen Schwachstellen für alle Assets ab.
5	Täglich	Integration von Microsoft TVM-Computern mit Schwachstellen (Delta-Import)	Ruft alle Informationen ab, die sich im vollständigen Schwachstellenimport der Organisation geändert haben, einschließlich der neuen, behobenen und aktualisierten Schwachstellen.

Angreifbare Elemente werden gemäß den von Ihnen festgelegten Gruppenregeln in Korrekturaufgaben gruppiert und basierend auf Ihren Zuweisungsregeln zur Korrektur zugewiesen. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben und Vulnerability Response Übersicht über Zuweisungsregeln.

CI-Suchregeln

Wenn Daten aus MS TVM importiert werden, Vulnerability Response Verwendet automatisch Computerdaten (Asset), um nach Übereinstimmungen in zu suchen Configuration Management Database (CMDB). CI-Suchregeln werden verwendet, um CIs zu identifizieren und sie VI-Datensätzen hinzuzufügen, wenn VIS erstellt werden. Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Integrationen von Schwachstellen von Drittparteien.

Hinweis:
Sobald Sie eine Regel entfernt haben, können Sie sie nicht wiederherstellen. Anstatt eine vorhandene Regel zu entfernen, sollten Sie sie deaktivieren.

Die folgenden MS TVM-Suchregeln sind im Lieferumfang des Basissystems enthalten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MAC_ADDRESS
- FQDN
- IP

Hinweis:
Sie können mehrere Werte für IP_ADDRESS und MAC_ADDRESS eines Assets verwenden. Eine CI-Suchregel berücksichtigt alle Werte für den Abgleich.

Erkannte Elemente

Sie können die CIs anzeigen, die während eines Imports aus der Integration von MS TVM-Computern erkannt wurden.

Hinweis:
Der Standardfilter für diese Liste ist auf festgelegt Nicht Abgeglichen . Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Weitere Informationen finden Sie unter Erkannte Elemente.

Computer-Tags

Computer-Tags, auch als Host-Tags bezeichnet, werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie weisen Ihren Computern Tags zu.

Alle Computer-Tags werden als Teil der Integration von MS TVM-Computern importiert. Computer-Tags werden im Allgemeinen zum Filtern verwendet Vulnerability Response Zuweisungsregeln und Regeln für Korrekturaufgaben. Die Tags werden im Formular „erkanntes Element“ angezeigt.

Hinweis:
Führen Sie die MS TVM-Computerintegration aus, bevor Sie erstellen Vulnerability Response Regeln für Zuweisungs- oder Korrekturaufgaben in Vulnerability Response Anwendung, damit alle Tags für diese Regeln verfügbar sind, bevor angreifbare Elemente importiert und gruppiert werden. Beachten Sie auch die folgenden Punkte zu Tags:

- Beim Tag-Speicher wird die Groß-/Kleinschreibung nicht beachtet. Wenn ein Paris-Tag erstellt wird, kann kein PARIS-Tag in der Computer-Tag-Tabelle gespeichert werden. Paris Und PARIS Werden vom System als dasselbe Computer-Tag betrachtet. Welches Tag zuerst importiert wird, ist das Tag, das gespeichert und erkannt wird.
- Die Verwendung von Computer-Tags als Gruppenschlüssel in einer Korrekturaufgabenregel kann zu unerwarteten Ergebnissen führen. Gruppenschlüssel sind Spalten in der Tabelle „Korrekturaufgaben“, während Computer-Tags nur für die Verwendung im Bedingungsgenerator vorgesehen sind.
- Computer-Tags werden von der globalen Systemeigenschaft sn_vul.Import_Host_Tags gesteuert. Diese Eigenschaft ist auf festgelegt Wahr Standardmäßig. Durch das Deaktivieren von Tags werden sie für alle deaktiviert ServiceNow AI Platform® Instanzen.

Nächste Schritte

Nachdem Sie heruntergeladen haben Vulnerability Response Integration mit Microsoft Threat and Vulnerability Management aus dem ServiceNow® Store, Installation und Konfiguration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden vom Setup-Assistenten in unterstützt Vulnerability Response. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Vulnerability Response-Integration mit der MS TVM-Anwendung mithilfe des Setup-Assistenten.

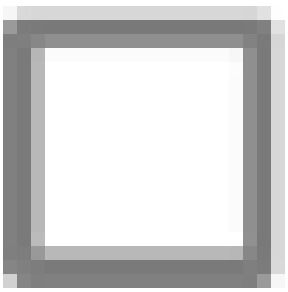
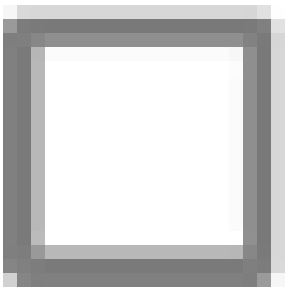
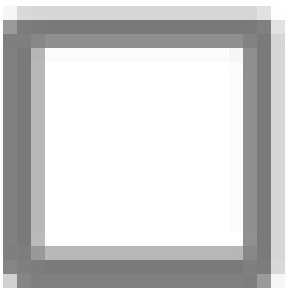
Vorbereitung auf die Microsoft Threat and Vulnerability Management Vulnerability Integration

Sie können sich auf vorbereiten ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) Schwachstellenintegration durch Ausführen von Setup-Aufgaben.

Bevor Sie mit der Verwendung einer Prüfliste beginnen

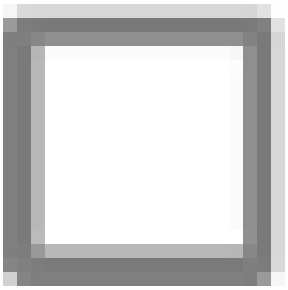
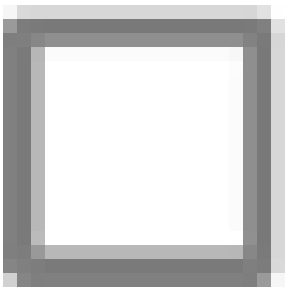
Zum Installieren und Konfigurieren von Vulnerability Response Durch die Integration mit der MS TVM-Anwendung können Sie die folgende Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Schwachstellendaten in importieren ServiceNow AI Platform® Instanz.

Prüfliste für Integrationsvorbereitung

Aufgabe	Beschreibung
	Stellen Sie sicher, dass Sie über eine der folgenden Informationen verfügen: • ClientSecret, clientId und TenantId für Ihren MS TVM-Account • Anwendername, Passwort, clientId und TenantId für Ihren MS TVM-Account. Informationen zu diesen Informationen finden Sie unter Einrichten Microsoft Azure für die MS TVM-Integration.
	Wenn nicht bereits installiert und aktiviert, installieren Sie Vulnerability Response Anwendung, bevor Sie die Drittanbieteranwendung installieren. Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe Vulnerability Response installieren. Diese Integration erfordert Version 14,0 von Vulnerability Response Oder später.
	Wenn Sie die Anwendung noch nicht in Ihrer Instanz haben, rufen Sie Berechtigungen ab, und laden Sie herunter Vulnerability Response Integration mit MS TVM-Anwendung in Ihren ServiceNow AI Platform® Instanz. Weitere Informationen finden Sie unter .

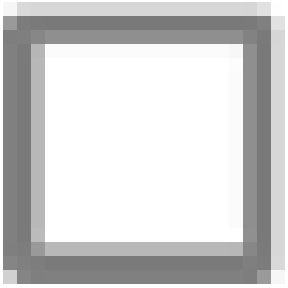
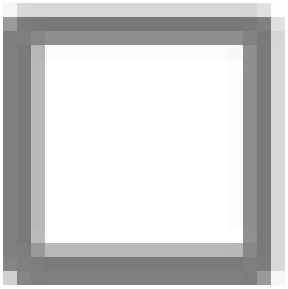
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für Integrationsvorbereitung (Fortsetzung)

Aufgabe	Beschreibung
	Schätzen Sie die Anzahl der angreifbaren Elemente, die Sie importieren möchten. Überprüfen Sie, ob Ihre Instanz die Anzahl der angreifbaren Elemente akzeptieren kann, die Sie importieren möchten. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an ServiceNow® Technischer Support.
	Stellen Sie sicher, dass Sie über die folgenden Gruppen oder Anwender verfügen, um die Integrationen zu verwalten und angreifbare Elemente zu beheben: **Administrator** Verwendet den Setup-Assistenten, um die Vulnerability Response-Integration mit der MS TVM-Anwendung zu installieren. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.Vulnerability_admin) und andere Rollen im Setup-Assistenten zu. **sn_vul.vulnerability_admin** Schließt die Konfiguration der MS TVM-Integration ab. Diese Rolle hat vollständigen Zugriff auf Vulnerability Response(VR)-Anwendung und ihre Datensätze. Dieser Administrator konfiguriert alle VR-Anwendungen und -Regeln und konfiguriert Integrationen von Drittparteien. **sn_vul_msft_tvm.configure_Integration** Konfiguriert die MS TVM Vulnerability Integration. Diese Rolle enthält die granulare Rolle sn_vul_msft_tvm.read_Integration. **sn_vul_msft_tvm.read_Integration** Zeigt Datensätze der MS TVM Vulnerability Integration an (liest). **Vulnerability Response-Gruppe** Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Anwender, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen sn_vul.read_all und sn_vul.Remediation_owner automatisch. Wenn Sie noch nicht erstellt haben, können Sie zusätzliche Gruppen erstellen und Anwender mit dem Modul „Anwenderverwaltung“ in Ihrer Instanz hinzufügen, bevor Sie den Setup-Assistenten verwenden. Weitere Informationen finden Sie unter Erstellen Sie eine Anwendergruppe . Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender in tun und sehen können Vulnerability Response Anwendung. Informationen zur anfänglichen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für Integrationsvorbereitung (Fortsetzung)

Aufgabe	Beschreibung
	Installieren Sie Vulnerability Response Integration mit NVD und Ausführen der NIST National Vulnerability Database Integration – API (nur CVE).
	Um eine verbesserte Leistung für Ihren ersten Import heraufzustufen, können Sie bestimmte Funktionen, Regeln oder Aufträge in Ihrer Instanz deaktivieren. • Deaktivieren Sie Schwachstellen-Rechner, wenn Sie sie nicht verwenden. Diese Rechner sowie alle von Ihnen definierten Rechner werden jedes Mal ausgeführt, wenn ein Datensatz für angreifbare Elemente erstellt oder aktualisiert wird. Weitere Informationen finden Sie unter Deaktivieren Sie den standardmäßigen Schwachstellenrechner, wenn er nicht verwendet wird . • Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung der Erfassung auswirken kann.

Sie sind bereit für Installieren und konfigurieren Sie die Vulnerability Response-Integration mit der MS TVM-Anwendung mithilfe des Setup-Assistenten.

Einrichten Microsoft Azure für die MS TVM-Integration

Richten Sie Ihren Account in ein Microsoft Azure-Portal für Remote-Zugriff auf die Microsoft Threat and Vulnerability Management (MS TVM)-API. Sie benötigen diesen Account, damit Sie auf den MS TVM-Mandanten zugreifen können, um Informationen zu Computern, Schwachstellen und Sicherheitsempfehlungen zu sammeln.

Vorbereitungen

Erforderliche Rolle: Microsoft Azure-Portal-Administrator.

Warum und wann dieser Vorgang ausgeführt wird

Führen Sie die folgenden Setup-Aufgaben in Ihrem aus Microsoft Azure-Portal, bevor Sie installieren ServiceNow® Anwendung für diese Integration.

Informationen zum Überprüfen, ob Sie Zugriff auf den neuesten Inhalt haben, finden Sie unter Microsoft-Dokument Website. Wenn Sie keine Anwendungs-ID für die OAuth 2,0-Authentifizierung in erstellt haben Microsoft Azure-Portal befolgen Sie die Schritte in diesem Verfahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich bei an Microsoft Azure-Portal mithilfe Ihrer Azure-Portal-Administrator-Anmeldeinformationen.
2. Klicken Sie im linken Navigationsbereich im Startbereich auf **Azure Active Directory** .
3. Klicken Sie im Übersichtsbereich auf **App-Registrierungen (Vorschau)** .
4. Klicken Sie im Bereich App-Registrierungen (Vorschau) auf **Neue Registrierung** .
   Das Formular „Anwendung registrieren“ wird angezeigt.
5. Füllen Sie im Formular die Felder aus.

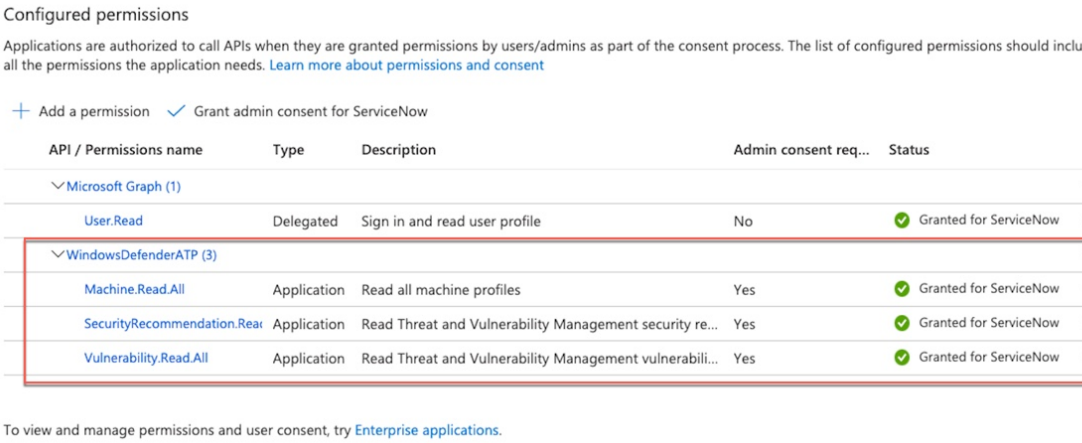
Registrierungsformular für ein Anwendungsformular

Feld	Beschreibung
Name	Name für die Anwendung. In diesem Beispiel ServiceNow MS TVM-Integration Ist eingegeben.
Unterstützte Account-Typen	Klicken Sie für diesen Account unter unterstützte Account-Typen auf **Accounts nur in diesem Organisationsverzeichnis (nur ServiceNow – einzelner Mandant)** .
Umleitungs-URL (optional)	Wenn Sie einen Wert für dieses Feld eingeben, wird er nicht von der Integration verwendet.

6. Klicken Sie auf **registrieren**.
   Die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) werden erstellt. Geben Sie diese Werte auf der Konfigurationsseite in ein **Client-ID** Und **Mandanten-ID** Felder während des Konfigurationsschritts in ServiceNow Setup-Assistent für VR-TVM-Integration. Dieser Schritt wurde in beschrieben Installieren und konfigurieren Sie die Vulnerability Response-Integration mit der MS TVM-Anwendung mithilfe des Setup-Assistenten.
7. Wenn die Anwendungs-ID (Client) in angezeigt wird ServiceNow Ms TVM-Integrationsbereich klicken Sie auf **Zeigen Sie API-Berechtigungen an** .
8. Navigieren zu **API-Berechtigungen anfordern** > **APIs, die meine Organisation verwendet**, Und klicken Sie dann auf **Windows Defender ATP** .
9. Klicken Sie im Bereich „ServiceNow MS TVM-Integration – API-Berechtigungen“ auf **Fügen Sie eine Berechtigung hinzu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Gewähren Sie Lesezugriff auf Computer, Schwachstellen und



Sicherheitsempfehlungen.

11. Klicken Sie Auf **Erteilen Sie die Zustimmung des Administrators für <Name Ihrer Organisation>** .

Hinweis:
Dient zur Authentifizierung als Anwendung von ServiceNow Führen Sie die folgenden Aktionen aus:

a. Navigieren zu **ServiceNow MS TVM-Integration** > **Zertifikate Und Geheimnisse**, Und klicken Sie dann auf **Neues geheimes Clientgeheimnis** .

b. Füllen Sie im Formular die Felder aus.

Formular „geheime Clientschlüssel“

Feld	Beschreibung
Beschreibung	Name der Anwendung.
Läuft ab	Ablaufdatum.

c. Klicken Sie auf **Hinzufügen**.

Die **Wert** Das Feld wird mit dem neuen geheimen Client ausgefüllt, dem neuen Passwort.

Hinweis:
Sie benötigen dieses Passwort, wenn Sie die Integration in konfigurieren ServiceNow AI Platform Instanz. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie die Vulnerability Response-Integration mit der MS TVM-Anwendung mithilfe des Setup-Assistenten.

d. Speichern Sie dieses Passwort an einem sicheren Ort. Nachdem Sie diese Seite verlassen haben, ist dieses Passwort nicht verfügbar.

Sie haben erfolgreich eine Anwendungs-ID für die Authentifizierung in erstellt Microsoft Azure-Portal.

Nächste Maßnahme

Sie sind bereit, Ihren einzurichten ServiceNow AI Platform® Instanz für die Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie die Vulnerability Response-Integration mit der MS TVM-Anwendung mithilfe des Setup-Assistenten

Installieren und konfigurieren Sie Vulnerability Response Integration mit Microsoft Threat and Vulnerability Management (MS TVM), damit Sie die aus MS TVM importierten Daten verwenden können, um Schwachstellen für Ihre Assets zu priorisieren und zu beheben.

Vorbereitungen

Bevor Sie ausführen ServiceNow® Microsoft Threat and Vulnerability Management Vulnerability Integration müssen Sie die Anwendung Vulnerability Response Integration mit Microsoft Threat and Vulnerability Management von herunterladen ServiceNow Store Und installieren und konfigurieren Sie es mit dem Setup-Assistenten in Vulnerability Response Anwendung.

Bevor Sie die MS TVM-Anwendung installieren, überprüfen Sie, ob Sie alle Elemente in abgeschlossen haben Vorbereitung auf die Microsoft Threat and Vulnerability Management Vulnerability Integration Prüfliste. Informationen zum Einrichten von finden Sie Microsoft Azure-Account, siehe Einrichten Microsoft Azure für die MS TVM-Integration.

Erforderliche Rollen:

- administrator für die anfängliche Zuweisung der Rolle „sn_vul.Vulnerability_admin“ und die Installation der Microsoft-Anwendung „Bedrohungs- und Schwachstellenmanagement“ im Setup-Assistenten
- Schwachstellenadministrator (sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)), um die Anwendung im Setup-Assistenten nach der Installation zu konfigurieren.

Warum und wann dieser Vorgang ausgeführt wird

Führen Sie das folgende Verfahren aus, bevor Sie die MS TVM-Integration installieren und konfigurieren.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung**an.

   Nach einigen Minuten werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz verfügbar sind.

2. Suchen Sie nach **Microsoft Bedrohungs- und Schwachstellenmanagement** Kachel und klicken Sie auf **Installieren** .

   Die Vulnerability Response Integration mit Microsoft Threat and Vulnerability Management-Anwendung, die Sie aus dem heruntergeladen haben ServiceNow Store Ist installiert.

3. Befolgen Sie die Anweisungen im Setup-Assistenten, um mit der Installation fortzufahren.
   Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.

Nächste Maßnahme

Nachdem Sie die Installation im Setup-Assistenten abgeschlossen haben, navigieren Sie zu **Integrationskonfiguration** > **Scannerintegrationen** In Setup-Assistent, um mit der Konfiguration fortzufahren. Weitere Informationen zur Ergänzung der im Setup-Assistenten bereitgestellten Hinweismeldungen finden Sie unter Konfigurieren Sie die MS TVM Vulnerability Integration mit dem Setup-Assistenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenabrufeinstellungen für die Microsoft Threat and Vulnerability Management Integration

Sie können Datenabrufeinstellungen verwenden, um den Typ und den Umfang der Daten zu bestimmen, die Sie aus importieren möchten ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) Schwachstellenintegration in Ihren ServiceNow AI Platform® Instanz.

Mit den Einstellungen für den Datenabruf können Sie die Daten steuern, die Sie importieren möchten. Sie können die Werte dieser Filter in Integrationsinstanzen festlegen. Um die Integrationsinstanzen anzuzeigen, navigieren Sie zu **Microsoft Threat and Vulnerability Management Vulnerability Integration** > **Integrationsinstanzen** Und klicken Sie auf Ihre MS TVM-Integration.

Klicken Sie auf der Seite „Integrationsinstanz“ auf **Integrationsinstanzparameter** Um eine Liste von Parametern anzuzeigen, oder klicken Sie auf **Schwachstellenintegrationen** Registerkarte für einen Zeitplan, REST-Details, Integrationsdetails, Datenquellen und Informationen zur Integrationsausführung.

Einstellungen und Filter für den Datenabruf für die MS TVM-Integrationen in Ihrem ServiceNow AI Platform Instanz

Die folgenden Einstellungen sind für die MS TVM-Integrationen in Ihrem verfügbar ServiceNow AI Platform Instanz. Diese und andere Konfigurationseinstellungen werden auf der Seite „Integrationsinstanz“ von angezeigt ServiceNow AI Platform Instanz. Möglicherweise möchten Sie diese Einstellungen für die ersten Integrationsausführungen in ihren Standardeinstellungen belassen.

MS TVM.

vi_size_limit

Definiert die Anzahl der Datensätze angreifbarer Elemente, die in den Ergebnissatz aus der Integration von MS TVM-Computer-Schwachstellen aufgenommen werden sollen. Diese Einstellung muss im int32-Format vorliegen. Der Standardwert ist 2.000.

Schwachstellen_size_limit

Definiert die Anzahl der Schwachstellendatensätze, die in den Ergebnissatz aus der Integration von MS TVM Vulnerability (CVE) aufgenommen werden sollen. Diese Einstellung muss im int32-Format vorliegen. Der Standardwert ist 2.000.

Recommendations_size_limit

Definiert die Anzahl der Schwachstellendatensätze, die in den Ergebnissatz aus der Integration von MS TVM-Empfehlungen aufgenommen werden sollen. Diese Einstellung muss im int32-Format vorliegen. Der Standardwert ist 2.000.

Asset_size_limit

Definiert die Anzahl der Schwachstellendatensätze, die in den Ergebnissatz aus der Integration von MS TVM-Computern aufgenommen werden sollen. Diese Einstellung muss im int32-Format vorliegen. Der Standardwert ist 2.000.

Machine_Filter

Filtert die Computer, die von MS TVM stammen. Dieser Filter wird auf die Integration von MS TVM-Computern angewendet. Der Standardwert besteht darin, Computer einzubeziehen, auf denen onBoardingStatus „Onboarding“ lautet.

REST-Nachrichten für die Microsoft Threat and Vulnerability Management Vulnerability Integration

Sie können die REST-Nachrichten für verwenden ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM) Vulnerability Integration zum Durchführen von Aufrufen der MS TVM API.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ms TVM-Zugriffstoken

Sie können auch die REST-Nachrichten für das MS TVM-Zugriffstoken verwenden, um das Zugriffstoken aus der MS TVM-API abzurufen, damit Sie REST-API-Anforderungen authentifizieren können. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Authentifizierungsanforderungen an MS TVM aus.

Ms TVM-Integration

Sie können die REST-Nachricht für die MS TVM-Integration verwenden, um Informationen aus MS TVM abzurufen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen aus, die an MS TVM zum Abrufen von Informationen gestellt werden. REST-Nachrichten enthalten die folgenden REST-Methoden.

REST-Methoden

REST-Methode	Beschreibung der Methode
Schwachstellen ABRUFEN	Ruft Informationen zu Schwachstellen und Exploit aus MS TVM ab.
RUFT Softwareschwachstellen nach Computer ab	Ruft alle offenen Schwachstellen ab.
RUFEN SIE Empfehlungen ab	Ruft die Liste aller umsetzbaren Sicherheitsempfehlungen ab, die sich auf die Organisation auswirken.
Computer ABRUFEN	Ruft die Sammlung von Assets ab.
RUFT Änderungen an Softwareschwachstellen nach Computer ab	Ruft alle Informationen ab, die sich im vollständigen Schwachstellenimport der Organisation geändert haben, einschließlich neuer, behobener und aktualisierter Schwachstellen.

Datentransformation für die Microsoft Threat and Vulnerability Management Vulnerability Integration

Nachdem Sie die Daten identifiziert haben, die Sie importieren möchten, werden die Daten aus dem abgerufen ServiceNow® Microsoft Threat and Vulnerability Management (MS TVM)-Anwendung, die über eine Reihe von Datenquellen verarbeitet und in Ihrer Instanz umgewandelt wurde.

Während der Installation werden normalisierte Schweregradzuordnungen im Modul „normalisierte Schweregradzuordnung“ installiert. Diese Zuordnungstransformation importiert Microsoft Schweregradstufen von Drittpartei-Schwachstellen auf Standardschweregrade für die Verarbeitung in Ihrer Instanz. Informationen zum Erstellen von Schweregradzuordnungen finden Sie unter Erstellen Sie einen Vulnerability Response Schweregradzuordnung.

Ms TVM-Computer-Import

Die Daten von den importierten Computern werden zuerst in die Tabelle „MS TVM-Computer-Import“ [sn_vul_msft_tvm_Machines_Import] geladen.

Die MS TVM-Computer-Transformation wird verwendet, um die Informationen zu importierten Computern zu transformieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem MS TVM-Computer-Import verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie nach **Microsoft TVM-Computer-Transformation** .

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Ms TVM-Computer transformieren Zuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Eindeutige ID für Assets. Diese ID ist der Source_ID des erkannten Elementdatensatzes zugeordnet.
u_ipaddresses.macAddress	mac_address	MAC-Adresse, die von der API dem Host-mac-Adressfeld des cmdb_ci-Datensatzes zugeordnet ist.
u_ipaddresses.ipAddress	ip_address	IP-Adressfeld, das dem IP-Adressfeld des cmdb_ci-Datensatzes zugeordnet ist.
u_lastseen	Last_Scan_date	Feld, das dem Feld Last_Scan_date im erkannten Elementdatensatz zugeordnet ist.
u_machinetags		Tags, die in sn_sec_cmn_Host_Tag gespeichert werden. Die Zuordnung von Tags zu Assets wird in sn_sec_cmn_m2m_src_ci_Tag gespeichert.
u_osplatform	os	Feld, das dem bs-Feld im cmdb_ci-Datensatz zugeordnet ist.
u_computerdnsName	fqdn	Feld, das das dnsname-Feld aus der API dem fqdn-Feld im cmdb_ci-Datensatz zuordnet.

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

Ms TVM-Computer transformieren die Zeitplanung und den Zweck des Zuordnungsskripts

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde).	Skript, das zum Initialisieren der Werte in der Bereichsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
	zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Skript, das verwendet wird, um Werte im Host zu aktualisieren und zu überprüfen, ob der Host vorhanden ist. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Bereichsvariablen (sn_vul_msft_tvm). Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten CIs verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Die Skripteinbindung MicrosoftTVMMachinesProcessor wird aus dem onBefore-Transformationsskript aufgerufen. Es übernimmt die Ausgabe aus der Integration der Microsoft TVM-Computer und wandelt sie in ein CI um. Alle Änderungen an dieser Skripteinbindung können die Transformation der Daten der Microsoft TVM-Computer in der CI- und erkannten Elementtabelle ändern.

Integration von MS TVM-Schwachstellen

Die importierten Schwachstellendaten werden zuerst in die Tabelle Microsoft TVM CVE (Schwachstellen) Import [sn_vul_msft_tvm_Vulnerabilities_Import] geladen.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem MS TVM-Schwachstellenimport verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie nach **Microsoft TVM-Schwachstellen – Transformation** .

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Microsoft TVM-Schwachstellen transformieren Zuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_id	id	Ordnet der ID-Spalte des Datensatzes „sn_vul_entry“ zu.
u_severity	Source_severity	Ordnet das Feld Schweregrad dem Schweregrad zu. Der Standardwert ist 5.
u_publishedon	date_published	Ordnet das Feld u_publishedon dem Veröffentlichungsdatum zu.
u_publicexploit	Public_Exploit	Ordnet das vom Scanner bereitgestellte u_publicexploit der Spalte „öffentlicher Exploit“ in der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft TVM-Schwachstellen transformieren Zuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
		Tabelle „Schwachstelleneintrag“ zu.
u_cvssv3	V3_Base_Score	Ordnet die cvssv3-Punktzahl der v3-Basispunktzahl im Schwachstelleneintragsdatensatz zu.
u_description	Zusammenfassung	Ordnet die Beschreibung dem Zusammenfassungsfeld im Schwachstelleneintragsdatensatz zu.
u_exploitinkit	malware_kit	Ordnet das Feld u_exploitinkit dem Malware-Kit in der Exploit-Tabelle zu.
u_exploittypes	type	Ordnet den Exploit-Typ dem Typ in der Exploit-Tabelle zu.
u_exploitverifiziert	Ist_Exploit_verifiziert	Ordnet das Feld u_exploitverifiziert dem verifizierten Exploit in der Exploit-Tabelle zu.
u_exploituris	Exploit_Links	Ordnet das Feld u_exploituris den Exploit-Links in der Exploit-Tabelle zu.

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde).	Skript, das zum Initialisieren der Werte in der Bereichsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Erstellen oder Aktualisieren der Werte in der NVD- oder der Drittpartei-Eintragstabelle verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Werte der neu erstellten Elemente und der Elemente verwendet wird, die aktualisiert und ignoriert wurden. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Import von ms TVM-Empfehlungen

Die importierten Empfehlungsdaten werden zuerst in die Tabelle „MS TVM-Empfehlungsimport“ [sn_vul_msft_tvm_Recom_Import] geladen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie die Daten aus dem Import von MS TVM-Empfehlungen verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie nach **Ms TVM-Empfehlungstransformation** .

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Ms TVM-Empfehlung – Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_RecommendedVendor	Recommended_Vendor	Ordnet das Feld u_empfehlendVendor der Spalte Lieferant zu.
u_Schwachstellen	Schwachstellen	Ordnet das Feld u_schwachstellen der Spalte Schwachstellen zu.
u_exposedMachinescount	src_exponiert_Machines_cnt	Ordnet das Feld u_exposedmachinescount der Spalte „Anzahl der gefährdeten Computer“ zu.
u_status	status	Ordnet den Status dem Feld Status im Empfehlungsdatensatz zu.
u_productname	product_name	Ordnet das Feld u_productname dem Produktnamen im Empfehlungsdatensatz zu.
u_nonproductiv_impactedAssets	Non_prod_Impact_Assets	Ordnet das Feld u_nonproductiv_impactedAssets der Spalte Betroffene Assets im Empfehlungsdatensatz zu.
u_activeAlert	Active_Alert	Ordnet das Feld u_activeAlert der Spalte aktive Warnung im Empfehlungsdatensatz zu.
u_RecommendedVersion	Recommended_Version	Ordnet das Feld „u_ommendedversion“ der Spalte „empfohlene Version“ im Empfehlungsdatensatz zu.
u_totalmachinecount	Total_MACHINE_count	Ordnet das Feld u_totalmachinecount der Spalte Gesamtanzahl der Computer im Empfehlungsdatensatz zu.
u_Exposureimpact	Exposure_Impact	Ordnet das Feld u_exposure-eimpact der Spalte „Risikoauswirkung“ im Empfehlungsdatensatz zu.
u_Recommendationname	Empfehlungsname	Ordnet das Feld u_Recommendationname der Spalte Empfehlungsname im Empfehlungsdatensatz zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ms TVM-Empfehlung – Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_Unterkategorie	Unterkategorie	Ordnet das Feld u_subcategory der Spalte Unterkategorie im Empfehlungsdatensatz zu.
u_id	source_id	Ordnet die Empfehlungs-ID aus MS TVM der Spalte „Quell-ID“ zu.
u_remediationtype	Remediation_type	Ordnet das Feld u_remediationtype der Spalte „Korrekturtyp“ im Empfehlungsdatensatz zu.
u_relatedcomponent	Related_component	Ordnet das Feld „u_relatedcomponent“ der Spalte „zugehörige Komponente“ im Empfehlungsdatensatz zu.
u_Recommendedprogram	Recommended_program	Ordnet das Feld u_recommended dprogram der Spalte „Empfohlenes Programm“ im Empfehlungsdatensatz zu.
u_Recommendationcategory	Recommendation_category	Ordnet das Feld u_Recommendationcategory der Spalte Empfehlungskategorie im Empfehlungsdatensatz zu.
u_publicexploit	Public_Exploit	Ordnet das Feld u_publicexploit der Spalte „Public Exploit“ im Empfehlungsdatensatz zu.
u_vendor	Lieferant	Ordnet das Feld u_Vendor der Spalte Lieferant im Empfehlungsdatensatz zu.
[Skript]	Integration_instance	Name der Instanz, aus der die Empfehlung importiert wird.
[Skript]	sys_domain	Domäne, in die dieser Datensatz importiert wird.

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

Zuordnungsskript für ms TVM-Empfehlung umwandeln

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde).	Skript, das zum Initialisieren der Werte in der Bereichsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Skript, das verwendet wird, um Werte in den Empfehlungen zu aktualisieren und zu überprüfen, ob die Empfehlungen vorhanden sind. Dieses Skript ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungsskript für ms TVM-Empfehlung umwandeln (Fortsetzung)

Wenn das Skript ausgeführt wird	Zweck
	zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Werte von Elementen verwendet wird, die erstellt, aktualisiert und ignoriert wurden. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Import von MS TVM-Computer-Schwachstellen

Die Transformationszuordnung für Schwachstellen auf MS TVM-Computern wird verwendet, um Informationen zu offenen und behobenen Schwachstellen zu transformieren, die aus MS TVM importiert werden.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem MS TVM-Computer-Schwachstellenimport verarbeitet werden.

Um auf die Transformationszuordnungen „offene und behobene Schwachstellen“ von MS TVM zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie nach **Ms TVM-Computer-Schwachstellen – Transformation** .

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Ms TVM-Computer-Schwachstellen transformieren Zuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_id	Erkennungsschlüssel	Ordnet das Feld u_ID der Spalte Erkennungsschlüssel in der Erkennungstabelle zu.
u_diskpfade	Nachweis	Ordnet das Feld u_diskpaths der Nachweisspalte in der Erkennungstabelle zu.
u_Registrypaths	Nachweis	Ordnet das Feld u_registrypaths der Nachweisspalte in der Erkennungstabelle zu.
u_Recommendedsecurityupdateid	Preferred_Solution	Ordnet das Feld u_ommendedsecurityupdateid der Spalte bevorzugte Lösung in der Tabelle „angreifbare Elemente“ zu, wenn die Lösung mit derselben ID in der Tabelle „sn_vul_Solution“ vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ms TVM-Computer-Schwachstellen transformieren Zuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_Recommendationreference	Empfehlung	Ordnet das Feld u_Recommendationreference der Spalte Empfehlung in der Tabelle für angreifbare Elemente zu.
u_cveid	Schwachstelle	Ordnet das Feld u_cveid der Spalte Schwachstelle in der Tabelle „angreifbare Elemente“ zu.
u_status	Source_Status	Ordnet das Feld u_Status der Spalte Quellstatus in der Erkennungstabelle zu.
u_eventtimestamp	Temporal_Punktzahl	Ordnet das Feld „u_eventtimestamp“ der Spalte „zuletzt gefunden“ in der Tabelle „angreifbare Elemente“ zu.
u_lastseentimestamp	last_seen	Ordnet das Feld „u_lastseentimestamp“ der Spalte „zuletzt gesehen“ in der Tabelle „angreifbare Elemente“ zu.
u_firstseentimestamp	first_seen	Ordnet das Feld u_firstseentimestamp der ersten Spalte in der Tabelle „angreifbare Elemente“ zu.
u_RecommendedsecurityUpdate	Solution_Summary	Ordnet das Feld u_ommendedsecurityUpdate der Spalte „Lösungszusammenfassung“ in der Tabelle „angreifbare Elemente“ zu.
u_Recommendedsecurityupdateurl	Solution_Summary	Ordnet das Feld u_ommendedsecurityupdateurl der Lösungszusammenfassungsspalte in der Tabelle „angreifbare Elemente“ zu.

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde).	Skript, das zum Initialisieren der Werte in der Bereichsvariablen (sn_vul_msft_tvm) für den Integrationsprozess verwendet wird. Dieses Skript ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
	zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Skript, das verwendet wird, um zu überprüfen, ob der Schwachstelleneintrag und die Erkennungen vorhanden sind. Wenn nicht, werden diese Datensätze in ihren jeweiligen Tabellen erstellt. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Aktualisieren der Anzahl der VIS und Erkennungen verwendet wird, wie aus MS TVM importiert. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Statusdiagramm der Integrationsausführung für die Microsoft Threat and Vulnerability Management Vulnerability Integration

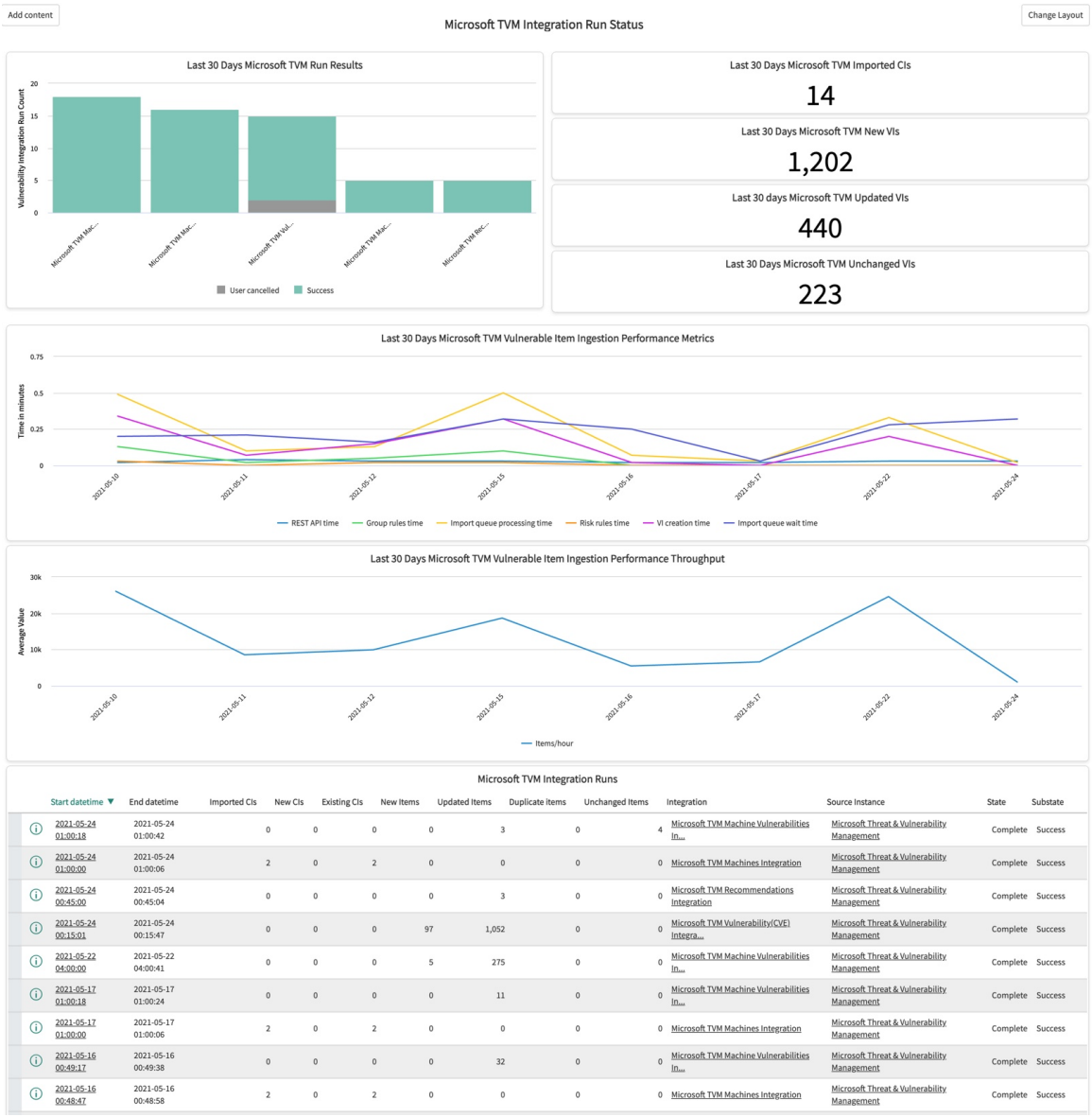
Sie können das Modul Microsoft Threat and Vulnerability Management (MS TVM) Integrationsausführungsstatus verwenden, um Ihnen eine grafische Ansicht des Status der MS TVM-Integrationsausführungen zu bieten.

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard ist in der neuen Experience-UI verfügbar.

Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Im Diagramm können Sie auf einen beliebigen Teil des Diagramms verweisen, um eine Zusammenfassung der für diesen Teil spezifischen Daten anzuzeigen. Wenn Sie auf ein Teil im Balkendiagramm klicken, wird eine Liste geöffnet, die detailliertere Informationen enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Statusdiagrammberichte der MS TVM-Integrationsausführung

Name	Beschreibung
Microsoft TVM-Ergebnisse der letzten 30 Tage	Anzahl der Integrationsausführungen, die für jede Integration abgeschlossen wurden. Dieser Bericht zeigt sowohl die erfolgreichen als auch die fehlgeschlagenen Ausführungen an. Jede Ausführung wird als Balken im Diagramm angezeigt.
Microsoft TVM – neue VIS der letzten 30 Tage	Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden.
Aktualisierte Microsoft TVM-VIS der letzten 30 Tage	Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden.
Microsoft TVM – unveränderte VIS der letzten 30 Tage	Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden.
Ms TVM-Integration wird ausgeführt	Datensätze der Integrationsausführung in einer Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Hinweis: **V16.1:** Um die Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit ServiceNow Erkennungsdaten in `sn_vul_detection`Tabelle. Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennung oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „bis datumsanzahl“ in der Instanz nach Abschluss der Integrationsausführung an.
Leistungsmetriken der Erfassung angreifbarer Microsoft TVM-Elemente der letzten 30 Tage	Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich zu den letzten 30 Tagen.
Leistungsdurchsatz der Erfassung angreifbarer Microsoft TVM-Elemente der letzten 30 Tage	Täglicher Durchsatz der Erfassung angreifbarer Elemente, der für die Microsoft TVM Host Detection-Integration in den letzten 30 Tagen gemessen wurde.
In den letzten 30 Tagen von Microsoft TVM importierte CIs	Anzahl der neuen Konfigurationselemente, die in den letzten 30 Tagen importiert wurden.

Überprüfen Sie den Status der Importausführung der Microsoft Threat and Vulnerability Management-Integration

Verwenden Sie den Importausführungsstatus Microsoft Threat and Vulnerability Management (MS TVM), um den Erfolg Ihrer Integrationsausführungen zu überprüfen und Probleme zu lokalisieren.

Vorbereitungen

Bei diesem Verfahren werden die folgenden Annahmen getroffen:

- Sie haben Vulnerability Response Und die MS TVM Vulnerability Integration installiert und konfiguriert.
- Importe von MS TVM Vulnerability Integration sind geplant und werden ausgeführt.

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur

1. Navigieren zu **Alle** > **Microsoft Bedrohungs- und Schwachstellenmanagement** > **Integrationen**an.
   a. Wählen Sie eine Integration aus.
   b. Klicken Sie auf die zugehörige Liste Vulnerability Integration wird ausgeführt.
2. Überprüfen Sie, ob der Status der Importe abgeschlossen ist und der Substatus Erfolg ist.
   Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:
   - Netzwerkunterbrechung.
   - Bitverfall bei der Datenübertragung, was zu beschädigten Daten während der Transformation führt.
3. **Wahlweise:** Wenn eine dieser Bedingungen angezeigt wird, die eine fehlgeschlagene Ausführung verursacht haben, klicken Sie auf **Jetzt ausführen** Und führen Sie die Integration erneut aus.

Teilen Sie Microsoft TVM-Erkennungen basierend auf der Schwachstelleninstanz auf, um angreifbare Elemente aufzuteilen

ServiceNow® Vulnerability Response ermöglicht die Aufteilung von Erkennungen aus Microsoft Threat and Vulnerability Management (MS TVM)-Scannern, wodurch für jede erkannte Schwachstelleninstanz ein eindeutiges angreifbares Element (VIT) erstellt werden kann. Diese Aufteilung ermöglicht die Zuweisung von Vits an verschiedene Korrekturteams, wodurch die Verwaltung und Nachverfolgung von Schwachstellen verbessert wird.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Nutzlast des Microsoft Threat and Vulnerability Management (MS TVM)-Scanners enthält Erkennungsdaten, wobei jeder Pfad innerhalb des Nachweises zum Aufteilen der Erkennungen verwendet wird. Das diskpath-Tag in der Nutzlast identifiziert den Standort der Schwachstelle und erleichtert so die genaue Identifizierung und Verwaltung von Schwachstellen gemäß ihren spezifischen Pfaden.

Prozedur

1. Legen Sie in der Tabelle „Drittpartei-Integrationen“ [sn_sec_int_Integration] fest **Nachweis in VI-Schlüssel einschließen** Spaltenwert auf „wahr“ für Tenable.io Und Tenable.sc.
2. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Aktivieren Sie im Formular „Port einbeziehen“ das Kontrollkästchen Port einbeziehen, und aktivieren Sie die Option **Klicken Sie hier** Link.
4. Wählen Sie in der Liste Nachweis zu VI-Schlüsseln hinzufügen die Option aus **Neu** .
5. Im Formular „Nachweis zum VI-Schlüssel hinzufügen – neuer Datensatz“ im **Schwachstelle** Fügen Sie das Microsoft Threat and Vulnerability Management (MS TVM) CVE hinzu, für das Sie den Nachweis einschließen möchten, und wählen Sie aus **Übermitteln** .
   Die ausgewählte Schwachstelle wird in der Liste Nachweis zu VI-Schlüsseln hinzufügen angezeigt.

Example: Aufteilen von Erkennungen vom Microsoft Threat and Vulnerability Management (MS TVM)-Scanner

Die folgende Erkennung vom Microsoft Threat and Vulnerability Management (MS TVM)-Scanner zeigt Beweise im Datenträgerpfad-Tag an.


```
          "id": "329f3283
fae116€796ff1b59c8dd56fef4067elf_mozilla_firefox_126.0.1.0_CVE-2024-7528",
         "deviceId":"329f3283fae116e796ff1b59c8dd56fef4067e1f",

         "rbacGroupId":
    "rbacGroupName": "Unassigned",
     "deviceName": "ip-0a1409fd.secops.com",
      "osPlatform": "WindowsServer2019",
       "oVersion": "10.0.17763.5936",
      "osArchitecture": "x64",
       "softwareVendor": "mozilla",
      "softwareName": "firefox",
      "softwareVersion": "126.0.1.0",

          "cveId"; "CVE-2024-7528",
         #vulnerabilitySeverityLevel": "High",
       #recommendedSecurityUpdate":; "mfsa2024-33",

      "recommendedSecurityUpdateId": null,

         "recommendedSecurityUpdateUrl": null,
          "diskPaths": ['c: llprogram files\lamazonllcfn-bootstraplilibcrypto-3.dll", "C: \lprogram
files\lamazon\lcfn-bootstrap\\libsst-3.dll,

        "registryPaths":
          1 "HKEY LOCAL, MACHINE\\SOFTWAREW\WOW6432Nodel
lMicrosoft|\Windows|1CurrentVersion\|Uninstalll\Mozilla Firefox 126.0.1 (x86 en-US)"


       #lastSeenTimestamp": "2024-08-28 19:36:07",

        "firstSeenTimestamp": "2024-08-06 20:32:34",

      "end0fSupportStatus": null,
        "end0fSupportDate": null,
     "exploitabilityLevel": "NoExploit",
        "recommendationReference": "va-_-mozilla-_-firefox",
```


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    "cvssScore": 8.8,
  "securityUpdateAvailable": true,
    "cveMitigationStatus": null
```

Verständnis der Integration der HCL BigFix-Patch-Orchestration mit Vulnerability Response

Mit können Sie Patches und Patch-Bereitstellungen für kritische Schwachstellen für große Gruppen von Assets verwalten Vulnerability Response Patch-Orchestration-Integration mit dem Produkt HCL BigFix.

Patch-Orchestration mit Vulnerability Response

Patch-Orchestration mit Vulnerability Response Verwendet geplante Importe aus Integrationen von Drittanbieterlösungen, Patch-Lieferanten und Schwachstellen-Scannern. Scannererkennungsdaten stimmen die Assets in Ihrer Umgebung mit Schwachstellen und den Patch-Updates ab, mit denen sie behoben werden können. Senden Sie Patch-Anforderungen zur Genehmigung, planen Sie Patch-Updates, um angreifbare Elemente zu lösen, und überwachen Sie den Korrekturfortschritt – alles aus Datensätzen in Vulnerability Response Anwendung in Ihrem ServiceNow AI Platform®.

Vulnerability Response Patch Orchestration mit HCL BigFix

Wenn die Integrationsanwendung Vulnerability Response Patch Orchestration mit HCL BigFix mit verwendet wird ServiceNow® Vulnerability Solution Management, Patch-Orchestration und Vulnerability Response Anwendungen, Schwachstellenmanager und Analysten können die folgenden Aufgaben ausführen:

- Weitere Kontextinformationen und Informationen zu den Arten von Patches und den Lösungen von Lieferanten (Patches) anzeigen.
- Zeigen Sie Schwachstellen- und Lösungsdaten sowie den Fortschritt der Schwachstellenkorrektur aus Datensätzen in an, und überwachen Sie sie Vulnerability Response Arbeitsbereiche.

IT-Spezialisten und Korrekturbesitzer können die folgenden Aufgaben ausführen:

- Stellen Sie Patches bereit, die vom BigFix-Produkt für unterstützt werden Windows, CentOS, MAC, Oracle und andere Assets in regelmäßigen, geplanten Intervallen außerhalb der Geschäftszeiten, um Arbeitskonflikte zu vermeiden.
- Identifizieren Sie nicht gepatchte Assets mit Schwachstellen oder Assets, die durch geplante Patches aus importierten Erkennungsdaten von Drittanbieterscannern erfolgreich aktualisiert wurden oder nicht erfolgreich aktualisiert wurden.
- Planen Sie verfügbare Patches aus dem IT-Korrekturarbeitsbereich oder aus der klassischen Umgebung für angreifbare, nicht gepatchte Assets aus Patch-Update, Korrekturaufgabe und erkannten Elementdatensätzen.

Schlüsselbegriffe in Vulnerability Response Und BigFix-Anwendungen

Konfigurationselement bzw. Configuration Item (CI)

CIs sind die vorhandenen Assets, die in aufgeführt sind Configuration Management Database (CMDB). BigFix ruft CIs, Computer auf.

Computergruppen

Im BigFix-Produkt verwendete Terminologie, die sich auf eine Gruppe von Assets bezieht.

Angreifbares Element

Eine importierte Schwachstelle, die einem vorhandenen Asset in Ihrer CMDB entspricht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanz

Ein eindeutiger Account der BigFix-Anwendung. Jeder Anwenderaccount kann eine Instanz in der BigFix-Anwendung sein. Dieser Begriff bezieht sich auch auf eine eindeutige, sichere Webadresse für einen ServiceNow AI Platform Instanz.

Integration

Eine -Integration ist eine geplante Aufgabe in ServiceNow AI Platform Die Informationen aus einer Drittparteiquelle abruft, z. B. die Integration mit den BigFix-Computern.

Lösung

Im Kontext dieser Integration gibt es zwei Arten von Lösungen, potenziell und bevorzugt. Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben könnte. Schwachstellen haben oft viele potenzielle Lösungen. #Eine bevorzugte Lösung entspricht der effektivsten Lösung für eine bestimmte erkannte Schwachstelle.

Patch

Software-Updates, die Schwachstellen beheben. In der BigFix-Anwendung werden Patches Fixlets genannt. Beispiel: BigFix hat Fixlets für Windows, CentOS, MAC, Oracle Und andere Produkte.

Bevorzugter Patch

Bevorzugte Patches sind Software-Updates, die bestimmte Schwachstellen beheben sollen. Patches werden nach der Bereitstellung den angreifbaren Elementen zugeordnet, die sich auf bestimmte Schwachstellen beziehen, und sie werden behoben.

Nachbesserungsaufgabe

Listen angreifbarer Elemente in Vulnerability Response Anwendung von Aktionen, die zum Beheben von Schwachstellen erforderlich sind.

Bereitstellung

Die Bereitstellung für die Zwecke dieser Integration bezieht sich darauf, wenn Sie einen Patch auf einen Computer anwenden, initiieren oder planen. BigFix ruft diese Bereitstellungen und Aktionen auf. Sie können für die Patches bereitstellen (Aktionen erstellen), die Sie von BigFix in heruntergeladen haben ServiceNow AI Platform. Navigieren Sie aus einzelnen Datensätzen in zu erkannten Elementen, Patches oder Korrekturaufgaben Vulnerability Response. Sie können Patches mit geplanten Aufgaben auf einzelnen Computern oder Computergruppen bereitstellen.

Bereitstellung in ServiceNow AI Platform Kann auch auf eine Integration verweisen, die mehrere Quellen unterstützt. Eine einzelne Integration wird als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie mehrere Bereitstellungen der BigFix Vulnerability-Integration in Ihrer Umgebung haben.

Vulnerability Solution Management und Vulnerability Response Patch Orchestration mit HCL BigFix Integration

Das Lösungsmanagement wird von bereitgestellt Vulnerability Solution Management Anwendung, A ServiceNow AI Platform Anwendung, die Ihre Schwachstellen-Ergebnisse mit der Aufgliederung der Lösungen (Patches) korreliert, die sie beheben. Identifizieren Sie die Software-Patches von Drittparteien für Produkte und Services, Konfigurations-Updates und andere Steuerungen, die die größten Auswirkungen auf Ihr Unternehmen haben. Zusammen mit Scannerinformationen von Drittparteien Solution Management for Vulnerability Response, Vulnerability Response, Und die Anwendungen Vulnerability Response Patch Orchestration mit HCL BigFix arbeiten zusammen, um bevorzugte Patches von der Lösung über die Schwachstelle bis zum angreifbaren Element zusammenzufassen, damit Sie Schwachstellen in Ihrer Umgebung beheben und schließen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Solution Management for Vulnerability Response, Vulnerability Response, Und die Vulnerability Response Patch Orchestration mit HCL BigFix Integration sind alle in verfügbar ServiceNow® Store.

Erforderliche ServiceNow AI Platform-Rollen

Die Integrationsinstallation, -Konfiguration und -Korrekturaufgaben erfordern die folgenden Rollen in Ihrem ServiceNow AI Platform Instanz.

Administrator

Anwender mit dieser Rolle erhalten Berechtigungen für Anwendungen in ServiceNow Store Und lädt sie in herunter ServiceNow AI Platform Instanzen.

sn_vul.vulnerability_admin

Anwender mit dieser Rolle aktivieren Anwendungen in ServiceNow AI Platform Instanz und schließt die Konfiguration von ab Vulnerability Response Anwendung. Diese Rolle hat vollständigen Zugriff auf Vulnerability Response(VR)-Anwendung und ihre Datensätze. Dieser Administratoranwender konfiguriert alle VR-Anwendungen, -Regeln und -Integrationen von Drittparteien.

sn_vul_bigfix.configure_Integration

Benutzer mit dieser Rolle konfigurieren die Anwendung BigFix Patch Orchestration Integration. Diese Rolle enthält die granulare Rolle sn_vul_bigfix.read_Integration.

sn_vul_bigfix.read_Integration

Anwender mit dieser Rolle können die#Datensätze von anzeigen (schreibgeschützt)Vulnerability Response Und die Anwendung BigFix Patch Orchestration Integration und Patch Orchestration-Daten.

sn_vul_Patch_orch.configure_Patch

Benutzer mit dieser Rolle können Patches konfigurieren und anwenden.

sn_vul_Patch_orch.read_Patch

Benutzer mit dieser Rolle können Patch-Informationen (schreibgeschützt) anzeigen.

Verantwortliche Vertragsgenehmigung

Weisen Sie Verwendungen den Genehmigergruppen der Genehmigerebene 1 und Genehmigerebene 2 zu, wenn übermittelte Patch-Anforderungen vor der Bereitstellung genehmigt werden sollen.

Weitere Informationen zum Zuweisen dieser Rollen mit dem Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zu finden Vulnerability Response-Rollen in Ihrem ServiceNow AI Platform, Siehe Vulnerability Response Personas und granulare Rollen.

CI-Suchregeln

Wenn Daten aus der BigFix-Anwendung importiert werden, wird Vulnerability Response Die Anwendung sucht automatisch nach Übereinstimmungen in Configuration Management Database (CMDB) Mit Computerdaten (Asset). CI-Suchregeln werden verwendet, um CIs (Assets) zu identifizieren und sie automatisch zu Datensätzen angreifbarer Elemente (VI) hinzuzufügen, wenn VIS erstellt werden.

Die folgenden CI-Suchregeln sind im Lieferumfang des Basissystems enthalten und werden verwendet, um CIs (Assets) zu identifizieren und hinzuzufügen Vulnerability Response Anwendung:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MAC_ADDRESS
- IP_ADDRESS
- DNS_NAME

Sie können mehrere Werte für die IP_ADDRESS eines Assets verwenden. Eine CI-Suchregel berücksichtigt alle Werte für den Abgleich. Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Integrationen von Schwachstellen von Drittparteien.

MID-Server

Die Vulnerability Response Patch Orchestration mit HCL BigFix-Integration ist eine lokale Integration. Erfordert einen eigenständigen MID-Server, der nicht Teil eines MID-Server-Clusters ist. Der MID-Server ist erforderlich, um Skripts auf Remote-Computern von Ihrer Instanz aus auszuführen, um Daten vom BigFix-Server zu importieren. APIs für diese Integration werden mit MID-Servern aufgerufen, die Sie in eingerichtet haben ServiceNow AI Platform Instanz. Weitere Informationen finden Sie unter Bereiten Sie sich auf den vor Vulnerability Response Patch-Orchestration-Integration mit HCL BigFix.

Integrationen und Abhängigkeiten von Vulnerability Response Patch-Orchestration-Integration mit HCL BigFix

Die folgenden Produkt- und Abhängigkeitsanwendungen sind für das Vulnerability Response Patch Orchestration mit HCL BigFix Integration erforderlich. Diese Anwendungen sind in verfügbar ServiceNow® Store.

Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch-Orchestration-Integration erforderlich sind

Dient zum Anzeigen von Patch-Orchestration-Daten und verfügbaren Updates (Patches) in den Arbeitsbereichen in Vulnerability Response, Die folgenden Anwendungen sind erforderlich. Alle aufgeführten Anwendungen sind in verfügbar ServiceNow® Store. Einige Anwendungen erfordern separate Abonnements.

Weitere Informationen zur Versionskompatibilität mit den erforderlichen Anwendungen und Familien-Releases finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema artikel in der HI Knowledge Base.

Anwendungs- und Release-Version
Vulnerability Response
Vulnerability Solution Management
Anwendung „Vulnerability Response Patch Orchestration“
Vulnerability Response Patch-Orchestration mit HCL BigFix-Anwendung
Security Support Common
Orchestration Des Sicherheitssupports
Eine unterstützte Drittanbieter-Anwendung für Schwachstellen-Scanner

Vulnerability Response Patch-Orchestration-Anwendungstabellen

Die Vulnerability Response Die Patch Orchestration-Anwendung enthält die folgenden Tabellen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Patch-Update [sn_vul_Patch_orch_Update]	Speichert Informationen zu den Patches, die in verschiedenen Instanzen verfügbar sind.
Geräteaktualisierung [sn_vul_Patch_orch_m2m_src_ci_Update]	Speichert Daten zu den bereitgestellten Patches zusammen mit dem Bereitstellungsstatus, die in erkannten Elementdatensätzen angezeigt werden.
Sammlung [sn_vul_Patch_orch_Collection]	Speichert Sammlungsdaten aus verschiedenen Instanzen.
Gerätesammlung [sn_vul_Patch_orch_m2m_src_ci_Collection]	Speichert Sammlungsdaten zu erkannten Elementen.
Patch-Bereitstellung [sn_vul_Patch_orch_Deployment]	Speichert Informationen zu bereitgestellten Patches zu Sammlungen und CIs.
Potenzieller Patch [sn_vul_Patch_orch_m2m_vuln_Patch]	Speichert Daten zu Patches und Schwachstellen, die die Patches identifizieren, die zur Behebung einer Schwachstelle verwendet werden können.

Integrationen der Patch-Orchestration für Vulnerability Response mit HCL BigFix

Die von entwickelten Integrationen ServiceNow® Engineering stellt die orchestrierte Lösungsbereitstellung mit dem BigFix-Produkt zusammen. Die folgenden Integrationen sind im enthalten Vulnerability Response Patch-Orchestration-Integration mit HCL BigFix-Anwendung, die Sie aus herunterladen ServiceNow® Store.

Nachdem Sie die Integrationsanwendung auf Ihrem installiert haben ServiceNow AI Platform Instanz, um diese Integrationen anzuzeigen, navigieren Sie zu **Integrationen** > **Integration der BigFix Patch Orchestration** > **Integrationen**an. Die Vulnerability Response Die Anwendung verarbeitet Daten in geplanten Zeitintervallen, die von diesen Integrationen mit BigFix-Endpunkten importiert werden.

Integration	Beschreibung
Integration der BigFix-Sammlung	• Diese Integration ist für die tägliche Ausführung geplant und wird zuerst in der verketteten Integrationsausführung ausgeführt. • Ruft die Computer und Computergruppen aus der BigFix-Anwendung ab, aus denen die Computergruppen (Konfigurationselemente) bestehen.
BigFix Fixlet-Integration	• Bei der Planung wird diese Integration durch Abschluss der BigFix Collection-Integration ausgelöst. Sie können es auch bei Bedarf ausführen. • Ruft Informationen zu allen verfügbaren Fixlets (Patches) vom BigFix-Server ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
BigFix-Geräte-Fixlet-Integration	• Bei der Planung wird diese Integration durch Abschluss der BigFix Fixlet-Integration ausgelöst. Sie können es auch bei Bedarf ausführen. • Ruft Informationen zu den Fixlets ab, die sich derzeit auf Computern (Assets) befinden, vom BigFix-Server.
Integration von BigFix-Aktionen	• Bei der Planung wird diese Integration durch Abschluss der BigFix Device Fixlet-Integration ausgelöst. Sie können es auch bei Bedarf ausführen. • Ruft Informationen zu den Patches ab, die vom IT-Team auf dem BigFix-Server geplant wurden.

Bereiten Sie sich auf den vor Vulnerability Response Patch-Orchestration-Integration mit HCL BigFix

Bereiten Sie sich auf die Integration vor, indem Sie die folgenden Setup-Aufgaben ausführen.

Vorbereitungen

Erforderliche Rollen: administrator für die Installation der Anwendungen und die Zuweisung von Rollen. Andere Rollen sind in der folgenden Tabelle aufgeführt.

Warum und wann dieser Vorgang ausgeführt wird

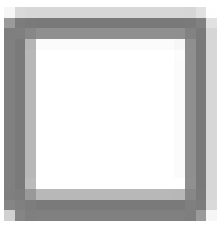
Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration.

Sie sind bereit für Installieren Sie Vulnerability Response Patch-Orchestration mit HCL BigFix-Anwendung.

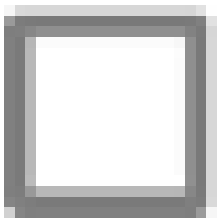
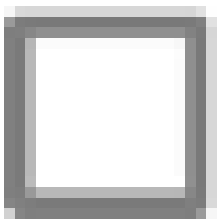
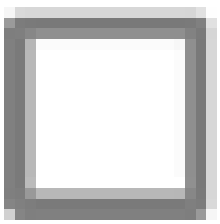
Prozedur

1. Für eine reibungslose Installation und Konfiguration von Vulnerability Response Patch Orchestration mit HCL BigFix-Anwendung patchen. Befolgen Sie die bereitgestellte Prüfliste.
2. Möglicherweise möchten Sie die folgende Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren.

   Importieren Sie nach der Installation und Konfiguration Schwachstellen- und Patch-bezogene Informationen in Ihren ServiceNow AI Platform® Instanz.

Aufgabe	Beschreibung
	(Optional) wenn Sie nicht bereits installiert und aktiviert sind, möchten Sie möglicherweise installieren Vulnerability Response Anwendung vor der Installation der Drittanbieteranwendung. Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe, Vulnerability Response installieren. Diese Integration erfordert Version 16,0 von Vulnerability Response Oder später.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

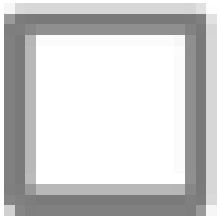
Aufgabe	Beschreibung
	Wenn nicht bereits installiert, rufen Sie Berechtigungen ab, und installieren Sie eine Scanner-Anwendung von Drittanbietern, um Schwachstellendaten zu importieren. Siehe Vulnerability Response-Integrationen Weitere Informationen zu Scannern von Drittanbietern, die von unterstützt werden Vulnerability Response. Weitere Informationen finden Sie unter .
	Wenn nicht bereits installiert, rufen Sie Berechtigungen ab, und laden Sie die Anwendung Vulnerability Response Patch Orchestration mit HCL BigFix auf Ihren herunter ServiceNow AI Platform® Instanz. Weitere Informationen finden Sie unter .
	Erhalten Sie BigFix-Anmeldeinformationen. Stellen Sie sicher, dass Sie Accountnamen, Passwörter und andere Serviceinformationen haben, die für Ihre BigFix-Produkte erforderlich sind, damit Sie Zugriff darauf haben.
	Stellen Sie sicher, dass Sie Gruppen oder Anwender haben, um die Integrationen zu verwalten und angreifbare Elemente zu korrigieren. **Administrator** Der Systemadministrator ruft Berechtigungen ab, lädt die Anwendung BigFix Patch Orchestration und die anderen für die Integration erforderlichen Anwendungen herunter und installiert sie. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.Vulnerability_admin) und andere Rollen im Setup-Assistenten in zu Vulnerability Response Oder aus dem Modul Anwenderverwaltung. **sn_vul.vulnerability_admin** Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der BigFix-Integrationen und der anderen Drittanbieteranwendungen ab. Diese Rolle hat vollständigen Zugriff auf Vulnerability Response(VR)-Anwendung und ihre Datensätze. Diese Rolle konfiguriert alle VR-Anwendungen, -Regeln, Drittanbieterintegrationen, Vulnerability Response Patch Orchestration und Vulnerability Solution Management-Anwendungen. **sn_vul_bigfix.configure_Integration**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Benutzer mit dieser Rolle konfigurieren die Anwendung BigFix Patch Orchestration Integration. Diese Rolle enthält die granularen Rollen sn_vul_bigfix.read_Integration und connection_admin, die es dem Anwender ermöglichen, eine Verbindung zur BigFix-Konsole herzustellen und die Integrationsinstanzen in zu konfigurieren ServiceNow AI Platform. **sn_vul_bigfix.read_Integration** Anwender mit dieser Rolle können die#Datensätze von anzeigen (schreibgeschützt) Vulnerability Response Und die Anwendung BigFix Patch Orchestration Integration und Patch Orchestration-Daten. **sn_vul_Patch_orch.configure_Patch** Benutzer mit dieser Rolle können Patches konfigurieren und anwenden. Patches, die von diesem Anwender aus Datensätzen für angreifbare Elemente und Patch-Updates angefordert werden, werden zur Genehmigung gesendet, wenn das Change-Management aktiv ist und Genehmiger zugewiesen werden. **sn_vul_Patch_orch.read_Patch** Benutzer mit dieser Rolle können Patch-Informationen in Datensätzen (schreibgeschützt) anzeigen. Diese Rolle wird mit den Rollen „sn_vul.Remediation_owner“ und „sn_vuln.Vulnerability_Analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind. **Verantwortliche Vertragsgenehmigung** Anwender, die der Genehmigerebene 1 und optional Genehmigergruppen der Genehmigerebene 2 zugewiesen sind, genehmigen übermittelte Patch-Anforderungen. Standardmäßig werden Patches vor der Bereitstellung zur Genehmigung an die Genehmigerebene 1-Gruppe übermittelt. Weitere Informationen zum Genehmigungsprozess finden Sie unter Patch-Orchestration mit Vulnerability Response. Weitere Informationen zum Einrichten von Genehmigern und Gruppen finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Der Systemadministrator führt die anfängliche Zuweisung von Rollen an Anwender und Gruppen für die Integration durch. Standardmäßig ist die Vulnerability Response-Gruppe verfügbar. Wenn Sie noch nicht erstellt haben, können Sie zusätzliche Gruppen für die Rollen von Korrekturspezialisten und Schwachstellenanalysten erstellen und Anwender mit dem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Modul „Anwenderverwaltung“ in Ihrer Instanz hinzufügen. Siehe Erstellen Sie eine Anwendergruppe .
	Stellen Sie sicher, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Aufträge in Ihrer Instanz aktiviert haben, die für die Integration erforderlich sind. ○ Die Vulnerability Response Patch Orchestration mit HCL BigFix ist eine lokale Integration, die die Verwendung eines eigenständigen MID-Servers erfordert. Weitere Informationen zu MID-Servern in Ihrer Instanz finden Sie unter MID-Server . ○ Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** Und suchen Sie das Plugin. Wenn nicht in Ihrer Instanz installiert, installieren und aktivieren Sie sie.

Nächste Maßnahme

Sie sind jetzt bereit für Installieren Sie Vulnerability Response Patch-Orchestration mit HCL BigFix-Anwendung.

Installieren Sie Vulnerability Response Patch-Orchestration mit HCL BigFix-Anwendung

Laden Sie die Anwendung Vulnerability Response Patch Orchestration mit HCL BigFix aus dem herunter ServiceNow® Store.

Vorbereitungen

Erforderliche Rollen: administrator für die anfängliche Zuweisung der Rolle „sn_vul.Vulnerability_admin“ und die Installation der Anwendung. Vulnerability admin (sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)), um das Vulnerability Response Patch Orchestration mit HCL BigFix und anderen Anwendungen zu konfigurieren, nachdem sie installiert wurden.

Warum und wann dieser Vorgang ausgeführt wird

Vergewissern Sie sich vor der Installation der Anwendung, dass Sie alle Elemente in der Prüfliste in abgeschlossen haben Bereiten Sie sich auf den vor Vulnerability Response Patch-Orchestration-Integration mit HCL BigFix.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach **Vulnerability Response Patch Orchestration mit HCL BigFix** Anwendung und klicken Sie auf **Installieren** .

   Mit dieser Aktion wird die Anwendung installiert, die Sie aus heruntergeladen haben ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Alternativ können Sie Anwendungen über den Setup-Assistenten installieren.
   Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.

Nächste Maßnahme

Navigieren Sie nach Abschluss der Installation zu **Alle** > **Integration der BigFix Patch Orchestration** > **Konfiguration** Um mit der Konfiguration fortzufahren.

Konfigurieren Sie Vulnerability Response Patch-Orchestration-Integration mit HCL BigFix

Nachdem Sie die Anwendung installiert haben, konfigurieren Sie sie mit Ihren BigFix-Account-Informationen, und validieren Sie Ihre Anmeldeinformationen.

Vorbereitungen

Erforderliche Rollen: sn_vul.Vulnerability_admin und sn_vul_bigfix.configure_Integration

Prozedur

1. Navigieren zu **Integration der BigFix Patch Orchestration** > **Konfiguration**an.
2. Füllen Sie die Felder mit Ihren BigFix-Informationen und -Anmeldeinformationen aus.

Feld	Beschreibung
Integrationsinstanz	Der Name des BigFix-Instanz-Accounts, den Sie verwenden möchten, z. B. `Integration von BigFix-Patch-Management` .
Hostname	Geben Sie die URL für den BigFix-Host ein.
Anwendername	Geben Sie Ihren BigFix-Account-Anwendernamen ein.
Passwort	Geben Sie Ihr BigFix-Account-Passwort ein.
MID-Server	Geben Sie den Namen des eigenständigen MID-Servers aus der Liste ein, den Sie verwenden möchten. Siehe Bereiten Sie sich auf den vor Vulnerability Response Patch-Orchestration-Integration mit HCL BigFix Weitere Informationen zu MID-Servern und Einrichtungsaufgaben in finden Sie in ServiceNow AI Platform®.

3. Klicken Sie auf Anmeldeinformationen speichern und testen.
   Der Status Ihrer Verbindung zwischen BigFix und Ihrem ServiceNow AI Platform® Instanz#wird im Feld Validierungsstatus angezeigt. Wenn kein erfolgreicher Test angezeigt wird, befolgen Sie die Anweisungen.
4. **Wahlweise:** Domänentrennung wird für diese Integration unterstützt.
   Sie können Ihrer Instanz mehrere Konfigurationen von hinzufügen. So fügen Sie zusätzliche Konfigurationen hinzu:

   a. Navigieren zu **Integration der BigFix Patch Orchestration Integrationsinstanzen** .

   b. Überprüfen Sie den Anwendungsbereich, `Vulnerability Response Patch Orchestration mit HCL BigFix` , Wird im Feld Anwendungsbereich angezeigt.

   c. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Füllen Sie das Formular aus.

Feld	Beschreibung
Name	Name für die Integrationsinstanz.
Anwendung	Vulnerability Response Patch Orchestration mit HCL BigFix
Integration	[Schreibgeschützt] BigFix-Patch-Management ist der Standard.
Aktiv	Standard ist aktiviert (ausgewählt). Wenn diese Option deaktiviert ist, ist die Instanz nicht aktiv.

e. Klicken Sie auf **Absenden**.
Ihre neue Integrationsinstanz wird in der Liste „Integrationsinstanzen“ angezeigt.

f. Wiederholen Sie die Schritte 1-3, um Ihre Integrationsinstanz zu konfigurieren und Ihre Anmeldeinformationen zu testen.

5. Richten Sie Genehmigungen für Patch-Anforderungen ein.
Standardmäßig ist eine Systemeigenschaft [**sn_vul_Patch_orch.Patch_Approval_required**] Ist aktiviert, sodass Patch-Bereitstellungen bei der Planung zur Überprüfung und Genehmigung an Anwender übermittelt werden, die der Genehmigungsgruppe „Patch-Update“ der Ebene 1 zugewiesen sind.

Wenn Anwender mit der Rolle „sn_vul_Patch_orch.configure_Patch“ Patches ohne Genehmigung planen sollen, können Sie [. Deaktivieren **sn_vul_Patch_orch.Patch_Approval_required**] Eigenschaft. Möglicherweise möchten Sie Genehmigungen aktivieren lassen, damit geplante Patches nicht mit den normalen Arbeitszeiten in Konflikt stehen.

Hinweis:
Wenn Sie die Systemeigenschaft „Genehmigung“ deaktivieren, kann jeder Anwender mit der Rolle „sn_vul_Patch_orch.configure_Patch“ Patches ohne Überprüfung und Genehmigung planen und bereitstellen.

So deaktivieren Sie als Anwender mit der Rolle sn_vul.Vulnerability_admin die Systemeigenschaft:

a. Navigieren zu **sys.properties.list**an.

b. Suchen **sn_vul_Patch_orch.Patch_Approval_required** Und klicken Sie darauf, um den Datensatz zu öffnen.

c. Geben Sie im Feld Wert ein `Falsch` .

d. Klicken Sie auf **Aktualisieren**.

6. Wenn Sie diese Eigenschaft nicht deaktivieren, müssen Sie Genehmiger für Patch-Anforderungen zuweisen. Führen Sie als Benutzer mit der Rolle sn_vul.Vulnerability_admin die folgenden Schritte aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Vulnerability Response** > **Administration** > **Genehmigungsregeln**an.

b. Wenn **Genehmigung für Patch-Update bereitstellen** Genehmigungsregel wird nicht in der Liste angezeigt. Klicken Sie auf **Alle** Rechts neben dem grünen Filtersymbol oben links im Bildschirm, um die gesamte Liste anzuzeigen.

c. Klicken Sie in der Liste auf **Genehmigung für Patch-Update bereitstellen** .

d. Klicken Sie im Datensatz bei ausgewählter Registerkarte Genehmigungskonfiguration auf **Genehmigung des Patch-Updates für Standardkonfiguration** .

e. Klicken Sie im Datensatz auf **Ebene 1: Patch-Update-Genehmigung** .

f. Fügen Sie dieser Gruppe Anwender hinzu.

Die dieser Gruppe zugewiesenen Anwender genehmigen Patch-Anforderungen, die von Anwendern mit der Rolle „sn_vul_Patch_orch.configure_Patch“ übermittelt werden. Navigieren Sie zu **Meine Genehmigungen** Zum Anzeigen und Verarbeiten der Anforderungen.

7. Klicken Sie Auf **Aktualisieren** Um Ihre Änderungen zu speichern.
8. **Wahlweise:** Sie können Genehmigungen auf mehreren Ebenen einrichten, sodass vor der Bereitstellung geplanter Patch-Anforderungen mehr als eine Genehmigung erforderlich ist.

a. Klicken Sie auf, während der Genehmigungsdatensatz für das Update des Standardkonfigurations-Patches angezeigt wird **Neu** .

b. Füllen Sie die Felder aus.

Feld	Beschreibung
Name	Name der Genehmigungsebene, z. B. **Ebene 2: Patch-Update-Genehmigung** .
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird.
Erforderliche Genehmigung	Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind: ▪ Ein Genehmiger erforderlich ▪ Alle Anwender müssen genehmigen
Reihenfolge	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Auftragseintrag von 100 vor einer Konfiguration mit einem Auftragseintrag von 200 ausgeführt.
Rolle	Wählen Sie eine Rolle für die Gruppe aus der Liste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel.
Genehmigungskonfiguration	Enthält die Genehmigungskonfigurationen.
Zuweisen mit	Wählen Sie eine Option aus: ▪ Anwender und Anwendergruppe ▪ Genehmigungstabellenfeld ▪ Skript
Gruppen	Genehmigerebenengruppe, die aus mehreren Anwendern besteht. Der Anwender muss über eine der folgenden von Ihnen angegebenen Rollen verfügen.
Anwender	Bearbeiten Sie die in den Gruppen aufgeführten Anwender.

c. Klicken Sie Auf **Übermitteln** Um Ihre Änderungen zu speichern.

Patch-Daten für anzeigen Vulnerability Response Patch-Orchestration-Integration mit HCL BigFix

Patch-Daten und Patch-Rollup-Daten sowie Informationen zu Schwachstellen und Korrekturstatus Ihrer Schwachstellen werden in Datensätzen in Ihrer Instanz angezeigt.

Patch-Daten in anzeigen Vulnerability Response Arbeitsbereiche

Erforderliche Rollen:

- Rolle „sn_vul_Patch_orch.configure_Patch“ zum Konfigurieren und Planen von Patches
- sn_vul_Patch_orch.read_Patch zum Anzeigen (schreibgeschützten) Patch-Informationen in Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.Remediation_owner“ und „sn_vuln.Vulnerability_Analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind

Im Arbeitsbereich „IT-Korrektur“ können Sie Patches anzeigen:

- In der Startseite-Ansicht, in der Sie auf Bewertungslisten klicken können, um Datensätze für bevorzugte Lösungen für VIS, angreifbare CIs und bevorzugte Patches für VIS anzuzeigen.
- In der Listenansicht, in der Sie alle Patch-Update-Datensätze (VPUs) über die Patches-Links und die Ihnen zugewiesenen angreifbaren Elemente (Vits) mit Patches anzeigen können.

Sie können Patches aus den folgenden Datensätzen planen:

- Aus Patch-Update (VPU)
- Korrekturaufgabe (RT)
- Erkannte Elementdatensätze (SDI)

Im Vulnerability Manager-Arbeitsbereich können Sie Patches anzeigen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In der Startansicht zu Überwachungsthemen können Sie bevorzugte und potenzielle Patches, geplante Patchdaten und, ob der Patch heruntergeladen wurde, alle auf anzeigen **Angreifbare Elemente** Registerkarte.
- In der Listenansicht zu Korrekturmaßnahmen, in der Sie Patch-Daten in VI-Datensätzen aus anzeigen können **Angreifbare Elemente** Registerkarte.

Navigieren Sie in der klassischen Umgebungsansicht zu **Alle** > **Vulnerability Response** > **Patches**an.

Patch-Update-Datensätze in den VR-Arbeitsbereichen und in der klassischen Umgebungsansicht

Patch-Daten und Patch-Rollup-Daten und -Status werden in Datensätzen in Ihrer Instanz angezeigt. Patch-Datensätze sind als Teil der Patch-Orchestration-Funktion dieser Integration mit enthalten Vulnerability Response. Zeigen Sie Patch-Datensätze (VPU) in an Vulnerability Response Arbeitsbereiche aus der Listenansicht im IT-Korrekturarbeitsbereich. Patch-Update-Datensätze sowohl in der klassischen Ansicht als auch Vulnerability Response Arbeitsbereiche enthalten die folgenden Daten:

- Daten und Informationen der Schwachstellenlösung von Patch-Lieferanten, die von der Anwendung „Schwachstellenlösungsmanagement“ importiert wurden.
- Quellkorrekturstatus, der die Gesamtzahl der Geräte mit einer bestimmten Schwachstelle enthält, die durch einen Patch behoben werden kann, und aller Geräte, für die Updates fehlen.
- Korrekturstatus, der % der korrigierten VIS und die Gesamtzahl der VIS enthält, die einen Patch als bevorzugten Patch haben.
- Zugeordnete Geräte, angreifbare Elemente, Patch-Bereitstellungen und Patch-Anforderungen in den zugehörigen Links zu Datensätzen in der Klassenansicht. Diese Daten werden auf Registerkarten in Datensätzen in angezeigt Vulnerability Response Arbeitsbereiche.
- Patch-Anforderungen, die Korrekturbesitzer zur Genehmigung übermittelt haben.

Status-Rollup für Datensätze angreifbarer Elemente

Weitere Informationen zum Status-Rollup zu Datensätzen finden Sie unter Patch-Daten- und Status-Rollup für Patch-Orchestration in Vulnerability Response.

Datensätze, in denen die Anzahl aktiver VI zusammengefasst wird

Um ein Rollup aller Patches für alle Schwachstellen zu vermeiden, erfasst die geplante Aufgabe nur Änderungen an der Anzahl der aktiven VI. Diese Anzahländerungen und zugehörigen Daten werden in für die folgenden Datensätze zusammengefasst Vulnerability Response:

- VIT
- RT
- Schwachstellenlösung
- Patch-Update

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzeigen von Daten für Patches ohne Lösungen

Weitere Informationen zum Anzeigen von Patches ohne Lösungen finden Sie unter Zeigen Sie Patches ohne Lösungen in an Vulnerability Response.

Daten mit patchen Vulnerability Response

Die Dashboards Vulnerability Management (PA) und CISO sind in einem Abonnement von enthalten Performance Analytics Für Vulnerability Response Anwendung. Wenn Sie ein Abonnement für haben Performance Analytics, Ist jedoch keine Patch-Orchestration-Integration installiert, die Registerkarte „Korrektur“ wird im CISO-Dashboard angezeigt, aber nicht mit Daten gefüllt.

Navigieren Sie für das Dashboard Vulnerability Management (PA) zu **Alle** > **Vulnerability Response** > **Übersicht**an. Klicken Sie auf **Korrektur** Registerkarte und scrollen Sie zum unteren Seitenrand, um Patch-Updates-Daten anzuzeigen: Geplante und nicht geplante Patches, Patches ohne Zieldaten und wöchentliche Anzahlen.

Navigieren Sie für das CISO-Dashboard zu **Alle** > **Vulnerability Response** > **CISO-Dashboard**an. Wenn die Registerkarte Übersicht ausgewählt ist, scrollen Sie zum Ende der Seite, um Daten zur Patch-Abdeckung anzuzeigen: Relevanz, geplante und nicht geplante Patches und Patches ohne Zieldaten.

Weitere Informationen zu finden Vulnerability Response Dashboards, siehe Wird standardmäßig verwendet Vulnerability Response Dashboards, Patch-Orchestration mit Vulnerability Response Arbeitsbereiche, Und Patch-Orchestration-Daten in anzeigen Vulnerability Response Dashboards.

Planen Sie Patches mit Vulnerability Response Patch-Orchestration-Integration HCL BigFix

Planen Sie Patches aus Datensätzen für Patch-Update- und Korrekturaufgaben in der Vulnerability Response Anwendung in Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen

Ab Version 16.1 können Sie Patches aus dem planen Vulnerability Response Arbeitsbereiche oder aus der klassischen Umgebung.

Erforderliche Rollen:

- Rolle „sn_vul_Patch_orch.configure_Patch“ zum Konfigurieren und Planen von Patches
- sn_vul_Patch_orch.read_Patch zum Anzeigen (schreibgeschützten) Patch-Informationen in Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.Remediation_owner“ und „sn_vuln.Vulnerability_Analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind

Prozedur

1. In der Schwachstelle Vulnerability Response Arbeitsbereiche navigieren als Anwender mit der Rolle „sn_vul.Remediation_owner“ zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**an.
2. Klicken Sie auf der Homepage auf **Bevorzugter Patch für VIS** .
   Die Liste der Patch-Update-Datensätze für die VIS mit bevorzugten Patches, die Ihnen zugewiesen sind, wird angezeigt.
3. Suchen Sie einen Datensatz, den Sie öffnen möchten, und klicken Sie, um ihn zu öffnen.
4. Alternativ können Sie in der Listenansicht im Arbeitsbereich auf klicken **Patches** > **Alle** Und suchen Sie einen Patch-Update-Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Patch-Update-Datensatz wird angezeigt. Sie sollten die Daten möglicherweise überprüfen, bevor Sie einen Patch planen, da möglicherweise bereits andere Patches geplant sind.

5. In der folgenden Tabelle erfahren Sie, welche Daten angezeigt werden und was Sie tun können.

6. Klicken Sie Auf **Patch Planen** .

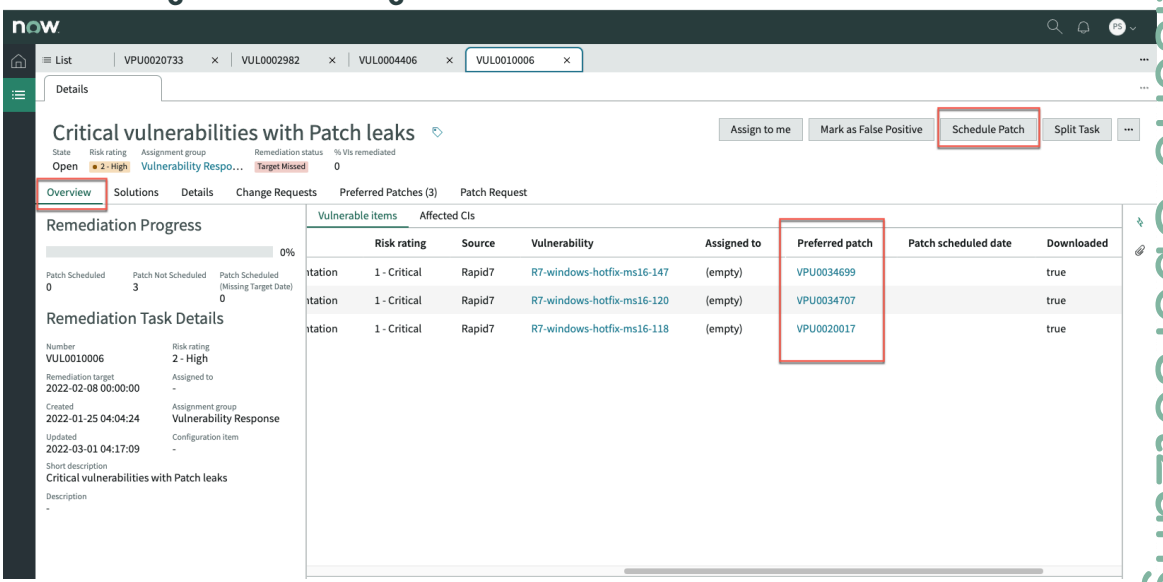
7. Füllen Sie die Felder im Dialogfeld aus.

8. Klicken Sie auf **Bereitstellen**.
   Die Patch-Anforderung wird zur Überprüfung an gesendet. Sie können den Status aller Ihrer übermittelten Anforderungen in anzeigen **Ausnahmeanforderungen** > **Meine Anforderungen** In der Listenansicht.

9. Alternativ können Sie Patches aus Korrekturaufgaben (RT) planen, die Ihnen oder Ihrer Gruppe zugewiesen sind.

Hinweis:
Die Option zum Planen eines Patches aus einem Korrekturaufgabendatensatz ist nur verfügbar, wenn Patches den VIS in der Aufgabe zugeordnet (zugeordnet) sind. Diese Patches werden in der Spalte „bevorzugter Patch“ angezeigt, wenn Sie bei ausgewählter Registerkarte „Übersicht“ nach rechts neben einem Korrekturaufgabendatensatz scrollen.

Korrekturaufgabe mit bevorzugten Patches



10. Klicken Sie Auf **Patch Planen** Aus dem RT-Datensatz und führen Sie die oben aufgeführten Schritte aus, um ihn im Dialogfeld zu planen.

11. Sie können Patches für die zuvor in der klassischen Umgebung aufgeführten Schritte planen.
    Um diese Datensätze zu finden, führen Sie die folgenden Schritte aus.

    a. Navigieren Sie in der klassischen Umgebung zu **Vulnerability Response** > **Patches** > **Alle**an.

    b. Suchen Sie in der angezeigten Liste nach einem Patch-Update-Datensatz.

    c. Navigieren Sie für Korrekturaufgaben zu **Vulnerability Response** > **Korrekturaufgaben** Und suchen Sie einen Datensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfolgen Sie den Korrekturstatus auf der Registerkarte Korrekturstatus. Am unteren Rand des Datensatzes werden Patch-Daten in den zugehörigen Links angezeigt.

d. Klicken Sie auf Patch planen, und füllen Sie die Felder aus.

Feld	Beschreibung
Bereitstellungsname	Geben Sie einen Namen für diese Patch-Bereitstellung ein. Dieser Name hilft Ihnen, Ihre Updates nachzuverfolgen.
Patch-Update	Wählen Sie eines aus den verfügbaren Patches in der Liste aus.
Assets	Wählen Sie eines aus: ▪ Computergruppe: Wählen Sie diese Option aus, wenn Sie eine Sammlung (eine Gruppe von Assets) für diesen Patch auswählen möchten. #Die Gruppen bestehen aus den Konfigurationselementen, die aus der BigFix-Anwendung importiert werden. ▪ Computerliste: Wählen Sie diese Option aus, wenn Sie einzelne Computer (Assets) für diesen Patch auswählen möchten. Im angezeigten Dialogfeld können Sie Daten zum Hersteller, zum Standort, zur Klasse, zum Zeitpunkt der letzten Aktualisierung und zum Wartungszeitplan anzeigen.
Startzeit und Endzeit	Geben Sie die Start- und Endzeiten für das Zeitfenster ein. Geben Sie ein, wann der Patch mit seiner Bereitstellung beginnen soll, und geben Sie den letzten Tag ein, an dem der Patch installiert werden kann.

REST-Nachrichten für die Integration der Patch-Orchestration von Vulnerability Response mit HCL BigFix

Die Vulnerability Response Die Patch-Orchestration-Integration mit HCL BigFix REST-Nachrichten wird verwendet, um Aufrufe an die BigFix-API zu tätigen.

BigFix-Anmeldung

Sie können auch die REST-Nachrichten für die BigFix-Anmeldung verwenden, um REST API-Anforderungen zu authentifizieren. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Authentifizierungsanforderungen an BigFix aus.

Parametername	Wert	Beschreibung
sourceType	Kumulativ	Gibt an, dass die Quellintegration Daten aus abruft. Verwendet von Code. Änderungen werden nicht empfohlen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Wert	Beschreibung
SortierDIR	desc	Gibt die Sortierrichtung für die aus der Integration abgerufenen Daten an. Änderungen werden nicht empfohlen.
SortierenFeld	severity	Gibt das Feld an, auf dem die Datensortierung basiert. Änderungen werden nicht empfohlen.
type	Vuln	Gibt den Typ der Daten an, die aus der Integration für die Asset-Integration abgerufen werden sollen. Änderungen werden nicht empfohlen.

BigFix-Integration

Sie können die REST-Nachricht für die BigFix-Integration verwenden, um Informationen aus BigFix abzurufen. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen aus, die an BigFix zum Abrufen von Informationen gestellt werden. REST-Nachrichten enthalten die folgenden REST-Methoden.

REST-Methoden

REST-Methode	Beschreibung
RUFEN SIE Daten ab	Ruft die Informationen von BigFix zu einem der folgenden Elemente basierend auf der angegebenen Abfrage ab: • Computer/Computergruppen • Fixlets • Relevante Fixlets auf Computern • Aktionen

Parametername	Wert	Beschreibung
URL	Dynamische Werte basierend auf Anwender	Gibt den Endpunkt der BigFix-Konsole an

BigFix – Patch bereitstellen

Sie können die REST-Nachricht für die BigFix-Integration verwenden, um Patches von Ihrem zu planen ServiceNow AI Platform® Zu BigFix. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen aus, die an BigFix zum Abrufen von Informationen gestellt werden. REST-Nachrichten enthalten die folgenden REST-Methoden.

REST-Methode	Beschreibung
Patch NACH der Bereitstellung	Plant den Patch für die BigFix-Konsole auf einzelnen/mehreren Computern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Wert	Beschreibung
URL	Dynamische Werte basierend auf Anwender	Gibt den Endpunkt der BigFix-Konsole an.
Titel	Dynamische Werte basierend auf Anwender	Titel der Bereitstellung.
Settings_Tag	XML-Tag-benannte Einstellungen mit Werten	Gibt Einstellungen an, die unterschiedliche Parameter haben und während der Planung des Patches an BigFix gesendet werden.
Computer_Tag	XML-Tag-benannte Computer mit Werten	Gibt eine Liste der Computer an, auf denen der Patch geplant wird.
site_name	Wert aus Patch-Update	Name des Standorts, an dem das Fixlet vorhanden ist.
Fixlet_ID	Wert aus Patch-Update	ID des Fixlets.

Datentransformation für die Patch-Orchestration-Integration mit HCL BigFix

Daten werden aus abgerufen Vulnerability Response Patch-Orchestration mit HCL BigFix-Integration, verarbeitet über eine Reihe von Datenquellen und transformiert in ServiceNow AI Platform® Instanz.

Import der BigFix-Sammlung

Die Daten aus den importierten Assets (Computer und Computergruppen) werden in die Tabelle „BigFix-Sammlungsimport“ [sn_vul_bigfix_Collection_Import] geladen. Der BigFix-Computer- und Computergruppenimport TM (Transformationszuordnung?) Wird verwendet, um die importierten Informationen umzuwandeln.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import der BigFix-Sammlung verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie BigFix Computer and Computer Groups Import TM. In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Timing der Umwandlungszuordnungsskript für BigFix-Computer und Computergruppen

Skript	Beschreibung
OnStart (wenn ein Importsatz eine Transformation erstellt hat).	Skript zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] für den Integrationsprozess. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Skript zum Erstellen und Aktualisieren von CIs basierend auf CI-Suchregeln und -Sammlungen sowie der Beziehung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Timing der Umwandlungszuordnungsskript für BigFix-Computer und Computergruppen (Fortsetzung)

Skript	Beschreibung
	zwischen ihnen. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Bereichsvariablen [sn_vul_bigfix]. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten CIs verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

BigFix Fixlet-Import

Die Daten aus den importierten Fixlets werden in die Tabelle „BigFix Fixlet-Import“ [sn_vul_bigfix_Patch_Update_Import] geladen.

BigFix Fixlet Import TM wird verwendet, um die importierten Informationen zu transformieren.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem BigFix Fixlet-Import verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie das BigFix Fixlet Import TM.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Transformationszuordnungsfelder für BigFix Fixlet-Import

Quellenfeld	Zielfeld	Beschreibung
u_id	artikel_ID	Eindeutige ID eines Fixlets in einer Site.
u_id	source_id	Eindeutige ID eines Fixlets in einer Site.
U_Site_Name	SN_vul_bigfix_Site_Name	Name der Website in BigFix, auf die sich das Fixlet bezieht.
U_Display_Name	Titel	Titel des Fixlets.
[Skript]	Bulletin_ID	Quell-ID der Lösung.
[Skript]	SN_vul_Solution	Lösung basierend auf der Quell-ID
U_Quelle	Bulletin_Source	Quelllieferant der Lösung.
[Skript]	Date_Release	Release-Datum des Fixlets.
U_Kategorie	Update_category	Kategorie des Fixlets.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transformationszuordnungsfelder für BigFix Fixlet-Import (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
[Skript]	Is_highest_supersedence	Boolescher Wert für, ob das Fixlet die höchste Ersetzung ist oder nicht.
[Skript]	Ist_heruntergeladen	Boolescher Wert, ob das Fixlet heruntergeladen wird oder nicht.
[Skript]	Integration_instance	Name der Instanz, aus der das Fixlet importiert wird.
U_Source_severity	Source_severity	Schweregrad des Fixlets.
U_applicable_count	NUM_total	Gesamtzahl der Geräte mit fehlenden Fixlets.
[Skript]	Last_modified	Datum der letzten Änderung des Fixlets.

Timing des BigFix Fixlet-Importtransformationszuordnungsskripts

Skript	Beschreibung
OnStart (wenn ein Importsatz eine Transformation erstellt hat).	Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Das Skript, das zum Aktualisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Fixlets verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Import von BigFix-Geräte-Fixlet

Die Daten aus den importierten relevanten Fixlets auf Computern werden in die Tabelle „Import von BigFix-Geräte-Fixlet“ [sn_vul_bigfix_device_Patch_Import] geladen.

BigFix Device Fixlet TM wird zum Transformieren der importierten Informationen verwendet.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import des BigFix-Geräte-Fixlets verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie das BigFix Device Fixlet TM.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Zeitplanung des BigFix-Geräte-Fixlet-Transformationsskripts

Skript	Beschreibung
OnStart (wenn ein Importsatz eine Transformation erstellt hat).	Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Erstellen und Aktualisieren von CIs basierend auf CI-Suchregeln und -Sammlungen sowie der Beziehung zwischen ihnen verwendet wird. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Bereichsvariablen [sn_vul_bigfix]. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten CIs verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Import von BigFix-Aktionen

Die Daten aus den importierten Aktionen werden in die Tabelle „Import von BigFix-Aktionen“ [sn_vul_bigfix_Deployment_Import] geladen.

Das TM „Import von BigFix-Aktionen“ wird zum Transformieren der importierten Informationen verwendet.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import von BigFix-Aktionen verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie das BigFix Fixlet Import TM.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Transformationszuordnungsfelder für BigFix-Aktionen importieren

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Eindeutige ID einer Aktion.
U_Name	name	Name der Aktion
[Skript]	SN_vul_bigfix_detected_item	Referenz des erkannten Elements, für das der Patch bereitgestellt wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transformationszuordnungsfelder für BigFix-Aktionen importieren (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
U_Status	status	Status der Aktion
[Skript]	SN_vul_Patch_orch_Update	Referenz des Patches
U_apply_count	Count_success	Erfolgsanzahl der Aktion.
U_retry_count	Erneut versuchen	Anzahl der Wiederholungen der Aktion.
[Skript]	Deployment_time	Startzeit der Aktion.
[Skript]	Frist	Endzeit der Aktion.
[Skript]	Source_created	Erstellungszeit der Aktion.
[Skript]	Integration_instance	Name der Instanz, aus der die Aktion importiert wird.

BigFix-Aktionen importieren Transformationszuordnungsskript-Timing

Skript	Beschreibung
OnStart (wenn ein Importsatz eine Transformation erstellt hat).	Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Das Skript, das zum Aktualisieren der Werte in der Bereichsvariablen [sn_vul_bigfix] verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Aktionen verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Beispiel-Workflow für die Integration der Patch-Orchestration von Vulnerability Response mit HCL BigFix

Ein Beispiel für die Funktionsweise der Patch-Orchestration mit dem Produkt HCL BigFix.

Vorbereitungen

Angenommen, Ihre gesamte Umgebung wird einmal alle drei Wochen gepatcht. Das letzte Patch-Fenster wurde vor einer Woche abgeschlossen, Sie möchten jedoch einen Patch anwenden, um eine kritische Schwachstelle zu beheben, die kürzlich bekannt wurde. Aufgrund der kritischen Natur dieser Schwachstelle können Sie nicht mehr zwei Wochen auf den nächsten geplanten Patch warten.

Erforderliche Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für den Vulnerability Manager-Arbeitsbereich.
- sn_vul.Remediation_owner zum Anzeigen des Arbeitsbereichs „IT-Korrekturbesitzer“.
- Rolle „sn_vul_Patch_orch.configure_Patch“ zum Konfigurieren und Planen von Patches.
- sn_vul_Patch_orch.read_Patch zum Anzeigen (schreibgeschützten) Patch-Informationen in Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.Remediation_owner“ und „sn_vuln.Vulnerability_Analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind.

Warum und wann dieser Vorgang ausgeführt wird
Als Schwachstellenmanager oder Analyst, der im Vulnerability Manager-Arbeitsbereich arbeitet, können Sie Überwachungsthemen erstellen oder vorhandene Überwachungsthemen bearbeiten, um importierte VIS mit kritischen Schwachstellen zu erfassen. Mit der Patch-Orchestration-Integration können Sie auch die Patches anzeigen, die Sie zum Beheben und Nachverfolgen dieser Schwachstellen verwenden möchten. Die folgende Tabelle enthält einige Beispiele mit den Bedingungen, die Sie für Überwachungsthemen für die Patch-Orchestration festlegen können. Verwenden Sie diese Beispiele, um Einstellungen zu bestimmen, die für Ihre Umgebung am besten geeignet sind. Siehe Erstellen Sie ein Überwachungsthema in Arbeitsbereich des Schwachstellenmanagers Weitere Informationen zum Einrichten des Überwachungsthemas.

Beispielbeobachtungsthemen für Patch-Orchestration im Vulnerability Manager-Arbeitsbereich

Name des Überwachungsthemas	Beschreibung
Kritische Schwachstellen mit Patch-Lecks	Risikobewertung ist 1 – Kritisch UND Grund ist „Patch nicht geplant“
Kritische Schwachstellen mit geplanten Patches (fehlende SLA)	Grund ist „Patch geplant“ (Zieldatum fehlt)
Kritische Schwachstellen mit geplanten Patches	Risikobewertung ist 1 – Kritisch UND Geplantes Patch-Datum ist nicht leer UND Grund ist „Patch geplant“

- Nachdem Sie als Schwachstellenmanager oder -Analyst die Überwachungsthemen und Korrekturmaßnahmen erstellt haben, generieren Sie Korrekturaufgaben. In VI-Datensätzen und Korrekturaufgaben können Sie Detailinformationen zur Registerkarte Erkennungen anzeigen und erkannte Elementdatensätze mit der Schwachstelle finden, die Sie nachverfolgen, zusammen mit den vom BigFix-Produkt importierten Assets.
- Als Schwachstellenanalyst oder -Administrator können Sie die Patch-Daten überwachen, die der Schwachstelle zugeordnet sind. Sie können auch einen Patch oder mehrere Patches für ein bestimmtes Asset (Konfigurationselement) aus einem erkannten Elementdatensatz bereitstellen.

Als IT-Korrekturspezialist haben Sie Optionen, wie Sie die Schwachstelle mit einer Patch-Bereitstellung beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können den Patch aus einem Patch-Update-Datensatz (VPU#) planen.
- Wenn angreifbaren Elementen (VI) bevorzugte Lösungen zugeordnet sind und sie Ihnen oder Ihren Gruppen zugewiesen sind, können Sie die Patches aus einer Korrekturaufgabe planen, die diese angreifbaren Elemente enthält.

Prozedur

1. Klicken Sie als IT-Korrekturspezialist im IT-Korrekturarbeitsbereich auf die Startansicht.
2. Klicken Sie in der Startansicht auf **Zugewiesene Korrekturaufgaben** Bewertungsliste zum Anzeigen der Datensätze.

   Für dieses Beispiel können Sie das Feld Kurzbeschreibung in der Korrekturaufgabe (VUL#) auf Text überprüfen, der sich auf Ihre kritische Schwachstelle bezieht. Angenommen, Sie wissen möglicherweise, dass Ihr Schwachstellenmanager ein Überwachungsthema namens kritische Schwachstellen mit Patch-Lecks erstellt hat, um VIS (VIT#) mit dieser kritischen Schwachstelle zu erfassen.

   Wenn der Datensatz geöffnet ist, können Sie auch die VIS und die bevorzugten Patches überprüfen und sehen, ob Sie oder eine Ihrer Gruppen bereits Patch-Anforderungen zur Genehmigung eingereicht hat.

3. Wenn Sie genügend Informationen haben, sollten Sie jetzt eine Anforderung für einen Patch aus dieser Korrekturaufgabe senden.

   Hinweis:
   Wenn die dem Datensatz zugeordneten VIS keine Patches aufweisen, die ihnen zugeordnet sind, wird die angezeigt **Patch Planen** Schaltfläche ist im Datensatz nicht verfügbar.

4. Klicken Sie Auf **Patch Planen** Und füllen Sie die Felder im Dialogfeld aus.
   Weitere Informationen zum Planen eines Patches finden Sie unter Planen Sie Patches mit Vulnerability Response Patch-Orchestration-Integration HCL BigFix.
5. Alternativ können Sie in der Listenansicht im IT-Korrekturarbeitsbereich auf die Links Korrekturaufgaben, angreifbare Elemente, Lösungen und Patches klicken, um diese Datensätze anzuzeigen.

   In diesem Beispiel kennen Sie anstelle des Namens eines Überwachungsthemas möglicherweise die Artikel-ID oder die Bulletin-ID und den Titel des Patches. Wenn ja, sollten Sie überprüfen, ob Ihnen oder Ihren Gruppen eines der VIS mit dieser Schwachstelle zugewiesen ist. Über Patch-Update-Datensätze können Sie Patch-Anforderungen übermitteln. In VI-Datensätzen können Sie nach potenziellen Patches suchen und die zugehörige Korrekturaufgabe öffnen, wenn Sie eine Patch-Anforderung übermitteln möchten.

6. Wenn Sie keinen Zugriff auf die Arbeitsbereiche haben oder Daten anzeigen und Patches aus der klassischen Umgebung planen möchten, gehen Sie wie folgt vor.

   a. Navigieren zu **Alle** > **Vulnerability Response** > **Patches** > **Alle**an.

   b. Suchen Sie den gewünschten Patch-Update-Datensatz.
   Sie sollten die Datensätze möglicherweise mit filtern Kritisch Risikopunktzahlen.

   c. Überprüfen Sie die Felder zugeordnete VIS und % korrigierte VIS auf der Registerkarte Korrekturstatus.
   Wenn für die VIS Patches verfügbar sind, wird **Patch Planen** Die Schaltfläche wird oben rechts im Datensatz angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wenn Sie eine Anforderung übermitteln möchten, klicken Sie auf **Patch Planen** .
Weitere Informationen zum Planen eines Patches finden Sie unter Planen Sie Patches mit Vulnerability Response Patch-Orchestration-Integration HCL BigFix.

e. Alternativ können Sie annehmen, dass Sie nicht über die Patch-ID-Informationen verfügen, aber Sie können das Feld Kurzbeschreibung für die Korrekturaufgaben überprüfen, die Ihrer Gruppe zugewiesen sind, auf Text, der sich auf Ihre kritische Schwachstelle bezieht.

f. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**an.

g. Suchen Sie den gewünschten Datensatz, und klicken Sie darauf, um ihn zu öffnen.
Überprüfen Sie im offenen Datensatz die Registerkarte Korrekturstatus auf VIS und % der korrigierten VIS. Klicken Sie auf die zugehörigen Links für VI-Datensätze, bevorzugte Lösungen, bevorzugte Patches und Patch-Anforderungen.

> **Hinweis:**
> Wenn die dem Datensatz zugeordneten VIS keine Patches aufweisen, die ihnen zugeordnet sind, wird die angezeigt **Patch Planen** Schaltfläche ist im Datensatz nicht verfügbar.

h. Klicken Sie Auf **Patch Planen** Aus dem Datensatz, wenn Sie eine Patch-Anforderung übermitteln möchten.

Verstehen von Vulnerability Response Patch-Orchestration-Integration mit Microsoft SCCM

Verwalten Sie Patches und Patch-Bereitstellungen für die kritischen Schwachstellen in Ihren Assets mit Vulnerability Response Integration mit Microsoft System Center Configuration Manager (SCCM)-Produkt.

Patch-Orchestration mit Vulnerability Response

Patch-Orchestration mit Vulnerability Response Verwendet geplante Importe aus Integrationen von Drittanbieterlösungen, Patch-Lieferanten und Schwachstellen-Scannern. Scannererkennungsdaten stimmen die Assets in Ihrer Umgebung mit Schwachstellen und den Patch-Updates ab, mit denen sie behoben werden können. Sie übermitteln Patch-Anforderungen zur Genehmigung, planen Patch-Updates, um angreifbare Elemente zu lösen, und überwachen den Korrekturfortschritt – alles von Ihrem aus ServiceNow AI Platform® Instanz.

Vulnerability Response Patch-Orchestration mit Microsoft SCCM

Wenn die Vulnerability Response Patch-Orchestration mit dem Microsoft Die SCCM-Anwendung wird mit verwendet ServiceNow® Vulnerability Solution Management, Patch-Orchestration und Vulnerability Response Anwendungen, Schwachstellenmanager und Analysten können die folgenden Aufgaben ausführen:

- Weitere Kontextinformationen und Informationen zu den Arten von Patches und den Lösungen von Lieferanten (Patches) anzeigen.
- Zeigen Sie Schwachstellen- und Lösungsdaten sowie den Fortschritt der Schwachstellenkorrektur aus Datensätzen in an, und überwachen Sie sie Vulnerability Response Arbeitsbereiche.

IT-Spezialisten und Korrekturbesitzer können die folgenden Aufgaben ausführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie Patches bereit, die von unterstützt werden Microsoft SCCM-Produkt für deren Windows, CentOS, macOS, Oracle, Und andere Assets in regelmäßigen, geplanten Intervallen außerhalb der Geschäftszeiten, um Konflikte mit der Arbeit zu vermeiden.
- Identifizieren Sie nicht gepatchte Assets mit Schwachstellen oder Assets, die durch geplante Patches aus importierten Erkennungsdaten von Drittanbieterscannern erfolgreich aktualisiert wurden oder nicht erfolgreich aktualisiert wurden.
- Planen Sie verfügbare Patches aus dem IT-Korrekturarbeitsbereich oder der klassischen Anwenderoberfläche für angreifbare, nicht gepatchte Assets aus Patch-Update, Korrekturaufgabe und erkannten Elementdatensätzen.

Schlüsselbegriffe in Vulnerability Response Und Microsoft SCCM-Anwendungen

Konfigurationselement bzw. Configuration Item (CI)

CIs sind die vorhandenen Assets, die in aufgeführt sind Configuration Management Database (CMDB). Microsoft SCCM ruft CIs, Geräte auf.

Sammlungen und Gerätesammlungen

In verwendete Terminologie Microsoft SCCM-Produkt, das sich auf eine Gruppe von Assets bezieht.

Angreifbares Element

Eine importierte Schwachstelle, die einem vorhandenen Asset in Ihrer CMDB entspricht.

Instanz

Ein eindeutiger Account von Microsoft SCCM-Anwendung. Jeder Anwenderaccount kann eine Instanz in sein Microsoft SCCM-Anwendung. Dieser Begriff bezieht sich auch auf eine eindeutige, sichere Webadresse für einen ServiceNow AI Platform Instanz.

Integration

Eine -Integration ist eine geplante Aufgabe in ServiceNow AI Platform Die Informationen aus einer Drittparteiquelle abruft, z. B. die Integration mit Microsoft SCCM-Computer.

Lösung

Im Kontext dieser Integration gibt es zwei Arten von Lösungen, potenziell und bevorzugt. Eine potenzielle Lösung ist eine Lösung, die eine Schwachstelle beheben könnte. Schwachstellen haben oft viele potenzielle Lösungen. #Eine bevorzugte Lösung entspricht der effektivsten Lösung für eine bestimmte erkannte Schwachstelle.

Patches

Software-Updates, die Schwachstellen beheben. In Microsoft SCCM-Anwendung, Patches werden aufgerufen, Patches. Beispiel: Microsoft SCCM hat Patches für Windows, CentOS, MAC, Oracle Und andere Produkte.

Bevorzugter Patch

Bevorzugte Patches sind Software-Updates, die bestimmte Schwachstellen beheben sollen. Patches werden nach der Bereitstellung den angreifbaren Elementen zugeordnet, die sich auf bestimmte Schwachstellen beziehen, und sie werden behoben.

Korrekturaufgabe oder, vor v15.0 von Vulnerability Response, Schwachstellengruppen

Listen angreifbarer Elemente in Vulnerability Response Anwendung von Aktionen, die zum Beheben von Schwachstellen erforderlich sind.

Bereitstellung

Die Bereitstellung für die Zwecke dieser Integration bezieht sich darauf, wenn Sie einen Patch auf einen Computer anwenden, initiieren oder planen. Sie können die von Ihnen heruntergeladenen Patches bereitstellen Microsoft SCCM in Ihrem ServiceNow AI Platform

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch Navigation zu erkannten Elementen, Patches oder Korrekturaufgaben aus einzelnen Datensätzen in Vulnerability Response. Sie können Patches mit geplanten Aufgaben auf einzelnen Computern oder Computergruppen bereitstellen.

Bereitstellung in ServiceNow AI Platform Kann auch auf eine Integration verweisen, die mehrere Quellen unterstützt. Eine einzelne Integration wird als Bereitstellung Ihrer Integration bezeichnet. Eine Bereitstellung bezieht sich auf die Integrationen und Produkte in Ihrer Umgebung. Beispielsweise können Sie mehrere Bereitstellungen von haben Microsoft Integration von SCCM-Schwachstellen in Ihrer Umgebung.

Vulnerability Solution Management Und Vulnerability Response Patch-Orchestration-Integration mit Microsoft SCCM

Die Vulnerability Solution Management Anwendung ist ein ServiceNow AI Platform Anwendung, die Ihre Schwachstellen-Ergebnisse mit der Aufgliederung der Lösungen (Patches) korreliert, mit denen sie behoben werden. Identifizieren Sie die Software-Patches von Drittparteien für Produkte und Services, Konfigurations-Updates und andere Steuerungen, die die größten Auswirkungen auf Ihr Unternehmen haben. Zusammen mit Scannerinformationen von Drittparteien Solution Management for Vulnerability Response, Vulnerability Response, Und Vulnerability Response Patch Orchestration mit Microsoft SCCM-Anwendungen arbeiten zusammen, um bevorzugte Patches von der Lösung über die Schwachstelle bis zum angreifbaren Element zusammenzufassen, damit Sie Schwachstellen in Ihrer Umgebung beheben und schließen können. Die Solution Management for Vulnerability Response, Vulnerability Response, Und Vulnerability Response Patch-Orchestration Microsoft SCCM-Integrationsanwendungen sind alle in verfügbar ServiceNow® Store.

Erforderliche ServiceNow AI Platform-Rollen

Die Integrationsinstallation, -Konfiguration und -Korrekturaufgaben erfordern die folgenden Rollen in Ihrem ServiceNow AI Platform Instanz.

Administrator

Anwender mit dieser Rolle erhalten Berechtigungen für Anwendungen in ServiceNow Store Und lädt sie in herunter ServiceNow AI Platform Instanzen.

sn_vul.vulnerability_admin

Anwender mit dieser Rolle aktivieren Anwendungen in ServiceNow AI Platform Instanz und schließt die Konfiguration von ab Vulnerability Response Anwendung. Diese Rolle hat vollständigen Zugriff auf Vulnerability Response(VR)-Anwendung und ihre Datensätze. Dieser Administratoranwender konfiguriert alle VR-Anwendungen, -Regeln und -Integrationen von Drittparteien.

sn_vul_sccm.configure_Integration

Anwender mit dieser Rolle konfigurieren Microsoft Anwendung „Integration von SCCM-Patch-Orchestration“. Diese Rolle enthält die granulare Rolle sn_vul_sccm.read_Integration.

sn_vul_sccm.read_Integration

Anwender mit dieser Rolle können die#Datensätze von anzeigen (schreibgeschützt)Vulnerability Response Und Microsoft SCCM-Patch-Orchestration-Integrationsanwendung und Patch-Orchestration-Daten.

sn_vul_Patch_orch.configure_Patch

Benutzer mit dieser Rolle können Patches konfigurieren und anwenden.

sn_vul_Patch_orch.read_Patch

Benutzer mit dieser Rolle können Patch-Informationen (schreibgeschützt) anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verantwortliche Vertragsgenehmigung

Weisen Sie Verwendungen den Genehmigergruppen der Genehmigerebene 1 und Genehmigerebene 2 zu, wenn übermittelte Patch-Anforderungen vor der Bereitstellung genehmigt werden sollen.

Weitere Informationen zum Zuweisen dieser Rollen mit dem Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.

CI-Suchregeln

Wenn Daten aus importiert werden Microsoft SCCM-Anwendung,#die Vulnerability Response Die Anwendung sucht automatisch nach Übereinstimmungen in Configuration Management Database (CMDB) Ressourcen-ID-Daten werden verwendet. CI-Suchregeln werden verwendet, um CIs (Assets) zu identifizieren und sie automatisch zu Datensätzen angreifbarer Elemente (VI) hinzuzufügen, wenn VIS erstellt werden. Die folgenden CI-Suchregeln werden mit dem Basissystem geliefert und verwendet, um CIs (Assets) zu identifizieren und den erkannten Elementen hinzuzufügen.

Diese Suchregel basiert auf den Daten, die vom Service Graph Connector mit SCCM eingegeben werden. Sie müssen die CMDB-Integration installieren und ausführen, bevor Sie die SCCM-Integrationen ausführen. Wenn Sie mehrere Installationen des SCCM-Servers haben, können Sie den Verbindungsalias für Service Graph Connector auf der Konfigurationsseite für SCCM-Patch-Orchestration konfigurieren.

MID-Server

Die Vulnerability Response Patch-Orchestration mit Microsoft SCCM ist eine lokale Integration. Es ist ein eigenständiges erforderlich Windows MID-Server, der nicht Teil eines MID-Server-Clusters ist. Der MID-Server ist erforderlich, um Skripts auf Remote-Computern von Ihrer Instanz aus auszuführen, um Daten vom SCCM-Server zu importieren. APIs für diese Integration werden mit MID-Servern aufgerufen, die Sie in eingerichtet haben ServiceNow AI Platform Instanz. Bereiten Sie sich auf den vor Vulnerability Response Patch-Orchestration-Integration mit Microsoft SCCM.

Integrationen und Abhängigkeiten von Vulnerability Response Patch Orchestration mit dem Microsoft SCCM-Anwendung

Die folgenden Produkt- und Abhängigkeitsanwendungen sind für die Patch-Orchestration von Vulnerability Response mit erforderlich Microsoft Integration von System Center Configuration Manager (SCCM). Diese Anwendungen sind in verfügbar ServiceNow® Store

Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch-Orchestration-Integration erforderlich sind

Dient zum Anzeigen von Patch-Orchestration-Daten und verfügbaren Updates (Patches) in den Arbeitsbereichen und der klassischen Anwenderoberfläche in Vulnerability Response, Die folgenden Anwendungen sind erforderlich. Alle aufgeführten Anwendungen sind in verfügbar ServiceNow® Store. Einige Anwendungen erfordern separate Abonnements.

Weitere Informationen zur Versionskompatibilität mit den erforderlichen Anwendungen und Familien-Releases finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema artikel in der HI Knowledge Base.

Anwendungs- und Release-Version
Vulnerability Response

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungs- und Release-Version
Vulnerability Solution Management
Anwendung „Vulnerability Response Patch Orchestration“
Vulnerability Response Patch Orchestration mit Microsoft SCCM-Anwendung
Security Support Common
Orchestration Des Sicherheitssupports
Service Graph Connector mit SCCM

Vulnerability Response Patch-Orchestration-Anwendungstabellen

Die Vulnerability Response Die Patch Orchestration-Anwendung enthält die folgenden Tabellen:

Tabelle	Beschreibung
Patch-Update [sn_vul_Patch_orch_Update]	Speichert Informationen zu den Patches, die in verschiedenen Instanzen verfügbar sind.
Geräteaktualisierung [sn_vul_Patch_orch_m2m_src_ci_Update]	Speichert Daten zu den bereitgestellten Patches zusammen mit dem Bereitstellungsstatus, die in erkannten Elementdatensätzen angezeigt werden.
Sammlung [sn_vul_Patch_orch_Collection]	Speichert Sammlungsdaten aus verschiedenen Instanzen.
Gerätesammlung [sn_vul_Patch_orch_m2m_src_ci_Collection]	Speichert Sammlungsdaten zu erkannten Elementen.
Patch-Bereitstellung [sn_vul_Patch_orch_Deployment]	Speichert Informationen zu bereitgestellten Patches zu Sammlungen und CIs.
Potenzieller Patch [sn_vul_Patch_orch_m2m_vuln_Patch]	Speichert Daten zu Patches und Schwachstellen, die die Patches identifizieren, die zur Behebung einer Schwachstelle verwendet werden können.

Vulnerability Response Patch Orchestration mit Microsoft SCCM-Integrationen

Die von entwickelten Integrationen ServiceNow® Engineering stellt die orchestrierte Lösungsbereitstellung mit zusammen Microsoft SCCM-Produkt. Die folgenden Integrationen sind in der Anwendung Microsoft SCCM Patch Orchestration Integration enthalten, die Sie aus herunterladen ServiceNow® Store.

Nachdem Sie die Integrationsanwendung auf Ihrem installiert haben ServiceNow AI Platform Instanz, um diese Integrationen anzuzeigen, navigieren Sie zu **Integrationen** > **Integration von SCCM-Patch-Orchestration** > **Integrationen**an. Die Vulnerability Response Die Anwendung verarbeitet Daten in geplanten Zeitintervallen, die von diesen Integrationen mit importiert werden Microsoft SCCM-Endpunkte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
Microsoft Integration der SCCM-Sammlung	• Diese Integration ist für die tägliche Ausführung geplant und wird zuerst in der verketteten Integrationsausführung ausgeführt. • Ruft die Gerätesammlungen aus den SCCM-Sammlungen ab.
Microsoft Integration der SCCM-Gerätesammlung	• Bei der Planung wird diese Integration durch Abschluss der SCCM-Sammlungsintegration ausgelöst. Sie können es auch bei Bedarf ausführen. • Diese Integration ruft die Geräte in jeder Sammlung ab. Diese Integration erstellt Datensätze in der Tabelle „erkannte Elemente“ und der Tabelle „Gerätesammlung“.
Microsoft Integration von SCCM-Patch-Update	• Bei der Planung wird diese Integration durch Abschluss der Integration der SCCM-Gerätesammlung ausgelöst. Sie können es auch bei Bedarf ausführen. • Ruft Informationen vom SCCM-Server zu den Patches ab, die auf Geräten (Assets) installiert sind oder fehlen.
Microsoft Integration von SCCM-Bereitstellungen	• Bei der Planung wird diese Integration durch Abschluss der Patch-Update-Integration ausgelöst. Sie können es auch bei Bedarf ausführen. • Ruft Informationen zu den Patches ab, die vom IT-Team auf dem SCCM-Server geplant wurden.

Bereiten Sie sich auf den vor Vulnerability Response Patch-Orchestration-Integration mit Microsoft SCCM

Bereiten Sie sich auf die Integration vor, indem Sie die folgenden Setup-Aufgaben ausführen.

Vorbereitungen

Erforderliche Rollen: administrator für die Installation der Anwendungen und die Zuweisung von Rollen. Andere Rollen sind in der folgenden Tabelle aufgeführt.

Warum und wann dieser Vorgang ausgeführt wird

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration.

Prozedur

1. Für eine reibungslose Installation und Konfiguration von Vulnerability Response Patch Orchestration mit Microsoft SCCM-Anwendung befolgen Sie die unten angegebene Prüfliste.
2. Möglicherweise möchten Sie die folgende Prüfliste ausdrucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Schwachstellen- und Patch-bezogene Informationen in importieren ServiceNow AI Platform® Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

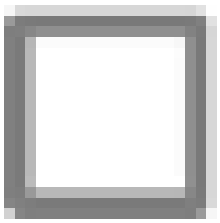
Aufgabe	Beschreibung
☐	(Optional) wenn Sie nicht bereits installiert und aktiviert sind, möchten Sie möglicherweise installieren Vulnerability Response Anwendung vor der Installation der Drittanbieteranwendung. Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe, Vulnerability Response installieren. Diese Integration erfordert Version 16,1 von Vulnerability Response Oder später.
☐	Wenn nicht bereits installiert, rufen Sie Berechtigungen ab, und installieren Sie eine Scanner-Anwendung von Drittanbietern, um Schwachstellendaten zu importieren. Siehe Vulnerability Response-Integrationen Weitere Informationen zu Scannern von Drittanbietern, die von unterstützt werden Vulnerability Response. Weitere Informationen finden Sie unter .
☐	Wenn nicht bereits installiert, rufen Sie Berechtigungen ab, und laden Sie die Vulnerability Response Patch Orchestration mit herunter Microsoft SCCM-Anwendung für Ihren ServiceNow AI Platform® Instanz. Weitere Informationen finden Sie unter .
☐	Erhalten Microsoft SCCM-Anmeldeinformationen. Stellen Sie sicher, dass Sie Accountnamen, Passwörter und andere Serviceinformationen haben, die für erforderlich sind Microsoft Produkte, damit Sie Zugriff darauf haben.
☐	Stellen Sie sicher, dass Sie Gruppen oder Anwender haben, um die Integrationen zu verwalten und angreifbare Elemente zu korrigieren. **Administrator** Der Systemadministrator ruft Berechtigungen ab, lädt herunter und installiert Microsoft SCCM-Patch-Orchestration-Anwendung und die anderen für die Integration erforderlichen Anwendungen. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.Vulnerability_admin) und andere Rollen im Setup-Assistenten in zu Vulnerability Response Oder aus dem Modul Anwenderverwaltung. **sn_vul.vulnerability_admin**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration von ab Microsoft SCCM-Integrationen und die anderen Drittanbieteranwendungen. Diese Rolle hat vollständigen Zugriff auf Vulnerability Response(VR)-Anwendung und ihre Datensätze. Diese Rolle konfiguriert alle VR-Anwendungen, -Regeln, -Integrationen von Drittparteien, Vulnerability Response Patch-Orchestration- und Schwachstellenlösungsmanagement-Anwendungen. **sn_vul_sccm.configure_Integration** Anwender mit dieser Rolle konfigurieren Microsoft Anwendung „Integration von SCCM-Patch-Orchestration“. Diese Rolle enthält die granularen Rollen sn_vul_sccm.read_Integration und connection_admin, die es dem Anwender ermöglichen, eine Verbindung zur SCCM-Konsole herzustellen und die Integrationsinstanzen in zu konfigurieren ServiceNow AI Platform. **sn_vul_sccm.read_Integration** Anwender mit dieser Rolle können die#Datensätze von anzeigen (schreibgeschützt) Vulnerability Response Und Microsoft SCCM-Patch-Orchestration-Integrationsanwendung und Patch-Orchestration-Daten. **sn_vul_Patch_orch.configure_Patch** Benutzer mit dieser Rolle können Patches konfigurieren und anwenden. Patches, die von diesem Anwender aus Datensätzen für angreifbare Elemente und Patch-Updates angefordert werden, werden zur Genehmigung gesendet, wenn das Change-Management aktiv ist und Genehmiger zugewiesen werden. **sn_vul_Patch_orch.read_Patch** Benutzer mit dieser Rolle können Patch-Informationen in Datensätzen (schreibgeschützt) anzeigen. Diese Rolle wird mit den Rollen „sn_vul.Remediation_owner“ und „sn_vuln.Vulnerability_Analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind. **Verantwortliche Vertragsgenehmigung** Anwender, die der Genehmigerebene 1 und optional Genehmigergruppen der Genehmigerebene 2 zugewiesen sind, genehmigen übermittelte Patch-Anforderungen. Standardmäßig werden Patches vor der Bereitstellung zur Genehmigung an die Genehmigerebene 1-Gruppe übermittelt. Weitere Informationen zum Genehmigungsprozess finden Sie unter Konfigurieren Sie die Patch-Orchestration für Vulnerability Response mit Microsoft SCCM-Integration. Weitere Informationen zum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Einrichten von Genehmigern und Gruppen finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Der Systemadministrator führt die anfängliche Zuweisung von Rollen an Anwender und Gruppen für die Integration durch. Standardmäßig ist Vulnerability Response Gruppe ist verfügbar. Wenn Sie noch nicht erstellt haben, können Sie zusätzliche Gruppen für die Rollen von Korrekturspezialisten und Schwachstellenanalysten erstellen und Anwender mit dem Modul „Anwenderverwaltung“ in Ihrer Instanz hinzufügen. Siehe Erstellen Sie eine Anwendergruppe .
	Stellen Sie sicher, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Aufträge in Ihrer Instanz aktiviert haben, die für die Integration erforderlich sind. ○ Die Vulnerability Response Patch-Orchestration mit Microsoft SCCM ist eine lokale Integration, die die Verwendung einer eigenständigen erfordert Windows MID-Server. Weitere Informationen zu MID-Servern in Ihrer Instanz finden Sie unter MID-Server . ○ Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** Und suchen Sie das Plugin. Wenn nicht in Ihrer Instanz installiert, installieren und aktivieren Sie sie.

Installieren Sie Vulnerability Response Patch-Orchestration mit Microsoft SCCM-Anwendung

Laden Sie die Anwendung aus dem herunter ServiceNow Store.

Vorbereitungen

Vergewissern Sie sich vor der Installation der Anwendung, dass Sie alle Elemente in der Prüfliste in abgeschlossen haben Bereiten Sie sich auf den vor Vulnerability Response Patch-Orchestration-Integration mit Microsoft SCCM.

Erforderliche Rollen: administrator für die anfängliche Zuweisung der Rolle „sn_vul.Vulnerability_admin“ und die Installation der Anwendung. Schwachstellenadministrator (sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) zum Konfigurieren von Vulnerability Response Patch-Orchestration Microsoft SCCM und andere Anwendungen, nachdem sie installiert wurden.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Unterproduktions- oder Entwicklungsinstanzen herunterladen, ist es nicht erforderlich, die Berechtigung zu erhalten. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
2. Suchen Sie nach **Vulnerability Response Patch Orchestration mit Microsoft SCCM** Anwendung und klicken Sie auf **Installieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit dieser Aktion wird die Anwendung installiert, die Sie aus heruntergeladen haben ServiceNow Store.

3. Alternativ können Sie Anwendungen über den Setup-Assistenten installieren.
   Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.

Nächste Maßnahme

Navigieren Sie nach Abschluss der Installation zu **Alle** > **Integration von Microsoft SCCM Patch Orchestration** > **Konfiguration** Um mit der Konfiguration fortzufahren.

Konfigurieren Sie die Patch-Orchestration für Vulnerability Response mit Microsoft SCCM-Integration

Nachdem Sie die Anwendung installiert haben, konfigurieren Sie sie mit Ihren Accountinformationen, und validieren Sie Ihre Anmeldeinformationen.

Vorbereitungen

Erforderliche Rollen: sn_vul.Vulnerability_admin und sn_vul_sccm.configure_Integration

Prozedur

1. Navigieren zu **Alle** > **Integration von Microsoft SCCM Patch Orchestration** > **Konfiguration**an.
2. Füllen Sie die Felder mit aus Microsoft SCCM-Informationen und -Anmeldeinformationen.

Feld	Beschreibung
Integrationsinstanz	Der Name des Microsoft SCCM-Instanz-Account, den Sie verwenden möchten, z. B. Microsoft SCCM-Patch-Management-Integration .
Hostname	Geben Sie die URL für ein Microsoft SCCM-Host.
Anwendername	Geben Sie ein Microsoft SCCM-Account-Anwendername.
Passwort	Geben Sie ein Microsoft SCCM-Account-Passwort.
MID-Server	Geben Sie den Namen des eigenständigen MID-Servers aus der Liste ein, den Sie verwenden möchten. Siehe Bereiten Sie sich auf den vor Vulnerability Response Patch-Orchestration-Integration mit Microsoft SCCM Weitere Informationen zu MID-Servern und Einrichtungsaufgaben in finden Sie in ServiceNow AI Platform®.

3. Klicken Sie auf Anmeldeinformationen speichern und testen.
   Der Status Ihrer Verbindung zwischen Microsoft SCCM und Ihr ServiceNow AI Platform® Instanz#wird im Feld Validierungsstatus angezeigt. Wenn kein erfolgreicher Test angezeigt wird, befolgen Sie die Anweisungen.
4. **Wahlweise:** Domänentrennung wird für diese Integration unterstützt.
   Sie können Ihrer Instanz mehrere Konfigurationen von hinzufügen. So fügen Sie zusätzliche Konfigurationen hinzu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Alle** > **Integration von Microsoft SCCM Patch Orchestration Integrationsinstanzen** .

b. Überprüfen Sie den Anwendungsbereich, Vulnerability Response Patch Orchestration mit Microsoft SCCM , Wird im Feld Anwendungsbereich angezeigt.

c. Klicken Sie auf **Neu**.

d. Füllen Sie das Formular aus.

Feld	Beschreibung
Name	Name für die Integrationsinstanz.
Anwendung	Vulnerability Response Patch Orchestration mit Microsoft SCCM
Integration	[Schreibgeschützt] Microsoft SCCM-Patch-Management ist der Standard.
Aktiv	Standard ist aktiviert. Wenn diese Option deaktiviert ist, ist die Instanz nicht aktiv.

e. Klicken Sie auf **Absenden**.
Ihre neue Integrationsinstanz wird in der Liste „Integrationsinstanzen“ angezeigt.

f. Wiederholen Sie die Schritte 1-3, um Ihre Integrationsinstanz zu konfigurieren und Ihre Anmeldeinformationen zu testen.

5. Richten Sie Genehmigungen für Patch-Anforderungen ein.
Standardmäßig ist eine Systemeigenschaft [**sn_vul_Patch_orch.Patch_Approval_required**] Ist aktiviert, sodass Patch-Bereitstellungen bei der Planung zur Überprüfung und Genehmigung an Anwender übermittelt werden, die der Genehmigungsgruppe „Patch-Update“ der Ebene 1 zugewiesen sind.

Wenn Anwender mit der Rolle „sn_vul_Patch_orch.configure_Patch“ Patches ohne Genehmigung planen sollen, können Sie [. Deaktivieren **sn_vul_Patch_orch.Patch_Approval_required**] Eigenschaft. Möglicherweise möchten Sie Genehmigungen aktivieren lassen, damit geplante Patches nicht mit den normalen Arbeitszeiten in Konflikt stehen.

Hinweis:
Wenn Sie die Systemeigenschaft „Genehmigung“ deaktivieren, kann jeder Anwender mit der Rolle „sn_vul_Patch_orch.configure_Patch“ Patches ohne Überprüfung und Genehmigung planen und bereitstellen.

So deaktivieren Sie als Anwender mit der Rolle sn_vul.Vulnerability_admin die Systemeigenschaft:

a. Navigieren zu **Alle** > **sys.properties.list**an.

b. Suchen **sn_vul_Patch_orch.Patch_Approval_required** Und klicken Sie darauf, um den Datensatz zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Geben Sie im Feld Wert ein Falsch .

d. Klicken Sie auf **Aktualisieren**.

6. Wenn Sie diese Eigenschaft nicht deaktivieren, müssen Sie Genehmiger für Patch-Anforderungen zuweisen. Führen Sie als Benutzer mit der Rolle sn_vul.Vulnerability_admin die folgenden Schritte aus.

a. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Genehmigungsregeln**an.

b. Wenn **Genehmigung für Patch-Update bereitstellen** Genehmigungsregel wird nicht in der Liste angezeigt. Klicken Sie auf **Alle** Rechts neben dem grünen Filtersymbol oben links im Bildschirm, um die gesamte Liste anzuzeigen.

c. Klicken Sie in der Liste auf **Genehmigung für Patch-Update bereitstellen** .

d. Klicken Sie im Datensatz bei ausgewählter Registerkarte Genehmigungskonfiguration auf **Genehmigung des Patch-Updates für Standardkonfiguration** .

e. Klicken Sie im Datensatz auf **Ebene 1: Patch-Update-Genehmigung** .

f. Fügen Sie dieser Gruppe Anwender hinzu.

Die dieser Gruppe zugewiesenen Anwender genehmigen Patch-Anforderungen, die von Anwendern mit der Rolle „sn_vul_Patch_orch.configure_Patch“ übermittelt werden. Navigieren Sie zu **Meine Genehmigungen** Zum Anzeigen und Verarbeiten der Anforderungen.

7. Klicken Sie Auf **Aktualisieren** Um Ihre Änderungen zu speichern.

8. **Wahlweise:** Sie können Genehmigungen auf mehreren Ebenen einrichten, sodass vor der Bereitstellung geplanter Patch-Anforderungen mehr als eine Genehmigung erforderlich ist.

a. Klicken Sie auf, während der Genehmigungsdatensatz für das Update des Standardkonfigurations-Patches angezeigt wird **Neu** .

b. Füllen Sie die Felder aus.

Feld	Beschreibung
Name	Name der Genehmigungsebene, z. B. **Ebene 2: Patch-Update-Genehmigung** .
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird.
Erforderliche Genehmigung	Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind: ▪ Ein Genehmiger erforderlich ▪ Alle Anwender müssen genehmigen
Reihenfolge	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Auftragseintrag von 100 vor einer Konfiguration mit einem Auftragseintrag von 200 ausgeführt.
Rolle	Wählen Sie eine Rolle für die Gruppe aus der Liste aus.
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel.
Genehmigungskonfiguration	Enthält die Genehmigungskonfigurationen.
Zuweisen mit	Wählen Sie eine Option aus: ▪ Anwender und Anwendergruppe ▪ Genehmigungstabellenfeld ▪ Skript
Gruppen	Genehmigerebenengruppe, die aus mehreren Anwendern besteht. Der Anwender muss über eine der folgenden von Ihnen angegebenen Rollen verfügen.
Anwender	Bearbeiten Sie die in den Gruppen aufgeführten Anwender.

c. Klicken Sie Auf **Übermitteln** Um Ihre Änderungen zu speichern.

Patch-Daten und Patch-Daten-Rollup für anzeigen Vulnerability Response Orchestration-Integration mit patchen Microsoft SCCM

Patch-Daten und Patch-Rollup-Daten sowie Informationen zu Schwachstellen und Korrekturstatus Ihrer Schwachstellen werden in Datensätzen in Ihrer Instanz angezeigt.

Patch-Daten in anzeigen Vulnerability Response Arbeitsbereiche

Erforderliche Rollen:

- Rolle „sn_vul_Patch_orch.configure_Patch“ zum Konfigurieren und Planen von Patches
- sn_vul_Patch_orch.read_Patch zum Anzeigen (schreibgeschützten) Patch-Informationen in Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.Remediation_owner“ und „sn_vuln.Vulnerability_Analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind

Im Arbeitsbereich „IT-Korrektur“ können Sie die Patches anzeigen:

- In der Startseite-Ansicht, in der Sie auf Bewertungslisten klicken können, um Datensätze für bevorzugte Lösungen für VIS, angreifbare CIs und bevorzugte Patches für VIS anzuzeigen.
- In der Listenansicht, in der Sie alle Patch-Update-Datensätze (VPUs) über die Patches-Links und die Ihnen zugewiesenen angreifbaren Elemente (Vits) mit Patches anzeigen können.

Sie können Patches aus den folgenden Datensätzen planen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aus Patch-Update (VPU)
- Korrekturaufgabe (RT)
- Erkannte Elementdatensätze (SDI)

Im Vulnerability Manager-Arbeitsbereich können Sie Patches anzeigen:

- In der Startansicht zu Überwachungsthemen können Sie bevorzugte und potenzielle Patches, geplante Patchdaten und, ob der Patch heruntergeladen wurde, alle auf anzeigen **Angreifbare Elemente** Registerkarte.
- In der Listenansicht zu Korrekturmaßnahmen, in der Sie Patch-Daten in VI-Datensätzen aus anzeigen können **Angreifbare Elemente** Registerkarte.

Navigieren Sie in der klassischen Umgebungsansicht zu **Alle** > **Vulnerability Response** > **Patches**an.

Patch-Update-Datensätze in den VR-Arbeitsbereichen und in der klassischen Umgebungsansicht

Patch-Daten und Patch-Rollup-Daten und -Status werden in Datensätzen in Ihrer Instanz angezeigt. Patch-Datensätze sind als Teil der Patch-Orchestration-Funktion dieser Integration mit enthalten Vulnerability Response. Zeigen Sie Patch-Datensätze (VPU) in an Vulnerability Response Arbeitsbereiche aus der Listenansicht im IT-Korrekturarbeitsbereich. Patch-Update-Datensätze sowohl in der klassischen Umgebung als auch Vulnerability Response Arbeitsbereiche enthalten die folgenden Daten:

- Daten und Informationen der Schwachstellenlösung von Patch-Lieferanten, die von der Anwendung „Schwachstellenlösungsmanagement“ importiert wurden.
- Quellkorrekturstatus, der die Gesamtzahl der Geräte mit einer bestimmten Schwachstelle enthält, die durch einen Patch behoben werden kann. Darüber hinaus enthält es auch und alle Geräte, für die Updates fehlen.
- Korrekturstatus, der % der korrigierten VIS und die Gesamtzahl der VIS enthält, die einen Patch als bevorzugten Patch haben.
- Zugeordnete Geräte, angreifbare Elemente, Patch-Bereitstellungen und Patch-Anforderungen in den zugehörigen Links zu Datensätzen in der Klassenansicht. Diese Daten werden auf Registerkarten in Datensätzen in angezeigt Vulnerability Response Arbeitsbereiche.
- Patch-Anforderungen, die Korrekturbesitzer zur Genehmigung übermittelt haben.

Status-Rollup für Datensätze angreifbarer Elemente

Weitere Informationen zum Status-Rollup zu Datensätzen finden Sie unter Patch-Daten- und Status-Rollup für Patch-Orchestration in Vulnerability Response.

Datensätze, in denen die Anzahl aktiver VI zusammengefasst wird

Um ein Rollup aller Patches für alle Schwachstellen zu vermeiden, erfasst die geplante Aufgabe nur Änderungen an der Anzahl der aktiven VI. Diese Anzahländerungen und zugehörigen Daten werden in für die folgenden Datensätze zusammengefasst Vulnerability Response:

- VIT
- RT

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schwachstellenlösung
- Patch-Update

Anzeigen von Daten für Patches ohne Lösungen

Weitere Informationen zum Anzeigen von Patches ohne Lösungen finden Sie unter Zeigen Sie Patches ohne Lösungen in an Vulnerability Response.

Daten mit patchen Vulnerability Response

Die Dashboards Vulnerability Management (PA) und CISO sind in einem Abonnement von enthalten Performance Analytics Für Vulnerability Response Anwendung. Wenn Sie ein Abonnement für haben Performance Analytics, Ist jedoch keine Patch-Orchestration-Integration installiert, die Registerkarte „Korrektur“ wird im CISO-Dashboard angezeigt, aber nicht mit Daten gefüllt.

Navigieren Sie für das Dashboard Vulnerability Management (PA) zu **Alle** > **Vulnerability Response** > **Übersicht**an. Klicken Sie auf **Korrektur** Registerkarte und scrollen Sie zum unteren Seitenrand, um Patch-Updates-Daten anzuzeigen: Geplante und nicht geplante Patches, Patches ohne Zieldaten und wöchentliche Anzahlen.

Navigieren Sie für das CISO-Dashboard zu **Alle** > **Vulnerability Response** > **CISO-Dashboard**an. Wenn die Registerkarte Übersicht ausgewählt ist, scrollen Sie zum Ende der Seite, um Daten zur Patch-Abdeckung anzuzeigen: Relevanz, geplante und nicht geplante Patches und Patches ohne Zieldaten.

Weitere Informationen zu finden Vulnerability Response Dashboards, siehe Wird standardmäßig verwendet Vulnerability Response Dashboards, Patch-Orchestration mit Vulnerability Response Arbeitsbereiche, Und Patch-Orchestration-Daten in anzeigen Vulnerability Response Dashboards.

Planen Sie Patches mit Microsoft SCCM-Integration mit Vulnerability Response

Planen Sie Patches aus Datensätzen für Patch-Update- und Korrekturaufgaben in der Vulnerability Response Anwendung in Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen
Ab Version 16.1 können Sie Patches aus dem planen Vulnerability Response Arbeitsbereiche oder aus der klassischen Umgebung.

Erforderliche Rollen:

- Rolle „sn_vul_Patch_orch.configure_Patch“ zum Konfigurieren und Planen von Patches
- sn_vul_Patch_orch.read_Patch zum Anzeigen (schreibgeschützten) Patch-Informationen in Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.Remediation_owner“ und „sn_vuln.Vulnerability_Analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind

Prozedur

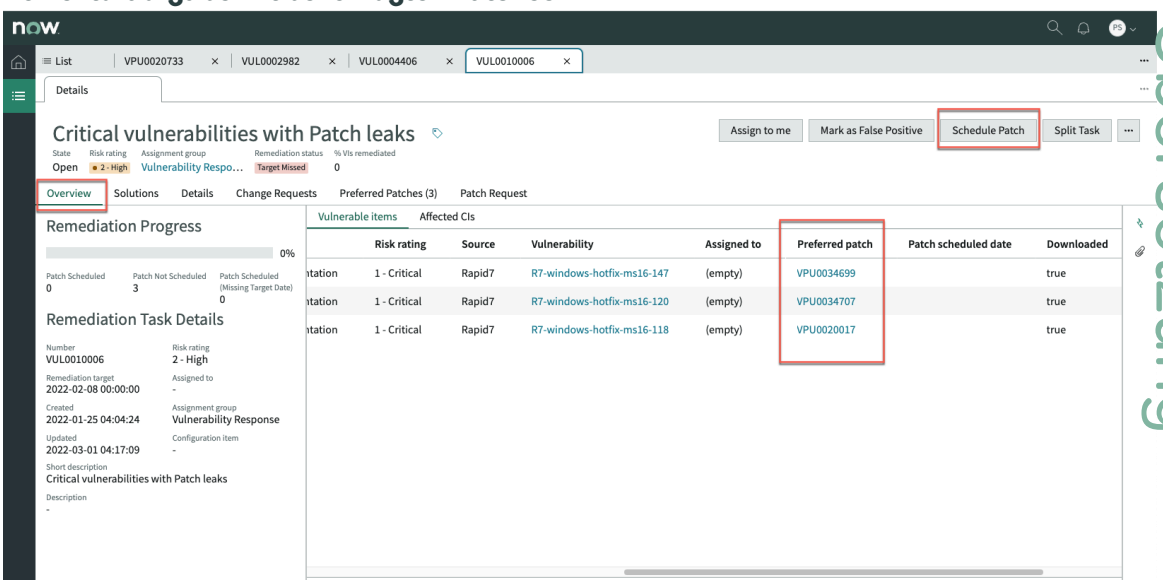
1. In der Schwachstelle Vulnerability Response Arbeitsbereiche navigieren als Anwender mit der Rolle „sn_vul.Remediation_owner“ zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**an.
2. Klicken Sie auf der Homepage auf **Bevorzugter Patch für VIS** .
   Die Liste der Patch-Update-Datensätze für die VIS mit bevorzugten Patches, die Ihnen zugewiesen sind, wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Suchen Sie einen Datensatz, den Sie öffnen möchten, und klicken Sie, um ihn zu öffnen.
4. Alternativ können Sie in der Listenansicht im Arbeitsbereich auf klicken **Patches** > **Alle** Und suchen Sie einen Patch-Update-Datensatz.
   Der Patch-Update-Datensatz wird angezeigt. Sie sollten die Daten möglicherweise überprüfen, bevor Sie einen Patch planen, da möglicherweise bereits andere Patches geplant sind.
5. In der folgenden Tabelle erfahren Sie, welche Daten im Arbeitsbereich „IT-Korrektur“ angezeigt werden und was Sie tun können.
6. Klicken Sie Auf **Patch Planen** .
7. Füllen Sie die Felder im Dialogfeld aus.
8. Klicken Sie auf **Bereitstellen**.
   Die Patch-Anforderung wird zur Überprüfung an gesendet. Sie können den Status aller Ihrer übermittelten Anforderungen in anzeigen **Ausnahmeanforderungen** > **Meine Anforderungen** In der Listenansicht.
9. Alternativ können Sie Patches aus Korrekturaufgaben (RT) planen, die Ihnen oder Ihrer Gruppe zugewiesen sind.

Hinweis:
Die Option zum Planen eines Patches aus einem Korrekturaufgabendatensatz ist nur verfügbar, wenn Patches den VIS in der Aufgabe zugeordnet (zugeordnet) sind. Diese Patches werden in der Spalte „bevorzugter Patch“ angezeigt, wenn Sie bei ausgewählter Registerkarte „Übersicht“ nach rechts neben einem Korrekturaufgabendatensatz scrollen.

Korrekturaufgabe mit bevorzugten Patches



10. Klicken Sie Auf **Patch Planen** Aus dem RT-Datensatz und führen Sie die oben aufgeführten Schritte aus, um ihn im Dialogfeld zu planen.
11. **Wahlweise:** In der klassischen Umgebung können Sie Patches für die zuvor beschriebenen Schritte planen. Um diese Datensätze zu finden, führen Sie die folgenden Schritte aus.
    a. Navigieren Sie in der klassischen Umgebung zu **Alle** > **Vulnerability Response** > **Patches** > **Alle**an.
    b. Suchen Sie in der angezeigten Liste nach einem Patch-Update-Datensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Navigieren Sie für Korrekturaufgaben zu **Vulnerability Response** > **Korrekturaufgaben** Und suchen Sie einen Datensatz.
Verfolgen Sie den Korrekturstatus auf der Registerkarte Korrekturstatus. Am unteren Rand des Datensatzes werden Patch-Daten in den zugehörigen Links angezeigt.

d. Klicken Sie Auf **Patch Planen** Und füllen Sie die Felder aus.

Feld	Beschreibung
Bereitstellungsname	Geben Sie einen Namen für diese Patch-Bereitstellung ein. Dieser Name hilft Ihnen, Ihre Updates nachzuverfolgen.
Beschreibung	Fügen Sie mehr Text für über den Patch hinzu. Diese Informationen werden im Feld Beschreibung des Patch-Update-Datensatzes angezeigt.
Bereitstellungstyp	Wählen Sie eine Option aus der Liste aus. ▪ Erforderlich: Dieser Patch ist ein erforderliches Update. ▪ Verfügbar: Dieser Patch ist nicht erforderlich, aber für die Bereitstellung verfügbar.
Sammlung	Wählen Sie eine Sammlung (Gruppe von Assets) aus der Liste aus, um fortzufahren. Diese Gruppen sind die aus SCCM importierten Asset-Sammlungen.
Bereitstellungszeit basierend auf	Wählen Sie eine Zeitzone aus der Liste aus, auf der Ihr Bereitstellungszeitfenster basieren soll.
Verfügbare Zeit	Legen Sie den Wert für den Zeitpunkt fest, zu dem der Patch zum ersten Mal für die Bereitstellung verfügbar wird.
Frist	Legen Sie die Frist fest. Dieser Wert gibt den letzten Tag an, an dem der Patch installiert werden kann.

e. Klicken Sie auf **Bereitstellen**.

REST-Nachrichten für Vulnerability Response Patch-Orchestration mit Microsoft SCCM

Die Vulnerability Response Patch-Orchestration mit Microsoft SCCM verwendet die Klassen SCCM Windows Management Instrumentation (WMI), um die SCCM-Server-API aufzurufen.

Übersicht über REST-Nachrichten

Die SMS-Anbieter Bietet API einen Interoperability-Zugriff über HTTPS, den sogenannten Administrationsservice. Der Administrationsservice ist eine REST-API (Repositorational State Transfer), die auf dem OData-v4-Protokoll (Open Data) basiert.

Siehe Was ist der Administrationsservice in Configuration Manager Um weitere Informationen zum Administrationsservice zu erhalten, verwenden Sie diese Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Da die erforderliche Authentifizierung das NTLM-Protokoll von Windows New Technology LAN Manager verwendet, werden Aufrufe an die APIs über den MID-Server mithilfe von PowerShell-Skripts getätigt.

Microsoft SCCM-Integration

Sie können die REST-Nachricht für verwenden Microsoft SCCM-Integration, von der Informationen abgerufen werden sollen Microsoft SCCM. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die an gestellten Anforderungen aus Microsoft SCCM zum Abrufen von Informationen. REST-Nachrichten enthalten die folgenden REST-Methoden.

WMI-Klassennamen:

- SMS_Collection
- SMS_DeploymentSummary

Parametername	Wert	Beschreibung
URL	Dynamische Werte basierend auf Anwender	Gibt den Endpunkt der SCCM-Konsole an

Microsoft SCCM-Patch bereitstellen

Sie können die REST-Nachricht für die Microsoft SCCM-Integration verwenden, um Patches von Ihrem zu planen ServiceNow AI Platform® Zu Microsoft SCCM. Änderungen an der Datensatzmethode der REST-Nachricht wirken sich auf die Anforderungen an SCCM zum Abrufen von Informationen aus. REST-Nachrichten enthalten die folgenden REST-Methoden.

REST-Methode	Beschreibung
Patch NACH der Bereitstellung	Plant den Patch für die SCCM-Konsole auf einem einzelnen/mehreren Computern.

Parametername	Wert	Beschreibung
URL	Dynamische Werte basierend auf Anwender	Gibt den Endpunkt der SCCM-Konsole an.
Titel	Dynamische Werte basierend auf Anwender	Titel der Bereitstellung.
Settings_Tag	XML-Tag-benannte Einstellungen mit Werten	Gibt Einstellungen an, die unterschiedliche Parameter haben und während der Planung des Patches an SCCM gesendet werden.
Computer_Tag	XML-Tag-benannte Computer mit Werten	Gibt eine Liste der Computer an, auf denen der Patch geplant wird.
site_name	Wert aus Patch-Update	Name der Site, auf der der Patch vorhanden ist.
Patch_ID	Wert aus Patch-Update	ID des Patches.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datentransformation für die Patch-Orchestration mit Microsoft SCCM-Integration

Daten werden aus der Patch-Orchestration mit abgerufen Microsoft SCCM-Integration, verarbeitet durch eine Reihe von Datenquellen und in umgewandelt ServiceNow AI Platform® Instanz.

SCCM-Sammlungsimport

Die Daten aus den importierten Sammlungen werden in die Tabelle „SCCM-Sammlungsimport“ [sn_vul_sccm_Collection_Import] geladen. Die SCCM-Sammlungen (Transformationszuordnung) werden zum Transformieren der importierten Informationen verwendet.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem SCCM-Sammlungsimport verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie SCCM-Sammlungstransformation. In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Quellenfeld	Zielfeld	Beschreibung
u_collectionid	source_id	Eindeutige ID der Sammlung.
u_name	name	Name der Sammlung
u_member-Anzahl	Device_count	Anzahl der Geräte in dieser Sammlung.
[Skript]	Integration_instance	Name der Instanz, aus der der Patch importiert wird.

SCCM-Sammlungsimport – Transformationsskript-Timing

Skript	Beschreibung
OnStart (wenn ein Importsatz eine Transformation erstellt hat).	Skript zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_sccm] für den Integrationsprozess. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Das Skript, das zum Aktualisieren der Werte in der Bereichsvariablen [sn_vul_sccm] verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Import von SCCM-Patch-Updates

Die Daten aus den importierten Patches werden in die Tabelle „SCCM-Patch-Update-Import“ [sn_vul_sccm_Patch_Update_Import] geladen.

Die SCCM-Patch-Update-Transformation wird verwendet, um die importierten Informationen zu transformieren.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem SCCM-Patch-Update-Import verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie die SCCM-Patch-Update-Transformation.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Transformationszuordnungsfelder für SCCM-Patch-Update-Import

Quellenfeld	Zielfeld	Beschreibung
[Skript]	URLs	URLs für den Patch.
u_nummissing	num_missing	Anzahl der Geräte ohne diesen Patch.
[Skript]	Date_Release	Patch-Release-Datum.
u_bulletinid	Bulletin_ID	Bulletin-ID für den Patch.
u_numtotal	num_total	Gesamtzahl der Geräte.
u_localizeddescription	Beschreibung	Beschreibung für den Patch.
[Skript]	Is_highest_supersedence	Ist der Patch mit dem höchsten Ersatz.
u_numnotanwendbar	num_Not_applicable	Anzahl der Geräte, die für diesen Patch nicht gelten.
u_iscontentbereitgestellt	Ist_heruntergeladen	Wenn Patch auf den SCCM-Server heruntergeladen wird.
u_numunbekannt	num_unknown	Gesamtzahl der unbekannten Geräte.
u_articleid	artikel_ID	Artikel-ID des Patches.
u_localizeddisplayname	Titel	Titel des Patches.
u_ci_ID	source_id	Eindeutige ID für den Patch in SCCM.
u_numpresent	num_present	Anzahl der Geräte, auf denen der Patch installiert ist.
[Skript]	Integration_instance	Name der Instanz, aus der der Patch importiert wird.
[Skript]	sn_vul_Solution	Lösung basierend auf der Quell-ID.
[Skript]	Last_modified	Datum der letzten Patch-Änderung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transformationszuordnungsfelder für SCCM-Patch-Update-Import (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_severity	Source_severity	Schweregrad des Patches.

SCCM-Patch-Update – Import der Transformationszuordnung – Skriptzeit

Skript	Beschreibung
OnStart (wenn ein Importsatz eine Transformation erstellt hat).	Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Das Skript, das zum Aktualisieren der Werte in der Bereichsvariablen [sn_vul_sccm] verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Import von SCCM-Geräte-Patch-Updates

Die Daten aus den importierten relevanten Patches auf Geräten werden in die Tabelle „Import von SCCM-Geräte-Patch-Updates“ [sn_vul_sccm_device_Patch_Import] geladen.

Die SCCM-Geräte-Patch-Update-Transformation wird verwendet, um die importierten Informationen zu transformieren.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import des SCCM-Geräte-Patch-Updates verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie die SCCM-Geräte-Patch-Update-Transformation.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

SCCM-Geräte-Patch-Update – Skriptzeitpunkt der Transformationszuordnung

Skript	Beschreibung
OnStart (wenn ein Importsatz eine Transformation erstellt hat).	Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCCM-Geräte-Patch-Update – Skriptzeitpunkt der Transformationszuordnung (Fortsetzung)

Skript	Beschreibung
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Erstellen und Aktualisieren von CIs basierend auf CI-Suchregeln und -Patches sowie der Beziehung zwischen ihnen verwendet wird. Basierend auf den Ergebnissen ändert dieses Skript die Werte in der Bereichsvariablen [sn_vul_sccm]. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Import der SCCM-Gerätesammlung

Die Daten aus den importierten Gerätesammlungen werden in die Tabelle „Import der SCCM-Gerätesammlung“ [sn_vul_sccm_device_Collection_Import] geladen.

Die Importumwandlung der SCCM-Gerätesammlung wird verwendet, um die importierten Informationen zu transformieren.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import der SCCM-Gerätesammlung verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie die SCCM-Gerätesammlungstransformation.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Zeitplan der Umwandlungszuordnung für Gerätesammlungsimport

Skript	Beschreibung
OnStart (wenn ein Importsatz eine Transformation erstellt hat).	Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Das Skript, das zum Erstellen und Aktualisieren von CIs basierend auf den CI-Suchregeln und -Sammlungen sowie der Beziehung zwischen ihnen verwendet wird. Basierend auf den Ergebnissen ändert dieses Skript Werte in der Bereichsvariablen [sn_vul_sccm]. Dieses Skript ist zur internen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitplan der Umwandlungszuordnung für Gerätesammlungsimport (Fortsetzung)

Skript	Beschreibung
	Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Transformationszuordnungsfelder für Import der SCCM-Gerätesammlung

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Eindeutige ID einer Aktion.
U_Name	name	Name der Aktion
[Skript]	SN_vul_sccm_detected_item	Referenz des erkannten Elements, für das der Patch bereitgestellt wird
U_Status	status	Status der Aktion
[Skript]	SN_vul_Patch_orch_Update	Referenz des Patches
U_apply_count	Count_success	Erfolgsanzahl der Aktion.
U_retry_count	Erneut versuchen	Anzahl der Wiederholungen der Aktion.
[Skript]	Deployment_time	Startzeit der Aktion.
[Skript]	Frist	Endzeit der Aktion.
[Skript]	Source_created	Erstellungszeit der Aktion.
[Skript]	Integration_instance	Name der Instanz, aus der die Aktion importiert wird.

SCCM-Bereitstellungsimport

Die Daten aus importierten Bereitstellungen werden in die Tabelle „SCCM-Bereitstellungsimport“ [sn_vul_sccm_Deployment_Import] geladen.

Die SCCM-Bereitstellungsimporttransformation wird verwendet, um die importierten Informationen zu transformieren.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem SCCM-Bereitstellungsimport verarbeitet werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Alle** > **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie die SCCM-Bereitstellungstransformation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCCM-Bereitstellungstransformationsfelder

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Eindeutige ID einer Bereitstellung.
u_name	name	Name der Bereitstellung.
[Skript]	Frist	Frist für die Bereitstellung.
u_numberinProgress	Count_Progress	Anzahl der Geräte, die für die Bereitstellung ausgeführt werden.
[Skript]	Deployment_time	Startzeit der Bereitstellung.
[Skript]	Integration_instance	Name der Instanz, aus der die Bereitstellung importiert wird.
[Skript]	Source_created	Erstellungszeit der Bereitstellung.
[Skript]	sn_vul_Patch_orch_Update	Referenz des Patches
[Skript]	sn_vul_Patch_orch_Collection	Referenz des erkannten Elements, auf dem der Patch bereitgestellt wird.
u_softwarename	name	Name der Bereitstellung.
u_numberother	Count_other	Andere Anzahl von Geräten für die Bereitstellung.
u_numberunbekannt	Count_unknown	Unbekannte Statusanzahl von Geräten für die Bereitstellung.
u_provimentid	source_id	Eindeutiger Bezeichner der Bereitstellung.
u_numbersuccess	Count_success	Erfolgsanzahl der Geräte für die Bereitstellung.
u_numbererrors	Count_error	Fehleranzahl der Geräte für die Bereitstellung.
u_numberTargeted	Count_total	Gesamtanzahl der Geräte für die Bereitstellung.

SCCM-Bereitstellungsimport – Transformationsskript-Timing

Skript	Beschreibung
OnStart (wenn ein Importsatz eine Transformation erstellt hat).	Skript, das zum Initialisieren der Werte in der Bereichsvariablen [sn_vul_sccm] für den Integrationsprozess verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Das Skript, das zum Aktualisieren der Werte in der Bereichsvariablen [sn_vul_sccm] verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SCCM-Bereitstellungsimport – Transformationsskript-Timing (Fortsetzung)

Skript	Beschreibung
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Skript, das zum Festlegen der Anzahl der erstellten, aktualisierten und ignorierten Elemente verwendet wird. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Beispiel-Workflow für Vulnerability Response Orchestration-Integration mit patchen Microsoft SCCM

Ein Beispiel für die Funktionsweise der Patch-Orchestration Microsoft SCCM.

Vorbereitungen

Angenommen, Ihre gesamte Umgebung wird einmal alle drei Wochen gepatcht. Das letzte Patch-Fenster wurde vor einer Woche abgeschlossen, Sie möchten jedoch einen Patch anwenden, um eine kritische Schwachstelle zu beheben, die kürzlich bekannt wurde. Aufgrund der kritischen Natur dieser Schwachstelle können Sie nicht mehr zwei Wochen auf den nächsten geplanten Patch warten.

Erforderliche Rollen:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für den Vulnerability Manager-Arbeitsbereich.
- sn_vul.Remediation_owner zum Anzeigen des Arbeitsbereichs „IT-Korrekturbesitzer“.
- Rolle „sn_vul_Patch_orch.configure_Patch“ zum Konfigurieren und Planen von Patches.
- sn_vul_Patch_orch.read_Patch zum Anzeigen (schreibgeschützten) Patch-Informationen in Datensätzen. Diese Rolle wird mit den Rollen „sn_vul.Remediation_owner“ und „sn_vuln.Vulnerability_Analyst“ geerbt, die für die Arbeitsbereiche „IT-Korrektur“ und „Schwachstellenmanager“ erforderlich sind.

Warum und wann dieser Vorgang ausgeführt wird

Als Schwachstellenmanager oder Analyst, der im Vulnerability Manager-Arbeitsbereich arbeitet, können Sie Überwachungsthemen erstellen oder vorhandene Überwachungsthemen bearbeiten, um importierte VIS mit kritischen Schwachstellen zu erfassen. Mit der Patch-Orchestration-Integration können Sie auch die Patches anzeigen, die Sie zum Beheben und Nachverfolgen dieser Schwachstellen verwenden möchten. Die folgende Tabelle enthält einige Beispiele mit den Bedingungen, die Sie für Überwachungsthemen für die Patch-Orchestration festlegen können. Verwenden Sie diese Beispiele, um Einstellungen zu bestimmen, die für Ihre Umgebung am besten geeignet sind. Siehe Erstellen Sie ein Überwachungsthema in Arbeitsbereich des Schwachstellenmanagers Weitere Informationen zum Einrichten des Überwachungsthemas.

Beispielbeobachtungsthemen für Patch-Orchestration im Vulnerability Manager-Arbeitsbereich

Name des Überwachungsthemas	Beschreibung
Kritische Schwachstellen mit Patch-Lecks	Risikobewertung ist 1 – Kritisch UND Grund ist „Patch nicht geplant“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielbeobachtungsthemen für Patch-Orchestration im Vulnerability Manager-Arbeitsbereich (Fortsetzung)

Name des Überwachungsthemas	Beschreibung
Kritische Schwachstellen mit geplanten Patches (fehlende SLA)	Grund ist „Patch geplant“ (Zieldatum fehlt)
Kritische Schwachstellen mit geplanten Patches	Risikobewertung ist 1 – Kritisch UND Geplantes Patch-Datum ist nicht leer UND Grund ist „Patch geplant“

- Nachdem Sie als Schwachstellenmanager oder -Analyst die Überwachungsthemen und Korrekturmaßnahmen erstellt haben, generieren Sie Korrekturaufgaben. In VI-Datensätzen und Korrekturaufgaben können Sie Detailinformationen zur Registerkarte Erkennungen anzeigen und erkannte Elementdatensätze mit der Schwachstelle finden, die Sie nachverfolgen, zusammen mit den vom SCCM-Produkt importierten Assets.
- Als Schwachstellenanalyst oder -Administrator können Sie die Patch-Daten überwachen, die der Schwachstelle zugeordnet sind. Sie können auch einen Patch oder mehrere Patches für ein bestimmtes Asset (Konfigurationselement) aus einem erkannten Elementdatensatz bereitstellen.

Als IT-Korrekturspezialist haben Sie Optionen, wie Sie die Schwachstelle mit einer Patch-Bereitstellung beheben.

- Sie können den Patch aus einem Patch-Update-Datensatz (VPU#) planen.
- Wenn angreifbaren Elementen (VI) bevorzugte Lösungen zugeordnet sind und sie Ihnen oder Ihren Gruppen zugewiesen sind, können Sie die Patches aus einer Korrekturaufgabe planen, die diese angreifbaren Elemente enthält.

Prozedur

1. Klicken Sie als IT-Korrekturspezialist im IT-Korrekturarbeitsbereich auf die Startansicht.
2. Klicken Sie in der Startansicht auf **Zugewiesene Korrekturaufgaben** Bewertungsliste zum Anzeigen der Datensätze.

   Für dieses Beispiel können Sie das Feld Kurzbeschreibung in der Korrekturaufgabe (VUL#) auf Text überprüfen, der sich auf Ihre kritische Schwachstelle bezieht. Angenommen, Sie wissen möglicherweise, dass Ihr Schwachstellenmanager ein Überwachungsthema namens kritische Schwachstellen mit Patch-Lecks erstellt hat, um VIS (VIT#) mit dieser kritischen Schwachstelle zu erfassen.

   Wenn der Datensatz geöffnet ist, können Sie auch die VIS und die bevorzugten Patches überprüfen und sehen, ob Sie oder eine Ihrer Gruppen bereits Patch-Anforderungen zur Genehmigung eingereicht hat.

3. Wenn Sie genügend Informationen haben, sollten Sie jetzt eine Anforderung für einen Patch aus dieser Korrekturaufgabe senden.

Hinweis:
Wenn die dem Datensatz zugeordneten VIS keine Patches aufweisen, die ihnen zugeordnet sind, wird die angezeigt **Patch Planen** Schaltfläche ist im Datensatz nicht verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie Auf **Patch Planen** Und füllen Sie die Felder im Dialogfeld aus.
   Weitere Informationen zum Planen eines Patches finden Sie unter Planen Sie Patches mit Microsoft SCCM-Integration mit Vulnerability Response.
5. Alternativ können Sie in der Listenansicht im IT-Korrekturarbeitsbereich auf die Links Korrekturaufgaben, angreifbare Elemente, Lösungen und Patches klicken, um diese Datensätze anzuzeigen.
   In diesem Beispiel kennen Sie anstelle des Namens eines Überwachungsthemas möglicherweise die Artikel-ID oder die Bulletin-ID und den Titel des Patches. Wenn ja, sollten Sie überprüfen, ob Ihnen oder Ihren Gruppen eines der VIS mit dieser Schwachstelle zugewiesen ist. Über Patch-Update-Datensätze können Sie Patch-Anforderungen übermitteln. In VI-Datensätzen können Sie nach potenziellen Patches suchen und die zugehörige Korrekturaufgabe öffnen, wenn Sie eine Patch-Anforderung übermitteln möchten.
6. Wenn Sie keinen Zugriff auf die Arbeitsbereiche haben oder Daten anzeigen und Patches aus der klassischen Umgebung planen möchten, gehen Sie wie folgt vor.

   a. Navigieren zu **Vulnerability Response** > **Patches** > **Alle**an.

   b. Suchen Sie den gewünschten Patch-Update-Datensatz.
      Sie sollten die Datensätze möglicherweise mit filtern Kritisch Risikopunktzahlen.

   c. Überprüfen Sie die Felder zugeordnete VIS und % korrigierte VIS auf der Registerkarte Korrekturstatus. Wenn für die VIS Patches verfügbar sind, wird **Patch Planen** Die Schaltfläche wird oben rechts im Datensatz angezeigt.

   d. Wenn Sie eine Anforderung übermitteln möchten, klicken Sie auf **Patch Planen** .
      Weitere Informationen zum Planen eines Patches finden Sie unter Planen Sie Patches mit Microsoft SCCM-Integration mit Vulnerability Response.

   e. Alternativ können Sie annehmen, dass Sie nicht über die Patch-ID-Informationen verfügen, aber Sie können das Feld Kurzbeschreibung für die Korrekturaufgaben überprüfen, die Ihrer Gruppe zugewiesen sind, auf Text, der sich auf Ihre kritische Schwachstelle bezieht.

   f. Navigieren zu **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**an.

   g. Suchen Sie den gewünschten Datensatz, und klicken Sie darauf, um ihn zu öffnen.
      Überprüfen Sie im offenen Datensatz die Registerkarte Korrekturstatus auf VIS und % der korrigierten VIS. Klicken Sie auf die zugehörigen Links für VI-Datensätze, bevorzugte Lösungen, bevorzugte Patches und Patch-Anforderungen.

      Hinweis:
      Wenn die dem Datensatz zugeordneten VIS keine Patches aufweisen, die ihnen zugeordnet sind, wird die angezeigt **Patch Planen** Schaltfläche ist im Datensatz nicht verfügbar.

   h. Klicken Sie Auf **Patch Planen** Aus dem Datensatz, wenn Sie eine Patch-Anforderung übermitteln möchten.

Qualys Vulnerability Integration verstehen

Die Qualys Produktsensoren erfassen die Daten und senden sie automatisch an die Qualys Anwendung, die die Informationen kontinuierlich analysiert und korreliert. Es lässt sich problemlos in integrieren Vulnerability Response Als Qualys Vulnerability Integration Dient zum Zuordnen von Schwachstellen zu CIs und Business-Services, um die Auswirkungen und Priorität potenziell böswilliger Bedrohungen zu bestimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Ihren Qualys Vulnerability Integration Verwenden **Schwachstelle** > **Administration** > **Setup-Assistent** Um den Datenabruf flexibler und skalierbarer zu machen.

Wenn Sie mehrere Bereitstellungen von haben Qualys Cloud Platform Anwendung können Sie für jede Bereitstellung eine Integration hinzufügen. Assets, die durch mehrere Drittanbieterbereitstellungen identifiziert werden, und ihre Schwachstellen werden konsolidiert und mit Ihrer CMDB abgeglichen. Diese Konsolidierung erfolgt auch dann, wenn sich Scanprozesse zwischen mehreren Bereitstellungen überschneiden. Daten, die aus jeder Bereitstellung stammen, werden identifiziert und in einer einzigen Instanz von verfügbar gemacht Vulnerability Response. Qualys Vulnerability Integration Knowledge Base-Datensätze werden über Bereitstellungen hinweg normalisiert, wodurch sichergestellt wird, dass Instanzen derselben Schwachstelle über alle Bereitstellungen hinweg als dieselbe Schwachstelle behandelt werden.

Hinweis:
Sie können die ursprüngliche Schwachstellenintegration nicht löschen, sie jedoch deaktivieren. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Hinweis:
Während Qualys Vulnerability Integration Erstellt Integrationen für Geräteliste, Asset-Gruppe, dynamische Suchliste und statische Suchliste. Sie sind für den normalen Betrieb nicht erforderlich.

Verfügbare Versionen

Release-Version für Yokohama	Release-Hinweise
Qualys Vulnerability Integration V12.7, v12.8	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Installierte Komponenten

Eine aktuelle Liste der Rollen, Integrationsaufträge und Tabellen, die mit der Integration installiert werden, sowie ein Link zu Anweisungen zum Anzeigen der derzeit in Ihrer Instanz installierten Elemente finden Sie unter Mit installierte Komponenten Qualys Vulnerability Integration.

Primäre und unterstützende Integrationen

Qualys Primäre und unterstützende Integrationen reichern die Schwachstellendaten in Ihrer Instanz an, indem Daten aus der Qualys Vulnerability Integration abgerufen werden. Eine Reihe geplanter Aufgaben ruft die Integrationen automatisch auf. Sie können sie auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird. Primäre und unterstützende Integrationen können geändert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Qualys Integrationen werden als geplante Aufgaben ausgeführt. Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Dieser Wert darf nicht geändert werden.

Hinweis:
Wenn Sie keinen gültigen Ausführungsanwender festlegen, werden bei jeder Ausführung der Integration mehrere, häufig doppelte Datenabrufanhänge in den Datenquellendatensätzen angezeigt. Mehrere Anhänge in der Datenquelle erhöhen die Verarbeitungszeit, was zu inkonsistenten Transformationsergebnissen führt.

Während des Imports werden CVE-Datensätze, die noch nicht vorhanden sind, als NVD-Datensätze erstellt und in Drittparteieinträgen für referenziert Qualys Standardmäßig.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Primäre Integrationen

Eine primäre Integration ist ein Einstiegspunkt zu Qualys Cloud Platform Interaktion mit Qualys API wird in einem Zeitplan aufgerufen.

Zeigen Sie die primären Integrationen an, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**an.

Unterstützende Integrationen

Eine unterstützende Integration ist ein Prozess, der weder nach einem Zeitplan noch ohne Aufruf durch eine primäre Integration ausgeführt werden soll.

Zeigen Sie die unterstützenden Integrationen an, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Administration** > **Unterstützende Integrationen**an.

Service Graph Connector für Qualys

Ab Version 2,2 ist Service Graph Connector für Qualys Ist über verfügbar ServiceNow® Store. Weitere Informationen finden Sie unter Service Graph Connector for Qualys .

Daten aus dem Qualys Datenquellenfelder werden mit der API „Global Asset“ und der API „Asset Management and Tagging“ importiert.

Globale Asset-API:

- Eine CSAM-Lizenz ist erforderlich.
- Asset-Informationen enthalten Details wie Hardwarekategorie und Betriebssystemkategorie.

API für Asset-Management und -Tagging:

- Eine CSAM-Lizenz ist nicht erforderlich
- Asset-Informationen enthalten keine Details zu Hardwarekategorie und BS-Kategorie.

Weitere Informationen finden Sie unter Service Graph Connector for Qualys APIs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

an.

CIs mit Identification and Reconciliation Engine (IRE) erstellen

Sie können die Identifizierungs- und Abgleichsmodul verwenden, um neue CIs zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann, der von einem Scanner einer Drittpartei importiert wurde. Aktivieren Sie das Plugin „CMDB-CI-Klassenmodelle“, um CIs mit den neuen Klassen zu erstellen. Andernfalls werden nicht übereinstimmende CIs in den nicht übereinstimmenden CI-Klassen erstellt. Weitere Informationen finden Sie unter CIs für werden erstellt Vulnerability Response Verwenden der Identifizierungs- und Abgleichsmodul. Weitere Informationen zum Konfigurieren der Kategorisierung nicht übereinstimmender Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert.

Suchlisten

Suchlisten werden in verwendet Qualys Zum Erstellen anwenderdefinierter Gruppen von Schwachstellen. Sie können sie speichern und für die Ticketerstellung und zum Anpassen von Schwachstellen-Scans und Berichten verwenden. Mit dem Modul „Suchlisten“ können Sie Suchlistendaten von Qualys in Ihre Instanz nach einem Zeitplan herunterladen.

Suchlisten werden aus abgerufen Qualys Mit Import Der Dynamischen Suchliste Und/oder Import Statischer Suchliste Datentransformationszuordnungen. In jeder dieser Transformationen können Sie Zeitpläne für die Durchführung des Imports definieren.

Optionsprofile

Optionsprofile sind mit verfügbar Qualys Scaneinstellungen. Ein Optionsprofil ist erforderlich, wenn Sie einen Scan von Ihrem aus initiieren ServiceNow AI Platform.

Optionsprofile werden aus importiert Qualys Produkt nach Option Profillistenintegration. Möglicherweise ziehen Sie es vor, die Option Profillistenintegration nach einem Import aus den Suchlisten-Integrationen auszuführen Qualys Dynamische Suchliste und Qualys Integrationen der statischen Suchliste, damit Sie sehen können, welche Suchlisten Optionsprofilen zugeordnet sind.

Asset-Gruppen

Asset-Gruppen werden in eingerichtet Qualys Plattform. Asset-Gruppen identifizieren, welche Scanner-Geräte zum Scannen übereinstimmender IP-Adressen verwendet werden, wenn ein Scan von initiiert wird ServiceNow AI Platform.

Asset-Gruppen, denen Geräte zugeordnet sind, werden aus abgerufen Qualys Durch die Integration der Asset-Gruppenliste.

Initiieren Sie die Integration der Geräteliste, nachdem Sie Asset-Gruppen importiert haben, um die Felder „Gerätename“ und „Gerätestatus“ in auszufüllen Qualys Standardanwendungsdatensätze in Ihrem ServiceNow AI Platform.

Host-Tags

Alle Host-Tags werden als Teil von importiert Qualys Integration der Hostliste. Host-Tags werden hauptsächlich zum Filtern verwendet Vulnerability Response Regeln für Zuweisungs- und Korrekturaufgaben. Sie werden im Formular „erkanntes Element“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Qualys Die Integration der Host-Liste muss ausgeführt werden, bevor Zuweisungs- oder Korrekturaufgabenregeln in erstellt werden Vulnerability Response Damit alle Tags in den Regeln vorhanden sein können und bevor angreifbare Elemente importiert und gruppiert werden.

- Beim Tag-Speicher wird die Groß-/Kleinschreibung nicht beachtet. Wenn ein **San Diego** Tag wird erstellt, dann ein **SAN DIEGO** Tag kann nicht in der Host-Tag-Tabelle gespeichert werden. „San Diego“ und „SAN DIEGO“ werden als dasselbe Host-Tag betrachtet. Das Tag, das importiert wurde, gewinnt zuerst.
- Die Verwendung von Host-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Host-Tags werden von der globalen Systemeigenschaft gesteuert **sn_vul.Import_Host_Tags** . Diese Eigenschaft ist standardmäßig auf „wahr“ festgelegt. Wenn Sie Tags deaktivieren, werden sie für alle Instanzen deaktiviert.

Host-Tags (auch als Asset-Tags bezeichnet) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Host-Assets Tags zuweisen. Beim Starten von Scans können Sie dann Tags auswählen, die den Hosts zugeordnet sind, die Sie scannen möchten. Mit dem Modul Host-Tags können Sie Host-Tag-Daten aus herunterladen Qualys Zu Ihrer Instanz auf einer geplanten Basis.

Öffnen Sie gelöste angreifbare Elemente erneut, die nicht von Scans geschlossen wurden

Angreifbare Elemente in auf „gelöst“ festgelegt ServiceNow AI Platform Instanz, die jedoch nicht von den Integrationsausführungen von Drittparteien in den Status „Geschlossen/behoben“ versetzt wurde, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Für Qualys Erkennungen: Wenn der Scanner weiterhin VIS findet, die auf „gelöst“ festgelegt wurden, aber dann nicht durch nachfolgende Scans in „Geschlossen/behoben“ versetzt wurden, werden diese VIS wieder in „Offen“ verschoben, wenn das Datum der letzten Suche nach dem Datum der Lösung liegt.

Einschränkungen des Datenabrufs

Standardmäßig gibt es keine Einschränkungen dafür, wie Daten abgerufen werden Qualys. Viele Datensätze können auf Schwachstellen mit niedrigem Schweregrad zurückzuführen sein, die ein Kunde nicht mit seinem Vulnerability Response-Prozess beheben möchte. Durch das Aktualisieren der entsprechenden REST-Nachrichten-/Methodenparameter kann dieses Verhalten geändert werden.

Die für dieses Update verantwortliche REST-Nachricht/Methode ist **Qualys-Host-Erkennung: Standard/Post** . Um die Werte zu aktualisieren, fügen Sie der Post-Methode einen neuen HTTP-Abfrageparameter mit den folgenden Werten hinzu:

- Name: Schweregrade
- Wert: 3-5 (oder ein beliebiger geeigneter Schweregrad)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Zugehörige Informationen

Qualys REST-Nachrichten

Vorbereitung für Qualys Vulnerability Integration

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Es ist wichtig, dass Sie sich auf die Integration vorbereiten, indem Sie diese Verfahren ausführen. Die Qualys Vulnerability Integration Es wird davon ausgegangen, dass Sie Qualys Cloud Platform-Scans in Ihrer Umgebung kennen und ausführen.

Hinweis:
Nehmen Sie alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor, bevor Sie die Integrationen ausführen.

Wichtige Voraussetzungen

Validieren Sie die Größenanpassung Ihrer Instanz basierend auf der Anzahl der angreifbaren Elemente, die Sie importieren möchten. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.

Verwenden Sie Filterung, um die Anzahl der Elemente für den ersten Import zu begrenzen und Ihre Bereitstellung zu phasen, indem Sie Filter in nachfolgenden Importen anpassen.

Die Qualys Scanner sind standardmäßig in deaktiviert Vulnerability Response Anwendung. Wenn Sie versuchen, einen erneuten Scan von den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, wird der **Erneut Scannen** Schaltfläche ist nicht verfügbar.

Auszuführende Aktionen

- Bestimmen Sie ein anfängliches Startdatum Für **Import Der Host-Erkennungsliste** Integrationen.

  Erwägen Sie die Einstellung von **Startzeit** Feld auf einige Stunden oder Tage in der Vergangenheit. Wählen Sie idealerweise das Datum des letzten Qualys-Scans aus. Das Startdatum kann Schwachstellen enthalten, die vor der Verwendung der Schwachstellenverwaltungslösung erkannt wurden. Legen Sie die früheste Startzeit für den Beginn Ihres Scanzyklus fest. Wenn es also eine Woche dauert, bevor alle Hosts gescannt werden, legen Sie diesen Wert auf eine Woche vor dieser Zeit fest.

- Fügen Sie den Rollen für admin, sn_vuln.admin und sn_vul_qualys.admin Anwender hinzu. Weitere Informationen finden Sie unter . Weisen Sie einem Anwender eine Rolle zu .

- Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

- Wenn Sie keine Schwachstellenrechner verwenden, Deaktivieren Sie den standardmäßigen Schwachstellenrechner, wenn er nicht verwendet wird, Zusätzlich zu allen anderen, die Sie definiert haben. Schwachstellenrechner werden jedes Mal ausgeführt, wenn ein Datensatz für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angreifbare Elemente erstellt oder aktualisiert wird, und können sich auf die Leistung des ersten Imports auswirken.

- Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung auswirkt. Vor dem ersten Import Deaktivieren Sie die Business-Regeln .
- Wenn Sie einen anderen Scanner als den Qualys-Standard verwenden möchten, finden Sie unter Richten Sie Scannergeräte ein .
- Halten Sie Ihre Qualys-Server-URL und Authentifizierungsanmeldeinformationen bereit. Die Anmeldeinformationen müssen ausreichende Berechtigungen zum Abrufen von Wissen-, Scan- und Erkennungsinformationen für ein Qualys-Abonnement bieten.
- Wenn Sie Host-Tags in verwenden möchten Vulnerability Response Regeln für Zuweisungs- oder Korrekturaufgaben, stellen Sie sicher, dass Qualys Die Integration der Hostliste wurde vor dem Erstellen von Regeln ausgeführt.

Qualys Vulnerability Integration installieren

Bevor Sie ausführen Qualys Vulnerability Integration In Ihrer Instanz müssen Sie installieren und konfigurieren Qualys Vulnerability Integration Anwendung. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Erforderliche Rolle: administrator zum Herunterladen und Installieren der Anwendung

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Navigieren Sie zu , um zu überprüfen, ob sie aktiviert ist **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.
Ruft Berechtigungen für ab Qualys Vulnerability Integration Anwendung und laden Sie sie auf Ihren herunter ServiceNow AI Platform® Instanz.	Wenn die Anwendung noch nicht auf Ihre Instanz heruntergeladen wurde, finden Sie weitere Informationen unter .
Bereiten Sie sich auf die Integration vor.	Weitere Informationen finden Sie unter Vorbereitung für Qualys Vulnerability Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**an.

   Nach einigen Minuten werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz verfügbar sind.

2. Suchen Sie nach Qualys Vulnerability Integration Kachel und klicken Sie auf **Installieren** .

3. Befolgen Sie die Anweisungen im Setup-Assistenten.
   Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.

4. Navigieren Sie zu **Integrationskonfiguration>Scannerintegrationen** In Setup-Assistent, um mit der Konfiguration fortzufahren.
   Weitere Informationen zum Ergänzen der im Setup-Assistenten bereitgestellten Hinweismeldungen finden Sie unter Konfigurieren Sie Qualys Vulnerability Integration Mit dem Setup-Assistenten.

Nächste Maßnahme

Aktivieren Sie die Scanner, da die Scanner in standardmäßig inaktiv sind Vulnerability Response Anwendung. Weitere Informationen zum Aktivieren von Qualys Scanner, siehe Aktivieren Sie Qualys Scanner.

Aktivieren Sie Qualys Scanner

Sie müssen die Scanner nach der Installation von aktivieren Qualys Vulnerability Integration Da die Scanner in standardmäßig deaktiviert sind Vulnerability Response Anwendung.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie versuchen, einen erneuten Scan von den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, wird der **Erneut Scannen** Schaltfläche ist nicht verfügbar.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**an.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und wählen Sie den Datensatz aus, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox **Aktiv**.
4. Wählen Sie **Aktualisieren**.
5. Das von Ihnen aktivierte Produkt wird in angezeigt **Quelle** Feld in einem angreifbaren Element und in Korrekturaufgaben-Datensätzen nach dem nächsten Import, und **Erneut Scannen** Ist als UI-Aktion verfügbar.

Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartition-Bezeichner für Qualys Vulnerability Integration

Erstellen Sie eindeutige Konfigurationselemente (Configuration Items, CIs) für Assets in Ihrer Umgebung, die IP-Adressen teilen. Identifizieren Sie die eindeutigen Assets in Ihrer Umgebung, und aktualisieren Sie die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen automatisch, um Ihnen weitere Details zu Ihren Schwachstellen zu geben.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig in Vulnerability Response Anwendung. Eine Möglichkeit, Ihre Assets zu identifizieren, ist die IP-Adresse. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, werden jedoch als ein CI in Ihrer CMDB gespeichert.

Wie in den folgenden Tabellen dargestellt, können mehrere Assets (CI) in Ihrer Umgebung IP-Adressen teilen, haben jedoch eindeutige Netzwerk- und Repository-IDs. Standardmäßig werden diese Assets jedoch als einzelnes CI identifiziert und gespeichert (CI 1) Während der IP-Adresssuche.

Standard-IP-Suche und CI-Erstellung

Quelle	IP-Adresse	NETWORK_ID	Konfigurationselement
Qualys Vulnerability Integration: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Quelle	IP-Adresse	REPOSITORY_ID	Konfigurationselement
Qualys Vulnerability Integration: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Sie können einzelne CIs für Assets mit derselben IP-Adresse erstellen, um sie als eindeutige Assets zu identifizieren. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartition-Bezeichners [Network_Partition_Identifier], indem Sie die geplante Aufgabe ausführen. *`Update existing discovered items with network partition identifier`*.

Diese geplante Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Integrationen von Assets und behobenen und offenen Schwachstellen für Qualys Vulnerability Integration Im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.

Wenn diese geplante Aufgabe aktiviert ist, wird der Netzwerkpartition-Bezeichner [Network_Partition_Identifier] zu vorhandenen CI-Datensätzen aus importierten Daten hinzugefügt. Vorhandene CIs, die von der IRE erstellt wurden, werden ebenfalls aktualisiert. Die geplante Aufgabe erstellt auch CIs, die ab dem nächsten Import den Netzwerkpartition-Bezeichner enthalten. Alternativ können Sie den Auftrag bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

Ab v14.0 von Vulnerability Response Und v12.1 des Qualys Vulnerability Integration Schwachstellenintegration, die CMDB-CI-Klassenmodelle (1,0.21.) Wird unterstützt. Die Klassenmodelle haben den Netzwerkpartition-Bezeichner [Network_Partition_Identifier] in den Identifizierungsregeln für Identification and Reconciliation (IRE).

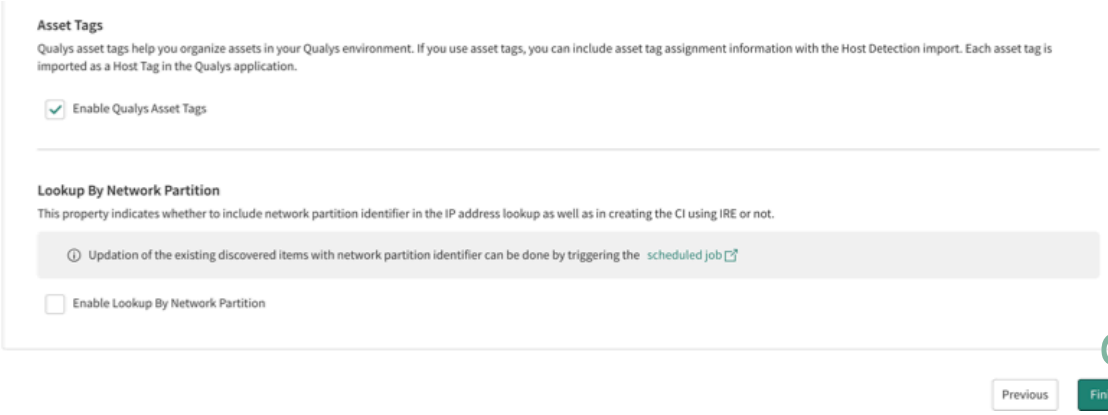
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Führen Sie die geplanten Aufgaben bei Bedarf aus.	Aktualisieren Sie Ihre vorhandenen erkannten Elemente. CIs für Ihre vorhandenen Qualys Vulnerability Integration Daten werden erstellt oder aktualisiert, um die Granularität des Netzwerkpartition-Bezeichners einzubeziehen. Erkannte Elemente, angreifbare Elemente und Erkennungsdatensätze werden alle mit den neuen CIs aktualisiert.
Warten Sie auf Importe neuer Daten aus den Integrationen mit den nächsten geplanten Aufgaben.	Erstellen Sie CIs für jedes neue Asset mithilfe des Netzwerkpartition-Bezeichners, beginnend mit der nächsten geplanten Aufgabe. CI-, angreifbare Element- und Erkennungsdatensätze werden alle aktualisiert, um die neue Granularität einzubeziehen. Neue CIs werden erstellt, wenn keine genaue Übereinstimmung gefunden wird.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**an.
2. Wählen Sie Aus Qualys Vulnerability Integration.
3. **Bearbeiten** Die erforderliche Integration.
4. Wählen **Hosterkennungskonfiguration**an.
5. Wählen **Suche nach Netzwerkpartition aktivieren** Kontrollkästchen in **Suche nach Netzwerkpartition**



Abschnitt.

6. Klicken Sie auf **Fertigstellen**.

Netzwerkpartition-Bezeichner „NETWORK_ID“ und „REPOSITORY_ID“, die in der IP-Suche und CI-Erstellung enthalten sind

Quelle	IP-Adresse	NETWORK_ID	CI für Assets ohne Netzwerkpartition-Bezeichner	CIs-Assets mit Netzwerkpartition-Bezeichner
Qualys Vulnerability Integration: Assets und Integrationen	123.12.12.141	03712	CI 1	CI 1

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quelle	IP-Adresse	NETWORK_ID	CI für Assets ohne Netzwerkpartition-Bezeichner	CIs-Assets mit Netzwerkpartition-Bezeichner
behobener und offener Schwachstellen				
	123.12.12.141	03713	CI 1	CI 2

Quelle	IP-Adresse	REPOSITORY_ID	CI für Assets ohne Netzwerkpartition-Bezeichner	CIs-Assets mit Netzwerkpartition-Bezeichner
Qualys: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Die Suchregeln für die IP-Adresse und die CI-Identifizierung der unvollständigen IP-Adresse enthalten automatisch das Attribut des Netzwerkpartition-Bezeichners für einen Datenimport aus den Integrationen „Assets“ und „Feste und offene Schwachstellen“ für Qualys Vulnerability Integration.

Nachdem Sie die geplante Aufgabe aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartition-Bezeichner enthalten, indem Sie geplante Aufgaben bei Bedarf starten. Die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen werden automatisch aktualisiert.

Optionale Qualys-Änderungen

Konfigurieren Sie optionale Änderungen, und optimieren Sie einige der Daten speziell für die Qualys-Integration.

Sie können dieses Startdatum im Setup-Assistenten oder über die primäre Integration zurücksetzen oder Business-Regeln ändern, um sie während eines ersten Imports zu deaktivieren.

Deaktivieren Sie benachrichtigungsbezogene Geschäftsregeln vor dem ersten Datensatzimport

Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln viele Benachrichtigungen generieren, die sich auf die Leistung auswirken. Diese Business-Regeln sollten geändert werden, um sie während des Imports zu deaktivieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu**Alle** > **Systemdefinition** > **Business-Regeln**an.
2. Suchen Sie nach **Betroffene ci-Benachrichtigungen** .
3. Öffnen Sie die Business-Regel, und fügen Sie diese Bedingung ein: `Current.sys_class_Name != „sn_vul_vulnerable_item“` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Aktualisieren**.
5. Wiederholen Sie diesen Vorgang für die folgenden Business-Regeln:
   - Benachrichtigungen über betroffene Kostenstellen
   - Benachrichtigungen der betroffenen Gruppe
   - Benachrichtigungen zu betroffenen Standorten

Hinweis:
Nach Abschluss des ersten Datensatzimports haben Sie die Möglichkeit, diese Business-Regeln erneut zu aktivieren. Erwägen Sie jedoch, sie deaktiviert zu lassen. Sie können eine große Anzahl von Benachrichtigungen generieren und sich auf die Leistung Ihrer Instanz auswirken.

Aktivieren Sie Qualys Integration der QVS-Punktzahl

Mit Qualys Integration der QVS-Punktzahl Sie können die QVS-Punktzahlen für CVEs automatisch ausfüllen, um das Schwachstellenrisiko in der Tabelle „sn_vul_nvd_entry.LIST“ genauer zu bewerten.

Vorbereitungen
Erforderliche Rolle: sn_vul_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Qualys-Integrationen** > **Integration der Qualys QVS-Punktzahl**an.
2. Wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren der Integration.

Hinweis:
Diese Funktion ist standardmäßig inaktiv.

Ergebnisse
Wenn die Integration ausgeführt wird, wird abgefragt Qualys Für die neuesten QVS-Punktzahlen der CVEs, die in den letzten 15 Tagen aktualisiert wurden, und füllt aus **Qualys-Schwachstellenpunktzahl** Spalte in der Tabelle [sn_vul_nvd_entry.LIST].

Hinweis:
Wenn die QVS-Punktzahl leer ist, wurde das CVE in den letzten 15 Tagen nicht aktualisiert.

Ändern Sie ein anfängliches Startdatum

Während der Installation mit dem Setup-Assistenten legen Sie ein erstes Startdatum für die Qualys-Integrationen fest. Sie können dieses Startdatum im Setup-Assistenten oder über die primäre Integration wie unten gezeigt zurücksetzen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird
Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**an.
2. Klicken Sie Auf **Qualys-Host-Erkennungsintegration** .
3. Klicken Sie Auf **Integrationsdetails** .
4. Legen Sie fest **Startzeit** Feld mit einem Wert in der Vergangenheit, sodass alle seit diesem Zeitpunkt gescannten und erkannten Schwachstellen erkannt werden.

   Wenn Sie konfiguriert haben Qualys Verwenden Sie den Setup-Assistenten, die **Startzeit** Das Feld ist vorab ausgefüllt, zunächst bis drei Monate vor dem heutigen Datum und anschließend bis zum heutigen Datum.

   Hinweis:
   Erwägen Sie, den Wert auf maximal einen Monat in der Vergangenheit festzulegen. Dadurch wird verhindert, dass große Datenmengen die Qualys-API-Quotenbeschränkungen überschreiten und Ausführungszeitüberschreitungen auslösen.

5. Klicken Sie auf **Absenden** oder **Aktualisieren**.
6. **Wahlweise:** Klicken Sie Auf **Jetzt Ausführen** Zur sofortigen Ausführung.

Erweitert Qualys Konfigurationen und Änderungen

Konfigurieren Sie erweiterte optionale Änderungen, und optimieren Sie einige der Daten speziell für Qualys Integration. Die meisten dieser Änderungen erfordern Codierung oder erweiterte Funktionen ServiceNow Oder Qualys Cloud Platform Fachwissen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für weitere Tipps für Qualys Importe, siehe Tipps zur Leistungsoptimierung für Qualys-Importaufträge wissensartikel in der HI Knowledge Base.

Ändern Sie die Zuordnungswerte Qualys in ServiceNow-Priorität und -Status

Ändern Sie Zuordnungswerte für Priorität und Status für Ihre Anforderungen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Dies ist eine erweiterte Anpassungsoption.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**an.
2. Suchen Sie nach **Qualys-Werte Zuordnen** Und öffnen Sie es.
3. Klicken Sie auf **Erweitert** Registerkarte.
4. Ändern Sie entsprechend Ihren Anforderungen.
   Die häufigsten Änderungen umfassen das Hinzufügen neuer Statuswerte oder die Überarbeitung der Relevanz oder Priorität.
5. Klicken Sie auf **Aktualisieren**.

Beschränken Sie die Möglichkeit, basierend auf einer Zuweisungsgruppe in einen Datensatz zu schreiben

Sie können Schreib-/Leserechte für Datensätze basierend auf der Mitgliedschaft für eine zugewiesene Gruppe beschränken. Ändern Sie Bedingungen und Skript basierend auf bestimmten Anforderungen.

Vorbereitungen
Erforderliche Rolle: Security_admin (erhöhte Rolle vom Administrator)

Hinweis:
Diese Aktion wird im Bereich Schwachstellen ausgeführt.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Zugriffssteuerung (ACL)**an.
2. Suchen Sie nach ACLs, die mit beginnen `sn_vul` .
3. Wählen Sie einen Zugriffssteuerungsdatensatz aus, z. B. `sn_vul_vulnerable_item` , **Vorgang Schreiben** .
4. Überprüfen Sie **Erweitert** Feld im Datensatz, falls erforderlich, um anzuzeigen **Rolle** Einträge.
5. Ändern Sie **Rolle** Skript für Ihre Anforderungen.
   Skriptbeispiel zum Ändern des Zugriffs nach Gruppe.

```
answer = (current.assigned_to == gs.getUserID() ||
 isMemberOfForScopedApp(current.assignment_group));
// Note: standard 'isMemberOf' does not work within Scoped App
// gs.getUser().isMemberOf(current.assignment_group);
function isMemberOfForScopedApp(groupID){
var result = false;
if (groupID != ''){
var userID = gs.getUserID();
var now_GR = new GlideRecord("sys_user_grmember");
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
gr.addQuery("group", groupID);
gr.addQuery("user", userID);
gr.query();
if (gr.next()){
result = true;
}
}
return result;
}
```

6. Klicken Sie auf **Aktualisieren**.

Richten Sie Scannergeräte ein

Wenn Sie Scans von initiieren ServiceNow AI Platform® Anstatt direkt von Qualys aus können Sie Scans für IP-Adressbereiche einrichten.

Vorbereitungen

Die Daten stammen aus dem Qualys Integration basiert auf Qualys Asset-Gruppen und ihre zugehörigen Standardgeräte (Scanner).

Wenn für die Zielbereiche der IP-Adressen keine Geräte konfiguriert sind, wird das Gerät, das als Standard für die Integrationsinstanz festgelegt ist, für den Scan verwendet.

Erforderliche Rolle: sn_vul_qualys.admin

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Scannergeräte**an.
2. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Gerätename	Sie werden aufgefordert, dieses Feld auszufüllen, wenn Sie einen Datensatz manuell erstellen. Geben Sie den Namen für ein Qualys Scannergerät, das zum Aufrufen von Scans für übereinstimmende Konfigurationselemente verwendet werden soll. Verwenden Sie `Extern` Wert, wenn der Scan mit einem externen Scanner gestartet werden soll.
Geräte-ID	Geben Sie den Gerätebezeichner für ein Qualys Scannergerät, das zum Aufrufen von Scans für übereinstimmende Konfigurationselemente verwendet werden soll. Sie werden aufgefordert, dieses Feld auszufüllen, wenn Sie einen Datensatz manuell erstellen. Verwenden Sie `0` Wert, wenn der Scan mit einem externen Scanner gestartet werden soll.
Gerätestatus	Zeigt den letzten Status des Scannergeräts für die vom zurückgegebenen Daten an Qualys Integration. Bei manuell erstellten Datensätzen wird der Status nur aktualisiert, wenn ein gültiger ist **Geräte-ID** Ist angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Asset-Gruppen-ID	Zeigt an Qualys Asset-Gruppenbezeichner, der diesen Datensatz erstellt hat. Dieses Feld zeigt nur einen Wert für Datensätze an, die von erstellt wurden Qualys Integration.
Asset-Gruppenname	Zeigt an Qualys Asset-Gruppenname, der diesen Datensatz erstellt hat. Dieses Feld zeigt nur einen Wert für Datensätze an, die von erstellt wurden Qualys Integration.
Reihenfolge	Geben Sie einen Wert ein, der zum Bestimmen der Scanpriorität verwendet werden soll. Für Geräte mit in Konflikt stehenden Kriterien erhält ein Gerät mit einem niedrigeren Reihenfolgewert eine höhere Priorität.
Manuell erstellt	Gibt an, ob dieser Datensatz manuell vom Anwender erstellt wurde.
Filtergruppe verwenden	Aktivieren Sie dieses Kontrollkästchen, um eine Filtergruppe für die Suche nach übereinstimmenden Konfigurationselementen zum Scannen anzugeben.
Filtergruppe	Wählen Sie die Filtergruppe aus, die Sie zum Suchen übereinstimmender Konfigurationselemente zum Scannen verwenden möchten. Dieses Feld wird nur angezeigt, wenn Sie ausgewählt haben **Verwenden Sie die Filtergruppe** .
IPs	Eine kommagetrennte Liste von IP-Adressen oder IP-Adressbereichen, die von dieser Appliance beim Aufrufen von Scans verwendet werden sollen.
Integrationsinstanz	Die Qualys Integrationsinstanz, die dieser Appliance zugeordnet ist.
Optionsprofil	Wählen Sie das Optionsprofil aus, das Sie für Scans für übereinstimmende Konfigurationselemente verwenden möchten.

3. Klicken Sie auf **Aktualisieren**.

Konfigurieren und verwalten Qualys Schwachstellen-Scanner und -Scans

Qualys Schwachstellen-Scans können durchgeführt werden, um Softwareschwachstellen zu finden, die sich auf Ihre CIs auswirken. Sie können Scans aus einem Datensatz für angreifbare Elemente initiieren oder direkt einen Scan-Datensatz für Konfigurationselemente (Configuration Items, CIs) und IP-Adressen erstellen.

Wenn Sie scannen Qualys Angreifbare Elemente direkt über den Bildschirm „angreifbare Elemente“ haben Sie auch die Möglichkeit, mehrere angreifbare Elemente gleichzeitig zu scannen.

Wenn Security Incident Response Ist aktiviert, können Sie auch einen Scan aus dem Security Incident-Katalog, einem Security Incident-Datensatz oder einer Security Scan-Anforderung initiieren.

Scans übermittelt von Qualys Angreifbare Elemente, die Security Incident Catalog, Security Incidents oder Security Scan-Anforderungen werden standardmäßig ausgeführt Qualys Scanner.

Sie können das Optionsprofil auswählen, das Sie für Scans für übereinstimmende Konfigurationselemente verwenden möchten.

- Optionsprofile enthalten Qualys Scaneinstellungen.
- Ein Optionsprofil ist erforderlich, wenn Sie eine initiieren Qualys Scannen Sie von Ihrem aus ServiceNow AI Platform®.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie von ServiceNow initiiert Qualys IP-Scan

Die Qualys Der im Basissystem enthaltene Scanner bietet eine Baseline-Integration zum Initiieren von Scans basierend auf IP-Adressen.

Vorbereitungen

Sie können das Optionsprofil auswählen, das Sie für Scans für übereinstimmende Konfigurationselemente verwenden möchten.

- Optionsprofile enthalten Qualys Scaneinstellungen.
- Ein Optionsprofil ist erforderlich, wenn Sie einen Qualys-Scan von Ihrem initiieren ServiceNow AI Platform®.

Erforderliche Rolle: sn_vul_qualys.admin

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**an.
2. Öffnen Sie den Datensatz Qualys.
3. Wählen Sie aus **Aktiv** Und **Standard** Kontrollkästchen.

   Auswählen **Aktiv** Ist erforderlich, um zu verwenden Qualys Zu scannender Scanner Qualys AES automatisch. Sie müssen auch nicht auswählen **Standard** Damit sie automatisch ausgeführt wird.

   Vor v12.0, **Aktiv** Ist erforderlich, um den Scanner zu verwenden. Wenn **Standard** Ist auch ausgewählt, wird der Scanner automatisch verwendet, ohne dass er während des Scans ausgewählt werden muss.
4. Klicken Sie für das Feld Quellintegration auf das Suchsymbol, und wählen Sie die Option für aus **Qualys** , Beispiel: **Qualys Cloud-Plattform** .
5. Klicken Sie auf **Aktualisieren**.
6. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**an.
7. Öffnen Sie **Integration Der Qualys-Asset-Gruppenliste** .
   a. Aktivieren Sie die Checkbox **Aktiv**.
   b. Klicken Sie auf **Jetzt ausführen**.
8. Führen Sie die folgenden Schritte aus, um Ihre Scanner-Geräte auszufüllen.

Hinweis:
Möglicherweise möchten Sie die Integration der Optionsprofilliste nach einem Import aus den Integrationen der Suchlisten, der dynamischen Qualys-Suchliste und der Integrationen der statischen Qualys-Suchliste ausführen, damit Sie sehen können, welche Suchlisten den Optionsprofilen zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Öffnen Sie **Integration Der Qualys-Optionsprofilliste** .

b. Aktivieren Sie die Checkbox **Aktiv**.

c. Klicken Sie auf **Jetzt ausführen**.

d. Führen Sie die in aufgeführten Schritte aus Richten Sie Scannergeräte ein Zum Konfigurieren Ihrer Scanner-Geräte.
Kehren Sie hierher zurück, nachdem Sie diese Schritte abgeschlossen haben, um mit der Konfiguration fortzufahren.

e. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**an.

f. Öffnen Sie **Integration Der Qualys-Geräteliste** .

g. Aktivieren Sie die Checkbox **Aktiv**.

h. Klicken Sie auf **Jetzt ausführen**.
Ihr Qualys Scannergeräte sind jetzt korrekt ausgefüllt.

Zugehörige Informationen

Qualys Vulnerability Integration verstehen

Scannen Sie mehrere Qualys Schwachstellen oder angreifbare Elemente

Sie können mehrere gleichzeitig scannen Qualys Schwachstellen oder angreifbare Elemente, die mindestens ein betroffenes Konfigurationselement (CI) oder eine im Formular ausgefüllte IP-Adresse enthalten.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_write

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Prozedur

1. Führen Sie einen der folgenden Schritte aus:
   - Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**an.
   - Navigieren zu **Alle** > **Vulnerability Response** > **Alle angreifbaren Elemente**an.
2. Aktivieren Sie die Kontrollkästchen für die Datensätze, die Sie scannen möchten.
3. Klicken Sie auf **Aktionen für ausgewählte Zeilen** Liste und klicken Sie auf **Erneut nach angreifbaren Elementen scannen** .
   Eine Nachricht mit einem Link zum Scan wird angezeigt, und die Arbeitsnotizen werden aktualisiert.
4. Klicken Sie auf den Link, um den Fortschritt oder die Ergebnisse des Scans anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Qualys automatischer Scan nach gelösten Korrekturaufgaben

Sie können den Scan planen, der automatisch ausgeführt wird, um Ihren zu aktualisieren Qualys Angreifbare Elemente.

Vorbereitungen

Nachdem eine Korrekturaufgabe auf übergegangen ist **Gelöst** , Wird automatisch ein Scan initiiert, um den Status der zugehörigen angreifbaren Elemente zu aktualisieren.

- Der Scan ist standardmäßig deaktiviert.
- Aktivieren Sie den Scan mit **Scan_on_Resolved** Integrationsinstanzparameter in **Qualys** Datensatz befindet sich in **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen** > **Qualys-IDs**an. Weitere Informationen finden Sie in den folgenden Schritten.
- Dieser Scan ist instanzspezifisch. Wenn Sie mehrere Instanzen haben und diesen Scan aktivieren oder deaktivieren möchten, müssen Sie deaktivieren **Scan_on_Resolved** Parameter in den Integrationsinstanzparametern in jeder Instanz, die geändert werden soll.
- Wenn der Scan aktiviert ist, können Sie den Scan bei Bedarf initiieren oder planen, dass der Scan nur innerhalb eines bestimmten Zeitfensters ausgeführt wird. Siehe Konfigurieren Qualys Erneute Scans, um nur innerhalb geplanter Intervalle ausgeführt zu werden Zum Festlegen der Start- und Endzeiten für das Zeitfenster.

Erforderliche Rolle: sn_vul_qualys.admin

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Integrationsinstanzen**an.
2. Wählen Sie Aus **Qualys** Zum Öffnen des Datensatzes.
   Die Integrationsinstanzparameter für Qualys Werden auf einer Registerkarte angezeigt.
3. Um den automatischen Scan zu aktivieren, suchen Sie nach `scan_on_resolved`Parameter.
4. Geben Sie in der Spalte Wert für die Eigenschaft ein `Wahr` .
5. Klicken Sie auf **Aktualisieren**.

Konfigurieren Qualys Erneute Scans, um nur innerhalb geplanter Intervalle ausgeführt zu werden

Für Qualys Schwachstellenintegration: Legen Sie die Parameter für Start- und Endzeit des Scans so fest, dass erneutes Scannen nur während der gewünschten Stunden ausgeführt werden oder verfügbar sind.

Vorbereitungen

Diese Konfiguration gilt sowohl für geplante erneute Scans als auch für die erneuten Scans, die Sie manuell in initiieren Qualys Produkt aus Ihrem ServiceNow AI Platform® Instanz.

Durch das Festlegen der Parameter für die Start- und Endzeit des Scans für Integrationsinstanzen können Sie Zeitfenster angeben, wenn ein erneuter Scan in durchgeführt wird Qualys Produkt ist verfügbar. Sie können beispielsweise angeben, dass erneutes Scannen nur außerhalb der Geschäftszeiten verfügbar ist, z. B. Mitternacht bis 10:00 UHR.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Einstellung ist instanzspezifisch. Wenn Sie mehrere Instanzen haben, müssen Sie die Werte „Scan_Start_time“ und „Scan_end_time“ in den Parametern der Integrationsinstanz in jeder Instanz konfigurieren, die Sie ändern möchten.

Erforderliche Rolle: sn_vul_qualys.admin

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen** > **Qualys-IDs**an.
2. Klicken Sie Auf **Qualys** Zum Öffnen des Datensatzes.
   Die Integrationsinstanzparameter für Qualys Werden angezeigt.
3. Geben Sie für den Parameter Scan_Start_time in der Spalte Wert die Zeit in der UTC-Zeitzone im 24-Stunden-Format (00:00 bis 24:00 Uhr) für die Startzeit des Fensters ein, für das erneut scans verfügbar sein sollen.
4. Geben Sie für Scan_end_time in der Spalte Wert Zeiten im gleichen Format (00:00 bis 24:00 Uhr) für die Endzeit des verfügbaren Fensters ein.
   Wenn Sie beispielsweise am selben Morgen eine Startzeit von 00:00 Uhr für den Parameter Scan_Start_time und eine Scan_end_time von 10:00 UHR eingeben, werden Scans, die außerhalb des Zeitfensters von Mitternacht bis 10:00 UHR geplant oder manuell gestartet werden, in die Warteschlange gestellt und zur Startzeit des Zeitfensters des folgenden Tages gestartet, 00:00.

   Im selben Beispiel wird der erneute Scan nicht sofort gestartet, wenn ein Korrekturbesitzer um 11:00 UHR manuell einen erneuten Scan initiiert, da er außerhalb der verfügbaren konfigurierten Scan-Zeiten liegt. Die Scan-Anforderung bleibt bis zum Beginn des Zeitfensters des folgenden Tages in der Warteschlange (in diesem Beispiel 00:00).
5. Klicken Sie Auf **Aktualisieren** Um Ihre Einstellungen zu speichern.

Qualys Grenzwerte für Schwachstellen-Scan-Rate

Sie können die Rate definieren, mit der verschiedene Arten von Scans durchgeführt werden, um die Anzahl der Anforderungen zu begrenzen, die an einen externen Scanner gesendet werden. Nachdem Sie Quotengrenzen definiert haben, können Sie sie auf anwenden Qualys Scanner.

Definieren Qualys Scan-Quotengrenzen

Sie können die Rate definieren, mit der verschiedene Arten von Scans durchgeführt werden, um die Last in Ihrer Scan-Warteschlange auszugleichen. Bedingungen, die im Quotenlimit definiert sind, bestimmen, ob die Quotengrenzen auf Einträge in der Warteschlange angewendet werden.

Vorbereitungen

Erforderliche Rolle: sn_vul.admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Quotengrenzdefinitionen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quotengrenzdefinition

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an, der die Bedingungen identifiziert, die der Warteschlangeneintrag erfüllen muss. Zum Beispiel Scans pro Minute
Bedingungen der Warteschlange	Geben Sie Bedingungen ein, die verwendet werden, um zu bestimmen, ob ein Scan-Eintrag in der Warteschlange dieser Quotengrenze unterliegt. Die Bedingungen dürfen nicht spezifisch für einen bestimmten Scanner sein.
Auswertungsskript	Schreiben Sie ein Skript mit der Logik, um den Eintrag in der Warteschlange auszuwerten. Es ist wichtig, dass das Skript „wahr“/„falsch“ zurückgibt, um zu definieren, ob der Eintrag verarbeitet wird. Erstellen Sie außerdem das Auswertungsskript auf dem ausgewerteten Eintrag in der Warteschlange.

4. Klicken Sie auf **Absenden**.

Wenden Sie Scan-Quotengrenzen auf an Qualys Scanner

Nachdem Sie mit Scan-Quotengrenzen definiert haben **Quotengrenzdefinitionen** , Sie können Quotenlimits auf bestimmte anwenden Qualys Scanner.

Vorbereitungen

Erforderliche Rolle: sn.vul_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scannerquotengrenzen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Scannerratenlimit

Feld	Beschreibung
Scanner	Wählen Sie den Scanner aus, auf den Sie ein Quotenlimit anwenden möchten.
Quotengrenze	Wählen Sie die Quotengrenze aus, die Sie auf diesen Scanner anwenden möchten.
Schwellenwert	Geben Sie den Schwellenwert ein, dem der ausgewählte Scanner für das ausgewählte Quotenlimit unterliegen soll. Wenn der Scanner beispielsweise 4 Scans pro Minute zulässt und das Quotenlimit als Anforderungen pro Minute definiert ist, würde der Schwellenwert 4 betragen.

4. Klicken Sie auf **Absenden**.

Zeigen Sie an Qualys Warteschlange für Schwachstellen-Scan

Anforderungen für Schwachstellen-Scan an übermittelt Qualys Die Integration von Schwachstellen-Scans wird in die Warteschlange gestellt, um Systemressourcen nicht zu überlasten. Sie können den Status von Anforderungen in der Warteschlange nach Bedarf anzeigen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

In der Liste der Scans in der Warteschlange enthält jeder Scan einen automatisch generierten Scan-Namen, der das gescannte CI identifiziert.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scan-Warteschlange**an. Alle Qualys Scan-Anforderungen, die übermittelt wurden, werden in einer Liste angezeigt. Die **Status** Die Spalte zeigt den aktuellen Status jedes Eintrags in der Warteschlange an. Ein Status von **Abgeschlossen** Gibt an, dass der Scan die Warteschlange verlassen hat. Dies bedeutet nicht unbedingt, dass die Verarbeitung des Scans abgeschlossen wurde. Wenn die Scans abgeschlossen wurden oder fehlgeschlagen sind, wird der **Wird Verarbeitet** Die Spalte zeigt den entsprechenden Text der Arbeitsnotizen.

   Hinweis:
   Wenn ein Hash-Wert zum Scannen übermittelt wurde und der Scanner kein Ergebnis findet **Status** Wird angezeigt **Abgeschlossen** Und die Arbeitsnotiz in **Wird Verarbeitet** Spalte gibt an **Unbekannt** .

2. Nachdem die Verarbeitung eines Scans abgeschlossen ist, klicken Sie auf einen Datensatz in der Warteschlange, um Details für die Scan-Anforderung anzuzeigen.

Aktivieren Sie den Basissystemfilter für bestätigte Erkennungsimporte

Aktivieren Sie einen Standardfilter mit Integrationsparametern, um nur bestätigte Erkennungen aus zu importieren Qualys Cloud Platform.

Vorbereitungen

Erforderliche Rolle: sn_vul_qualys.admin, sn_vul.vr_Import_admin

Warum und wann dieser Vorgang ausgeführt wird

Der Instanzparameter „include_only_confirmed“ für die Basissystemintegration ist verfügbar, um eine gefilterte Liste von Erkennungen aus zu importieren Qualys Cloud Platform. Standardmäßig ist dieser Parameter auf festgelegt *FALSCH* , Und alle Erkennungen, ob potenziell, bestätigt oder informativ, werden importiert.

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Integrationsinstanzen**an.
2. Öffnen Sie die Qualys Cloud-Plattformintegration aus der Liste Integrationsinstanzen.
3. Öffnen Sie in der Liste „Parameter der Integrationsinstanz“ die Option „ *include_only_confirmed*Parameter „.
4. Aktualisieren Sie den Standardwert auf *Wahr* .
5. Klicken Sie auf **Aktualisieren**.
   Sie haben den Filter aktiviert, um bestätigte Erkennungen aus zu importieren Qualys Cloud Platform Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Standardmäßig nur bestätigte Erkennungen von Qualys Cloud Platform Integrationen werden importiert, wenn der nächste Qualys-Schwachstellenimport ausgeführt wird. Alle anderen Erkennungen wie informativ und potenziell werden ignoriert und nicht importiert. Weitere Informationen finden Sie unter Zeigen Sie Erkennungsdaten für angreifbare Elemente von Vulnerability Response an .

Initiieren Sie einen erneuten Scan für Qualys Vulnerability Integration

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen den geplanten Scanzyklen behoben wurden, indem Sie erneutes Scannen in initiieren Qualys Produkt aus Ihrem ServiceNow AI Platform Bei Bedarf.

Vorbereitungen
Sie können erneutes Scannen über die Vulnerability Response-Arbeitsbereiche initiieren. Weitere Informationen finden Sie unter Scannen Sie Datensätze und Korrekturaufgaben in erneut Arbeitsbereich des Schwachstellenmanagers und Scannen Sie angreifbare Elemente und Korrekturaufgaben in erneut Arbeitsbereich für IT-Korrekturen.

Informationen zum Initiieren von erneuten Scans in der klassischen Umgebung finden Sie in den folgenden Abschnitten.

Erforderliches Setup für erneute Scans in Qualys Produkt von initiiert ServiceNow AI Platform:

Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für initiieren Qualys Produkt aus Ihrem ServiceNow AI Platform® Instanz.

Um den Overhead und das Volumen für geplante, vollständige Scans, Korrekturbesitzer, IT-Spezialisten, Schwachstellenanalysten zu reduzieren, oder Schwachstellenmanager können bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen in Assets (Konfigurationselementen) in ihren Umgebungen initiieren. Sie können erneutes Scannen in initiieren Qualys Produkt aus angreifbaren Elementen (VI), Korrekturaufgaben (RT), Drittparteieinträgen (TPE) oder erkannten Elementdatensätzen von Ihrem ServiceNow AI Platform Instanz.

Durch erneutes Scannen können Sie verifizieren, ob Ihre Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben haben.

Anwendungsfall:

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen einmal gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, aber Sie haben gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Ihrem aus initiieren ServiceNow AI Platform Für Qualys Angreifbare Elemente.

Sie können erneute Scans für VIS initiieren, die haben Qualys Als Quelle in anderen status als „Geschlossen“. Siehe Scannen Sie Datensätze und Korrekturaufgaben in erneut Arbeitsbereich des Schwachstellenmanagers und Scannen Sie angreifbare Elemente und Korrekturaufgaben in erneut Arbeitsbereich für IT-Korrekturen.

Stellen Sie sicher, dass Sie das folgende Setup abgeschlossen haben, das für erneute Scans erforderlich ist. Sehen Sie sich die Schritte an, die mit Konfigurieren und verwalten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

beginnen Qualys Schwachstellen-Scanner und -Scans, die in den vorherigen Abschnitten aufgeführt sind, um weitere Informationen zu erhalten.

Erforderliche Rolle: sn_vul_manually_initiate_rescan

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**an.
2. Suchen Sie den Datensatz des angreifbaren Elements, aus dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   Hinweis:
   Sie können erneutes Scannen für VIS nur mit initiieren Qualys Als Quelle. Verifizieren Qualys Wird in angezeigt **Quelle** Spalte in den VI-Listenansichten oder in **Quelle** Felder in einzelnen Datensätzen. Sie können den Bedingungsgenerator verwenden, um VIS nach Quelle zu gruppieren. Oder wenn die Spalte Quelle in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf **Liste Personalisieren** Symbol (Zahnradsymbol), und verwenden Sie zum Verschieben den Slushbucket **Quelle** Von **Verfügbar** Bis **Ausgewählt** .

3. Alternativ navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**, **Vulnerability Response** > **Bibliotheken** > **Drittpartei**, Oder bis **Erkannte Elemente** Für die Korrekturaufgabe, den Drittparteieintrag oder die Datensätze erkannter Elemente, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl, die **Erneut Scannen** Die Schaltfläche ist für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss das VI aus dem stammen Qualys Produkt und in einem anderen Status als **Geschlossen** . Für mehrere VI-Datensätze müssen alle VIS haben Qualys Als Quelle und in einem anderen Status als **Geschlossen** .
   - In einem RT-Datensatz kann sich die Korrekturaufgabe in einem anderen Status als befinden **Geschlossen** , Und alle zugehörigen VIS müssen haben Qualys Als Quelle.
   - Bei einem Drittpartei-Eintrag-Datensatz (TPE) muss dem Datensatz mindestens ein zugeordneter VI-Datensatz in einem anderen Status als zugeordnet sein **Geschlossen** Mit Qualys Als Quelle.
   - In einem erkannten Elementdatensatz ist dem Konfigurationselement mindestens ein VI zugeordnet Qualys Als Quelle in einem anderen Status als **Geschlossen** .

4. Klicken Sie oben rechts im ausgewählten Datensatz auf **Erneut Scannen** .
   Wählen Sie im angezeigten Dialogfeld eines aus, um fortzufahren.

Option	Beschreibung
Wählen Sie aus **Geben Sie Optionsprofile an** Kontrollkästchen.	Wählen Sie in der Liste das Optionsprofil für aus Qualys Scanner, den Sie für den erneuten Scan verwenden möchten. Dies sind die Geräte (Scanner), die Sie konfiguriert und unter aufgelistet haben **Qualys Schwachstellenintegration** > **Scannergeräte**an.
Löschen Sie **Geben Sie Optionsprofile an** Kontrollkästchen (nicht ausgewählt).	Die Qualys Optionsprofil für den Scanner, den Sie als Standardscanner in der Liste „Scanner-Geräte“ festgelegt haben, wird für den Scan verwendet. Weitere Informationen zum Festlegen der Standardscanner, die Sie über initiieren ServiceNow AI Platform, Setup-Scanner-Geräte, die im vorherigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Abschnitt aufgeführt sind, um weitere Informationen zu erhalten.

5. Klicken Sie Auf **Scan Anfordern** .

   Eine Nachricht wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird. Der Status für alle erneuten Scans kann jederzeit unter den zugehörigen Scan-Listen in den Datensätzen VI, RT, TPE und erkannte Elemente gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht auf **Zeigen Sie Details an** Zum Anzeigen des Status des erneuten Scans und zum Anzeigen anderer erneutes Scans, die aus einem bestimmten Datensatz gestartet wurden.

   Ihre Instanz verfolgt den Status des erneuten Scans, bis er erfolgreich abgeschlossen ist oder bis der festgelegte Nachverfolgungszeitraum abgelaufen ist, je nachdem, was zuerst geschieht. Durch die Zeitüberschreitung wird der Scan nicht beendet. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, an dem der ServiceNow AI Platform Die Nachverfolgung des Status des erneuten Scans wurde beendet, nicht wenn der tatsächliche erneute Scan beendet wurde.

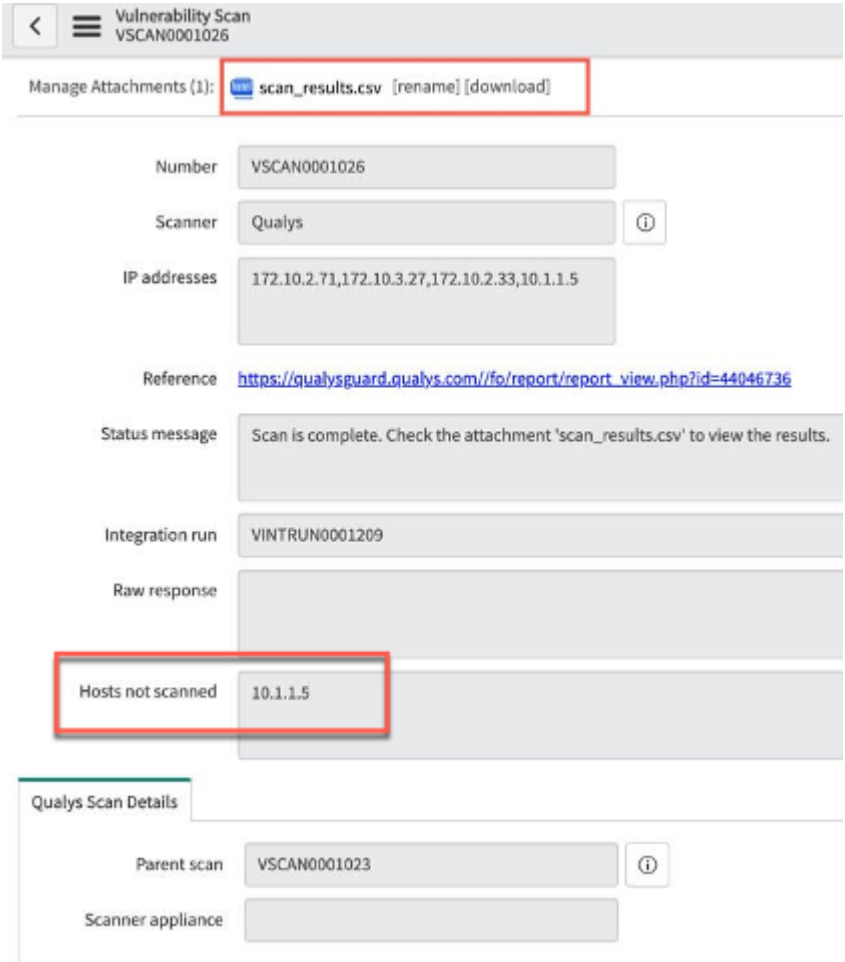
   Nachdem der erneute Scan erfolgreich abgeschlossen wurde, wird die Qualys Die Integration der Host-Erkennung wird automatisch initiiert, um Ihre angreifbaren Elemente zu aktualisieren. Je nachdem, wie viele VIS Sie haben, werden Ihre Erkennungen, VIS und RTS nach Abschluss von aktualisiert Qualys Scan der Host-Erkennungsintegration. Navigieren Sie zu diesen Datensätzen, um die Aktualisierungen anzuzeigen, nachdem die Host-Erkennungsintegration abgeschlossen wurde.

   Dieser Scan ist instanzspezifisch und kann deaktiviert werden. Weitere Informationen zu finden Qualys Integrationen und Informationen zum Anzeigen der Integrationen finden Sie unter Qualys Vulnerability Integration verstehen.

Nächste Maßnahme

Sie können einen CSV-Anhang im Scan-Datensatz anzeigen, um Details zu den erneuten Scans anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wie im vorherigen Bild gezeigt, werden während des erneuten Scans keine mit diesen Assets verknüpften Erkennungen und VIS aktualisiert, wenn Hosts (Konfigurationselemente) in Ihrer Umgebung nicht zugänglich sind. Damit Sie verstehen, warum sie nicht enthalten sind, werden die Asset-IP-Adressen für diese CIs nach Abschluss des erneuten Scans in Schwachstellendatensätzen im Feld Hosts nicht gescannt aufgeführt.

Qualys Metadaten für Schwachstellen

Die Qualys Die Integration der Host-Erkennung wurde erweitert, um weitere Felder aus einzubeziehen Qualys. Diese Felder helfen beim Filtern nicht ausnutzbarer Felder Linux Schwachstellen. Diese Erweiterung verbessert die Integration auf der Erkennungsebene und auf der Ebene angreifbarer Elemente (VIS).

Importieren Sie zusätzliche Metadaten aus Qualys

Importieren Sie zusätzliche Metadaten für Schwachstellen-Elemente (VIS), um Schwachstellen basierend auf den Auswirkungen auf einen Kernel oder einen Service zu filtern.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**an.
2. Klicken Sie unter Integrationskonfiguration auf **Scanner-Integrationen** .
3. Klicken Sie unter installierte Anwendung auf **Bearbeiten** Für Qualys Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie Auf **Hosterkennungskonfiguration** .
5. Navigieren zu **Weitere Metadaten für Erkennungen importieren**an.
6. Um zusätzliche Metadaten aus zu importieren Qualys, Aktivieren Sie manuell eines der folgenden Kontrollkästchen, die Sie benötigen.
   - **Kernel-Metadaten** : Identifiziert Schwachstellen, die in ausgeführten oder nicht ausgeführten Linux-Kernels gefunden wurden.

     Wenn der Wert der zurückgegebenen Metadaten ist **Nein** , Bedeutet dies, dass die Schwachstelle aufgrund eines nicht ausgeführten Kernels nicht ausnutzbar ist. Informationen zu den abgerufenen Werten finden Sie unter Qualys Metadatenwerte für Schwachstellen.
   - **Servicemetadaten** : Identifiziert Schwachstellen, die in ausgeführten oder nicht ausgeführten Ports oder Services gefunden wurden.
   - **Nutzbare Konfigurationsmetadaten** : Identifiziert Schwachstellen, die aufgrund der aktuellen Hostkonfiguration ausnutzbar sein können oder nicht.

   Hinweis:
   Standardmäßig sind diese Kontrollkästchen nicht aktiviert.
7. Führen Sie aus Qualys Host-Erkennungsintegration mit einem Rückdatum.
   Weitere Informationen zum Festlegen des Startdatums finden Sie unter Optionale Qualys-Änderungen.

Ergebnisse
Die Metadaten wurden importiert.

Nächste Maßnahme
Um die importierten Metadaten anzuzeigen, geben Sie ein `sn_vul_Detection.list` In der Filternavigation. Die Liste der Erkennungen angreifbarer Elemente wird angezeigt. Weitere Informationen zu den Werten, die in den neu hinzugefügten Spalten angezeigt werden, finden Sie unter Qualys Metadatenwerte für Schwachstellen.

Qualys Metadatenwerte für Schwachstellen

Wenn die Kernel-Metadaten, Service-Metadaten und Konfigurationsmetadaten importiert werden, werden auch einige Werte abgerufen. Die Werte **0** , **1** Und **Nicht verfügbar** Werden im Back-End verarbeitet und in konvertiert **Nein** , **Ja** Und **Leer** Entsprechend.

Diese Werte werden in den folgenden Spalten in der Liste Schwachstellenelementerkennungen und Schwachstellenelemente ausgefüllt:

- Betrifft Spalte „ausgeführter Service“
- Betrifft die Spalte der ausnutzbaren Konfiguration
- Betrifft die ausgeführten Kernel-Spalten

Hinweis:

- Diese Spalten sind standardmäßig nicht sichtbar. Weitere Informationen zum Konfigurieren des Formularlayouts finden Sie unter Konfigurieren Sie das Formularlayout
- Bei älteren Erkennungen können die Werte für diese Spalten leer sein. Um die Daten zu aktualisieren, führen Sie eine zurückdatierte Qualys Host Detection Integration aus. Weitere Informationen zum Festlegen des Startdatums finden Sie unter Optionale Qualys-Änderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Tabelle zeigt die abgerufenen Werte und ihre Bedeutung.

Abgerufene Feldwerte und ihre Bedeutung

Feld	Wert	Bedeutung
AFFECT_RUNNING_KERNEL	0	Schwachstelle wurde in einem nicht ausgeführten Kernel gefunden. Die Schwachstelle kann nicht ausgenutzt werden.
AFFECT_RUNNING_KERNEL	1	Schwachstelle wurde in einem ausgeführten Kernel gefunden. Die Schwachstelle ist ausnutzbar.
AFFECT_RUNNING_KERNEL	Nicht verfügbar	Schwachstelle ist keine Kernel-bezogene Schwachstelle.
AFFECT_RUNNING_SERVICE	1	Schwachstelle wurde in nicht ausgeführten Ports oder Services gefunden. Die Schwachstelle kann nicht ausgenutzt werden.
AFFECT_RUNNING_SERVICE	0	Schwachstelle wurde in ausgeführten Ports oder Services gefunden. Die Schwachstelle ist ausnutzbar.
AFFECT_RUNNING_SERVICE	Nicht verfügbar	Schwachstelle ist keine zugehörige Schwachstelle.
AFFECT_EXPLOITABLE_CONFIG	1	Schwachstelle ist aufgrund der Hostkonfiguration nicht ausnutzbar.
AFFECT_EXPLOITABLE_CONFIG	0	Schwachstelle ist aufgrund der Hostkonfiguration ausnutzbar.
AFFECT_EXPLOITABLE_CONFIG	Nicht verfügbar	Schwachstelle ist keine zugehörige Schwachstelle.

Legen Sie zusätzliche Filterparameter für fest Qualys Importe

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit an Qualys Vulnerability Integration Damit Sie die Schwachstellendaten weiter verfeinern können, die Sie mit dem importieren Qualys Integrationen.

Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, damit Sie nur bestimmte Schwachstellendetails überprüfen können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die nach bestimmten IPs oder IP-Bereichen gefiltert sind. Oder Sie möchten nur Computer importieren, die sich in Ihrem Bereich befinden, z. B. nur Computer in Ihrem Unternehmensnetzwerk, die keine externen Geräte sind.

Um Ihnen beim Sammeln dieser Daten zu helfen, können Sie hinzufügen Qualys Parameter, die Ihnen beim Importieren der spezifischen Schwachstellendetails helfen, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder -Codierung können Sie mit dieser Funktion Ihre HTTP-Anforderungsinformationen anpassen Qualys Parameter in Ihrem ServiceNow AI Platform. Sie ändern oder fügen diese Werte Ihrem HTTP-Methodendatensatz unter der REST-Methode für die unterstützte hinzu Qualys Integrationen von Qualys Vulnerability Integration.

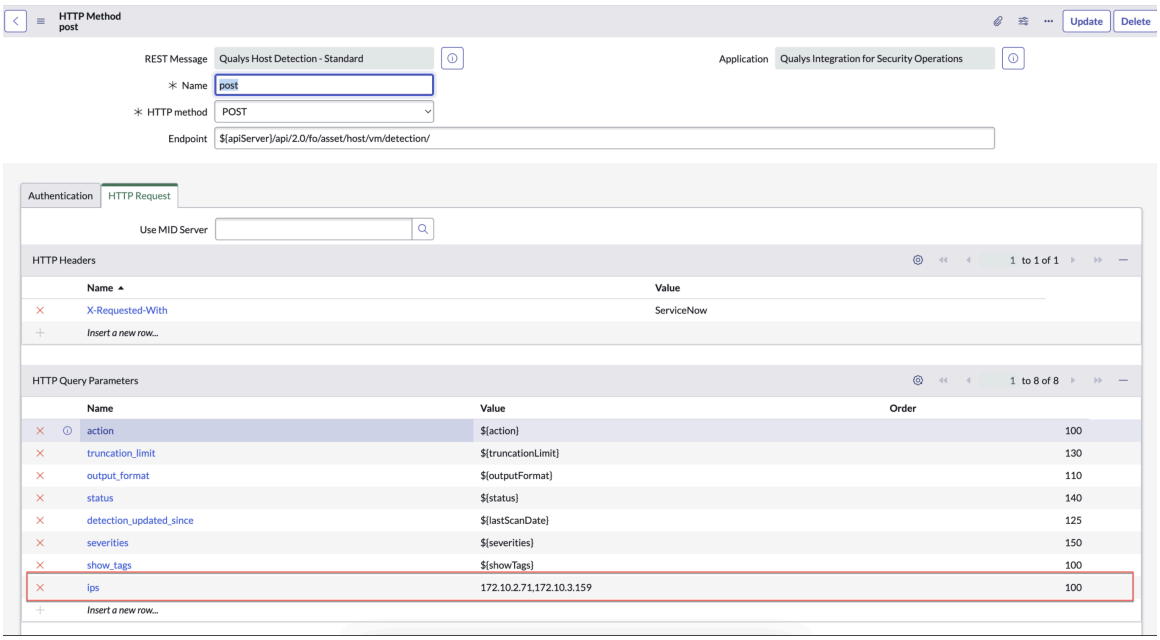
Erforderliche Rolle: sn_vul.Vulnerability_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Suchen Sie die von unterstützten Parameter Qualys Produkt auf der Entwicklerwebsite, das Sie für Ihre Filterung verwenden möchten.
   Parameter und Werte, die Sie aus eingeben Qualys Produkte werden nur auf Integrationsinstanzebene in unterstützt ServiceNow AI Platform. Alle Qualys Integrationen unterstützen das Filtern mithilfe von Abfrageparametern.
2. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**an.
3. Auf der Qualys Integrationslistenseite klicken Sie auf den Datensatz für die Integration, die Sie öffnen möchten.
4. Mit Qualys Registerkarte „REST-Details“ ausgewählt. Suchen und klicken Sie auf das Informationssymbol (I) für die REST-Methode gefolgt von **Öffnen Sie Den Datensatz** Zum Öffnen des HTTP-Methodendatensatzes.
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Fügen Sie in den HTTP-Abfrageparametern für den Anforderungstext die Werte hinzu, die Sie von erhalten haben Qualys Entwickler-Site.

   In der folgenden Abbildung als Beispiel der Parameter, der nur bestimmte IP-Adressen/-Bereiche erfasst, *ips={value}*Wurde hinzugefügt. In diesem Fall **Wert** Ist mindestens eine von Ihnen angegebene IPs/Bereiche. Mehrere Einträge sind durch Kommas getrennt, 172.10.2,71, 172.10.3.159 , Und ein Bereich wird mit einem Bindestrich angegeben, 10.10.10.1-10.10.10.100 . Weitere Informationen finden Sie unter Qualys Entwickler-Website für weitere Informationen.



   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie unter Qualys Dokumentation für weitere Informationen zur Trennung der einzelnen Werte.

   Hinweis:
   Sie sollten sich Ihrer API-Anforderungen bewusst sein. Möglicherweise müssen Sie diese API-Eigenschaften den Abfrageparametern oder dem Textkörper hinzufügen.

   Einige andere Parameter, die Sie möglicherweise in nützlich finden Qualys Entwickler-Site:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `ag_ids` – IDs der abzurufenden Asset-Gruppenliste. Dieser Parameter stellt sicher, dass nur Computer in Ihrem Bereich einbezogen werden.
- `qids` – Dieser Parameter beschränkt die Ergebnisse auf bestimmte Schwachstellen (QID in der Tabelle „Drittpartei-Eintrag“). Diese Einstellung verhindert, dass Ihr System mit Informationsdatensätzen überflutet wird.

7. Klicken Sie auf **Aktualisieren**.

Beheben von Qualys Schwachstellenintegrationsproblemen

Einige häufig aufgetretene Probleme werden zusammen mit Problemumgehungen besprochen.

Anhänge werden nach dem Import nicht angezeigt

Wenn Anhänge nach Importen von Drittparteien-Integrationen nicht wie erwartet für Datenquellen oder in einem Security Incident angezeigt werden, überprüfen Sie Ihre IP-Einschränkungen.

IP-Zugriffsbeschränkungen können verhindern, dass Anhänge angezeigt werden, es sei denn, Sie sind über eine sichere IP angemeldet. Da bei jedem Import ein neuer Anhang hinzugefügt wird, kann dies zu Duplikaten führen, die Sie entfernen müssen.

Wenn Sie beispielsweise eine Host-Importintegration einer Drittpartei ausführen und keine Anhänge in Ihren Datenquellen sehen, überprüfen Sie Ihre IP-Einschränkungen, und fügen Sie der Safe-Liste Anwender hinzu, bevor Sie den Import durchführen.

Ändern Sie Transformationszuordnungen

Transformationszuordnungen werden mit Basiskonfigurationen bereitgestellt und sind normalerweise ausreichend. Sie können Transformationszuordnungen je nach Bedarf Ihrer Organisation ändern.

Vorbereitungen

Erforderliche Rolle: sn_vul_qualys.admin + Import_admin

Prozedur

1. Navigieren zu **Alle** > **System-Importsätze** > **Administration** > **Transformationszuordnungen** Zum Anzeigen der REST-Nachrichten.
2. Filtern Sie die resultierende Liste nach Anwendung, und beschränken Sie die Liste auf **Qualys-Schwachstellenintegration** Anwendung.
3. Ändern Sie die Transformationszuordnungen entsprechend den Kundenanforderungen.

   Details zu den von der Qualys-API bereitgestellten Daten finden Sie unter Qualys-API-Dokumentation .

Überprüfen Sie die Größe der XML-Anhangseigenschaft

Überprüft, ob die XML-Anhangseigenschaft für große Dateien ausreicht.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Import Export**an.
2. Scrollen Sie nach unten zu **Importeigenschaften** > **XML-Format** Unten auf der Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Ändern Sie bei Bedarf den Wert in 250, und klicken Sie auf **Speichern** .

Zugehörige Informationen

Verfügbare Systemeigenschaften

Einschränkungen des Datenabrufs

Standardmäßig gibt es keine Einschränkungen beim Abrufen von Daten aus Qualys. Viele Datensätze können auf Schwachstellen mit niedrigem Schweregrad zurückzuführen sein, die ein Kunde nicht mit seinem Vulnerability Response-Prozess beheben möchte. Durch das Aktualisieren der entsprechenden REST-Nachrichten-/Methodenparameter kann dieses Verhalten geändert werden.

Die für dieses Update verantwortliche REST-Nachricht/Methode ist **Qualys-Host-Erkennung: Standard/Post** . Um die Werte zu aktualisieren, fügen Sie der Post-Methode einen neuen HTTP-Abfrageparameter mit den folgenden Werten hinzu:

- Name: Schweregrade
- Wert: 3-5 (oder ein beliebiger geeigneter Schweregrad)

Fehler bei der Qualys Knowledge Base-Integration wird behoben

Lösen Qualys Fehler bei der Knowledge Base-Integration durch Reduzierung der von empfangenen Nutzlastanhangsgröße Qualys Bis zum angegebenen Grenzwert.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Stellen Sie sicher, dass die Nutzlast-Anhangsgröße innerhalb des angegebenen Grenzwerts liegt.
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**an.
   b. Wählen Sie aus **Integrationsinstanzparameter** Registerkarte.
   c. Wählen Sie Aus **max_delta_days** Und ändern Sie den Standardwert in 3.
2. Wenn die Integration weiterhin fehlschlägt, führen Sie die folgenden Schritte aus:
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Primäre Integrationen**an.
   b. Wählen Sie Aus **Qualys Knowledge Base** .
   c. Wählen Sie aus **Integrationsdetails** Registerkarte.
   d. In **Startzeit** Wählen Sie das aktuelle Datum aus, um die Ausführung der Ausführung für diesen Tag zu überspringen.
   e. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Wählen Sie aus **Integrationsinstanzparameter** Registerkarte.

g. Wählen Sie Aus **kb_Backfill_Full_Import** Und ändern Sie den Standardwert in „wahr“.

Ergebnisse

Durch die Ausführung der Qualys Knowledge Base Backfill-Integration werden alle Drittparteieinträge (TPEs) im System aktualisiert. Während die Qualys Host Detection-Integration einen Platzhaltereintrag erstellt, aktualisiert die Qualys Knowledge Base Backfill-Integration ihn.

Qualys Vulnerability Integration Berichterstellung

Die Qualys Cloud PlatformÜbersicht ist eine Ansicht der Führungskraft der Schwachstellenaktivität. Durch die Bereitstellung von Trends, Berichten und Drilldowns zu bestimmten Daten kann ein Administrator oder Analyst Problembereiche schnell erkennen. Die Diagramme werden nach angreifbaren Elementen und mit Daten gefüllt Qualys Knowledge Base-Daten wurden abgerufen.

Datenvisualisierungen in Vulnerability Response Arbeitsbereiche

Die Vulnerability Response Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie Ihren Korrekturfortschritt überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen, die aktualisiert werden, wenn sich Schwachstellendaten ändern. Siehe Vulnerability Response Arbeitsbereiche, Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen erkunden Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen.

Vorherige Versionen von Vulnerability Response

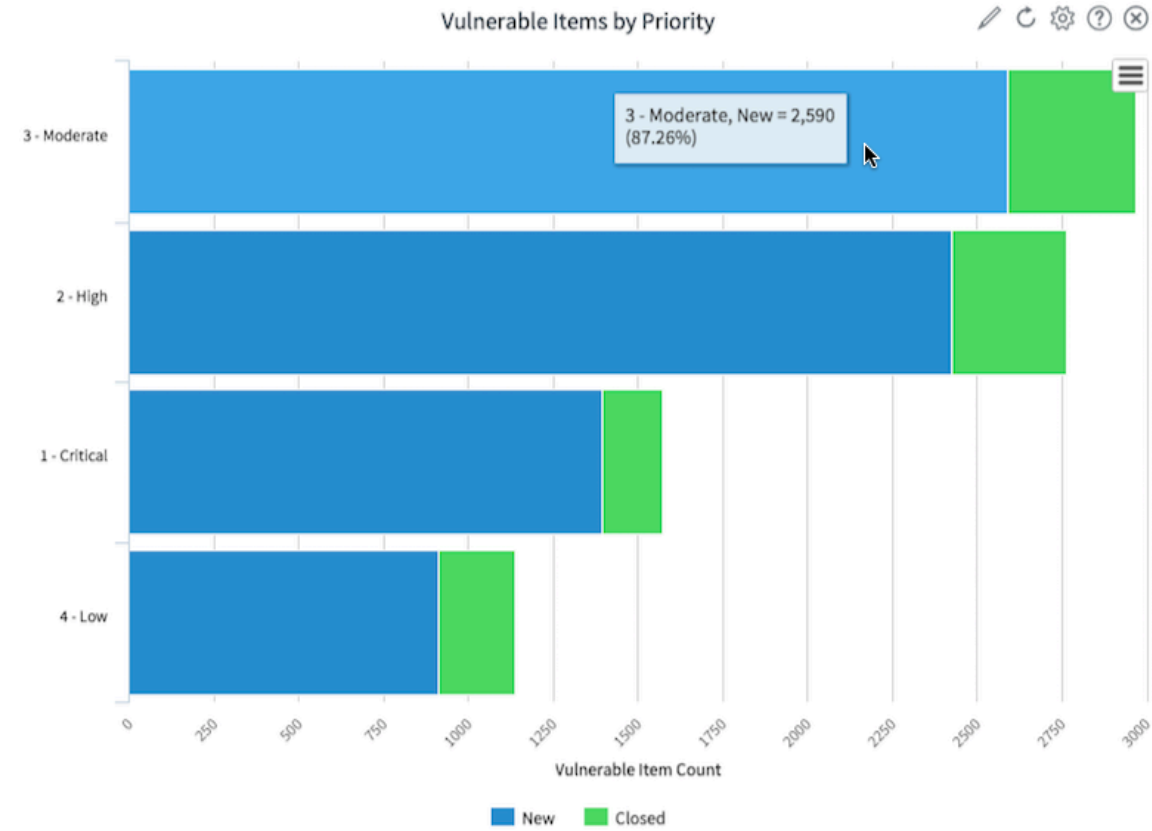
Schwachstellenanalysten können auch die Standard-Dashboards in der klassischen Umgebung verwenden, um Schwachstellendaten zu überwachen. Weitere Informationen finden Sie unter Wird standardmäßig verwendet Vulnerability Response Dashboards.

Hinweis:
Mit Qualys Cloud Platform Bei der Schwachstellenintegration wird davon ausgegangen, dass in Ihrer Instanz Optimierungen, Tests und Bereitstellungen durchgeführt wurden. Diese Funktionen sind Bereiche, die über den Umfang der Produktdokumentation hinausgehen. Wenn Sie Hilfe benötigen, wenden Sie sich an Kundenservice und Support.

In jedem Diagramm können Sie auf einen beliebigen Teil eines Diagramms zeigen (Balken, Kreis, Datenpunkt usw.), um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel Qualys Vulnerability Integration Diagramm



Die folgenden Berichte sind im verfügbar Qualys Cloud Platform Homepage.

Qualys Vulnerability Integration Übersichtsberichte

Name	Visuell	Beschreibung
Mit Qualys synchronisierte CIs	Balkendiagramm	Zeigt die Anzahl der offenen angreifbaren Elemente an, die für jedes CI aufgezeichnet wurden, von den meisten bis zum wenigsten.
Offene angreifbare Qualys-Elemente	Balkendiagramm	Zeigt die Anzahl der offenen angreifbaren Elemente an, die Schwachstellen zugeordnet sind (CVE-Datensätze), von den meisten bis zu den geringsten.
Angreifbare Qualys-Elemente insgesamt	Balkendiagramm	Zeigt die Anzahl der ignorierten angreifbaren Elemente an, die innerhalb von 7 Tagen ablaufen sollen.
Angreifbare Elemente nach Priorität	Trend	Zeigt die Anzahl der pro Woche aufgezeichneten Schwachstelleneinträge an.
QID-Verbreitung	Balkendiagramm	Zeigt die Anzahl der für jedes Modell aufgezeichneten angreifbaren Elemente an, von den meisten bis zu den wenigsten.
Offene angreifbare Qualys-Elemente	Liste	Zeigt die Anzahl der für jeden Herausgeber aufgezeichneten angreifbaren Elemente an, von den meisten bis zu den wenigsten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Qualys Statusdiagramm der Integrationsausführung

Die Qualys Das Modul „Integrationsausführungsstatus“ ist eine grafische Ansicht des Status von Qualys Integrationsausführungen.

Um den Status von Integrationsausführungen anzuzeigen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Status der Integrationsausführung**an.

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard ist in der neuen Experience-UI verfügbar.

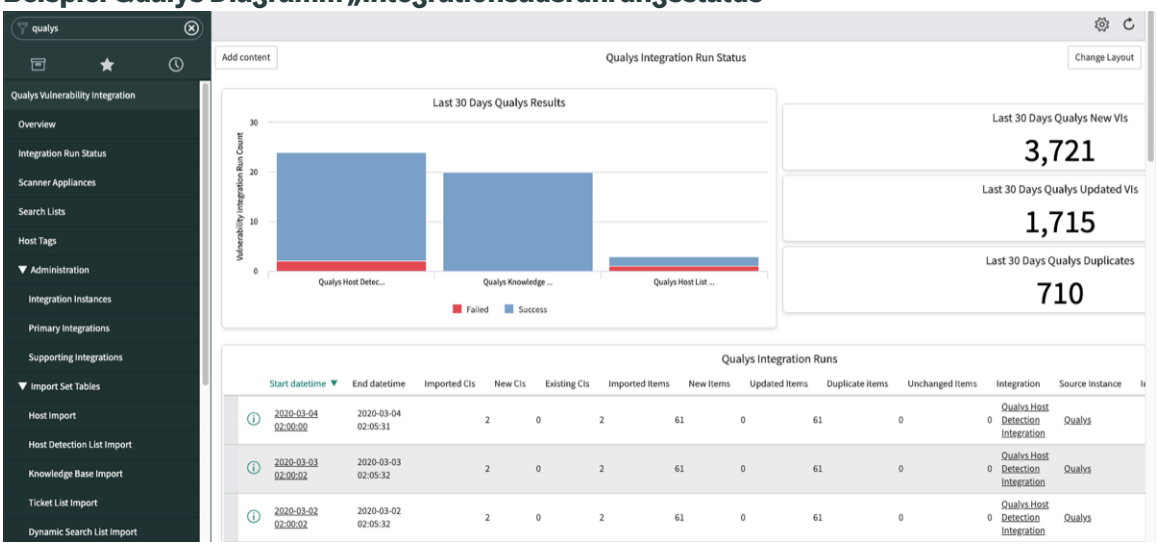
Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Zeigen Sie im Diagramm auf ein beliebiges Teil (Balken, Kreis, Datenpunkt usw.), um allgemeine Daten anzuzeigen, die für dieses Teil spezifisch sind. Wenn Sie auf einen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Die Qualys Status der Integrationsausführung zeigt den Ausführungsstatus der Schwachstellenintegration für die letzten 30 Tage an. Die aktualisierte VIS-Anzahl von Qualys[qualys] gibt die Anzahl aller eindeutigen Erkennungen im selben Asset an. Das VI wird dann mit der neuen Erkennung aktualisiert.

Hinweis:
Die Anzahl der Ausführungen der Schwachstellenintegration wird nur für die Integrationen angezeigt, die auf den Status „aktiv“ gesetzt sind. Navigieren zu **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen** Und legen Sie den Status auf aktiv fest.

Beispiel Qualys Diagramm „Integrationsausführungsstatus“



- Die Werte in der Spalte importierte Elemente stellen die Gesamtzahl der Datensätze dar Die aus einer Integrationsausführung erstellt wurden.
- In der Spalte neue Elemente wird die Anzahl der Datensätze angezeigt Die aus einer Integrationsausführung erstellt wurden.
- Die Spalte „doppelte Elemente“ ist nicht mehr ausgefüllt. Möglicherweise möchten Sie diese Spalte aus der Anzeige entfernen.
- In der Spalte „aktualisierte Elemente“ wird die Anzahl der Datensätze angezeigt Werden während einer Integrationsausführung aktualisiert. Dieser Wert ist nicht die Anzahl der eindeutigen Datensätze Die aktualisiert wurden. Wenn zum Beispiel ein Datensatz Wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

während der Integrationsausführung zweimal aktualisiert, wird sie zweimal gezählt und als angezeigt 2 Aktualisierte Elemente.

- In der Spalte „unveränderte Elemente“ werden Datensätze angezeigt Während der Integrationsausführung gefunden, die bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hatte.

Hinweis:
Integrationsausführungen mit null Ergebnissen für alle vier der folgenden Werte: **Neue CIs** , **Vorhandene CIs** , **Neue Elemente** , Und **Aktualisierte Elemente** Werden aus gefiltert **Qualys-Integration Wird Ausgeführt** Liste.

Qualys Statusdiagrammberichte der Integrationsausführung

Name	Beschreibung
Letzte 30 Tage Qualys Ergebnisse	Die Anzahl der für jede Integration abgeschlossenen Integrationsausführungen. Zeigt sowohl erfolgreiche als auch fehlgeschlagene Ausführungen an. In einer Balkenvisualisierung ausführen.
Letzte 30 Tage Qualys Neue VIS	Die Anzahl der neuen Datensätze In den letzten 30 Tagen importiert. Wird als Ganzzahl angezeigt.
Letzte 30 Tage Qualys Aktualisierte VIS	Die Anzahl der aktualisierten Datensätze In den letzten 30 Tagen importiert. Wird als Ganzzahl angezeigt.
Letzte 30 Tage Qualys Duplikate	Die Anzahl der doppelten Datensätze In den letzten 30 Tagen importiert. Wird als Ganzzahl angezeigt.
Qualys Integrationsausführungen	Die Datensätze der Integrationsausführung in einer Liste. **Hinweis:** **V16.1:** Um die Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit ServiceNow Erkennungsdaten in `sn_vul_detection`Tabelle. Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennung oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „bis datumsanzahl“ in der Instanz nach Abschluss der Integrationsausführung an.
Letzte 30 Tage Qualys Leistungsmetriken Der Erfassung Angreifbarer Elemente	Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich zu den letzten 30 Tagen.
Letzte 30 Tage Qualys Leistungsdurchsatz Der Erfassung Angreifbarer Elemente	Täglicher Durchsatz der Erfassung angreifbarer Elemente, gemessen für Qualys Integration der Host-Erkennung für die letzten 30 Tage.

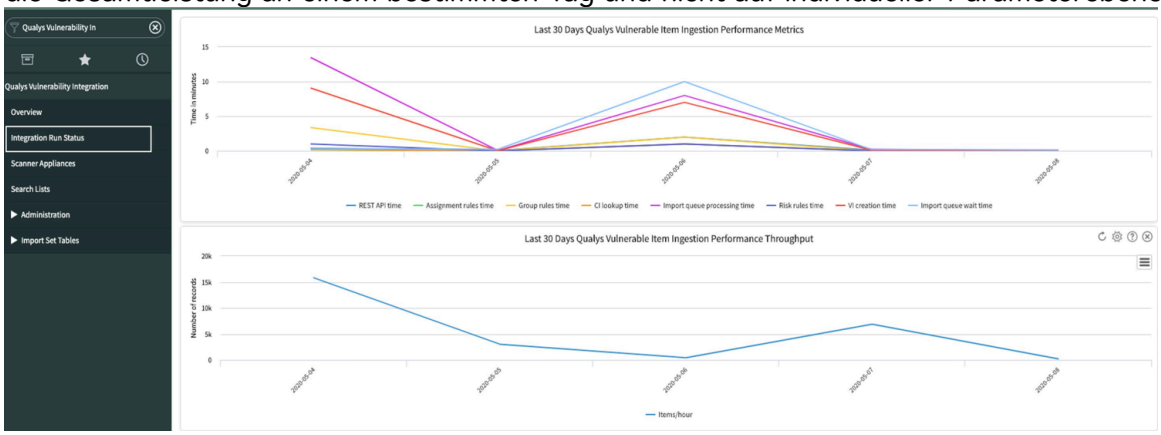
Mehrere Faktoren können sich auf die Leistung der Integrationsausführung auswirken, z. B. die Datenmenge und die Zeit, die für die Verarbeitung dieser Daten benötigt wird. Zwei Diagramme vergleichen die Leistungsmetriken:

- Qualys Leistungsmetriken der Erfassung angreifbarer Elemente: Tägliche Leistungsmetriken für Zuweisungsregeln, Gruppenregeln, Risikoregeln, Warteschlangenwartezeit, Warteschlangenverarbeitungszeit, und andere Statistiken für angreifbare Elemente in den letzten 30 Tagen, um die Ursache für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Leistungsabweichungen zu identifizieren. Die Leistung wird basierend auf der für jede Aktivität benötigten Zeit berechnet. Diese Parameter werden auf Ebene der Integrationsausführung berechnet und zugeordnet. Jeder Parameter ist zur einfachen Identifizierung farbcodiert.

- Qualys Leistungsdurchsatz der Erfassung angreifbarer Elemente: Vergleichen Sie den täglichen Erfassungsdurchsatz angreifbarer Elemente für Qualys Integration der Host-Erkennung. Der Durchsatz wird in Elementen pro Stunde gemessen. Dieser Bericht zeigt die Gesamtleistung an einem bestimmten Tag und nicht auf individueller Parameterebene.



Qualys-Datentransformation

Die von Qualys abgerufenen Daten werden über eine Reihe von Datenquellen und Transformationen verarbeitet.

Die meisten Transformationen für Qualys Vulnerability Integration Werden mithilfe von Transformationsskripts ausgeführt. Diese Skripts dienen zur internen Verwendung. Das Löschen wird nicht empfohlen. Änderungen erfordern Codierung oder erweitert ServiceNow Oder Qualys Vulnerability Integration Fachwissen. Die verbleibenden Karten sind in diesem Abschnitt aufgeführt und verwenden Feldzuordnungen.

Hinweis:
Während der Installation normalisierte Schweregradzuordnungen, die die Transformation importiert hat Qualys Cloud Platform Schweregradstufen auf Standard ServiceNow Schweregradstufen, werden in installiert Vulnerability Response Normalisiertes Schweregradzuordnungsmodul. Weitere Informationen finden Sie unter Erstellen Sie einen Vulnerability Response Schweregradzuordnung.

Import dynamische Suchliste

Die Transformationszuordnung der dynamischen Qualys-Suchliste wird verwendet, um dynamische Qualys-Suchlisten zu transformieren und zu importieren. Änderungen an dieser Transformation ändern, wie dynamische Suchlisten verarbeitet und in das System eingefügt werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Import Der Dynmaic-Suchliste**an.

Die Tabelle zeigt die Felder, die derzeit transformiert werden.

Transformationszuordnungsfelder der dynamischen Qualys-Suchliste

Quellfeld	Zielfeld	Beschreibung
u_id	id	Wird als Bezeichner für die dynamische Qualys-Suchliste verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transformationszuordnungsfelder der dynamischen Qualys-Suchliste (Fortsetzung)

Quellfeld	Zielfeld	Beschreibung
[Skript]	list_type	Der Typ der Suchliste. Dynamisch ist der Standard für die Transformation der dynamischen Suchliste.
u_title	Titel	Der Name in Qualys für diese Suchliste.

Neben Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.

Dynamische Qualys-Suchliste – Transformationsskript für Zeitplan und Zweck der Zuordnung

Wenn das Skript ausgeführt wird	Zweck des Skripts
OnAfter (nachdem die Transformation eines Importsatzes abgeschlossen wurde).	Erstellt die Beziehungen zwischen Suchlisten und ihren zugehörigen Schwachstellen. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen.

Import statische Suchliste

Die Transformationszuordnung der statischen Qualys-Suchliste wird verwendet, um statische Qualys-Suchlisten zu transformieren und zu importieren. Änderungen an dieser Transformation ändern, wie statische Suchlisten verarbeitet und in das System eingefügt werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Import statische Suchliste**an.

Die Tabelle zeigt die Felder, die derzeit transformiert werden.

Transformationszuordnungsfelder der statischen Qualys-Suchliste

Quellfeld	Zielfeld	Beschreibung
u_id	id	Wird als Bezeichner für die statische Qualys-Suchliste verwendet.
u_title	Titel	Der Name in Qualys für diese Suchliste.
[Skript]	list_type	Der Typ der Suchliste. Statisch ist der Standard für die Transformation der statischen Suchliste.

Neben Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transformationsskript für Qualys-statische Suchliste – Zeitpunkt und Zweck der Zuordnung

Wenn das Skript ausgeführt wird	Zweck des Skripts
OnAfter (nachdem die Transformation eines Importsatzes abgeschlossen wurde).	Erstellt die Beziehungen zwischen Suchlisten und ihren zugehörigen Schwachstellen. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen.

Assetgruppenimport

Die Transformationszuordnung für Qualys Asset Group Appliance wird verwendet, um Qualys Asset Group-Daten zu transformieren, um Scanner-Appliance-Datensätze zu erstellen. Änderungen an dieser Transformation ändern, wie Scanner-Appliances erstellt und geändert werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Assetgruppenimport**an.

Die Tabelle zeigt die Felder, die derzeit transformiert werden.

Transformationszuordnungsfelder der Qualys-Asset-Gruppe

Quellfeld	Zielfeld	Beschreibung
u_id	id	Wird als Bezeichner für die Qualys-Asset-Gruppe verwendet.
[Skript]	Manuell	Geskripteter Wert, um zu bestimmen, wie der Zieldatensatz erstellt wurde. Wenn dieses Feld durch Transformationen erstellt wird, ist es immer falsch.
[Skript]	ips	Die IP-Adressen, die der zu transformierenden Asset-Gruppe zugeordnet sind.
u_default_Appliance_ID	Appliance_ID	Der Qualys-Gerätebezeichner für das Standardgerät in dieser Asset-Gruppe.
u_title	Asset_Group_Name	Der Name der Qualys-Asset-Gruppe.

Neben Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.

Zeitpunkt und Zweck der Qualys-Asset-Gruppe-Transformationszuordnung

Wenn das Skript ausgeführt wird	Zweck des Skripts
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Das Skript, das die Importe von Asset-Gruppen auf Asset-Gruppen mit einer Standardanwendung und einem Satz zugeordneter IP-Adressen beschränkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitpunkt und Zweck der Qualys-Asset-Gruppe-Transformationszuordnung (Fortsetzung)

Wenn das Skript ausgeführt wird	Zweck des Skripts
	Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen.

Appliance-Import

Die Zuordnung „Qualys-Appliance-Transformation“ wird verwendet, um Qualys-Appliance-Daten in Appliance-Datensätze umzuwandeln. Dies wird verwendet, um die Appliance-Datensätze zu aktualisieren, die anfänglich aus dem Asset-Gruppenimport erstellt würden. Änderungen an dieser Transformation ändern, wie Appliance-Datensätze mit Appliance-Details aktualisiert werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Importsatztabellen** > **Appliance-Import**an.

Die Tabelle zeigt die Felder, die derzeit transformiert werden.

Zuordnungsfelder der Qualys-Appliance-Transformation

Quellfeld	Zielfeld	Beschreibung
u_name	Appliance_Name	Der Name des Qualys-Scannergeräts.
u_status	Appliance_Status	Der zuletzt gemeldete Status des Qualys-Scannergeräts.
u_id	Appliance_ID	Der Bezeichner des Qualys-Geräts.

Neben Feldzuordnungen gibt es auch ein Transformationsskript, das während des Transformationsprozesses ausgeführt wird.

Die folgende Tabelle zeigt, wann dieses Skript ausgeführt wird und wofür es verwendet wird.

Zeitplan und Zweck der Qualys-Appliance-Transformationszuordnung

Wenn das Skript ausgeführt wird	Zweck des Skripts
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Wird verwendet, um Gerätenamen und -Status für die angegebene ID zu aktualisieren. Für den internen Gebrauch. Das Ändern oder Löschen wird nicht empfohlen.

Qualys REST-Nachrichten

Qualys-REST-Nachrichten werden verwendet, um Aufrufe an die Qualys-API zu tätigen.

Ab Version 12.9.2 von Qualys, Sie haben die Möglichkeit zwischen Standardauthentifizierung oder OAuth zu wählen. Der Instanzparameter Qualys Cloud-Authentifizierungsmethode ist für die Standardauthentifizierung vorkonfiguriert. Wenn Sie OAuth verwenden möchten, müssen Sie den Integrationsinstanzparameter ändern und dann die Rest-Nachricht direkt für OAuth einrichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachricht der Qualys-Host-Erkennung

Die REST-Nachricht Qualys-Host-Erkennung führt den ersten Aufruf an die Host-Listenerkennungs-API für die Qualys-Host-Erkennungsintegration durch.

REST-Nachrichtenparameter der Qualys-Hosterkennung

Parametername	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter. Änderungen sind nicht erforderlich.
output_format	XML	Legt das Format des von Qualys zurückgegebenen Berichts fest. Die verschiedenen Skripts und Transformationen übernehmen XML, daher werden Änderungen am Wert nicht empfohlen.
Detection_processed_After	${lastScanDate}	Zeigt nur Erkennungen an, deren Erkennungsstatus sich nach einem bestimmten Datum und einer bestimmten Uhrzeit geändert hat. Bei Erkennungen, die sich nie geändert haben, wird das Datum auf das letzte Erkennungsdatum angewendet.
Truncation_limit	500	Die Anzahl der Hosts, von denen Daten gemäß Anforderung abgerufen werden sollen. Dieser Parameter wird für Paginierungszwecke verwendet. Der Standardwert ist 500, es können jedoch größere oder kleinere Werte verwendet werden. Legen Sie nicht auf weniger als 100 fest, da dies die Systemlast erheblich erhöht. Kleinere Werte erfordern mehr Aufrufe der Qualys-API, und größere Werte führen zu größeren zu verarbeitenden Ergebnissätzen und potenziellen Datenabruf-/Verarbeitungszeitüberschreitungen.
status	Neu, Behoben, Aktiv, Erneut Geöffnet	Erkennungsstatus, die aus Qualys abgerufen werden sollen. Standardmäßig werden alle Status abgerufen. Für große Datenabrufe (häufig der anfängliche Datenabruf) kann es vorteilhaft sein, feste Status aus dieser Liste auszuschließen. Es ist wichtig, den Status behoben einzubeziehen, wenn Schwachstellen aktualisiert werden, die bereits im System vorhanden sind.

REST-Nachricht für Paginierung der Qualys-Hosterkennung

Die REST-Nachricht „Host-Erkennungspaginierung“ verarbeitet Paginierungsanforderungen an die Host-Erkennungs-API.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Erkennung des primären Hosts ausgeführt wird und die Qualys-API eine URL zum Abrufen der nächsten Seite mit Daten bereitstellt, ruft diese REST-Nachricht diese zusätzlichen Daten ab. Diese Daten werden vom Host-Erkennungs-Paginierungs-Handler verwendet.

DER REST der Host-Erkennungs-Paginierung ist eine spezialisierte REST-Nachricht und nicht zum Ändern vorgesehen.

REST-Nachricht der Qualys Knowledge Base (Auffüllung)

Die REST-Nachricht Qualys Knowledge Base (Backfill) ruft Qualys Knowledge Base-Daten basierend auf dem Zeitstempel der letzten Änderung der Schwachstellendaten für die Qualys Knowledge Base-Integration ab.

Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderung an Qualys aus, Knowledge Base-Informationen abzurufen.

Die folgende Tabelle zeigt die gesendeten Anforderungsparameter.

Qualys Knowledge Base (Auffüllung) REST-Nachrichtenparameter

Parameter	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter. Änderungen werden nicht empfohlen.
details	Alle	Gibt die Detailstufe an, die für abgerufene Schwachstellen angezeigt wird. Kann nach Bedarf geändert werden.
ids	${qIDs}	Gibt an, welche QIDs von Qualys abgerufen werden sollen. Referenziert im Code. Änderungen werden nicht empfohlen.

REST-Nachricht der Qualys Knowledge Base (datumsbasiert)

Die REST-Nachricht Qualys Knowledge Base (datumsbasiert) wird verwendet, um Qualys Knowledge Base-Daten basierend auf dem Zeitstempel der letzten Änderung der Schwachstellendaten abzurufen. Diese Nachricht wird von der Qualys Knowledge Base-Integration verwendet.

Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderung an Qualys aus, Knowledge Base-Informationen abzurufen.

Die folgende Tabelle zeigt die gesendeten Anforderungsparameter.

Qualys Knowledge Base (datumsbasiert) REST-Nachrichtenparameter

Quellfeld	Zielfeld	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter. Änderungen werden nicht empfohlen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Qualys Knowledge Base (datumsbasiert) REST-Nachrichtenparameter (Fortsetzung)

Quellfeld	Zielfeld	Beschreibung
details	Alle	Gibt die Detailstufe an, die für abgerufene Schwachstellen angezeigt wird. Kann nach Bedarf geändert werden.
Last_modified_After	${dateStart}	Gibt an, wann mit dem Abrufen von Verlaufsdaten begonnen werden soll. Wird vom Code verwendet, um die Startzeit zu bestimmen und die Paginierung zu unterstützen. Änderungen oder Entfernen werden nicht empfohlen.
Last_modifiedbefore	${dateEnd}	Gibt an, wann das Abrufen von Verlaufsdaten beendet werden soll. Wird von Code verwendet, um die Endzeit zu bestimmen und die Paginierung zu unterstützen. Änderungen oder Entfernen werden nicht empfohlen.

REST-Nachricht für Qualys-Tickets

Die REST-Nachricht „Qualys-Tickets“ ruft Qualys-Ticketinformationen für die Qualys-Ticketintegration ab. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die an Qualys gestellten Anforderungen zum Abrufen von Ticketinformationen aus.

Die Tabelle zeigt die gesendeten Anforderungsparameter.

REST-Nachrichtenparameter für Qualys-Tickets

Parametername	Wert	Beschreibung
Modified_since_datetime	${lastRunDatetime}	Gibt das Datum der letzten Ausführung der Integration und das Datum an, nach dem Daten abgerufen werden sollen. Verwendet von Code. Änderungen werden nicht empfohlen.
Since_Ticket_number	${lastTicketNumber}	Gibt an, welches Ticket zuletzt von Qualys abgerufen wurde. Wird für Paginierung verwendet. Änderungen werden nicht empfohlen.
Show_vuln_Details	1	Gibt an, ob die Schwachstellendetails abgerufen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Teilen Sie Qualys-Erkennungen basierend auf der Schwachstelleninstanz auf

Mit Vulnerability Response können Sie Erkennungen von Qualys-Scannern aufteilen und für jede erkannte Schwachstelleninstanz ein eindeutiges angreifbares Element (VIT) erstellen. Dies unterstützt eine präzisere Zuweisung an Korrekturteams und verbessert das Schwachstellenmanagement und die Nachverfolgung.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Nutzlast des Qualys-Scanners enthält Erkennungsdaten mit Nachweisdetails. Jeder Pfad im Nachweis wird verwendet, um Schwachstelleninstanzen zu identifizieren und aufzuteilen. Das Ausgabe-Tag in der Nutzlast gibt den Standort der Schwachstelle an, wodurch eine genaue Trennung und Verwaltung von Erkennungen ermöglicht wird.

Prozedur

1. Aktivieren Sie die Aufteilung der Erkennung
   a. Navigieren Sie zur Tabelle „Drittpartei-Integration“ [sn_sec_int_Integration].
   b. Öffnen Sie den Datensatz für `Qualys Cloud-Plattform` .
   c. Legen Sie die Eigenschaft `Include proof VI key` auf *true* fest.
   d. Speichern Sie den Datensatz.
2. **Wahlweise:** Schließen Sie bestimmte QIDs von der Erkennungsaufteilung aus
   a. Öffnen Sie die Systemeigenschaft [sn_vul_qualys.Skip_Split_Detection_IDs].
   b. In **Wert** Feld eine kommagetrennte Liste von QIDs eingeben, die Sie von der Aufteilung ausschließen möchten.

      Hinweis:
      Standardmäßig sind die folgenden QIDs aufgrund des Volumens ihrer Ergebnisse von der Aufteilung ausgeschlossen: QID-989920, QID-993308, QID-5001711, QID-5001632.

   c. Speichern Sie die Eigenschaft.
3. Stellen Sie sicher, dass QIDs für die Aufteilung aufgeführt sind
   a. Navigieren Sie zur Tabelle „Nachweisschlüssel-Schwachstellenliste“ [sn_vul_proof_key_Vulnerability_list].
   b. Stellen Sie sicher, dass die QIDs, die Sie aufteilen möchten, aufgeführt sind.

Ergebnisse

Nach der Ausführung von `Qualys-Host-Erkennungsintegration` , Erkennungen werden basierend auf Nachweisen aufgeteilt, sodass für jede Schwachstelleninstanz einzelne angreifbare Elemente (Vits) erstellt werden. Sie können die Ergebnisse in der Tabelle „Erkennungen von Schwachstellenelementen“ [sn_vul_Detection_list] überprüfen, in der jede Erkennung als separater Datensatz angezeigt wird.

Mit installierte Komponenten Qualys Vulnerability Integration

Die folgenden Rollen, Integrationsaufträge und Tabellen werden mit installiert Qualys Vulnerability Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Zeigen Sie gefilterte Listen für Komponenten an, die mit einer Anwendung installiert wurden

Filtern Sie die Tabelle „Anwendungsdateien“ so, dass nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert werden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, sollte installiert werden, damit ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Führen Sie die folgenden Schritte aus, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im Filternavigator ein **sys_metadata.list** Um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) aus, und wählen Sie, **Anwendung** > **ist** Gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**an.
3. Wählen Sie im Bedingungsgenerator aus, um einen zweiten Filter hinzuzufügen **UND** , Und wählen Sie dann aus, **Klasse** > **ist ein** Und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle** , **Geplante Aufgabe** , Oder **Tabelle** .
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die von Ihnen ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul_qualys.read	Hat Lesezugriff auf Qualys Vulnerability Integration Datensätze.	
sn_vul_qualys.user	Anwender für Qualys Vulnerability Integration. Kann Datensätze lesen und schreiben	sn_vul_qualys.read
sn_vul_qualys.admin	Administrator für Qualys Vulnerability Integration. Sie können beispielsweise Startdaten der Integration ändern und einige erweiterte Konfigurationseinstellungen vornehmen.	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_Integration	Kann konfigurieren Qualys Vulnerability Integration	sn_vul_qualys.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationsaufträge installiert

Integrationsauftrag	Beschreibung
Qualys Integration Der Statischen Suchliste	Synchronisiert Qualys Suchlisten zum Suchen von Einträgen für angreifbare Elemente. Ruft nur statische Listentypdatensätze ab.
Qualys Umfassende Integration Der Host-Erkennung	Ruft Host- und Schwachstellendaten von ab Qualys Und verarbeitet sie in Ihrer Instanz. Er koordiniert die REST-Nachrichtenaufrufe an die Host-Erkennungs-API. Die Ausgabe dieser Integration sind angreifbare Elemente. Diese Integration importiert alle status der Schwachstelle: Neu, behoben, aktiv und erneut geöffnet. Standardmäßig ist diese Integration inaktiv und wird wöchentlich ausgeführt. **Hinweis:** Nachdem diese Integration aktiviert wurde, importiert der tägliche umfassende Auftrag nur die status Neu, behoben und erneut geöffnet.
Qualys Integration Der Hostliste	Ruft authentifizierte und nicht authentifizierte Host-Scan-Daten und Host-Tags von ab Qualys Einmal pro Woche und speichert es im Modul „erkannte Elemente“ in Ihrer Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht gescannt wurden.
Qualys Integration Der Host-Erkennung	Ruft Host- und Schwachstellendaten von ab Qualys Und verarbeitet sie in Ihrer Instanz. Er koordiniert die REST-Nachrichtenaufrufe an die Host-Listenerkennungs-API. Die Ausgaben dieser Integration sind angreifbare Elemente. Qualys Host-Tags werden in diese Integration importiert.
Qualys Ticketintegration	Ruft Ab Qualys Tickets und fügt sie Ihrer Instanz hinzu. Er koordiniert die REST-Nachrichtenaufrufe an die Ticketlisten-API. Seit gibt es häufig weniger Tickets als Host-Erkennungen Qualys Einstellungen können die Erkennungen einschränken, die zu einem Ticket führen.
Qualys Integration Der Optionsprofilliste	Ruft Optionsprofile aus dem ab Qualys Produkt. Optionsprofile enthalten Scan-Einstellungen, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationsauftrag	Beschreibung
	erforderlich sind, wenn Sie Scans über starten ServiceNow AI Platform Instanz.
Qualys Integration Der Geräteliste	Ruft Informationen zum Scanner-Gerät von ab Qualys.
Qualys Asset-Gruppenintegration	Ruft Asset-Gruppeninformationen von ab Qualys. Asset-Gruppen werden verwendet, um zu identifizieren, welche Scanner-Geräte zum Scannen übereinstimmender Konfigurationselemente verwendet werden sollen.
Qualys Knowledge Base (Auffüllen)	Ruft Ab Qualys Knowledge Base-Einträge. Ausführung nach geplant Qualys Integration Der Host-Erkennung. Aktualisiert Ihre Instanz mit allen QIDs, auf die in der Integration der Host-Erkennung verwiesen wurde, aber nicht im System vorhanden waren.
Qualys Knowledge Base	Ruft Ab Qualys Knowledge Base-Einträge. Die abgerufenen Daten basieren auf dem Datum, an dem die Schwachstellen aktualisiert wurden Qualys Und seit der letzten Ausführung der Integration. Diese Daten sind nützlich, um Verlaufsdaten in Ihre -Instanz auszufüllen und sicherzustellen, dass Qualys Bezeichner (QIDs) sind aktuell.
Qualys Integration Der Dynamischen Suchliste	Synchronisiert Qualys Durchsuchen Sie Listen, um angreifbare Einträge zu finden, und ruft dynamische Listentypdatensätze ab.
Die Erkennungen für den aktualisierten Schlüssel für werden korrigiert Qualys	Eine Kombination von Feldern mit einem Hash, die eine Möglichkeit zum Identifizieren und Verknüpfen einer Erkennung mit einem boten Qualys Angreifbares Element.
Qualys Aktualisieren Sie vorhandene erkannte Elemente mit dem Netzwerkpartition-Bezeichner	Aktualisiert Ihre vorhandenen erkannten Elemente. CIs für Ihre vorhandenen Qualys Schwachstellenintegrationsdaten werden erstellt oder aktualisiert, um die Granularität des Netzwerkpartition-Bezeichners zu enthalten.

Installierte Tabellen

Tabelle	Beschreibung
Schwachstelle der Suchliste sn_vul_qualys_m2m_search_list_vul	Speichert die Zuordnung zwischen Qualys Suchliste und eine Schwachstelle.
Qualys Schwachstellen-Scanner	Tabelle, die Schwachstellen-Scanner erweitert, um Scannerinformationen für zu speichern Qualys Funktion erneut scannen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_vul_qualys_Scanner	
Qualys Listen Durchsuchen sn_vul_qualys_search_list	Speichert Suchlisten, die von abgerufen wurden Qualys Integration der Suchliste.
Qualys Geräteimport sn_vul_qualys_Appliance_imp	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.
Qualys CI sn_vul_qualys_ci	Tabelle wird nicht mehr verwendet.
Host-Erkennungspaginierung sn_vul_qualys_Host_Detection_Pagination	Tabelle wird nicht mehr verwendet.
Qualys Integrationsausführung sn_vul_qualys_Integration_Run	Tabelle wird nicht mehr verwendet.
Qualys Integration sn_vul_qualys_Integration	Tabelle, die die Schwachstellenintegration erweitert und alle zugehörigen Integrationen speichert Qualys.
Qualys Import Statischer Suchliste sn_vul_qualys_static_search_list_imp	Tabelle, die die Importsatzzeile erweitert. Feldzuordnungen werden verwendet, um Daten in die Zieltabelle umzuwandeln. Qualys Listen Durchsuchen.
Qualys Knowledge Base sn_vul_qualys_Knowledge_Base	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.
Qualys Ticketliste sn_vul_qualys_Ticket_list_imp	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.
Qualys Optionsprofil sn_vul_qualys_Option_Profile	Tabelle, in der die von abgerufenen Optionsprofile gespeichert werden Qualys. Diese Tabelle, die mit dem erneuten Scan verwendet wird.
Qualys Import Der Dynamischen Suchliste sn_vul_qualys_Dynamic_search_list_imp	Tabelle, die die Importsatzzeile erweitert. Feldzuordnungen werden verwendet, um Daten in die Zieltabelle umzuwandeln. Qualys Listen Durchsuchen.
Qualys Importsatz Erneut Ausführen sn_vul_qualys_Import_Rerun	Tabelle wird nicht mehr verwendet.
Qualys Optionsprofilimport sn_vul_qualys_Option_Profile_Import	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rapid7 Vulnerability-Integration verstehen

Die ServiceNow® Rapid7 Vulnerability-Integration Verwendet Daten, die aus importiert wurden Rapid7 Data Warehouse oder Rapid7 InsightVM Produkte, mit denen Sie die Auswirkungen und Priorität potenziell schädlicher Bedrohungen bestimmen können.

Rapid7 Nexpose Sensoren erfassen Daten und senden sie automatisch Zu Rapid7 Data Warehouse (lokal) oder Rapid7 InsightVM(Cloudbasierte) Produkte, die die Informationen kontinuierlich analysieren und korrelieren. Es lässt sich problemlos in integrieren ServiceNow® Vulnerability Response Dient zum Zuordnen von Schwachstellen zu CIs und Services. Die Rapid7 Vulnerability-Integration Ergänzt die Schwachstellendaten in Ihrer Instanz.

Rapid7 Integrationen sind Einstiegspunkte, die mit interagieren Rapid7 Data Warehouse oder Rapid7 InsightVM Produkte, aufgerufen als geplante Aufgaben. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird. Die geplanten Aufgaben werden automatisch und in der angegebenen Reihenfolge ausgeführt. Sie können einzelne geplante Aufgaben auch manuell ausführen.

Hinweis:

Wenn Sie beide verwenden Rapid7 Data Warehouse und Rapid7 InsightVM Als Quellen für Ihre Daten laufen Sie das Risiko doppelter Schwachstellendatensätze aus.

Hinweis:

Bei der Migration von **Data Warehouse** Integrationstyp zu **InsightVM** Geben Sie ein, Sie können Ihre vorhandenen Data Warehouse-Datensätze deduplizieren. Weitere Informationen finden Sie unter Deduplizieren Rapid7 Vulnerability-Integration Data Warehouse-Datensätze.

Wenn Sie mehrere Bereitstellungen von haben Rapid7 InsightVM Schwachstellenintegration können Sie für jede Bereitstellung eine Integration hinzufügen. Assets, die durch mehrere Drittanbieterbereitstellungen identifiziert werden, und ihre Schwachstellen werden konsolidiert und mit Ihrer CMDB abgeglichen. Diese Konsolidierung erfolgt auch dann, wenn sich Scanprozesse zwischen mehreren Bereitstellungen überschneiden. Daten, die aus jeder Bereitstellung stammen, werden identifiziert und in einer einzigen Instanz von verfügbar gemacht Vulnerability Response.

Hinweis:

Sie können die ursprüngliche Schwachstellenintegration nicht löschen, sie jedoch deaktivieren. Aus deaktivierten Vorlagen erstellte Integrationen sind standardmäßig deaktiviert.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Verfügbare Versionen

Release-Version für Yokohama	Release-Hinweise
Rapid7 Vulnerability-Integration V13.6, 13,7	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen

Rapid7 Schwachstellenintegrationsaufgaben umfassen die folgenden Rollen.

- sn_vul_r7.admin: Kann Datensätze lesen, schreiben und löschen.
- sn_vul_r7.user: kann Datensätze lesen und schreiben.
- sn_vul_r7.read: Kann Datensätze lesen.

Rapid7 Vulnerability-Integration-Integrationen

Um anzuzeigen Rapid7 Vulnerability-Integration, Navigieren Sie zu **Rapid7** > **Administration** > **Integrationen**an.

Die folgenden Integrationen sind im Basissystem enthalten.

Rapid7 Data Warehouse-Integrationen

Integration	Beschreibung
Rapid7 Vulnerability-Integration	Ruft Schwachstellendaten von ab Rapid7 Nexpose Und verarbeitet sie in Ihrer Instanz.
Rapid7 Asset-Listenintegration	Ruft Scan-Daten einmal pro Woche von ab Rapid7 Nexpose Data Warehouse und speichert es im Modul „erkannte Elemente“ in Ihrer Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht mit gescannt wurden **Letzter Scan** Datum. Zeigen Sie an **Letzter Scan** Zeit in der Liste „erkannte Elemente“ in Vulnerability Response.
Rapid7 Kategorieintegration	Ruft Kategorieinformationen von ab Rapid7 Nexpose. Kategorien bieten eine allgemeine Klassifizierung für Schwachstellen.
Rapid7 Exploit-Integration	Ruft Exploit-Informationen von ab Rapid7 Nexpose.
Rapid7 Integration Des Malware-Kits	Ruft Informationen zum Malware-Kit von ab Rapid7 Nexpose.
Rapid7 Referenzintegration	Ruft Verweise auf externe regulatorische Dokumente wie CVEs oder Lieferantenspezifische Schwachstellenreferenzen ab.
Rapid7 Lösungsintegration	Ruft Lösungsdaten von ab Rapid7 Nexpose, Der empfohlene Lösungen für bestimmte Schwachstellen bereitstellt.
Rapid7 Integration Der Ersatzlösung	Ruft Informationen darüber ab, welche Lösungen durch andere Lösungen ersetzt werden.
Rapid7 Erforderliche Lösungsintegration	Ruft Informationen zu den Lösungen ab, die Voraussetzungen für andere Lösungen sind. Wenn diese Integration ausgeführt wird, wird die Zuordnung von Lösungen und erforderlichen Lösungen aus dem abgerufen Rapid7 Data Warehouse. **Hinweis:** Diese Integration funktioniert nur, wenn Vulnerability Solution Management Plugin ist aktiviert.
Rapid7 Integration Der Schwachstellenlösungszuordnung	Ruft die Zuordnung ab, um Lösungen Schwachstellen zuzuordnen.
Rapid7 Integration Angreifbarer Elemente	Ruft Daten zu angreifbaren Elementen von ab Rapid7 Nexpose Und verarbeitet sie in Ihrer Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rapid7 Data Warehouse-Integrationen (Fortsetzung)

Integration	Beschreibung
	Die Ausgaben dieser Integration sind angreifbare Elemente.
Rapid7 Integration Der Lösung Angreifbarer Elemente	Ruft Informationen darüber ab, welche angreifbaren Elemente in als geschlossen markiert sind Rapid7 Nexpose Und schließt die entsprechenden angreifbaren Elemente in Vulnerability Response.
Rapid7 Site-Integration	Ruft Site-Daten von ab Rapid7 Nexpose. Eine Website ist eine Sammlung von Assets, die für einen Scan bestimmt sind.
Rapid7 Asset-Listenintegration	Ruft einmal pro Woche Host-Tags und Scan-Daten aus dem ab Rapid7 Data Warehouse und speichert es im Modul „erkannte Elemente“ in Ihrer Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht mit gescannt wurden **Letzter Scan** Datum. Zeigen Sie an **Letzter Scan** Zeit in der Liste „erkannte Elemente“ in Vulnerability Response
Rapid7 Umfassende Integration Angreifbarer Elemente	Importiert alle Rapid7-Erkennungen für alle Konfigurationselemente, die seit der letzten erfolgreichen Integrationsausführung gescannt wurden. Basierend auf den aktuell importierten Daten werden angreifbare Elemente, die kürzlich während Scans nicht gefunden wurden, automatisch in „Geschlossen“ versetzt, wenn das Modul „veraltete angreifbare Elemente automatisch schließen“ aktiviert ist.

Rapid7 InsightVM-Integrationen

Integration	Beschreibung
Rapid7 Integration angreifbarer Elemente – API	Ruft Daten zu angreifbaren Elementen von ab Rapid7 InsightVM und verarbeitet es in Ihrer Instanz.
Rapid7 Vulnerability-Integration – API	Ruft Referenz-, Kategorie-, Exploit-, Malware-Kit- und Schwachstellendaten von ab Rapid7 InsightVM und verarbeitet es in Ihrer Instanz.
Rapid7 Asset-Listenintegration: API	Ruft Host-Tags und Scan-Daten einmal pro Woche von ab Rapid7 InsightVM Und speichert sie im Modul „erkannte Elemente“ in Ihrer Instanz. Hilft bei der Identifizierung von Assets, die in letzter Zeit nicht mit gescannt wurden **Letzter Scan** Datum. Zeigen Sie an **Letzter Scan** Zeit in der Liste „erkannte Elemente“ in Vulnerability Response.
Rapid7 Umfassende Integration angreifbarer Elemente – API	Importiert alle Rapid7-Erkennungen für alle Konfigurationselemente, die seit der letzten erfolgreichen Integrationsausführung gescannt wurden. Basierend auf den aktuell importierten Daten werden angreifbare Elemente, die kürzlich während Scans nicht gefunden wurden, automatisch in „Geschlossen“ versetzt, wenn das Modul „veraltete angreifbare Elemente automatisch schließen“ aktiviert ist.
Rapid7 Site-Integration	Ruft Websitedaten aus dem ab Rapid7 InsightVM Produkt. Diese Integration ist so festgelegt, dass sie wöchentlich um 00:00:00 ausgeführt wird.

Während des Imports werden nicht bereits vorhandene CVE-Datensätze als NVD-Datensätze erstellt und in Drittparteieinträgen für referenziert Rapid7 Standardmäßig. Die Vorlagenintegration für Rapid7 Kann nicht gelöscht werden. Deaktivieren Sie es stattdessen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Service Graph Connector für Rapid7

Ab Version 2,0 ist Service Graph Connector für Rapid7 über verfügbar ServiceNow® Store. Weitere Informationen finden Sie unter Service Graph Connector for Rapid7 .

CI-Suchregeln

CI-Suchregeln legen fest, wie ausgefüllt werden soll **Konfigurationselement** Feld in einem Datensatz eines angreifbaren Elements.

Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Integrationen von Schwachstellen von Drittparteien.

Informationen zum Erstellen oder Bearbeiten von Suchregeln finden Sie unter Erstellen Sie eine Vulnerability Response-CI-Suchregel.

Hinweis:
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

Erkannte Elemente

Dieses Modul listet Konfigurationselemente auf, die während des Imports aus dem erkannt wurden Rapid7 Integrationen angreifbarer Elemente (Data Warehouse oder InsightVM-API) und Rapid7 Asset-Listenintegration: API. Die Rapid7 Asset-Listenintegration: Die API importiert alle Rapid7-Assets, die seit der letzten Integrationsausführung auf Schwachstellen gescannt wurden. Die Rapid7 Integration der Data Warehouse-Asset-Liste ist enthalten.

Hinweis:
Der Standardfilter für diese Liste ist auf festgelegt **Nicht Abgeglichen** . Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Siehe Erkannte Elemente In Vulnerability Response Weitere Informationen zum Modul „erkannte Elemente“.

Host-Tags

Host-Tags werden als Teil von importiert Rapid7 Asset-Listenintegration: API-Integration für Rapid7 InsightVM. Sie werden hauptsächlich zum Filtern verwendet Vulnerability Response Regeln für Zuweisungs- und Korrekturaufgaben in Rapid7 InsightVM. Sie werden im Formular „erkanntes Element“ angezeigt.

Host-Tags

Hinweis:
Die Rapid7 Asset-Listenintegration: Die API-Integration muss ausgeführt werden, bevor Zuweisungs- oder Korrekturaufgabenregeln in erstellt werden Vulnerability Response Damit alle Tags in den Regeln vorhanden sein können und bevor angreifbare Elemente importiert und gruppiert werden.

- Beim Tag-Speicher wird die Groß-/Kleinschreibung nicht beachtet. Wenn ein **San Diego** Tag wird erstellt, dann ein **SAN DIEGO** Tag kann nicht in der Host-Tag-Tabelle gespeichert werden. „San Diego“ und „SAN DIEGO“ werden als dasselbe Host-Tag betrachtet. Das Tag, das importiert wurde, gewinnt zuerst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Verwendung von Host-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Host-Tags werden von der globalen Systemeigenschaft gesteuert **sn_vul.Import_Host_Tags** . Diese Eigenschaft ist standardmäßig auf „wahr“ festgelegt. Wenn Sie Tags deaktivieren, werden sie für alle Instanzen deaktiviert.

Standorte

Eine Website ist eine Sammlung von Assets, die für einen Scan bestimmt sind. Eine Site besteht aus Ziel-Assets, einer Scan-Vorlage, einem oder mehreren Scan-Engines und anderen Scan-bezogenen Einstellungen wie Zeitplänen oder Warnungen. Sites werden von verwaltet Rapid7 Anwendungen.

Rapid7 Vulnerability-Integration Durch die Standortfilterung während der Konfiguration können Sie Assets während des Imports nach Site kategorisieren und anfordern. Siehe Wird gefiltert nach Rapid7 Sites Weitere Informationen zum Filtern von Importen.

Die Rapid7 Data Warehouse und Rapid7 InsightVM Siteintegrationen importieren Sites als wöchentliche geplante Aufgabe.

Um die importierten Sites in einer Liste anzuzeigen, navigieren Sie zu **Rapid7** > **Standorte**an.

Öffnen Sie gelöste angreifbare Elemente erneut, die nicht von Scans geschlossen wurden

Angreifbare Elemente in auf „gelöst“ festgelegt ServiceNow AI Platform Instanz, die jedoch nicht von den nachfolgenden Integrationsausführungen auf „Geschlossen/behoben“ umgestellt wurde, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Für Rapid7 Erkennungen ist jetzt auf der Rapid7-Konfigurationsseite in Ihrer Instanz eine Option verfügbar, um gelöste VIS nach Alter erneut zu öffnen. Wenn diese Option aktiviert ist, werden VIS auf „gelöst“ festgelegt, aber dann nicht auf „Geschlossen/behoben“ umgestellt, indem nachfolgende Scans nach der von Ihnen eingegebenen Anzahl von Tagen zurück zu „Offen“ übergehen.

CIs mit Identification and Reconciliation Engine (IRE) erstellen

Sie können die Identifizierungs- und Abgleichsmodul verwenden, um neue CIs zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann, der von einem Scanner einer Drittpartei importiert wurde. Aktivieren Sie das Plugin „CMDB-CI-Klassenmodelle“, um CIs mit den neuen Klassen zu erstellen. Andernfalls werden nicht übereinstimmende CIs in den nicht übereinstimmenden CI-Klassen erstellt. Weitere Informationen finden Sie unter CIs für werden erstellt Vulnerability Response Verwenden der Identifizierungs- und Abgleichsmodul. Weitere Informationen zum Konfigurieren der Kategorisierung nicht übereinstimmender Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert.

Angreifbare Elemente erneut scannen

Initiieren Sie erneutes Scannen in Rapid7 Plattform, um sicherzustellen, dass Ihre angreifbaren Elemente zwischen den geplanten Scanzyklen behoben wurden. Weitere Informationen finden Sie unter Initiieren Sie einen erneuten Scan für Rapid7 Schwachstellenintegration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Rapid7 Lösungsmanagement

Wenn Sie aktiviert haben Vulnerability Solution Management-Plugin, dann Rapid7 Lösungen für beide Rapid7 Data Warehouse und Rapid7 InsightVM Wird in der Tabelle „Schwachstellenlösungen“ [sn_vul_Solution] ausgefüllt. Wenn Sie jedoch nicht aktiviert haben Vulnerability Solution Management Plugin, dann Rapid7 Vulnerability-Integration Funktioniert unverändert und importiert die Lösungen in die anwenderdefinierte Tabelle [sn_vul_r7_Solution]. Weitere Informationen finden Sie unter Rapid7 Lösungsmanagement.

Vorbereitung für Rapid7 Vulnerability-Integration

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die Rapid7 Vulnerability-Integration Es wird davon ausgegangen, dass Sie mit vertraut sind und ausführen Rapid7 Data Warehouse oder Rapid7 InsightVM Produktscans in Ihrer Umgebung.

Erforderliche Rolle: Administrator

Die Rapid7 Scanner sind standardmäßig in deaktiviert Vulnerability Response Anwendung. Wenn Sie versuchen, einen erneuten Scan von den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, wird der **Erneut Scannen** Schaltfläche ist nicht verfügbar.

Bevor Sie herunterladen Rapid7 Vulnerability-Integration Anwendung aus dem ServiceNow® Store Und installieren Sie es auf Ihrer Instanz, überprüfen Sie die folgenden Informationen zu den Integrationstypen, und richten Sie Informationen ein:

Es gibt zwei Arten von Integrationen im Lieferumfang von Rapid7 Vulnerability-Integration Das ist in verfügbar ServiceNow® Store:

- Rapid7 InsightVM
- Rapid7 Data Warehouse

Die Rapid7 Data Warehouse-Typ:

- Erfordert Ihren Rapid7 URL des Data Warehouse-Servers und Anmeldeinformationen zur Authentifizierung
- Erfordert einen MID-Server
- Verwendet einen PostgresSQL-Treiber, um Abfragen im Data Warehouse auszuführen
- Unterstützt nicht mehrere Instanzen

Die Rapid7 InsightVM Integrationstyp:

- Ist Cloud-basiert und verwendet eine REST-API. Diese Integration erfordert einen API-Schlüssel aus Ihrem Rapid7 Insight-Account.
- Unterstützt mehrere Instanzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Siehe Richten Sie für ein Rapid7 Data Warehouse-Integration(Data Warehouse) und Richten Sie für ein Rapid7 InsightVM Integration Weitere Informationen zu Setup-Anforderungen für diese Integrationstypen.

Richten Sie für ein Rapid7 Data Warehouse-Integration

Die Rapid7 Data Warehouse Die Integration ist einer der Integrationstypen, die in enthalten sind Rapid7 Vulnerability-Integration Rapid7 Vulnerability-Integration.

Vorbereitungen

Bevor Sie ausführen Rapid7 Data Warehouse-Integration führen Sie die folgenden Setup-Aufgaben aus:

- Rufen Sie ab Rapid7 Data Warehouse-Add-on. Siehe Rapid7 Website Und Dokumentation zum Erwerb und Installieren dieses Add-ons.
- Ruft den aktuellen PostgresSQL-Treiber ab. Wechseln Sie zu https://jdbc.postgresql.org/ Und Laden Sie den neuesten Treiber herunter.
- Ein MID-Server zum Ausführen von Abfragen für das Data Warehouse. Siehe MID-Server Weitere Informationen zum Einrichten eines MID-Servers.

  Notieren Sie sich den Namen des Data Warehouse. Die Rapid7 Der Data Warehouse-Integrationstyp unterstützt nur eigenständige MID-Server. Geclusterte MID-Server werden nicht unterstützt.

- Holen Sie sich Ihren Rapid7 URL des Data Warehouse-Servers und Anmeldeinformationen zur Authentifizierung, und haben Sie Zugriff darauf.

Erforderliche Rolle: Der Systemadministrator [admin] lädt die App herunter und installiert sie. sn_vul.Vulnerability_admin oder sn_vul.admin überwacht die Konfiguration und verifiziert die erwarteten Ergebnisse.

Prozedur

1. Melden Sie sich bei an ServiceNow AI Platform Instanz, die Sie installieren möchten Rapid7 Vulnerability-Integration Anwendung auf.
2. Installieren Sie die PostgreSQL JAR-Datei, die Sie in den zuvor aufgeführten Setup-Aufgaben heruntergeladen haben.

   a. In Ihrem ServiceNow AI Platform Instanz, navigieren Sie zu **Alle** > **MID-Server** > **JAR-Dateien**an.

   b. Klicken Sie auf **Neu**.

   c. Geben Sie den Namen des PostgresSQL-Treibers ein, den Sie zuvor heruntergeladen haben.

      Geben Sie optional ein **Version** , **Quelle** , Und **Beschreibung** Informationen. Verlassen Sie die **Aktiv** Kontrollkästchen ausgewählt.

   d. Hängen Sie die heruntergeladene JAR-Datei mithilfe des Büroklammer-Symbols an Im Header.

   e. Klicken Sie auf **Absenden**.

   Sie haben das Setup für abgeschlossen Rapid7 Data Warehouse-Integration. Wenn Sie die Anforderungen für nicht überprüft haben Rapid7 InsightVM Integration, bevor Sie installieren Rapid7 Vulnerability-Integration,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Siehe Richten Sie für ein Rapid7 InsightVM Integration Und Vorbereitung für Rapid7 Vulnerability-Integration.

Um Schritte zum Abrufen von Berechtigungen zu erhalten, laden Sie herunter, und installieren Sie Rapid7 Vulnerability-Integration, Siehe Rapid7 Vulnerability-Integration installieren.

Richten Sie für ein Rapid7 InsightVM Integration

Die Rapid7 InsightVM Die Integration ist einer der Integrationstypen, die in enthalten sind Rapid7 Vulnerability-Integration Rapid7 Vulnerability-Integration.

Vorbereitungen

Bevor Sie ausführen Rapid7 InsightVM Integration: Führen Sie die folgenden Setup-Aufgaben aus.

Erforderliche Rolle: Der Systemadministrator [admin] lädt die App herunter und installiert sie. sn_vul.Vulnerability_admin oder sn_vul.admin überwacht die Konfiguration und verifiziert die erwarteten Ergebnisse.

Prozedur

1. Für Rapid7 InsightVM Integrationstyp, halten Sie Ihre Region und den API-Schlüssel bereit.
   Kontakt Rapid7 Um die entsprechende Region und den entsprechenden API-Schlüssel zu erhalten.
   Sie haben das Setup für abgeschlossen Rapid7 InsightVM Integration. Wenn Sie die Anforderungen für nicht überprüft haben Rapid7 Data Warehouse-Integration, bevor Sie installieren Rapid7 Vulnerability-Integration, Siehe Richten Sie für ein Rapid7 Data Warehouse-Integration Und Vorbereitung für Rapid7 Vulnerability-Integration.
2. Um Schritte zum Abrufen von Berechtigungen zu erhalten, laden Sie herunter, und installieren Sie Rapid7 Vulnerability-Integration, Siehe Rapid7 Vulnerability-Integration installieren.

Rapid7 Vulnerability-Integration installieren

Nachdem Sie die Einrichtungsschritte für die Integration abgeschlossen haben, damit sie ordnungsgemäß in integriert wird Vulnerability Response, Rufen Sie Berechtigungen ab, laden Sie die Anwendung herunter, und installieren Sie sie auf Ihrem ServiceNow AI Platform® Instanz.

Vorbereitungen

Erforderliche Rollen: administrator für Download und Installation überwacht sn_vuln.admin die Konfiguration und verifiziert die erwarteten Ergebnisse.

1. Siehe Vorbereitung für Rapid7 Vulnerability-Integration, Richten Sie für ein Rapid7 Data Warehouse-Integration Und Richten Sie für ein Rapid7 InsightVM Integration Für weitere Informationen zu den Integrationstypen und Setup-Anforderungen für Rapid7 Vulnerability-Integration.
2. Schließen Sie die folgende Setup-Prüfliste ab, bevor Sie sie herunterladen und installieren. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.
3. Nachdem die Anwendung aktiviert wurde, führen Sie die unten aufgeführten Schritte aus, um zu konfigurieren Rapid7 Vulnerability-Integration.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow AI Platform Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich. Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response. • Der Systemadministrator [admin] installiert die App. Wenn nicht bereits zugewiesen, weist der Administrator die Rolle „Schwachstellenadministrator“ [sn_vul.Vulnerability_admin oder sn_vul.admin] zu. • Der Schwachstellenadministrator überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Die Rapid7 Die administratorrolle wird geerbt, wenn Ihnen in eine Administratorrolle zugewiesen wird Vulnerability Response(VR)-Anwendung.
Validieren Sie die Größenanpassung Ihrer Instanz basierend auf der Anzahl der angreifbaren Elemente, die Sie importieren möchten.	Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.
Richten Sie die Filterung ein	Verwenden Sie Filterung, um die Anzahl der Elemente für den ersten Import zu begrenzen und Ihre Bereitstellung zu

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	phasen, indem Sie Filter in nachfolgenden Importen anpassen.
Deaktivieren Sie Schwachstellenrechner	Wenn Sie keine Schwachstellenrechner verwenden, Deaktivieren Sie den standardmäßigen Schwachstellenrechner, wenn er nicht verwendet wird, Zusätzlich zu allen anderen, die Sie definiert haben. Schwachstellenrechner werden jedes Mal ausgeführt, wenn ein Datensatz für angreifbare Elemente erstellt oder aktualisiert wird, und können sich auf die Leistung des ersten Imports auswirken.
Behalten Sie den Standardwert für den Anwender „Ausführen als“ bei	Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.
Mithilfe von Host-Tags	Wenn Sie Host-Tags in verwenden möchten Vulnerability Response Regeln für Zuweisungs- oder Korrekturaufgaben: Führen Sie die Rapid7 Asset List-Integration aus, bevor Sie Regeln erstellen.
Vorhandene Datensätze deduplizieren	Bei der Migration von **Data Warehouse** Integrationstyp zu **InsightVM** Typ Sie können Ihre vorhandenen Data Warehouse-Datensätze deduplizieren. Weitere Informationen finden Sie unter Deduplizieren Rapid7 Vulnerability-Integration Data Warehouse-Datensätze.

Prozedur

1. Melden Sie sich bei der Instanz an, die Sie installieren möchten Rapid7 Vulnerability-Integration Anwendung auf.
2. Navigieren Sie zu ServiceNow Store Und melden Sie sich an.
3. In ServiceNow Store, Suchen Sie nach Rapid7 Vulnerability-Integration Anwendung.

   Hinweis:
   In ServiceNow Store, Die Anwendung wird aufgerufen, Rapid7 Integration für Security Operations. Diese Anwendung erfordert ein Abonnement.

4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Erwägen Sie, das zu lesen **Andere Anforderungen** Und **Abhängigkeiten** Abschnitte, falls zutreffend.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. In Ihrem ServiceNow AI Platform Instanz, navigieren Sie zu **Systemanwendungen** > **Alle Anwendungen** > **Alle**an.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Im Dialogfeld „Installieren“ wird Ihr Abhängigkeitsstatus angezeigt. Wenn Sie eine Abhängigkeitsanwendung benötigen, wird die gewünschte Anwendung angezeigt. Befolgen Sie die Anweisungen im Dialogfeld, um zu installieren Rapid7 Vulnerability-Integration Anwendung in Ihrer Instanz.

Hinweis:
Der Schwachstellenadministrator kann jetzt die Konfiguration der Anwendung abschließen. Weitere Informationen finden Sie unter Konfigurieren Sie die Eigenschaften Rapid7 Vulnerability-Integration.

Konfigurieren Sie die Eigenschaften Rapid7 Vulnerability-Integration

Konfigurieren Sie Rapid7 Vulnerability-Integration Nachdem die Anwendung auf Ihrem installiert und aktiviert wurde ServiceNow AI Platform®.

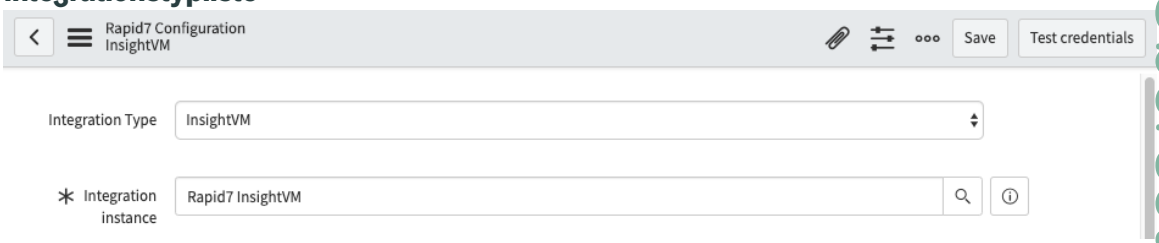
Vorbereitungen

Erforderliche Rolle: Der Administrator [admin] lädt die App herunter und installiert sie. sn_vul.Vulnerability_admin oder sn_vul.admin überwacht die Konfiguration und verifiziert die erwarteten Ergebnisse.

Prozedur

1. Nachdem die Anwendung aktiviert (installiert) wurde, navigieren Sie zu **Rapid7 Vulnerability-Integration** > **Administration** > **Konfiguration**an.
2. Wählen Sie einen Integrationstyp aus der Liste aus.

Integrationstypliste



3. Wählen Sie eine Integrationsinstanz aus.
   Der Standard Rapid7 InsightVM Integrationsinstanz ist standardmäßig ausgewählt. Wenn dies der gewünschte Integrationstyp ist, führen Sie die folgenden Schritte aus. Wenn Sie konfigurieren möchten Rapid7 Data Warehouse-Integrationstyp, fahren Sie mit Schritt 4 fort.

   a. Mit **Integrations-Setup** Registerkarte, die im angezeigten Formular ausgewählt ist, füllen Sie die Felder aus:

Registerkarte „Integrationseinrichtung“ für den Integrationstyp „InsightVM“

Feld	Beschreibung
InsightVM-Region	Die Server-URL, die Sie von erworben haben Rapid7 Website.
API-Schlüssel	Der API-Schlüssel, den Sie von erworben haben Rapid7 Insight-Account.
Validierungsstatus	Schreibgeschützt: Status des Validierungsprozesses für Anmeldeinformationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Überprüfen Sie die erfolgreiche Konfiguration, indem Sie auf klicken **Test-Anmeldeinformationen** . Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, geben Sie Ihre Daten erneut ein.

c. Klicken Sie nach einem erfolgreichen Test auf **Speichern** .

d. Klicken Sie auf **Importkonfiguration** Registerkarte.

Füllen Sie die Felder des angezeigten Formulars aus.

Registerkarte „Konfiguration importieren“ für InsightVM

Feld	Beschreibung
CVSS-Mindestpunktzahl	Minimale CVSS-Punktzahl für angreifbare Elemente, die zum Filtern angreifbarer Elemente während des Imports verwendet wird.
Max. CVSS-Punktzahl	Maximale CVSS-Punktzahl für angreifbare Elemente, die zum Filtern angreifbarer Elemente während des Imports verwendet wird.
Standortfilter	Beschränkt die Daten auf Rapid7 InsightVMSites, die aus der Siteliste ausgewählt wurden. Weitere Informationen finden Sie unter Wird gefiltert nach Rapid7 Sites. Sie können mehr als eine Website auswählen. Die Standardeinstellung (leer) enthält alle Sites. Um die Siteliste vorab auszufüllen, führen Sie die Rapid7 Site Integration – API aus, bevor Sie dieses Feld festlegen. Informationen zur Verwendung der Standortfilterung finden Sie unter Wird gefiltert nach Rapid7 Sites.
CVE-Eintrag automatisch erstellen	Die Systemeigenschaft zum Erstellen eines CVE-Eintrags ist standardmäßig aktiv (wahr). CVE-Platzhalter werden automatisch mit der Rapid7-Wissenserfassung erstellt, wenn die CVE-ID nicht vorhanden ist. Wenn diese Funktion inaktiv sein soll, deaktivieren Sie die Eigenschaft [sn_vul_r7.create_cve_for_Vulnerabilities] in der Liste „Systemeigenschaften“.
Gelöste nach Alter erneut öffnen	Wenn diese Option ausgewählt ist, werden angreifbare Elemente automatisch erneut geöffnet, wenn die Anzahl der Tage, die sie gelöst, aber nicht geschlossen wurden, dem in angezeigten Wert entspricht **Gelöst nach erneut öffnen** Feld.

e. Klicken Sie auf **Speichern**.

Für mehrere Bereitstellungen von Rapid7 InsightVM Integrationstyp:

f. Ein **Integrationsinstanz** Feld Öffnen Sie die Suchliste Und wählen Sie eine vorhandene Integrationsinstanz aus, oder klicken Sie auf **Neu** Im Popup-Menü.

g. Für **Neu** , Geben Sie ein **Name** Klicken Sie für die Integrationsinstanz auf **Übermitteln** . Der Integrationstyp wird in angezeigt Rapid7 Konfigurationsformular.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können jede Integrationsinstanz außer der Standardinstanz löschen. Durch das Löschen einer Instanz wird Folgendes gelöscht (ohne VIS):

- Integrationen
- Instanzparameter
- Integrationsausführungen
- Integrationsprozesse
- Die Instanzspalte im VI ist als leer markiert

h. Überprüfen Sie die erfolgreiche Konfiguration, indem Sie auf klicken **Test-Anmeldeinformationen** .

i. Klicken Sie nach einem erfolgreichen Test auf **Speichern** .

4. Erweitern Sie im Feld Integrationstyp die Liste, und klicken Sie auf **Data Warehouse** .

a. Wählen Sie aus **Integrations-Setup** Registerkarte.

Füllen Sie die Felder des angezeigten Formulars aus.

Registerkarte „Integrationseinrichtung“ für den Typ „Data Warehouse-Integration“

Feld	Beschreibung
JDBC-Anmeldeinformationsname	Name Ihrer Data Warehouse-Anmeldeinformationen.
Anwendername	Rapid7 Data Warehouse-Anwendername.
Passwort	Passwort für Rapid7 Data Warehouse.
Validierungsstatus	Schreibgeschützt: Status des Validierungsprozesses für Anmeldeinformationen.
Validierungsdetail	Schreibgeschützt: Nur Data Warehouse. Zeigt zusätzliche Informationen zur Validierungsprüfung an, nachdem Sie mindestens einmal auf Anmeldeinformationen testen geklickt haben. Dies kann beim Debugging Ihres Setups nützlich sein (z. B. wenn Sie überprüfen, ob Ihr MID-Server falsch konfiguriert ist oder Sie nur die falschen Anmeldeinformationen haben.
DNS/IP des Datenbankservers	DNS- oder IP-Adresse für Ihr Data Warehouse.
Datenbankanschluss	Port, der für Ihre Data Warehouse-Integration verwendet werden soll.
Datenbankname	Name Ihres Data Warehouse.
Offset der Datenverzögerung (in Tagen)	Die Offset-Faktoren der Datenverzögerung in der Verzögerung zwischen den Echtzeitdaten in Rapid7 Nexpose Scanner und die Daten im Data Warehouse.
MID-Server	Zu verwendender MID-Server. Nur eigenständige MID-Server werden unterstützt. Geclusterte MID-Server werden nicht unterstützt.
Timeout für MID-Server (Min.)	Anzahl der Minuten, die gewartet werden soll, bis der MID-Server antwortet, bevor die Integrationsausführung eine Zeitüberschreitung eintritt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Überprüfen Sie die erfolgreiche Konfiguration, indem Sie auf klicken **Test-Anmeldeinformationen** .

c. Klicken Sie nach einem erfolgreichen Test auf **Speichern** .

d. Klicken Sie auf **Importkonfiguration** Registerkarte.

Füllen Sie die Felder des angezeigten Formulars aus.

Registerkarte „Konfiguration importieren“ für Data Warehouse

Feld	Beschreibung
Vor v12.0: Kontrollkästchen „CVE-Eintrag erstellen“	Wenn diese Option aktiviert ist, werden Platzhalter für CVEs, die noch nicht vorhanden sind, als NVD-Datensätze erstellt und im Drittparteieintrag für Rapid7 referenziert. Wenn diese Option deaktiviert ist, werden diese CVEs ignoriert.
CVSS-Mindestpunktzahl	Minimale CVSS-Punktzahl für angreifbare Elemente, die zum Filtern angreifbarer Elemente während des Imports verwendet wird.
Max. CVSS-Punktzahl	Maximale CVSS-Punktzahl für angreifbare Elemente, die zum Filtern angreifbarer Elemente während des Imports verwendet wird.
Standortfilter	Beschränkt die importierten Sites-Integrationsdaten auf die ausgewählten Sites. Sie können mehrere auswählen. **Hinweis:** Da die Standardeinstellung für den Import von Daten aus allen Sites ist, müssen Sie den Filter nicht verwenden, wenn Sie alle Sites wünschen. Dadurch wird die Anforderung verlangsamt.
Gelöste nach Alter erneut öffnen	Wenn diese Option ausgewählt ist, werden angreifbare Elemente automatisch erneut geöffnet, wenn die Anzahl der Tage, die sie gelöst, aber nicht geschlossen wurden, dem in angezeigten Wert entspricht **Gelöst nach erneut öffnen** Feld.

5. Klicken Sie auf **Speichern**.

6. **Wahlweise:** Wenn Sie ein Startdatum in festlegen möchten Rapid7 Schwachstellenintegration – API und Rapid7 Integration von angreifbaren Elementen – API-Integrationsdatensätze zum Abrufen von Verlaufsdaten während des ersten Imports aus dem Rapid7 Scannen Sie, führen Sie die folgenden Schritte aus.
Sie können diese Daten verwenden, um Ihnen bei zu helfen Veraltete Erkennungen in werden geschlossen Vulnerability Response.

a. Navigieren zu **Rapid7 Vulnerability-Integration** > **Administration** > **Integrationen**an.
Die Rapid7 Die Integrationsliste wird angezeigt.

b. Klicken Sie auf einen der Integrationsdatensätze, um ihn zu öffnen.

(Optional) Klicken Sie am oberen Rand des Formulars auf **Hier** Link zum Bearbeiten des Datensatzes.

Die **Importieren seit** Datumsfeld in Rapid7 Integrationen sind standardmäßig leer, mit Ausnahme von Rapid7 Schwachstellenintegration: API und Rapid7-Integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für angreifbare Elemente – API. Für diese Integrationen werden diese Felder auf 1998-12-31 oder 1999-01-01-01 festgelegt.

Dient zum Abrufen von Verlaufsdaten während des ersten Imports aus der Rapid7 Scannen und legen Sie ein Startdatum in den entsprechenden Integrationsdatensätzen fest. Dieser Prozess funktioniert für jeden Rapid7 Integration mit den folgenden Ausnahmen:

- Die Rapid7 Exploit- und Malware-Kit-Integrationen zeigen nicht an **Importieren seit** Feld, da sie keine Delta-Updates durchführen und daher dieses Feld nicht verwenden.
- Die Rapid7 Bei der Integration der Asset-Liste wird das Feld ignoriert, da die Absicht darin besteht, alle Daten abzurufen.
- Für die erste Ausführung von Rapid7 InsightVM Umfassende Integration angreifbarer Elemente: API, wenn das Modul „veraltete angreifbare Elemente automatisch schließen“ aktiviert ist und **Importieren seit** Feld ist leer.

  Wenn Sie die Funktion zum automatischen Schließen aktivieren, ist eine erfolgreiche Ausführung über die Rapid7 Comprehensive Angreifbare Element Integration oder die Rapid7 Comprehensive Angreifbare Element Integration – API erforderlich. Diese Integrationen sind standardmäßig deaktiviert.

  Wenn Sie aktivieren Rapid7 InsightVM Umfassende Integration angreifbarer Elemente: API, wenn Sie verlassen **Importieren seit** Feld leer auf der Integrationskonfigurationsseite, der Wert in **Tage her** Das Feld des Formulars „veraltete angreifbare Elemente automatisch schließen“ wird auch für verwendet **Importieren seit** Datum der ersten Integrationsausführung. Der Standardwert für das automatische Schließen veralteter angreifbarer Elemente ist (90 Tage).

  Beispiel: Wenn **Tage her** Das Feld im Formular „veraltete angreifbare Elemente automatisch schließen“ ist 90 und **Importieren seit** Feld auf der Konfigurationsseite „Rapid7 umfassende Integration angreifbarer Elemente – API“ ist leer. Die erste Integrationsausführung importiert die Daten der letzten 90 Tage.

  Diese Beziehung zwischen **Importieren seit** Und **Tage her** Felder gelten nur für die erste Integrationsausführung. Ändern Sie danach **Tage her** Das Feld im Formular „veraltete angreifbare Elemente automatisch schließen“ wirkt sich nicht auf aus **Importieren seit** Feld auf der Konfigurationsseite „Rapid7 umfassende Integration angreifbarer Elemente – API“. Das Feld wird in die Startzeit der ersten Ausführung geändert, sodass bei der nachfolgenden Integration nur die Delta-Informationen importiert werden

  Die **Importieren seit** Das Feld kann bearbeitet werden, und Sie können für jede der Integrationen beliebige Werte eingeben.

7. Navigieren zu **Alle** > **sn_sec_int_impl.list** > **Rapid7 InsightVM**an.

a. Die **Import_startime_buffer_Comprehensive** Der Integrationsinstanzparameter legt eine Pufferzeit von 24 Stunden vor der in angegebenen Zeit fest **Importieren seit** Feld, damit die Assets, die ab dieser Pufferzeit gescannt werden, während abgerufen werden **Rapid7 – umfassende Integration angreifbarer Elemente – API** Integrationsausführung.
Sie können diese Pufferzeit entsprechend Ihren Anforderungen ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Wahlweise: Legen Sie fest **CLOSE_Stale_Detections** Parameter bis *Wahr* Zum Schließen der veralteten Erkennungen, die nicht mehr über die Rapid7-API für die Assets gesendet werden, die über die Rapid7-API gescannt und abgerufen werden **Rapid7 – umfassende Integration angreifbarer Elemente – API** .

Sie haben die Einrichtungs-, Installations- und Konfigurationsschritte für erfolgreich abgeschlossen Rapid7 Vulnerability-Integration. Sie sind jetzt bereit, importierte Daten zu überprüfen und zu verifizieren.

Nächste Maßnahme

Die Rapid7 Und Qualys Scanner sind standardmäßig in deaktiviert Vulnerability Response Anwendung. Wenn Sie versuchen, einen erneuten Scan von den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, wird der **Erneut Scannen** Schaltfläche ist nicht verfügbar.

So aktivieren Sie diese Scanner als Anwender mit der Rolle sn_vul.Vulnerability_admin:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**an.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um es zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle in Datensätzen für angreifbare Elemente und Korrekturaufgaben angezeigt **Erneut Scannen** Ist als UI-Aktion verfügbar.

Wenn Ihre Umgebung domänengetrennte Importe erfordert, finden Sie weitere Informationen unter Erstellen Sie domänengetrennte Importe für eine Integration.

Informationen zum Erstellen oder Verfeinern Ihrer Suchregeln vor dem Import finden Sie unter Erstellen Sie eine Vulnerability Response-CI-Suchregel.

Wird gefiltert nach Rapid7 Sites

Nach Website filtern für Rapid7 InsightVM Integrationstypen sowie Rapid7 Nexpose Data Warehouse-Integrationstypen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Hinweis:
Die Verwendung der Standortfilterung kann sich auf die Leistung auswirken. Informationen zur Leistung und andere Überlegungen vor der Verwendung der Standortfilterung finden Sie unter KB0789221 .

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

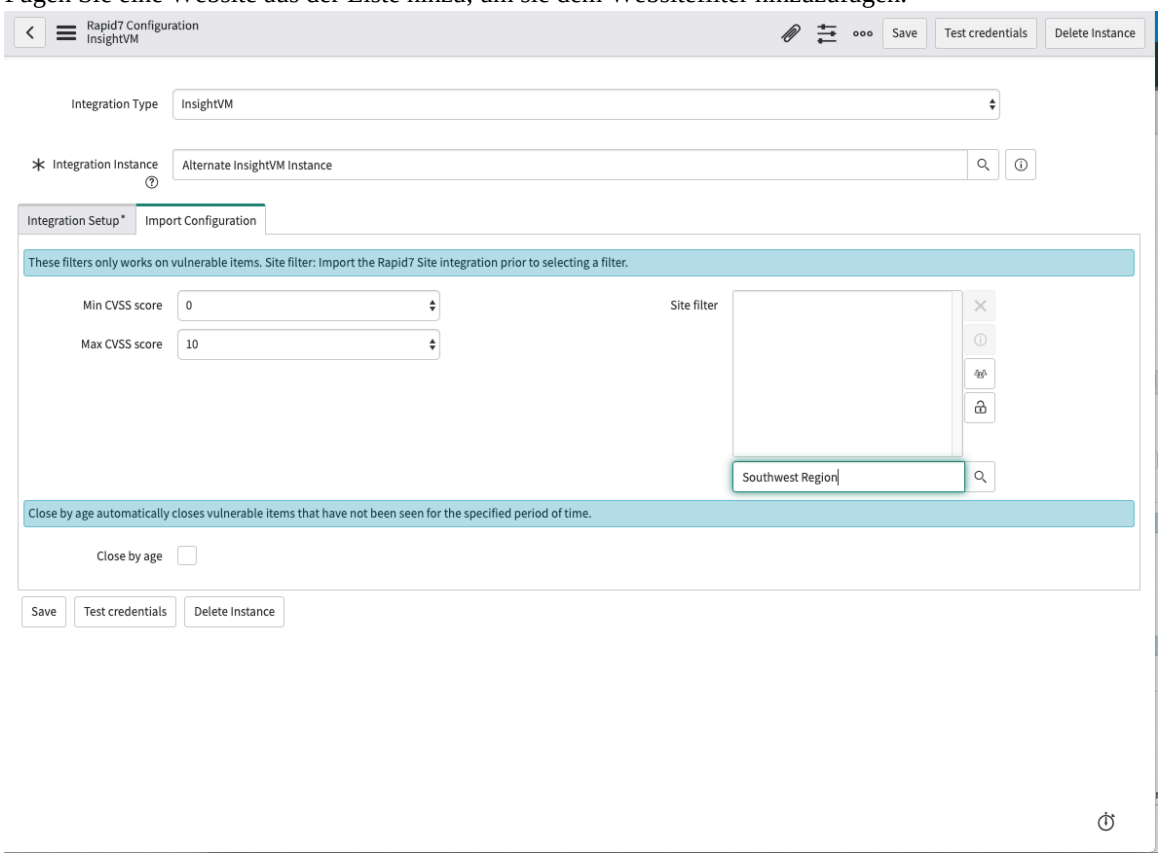
1. Navigieren zu **Alle** > **Rapid7 Vulnerability-Integration** > **Konfiguration**an.
2. Wählen Sie eine Integrationsinstanz aus.
3. Klicken Sie auf **Importkonfiguration** Registerkarte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie alle Sites wünschen, lassen Sie das Feld Standortfilter leer. Kein Standortfilter entspricht dem Hinzufügen aller Sites.

Sites sind für Integrationsinstanzen spezifisch. Die Suchliste für die Standortfilterung zeigt beide an Rapid7 InsightVM Und Rapid7 Nexpose Data Warehouse-Integrationsinstanzstandorte. Stellen Sie sicher, dass die von Ihnen ausgewählte Website mit der von Ihnen ausgewählten Integrationsinstanz übereinstimmt. Wenn Sie beispielsweise versehentlich einen Data Warehouse-Standort auswählen, funktioniert dieser Standort nicht für die Standortfilterung nach Rapid7 InsightVM.

4. Klicken Sie auf die Suchliste, um die Site-Datensätze für die aktuelle Integrationsinstanz anzuzeigen.
5. Fügen Sie eine Website aus der Liste hinzu, um sie dem Websitefilter hinzuzufügen.



6. Wiederholen Sie die Auswahl, um zusätzliche Sites hinzuzufügen.
7. Klicken Sie auf **Speichern**.
Diese Sites werden verwendet, um beim nächsten Import nach Site zu filtern. Siehe Stellen Sie Ihre Rapid7 InsightVM-Site-Tags vor Informationen zum Hinzufügen der PRÄFIXWEBSITE zu Ihren Site-Daten.

Stellen Sie Ihre Rapid7 InsightVM-Site-Tags vor

Fügen Sie das Präfix SITE zu hinzu Rapid7 InsightVM Site-Tags, um sie in Ihrer Liste von Tags hervorzuheben.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Hinweis:
Wechseln Sie bei Bedarf Ihren Bereich zur Rapid7-Integration für Security Operations.

Prozedur

1. Geben Sie im linken Navigationsfeld Folgendes ein: *sys_properties.list*.
2. Unter **Name** , Suche nach: *sn_vul_r7.prefix_site_to_rapid7_tags*.
3. Öffnen Sie *sn_vul_r7.prefix_site_to_rapid7_tags*.
4. Ändern **Wert** Bis **Wahr** .
5. Klicken Sie auf **Aktualisieren**.
   Neue und vorhandene Site-Tags werden beim nächsten Import von vorangestellt Rapid7 InsightVM.

Rapid7 Vulnerability-Integration Führen Sie das Statusdiagramm aus

Rapid7 Nexpose Sensoren erfassen die Daten und senden sie automatisch an die Rapid7 Nexpose Oder Rapid7 InsightVM Produkte, die die Informationen kontinuierlich analysieren und korrelieren.

Datenvisualisierungen in Vulnerability Response Arbeitsbereiche

Die Vulnerability Response Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie Ihren Korrekturfortschritt überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen, die aktualisiert werden, wenn sich Schwachstellendaten ändern. Siehe Vulnerability Response Arbeitsbereiche, Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen erkunden Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen.

Rapid7 Vulnerability-Integration Funktioniert einfach mit Vulnerability Response Dient zum Zuordnen von Schwachstellen zu CIs und Business-Services, um die Auswirkungen und Priorität potenziell böswilliger Bedrohungen zu bestimmen. Die Rapid7 Vulnerability-Integration Das Modul „Ausführungsstatus“ ist eine grafische Ansicht des Status von Rapid7 Vulnerability-Integration Wird ausgeführt.

Um diese Daten in der Legacy-Ansicht anzuzeigen, navigieren Sie zu **Alle** > **Integration Aller Rapid7-Schwachstellen** > **Status der Integrationsausführung**an.

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard ist in der neuen Experience-UI verfügbar.

Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Vorherige Versionen von Vulnerability Response

Zeigen Sie im Diagramm auf ein beliebiges Teil (Balken, Kreis, Datenpunkt usw.), um allgemeine Daten anzuzeigen, die für dieses Teil spezifisch sind. Wenn Sie auf einen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

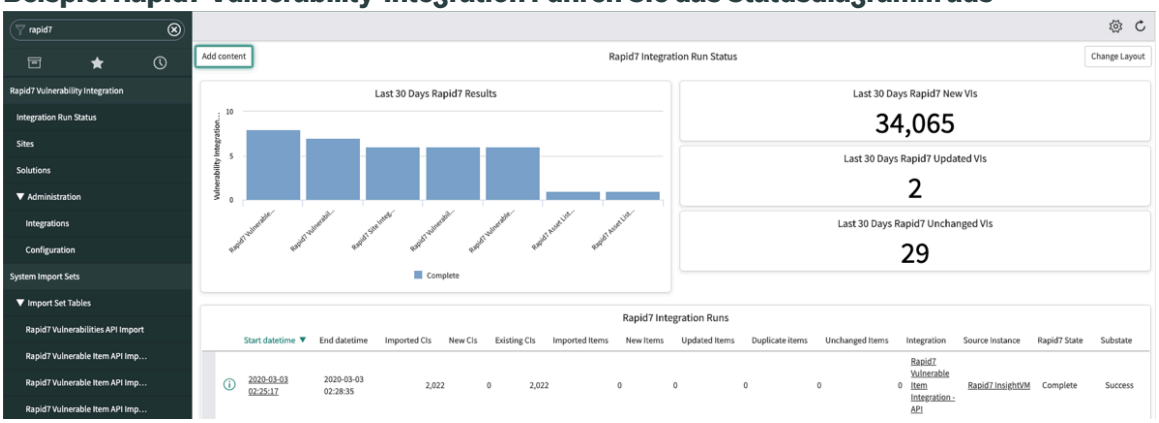
Mehrere Faktoren können sich auf die Leistung der Integrationsausführung auswirken, z. B. die Datenmenge und die Zeit, die für die Verarbeitung dieser Daten benötigt wird. Zwei neue Diagramme wurden hinzugefügt, um die Leistungsmetriken zu vergleichen:

- Rapid7 Leistungsmetriken der Erfassung angreifbarer Elemente: Tägliche Leistungsmetriken für Zuweisungsregeln, Gruppenregeln, Risikoregeln, Warteschlangenwartezeit, Warteschlangenverarbeitungszeit, und andere Statistiken für angreifbare Elemente in den letzten 30 Tagen, um die Ursache für Leistungsabweichungen zu identifizieren.
- Rapid7 Leistungsdurchsatz der Erfassung angreifbarer Elemente: Vergleichen Sie den täglichen Erfassungsdurchsatz angreifbarer Elemente für Rapid7 Integration angreifbarer Elemente: API. Der Durchsatz wird in Elementen pro Stunde gemessen.

Hinweis:
In Rapid7, Diese Diagramme werden nur für die Insight VM-Integration unterstützt.

Status der Rapid7-Integrationsausführung

Beispiel Rapid7 Vulnerability-Integration Führen Sie das Statusdiagramm aus



- Der Wert in der Spalte importierte Elemente stellt die Gesamtzahl der angreifbaren Elemente dar, die aus einer Integrationsausführung erstellt werden.
- In der Spalte neue Elemente wird die Anzahl der angreifbaren Elemente angezeigt, die aus einer Integrationsausführung erstellt werden.
- Die Spalte „doppelte Elemente“ ist nicht mehr ausgefüllt. Möglicherweise möchten Sie diese Spalte aus der Anzeige entfernen.
- In der Spalte „aktualisierte Elemente“ wird angezeigt, wie oft angreifbare Elemente während einer Integrationsausführung aktualisiert werden. Dieser Wert ist nicht die Anzahl der eindeutigen angreifbaren Elemente, die aktualisiert werden. Wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

beispielsweise ein angreifbares Element während der Integrationsausführung zweimal aktualisiert wird, wird es zweimal gezählt und als angezeigt 2 Aktualisierte Elemente.

- In der Spalte „unveränderte Elemente“ werden angreifbare Elemente angezeigt, die während der Integrationsausführung gefunden wurden und bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da keiner der relevanten Feldwerte geändert wurde.

Hinweis:
Integrationsausführungen mit null Ergebnissen für alle vier der folgenden Werte: **Neue CIs** , **Vorhandene CIs** , **Neue Elemente** , Und **Aktualisierte Elemente** Werden aus gefiltert **Rapid7-Integrationsausführungen** Liste.

Rapid7 Vulnerability-Integration Führen Sie Statusdiagrammberichte aus

Name	Beschreibung
Letzte 30 Tage Rapid7 Ergebnisse	Die Anzahl der für jede Integration abgeschlossenen Integrationsausführungen. Zeigt sowohl erfolgreiche als auch fehlgeschlagene Ausführungen an. In einer Balkenvisualisierung ausführen.
Letzte 30 Tage Rapid7 Neue VIS	Die Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Letzte 30 Tage Rapid7 Aktualisierte VIS	Die Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Letzte 30 Tage Rapid7 Duplikate	Die Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Rapid7 Integrationsausführungen	Die Datensätze der Integrationsausführung in einer Liste. **Hinweis:** **V16.1:** Um die Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit ServiceNow Erkennungsdaten in `sn_vul_detection`Tabelle. Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennung oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „bis datumsanzahl“ in der Instanz nach Abschluss der Integrationsausführung an.
Letzte 30 Tage Rapid7 Leistungsmetriken Der Erfassung Angreifbarer Elemente	Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich zu den letzten 30 Tagen.
Letzte 30 Tage Rapid7 Leistungsdurchsatz Der Erfassung Angreifbarer Elemente	Täglicher Durchsatz der Erfassung angreifbarer Elemente für Rapid7 Integration angreifbarer Elemente: API, die in den letzten 30 Tagen gemessen wurde.

Zeigen Sie an Rapid7 Vulnerability-Integration Status-Dashboard für Importausführungen

Verwenden Sie Rapid7 Dashboard „Schwachstellenimport – Ausführungsstatus“, um den Erfolg Ihrer Integrationsausführungen zu verifizieren, Probleme zu lokalisieren und Ihre Korrekturentscheidungen zu unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rollen: sn_vuln.admin

Warum und wann dieser Vorgang ausgeführt wird
Bei diesem Verfahren werden die folgenden Annahmen getroffen.

- Sie haben Vulnerability Response Und Rapid7 Vulnerability-Integration Installiert und konfiguriert.
- Rapid7 Vulnerability-Integration Importe sind geplant und werden ausgeführt.
- Rapid7 Statusdiagramme der Integrationsausführung werden verwendet.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 19,0 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur
1. Navigieren zu **Rapid7** > **Status der Integrationsausführung**an.

   Ab Version 19,0 von Vulnerability Response, Dieses Dashboard ist in der neuen Experience-UI verfügbar.

   Hinweis:
   Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

2. Wenn Sie nicht verwenden Rapid7 Statusdiagramm der Integrationsausführung, navigieren Sie zu **Rapid7** > **Integrationen**an.
   a. Wählen Sie eine Integration aus.
   b. Klicken Sie auf **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste.
3. Überprüfen Sie, ob alle Importe erfolgreich waren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trouble?

Die häufigsten Ursachen für eine fehlgeschlagene Ausführung:

- Netzwerkunterbrechung
- Bitverfall bei der Datenübertragung, was zu beschädigten Daten während der Transformation führt

Klicken Sie für alle diese Bedingungen auf **Jetzt ausführen** Und führen Sie die Integration erneut aus.

Deduplizieren Rapid7 Vulnerability-Integration Data Warehouse-Datensätze

Bei der Migration zu **InsightVM** Integrationstyp aus dem **Data Warehouse** Integrationstyp: Sie können vorhandene angreifbare Data Warehouse-Elemente deduplizieren, solange sie zu denselben Quelldaten gehören wie Ihr Rapid7 InsightVM Daten.

Vorbereitungen

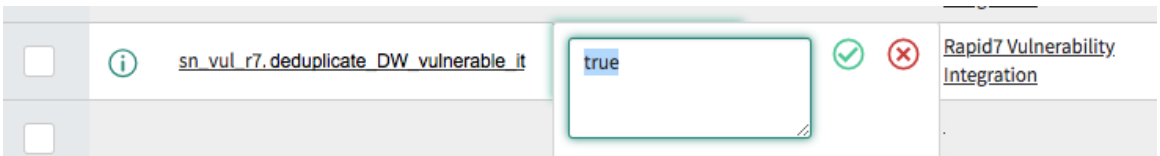
Erforderliche Rolle: sn_vul_r7.admin oder, sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Diese Deduplizierung funktioniert nur bei der Migration von Rapid7 Nexpose Data Warehouse zu Rapid7 InsightVM Integration angreifbarer Elemente.

Prozedur

1. Navigieren zu **Alle** > **Schnell 7** > **Integrationen**an.
2. Alle festlegen Rapid7 Nexpose Data Warehouse-Integrationen **Aktiv** Spalteneinstellungen bis **Falsch** , Deaktivierung der Integrationen.
3. Geben Sie Ein sys_properties.list Im linken Navigationsbereich.
4. Suchen Sie nach **Name** : sn_vul_r7.deduplicate_DW_vulnerable_item .
5. Ändern Sie **Wert** Feld bis **Wahr** .



6. Klicken Sie auf das grüne Häkchensymbol .
   Während des nächsten Rapid7 InsightVM Import der Integration angreifbarer Elemente, jede Übereinstimmung mit vorhandenen Data Warehouse-Datensätzen verhindert, dass ein doppeltes angreifbares Element erstellt wird.

Initiieren Sie einen erneuten Scan für Rapid7 Schwachstellenintegration

Initiieren Sie erneutes Scannen in Rapid7 Plattform, um sicherzustellen, dass Ihre angreifbaren Elemente zwischen den geplanten Scanzyklen behoben wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Hinweis:
Scannt erneut für Rapid7 Angreifbare Data Warehouse-Elemente werden nicht unterstützt.

Sie können erneutes Scannen über die Vulnerability Response-Arbeitsbereiche initiieren. Weitere Informationen finden Sie unter Scannen Sie Datensätze und Korrekturaufgaben in erneut Arbeitsbereich des Schwachstellenmanagers und Scannen Sie angreifbare Elemente und Korrekturaufgaben in erneut Arbeitsbereich für IT-Korrekturen.

Erforderliche Rollen: Erforderliche Rollen: sn_vul.write_all oder sn_vul.write_assigned

Warum und wann dieser Vorgang ausgeführt wird

Informationen zu erneuten Scans in der klassischen Umgebung finden Sie in den folgenden Abschnitten.

Erneutes Scannen wird unterstützt. Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente initiieren, die aus importiert wurden Rapid7 InsightVM Integrationen von Ihrem ServiceNow AI Platform® Instanz.

Hinweis:
Die Rapid7 Scanner ist standardmäßig in deaktiviert Vulnerability Response Anwendung. Wenn Sie versuchen, einen erneuten Scan über die angreifbaren Elemente oder Korrekturaufgaben durchzuführen, die haben Rapid7 Anwendung als Quelle ist die Schaltfläche „erneut scannen“ nicht verfügbar.

Um den Overhead und das Volumen für geplante, vollständige Scans, Korrekturbesitzer, IT-Spezialisten, Schwachstellenanalysten zu reduzieren, oder Schwachstellenmanager können bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen in Assets (Konfigurationselementen) in ihren Umgebungen initiieren. Sie können erneutes Scans aus angreifbaren Elementen (VI), Korrekturaufgaben (RT), Drittparteieinträgen (TPE) oder erkannten Elementdatensätzen aus Ihrem initiieren ServiceNow AI Platform® Instanz.

Durch erneutes Scannen können Sie verifizieren, ob Ihre Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben haben.

Beispielsweise wird Ihre gesamte Umgebung alle drei Wochen einmal gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, aber Sie haben gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Ihrem aus initiieren ServiceNow AI Platform Für Rapid7 Angreifbare Elemente. Sie können aktualisierte Ergebnisse für Ihre angreifbaren Elemente beim nächsten geplanten Import von anzeigen Rapid7 InsightVM Integrationen von Schwachstellen und angreifbaren Elementen.

Prozedur

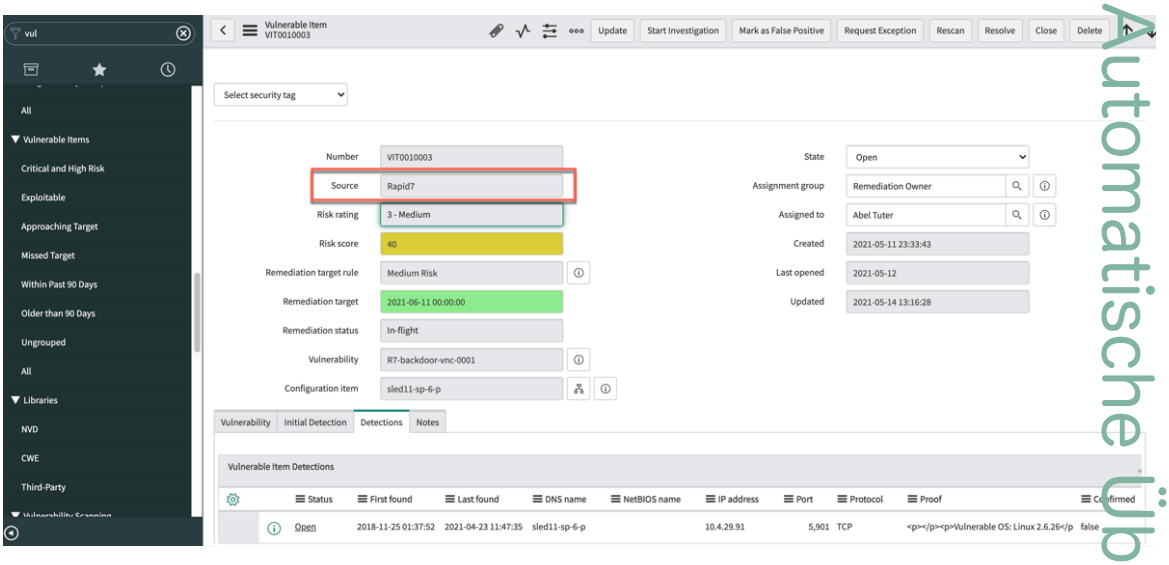
1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**an.
2. Suchen Sie den Datensatz des angreifbaren Elements, aus dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Initiieren Sie erneutes Scannen für VIS mit Rapid7 Als Quelle. Verifizieren Rapid7 Wird in angezeigt **Quelle** Spalte in den VI-Listenansichten oder in **Quelle** Felder in einzelnen Datensätzen. Sie können den Bedingungsgenerator verwenden, um VIS nach Quelle zu gruppieren. Oder, wenn **Quelle** Spalte wird in der VI-Listenansicht nicht angezeigt. Klicken Sie oben links in der Liste auf das Zahnradsymbol, und verschieben Sie es **Quelle** Von **Verfügbar** Bis **Ausgewählt** .

Wenn Sie erneute Scans initiieren, vermeiden Sie, gleichzeitig Scans für eine Quell-ID aus mehreren Quellen auszulösen. Die neueste Scan-Anforderung tritt ein Fehler auf.

Wenn Sie beispielsweise einen erneuten Scan für ein VI aus einem VI-Datensatz initiieren und auch einen weiteren erneuten Scan aus einem Korrekturaufgabendatensatz anfordern, der dasselbe VI enthält, ist es wahrscheinlich, dass die zweite Anforderung fehlschlägt.



3. Alternativ navigieren Sie zu **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** Für die Korrekturaufgaben- bzw. Drittpartei-Eintragsdatensätze, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl, die **Erneut Scannen** Die Schaltfläche ist für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss das VI aus dem stammen Rapid7 Produkt und in einem anderen Status als „Geschlossen“. Für mehrere VI-Datensätze müssen alle VIS, die Sie in der Listenansicht auswählen, aus dem stammen Rapid7 Produkt und in einem anderen Status als „Geschlossen“.
   - In einem Korrekturaufgabendatensatz kann sich die Korrekturaufgabe in einem anderen Status als „Geschlossen“ befinden, und alle zugehörigen VIS müssen aus dem stammen Rapid7 Produkt.
   - In einem Drittpartei-Eintrag-Datensatz (TPE) muss der Datensatz mindestens einen zugehörigen VI-Datensatz aus dem aufweisen Rapid7 Produkt in einem anderen Status als „Geschlossen“.
   - In einem erkannten Elementdatensatz muss das VI aus dem stammen Rapid7 Produkt und in einem anderen Status als **Geschlossen** .

4. Klicken Sie oben rechts im Datensatz auf **Erneut Scannen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

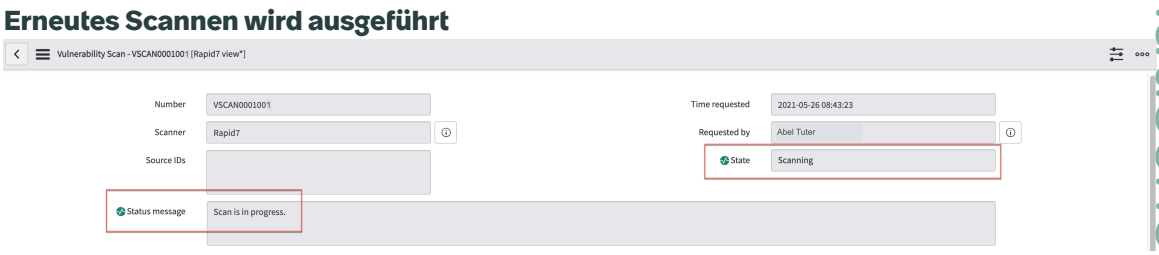
Wählen Sie für Listenansichten die VIS aus der Liste aus, die Sie erneut scannen möchten, und aus **Aktion für ausgewählte Zeilen** Liste, wählen Sie aus **Erneut Scannen** .

5. Bestätigen Sie im angezeigten Popup-Fenster den erneuten Scan.
   Eine Meldung wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird (**In Warteschlange**). Klicken Sie in der Nachricht auf **Zeigen Sie Details an** Link zum Überprüfen des Status des erneuten Scans (untergeordneter Scan) und zum Anzeigen anderer aus dem Datensatz gestarteter erneuter Scans. Der Status für alle erneuten Scans kann jederzeit unter der zugehörigen Liste Scans am unteren Rand des VI, der Korrekturaufgabe, des TPE und der erkannten Elementdatensätze gefunden werden, die Sie zum Starten der erneuten Scans verwenden.

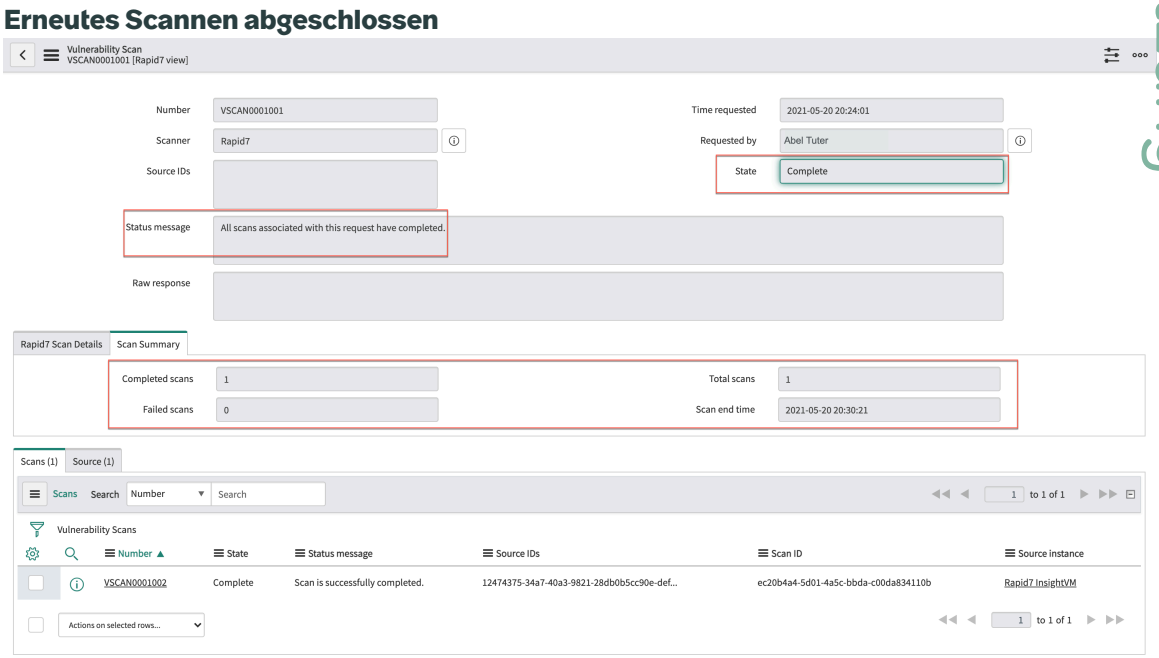
   Wenn der Scan ausgeführt wird, ändert sich das Feld Status in **Wird Gescannt** , Und das Feld Statusnachricht wird angezeigt **Scan wird ausgeführt** .

   Hinweis:
   Jeder erneute Scan unterstützt 500 Assets pro Scan. Wenn Ihre Anforderung mehr als 500 Assets enthält, werden weitere untergeordnete Scans angefordert.

   Ihr ServiceNow AI Platform® Die Instanz verfolgt den Status des erneuten Scans, bis er erfolgreich abgeschlossen ist, oder bis der festgelegte Nachverfolgungszeitraum abgelaufen ist, je nachdem, was zuerst geschieht.



   Durch die Zeitüberschreitung wird der Scan nicht beendet. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, an dem der ServiceNow AI Platform® Die Nachverfolgung des Status des erneuten Scans wurde beendet, nicht wenn der tatsächliche erneute Scan beendet wurde. Alle VIS, die in „Geschlossen/behoben“ übergegangen sind oder übergehen werden, werden mit dem nächsten geplanten Import von importiert Rapid7 Integrationen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

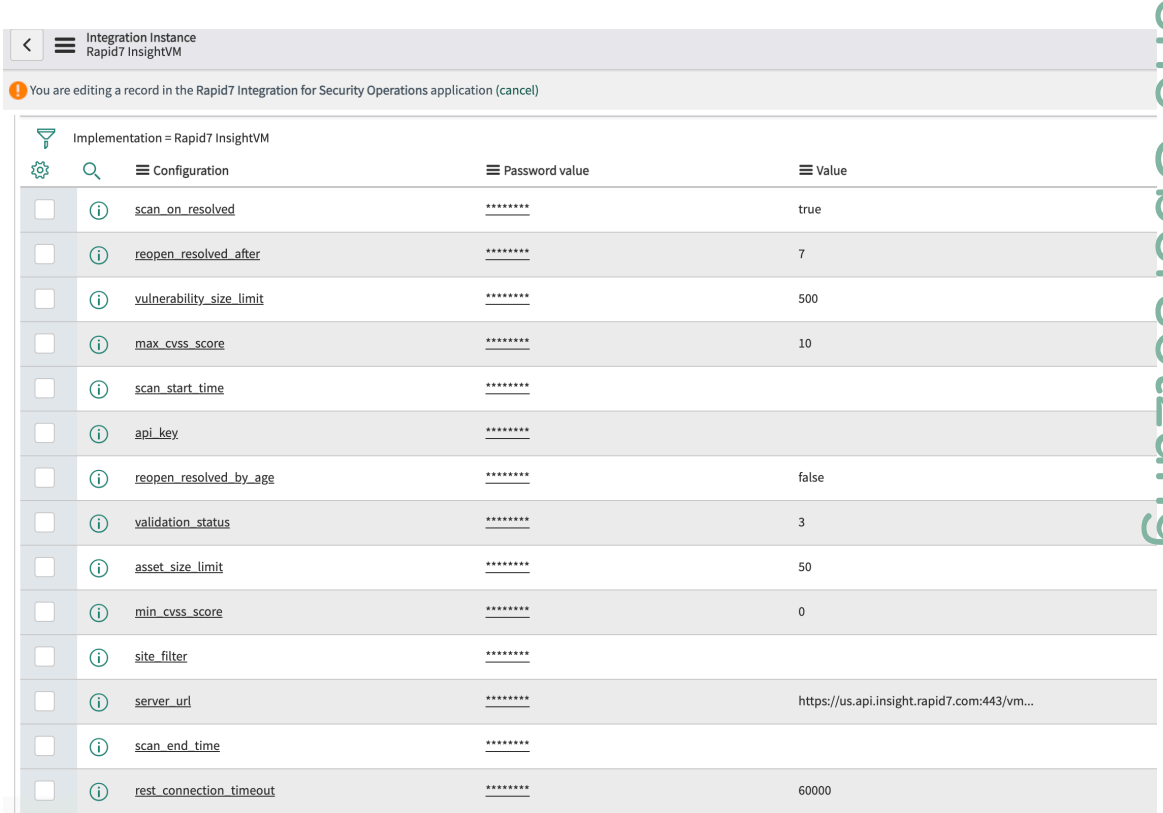
Alternativ können Sie bei Bedarf einen erneuten Scan für eine bestimmte Schwachstelle in einem bestimmten Asset initiieren. Sie können die Ergebnisse dieser Scans anzeigen, sobald der Scan für die aktualisierten VI-, Korrekturaufgabe-, TPE- und erkannten Elementdatensätze abgeschlossen ist, aus denen Sie den Scan gestartet haben.

Der Wert des Felds Status in Schwachstellen-Scan-Datensätzen wird aus importiert Rapid7. Wenn der Scan erfolgreich abgeschlossen ist, wird der Status auf „Abgeschlossen“ festgelegt. Wenn der Scan nicht erfolgreich abgeschlossen wird, wird ein Fehlerwert angezeigt.

Automatische Scans und geplante Scans

Als Schwachstellenmanager oder Analyst können Sie angeben und planen, wann erneutes Scannen für VIS und RTS initiiert werden. Sie können auch automatische Scans für VIS und Korrekturaufgaben aktivieren, die auf „Lösen“ festgelegt sind.

6. Um die Integrationsparameter in der Integrationsinstanz zu ändern, navigieren Sie zu **Rapid7 Vulnerability-Integration** > **Administration** > **Konfiguration**an.
7. Im Rapid7-Konfigurationsdatensatz, wenn nicht ausgewählt, aus **Integrationstyp** Liste, wählen Sie aus **Rapid7 InsightVM** .
8. Rechts von **Integrationsinstanz** Klicken Sie auf das Informationssymbol, gefolgt von **Öffnen Sie Den Datensatz** .
9. Suchen Sie im Rapid7 InsightVM-Datensatz der Integrationsinstanz nach den Parametern für die Planung von Scans, und bearbeiten Sie sie nach Bedarf.



scan_on_resolved Gibt an, ob der Scan initiiert wird, wenn eine Schwachstelle gelöst wird. Der Standardwert ist **Falsch** (Deaktiviert).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn dieser Parameter auf festgelegt ist Wahr Wenn ein VI oder RT auf „gelöst“ festgelegt wird, wird automatisch der Workflow zum erneuten Scannen des jeweiligen VI und der Korrekturaufgabe ausgelöst.

Scan_Start_time

Legen Sie die Startzeit des Scans in fest **HH:mm** (24-Stunden-Format) in der UTC-Zeitzone für die Startzeit des Fensters, für das erneute Scans verfügbar sein sollen.

Der Standardwert ist 00:00 .

Scan_end_time

Legen Sie die Endzeit des Scans in fest **HH:mm** (24-Stunden-Format) in der UTC-Zeitzone für die Endzeit des verfügbaren Scanfensters.

Der Standardwert ist 23:59 .

Wenn ein Scan innerhalb des geplanten Zeitfensters initiiert wird, wird er sofort gestartet. Wenn der Scan außerhalb des Fensters initiiert wird, wird er für das nächste geplante Fenster in die Warteschlange gestellt.

Beispiel: Wenn Sie eine Startzeit von eingeben 00:00 Für *scan_start_time*Parameter, und ein *scan_end_time*Von 10:00 UHR am selben Morgen werden Scans, die außerhalb des Zeitfensters von Mitternacht bis 10:00 UHR geplant oder manuell gestartet werden, in die Warteschlange gestellt und zur Startzeit des Zeitfensters des folgenden Tages gestartet 00:00 .

Wenn Sie im selben Beispiel um 11:00 UHR manuell einen erneuten Scan initiieren, wird der erneute Scan nicht sofort gestartet, da er außerhalb der verfügbaren konfigurierten Scan-Zeiten liegt. Die Scan-Anforderung bleibt bis zum Beginn des Zeitfensters des folgenden Tages in der Warteschlange, in diesem Beispiel 00:00 .

Legen Sie zusätzliche Filterparameter für fest Rapid7 InsightVM Importe

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit an Rapid7 Integration for Security Operations Damit Sie die mit importierten Schwachstellendaten weiter verfeinern können Rapid7 InsightVM Produkt.

Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie Daten aus Ihren Abfragen filtern, damit Sie nur bestimmte Schwachstellendetails überprüfen können. Beispielsweise möchten Sie nur importierte Schwachstellen anzeigen, die sind Kritisch Und Schwerwiegend .

Um Ihnen beim Sammeln dieser Daten zu helfen, fügen Sie hinzu Rapid7 Parameter, die Ihnen beim Importieren der spezifischen Schwachstellendetails helfen, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder -Codierung können Sie ab v13.4 Ihre HTTP-Anforderungsinformationen mit anpassen Rapid7 InsightVM Parameter in Ihrem ServiceNow AI Platform. Folgendes Rapid7 InsightVM Integrationen unterstützen das Filtern durch Hinzufügen von JSON-Inhalten im Anforderungstext:

- Rapid7 InsightVM Integrations-API für angreifbare Elemente
- Rapid7 InsightVM Schwachstellenintegrations-API
- Rapid7 InsightVM

Sie sollten wissen, wie Sie verwenden JSON Zeichenfolgen für diese Funktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_vul.Vulnerability_admin

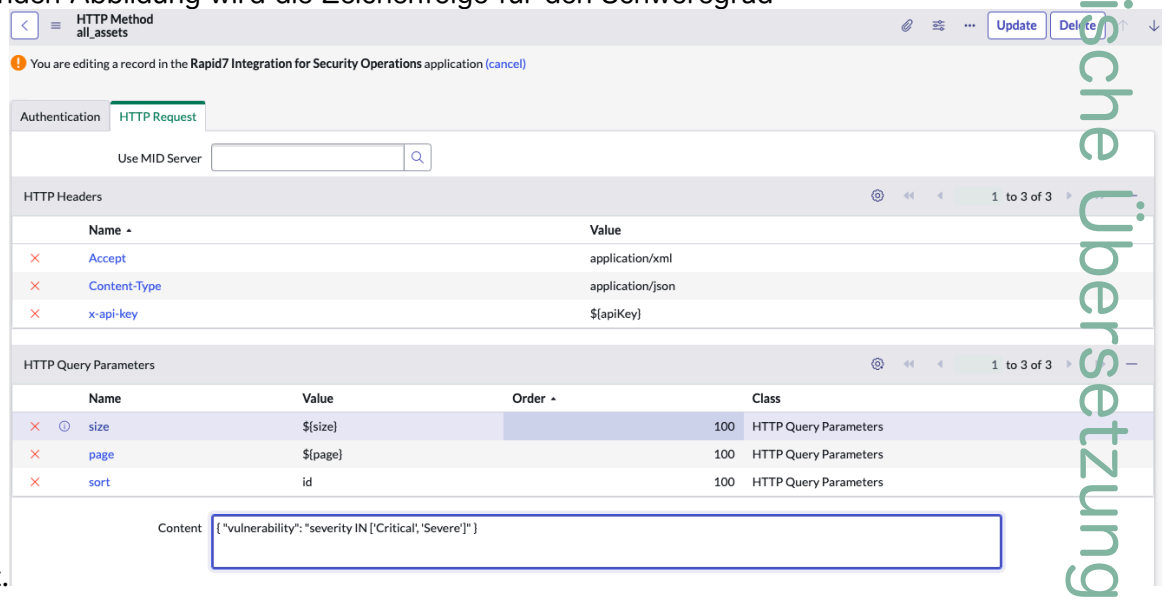
Prozedur

1. Suchen Sie die von unterstützten Parameter Rapid7 InsightVM Produkt auf der Rapid7 Entwickler-Site, die Sie für Ihre Filterung verwenden möchten.

   Sie können die Parameter für den Anforderungstext erstellen, indem Sie auf verweisen Rapid7 Dokumentation. Parameter und Werte, die Sie aus eingeben Rapid7 InsightVM Produkte werden nur auf Integrationsinstanzebene unterstützt.

2. Navigieren zu **Alle** > **Rapid7 Vulnerability-Integration** > **Administration** > **Integrationen**an.
3. Klicken Sie auf der Listenseite „Rapid7-Integrationen“ auf den Datensatz für Rapid7 InsightVM Integration, die Sie öffnen möchten.
4. Klicken Sie rechts auf der Seite auf das Informationssymbol (I) für die REST-Nachricht gefolgt von **Öffnen Sie Den Datensatz** .
5. Wenn die Registerkarte HTTP-Anforderung ausgewählt ist, klicken Sie unter HTTP-Methoden in der Spalte Name auf ein Element, um seine HTTP-Abfrageparameter zu öffnen.
6. Geben Sie unter HTTP-Methodendatensatz unter HTTP-Abfrageparameter im Feld Inhalt die Parameterwerte ein, die Sie im gefunden haben Rapid7 Entwickler-Site.

   In der folgenden Abbildung wird die Zeichenfolge für den Schweregrad hinzugefügt.



   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie unter Rapid7 Dokumentation für weitere Informationen zur Trennung der einzelnen Werte.

7. Klicken Sie auf **Aktualisieren**.

Verständnis der Shodan-Exploit-Integration

Die ServiceNow® Shodan Die Exploit-Integrationsanwendung verwendet Daten, die aus importiert wurden Shodan Suchmaschine, mit der Sie die Auswirkung und Priorität potenziell schädlicher Exploits bestimmen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Shodan Exploit Integration

Die Shodan Die Suchmaschine sammelt Exploit-Daten, und die Shodan-API macht diese Datenbank für verfügbar ServiceNow AI Platform®. Es lässt sich problemlos in integrieren ServiceNow® Vulnerability Response Anwendung zum Zuordnen von Exploits zu Schwachstellen von Drittanbietern, um die Exploit-Daten in Ihrer Instanz zu ergänzen.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Täglich rufen geplante Aufgaben die Integrationen automatisch in der Reihenfolge auf, in der sie aufgelistet werden. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Verfügbare Versionen

Release-Version für Yokohama	Release-Hinweise
Shodan Exploit-Integration V10.6, 10,7	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Rollen

Shodan Exploit-Integrationsaufgaben umfassen die folgenden Rollen.

- sn_vul_shodan.admin: Anwender mit dieser Rolle können Datensätze lesen, schreiben und löschen.
- sn_vul_shodan.user: Anwender mit dieser Rolle können Datensätze lesen und schreiben.
- sn_vul_shodan.read: Anwender mit dieser Rolle können Datensätze lesen.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

SHODAN-Exploit-Integrationen

Um anzuzeigen Shodan Exploit-Integrationen, navigieren Sie zu **Alle** > **Shodan Exploit Integration** > **Integrationen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Integrationen sind im Basissystem enthalten. Diese Integrationen sind standardmäßig aktiv.

SHODAN-Exploit-Integrationen

Integration	Beschreibung
SHODAN ExploitDB-Integration	Ruft ExploitDB-Daten von ab Shodan Und ergänzt Ihre Schwachstellendaten von Drittparteien. Diese Integration ist so festgelegt, dass sie täglich um 03:15:00 Uhr ausgeführt wird.
Shodan-Metasploit-Integration	Ruft Metasploit-Informationen von ab Shodan Und ergänzt Ihre Schwachstellendaten von Drittparteien. Diese Integration ist so festgelegt, dass sie täglich um 01:15:00 ausgeführt wird.

Informationen zum Ändern der Standardstartzeit für die geplanten Integrationsimporte finden Sie unter Festlegen Shodan Exploit-Integrationsimportzeit.

Informationen zum Anzeigen von Exploit-Daten in Schwachstellen von Drittparteien finden Sie unter Anzeigen Vulnerability Response Schwachstellenbibliotheken.

Ändern anderer Shodan Einstellungen für die Exploit-Integration erfordern erweiterte Elemente ServiceNow Und Vulnerability Response Fachwissen und übersteigt den Umfang der Produktdokumentation.

Vorbereitung für Shodan Exploit-Integration

Ein erfolgreich Shodan Die Exploit-Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die Shodan Exploit-Integration setzt voraus, dass Sie mit vertraut sind Shodan Suchmaschine und API.

Vorbereitungen

Die Shodan Exploit-Integration erfordert einen API-Schlüssel. Registrieren Sie sich bei Shodan Website Für ein kostenloses Abonnement zum Erwerb dieses Schlüssels.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

- Wenn Sie keine NIST Vulnerability Database (NVD)-Daten in importiert haben Vulnerability Response, Tun Sie dies, bevor Sie installieren Shodan Exploit-Integration. Durch das Importieren der NVD-Daten wird sichergestellt, dass Ihre CVE-Daten (Common Vulnerability and Exposure) die Exploit-Datensätze automatisch ausfüllen.

  Ohne NVD-Daten wird im Exploit-Datensatz ein Platzhalter erstellt und erst beim nächsten NVD-Update eingegeben. Weitere Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken.

- Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie Shodan Exploit-Integration Für Security Operations

Bevor Sie ausführen können Shodan Exploit-Integration Laden Sie es in Ihrer Instanz herunter, und installieren Sie es aus dem ServiceNow Store. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

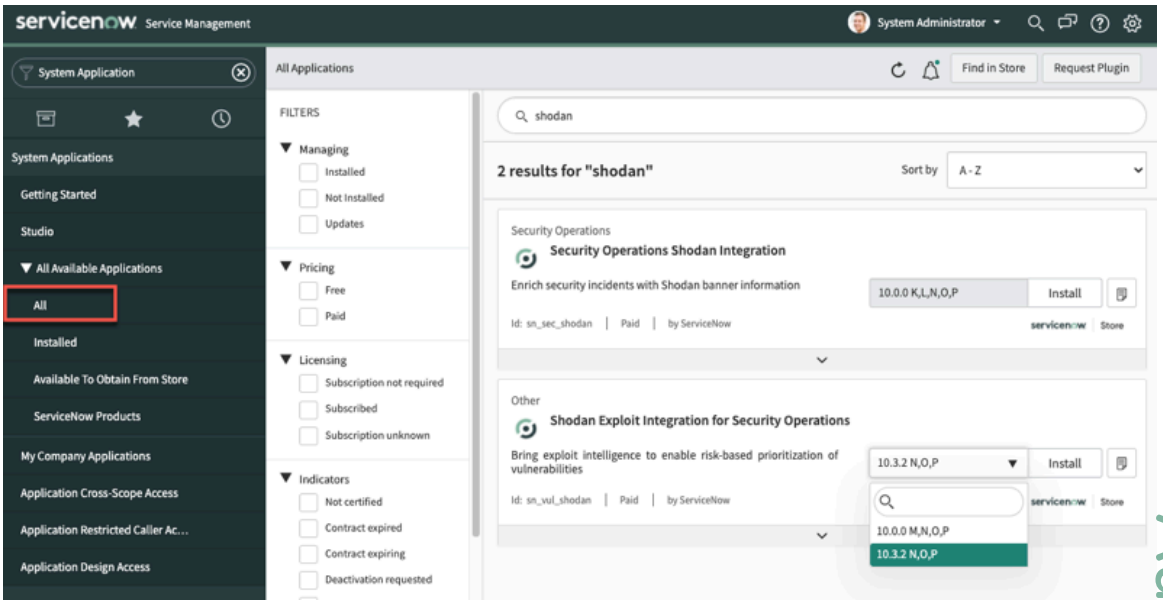
Setupaufgaben	Beschreibung
Überprüfen Sie, ob Sie gültig sind ServiceNow Berechtigungen für Vulnerability Response Anwendung und Shodan Exploit-Integration Für Security Operations Anwendung.	Navigieren Sie zu , um Berechtigungen zu überprüfen **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Weitere Informationen zum Abrufen von Berechtigungen für Security Operations Anwendung aus dem ServiceNow Store, Siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung.
(Optional) wenn Sie nicht bereits installiert und aktiviert sind, möchten Sie möglicherweise installieren Vulnerability Response Anwendung vor der Installation der Drittanbieteranwendung.	Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe, Vulnerability Response installieren.
Haben Shodan Exploit-Integrations-API-Schlüssel handlich.	Weitere Informationen finden Sie unter Vorbereitung für Shodan Exploit-Integration.

Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei an ServiceNow AI Platform Instanz, die Sie installieren möchten Shodan Exploit-Integration Anwendung auf.
2. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
3. Suchen Sie nach Shodan Exploit-Integration Für Security Operations Anwendung, wählen Sie die gewünschte Version aus, und klicken Sie auf **Installieren** .

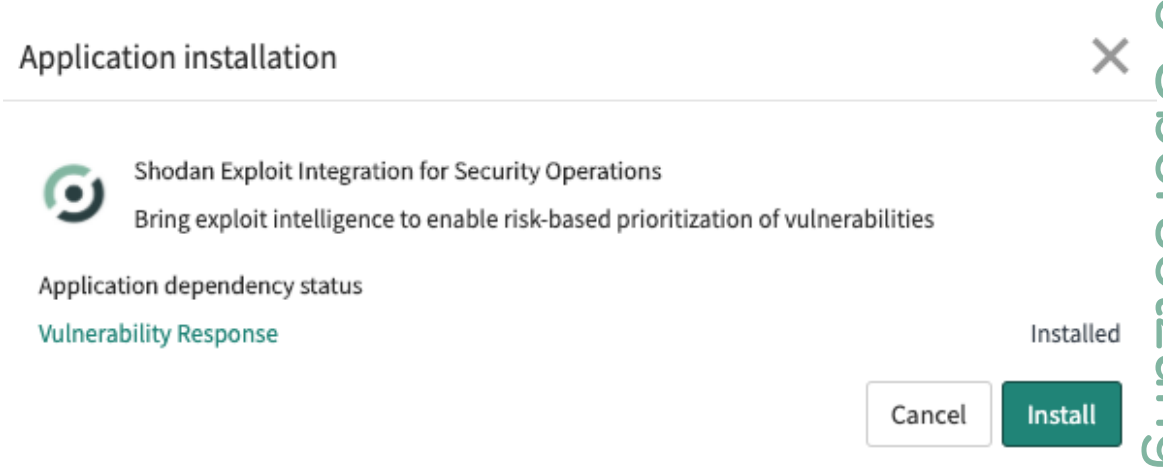
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Wenn Sie berechtigt sind, ein Update für diese Anwendung zu erhalten **Aktualisieren** Schaltfläche wird angezeigt.

Im Dialogfeld „Anwendungsinstallation“ wird der Status der Anwendungsabhängigkeit angezeigt. Alle erforderlichen Abhängigkeiten, die noch nicht installiert sind, werden automatisch zusammen mit der Anwendung installiert.

4. Klicken Sie im Dialogfeld auf **Installieren** .

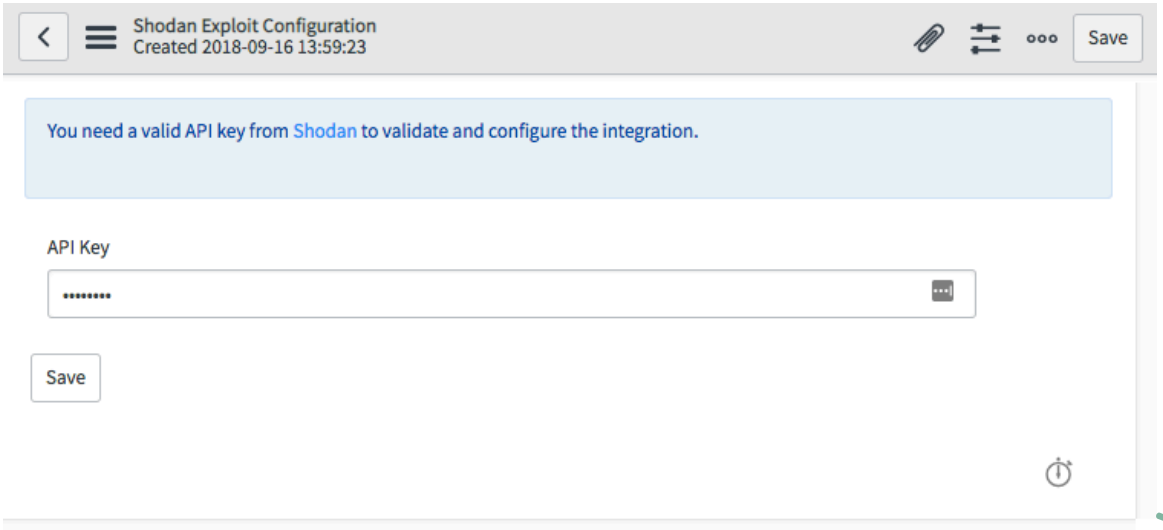


Das Dialogfeld „Installation“ zeigt an, wann die Installation erfolgreich abgeschlossen wurde.

5. Schließen Sie das Dialogfeld „Installieren“.
6. Navigieren zu **Shodan Exploit Integration** > **Konfiguration**an.
7. Geben Sie ein Shodan API-Schlüssel.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Klicken Sie auf **Speichern**.
   Ihr Shodan Exploit-Integration Konfiguration ist abgeschlossen.

Festlegen Shodan Exploit-Integrationsimportzeit

Sie können die Startzeit für zurücksetzen Shodan Exploit-Integrationen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Nach dem ersten Import Shodan Exploit-Integrationen bringen Delta-Daten ein, es sei denn, ein vollständiger Import wird angefordert. Siehe Führen Sie ein Handbuch durch Shodan Exploit-Import Weitere Informationen zu vollständigen Importen.

Prozedur

1. Navigieren zu **Alle** > **Shodan Exploit Integration** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf den Link, um den Datensatz zu bearbeiten.
4. Legen Sie das neue fest **Ausführen** Und **Zeit** Optionen.
   Die Zeit wird als Stunden in Ortszeit berechnet. Die Standardzeit für Shodan Exploit-Importe sind 03:15:00.
5. Klicken Sie auf **Aktualisieren**.
   Die neue Zeit wird für den nächsten geplanten Import verwendet.

Führen Sie ein Handbuch durch Shodan Exploit-Import

Wenn Ihr anfänglicher Import fehlgeschlagen ist oder Sie nicht auf den geplanten anfänglichen Import warten möchten, können Sie unabhängig von der täglichen geplanten Aufgabe einen vollständigen Datenimport durchführen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Shodan Exploit Integration** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
3. Wählen Sie aus **Vollständiger Datenimport** Kontrollkästchen.
4. Klicken Sie auf **Jetzt ausführen**.
   Sobald der Import abgeschlossen ist, wird das Kontrollkästchen deaktiviert, und Delta-Importe werden fortgesetzt.

Zeigen Sie an Shodan Ausführungsstatus des Exploit-Integrationsimports

Verwenden Sie die zugehörige Liste „Ausführungen der Schwachstellenintegration“, um den Erfolg Ihrer Integrationsausführungen zu überprüfen und Probleme zu lokalisieren , Und informieren Sie Ihre Korrekturentscheidungen.

Vorbereitungen

So zeigen Sie den Status der Shodan-Importausführung an:

- Die Vulnerability Response Anwendung und Shodan Exploit-Integration muss installiert und konfiguriert sein.
- Die Shodan Exploit-Integrationsimporte müssen geplant und ausgeführt werden.

Erforderliche Rolle: sn_vuln.admin

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Shodan Exploit Integration** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste.
4. Überprüfen Sie, ob alle Importe erfolgreich waren.

Trouble?

Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:

- Netzwerkunterbrechung
- Bitverfall bei der Datenübertragung, was zu beschädigten Daten während der Transformation führt

Wenn eine dieser Bedingungen auftritt, wählen Sie aus **Vollständiger Datenimport** Klicken Sie auf das Kontrollkästchen **Jetzt Ausführen** , Und führen Sie die Integration erneut aus.

Verständnis der Tenable-Schwachstellenintegration

Die Vulnerability Response Integration with Tenable Anwendung entwickelt von ServiceNow Engineering für die Tenable-Schwachstellenintegration verwendet Daten, die aus importiert wurden Tenable.io, Tenable.sc, Und Tenable.cs Produkte, mit denen Sie Schwachstellen für Ihre Assets priorisieren und beheben können. Die Anwendung ist mit einem separaten Abonnement als verfügbar ServiceNow® Store.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Die Tenable-Schwachstellenintegration verwendet drei Tenable-Integrationen, Tenable.io, Tenable.sc Und Tenable.cs, Um Scannerdaten von Drittparteien zu Ihren Assets und Schwachstellen zu importieren. Die Vulnerability Response Integration with Tenable Die Anwendung unterstützt Tenable.sc Produkt ab Version 5,13 und Tenable.cs Produkt ab Version 5,0.1.

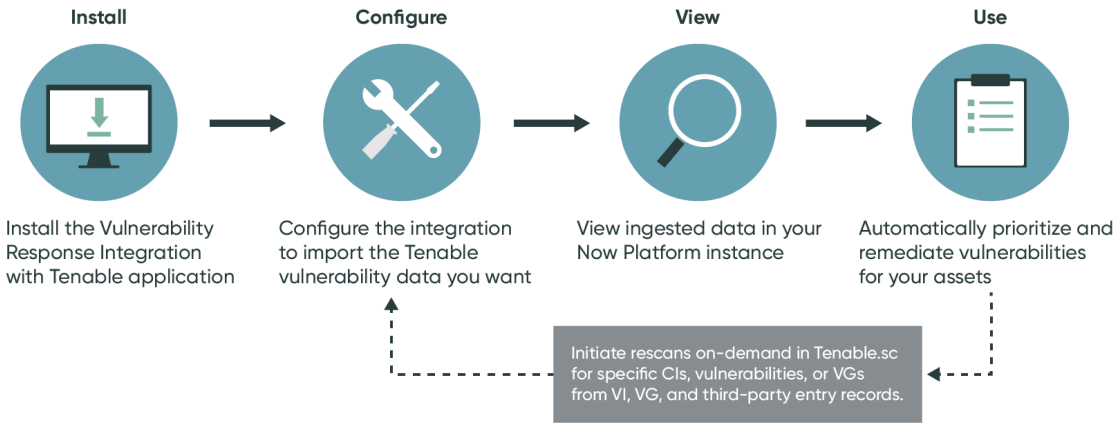
- Tenable.io Ist eine cloudbasierte Enterprise-Integration.
- Tenable.sc Ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn der verwendet wird Tenable.sc Produkt und Ihr ServiceNow AI Platform Instanz befindet sich in derselben Umgebung.
- Wenn Tenable.sc Produkt und Ihr ServiceNow AI Platform Instanz befindet sich nicht in derselben Umgebung, Sie müssen einen MID-Server verwenden.
- Tenable.cs Ist eine cloudbasierte Enterprise-Integration.

Die Vulnerability Response Integration with Tenable Anwendung ist auf verfügbar ServiceNow Store Mit einem separaten Abonnement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Listen und Beschreibungen der Integrationen in Tenable Vulnerability Integration, Siehe Tenable.io Integrationen mit Vulnerability Response Und Konfigurations-Compliance Anwendungen Und Tenable.sc Integrationen mit Vulnerability Response Anwendung.

Tenable-Schwachstellen-Integration



Verfügbare Versionen für Yokohama

Freigabeversion	Release-Hinweise
Vulnerability Response Integration with Tenable V3.13.1, v4.1, v5.0.1	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Begriffe und wichtige Funktionen der Integrationen

Angreifbare Elemente und Schwachstellen

Ein angreifbares Element wird in erstellt ServiceNow AI Platform Instanz, wenn:

- Eine importierte Schwachstelle von einem Scanner eines Drittanbieters wird mit einem vorhandenen Asset (einem Konfigurationselement in Ihrem) abgeglichen CMDB). Das Tenable-Produkt bezieht sich auf diese Übereinstimmungen als **Schwachstellen** .
- Eine importierte Schwachstelle von einem Scanner eines Drittanbieters wird nicht mit einem vorhandenen Asset in Ihrem abgeglichen CMDB. In diesem Fall wird auch ein nicht übereinstimmendes CI zusammen mit einem angreifbaren Element erstellt.

  Für nicht abgeglichene CIs können Sie auch die Identification and Reconciliation Engine (IRE) verwenden, um CIs in zwei neuen Klassen zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter CIs für werden erstellt Vulnerability Response Verwenden der Identifizierungs- und Abgleichsmodul.

Einträge und Plugins von Drittanbietern für Schwachstellen

Einträge für Schwachstellen von Drittparteien werden aus Scannern von Drittparteien importiert und in der Tabelle „Schwachstelleneinträge von Drittparteien“ in aufgeführt ServiceNow

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AI Platform Instanz. Ab v24.0 von Vulnerability Response, Die Spalte Software in der Tabelle „Drittanbieter-Schwachstelleneinträge“ füllt die CPEs (Common Platform Enumerations, CPEs) aus, die einer Drittpartei zugeordnet sind Eintrag . Einträge von Drittpartei-Schwachstellen aus Tenable werden in erfasst Vulnerability Response Und mit vorhandenen Assets abgeglichen, die in aufgeführt sind CMDB. Tenable bezieht sich auf Einträge von Drittpartei-Schwachstellen als **Plugins** .

Konfigurationselement bzw. Configuration Item (CI)

Konfigurationselemente sind die vorhandenen Assets, die in aufgeführt sind CMDB.

Erkanntes Element

Assets, die aus dem Import von Tenable-Assets erfasst werden, werden mit vorhandenen Konfigurationselementen in abgeglichen CMDB. Importierte Assets werden aktualisiert.

Wenn keine Übereinstimmung gefunden wird, wird ein CI in der nicht abgeglichenen CI-Klasse von erstellt CMDB. Wenn das Plugin „CMDB CI-Klassenmodelle“ aktiviert ist, erstellt die Identification and Reconciliation Engine (IRE) CIs mit neuen Klassen. Weitere Informationen finden Sie unter CIs für werden erstellt Vulnerability Response Verwenden der Identifizierungs- und Abgleichsmodul. Wenn das ursprüngliche, nicht abgeglichene CI neu klassifiziert wird, werden erkannte Elementdatensätze entsprechend dem Status aktualisiert. Erkannte Elemente geben Ihnen Einblick, wie Assets identifiziert und CIs in zugeordnet werden CMDB.

CI-Suchregeln

Wenn Daten aus einer Drittpartei-Integration importiert werden, verwendet Vulnerability Response automatisch Host-(Asset-)Daten, um nach Übereinstimmungen in der Configuration Management-Datenbank zu suchen (CMDB). CI-Suchregeln werden verwendet, um CIs zu identifizieren und sie VI-Datensätzen hinzuzufügen, wenn Vits erstellt werden, um Sie bei der Korrektur zu unterstützen.

Erneut scannen und Korrekturscan

Sie können einen gezielten erneuten Scan-Befehl für ein bestimmtes Konfigurationselement, eine Korrekturaufgabe oder einen Drittparteieintrag direkt aus den Datensätzen für angreifbare Elemente, Korrekturaufgaben und Schwachstelleneinträge von Drittparteien in Ihrem initiieren ServiceNow AI Platform Instanz. Tenable bezieht sich auf diesen erneuten Scan als **Korrekturscan** .

Schließen Sie ältere VIS automatisch

Mit dem Modul „veraltete angreifbare Elemente automatisch schließen“ in Ihrem ServiceNow AI Platform, Sie können ältere, veraltete angreifbare Elemente (VI) bereinigen, die kürzlich von Ihren Drittpartei-Integrationen nicht gefunden wurden. Diese VIS werden nach verschoben **Geschlossen** Hilft Ihnen, die Anzahl der aktiven angreifbaren Elemente und Korrekturaufgaben zu reduzieren und Assets in abzugleichen CMDB. Sie können alle Integrationen mit verwenden Vulnerability Response Integration with Tenable Dient zum automatischen Schließen veralteter VIS.

Instanz

Dieser Begriff bezieht sich auf ein eindeutiges Vorkommen von ServiceNow AI Platform® Anwendung.

Integration

Eine -Integration ist eine produktspezifische Referenz zu einer -Integration, z. B. Tenable.io Assets-Integration oder Tenable.sc Plugin-Integration. Dies sind die separaten Integrationen, die zu bestimmten Tenable-Produkten in der Tenable-Schwachstellenintegration in Ihrer Instanz gehören.

Integrationsinstanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Begriff bezieht sich auf die separaten Tenable-Integrationen, die nach aufgeführt sind Tenable.io Und Tenable.sc Produkte.

Bereitstellung

Wenn eine Integration mehrere Quellen unterstützt, wird eine einzelne, eindeutige Integration als Bereitstellung Ihrer Integration bezeichnet. Der Begriff wird verwendet, um auf die Integrationen und Produkte in Ihrer Umgebung zu verweisen. Beispielsweise können Sie mehrere Bereitstellungen verschiedener Integrationen von haben Tenable.io Und Tenable.sc Produkte in Ihrer Umgebung.

Die Tenable.io, Tenable.sc, Und Tenable.cs Integrationen umfassen auch die folgenden wichtigen Funktionen:

- Konfigurationsbewertungsergebnisse, d. h. Testergebnisse zusammen mit Richtlinien, Konfigurationstests (Steuerungen) und Bezugsvermerke mit autorisierenden Quellen können in importiert werden Konfigurations-Compliance Anwendung mit Tenable.io Produkt. Siehe Tenable.io Integrationen mit Vulnerability Response Und Konfigurations-Compliance Anwendungen Und Konfigurations-Compliance erkunden Um weitere Informationen zur Funktionsweise dieser Integration mit zu erhalten Konfigurations-Compliance Anwendung.
- Ab v2.1 des Tenable Vulnerability Integration, Erstellen Sie eindeutige Konfigurationselemente (Configuration Items, CIs), die verschiedene Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung enthalten, die dieselbe IP-Adresse verwenden. Identifizieren Sie die eindeutigen Assets in Ihrer Umgebung, und aktualisieren Sie die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen, um Ihnen weitere Details zu Ihren Schwachstellen zu geben.
- Sie können planen, wann die Aufträge für alle ausgeführt werden sollen Tenable.io, Tenable.sc Und Tenable.cs Integrationen. Sie können geplante Aufgaben auch bei Bedarf manuell ausführen.
- Für Asset-Importe mit Tenable.io, Sie können Asset-Tags aktivieren, um die in aufgeführten Assets zu organisieren und nachzuverfolgen CMDB In Tenable.io Umgebung.
- Die Tenable.io, Tenable.sc Und Tenable.cs Integrationen ermöglichen es Ihnen, CI-Suchregeln zu konfigurieren, um zu definieren, wie Asset-Daten aus Drittparteiquellen zur Identifizierung von Konfigurationselementen (Configuration Items, CIs) in verwendet werden ServiceNow AI Platform CMDB.
- Die Tenable.io, Tenable.sc Und Tenable.cs Mit Integrationen können Sie Importfilter für den Schwachstellenimport festlegen, sodass Sie nur die gewünschten Schwachstellen aus Tenable importieren. Für Tenable.io, Sie haben die Möglichkeit zum Importieren **Behoben** Schwachstellen aus Tenable mit dem Schwachstellenimport.
- Für Tenable.sc, Sie haben die Möglichkeit, bei Bedarf erneut scans direkt aus einem angreifbaren Element, einer Korrekturaufgabe und Drittpartei-Eintragsdatensätzen in zu initiieren ServiceNow AI Platform Instanz. Wenn VIS auf geändert wurden **Geschlossen/ Behoben** Wurden in Ihrer Instanz jedoch noch nicht aktualisiert, können Sie überprüfen, ob Schwachstellen in bestimmten Konfigurationselementen behoben wurden. Weitere Informationen finden Sie unter Initiieren Sie einen erneuten Scan für Tenable.sc Integration.

Die folgenden Abschnitte enthalten weitere Details zu den Tenable-Integrationen.

Erforderliche ServiceNow AI Platform-Rollen

Die Integrationsaufgaben erfordern die folgenden Rollen in Ihrem ServiceNow AI Platform Instanz.

Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Systemadministrator verwendet den Setup-Assistenten, um zu installieren Vulnerability Response Integration with Tenable Anwendung. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.Vulnerability_admin) und andere Rollen im Setup-Assistenten zu.

sn_vul.vulnerability_admin

Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der Tenable-Integrationen im Setup-Assistenten ab. Diese Rolle hat vollständigen Zugriff auf Vulnerability Response(VR)-Anwendung und ihre Datensätze. Der Schwachstellenadministrator konfiguriert alle VR-Anwendungen und -Regeln für installierte Drittanbieterintegrationen.

sn_vul_Tenable.configure_Integration

Diese Rolle enthält die granulare Rolle sn_vul_Tenable.read_Integration, und Anwender mit dieser Rolle können konfigurieren Vulnerability Response Integration with Tenable Anwendung.

sn_vul_Tenable.read_Integration

Benutzer mit diesen Rollen können Datensätze von anzeigen (lesen), aber nicht bearbeiten Vulnerability Response Integration with Tenable Anwendung.

Vulnerability Response-Gruppe

Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Anwender, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen sn_vul.read_all und sn_vul.Remediation_owner automatisch.

Angreifbare Elemente

Angreifbare Elemente werden gemäß den Regeln für Korrekturaufgaben in Korrekturaufgaben gruppiert und basierend auf Ihren Zuweisungsregeln zur Korrektur zugewiesen. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben und Vulnerability Response Übersicht über Zuweisungsregeln.

Suchregeln für Konfigurationselement (Configuration Item, CI)

CI-Suchregeln identifizieren CIs und bestimmen, wann sie einem angreifbaren Element hinzugefügt werden sollen. Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Integrationen von Schwachstellen von Drittparteien.

Hinweis:
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen von Regeln.

Folgendes Tenable.io Suchregeln sind im Lieferumfang des Basissystems enthalten.

- MAC_ADDRESS
- FQDN
- NetBIOS
- HostName
- DNS
- IP

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Tenable.io CI-Suchregeln priorisieren und füllen die nicht leeren Netzwerkschnittstellenwerte (FDQN, IPV4 und MacAddress) gegenüber den regulären FDQN-, IPV4- und MacAddress-Werten für ein erkanntes Element aus. Wenn diese Netzwerkschnittstellenwerte leer sind, werden die regulären FDQN-, IPV4- und MacAddress-Werte für ein erkanntes Element ausgefüllt.

Folgendes Tenable.sc Suchregeln sind im Lieferumfang des Basissystems enthalten.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Hinweis:
Für ein Asset werden mehrere Werte für ip_address, mac_address, fqdns und Network_Interfaces verwendet. Alle Werte werden in CI-Suchregeln für den Abgleich berücksichtigt. Alle Werte werden verwendet, um mehrere Netzwerkadapter mit IRE zu erstellen.

Die Tenable.cs Suchregel „Cloud-Ressourcen-ID“ wird mit dem Basissystem geliefert.

Weitere Informationen zum Konfigurieren der Kategorisierung nicht übereinstimmender Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert.

Neue Eigenschaften zum Ignorieren von IP-Adressen

In Tenable.io, Es sind zwei Eigenschaften verfügbar, wenn Sie mehrere IP-Adressen oder mehrere Mac-Adressen als Teil Ihrer CI-Suchregeln ignorieren möchten:

IgnoreIPAddress

Eine Liste von IP-Adressen, die für die CI-Suche und die CI-Erstellung ignoriert werden sollen.

IgnoreMacAddress

Eine Liste von MAC-Adressen, die bei der CI-Suche oder CI-Erstellung ignoriert werden sollen.

Erkannte Elemente

Dieses Modul listet Konfigurationselemente auf, die während des Imports aus den Tenable-Integrationen für angreifbare Elemente und den Tenable-Asset-Integrationen erkannt wurden.

Hinweis:
Der Standardfilter für diese Liste ist auf festgelegt Nicht Abgeglichen . Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Weitere Informationen zum Modul „erkannte Elemente“ finden Sie unter Erkannte Elemente.

Asset-Tags

Asset-Tags (auch als Host-Tags bezeichnet) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Assets Tags zuweisen. Beim Starten der Scans können Sie dann Tags auswählen, die den Assets zugeordnet sind, die Sie scannen möchten. Mit dem Modul „Asset-Tags“ können Sie Asset-Tag-Daten aus herunterladen Tenable.io Zu Ihrer Instanz auf einer geplanten Basis. Asset-Daten, die Asset-Tags enthalten, werden aus abgerufen Tenable.io Und mit transformiert Tenable.io-Asset-Transformation Integrationstransformationszuordnungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Asset-Tags werden als Teil von importiert Tenable.io Asset-Integration. Asset-Tags werden zum Filtern verwendet Vulnerability Response Zuweisungsregeln und Regeln für Korrekturaufgaben. Die Tags werden im Formular „erkanntes Element“ angezeigt.

Hinweis:
Führen Sie aus Tenable.io Asset-Integration vor dem Erstellen Vulnerability Response Zuweisungsregeln oder Regeln für Korrekturaufgaben in Vulnerability Response Anwendung, damit alle Tags für diese Regeln verfügbar sind, bevor angreifbare Elemente importiert und gruppiert werden. Beachten Sie auch die folgenden Punkte zu Tags:

- Beim Tag-Speicher wird die Groß-/Kleinschreibung nicht beachtet. Wenn Sie beispielsweise ein Tag erstellen, um Assets an Ihrem San Diego-Standort zu beschreiben, und erstellen Sie `San Diego` Tag, können Sie nicht auch erstellen `SAN DIEGO` Kennzeichnen und in der Asset-Tag-Tabelle speichern. `San Diego` Und `SAN DIEGO` Werden vom System als dasselbe Asset-Tag betrachtet. Welches Tag zuerst importiert wird, ist das Tag, das gespeichert und in Zukunft erkannt wird.
- Die Verwendung von Asset-Tags als Gruppenschlüssel in einer Korrekturaufgabenregel kann zu unerwarteten Ergebnissen führen. Asset-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Asset-Tags werden von der globalen Systemeigenschaft sn_vul.Import_Asset_Tags gesteuert. Diese Eigenschaft ist auf festgelegt Wahr Standardmäßig. Durch das Deaktivieren von Tags werden sie für alle deaktiviert ServiceNow AI Platform® Instanzen.

Datenabruffilter

Mit den Einstellungen für den Datenabruf können Sie insbesondere den Typ und den Umfang der Daten bestimmen, die Sie aus der Tenable-Anwendung in importieren möchten ServiceNow AI Platform® Instanz. Eine Liste der am häufigsten verwendeten Einstellungen finden Sie unter Datenabrufeinstellungen für die Tenable-Schwachstellenintegration.

Schwachstellenprioritätsbewertung (VPR)

Die Vulnerability Priority Rating (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit einem neuen Standardrisikorechner in verwendet wird Vulnerability Response. Die Tenable-Risikoregel wird mit installiert Vulnerability Response Integration with Tenable Anwendung als Teil des Standardrisikorechners in den Schwachstellenrechnern von Vulnerability Response.

Diese Risikoregel ist standardmäßig inaktiv.

Durch Aktivieren der Tenable-Risikorechnerregel werden die importierten VPR-Werte zur Berechnung der Risikopunktzahl für angreifbare Elemente verwendet. Die Standardgewichtungsverteilung für diesen Risikorechner: VPR = 70 %, Asset = 15 % und Geschäftsrelevanz = 15 %. Das Aktivieren dieser Tenable-Risikorechner-Regel kann sich auf Ihre Leistung der Datenerfassung auswirken. Weitere Informationen zu finden Vulnerability Response Rechner und die Tenable-Risikorechnerregel finden Sie unter Vulnerability Response Rechner und Regeln für Schwachstellenrechner.

Installation und Konfiguration

Nachdem Sie heruntergeladen haben Vulnerability Response Integration with Tenable Von ServiceNow® Store, Installation und Konfiguration werden vom Setup-Assistenten in unterstützt Vulnerability Response. Weitere Informationen finden Sie unter Wird Konfiguriert Vulnerability Response Mit dem Setup-Assistenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io Integrationen mit Vulnerability Response Und Konfigurations-Compliance Anwendungen

Die Tenable.io Integrationen in Vulnerability Response Integration with Tenable-Anwendungen sind in verfügbar Vulnerability Response Und Konfigurations-Compliance Anwendungen.

Liste von Tenable.io Integrationen

Mehrere Quellen werden für alle unterstützt Tenable.io Und Tenable.sc Integrationen. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in hinzufügen und bereitstellen Vulnerability Response. Sie installieren und konfigurieren auch Vulnerability Response Integration with Tenable Anwendung aus Setup-Assistent.

Tenable.io Ist eine cloudbasierte Enterprise-Integration. In der folgenden Tabelle finden Sie die Namen und Beschreibungen der unterstützten Integrationen für Tenable.io Produkt.

Die Tenable.io Integration von Compliance-Ergebnissen und der Tenable.io Compliance-Ergebnisse – Backfill-Integration ist standardmäßig inaktiv.

So aktivieren Sie sie:

1. Navigieren zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**an.
2. Klicken Sie in der Liste Tenable-Integrationen auf einen Integrationsnamen, um den Datensatz zu öffnen, und wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren. Möglicherweise möchten Sie die Zeitplaneinstellungen in ihren Standardwerten belassen, damit diese Integrationen beginnen.

Tenable.io-Integrationen

Integration	Beschreibung
Tenable.io Asset-Integration	• Ruft alle Asset-Daten, einschließlich Asset-Tags, aus dem ab Tenable.io Produkt und verarbeitet es in Ihrer Instanz. • Ab v3.0, wenn Tenable.io Die Integration von Compliance-Ergebnissen ist aktiviert. Sie können sichere Konfigurationsbewertungsdaten zusammen mit importierten Asset-Daten importieren. Diese Daten können Ihnen helfen, die konfigurationsbezogenen Schwachstellen in Ihren Assets zu identifizieren und darauf zu reagieren. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die dieselbe IP-Adresse haben. • Koordiniert die REST-Nachrichtenaufrufe an die Asset-API. • Die Ausgabe dieser Integration ist erkannte Elemente. • Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_Chunk_Status] gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. • Ab v2.2, `Last Scan Time`Wird nur für Assets mit Schwachstellen importiert und aktualisiert.
Tenable.io Integration Von Compliance-Ergebnissen	• Ab v3.0 können Sie mit importierten sicheren Konfigurationsbewertungsdaten aus der Compliance-Ergebnisintegration zusammen mit importierten Daten aus der Asset-Integration die konfigurationsbezogenen Schwachstellen in Ihren Assets identifizieren und darauf reagieren. • Wenn diese Option aktiviert ist, werden allgemeine sichere Konfigurationsbewertungsdaten abgerufen und in verarbeitet ServiceNow AI Platform Instanz. Importierte Daten umfassen Testergebnisse zusammen mit Richtlinien, Konfigurationstests (Steuerungen) und Bezugsvermerke mit autorisierenden Quellen. • Bewertungsdaten für fehlende Assets oder Assets ohne Asset-IDs werden nicht importiert. • Wenn ein Testergebnis importiert wird und das entsprechende Asset nicht in Ihrer Instanz abgeglichen werden kann, wird das Testergebnis ignoriert, und die ID für das fehlende Asset wird in einem temporären Datensatz in der Tabelle [sn_vul_tenable_missing_Asset] gespeichert. • Der Gesamtwert der ignorierten (fehlenden) Assets wird in aufgeführt **Ignorierte CIs** Feld auf der **Konfiguration** Registerkarte im Datensatz der Integrationsausführung für diese Integration.
Tenable.io Integration Der Compliance-Ergebnisse Im Backfill	• Wenn diese Option aktiviert ist, wird diese Integration automatisch ausgeführt, nachdem die Asset-Integration als Teil einer verketteten Integrationsausführung erfolgreich abgeschlossen wurde. Diese Integration stimmt Konfigurationsbewertungsdaten mit fehlenden Assets ab, die in der Tabelle [sn_vul_TENABLE_missing_Asset] aufgeführt sind. • Importiert bis zu 200 Asset-IDs für alle fehlenden Assets, die in der Instanz erkannt oder vorhanden sind, nachdem der Import der Asset-Integration erfolgreich abgeschlossen wurde. • Entfernt die temporären Datensätze aus der Tabelle [sn_vul_TENABLE_missing_Asset], wenn Assets mit entsprechenden Konfigurationsbewertungsdaten abgeglichen werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
Tenable.io Integration Von Anmeldeinformationen Scannen	• Diese Integration ruft die in konfigurierten Scan-Anmeldeinformationen ab Tenable.io. • Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API. • Die Ausgabe dieser Integration ist Scan-Anmeldeinformationen, die in der Tabelle [sn_vul_Tenable_Scan_credential] ausgefüllt sind. • Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scananforderungen von initiiert werden ServiceNow AI Platform. • Diese Integration wird wöchentlich ausgeführt.
Tenable.io Vorlagenintegration	Ein Vorlagendatensatz wird an gesendet Tenable.io Während des erneuten Scans. Diese Integration ruft verfügbare ab Tenable.io Anmeldeinformationen, die für erneute Scans verwendet werden sollen. Anmeldeinformationen sind instanzspezifisch, und ein einzelner Vorlagendatensatz wird importiert und vorübergehend sicher in der Tabelle [sn_vul_Tenable_io_template] gespeichert.
Tenable.io Plugin-Integration	• Ruft die Plugin-Daten aus dem ab Tenable.io Produkt. Abgerufene Daten basieren auf dem Datum, an dem die Plugins zuletzt von einem aktualisiert wurden Tenable.io Integrationsausführung. • Dieser Import stellt sicher, dass die Tenable.io Bezeichner (zehn IDs) sind aktuell. • Koordiniert die REST-Nachrichtenaufrufe an die Plugin-API. • Die Ausgabe dieser Integration ist Schwachstellen von Drittparteien.
Tenable.io Integration Behobener Schwachstellen	• Ruft Schwachstellendaten basierend auf Schweregradfiltern aus ab Tenable.io Produkt und verarbeitet es in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich in befinden **Öffnen** Und **Erneut Geöffnet** status, da diese Datensätze eine Korrektur erfordern. Vorhandene angreifbare Elemente werden von Vulnerability Response aktualisiert, wenn Erkennungen sind **Behoben** , Aber angreifbare Elemente werden für nicht erstellt **Behoben** Erkennungen standardmäßig, da Tenable berücksichtigt **Behoben** Schwachstellen **Gemindert** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	• Wenn die Kennzeichnung **Erstellen Sie Zeiten für Schwachstellen für Erkennungen behobener Schwachstellen** Ist im Setup-Assistenten aktiviert, neue VIS werden in erstellt **Behoben** geben sie den status an, damit Sie Einblick in die Erkennungen haben, die sie erstellt haben. Da VIS für erstellt werden **Behoben** Erkennungen, die in Ihrer Instanz nicht bereits vorhanden sind, können sich negativ auf Ihre Importleistung auswirken. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, damit dies möglich ist **Behoben** Erkennungen aktualisieren nur die status vorhandener angreifbarer Elemente. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die dieselbe IP-Adresse haben. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration ist **Geschlossen/Behoben** Angreifbare Elemente (VIS). Außerdem werden Assets und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind. • Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_Chunk_Status] gespeichert. Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. Diese Integrationsausführung ist geplant. Es handelt sich um eine verkettete Integration, d. h. nach erfolgreichem Abschluss einer Ausführung wird die unten beschriebene Integration offener Schwachstellen ausgelöst. Ab Tenable v3.3 können Sie die folgenden Informationen für die Ausführungen der Schwachstellenintegration anzeigen: • **Blöcke insgesamt:** Gesamtanzahl der Blöcke, die von Tenable generiert werden • **Verfügbare Blöcke:** Anzahl der Blöcke, die für heruntergeladen werden können ServiceNow
Tenable.io Integration Offener Schwachstellen	• Diese Integration wird nach erfolgreichem Abschluss von ausgelöst Tenable.io Integration Behobener Schwachstellen. • Ruft Schwachstellendaten basierend auf den Schweregradfiltern aus ab Tenable.io Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die dieselbe IP-Adresse haben. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration ist **Neu/Erneut Geöffnet** Angreifbare Elemente (VIS). Außerdem werden Konfigurationselemente und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind. Tenable berücksichtigt aktive Schwachstellen **Kumulativ** (Aktuell). • Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_Chunk_Status] gespeichert. Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. Ab Tenable v3.3 können Sie die folgenden Informationen für die Ausführungen der Schwachstellenintegration anzeigen: • **Blöcke insgesamt:** Gesamtanzahl der Blöcke, die von Tenable generiert werden • **Verfügbare Blöcke:** Anzahl der Blöcke, die für heruntergeladen werden können ServiceNow
Tenable.io/Scan-Metadatenintegration	Diese Integration ruft Metadaten vom Endpunkt „/Scans“ ab. Ruft Scan-Informationen basierend auf der Last_schedule_ID aus den vorhandenen Asset-Daten in ab Tenable.io. Die Integration des Endpunkts „/scans“ aus Tenable.io Umfasst die folgenden Implementierungsschritte: • **Tabellenerstellung** : Eine neue anwenderdefinierte Tabelle, **sn_vul_Tenable_Scan** , Wird erstellt, um Scan-Metadaten zu speichern, die aus abgerufen wurden Tenable.io/Scans-Endpunkt. Dies umfasst Details wie Scan-ID, Name, Status, Startzeit, Endzeit, und Scan-Typ. • **Datenzuordnung** : Ein Referenzfeld wird zwischen erkannten Elementen (Konfigurationselementen oder Schwachstellen) und dem entsprechenden aktuellen Scan-Datensatz in eingerichtet **sn_vul_Tenable_Scan** Tabelle. Mit dieser Verknüpfung können Sie: ○ Zeigen Sie die neuesten Scan-Informationen an, die jedem erkannten Element zugeordnet sind. ○ Verbessern Sie den Kontext für Entscheidungen zur Selektierung und Korrektur von Schwachstellen. ○ Verbessern Sie die Auditierbarkeit und Berichterstellungsfunktionen, indem Sie einen Verlaufsdatensatz von Scan-Aktivitäten pflegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc Integrationen mit Vulnerability Response Anwendung

Die Tenable.sc Integrationen in Vulnerability Response Integration with Tenable Anwendung.

Beginnend mit Vulnerability Response V20.0: Wenn ein Asset von einem Service Desk-Mitarbeiter gescannt wird, wird in der Spalte „Agent vorhanden“ in der Liste „erkannte Elemente“ der Wert „wahr“ angezeigt. Dies gibt an, dass der Scan authentisch ist.

Liste von Tenable.sc Integrationen

Mehrere Quellen werden für alle unterstützt Tenable.io Und Tenable.sc Integrationen. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in hinzufügen und bereitstellen Vulnerability Response. Sie können auch installieren und konfigurieren Vulnerability Response Integration with Tenable Anwendung aus Setup-Assistent.

- Tenable.sc Ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn der verwendet wird Tenable.sc Produkt und Ihr ServiceNow AI Platform Instanz befindet sich in derselben Umgebung.
- Wenn Tenable.sc Produkt und Ihr ServiceNow AI Platform Instanz befindet sich nicht in derselben Umgebung, Sie müssen einen MID-Server verwenden.

Tenable.sc-Integrationen

Integration	Beschreibung
Tenable.sc Asset-Integration	Um die Erstellung doppelter erkannter Elemente mit importierten Asset-Daten zu vermeiden, wird die Asset-Integration von verwendet Tenable.sc Das Produkt besteht aus zwei Integrationen. **Die Tenable.scÖffnen Sie Die Asset-Integration** Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable berücksichtigt **Kumulativ** (Aktuell), oder **Öffnen** . Die angreifbaren Elemente (VIS), die in Ihrer Instanz mit diesen importierten Asset-Daten erstellt werden, gelten als offen, d. h. in **Öffnen** status. Diese angreifbaren Elemente erfordern eine Untersuchung und müssen möglicherweise behoben werden. **Die Tenable.sc Integration Von Anlagegütern** Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable berücksichtigt **Gemindert** (Nicht mehr angreifbar) oder **Behoben** . Die angreifbaren Elemente für diese Assets werden aus dem übergehen **Öffnen** status zu **Geschlossen/Behoben** status in Ihrer Instanz, da die Ergebnisse von Scans zeigen, dass sie nicht mehr angreifbar sind. • Ruft alle Asset-Daten aus dem ab Tenable.sc Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
	Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die eine IP-Adresse teilen. • Koordiniert die REST-Nachrichtenaufrufe an die Assets-API. • Die Ausgabe dieser Integration ist erkannte Elemente. • Der Tenable-Abfragefilter, den Sie im Setup-Assistenten auswählen, gilt auch für Tenable.sc Asset-Integration. Nur die Assets mit den Schwachstellen, die den Bedingungen des Abfragefilters entsprechen, werden importiert.
Tenable.sc Plugin-Integration	• Ruft die Plugin-Daten aus dem ab Tenable.sc Produkt. Abgerufene Daten basieren auf dem Datum, an dem die Plugins zuletzt von einem aktualisiert wurden Tenable.sc Integrationsausführung. • Dieser Import stellt sicher, dass die Tenable.sc Bezeichner (zehn IDs) sind aktuell, und nur aktive Schwachstellen werden importiert. • Koordiniert die REST-Nachrichtenaufrufe an die Plugins-API. • Die Ausgabe dieser Integration ist Schwachstellen von Drittparteien.
Tenable.sc Integration Behobener Schwachstellen	• Ruft Schwachstellendaten basierend auf Schweregradfiltern aus ab Tenable.sc Produkt und verarbeitet es in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich in befinden **Öffnen** Und **Erneut Geöffnet** status, da diese Datensätze eine Korrektur erfordern. Vorhandene angreifbare Elemente werden von Vulnerability Response aktualisiert, wenn Erkennungen sind **Behoben** , Aber angreifbare Elemente werden für nicht erstellt **Behoben** Erkennungen standardmäßig, da Tenable berücksichtigt **Behoben** Schwachstellen **Gemindert** . • Wenn die Kennzeichnung **Erstellen Sie Zeiten für Schwachstellen für Erkennungen behobener Schwachstellen** Ist im Setup-Assistenten aktiviert, erstellt es VIS in **Behoben** geben sie den status an, damit Sie Einblick in die Erkennungen haben, die sie erstellt haben. AS VIS werden für erstellt **Behoben** Erkennungen, die in Ihrer Instanz nicht vorhanden sind. Dies kann sich negativ auf Ihre Importleistung auswirken. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, damit dies möglich ist **Behoben** Erkennungen aktualisieren nur die status vorhandener angreifbarer Elemente. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
	Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die eine IP-Adresse teilen. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. Die Ausgabe dieser Integration ist **Geschlossen/Behoben** Angreifbare Elemente (VIS). Außerdem werden Assets und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind. Diese Integrationsausführung ist eine geplante Ausführung. Es handelt sich um eine verkettete Integration, was bedeutet, dass nach erfolgreichem Abschluss einer Ausführung die verwendet wird Tenable.sc„Integration offener Schwachstellen“, die als Nächstes beschrieben wird, wird ausgelöst. **Hinweis:** Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen.
Tenable.sc Integration Offener Schwachstellen	• Diese Integration wird nach erfolgreichem Abschluss von ausgelöst Tenable.sc Integration Behobener Schwachstellen. • Ruft Schwachstellendaten basierend auf den in ausgewählten Abfragefiltern ab Tenable.sc Produkt und verarbeitet es in Ihrer Instanz. • Erstellt entsprechende angreifbare Elemente für aktive Schwachstellen. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die eine IP-Adresse teilen. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration ist **Aktualisieren/ Neu erstellen** Angreifbare Elemente (VIS), wenn sie nicht vorhanden sind. Außerdem werden Konfigurationselemente und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind. **Hinweis:** Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
Tenable.sc Integration Von Anmeldeinformationen Scannen	• Diese Integration ruft die in konfigurierten Scan-Anmeldeinformationen ab Tenable.sc. • Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API. • Die Ausgabe dieser Integration ist Scan-Anmeldeinformationen, die in der Tabelle [sn_vul_Tenable_Scan_credential] ausgefüllt sind. • Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scananforderungen von initiiert werden ServiceNow AI Platform. • Diese Integration wird wöchentlich ausgeführt.

Tenable.sc Integration Von Schwachstellen Auffüllen	• Diese Backfill-Integration importiert alle offenen und behobenen Schwachstellen, die während eines Imports möglicherweise nicht berücksichtigt wurden.
	• Diese Integration importiert sowohl offene als auch behobene Schwachstellen aus den letzten sieben Tagen, um Ihre Erkennungen und angreifbaren Elemente zu aktualisieren.
	• Diese Integration kann sich auf Ihre Leistung auswirken.
	• Diese Integration ist standardmäßig inaktiv.
	• Um Ihre Schwachstellendaten zu aktualisieren und potenzielle Leistungsprobleme zu vermeiden, ziehen Sie es möglicherweise vor, die Tenable.sc-Integrationen für behobene Schwachstellen und offene Schwachstellenintegrationen so zu planen, dass sie ausgeführt werden, wenn keine anderen Scans ausgeführt werden.
	• Die Ausgabe dieser Integration lautet:
	  ○ **Geschlossen/Behoben** Angreifbare Elemente (VIS). Außerdem werden Assets und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind.
	  ○ Bis **Aktualisieren/Neu erstellen** Angreifbare Elemente (VIS), wenn sie nicht vorhanden sind. Außerdem werden Konfigurationselemente und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind.

Anwenderauthentifizierung und Tenable.sc

Die Anwenderauthentifizierung wird von unterstützt ServiceNow AI Platform® Instanz und Version 5,13 von Tenable.sc Produkt. Anwenderauthentifizierung ist erforderlich, wenn Sie Version 5,12 und früher von verwenden Tenable.sc Produkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie Anwenderauthentifizierung für auswählen Tenable.sc Integrationen, Token laufen möglicherweise ab und werden während der Integrationsausführungen ersetzt. In der Spalte Notizen im Datensatz Vulnerability Integration Run (VIN) wird die folgende Meldung für einen Prozess angezeigt, wenn ein Token abläuft: Fehler: Token-Validierung ist fehlgeschlagen . Wenn diese Nachricht angezeigt wird, ist keine Aktion erforderlich. Abgelaufene Token werden automatisch im Hintergrund aktualisiert, und die Meldung weist nicht auf eine Pause oder einen Fehler beim Integrationsprozess hin.

Tenable.cs Integrationen mit Vulnerability Response Und Container Vulnerability Response Anwendung

Die Tenable.cs Integrationen in Vulnerability Response Integration with Tenable-Anwendungen sind in Vulnerability Response und verfügbar Container Vulnerability Response Anwendungen.

Ab v20.0 Vulnerability Response, Wenn ein Asset von einem Service Desk-Mitarbeiter gescannt wird, wird in der Spalte „Service Desk-Mitarbeiter vorhanden“ in der Liste „erkannte Elemente“ „wahr“ angezeigt, was angibt, dass der Scan authentisch ist.

Liste von Tenable.cs Integrationen

Mehrere Quellen werden für alle unterstützt Tenable.io, Tenable.sc, Und Tenable.cs Integrationen. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in hinzufügen und bereitstellen Vulnerability Response. Sie können auch installieren und konfigurieren Vulnerability Response Integration with Tenable Anwendung aus Setup-Assistent.

Tenable.cs Ist eine cloudbasierte Enterprise-Integration. In der folgenden Tabelle finden Sie die Namen und Beschreibungen der unterstützten Integrationen für Tenable.cs Produkt.

Tenable.cs-Integrationen

Integration	Beschreibung
Tenable.cs Integration Von Cloud-Container-Assets	• Ruft alle Container-Asset-Daten aus dem ab Tenable.cs Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs. Koordiniert die REST-Nachrichtenaufrufe an die Asset-API. Die Ausgabe dieser Integration ist erkannte Container-Images, Docker-Images und Container-Repositorys.
Tenable.cs Öffnen Sie Die Integration Von Cloud-Container-Schwachstellen	Wenn diese Option aktiviert ist, wird diese Integration automatisch ausgeführt, nachdem die Integration der Container-Assets als Teil einer verketteten Integrationsausführung erfolgreich abgeschlossen wurde. • Ruft Container-Schwachstellendaten basierend auf den Schweregradfiltern aus ab Tenable.cs Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. Die Ausgabe dieser Integration ist neue/erneut geöffnete angreifbare Container-Elemente (CVIS). Wenn sie nicht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs-Integrationen (Fortsetzung)

Integration	Beschreibung
	vorhanden sind, werden auch erkannte Container-Images, Docker-Images, Container-Repositorys, Image-Ergebnisse, Drittparteieinträge erstellt. und Common Vulnerabilities and Exposures (CVE).
Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container	Diese Integration wird nach erfolgreichem Abschluss von ausgelöst Tenable.csÖffnen Sie Die Integration Von Cloud-Container-Schwachstellen. • Ruft Container-Schwachstellendaten basierend auf den Schweregradfiltern aus ab Tenable.cs Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. Die Ausgabe dieser Integration ist neue/erneut geöffnete angreifbare Container-Elemente (CVIS). Wenn sie nicht vorhanden sind, werden auch Discovery-Container-Images, Docker-Images, Container-Repositorys, Image-Ergebnisse, Drittparteieinträge erstellt. und CVEs. Bildergebnisse werden im Status „Geschlossen“ erstellt.
Tenable.cs Öffnen Sie Die Integration Von Cloud-Host-Schwachstellen	• Ruft Schwachstellendaten basierend auf den Schweregradfiltern aus ab Tenable.cs Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. Die Ausgabe dieser Integration ist neue/erneut geöffnete angreifbare Elemente (VIS). Wenn sie nicht vorhanden sind, werden auch Konfigurationselemente, Drittparteieinträge und CVEs erstellt. Schwachstellenerkennungen werden im Status „Offen“ erstellt.
Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen	Diese Integration wird nach erfolgreichem Abschluss von ausgelöst Tenable.csÖffnen Sie Die Integration Von Cloud-Host-Schwachstellen. • Ruft Schwachstellendaten basierend auf den Schweregradfiltern aus ab Tenable.cs Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs-Integrationen (Fortsetzung)

Integration	Beschreibung
	Die Ausgabe dieser Integration lautet „angreifbare Elemente schließen“ (VIS). Wenn sie nicht vorhanden sind, werden auch Konfigurationselemente, Drittparteieinträge und CVEs erstellt. Schwachstellenerkennungen werden im Status „Geschlossen“ erstellt.

Anwenderauthentifizierung und Tenable.sc

Die Anwenderauthentifizierung wird von unterstützt ServiceNow AI Platform® Instanz und Version 5,13 von Tenable.sc Produkt. Anwenderauthentifizierung ist erforderlich, wenn Sie Version 5,12 und früher von verwenden Tenable.sc Produkt.

Wenn Sie Anwenderauthentifizierung für auswählen Tenable.sc Integrationen, Token laufen möglicherweise ab und werden während der Integrationsausführungen ersetzt. In der Spalte Notizen im Datensatz Vulnerability Integration Run (VIN) wird die folgende Meldung für einen Prozess angezeigt, wenn ein Token abläuft: Fehler: Token-Validierung ist fehlgeschlagen . Wenn diese Nachricht angezeigt wird, ist keine Aktion erforderlich. Abgelaufene Token werden automatisch im Hintergrund aktualisiert, und die Meldung weist nicht auf eine Pause oder einen Fehler beim Integrationsprozess hin.

Vorbereitung auf die Tenable-Schwachstellenintegration

Bereiten Sie sich auf den vor ServiceNow® Tenable-Schwachstellenintegration durch Ausführen der folgenden Setup-Aufgaben.

Bevor Sie beginnen

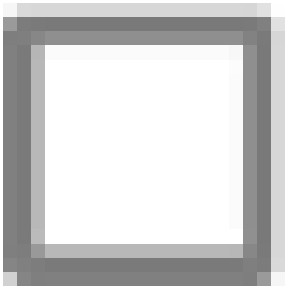
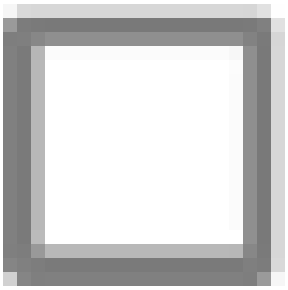
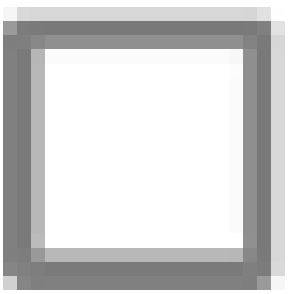
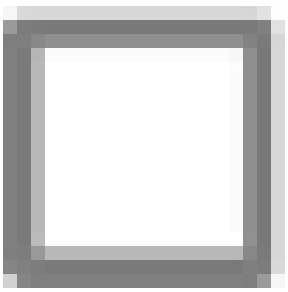
Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Für eine reibungslose Installation und Konfiguration von Vulnerability Response Integration with Tenable Anwendung möchten Sie möglicherweise die folgende Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Schwachstellendaten in importieren ServiceNow AI Platform® Instanz.

Hinweis:
Wenn Sie Daten mit der Tenable-Build-Integration importiert haben und mit der Verwendung von beginnen möchten ServiceNow® Vulnerability Response-Integration mit Tenable, siehe

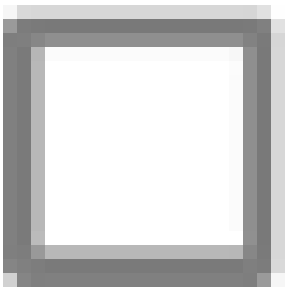
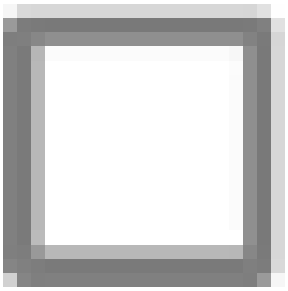
Für aktuelle Datenbereinigung und -Migration von der Tenable-Build-Integration zur von erstellten Integration ServiceNow, Siehe Richtlinien für die Migration von der Tenable Vulnerability Response-Integration zur ServiceNow Vulnerability Response-Integration mit Tenable [KB0960667] artikel.

Erforderliche Rolle: Administrator zum Herunterladen und Installieren der Anwendung.

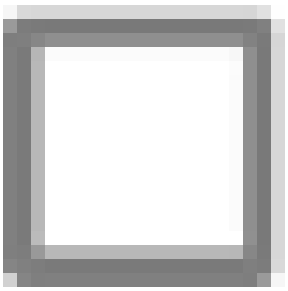
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	(Optional) wenn Sie nicht bereits installiert und aktiviert sind, möchten Sie möglicherweise installieren Vulnerability Response Anwendung vor der Installation der Drittanbieteranwendung. Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe, Vulnerability Response installieren. Diese Integration erfordert Version 12,1 von Vulnerability Response Oder später.
	Wenn Sie es noch nicht in Ihrer Instanz haben, rufen Sie Berechtigungen ab, und laden Sie herunter Vulnerability Response Integration with Tenable Anwendung für Ihren ServiceNow AI Platform® Instanz. Die Vulnerability Response Integration with Tenable Die Anwendung unterstützt Tenable.sc Produkt ab Version 5,13 Und Tenable.cs Produkt ab Version 5,0.1. .
	Schätzen Sie die Anzahl der angreifbaren Elemente, die Sie importieren möchten. Überprüfen Sie, ob Ihre Instanz die Anzahl der angreifbaren Elemente akzeptieren kann, die Sie importieren möchten. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an ServiceNow® Technischer Support.
	Stellen Sie sicher, dass Sie Gruppen oder Anwender haben, um die Integrationen zu verwalten und angreifbare Elemente zu korrigieren. **Administrator** Der Systemadministrator verwendet den Setup-Assistenten, um zu installieren Vulnerability Response Integration with Tenable Anwendung. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.Vulnerability_admin) und andere Rollen im Setup-Assistenten zu. **sn_vul.vulnerability_admin** Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der Tenable-Integrationen ab. Diese Rolle hat vollständigen Zugriff auf Vulnerability Response(VR)-Anwendung und ihre Datensätze. Konfiguriert alle VR-Anwendungen und -Regeln und konfiguriert Integrationen von Drittparteien. **sn_vul_Tenable.configure_Integration** Kann die Tenable-Schwachstellenintegration konfigurieren. Diese Rolle enthält die granulare Rolle sn_vul_Tenable.read_Integration. **sn_vul_Tenable.read_Integration**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Kann Datensätze der Tenable-Schwachstellenintegration anzeigen (lesen). **Vulnerability Response-Gruppe** Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Anwender, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen sn_vul.read_all und sn_vul.Remediation_owner automatisch. Der Systemadministrator führt die anfängliche Zuweisung von Rollen an Anwender und Gruppen im Setup-Assistenten für die Integration durch. Standardmäßig ist die Vulnerability Response-Gruppe verfügbar. Wenn Sie noch nicht erstellt haben, können Sie zusätzliche Gruppen erstellen und Anwender mit dem Modul „Anwenderverwaltung“ in Ihrer Instanz hinzufügen, bevor Sie den Setup-Assistenten verwenden. Siehe Erstellen Sie eine Anwendergruppe . Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender in der Vulnerability Response-Anwendung tun und sehen können. Informationen zur anfänglichen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.
	Um eine verbesserte Leistung für Ihren ersten Import heraufzustufen, sollten Sie möglicherweise bestimmte Funktionen, Regeln oder Aufträge in Ihrer Instanz deaktivieren. • Deaktivieren Sie Schwachstellen-Rechner, wenn Sie sie nicht verwenden. Diese Rechner sowie alle von Ihnen definierten Rechner werden jedes Mal ausgeführt, wenn ein Datensatz für angreifbare Elemente erstellt oder aktualisiert wird. Siehe Deaktivieren Sie Schwachstellen-Rechner . • Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung auswirkt. Vor dem ersten Import sollten Sie benachrichtigungsbezogene Geschäftsregeln deaktivieren, wie in beschrieben Importieren Sie Änderungen für die Tenable-Schwachstellenintegration.
	Stellen Sie sicher, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Aufträge in Ihrer Instanz aktiviert haben, die für die Integration erforderlich sind. • Tenable.sc Ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn der verwendet wird Vulnerability Response Integration with Tenable Produkt und Ihr ServiceNow AI Platform Instanz befindet sich in derselben Umgebung. Wenn Tenable.sc Produkt und Ihr ServiceNow AI Platform Instanz befindet sich nicht in derselben Umgebung, Sie müssen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	einen MID-Server verwenden. Weitere Informationen zu MID-Servern in Ihrer Instanz finden Sie unter MID-Server . • Überprüfen Sie, ob das IntegrationHub-Plugin installiert und aktiviert ist. Dieses Plugin ermöglicht es Basissystemkomponenten, externe Systeme mithilfe von Integrations-APIs aufzurufen, und aktiviert Protokollschritte wie REST. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** Und suchen Sie das Plugin. Wenn nicht in Ihrer Instanz installiert, installieren und aktivieren Sie sie.
	Tenable-Anmeldeinformationen abrufen. Stellen Sie sicher, dass Sie Accountnamen, Passwörter und andere Serviceinformationen haben, die für Ihre Tenable-Produkte erforderlich sind, damit Sie Zugriff darauf haben. Tenable.io Erfordert Administratorzugriff mit einem Berechtigungsattribut größer oder gleich 64. Tenable.sc Erfordert Sicherheitsanalysten oder -Manager-Zugriff. **Hinweis:** Ab v3.8 von Vulnerability Response Integration with Tenable, Zugriff auf Tenable.io Benötigt keine Administratorrechte mehr. Ein Standardanwender mit einem Berechtigungsattribut von 16 kann auch auf das Produkt zugreifen.

Sie sind bereit für Installieren Sie Vulnerability Response Integration with Tenable Anwendung mit Setup-Assistent.

Installieren Sie Vulnerability Response Integration with Tenable Anwendung mit Setup-Assistent

Bevor Sie ausführen ServiceNow® Tenable-Schwachstellenintegration müssen Sie herunterladen Vulnerability Response Integration with Tenable Anwendung aus dem ServiceNow Store Und installieren und konfigurieren Sie es mit dem Setup-Assistenten in Vulnerability Response Anwendung.

Vorbereitungen

Bevor Sie die Tenable-Anwendung installieren, überprüfen Sie, ob Sie alle Elemente in der Prüfliste in abgeschlossen haben Vorbereitung auf die Tenable-Schwachstellenintegration.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Erforderliche Rollen: administrator für die anfängliche Zuweisung der Rolle „sn_vul.Vulnerability_admin“ und die Installation der Tenable-Anwendung im Setup-Assistenten. Schwachstellenadministrator (sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet), um die Anwendung im Setup-Assistenten nach der Installation zu konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung**an.

   Nach einigen Minuten werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz verfügbar sind.

2. Suchen Sie nach **Tenable (Tenable-Plattform)** Kachel und klicken Sie auf **Installieren** .

   Mit dieser Aktion wird installiert Vulnerability Response Integration with Tenable Anwendung, die Sie aus heruntergeladen haben ServiceNow Store.

3. Befolgen Sie die Anweisungen im Setup-Assistenten, um mit der Installation fortzufahren.

4. Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.

Nächste Maßnahme

Nachdem Sie die Installation im Setup-Assistenten abgeschlossen haben, navigieren Sie zu **Integrationskonfiguration>Scannerintegrationen** In Setup-Assistent, um mit der Konfiguration fortzufahren. Weitere Informationen zur Ergänzung der im Setup-Assistenten bereitgestellten Hinweismeldungen finden Sie unter Konfigurieren Sie die Tenable-Schwachstellenintegration mit dem Setup-Assistenten.

Datenabrufeinstellungen für die Tenable-Schwachstellenintegration

Die folgenden Datenabrufeinstellungen helfen Ihnen, den Typ und den Umfang der Daten zu bestimmen, die Sie aus importieren möchten ServiceNow® Tenable-Schwachstellenintegration für Ihren ServiceNow AI Platform® Instanz.

Die in den folgenden Abschnitten beschriebenen Einstellungen helfen Ihnen, die Daten zu steuern, die Sie importieren möchten. Darüber hinaus können Sie die Werte dieser Filter in Integrationsinstanzen festlegen. Um Integrationsinstanzen anzuzeigen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Integrationsinstanzen** Und wählen Sie Ihre Integration aus, Tenable.io, Tenable.sc, Oder Tenable.cs.

Wählen Sie auf der angezeigten Seite „Integrationsinstanz“ die Integrationsinstanzparameter aus, um eine Liste von Parametern anzuzeigen, oder die Registerkarten Schwachstellenintegrationen für einen Zeitplan, REST-Details, Integrationsdetails, Datenquellen und Informationen zur Integrationsausführung.

Allgemeine Schweregrad- und Abrufeinstellungen und Filter für Tenable.io, Tenable.sc Und Tenable.cs In Ihrem ServiceNow AI Platform Instanz

Die folgenden Einstellungen sind für verfügbar Tenable.io, Tenable.sc, Und Tenable.cs Integrationen in Ihrem ServiceNow AI Platform Instanz. Diese und andere Konfigurationseinstellungen werden auf der Seite „Integrationsinstanz“ von angezeigt ServiceNow AI Platform Instanz. Möglicherweise möchten Sie diese Einstellungen für die ersten Integrationsausführungen in ihren Standardeinstellungen belassen.

Tenable.io

INSERT_fixed

Wenn Sie aktivieren **INSERT_fixed** Kennzeichnung im Setup-Assistenten für die Integration des Schwachstellenimports. Neue VIS werden für Erkennungen in erstellt **Behoben** status, der in Ihrer Instanz nicht vorhanden ist.

Schweregrad_Critical

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Filter ist standardmäßig aktiviert (wahr), um Schwachstellen mit Schweregrad „Kritisch“ von zu empfangen Tenable.ioÖffnen Sie Schwachstellen und Tenable.io Integrationen Behobener Schwachstellen.

Schweregrad_hoch

Dieser Filter ist standardmäßig aktiviert (wahr), um Schwachstellen mit hohem Schweregrad von zu empfangen Tenable.ioÖffnen Sie Schwachstellen und Tenable.io Integrationen Behobener Schwachstellen.

Schweregrad_Medium

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit mittlerem Schweregrad von zu empfangen Tenable.ioÖffnen Sie Schwachstellen und Tenable.io Integrationen Behobener Schwachstellen.

Schweregrad_Info

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit Schweregrad auf Informationsebene von zu erhalten Tenable.ioÖffnen Sie Schwachstellen und Tenable.io Integrationen Behobener Schwachstellen.

Schweregrad_niedrig

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit niedrigem Schweregrad von zu empfangen Tenable.ioÖffnen Sie Schwachstellen und Tenable.io Integrationen Behobener Schwachstellen.

size

Diese Einstellung definiert die Anzahl der Plugin-Datensätze, die in den Ergebnissatz von aufgenommen werden sollen Tenable.io Plugins-Integration. Muss im int32-Format vorliegen. Der Standardwert ist 1.000. Die maximale Größe beträgt 000.

num_Assets

Die maximale Anzahl von Schwachstellen pro exportiertem Block aus Tenable.io Schwachstellen behoben und Tenable.ioÖffnen Sie Schwachstellen-Integrationen. Der Standardwert beträgt 50.

chunk_size

Gibt die Anzahl der Assets pro exportiertem Block von an Tenable.io Asset-Integration. Der Standardwert ist 1.000.

Tenable.sc

Async_Request

Dieser Parameter ist standardmäßig inaktiv (falsch). Aktivieren oder deaktivieren Sie diesen Parameter, um asynchrone oder synchrone API-Aufrufe mit durchzuführen Tenable.sc Entsprechend. Wenn bei synchronen Anrufen eine Zeitüberschreitung von 30 Sekunden auftritt, wenden Sie sich an den Support für das Tenable-Produkt, um die Box zu optimieren. Dieser Parameter gilt nach der Aktivierung für alle Integrationen von Tenable.sc. Für Bestandskunden, die asynchrone Aufrufe verwenden, ist ein Korrekturskript verfügbar, das dem vorhandenen einen neuen Parameter „async_Request“ hinzufügt Tenable.sc Integrationsinstanzen. Um die Korrekturskripts anzuzeigen, navigieren Sie zu **Systemdefinition** > **Korrekturskripts**an.

INSERT_fixed

Wenn Sie aktivieren **INSERT_fixed** Kennzeichnung im Setup-Assistenten für die Integration des Schwachstellenimports. Neue VIS werden für Erkennungen in erstellt **Behoben** status, der in Ihrer Instanz nicht vorhanden ist.

Offset

Gibt die Anzahl der Assets, Plugins und Schwachstellen an, die in einer Integrationsausführung importiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abfragefilter

Abfragefilter werden in der Tenable-Konsole konfiguriert. Diese Abfragefilter haben IDs, die im Setup-Assistenten oder auf der Seite „Integrationsinstanzen“ in ausgewählt werden können ServiceNow AI Platform Instanz. Diese Filter werden beim Abrufen der Daten aus angewendet Tenable.sc Integrationen.

Tenable.cs

Compute_severity_Critical

Dieser Filter ist standardmäßig aktiviert (wahr), um Schwachstellen mit Schweregrad „Kritisch“ von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Host-Schwachstellen und Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen.

Compute_severity_High

Dieser Filter ist standardmäßig aktiviert (wahr), um Schwachstellen mit hohem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Host-Schwachstellen und Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen.

Compute_severity_Medium

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit mittlerem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Host-Schwachstellen und Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen.

Compute_severity_info

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit Schweregrad auf Informationsebene von zu erhalten Tenable.csÖffnen Sie die Integration von Cloud-Host-Schwachstellen und Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen.

Compute_severity_low

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit niedrigem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Host-Schwachstellen und Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen.

Container_severity_Critical

Dieser Filter ist standardmäßig aktiviert (wahr), um Container-Schwachstellen mit Schweregrad „Kritisch“ von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container.

Container_severity_High

Dieser Filter ist standardmäßig aktiviert (wahr), um Container-Schwachstellen mit hohem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container.

Container_severity_Medium

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Container-Schwachstellen mit mittlerem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container.

Container_Schweregrad_Info

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit Schweregrad auf Informationsebene von den Container-Schwachstellen von zu erhalten Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container.

Container_severity_low

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Container-Schwachstellen mit niedrigem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container.

Asset_page_limit

Diese Einstellung definiert die Anzahl der Container-Asset-Datensätze, die in den Ergebnissatz von aufgenommen werden sollen Tenable.cs Integration Von Cloud-Container-Assets. Der Standardwert ist 1.000. Die maximale Größe beträgt 1.000.

Vuln_page_limit

Diese Einstellung definiert die Anzahl der Schwachstellendatensätze, die in den Ergebnissatz von aufgenommen werden sollen Tenable.cs Integration Offener Cloud-Host-Schwachstellen, Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen, Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen, und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container. Der Standardwert ist 1.000. Die maximale Größe beträgt 000.

REST-Nachrichten für die Tenable-Schwachstellenintegration

Die ServiceNow® Tenable Vulnerability Integration REST-Nachrichten werden verwendet, um Aufrufe an die Tenable-API zu tätigen.

Tenable.io Asset-REST-Nachricht

Die Tenable.io Die Asset-REST-Nachricht ruft Asset-Informationen für ab Tenable.io Asset-Integration. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die an gestellten Anforderungen aus Tenable.io Dient zum Abrufen von Asset-Informationen. Der Exportauftrag für Assets wird mit den folgenden Filtern übermittelt:

- „Is_deleted“: Falsch
- „Is_license“: Wahr

Tenable.io Plugins-REST-Nachricht

Die Tenable.io DIE Plugins-REST-Nachricht ruft Plugin-Informationen für ab Tenable.io Plugin-Integration. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die an gestellten Anforderungen aus Tenable.io Zum Abrufen von Plugins-Informationen.

Tenable.io REST-Nachricht für Schwachstellen

Die Tenable.io DIE REST-Nachricht „Schwachstellen“ ruft Schwachstelleninformationen für offene und geschlossene Schwachstellen aus dem ab Tenable.io Schwachstellenintegration. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die an gestellten Anforderungen aus Tenable.io Zum Abrufen von Informationen zu Schwachstellen.

Tenable.sc fragt DIE REST-Nachricht ab

Die Rest-Nachricht Tenable.sc Queries ruft die Abfragefilterinformationen für die Tenable.sc Asset-Integration und Tenable.sc-Schwachstellenintegration ab, bei der der Abfragefilter konfiguriert ist.

Tenable.sc Plugins-REST-Nachricht

Die Tenable.sc Die Plugin-REST-Nachricht ruft Plugin-Informationen für ab Tenable.sc Plugins-Integration. Änderungen am Datensatz der REST-Nachricht „Plugins abrufen“ wirken sich auf die an gestellten Anforderungen aus Tenable.sc Zum Abrufen von Plugins-Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Wert	Beschreibung
type	aktiv	Gibt an, dass das Quell-Tenable Daten aus abruft. Verwendet von Code. Änderungen werden nicht empfohlen.
Felder	id, Beschreibung, cvssVector,cvssV3Vector, cvssV3TemporalVector, synopsis, cvssVector, baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, Name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, Familie, Risikofaktor, cpe, seeAlso, Lösung, exploitAvailable, exploitFrameworks, type, Copyright, Version, sourcefile, Abhängigkeiten, requidPorts, requidUDPPorts, srcPort, dstPort,Protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	Gibt die Liste der aus Tenable importierten Felder an.

Tenable.sc REST-Nachricht für Schwachstellen

Die Tenable.sc DIE REST-Nachricht „Schwachstellen“ ruft Schwachstelleninformationen aus dem ab Tenable.sc Integration. Änderungen an der REST-Nachricht „Schwachstellen abrufen“ oder „gepatchte Schwachstellen abrufen“ oder ab v14.0 Vulnerability Response Und v2.2 der Tenable-Schwachstellenintegration, Datensatz „Schwachstellen im Backfill abrufen“ wirkt sich auf die Anforderungen aus, an die gestellt wird Tenable.sc Zum Abrufen von Informationen zu Schwachstellen.

Tenable.sc REST-Nachricht „Anmeldeinformationen scannen“

Tenable.sc REST-Nachricht der Richtlinie

Die Tenable.sc Die POST-REST-Nachricht der Richtlinie fügt eine Richtlinie für angeforderte Plugins hinzu. Generierte Richtlinie wird in verwendet Tenable.sc Scan-Anforderungen.

Tenable.sc REST-Nachricht scannen

Die Nachricht Tenable.sc Scan NACH REST fügt einen Scan hinzu, der von dem Zugriff und der Berechtigung abhängig ist, die im Anforderungstext der Rest-Nachricht definiert sind. Es verwendet Richtlinie, Plugin-ID und IP(s) im Anforderungstext für die Scan-Anforderung.

Tenable.sc REST-Nachricht des Scan-Ergebnisses

Die Tenable.sc Die Meldung „Scan-Ergebnis ABRUFEN“ enthält Scan-Details des Scans, der mithilfe der Scan-REST-Nachricht generiert wurde. Es verwendet die scanResultId in der Antwort der Scan-REST-Nachrichten und ruft Scan-Details für den ausgelösten Scan ab.

Tenable.sc Scan-Anmeldeinformationen

Die Tenable.sc Die REST-Nachricht „Anmeldeinformationen scannen“ ruft die Anmeldeinformationen von ab Tenable.sc. Änderungen am Datensatz der REST-Nachricht mit der Methode „Import“ wirken sich auf die an gestellten Anforderungen aus Tenable.sc Zum Abrufen der Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Wert	Beschreibung
Felder	id,Name,Beschreibung,Typ	Gibt die Liste der aus importierten Felder an Tenable.sc
Filter	Verwendbar	Gibt an, dass die Integration nur nutzbare Anmeldeinformationen von abruft Tenable.sc Änderungen an einem der Parameter werden nicht empfohlen.

Tenable.cs GraphQL-REST-Nachricht: Die Tenable.cs Die GraphQL-REST-Nachricht ruft Container-Asset-Informationen, Host- und Container-Schwachstelleninformationen für ab Tenable.cs Integration. Änderungen am Datensatz der REST-Nachricht „Container-Assets abrufen“, „Container-Schwachstellen abrufen“, „Schwachstellen berechnen“ abrufen wirken sich auf die an gestellten Anforderungen aus Tenable.cs Zum Abrufen von Asset- und Schwachstelleninformationen.

Datentransformation für die Tenable-Schwachstellenintegration

Nachdem Sie die zu importierenden Daten identifiziert haben, werden sie aus dem Tenable-Produkt abgerufen und über eine Reihe von Datenquellen und Transformationen in Ihrer Instanz verarbeitet.

Während der Installation werden normalisierte Schweregradzuordnungen im Modul „normalisierte Schweregradzuordnung“ installiert. Diese Zuordnungen transformieren importierte Tenable-Schweregrade in Standardschweregrade zur Verarbeitung in Ihrer Instanz. Informationen zum Erstellen von Schweregradzuordnungen finden Sie unter Zuordnung des Schweregrads von Vulnerability Response erstellen in Vulnerability Response Dokumentation.

Tenable.io-Asset-Import

Importierte Asset-Daten werden zuerst in die Tabelle „Tenable.io-Asset-Import“ [sn_vul_Tenable_io_Asset_Import] geladen.

Die Transformationszuordnung Tenable.io Asset Integration wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Import von Tenable-Assets verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach Tenable.io-Asset-Transformation .

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Tenable.io Asset-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Tenable stellt eine eindeutige ID für Assets bereit und ordnet dem erkannten Elementdatensatz zu und wird für die CI-Suche verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io Asset-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_ipv4s	ip_address	Ordnet den ersten ip-Wert dem Feld ip_address im erkannten Elementdatensatz zu.
u_mac_address	mac_address	Ordnet den ersten mac_address-Wert dem mac-Adressfeld im erkannten Elementdatensatz zu.
u_fqdns	fqdn	Ordnet den ersten fqdn-Wert dem fqdn-Feld im erkannten Elementdatensatz zu.
u_netbios_names	netbios	Ordnet den ersten netbios-Wert dem Feld netbios im erkannten Elementdatensatz zu.
u_Operating_Systems	os	Ordnet den ersten BS-Wert dem Feld „betriebssystem“ im erkannten Elementdatensatz zu.
(Vor v14.0 Vulnerability Response Und v2.2 der Tenable-Schwachstellenintegration) u_Last_Scan_time	Last_Scan_date	Ordnet das Feld Last_Scan_date im erkannten Elementdatensatz zu.
u_Last_authenticated_Scan_date	Last_auth_Scan_date	Ordnet das Feld Last_auth_Scan_date im erkannten Elementdatensatz zu.
[Skript]	name	Ordnet den Hostnamen anhand der Logik des Skripts zu.
u_tags		Die Tags werden in sn_sec_cmn_Host_Tag gespeichert. Die Zuordnung von Tags zu Assets wird in sn_sec_cmn_m2m_src_ci_Tag gespeichert.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Tenable.io Asset-Transformationsskript für Zeitplan und Zweck der Zuordnung

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Initialisiert die Werte in Import_Set für den Integrationsprozess. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Aktualisiert Werte im Host und überprüft, ob der Host vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einem Import_Set. Dieses Skript ist zur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
	internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Legt die Werte von neu erstellten CIs und von CIs fest, die aktualisiert und ignoriert wurden.dieses Skript ist für die interne Verwendung vorgesehen, und das Ändern oder Löschen dieser CIs wird nicht empfohlen.

Tenable.io-Plugins-Integration

Die Transformationszuordnung Tenable.io-Plugins wird verwendet, um Plugins zu transformieren, die aus Tenable.io importiert wurden.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern die Verarbeitung von Daten, die von den Tenable-Plugins empfangen werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach der Tenable.io-Plugin-Transformation.

Die Nutzlast des Tenable.io-Plugins enthält alle Felder in der Spalte u_attributes der Tabelle „sn_vul_Tenable_io_Plugin_Import“. Das Attributfeld wird analysiert und den Datensätzen der Drittpartei-Eintragstabelle zugeordnet, wie in der folgenden Tabelle aufgeführt.

Quellenfeld	Zielfeld	Beschreibung
id	id	Ordnet die ID aus der Quelle zu und fügt ihr das TEN-Präfix hinzu. Wenn die empfangene ID beispielsweise 12345 lautet, lautet die ID in der Zieltabelle TEN-12345.
Beschreibung	Zusammenfassung	Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu.
[Skript]	Quelle	Die Quelle für den importierten Drittparteieintrag (TPE) ist Tenable.io.
[Skript]	Source_instance	Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert.
Familie	Kategorie	Ordnet die Familie des Plugins der Kategoriespalte zu
Plugin_Modification_date	Last_modified	Ordnet Plugin_modify_date dem Feld „zuletzt geändert“ zu.
Plugin_publication_date	date_published	Ordnet Plugin_publication_date dem Veröffentlichungsdatum zu.
Has_Patch	Remediation_type	Ordnet den Korrekturtyp aus dem Wert „has_Patch“ zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
synopsis	Bedrohung	Ordnet die Bedrohungsinformationen zu dieser Schwachstelle zu.
cvss_Base__Score	Punktzahl	Ordnet die Basispunktzahl des Common Vulnerability Scoring System (CVSS) der Punktzahlspalte in der Drittpartei-Eintragstabelle zu.
Lösung	Lösung	Ordnet die vom Scanner bereitgestellte Lösung der Lösungsspalte in der Drittpartei-Eintragstabelle zu.
Exploit_available	Exploit	Ordnet die vom Scanner bereitgestellte Exploit_available der Exploit-Spalte in der Drittpartei-Eintragstabelle zu.
vpr.Punktzahl	Source_Risk_Score	Ordnet die vom Scanner bereitgestellte vpr-Punktzahl der Tabelle „Source_Risk_Score“ in der Drittpartei-Eintragsdatei zu.
[Skript]	Source_Risk_Rating	Ordnet die vpr-Punktzahl der Standard-Risikobewertung basierend auf den Punktzahlbereichen zu: • 9–10: Kritisch • 7–9: Hoch • 4–7: Mittel • 0–4: Niedrig
vpr.Driver.age_of_vuln	Age_of_vuln	Ordnet das Alter der Schwachstelle vom Scanner der Spalte „age_of_vuln“ in der Tabelle „Drittpartei-Eintrag“ zu.
vpr.drivers.Exploit_Code_Reife	Exploit_Code_Reife	Ordnet die Exploit-Code-Reife vom Scanner Exploit_Code_Reife in der Drittpartei-Eintragstabelle zu.
vpr.drivers.product_coverage	Product_Coverage	Ordnet die Produktabdeckung vom Scanner zu „Product_Coverage“ in der Drittpartei-Eintragstabelle zu.
vpr.Treiber.Threat_sources_last28	Threat_sources	Ordnet Bedrohungsquellen der letzten 28 Tage vom Scanner den Threat_sources in der Drittpartei-Tabelle zu.
vpr.Treiber.Threat_Intensity_last28	Threat_Intensity	Ordnet die Bedrohungsintensität in den letzten 28 Tagen aus dem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		Scanner Threat_Intensity in der Drittpartei-Eintragstabelle zu.
vpr.Treiber.Threat_recency	Threat_recency	Ordnet die Bedrohungsaktualisierungsinformationen aus dem Scanner Threat_recency in der Drittpartei-Eintragstabelle zu.
vpr.drivers.cvss3_Impact_Score	V3_Impact_subscore	Ordnet die cvss3-Auswirkungspunktzahl der Spalte v3_impact_subscore in der Drittpartei-Eintragstabelle zu.
cvss_temporal_Punktzahl	cvss_temporal_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v2 zu.
cvss_v3_temporal_Score	V3_temporal_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v3 zu.
risk_factor	Source_severity	Wird dem Quellschweregrad in der Drittpartei-Eintragstabelle zugeordnet.
name	name	Ordnet den Namen des Plugins dem Namen in der Drittpartei-Eintragstabelle zu.
stig_severity	stig_severity	Ordnet die vom Scanner bereitgestellte vpr-Punktzahl der Quelle_Risk_Score in der Tabelle „Drittpartei-Eintrag“ zu.
Plugin_type	Check_type	Ordnet den Plugin-Typ Check_type in der Drittpartei-Eintragstabelle zu.
Nicht supported_by_Vendor	Nicht supported_by_Vendor	Ordnet das Feld nicht supported_by_Vendor der Spalte nicht supported_by_Vendor zu.
[Skript]	Exploit_Attack_Vector	Die Spalte „Exploit_Attack_Vector“ in der Drittpartei-Eintragstabelle wird basierend auf den Spalten „Exploit_available“ und „v3_Attack_Vector“ der ausgefüllt.

Zusätzlich zu den direkten Feldern werden anderen Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

Quellenfeld	Beschreibung
cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dieselben Common Vulnerabilities and Exposures (CVE) in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden werden, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie in sn_vul_m2m_entry_cve.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Beschreibung
bid	Die Liste der Fehlertraqs wird als Referenz hinzugefügt.
Siehe_auch	Die Liste der URLs wird als Referenz hinzugefügt.
xrefs	Die Liste der X-REF wird als Referenz hinzugefügt.
[Skript]	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das anwendbare Exploit-Framework und Plugin in sn_vul_m2m_Framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Initialisiert die Werte in Import_Set für den Integrationsprozess. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Aktualisiert die Werte im Drittparteieintrag und überprüft, ob der Drittparteieintrag vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einem Drittparteieintrag. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Legt die Werte der neu erstellten CIs und der CIs fest, die aktualisiert und ignoriert wurden. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Die Skripteinbindung TenableIOPluginsImportProcessor wird aus dem onBefore-Transformationsskript aufgerufen. Es verwendet die Ausgabe der Integration von Tenable.io-Plugins und wandelt sie in um ServiceNow AI Platform Einträge zu Schwachstellen von Drittparteien. Alle Änderungen an dieser Skripteinbindung können die Transformation von Tenable.io-Plugins-Daten in der Drittpartei-Eintragstabelle ändern.

Import von Tenable.io-Schwachstellen

Die Transformationszuordnung Tenable.io für angreifbare Elemente wird verwendet, um Informationen zu offenen und behobenen Schwachstellen zu transformieren, die aus Tenable.io importiert wurden.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import von Tenable-Schwachstellen verarbeitet werden.

Dieselbe Transformationszuordnung wird sowohl für die Tenable.io-Integration von behobenen Schwachstellen als auch für die Tenable.io-Integration offener Schwachstellen verwendet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach Transformationszuordnung für angreifbares Tenable.io-Element .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_Asset.uuID	id	UUID wird dem ID-Feld des cmdb_ci-Datensatzes zugeordnet.
u_Asset.ipv4	ip_address	Das Feld ipv4 wird dem ip-Adressfeld des cmdb_ci-Datensatzes zugeordnet.
u_Asset.Last_authenticated_results	Last_auth_Scan_date	Das Datum des letzten authentifizierten Scans wird dem Datum des letzten Authentifizierungsscans des cmdb_ci-Datensatzes zugeordnet.
u_Asset.mac_addess	mac_address	Die Mac-Adresse wird dem Feld „Host-mac-Adresse“ des cmdb_ci-Datensatzes zugeordnet.
u_asset.netbios_name	netbios	NetBIOS wird dem Feld netbios des Datensatzes „cmdb_ci“ zugeordnet.
u._Plugin.cvss3_Base_score	V3_Base_Score	Die CVSS v3-Basispunktzahl wird der v3-Basispunktzahl des Drittpartei-Eintragsdatensatzes zugeordnet.
u._Plugin.cvss3_temporal_Score	V3_temporal_Punktzahl	Die temporäre CVSS v3-Punktzahl wird der temporären v3-Punktzahl im Drittparteieintragsdatensatz zugeordnet.
u._Plugin.cvss_Base_Score	Punktzahl	CVSS-Basispunktzahl wird dem Punktzahlfeld des Drittparteieintragsdatensatzes zugeordnet.
u._Plugin.cvss_temporal_Score	Temporal_Punktzahl	Die temporäre Punktzahl wird der temporären Punktzahl im Drittparteieintragsdatensatz zugeordnet.
u_plugin.description	Zusammenfassung	Die Beschreibung wird dem Zusammenfassungsfeld im Drittparteieintragsdatensatz zugeordnet.
u_Plugin.family	Kategorie	Ordnet die Familie des Plugins der Kategoriespalte des Drittpartei-Eintragsdatensatzes zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_Plugin.Modification_date	Last_modified	Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Drittpartei-Eintragsdatensatz zugeordnet.
u_Plugin.publication_date	date_published	Das Veröffentlichungsdatum wird dem Feld Veröffentlichungsdatum des Drittpartei-Eintragsdatensatzes zugeordnet.
u_Plugin.Risk_factor	Source_severity	Der Risikofaktor wird dem Feld „Source_severity“ des Drittpartei-Eintragsdatensatzes zugeordnet.
u_Plugin.Lösung	Lösung	Die Lösung wird dem Lösungsfeld des Drittpartei-Eintragsdatensatzes zugeordnet.
u_Plugin.Synopse	Bedrohung	Die Synopse wird dem Bedrohungsfeld des Drittpartei-Eintragsdatensatzes zugeordnet.
u_Schweregrad_ID	Priorität	Priorität wird der Schweregrad-ID aus der Nutzlast zugeordnet. Der Standardwert ist 5.
u_Plugin.Exploit_available	Exploit	Ordnet die vom Scanner bereitgestellte Exploit_available der Exploit-Spalte in der Drittpartei-Eintragstabelle zu.
vpr.Punktzahl	Source_Risk_Score	Ordnet die vom Scanner bereitgestellte vpr-Punktzahl der Quelle_Risk_Score in der Tabelle „Drittpartei-Eintrag“ zu.
[Skript]	Source_Risk_Rating	Ordnet die vpr-Punktzahl der Standard-Risikobewertung basierend auf den Punktzahlbereichen zu: • 9–10: Kritisch • 7–9: Hoch • 4–7: Mittel • 0–4: Niedrig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_Plugin.vpr.drivers.age_of_vuln	Age_of_vuln	Ordnet das Alter der Schwachstelle aus dem Scanner Age_of_vuln in der Drittpartei-Eintragstabelle zu.
u_Plugin.vpr.drivers.Exploit_Code_Reife	Exploit_Code_Reife	Ordnet die Exploit-Code-Reife vom Scanner Exploit_Code_Reife in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.product_coverage	Product_Coverage	Ordnet die Produktabdeckung vom Scanner zu „Product_Coverage“ in der Drittpartei-Eintragstabelle zu.
u_Plugin.vpr.Treiber.Threat_sources_last28	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner Threat_sources in der Drittpartei-Eintragstabelle zu.
u_Plugin.vpr.Treiber.Threat_Intensity_last28	Threat_Intensity	Ordnet die Bedrohungsintensität in den letzten 28 Tagen aus dem Scanner Threat_Intensity in der Drittpartei-Eintragstabelle zu.
u_Plugin.vpr.Driver.Threat_recency	Threat_recency	Ordnet die Bedrohungsaktualisierungsinformationen aus dem Scanner Threat_recency in der Drittpartei-Eintragstabelle zu.
u_Plugin.vpr.drivers.cvss3_Impact_Score	V3_Impact_subscore	Ordnet die CVSS3 v3-Auswirkungspunktzahl der Spalte v3_Impact_subscore in der Drittpartei-Eintragstabelle zu.
u_Plugin.type	Check_type	Ordnet den Plugin-Typ Check_type in der Drittpartei-Eintragstabelle zu.
u_Plugin.Unsupported_by_Vendor	Nicht supported_by_Vendor	Ordnet das Feld nicht supported_by_Vendor im Plugin der Spalte nicht supported_by_Vendor zu.
[Skript]	Exploit_Attack_Vector	Die Spalte „Exploit_Attack_Vector“ in der Drittpartei-Eintragstabelle wird basierend auf den Spalten „Exploit_available“ und „v3_Attack_Vector“ der ausgefüllt.
u_Plugin.Family_ID	Family_ID	Ordnet die Plugin-Familien-ID der Spalte „Family_ID“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		in der Tabelle „Drittpartei-Eintrag“ zu.
port	port	Port wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.
protocol	protocol	Protokoll wird dem Protokollfeld des Datensatzes für angreifbare Elemente zugeordnet.
u_first_found	first_found	„Zuerst gefunden“ wird dem Feld „zuerst gefunden“ des Datensatzes des angreifbaren Elements zugeordnet.
u_Last_found	Last_found	„Zuletzt gefunden“ wird dem Feld „zuletzt gefunden“ des Datensatzes für angreifbare Elemente zugeordnet.
u_state	Status	Status wird dem Feld Status im Datensatz des angreifbaren Elements zugeordnet
[Skript]	Quelle	Die Quelle der Integration ist ausgefüllt. Die aus dieser Integration erstellten angreifbaren Elemente haben Tenable.io als Quelle.
[Skript]	Integration_instance	„Integration_instance“ ist der Name der Instanz, aus der das angreifbare Element importiert wird.
u_plugin.name	name	Ordnet den Namen des Plugins dem Namen in der Drittpartei-Eintragstabelle zu.
u_Plugin.stig_severity	stig_severity	Ordnet den stig-Schweregrad des Plugins der stig-Schweregrad-Spalte in der Drittpartei-Eintragstabelle zu

Zusätzlich zu den direkten Feldern werden anderen Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

Quellenfeld	Beschreibung
cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie in sn_vul_m2m_entry_cve.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Beschreibung
bid	Die Liste der Fehlertraqs wird als Referenz hinzugefügt.
Siehe_auch	Die Liste der URLs wird als Referenz hinzugefügt.
xrefs	Die Liste der X-REF wird als Referenz hinzugefügt.
[Skript]	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das anwendbare Exploit-Framework und Plugin in sn_vul_m2m_Framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Tenable-E/A-Schwachstellenprozessor löst aus, der mithilfe des Importsatzes Daten aus Tenable.io importiert und jeden Datensatz in die CMDB-CI-Tabelle, die Tabelle „angreifbare Elemente“ und die Tabelle „Schwachstellen“ von Drittanbietern lädt. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Überprüft, ob der Drittparteieintrag und die Erkennungen vorhanden sind. Wenn nicht, werden diese Datensätze in ihren jeweiligen Tabellen erstellt. isn’tDieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Aktualisiert die Anzahl der CIs, Vits und Erkennungen wie aus Tenable.io importiert. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Tenable.sc-Asset-Import

Asset-Daten, die aus Tenable.sc importiert wurden, werden zuerst in die Tabelle „Tenable.sc Asset-Import“ (sn_vul_Tenable_sc_Asset_Import) geladen. Die Transformationszuordnung Tenable.sc Asset Integration wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Import von Tenable-Assets verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach Tenable.sc Asset-Transformation .

Quellenfeld	Zielfeld	Beschreibung
u_uuid	id	Die UUID wird nicht aus der Tenable-API ausgefüllt, daher wird das Attribut „u_uniqueness“ verwendet, um ein eindeutiges UUID-Feld für Assets zu erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		und dem cmdb_ci-Datensatz zuzuordnen.
u_ip	ip_address	Ordnet das ip-Feld aus der API dem Feld ip_address in einem cmdb_ci-Datensatz zu.
u_macaddress	mac_address	Ordnet das mac-Adressfeld aus der API dem Adressfeld im cmdb_ci-Datensatz zu.
u_dnsname	fqdn	Ordnet das dnsname-Feld aus der API dem fqdn-Feld im cmdb_ci-Datensatz zu.
u_netbiosname	netbios	Ordnet das netbios-Feld aus der API dem netbios-Feld im cmdb_ci-Datensatz zu.
u_Oscpe	os	Die BS-Informationen werden aus dem Oszillosattribut in der Nutzlast extrahiert und dem Feld „betriebssystem“ im cmdb_ci-Datensatz zugeordnet.
u_lastauthrun	Last_auth_Scan_date	Ordnet das Feld lastauthrun aus der API dem Feld Last_auth_Scan_date im erkannten Elementdatensatz zu.
u_lastauthrun und u_lastunauthrun	Last_Scan_date	Der lastauthrun wird aus der Tenable-API oder lastunauthrun extrahiert. Das Feld Last_Scan_date im erkannten Elementdatensatz wird basierend auf dem Wert ausgefüllt, der in der Nutzlast angezeigt wird.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Initialisiert die Werte in Import_Set für den Integrationsprozess. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Aktualisiert die Werte im Host und überprüft, ob der Host vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einem Import_Set. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Legt die Werte der neu erstellten CIs und der CIs fest, die aktualisiert und ignoriert wurden. Dieses Skript

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
	ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Import von Tenable.sc-Plugins

Plugins-Daten, die aus Tenable.sc importiert werden, werden zuerst in die Tabelle „Plugins-Import“ (sn_vul_Table_sc_Plugin_Import) von Tenable.sc geladen. Die Tenable.sc-Plugin-Transformationszuordnung wird verwendet, um die importierten Plugin-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Plugin-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach Tenable.sc-Plugin-Transformationszuordnung .

Quellenfeld	Zielfeld	Beschreibung
u_id	id	Ordnet die ID aus der Quelle zu und fügt das TEN-Präfix hinzu. Wenn die empfangene ID beispielsweise 12345 lautet, lautet die ID in der Zieltabelle TEN-12345.
u_description	Zusammenfassung	Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu.
[Skript]	Quelle	Aus dieser Integration importierte TPE hat Tenable.sc als Quelle.
[Skript]	Source_instance	Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert.
u_Family	Kategorie	Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte zu.
u_Plugin_Modification_date	Last_modified	Ordnet Plugin_modify_date dem Feld „zuletzt geändert“ zu.
u_Plugin_publication_date	date_published	Ordnet Plugin_publication_date dem Veröffentlichungsdatum zu.
u_has_Patch	Remediation_type	Ordnet den Korrekturtyp aus dem Wert „has_Patch“ zu.
u_Synopse	Bedrohung	Ordnet die Bedrohungsinformationen zu dieser Schwachstelle zu.
u_cvss_Base_Score	Punktzahl	Ordnet die CVSS-Basispunktzahl der Punktzahlspalte in der Drittpartei-Eintragstabelle zu.
u_Solution	Lösung	Ordnet die vom Scanner bereitgestellte Lösung der Spalte „Lösung“ in der Tabelle „Drittpartei-Einträge“ zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_cvss_temporal_Punktzahl	cvss_temporal_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v2 zu.
u_cvss_v3_temporal_Score	V3_temporal_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v3 zu.
u_Risk_factor	Quellenschweregrad	Wird dem Quellschweregrad in der Drittpartei-Eintragstabelle zugeordnet.
u_cvss_v3_Base_Score	V3_Base_Score	Ordnet die CVSS-Basispunktzahl in der Drittpartei-Eintragstabelle zu.
u_Exploit_available	Exploit	Ordnet das vom Scanner bereitgestellte exploitAvailable der Exploit-Spalte in der Tabelle „Drittpartei-Eintrag“ zu.
u_vpr_Punktzahl	Source_Risk_Score	Ordnet die VPR-Punktzahl aus dem Scanner der Quell-Risikopunktzahl in der Drittpartei-Eintragstabelle zu.
[Skript]	Source_Risk_Rating	Ordnet die vpr-Punktzahl der Standard-Risikobewertung basierend auf den Punktzahlbereichen zu: • 9–10: Kritisch • 7–9: Hoch • 4–7: Mittel • 0–4: Niedrig
u_vpr_context[ID=age_of_vuln]	Age_of_vuln	Ordnet das Alter der Schwachstelle aus dem Scanner Age_of_vuln in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID=Exploit_Code_Reife]	Exploit_Code_Reife	Ordnet die Exploit-Code-Reife vom Scanner Exploit_Code_Reife in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID=Product_Coverage]	Product_Coverage	Ordnet die Produktabdeckung vom Scanner zu „Product_Coverage“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID="Threat_sources_last_28"]	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner zu Threat_sources in der Drittparteitabelle zu.
u_vpr_context[ID="Threat_Intensity_last_28"]	Threat_Intensity	Ordnet die Bedrohungsintensität in den letzten 28 Tagen aus dem Scanner Threat_Intensity in der Drittpartei-Eintragstabelle zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_vpr_context[ID=”Threat_recency”]	Threat_recency	Ordnet die Bedrohungsaktualisierungsinformationen aus dem Scanner Threat_recency in der Eintragstabelle des dritten Teils zu.
u_vpr_context[ID=cvssV3_impactScore]	V3_Impact_subscore	Ordnet die CVSS v3-Auswirkungsbewertung aus dem Scanner v3_impact_subscore in der Drittpartei-Eintragstabelle zu.
u_name	name	Ordnet den Namen des Plugins der Namensspalte in der Drittpartei-Eintragstabelle zu.
u_stig_severity	stig_severity	Ordnet das Feld „stig_severity“ im Plugin „stig_severity“ in der Drittpartei-Eintragstabelle zu.
u_Check_type	Check_type	Ordnet den Prüftyp Check_type in der Drittpartei-Eintragstabelle zu.
u_family.ID	Family_ID	Ordnet das Plugin „Family_ID“ der „family_ID“ in der Drittpartei-Eintragstabelle zu.
[Skript]	Exploit_Attack_Vector	Die Spalte „Exploit_Attack_Vector“ in der Drittpartei-Eintragstabelle wird basierend auf den Spalten „Exploit_available“ und „v3_Attack_Vector“ der ausgefüllt.

Zusätzlich zu den direkten Feldern werden anderen Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

Quellenfeld	Beschreibung
u_cpe	Die Liste der CPEs wird als Referenz hinzugefügt.
u_See_auch	Die Liste der URLs wird als Referenz hinzugefügt.
u_Exploit_Frameworks	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das anwendbare Exploit-Framework und Plugin in sn_vul_m2m_Framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Diese Transformation wird verwendet, um die Werte in Import_Set für den Integrationsprozess zu initialisieren. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Funktion, die verwendet wird, um die Werte im Drittparteieintrag zu aktualisieren und zu überprüfen, ob der Drittparteieintrag vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einem Drittparteieintrag. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Diese Transformation wird verwendet, um die Werte von Plugins festzulegen, die erstellt und ignoriert wurden. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Die Skripteinbindung TenableSCPluginsImportProcessor wird aus dem onBefore-Transformationsskript aufgerufen. Es übernimmt die Ausgabe aus der Plugin-Integration Tenable.sc und wandelt sie in um ServiceNow Einträge zu Schwachstellen von Drittparteien. Alle Änderungen an dieser Skripteinbindung können die Transformation von Tenable.sc-Plugins-Daten in der Drittpartei-Eintragstabelle ändern.

Import von Tenable.sc-Schwachstellen

Die Transformationszuordnung Tenable.sc offene Schwachstellen wird verwendet, um importierte Daten aus der Tenable.sc-Integration offener Schwachstellen zu transformieren, und die Transformationszuordnung Tenable.sc und behobene Schwachstellen werden verwendet, um importierte Daten aus der Tenable.sc-Integration für behobene Schwachstellen zu transformieren.

Hinweis:
Änderungen an diesen Transformationszuordnungen ändern, wie Daten aus dem Import von behobenen/offenen Tenable-Schwachstellen verarbeitet werden.

Um auf die Transformationszuordnungen Tenable.sc offene und behobene Schwachstellen zuzugreifen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationsinstanzen** > **Tenable.sc – Integration von behobenen/offenen Schwachstellen** > **Datenquellen** > **Tenable.sc offene/behobene Schwachstellen** > **Transformationen**an.

Quellenfeld	Zielfeld	Beschreibung
u_Pluginid	ID	Wird als Bezeichner für das Plugin verwendet. Dieses Feld ist der Plugin-ID im Drittpartei-Eintragsdatensatz zugeordnet.
u_risikofaktor	Source_severity	Dieses Feld ist Source_severity im Drittpartei-Eintragsdatensatz zugeordnet.
u_severity	Priorität	Das Prioritätsfeld wird dem Schweregrad zugeordnet. Der Standardwert ist 5.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_hasbeengemindert	Status	Wurde gemindert ist dem Statusfeld des Schwachstellendatensatzes zugeordnet. Für die Integration behobener Schwachstellen befinden sich alle VIS im Status „Geschlossen“.
u_ip	ip_address	Die IP-Adresse wird dem Host-ip-Feld der Tabelle „cmdb_ci“ zugeordnet.
u_Port	port	Port wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.
u_protocol	protocol	Das Protokoll wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.
u_firstSeen	first_found	Der erste sichtbare Wert wird dem Feld zuerst gefunden des VI-Datensatzes zugeordnet.
u_lastSeen	Last_found	Der zuletzt gesehene Wert wird dem Feld zuletzt gefunden des VI-Datensatzes zugeordnet.
u_exploitAvailable	Exploit	ExploitAvailable wird dem Exploit-Feld im Drittpartei-Eintragsdatensatz zugeordnet.
u_Synopse	Bedrohung	Die Synopse wird dem Bedrohungsfeld im Drittparteieintragsdatensatz zugeordnet.
u_description	Zusammenfassung	Die Beschreibung wird dem Zusammenfassungsfeld im Drittparteieintragsdatensatz zugeordnet.
u_Solution	Lösung	Die Lösung wird dem Lösungsfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_basescore	Punktzahl	BaseScore wird dem Punktzahlfeld im Drittparteieintragsdatensatz zugeordnet.
u_temporalScore	Temporal_Punktzahl	Die temporäre Punktzahl wird der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		temporären Punktzahl im Drittparteieintragsdatensatz zugeordnet.
u_cvssv3basescore	V3_Base_Score	Cvssv3basescore wird der v3-Basispunktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u_cvsstemporalPunktzahl	V3_temporal_Punktzahl	Die temporäre Cvssv3Punktzahl wird der temporären v3-Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u_Pluginpubdate	date_published	Das Veröffentlichungsdatum des Plugins wird dem Veröffentlichungsdatum des Plugins im Drittpartei-Eintragsdatensatz zugeordnet.
u_Pluginmoddate	Last_modified	Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Drittpartei-Eintragsdatensatz zugeordnet.
u_dnsname	fqdn	DnsName wird dem FQDN-Feld des cmdb_ci-Datensatzes zugeordnet.
u_macaddress	mac_address	MacAddress wird dem Feld „mac_address“ des Datensatzes „cmdb_ci“ zugeordnet.
u_netbiosName	netbios	NetbiosName wird dem Feld „NETBIOS“ des cmdb_ci-Datensatzes zugeordnet.
u_ip	ip	IP ist dem IP-Feld des cmdb_ci-Datensatzes zugeordnet.
hostUniqueness	uuid	Die Hosteindeutigkeit ist keinem Feld zugeordnet, wird jedoch verwendet, um die UUID für den Host zu bestimmen.
u_Family	Kategorie	Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		des Drittpartei-Eintragsdatensatzes zu.
u_plugintext	Nachweis	Plugin-Text wird dem Nachweis im tpe-Datensatz zugeordnet.
[Skript]	Quelle	Die Quelle der Integration ist ausgefüllt. Die aus dieser Integration erstellten angreifbaren Elemente haben Tenable.sc als Quelle.
[Skript}	Integration_instance	„Integration_instance“ ist der Name der Instanz, aus der das angreifbare Element importiert wird.
u_vpr_Punktzahl	Source_Risk_Score	Ordnet die VPR-Punktzahl aus dem Scanner der Quell-Risikopunktzahl in der Drittpartei-Eintragstabelle zu.
[Skript]	Source_Risk_Rating	Ordnet die vpr-Punktzahl der Standard-Risikobewertung basierend auf den Punktzahlbereichen zu: • 9 Bis 10: Kritisch • 7–9: Hoch • 4–7: Mittel • 0–4: Niedrig
u_vpr_context[ID=age_of_vuln]	Age_of_vuln	Ordnet das Alter der Schwachstelle aus dem Scanner Age_of_vuln in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID=Exploit_Code_Reife]	Exploit_Code_Reife	Ordnet die Exploit-Code-Reife vom Scanner Exploit_Code_Reife in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID=Product_Coverage]	Product_Coverage	Ordnet die Produktabdeckung vom Scanner zu „Product_Coverage“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID="Threat_sources_Last_28]	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		Tagen vom Scanner Threat_sources in der Drittparteitabelle zu.
u_vpr_context[ID="Threat_Intensity_Last_28]	Threat_Intensity	Ordnet die Bedrohungsintensität in den letzten 28 Tagen aus dem Scanner Threat_Intensity in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID=”Threat_recency”]	Threat_recency	Ordnet die Bedrohungsaktualisierungsinformationen aus dem Scanner Threat_recency in der Eintragstabelle des dritten Teils zu.
u_vpr_context[ID=cvssV3_impactScore]	V3_Impact_subscore	Ordnet die CVSS v3-Auswirkungsbewertung aus dem Scanner v3_impact_subscore in der Drittpartei-Eintragstabelle zu.
u_pluginname	name	Ordnet den Namen des Plugins der Namensspalte in der Eintragstabelle von Drittparteien zu.
u_stigseverity	stig_severity	Ordnet das Feld „stig_severity“ im Plugin „stig_severity“ in der Eintragstabelle von Drittparteien zu.
u_checktype	Check_type	Ordnet den Prüftyp Check_type in der Drittpartei-Eintragstabelle zu.
u_family.ID	Family_ID	Ordnet das Plugin „Family.ID“ der „family_ID“ in der Drittpartei-Eintragstabelle zu.
[Skript]	Exploit_Attack_Vector	Die Spalte „Exploit_Attack_Vector“ in der Tabelle „Third_Party_entry“ wird basierend auf den Spalten „Exploit_available“ und „v3_Attack_Vector“ ausgefüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Beschreibung
u_cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung befindet sich in sn_vul_m2m_entry_cve.
u_bid	Die Liste der Fehlertraqs wird als Referenz hinzugefügt.
u_cpe	Die Liste der CPEs wird als Referenz hinzugefügt.
u_seeauch	Die Liste der URLs wird als Referenz hinzugefügt.
u_xrefs	Die Liste der X-Referenzen wird als Referenz hinzugefügt.
u_exploitFrameworks	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das anwendbare Exploit-Framework und Plugin in sn_vul_m2m_Framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Diese Transformation wird verwendet, um die Werte in Import_Set für den Integrationsprozess zu initialisieren. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Funktion, die verwendet wird, um die Werte in der Schwachstelle zu aktualisieren und zu überprüfen, ob die Schwachstelle vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einer Tabelle für angreifbare Elemente. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Diese Transformation wird verwendet, um die Werte neuer erstellter VIS und von VIS festzulegen, die aktualisiert und ignoriert wurden. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Tenable.cs Container-Asset-Import

Importierte Asset-Daten werden zuerst in geladen Tenable.cs Container-Asset-Import [sn_vul_TENABLE_cs_Container_Asset_Import] Tabelle.

Die Tenable.cs Die Container-Asset-Transformationszuordnung wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem geändert werden Tenable.cs Container-Asset-Import wird verarbeitet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

System-Importsätze > Transformationszuordnungen. Suchen Sie nach Tenable.cs Container-Asset-Transformation.

In den folgenden Tabellen werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Tenable.cs Container-Asset-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_Digest	Image_ID	Tenable bietet einen eindeutigen Digest für die Container-Assets und ordnet dem erkannten Container-Image und dem Docker-Image-Datensatz zu und wird für die CI-Suche verwendet.
u_Digest	Image_Digest	Tenable bietet einen eindeutigen Digest für die Container-Assets und ordnet dem erkannten Container-Image und dem Docker-Image-Datensatz zu und wird für die CI-Suche verwendet.
u_name	name	Ordnet dem Namensfeld des Docker-Image-Datensatzes zu.
u_repositoryuri	name	Ordnet dem Container-Repository-Datensatz zu
u_repositoryuri	Repository	Ordnet dem erkannten Container-Image-Datensatz zu.
u_virtualMachines	Host_list	Ordnet dem erkannten Container-Image-Datensatz zu
u_Bezeichnungen	Image_Bezeichnungen	Ordnet den ersten BS-Wert dem bs-Feld des erkannten Elementdatensatzes zu.
u_Cluster	Image_Cluster	Ordnet dem erkannten Container-Image-Datensatz zu
u_imagetags	tags	Ordnet dem erkannten Container-Image-Datensatz zu
u_cloudProvider	Cloud_Provider	Ordnet dem erkannten Container-Image-Datensatz zu
u_accountid	Cloud_Account_IDs	Ordnet dem erkannten Container-Image-Datensatz zu
u_region	Cloud_Regions	Ordnet dem erkannten Container-Image-Datensatz zu
u_operatingsystem	os	Ordnet dem erkannten Container-Image-Datensatz zu
u_Scantime	Last_Scan_date	Ordnet dem erkannten Container-Image-Datensatz zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Tenable.cs Zeitplan und Zweck der Container-Asset-Transformationszuordnung

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Diese Transformation wird verwendet, um die Werte in Import_Set für den Integrationsprozess zu initialisieren. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Eine Funktion, mit der Werte im Host aktualisiert und überprüft werden, ob der Host vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einem Import_Set. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Diese Transformation wird verwendet, um die Werte von neu erstellten CIs und CIs festzulegen, die aktualisiert und ignoriert wurden. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Tenable.cs Import Von Container-Schwachstellen

Importierte Container-Schwachstellendaten werden zuerst in geladen Tenable.cs Container-Schwachstellenimport [sn_vul_TENABLE_cs_Container_vuln_Import] Tabelle.

Die Tenable.cs Die Container-Schwachstellen-Transformationszuordnung wird verwendet, um die importierten Container-Schwachstelleninformationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem geändert werden Tenable.cs Container-Schwachstellenimport wird verarbeitet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach Tenable.cs Container-Schwachstellen-Transformation.

In den folgenden Tabellen werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
[Skript]	Image_ID	Digest wird aus dem Feld „Resource.ID“ aus der API extrahiert und dem Feld „image_ID“ des erkannten Container-Image- und Docker-Image-Datensatzes zugeordnet.
[Skript]	Image_Digest	Digest wird aus dem Feld „Resource.ID“ aus der API extrahiert und dem Feld

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
		„image_Digest“ des erkannten Container-Image- und Docker-Image-Datensatzes zugeordnet.
[Skript]	name	Repository-Informationen werden aus dem Namensfeld extrahiert und dem Docker-Image- und Container-Repository-Datensatz zugeordnet.
[Skript]	Repository	Repository-Informationen werden aus dem Namensfeld extrahiert und zugeordnet, um den Container-Image-Datensatz zu erkennen.
u_resource.Bezeichnungen	Image_Bezeichnungen	Ordnet dem erkannten Container-Image-Datensatz zu
u_resource.CloudProvider	Cloud_Provider	Ordnet dem erkannten Container-Image-Datensatz zu
u_resource. AccountId	Cloud_Account_IDs	Ordnet dem erkannten Container-Image-Datensatz zu
u_resource.Region	Cloud_Regions	Ordnet dem erkannten Container-Image-Datensatz zu
u_Vulnerability. ID	id	Ordnet die ID aus der Quelle zu und fügt das TEN-Präfix hinzu. Wenn die empfangene ID beispielsweise 12345 lautet, lautet die ID in der Tabelle „Drittpartei-Eintrag“ TEN-12345.
u_Vulnerability. Beschreibungs-Id	Zusammenfassungs-ID	Wird dem Drittpartei-Eintragsdatensatz zugeordnet. Oder CVE-Datensatz.
u_Vulnerability.Schweregrad	v4_Base_severity	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.VprScore	Source_Risk_Score	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.VprSchweregrad	Source_severity	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.AttackVector	v4_Attack_Vector	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.ExploitReife	v4_Exploit_Reife	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
[Skript]	Quelle	Die Quelle für importierte TPE ist Tenable.cs.
u_Vulnerability.ID	name	Ordnet dem Datensatz der Schwachstellenreferenzen zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_Vulnerability. Links	URL	Ordnet dem Datensatz der Schwachstellenreferenzen zu
	Schwachstelle	Verweis auf TPE oder CVE im Datensatz der Schwachstellenreferenzen
u_Software.Name	name	Ist dem Container-Image-Paket-Datensatz zugeordnet
u_Software.Version	Version	Ist dem Container-Image-Paket-Datensatz zugeordnet
u_Software.Typ	Package_type	Ist dem Container-Image-Paket-Datensatz zugeordnet
u_softwarepfade	path	Ist dem Container-Image-Paket-Datensatz zugeordnet
u_gelöst	status	Ordnet dem Container-Image-Ergebnisdatensatz zu
u_firstscantime	first_found	Ordnet dem Container-Image-Ergebnisdatensatz zu
u_resource.ScanTime	Last_found	Ordnet dem Container-Image-Ergebnisdatensatz zu
u_Vulnerability.Description	Nachweis	Ordnet dem Container-Image-Ergebnisdatensatz zu
u_gelöst	Status	Ordnet dem Datensatz des angreifbaren Containerelements zu
u_firstscantime	first_found	Ordnet dem Datensatz des angreifbaren Containerelements zu
u_resource.ScanTime	Last_found	Ordnet dem Datensatz des angreifbaren Containerelements zu
[Skript]	Quelle	Die Quelle für den Datensatz des angreifbaren Containerelements ist Tenable.cs.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Tenable.cs Zeitplan und Zweck der Container-Schwachstellen-Transformationszuordnung

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Löst den TenableCS Container Vulnerabilities Processor aus, der Daten aus importiert Tenable.cs Mithilfe des Importsatzes und lädt jeden Datensatz in die CMDB-CI-Tabelle, die Tabelle „Angreifbares Element“, die Tabelle „Drittanbieter-Schwachstelleneintrag“, die Referenztabelle für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Zeitplan und Zweck der Container-Schwachstellen-Transformationszuordnung (Fortsetzung)

Wenn das Skript ausgeführt wird	Zweck
	Schwachstellen, das Container-Image-Paket, das Container-Image-Ergebnis und das angreifbare Container-Element. Das Ändern oder Löschen wird nicht empfohlen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist)	Überprüft, ob der Drittparteieintrag und die Bildergebnisse vorhanden sind. Wenn nicht, werden diese Datensätze in ihren jeweiligen Tabellen erstellt. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist)	Aktualisiert die Anzahl der CIs, Vits und Ergebnisse wie aus importiert Tenable.cs. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Tenable.cs Vulnerability-Import Berechnen

Importierte Host-Schwachstellendaten werden zuerst in geladen Tenable.cs Tabelle „Import von Compute-Schwachstellen“ [sn_vul_TENABLE_cs_Compute_vuln_Import].

Die Tenable.cs Die Transformationszuordnung „Schwachstellen berechnen“ wird verwendet, um die importierten Informationen zur Host-Schwachstelle zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem geändert werden Tenable.cs Import von Compute-Schwachstellen wird verarbeitet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **System-Importsätze**an. Suchen Sie nach Tenable.cs Transformation Für „Schwachstellen Berechnen“.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_resource.ID	object_id	Wird dem CMDB-CI-Datensatz zugeordnet.
u_resource.Name	name	Wird dem CMDB-CI-Datensatz zugeordnet.
	Asset_category	Cloud ist im erkannten Elementdatensatz als Asset-Kategorie zugeordnet.
U_resource.CloudProvider	Cloud_Service_Provider	Wird dem erkannten Elementdatensatz zugeordnet
u_resource.Region	Cloud_Region	Wird dem erkannten Elementdatensatz zugeordnet
u_resource.AccountId	cloud_account	Wird dem erkannten Elementdatensatz zugeordnet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_resource. CloudProvider	Cloud_resource_type	Wird dem erkannten Elementdatensatz zugeordnet
u_resource.ID	resource_id	Wird dem erkannten Elementdatensatz zugeordnet
u_resource.Name	resource_name	Wird dem erkannten Elementdatensatz zugeordnet
u_Vulnerability.ID	id	Ordnet die ID aus der Quelle zu und fügt das TEN-Präfix hinzu. Wenn die empfangene ID beispielsweise 12345 lautet, lautet die ID in der Tabelle „Drittpartei-Eintrag“ TEN-12345. Ordnet die ID auch CVEs zu.
u_Vulnerability. Beschreibung	Zusammenfassung	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.Schweregrad	v4_Base_severity	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.VprScore	Source_Risk_Score	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.VprSchweregrad	Source_severity	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.AttackVector	v4_Attack_Vector	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.ExploitReife	v4_Exploit_Reife	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
[Skript]	Quelle	Die Quelle für importierte TPE ist Tenable.cs.
u_Vulnerability.ID	name	Ordnet dem Datensatz der Schwachstellenreferenzen zu
u_Vulnerability.Links	URL	Ordnet dem Datensatz der Schwachstellenreferenzen zu
	Schwachstelle	Verweis auf TPE oder CVE im Datensatz der Schwachstellenreferenzen
u_gelöst	status	Ordnet dem Erkennungsdatensatz für angreifbare Elemente zu
u_firstscantime	first_found	Ordnet dem Erkennungsdatensatz für angreifbare Elemente zu
u_resource.ScanTime	Last_found	Ordnet dem Erkennungsdatensatz für angreifbare Elemente zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_softwarepfade	Nachweis	Ordnet dem Erkennungsdatensatz für angreifbare Elemente zu
u_softwareresolutionVersionen	Solution_Summary	Ordnet dem Erkennungsdatensatz für angreifbare Elemente zu
u_gelöst	Status	Ist dem Datensatz des angreifbaren Elements zugeordnet
u_firstscantime	first_found	Ist dem Datensatz des angreifbaren Elements zugeordnet
u_resource.ScanTime	Last_found	Ist dem Datensatz des angreifbaren Elements zugeordnet
[Skript]	Quelle	Die Quelle für den Datensatz für angreifbare Elemente ist Tenable.cs.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Tenable.cs Zeitplan und Zweck der Konvertierungszuordnung für „Schwachstellen berechnen“

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Löst Tenable CS Compute Vulnerabilities Processor aus, der Daten aus importiert Tenable.cs Mithilfe des Importsatzes und lädt jeden Datensatz in die CMDB-CI-Tabelle, die Tabelle „angreifbare Elemente“ und die Tabelle „Schwachstellen von Drittparteien“. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Überprüft, ob der Drittparteieintrag und die Erkennungen vorhanden sind. Wenn nicht, werden diese Datensätze in ihren jeweiligen Tabellen erstellt. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Aktualisiert die Anzahl der CIs, Vits und Erkennungen wie aus importiert Tenable.cs. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_Digest	Image_ID	Ein eindeutiger Digest, der von Tenable für die Container-Assets

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
		bereitgestellt wird. Er wird dem erkannten Container-Image und dem Docker-Image-Datensatz zugeordnet und für die CI-Suche verwendet.
u_name	name	Ordnet dem Namensfeld des Docker-Image-Datensatzes zu.

Legen Sie zusätzliche Filterparameter für fest Tenable.io Importe

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit an Tenable Vulnerability Integration Damit Sie die mit importierten Schwachstellendaten weiter verfeinern können Tenable.io Produkt.

Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, damit Sie nur bestimmte Schwachstellendetails überprüfen können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die gefiltert werden `cidr_range`, `num_assets`, `indexed_at`, Und `plugin_family`. Oder sagen Sie, Sie möchten eine ausführen Tenable.io Integration so, dass eine Ausführung alle vier Stunden nur kritische Schwachstellen importiert und eine andere alle 24 Stunden ausgeführt wird, um alle anderen nicht kritischen Schwachstellen abzurufen.

Um Ihnen beim Sammeln dieser Daten zu helfen, können Sie Tenable-unterstützte Parameter hinzufügen, damit Sie die spezifischen Schwachstellendetails importieren können, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder Codierung können Sie mit dieser Funktion Ihre HTTP-Anforderungsinformationen mit Tenable-Parametern in anpassen ServiceNow AI Platform. Folgendes Tenable.io Integrationen unterstützen das Filtern durch Bereitstellung von JSON-Inhalten im Anforderungstext:

- Asset-Integration
- Integration Von Behobenen Schwachstellen
- Integration Offener Schwachstellen

Sie sollten wissen, wie Sie verwenden JSON Zeichenfolgen für diese Funktion.

Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Suchen Sie die von unterstützten Parameter Tenable.io Produkt auf der Entwicklerwebsite, das Sie für Ihre Filterung verwenden möchten.

   Parameter und Werte, die Sie aus eingeben Tenable.io Produkte werden nur auf Integrationsinstanzebene unterstützt.

2. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**an.
3. Klicken Sie auf der Listenseite Tenable-Integrationen auf den Datensatz für Tenable.io Integration, die Sie öffnen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wenn die Registerkarte Tenable-REST-Methoden ausgewählt ist, klicken Sie auf das Informationssymbol (I) für REST-Methode gefolgt von **Öffnen Sie Den Datensatz** .
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Um den Datensatz zu bearbeiten, klicken Sie oben auf der Seite auf den Link in . um den Datensatz zu bearbeiten, klicken Sie auf **Hier** .
7. Geben Sie im Datensatz „REST-Methode“ im Feld Inhalt den JSON-Inhalt ein, den Sie als Teil des Anforderungstexts verwenden möchten.

   Beispielsweise können Sie den Schweregradparameter für importierte Schwachstellen als festlegen: `{"filters": {"severity": ["critical"]}}`Für Tenable.io Asset-Integration, sodass nur kritische Schwachstellen importiert werden (CVSS-Punktzahl von 10,0).

   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie unter Tenable.io Dokumentation für weitere Informationen zur Trennung der einzelnen Werte.
8. Klicken Sie auf **Aktualisieren**.

Tenable-Schwachstellenintegration – Berichterstellung

Zeigen Sie Berichte zu Schwachstellen und angreifbaren Elementen in an Vulnerability Response Dashboards.

Datenvisualisierungen in Vulnerability Response Arbeitsbereiche

Die Vulnerability Response Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie Ihren Korrekturfortschritt überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen, die aktualisiert werden, wenn sich Schwachstellendaten ändern. Siehe Vulnerability Response Arbeitsbereiche, Arbeitsbereich des Schwachstellenmanagers erkunden Und Arbeitsbereich für IT-Korrekturen erkunden Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen.

Vorherige Versionen von Vulnerability Response

Das Dashboard „Vulnerability Response-Übersicht“ (Vulnerability Management) bietet einen Überblick über Schwachstellen und angreifbare Elemente, sodass der Schwachstellenadministrator Problembereiche schnell erkennen kann. Mit dem Vulnerability Response-Remediation-Dashboard (Vulnerability Remediation) kann sich ein Korrekturspezialist auf die Korrekturaufgaben und angreifbaren Elemente konzentrieren, die er besitzt.

Weitere Informationen finden Sie unter Wird standardmäßig verwendet Vulnerability Response Dashboards.

Erforderliche Rolle: Korrekturbesitzer.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender in der Vulnerability Response-Anwendung tun und sehen können. Informationen zur anfänglichen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.

Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren Sie zum Anzeigen des Dashboards zu **Vulnerability Response** > **Korrekturübersicht**an.

Statusdiagramm der Integrationsausführung für die Tenable-Schwachstellenintegration

Das Modul Tenable-Integrationsausführungsstatus bietet Ihnen eine grafische Ansicht des Status von Tenable-Integrationsausführungen.

Zeigen Sie im Diagramm auf einen beliebigen Teil des Diagramms, um eine Zusammenfassung der für diesen Teil spezifischen Daten anzuzeigen. Wenn Sie auf ein Teil im Balkendiagramm klicken, wird eine Liste geöffnet, die detailliertere Informationen enthält.

Erforderliche Rolle: Schwachstellenadministrator.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender in der Vulnerability Response-Anwendung tun und sehen können. Informationen zur anfänglichen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.

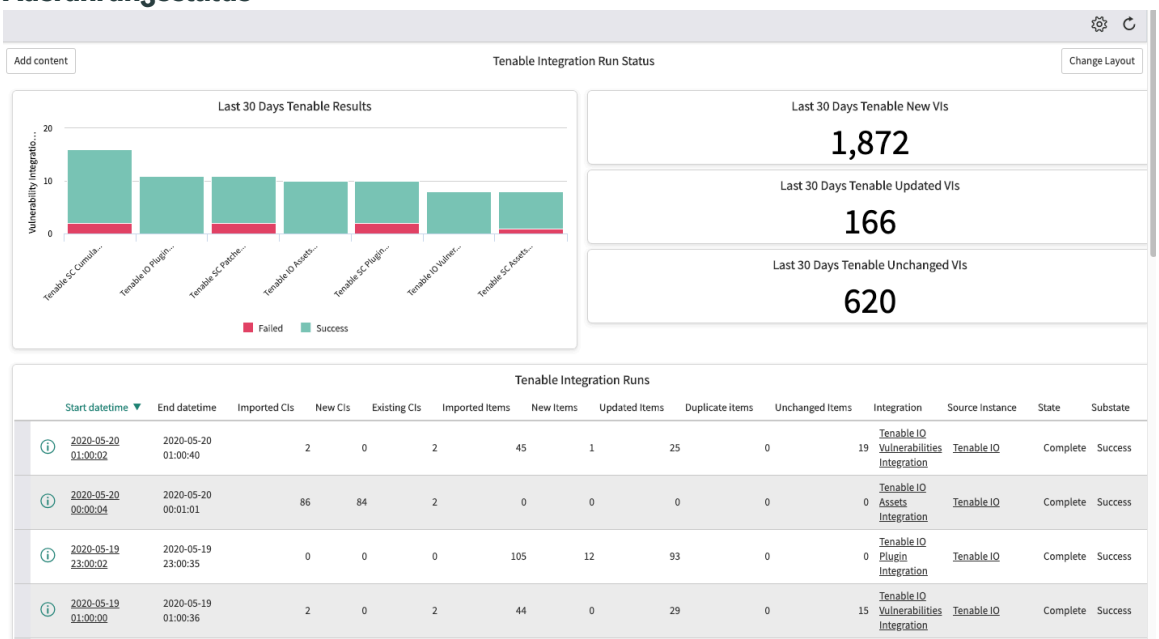
Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Um die Daten anzuzeigen, navigieren Sie zu **Alle** > **Tenable-Schwachstellen-Integration** > **Status der Integrationsausführung**an.

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard ist in der neuen Experience-UI verfügbar.

Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Ausführungsstatus



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

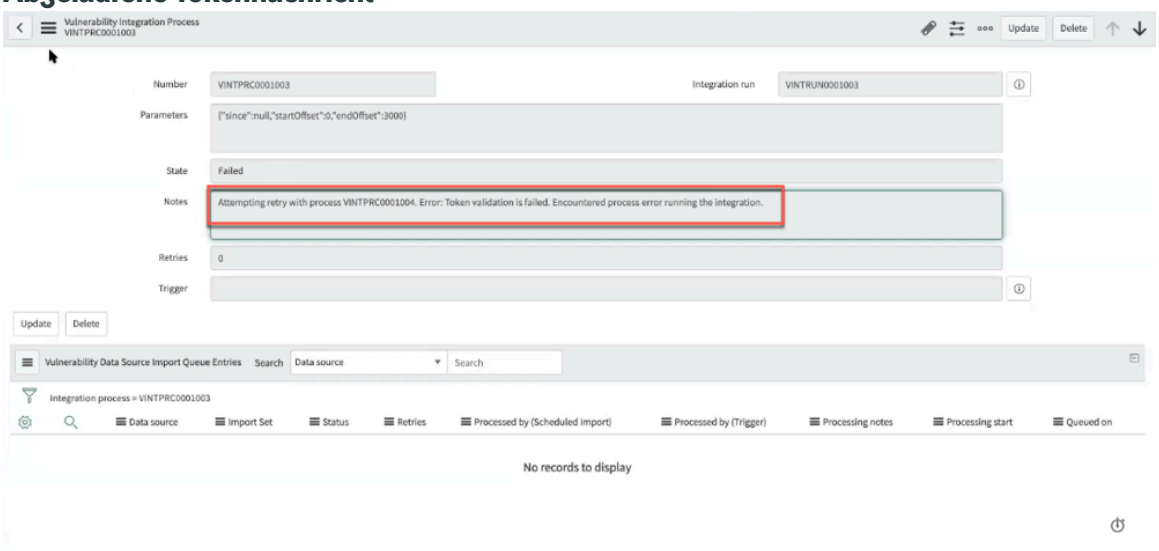
Statusdiagrammberichte der Tenable-Integrationsausführung

Name	Beschreibung
Tenable-Ergebnisse der letzten 30 Tage	Die Anzahl der für jede Integration abgeschlossenen Integrationsausführungen. Zeigt sowohl erfolgreiche als auch fehlgeschlagene Ausführungen an. Jede Ausführung wird als Balken im Diagramm angezeigt.
Neue Tenable-AEs der letzten 30 Tage	Die Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Aktualisierte Tenable-AEs der letzten 30 Tage	Die Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Unveränderte Tenable-AEs der letzten 30 Tage	Die Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Tenable-Integrationsausführungen	Die Datensätze der Integrationsausführung in einer Liste. **Hinweis:** **V16.1:** Um die Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit ServiceNow Erkennungsdaten in `sn_vul_detection`Tabelle. Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennung oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „bis datumsanzahl“ in der Instanz nach Abschluss der Integrationsausführung an.

Ablauf der Token-Validierung

Wenn eine Tenable.sc-Integrationsausführung aus irgendeinem Grund fehlschlägt, läuft das Authentifizierungstoken für Tenable.sc automatisch ab, und im Datensatz des Schwachstellenintegrationsprozesses wird eine Meldung angezeigt.

Abgelaufene Tokennachricht



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für den nächsten Integrationsprozess wird automatisch ein neues Token generiert. Alle Integrationsprozesse, fehlgeschlagen und erfolgreich, werden auf der Registerkarte Prozess der Schwachstellenintegration im Datensatz „Prozess der Schwachstellenintegration“ angezeigt.

Initiieren Sie einen erneuten Scan für Tenable.sc Integration

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen den geplanten Scanzyklen behoben wurden, indem Sie erneutes Scannen in der Tenable-Plattform initiieren. Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für initiieren Tenable.sc Produkt aus Ihrem ServiceNow AI Platform® Instanz.

Vorbereitungen

Erforderliche Rollen: sn_vul.write_all oder sn_vul.write_assigned

Hinweis:

Tenable.sc Unterstützt nicht das Starten eines erneuten Scans auf Agent-basierten Computern.

Vergewissern Sie sich, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**an.

Warum und wann dieser Vorgang ausgeführt wird

Informationen zum Initiieren eines erneuten Scans über die Arbeitsbereiche finden Sie unter Erneut Scannen Tenable.io Und Tenable.sc Angreifbare Elemente aus dem Vulnerability Response Arbeitsbereiche.

Führen Sie die unten aufgeführten Schritte aus, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

Um den Overhead und das Volumen für geplante, vollständige Scans, Korrekturbesitzer, IT-Spezialisten, Schwachstellenanalysten zu reduzieren, oder Schwachstellenmanager können bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen in Assets (Konfigurationselementen) in ihren Umgebungen initiieren. Sie können erneutes Scans aus angreifbaren Elementen (VI), Korrekturaufgaben (RT), Drittparteieinträgen (TPE) oder erkannten Elementdatensätzen aus Ihrem initiieren ServiceNow AI Platform Instanz.

Erneutes Durchsuchen erlauben Ihren Korrekturbesitzer und Schwachstellenanalysten Um sicherzustellen, dass Ihre Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben haben.

Beispielsweise wird Ihre gesamte Umgebung alle drei Wochen einmal gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, aber Sie haben gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Ihrem aus initiieren ServiceNow AI Platform Für Tenable.sc Angreifbare Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie einen erneuten Scan von Ihrem anfordern ServiceNow AI Platform® Instanz auswählen Vulnerability Response Integration with Tenable Anmeldeinformationen sind optional. Die ServiceNow® Tenable.sc Die Integration von Scan-Anmeldeinformationen importiert und aktualisiert Scanner-Anmeldeinformationen aus dem Tenable.sc Produkt in Ihrer Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationsdaten zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten. Die ServiceNow® Tenable.sc Integration von Scan-Anmeldeinformationen ist aktiviert (Aktiv) Automatisch aus dem Setup-Assistenten in Ihrer Instanz heraus, wenn Sie konfigurieren Tenable.sc Integrationen von Schwachstellen (Tenable.sc Integrationen offener und behobener Schwachstellen).

Beachten Sie die folgenden Informationen zu den Anmeldeinformationen, die Sie importieren, damit Ihre Anwender sie nach Bedarf von Ihrem aus sehen können ServiceNow AI Platform Instanz:

- Anmeldeinformationen, die mit erstellt wurden Tenable.sc Die Administratoranwenderrolle steht Anwendern in allen Ihren Organisationen zur Verfügung.
- Anmeldeinformationen, die mit erstellt wurden Tenable.sc Die Rolle „Organisationsanwender“ ist nur für Anwender innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden nicht in importiert ServiceNow AI Platform Für Anwender außerhalb der Organisation des Erstellers, es sei denn, sie sind für den Account des Anwenders freigegeben, der für die Verbindung mit der Instanz verwendet wird.

Siehe Tenable.sc Dokumentationswebsite für weitere Informationen.

Siehe Konfigurieren Sie die Tenable-Schwachstellenintegration mit dem Setup-Assistenten Weitere Informationen zum Konfigurieren von Tenable.sc Anwendung. Um weitere Informationen zur Integration von Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Alle** > **Tenable-Schwachstellen-Integration** > **Integrationen** > **Tenable.sc – Integration von Scan-Anmeldeinformationen**an.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- *sn_sec_cmn.record_threshold_heartbeat*: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- *sn_sec_cmn.maximum_heartbeat_delay*: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**an.
2. Suchen Sie den Datensatz des angreifbaren Elements, aus dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   Hinweis:
   Sie können erneutes Scannen für VIS nur mit initiieren Tenable.sc Als Quelle. Verifizieren Tenable.sc Wird in angezeigt **Quelle** Spalte in den VI-Listenansichten oder in **Quelle** Felder in einzelnen Datensätzen. Sie können den Bedingungsgenerator verwenden, um VIS nach Quelle zu gruppieren. Oder wenn die Spalte Quelle in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf **Liste Personalisieren** Symbol (Zahnradsymbol), und verwenden Sie zum Verschieben den Slushbucket **Quelle** Von **Verfügbar** Bis **Ausgewählt** .

3. Alternativ navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** Für die Korrekturaufgaben- bzw. Drittpartei-Eintragsdatensätze, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl, die **Erneut Scannen** Die Schaltfläche ist für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss das VI aus dem stammen Tenable.sc Produkt und in einem anderen Status als **Geschlossen** . Bei mehreren VI-Datensätzen müssen alle VIS aus dem Tenable.sc-Produkt stammen und einen anderen Status als aufweisen **Geschlossen** .
   - In einem RT-Datensatz kann sich die Korrekturaufgabe in einem anderen Status als befinden **Geschlossen** , Und alle zugeordneten VIS müssen aus dem stammen Tenable.sc Produkt.
   - In einem Drittpartei-Eintrag-Datensatz (TPE) muss der Datensatz mindestens einen zugehörigen VI-Datensatz aus dem aufweisen Tenable.sc Produkt in einem anderen Status als **Geschlossen** .

4. Klicken Sie oben rechts im Datensatz auf **Erneut Scannen** .
   Sie werden aufgefordert, die Scanner-Anmeldeinformationen auszuwählen, um auf den Scanner zuzugreifen. Dies sind die Anmeldeinformationen, die von importiert wurden Tenable.sc Integration Von Anmeldeinformationen Scannen.
5. Wählen Sie im Dialogfeld die gewünschten Filter und Anmeldeinformationstypen aus.
6. Klicken Sie Auf **Scan Anfordern** .

   Eine Nachricht wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird. Der Status für alle erneuten Scans kann jederzeit unter den zugehörigen Scan-Listen in den VI-, RT- und TPE-Datensätzen gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht auf **Zeigen Sie Details an** Zum Anzeigen des Status des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erneuten Scans und zum Anzeigen anderer erneutes Scans, die aus einem bestimmten Datensatz gestartet wurden.

Das Feld Status im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Das untergeordnete Element scannt Importdaten. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans.

Ihr ServiceNow AI Platform® Die Instanz verfolgt den Status des erneuten Scans, bis er erfolgreich abgeschlossen ist, oder bis der festgelegte Nachverfolgungszeitraum abgelaufen ist, je nachdem, was zuerst geschieht. Durch die Zeitüberschreitung wird der Scan nicht beendet. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, an dem der ServiceNow AI Platform® Die Nachverfolgung des Status des erneuten Scans wurde beendet, nicht wenn der tatsächliche erneute Scan beendet wurde. Alle VIS, die in übergegangen sind oder übergehen werden **Geschlossen/Behoben** Werden mit dem nächsten geplanten Import der Tenable.sc-Integration für behobene Schwachstellen importiert.

Initiieren Sie einen erneuten Scan für Tenable.io Integration

Überprüfen Sie, ob Ihre angreifbaren Elemente zwischen den geplanten Scanzyklen behoben wurden, indem Sie erneutes Scannen in der Tenable-Plattform initiieren. Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für initiieren Tenable.io Produkt aus Ihrem ServiceNow AI Platform® Instanz.

Vorbereitungen

Erforderliche Rollen: sn_vul.write_all oder sn_vul.write_assigned

Vergewissern Sie sich, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**an.

Warum und wann dieser Vorgang ausgeführt wird

- Siehe und Scannen Sie Datensätze und Korrekturaufgaben in erneut Arbeitsbereich des Schwachstellenmanagers Und Scannen Sie angreifbare Elemente und Korrekturaufgaben in erneut Arbeitsbereich für IT-Korrekturen Dient zum Initiieren eines erneuten Scans in den Vulnerability Response-Arbeitsbereichen.
- Führen Sie die unten aufgeführten Schritte aus, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

Hinweis:
Tenable.io Unterstützt nicht das Starten eines erneuten Scans auf Agent-basierten Computern.

Um den Overhead und das Volumen geplanter, vollständiger Scans zu reduzieren, können Sie als Korrekturbesitzer, IT-Spezialist, Schwachstellenanalyst oder Schwachstellenmanager bei Bedarf gezielte erneute Scans initiieren. Sie können in Ihren Umgebungen nach bestimmten Schwachstellen für Assets (Konfigurationselemente) suchen. Sie können erneutes Scannen aus Datensätzen für angreifbare Elemente (VI), Korrekturaufgaben (VUL), Drittparteieintrag (TPE) oder erkannte Elemente (SDI) von Ihrem initiieren ServiceNow AI Platform Instanz. Durch erneutes Scannen können Sie verifizieren, ob Ihre Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie einen erneuten Scan von Ihrem anfordern ServiceNow AI Platform® Instanz auswählen Vulnerability Response Integration with Tenable Anmeldeinformationen sind optional. Die ServiceNow® Tenable.io Die Integration von Scan-Anmeldeinformationen importiert und aktualisiert Scanner-Anmeldeinformationen aus dem Tenable.io Produkt in Ihrer Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationsdaten zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten.

Die folgenden Informationen beschreiben die Anmeldeinformationen, die Sie importieren, damit Ihre Anwender sie nach Bedarf von Ihrem aus sehen können ServiceNow AI Platform Instanz:

- Anmeldeinformationen, die mit erstellt wurden Tenable.io Die Administratoranwenderrolle steht Anwendern in allen Ihren Organisationen zur Verfügung.
- Anmeldeinformationen, die mit erstellt wurden Tenable.io Die Rolle „Organisationsanwender“ ist nur für Anwender innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden nicht in importiert ServiceNow AI Platform Für Anwender außerhalb der Organisation des Erstellers, es sei denn, sie sind für den Account des Anwenders freigegeben, der für die Verbindung mit der Instanz verwendet wird.

  Siehe Tenable.io Dokumentationswebsite für weitere Informationen.

- Die Tenable.io Vorlagenintegration und Tenable.io Die Integration von Scan-Anmeldeinformationen muss aktiviert werden, bevor erneute Scans initiiert werden. Um weitere Informationen zur Integration von Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Integrationen** > **Tenable.io-Scan-Anmeldeinformationsintegration**an.

  Standardmäßig sind die Integrationen für Vorlagen und Scan-Anmeldeinformationen deaktiviert. Wenn Sie Ihre Anmeldeinformationen für eingeben Tenable.io, Alle Tenable.io Integrationen werden automatisch aktiviert. So aktivieren oder deaktivieren Sie diese Integrationen manuell:

  1. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**an.
  2. Suchen Sie in der angezeigten Liste nach Tenable.io Gewünschte Integrationsdatensätze.
  3. Öffnen Sie jeden Datensatz, und wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren der Integration.
  4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
  5. Kehren Sie zum Setup-Assistenten zurück, um mit Ihrer Konfiguration für fortzufahren Tenable Vulnerability Integration Mit Vulnerability Response.

Siehe Konfigurieren Sie die Tenable-Schwachstellenintegration mit dem Setup-Assistenten Weitere Informationen zum Konfigurieren von Tenable.io Und Tenable.sc Produkte.

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen einmal gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, aber Sie haben gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Ihrem aus initiieren ServiceNow AI Platform Für Tenable.io Angreifbare Elemente.

Sie können aktualisierte Ergebnisse in den Datensätzen anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration von behobenen Schwachstellen initiiert haben.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**an.
2. Suchen Sie den Datensatz des angreifbaren Elements, aus dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   Hinweis:
   Wenn Sie verwenden Tenable.io Scanner, können Sie nur mit erneutes Scannen für VIS initiieren Tenable.io Als Quelle. Verifizieren Tenable.io Wird in angezeigt **Quelle** Spalte in den VI-Listenansichten oder in **Quelle** Felder in einzelnen Datensätzen. Sie können den Bedingungsgenerator verwenden, um VIS nach Quelle zu gruppieren. Oder wenn die Spalte Quelle in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf **Liste Personalisieren** Symbol (Zahnradsymbol), und verwenden Sie zum Verschieben den Slushbucket **Quelle** Von **Verfügbar** Bis **Ausgewählt** .

3. Alternativ navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** Für die Datensätze, die Sie für den erneuten Scan verwenden möchten.

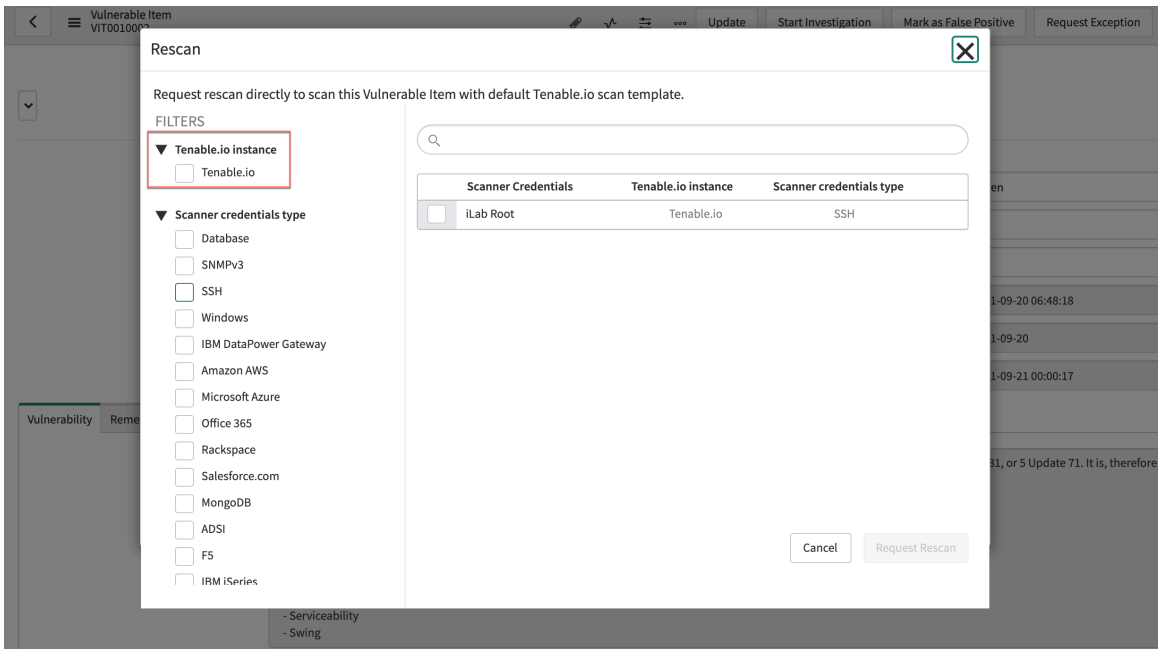
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängig von Ihrer Auswahl, die **Erneut Scannen** Die Schaltfläche ist für die folgenden Datensätze verfügbar:

- In einem einzelnen VI-Datensatz muss sich das VI in einem anderen Status als befinden **Geschlossen** . Bei mehreren VI-Datensätzen müssen alle VIS aus dem stammen Tenable.io Produkt und in einem anderen Status als **Geschlossen** .
- Für Korrekturaufgabendatensätze nur Korrekturaufgaben in einem anderen Status als **Geschlossen** Werden unterstützt. Alle zugeordneten VIS müssen sich in einem anderen Status als befinden **Geschlossen** Und verwenden Tenable.io Als Quelle.
- In einem Drittpartei-Eintrag-Datensatz (TPE) muss der Datensatz mindestens einen zugehörigen VI-Datensatz aus dem aufweisen Tenable.io Produkt in einem anderen Status als **Geschlossen** .
- Bei Datensätzen erkannter Elemente muss dem Datensatz mindestens ein VI-Datensatz aus dem zugeordnet sein Tenable.io Produkt in einem anderen Status als **Geschlossen** .
- In der Liste angreifbare Elemente können Sie einzelne angreifbare Elemente auswählen, die Sie erneut scannen möchten. Verwenden Sie das Menü Aktionen für ausgewählte Zeilen unten links im Bildschirm, um den erneuten Scan zu starten. Sie werden aufgefordert, Ihre Anmeldeinformationen einzugeben.

4. Klicken Sie oben rechts in einem Datensatz auf **Erneut Scannen** .
   Sie werden aufgefordert, die Instanz oder Instanzen für den erneuten Scan und die Scanner-Anmeldeinformationen auszuwählen, die Sie für den Zugriff auf den Scanner verwenden möchten. Die angezeigten Anmeldeinformationen sind die, die von importiert wurden Tenable.io Integration Von Anmeldeinformationen Scannen.
5. Wählen Sie im Dialogfeld die Instanz und/oder Instanzen und die Anmeldeinformationstypen aus, die Sie verwenden möchten.

   Im folgenden Bild eine Integrationsinstanz, Tenable.io Wird angezeigt. Wenn Sie mehr als einen haben Tenable.io-Instanz werden sie alle unter angezeigt Tenable.io Abschnitt im Formular.



6. Klicken Sie Auf **Erneutes Scannen Anfordern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Meldung wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird und ein übergeordneter Scan-Datensatz erstellt wird. Der Status für alle untergeordneten Scans kann jederzeit unter den zugehörigen Scan-Listen in den VI-, Korrekturaufgabe-, TPE- und SDI-Datensätzen gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht auf **Zeigen Sie Details an** Zum Anzeigen des Status des erneuten Scans und zum Anzeigen anderer erneutes Scans, die aus einem bestimmten Datensatz gestartet wurden.

Das Feld Status im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Das untergeordnete Element scannt Importdaten. Jeder Scan unterstützt eine eindeutige Kombination aus Integrationsinstanz, TPE, IP und Netzwerk-ID. Möglicherweise werden mehrere untergeordnete Scans in einem übergeordneten Scan-Datensatz angezeigt. Beispielsweise beträgt die maximale Anzahl von IP-Adressen, die ein untergeordneter Scan unterstützen kann, 1000. Wenn für ein angreifbares Element 1002 IPs vorhanden sind, werden zwei untergeordnete Scans erstellt und in der zugehörigen Liste „Scans“ aufgeführt, um die Anforderung zu unterstützen. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans, und sein Status spiegelt den Status der untergeordneten Scans wider.

Ihr ServiceNow AI Platform® Die Instanz verfolgt den Status des erneuten Scans, bis er erfolgreich abgeschlossen ist, oder bis der festgelegte Nachverfolgungszeitraum abgelaufen ist, je nachdem, was zuerst geschieht. Durch die Zeitüberschreitung wird der Scan nicht beendet. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, an dem der ServiceNow AI Platform® Die Nachverfolgung des Status des erneuten Scans wurde beendet, nicht wenn der tatsächliche erneute Scan beendet wurde. Alle VIS, die in übergegangen sind oder übergehen werden **Geschlossen/Behoben** Werden mit dem nächsten geplanten Import von importiert Tenable.io Integration Behobener Schwachstellen.

Für Scans, die fehlerhaft sind, können Sie die untergeordneten Scans im übergeordneten Scan-Datensatz überprüfen. Zeigen Sie den Fehler in der Antwortnutzlast des untergeordneten Scans an.

Sie können aktualisierte Ergebnisse in den Datensätzen anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration von behobenen Schwachstellen initiiert haben.

Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartition-Bezeichner für Tenable Vulnerability Integration

Erstellen Sie eindeutige Konfigurationselemente (Configuration Items, CIs) für Assets in Ihrer Umgebung, die IP-Adressen teilen. Identifizieren Sie die eindeutigen Assets in Ihrer Umgebung, und aktualisieren Sie die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen automatisch, um Ihnen weitere Details zu Ihren Schwachstellen zu geben.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig in Vulnerability Response Anwendung. Eine Möglichkeit, Ihre Assets zu identifizieren, ist die IP-Adresse. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, werden jedoch als ein CI in Ihrer CMDB gespeichert.

Wie in den folgenden Tabellen dargestellt, können mehrere Assets (CI) in Ihrer Umgebung IP-Adressen teilen, haben jedoch eindeutige Netzwerk- und Repository-IDs. Standardmäßig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden diese Assets jedoch als einzelnes CI identifiziert und gespeichert (CI 1) Während der IP-Adresssuche.

Standard-IP-Suche und CI-Erstellung

Quelle	IP-Adresse	Netzwerk_ID	Konfigurationselement
Tenable.io: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Quelle	IP-Adresse	Repository_ID	Konfigurationselement
Tenable.sc: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Sie können einzelne CIs für Assets mit derselben IP-Adresse erstellen, um sie als eindeutige Assets zu identifizieren. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartition-Bezeichners [Network_Partition_Identifier], indem Sie die geplante Aufgabe ausführen. *`Update existing discovered items with network partition identifier`*.

Diese geplante Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Assets und die Integrationen für behobene und offene Schwachstellen für Tenable.io Und Tenable.sc Produkte im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.

Wenn diese geplante Aufgabe aktiviert ist, wird der Netzwerkpartition-Bezeichner [Network_Partition_Identifier] zu vorhandenen CI-Datensätzen aus importierten Daten hinzugefügt. Vorhandene CIs, die von der IRE erstellt wurden, werden ebenfalls aktualisiert. Die geplante Aufgabe erstellt auch CIs, die ab dem nächsten Import den Netzwerkpartition-Bezeichner enthalten. Alternativ können Sie den Auftrag bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

Wenn Sie ein Upgrade ab v14.0 von durchführen Vulnerability Response Und v2.2 der Tenable-Schwachstellenintegration, der CMDB-CI-Klassenmodelle (1,0.21.) Wird unterstützt. Die Klassenmodelle haben den Netzwerkpartition-Bezeichner [Network_Partition_Identifier] in den Identifizierungsregeln für Identification and Reconciliation (IRE).

Option	Beschreibung
Führen Sie die geplanten Aufgaben bei Bedarf aus.	Aktualisieren Sie Ihre vorhandenen erkannten Elemente. CIs für Ihre vorhandenen Tenable-Daten werden erstellt oder aktualisiert, um die Granularität des Netzwerkpartition-Bezeichners einzubeziehen. Erkannte Elemente, angreifbare Elemente und Erkennungsdatensätze werden alle mit den neuen CIs aktualisiert.

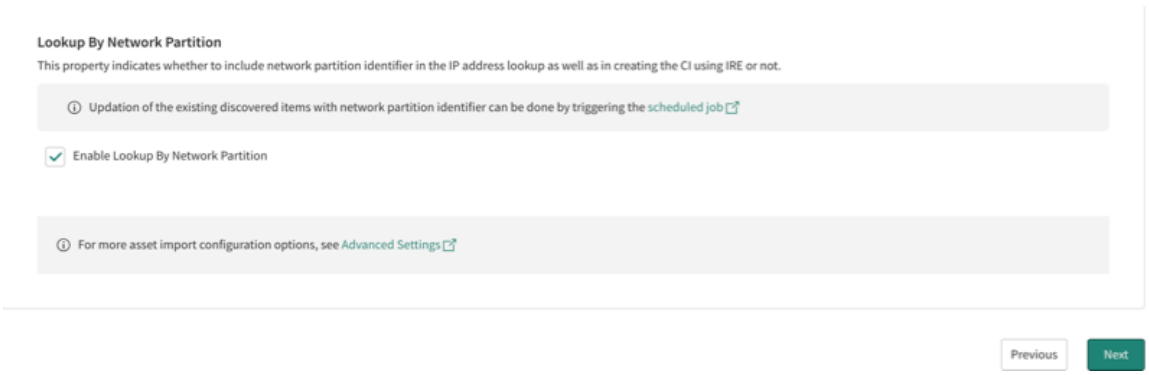
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Option	Beschreibung
Warten Sie auf Importe neuer Daten aus den Integrationen mit den nächsten geplanten Aufgaben.	Erstellen Sie CIs für jedes neue Asset mithilfe des Netzwerkpartition-Bezeichners, beginnend mit der nächsten geplanten Aufgabe. CI-, angreifbare Element- und Erkennungsdatensätze werden alle aktualisiert, um die neue Granularität einzubeziehen. Neue CIs werden erstellt, wenn keine genaue Übereinstimmung gefunden wird.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**an.
2. Wählen Sie Aus Tenable.io Integrationen oder Tenable.sc Integrationen.
3. **Bearbeiten** Die erforderliche Integration.
4. Auswahlvorgang **Konfiguration des Asset-Imports**an.
5. Auswahlvorgang **Suche nach Netzwerkpartition aktivieren** Kontrollkästchen in **Suche nach Netzwerkpartition aktivieren** Abschnitt.



6. Klicken Sie auf **Next (Weiter)**.

Netzwerkpartition-Bezeichner „NETWORK_ID“ und „REPOSITORY_ID“ sind enthalten, und aktualisieren Sie vorhandene CIs, oder erstellen Sie CIs mit der nächsten geplanten Aufgabe.

Attribut des Netzwerkpartition-Bezeichners, das in der IP-Suche und CI-Erstellung enthalten ist

Quelle	IP-Adresse	NETWORK_ID	CI für Assets ohne Netzwerkpartition-Bezeichner	CIs-Assets mit Netzwerkpartition-Bezeichner
Tenable.io: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quelle	IP-Adresse	REPOSITORY_ID	CI für Assets ohne Netzwerkpartition-Bezeichner	CIs-Assets mit Netzwerkpartition-Bezeichner
Tenable.sc: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Bei der nächsten geplanten Aufgabe enthalten die Suchregeln für die IP-Adresse und die CI-Identifizierung der unvollständigen IP-Adresse automatisch das Attribut Netzwerkpartition-Bezeichner für einen Datenimport aus den Assets und Integrationen für behobene und offene Schwachstellen für Tenable.io Und Tenable.sc Produkte.

Nachdem Sie die Systemeigenschaft aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartition-Bezeichner enthalten, indem Sie die geplanten Aufgaben bei Bedarf starten.

Importieren Sie Änderungen für die Tenable-Schwachstellenintegration

Konfigurieren Sie optionale Änderungen, und optimieren Sie einige der Daten speziell für die Importintegration von Tenable-Schwachstellen in ServiceNow® Tenable-Schwachstellenintegration.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Dieser Satz von Aufgaben erfordert Codierung und fortgeschrittenes Wissen über ServiceNow AI Platform.

Führen Sie die folgenden Schritte aus, um domänengetrennte Importe für die Tenable-Schwachstellenintegrationen zu erstellen. Das folgende Beispiel bezieht sich auf die Integration von Tenable.io Open Vulnerabilities, dieser Inhalt gilt jedoch für die anderen Tenable-Integrationen.

Prozedur

1. Erstellen Sie eine Domäne.
2. Erstellen Sie für jede von Ihnen erstellte Domäne einen Anwender, und weisen Sie den Anwender dieser Domäne zu.

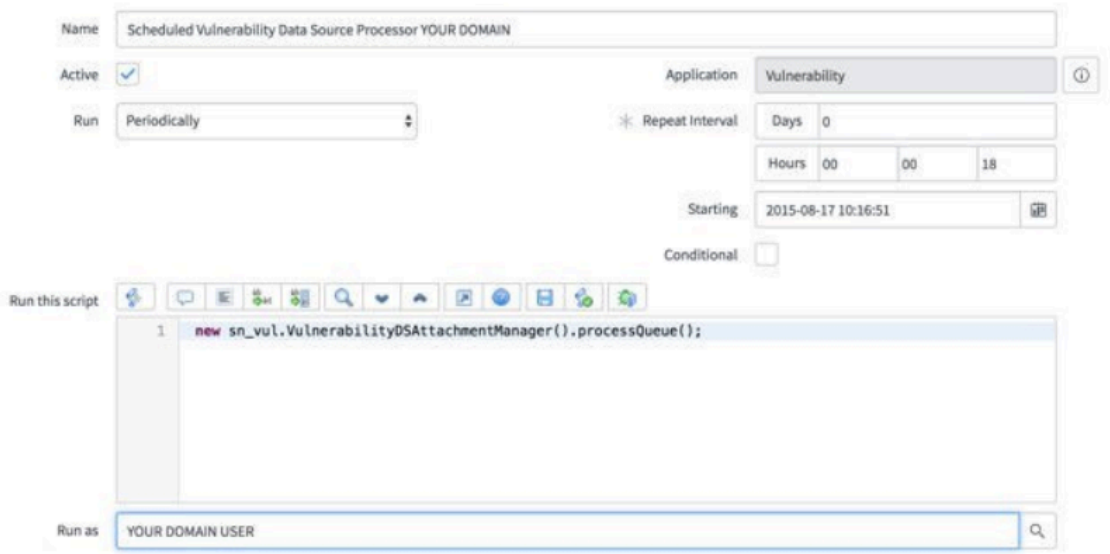
   Stellen Sie sich diesen Anwender als Run_as-Platzhalter für die Domäne in Tenable.io vor.
3. Integration Offener Schwachstellen.
   Der Anwender entspricht dem VR.System-Anwender in der globalen Domäne und muss über die folgenden Rollen verfügen: sn_vul.Tenable_configure_Integration, Import_admin und sn_vul.Vulnerability_write. Dieser Anwender benötigt Zugriff auf Datenquellen, Transformationszuordnungen und Schwachstellendaten.

   Hinweis:
   Betrachten Sie diesen Anwender als spezifisch für diese Rolle. Der Anwender darf keinen anderen Zweck haben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Erstellen Sie in jeder Domäne eine geplante Aufgabe, indem Sie den unter gefundenen Datenquellenprozessor für geplante Schwachstellen kopieren **Systemdefinition** > **Geplante Aufgaben**an.
5. Hängen Sie die Domäne an den Namen an, um die geplante Aufgabe zu identifizieren.
6. Ändern Sie den Run_as-Anwender in den Anwender, den Sie im vorherigen Schritt erstellt haben.

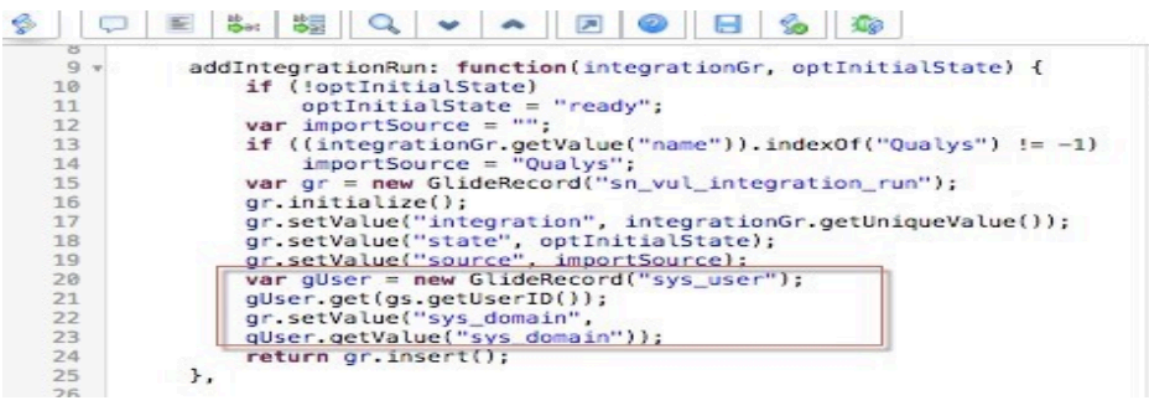
Hinweis:
Bearbeiten Sie die folgende UI-Aktion, damit die Integration in der Anwenderdomäne „Run_as“ ausgeführt wird.



7. Bearbeiten Sie die UI-Aktion Now ausführen in der Tenable.io Open Vulnerabilities Integration, um diesen Codeblock oben in der Datei hinzuzufügen.
```
//sys id below is of Tenable.io integration if(current.sys_id ==
"4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
```

Hinweis:
Bearbeiten Sie die folgenden Skripteinbindungen, damit die Integration in der Anwenderdomäne „Run_as“ ausgeführt wird.

8. Bearbeiten Sie die Skripteinbindungsmethode „VulnerabilityIntegrationUtils“ addIntegrationRun, um den hervorgehobenen Code hinzuzufügen.

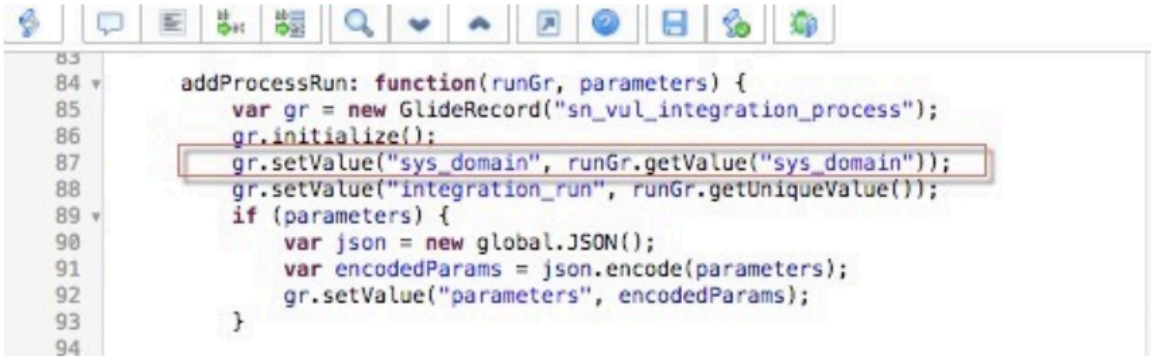


```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Bearbeiten Sie die Skripteinbindungsmethode „VulnerabilityIntegrationUtils“ addProcessRun, um den hervorgehobenen Code hinzuzufügen.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Bearbeiten Sie die DataSourceVulnReportRefreshProcessor-Skripteinbindungsmethode _processFromDataSourceGroups, um diesen ursprünglichen Code zu ändern: Ursprünglicher _processFromDataSourcesGroups-Code in bearbeiteter _processFromDataSourcesGroups-Code.
11. Bearbeiten Sie die Skripteinbindungsmethode VulnerabilityDSAttachmentManager, QueueItem, um die folgenden hervorgehobenen Codeblöcke QueueItem, _getNext, _processQueueEntry hinzuzufügen.

Sie sind bereit für domänengetrennte Host-Erkennungsimporte.

Deaktivieren Sie Rechner vor dem Import

Führen Sie die folgenden Schritte aus, um den Standardrechner zu deaktivieren, wenn er nicht verwendet wird. Wenn Sie keine Schwachstellenrechner verwenden, sollten Sie die Standardrechner zusätzlich zu allen anderen von Ihnen definierten Rechnern deaktivieren. Schwachstellenrechner werden jedes Mal ausgeführt, wenn auf einen Datensatz für angreifbare Elemente zugegriffen wird, und können sich auf die Instanzleistung auswirken.

Erforderliche Rolle: sn_vul.Vulnerability_admin.

12. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Schwachstellen-Rechner**an.
13. Öffnen Sie die Gruppe Schwachstellenauswirkung.
14. Öffnen Sie den Punktzahl- und servicebasierten Auswirkungsrechner.
15. Deaktivieren Sie das Feld aktiv, um den Rechner zu deaktivieren.
16. Klicken Sie auf Aktualisieren.

Sie haben den Standardrechner deaktiviert.

Deaktivieren Sie benachrichtigungsbasierte Business-Regeln vor dem ersten Import

Führen Sie die folgenden Schritte aus, um die Benachrichtigungsbezogenen Geschäftsregeln vor dem ersten Datensatzimport zu deaktivieren. Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln viele Benachrichtigungen generieren, die sich auf die Leistung auswirken. Diese Business-Regeln sollten geändert werden, um sie während des Imports zu deaktivieren.

Erforderliche Rolle ist sn_vul.Vulnerability_admin.

17. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**an.
18. Suchen Sie nach betroffenen ci-Benachrichtigungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

19. Öffnen Sie die Business-Regel, und fügen Sie die folgende Bedingung ein: `current.sys_class_name != “sn_vul_vulnerable_item"`.
20. Klicken Sie auf **Aktualisieren**.
21. Wiederholen Sie diesen Vorgang für die folgenden Business-Regeln:
    - Benachrichtigungen über betroffene Kostenstellen
    - Benachrichtigungen der betroffenen Gruppe
    - Benachrichtigungen zu betroffenen Standorten

Hinweis:
Nach Abschluss des ersten Datensatzimports haben Sie die Möglichkeit, diese Business-Regeln erneut zu aktivieren. Erwägen Sie jedoch, sie deaktiviert zu lassen. Sie können eine große Anzahl von Benachrichtigungen generieren und sich auf die Leistung Ihrer Instanz auswirken.

Ändern Sie ein anfängliches Startdatum

Führen Sie die folgenden Schritte aus, um ein anfängliches Startdatum zu ändern. Während der Installation mit dem Setup-Assistenten legen Sie ein erstes Startdatum für die Tenable-Integrationen fest. Sie können dieses Startdatum im Setup-Assistenten oder über die primäre Integration zurücksetzen, wie in den folgenden Schritten gezeigt.

22. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**an.
23. Klicken Sie auf eine beliebige Integration.
24. Klicken Sie Auf Integrationsdetails.
25. Legen Sie das Feld Startzeit auf einen Wert in der Vergangenheit fest, damit alle seit dieser Zeit gescannten und erkannten Schwachstellen erkannt werden.

    Wenn Sie Tenable mit dem Setup-Assistenten konfiguriert haben, wird das Feld Startzeit vorab ausgefüllt, zunächst drei Monate vor dem heutigen Datum und anschließend bis zum heutigen Datum. Hinweis: Erwägen Sie, den Wert auf maximal einen Monat in der Vergangenheit festzulegen. Dadurch wird verhindert, dass große Datenmengen die Beschränkungen der Tenable-API-Rate überschreiten und Ausführungszeitüberschreitungen auslösen.

26. Klicken Sie auf **Absenden** oder **Aktualisieren**.
27. **Wahlweise:** Klicken Sie Auf **Jetzt Ausführen** Zur sofortigen Ausführung.

Teilen Sie Tenable-Erkennungen basierend auf der Schwachstelleninstanz auf, um angreifbare Elemente aufzuteilen

ServiceNow® Vulnerability Response ermöglicht die Aufteilung von Erkennungen von Tenable-Scannern, wodurch für jede erkannte Schwachstelleninstanz ein eindeutiges angreifbares Element (VIT) erstellt werden kann. Diese Aufteilung ermöglicht die Zuweisung von Vits an verschiedene Korrekturteams, wodurch die Verwaltung und Nachverfolgung von Schwachstellen verbessert wird.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Nutzlast des Tenable-Scanners enthält Erkennungsdaten, wobei jeder Pfad innerhalb des Nachweises zum Aufteilen der Erkennungen verwendet wird. Das Ausgabe-Tag in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Nutzlast identifiziert den Standort der Schwachstelle und erleichtert die genaue Identifizierung und Verwaltung von Schwachstellen gemäß ihren spezifischen Pfaden.

Prozedur

1. Legen Sie in der Tabelle „Drittpartei-Integrationen“ [sn_sec_int_Integration] fest **Nachweis in VI-Schlüssel einschließen** Spaltenwert auf „wahr“ für Tenable.io, Tenable.sc, Und Tenable.cs.
2. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**an.
3. Für Tenable.cs Produkt, navigieren Sie zu **Erkennungsschlüsselkonfiguration** Tabelle [sn_vul_Detection_key_config], wählen Sie aus Tenable.cs Aufzeichnen und aktualisieren,
4. Wählen Sie im Formular „Port einbeziehen“ die aus **Port einschließen** Aktivieren Sie das Kontrollkästchen, und aktivieren Sie das **Klicken Sie hier** Link (gilt nur für Tenable.io und Tenable.sc).
5. Wählen Sie in der Liste Nachweis zu VI-Schlüsseln hinzufügen die Option aus **Neu** .
6. Im Formular „Nachweis zum VI-Schlüssel hinzufügen – neuer Datensatz“ im **Schwachstelle** Fügen Sie die Tenable-ID hinzu, für die Sie den Nachweis einschließen möchten.

   Hinweis:
   Sie können die Erkennungen nur basierend auf Pfadinformationen oder durch Kombination von Pfad- und Versionsdetails aufteilen. Weitere Informationen finden Sie im Abschnitt „Erkennungen von Tenable-Scannern aufteilen“ auf dieser Seite.

7. In **Regulärer Ausdruck zum Aufteilen von Tenable-Vits** Feld:
   - Teilen Sie die Erkennung nur basierend auf dem Pfad auf, indem Sie Pfad eingeben\s+:\s+([A\n]+).
   - Teilen Sie die Erkennung basierend auf Pfad und installierten und festen Versionen auf, indem Sie Pfad\s+:\s+([A\n]+)\n\s+Installed\s+Version\s+:\s+([A\n]+)\n\s+Fixed\s+Version\s+:\s+([A\n]+) eingeben.
8. Wählen Sie **Absenden**.

Example: Trennung von Erkennungen von Tenable-Scannern

Die folgende Erkennung von einem Tenable-Scanner zeigt einen Nachweis im Ausgabe-Tag, der sowohl Pfad- als auch Versionsinformationen enthält.

```
    "results":


            "asset":
                "agent_uuid": *92124caabdb9459baa9d053186df48b9",
               "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
               "device_ type": "aws-ec2-instance",
                "fqdn": "ip-ac0a0004. secops.com",
                "hostname": "ip-ac0a0004",
        "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
                "ipv4": "18.220.145.158",
                "last_authenticated_results": "2024-05-17T03:34:04.424Z",

                "mac_address": "0a:3e:8b:ed:63:e6",
               "netbios name": "IP-AC0A0094".
               "operating_system": [
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                    "Microsoft Windows Server 2019 Datacenter Build 17763"


                  "network_id": "00000000-0000-0000-0000-000000000008",

                 "tracked": true


            "output": "In                    C: 11 Program Files (x86) \ \Common
Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed
version
                                                                    Path
            "plugin":
                  "bid":
                       123456


                  "checks_for_default_account": false,
                "checks_for malware": false,

                   "coe":
                 "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"


                  "cvSs3_base_score": 7.8,
                 "cvss3 temporal score": 7.0,

                 "cvss3_temporal_vector": {
                       "exploitability": "Proof-of-Concept",
                       "remediation level": "Official Fix",
                        "report_confidence": "Confirmed",
                        "raw": "E: P/RL:0/RC: C"
```


Verstehen von Atlassian Jira Integration mit Vulnerability Response

Die Atlassian Jira Integration mit Vulnerability Response Ermöglicht es Ihnen, verschiedene Problemnachverfolgungs- und agiles Management-Tools zur Nachverfolgung der Maßnahmen zur Schwachstellenbeseitigung zu nutzen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht

ServiceNow® Vulnerability Response Ist in integriert Atlassian Jira Um Probleme zu erstellen, die Schwachstellen entsprechen, und die Problementität in synchronisiert Jira Und die Entität des Schwachstellenelements in Vulnerability Response bidirektional, um die neuesten Updates widerzuspiegeln. Schwachstellenmanager erfordern Schwachstellenelemente in ServiceNow Vulnerability Response Muss erstellt und Korrekturanwendern zugewiesen werden (Entwickler im Fall von Application Vulnerability Response) In ihrem bevorzugten Datensatzsystem und Problemmanagement-Tool wie Atlassian Jira. Jeder Fortschritt, der für die Schwachstellen im Problemmanagement-Tool ausgeführt wird, sollte in aktualisiert werden ServiceNow Vulnerability Response Für Sichtbarkeit für Schwachstellenmanager. Außerdem alle Updates,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die von Schwachstellenmanagern in vorgenommen wurden Vulnerability Response Für Schwachstellen müssen Elemente auch an das Problem-Management-Tool übergeben werden, damit Korrekturanwender sichtbar sind.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response	Versionshinweise zur Vulnerability Response-Integration
Vulnerability Response und Konfigurations-Compliance für Container	Release-Hinweise für Container Vulnerability Response
Jira-Spoke	Release-Hinweise für Jira-Spoke

Jira Schwachstellenintegrationen

Um anzuzeigen Jira Schwachstellenintegration, navigieren Sie zu **Alle** > **Agile-Management für VR** > **Agile-Tools konfigurieren** .

Die folgenden Integrationen sind im Basissystem enthalten. Diese Integrationen sind standardmäßig nicht alle aktiv.

Nach der ersten Ausführung werden täglich geplante Aufgaben verkettet, um die Integrationen automatisch in der Reihenfolge auszuführen. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Vorbereitung für Jira Vulnerability Response Integration

Ein erfolgreich Jira Die Schwachstellenintegration erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die Jira Vulnerability Response Bei der Integration wird davon ausgegangen, dass Sie mit vertraut sind Jira Produkt und API.

Mit Agile Integration für installierte Komponenten Vulnerability Response Und Jira Integration für Vulnerability Response

Bei der Aktivierung des Plugins „Agile Integration for Vulnerability Response“ und „Jira Integration for Vulnerability Response“ werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Anwenderrollen.

Installierte Rollen

Rollentitel [name]	Beschreibung
Agile-Tool-Administrator [sn_vul_agile.Agile_Tool_admin]	Ermöglicht Ihnen das Erstellen einer Konfigurationsregel für Agile Management, um Probleme zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Rollen (Fortsetzung)

Rollentitel [name]	Beschreibung
	erstellen oder zu aktualisieren. Erstellen Sie Regelkonfigurationen für Agile Management.
JIRA-Administrator [sn_vul_jira.admin]	Ermöglicht Ihnen die Auswahl des Agile-Tools, um Probleme für die ausgewählte Entitätstabelle zu erstellen.

Installierte Tabellen

Tabelle	Beschreibung
Agile-Tool-Konfiguration [sn_vul_Agile_Tool_rule_config]	Enthält Konfigurationsregeln zum Erstellen von Problemen auf der Agile-Plattform.
Agile-Tool-Feldzuordnung [sn_vul_Agile_Tool_field_Mapping]	Enthält die Feldzuordnung der Konfigurationsregel.
Statuszuordnung des Agile-Tools [sn_vul_Agile_Tool_State_Mapping]	Enthält die Statuszuordnung des Jira-Problemstatus mit dem Status „Angreifbares Anwendungselement“, „Angreifbares Container-Element“, „Anwendungskorrekturaufgabe“ und „Container-Korrekturaufgabe“.
Agile-Tool-Manifest [sn_vul_agile_Tool_manifest]	Enthält Nutzlast für die Problemerstellung.
Agile-Tool-Datenressource [sn_vul_Agile_Tool_Data_resource]	Enthält die Informationen zum erstellten Jira-Problem.
JIRA-Administrator [sn_vul_jira.admin]	Ermöglicht Ihnen die Auswahl des Agile-Tools, um Probleme für die ausgewählte Entitätstabelle zu erstellen.

Installieren Sie die Vulnerability Response-Integration mit Jira

Bevor Sie die Integration auf Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit die ausgeführt werden kann Jira Produkt ist ordnungsgemäß in integriert Application Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Erforderliche Rolle: admin.

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob die Anwendung Vulnerability Response installiert und aktiviert ist.	• Jira Integration for Vulnerability Response erfordert die Anwendung Vulnerability Response. • Stellen Sie für die aktuelle Version von Jira Integration for Vulnerability Response sicher, dass Sie die neueste Version von Vulnerability Response installiert haben. Siehe KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema . • Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Installieren Sie Vulnerability Response .
Überprüfen Sie, ob das Plugin „Integration Hub“ installiert ist.	• Jira-Spoke erfordert den Integration Hub. • Siehe KB1112383 Für Integration Hub-Installation. • Weitere Informationen finden Sie unter Rechtliche Zeitpläne – IntegrationHub-Übersicht .
Überprüfen Sie, ob die neueste Version von ist Jira Spoke Ist installiert.	Siehe KB0792632 Für die Installation der Jira-Spoke.
Überprüfen Sie, ob die Vulnerability Response-Integration mit Agile Management installiert ist.	Die Integration von Vulnerability Response mit Atlassian Jira erfordert diese Integration.

Prozedur

1. Melden Sie sich bei der Instanz an, die Sie installieren möchten Jira Vulnerability Response Integration auf.
2. Navigieren Sie zum ServiceNow Store.
3. In ServiceNow Store, Suchen Sie nach Vulnerability Response Integration mit Jira Anwendung.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Erwägen Sie, das zu lesen **Andere Anforderungen** Und **Abhängigkeiten** Abschnitte, falls zutreffend.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**an.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Konfigurieren Sie Regeln in der Agile-Tool-Konfiguration

Jira Probleme werden auf erstellt Jira Plattform, wenn die in den Feldern Angreifbares Anwendungselement, angreifbares Container-Element, Anwendungskorrekturaufgabe und Container-Korrekturaufgabe erstellten Datensätze den in der Agile-Tool-Konfiguration erstellten Regeln entsprechen.

Vorbereitungen

Erforderliche Rollen: sn_vul.App_read_all, sn_vul_Container.read_all, sn_vul_agile.agile_Tool_admin oder sn_vul_jira.admin.

Prozedur

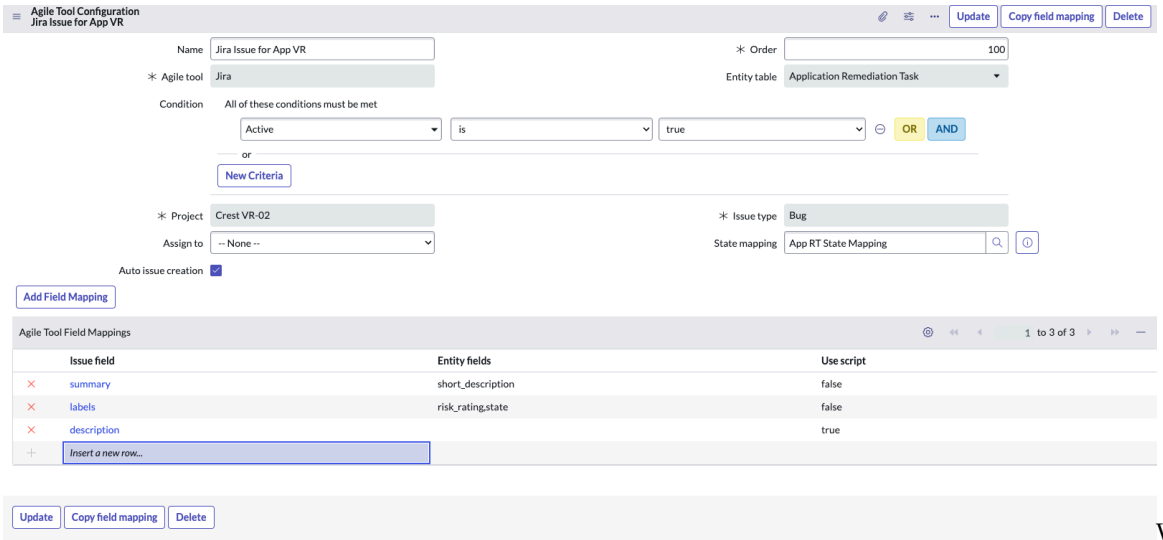
1. Navigieren zu **Alle** > **Agile-Management für VR** > **Agile-Tools konfigurieren**an.
2. Um eine neue Konfigurationsregel in der Agile Tool-Konfiguration zu erstellen, wählen Sie aus **Neu** .
3. Füllen Sie im Formular die Felder aus.

Konfigurationsformular für Agile-Tool

Feld	Beschreibung
Name	Name der Agile-Tool-Konfiguration.
Reihenfolge	Reihenfolge der Agile-Tool-Konfiguration.
Agile-Tool	Das Agile-Tool zum Erstellen von Problemen auf der spezifischen Agile-Plattform.
Entitätstabelle	Tabelle, auf die die Konfigurationsregel angewendet werden soll.
Bedingung	Filterbedingung für die ausgewählte Entitätstabelle, um Probleme auf der Agile-Plattform zu erstellen.
Automatische Problemerstellung	Die Konfigurationsregel wird nur abgefragt, wenn ein neuer Datensatz in der ausgewählten Entitätstabelle erstellt wird, wenn das Kontrollkästchen aktiviert ist. **Hinweis:** Der Anwender muss die Listenaktion verwenden, um Probleme für vorhandene Entitätsdatensätze zu erstellen.
Projekt	Das Projekt, in dem das Jira-Problem erstellt wird.
Problemtyp	Der Typ des Problems, das in einem bestimmten Projekt erstellt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zuweisen an	Der Beauftragte, dem das Problem bei der Erstellung des Problems zugewiesen werden soll. Um die erstellten Probleme als nicht zugewiesen beizubehalten, wählen Sie „keine“ aus.
Statuszuordnung	Die vorhandenen Statuszuordnungen aus der Tabelle „Agile Tool-Statuszuordnung“ oder erstellen Sie eine neue Statuszuordnung zwischen dem Problemstatus in der Agile-Plattform und dem ServiceNow entitätstabellenstatus.



Wenn die Anwendung installiert ist, werden die Anwendungskorrekturaufgabe und die Container-Korrekturaufgabe standardmäßig im Feld Entitätstabelle im Formular „Agile-Tool-Konfiguration“ angezeigt.

4. Um das Angreifbare Anwendungselement und das angreifbare Container-Element in der Auswahlliste Entitätstabelle hinzuzufügen, navigieren Sie zu **Systemeigenschaften** > **sn_vul_agile.tablesToAnzeigen** Und fügen Sie alle im Feld Wert hinzu.

Formular für Systemeigenschaften

Feld	Beschreibung
Auswahlmöglichkeiten	Durch Kommas getrennte Werte für eine Auswahlliste.
Wert	Legen Sie den gewünschten Wert für die Eigenschaft fest. Alle Eigenschaftswerte werden als Zeichenfolgen gespeichert. Behandeln Sie die Ergebnisse beim Abrufen von Eigenschaften mit der Methode gs.getProperty() als Zeichenfolgen. Beispielsweise gibt eine Eigenschaft „wahr|falsch“ „wahr“ oder „falsch“ (Zeichenfolgen) zurück, nicht das boolesche Äquivalent.

5. Wählen Sie den vorhandenen Statuszuordnungsdatensatz aus, oder erstellen Sie eine neue Statuszuordnung in der Agile Tool-Statuszuordnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Agile Tool-Statuszuordnung“

Feld	Beschreibung
Name	Fügen Sie den eindeutigen Namen der Statuszuordnung ein.
Agile-Tool	Wählen Sie das Agile-Tool aus.
Entitätstabelle	Wählen Sie die Quelltabelle aus, für die die Statuszuordnung erstellt wird.
Projekt	Wählen Sie das Projekt aus, dem der Status zugeordnet wird.
ServiceNow-Entitätsstatus	Wählen Sie den Status aus, den Sie dem agilen Toolstatus zuordnen möchten.
Agile-Tool-Status	Wählen Sie den Status aus, den Sie zuordnen möchten, aus den status des Schwachstellenelements.

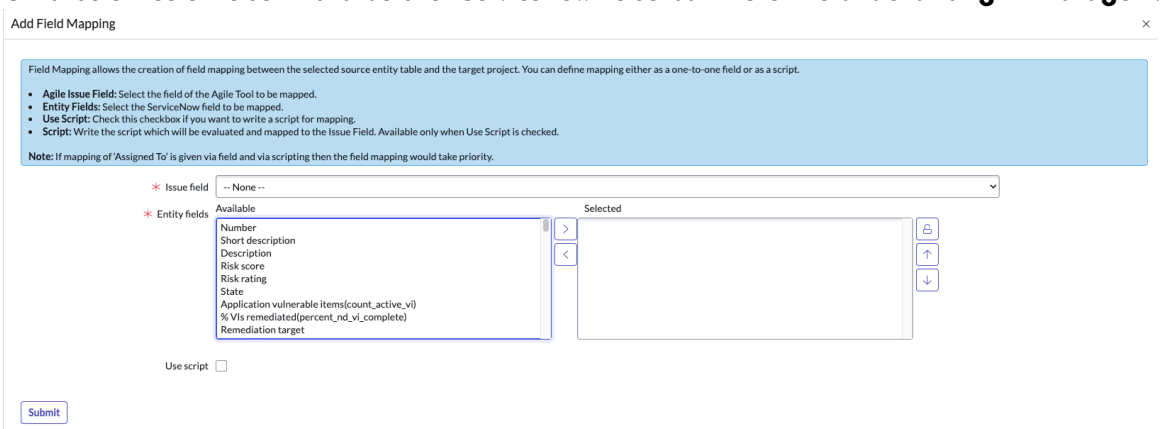
6. Klicken Sie auf **Speichern und Projekte abrufen** Um die Projekte in der Konfigurationsregel „Projekt“ abzurufen und die Anmeldeinformationen des Agile-Tools zu validieren.

   Tipp:
   Sie können die Systemeigenschaft festlegen **ProjectsPageSize** Dient zum Abrufen einer bestimmten Anzahl von Projekten pro Seite.

7. Navigieren Sie zu **Systemeigenschaften** > **sn_vul_jira.projectsPageSize** Und fügen Sie die Anzahl der pro Seite abzurufenden Projekte im Feld Wert für Jira Cloud hinzu.
8. Wählen Sie in der Konfigurationsregel Projekt, Problemtyp und Zuweisen an aus, nachdem die Projekte abgerufen wurden.

   Die Standardfeldzuordnung wird in der eingebetteten Liste der Agile-Tool-Feldzuordnungen ausgefüllt. Standardmäßig werden die Felder „Zusammenfassung“ und „Beschreibung“ von Problemen zugeordnet.

9. Um andere Problemfelder mit zuzuordnen ServiceNow Felder auf klicken **Feldzuordnung Hinzufügen** .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Sie müssen nur Felder für Zeichenfolge und Auswahltyp zuordnen.
- Stellen Sie sicher, dass alle Problem-Pflichtfelder aus dem Agile-Tool ordnungsgemäß dem Entitätsfeld zugeordnet sind.

Formular „Agile Tool-Statuszuordnung“

Feld	Beschreibung
Problemfeld	Enthält die Problemfelder des aktuell ausgewählten Projekts und Problemtyps in der Konfigurationsregel.
Entitätsfelder	Enthält die Felder der Entitätstabelle, die in der Konfigurationsregel ausgewählt wurde.
Verwenden Sie das Skript	Wählen Sie diese Option aus, um das Skript für die Zuordnung der Problemfelder zu Entitätsfeldern zu verwenden.
Skript	Skript zum Zuordnen des Problemfelds zu Entitätsfeldern.

10. Klicken Sie Auf **Übermitteln** Im Glide-Modal zum Senden des Feldzuordnungsdatensatzes in der Tabelle „Agile Tool-Feldzuordnungen“.

    Hinweis:
    Wenn Sie die Pflichtfelder nicht zuordnen, werden für diese Konfigurationsregel keine Probleme erstellt.

    Pflichtfelder werden oben im Formular „Agile-Tool-Konfiguration“ angezeigt.
    Alle Feldzuordnungen für eine bestimmte Konfigurationsregel werden in der eingebetteten Liste der Tabelle „Agile-Tool-Feldzuordnung“ in der Tabelle „Agile-Tool-Konfiguration“ angezeigt.

11. Klicken Sie mit der rechten Maustaste in den Header, um Ihre Änderungen zu speichern.
    Der gespeicherte Datensatz ist in der Tabelle „Agile-Tool-Konfiguration“ sichtbar. Wenn ein Datensatz in den Feldern „Angreifbares Anwendungselement“, „Angreifbares Container-Element“, „Anwendungskorrekturaufgabe“ und „Container-Korrekturaufgabe“ mit einer Konfigurationsregel übereinstimmt, wird das Problem für den Datensatz gemäß der Zuordnung in der Konfigurationsregel erstellt.

12. Navigieren Sie zu **Systemeigenschaften** > **sn_vul_jira.cloudMassengröße** Und legen Sie die Anzahl der pro Batch zu erstellenden Probleme im Feld Wert fest.

    Hinweis:
    Die maximale Anzahl von Problemen, die pro Batch in der Jira-Cloud erstellt werden können, beträgt 50).

    Sie können die Batch-Größe zum Erstellen von Problemen auf dem Jira-Server festlegen.

13. Navigieren Sie zu **Systemeigenschaften** > **sn_vul_jira.onPremMassenIssue** Und legen Sie die Anzahl der Probleme fest, die pro Batch in erstellt werden sollen **Wert** Feld.
    Sie können die Fehleranzahl auch im Feld Wert in der Systemeigenschaft festlegen, um die Datensätze in der Manifesttabelle zu verarbeiten, um Jira-Probleme bis zu einer bestimmten Fehleranzahl zu erstellen.

14. Navigieren Sie zu **Systemeigenschaften** > **sn_vul_Agile.ManifestFehleranzahl** Und legen Sie die maximale Anzahl der Verarbeitungen des Manifests mit Fehler fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie agiles Problem manuell mithilfe der Listenaktion

Wenn eine Listenaktion „Jira-Problem erstellen“ ausgelöst wird, sollten Datensätze, die den Regelkonfigurationskriterien entsprechen, für „Jira-Problem erstellen“ berücksichtigt werden, und diese Datensätze sollten in der Tabelle „sn_vul_agile_Tool_manifest“ mit der in der Konfigurationsregel ausgewählten Zuordnung erfasst werden.

Vorbereitungen

Erforderliche Rolle: sn_vul_agile.agile_Tool_admin oder sn_vul_jira.admin, sn_vul.App_read_all, sn_vul_Container.read_all.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste** > **Korrekturaufgaben/angreifbare Anwendungselemente/angreifbare Container-Elemente**an.
2. Wählen Sie mehrere Datensätze aus, um Jira-Probleme zu erstellen, und klicken Sie auf **Jira-Problem Erstellen** .
   Die ausgewählten Datensätze sollten die Feldzuordnung und die Statuszuordnung des zugehörigen Agile-Tools berücksichtigen.
   Die ausgewählten Datensätze, die die Konfigurationsregelbedingung erfüllen, sollten für die Erstellung von Jira-Problemen in Frage kommen, und diese Datensätze sollten zu hinzugefügt werden `sn_vul_agile_tool_manifest`Tabelle.

Erstellen Sie agiles Problem manuell mithilfe der Formularaktion

Erstellen Sie ein agiles Problem manuell mithilfe der Formularaktion. Wenn der Datensatz mit einer Konfigurationsregelbedingung übereinstimmt, wird ein Popup-Feld mit Werten ausgefüllt, die in der Konfigurationsregel ausgewählt sind. Wenn er keinem Kriterium entspricht, kann der Anwender Werte für vordefinierte Felder auswählen.

Vorbereitungen

Stellen Sie sicher, dass alle obligatorischen Problemfelder aus dem Agile-Tool ordnungsgemäß dem Entitätsfeld zugeordnet sind.

Erforderliche Rollen: sn_vul_agile.agile_Tool_admin oder sn_vul_jira.admin, sn_vul.App_read_all, sn_vul_Container.read_all.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste** > **Korrekturaufgaben/angreifbare Anwendungselemente/angreifbare Container-Elemente**an.
2. Wählen Sie einen beliebigen Datensatz aus, um ein agiles Problem manuell zu erstellen.
3. Wählen Sie Aus **Agile-Problem Erstellen** .
4. Fügen Sie gültige Details für die genannten Felder ein.

   Wenn der Datensatz die Bedingung einer Konfigurationsregel erfüllt, sollten die folgenden Felder mit dem konfigurierten Wert ausgefüllt werden, und der Anwender kann die Feldwerte ändern.

Feld	Beschreibung
Projekt	Wählen Sie das Projekt aus, in dem das Jira-Problem erstellt wird.
Problemtyp	Wählen Sie den Typ des Problems aus, das in einem bestimmten Projekt erstellt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zuweisen an	Wählen Sie den Beauftragten aus, dem das Problem bei der Erstellung des Problems zugewiesen werden soll.
Feldzuordnung	Wählen Sie die Problemtypfelder des Agile-Tools aus, und fügen Sie die direkten Werte für das ausgewählte Feld ein.

5. Wählen Sie Aus **Agile-Problem Erstellen** Um den Datensatz zu übermitteln.
   Nach dem Senden des Datensatzes wird der Datensatzeintrag in der Tabelle „sn_vul_agile_Tool_manifest“ erstellt.

Synchronisieren Sie den Status des manuell Jira Problem

Aktualisieren Sie den Status des einzelnen Datensatzes, indem Sie auf klicken **Agile-Status Synchronisieren** Schaltfläche des Formularkontextmenüs und aktualisieren Sie die status mehrerer Datensätze, indem Sie auf die Listenaktion klicken **Agile-Status Synchronisieren** Der Tabelle „Angreifbares Anwendungselement“, „Angreifbares Container-Element“ und „Korrekturaufgabe“ im Vulnerability Manager-Arbeitsbereich.

Vorbereitungen
Erforderliche Rollen: sn_vul_agile.agile_Tool_admin oder sn_vul_jira.admin, sn_vul.App_read_all, sn_vul_Container.read_all.

Warum und wann dieser Vorgang ausgeführt wird
Der Status wird von synchronisiert ServiceNow Zum agilen Tool, wenn der Entitätsstatus in geschlossen ist ServiceNow Oder wenn eine Entität erneut geöffnet wird (d. h. Status ist Offen). Alle anderen status werden vom Agile-Tool in angezeigt ServiceNow. Der Anwender darf keinen Status für die Datensätze synchronisieren, deren zugeordnete konfigurierte Regel keine Statuszuordnung oder die Probleme aufweist, die direkt aus der Formularaktion erstellt werden.

Prozedur
1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste** > **Korrekturaufgaben/angreifbare Anwendungselemente/angreifbare Container-Elemente**an.
2. Wählen Sie mehrere Datensätze aus, um Jira-Probleme zu erstellen, und klicken Sie auf **Agile-Status Synchronisieren** .
   Status der Datensätze, für die bereits Probleme erstellt wurden, werden aktualisiert, wenn sich der Datensatz nicht im Status „Geschlossen“ befindet und die Statuszuordnung für die ausgewählten Datensätze in der Konfigurationsregel vorhanden ist.
3. Öffnen Sie einen Datensatz und den **Agile-Status Synchronisieren** Ist im Kontextmenü des Formulars sichtbar, wenn die folgenden Bedingungen erfüllt sind.
   - Problem wird für den Datensatz erstellt, und der Datensatz befindet sich nicht im Status „Geschlossen“
   - Für den Datensatz ist eine Statuszuordnung vorhanden
4. Klicken Sie Auf **Agile-Status Synchronisieren** Dient zur Synchronisierung des Agile-Status mit dem zugeordneten Status.
   Sie können die Systemeigenschaft festlegen, um die Batchgröße zum Abrufen des Problemstatus aus Jira festzulegen.
5. Navigieren zu **Systemeigenschaft** > **sn_vul_jira.bulkIssueStatusSize** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für Jira-Server die maximale Anzahl der zurückzugebenden Probleme (standardmäßig 50). Der maximal zulässige Wert wird von der Jira-Eigenschaft „jira.search.views.default.max' bestimmt. Wenn Sie einen Wert angeben, der höher als diese Zahl ist, werden Ihre Suchergebnisse gekürzt.
- Wenn das Problem aus einer Formularaktion erstellt wird oder die konfigurierte Regel keine Statuszuordnung aufweist, werden diese Datensätze für die Statussynchronisierung nicht berücksichtigt.

Konfigurieren Sie den Planer, um Probleme automatisch zu erstellen

Konfigurieren Sie den Planer so, dass er ausgeführt und automatisch erstellt wird Jira Probleme für die Datensätze, die in der Tabelle „sn_vul_agile_Tool_manifest“ erstellt wurden.

Vorbereitungen
Erforderliche Rolle: admin oder schedule_admin.

Warum und wann dieser Vorgang ausgeführt wird
Alle Datensätze des angreifbaren Anwendungselements, des angreifbaren Container-Elements, der Anwendungskorrekturaufgabe und der Container-Korrektur, die in der Tabelle „sn_vul_agile_manifest“ erstellt wurden, werden für berücksichtigt Jira Problemerstellung.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben** > **Erstellen Sie Jira-Probleme**an.
2. Sie können die Felder Ausführen, Zeitzone und Zeit im geplanten Skript ändern.

Formular „Geplante Skript-Ausführung“

Feld	Beschreibung
Ausführen	Zeitintervall für die Ausführung der geplanten Aufgabe: ○ Täglich: Wird täglich zu einer bestimmten Zeit ausgeführt. ○ Wöchentlich: Wird wöchentlich zu einer bestimmten Uhrzeit und einem bestimmten Tag ausgeführt. ○ Monatlich: Wird monatlich zu einer bestimmten Uhrzeit und einem bestimmten Tag des Monats ausgeführt. ○ Wird regelmäßig in einem festgelegten Wiederholungsintervall ausgeführt. ○ Einmal: Wird nur für ein einzelnes Vorkommen ausgeführt. ○ Bei Bedarf: Wird sofort bei Bedarf ausgeführt. ○ Geschäftskalender: Eintragsstart: Wird an den Startdaten für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Eine geplante Aufgabe wird für das Startdatum jedes Geschäftseintrags ausgeführt, den Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	für den Geschäftskalender definiert haben. Wenn der Geschäftskalender beispielsweise ein Geschäftsjahr darstellt und das Beginndatum jedes Eintrags ein Geschäftsmonat ist, wird die geplante Aufgabe am ersten Tag jedes Monats ausgeführt. ○ Geschäftskalender: Eintragsende – wird für das Enddatum des Geschäftskalenders ausgeführt, den Sie im Feld auswählen. Diese Auswahl wird auf dieselbe Weise ausgeführt wie Geschäftskalender: Eintragsbeginn, jedoch für die Enddaten der zugehörigen Geschäftskalendereinträge. **Hinweis:** Wenn Sie Geschäftskalender: Eintragsbeginn oder Geschäftskalender: Eintragsende auswählen, können Sie einen Offset-Faktor anwenden, um die Ausführung der Aufgabe vor oder nach der Zeitspanne des ausgewählten Geschäftskalenders zu planen. Weitere Informationen finden Sie in den Feldern Offset-Typ und Offset. Weitere Informationen zum Erstellen und Verwenden von Geschäftskalendern und zum Definieren von Geschäftskalendereinträgen finden Sie unter Create a business calendar Und Define business calendar entries .
Tag	Tag, an dem die geplante Aufgabe ausgeführt werden soll ○ Wenn für Ausführen die Option Wöchentlich festgelegt ist, geben Sie den Wochentag an. Wählen Sie zum Beispiel „Mittwoch“ aus. ○ Wenn Ausführen auf Monatlich eingestellt ist, wählen Sie den Tag im Monat. Wählen Sie beispielsweise 25 für den 25. Tag des Monats aus. Dieses Feld wird nur angezeigt, wenn Sie im Feld Ausführen die Option Monatlich oder Wöchentlich auswählen.
Wiederholungsintervall	Dauer des Wiederholungsintervalls für jede geplante Aufgabenausführung. Geben Sie die Dauer in Tagen, Stunden oder Minuten ein. Beispiel:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Um die regelmäßige Aufgabe alle vier Tage auszuführen, geben Sie in das Feld Tage den Wert 04 ein. ○ Um sie alle 26 Stunden auszuführen, geben Sie in das Feld Stunden den Wert 26 ein. ○ Wenn die regelmäßige Aufgabe in einem Intervall von 13:30:25 wiederholt werden soll, geben Sie in das Feld Stunden den Wert 13 ein. Geben Sie anschließend in die beiden nachstehenden unbeschrifteten Felder die Werte 30 und 25 ein.
Zeit	Uhrzeit, zu der die geplante Aufgabe ausgeführt werden soll, ausgedrückt in Stunden, Minuten und Sekunden im 24-Stunden-Format. Die Auswahl, die Sie im Feld Zeitzone treffen, bestimmt die Zeitzone für diesen Eintrag.
Zeitzone	Zeitzone, die mit dem Eintrag im Feld Zeit verwendet werden soll, wenn Sie die Uhrzeit angeben, zu der die regelmäßige Aufgabe ausgeführt werden soll. Wählen Sie einen Zeitzoneneintrag aus: ○ **Keine** : Verwenden Sie die Standardzeitzone für den angemeldeten Anwender, der die geplante Aufgabe erstellt. Die geplante Aufgabe wird beispielsweise um 16:45 Uhr US-Pazifik-Zeit ausgeführt, wenn es sich um die für den Benutzer zugewiesene Zeitzone handelt und wenn Sie 16:45 in das Feld Zeit eingeben. ○ **Zeitzone des Systems verwenden**: Verwenden Sie die standardmäßige Systemzeitzone, die für die Instanz angegeben ist, in der sie ausgeführt wird. Die regelmäßige Aufgabe wird beispielsweise um 22:15 Uhr Londoner Zeit ausgeführt, wenn Europa/London die standardmäßige Systemzeitzone für die Instanz ist und Sie 22:15 in das Feld Zeit eingeben. ○ Tatsächliche Zeitzone. ○ Beispielsweise wird die geplante Aufgabe um 13:30 Uhr in ausgeführt USA Östliche Zeitzone, wenn Sie US/Eastern auswählen und 13:30 Uhr in das Zeitfeld eingeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
run_as	Standardmäßig muss der Feldwert „Run_ as“ leer sein. Der Anwender kann den Wert als Domänenanwenderwert festlegen, um ein Problem für eine bestimmte Domäne zu erstellen.

Konfigurieren Sie den Planer, um Probleme automatisch zu aktualisieren

Konfigurieren Sie den Planer, um zu aktualisieren Jira Probleme automatisch für die Datensätze, die in der Tabelle „sn_vul_agile_Tool_manifest“ hinzugefügt wurden.

Vorbereitungen
Erforderliche Rolle: admin oder schedule_admin.

Warum und wann dieser Vorgang ausgeführt wird
Alle Datensätze des angreifbaren Anwendungselements, des angreifbaren Container-Elements, der Anwendungskorrekturaufgabe und der Container-Korrektur, die in der Tabelle „sn_vul_agile_manifest“ erstellt wurden, werden für berücksichtigt Jira Problem-Update. Wenn der Datensatz geschlossen wird und Kommentare hinzugefügt werden, sollten auch diese Werte auf die zugeordnete aktualisiert werden Jira Problem.

Hinweis:

- Die geplante Aufgabe „Probleme aktualisieren“ aktualisiert nicht Jira status, wenn der Workflow für das ausgewählte Agile-Problemprojekt Anwender daran hindert, den Status direkt von einem anderen Status aus zu ändern.
- Wenn Sie einen Entitätsdatensatz mit zusätzlichen Kommentaren schließen, wird zum Zeitpunkt der Aktualisierung nur der letzte Kommentar berücksichtigt, und beim nächsten Update werden alle Kommentare dem zugeordneten hinzugefügt Jira.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben** > **Aktualisieren Sie Jira-Probleme**an.
2. Sie können ändern **Ausführen** , **Zeitzone** , Und **Zeit** Felder im geplanten Skript.

Formular „Geplante Skript-Ausführung“

Feld	Beschreibung
Ausführen	Zeitintervall für die Ausführung der geplanten Aufgabe: ○ Täglich: Wird täglich zu einem bestimmten Zeitpunkt ausgeführt ○ Wöchentlich: Wird wöchentlich zu einer bestimmten Uhrzeit und einem bestimmten Tag ausgeführt. ○ Monatlich: Wird monatlich zu einer bestimmten Uhrzeit und einem bestimmten Tag des Monats ausgeführt. ○ Regelmäßig: Wird in einem vorgegebenen, sich wiederholenden Intervall ausgeführt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Einmal: Wird nur für ein einzelnes Vorkommen ausgeführt ○ Bei Bedarf: Wird bei Bedarf sofort ausgeführt ○ Geschäftskalender: Eintragsstart: Wird an den Starteintragsdaten für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Eine geplante Aufgabe wird für das Startdatum jedes Geschäftseintrags ausgeführt, den Sie für den Geschäftskalender definiert haben. Wenn der Geschäftskalender beispielsweise ein Geschäftsjahr darstellt und das Beginndatum jedes Eintrags ein Geschäftsmonat ist, wird die geplante Aufgabe am ersten Tag jedes Monats ausgeführt. ○ Geschäftskalender: Eintragsende: Wird für das Enddatum des Geschäftskalenders ausgeführt, den Sie im Feld auswählen. Diese Auswahl wird auf dieselbe Weise ausgeführt wie Geschäftskalender: Eintragsbeginn, jedoch für die Enddaten der zugehörigen Geschäftskalendereinträge. **Hinweis:** Wenn Sie Geschäftskalender: Eintragsbeginn oder Geschäftskalender: Eintragsende auswählen, können Sie einen Offset-Faktor anwenden, um die Ausführung der Aufgabe vor oder nach der Zeitspanne des ausgewählten Geschäftskalenders zu planen. Weitere Informationen finden Sie in den Feldern Offset-Typ und Offset. Weitere Informationen zum Erstellen und Verwenden von Geschäftskalendern und zum Definieren von Geschäftskalendereinträgen finden Sie unter und Create a business calendar Define business calendar entries .
Tag	Tag, an dem die geplante Aufgabe ausgeführt werden soll ○ Wenn für Ausführen die Option Wöchentlich festgelegt ist, geben Sie den Wochentag an. Wählen Sie zum Beispiel „Mittwoch“ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Wenn Ausführen auf Monatlich eingestellt ist, wählen Sie den Tag im Monat. Wählen Sie beispielsweise 25 für den 25. Tag des Monats aus. Dieses Feld wird nur angezeigt, wenn Sie im Feld Ausführen die Option Monatlich oder Wöchentlich auswählen.
Wiederholungsintervall	Dauer des Wiederholungsintervalls für jede geplante Aufgabenausführung. Geben Sie die Dauer in Tagen, Stunden oder Minuten ein. Beispiel: ○ Um die regelmäßige Aufgabe alle vier Tage auszuführen, geben Sie in das Feld Tage den Wert 04 ein. ○ Um sie alle 26 Stunden auszuführen, geben Sie in das Feld Stunden den Wert 26 ein. ○ Wenn die regelmäßige Aufgabe in einem Intervall von 13:30:25 wiederholt werden soll, geben Sie in das Feld Stunden den Wert 13 ein. Geben Sie anschließend in die beiden nachstehenden unbeschrifteten Felder die Werte 30 und 25 ein.
Zeit	Uhrzeit, zu der die geplante Aufgabe ausgeführt werden soll, ausgedrückt in Stunden, Minuten und Sekunden im 24-Stunden-Format. Die Auswahl, die Sie im Feld Zeitzone treffen, bestimmt die Zeitzone für diesen Eintrag.
Zeitzone	Zeitzone, die mit dem Eintrag im Feld Zeit verwendet werden soll, wenn Sie die Uhrzeit angeben, zu der die regelmäßige Aufgabe ausgeführt werden soll. Wählen Sie einen Zeitzoneneintrag aus: ○ Keine: Verwenden Sie die Standardzeitzone für den angemeldeten Anwender, der die geplante Aufgabe erstellt. Beispielsweise wird die geplante Aufgabe um 16:45 Uhr ausgeführt. US/Pazifik-Zeit, wenn es sich um die zugewiesene Zeitzone des Anwenders handelt, und Sie geben 16:45 Uhr in das Zeitfeld ein. ○ Zeitzone des Systems verwenden: Verwenden Sie die standardmäßige Systemzeitzone, die für die Instanz angegeben ist, in der sie ausgeführt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	wird. Beispielsweise wird die geplante Aufgabe um 22:15 Uhr London-Zeit ausgeführt, wenn Europa/London die Standardsystemzeitzone für die Instanz ist, und Sie geben 22:15 Uhr in das Feld Zeit ein. ○ Tatsächliche Zeitzone. ○ Beispielsweise wird die geplante Aufgabe um 13:30 Uhr in der Zeitzone „US Eastern“ ausgeführt, wenn Sie US/Eastern auswählen und 13:30 Uhr in das Feld Zeit eingeben.
run_as	Standardmäßig ist **Ausführen_ als** Feldwert ist leer. Sie können den Wert auf einen Domänenanwender festlegen, um ein Problem für eine bestimmte Domäne zu erstellen.

Konfigurieren Sie den Planer, um zu synchronisieren Jira Status bis ServiceNow® Automatisch

Konfigurieren Sie den Planer, um den Status von zu synchronisieren Jira Probleme mit Anwendungs-Schwachstellenelement, Container-Schwachstellenelementen und Aufgaben in der Tabelle „sn_vul_agile_manifest“.

Vorbereitungen
Erforderliche Rolle: Schedule_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Der Planer wird automatisch gemäß dem konfigurierten Zeitplan ausgeführt. Der Status der Datensätze, die in der Tabelle „Angreifbares Anwendungselement“, „Angreifbares Container-Element“, „Anwendungskorrekturaufgabe“ und „Container-Korrekturaufgabe“ erstellt wurden und in Probleme erstellt wurden Jira Wird entsprechend dem aktuellen Status des Problems in aktualisiert Jira Plattform basierend auf der Statuszuordnung in der Konfigurationsregel.

Alle Datensätze des angreifbaren Anwendungselements, des angreifbaren Container-Elements, der Anwendungskorrekturaufgabe und der Containerkorrektur, die in der Tabelle „sn_vul_agile_manifest“ erstellt wurden, werden für berücksichtigt Jira Problemerstellung.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben** > **Synchronisierungsstatus**an.
2. Sie können die Felder Ausführen, Zeitzone und Zeit im geplanten Skript ändern.

Formular „Geplante Skript-Ausführung“

Feld	Beschreibung
Ausführen	Zeitintervall für die Ausführung der geplanten Aufgabe:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Täglich: Wird täglich zu einem bestimmten Zeitpunkt ausgeführt ○ Wöchentlich: Wird wöchentlich zu einer bestimmten Uhrzeit und einem bestimmten Tag ausgeführt. ○ Monatlich: Wird monatlich zu einer bestimmten Uhrzeit und einem bestimmten Tag des Monats ausgeführt. ○ Regelmäßig: Wird in einem vorgegebenen, sich wiederholenden Intervall ausgeführt ○ Einmal: Wird nur für ein einzelnes Vorkommen ausgeführt ○ Bei Bedarf: Wird bei Bedarf sofort ausgeführt ○ Geschäftskalender: Eintragsstart: Wird an den Starteintragsdaten für den Geschäftskalender ausgeführt, den Sie im Feld auswählen. Eine geplante Aufgabe wird für das Startdatum jedes Geschäftseintrags ausgeführt, den Sie für den Geschäftskalender definiert haben. Wenn der Geschäftskalender beispielsweise ein Geschäftsjahr darstellt und das Beginndatum jedes Eintrags ein Geschäftsmonat ist, wird die geplante Aufgabe am ersten Tag jedes Monats ausgeführt. ○ Geschäftskalender: Eintragsende: Wird für das Enddatum des Geschäftskalenders ausgeführt, den Sie im Feld auswählen. Diese Auswahl wird auf dieselbe Weise ausgeführt wie Geschäftskalender: Eintragsbeginn, jedoch für die Enddaten der zugehörigen Geschäftskalendereinträge. **Hinweis:** Wenn Sie Geschäftskalender: Eintragsbeginn oder Geschäftskalender: Eintragsende auswählen, können Sie einen Offset-Faktor anwenden, um die Ausführung der Aufgabe vor oder nach der Zeitspanne des ausgewählten Geschäftskalenders zu planen. Weitere Informationen finden Sie in den Feldern Offset-Typ und Offset. Weitere Informationen zum Erstellen und Verwenden von Geschäftskalendern und zum Definieren von Geschäftskalendereinträgen finden Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	unter Create a business calendar Und Define business calendar entries .
Tag	Tag, an dem die geplante Aufgabe ausgeführt werden soll ○ Wenn für Ausführen die Option Wöchentlich festgelegt ist, geben Sie den Wochentag an. Wählen Sie zum Beispiel „Mittwoch“ aus. ○ Wenn Ausführen auf Monatlich eingestellt ist, wählen Sie den Tag im Monat. Wählen Sie beispielsweise 25 für den 25. Tag des Monats aus. Dieses Feld wird nur angezeigt, wenn Sie im Feld Ausführen die Option Monatlich oder Wöchentlich auswählen.
Wiederholungsintervall	Dauer des Wiederholungsintervalls für jede geplante Aufgabenausführung. Geben Sie die Dauer in Tagen, Stunden oder Minuten ein. Beispiel: ○ Um die regelmäßige Aufgabe alle vier Tage auszuführen, geben Sie in das Feld Tage den Wert 04 ein. ○ Um sie alle 26 Stunden auszuführen, geben Sie in das Feld Stunden den Wert 26 ein. ○ Wenn die regelmäßige Aufgabe in einem Intervall von 13:30:25 wiederholt werden soll, geben Sie in das Feld Stunden den Wert 13 ein. Geben Sie anschließend in die beiden nachstehenden unbeschrifteten Felder die Werte 30 und 25 ein.
Zeit	Uhrzeit, zu der die geplante Aufgabe ausgeführt werden soll, ausgedrückt in Stunden, Minuten und Sekunden im 24-Stunden-Format. Die Auswahl, die Sie im Feld Zeitzone treffen, bestimmt die Zeitzone für diesen Eintrag.
Zeitzone	Zeitzone, die mit dem Eintrag im Feld Zeit verwendet werden soll, wenn Sie die Uhrzeit angeben, zu der die regelmäßige Aufgabe ausgeführt werden soll. Wählen Sie einen Zeitzoneneintrag aus: ○ -Keine-: Verwenden Sie die Standardzeitzone für den angemeldeten Benutzer, der die regelmäßige Aufgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	erstellt. Die geplante Aufgabe wird beispielsweise um 16:45 Uhr US-Pazifik-Zeit ausgeführt, wenn es sich um die für den Benutzer zugewiesene Zeitzone handelt und wenn Sie 16:45 in das Feld Zeit eingeben. ○ Zeitzone des Systems verwenden: Verwenden Sie die standardmäßige Systemzeitzone, die für die Instanz angegeben ist, in der sie ausgeführt wird. Beispielsweise wird die geplante Aufgabe um 22:15 Uhr London-Zeit ausgeführt, wenn Europa/London die Standardsystemzeitzone für die Instanz ist, und Sie geben 22:15 Uhr in das Feld Zeit ein. ○ Tatsächliche Zeitzone. ○ Beispielsweise wird die geplante Aufgabe um 13:30 Uhr in der Zeitzone „US Eastern“ ausgeführt, wenn Sie US/Eastern auswählen und 13:30 Uhr in das Feld Zeit eingeben.
run_as	Standardmäßig ist der Feldwert Run_ as leer. Sie können den Wert als Wert des erforderlichen Domänenanwenders festlegen, um ein Problem für eine bestimmte Domäne zu erstellen.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute-Integration

Mit der Prisma Cloud Compute-Integration können Sie Hosts scannen, um Schwachstellen zu erkennen.

Ab Version 24.02.0 von Vulnerability Response, Sie können die Prisma Cloud Compute-Integration verwenden, um Schwachstellen auf den ausgeführten Hosts zu importieren. Die Prisma-Host-APIs ermöglichen das Abrufen umfassender Schwachstelleninformationen für einen bestimmten Host und bieten auch einen Snapshot der Host-Schwachstellen zu einem bestimmten Zeitpunkt. Diese API ermöglicht die regelmäßige Synchronisierung zwischen Prisma- und ServiceNow-Instanz. Da Prisma sowohl als SaaS-Lösung (Software as a Service) als auch als lokale Lösung angeboten wird, ist die Verwendung eines MID-Servers erforderlich, um Prisma-APIs von der ServiceNow-Instanz aus aufzurufen. Darüber hinaus müssen Sie verwenden MID-Server Wenn Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Produkt und Ihr ServiceNow AI Platform Instanz befindet sich nicht in derselben Umgebung. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .

Sie können auch Berichte zu Schwachstellen und angreifbaren Elementen in anzeigen Vulnerability Response Dashboards. Diese Schwachstellen können dann priorisiert und behoben werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen werden angezeigt

Sie können die Integrationen anzeigen, die Teil von sind Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Um die Integrationen anzuzeigen, navigieren Sie zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Integrationen**an.

Die folgenden Integrationen sind verfügbar.

Ausführungssequenz	Zeitplan	Integration	Beschreibung
1	Täglich	Integration Von Prisma-Cloud-Compute-Hosts	Ruft Host-Schwachstellen ab und erstellt Vits, Erkennungen und erkannte Elemente für Hosts.

Hinweis:
Wenn das Plugin „Container Vulnerability Response“ installiert ist, können Sie auch Integrationen im Zusammenhang mit Container Vulnerability Response anzeigen.

Prisma-Integration Prozess

Wenn Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Wird ausgeführt, überprüft es, ob in der Tabelle National Vulnerability Database (NVD) eine Common Vulnerability and Exposure (CVE) vorhanden ist. Wenn sie bereits vorhanden ist, werden die vorhandenen Informationen verwendet. Wenn das CVE jedoch nicht gefunden wird, werden Platzhalterdatensätze in der NVD-Tabelle generiert. Beim Erstellen dieser Platzhalter-NVD-Datensätze werden anfänglich nur das CVE und sein Name ausgefüllt. Andere Details werden nicht mit der Annahme ausgefüllt, dass die NVD-Integration diese Details später ausfüllt. Wenn der Parameter der Integrationsinstanz *update_nvd*lst auf „wahr“ festgelegt, werden die Platzhalter-NVD-Datensätze aktualisiert. Standardmäßig ist der Instanzparameter auf „falsch“ festgelegt. Mindestens bis die NVD-Integration ausgeführt wird und diese Details ausfüllt, müssen Sie jedoch etwas über das CVE wissen, z. B. seinen Schweregrad oder einige grundlegende Informationen zum Problem. Um diese Anforderung zu erfüllen, die Felder **Exploit ist vorhanden** Und **Korrekturnotizen** Werden mit den aus Prisma erhaltenen Details ausgefüllt. Darüber hinaus kann diese Konfiguration angepasst werden, sodass Sie basierend auf den von Prisma bereitgestellten Informationen andere Felder angeben können, die Sie im NVD-Eintrag ausfüllen möchten.

Vorbereitung für Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Sie können sich auf vorbereiten Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Durch Ausführen von Setup-Aufgaben.

Bevor Sie beginnen

Zum Installieren und Konfigurieren von Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung können Sie die folgende Prüfliste drucken. Vergewissern Sie sich, dass die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und die Schwachstellendaten in importieren ServiceNow AI Platform® Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für Integrationsvorbereitung

Aufgabe	Beschreibung
☐	Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen: • API-Basis-URL • Anwendername und Passwort. Diese Anmeldeinformationen werden verwendet, um die Schwachstellen aus der Prisma Cloud Compute-Integration abzurufen. Weitere Informationen finden Sie unter https://pan.dev/compute/api/ **Hinweis:** MID-Server Ist optional. Die für die Prisma Cloud Compute-Integration verwendeten Anwenderanmeldeinformationen benötigen die Berechtigung zum Überwachen der Images. Siehe folgenden Code: `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	Wenn nicht bereits installiert und aktiviert, installieren Sie Vulnerability Response Anwendung, bevor Sie die Drittanbieteranwendung installieren. Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe Vulnerability Response installieren. Diese Integration erfordert Version 16,1 von Vulnerability Response Oder später.
☐	Rufen Sie Berechtigungen ab, und laden Sie herunter Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung auf Ihrem ServiceNow AI Platform® Instanz.
☐	Schätzen Sie die Anzahl der angreifbaren Elemente, die Sie importieren möchten. Überprüfen Sie, ob Ihre Instanz die Anzahl der angreifbaren Elemente akzeptieren kann, die Sie importieren möchten. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an ServiceNow Technischer Support.
☐	Stellen Sie sicher, dass Sie über die folgenden Gruppen oder Anwender verfügen, um die Integrationen zu verwalten und die angreifbaren Elemente zu beheben: **Administrator** Installieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Wenn nicht zugewiesen, weist der Administrator den Container-Schwachstellenadministrator (sn_vul_Container.Vulnerability_admin) und andere Rollen zu. **sn_vul_Container.Vulnerability_admin** Schließt die Konfiguration der Prisma Cloud Compute-Integration ab. Diese Rolle hat vollständigen Zugriff auf Container

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für Integrationsvorbereitung (Fortsetzung)

Aufgabe	Beschreibung
	Vulnerability Response(CVR)-Anwendung und ihre Datensätze. Dieser Administrator konfiguriert Integrationen und Regeln in Container Vulnerability Response. **Vulnerability Response-Gruppe** Standardmäßig ist die Vulnerability Response-Gruppe verfügbar. Anwender, die der Vulnerability Response-Gruppe zugewiesen sind, erben sn_vul.read_all, sn_vul_Container.read_all. **Besitzergruppe Für Container-Korrektur** Standardmäßig ist die Besitzergruppe Container-Korrektur verfügbar. Anwender, die dieser Gruppe zugewiesen sind, erben sn_vul_Container.Remediation_owner. Der Besitzer der Container-Korrektur korrigiert Container-Schwachstellen, die ihm oder einer Gruppe zugewiesen sind, zu der er gehört. **Schwachstellenanalyst** Anwender, die der Container-Schwachstellenanalyst-Gruppe zugewiesen sind, erben sn_vul.Vulnerability_Analyst. Der Schwachstellenanalyst überwacht die Nachbesserung aller angreifbaren Elemente. Wenn Sie noch nicht erstellt haben, können Sie zusätzliche Gruppen erstellen und Anwender mit dem Modul „Anwenderverwaltung“ in Ihrer Instanz hinzufügen. Weitere Informationen finden Sie unter Erstellen Sie eine Anwendergruppe .
☐	Installieren Sie Vulnerability Response Integration mit NVD und Ausführen der NIST National Vulnerability Database Integration – API (nur CVE).

Sie sind bereit für Konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute installieren

Bevor Sie die Integration in Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte aus, damit das Prisma Cloud Compute-Produkt ordnungsgemäß in integriert wird Vulnerability Response Und Container Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich bei der Instanz an, die Sie installieren möchten Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Ein.
2. Navigieren Sie zum ServiceNow Store.
3. In ServiceNow Store, Suchen nach Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie **Andere Anforderungen** Und **Abhängigkeiten** Abschnitte, falls erforderlich.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Aktualisieren Sie **Instanzname** Und **Grund für die Instanz** Felder, und klicken Sie auf **Validieren Sie Die Instanz** .
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**an.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.

Ergebnisse
Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Nächste Maßnahme
Konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Für Ihre Umgebung. Weitere Informationen finden Sie unter Konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung.

Konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung

Installieren und konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung zum Importieren von Daten aus Prisma Cloud Compute. Sie können die importierten Daten verwenden, um Schwachstellen für Ihre Hosts zu priorisieren und zu beheben.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie die E-Mail von ServiceNow Die Sie über die Integration erhalten haben.
2. Melden Sie sich als Administrator bei Ihrer Instanz an.
3. Befolgen Sie die Anweisungen in der E-Mail, um den zu erhalten Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
4. Navigieren zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Administration** > **Konfiguration**an.
   Füllen Sie die Felder im Formular „Prisma-Cloud-Compute-Konfiguration“ aus. Weitere Informationen finden Sie unter Formular „Konfiguration von Prisma-Cloud-Computing“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie in der Liste Projekte eine der Optionen aus **Alle Projekte** Oder **Bestimmte Projekte** Um entweder alle Projekte oder ausgewählte Projekte zu konfigurieren.
   Wenn Sie auswählen **Bestimmte Projekte** , Sie können die Projekte aus der Liste verfügbar auswählen.
6. Schließen Sie die Konfiguration ab, indem Sie eine der Optionen auswählen **Beenden** Oder **Anmeldeinformationen speichern und testen** .
   - Wenn Sie ein Projekt konfiguriert haben, wählen Sie aus **Beenden** .
   - Wenn Sie kein Projekt konfiguriert haben, wählen Sie aus **Anmeldeinformationen speichern und testen**
7. Zeigen Sie die neu erstellte Instanz an, indem Sie zu navigieren **Prisma-Cloud-Computing-Integration** > **Administration** > **Integrationsinstanzen**an.
8. Zeigen Sie die Projekte an, die Sie zuvor konfiguriert haben, indem Sie auswählen **Integrationsinstanzparameter** .
9. Führen Sie die neu erstellte Integrationsinstanz aus, um die angreifbaren Elemente zu importieren.
   Die Vits werden basierend auf der Granularität weiter erstellt.
10. Konfigurieren Sie die Granularität eines angreifbaren Elements.

    a. Navigieren zu **Prisma-Cloud-Computing-Integration** > **Image-Schwachstellenschlüssel konfigurieren**

    b. Konfigurieren Sie die Granularität der Vits, indem Sie die erforderlichen Kontrollkästchen aktivieren.
    Die angreifbaren Elemente werden basierend auf den beim nächsten Import ausgewählten Schlüsseln erstellt.

    Hinweis:
    Standardmäßig wird eine VIT für eine Kombination aus Image-Repository,] Schwachstelle und Image-Tag erstellt. Sie können dem Schlüssel Komponenten hinzufügen, um eine weitere Granularität zu erzielen. Sie können beispielsweise ein CVIT für eine Kombination aus Image-Repository, Schwachstelle, Image-Tag und Cluster erstellen. Sobald die Ergebnisse angreifbarer Elemente oder angreifbarer Elemente erstellt wurden, können die Kontrollkästchen nicht mehr bearbeitet werden.

Statusdiagramm der Integrationsausführung für Prisma Cloud Compute-Integration

Das Modul „Status der Prisma Cloud Compute-Integration“ bietet Ihnen eine grafische Ansicht des Status von Prisma Cloud Compute-Integrationsausführungen.

Zeigen Sie im Diagramm auf einen beliebigen Teil des Diagramms, um eine Zusammenfassung der für diesen Teil spezifischen Daten anzuzeigen. Wenn Sie auf ein Teil im Balkendiagramm klicken, wird eine Liste geöffnet, die detailliertere Informationen enthält.

Erforderliche Rolle: Schwachstellenadministrator

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender in der Vulnerability Response-Anwendung tun und sehen können. Informationen zur anfänglichen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.

Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

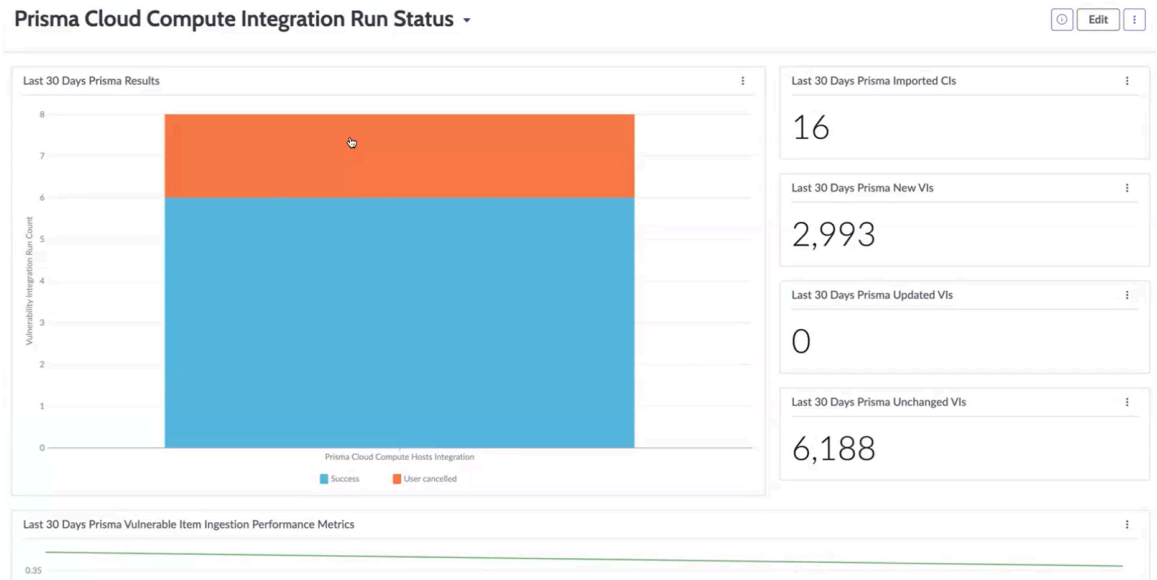
Um die Daten anzuzeigen, navigieren Sie zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Status der Integrationsausführung**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard ist in der neuen Experience-UI verfügbar.

Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Ausführungsstatus



Statusdiagrammberichte der Prisma Cloud Compute-Integration

Name	Beschreibung
Prisma-Ergebnisse der letzten 30 Tage	Die Anzahl der für die Integration abgeschlossenen Integrationsausführungen. Zeigt sowohl erfolgreiche als auch fehlgeschlagene Ausführungen an. Jede Ausführung wird als Balken im Diagramm angezeigt.
In den letzten 30 Tagen importierte Prisma-CIs	Die Anzahl der Configuration Items (CIs), die in den letzten 30 Tagen von Prisma importiert wurden. Wird als Ganzzahl angezeigt.
Neue Prisma-VIS der letzten 30 Tage	Die Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Aktualisierte Prisma-VIS der letzten 30 Tage	Die Anzahl der aktualisierten angreifbaren Elemente (VIS), die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Unveränderte Prisma-VIS der letzten 30 Tage	Die Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Leistungsmetriken Der Erfassung Angreifbarer Prisma-Elemente In Den Letzten 30 Tagen	Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich zu den letzten 30 Tagen.

Verstehen von Wiz Vulnerability Response Integration

Importieren Sie Schwachstellen- und Compliance-Daten aus Wiz Scanner in Ihren ServiceNow® KI-Plattforminstanz, mit der Sie tiefere Einblicke in Ihre Cloud-Infrastrukturrisiken erhalten. Diese Integrationen bieten Ihnen eine umfassende Bewertung Ihrer allgemeinen Cloud-Sicherheitslage und helfen Ihnen, Korrekturmaßnahmen direkt von Ihrer Instanz aus durchzuführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen, die in enthalten sind Vulnerability Response Integration mit Wiz

Die Vulnerability Response Integration mit Wiz Enthält die folgenden Integrationen, die Schwachstellen- und Compliance-Daten importieren:

- Wiz Host-Schwachstellenintegration
- Wiz Container Vulnerability Response Integration
- Wiz Konfigurations-Compliance (Testergebnisse) Integration und Problemintegration

Vorteile und Anwender für die Integrationen

Leistung	Wiz Integration	Anwender
Importieren und bewerten Sie frühzeitige Erkennungen von Host-Schwachstellen und -Schwachstellen auf ausgeführten Hosts. Die Host-Schwachstellenintegration importiert Ergebnisse im Zusammenhang mit virtuellen Computern und serverlosen Assets in Ihrer Cloud-Umgebung. Diese Ergebnisse werden angreifbaren Host-Elementen (Vits) in zugeordnet Vulnerability Response Anwendung zur Unterstützung von Korrekturworkflows.	Wiz Host-Schwachstellenintegration.	Schwachstellenmanager, Analysten und Cloud-Sicherheitsteams
Importieren und bewerten Sie Container-Image-Schwachstellendaten für angreifbare und nicht konforme Assets in Ihrer Cloud-Infrastruktur. Ergebnisse werden angreifbaren Container-Elementen (CVITs) zugeordnet, um Selektierung, Risikopriorisierung und gezielte Korrektur-Workflows für containerbasierte Arbeitsauslastungen zu unterstützen.	Wiz Container-Schwachstellenintegration.	Schwachstellenmanager, Analysten und Cloud-Sicherheitsteams
Importieren und bewerten Sie Konfigurationstestergebnisse aus Wiz Um nicht konforme Cloud-Konfigurationen zu erkennen. Ergebnisse werden Cloud-Testergebnissen (CTRs) in zugeordnet Konfigurations-Compliance Anwendung, mit der Sie Sicherheitsrichtlinien und -Standards in Ihrer Cloud-Umgebung durchsetzen können. **Hinweis:** Hostkonfigurationen von Wiz Werden nicht importiert.	Wiz Konfigurations-Compliance Integration (Wiz Testergebnisse).	Schwachstellenmanager, Analysten und Cloud-Sicherheitsteams
Importieren Wiz Probleme, die Assets identifizieren, die an toxischen Kombinationen von Schwachstellen und Fehlkonfigurationen beteiligt sind.	Wiz Probleme Bei Der Integration.	Schwachstellenmanager, Analysten und Cloud-Sicherheitsteams

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Leistung	Wiz Integration	Anwender
Diese Ergebnisse werden CTRs zugeordnet und mit gekennzeichnet Wiz-Probleme Als Quelle, die Ihnen hilft, Assets nachzuverfolgen und zu beheben, die komplexe Multi-Vektor-Risiken darstellen können.		
Wenden Sie Korrekturschritte auf angreifbare Host-Elemente (Vits), angreifbare Container-Elemente (CVTs), Cloud-Testergebnisse (CTRs) und bezeichnete CTRs an Wiz-Probleme .	Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance Anwendungen.	Korrekturbesitzer

Empfehlungen für weitere Themen

Weitere Informationen zum Installieren, Konfigurieren und Anzeigen importierter Daten mit finden Sie Wiz Vulnerability Response-Integration, siehe:

- Aktivieren Sie Wiz Vulnerability Response Integrationsanwendung
- Konfigurieren Sie Wiz Vulnerability Response Integration
- Legen Sie die Filterung für fest Wiz Integration Von Host-Schwachstellen
- Legen Sie die Filterung für fest Wiz Integration Von Container-Schwachstellen
- Legen Sie die Filterung für fest Wiz Integration Von Testergebnissen
- Legen Sie die Filterung für fest Wiz Probleme Bei Der Integration
- Feldzuordnung für Wiz Vulnerability Response-Integrationen

Aktivieren Sie Wiz Vulnerability Response Integrationsanwendung

Aktivieren Sie die erforderliche Anwendung.

Vorbereitungen
Überprüfen Sie, ob Sie die Prüflisten überprüft und Folgendes installiert haben ServiceNow® Anwendungen:

- Installation von Vulnerability Response Und unterstützte Anwendungen Die die NVD-Integration umfassen, Vulnerability Response Integration mit CISA und der geplanten CWE-Aufgabe.
- Vulnerability Response und Configuration Compliance für Container.
- Konfigurations-Compliance.

  Diese Anwendungen sind als separate Abonnements verfügbar. Siehe Install a ServiceNow Store application Weitere Informationen zur Installation von Store-Anwendungen.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen**an.
2. Suchen Sie nach Wiz Vulnerability Response Integrationsanwendung .
3. Wählen Sie die Karte aus, um sie zu öffnen, und wählen Sie sie aus **Installieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Siehe Install a ServiceNow Store application Weitere Informationen zur Installation von Store-Anwendungen.
Das Dialogfeld Abhängigkeitsprüfliste wird angezeigt. Wählen Sie beliebig aus **(Muss installiert werden)** Links zum Installieren der erforderlichen Abhängigkeiten, die Sie noch nicht installiert haben.

4. Wählen Sie Aus **Installieren** Im Dialogfeld „Anwendungsinstallation“.
   Eine Meldung wird angezeigt, nachdem die Anwendung erfolgreich installiert wurde. Sie sind bereit für Konfigurieren Sie Wiz Vulnerability Response Integration.
5. Navigieren zu **Alle** > **Wiz-Schwachstellenintegration** > **Administration** > **Integrationen**an.
6. Überprüfen Sie, ob die Integrationen, mit denen Sie Daten importieren möchten, aktiviert sind (Spalte „aktiv“ auf festgelegt Wahr).
7. Wählen Sie einen Datensatz aus, um ihn zu öffnen und die Integrationen zu aktivieren oder zu deaktivieren.

Konfigurieren Sie Wiz Vulnerability Response Integration

Konfigurieren Sie die Integration in Wiz Service-Account und weisen Sie Rollen in zu ServiceNow KI-Plattforminstanz.

Vorbereitungen

Sie müssen die Integrationskachel in konfigurieren Wiz Account, der für diese Integration mit den vorausgewählten Berechtigungen erstellt wurde. Siehe Wiz Produktdokumentation für weitere Informationen.

Erforderliche Rolle:

- administrator zum Zuweisen von Rollen in Ihrem ServiceNow KI-Plattforminstanz.

Prozedur

1. Weisen Sie Anwendern für die Rollen zu Wiz-Integration und für die -Anwendungen, die in der -Integration in unterstützen ServiceNow KI-Plattforminstanz.

   a. Navigieren zu **Benutzeradministration** > **Anwender**

   b. Weisen Sie die folgenden Rollen zu.

   - sn_vul.Vulnerability_admin zum Konfigurieren von Vulnerability Response Und Container Vulnerability Response Anwendungen.
   - sn_vulc.admin
   - sn_vul_wiz.configure_Integration zum Einrichten der Integration.
   - sn_vul_wiz.read_Integration für die Anwender in Ihrer Organisation, die Daten und Datensätze für diese Integration anzeigen möchten.

   c. Siehe User administration Weitere Informationen zum Erstellen von Anwendern und zum Verwalten von Rollen.

2. Navigieren Sie als Anwender mit der Rolle sn_vul_wiz.configure_Integration zu **Alle** > **Wiz-Schwachstellenintegration** > **Administration** > **Konfiguration** In Ihrer Instanz.
3. Füllen Sie die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Integrationsinstanz	Vulnerability Response-Integration mit Wiz.
Authentifizierungs-URL	Authentifizierungs-URL, die Sie in eingegeben haben Wiz Umgebung.
API-URL	API-URL, die Sie in eingegeben haben Wiz Umgebung.
Client-ID	Client-ID, die Sie für diese Integration verwenden möchten, die Sie in eingegeben haben Wiz Umgebung.
Geheimer Clientschlüssel	Geheimer Client-Schlüssel, den Sie für diese Integration verwenden möchten, die Sie in eingegeben haben Wiz Umgebung.

4. **Wählen Sie Speichern und testen** .
   Wenn die Anmeldeinformationen erfolgreich gespeichert und validiert wurden, wird eine Meldung angezeigt. Sie können Filterung für die Integrationsimporte auswählen.

Legen Sie die Filterung für fest Wiz Integration Von Host-Schwachstellen

Legen Sie die Filterwerte fest, um die gewünschten Host-Schwachstellendaten zu importieren.

Vorbereitungen

Erforderliche Rolle: sn_vul_wiz.configure_Integration

Prozedur

1. Navigieren zu **Alle** > **Wiz-Schwachstellenintegration** > **Administration** > **Konfiguration**an.
2. Wenn nicht bereits ausgewählt, wählen Sie aus **Konfiguration Von Host-Schwachstellen** Registerkarte.
3. Füllen Sie die Felder aus.
   Diese angezeigten Felder enthalten Filter zum Importieren grundlegender Host-Schwachstellendaten. Um weitere Filteroptionen anzuzeigen, wählen Sie aus **Erweitert** Kontrollkästchen, und weitere Informationen finden Sie in der nächsten Tabelle.

Feld	Beschreibung
Erste(r)	Paginierung. Geben Sie einen Wert ein. Möglicherweise möchten Sie mit 1000 beginnen.
Schweregrad	Schweregrad wird gefunden. „Keine“ ist der Standard. Wenn diese Option ausgewählt ist, werden keine Daten für dieses Feld importiert. Sie können mehrere Werte angeben: ○ KEINE: Assets OHNE verfügbare Schweregradwerte zurückgeben. ○ LOW ○ MEDIUM

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ HIGH ○ CRITICAL
Ressourcenstatus	Gibt nur Schwachstellenergebnisse für Assets mit diesen Status zurück. Sie können mehrere Werte angeben: ○ Keine (Standard): Wenn diese Option ausgewählt ist, werden keine Daten für dieses Feld importiert. ○ Aktiv ○ Fehler ○ Inaktiv
Ressourcentyp	Filtern Sie nach diesen Objekttypen. Sie können beide Werte angeben: ○ Keine (Standard): Wenn diese Option ausgewählt ist, werden keine Daten für dieses Feld importiert. ○ VIRTUAL_MACHINE ○ SERVERLESS

4. Aktivieren Sie das Kontrollkästchen Erweitert, um weitere Filteroptionen anzuzeigen.

   Für die meisten Felder können Sie mehrere Werte angeben. --Keine-- Ist (Standard). Wenn --Keine-- Bleibt für ein Feld ausgewählt, für dieses Feld werden keine Daten importiert.

Feld	Beschreibung
Status	Nach Ergebnisstatus filtern: ○ OFFEN ○ ABGELEHNT ○ RESOLVED
Erkennungsmethode	Filtern Sie nach Schwachstellenergebnissen, die mit diesen Erkennungsmethoden gefunden wurden: ○ PACKAGE ○ DEFAULT_PACKAGE ○ LIBRARY ○ BS ○ INSTALLED_PROGRAM ○ INSTALLED_PROGRAM_BY_SERVICE ○ FILE_PATH

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schweregrad des zugehörigen Problems	○ CRITICAL ○ HIGH ○ INFORMATIONAL ○ LOW ○ MEDIUM
Schwachstelle	Filtern Sie nach Schwachstellen-Ergebnissen mit übereinstimmenden externen IDs, die Sie eingeben, z. B. CVE-1234-5678,CVE-9110-26117.
Hat öffentlichen Exploit	Filtern Sie nach Schwachstellen-Ergebnissen für Schwachstellen mit einem verfügbaren Exploit: (Wahr/falsch).
Projekt-ID	Filtern Sie nach Schwachstellen-Ergebnissen mit Zeichenfolgen, die Sie für die angegebenen Projekte eingeben.
Hat Korrektur	Filtern Sie nach Schwachstellen-Ergebnissen für Schwachstellen mit einer verfügbaren Korrektur (wahr/falsch).
Ressource	Filtern Sie nach einer von Ihnen eingegebenen Ressource.
Ressource hat Administratorberechtigungen	Filtern Sie nach Schwachstellen-Ergebnissen für Assets mit Administratorrechten (wahr/falsch).
Abonnement	Importieren Sie Ergebnisse aus den folgenden Zeichenfolgen für externe Abonnements: (AWS-Account, Azure-Abonnement, GCP-Projekt und OCI-Compartment). Sie können mehrere Werte in einem Array angeben. Wenn Sie keinen Wert angeben, werden alle Abonnements zurückgegeben.
Hat CISA-KEV-Exploit	Filtern Sie nach Schwachstellen-Ergebnissen für Schwachstellen mit einem verfügbaren CISA-KEV-Exploit (wahr/falsch).
Ressource hat hochrangige Zugriffsrechte	Filtern Sie nach Schwachstellen-Ergebnissen für Assets mit hohen Berechtigungen (wahr/falsch).
Ressource hat ausgedehntes Internetrisiko	Filtern Sie nach Schwachstellen-Ergebnissen für Assets mit hohem Internetrisiko (wahr/falsch).
Ressource hat eingeschränktes Internetrisiko	Filtern Sie nach Schwachstellen-Ergebnissen für Assets mit geringem Internetrisiko (wahr/falsch).
Zuerst gesehen um (Nach)	Filtern Sie nach Assets, die ab einem von Ihnen ausgewählten Datum angezeigt werden.
Gelöst um (nach)	Filtern Sie nach Assets mit Schwachstellen, die ab einem von Ihnen ausgewählten Datum gelöst wurden.
Aktualisiert um (nach)	Filtern Sie nach Assets, die ab einem von Ihnen ausgewählten Datum aktualisiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Wählen Sie Speichern und testen** .
   Wenn die Anmeldeinformationen gespeichert und erfolgreich validiert wurden, wird eine Meldung angezeigt. Sie können Filtern für einen anderen Integrationsimport auswählen.

Legen Sie die Filterung für fest Wiz Integration Von Container-Schwachstellen

Legen Sie die Filterwerte fest, um die gewünschten Container-Schwachstellendaten zu importieren.

Vorbereitungen

Erforderliche Rolle: sn_vul_wiz.configure_Integration

Prozedur

1. Navigieren zu **Alle** > **Wiz-Schwachstellenintegration** > **Administration** > **Konfiguration**an.
2. Wählen Sie aus **Konfiguration Von Container-Schwachstellen** Registerkarte.
3. Füllen Sie die Felder aus.

   Für einige Felder können Sie mehrere Werte angeben. --Keine-- Ist (Standard). Wenn --Keine-- Bleibt für ein Feld ausgewählt, für dieses Feld werden keine Daten importiert.

Feld	Beschreibung
Erste(r)	Paginierung. Geben Sie einen Wert ein. Möglicherweise möchten Sie mit 1000 beginnen.
Hat öffentlichen Exploit	Filtern Sie nach Schwachstellen-Ergebnissen für Schwachstellen mit einem verfügbaren Exploit: (Wahr/falsch).
Abonnement	Importieren Sie Ergebnisse aus den folgenden Zeichenfolgen für externe Abonnement-IDs: (AWS-Account, Azure-Abonnement, GCP-Projekt und OCI-Compartment). Wenn Sie keinen Wert angeben, werden alle Abonnements zurückgegeben.
Hat Korrektur	Importieren Sie Schwachstellenergebnisse für Schwachstellen mit einer verfügbaren Korrektur (wahr/falsch).
Schwachstelle	Importieren Sie Schwachstellenergebnisse mit übereinstimmenden externen IDs, z. B. CVE-1234-5678,CVE-9110-26117.
Hat CISA-KEV-Exploit	Importieren Sie nur Schwachstellenergebnisse für Schwachstellen mit einem verfügbaren CISA-KEV-Exploit (wahr/falsch).
Projekt-ID	Importieren Sie nur Schwachstellenergebnisse für die angegebenen Projekte (Zeichenfolgen).
Ressource hat hochrangige Zugriffsrechte	Gibt nur Schwachstellenergebnisse zurück, die hohe Berechtigungen haben (wahr/falsch).
Ressourcenstatus	Gibt nur Ergebnisse mit diesen Status zurück. Sie können mehrere Werte angeben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Aktiv ○ Fehler ○ Inaktiv
Ressource hat Administratorberechtigungen	Gibt nur Schwachstellenergebnisse zurück, die über Administratorrechte verfügen. (Wahr/falsch)
Erkennungsmethode	Filtern Sie nach Schwachstellenergebnissen, die mit diesen Erkennungsmethoden gefunden wurden: ○ DEFAULT_PACKAGE ○ FILE_PATH ○ INSTALLED_PROGRAM ○ INSTALLED_PROGRAM_BY_SERVICE ○ LIBRARY ○ BS ○ PACKAGE
Ressource hat eingeschränktes Internetrisiko	Filtern Sie nach Schwachstellen-Ergebnissen mit geringem Internetrisiko (wahr/falsch).
Schwachstellenschweregrad	Ergebnisse nach Schwachstellenschweregrad filtern: ○ CRITICAL ○ HIGH ○ LOW ○ MEDIUM
Status	Ergebnisse nach Status filtern: ○ OFFEN ○ RESOLVED

4. **Wählen Sie Speichern und testen** .
   Wenn die Anmeldeinformationen gespeichert und erfolgreich validiert wurden, wird eine Meldung angezeigt. Sie können Filtern für einen anderen Integrationsimport auswählen.
5. **Wahlweise:** Konfigurieren Sie die Granularität der angreifbaren Container-Elemente (CVITs), indem Sie die Schlüsselkombination angeben.

   (Optional) Ein CVIT wird standardmäßig durch die Kombination von Image-Repository, Schwachstelle und Image erstellt. Sie können dem Schlüssel Komponenten hinzufügen, um eine weitere Granularität zu erzielen. Erstellen Sie beispielsweise ein CVIT für eine Kombination aus Image-Repository, Schwachstelle, Image und Cluster.

   Navigieren Sie zum Konfigurieren der Granularität zu **Alle** > **Wiz-Schwachstellenintegration** > **Administration** > **CVS-basierte-VI-Granularität konfigurieren**an.

   Wählen Sie die Schlüssel aus, die Sie hinzufügen möchten. Wenn Daten importiert werden, werden Schlüssel berücksichtigt, und CVITs werden erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie die Filterung für fest Wiz Integration Von Testergebnissen

Legen Sie die Filterwerte fest, um die gewünschten Cloud-Testergebnisdaten zu importieren.

Vorbereitungen

Erforderliche Rolle: sn_vul_wiz.configure_Integration

Prozedur

1. Navigieren zu **Alle** > **Wiz-Schwachstellenintegration** > **Administration** > **Konfiguration**an.
2. Wählen Sie aus **Testergebniskonfiguration** Registerkarte.
3. Füllen Sie die Felder aus.

Für einige Felder können Sie mehrere Werte angeben. --Keine-- Ist (Standard). Wenn --Keine-- Bleibt für ein Feld ausgewählt, für dieses Feld werden keine Daten importiert.

Hinweis:
Hostkonfigurationen von Wiz Werden nicht importiert.

Feld	Beschreibung
Schweregrad	Wählen Sie eine Option für die Schweregradfilterung aus: ○ LOW ○ MEDIUM ○ HIGH ○ CRITICAL ○ KEINE: Gibt Ergebnisse ohne verfügbare Schweregradwerte zurück. Möglicherweise möchten Sie mit HOCH oder KRITISCH beginnen, um Ihren Import auf Ergebnisse von kritischer Bedeutung zu beschränken.
Projekt-ID	Geben Sie nur Cloud-Konfigurationsergebnisse für Projekte an, z. B. Mit dem Namen „Projekt-ID“ .
Cloud-Plattform	Konfigurationsergebnisse nach Cloud-Plattform. Sie können mehrere Werte angeben, z. B. AWS, GitHub, Terraform, OPENAI, GKE, OKE, EKS, AKS.
Abonnement-ID	Geben Sie diese durch Eingabe der Abonnement-ID an. Sie können mehrere Werte in einem Array angeben.
Ressourcenstatus	Nach Status angeben: ○ Aktiv ○ Fehler ○ Inaktiv

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Framework-Kategorie	Geben Sie Sicherheits-Frameworks, Sicherheitsunterkategorien oder Sicherheitskategorien ein. Sie können mehrere Werte angeben.
Ressourcentyp	Entitätstypen. Sie können mehrere Werte angeben, z. B. BUCKET, DATENBANK
Nativer Typ	Geben Sie Ergebnisse basierend auf dem nativen Typ der Cloud-Ressource an, z. B. Bucket .
Verfügt über Korrektur	Geben Sie die Ergebnisse mit an (WAHR) Oder ohne (FALSCH) Korrekturanweisungen.
Erste(r)	Paginierung. Geben Sie einen Wert ein. Möglicherweise möchten Sie mit 1000 beginnen.
Analysiert nach	Filtern Sie Ergebnisse, die analysiert wurden, ab einem von Ihnen ausgewählten Datum.
Status	Nach Status filtern: ○ OFFEN ○ RESOLVED

4. **Wählen Sie Speichern und testen** .
   Wenn die Anmeldeinformationen gespeichert und erfolgreich validiert wurden, wird eine Meldung angezeigt. Sie können Filtern für einen anderen Integrationsimport auswählen.

Legen Sie die Filterung für fest Wiz Probleme Bei Der Integration

Legen Sie die zu importierenden Filterwerte fest Wiz Probleme, die Assets identifizieren, die an toxischen Kombinationen von Schwachstellen und Fehlkonfigurationen beteiligt sind.

Vorbereitungen

Erforderliche Rolle: sn_vul_wiz.configure_Integration

Prozedur

1. Navigieren zu **Alle** > **Wiz-Schwachstellenintegration** > **Administration** > **Konfiguration**an.
2. Wählen Sie aus **Problemkonfiguration** Registerkarte.
3. Füllen Sie die Felder aus.

   Für einige Felder können Sie mehrere Werte angeben. --Keine-- Ist (Standard). Wenn --Keine-- Bleibt für ein Feld ausgewählt, für dieses Feld werden keine Daten importiert.

Feld	Beschreibung
Schweregrad	Nach Ergebnisschweregrad filtern. ○ LOW ○ MEDIUM ○ HIGH

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ CRITICAL ○ INFORMATIONAL
Projekt-ID	Importieren Sie nur Ergebnisse für die angegebenen Projekte (Zeichenfolgen).
Problemtyp	Probleme nach Regeltyp, von dem sie generiert werden. ○ CLOUD_CONFIGURATION ○ THREAT_DETECTION ○ TOXIC_COMBINATION
Abonnement-ID	Geben Sie Ergebnisse an, indem Sie eine Abonnement-ID eingeben. Sie können mehrere Werte in einem Array angeben.
Cloud-Plattform	Konfigurationsergebnisse nach Cloud-Plattform. Sie können mehrere Werte angeben, z. B. AWS, GitHub, Terraform, OPENAI, GKE, OKE, EKS, AKS.
Framework-Kategorie	Geben Sie Sicherheits-Frameworks, Sicherheitsunterkategorien oder Sicherheitskategorien ein. Sie können mehrere Werte angeben.
Nativer Typ	Probleme basierend auf dem nativen Typ der Cloud-Ressource, z. B. Bucket .
Erste(r)	Paginierung. Geben Sie einen Wert ein. Möglicherweise möchten Sie mit 1000 beginnen.
Status	Nach Status filtern: ○ OFFEN ○ IN PROGRESS ○ RESOLVED

4. **Wählen Sie Speichern und testen** .
   Wenn die Anmeldeinformationen gespeichert und erfolgreich validiert wurden, wird eine Meldung angezeigt. Sie können Filtern für einen anderen Integrationsimport auswählen.

Feldzuordnung für Wiz Vulnerability Response-Integrationen

Überprüfen Sie Quell- und Zielfelder, und zeigen Sie importierte Daten zu Tabellen und Datensätzen in Ihrem an ServiceNow KI-Instanz der Now Platform.

Feldzuordnung für Host-Schwachstellenintegration

Wiz Feld	ServiceNow Tabellenspalte	ServiceNow Feldspalte
Beschreibung	sn_vul_Detection	Nachweis
status	sn_vul_Detection	Source_Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wiz Feld	ServiceNow Tabellenspalte	ServiceNow Feldspalte
LastDetectedAt	sn_vul_Detection	Last_found
ErstDetectedAt	sn_vul_Detection	first_found
vulnerableAsset.name	sn_vul_Detection	dns
Korrektur	sn_vul_Detection	Solution_Summary
Angreifbares Asset.ipAddresses[0]	sn_vul_Detection	ip_address
VendorSchweregrad	sn_vul_Detection	Source_severity
Fixierte Version	sn_vul_Detection	Fixed_Version
status	sn_vul_Detection	Ist_ignoriert
status	sn_vul_Detection	status
name	sn_vul_nvd_entry	id
Punktzahl	sn_vul_nvd_entry	V3_Base_Score
CVEBeschreibung	sn_vul_nvd_entry	Zusammenfassung
VendorSchweregrad	sn_vul_nvd_entry	Source_severity
Cvssv3.attackVector	sn_vul_nvd_entry	V3_Attack_Vector
Cvssv3.attackComplexity	sn_vul_nvd_entry	V3_Attack_Complex
Cvssv3.VertraulichkeitImpact	sn_vul_nvd_entry	V3_Vertraulichkeit_Auswirkung
Cvssv3.privilegesRequired	sn_vul_nvd_entry	V3_Privilegien_erforderlich
cvssv3.integrityImpact	sn_vul_nvd_entry	V3_Integrity_Impact
cvssv3.userInteractionRequired	sn_vul_nvd_entry	V3_user_Interaction
HasExploit	sn_vul_nvd_entry	Exploit
HasCisaKevExploit	sn_vul_nvd_entry	cisa_exists
SchwachstellenAsset.Tags	sn_sec_cmn_src_ci	Host_Tag
vulnerableAsset.id	sn_sec_cmn_src_ci	source_id
vulnerableAsset.name	sn_sec_cmn_src_ci	name
SchwachstellenAsset.Region	sn_sec_cmn_src_ci	Cloud_Region
vulnerableAsset.providerUniqueId	sn_sec_cmn_src_ci	resource_id
SchwachstellenAsset.cloudPlatform	sn_sec_cmn_src_ci	Cloud_Service_Provider
SchwachstellenAsset.Typ	sn_sec_cmn_src_ci	assetType
ZugehörigIssueAnalytics	sn_sec_cmn_src_ci	Source_Data
SchwachstellenAsset.nativeType	sn_sec_cmn_src_ci	Cloud_resource_type
SchwachleAsset.subscriptionExternalId	sn_sec_cmn_src_ci	cloud_account
vulnerableAsset.name	sn_sec_cmn_src_ci	resource_name
SchwachstellenAsset.ImageName	sn_sec_cmn_src_ci	image_id
Angreifbares Asset.*	sn_sec_cmn_src_ci	Source_Data
LastDetectedAt	sn_sec_cmn_src_ci	Source_Data

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldzuordnung für Container-Schwachstellenintegration

Wiz Feld	ServiceNow Tabellenspalte	ServiceNow Feldspalte
imageID	sn_vul_Container_image	image_id
vulnerableAsset.name	sn_vul_Container_image	image_name
SchwachstellenAsset.Repository.externalId nach ##	sn_vul_Container_image	Registrierung
SchwachstellenAsset.Repository.externalId vor ##	sn_vul_Container_image	Repository
SchwachstellenAsset.Tags	sn_vul_Container_image	Image_Bezeichnungen
Projekte	sn_vul_Container_image	Image_Projects
SchwachstellenAsset.Region	sn_vul_Container_image	Cloud_Regions
SchwachstellenAsset.cloudPlatform	sn_vul_Container_image	Cloud_Provider
SchwachleAsset.subscriptionExternalId	sn_vul_Container_image	Cloud_Account_IDs
vulnerableAsset.executionControllers.nvestors.name	sn_vul_Container_image	Image_Namespace
vulnerableAsset.executionControllers.nvestors.name	sn_vul_Container_image	Image_Cluster
vulnerableAsset.executionControllers.nvestors.name	sn_vul_Container_image_vulnerable_item	Image_Cluster
vulnerableAsset.executionControllers.nvestors.name	sn_vul_Container_image_vulnerable_item	Image_Namespace
SchwachstellenAsset.Repository.externalId vor ##	sn_vul_Container_image_vulnerable_item	Image_Repository
LayerMetadaten.isBaseLayer	sn_vul_Container_image_results	Ist_Base_image
ErstDetectedAt	sn_vul_Container_image_results	first_found
LastDetectedAt	sn_vul_Container_image_results	Last_found
DetailedName	sn_vul_Container_image_Package	name
Version	sn_vul_Container_image_Package	Version
LocationPath	sn_vul_Container_image_Package	path
name	sn_vul_nvd_entry	id
Punktzahl	sn_vul_nvd_entry	V3_Base_Score
CVEBeschreibung	sn_vul_nvd_entry	Zusammenfassung
Vendorschweregrad	sn_vul_nvd_entry	Source_severity
Cvssv3.attackVector	sn_vul_nvd_entry	V3_Attack_Vector
Cvssv3.attackComplexity	sn_vul_nvd_entry	V3_Attack_Complex
Cvssv3.VertraulichkeitImpact	sn_vul_nvd_entry	V3_Vertraulichkeit_Auswirkung
Cvssv3.privilegesRequired	sn_vul_nvd_entry	V3_Privilegien_erforderlich
cvssv3.integrityImpact	sn_vul_nvd_entry	V3_Integrity_Impact
cvssv3.userInteractionRequired	sn_vul_nvd_entry	V3_user_Interaction
HasExploit	sn_vul_nvd_entry	HasExploit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wiz Feld	ServiceNow Tabellenspalte	ServiceNow Feldspalte
LayerMetadaten.isBaseLayer	sn_vul_Container_image_Layer	Basisebene
layerMetadata.details	sn_vul_Container_image_Layer	Anweisung
layerMetadata.id	sn_vul_Container_image_Layer	id
status	sn_vul_Container_image_results	Ist_ignoriert
Validieren_at_Runtime	sn_vul_Container_image_results	Validieren_at_Runtime
id	sn_vul_Container_image_results	Unique_key

Konfigurations-Compliance Zuordnung des Integrationsfelds für Testergebnisse

Wiz Feld	ServiceNow Tabellenspalte	ServiceNow Feldspalte
Regel.ID	sn_vulc_Test	source_id
rule.name	sn_vulc_Test	short_description
Regel.Korrekturanweisungen	sn_vulc_Test	Korrektur
rule.description	sn_vulc_Test	Beschreibung
severity	sn_vulc_Test	Source_Relevanz
status	sn_vulc_result	Ergebnis
id	sn_vulc_result	source_id
Analysiert At	sn_vulc_result	last_seen
Erstes SeenAt	sn_vulc_result	first_seen
Regel.Korrekturanweisungen	sn_vulc_result	Korrektur
Resource.nativeType	sn_sec_cmn_src_ci	Source_Data
Resource.type	sn_sec_cmn_src_ci	Source_Data
id	sn_vulc_result	Beschreibung
id	sn_vulc_result	source_id
securitySubCategories.category.framework.id	sn_vulc_auth_src	source_id
securitySubCategories.category.framework.name	sn_vulc_auth_src	short_description
securitySubCategories.category.framework.description	sn_vulc_auth_src	Beschreibung
securitySubCategories.id	sn_vulc_Zitat	Abschnitt
Sicherheitsunterkategorien.Titel	sn_vulc_Zitat	Abschnittsname
resource.projects	sn_sec_cmn_src_ci	Projekte
status	sn_vulc_result	Ist_ignoriert

Probleme bei der Integration der Feldzuordnung

Hinweis:
Daten, die für die Ergebnisse von Problemintegration zu Cloud-Tests (CTRs) zugeordnet sind, werden mit gekennzeichnet Wiz-Probleme Als Quelle, die Ihnen hilft, diese CTRs von den Testergebnisintegrations-CTRs zu unterscheiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wiz Feld	ServiceNow Tabellenspalte	ServiceNow Feldspalte
sourceRule.id	sn_vulc_Test	source_id
sourceRule.name	sn_vulc_Test	short_description
SourceRule.resolutionRecommendation/ sourceRule.RemediationInstructions	sn_vulc_Test	Korrektur
sourceRule.description	sn_vulc_Test	Beschreibung
severity	sn_vulc_Test	Source_Relevanz
createdAt	sn_vulc_result	first_seen
updatedAt	sn_vulc_result	last_seen
status	sn_vulc_result	Ergebnis
id	sn_vulc_result	source_id
SourceRule.resolutionRecommendation/ sourceRule.RemediationInstructions	sn_vulc_result	Korrektur
SourceRule.controlDescription	sn_vulc_result	Beschreibung
EntitySnapshot.nativeType	sn_sec_cmn_src_ci	Source_Data
EntitySnapshot.type	sn_sec_cmn_src_ci	Source_Data
Wiz-Problem“	sn_vulc_result	result_type
id	sn_vulc_result	Beschreibung
severity	sn_vulc_Test	Source_Relevanz
id	sn_vulc_result	source_id
sourcerule.securitySubCategories.category.framework.id	sn_vulc_result	source_id
sourcerule.securitySubCategories.category.framework.name	sn_vulc_result	short_description
sourcerule.securitySubCategories.category.framework.description	sn_vulc_result	Beschreibung
sourcerule.securitySubCategories.id	sn_vulc_Zitat	Abschnitt
sourcerule.securitySubCategories.title	sn_vulc_Zitat	Abschnittsname
Projekte	sn_sec_cmn_src_ci	Projekte
status	sn_vulc_result	Ist_ignoriert

Zuordnung zu angreifbaren Elementen und Testergebnisdatensätzen

- Ergebnisse der Host-Schwachstellen werden angreifbaren Host-Elementen (Vits) zugeordnet.
- Container-Schwachstellen-Ergebnisse werden angreifbaren Container-Elementen (CVITs) zugeordnet.
- Konfigurationstestergebnisse werden Cloud-Testergebnisdatensätzen (CTRs) in zugeordnet Konfigurations-Compliance Anwendung.
- Problemergebnisse werden Cloud-Testergebnisdatensätzen (CTRs) in zugeordnet Konfigurations-Compliance Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie manuell eine Schwachstellenintegration

Schwachstellenintegrationen bieten Kunden und Lieferanten die Möglichkeit, die Schwachstellendaten in ihrer Instanz durch Abrufen von Daten von externen Systemen und Lieferanten zu ergänzen. Diese Fähigkeit kann den Lebenszyklus der Schwachstellenbeseitigung vereinfachen, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Detaillierte Anweisungen zum Erstellen von Integrationen finden Sie unter Definieren Sie eine neue Schwachstellenintegration.

Definieren Sie eine neue Schwachstellenintegration

Eine Schwachstellenintegration ruft Berichtsdaten aus einem Drittparteisystem ab, um im Allgemeinen Schwachstellendaten abzurufen, und verarbeitet diese Berichtsdaten mithilfe von Datenquellen oder einem anwenderdefinierten Prozessor.

Vorbereitungen

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Integrationen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder nach Bedarf aus.

Schwachstellenintegration

Feld	Beschreibung
Name	Ein beschreibender Name für die Integration.
Aktiv	Gibt an, ob die Integration aktiv ist. Wenn Sie nicht möchten, dass sie für einen bestimmten Zeitraum ausgeführt wird, können Sie die Parameter einrichten, die Sie verwenden möchten, und den Auftrag deaktivieren.
Ausführen	Die Häufigkeit, mit der die Integration ausgeführt werden soll, täglich, wöchentlich, regelmäßig usw. Wie bereits erwähnt, werden nachfolgende Felder basierend auf Ihren Einstellungen in diesem Feld angezeigt oder nicht.
Tag	Der Tag, an dem die Integration ausgeführt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Wenn Sie ausgewählt haben **Wöchentlich** In **Ausführen** Feld zeigt dieses Feld die Wochentage an. ○ Wenn Sie ausgewählt haben **Monatlich** In **Ausführen** Feld zeigt dieses Feld die Tage des Monats an.
Zeit	Die Zeit, zu der die Integration beginnen soll. Dieses Feld wird nur angezeigt, wenn Sie ausgewählt haben **Täglich** , **Wöchentlich** , Oder **Monatlich** In **Ausführen** Feld.
Anwendung	[Schreibgeschützt] der Name der Anwendung, für die diese Integration erstellt wurde.
Wiederholungsintervall	Wenn Sie ausgewählt haben **Regelmäßig** In **Ausführen** Feld zeigt dieses Feld die Anzahl der Tage und Stunden an, bevor die Integration erneut ausgeführt wird.
Wird gestartet	Wenn Sie ausgewählt haben **Regelmäßig** In **Ausführen** Feld zeigt dieses Feld die Daten und die Uhrzeit an, die als Ausgangspunkt für regelmäßige Aktualisierungen verwendet werden sollen.
Bedingt	Wählen Sie dieses Feld aus, wenn Sie bedingte Parameter hinzufügen möchten.
Bedingung	Wenn Sie ausgewählt haben **Bedingt** Kontrollkästchen: Geben Sie die Bedingungen hier ein.
Integrationsdetails	
Integrationsskript	Wählen Sie die Skripteinbindung aus, die die VulnerabilityIntegrationBase erweitert, die ausgeführt werden soll, wenn die Integration ausgeführt wird. Dieses Skript definiert, wie Daten aus einem Drittparteisystem abgerufen werden.
Integrationswerksskript	Geben Sie ein Skript ein, das definiert, wie die für ausgewählte Skripteinbindung erstellt werden soll **Integrationsskript** . Weitere Informationen finden Sie unter Integrationswerksskriptfelder. **Hinweis:** Skripts erfordern beides ServiceNow Und Vulnerability Response Fachwissen.
Berichtsprozessorstrategie	Wählen Sie die Strategie aus, die Sie verwenden möchten, um die Daten zu verarbeiten, die vom Integrationsskript zurückgegeben werden, wenn die Integration ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Wählen Sie Aus **Datenquellenanhang** Wenn Sie Daten mit einer Datenquelle verarbeiten möchten. ○ Wählen Sie Aus **Anwenderdefinierter Berichtsprozessor** Zum Auswählen eines anwenderdefinierten Prozessors.
Berichtsprozessor-Skript	Wenn Sie ausgewählt haben **Anwenderdefinierter Berichtsprozessor** In **Berichtsprozessorstrategie** Feld die Skripteinbindung auswählen, die die Skripteinbindung VulnerabilityReportProcessorBase erweitert, die bei Ausführung der Integration ausgeführt werden soll. Dieses Skript definiert, wie die vom Integrationsskript zurückgegebenen Daten verarbeitet werden.
Prozessorwerksskript	Geben Sie ein Skript ein, das definiert, wie die für ausgewählte Skripteinbindung erstellt werden soll **Berichtsprozessor** .

4. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Integrationsskript für Schwachstellen

Berichtsprozessorstrategien

Integrationswerksskriptfelder

Führen Sie eine Schwachstellenintegration manuell aus

Integrationsskript für Schwachstellen

Im Formular „Schwachstellenintegration“ ist das Integrationsskript ein Verweis auf eine Skripteinbindung, die die Skripteinbindung VulnerabilityIntegrationBase erweitert.

Die in diesem Skript enthaltene Funktionalität wird vom VulnerabilityIntegrationController aufgerufen, um zu verwalten, wie Daten aus einer externen Datenquelle abgerufen werden. Jede Unterklasse von VulnerabilityIntegrationBase hat Zugriff auf kontextbezogene Informationen zum Aufrufprozess. Diese Informationen sind über die folgenden Mitgliedsvariablen verfügbar:

- IntegrationGr: Ein GlideRecord des Schwachstellenintegrationsdatensatzes, der die Ausführung der Integration angefordert hat.
- IntegrationProcessGr: Ein GlideRecord, der kontextbezogene Informationen für den aktuellen Prozess einer Integration bereitstellt.

Der Schwachstellenprozess enthält spezielle Parameter, die in einer Integration verwendet werden sollen, im Allgemeinen zu Paginierungszwecken. Jeder Ausführung einer Schwachstellenintegration (als Schwachstellenintegrationsausführung bezeichnet) ist mindestens ein Schwachstellenintegrationsprozess zugeordnet. Für

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen mit mehreren Aufrufen gibt es mindestens einen Datensatz für den Schwachstellenintegrationsprozess für jede Ausführung der Schwachstellenintegration.

Die Skripteinbindung muss eine Implementierung für bereitstellen `Abrufen von Daten ()` Methode und gibt ein Objekt zurück, das vom Berichtsprozessorskript verarbeitet wird. Das von „retrieData“ zurückgegebene Objekt ist ein einfaches Objekt mit Eigenschaften für Content, contentType und Erweiterung.

Hier ist ein Screenshot von VulnerabilityIntegrationBase.retrieData():

SchwachstellenIntegrationBase.RetriegeDaten()

```
/**
 * Retrieves data (generally from an external system) to be passed to a report processor.
 * Subclasses (i.e. concrete implementations of a Vulnerability Integration) should implement/override this
 * function.
 * The class should return an object structured as follows:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 * For multipage integrations (where multiple calls/integration processes must run), this function should check
 * the integrationProcessGr's parameters.
 */
retrieveData: function() {
    return {contents: "", contentType: "", extension: ""};
},
```

Die Logik in `Abrufen von Daten ()` Hängt von der Schnittstelle ab, die zum Abrufen der Daten erforderlich ist. Wenn die Quelle der abgerufenen Daten beispielsweise über eine REST-API verfügt, könnte der Text dieser Methode den REST-Endpunkt aufrufen, wahrscheinlich über RESTMessageV2. Die Antwort des Aufrufs kann dann analysiert oder in einen Anhang eingefügt werden, und die Details können zum Erstellen des Rückgabeobjekts verwendet werden.

Einzelruf-Integrationen

Integrationsskripts für Einzelruf (einzelne Seite) sind die einfachsten Integrationstypen. Zum Abrufen von Daten ist ein Anruf erforderlich, häufig mit einer externen Datenquelle. Für Integrationen mit einer Seite/einem Anruf muss nur „Retrieve Data()“ implementiert werden.

Es folgt ein Beispiel, das ein einfaches Integrationsskript für einen einzelnen Anruf demonstriert. Erstellt ein RESTMessageV2 und führt es aus. Anschließend wird ein Objekt zurückgegeben, das den Antworttext als Inhalt verwendet, zusammen mit einem angenommenen contentType und einer Erweiterung.

Einzelruf-Integrationsskript

```
var SingleRunVulnerabilityIntegration = Class.create();
SingleRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.
     */
    retrieveData: function() {
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'SingleRunVulnerabilityIntegration'
});
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen für mehrere Anrufe

Integrationsskripts für mehrere Aufrufe (oder mehrere Seiten) sind etwas komplizierter. Sie erfordern mehrere Aufrufe einer Datenquelle, um Daten abzurufen.

Wie bei einer Einzelanruf-Integration muss für eine Integration mit mehreren Anrufen auch „retrieData()“ implementiert sein. Im Textkörper von „retrieData()“ verwendet die Integration die von VulnerabilityIntegrationBase bereitgestellten Methoden hasMoreData() und setNextRunParameters().

Die Methode hasMoreData() akzeptiert einen einzelnen booleschen Wert, der den VulnerabilityIntegrationController anweist, weitere Prozesse einzufügen, um mehr Daten abzurufen. Bei der Übergabe von „wahr“ an hasMoreData() wird ein Aufruf von „setNextRunParameters()“ ausgeführt, um dem nächsten Prozess Kontext bereitzustellen.

Die Methode „setNextRunParameters()“ akzeptiert ein einzelnes Objekt, das Kontextinformationen bereitstellt, die vom nächsten Aufruf zum Abrufen von Data() verwendet werden sollen. Dieses Objekt wird verwendet, um den Status an nachfolgende Aufrufe zum Abrufen von Daten () zu übergeben. Ein Beispiel für einen Anwendungsfall besteht darin, ein Objekt, das die aktuelle Seitenzahl und Seitengröße angibt, an einen Webservice zu übergeben.

Bei Integrationen mit mehreren Aufrufen überprüft jeder aufrufbezogene Aufruf zuerst die aktuellen Prozessparameter. Die Methode _getProcessParameters() wird allen VulnerabilityIntegrationBase zur Verfügung gestellt, um die vom vorherigen Prozess festgelegten Parameter abzurufen. Wenn keine Parameter vorhanden sind, bedeutet dies, dass es sich um den ersten Prozess handelt.

Es folgt ein Screenshot eines Beispielskripts für die Integration mehrerer Anrufe. Dieses Skript erweitert das Beispiel für die Einzelruf-Integration und demonstriert, dass Aufrufe an einen REST-Endpunkt getätigt werden, der über grundlegende Paginierungsunterstützung verfügt. Es zeigt, wie Sie eine einzelne Seite mit Daten abrufen können, erkennen, dass mehr Daten abgerufen werden müssen, und dann dem nächsten Prozess mitteilen, welche Seite abgerufen werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationsskript für mehrere Anrufe

```
var MultiRunVulnerabilityIntegration = Class.create();
MultiRunVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);
        var response = message.execute();
        var responseBody = response.haveError() ? response.getErrorMessage() : response.getBody();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responseBody, contentType: "application/xml", extension: "xml"};
    },

    type: 'MultiRunVulnerabilityIntegration'
});
```

Anhänge als Abrufen von Daten () Rückgabewerte

Manchmal ist es vorzuziehen, einen Anhang aus „retrieData()“ zurückzugeben. Die Logik zum Erstellen und/oder Abrufen eines Anhangs ist implementierungsspezifisch, aber nachdem der Anhang bekannt ist, können seine Informationen zurückgegeben werden.

Um einen Anhang bereitzustellen, gibt „retrieData()“ ein Objekt wie folgt zurück:

```
{
    contents: "attachment-sys-id",
    contentType: "sys_attachment"
}
```

Ein Beispiel, das sich auf erstreckt Vorheriges Beispiel , Speichert aber den Antworttext der REST-Nachricht im folgenden Integrationsprozess-Datensatz. Dann wird dieser Anhangsbezeichner als Inhalt des Rückgabeobjekts zurückgegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anhang aus „Retrieve Data“ zurückgeben

```
var MultiRunAttachVulnerabilityIntegration = Class.create();
MultiRunAttachVulnerabilityIntegration.prototype = Object.extendsObject(sn_vul.VulnerabilityIntegrationBase, {
    initialize: function() { },

    /**
     * Sample retrieveData() where fictional RESTMessage is executed and XML response body is
     * returned.  This call is paginated, so we need to figure out the range to pull
     * for each call.
     *
     * For simplicity, we'll say that a status code != 200 means we've reached the end of data
     * from the server, or if we cap out past our maxPages member variable.
     *
     */
    maxPages: 5,
    retrieveData: function() {
        var currentParams = this._getProcessParameters();
        var pageSize = 100;
        var page = 1;
        if (currentParams) {
            page = currentParams.page;
        }
        var message = new sn_ws.RESTMessageV2("My Vuln REST", "get");
        message.setQueryParameter("pageSize", pageSize);
        message.setQueryParameter("page", page);

        var table = this.integrationProcessGr.getTableName();
        var sysId = this.integrationProcessGr.getUniqueValue();
        var fileName = this.integrationProcessGr.getValue("number") + ".xml";
        message.saveResponseBodyAsAttachment(table, sysId, fileName);
        var response = message.execute();
        var responsSysId = response.getResponseAttachmentSysid();
        if (response.getStatusCode() != 200 || page >= this.maxPages) {
            this.hasMoreData(false);
            this.setNextRunParameters(null);
        } else {
            this.hasMoreData(true);
            this.setNextRunParameters({
                page: page + 1
            });
        }
        return {contents: responsSysId, contentType: "sys_attachment", extension: "xml"};
    },

    type: 'MultiRunAttachVulnerabilityIntegration'
});
```

Berichtsprozessorstrategien

Die **Berichtsprozessorstrategie** Das Feld im Formular „Schwachstellenintegration“ wird verwendet, um die Methode zur Verarbeitung der Daten auszuwählen, die vom Schwachstellenintegrationsskript zurückgegeben werden, wenn der Schwachstellenintegrationsprozess ausgeführt wird.

Der Standardwert ist **Datenquellenanhang** . Diese Methode ist die Baseline-Implementierung, bei der die abgerufenen Daten an eine Datenquelle übergeben werden, die in das System importiert werden soll. Auswählen **Anwenderdefinierter Berichtsprozessor** Ermöglicht Ihnen die Auswahl eines anwenderdefinierten Prozessorskripts für die Verarbeitung der Daten.

Verwenden Sie die Berichtsprozessorstrategie für Datenquellenanhänge

Die Berichtsprozessorstrategie „Datenquellenanhang“ wird verwendet, um vom Integrationsskript abgerufene Daten an konfigurierte Datenquellen zu übergeben.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_write

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Integrationen** Und Erstellen Sie eine neue Integration .
2. In **Berichtsprozessorstrategie** Feld auswählen **Datenquellenanhang** .
3. Klicken Sie mit der rechten Maustaste in den Formularheader, und klicken Sie auf **Speichern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. In **Datenquellen Der Schwachstellenintegration** Zugehörige Liste, klicken Sie auf **Neu** .
5. Definieren Sie die zu verwendende Datenquelle.
6. Klicken Sie auf **Absenden**.
7. Wiederholen Sie die Schritte 4 bis 6, wenn Sie zusätzliche Datenquellen benötigen.
   Geben Sie die Reihenfolge an, in der die mehreren Datenquellen Informationen im senden **Reihenfolge** Feld.
8. Klicken Sie auf **Aktualisieren**.

Über anwenderdefinierte Berichtsprozessorskripts

Im Formular „Schwachstellenintegration“ ist der Berichtsprozessor ein Verweis auf eine Skripteinbindung, die die Skripteinbindung VulnerabilityReportProcessorBase erweitert. Die in diesem Skript enthaltene Funktionalität wird vom VulnerabilityIntegrationController aufgerufen und definiert die Methode, mit der die vom Integrationsskript zurückgegebenen Daten verarbeitet werden.

Jede Unterklasse von VulnerabilityReportProcessorBase hat Zugriff auf kontextbezogene Informationen zum Aufrufprozess. Diese Informationen sind über die folgenden Mitgliedsvariablen verfügbar:

- IntegrationGr: Ein GlideRecord des Schwachstellenintegrationsdatensatzes, der die Ausführung der Integration angefordert hat.
- IntegrationProcessGr – GlideRecord des Schwachstellenprozesses, der kontextbezogene Informationen für den aktuellen Prozess einer Integration bereitstellt.

Die Skripteinbindung muss eine Implementierung für bereitstellen `ProcessReport()` Methode. Das an „processReport()“ übergebene Objekt ist das von „retrieData“ zurückgegebene Objekt und somit ein einfaches Objekt mit Eigenschaften für „content“, „contentType“ und „Extension“. Die tatsächliche Logik in processReport() ist implementierungsspezifisch und abhängig von den bereitgestellten Berichtsdaten.

Hier ist ein Screenshot von VulnerabilityReportProcessorBase.processReport():

Anwenderdefiniertes Berichtsprozessorskript

```
/*
 * Processes the reportData that was pulled by a Vulnerability Integration's retrieveData().
 * The expectation is that retrieveData() will return an object that matches this function's input parameter.
 *
 * @param reportData = object with the following format:
 *
 * {
 *    contents: raw contents of data to process, usually a string.  If the integration creates an attachment
 *              this value should be the attachment sys_id.
 *    contentType: the mimeType of the content.  If the content is an attachment sys_id,
 *                 this should be sys_attachment.  The sys_attachment record itself should have the
 *                 content type specified.
 *    extension: the file extension that should be used for this content in the event the processor
 *               needs to write the contents to a file (such as a new attachment).
 * }
 *
 */
processReport: function(reportData) {
    return;
},
```

Integrationswerksskriptfelder

Das Formular „Schwachstellenintegration“ enthält das Integrationswerksskript und, wenn **Anwenderdefinierter Berichtsprozessor** Die Berichtsprozessorstrategie ist ausgewählt, das Prozessor-Werksskript. Diese Felder werden verwendet, um die Logik zur tatsächlichen Instanziierung des Objekts bereitzustellen, das durch die Skripteinbindungsreferenzfelder, das Integrationsskript und den Berichtsprozessor definiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Skripteinbindung ausgewählt ist, werden beide Felder mit einem Konstruktoraufruf ohne Argument vorab ausgefüllt. Oft ist dies ausreichend, aber es kann Anlässe geben, bei denen mehr Logik erforderlich ist, um das Skriptobjekt zu instanziieren.

Der integrationProcessGr-Datensatz wird den Werksskriptfeldern zugänglich gemacht, sodass prozessspezifische Informationen nach Bedarf verwendet werden können.

Führen Sie eine Schwachstellenintegration manuell aus

Schwachstellenintegrationen für Vulnerability Response Und Application Vulnerability Response Sind für die geplante Ausführung konfiguriert. Sie können sie jedoch bei Bedarf manuell ausführen.

Vorbereitungen
Erforderliche Rollen:

- sn_vul.read_Integrations (Vulnerability Response)
- sn_vul.App_read_Integrations (Application Vulnerability Response)

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird
Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen**an.
2. Öffnen Sie den Datensatz für die Integration, die Sie ausführen möchten.
3. Klicken Sie auf **Jetzt ausführen**.

Manuelle Erfassung von Schwachstellen

Erfassen Sie Schwachstellen manuell in Vulnerability Response Anwendung, damit Sie sie schnell beheben können, ohne auf Scannerergebnisse warten zu müssen.

Scanner von Drittparteien wie Rapid7 Helfen Sie beim Importieren von Schwachstellendaten in Vulnerability Response Und verarbeiten Sie die Daten, um die Ergebnisse zu melden. Mit der Integration der manuellen Erfassung können Sie die Schwachstellen proaktiv erfassen und beheben, anstatt darauf zu warten, dass Scanner die gefährdeten Assets melden. Die manuelle Erfassung von Schwachstellen schützt die Assets effektiv vor unbekannten Bedrohungen wie Zero-Day-Exploits.

Manuelle Erfassung von Schwachstellen

Sie können die Schwachstellendaten importieren, indem Sie eine Vorlage in den folgenden Dateiformaten hochladen:

- Excel
- Kommagetrennter Wert (CSV)

Um auf die Vorlage zuzugreifen und sie herunterzuladen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung Des Schwachstellenelements** > **Datei hochladen – UI**an.

Stellen Sie sicher, dass Sie beim Ausfüllen der Datensätze in der Vorlage die folgenden wichtigen Punkte beachten:

- Machen Sie keine Eingabefehler in den Datensätzen der Spalte „Schweregrad/Status“. Bei einem Tippfehler wird der Datensatz übersprungen.
- Ändern Sie die Spaltennamen nicht.
- Geben Sie keine Spaltennamen in eine Zeile außer in die erste Zeile ein.
- Ändern Sie die Reihenfolge der Blätter in nicht Microsoft ExcelVorlage. Die Schwachstellendaten müssen immer im zweiten Blatt vorhanden sein.
- Fügen Sie keine Details zu Schwachstellen in ein Blatt mit Ausnahme des Blatts „manuelle Erkennungen eingeben“ ein.
- Verwenden Sie keine Zeichen außer alphanumerischen Zeichen und Sonderzeichen wie Bindestrich (-), Punkt (.), Plus (+), Unterstrich (_), Leerzeichen, Klammern „(„)“ und at-Symbol (@) für den Dateinamen.

Anweisungen zum Ausfüllen der Daten in der Vorlage finden Sie unter Vorlage für die manuelle Erfassung von Schwachstellen.

Ab v24.0.6 von Vulnerability Response, Sie können auch zusätzliche Spalten in erstellen Microsoft Excel Vorlage. Weitere Informationen finden Sie unter KB1646630 .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen der manuellen Erfassung

Die Integration wird ausgelöst, wenn eine Datei hochgeladen wird. Basierend auf dem Typ der hochgeladenen Datei wird die zugehörige Integration ausgelöst.

Um die Integrationen anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung Des Schwachstellenelements** > **Integrationen**an.

Die folgenden Integrationen der manuellen Erfassung des Basissystems sind standardmäßig verfügbar.

Integrationen

Integrationstyp	Beschreibung
Manuelle Erfassung – Excel-Integration	Ruft Daten ab, indem die neuesten abgerufen werden Microsoft ExcelDatei aus der Tabelle „Push-Warteschlange für Schwachstellenerfassung“ hochgeladen und den Anhang in die entsprechende Integrationsausführung kopiert.
CSV-Integration der manuellen Erfassung	Ruft Daten ab, indem die neueste CSV-Datei abgerufen wird, die aus der Tabelle „Push-Warteschlange für Schwachstellenerfassung“ hochgeladen wurde, und kopiert den Anhang in die entsprechende Integrationsausführung.

Die Integration von Drittparteien mit manueller Erfassung erstellt standardmäßig eine Integrationsinstanz mit den folgenden beiden Integrationsinstanzparametern:

- max_input_Records: Definiert die Anzahl der Datensätze, die in der Vorlage erstellt werden können. Wenn Sie mehr Datensätze hinzufügen, als in diesem Parameter angegeben ist, werden die zusätzlichen Datensätze übersprungen. Die Anzahl der Datensätze kann in der Wertspalte aktualisiert werden. Die empfohlene Anzahl von Datensatzerstellungen in der Vorlage beträgt 1000. Alles über diesem Wert kann zu Leistungsproblemen führen.
- INSERT_fixed: Importiert Erkennungen von behobenen Schwachstellen.

Um die Parameter der Integrationsinstanz anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung Des Schwachstellenelements** > **Integrationen** Und klicken Sie auf die Quellinstanz einer beliebigen Integration. Alternativ können Sie zu navigieren **Alle** > **Vulnerability Response** > **Integrationsinstanzen** Und klicken Sie auf **Manuelle Erfassung** .

Erfassen Sie Schwachstellen manuell

Erfassen Sie Schwachstellen manuell, indem Sie eine Vorlage mit Schwachstellendaten hochladen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Datei hochladen – UI**an.
2. Klicken Sie auf die Excel- oder CSV-Links, und laden Sie die Vorlage im entsprechenden Format herunter.
3. Geben Sie in der Vorlage die Schwachstellendaten in die Datensätze ein.
   Anweisungen zum Ausfüllen der Daten in der Vorlage finden Sie unter Vorlage für die manuelle Erfassung von Schwachstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie Auf **Datei Importieren** Und laden Sie die aktualisierte Vorlage hoch.
5. Klicken Sie auf **Absenden**.
   Die Seite Schwachstellenintegration Push-Warteschlangen wird angezeigt. Sie können die Liste der Integrationsinstanzen, den Status der Integrationsausführungen und Protokollnotizen anzeigen, nachdem die Integrationsausführung abgeschlossen ist.

Nächste Maßnahme

Nachdem Sie die Datei hochgeladen haben, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Integrationen**an. Stellen Sie sicher, dass die Integrationsausführung erfolgreich ist.

Überprüfen Sie die Ausführung der manuellen Integration

Stellen Sie sicher, dass die Integrationsausführung erfolgreich ist. Zeigen Sie die Anzahl der einzelnen Erkennungen und der angreifbaren Elemente (VIS) an, die aufgrund der Integrationsausführung erstellt oder aktualisiert wurden.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Integrationen**an.
2. Klicken Sie auf den Namen der Integration basierend auf dem hochgeladenen Dateityp.
3. Klicken Sie auf **Schwachstellenintegration Wird Ausgeführt** Registerkarte.
4. Klicken Sie auf die Nummer der Integrationsausführung.
5. Klicken Sie auf **Elemente** Registerkarte.
6. Überprüfen Sie die Informationen in **Elemente** Registerkarte.

Registerkarte „Elemente“

Registerkarte/Feld	Beschreibung
Registerkarte „Elemente“	Zeigt die Gesamtzahl der importierten VIS an. Sie können die Gesamtzahl der importierten Erkennungen anzeigen, indem Sie die auf der Registerkarte Erkennungen aufgeführten Nummern hinzufügen.
Neue Elemente	Zeigt die Anzahl der angreifbaren Elemente an, die aus dieser Integrationsausführung erstellt werden.
Importierte Elemente	Zeigt die Summe aller Felder in diesem Abschnitt an.
Doppelte Elemente	Zeigt doppelte Elemente an. Dieses Feld ist nicht mehr ausgefüllt.
Aktualisierte Elemente	Zeigt an, wie oft angreifbare Elemente während dieser Integrationsausführung aktualisiert werden. Dieser Wert ist nicht die Anzahl der eindeutigen angreifbaren Elemente, die aktualisiert werden. Wenn beispielsweise ein angreifbares Element während der Integrationsausführung zweimal

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte/Feld	Beschreibung
	aktualisiert wird, wird es zweimal gezählt und als angezeigt 2 Aktualisierte Elemente.
Unveränderte Elemente	Zeigt während der Integrationsausführung gefundene angreifbare Elemente an, die in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da keiner der relevanten Feldwerte geändert wurde.

Nächste Maßnahme

Nachdem Sie überprüft haben, ob die Integrationsausführung erfolgreich ist, navigieren Sie zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Verlauf hochgeladener Dateien**an. Überprüfen Sie, ob fehlerhafte Datensätze aus den Notizen vorhanden sind.

Konfigurieren Sie das automatische Schließen manueller Erkennungen

Aktivieren Sie das automatische Schließen manueller Erkennungen, um veraltete manuelle Erkennungen automatisch zu schließen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Datei hochladen – UI**an.
2. Klicken Sie Auf **Ändern Sie Die Konfiguration Für Das Automatische Schließen** .
3. Klicken Sie auf **Manuelle Erkennungen** Registerkarte.
4. Stellen Sie sicher, dass **Manuelle Erkennungen automatisch schließen** Das Kontrollkästchen ist aktiviert.
5. In **Zuletzt gefundene manuelle Erkennungen (vor Tagen)** Geben Sie die Anzahl der Tage ein, nach denen die manuellen Erkennungen geschlossen werden sollen.
   Der Standardwert ist 90 Tage. Sie können einen beliebigen positiven Wert für die Anzahl der Tage eingeben.

Upload-Status überprüfen

Überprüfen Sie, ob die Ausführung der Schwachstellenintegration erfolgreich, teilweise erfolgreich oder ein Fehler war.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Manuelle Erfassung von angreifbaren Elementen** > **Verlauf hochgeladener Dateien**an.
2. Überprüfen Sie in der Tabelle „Push-Warteschlangen für Schwachstellenintegration“ die Zeit des Uploads und den Status des Uploads in den Spalten erstellt und Status.
3. **Wahlweise:** In **Notizen** Feld, zeigen Sie den Grund für den Fehler an.

Vorlage für die manuelle Erfassung von Schwachstellen

Die Vorlage enthält Spalten, die mit Daten zu Schwachstellen und Konfigurationselementen (Configuration Item, CI) gefüllt werden müssen. Nachdem die Vorlage ausgefüllt und hochgeladen wurde, werden die Daten verarbeitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anweisungen zum Ausfüllen der Vorlage

Um die Details in die Vorlage einzugeben, befolgen Sie die Anweisungen in der folgenden Tabelle.

Vorlagenanweisungen

Spalte	Erforderlich/ Optional?	Zeichenfolgenlänge (max.)/ gültige Werte	Beschreibung
Asset-ID	Optional	255	Universal Unique Bezeichner (UUID) oder Asset-ID. Dies kann der von einem Scanner generierte Wert sein.
Geben Sie Informationen in mindestens eine der folgenden fünf Spalten ein:			
MAC-Adresse	Erforderlich	24	Host- oder Asset-Informationen. Die Kombination aller angegebenen Werte muss für ein Asset eindeutig sein.
FQDN	Erforderlich	255	
NETBIOS	Erforderlich	255	
IP-Adresse	Erforderlich	255	
Hostname	Erforderlich	255	
Die verbleibenden Spalten hängen nicht voneinander ab.			
Schwachstellen-ID	Erforderlich	255	Stellt eine Schwachstelle in der National Vulnerability Database (NVD) oder eine ID dar, die von einem Scanner einer Drittpartei zurückgegeben wird.
Schwachstellenzusammenfassung	Optional	512	Kurze Beschreibung der Schwachstelle. Sie wird der Datenbank nur hinzugefügt, wenn die Schwachstellen-ID nicht verfügbar ist.
Schweregrad	Optional	Kritisch, hoch, Mittel, niedrig, keine	Schweregrad der Schwachstelle. Sie wird der Datenbank nur hinzugefügt, wenn die Schwachstellen-ID nicht verfügbar ist. Wenn der Datensatz leer ist, wird er standardmäßig als kritisch betrachtet.
Port	Optional	Nicht zutreffend	Port, über den die Schwachstelle erkannt wird. Der Wert muss eine gültige Ganzzahl sein. Wenn eine ungültige Eingabe vorhanden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorlagenanweisungen (Fortsetzung)

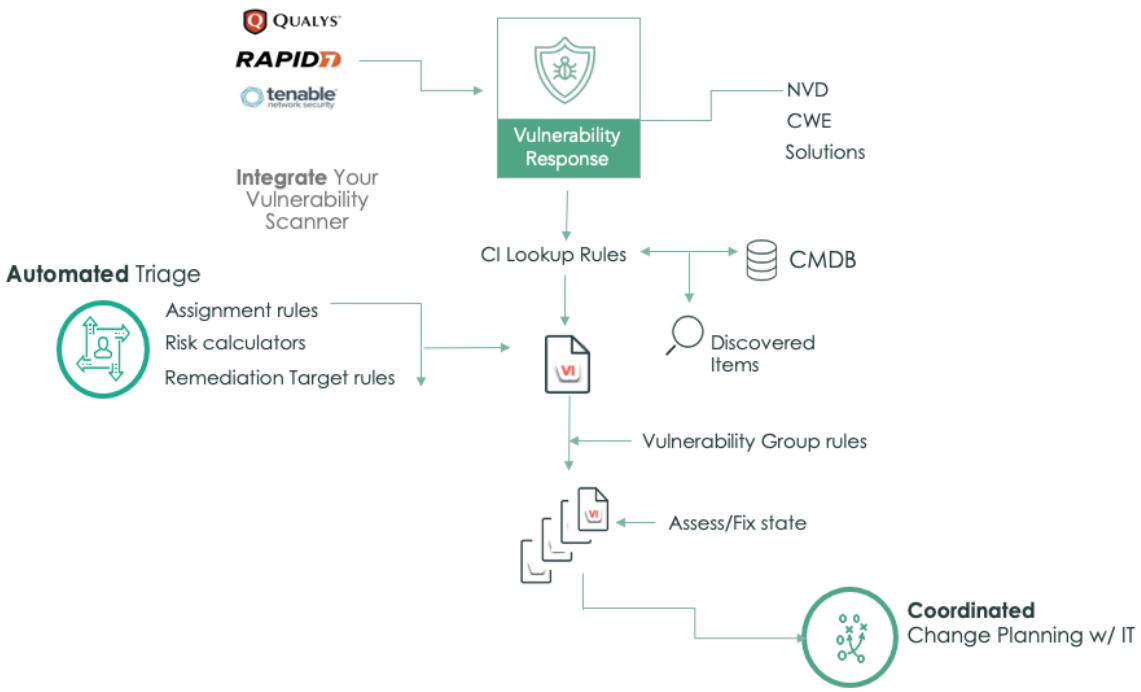
Spalte	Erforderlich/ Optional?	Zeichenfolgenlänge (max.)/ gültige Werte	Beschreibung
			ist, wird der Datensatz übersprungen.
Protokoll	Optional	40	Typ des verwendeten Netzwerkprotokolls.
Nachweis	Optional	4000	Stellt den Standort oder den Systempfad der Schwachstelle dar.
Status	Optional	Offen, behoben	Status der Erkennung. Wenn der Datensatz leer ist, gilt er standardmäßig als offen.

Vulnerability Response Korrekturübersicht

Vulnerability Response Die Fehlerkorrektur ist ein abgestufter Prozess, der aus der Überprüfung des Importabschlusses, der Selektierung neuer Schwachstellen und der Überwachung des Fortschritts bis zum Abschluss besteht. Auf diese Weise wird die Korrektur verwaltbar, zeitnah und in vielerlei Hinsicht automatisiert.

Das Verständnis Ihrer Sicherheitslage in den gesamten Unternehmens-Assets hilft Ihnen, die kritischsten Schwachstellen für die Behebung zu identifizieren. Dieser Korrekturprozess erfordert das Vulnerability Response Und eine Drittpartei-Integration wie Qualys Vulnerability Integration Sind installiert und konfiguriert.

Flow des Integrationsprozesses für Vulnerability Response



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verifiziert den erfolgreichen Abschluss von Integrationsimporten von Drittparteien

Die erste Phase dieses Prozesses besteht darin, sicherzustellen, dass alles ordnungsgemäß funktioniert. Vulnerability Response Ist voreingestellt, um Schwachstellen in der National Vulnerability Database (NVD) und CWE-Schwachstellen (Common Enumeration Sschwäche) herunterzuladen. Importe von Drittparteien liefern Ihnen die Daten, die Sie zum Erstellen angreifbarer Elemente und Korrekturaufgaben benötigen. Eine erfolgreiche Fehlerkorrektur hängt vom konsistenten und erfolgreichen Import von Schwachstellen und angreifbaren Elementen ab.

Während des Imports von CI-Suchregeln stimmen Assets von Drittparteien mit Assets in ab Configuration Management Database (CMDB). Alle Assets werden im Modul „erkannte Elemente“ gespeichert. CI-Informationen sind für die Lösungsimplementierung entscheidend.

Hinweis:
Sobald eine Drittanbieterintegration installiert und konfiguriert wurde, gibt es einige Instanzen, in denen ein Import fehlschlagen kann, z. B. wenn der Drittanbieter seine API-Aufrufe drosselt. Wenn Importe fehlschlagen, erfordern sie ein Eingreifen.

Integrationsstatusausführungsberichte für die unterstützten Drittanbieterintegrationen werden mit den Anwendungen geliefert, um Ihnen einen grafischen Überblick über Ihre Importe zu geben. Verwenden Sie diesen Bericht, oder erstellen Sie einen eigenen, um einfach festzustellen, ob Ihr letzter Import erfolgreich war. Weitere Informationen zu unterstützten Integrationen finden Sie unter Vulnerability Response-Integrationen.

Überprüfen und selektieren Sie Schwachstellen und angreifbare Elemente

In der nächsten Korrekturphase müssen neue Schwachstellen und angreifbare Elemente überprüft werden. Ein angreifbares Element (VI) ist eine erkannte Kombination aus Schwachstelle und Konfigurationselement (CI). Während angreifbare Elemente gebildet werden, werden verschiedene Regeln ausgeführt, die VIS zuweisen, das Risiko bestimmen und Korrekturziele festlegen. Passen Sie alle Regeln nach Bedarf an, um sicherzustellen, dass die angreifbaren Elemente erfolgreich selektiert wurden.

Überwachen Sie den Fortschritt der vorhandenen Schwachstellenbeseitigung

Die letzte Phase der Korrektur besteht in der Überwachung Ihres Fortschritts.

- Überprüfen Sie den Status von Importen für Patch-Implementierungen, die nicht angezeigt wurden, und verfolgen Sie IT Operations.
- Verfolgen Sie den Fortschritt der regulatorischen Compliance-Verpflichtungen, und stellen Sie sicher, dass sie abgeschlossen werden.
- Überprüfen Sie den Status des zurückgestellten Elements, und überarbeiten oder implementieren Sie Korrekturen.
- Überwachen Sie Schwachstellenmanagement-Dashboards. Um Trends zu überprüfen, Berichte in Echtzeit anzuzeigen und Metriken zu verwenden, die Ihre Korrekturzielerreichungsraten nachverfolgen, sollten Sie Ihre Prozesse mit überwachen Performance Analytics Für Vulnerability Response Anwendung.
- Veraltete Erkennungen in werden geschlossen Vulnerability Response.

Überprüfen Sie den erfolgreichen Abschluss von Vulnerability Response Integrationsimporte

Die einfachste Möglichkeit, zu bestimmen, ob Ihre Importe erfolgreich waren, besteht in der Verwendung eines Dashboard „Integrationsausführungsstatus“. Das Dashboard

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Integrationsausführungsstatus“ bietet ein Beispiel für eine grafische Ansicht des Status von Integrationsausführungen von Drittparteien.

Die Qualys Und Rapid7 Schwachstellenintegrationen haben ein Dashboard für den Status der Integrationsausführung. Siehe Qualys Statusdiagramm der Integrationsausführung Oder Rapid7 Vulnerability-Integration Führen Sie das Statusdiagramm aus Für detaillierte Informationen zum Diagramminhalt.

Hinweis:
Diagramme für Integrationen, die nicht von bereitgestellt wurden ServiceNow®, Kann aus Berichten in einem Dashboard erstellt werden, erfordert jedoch möglicherweise ServiceNow Fachwissen. Weitere Informationen zum Erstellen von Berichten und Dashboards finden Sie unter Erste Schritte mit Berichten Und Dashboards .

Anzeigen Vulnerability Response Erkennungsdaten für angreifbare Elemente

Die vollständigen Daten, die von Ihren Scannerintegrationen von Drittanbietern mit erfasst wurden Vulnerability Response Werden auf den Registerkarten Erkennungen und erste Erkennungen in den Datensätzen angreifbarer Elemente (VIT) angezeigt. Sie wird auch in Erkennungsdatensätzen in der Liste Erkennung angreifbarer Elemente in angezeigt ServiceNow AI Platform® Instanz.

Vorbereitungen

Drittpartei-Integrationen rufen Erkennungsdaten für angreifbare Elemente ab. Erkennungen sind eindeutige Vorkommen von Schwachstellen, wie von den Scannern gemeldet. Erkennungsdaten werden mit angreifbaren Elementen gekoppelt, und der VI-Status wird basierend auf dem Status der Erkennungen aktualisiert. Wenn kein VI gefunden wird, wird ein neues erstellt. Erkennungen werden nur durch Daten geöffnet oder geschlossen, die direkt von einem Scanner gefunden werden.

Erforderliche Rolle:

- sn_vuln.admin initiiert Integrationsausführungen und zeigt Erkennungsdaten für angreifbare Elemente an.
- sn_vul.Remediation_owner sind angreifbare Elemente zugewiesen, die aus Erkennungen angreifbarer Elemente erstellt wurden, und zeigen Daten in VI-Datensätzen an.

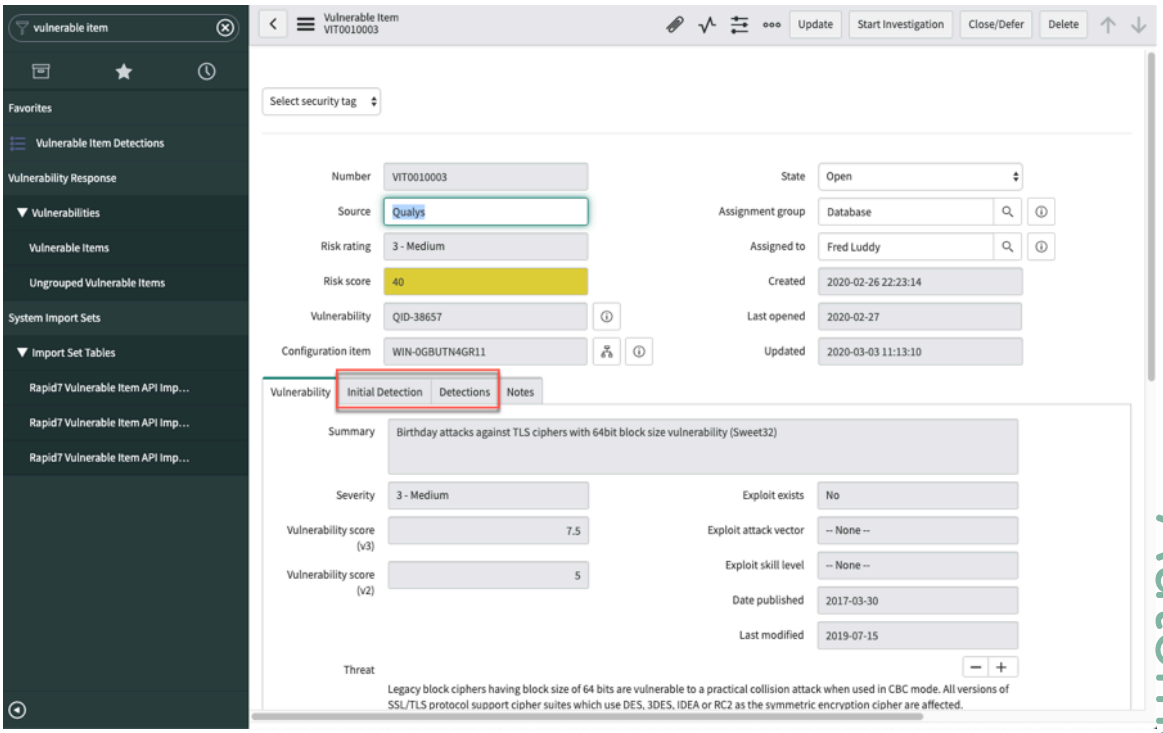
Prozedur

1. Um die Erkennungsdaten für angreifbare Elemente anzuzeigen, navigieren Sie zu einem Datensatz für angreifbare Elemente, und öffnen Sie ihn.

   Der Datensatz wird mit den Registerkarten „anfängliche Erkennungen“ und „Erkennungen“ angezeigt.

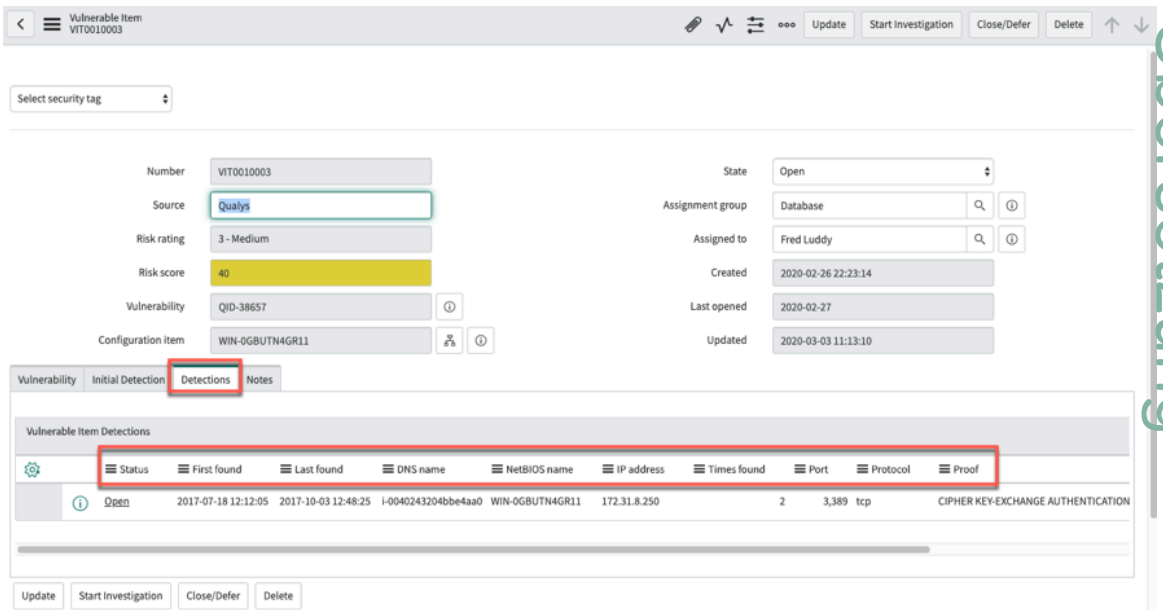
   Hinweis:
   Daten, die zuvor auf der Registerkarte Konfigurationsdetails angezeigt wurden, werden zusammen mit anderen Erkennungsdaten auf den Registerkarten „erste Erkennung“ und „Erkennungen“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Klicken Sie auf **Erkennungen** Registerkarte.

Wenn ein angreifbares Element aus den Ergebnissen eines Drittpartei-Scans erstellt wird, werden die Daten aus dem Scan im Erkennungsdatensatz angezeigt, wie in der folgenden Abbildung dargestellt.



Jede Zeile im Abschnitt „Erkennungen angreifbarer Elemente“ stellt Daten aus einer eindeutigen Erkennung dar. In der Spalte „erste gefundene Elemente“ wird das Datum angezeigt, an dem das angreifbare Element erstmals vom Scanner erkannt wurde. In der Spalte zuletzt gefunden wird das Datum der neuesten Erkennung angezeigt. Im Feld Quelle wird der Scanner angezeigt, der die Daten abgerufen hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Für Qualys, Bei Erkennungen angreifbarer Elemente sind die folgenden Felder im VI-Datensatz veraltet und werden nicht mehr ausgefüllt:

- Qualys Schweregrad
- Zuletzt aktualisiert von Quelle

Auch für Qualys, Wie in der vorangehenden Abbildung gezeigt, wird der Wert aus dem Scan nach Ergebnissen in der Nachweisspalte des Erkennungsdatensatzes angezeigt, wenn ein VI aus einem Scan erstellt wird. Dieser Wert wird jedoch nicht im oberen Teil des VI-Datensatzes angezeigt.

Wenn in Rapid7 ein VI aus einem Scan erstellt wird, kann der Wert für den Nachweis aus dem Scan sowohl in der Nachweisspalte im Erkennungsdatensatz als auch im oberen Teil des VI-Datensatzes angezeigt werden, aber nicht standardmäßig. Um diesen Wert im oberen Teil des VI-Datensatzes anzuzeigen, wählen Sie im Formularlayout das Feld Nachweis aus.

3. **Wahlweise:** Führen Sie die folgenden Schritte aus, um das Layout der Registerkarte Erkennungen im Datensatz zu konfigurieren.

   a. Die folgenden Spalten werden standardmäßig auf der Registerkarte Erkennungen angezeigt.

   - Status
   - Zuerst gefunden (Daten)
   - Zuletzt gefunden (Datum)
   - DNS-Name
   - Net BIOSName
   - IP-Adresse
   - Anzahl Ermittlungen
   - Port
   - Protokoll
   - Nachweis
   - SSL

   Hinweis:

   (Optional) Hinweis: Wenn in einer Spalte kein Wert vorhanden ist, wurden die Daten für dieses Feld vom Scanner nicht erkannt.

   b. Klicken Sie auf das Zahnradsymbol ( ), um Ihre Ansicht zu personalisieren.

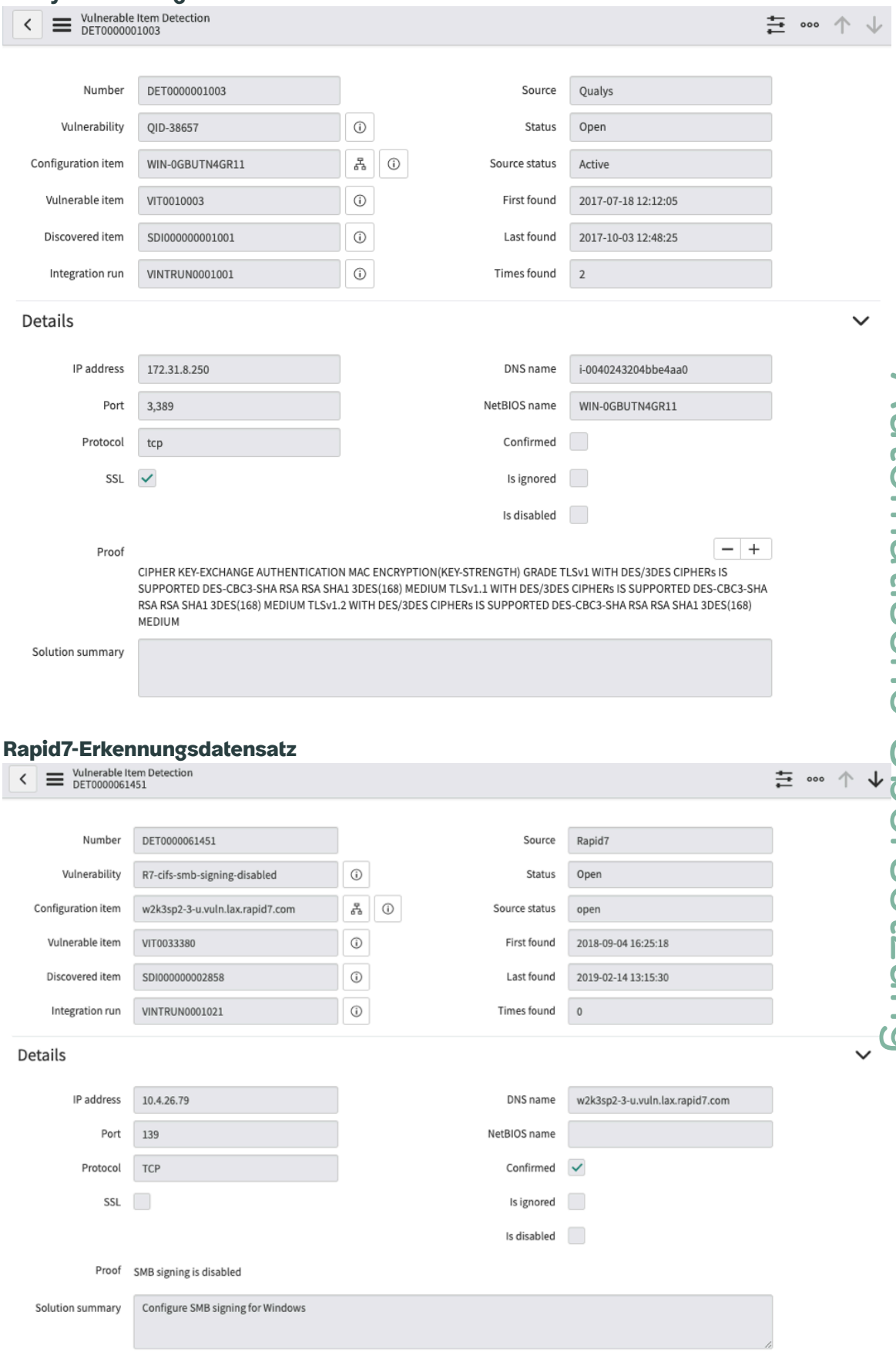
   c. Wählen Sie die Spalten aus dem Slushbucket aus, um bestimmte Daten anzuzeigen, und klicken Sie auf **OK**.

4. Wenn die Registerkarte Erkennungen ausgewählt ist, klicken Sie in der Spalte Status auf ein Element, um den Erkennungsdatensatz zu öffnen und die Details anzuzeigen, die diesem angreifbaren Element zugeordnet sind, einschließlich einer Lösungszusammenfassung (nur Rapid7 InsightVM-Integration).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Qualys Erkennungsdatensatz



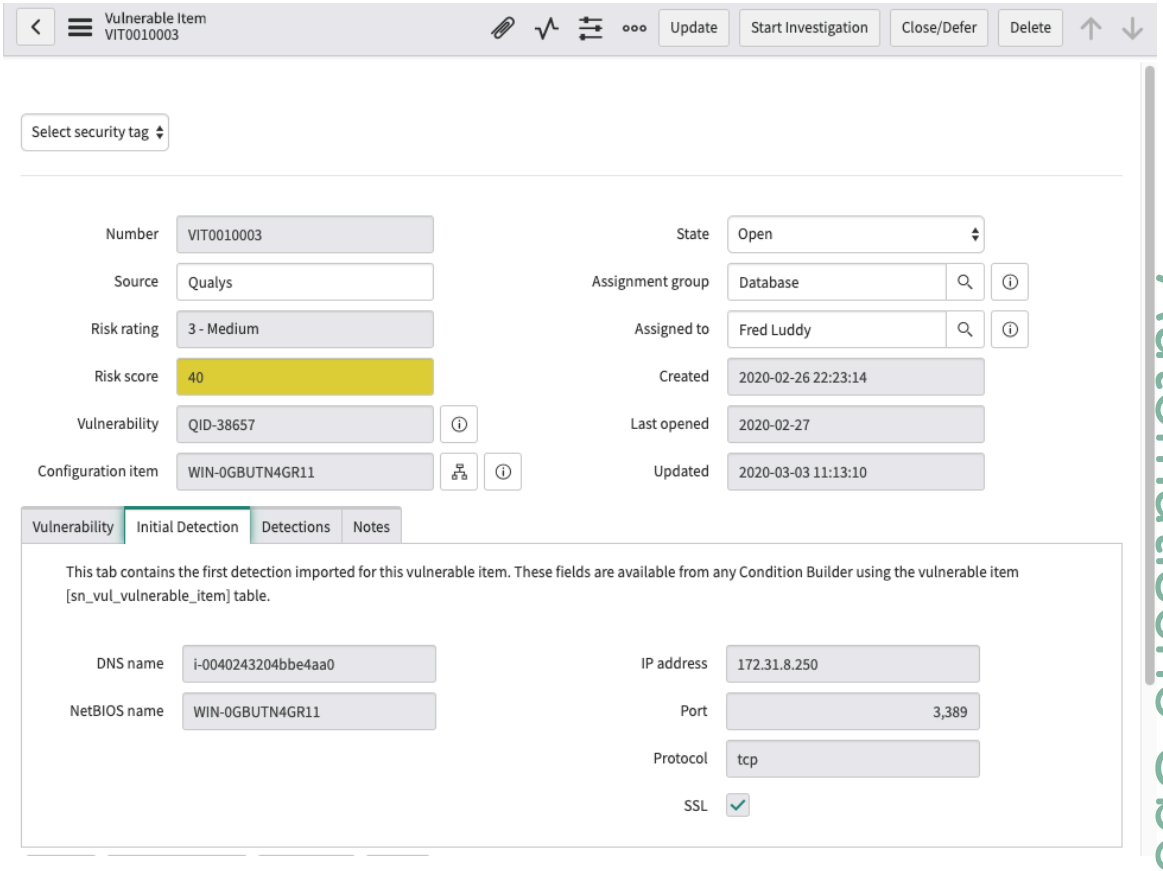
Rapid7-Erkennungsdatensatz

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Kehren Sie zum Datensatz zurück, und wählen Sie die Registerkarte erste Erkennung aus.

   Auf der Registerkarte anfängliche Erkennungen werden die Daten angezeigt, die beim ersten Auftreten der Erkennung vom Scanner des Drittanbieters importiert wurden. Diese Informationen auf der Registerkarte „erste Erkennung“ ändern sich nicht, wenn Erkennungsdaten aktualisiert werden.

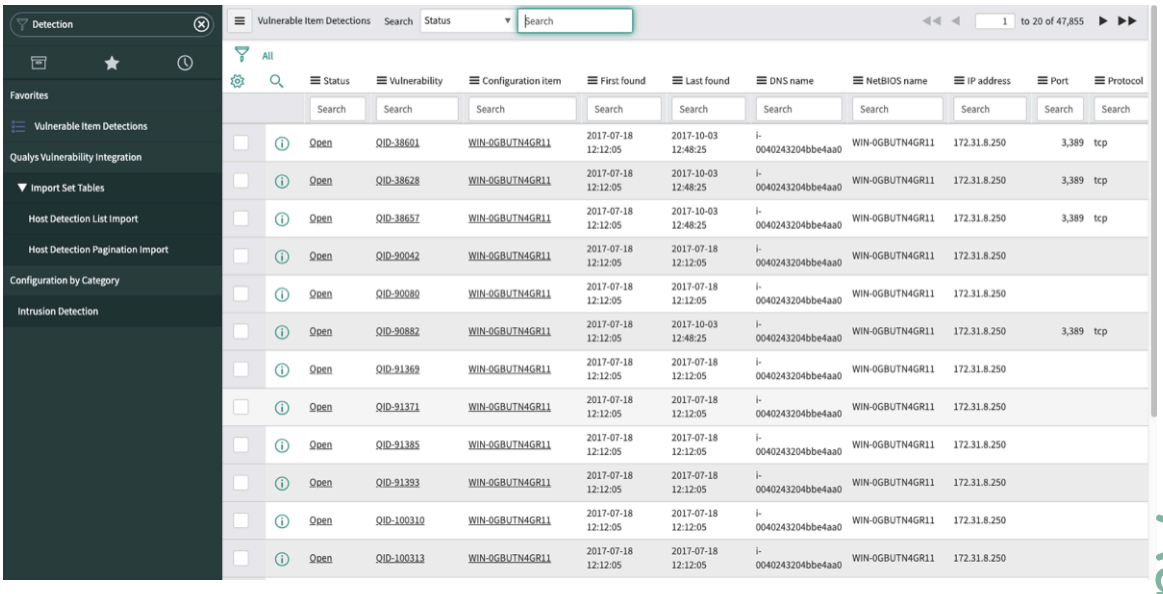


6. **Wahlweise:** Navigieren Sie zu Erkennungen angreifbarer Elemente, um die Erkennungsliste für angreifbare Elemente anzuzeigen.

   (Optional) Die Liste Erkennung angreifbarer Elemente wird angezeigt. Jede Zeile in der Liste der Erkennungen angreifbarer Elemente stellt eine eindeutige Erkennung dar. Die Spalten zeigen dieselben Daten wie der VI-Datensatz an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erkennungen werden nur von Daten geöffnet oder geschlossen, die von einem Scanner gefunden werden. Sie werden nicht von VIS aus einem Rollup ausgeführt. Wenn Erkennungen importiert werden, werden sie verwendet, um VIS zu erstellen und die status von VISzu aktualisieren Wenn alle Erkennungen für ein angreifbares Element geschlossen sind, wird dieses angreifbare Element geschlossen. Im VI-Datensatz lautet der Status Geschlossen , Und der Substatus ist Behoben .

Hinweis:

Fehler werden protokolliert, während:

- Vom Scanner abgerufene Anhänge werden verarbeitet.
- Erstellen oder Aktualisieren von Erkennungen oder angreifbaren Elementen.

Informationen zur Behandlung von Erkennungsfehlern finden Sie unter Fehlerbehandlung für Erkennungen.

Wenn alle VIS für eine Korrekturaufgabe geschlossen sind, wird die Korrekturaufgabe geschlossen.

Geschlossene VIS mit einem Substatus von **Behoben** Oder **Veraltet** Werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die VIS mit der neuen Schwachstelle abgeglichen werden können.

Angreifbare Elemente auf festgelegt **Gelöst** In Ihrer Instanz, aber nicht zu übergegangen **Geschlossen/Behoben** Durch die nachfolgenden Integrationsausführungen werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Wenn alle VIS für eine Korrekturaufgabe geschlossen sind, wird der Datensatz geschlossen.

Angreifbare Elemente, die in Ihrer Instanz auf „gelöst“ festgelegt sind, aber nicht durch die nachfolgenden Integrationsausführungen auf „Geschlossen/behoben“ umgestellt wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

Für Rapid7 Erkennungen ist jetzt auf der Rapid7-Konfigurationsseite in Ihrer Instanz eine Option verfügbar, um gelöste VIS nach Alter erneut zu öffnen. Wenn diese Option aktiviert ist, werden VIS auf festgelegt **Gelöst** Aber dann nicht zu übergegangen **Geschlossen/Behoben** Durch nachfolgende Scans gehen zurück zu **Öffnen** Nach der von Ihnen eingegebenen Anzahl von Tagen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Qualys Erkennungen, wenn der Scanner weiterhin VIS findet, die auf „gelöst“ festgelegt wurden, aber dann nicht auf übergegangen wurden **Geschlossen/Behoben** Durch nachfolgende Scans werden diese VIS zurück zu verschoben **Öffnen** Wenn das Datum der letzten Suche nach dem Datum der Lösung liegt.

Nächste Maßnahme

Um weitere Daten anzuzeigen, einschließlich der Element- und Erkennungsanzahlen, können Sie Verifizieren Vulnerability Response Erkennungsdaten für angreifbare Elemente in VINTRUN-Datensätzen (Integrationsausführung).

Verifizieren Vulnerability Response Erkennungsdaten für angreifbare Elemente in VINTRUN-Datensätzen (Integrationsausführung)

Von -Integrationsausführungsdatensätze in Ihrem ServiceNow AI Platform® Instanz können Sie Erkennungsdaten für angreifbare Elemente der Drittpartei-Integration basierend auf Datum und Uhrzeit der Scans finden. Überprüfen Sie, ob der Scan erfolgreich abgeschlossen wurde, und zeigen Sie die Anzahl (Anzahl) einzelner Erkennungen sowie alle angreifbaren Elemente (VIS) an, die direkt als Ergebnis der Scans erstellt oder aktualisiert werden.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vuln.admin (veraltet)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Möglicherweise bevorzugen Sie die Informationen zur Integrationsausführung, entweder Datum und Uhrzeit des Scans oder die Datensatznummer der Integrationsausführung (VINTRUN#) aus dem angreifbaren Element oder Erkennungsdatensätzen, damit Sie bestimmte Datensätze aus den folgenden Listen finden können.

Prozedur

1. Wählen Sie eine, um fortzufahren.

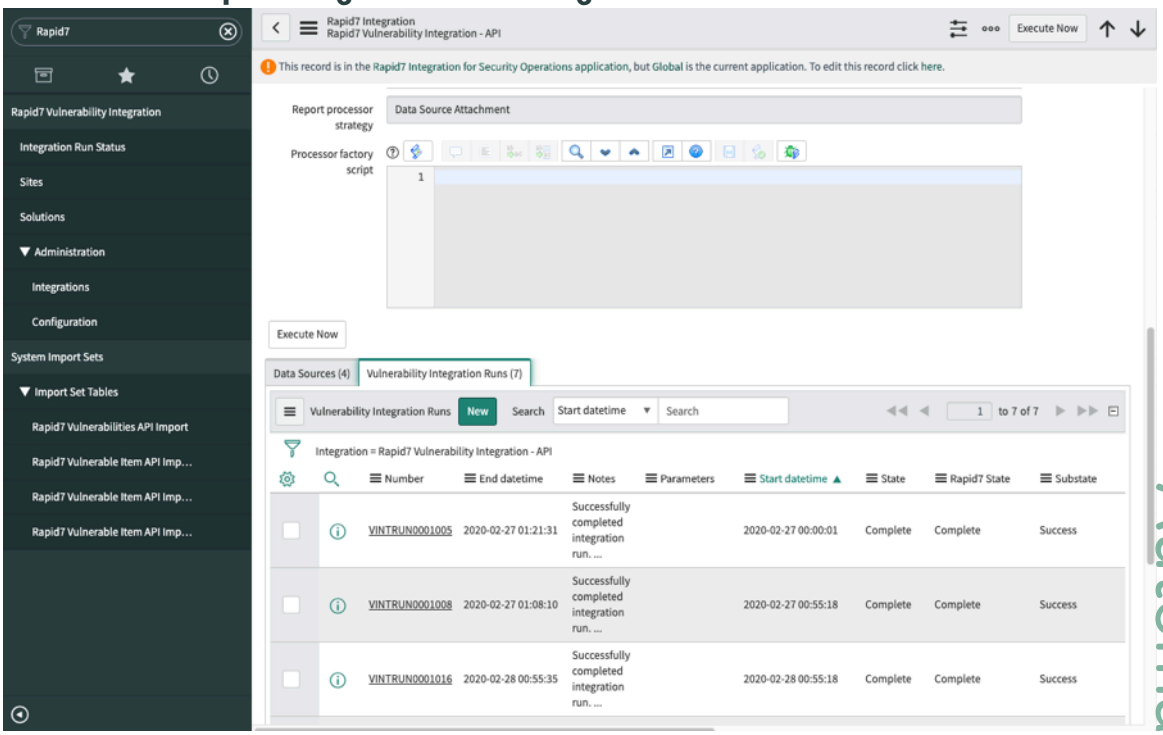
2. Unten auf der angezeigten Seite: Klicken Sie auf **Schwachstellenintegration Wird Ausgeführt** Registerkarte .

3. Klicken Sie auf ein Element in den Spalten Nummer oder Importquelle, um einen Datensatz zu öffnen.

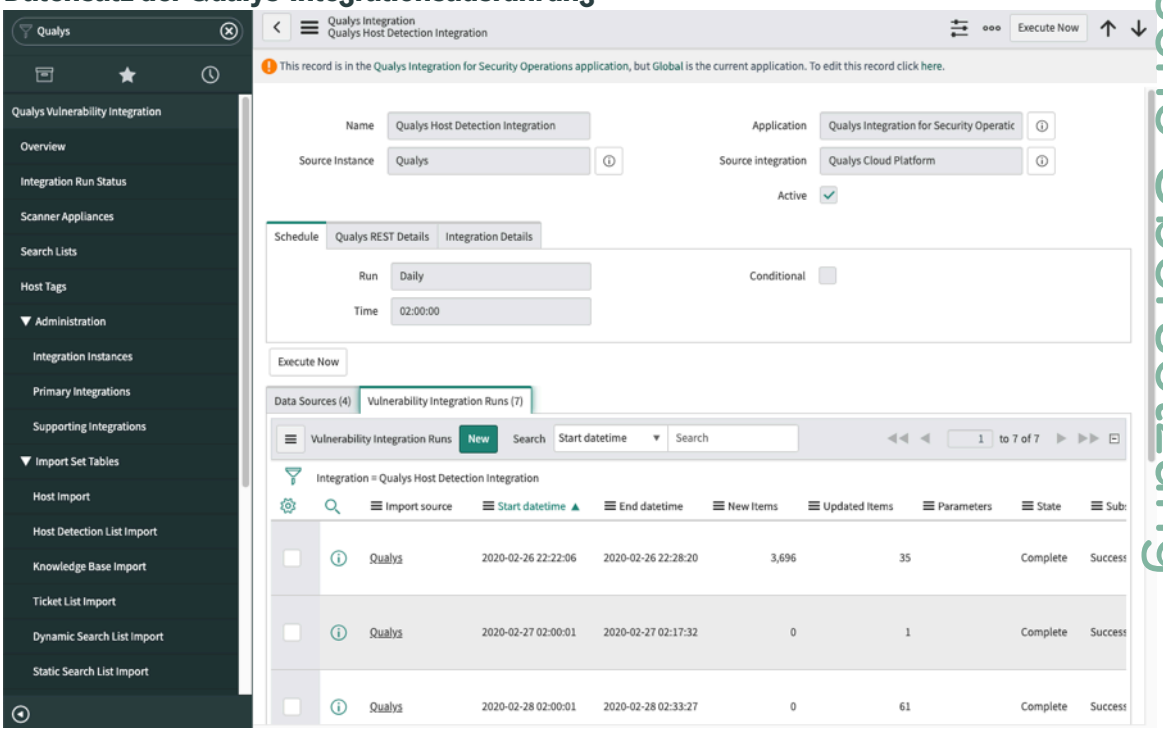
   Der Datensatz der Integrationsausführung wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensatz der Rapid7-Integrationsausführung

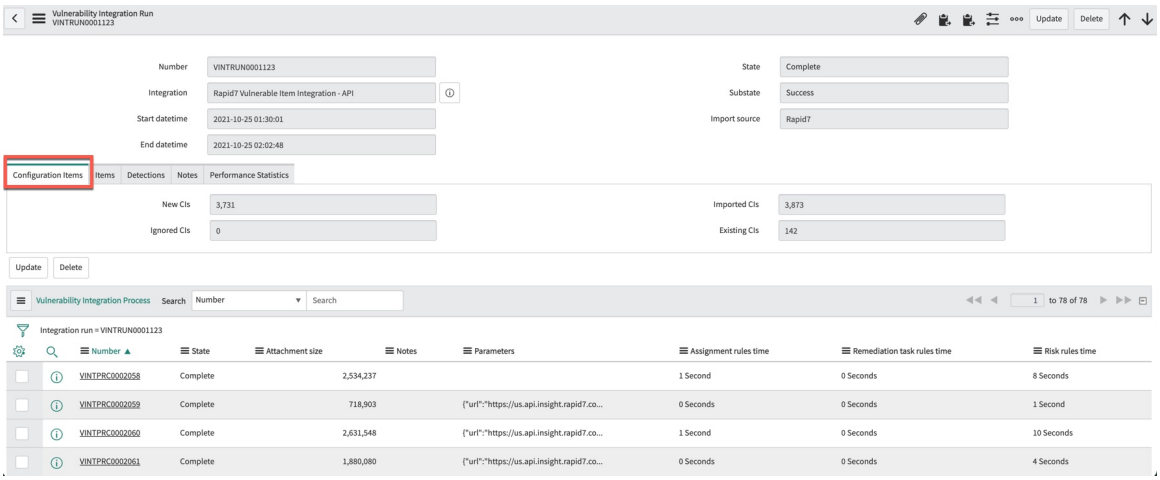


Datensatz der Qualys-Integrationsausführung



Der Datensatz der Integrationsausführung wird angezeigt. Sie können im Feld Status überprüfen, ob die Integration erfolgreich ausgeführt wurde. Wählen Sie aus **Konfigurationselemente** Registerkarte.

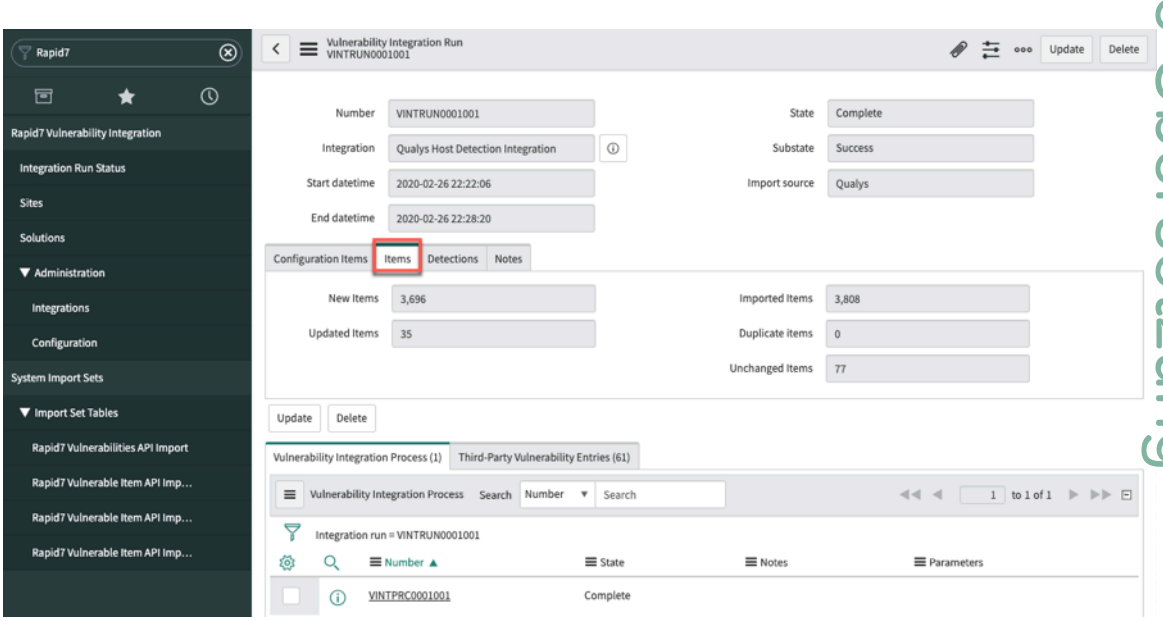
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Auf der Registerkarte Konfigurationselemente werden die folgenden Informationen angezeigt:

- Auf der Registerkarte Konfigurationselemente wird die Gesamtzahl der importierten Konfigurationselemente angezeigt.
- Im Feld neue CIs wird die Anzahl der CIs angezeigt, die als Teil dieser Integrationsausführung erstellt wurden.
- Im Feld importierte CIs wird die Summe aller CIs in diesem Abschnitt angezeigt.
- Der Wert des Felds „ignorierte CIs“ ist für immer 0 Vulnerability ResponseIntegrationen.
- Im Feld vorhandene CIs wird die Gesamtzahl der bereits vorhandenen CIs angezeigt.

Klicken Sie auf **Elemente** Registerkarte.



Auf der Registerkarte Elemente werden die folgenden Informationen angezeigt:

- Auf der Registerkarte Elemente wird die Gesamtzahl der importierten VIS angezeigt. Sie können die Gesamtzahl der importierten Erkennungen anzeigen, indem Sie die auf der Registerkarte Erkennungen aufgeführten Nummern hinzufügen.
- Im Feld neue Elemente wird die Anzahl der angreifbaren Elemente angezeigt, die aus dieser Integrationsausführung erstellt werden.
- Das Feld importierte Elemente zeigt die Summe aller Felder in diesem Abschnitt an.

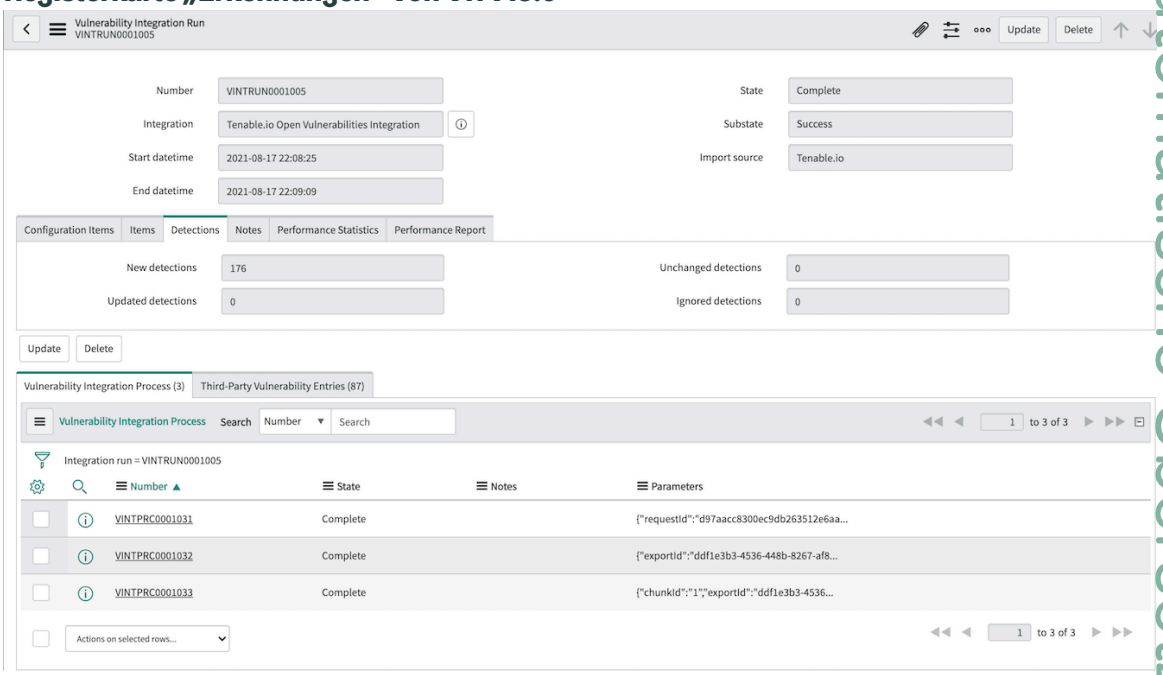
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das Feld doppelte Elemente ist nicht mehr ausgefüllt.
- Im Feld aktualisierte Elemente wird angezeigt, wie oft angreifbare Elemente während dieser Integrationsausführung aktualisiert werden. Dieser Wert ist nicht die Anzahl der eindeutigen angreifbaren Elemente, die aktualisiert werden. Wenn beispielsweise ein angreifbares Element während der Integrationsausführung zweimal aktualisiert wird, wird es zweimal gezählt und als angezeigt 2 Aktualisierte Elemente.
- Das Feld unveränderte Elemente zeigt angreifbare Elemente an, die während der Integrationsausführung gefunden wurden und bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da keiner der relevanten Feldwerte geändert wurde.

4. Klicken Sie auf **Erkennungen** Registerkarte.

   Diese Registerkarte wird nur angezeigt, wenn die Integrationsausführung Erkennungen aufweist. Sie können die Gesamtzahl der importierten Erkennungen überprüfen, indem Sie die aufgeführten Nummern hinzufügen.

Registerkarte „Erkennungen“ Von VR v15.0



Hinweis:
Vor v15.0 gab es kein Feld für ignorierte Erkennungen.

Auf der Registerkarte Erkennungen werden die folgenden Informationen angezeigt:

- Ab v15 wurde ein neues Feld „Erkennungen ignoriert“ hinzugefügt, um die Erkennungen nachzuverfolgen, die zuvor ignoriert wurden. Mit dieser Implementierung wird die Anzahl der importierten Erkennungen und die Anzahl, die in den Datensätzen der Integrationsausführung nachverfolgt wird, konsistent. Diese Funktionalität wurde für alle Scanner implementiert, d. h. Qualys Vulnerability Integration, Rapid7 Vulnerability-Integration, Tenable Vulnerability Integration Und Microsoft TVM.
- Im Feld neue Erkennungen werden neue Erkennungen angezeigt, die während dieser Integrationsausführung erstellt werden.
- Im Feld unveränderte Erkennungen werden während der Integrationsausführung gefundene Erkennungen angezeigt, die bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da keiner der relevanten Feldwerte geändert wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Im Feld aktualisierte Erkennungen wird angezeigt, wie oft Erkennungen während dieser Integrationsausführung aktualisiert werden. Dieser Wert ist nicht die Anzahl der aktualisierten eindeutigen Erkennungen. Wenn beispielsweise eine Erkennung im Rahmen der Integrationsausführung zweimal aktualisiert wird, wird sie zweimal gezählt und als angezeigt 2 Erkennungen aktualisiert.

Hinweis:
Erkennungen, die in diesen Anzahlen nicht angezeigt werden, sind Erkennungen, die sich im Status „Geschlossen“ (behoben) befinden, da feste Datensätze zum Aktualisieren vorhandener VIS verwendet werden. Wenn Sie mehr Transparenz für diese Erkennungsdatensätze wünschen, können Sie die geschlossenen VIS anzeigen, die erstellt werden, wenn kein vorhandenes übereinstimmendes VI in einem offenen Status vorhanden ist. Weitere Informationen zu Schwachstellen im Status „behoben“, die Sie im Setup-Assistenten für die Qualys-Integration aktivieren können, finden Sie unter Wird Konfiguriert Vulnerability Response Mit dem Setup-Assistenten.

5. Klicken Sie auf ein Element in den Spalten Nummer oder Importquelle, um einen Datensatz zu öffnen.

Patch-Daten anzeigen und Patches planen in Vulnerability Response

Ab v16.1 von Vulnerability Response, Sie können Patches planen und Patch-Daten zusammen mit Lösungs- und anderen Schwachstelleninformationen für Datensätze in der klassischen Umgebung und in anzeigen Vulnerability Response Arbeitsbereiche in Ihrem ServiceNow AI Platform Instanz.

Erforderliche Rollen

Anwender benötigen Rollen, die für die Patch-Orchestration-Integration spezifisch sind, die Sie verwenden, um Ihre Patches zu importieren, um Daten anzuzeigen und Patches zu planen. Weitere Informationen finden Sie in den unterstützten Integrationen.

- Verständnis der Integration der HCL BigFix-Patch-Orchestration mit Vulnerability Response und Verstehen von Vulnerability Response Patch-Orchestration-Integration mit Microsoft SCCM.
- Patch-Orchestration-Daten in anzeigen Vulnerability Response Dashboards In der klassischen Umgebung.
- Zeigen Sie Daten zu Bewertungslisten in an Vulnerability Response Arbeitsbereiche.

Patches werden geplant

Sie können Patches aus den folgenden Datensätzen planen:

- Patch-Update (VPU)
- Korrekturaufgabe (RT)
- Erkanntes Element (SDI)

Daten in der klassischen Umgebung patchen

Aus der klassischen Umgebung in Vulnerability Response Anwendung:

- Um Patch-Update-Datensätze anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Patches**an.
- Um Lösungen anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Lösungen**an.
- Um Ihnen zugewiesene VIS mit Patches anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Mir zugewiesen mit Patches**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um Korrekturaufgaben anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Mir zugewiesen mit Patches**
- Um erkannte Elementdatensätze anzuzeigen, navigieren Sie zu **Alle** > **Security Operations** > **Erkannte Elemente**an.

Patch-Daten- und Status-Rollup für Patch-Orchestration in Vulnerability Response

Ab v16.1 von Vulnerability Response Patch-Daten und -status werden in Patch-Update und anderen Datensätzen in zusammengefasst Vulnerability Response Anwendung.

Patch-Update-Datensätze in den Arbeitsbereichen in der klassischen Umgebung in Vulnerability Response

Informationen zu Patches, Schwachstellenlösungen und Schwachstellen sind alle in verbunden Vulnerability Response Anwendung.

Patch-Daten und Patch-Rollup-Daten und -Status werden in Datensätzen in Ihrer Instanz angezeigt. Patch-Datensätze sind als Teil der Patch-Orchestration-Funktion dieser Integration mit enthalten Vulnerability Response. Zeigen Sie Patch-Datensätze (VPU) in Vulnerability Response-Arbeitsbereichen in der Listenansicht im IT-Korrekturarbeitsbereich an. Patch-Update-Datensätze sowohl in der klassischen Ansicht als auch in den Vulnerability Response-Arbeitsbereichen enthalten die folgenden Daten:

- Daten und Informationen der Schwachstellenlösung von Patch-Lieferanten, die von der Anwendung „Schwachstellenlösungsmanagement“ importiert wurden.
- Quellkorrekturstatus, der die Gesamtzahl der Geräte mit einer Schwachstelle enthält, die durch einen Patch behoben werden kann, und aller Geräte, für die Updates fehlen.
- Korrekturstatus, der % der korrigierten VIS und die Gesamtzahl der VIS enthält, die einen Patch als bevorzugten Patch haben.
- Zugeordnete Geräte, angreifbare Elemente, Patch-Bereitstellungen und Patch-Anforderungen in den zugehörigen Links zu Datensätzen in der Klassenansicht. Diese Daten werden auf Registerkarten in Datensätzen in den Vulnerability Response-Arbeitsbereichen angezeigt.
- Patch-Anforderungen, die Korrekturbesitzer zur Genehmigung übermittelt haben.

Erforderliche Rollen

Anwender benötigen Rollen, die für die Patch-Orchestration-Integration spezifisch sind, die Sie verwenden, um Daten anzuzeigen und Patches zu planen. Weitere Informationen finden Sie in den unterstützten Integrationen.

- Verständnis der Integration der HCL BigFix-Patch-Orchestration mit Vulnerability Response und Verstehen von Vulnerability Response Patch-Orchestration-Integration mit Microsoft SCCM.
- Patch-Orchestration-Daten in anzeigen Vulnerability Response Dashboards In der klassischen Umgebung.
- Zeigen Sie Daten zu Bewertungslisten in an Vulnerability Response Arbeitsbereiche.

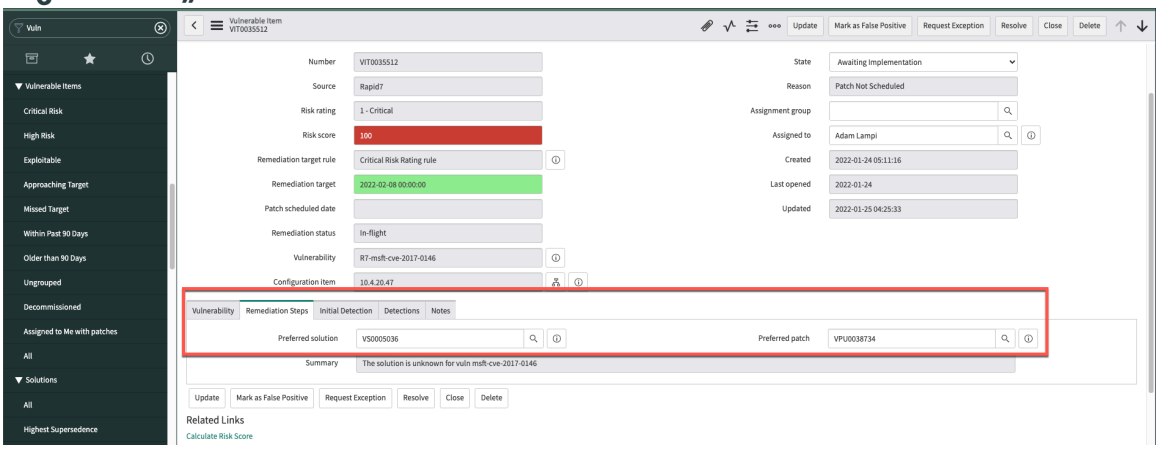
Patch-Daten- und Status-Rollup

Um die angreifbaren Elemente anzuzeigen, die Patches enthalten und Ihnen in der klassischen Umgebung zugewiesen sind, navigieren Sie zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Mir mit Patches zugewiesen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein Datensatz eines angreifbaren Elements mit einem bevorzugten Patch ausgefüllt wird, wird er automatisch zu geändert **Warten Auf Implementierung** Nur, wenn der Status des VI nicht lautet **Geschlossen** , **Gelöst** , **Zurückgestellt** Oder **Wird Überprüft** . Um Detailinformationen zu den Daten anzuzeigen, um die bevorzugte Lösung und andere Daten anzuzeigen, klicken Sie auf **Korrektur** Registerkarte im VI-Datensatz.

Registerkarte „Korrekturschritte“



Ein VI mit einem bevorzugten Patch geht zu über **Warten Auf Implementierung** In den folgenden Fällen:

- Wenn die Bereitstellung eines Patches für ein CI geplant ist, das Teil eines Sammlungsimports ist und dem CI ein VI zugeordnet ist, ist der Grund für das VI **Warten Auf Implementierung** Ist **Patch Geplant** .
- Wenn die Bereitstellung eines Patches für ein CI geplant ist, das Teil eines Sammlungsimports ist und dem CI ein VI zugeordnet ist, und das Korrekturzieldatum (Frist), das nach dem Datum der Zeit bis zur Korrektur (Time to Remediation, TTR) liegt, lautet der Status des VI **Warten Auf Implementierung** Mit dem Grund als **Patch Geplant (Zieldatum Fehlt)** .
- Wenn ein Patch nicht für die Bereitstellung auf einem CI geplant ist, das Teil eines Sammlungsimports ist, lautet der Status des VI **Warten Auf Implementierung** , Mit dem Grund als **Patch Nicht Geplant** .

Klicken Sie auf **Bevorzugter Patch** Informationssymbol zum Öffnen der Patch-Updates und Anzeigen der folgenden Informationen in den zugehörigen Links:

Angreifbare Elemente

Angreifbare Elemente, die diesem Patch zugeordnet sind.

Zugeordnete Geräte

Geräte, die Updates haben und für die Updates fehlen.

Patch-Bereitstellungen

Für diesen Patch geplante Bereitstellungen auf einzelnen Computern (Assets) oder auf Gruppen von Assets.

Patch-Anforderungen

Eine Liste von Patch-Anforderungen, die zur Genehmigung gesendet wurden, bevor sie für die Bereitstellung geplant sind.

Potenzielle Patches

Patches, die eine Schwachstelle beheben könnten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie auf **Informationen zu bevorzugten Patches** Symbol zum Öffnen des Datensatzes, um die zuvor aufgeführten Informationen zusätzlich zu den folgenden Patch-Update-Daten anzuzeigen:

Quellenkorrekturstatus

Die Gesamtzahl der Geräte, die diesen Patch erfordern, und aller Geräte, die den Patch nicht haben.

Nachbesserungsstatus

Der Status (VIS insgesamt, % korrigiert, VIS zurückgestellt) für die VIS, die diesen bevorzugten Patch haben.

Bevorzugte Patches und Lösungen

Wenn eine importierte Schwachstelle mit einem Asset in Ihrem übereinstimmt Configuration Management Database (CMDB), In wird ein angreifbares Element (VI) erstellt Vulnerability Response. Wenn das Configuration Item (CI), das diesem VI zugeordnet ist, auch von einem externen Patch-Lieferanten importiert wird und als fehlender Patch für dieselbe Schwachstelle angezeigt wird, wird ein bevorzugter Patch aufgelistet und ein Rollup für Ihre Lösungen durchgeführt. Diese Informationen informieren Sie darüber, dass ein Asset (CI) über eine Korrektur aus einem verfügbaren Patch verfügt, die für seine Schwachstelle am besten geeignet ist.

Anzeigen von Patches ohne Lösungen

Wenn nach einem Import keine Daten zur Schwachstellenlösung verfügbar sind, wird die verwendet **Schwachstellenlösung** Feld im Patch-Update-Datensatz ist leer. Weitere Informationen zum Anzeigen von Informationen für diese Patchtypen finden Sie unter Zeigen Sie Patches ohne Lösungen in an Vulnerability Response.

Zeigen Sie Patches ohne Lösungen in an Vulnerability Response

Ab v16.0 von Vulnerability Response, Für Patches, die nach einem Import keine Lösungen haben, sucht das System dann in den Schwachstellen-Referenzdaten nach Patch-IDs, damit Sie diese Patches in Schwachstellen-Datensätzen anzeigen können.

Patches ohne Lösungen

Erforderliche Rolle: sn_vul.Vulnerability_admin.

Die aus den Anwendungen Patch Orchestration und Schwachstellenlösung sowie Patch-Scanner-Integrationen importierten Daten werden verarbeitet, verbunden und in angezeigt Vulnerability Response Anwendung für Patch-Update-Datensätze.

Wenn eine Lösung für eine Schwachstelle vorhanden ist, werden zugehörige Informationen in Ihrer Instanz korreliert und von den Patches über Schwachstellenlösungen und zu den Schwachstellen zusammengefasst. Um diese Informationen anzuzeigen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Patches** > **Alle**an.

Wenn nach einem Import keine Daten zur Schwachstellenlösung verfügbar sind, wird die verwendet **Schwachstellenlösung** Feld im Patch-Update-Datensatz ist leer. Damit Sie die zugehörigen Lösungsinformationen für diese Patches sehen können, ist eine Systemeigenschaft [**sn_vul_patch_orch.no_solution_patch_rollup**] Ist standardmäßig in Ihrer Instanz aktiviert. Diese Eigenschaft sucht nach Bulletin-IDs und Artikel-IDs in den Schwachstellen-Referenzdaten aus Scannerimporten. Wenn eine Übereinstimmung gefunden wird, werden die zugehörigen Daten in der Tabelle „potenzielle Patches“ ausgefüllt, und diese Informationen werden in den zugehörigen Listen der Schwachstellendatensätze angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie eine große Anzahl von Schwachstellen haben oder die geplante Rollup-Aufgabe lange dauert, sollten Sie diese Systemeigenschaft deaktivieren, um mögliche Leistungsprobleme zu vermeiden. Beachten Sie jedoch, dass importierte Lösungsdaten, wenn Sie diese Systemeigenschaft deaktivieren, weder nach Ihren Schwachstellen gesucht noch in einem Rollup zusammengefasst werden, ohne dass Lösungen vorhanden sind.

Führen Sie als Anwender mit der Rolle sn_vul.Vulnerability_admin die folgenden Schritte aus, um die Systemeigenschaft zu deaktivieren:

1. Navigieren zu **sys.properties.list**an.
2. Suchen **sn_vul_patch_orch.no_solution_patch_rollup** Und klicken Sie darauf, um den Datensatz zu öffnen.
3. Geben Sie im Feld Wert ein `Falsch` .
4. Klicken Sie auf **Aktualisieren**.

Patch-Orchestration-Daten in anzeigen Vulnerability Response Dashboards

Ab v16.1 können Sie Patch-Update-Daten in der klassischen Umgebung in den Dashboards anzeigen, die in enthalten sind Vulnerability Response Anwendung.

Die Vulnerability Response Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie Ihren Korrekturfortschritt überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen, die aktualisiert werden, wenn sich Schwachstellendaten ändern. Siehe Arbeitsbereich des Schwachstellenmanagers und Arbeitsbereich für IT-Korrekturen erkunden, um weitere Informationen zu erhalten.

Sie können diese Daten auch in den Dashboards CISO und Vulnerability Management (PA) anzeigen, wenn Sie ein Abonnement für haben Performance Analytics.

Sie können Patch-Daten auch in der klassischen Umgebung anzeigen. Weitere Informationen zu den erforderlichen Rollen und zum Anzeigen von Daten in finden Sie Vulnerability Response Dashboards in der klassischen Umgebung, die in enthalten sind Vulnerability Response Anwendungen und Anwendungen, die ein separates Abonnement erfordern, finden Sie unter Wird standardmäßig verwendet Vulnerability Response Dashboards.

Zeigen Sie eine Lösung an

Zeigen Sie alle Lösungen, Lösungen mit höchster Ersetzung und Lösungen an, die angreifbaren Elementen zugeordnet sind, um Ihre Korrekturaktivitäten zu unterstützen.

Vorbereitungen

Erforderliche Rolle: sn_vul.read, sn_vul.Vulnerability_admin oder sn_vul.Remediation_owner
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Als Schwachstellenanalyst oder Korrekturbesitzer können Sie verschiedene Lösungssätze im Zusammenhang mit angreifbaren Elementen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Lösungsdatensätze sind mit Ausnahme von schreibgeschützt **Notizen** In **Interne Notizen** Abschnitt- oder anwendererstellte Lösungen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Lösungen**an.
2. Wählen Sie eine Lösungsliste aus.

   Hinweis:
   Sie können eine Lösungsliste mithilfe von Platzhaltern für den Produktnamen filtern.

3. Klicken Sie zum Überprüfen auf die einzelnen Elemente.
4. **Wahlweise:** Geben Sie unter Notizen ein **Notizen** Registerkarte und Rechtsklick **Speichern** Um auf der Seite zu bleiben, oder klicken Sie auf **Aktualisieren** Um zu speichern und zu zurückzukehren **Schwachstellenlösungen** Liste.

   Hinweis:
   Wenn Sie nur über die Rolle sn_vul.read verfügen, können Sie diesen Schritt nicht ausführen.

Erstellen Sie eine Schwachstellenlösung

Erstellen Sie eine Schwachstellenlösung, damit Sie Schwachstellenlösungen nachverfolgen können, die nicht durch Inhalte von Drittanbieterlösungen abgedeckt sind.

Vorbereitungen

Erforderliche Rolle: admin, sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) oder Vulnerability.write Vulnerability Solution Management Ist eine Funktion, die in verfügbar ist Vulnerability Response Anwendung. Vulnerability Solution Management Erforderlich Ein separates Abonnement.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Lösung aus einer der Lösungslisten erstellen. Sie müssen die Anwendung Schwachstellenlösungsmanagement installieren, bevor Sie eine Lösung erstellen können.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Lösungen**an.
2. Lösungsliste auswählen: **Alle** , **Höchster Ersatz** Oder **Mit Angreifbaren Elementen** .
3. Klicken Sie auf **Neu**.
4. Füllen Sie die bearbeitbaren Felder im Formular entsprechend aus.
   Sie können alle nicht verwendeten Felder leer lassen. Weitere Informationen zu einzelnen Feldern finden Sie unter Lösungsformularfelder.
5. Rechtsklick **Speichern** Im Header.
   Der Lösungsdatensatz wird hinzugefügt und wird in angezeigt **Alle** Und **Höchster Ersatz** Listen, standardmäßig.
6. Die zugehörigen Listen werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können diese Lösung den folgenden zugehörigen Listen zuordnen: **Angreifbare Elemente** , **Schwachstellen Von Drittparteien** , **CVEs** , **Ersatzlösungen** Und **Vorangehende Lösungen** . Wählen Sie eine Schwachstelle oder Lösung aus, und klicken Sie auf **Übermitteln** .

Hinweis:

Vulnerability Solution Management Ordnet angreifbare Elemente und Korrekturaufgaben automatisch Lösungen zu, wenn Schwachstellendatensätze manuell Lösungen zugeordnet werden.

Angreifbare Elemente, die manuell einer anderen Lösung zugewiesen wurden, werden nicht automatisch mit Lösungsänderungen auf Schwachstellenebene aktualisiert.

Wenn Sie die Beziehung zwischen einer Schwachstelle einer Drittpartei und einer Lösung ausschließen möchten, da sie für das von Ihnen zu korrigierende CI nicht relevant ist oder in Ihrer Umgebung kein Problem darstellt, finden Sie unter Schließen Sie Lösungen manuell aus Drittpartei-Datensätzen aus, oder umgekehrt.

Schließen Sie Lösungen manuell aus Drittpartei-Datensätzen aus, oder umgekehrt

Schließen Sie die Beziehung zwischen einer Schwachstelle einer Drittpartei und einer Lösung aus, da sie für das von Ihnen zu korrigierende CI nicht relevant ist oder in Ihrer Umgebung kein Problem darstellt. Schließen Sie Lösungen manuell aus, indem Sie entweder eine Schwachstelle oder einen Lösungsdatensatz einer Drittpartei verwenden.

Vorbereitungen

Erforderliche Rolle:

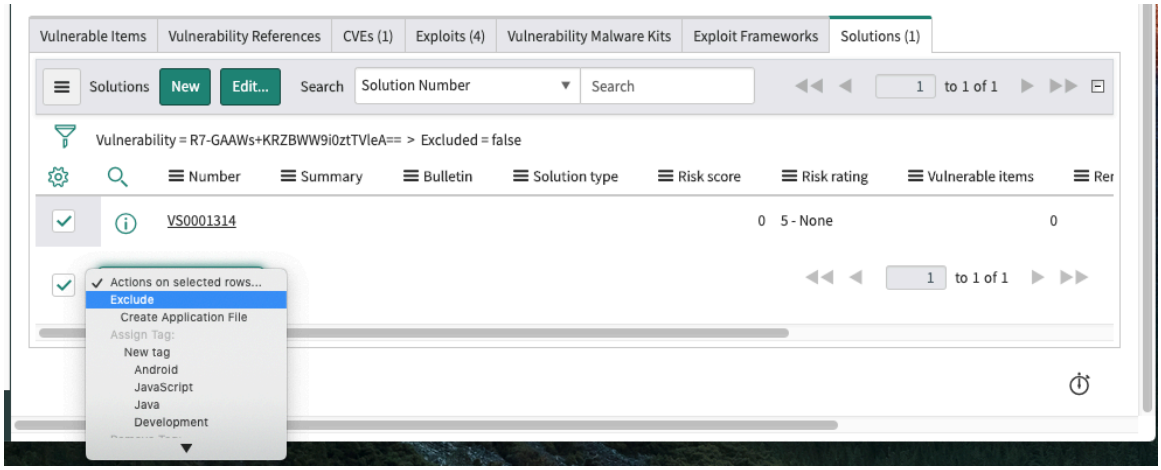
- sn_vul.schreiben
- sn_vul.remediation_owner

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken** > **Drittpartei** oder **Vulnerability Response** > **Alle Lösungen**
2. Öffnen Sie einen Datensatz einer Drittpartei-Schwachstelle oder -Lösung.
   a. Für einen Drittpartei-Datensatz: Wählen Sie aus **Lösungen** Zugehörige Registerkarte.
   b. Für einen Lösungsdatensatz: Wählen Sie aus **Schwachstellen Von Drittparteien** Zugehörige Registerkarte.
3. Aktivieren Sie das Kontrollkästchen neben jedem Schwachstellen- oder Lösungsdatensatz, den Sie ausschließen möchten.
4. Von **Aktionen für ausgewählte Zeilen** Dropdown-Menü auswählen **Ausschließen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Drittpartei- oder Lösungsdatensatz wird nicht mehr auf der zugehörigen Registerkarte angezeigt.

Beziehungen von Drittpartei-Schwachstellen zu Lösungen werden auch ausgeschlossen, wenn Lösungen aktualisiert werden oder wenn der nächtliche Auftrag aktiviert ist.

Beziehungen von Drittpartei-Schwachstellen zu Lösungen werden während der nächtlichen geplanten Aufgabe ausgeschlossen .

Das Ausschließen von Schwachstellen von Drittparteien bedeutet, dass die Lösung nicht mehr ein Faktor für eine bevorzugte Lösungsbewertung ist. Ausschlussauswirkungen:

- Alle Anzahlen für Lösungen, da die Schwachstelle der Drittpartei, angreifbare Elemente (VIS) und Konfigurationselemente (Configuration Items, CIs), die an die Schwachstelle der Drittpartei angehängt sind, nicht mehr auf die Lösung angerechnet werden.
- Bestimmung der bevorzugten Lösung für die Schwachstelle der Drittpartei und durch Erweiterung der bevorzugten Lösung aller angehängten VIS und Korrekturaufgaben, die das VI enthalten

Schwachstellen automatisch selektieren

Die Überprüfung und Selektierung neuer Schwachstellen ist erforderlich, um eine erfolgreiche Behebung sicherzustellen. Wandeln Sie Schwachstellenimporte mit automatisierter Zuweisung angreifbarer Elemente (VI), Risikoberechnung, Korrekturzielen und VI-Gruppierung in Korrekturaufgaben um.

Beginnen Sie mit importierten Schwachstellen, gleichen Sie die Assets ab, die nicht in der CMDB gefunden wurden, priorisieren Sie die Ergebnisse, übersetzen Sie dies in Korrekturaktivitäten, die automatisch zugewiesen werden, orchestrieren Sie den Korrekturprozess, und bestätigen Sie den Abschluss mit einem Validierungsscan.

Neue angreifbare Elemente werden normalerweise beim Import basierend auf den Regeln für Korrekturaufgaben in Korrekturaufgaben sortiert. Manchmal können angreifbare Elemente nicht gruppiert werden oder enthalten kein erkanntes Konfigurationselement.

Eine Übersicht über den Schwachstellen-Selektierungsprozess:

- Melden Sie sich bei der Vulnerability Response-Instanz an.
- Überprüfen Sie, ob Ihre Regeln (CI-Suche, Zuweisung) für angreifbare Elemente wie erwartet funktionieren. Informationen zum Überarbeiten von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Integrationen von Schwachstellen von Drittparteien. Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Aufgrund des großen Volumens bei Datenimporten sollte bei der automatisierten Zuweisung angreifbarer Elemente Vorsicht walten gelassen werden.

- Überprüfen Sie, ob Ihre Korrekturziele korrekt sind. Siehe Vulnerability Response Korrekturzielregeln Um Informationen zur Funktionsweise und Überarbeitung von Korrekturzielregeln zu erhalten.
- Zeigen Sie nicht gruppierte angreifbare Elemente an .
  - Wenn Sie sich die nicht gruppierten angreifbaren Elemente ansehen, sollten Sie Ihre Gruppenregeln überarbeiten und einen erneuten Scan durchführen. Weitere Informationen finden Sie unter Erstellen oder bearbeiten Vulnerability Response Regeln für Korrekturaufgaben.
  - Gruppieren Sie die angreifbaren Elemente manuell. Erstellen Sie manuell eine Korrekturaufgabe in Vulnerability Response Weitere Informationen finden Sie unter .
  - Überarbeiten Sie die Risikopunktzahlen für die angreifbaren Elemente in Ihren Korrekturaufgaben. Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln für Schwachstellenrechner.
  - Schließen Sie ältere angreifbare Elemente, die kürzlich von Ihren Drittpartei-Integrationen nicht erkannt wurden. Weitere Informationen finden Sie unter Automatisches Schließen angreifbarer Elemente und Erkennungen.
- Zeigen Sie nicht abgeglichene Konfigurationselemente an, und klassifizieren Sie sie erneut.
- Recherchieren Sie, was für die Korrektur getan werden muss.

  Dieser Schritt kann Folgendes umfassen:

  - Bestimmen Sie, womit Sie jetzt umgehen und was Sie zurückstellen können. Diese Bestimmung basiert häufig auf der Risikopunktzahl, betroffenen Systemen und Patches mit Change-Fenstern.

    Hinweis:
    Korrekturzielregeln gehören zu angreifbaren Elementen. Diese Regeln werden ausgeführt, wenn das angreifbare Element importiert wird. Diese Regeln wurden zuvor im Setup-Assistenten erstellt.

  - Aktualisieren Sie angreifbare Elemente , Falls erforderlich, und Zeigen Sie den Korrekturzielstatus von an Vulnerability Response Angreifbares Element.
  - Erstellen Sie einen **Change-Anforderung** Und weisen Sie die Korrekturaufgabe einer Zuweisungsgruppe (IT Operations) zur Korrektur zu.

    Hinweis:
    Wenn die Schwachstelle einen Security Incident darstellt, und Security Incident Response Plugin (com.snc.security_incident) ist aktiviert. Sie können stattdessen Security Incident-Datensätze aus den Korrekturaufgaben erstellen.

  - Verschieben Sie nach dem Senden einer oder mehrerer Change-Anforderungen den Gruppenstatus in „wird untersucht“.

Bearbeiten Sie angreifbare Elemente in Massenarbeit Vulnerability Response

Bearbeiten Sie angreifbare Elemente in Massen Um Zeit zu sparen Durch Auswahl von Feldern und Ausführen eines asynchronen Massenbearbeitungsauftrags im Hintergrund.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Wichtig:
Die Massenbearbeitungsfunktion ist für angreifbare Host-Elemente in verfügbar Arbeitsbereich des Schwachstellenmanagers. Weitere Informationen finden Sie unter Massenbearbeitung in verwenden Arbeitsbereich des Schwachstellenmanagers.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Schwachstellen** > **Angreifbare Elemente**an.
2. Wählen Sie die angreifbaren Elemente aus, indem Sie eine der folgenden Aktionen ausführen:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie verwenden möchten **Nur Ausgewählte Elemente** Option in #unique_155_Connect_42_entry-be-record-selection Feld.
   - Wenden Sie Filter an, wenn Sie verwenden möchten **Alle angreifbaren Elemente, die dem Filter entsprechen** Option in #unique_155_Connect_42_entry-be-record-selection Feld.
3. Wählen Sie aus **Massenbearbeitung** Schaltfläche.
4. Füllen Sie die Felder im Modal „Massenbearbeitung“ aus.

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nur ausgewählte angreifbare Elemente ○ Alle angreifbaren Elemente, die dem Filter entsprechen ○ Nachbesserungsaufgabe ○ Verwundbarkeitseintrag
Status	Ändern Sie für **Status** Im angreifbaren Element. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nicht aktualisieren ○ Öffnen ○ Wird untersucht ○ Warten auf Implementierung ○ Zurückgestellt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ▪ Wenn Sie diese Option auswählen, werden die Felder Grund, Kurzbeschreibung, bis und zusätzliche Informationen angezeigt. ▪ Wenn Sie Vits zurückstellen, wird eine Korrekturaufgabe erstellt, und diese Aufgabe wird zur Genehmigung gesendet. ○ Geschlossen **Hinweis:** ▪ Wenn Sie diese Option auswählen, um die Datensätze als falsch positiv zu markieren, werden die Felder Grund, Kurzbeschreibung, bis und zusätzliche Informationen angezeigt. ▪ Wenn Sie die Datensätze als falsch positiv markieren, wird eine Korrekturaufgabe erstellt, und diese Aufgabe wird zur Genehmigung gesendet. ○ Gelöst
Bevorzugte Lösung	Lösung, die darauf ausgerichtet ist, alle angreifbaren Elemente zu korrigieren, die für die Massenbearbeitung ausgewählt sind. Wählen Sie den Change für aus **Bevorzugte Lösung** Feld im Angreifbaren Element (Vits). Auswahlmöglichkeiten stammen aus einer Suchliste verfügbarer bevorzugter Lösungen für die ausgewählten Vits.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ◦ Der Satz der verfügbaren bevorzugten Lösungen ist ein Schnittpunkt aller potenziellen Lösungen der Schwachstellen in allen ausgewählten Vits. ◦ Bei Auswahl von **Datensatzauswahl** > **Schwachstelleneintrag** Für eine Massenbearbeitung alle Vits für die Schwachstelle Wird Auf die ausgewählte bevorzugte Lösung festgelegt werden. **Hinweis:** Dieser Vorgang legt nicht fest **Bevorzugte Lösung** Auf der Ebene des Schwachstelleneintrags. Wird festgelegt **Bevorzugte Lösung** Auf der Ebene des Schwachstelleneintrags würde festlegen **Bevorzugte Lösung** Für alle neuen Vits in Zukunft. Die Massenbearbeitung ändert nur den aktuellen Satz von Vits. ◦ Eindeutige Schwachstellen für die Auswahlkriterien sind auf 500 beschränkt. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, Vits mit verschiedenen Kriterien zum Festlegen von auszuwählen **Bevorzugte Lösung** . ◦ Die Gesamtzahl der Lösungen, die in der Suchliste angezeigt werden können, ist auf 170 begrenzt. Wenn mehr als 170 Lösungen vorhanden sind, wird eine Warnmeldung angezeigt. Der aktualisierte Wert wird in der Listenansicht der angreifbaren Elemente angezeigt.
Bevorzugt Patch	Patch, der darauf ausgerichtet ist, alle für die Massenbearbeitung ausgewählten angreifbaren Elemente zu beheben. **Hinweis:** ◦ Sie müssen Patch Orchestration installieren, um die Liste der bevorzugten Patches anzuzeigen. ◦ Der Satz der verfügbaren bevorzugten Patches ist eine Kreuzung aller potenziellen Patches in allen ausgewählten Vits. ◦ Eindeutige Schwachstellen für die Auswahlkriterien sind auf 500 beschränkt. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, Vits mit verschiedenen Kriterien zum Festlegen von auszuwählen **Bevorzugter Patch** . ◦ Die Gesamtzahl der Patches, die in der Suchliste angezeigt werden können, ist auf 170 begrenzt. Wenn mehr als 170 Patches vorhanden sind, wird eine Warnmeldung angezeigt.
Grund	Grund für die Zurückstellung von Datensätzen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Warten auf Wartungsfenster ○ Behebung nicht verfügbar ○ Risiko akzeptiert ○ Ausgleichende Steuerung vorhanden ○ Sonstige Grund für das Schließen von Datensätzen: ○ Falsch Positiv **Hinweis:** ▪ Wenn Sie diese Option auswählen, werden die Felder Kurzbeschreibung, bis und zusätzliche Informationen angezeigt. ▪ Eine Korrekturaufgabe wird erstellt, wenn Sie die Datensätze als falsch-positiv markieren, und diese Aufgabe wird zur Genehmigung gesendet. ○ Abgebrochen ○ Repariert **Hinweis:** Dieses Feld wird angezeigt, wenn Sie den Status als zurückgestellt oder Geschlossen auswählen.
Kurzbeschreibung	Kurze Notiz, die den Grund für Zurückstellung und geschlossene falsch positive Anforderungen beschreibt. Diese Informationen spiegeln sich im Feld Beschreibung der Korrekturaufgabe wider, die für Zurückstellungs- und geschlossene falsch positive Anforderungen erstellt wird. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie den Status als zurückgestellt und als falsch positiv geschlossen auswählen.
Bis	Datum, bis zu dem der Datensatz zurückgestellt bleibt. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie Status als zurückgestellt auswählen.
Zusätzliche Information	Alle anderen erforderlichen Informationen. Diese Informationen spiegeln sich im Feld zusätzliche Informationen auf der Registerkarte Übersicht wider. Wenn Ihre Zurückstellungsanforderung genehmigt wird, werden diese zusätzlichen Informationen als Zurückstellungshinweise sowohl in VIT als auch in der Korrekturaufgabe angezeigt. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie den Status als zurückgestellt und als falsch positiv geschlossen auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zuweisung aufheben	Alle ausgewählten Elemente werden für die Zuweisungsgruppe und den Korrekturbesitzer nicht zugewiesen. Weitere Informationen dazu, wie ein Korrekturbesitzer die Zuweisungen aus angreifbaren Elementen entfernen kann, finden Sie unter Entfernen Sie Zuweisungen aus angreifbaren Elementen für Sie oder Ihre Gruppen . **Hinweis:** ○ Dieses Feld wird angezeigt, wenn Sie Status als nicht aktualisieren auswählen. ○ Wenn Sie die Zuweisung von Datensätzen aufheben, wird eine Korrekturaufgabe erstellt, und diese Aufgabe wird zur Genehmigung gesendet.
Zuweisungsgruppe	Zuweisungsgruppe für die VIT. Wählen Sie manuell oder Zuweisungsempfehlungen verwenden aus, wenn diese Option aktiviert ist. **Hinweis:** Dieses Feld ist deaktiviert, wenn Sie auswählen **Zuweisung Aufheben** Kontrollkästchen.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

5. Wählen Sie **OK**.
   Ein asynchroner Massenbearbeitungsauftrag aktualisiert die ausgewählten Datensätze. Die Auftragsnummer mit einem Link wird auf der Seite „angreifbare Elemente“ angezeigt, auf der Sie ihren Status anzeigen können. Eine Korrekturaufgabe wird mit den ausgewählten angreifbaren Elementen erstellt, wenn Sie angreifbare Elemente in einem Massenvorgang zurückstellen, die Zuweisung aufheben oder schließen (falsch positiv). Und diese Korrekturaufgabe wird zur Genehmigung gesendet.

Gruppierung Aufgehoben Vulnerability Response Angreifbare Elemente

Angreifbare Elemente werden automatisch einer Korrekturaufgabe zugewiesen, wenn sie importiert werden. Wenn beispielsweise ein angreifbares Element (VI) manuell erstellt wird, kann das VI jedoch manchmal zu einem verwaisten Element werden. Die **Gruppierung Aufgehoben** Das Modul „angreifbare Elemente“ listet diese angreifbaren Elemente ohne Gruppe auf.

Hinweis:
Automatisierte Integrationsprozesse erstellen keine verwaisten Elemente, daher wird erwartet, dass dieser Anwendungsfall klein ist.

Die Aufhebung der Gruppierung erfolgt, wenn ein angreifbares Element ohne Schwachstelle erstellt wurde oder keine Korrekturaufgabenregel vorhanden ist, die das VI einer Gruppe zuweist.

Überprüfen Sie in diesem Fall die Liste der nicht gruppierten angreifbaren Elemente, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Nicht gruppiert**an.

Nach der Überprüfung haben Sie folgende Auswahlmöglichkeiten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können Erstellen oder bearbeiten Vulnerability Response Regeln für Korrekturaufgaben Um Elemente zu erfassen, die in dieser Liste angezeigt werden.
- Sie können Erstellen Sie manuell eine Korrekturaufgabe in Vulnerability Response Und fügen Sie der Gruppe manuell Elemente aus dieser Liste hinzu, oder definieren Sie eine Bedingung, die diesen Elementen entspricht.
- Sie können eine vorhandene Korrekturaufgabe und öffnen Fügen Sie der Gruppe alle relevanten angreifbaren Elemente hinzu Solange sie sich im Status „Offen“ oder „wird untersucht“ befindet.

Hinweis:
Manuell hinzugefügte angreifbare Elemente werden nicht automatisch durch Regeln für Korrekturaufgaben oder Gruppenbedingungen aus Korrekturaufgaben entfernt.

Weitere Informationen zum Verhalten von Korrekturaufgaben und Aufgabenregeln finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.

Ansicht nicht gruppiert Vulnerability Response Angreifbare Elemente

Angreifbare Elemente, die keiner Gruppe zugewiesen sind, werden in einer anzeigbaren Liste platziert.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Schwachstellen** > **Nicht gruppierte angreifbare Elemente**an.
2. Überprüfen Sie die angreifbaren Elemente in der Liste.
3. Klicken Sie auf jedes angreifbare Element, um anzuzeigen und zu bestimmen, wie in eine Gruppe aufgenommen werden soll.

Fügen Sie einer Korrekturaufgabe manuell ein angreifbares Element hinzu

Wenn ein angreifbares Element nicht gruppiert ist, können Sie es einer Korrekturaufgabe hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Notieren Sie die Nummer der angreifbaren Person.
2. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**an.
3. Wählen Sie eine Korrekturaufgabe (VUL) für Ihr angreifbares Element aus.
4. Wählen Sie Aus **Bearbeiten** Unten rechts.
5. Geben Sie ein **Angreifbares Element** Nummer im Suchfeld für Sammlung.
6. Wählen Sie das angreifbare Element aus der Sammlung aus, und fügen Sie es der Liste hinzu.
7. Klicken Sie auf **Speichern**.

Entfernen Sie Zuweisungen aus angreifbaren Elementen und Korrekturaufgaben

Löschen Sie **Zugewiesen an** Und **Zuweisungsgruppe** Felder in Datensätzen angreifbarer Elemente in Vulnerability Response, Application Vulnerability Response, Und Container Vulnerability Response Anwendungen.

Vorbereitungen

Erforderliche Rollen:

- sn_vul.Remediation_owner oder sn_vul.Vulnerability_Analyst für angreifbare Elemente (Vits) und Korrekturaufgaben (VULs).
- sn_vul.App_sec_Manager für Application Vulnerability Response Angreifbare Elemente (AVITs) und Korrekturaufgaben (AVULs).
- sn_vul_Container.Remediation_owner oder sn_vul_Container.Vulnerability_Analyst für angreifbare Container-Elemente (CVITs) und Korrekturaufgaben (CVULs).

Warum und wann dieser Vorgang ausgeführt wird

Die **Zuweisung Aufheben** Die UI-Aktion wird sowohl in der klassischen Umgebung als auch in den Arbeitsbereichen für die folgenden Datensätze in einem anderen Status als „Geschlossen“ oder „gelöst“ unterstützt:

- Korrekturaufgaben (VULs, AVULs und CVULs). Wenn eine Korrekturaufgabe mit dieser Funktion aktualisiert wird, wird **Zugewiesen an** Und **Zuweisungsgruppe** Felder in allen zugehörigen Vits, die dieselbe Zuweisungsgruppe haben, werden ebenfalls gelöscht.
- Angreifbare Elemente (Vits).
- Angreifbare Anwendungselemente (AVITs).
- Angreifbare Container-Elemente (CVITs).

Wichtig:
Sie können die Zuweisung von angreifbaren Host-Elementen in Massenmedien in aufheben Arbeitsbereich des Schwachstellenmanagers. Weitere Informationen finden Sie unter Massenbearbeitung in verwenden Arbeitsbereich des Schwachstellenmanagers.

Prozedur

1. Navigieren Sie entweder in der klassischen Umgebung oder im IT-Korrekturbesitzerbereich zu einem Datensatz für angreifbare Elemente (Angreifbare Elemente, VIT), der Ihnen zugewiesen ist und sich in einem anderen Status als „Geschlossen“ oder „gelöst“ befindet.
2. Zum Löschen von **Zugewiesen an** Und **Zuweisungsgruppe** Wählen Sie in der klassischen Ansicht oben im Datensatz die Option aus **Zuweisung Aufheben** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Alternativ navigieren Sie zu einem Datensatz für angreifbare Elemente (VIT, AVIT oder CVIT) im IT-Korrekturarbeitsbereich, der Ihnen oder Ihren Gruppen zugewiesen ist, und klicken Sie auf **Zuweisung**

Aufheben Im Menü „weitere Optionen“ ( ), um die Zuweisungsfelder zu löschen.

4. Öffnen Sie für Datensätze von Korrekturaufgaben im Arbeitsbereich, die Ihnen oder Ihren Gruppen zugewiesen sind, eine Datensatzauswahl **Zuweisung Aufheben** Im Menü „weitere Optionen“ (

), um die Zuweisungsfelder zu löschen.

5. Geben Sie im Dialogfeld „Zuweisung aufheben“ für angreifbare Elemente und Korrekturaufgaben Arbeitsnotizen an, und wählen Sie aus **Übermitteln** .
Die Anforderung zur Genehmigung der Statusänderung wird zur Genehmigung übermittelt.

Hinweis:
Für Korrekturaufgaben werden Sie benachrichtigt, dass **Zugewiesen an** Und **Zuweisungsgruppe** Felder in allen zugeordneten Vits einer Korrekturaufgabe werden ebenfalls gelöscht.

Nachdem die Anforderung zum Löschen der Felder für eine Korrekturaufgabe genehmigt wurde, alle **Zugewiesen an** Und **Zuweisungsgruppe** Felder in ihren angreifbaren Elementen, die dieselbe Zuweisungsgruppe haben, werden ebenfalls nicht zugewiesen. Wenn ein angreifbares Element eine andere Zuweisungsgruppe hat als die zugehörige Korrekturaufgabe, wird die Zuweisung nicht aufgehoben. In den meisten Fällen wurden diese angreifbaren Elemente manuell zugewiesen.

6. Zeigen Sie die folgenden Informationen an:
   - Die von Ihnen angegebenen Arbeitsnotizen werden im Abschnitt Notizen angezeigt.
   - Auf der **Genehmigung Der Statusänderung** Registerkarte wird der Genehmigungsdatensatz für Statusänderungen mit dem Status in Überprüfung angezeigt, was zur Nachverfolgung des Genehmigungs-Workflows beiträgt.
   - Auf der **Angeforderte Genehmigungen** Registerkarte wird Ihre Anforderung zum Entfernen von Ihnen oder Ihrer Zuweisungsgruppe im Status „angefordert“ angezeigt.

Ergebnisse

Die Anforderung wird mit einem standardmäßigen Genehmigungs-Workflow auf einer Ebene genehmigt. Weitere Informationen finden Sie unter Genehmigen oder lehnen Sie eine Anforderung zum Aufheben der Zuweisung in ab Vulnerability Response.

- Wenn Ihre Anforderung genehmigt ist, wechseln der Status „Genehmigungsdatensatz“ und der Datensatz „angeforderte Genehmigung“ in den Status „genehmigt“. Sie und Ihre Gruppen werden aus entfernt **Zugewiesen an** Und **Zuweisungsgruppe** Felder. Nicht Zugewiesen Wird in angezeigt **Zuweisungstyp** Und die Korrekturaufgabe und Vits werden in der Liste des Moduls nicht zugewiesen für jedes Produkt angezeigt.

  Benachrichtigungen, dass Datensätze nicht zugewiesen werden, werden automatisch an Schwachstellenmanager oder Analysten in der Benachrichtigungsgruppe „Zuweisung aufheben“ gesendet. Informationen zum Konfigurieren der Genehmigungskennzeichnung,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Benachrichtigungen und der Standardzuweisungsgruppe finden Sie unter Entfernen von Zuweisungen aus angreifbaren Elementen und Korrekturaufgaben .

- Wenn Ihre Anforderung abgelehnt wird, wechseln der Status des Change-Genehmigungsdatensatzes und des Datensatzes der angeforderten Genehmigung in den Status abgelehnt.

Hinweis:
Als Schwachstellenadministrator können Sie festlegen `sn_vul.unassign_vr.approval_required` Systemeigenschaft zu **Falsch** Zum Deaktivieren des Genehmigungsprozesses.

Nächste Maßnahme
Navigieren Sie zu nicht zugewiesene Module für Vulnerability Response Und Application Vulnerability Response Container Vulnerability ResponseÜberwachen Sie alle nicht zugewiesenen Datensätze auf Elemente, die in Ihren Bereich fallen könnten, und weisen Sie sie sich selbst neu zu.

Genehmigen oder lehnen Sie eine Anforderung zum Aufheben der Zuweisung in ab Vulnerability Response

Genehmigen Sie Anforderungen zum Entfernen angreifbarer Elemente aus einer Zuweisungsgruppe oder einem einzelnen Anwender in Vulnerability Response Anwendung.

Vorbereitungen
Erforderliche Rolle: Zum Aufheben der Zuweisung von Genehmigungen ist ein Genehmiger in der Gruppe „Genehmiger – Ebene 1“ erforderlich.

- sn_vul.unassign_Approver für AVITs und Vits
- sn_vul_Container.unassign_Approver für CVITs

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig wird eine Genehmigungskonfiguration bereitgestellt, und eine Genehmigungsgruppe zum Aufheben der Zuweisung wird erstellt. Anwender der Gruppe „Genehmiger aufheben – Ebene 1“ können die Anforderung genehmigen. Diese Gruppe enthält standardmäßig die Rolle „Genehmiger aufheben“, sn_vul.unassign_Approver. Sie können eine neue Gruppe ändern oder erstellen und die Genehmigungskonfiguration aktualisieren. Um eine Genehmigungsregel zu konfigurieren, wählen Sie eine der folgenden Genehmigungsregeln im Modul „Genehmigungsregeln“ aus, und navigieren Sie zur Genehmigungskonfiguration im **Genehmigungskonfigurationen** Registerkarte:

- `Vulnerable item field change request` Für ein angreifbares Element.
- `Vulnerability field change request` Für eine Korrekturaufgabe.
- `Application vulnerability field change request` Für ein angreifbares Anwendungselement (AVIT).
- `Approval for container management` Für ein angreifbares Container-Element (CVIT).

Weitere Informationen zu Genehmigungsregeln und -Konfigurationen finden Sie unter Genehmigungs-Workflow-Konfigurationen für Anforderung zum Aufheben der Zuweisung.

Wichtig:
Sie können Anforderungen in genehmigen oder ablehnen Arbeitsbereich des Schwachstellenmanagers. .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Meine Genehmigungen** Für Vits und AVITs. Alternativ navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Meine Genehmigungen** Für CVITs.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie ab, indem Sie die entsprechenden Kommentare hinzufügen.

Automatisches Schließen angreifbarer Elemente und Erkennungen

Sie können veraltete Erkennungen und angreifbare Elemente (VIS), die stillgelegten CIs zugeordnet sind, mithilfe des Moduls „Regeln für automatisches Schließen“ automatisch schließen.

Sie können veraltete Erkennungen und VIS in den folgenden Szenarien automatisch schließen:

- Veraltete Erkennungen in automatisch schließen Vulnerability Response
- Schließen Sie angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch

Informationen zum Arbeiten mit stillgelegten Konfigurationselementen finden Sie unter Arbeiten mit stillgelegten Konfigurationselementen Und Erstellen Sie Regeln für das automatische Schließen.

Arbeiten mit stillgelegten Konfigurationselementen

Außer Betrieb genommene Konfigurationselemente (CIs) werden in den Status „stillgelegt“, „archiviert“ oder „gelöscht“ verschoben Configuration Management Database (CMDB). Vulnerability Response Enthält angreifbare Elemente (VIS), die aus CIs bestehen. Wenn der Status eines CI auf „stillgelegt“ aktualisiert wird, werden die zugehörigen VIS mit dem Substatus „CI außer Betrieb genommen“ geschlossen.

Hinweis:
Ab v25.0.3 von Vulnerability Response, Wird eine neue Regel für das automatische Schließen „CI außer Betrieb genommen“ eingeführt, um die angreifbaren Elemente und Erkennungen im Zusammenhang mit außer Betrieb genommenen CIs zu schließen.

Wenn die CMDB den Status der Lebenszyklusphase eines CI in „stillgelegt“ ändert, können Sie die zugehörigen VIS automatisch schließen. Weitere Informationen zum automatischen Schließen der zugehörigen VIS finden Sie unter Schließen Sie angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch.

Das stillgelegte CI wird schließlich archiviert oder endgültig aus dem gelöscht CMDB.

Auswirkung der Stilllegung der CIs:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Auswirkung auf erkannte Elemente:** Wenn das CI stillgelegt wird, wird das zugehörige erkannte Element (DI) als „CI außer Betrieb genommen“ markiert.
- **Auswirkung auf angreifbare Elemente:** Wenn der Status eines DI auf „CI außer Betrieb genommen“ aktualisiert wird, wird das zugehörige VI geschlossen, und der Abschnitt „Notizen“ wird automatisch aktualisiert.

Hinweis:
Der Status eines DI wird automatisch auf „CI außer Betrieb genommen“ aktualisiert, wenn der Lebenszyklusstatus eines CI aktualisiert wird. Andererseits wird der Status eines VI nur dann auf „Geschlossen“ aktualisiert, wenn der **VIS, die mit stillgelegten CIs verknüpft sind, automatisch schließen** Option ist aktiviert. Weitere Informationen zum automatischen Schließen der zugehörigen VIS finden Sie unter Schließen Sie angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch.

Die geplante Aufgabe *`Close detections/VIs for decommissioned CIs`*Wird täglich für die aktualisierte DIS ausgeführt. Wenn die Konfigurationsoption für das automatische Schließen für stillgelegte CIs aktiviert ist, identifiziert sie den DI, der ein stillgelegtes CI enthält, und schließt das zugehörige VI mit dem Substatus „CI außer Betrieb genommen“. Wenn alle VIS in einer Korrekturaufgabe geschlossen sind und ihr Substatus „CI außer Betrieb genommen“ lautet, wird die Korrekturaufgabe auch mit dem Substatus „Abgebrochen“ geschlossen. Um die außer Betrieb genommenen VIS anzuzeigen, navigieren Sie zu **Vulnerability Response** > **Angreifbare Elemente** > **Außer Betrieb genommen**an.

Hinweis:
Wenn ein CI vom Status „stillgelegt“ in den ursprünglichen Status zurückversetzt wird, wird auch der Eintrag „erkannte Elemente“ aktualisiert. VIS werden automatisch geöffnet, wenn Daten erneut vom Scanner erfasst werden.

Schließen Sie angreifbare Elemente im Zusammenhang mit stillgelegten CIs automatisch

Wenn Configuration Management Database (CMDB)Ändert den Status der Lebenszyklusphase eines Konfigurationselements (Configuration Item, CI) in „stillgelegt“. Sie können die zugehörigen angreifbaren Elemente (VIS) und Erkennungen automatisch schließen.

Vorbereitungen
Erforderliche Rolle: sn_vul.admin

Warum und wann dieser Vorgang ausgeführt wird
Beginnend mit v22.0 von Vulnerability Response, Um die zugehörigen VIS und Erkennungen automatisch zu schließen, müssen Sie die Systemeigenschaft aktivieren *`sn_vul_cmn.auto_close_vis_linked_retired_cis`*Dient zum automatischen Schließen von VIS, die stillgelegten CIs zugeordnet sind. Um die Option zu aktivieren, legen Sie das Wertfeld auf „1“ fest. Um die Option zu deaktivieren, legen Sie das Wertfeld auf „0“ fest.

Während eines Upgrades, wenn die Systemeigenschaft *`sn_vul_cmn.auto_close_vis_linked_retired_cis`*Ist in v21.0 von ausgewählt Vulnerability Response, Dann bleibt der Wert „1“. Wenn diese Option aktiviert ist, werden alle neuen oder vorhandenen VIS und Erkennungen, die für dasselbe CI gemeldet werden, automatisch erstellt oder mit dem Status „Geschlossen“ aktualisiert. Dies basiert auf der Asset-ID in der Scanner-Nutzlast und dem Status des Eintrags „erkannte Elemente“. Weitere Informationen zu den Auswirkungen stillgelegter CIs finden Sie unter Arbeiten mit stillgelegten Konfigurationselementen

an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Der Status eines DI wird immer dann auf „CI außer Betrieb genommen“ aktualisiert, wenn der Lebenszyklusstatus eines CI aktualisiert wird. Andererseits wird der Status eines VI nur dann auf „Geschlossen“ aktualisiert, wenn der **VIS, die mit stillgelegten CIs verknüpft sind, automatisch schließen** Option ist aktiviert.
- Die im folgenden Verfahren bereitgestellten Informationen gelten nur für Versionen vor v22.0 von Vulnerability Response. Ab v22.0 von Vulnerability Response, Sie haben die Möglichkeit, zusätzliche Suchoptionen zu konfigurieren. Weitere Informationen finden Sie unter Erstellen Sie Regeln für das automatische Schließen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Konfiguration für automatisches Schließen** > **Konfigurationselement-Lebenszyklus**an.
2. Um angreifbare Elemente, die den stillgelegten CIs zugeordnet sind, automatisch zu schließen, wählen Sie aus **VIS, die mit stillgelegten CIs verknüpft sind, automatisch schließen** Kontrollkästchen.
3. Wählen Sie **Aktualisieren**.

Hinweis:

Wenn ein CI bereits vor stillgelegt wurde **VIS, die mit stillgelegten CIs verknüpft sind, automatisch schließen** Option ist aktiviert. VIS werden nur für neue Erkennungen von Scannern erstellt. Der Status dieser VIS ist „Geschlossen“, und der Substatus ist „CI außer Betrieb genommen“.

Sie können VIS mit dem Status „CI außer Betrieb genommen“ nicht manuell erneut öffnen **Erneut Öffnen** Oder **Massenbearbeitung** Optionen.

Geschlossene VIS mit dem Substatus „behoben“ oder „veraltet“ werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die VIS mit der neuen Schwachstelle abgeglichen werden können. Weitere Informationen finden Sie unter Erkennungen, Korrekturaufgaben und status angreifbarer Elemente.

Veraltete Erkennungen in werden geschlossen Vulnerability Response

Das Modul „veraltete Erkennungen automatisch schließen“ hilft Ihnen, ältere, veraltete angreifbare Erkennungen automatisch zu bereinigen, die kürzlich von Ihren Drittanbieterintegrationen nicht gefunden wurden. Durch das Verschieben dieser Erkennungen in „Geschlossen“ wird die Anzahl der aktiven angreifbaren Elemente und Korrekturaufgaben in Ihrem reduziert ServiceNow AI Platform Instanz und hilft Ihnen beim Abgleich von Assets in Ihrer CMDB.

Übersicht und wichtige Begriffe

Um die Rollup-Erkennungsdaten für Ihre angreifbaren Elemente genauer zu gestalten, hilft Ihnen das Modul „veraltete Erkennungen automatisch schließen“, ältere Erkennungen für veraltete angreifbare Elemente zu bereinigen, die kürzlich von Ihren Drittanbieterintegrationen nicht gefunden wurden. Weitere Informationen zu dieser Funktion finden Sie im Anwendungsfall unten.

In vorherigen Versionen von Vulnerability Response, Das Modul „angreifbare Elemente automatisch schließen“ hat angreifbare Elemente, die nicht kürzlich von Ihren Drittanbieter-Scannerintegrationen gefunden oder aktualisiert wurden, automatisch auf „Geschlossen – Veraltet“ gesetzt.

Bevor Sie die Funktion „veraltete Erkennungen automatisch schließen“ aktivieren, überprüfen Sie die folgenden Begriffe, wie status für angreifbare Elemente und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturaufgaben zusammengefasst werden, und die Voraussetzungen für Ihre Drittpartei-Integrationen, die Erkennungsdaten importieren.

Informationen zum Aktivieren der Funktion finden Sie unter Veraltete Erkennungen in automatisch schließen Vulnerability Response.

Wichtige Begriffe

Veraltete Erkennungen

Bezieht sich auf Erkennungen, die angreifbaren Elementen in zugeordnet sind ServiceNow AI Platform® Instanzen, die veraltet sind und von Integrationsscans von Drittparteien seit längerer Zeit nicht gefunden, aktualisiert oder erkannt wurden.

Zuletzt gefundene Erkennungen

Diese Suchoption verwendet ein Datum und eine Uhrzeit, die vom Scanner des Drittanbieters bereitgestellt werden. Dieser Begriff bezieht sich auf das aktuellste oder späteste Datum und die Uhrzeit, zu der Erkennungen vom Scanner erneut gefunden wurden.

Zuletzt gescannte Assets

Diese Suchoption verwendet ein Datum und eine Uhrzeit, die vom Scanner des Drittanbieters bereitgestellt werden. Dieser Begriff bezieht sich auf das aktuelle Datum und die Uhrzeit, zu der ein Asset zuletzt von einem Scanner einer Drittpartei gescannt wurde.

Anwendungsfall

Manchmal können Assets (Konfigurationselemente) in Ihrer Umgebung außer Betrieb genommen oder von Drittanbieterscannern gelöscht werden, und ihre zugehörigen Erkennungen werden nicht durch Erkennungen angreifbarer Elemente aktualisiert. Daher werden die Erkennungen und die zugehörigen angreifbaren Elemente in nicht aktualisiert Vulnerability Response Anwendung, und sie werden inaktiv (veraltet).

Um diese veralteten Erkennungen mit unveränderten Daten zu angreifbaren Elementen zu schließen und die Anzahl der aktiven VIS- und Korrekturaufgaben (RTS) zu reduzieren, aktivieren Sie das automatische Schließen veralteter Erkennungen. Diese Funktion schließt automatisch Erkennungen angreifbarer Elemente, die von Ihren Scannerintegrationen von Drittanbietern nicht kürzlich gefunden oder aktualisiert wurden, basierend auf Suchkriterien und einem von Ihnen festgelegten Alter in Tagen.

Angenommen, ein bestimmtes Konfigurationselement (Configuration Item, CI) hat mehrere Asset-IDs, und eine dieser IDs wurde in den letzten 90 Tagen nicht bei einer Erkennung von einem Scanner eines Drittanbieters importiert. Diese Funktion schließt automatisch diese Erkennung, die keine neuen Schwachstellendaten enthält, sodass das zugehörige VI geschlossen werden kann.

Da einem VI mehr als eine Erkennung zugeordnet sein kann, übergeht diese Funktion nur die Erkennungen, die durch die von Ihnen festgelegten Parameter als veraltet festgelegt wurden. Wenn einem VI beispielsweise vier Erkennungen zugeordnet sind und zwei Erkennungen veraltet sind, d. h. dass in den letzten 90 Tagen keine neuen Schwachstellendaten importiert wurden, schließt diese Funktion nur die veralteten Erkennungen. Bevor das VI geschlossen werden kann, müssen Sie zuerst die beiden anderen offenen Erkennungen korrigieren.

Rollup der erkennungsstatus zu VIS

Um die automatisch geschlossenen Erkennungen von Erkennungen zu unterscheiden, die von Drittanbieterscannern geschlossen wurden, wurde ein neuer Wert für das Feld Status, Veraltet, hinzugefügt. Die möglichen Werte für dieses Feld sind Offen, Geschlossen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und Veraltet. Veraltet gibt an, dass eine Erkennung durch die Erkennungsfunktion zum automatischen Schließen geschlossen wurde.

Statusvorrang: „Offen“ > „Geschlossen“ > „Veraltet“.

1. Wenn Erkennungen offen sind, bleibt der zugeordnete VI-Status offen.
2. Wenn keine Erkennungen offen sind, einige geschlossen sind und einige veraltet sind, wechselt der zugehörige VI-Status in „Geschlossen – behoben“.
3. Wenn alle Erkennungen veraltet sind, wechselt der zugeordnete VI-Status in Geschlossen – Veraltet.

   Beginnend mit Vulnerability Response20.0: Wenn die Erkennung veraltet ist und sich das zugehörige VI im Status Geschlossen befindet, wechselt der Status des VI nicht in Geschlossen – Veraltet. Dadurch soll verhindert werden, dass das VI erneut geöffnet wird, wenn eine neue Erkennung identifiziert wird, sodass Sie vermeiden können, dass der gesamte falsch positive Anforderungs- und Genehmigungsprozess durchlaufen wird. Um dieses Verhalten umzukehren, deaktivieren Sie **Veraltete Erkennungen für geschlossene VIS ignorieren** Kontrollkästchen im Formular „Konfiguration automatisch schließen“. Weitere Informationen finden Sie unter Veraltete Erkennungen in automatisch schließen Vulnerability Response.

Rollup von VI-status zu Korrekturaufgaben (VUL)

Statusvorrang: Offen > Geschlossen – behoben > Geschlossen – Veraltet.

1. Wenn VIS in einer ANGREIFBAREN Aufgabe (Korrekturaufgabe) „Offen“ sind, wird der Status „UNGÜLTIG“ nicht geändert.
2. Wenn mindestens ein VI „Geschlossen – behoben“ ist und der Rest „Geschlossen – Veraltet“ ist, wechselt der Status „ANFECHTEN“ in „Geschlossen – behoben“.
3. Wenn alle VIS in einer ANFECHTUNG geschlossen – Veraltet sind, wechselt der Status „ANFECHTUNG“ in „Geschlossen – Abgebrochen“.
4. Wenn ein VIS als „Geschlossen – falsch positiv“ geschlossen wird, wird der WIDERRUF nicht automatisch geschlossen.

Weitere Informationen zu Status-Rollup- und Rolldown-Szenarien finden Sie unter . Status-Rollup- und Rollup-Szenarien.

Erkennungen und Integrationsanforderungen von Drittparteien automatisch schließen

Microsoft TVM-Anwender und Erkennung veralteter Elemente automatisch schließen

Prüflistenelement	Beschreibung
Die Microsoft TVM-Schwachstellenintegration	Mit der Microsoft TVM Vulnerability Integration, wenn Sie auswählen **Zuletzt gefundene Erkennungen** Um Ihre Suche auf zu basieren, erfordert diese Funktion eine erfolgreiche Ausführung der Microsoft TVM Machine Vulnerabilities Integration (vollständiger Import) innerhalb der letzten sieben Tage. Diese Integration wird wöchentlich ausgeführt. Wenn das automatische Schließen veralteter Erkennungen aktiviert und für konfiguriert sind **Zuletzt gefundene Erkennungen** , Und die Microsoft TVM-Computer-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüflistenelement	Beschreibung
	Schwachstellen-Integration deaktiviert ist oder ein Datenimport innerhalb der letzten sieben Tage nicht erfolgreich abgeschlossen wurde, wird die geplante Aufgabe zum Schließen von Erkennungen weiterhin täglich ausgeführt, einige veraltete Erkennungen werden jedoch möglicherweise nicht wie erwartet geschlossen. Wenn Sie auswählen **Zuletzt gescannte Assets** Um Ihre Suche auf zu basieren, ist die Ausführung der Integration von Microsoft TVM-Rechnerschwachstellen nicht erforderlich. So aktivieren Sie diese Integration: **1.** Navigieren zu **Microsoft TVM-Schwachstellenintegration** > **Administration** > **Integration**an. **2.** Suchen und aktivieren Sie **Integration von Microsoft TVM-Computer-Schwachstellen (vollständiger Import)** .
(Optional) Stellen Sie mehrere Instanzen der Microsoft TVM-Integrationen in Ihrer Umgebung bereit.	Sie können optional mehrere Instanzen der Integrationen in Ihrer Umgebung bereitstellen. Das automatische Schließen veralteter Erkennungen ist nicht instanzspezifisch und in Ihrer Umgebung entweder aktiviert oder deaktiviert. Veraltete Erkennungen werden in Instanzen, die erfolgreich abgeschlossen wurden, automatisch in „Veraltet“ überführt. Wenn das automatische Schließen veralteter Erkennungen aktiviert ist und Sie die Integrationen deaktivieren, die wöchentlich in einer Instanz ausgeführt werden, wird die geplante Aufgabe zum Schließen von Erkennungen weiterhin täglich ausgeführt, einige Erkennungen werden jedoch möglicherweise nicht wie erwartet automatisch in Veraltet übergehen.

Qualys Anwender und veraltete angreifbare Elemente automatisch schließen

- Beliebig aktiviert Qualys Drittpartei-Integrationen, die Erkennungsdaten abrufen, können mit diesem Modul ausgeführt werden. Es gibt keine spezifischen Qualys Anwendungen erforderlich.
- Sie können optional mehrere Instanzen von bereitstellen Qualys Integrationen in Ihrer Umgebung.
- Das automatische Schließen veralteter Erkennungen ist nicht instanzspezifisch und in Ihrer Umgebung entweder aktiviert oder deaktiviert. Veraltete Erkennungen werden in allen Instanzen automatisch in veraltet überführt.

Rapid7 Anwender und veraltete Erkennungen automatisch schließen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüflistenelement	Beschreibung
Die Rapid7 Schwachstellenintegration	Wenn Sie auswählen **Zuletzt gefundene Erkennungen** Um Ihre Suche auf zu basieren, erfordert diese Funktion die erfolgreiche Ausführung eines der Rapid7 Umfassende Integrationen angreifbarer Elemente innerhalb der letzten sieben Tage. Diese umfassenden Integrationen werden wöchentlich ausgeführt: • Für Rapid7 Nexpose Data Warehouse, eine erfolgreiche Ausführung aus dem Rapid7 Umfassende Integration angreifbarer Elemente ist erforderlich. • Für Rapid7 InsightVM, Eine erfolgreiche Ausführung von Rapid7 Umfassende Integration angreifbarer Elemente – API ist erforderlich. Wenn das automatische Schließen veralteter Erkennungen aktiviert und für konfiguriert ist **Zuletzt gefundene Erkennungen** , Und Rapid7 Umfassende Integrationen angreifbarer Elemente sind deaktiviert, oder ein Datenimport wurde innerhalb der letzten sieben Tage nicht erfolgreich abgeschlossen. Die geplante Aufgabe zum Schließen von Erkennungen wird weiterhin täglich ausgeführt, einige veraltete Erkennungen werden jedoch möglicherweise nicht wie erwartet geschlossen. Wenn Sie auswählen **Zuletzt gescannte Assets** Um Ihre Suche auf zu basieren, keine umfassende Rapid7 Integrationsausführung ist erforderlich. So aktivieren Sie diese Integrationen: **1.** Navigieren zu **Rapid7 Vulnerability-Integration** > **Administration** > **Integration**an. **2.** Suchen und aktivieren Sie Rapid7 Umfassende Integration angreifbarer Elemente, die Sie benötigen. **Hinweis:** Zusätzlich zu diesen Integrationen, die wöchentlich ausgeführt werden, Rapid7 Nexpose Und Rapid7 InsightVM Jedes hat VI-Integrationen, die täglich ausgeführt werden, die Rapid7-Integration für angreifbare Elemente und die Rapid7-Integration für angreifbare Elemente – API. Wenn sowohl täglich als auch wöchentlich Rapid7 Integrationen sind aktiviert, es wird jeweils nur eine Integration ausgeführt. Wenn einer dieser Integrationsaufträge ausgeführt wird, wird der Auftrag für die andere Integration bis zur nächsten geplanten Aufgabe übersprungen.
(Optional) Stellen Sie mehrere Instanzen von bereit Rapid7 Integrationen in Ihrer Umgebung.	Sie können optional mehrere Instanzen der umfassenden Integrationen in Ihrer Umgebung bereitstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüflistenelement	Beschreibung
	Das automatische Schließen veralteter Erkennungen ist nicht instanzspezifisch und in Ihrer Umgebung entweder aktiviert oder deaktiviert. Veraltete Erkennungen werden in Instanzen, die erfolgreich abgeschlossen wurden, automatisch in „Veraltet“ überführt. Wenn das automatische Schließen veralteter Erkennungen aktiviert ist und Sie die Integrationen deaktivieren, die wöchentlich in einer Instanz ausgeführt werden, wird die geplante Aufgabe zum Schließen von Erkennungen weiterhin täglich ausgeführt, einige Erkennungen werden jedoch möglicherweise nicht wie erwartet automatisch in Veraltet übergehen.

Tenable-Schwachstellenintegrationsanwender und veraltete angreifbare Elemente automatisch schließen

- Alle aktivierten Integrationen aus der Tenable-Schwachstellenintegration, die Erkennungsdaten abrufen, können mit diesem Modul ausgeführt werden. Es sind keine spezifischen Tenable-Schwachstellenintegrationen erforderlich.
- Sie können optional mehrere Instanzen der Tenable-Schwachstellenintegration in Ihrer Umgebung bereitstellen.
- Das automatische Schließen veralteter Erkennungen ist nicht instanzspezifisch und in Ihrer Umgebung entweder aktiviert oder deaktiviert. Veraltete Erkennungen werden automatisch zu übergehen **Veraltet** Auf allen Instanzen.

Nachdem Sie überprüft haben, ob Ihre Integrationen ordnungsgemäß konfiguriert sind, finden Sie unter Veraltete Erkennungen in automatisch schließen Vulnerability Response Zum Aktivieren der Funktion.

Aktualisieren Sie Informationen von „veraltete angreifbare Elemente automatisch schließen“ auf „veraltete Erkennungen automatisch schließen“

Wenn Sie für das Modul „veraltete Erkennungen automatisch schließen“ zuvor veraltete angreifbare Elemente automatisch schließen verwendet haben:

- Der Wert für die Anzahl der Tage, die Sie für eingegeben haben **Zuletzt gescannte Assets** Die Option „veraltete angreifbare Elemente automatisch schließen“ wird automatisch für beibehalten **Zuletzt gescannte Assets** In „veraltete Erkennungen automatisch schließen“.
- Der Wert für die Anzahl der Tage, die Sie für eingegeben haben **Zuletzt gefundene angreifbare Elemente** Die Option „veraltete angreifbare Elemente automatisch schließen“ wird automatisch für beibehalten **Zuletzt gefundene Erkennungen** In „veraltete Erkennungen automatisch schließen“.
- Vorhandene offene Erkennungen mit angreifbaren Elementen als „Geschlossen – Veraltet“ werden gemäß den Konfigurationseinstellungen für das automatische Schließen in „Veraltet“ geändert, wenn *`Auto-Close Stale Detections`*Die geplante Aufgabe wird nach dem Upgrade ausgeführt.

Rollup-Informationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn ein angreifbares Element vor dem Upgrade als veraltet geschlossen wurde und alle seine Erkennungen nach dem Upgrade als veraltet markiert sind, bleibt der VI-Status „Geschlossen – Veraltet“.
- Wenn ein angreifbares Element vor dem Upgrade als veraltet geschlossen wurde und nur einige seiner Erkennungen nach dem Upgrade als veraltet markiert sind und der Rest vom Scanner geschlossen wurde, wechselt das angreifbare Element gemäß der Rollup-Logik zu Geschlossen – behoben.

Veraltete Erkennungen in automatisch schließen Vulnerability Response

Aktivieren Sie das automatische Schließen veralteter Erkennungen, um veraltete angreifbare Erkennungen automatisch zu schließen, die kürzlich von Ihren Drittanbieterintegrationen nicht gefunden wurden.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vuln.admin (veraltet) oder ein Schwachstellenmanager mit der granularen Rolle sn_vul.manage_Auto_close_stale_VI.

Weitere Informationen zu dieser Funktion, wichtigen Begriffen und allen Setups, die möglicherweise für Ihre Drittanbieterintegrationen erforderlich sind, die Erkennungsdaten importieren, finden Sie unter Veraltete Erkennungen in werden geschlossen Vulnerability Response Weitere Informationen finden Sie unter .

Hinweis:
Die im folgenden Verfahren bereitgestellten Informationen gelten nur für Versionen vor v22.0 von Vulnerability Response. Ab v22.0 von Vulnerability Response, Sie haben die Möglichkeit, zusätzliche Suchoptionen zu konfigurieren. Weitere Informationen finden Sie unter Erstellen Sie Regeln für das automatische Schließen.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Administration** > **Konfiguration für automatisches Schließen** > **Veraltete Erkennungen**an.
   Das Formular „veraltete Konfiguration automatisch schließen“ wird angezeigt.
2. Füllen Sie die Felder aus.
3. Für **Veraltete Erkennungen basierend auf automatisch schließen** Wählen Sie eine Option für Ihre Suche aus.

   Beide Suchen entsprechen dem Alter älterer, veralteter Erkennungen in Tagen zu einem von Ihrem Scanner angegebenen Datum.

   Hinweis:
   Beginnend mit v22.0 von Vulnerability Response, Die Optionen **Zuletzt gefundene Erkennungen** Und **Zuletzt gescannte Assets** Werden als Liste erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Zuletzt gefundene Erkennungen** . Diese Option sucht nach dem aktuellsten oder neuesten Datum, an dem Erkennungen vom Scanner erneut gefunden wurden.

  Hinweis:
  Für Rapid7 Und Microsoft TVM-Anwender wird eine Warnmeldung angezeigt, dass aktuelle Erkennungsinformationen erforderlich sind.

  Wenn Sie auswählen **Zuletzt gefundene Erkennungen** Um Ihre Suche auf zu basieren, erfordert diese Funktion eine erfolgreiche Integrationsausführung von einem der Rapid7 Umfassende Integrationen angreifbarer Elemente innerhalb der letzten sieben Tage.

  Wenn Sie auswählen **Zuletzt gefundene Erkennungen** Damit Ihre Suche auf basiert, erfordert diese Funktion eine erfolgreiche Integrationsausführung der Microsoft TVM-Computer-Schwachstellen-Integration (vollständiger Import) innerhalb der letzten sieben Tage.

- **Zuletzt gescannte Assets** . Diese Option sucht nach dem aktuellen Datum, an dem ein Asset zuletzt von einem Scanner einer Drittpartei gescannt wurde.

4. Für Rapid7 Und Microsoft Nur TVM-Anwender. Überprüfen Sie, ob alle erforderlichen Integrationen aktiviert sind.
   Siehe Rapid7 Vulnerability-Integration verstehen und Verständnis der Integration von Microsoft Threat and Vulnerability Management Vulnerability, um weitere Informationen zu erhalten.
5. Um das Modul zu aktivieren, klicken Sie auf das Kontrollkästchen aktiv, um es auszuwählen.
6. In **Zuletzt gefundene Erkennungen (vor Tagen)** Geben Sie das Alter älterer, veralteter Erkennungen in der Anzahl der Tage ein.

   Der Standardwert ist 90 Tage. Sie können einen beliebigen positiven Wert für die Anzahl der Tage eingeben. Dieser Wert wird verwendet, um einem von Ihrem Scanner bereitgestellten Datum zu entsprechen. Mit 90 und **Zuletzt gefundene Erkennungen** Angezeigt werden alle Erkennungen, die in den letzten 90 Tagen nicht gefunden wurden, automatisch geschlossen. Mit 90 und **Zuletzt gescannte Assets** Angezeigt werden alle Erkennungen, die Assets zugeordnet sind, die in den letzten 90 Tagen nicht gescannt wurden, automatisch geschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Es besteht eine Beziehung zwischen **Zuletzt gefundene Erkennungen/zuletzt gescannte Assets (vor Tagen)** Feld für diese Funktion und den **Importieren seit** Feld in der Rapid7 Comprehensive Angreifbare Item Integration – API und der Microsoft TVM Machine Vulnerabilities Integration.

Für diese Integrationen **Importieren seit** Das Feld auf den Konfigurationsseiten ist standardmäßig leer.

Wenn Sie keinen Wert eingeben oder das Feld keinen Wert hat, werden die Daten für die Anzahl der in konfigurierten Tage angezeigt **Zuletzt gefundene Erkennungen/ zuletzt gescannte Assets (vor Tagen)** Feld wird verwendet.

Beispiel: Die Anzahl der Tage, die im Konfigurationsformular für das automatische Schließen definiert sind `90`, Und **Importieren seit** Das Feld ist auf den Integrationskonfigurationsseiten leer, dann importiert die erste Integrationsausführung die Daten der letzten 90 Tage. Die **Importieren seit** Felder für Rapid7 Umfassende Integration angreifbarer Elemente – API und die Integration von Microsoft TVM-Computer-Schwachstellen können bearbeitet werden, sodass Sie auch beliebige Werte angeben können. Der Wert für 90 Tage wird als Standard bereitgestellt, wenn das Feld leer bleibt, damit die Funktion zum automatischen Schließen die falsch positiven Ergebnisse nicht schließt.

Diese Beziehung zwischen diesen Feldern gilt nur für die erste Integrationsausführung. Ändern Sie danach **Zuletzt gefundene Erkennungen/ zuletzt gescannte Assets (vor Tagen)** Das Feld im Formular „veraltete angreifbare Erkennungen automatisch schließen“ wirkt sich nicht auf aus **Importieren seit** Feld auf den Integrationskonfigurationsseiten. Das Feld wird in die Startzeit der ersten Ausführung geändert, sodass bei der nachfolgenden Integration nur die Delta-Informationen importiert werden.

7. **Wahlweise:** Wählen Sie aus **Veraltete Erkennungen für zurückgestellte VIS ignorieren** Kontrollkästchen zum Ignorieren veralteter Erkennungen, die zurückgestellten VIS oder VIS zugeordnet sind, die derzeit für die Zurückstellung überprüft werden.

   (Optional) Wenn Sie diese Option deaktiviert lassen, werden alle Erkennungen, die Ihren Kriterien entsprechen, geschlossen, die zurückgestellten VIS zugeordnet sind, oder VIS, die zur Zurückstellung überprüft werden. Die zurückgestellten VIS oder VIS, die überprüft werden und diesen Erkennungen entsprechen, werden ebenfalls basierend auf der Rollup-Logik automatisch geschlossen. Weitere Informationen zur Rollup-Logik finden Sie unter Veraltete Erkennungen in werden geschlossen Vulnerability Response Und Status-Rollup- und Rollup-Szenarien.

   Wenn Sie diese Option aktivieren, werden alle Erkennungen, die Ihren Kriterien entsprechen, die zurückgestellten VIS oder VIS zugeordnet sind, die für eine Zurückstellung überprüft werden, beim automatischen Schließen übersprungen.

8. **Wahlweise:** Deaktivieren Sie **Veraltete Erkennungen für geschlossene VIS ignorieren** Kontrollkästchen.

   (Optional) Standardmäßig ist dieses Kontrollkästchen aktiviert, damit das geschlossene VI nicht erneut geöffnet wird, wenn eine neue Erkennung im Zusammenhang mit diesem geschlossenen VI identifiziert wird. Weitere Informationen zur Rollup-Logik finden Sie unter Veraltete Erkennungen in werden geschlossen Vulnerability Response Und Status-Rollup- und Rollup-Szenarien.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

   Die regelmäßige *Auto-Close Stale Detections*-Aufgabe wird täglich ausgeführt. Der Auftrag bestimmt, ob Sie das Datum ausgewählt haben, an dem Erkennungen zuletzt gefunden wurden, oder das Datum, an dem Assets zuletzt gescannt wurden. Anschließend werden die entsprechenden Erkennungen in den Status „Veraltet“ versetzt. Es ist wichtig zu beachten, dass die Funktion „Veraltete Erkennung automatisch schließen“ nur veraltete Erkennungen für aktive Integrationsinstanzen schließt. Angreifbare Elemente und Erkennungen, die aktiven Integrationsinstanzen zugeordnet sind, werden geschlossen. Ab v22.0 von Vulnerability Response Die geplante Aufgabe wurde geändert, um die allgemeine Tabelle [sn_vul_cmn_Auto_close_rule] zu berücksichtigen.

   Nachdem die Erkennungen als veraltet markiert wurden und der Scanner meldet, dass diese Erkennung erneut gefunden wird, wechselt das Feld Status der Erkennungen in Offen. Die entsprechenden angreifbaren Elemente der Erkennung werden ebenfalls erneut geöffnet.

   Wenn die Erkennung als veraltet markiert ist und der Scanner feststellt, dass sie behoben ist, wechselt die Erkennung außerdem zu Geschlossen. Für den Status wird auch ein Rollup zu den VIS durchgeführt.

Erstellen Sie Regeln für das automatische Schließen

Verwenden Sie Regeln zum automatischen Schließen, um ältere Erkennungen basierend auf den von Ihnen festgelegten Filterbedingungen automatisch zu schließen.

Vorbereitungen

Erforderliche Rolle: sn_vul.manage_Auto_close_stale_VI

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Regeln für automatisches Schließen**an.

   Das Basissystem bietet die folgenden Regeln für das automatische Schließen:

   - **Zuletzt gescannte Assets** : Erkennungen, die Assets zugeordnet sind, die in den letzten 90 Tagen nicht gescannt wurden, werden auf übertragen **Veraltet** status.
   - **Zuletzt gefundene manuelle Erkennungen** : Manuelle Erkennungen, die in den letzten 90 Tagen nicht gefunden wurden. Wenn Sie aktivieren **Zuletzt gefundene Erkennungen** Datensatz, dann erfordert diese Funktion eine erfolgreiche Integrationsausführung von Rapid7 Umfassende Integrationen angreifbarer Elemente und Integration von Microsoft TVM-Rechnerschwachstellen (vollständiger Import) innerhalb der letzten sieben Tage.
   - **Zuletzt gefundene Erkennungen** : Erkennungen, die in den letzten 90 Tagen nicht gefunden wurden.

2. Wählen Sie Aus **Neu** Dient zum Erstellen einer neuen Regel zum automatischen Schließen.

3. Füllen Sie die Felder des Formulars aus.

Feld	Wert
Name	Name der Regel zum automatischen Schließen.
Aktiv	Option zum Aktivieren der Regel. Wenn diese Option aktiviert ist, werden alle Erkennungen, die den Filterkriterien entsprechen, automatisch geschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Zurückgestellte Elemente ignorieren	Wenn diese Option ausgewählt ist, werden alle Erkennungen angezeigt, die dem zugeordnet sind **Wird überprüft** Oder **Zurückgestellt** status werden ignoriert und nicht geschlossen. Wenn Sie diese Option deaktivieren, werden alle Erkennungen geschlossen, die Ihren Kriterien entsprechen.
Ausführungsreihenfolge	Eindeutiger Wert für die Ausführung der Regel zum automatischen Schließen. Dieser Wert bestimmt die Reihenfolge der Ausführung. Der Standardwert ist 100.
Beschreibung	Beschreibung der Regel zum automatischen Schließen.
Bedingung	Filterbedingungen, die verwendet werden, um Erkennungen zu identifizieren, die geschlossen werden sollen.

4. Wählen Sie **Absenden**.

Die regelmäßige *`Auto-Close Stale Detections`*-Aufgabe wird täglich ausgeführt. Identifiziert Erkennungen basierend auf den angegebenen Bedingungen und überträgt die übereinstimmenden zu **Veraltet** status. Der Auftrag verarbeitet die folgenden Szenarien:

- Wenn alle Erkennungen in einem angreifbaren Element (VIT) als veraltet markiert sind, wird die VIT geschlossen, wobei der Substatus auf „Veraltet“ festgelegt ist.
- Wenn mindestens eine Erkennung innerhalb einer VIT offen bleibt, während sich andere im Status „Veraltet“ befinden, bleibt die VIT offen.
- In Fällen, in denen Erkennungen mit dem Status „Geschlossen“ und „Veraltet“ innerhalb einer VIT vorhanden sind, wird die VIT mit dem Substatus „behoben“ geschlossen.

Wenn Sie ein Upgrade auf die neueste Version von durchführen Vulnerability Response, Die in Ihren Regeln für das automatische Schließen festgelegten Bedingungen werden ebenfalls entsprechend aktualisiert. Wenn die Regeln außerdem verschiedenen Domänen zugeordnet sind, werden die Regeln speziell innerhalb dieser Domänen erstellt.

Klassifizieren Sie nicht klassifizierte Hardware erneut

Klassifizieren Sie nicht klassifizierte Hardware neu, indem Sie die CI-Suchregeln aktualisieren.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Warum und wann dieser Vorgang ausgeführt wird

Die Tabelle „Host-Importzuordnung“ [sn_sec_cmn_src_cmdb_Map] zeigt die eingehenden Variablen der Nutzlast und die entsprechenden Zuweisungen in der Tabelle „erkannte Elemente“ an. Gelegentlich können Diskrepanzen bei Benennungskonventionen zwischen Scanner und Discovery dazu führen, dass die Hardware nicht klassifiziert wird. Stellen Sie beim Erstellen eines neuen nicht klassifizierten Hardware-CI sicher, dass der Name in der Nutzlast nur den Hostnamen enthält. Wenn Discovery das Asset später identifiziert, kann es in die entsprechende CI-Klasse neu klassifiziert werden. Bei Bedarf kann ein Skript geschrieben werden, um einen abgeleiteten Wert zu generieren, der sowohl in Discovery als auch in Configuration Management Database (CMDB) mit dem CIs-Namen übereinstimmt.

Wenn die Identification and Reconciliation Engine (IRE) aktiviert ist, wird die Option „Neu klassifizieren“ aus erkannten Elementen nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zur Tabelle Host-Importzuordnungen [sn_sec_cmn_src_cmdb_Map].
2. Wählen Sie eine Quelle aus.
3. Wählen Sie in der Liste Zielfeld die Option aus **Name** .
   Die **Skript verwenden** Das Kontrollkästchen wird sichtbar.

   Hinweis:
   - Das Skript ist nur verfügbar, wenn **Name** Ist aus der Liste „Zielfeld“ ausgewählt.
   - Um ein Skript für andere Optionen in der Liste „Zielfeld“ hinzuzufügen, müssen Sie die UI-Richtlinie deaktivieren, indem Sie:
     - „Skript verwenden auf „falsch“ festlegen“ wird deaktiviert.
     - Deaktivieren von „Skript verwenden anzeigen oder ausblenden“.
     - Die Bedingung „Zielfeld ist Name“ wird in der „Skriptrichtlinie anzeigen oder ausblenden“ entfernt.
   - Die Tabelle „Host-Importzuordnungen“ wird mit zwei neuen Spalten aktualisiert: Skript und Skript verwenden.

4. Wählen Sie aus **Skript verwenden** Kontrollkästchen.
   Die **Skript** Das Feld zeigt das Standardskript an, Sie haben jedoch die Möglichkeit, ein anwenderdefiniertes Skript zu erstellen. In diesem Feld können Sie die Quell- und abgeleiteten Werte angeben, die an der Benennungskonvention der Datenbank ausgerichtet werden sollen. Der vom Skript generierte Wert wird in sourcePayload['DERIVED'][rule.Source_field] gespeichert. Stellen Sie sicher, dass die CI-Suchregeln so angepasst sind, dass Quellnutzlast, abgeleitete und Zielattribute verwendet werden, wenn Sie die entsprechenden Tabellen einchecken.
5. Um das Skript auf ältere doppelte Datensätze anzuwenden, gehen Sie wie folgt vor:
   a. Navigieren zu **Alle** > **Vulnerability Response** > **Erkannte Elemente**an.
   b. Wählen Sie die doppelten Datensätze aus.
   c. Wählen Sie in der Liste Aktion für ausgewählte Zeilen die Option aus **Wenden Sie die CI-Suchregeln erneut an** .
      Zeigt eine Übereinstimmung mit einem vorhandenen Asset an.
6. Um das Skript für anzuwenden Tenable.io, Gehen Sie wie folgt vor:
   a. Navigieren zu **Vulnerability Response Host-Importzuordnungen** .
   b. Wählen Sie das Skript für die Zeile mit NetBIOS, HOSTNAMEN und FQDNS-Namen als aus **Quelle** Feld.
   c. Aktualisieren Sie das Skript für jedes Element.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Für Tenable.io, Gibt der Scanner ein Array für NetBIOS, HOSTNAMEN und FQDNS-Namen zurück, für die das Skript nicht wie erwartet funktioniert.

Da die Host-Importzuordnung für Tenable.io Enthält **netbios_Name** In **Quelle** Feld müssen Sie ein Skript schreiben. Während der Suche ein anderes Quellfeld **NETBIOS** Wird verwendet, das ein Array von Werten aufweist. Daher wird der Tabelle eine neue Zeile hinzugefügt, und dieselbe Logik muss in einer Schleife im Skript geschrieben werden. Gleichermaßen für **FQDNS** Und **HOSTNAMEN** .

7. Um das Skript für anzuwenden Rapid7, Gehen Sie wie folgt vor:
   a. Navigieren zu **Alle** > **Vulnerability Response Host-Importzuordnungen** .
   b. Für Rapid7 Zeilen mit FQDN und Hostname aktualisieren Sie die Suchmethode auf Skript.

Hinweis:
Für Rapid7, Die CI-Suchmethode ist auf Feldübereinstimmung für FQDN und Hostname festgelegt, was verhindert, dass das Skript verwendet wird.

Erstellen Sie manuell eine Korrekturaufgabe in Vulnerability Response

Das manuelle Erstellen einer Korrekturaufgabe erfolgt, wenn Sie angreifbare Elemente nach etwas anderem als den Regelkriterien für Korrekturaufgaben gruppieren möchten. Sie können beispielsweise Aufgaben für einen bestimmten Manager oder für aktive neue Exploits wie Ransomware erstellen, die verschiedene Schwachstellen enthalten. Sie können sie auch verwenden, um nicht gruppierte angreifbare Elemente zu gruppieren.

Wichtig:
Sie können Host-Korrekturaufgaben in erstellen:

- Arbeitsbereich des Schwachstellenmanagers Als Anwender mit sn_vul.Vulnerability_Analyst, Oder Rolle sn_vul.Vulnerability_admin.
- Arbeitsbereich für IT-Korrekturen Als Anwender mit der Rolle „sn_vul.Remediation_owner“.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_Analyst, sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**an.

   Regeln für Korrekturaufgaben funktionieren genauso wie Regeln für Korrekturaufgaben, die zuvor gearbeitet wurden, und stehen Ihnen weiterhin zur Verfügung. Sie können jedoch die Regeln für Korrekturaufgaben inaktiv lassen, da Sie sich an die Funktionen gewöhnen, die Ihren Sicherheitsmanagern und IT-Teams in den Arbeitsbereichen zur Verfügung stehen.

2. Wählen Sie eine der Kategorien für Aufgaben aus, um die Liste zu öffnen.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.
   Informationen zu bestimmten Feldern finden Sie unter Formularfelder für Korrekturaufgabe.
5. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Aufgabe erstellt wird, verwenden Sie **Bedingung** Oder **Filtergruppe** Filtertyp **Angreifbares Element** Die zugehörige Liste sucht nach allen übereinstimmenden angreifbaren Elementen und zeigt sie an.

Sie können den zugehörigen Link verwenden, **Überprüfen Sie erneut auf Schwachstellen** Dient zum manuellen Auslösen eines ServiceNow®– Scan initiiert. Informationen zum Konfigurieren eines Schwachstellen-Scanners finden Sie unter Konfigurieren und verwalten Qualys Schwachstellen-Scanner und -Scans.

Für eine Qualys Vulnerability Integration ist im ein Standardscanner vorinstalliert **Schwachstellen-Scanner** Modul. Dieser Scanner ist standardmäßig deaktiviert. Wählen Sie aus **Aktiv** Und **Standard** Kontrollkästchen zum Aktivieren des Qualys-Scanners für die Verwendung von **Suchen Sie nach Schwachstellen** Zugehöriger Link in den Formularen „Korrekturaufgabe“ und „angreifbare Elemente“.

Die **Status aktualisieren** Der zugehörige Link zeigt Datum und Uhrzeit der letzten Aktualisierung an. Es werden Informationen aus den VIS in der Korrekturaufgabe zusammengefasst. Weitere Informationen finden Sie unter Formularfelder für Korrekturaufgabe. Wenn eine Aufgabe basierend auf einer bestimmten Schwachstelle erstellt wird, wird diese Schwachstelle im Formular „Korrekturaufgabe“ aufgeführt.

Wenn Sie ein zugehöriges angreifbares Element öffnen, werden alle zugehörigen Korrekturaufgabeneinträge unter angezeigt **Korrekturaufgabe** Registerkarte „zugehörige Liste“.

Fügen Sie der Vulnerability Response-Gruppe Anwender hinzu

Wenn die Funktion „Schließen/Zurückstellen“ verwendet wird, um ein angreifbares Element zurückzustellen oder zu schließen, ohne dass ein Scan erforderlich ist, wird die verwendet Vulnerability Response Die Gruppe wird benachrichtigt, die Anforderung zu genehmigen oder abzulehnen. Sie können die entsprechenden Anwender zuweisen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**an.
2. Öffnen Sie Vulnerability Response Gruppe.
3. Klicken Sie auf **Gruppenmitglieder** Zugehörige Liste, und klicken Sie auf **Bearbeiten** .
4. Wählen Sie einen oder mehrere Namen in aus **Sammlung** Liste.
5. Klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **Speichern**.

Zugehörige Informationen

Einen Benutzer erstellen

Verwalten Sie einzelne angreifbare Elemente manuell

Angreifbare Elemente stellen ein Konfigurationselement (Configuration Item, CI) mit einer bestimmten Schwachstelle dar. Angreifbare Elemente werden aus Drittparteiquellen importiert oder mithilfe der SAM-NVD-Informationen (Link) Schwachstelleneinträge mit Softwaredatensätzen verglichen, die aus der Software abgerufen wurden Asset-Management Modul.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angreifbare Elemente sind in Korrekturaufgaben enthalten, die durch Schwachstellenregeln definiert sind. Normalerweise sind Korrekturaufgaben der Ort, an dem Gruppen angreifbarer Elemente zugewiesen und bearbeitet werden.

Angreifbare Elemente können in der Massenaktion angezeigt und bearbeitet werden **Angreifbare Elemente** Modul. Datensätze für angreifbare Elemente zeigen Informationen von der Schwachstelle in an **Schwachstelle** Registerkarte. Diese Registerkarte kann angeben, ob öffentliche oder aktive Exploits dafür vorhanden sind. Außerdem wird angezeigt, ob sie durch einen Patch, eine Konfigurationsänderung oder eine Kombination aus beiden behoben werden kann. Wenn IP-Adressen während der Deduplizierung gefunden werden, werden sie in einer zugehörigen Liste angezeigt.

Wenn ein CI aus der CMDB entfernt wird, werden auch alle zugehörigen angreifbaren Elemente entfernt.

Wenn einer Korrekturaufgabe ein angreifbares Element hinzugefügt wird, wird die Gruppe in angezeigt **Korrekturaufgaben** Liste der angreifbaren Elemente.

Wenn eine Aufgabe erstellt wird, die sich auf ein angreifbares Element auswirkt, wird die Aufgabe in angezeigt **Betrifft Aufgaben** Zugehörige Liste der angreifbaren Elemente.

Angreifbare Elemente können manuell erstellt werden. Sie können Security Incidents oder Change-Anforderungen erstellen und manuell schließen oder zurückstellen. Regeln für Korrekturaufgaben können auf manuell erstellte angreifbare Elemente angewendet werden.

Korrekturaufgaben und Regeln für Korrekturaufgaben wurden erweitert, um die Aufgabenfunktionalität zu übernehmen. Angreifbare Elemente können nicht als übergeordnete Aufgabe verknüpft werden.

Erstellen Vulnerability Response Angreifbare Elemente

Mehrere Methoden erstellen angreifbare Elemente (VI). In der Regel wird eine Integration in einen Schwachstellen-Scanner installiert und so konfiguriert, dass Ergebnisse jeden Abend importiert werden. Es gibt Fälle, z. B. physische Sicherheitsschwachstellen, in denen Sie angreifbare Elementdatensätze manuell hinzufügen möchten.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_write

Warum und wann dieser Vorgang ausgeführt wird

VIS, die Sie manuell erstellen, und automatisch erstellte VIS werden durch Regeln für Korrekturaufgaben und Gruppenbedingungen automatisch hinzugefügt und aus Korrekturaufgaben entfernt.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**an.
2. Wählen Sie eine Kategorie aus, um die Liste zu öffnen.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.
   Informationen zu den Feldern für angreifbare Elemente finden Sie unter . Vulnerability Response Formularfelder für angreifbare Elemente.
5. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.

   Die Regeln für Korrekturaufgaben bewerten das angreifbare Element und fügen es einer vorhandenen Aufgabe hinzu, oder erstellen eine neue Aufgabe. Wenn die Auswertung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

fehlschlägt, wird das angreifbare Element zu hinzugefügt **Nicht Gruppierte Angreifbare Elemente** Liste.

Wenn Sie ein neues angreifbares Element speichern, alle Rechner aktiviert Ausführen.

Hinweis:
Nur ein Rechner pro **Zielfeld** Darf gleichzeitig aktiv sein. Wenn Sie eine aktivieren, werden alle anderen mit derselben Option aktiviert **Zielfeld** Sind deaktiviert.

6. Sie können auf eine der zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

Sie können den zugehörigen Link verwenden, **Suchen Sie nach Schwachstellen** Dient zum manuellen Auslösen eines ServiceNow®– Scan initiiert. Informationen zum Konfigurieren eines Schwachstellen-Scanners finden Sie unter Konfigurieren und verwalten Qualys Schwachstellen-Scanner und -Scans.

Für eine Qualys Vulnerability Integration ist im ein Standardscanner vorinstalliert **Schwachstellen-Scanner** Modul. Dieser Scanner ist standardmäßig deaktiviert. Wählen Sie aus **Aktiv** Und **Standard** Kontrollkästchen zum Aktivieren des Qualys-Scanners für die Verwendung von **Suchen Sie nach Schwachstellen** Zugehöriger Link in den Formularen „Korrekturaufgabe“ und „angreifbare Elemente“.

Die folgenden Bearbeitungs- und Korrekturoptionen werden über die Header-Leiste verfügbar:

- Update: Speichert Aktualisierungen im Formular.
- Security Incident erstellen: Erstellt einen Security Incident.
- Schließen: Schließt das Element. Wenn alle Elemente in ihrer Gruppe geschlossen sind, wird die Korrekturaufgabe automatisch geschlossen.
- Ausnahme anfordern: Sendet eine Anforderung zum Zurückstellen eines Elements.
- Lösen: Löst das Element auf.
- Löschen: Entfernt das angreifbare Element.

Zugehörige Informationen

Bearbeiten Sie angreifbare Elemente in Massenarbeit Vulnerability Response

Ein angreifbares Element zurückstellen

Wenn Sie feststellen, dass das Problem, das einem angreifbaren Element (VIT) zugeordnet ist, ein geringes Risiko aufweist und sofort ohne weitere Analyse zurückgestellt werden kann, können Sie verwenden **Zurückstellen** Funktion.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Eine geplante Aufgabe wird jeden Tag ausgeführt, um nach zurückgestellten angreifbaren Elementen zu suchen, die ihr Wiedereröffnungsdatum erreicht haben. An dem Tag, an dem die Zurückstellung des VI abläuft, wird der Datensatz erneut geöffnet.

Beginnend mit Vulnerability Response V20.0, bevor ein zurückgestelltes VI erneut geöffnet wird Überprüfen Sie den Ablauf der Zurückstellung für angreifbare Elemente und Gruppen Die geplante Aufgabe überprüft, ob eine Ausnahmeregel für ein zurückgestelltes VI gilt, und aktualisiert den **Grund** Und **Bis** Felder gemäß der Ausnahmeregel. Der Status des VI bleibt bis zum letzten Ablaufdatum zurückgestellt.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**an.
2. Öffnen Sie ein angreifbares Element.
3. Klicken Sie Auf **Ausnahme Anfordern** .
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Bis	Wählen Sie das Datum aus, an dem der Status zurückgestellt abläuft und die Korrekturaufgabe erneut aktiviert wird. **Hinweis:** Ab Version 18,0 von Vulnerability Response(VR): Wenn ein zurückgestelltes angreifbares Element vor Ablauf des Ausnahmefensters von einem Scanner geschlossen und erneut geöffnet wird, wird der Status der VIT in den zurückgestellten Status zurückgesetzt, wobei das aktive Ausnahmefenster berücksichtigt wird. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft sn_vul.auto_defer_vit_in_active_exception_window auf „wahr“ fest. Außerdem wird das Datum „Zurückgestellt bis“ auch dann beibehalten, wenn das angreifbare Element geschlossen wurde oder die Ausnahme abläuft. Die erforderliche Rolle ist „sn_vul.Manage_Exception_Configuration“ für Lese- und Schreibvorgänge. Wenn, nachdem der Datensatz übermittelt wurde E-Mail-Benachrichtigungen Sind definiert, Mitglieder von Vulnerability Response Gruppe erhält eine E-Mail, wenn das Ablaufdatum innerhalb einer Woche liegt. Wenn das Zurückstellungsdatum abläuft, wird das angreifbare Element auf „Offen“ zurückgesetzt, und eine zweite E-Mail-Benachrichtigung wird gesendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Grund	Geben Sie den Grund für die Zurückstellung des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Falsch positiv ○ Korrektur nicht verfügbar ○ Risiko akzeptiert ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Klicken Sie auf **Absenden**.
   Die Gruppe ist markiert **Wird Überprüft** . A **Erneut Öffnen** Der zugehörige Link wird angezeigt. Das Datum und der Grund der erneuten Öffnung werden in Arbeitsnotizen unter angezeigt **Statusänderungsgenehmigungen** Registerkarte.

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element an

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element an, bevor es das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch eine Verlängerung über anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Vulnerability Manager-Arbeitsbereich an.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**an.
2. Öffnen Sie ein zurückgestelltes angreifbares Element.
3. Wählen Sie Aus **Verlängerung Anfordern** .

> **Hinweis:**
> Die Schaltfläche „Verlängerung anfordern“ ist nur sichtbar, wenn der Status des angreifbaren Elements „Zurückgestellt“ lautet.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem das zurückgestellte angreifbare Element zur Korrektur verlängert werden muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Grund	Geben Sie den Grund für die Zurückstellung des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Risiko akzeptiert ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei der Übermittlung der Anforderung und der nachfolgenden Aktion durch den Genehmiger wird eine E-Mail ausgelöst.

   Hinweis:
   - Die Anforderung durchläuft zwei Genehmigungsebenen.
   - Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End.

6. Nachdem die Anforderung genehmigt wurde, werden „bis“, „Grund“ und „Zurückstellungshinweise“ aktualisiert.

Aktualisieren Vulnerability Response Angreifbare Elemente

Die **Status aktualisieren** Der zugehörige Link wird verwendet, um angreifbare Elemente zu überprüfen, um festzustellen, ob zusätzliche angreifbare Elemente vorhanden sind, die zu einer Korrekturaufgabe gehören. Verwenden Sie diese Option, wenn eine Aktualisierung außerhalb der geplanten Aufgabe gerechtfertigt ist.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_write oder, sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Die **Status aktualisieren** Der zugehörige Link kann nur im Formular „Korrekturaufgabe“ in bearbeitet werden **Öffnen** Oder **Wird Untersucht** status, die eine Filtergruppe verwenden oder deren Filtertyp „Bedingung“ ist. Diese Inspektion wird unabhängig vom Status von durchgeführt **Aktualisieren Sie angreifbare Elemente automatisch** Kontrollkästchen.

Beginnend mit v22.0 von Vulnerability Response, **Status Aktualisieren** Die Schaltfläche ist in der Datensatzansicht für Korrekturaufgaben in verfügbar Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**an.
2. Öffnen Sie einen beliebigen Datensatz in **Öffnen** Oder **Wird Untersucht** status.
3. Klicken Sie auf **Status aktualisieren** Link.
   Neue angreifbare Elemente werden unter angezeigt **Angreifbare Elemente** Registerkarte.

Identifizieren und eskalieren Sie Sicherheitsprobleme in Drittanbietersoftware

Sie können Softwareschwachstellen anzeigen, die aus Drittparteieinträgen zurückgegeben wurden, um die Korrektur zu bestimmen. Verwenden Sie diese Informationen, um die Einträge der angreifbaren Software mit einer Software abzugleichen Asset-Management Discovery-Modell.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_write

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Bibliotheken** > **Drittpartei**an.
   Eine Liste der heruntergeladenen angreifbaren Software wird angezeigt.
2. Klicken Sie auf einen Softwaredatensatz, um Informationen zu Schwachstellen anzuzeigen.
3. Klicken Sie auf die folgenden zugehörigen Listen, um weitere Informationen zur Identifizierung von Schwachstellen zu erhalten.
   Wenn Schwachstellen identifiziert und angreifbare Elemente erstellt wurden, können Sie dies Lösen Sie Korrekturaufgaben, Nach Bedarf.

Identifizieren und eskalieren Sie Sicherheitsprobleme mit NVD

Wenn CVE-ID-Datensätze (Common Vulnerability and Exposures Identifier) aus der National Vulnerability Database (NVD) heruntergeladen werden, werden sie mit der Software in Ihrem Unternehmensnetzwerk verglichen, die vom Software Asset Discovery-Modell identifiziert wurde. Wenn eine CVE-ID mit angreifbarer Software oder Konfigurationselement in Ihrem Netzwerk übereinstimmt, wird ein angreifbares Element erstellt. Sie verwenden die Informationen im CVE-ID-Datensatz, um zu entscheiden, ob das angreifbare Element zur Korrektur eskaliert werden soll.

Vorbereitungen

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Bibliotheken** > **NVD**an.
   Eine Liste der CVE-IDs, die vom NVD heruntergeladen wurden, wird angezeigt. Updates aus dem NVD können bei Bedarf und durch geplante Ausführungen aus den NIST National Vulnerability Database Integration-Datensätzen unter durchgeführt werden **Alle** > **Administration** > **Integrationen**an.
2. Klicken Sie auf einen CVE-Datensatz, um die folgenden Informationen anzuzeigen:
   - Eine Zusammenfassung für die CVE-ID.
   - Ein Verweis auf einen CWE-Eintrag (Common Weakness Enumeration), falls zutreffend.
   - Die Schwachstellenpunktzahl der CVE-ID im Common Vulnerability Scoring System (CVSS). Weitere Informationen zum CVSS finden Sie unter Website der nationalen Schwachstellendatenbank .
3. Klicken Sie auf die zugehörigen Listen, um weitere Informationen zu Schwachstellen zu erhalten.

   Verwundbarkeitsreferenzen

   Name, Beschreibung und URL für die angegebene Schwachstelle und wo darauf verwiesen wird.

   Exploits

   Details.

   Schwachstellen

   Liste der CWE-Schwachstellen.
4. Klicken Sie auf die folgenden zugehörigen Listen, um weitere Informationen zur Identifizierung von Schwachstellen zu erhalten.
   Wenn Schwachstellen identifiziert und angreifbare Elemente erstellt wurden, können Sie dies Lösen Sie Korrekturaufgaben, Nach Bedarf.

Identifizieren und eskalieren Sie Sicherheitsprobleme mit CWE

Zeigen Sie die Bibliothek der CWE-Datensätze (Common Schwachstellen Enumeration) aus der National Vulnerability Database (NVD) an, um zu verstehen, wie sie mit den CVE-Datensätzen (Common Vulnerability and Exposure) in Zusammenhang stehen. Verwenden Sie dann diese Informationen, um die Einträge der angreifbaren Software mit einer Software abzugleichen Asset-Management Discovery-Modell.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_write

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Bibliotheken** > **CWE**an.
   Eine Liste der heruntergeladenen angreifbaren Software wird angezeigt.
2. Klicken Sie auf einen CWE-Softwaredatensatz, um Informationen zu Schwachstellen anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf die folgenden zugehörigen Listen, um weitere Informationen zur Identifizierung von Schwachstellen zu erhalten.
   Wenn Schwachstellen identifiziert und angreifbare Elemente erstellt wurden, können Sie dies Lösen Sie Korrekturaufgaben, Nach Bedarf.

Zeigen Sie den Korrekturzielstatus von an Vulnerability Response Angreifbares Element

Wenn ein angreifbares Element sein Korrekturzieldatum fast erreicht (oder überschritten) hat, wie durch eine Korrekturzielregel definiert, wird der Datensatz des angreifbaren Elements mit einem Status aktualisiert. Diese Informationen können dem Analysten helfen, bevorstehende Korrekturaktivitäten proaktiv zu überwachen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.vulnerability_admin
- sn_vul.read_Remediation_target_rules [schreibgeschützt]

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

A Geplante Aufgabe Angerufen **Bewerten Sie Korrekturziele** Wird einmal pro Tag ausgeführt, um das aktuelle Datum mit dem Korrekturdatum für angreifbare Elemente zu vergleichen, das in der zugehörigen Korrekturzielregel angegeben ist. Wenn das aktuelle Datum innerhalb der Anzahl von Tagen liegt, bevor die Korrektur überfällig ist, wird dem Datensatz des angreifbaren Elements ein Korrekturstatus hinzugefügt.

Weitere Informationen zu Korrekturzielregeln finden Sie unter Vulnerability Response Korrekturzielregeln.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Angreifbare Elemente**an.
2. Klicken Sie auf das angreifbare Element, das Sie überprüfen möchten.
   Wenn das Korrekturdatum für das angreifbare Element innerhalb des Bereichs der in der Korrekturzielregel festgelegten Bedingungen liegt, wird der **Status Des Korrekturziels** Registerkarte ist sichtbar.
3. Klicken Sie auf **Status Des Korrekturziels** Registerkarte.
4. Klicken Sie auf den Korrekturzielstatusdatensatz, um ihn zu überprüfen.

Hinweis:
Informationen zum Anzeigen der Anzahl der angreifbaren Elemente, die sich dem Ziel, dem laufenden und dem veralteten Ziel nähern, finden Sie unter Wird standardmäßig verwendet Vulnerability Response Dashboards.

Zugehörige Informationen

Erstellen oder bearbeiten Vulnerability Response Korrekturzielregeln

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeiten mit nicht abgeglichenen CIs

Als Schwachstellenmanager und -Analyst können Sie nicht abgeglichene Konfigurationselemente (Configuration Items, CIs) anzeigen und neu klassifizieren, nicht abgeglichene erkannte Elemente abgleichen, CI-Suchregeln erneut auf die ausgewählten erkannten Elemente anwenden und vorhandene CIs deduplizieren.

Zeigen Sie nicht abgeglichene Konfigurationselemente an, und klassifizieren Sie sie erneut

Konfigurationselemente (CIs), die nicht in gefunden werden Configuration Management Database (CMDB) Werden in einer anzeigbaren Liste erkannter Elemente platziert. Diese Liste bietet eine bequeme Möglichkeit, nicht abgeglichene CIs neu zu klassifizieren.

Vorbereitungen

Erforderliche Rolle:
sn_vul.read (Minimum zum Anzeigen nicht übereinstimmender CIs)

und

itil oder Asset (zum erneuten Klassifizieren)

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird

Als Schwachstellenanalyst können Sie nicht übereinstimmende CIs anzeigen.

Die Aktion „Neu klassifizieren“ ist nur für verfügbar `sn_sec_cmn_unmatched_ci`Klassen-CIs, wenn Sie entweder die Rolle itil oder Asset innehaben. Sobald ein CI neu klassifiziert wurde, kann es nicht mehr über die Anwenderoberfläche neu klassifiziert werden. Sie können über das CI-Formular oder die CI-Listenansicht neu klassifizieren, indem Sie ändern **Klasse** Wert.Weitere Informationen finden Sie unter Reclassify a CI .

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **Erkannte Elemente**an.
2. Klicken Sie zum Überprüfen auf die einzelnen Elemente.
3. Um Korrekturen an den Informationen in vorzunehmen **Erkanntes Element** Formularfelder bearbeiten Sie auf dieser Seite, und klicken Sie mit der rechten Maustaste **Speichern** .
   Alle Daten, die zu diesen Feldern hinzugefügt oder in diesen Feldern verbleiben, werden an das Ergebnis übertragen **Konfigurationselement** Wenn er neu klassifiziert wird.
4. Wenn alles richtig aussieht, klicken Sie auf **Neu Klassifizieren** .
5. Wählen Sie in der Auswahlliste eine aus **Klassenname** Und klicken Sie auf **Übermitteln** .
   Die **Erkanntes Element Klasse** Wird aktualisiert, die **Status** Das Feld wird in „erneut klassifiziert“ geändert, und alle Daten befinden sich in der CMDB.

Nicht übereinstimmende erkannte Elemente abstimmen

Erstellen Sie eine geplante Aufgabe, um nicht übereinstimmende erkannte Elemente abzugleichen.

Vorbereitungen

Erforderliche Rollen: administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Ein angreifbares Element (VI) besteht aus einer Schwachstelle und einem Konfigurationselement (CI). Wenn ein VI erstellt wird, kann das CI, das ihm zum Zeitpunkt der Erstellung hinzugefügt wird, ein veraltetes CI sein. Nicht übereinstimmende CI-Informationen werden nicht abgeglichen, wenn sich die Informationen in der CMDB ändern. Zum Abgleich wenden Sie Suchregeln für Konfigurationselemente (Configuration Item, CI) auf die Elemente an, die sich in einem nicht abgeglichenen Status befinden, wenn die CMDB mit den neuesten CIs aktualisiert wird.

Sie können einen geplanten Aufgabenbedarf ausführen, um die CI-Übereinstimmungsregel für die erkannten Elemente in einem nicht abgeglichenen Status erneut anzuwenden. Wenn sich das CI nach erneuter Anwendung der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Betroffene Erkennungen und angreifbare Elemente werden ebenfalls aktualisiert. Details finden Sie unter CI-Änderungen für erkannte Elemente.

Prozedur

1. Navigieren zu **Alle** > **Security Operations > Nicht Abgeglichene Erkannte Elemente Abgleichen**an.
2. Klicken Sie auf der Seite Hintergrundaufträge auf **Erstellen Sie einen Abgleichsauftrag** .
3. Füllen Sie im Formular die Felder aus.

Hinweis:
Sie können nur bearbeiten **Parameter** Feld.

Formular „Hintergrundauftrag“

Feld	Beschreibung
Anzahl	Eindeutige Auftragsnummer.
Erstellt von	Anwender, der den Auftrag erstellt hat.
Parameter	Parameter zum Abgleichen der nicht übereinstimmenden erkannten Elemente: ○ Grenzwert: Maximale Anzahl erkannter Elemente, die abgeglichen werden sollen. Wenn Sie keinen Wert eingeben, werden 10.000 erkannte Elemente abgeglichen. ○ FirstDiscovereditem: Erstes erkanntes Element, das abgeglichen werden muss. Wenn Sie keinen Wert eingeben, beginnt der Abgleichsprozess mit dem ersten erkannten Element.
Status	Aktueller Status des Hintergrundauftrags.
Statusbeschreibung	Beschreibung des aktuellen Status des Hintergrundauftrags.
Auftragstyp	Typ des Auftrags. Der Wert ist **Nicht übereinstimmende erkannte Elemente abgleichen** .
Gestartet um	Zeit, zu der der Auftrag gestartet wurde.
Endete um	Zeit, zu der der Auftrag abgeschlossen wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Auftragsdauer	Gesamtzeit, die für den Abschluss des Auftrags benötigt wurde.
Substatus	Substatus für den ausgewählten Status.
Notizen	Anzahl der Datensätze, die verarbeitet wurden.

4. Klicken Sie auf **Absenden**.

Hinweis:

- Um die Ausführung des Auftrags zu beenden, klicken Sie auf **Abbrechen** .
- Sie können nicht übereinstimmende CIs nicht abgleichen oder CI-Suchregeln nicht erneut anwenden, während Sie Hosts oder angreifbare Elemente importieren.

5. Beginnend mit Vulnerability Response V26.0.11 können Sie „Suchregeln erneut anwenden“ für ausgewählte oder gefilterte Elemente in der Tabellenansicht „erkannte Elemente“ verwenden.

Hinweis:
Ab der oben genannten Version wird die geplante Aufgabe „nicht abgeglichene erkannte Elemente abgleichen“ deaktiviert.

6. **Wahlweise:** Auswahlvorgang **Alle** > **Security Operations >Wenden Sie Suchregeln erneut an** Für ausgewählte oder gefilterte Elemente in der Tabelle „erkannte Elemente“.

Hinweis:
Wenn kein Filter angewendet wird, wird die Option erneut anwenden deaktiviert.

Nach der erneuten Anwendung wird eine Hintergrundauftrags-URL oder eine Fehlermeldung angezeigt, sobald die Integration ausgeführt wird.

Wenden Sie CI-Suchregeln erneut auf ausgewählte erkannte Elemente an

Wenden Sie die Suchregeln für Konfigurationselemente (Configuration Item, CI) erneut auf ausgewählte erkannte Elemente aus den Auswahlaktionen der Listenansicht „erkannte Elemente“ an. Wenn sich das CI ändert, nachdem Sie die Regeln erneut anwenden, werden die erkannten Elemente mit dem neuen CI und den betroffenen Erkennungen aktualisiert. Angreifbare Elemente werden ebenfalls aktualisiert.

Vorbereitungen
Erforderliche Rollen: administrator

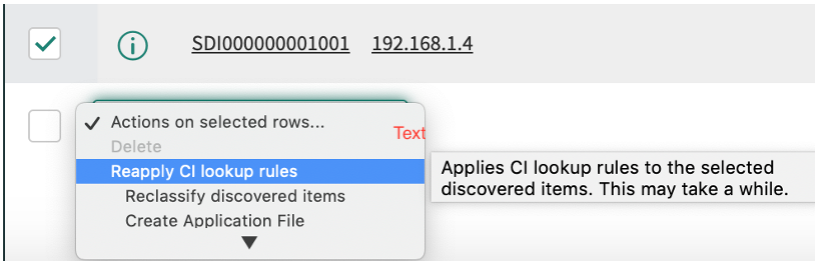
Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen finden Sie unter CI-Änderungen für erkannte Elemente.

Weitere Informationen zu den Konzepten des CI-Abgleichs und der CMDB, der Suche nach erkannten Elementen, der regelbasierten Identifizierung und anderen detaillierten Informationen zur Funktionsweise des CI-Abgleichs finden Sie unter CI-Übereinstimmung im Vulnerability Response-artikel [KB0998706] In der HI Knowledge Base.

Prozedur

1. Navigieren zu **Alle** > **Sicherheitsvorgänge** > **CMDB** > **Erkannte Elemente**an.
2. Wählen Sie die erforderlichen erkannten Elemente aus, und klicken Sie auf **Aktion für ausgewählte Zeilen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie in der Liste aus **Wenden Sie die CI-Suchregeln erneut an** .

   Hinweis:

   Beginnend mit Vulnerability Response V24.0.6. Sie können die erneute Anwendung von CI-Suchregeln auf erkannte Elemente mit dem Substatus „CI außer Betrieb genommen“ überspringen, indem Sie die Systemeigenschaft aktivieren *`sn_sec_cmn.skipItemsWithCIDecommissioned`*.

   Die Regeln werden auf diese erkannten Elemente erneut angewendet.

4. Klicken Sie Auf **Status anzeigen** In der Nachricht.

   Der Status wird im Hintergrundauftragsformular angezeigt.

   Hinweis:
   In **Notizen** Feld, die Erkannte Elemente konnten aufgrund einer Ausnahme nicht verarbeitet werden Attribut mit einem Wert ungleich Null gibt an, dass beim erneuten Anwenden einer CI-Suchregel ein Fehler oder eine Ausnahme aufgetreten ist. Weitere Details finden Sie in den Systemprotokollen.

5. „Erneut anwenden“ gilt nur für Elemente, die innerhalb der letzten 90 Tage gescannt wurden, basierend auf **Last_Scan_date, Last_comp_Scan_date, non_infra_Last_Scan_date, non_infra_Last_comp_Scan_date** Spalte.

   Systemeigenschaft „ci_Lifecycle_Status_Source“ (Umfang = sn_sec_cmn) zum Konfigurieren von CI-Lebenszyklusstatusspalten (z. B. Installationsstatus, Betriebsstatus) hinzugefügt. Sie können zusätzliche Spalten für die Stilllegung von CIs konfigurieren.

   Spalten werden der Listenansicht des Hintergrundauftrags hinzugefügt:

   - Verstrichene Zeit (ms): Die Zeit, die für die Verarbeitung des Hintergrundauftrags erforderlich ist.
   - Verarbeitete Elemente: Die Anzahl der bis jetzt verarbeiteten Elemente.
   - Gesamtzahl der zu verarbeitenden Elemente: Die Gesamtzahl der noch zu verarbeitenden Elemente.
   - Zeit bis Abschluss (ms): Die verbleibende Zeit bis zur Verarbeitung des Hintergrundauftrags. Diese Spalten bieten Einblick in den Auftragsfortschritt. Diese Spalten sind für jede Formularansicht verfügbar, die Sie je nach Anforderung hinzufügen können.

Wenden Sie die Verbesserungen der CI-Suchregeln erneut an

Wenden Sie die Suchregeln für Konfigurationselemente (Configuration Item, CI) erneut auf ausgewählte erkannte Elemente wie betriebssystem und netbios an.

Vorbereitungen
Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

- Werte von betriebssystem und netbios, die in Quelldaten vorhanden sind, müssen vor dem Konfigurationselement ausgefüllt werden, während diese Felder im erkannten Element ausgefüllt werden.
- Bei leeren Werten von Betriebssystem und NETBIOS in Quelldaten werden die Werte aus dem Konfigurationselement übernommen, während diese Felder in der Tabelle „erkannte Elemente“ ausgefüllt werden.

Prozedur

1. Navigieren zu **Alle** > **Sicherheitsvorgänge** > **CMDB** > **Erkannte Elemente**an.
2. Wählen Sie die erforderlichen erkannten Elemente aus, und klicken Sie auf **Aktion für ausgewählte Zeilen** .
3. Wählen Sie in der Liste aus **Wenden Sie die CI-Suchregeln erneut an** .

   Die Regeln werden auf diese erkannten Elemente erneut angewendet.

Schritte zur Verhinderung doppelter oder verwaister Datensätze nach der Ausführung Vulnerability Response CI-Suchregeln

Ergreifen Sie Schritte, um zu verhindern, dass doppelte oder verwaiste Datensätze durch Übereinstimmungen entstehen (Konfigurationselemente (CIs) innerhalb von CMDB.

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Iterieren und Durchführen des Abgleichs in der CMDB verwendet wird, kann zu längeren Verarbeitungszeiten führen. Gründliches Testen und Debugging von Verarbeitungsskripts in den Regeln trägt dazu bei, das Potenzial von Problemen später im Prozess zu mindern.

Doppelte oder verwaiste Datensätze werden verhindert

- Verwenden Sie kleine Teilmengen von Daten, die für die getestete CI-Suchregel spezifisch sind.
  - Setzen Sie alle CI-Suchregeln, mit Ausnahme der getesteten, auf Inaktiv.
  - Analysieren Sie die importierten CIs, um sicherzustellen, dass Sie das erwartete Verhalten beobachten und die Übereinstimmung ordnungsgemäß erfolgt.
- Überprüfen Sie übereinstimmende CIs
  - Überprüfen Sie die Anzahl der übereinstimmenden CIs im Vergleich zu nicht übereinstimmenden CIs. Stellen Sie sicher, dass der Prozentsatz akzeptabel ist. Sehen Sie sich nicht nur die erste Seite an, die wahrscheinlich die erste eingefügte Seite ist.
  - Suchen Sie manuell nach einigen CIs.
  - Überprüfen Sie, ob Benennungs- oder Feldprobleme auftreten (z. B. Suche nach einer bestimmten Domäne).

    Fügen Sie gegebenenfalls zusätzliche Übereinstimmungsregeln hinzu.
- Überprüfen Sie nicht abgeglichene CIs
  - Navigieren Sie zur Tabelle „nicht abgeglichene CIs“.
  - Nach Konfigurationselementklasse gruppieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überprüfen Sie alle Klassen, die nicht richtig aussehen (Zertifikate, Netzwerkkarten, Bilder).
  - Finden Sie heraus, warum sie nicht mit dem richtigen CI übereinstimmen?
  - Soll die Klasse ausgeschlossen werden?
  - Soll die Klasse auf eine zugehörige Klasse hochgestuft werden?
- Überprüfen Sie CI-status wie **Stillgelegt** .
- Entfernen Sie Testdaten
  - Sobald Sie mit der Beobachtung des richtigen oder erwarteten Verhaltens bei der CI-Übereinstimmung beginnen, beginnen Sie von vorn.
  - Beginnen Sie von vorne, indem Sie die für das Testen verwendeten Daten löschen: (Siehe **Daten werden aus Tabellen gelöscht** Abschnitt)
    - Erkannte Elemente
    - Angreifbare Elemente
    - Korrekturaufgaben
  - Alle CI-Übereinstimmungsregeln werden manuell erneut ausgeführt.

Für weitere Informationen zu CI-Suchregeln und Qualys, Siehe KB0750656 artikel.

Für weitere Informationen zu CI-Suchregeln und Rapid7, Siehe KB0818096 .

Daten werden aus Tabellen gelöscht

Manchmal haben Sie Daten importiert und stellen fest, dass etwas nicht stimmt. Wenn in einer Entwicklungs- oder Leistungsumgebung etwas nicht stimmt, könnten Sie sich von einer besseren Umgebung zurückziehen, aber das ist nicht immer eine Option.

Hinweis:
Das Ausführen dieser Aktionen erfordert ServiceNow Fachwissen.

Es gibt vier Optionen zum Löschen von Daten aus Tabellen:

- Verwenden **Löschen Sie Alle Datensätze** Ein **Tabellenkonfiguration** .
- Konfigurieren Sie **Tabellenbereinigung** Indem Sie zu navigieren **Automatisch Entleeren** (sys_Auto_Flush.list) und erstellt eine neue **Automatisch leeren** Datensatz.
- Kürzen Sie gs.truncateTable mit einem Hintergrundskript.

  Verwenden `truncateTable`Erfordert das Deaktivieren des Kontrollkästchens „Datensatz für Rollback“ in den Hintergrundskripts. Andernfalls werden eine Kopie der Tabelle und der zugehörigen kaskadierenden Tabellen erstellt, dauern zu lange und schlagen höchstwahrscheinlich fehl.

  Hinweis:
  Niemals verwenden `truncateTable`In einer Produktionsumgebung. Wenden Sie sich an Ihren Support-Mitarbeiter, bevor Sie große Löschungen in Produktions- oder freigegebenen Umgebungen ausführen.

Deduplizierung vorhandener Konfigurationselemente

Immer wenn Konfigurationselemente (Configuration Items, CIs) durch eine Deduplizierungsaufgabe aktualisiert werden, werden auch die erkannten Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(DIS) aktualisiert, die sich auf diese CIs beziehen. Die angreifbaren Elemente (VIS) und Erkennungen werden ebenfalls mit dem CI aktualisiert.

Weitere Informationen finden Sie unter CI-Änderungen für erkannte Elemente.

Zugehörige Informationen

Deduplizierungsaufgaben nachbessern

Lösen Sie Korrekturaufgaben

Die Flexibilität, die inhärent ist Vulnerability Response Ermöglicht Ihnen die Behebung von Schwachstellen auf die für Ihre Sicherheitsorganisation geeignete Weise.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird

Sobald Sie benachrichtigt werden, dass eine Change-Anforderung gelöst wurde, verschieben Sie den Status der Korrekturaufgabe in gelöst, und warten Sie auf den nächsten Scan. Erneutes Scannen wird automatisch durch den im Setup-Assistenten konfigurierten Importzeitplan einer Drittpartei ausgelöst.

Hinweis:

Wenn die Statussynchronisierung aktiviert ist, werden Korrekturaufgaben automatisch in den Status gelöst verschoben, nachdem eine Change-Anforderung, die einer Korrekturaufgabe zugeordnet ist, implementiert wurde und sich im Status Überprüfen befindet. Weitere Informationen finden Sie unter Change-Management für Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Mir zugewiesen**an.
2. Klicken Sie auf einen Datensatz, der sich im Status Offen befindet.

   Der Status Offen gibt an, dass der Datensatz noch nicht bearbeitet wurde. Das Formular zeigt Folgendes an:

   - Informationen zur Korrekturaufgabe
   - Gruppenkonfigurationsdetails
   - Notizen
   - Zugeordnete angreifbare Elemente
   - Aufgaben-SLAs
   - Change-Anforderungen
3. Führen Sie Ihre Analyse der Gruppe durch.
4. Wenn Sie bereit sind, mit der Arbeit am Datensatz zu beginnen, wählen Sie eine der folgenden Optionen aus.

Option	Bezeichnung
Wenn das angreifbare Element ein Risiko für Ihre IT-Umgebung darstellt, erstellen Sie einen CHG-Datensatz, und eskalieren Sie das Problem an Change-Management Team.	Weisen Sie die Gruppe der entsprechenden Gruppe oder Einzelperson zu, und klicken Sie auf **Erstellen Sie Einen Change** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Wenn das angreifbare Element ein potenzielles Sicherheitsrisiko für Ihre Organisation darstellt, erstellen Sie einen Security Incident-Datensatz, und eskalieren Sie das Problem an den Security Incident Response Team.	Klicken Sie auf **Security Incident erstellen**. Diese Schaltfläche wird nur angezeigt, wenn Security Incident Response Ist aktiviert. Eine Berechnung der Geschäftsauswirkung wird angewendet, der Incident wird zuge–wiesen, und der Security Incident wird er–stellt.

Nachdem Sie eine Change-Anforderung erstellt haben, wird der entsprechende Datensatz in angezeigt **Change-Anforderungen** Zugehörige Liste im Formular „Schwachstellengruppe“.

5. Wenn Sie feststellen, dass das Problem ein geringes Risiko aufweist und zurückgestellt werden kann, klicken Sie auf **Ausnahme Anfordern** .
   Weitere Informationen zum Zurückstellen einer Korrekturaufgabe finden Sie unter Eine Korrekturaufgabe zurückstellen.
6. Wenn Sie feststellen, dass das Problem sofort ohne weitere Analyse geschlossen werden kann, klicken Sie auf **Schließen** .
   Weitere Informationen zum Schließen einer Korrekturaufgabe finden Sie unter Schließen Sie eine Korrekturaufgabe. Ab v23.0 von Vulnerability Response, **Schließen** Schaltfläche wurde für eine Korrekturaufgabe entfernt.

Eine geplante Aufgabe für die Integration von Drittparteien aktualisiert und scannt Datensätze automatisch in einem festgelegten Intervall. Die angreifbaren Elemente werden zum nächsten geplanten Datum und zur nächsten geplanten Uhrzeit gescannt. Alternativ können Sie manuell einen Schwachstellen-Scan mit initiieren **Suchen Sie nach Schwachstellen** Zugehöriger Link.

Wenn der Scan die Schwachstelle im Konfigurationselement erneut findet und sie nicht als behoben markiert wird, kehrt das angreifbare Element in den Status „wird untersucht“ zurück. Wenden Sie sich an IT Operations, um die Change-Anforderung erneut zu öffnen.

Wenn der Scan die Schwachstelle nicht findet und zurückgibt, dass das angreifbare Element als behoben markiert wurde, wechselt das angreifbare Element in den Status Geschlossen-behoben und wird während des Imports geschlossen.

Nur wenn sich alle angreifbaren Elemente in einer Aufgabe im Status „Geschlossen – behoben“ befinden, wird die Korrekturaufgabe automatisch geschlossen. Korrekturaufgaben mit angreifbaren Elementen im status „Geschlossen“ außer „behoben“ müssen manuell geschlossen werden.

Eine Korrekturaufgabe zurückstellen

Wenn Sie feststellen, dass das Problem, das einer Korrekturaufgabe zugeordnet ist (VUL), eine niedrige Priorität hat und sofort ohne weitere Analyse zurückgestellt werden kann, können Sie verwenden **Ausnahme Anfordern** Funktion.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Korrekturaufgabe aus einem Korrekturaufgabendatensatz in zurückstellen Vulnerability Response Arbeitsbereiche. Nachdem Sie die Anforderung übermittelt haben, wird sie zur Genehmigung gesendet. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine geplante Aufgabe wird jeden Tag ausgeführt, um nach zurückgestellten Korrekturaufgaben zu suchen, die ihr Wiedereröffnungsdatum erreicht haben. An dem Tag, an dem die Zurückstellung der Aufgabe abläuft, wird die Aufgabe erneut geöffnet.

Hinweis:
Sie können Change-Anforderungen und Korrekturaufgaben manuell durch die status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist. Wenn das System jedoch registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder es aus einer Korrekturaufgabe entfernen, kann die Statussynchronisierung Ihren manuellen Eingriff möglicherweise überschreiben. Change-anforderungsstatus verschieben Korrekturaufgaben jedoch nicht automatisch aus den status „Geschlossen“ oder „Zurückgestellt“.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**an.
2. Öffnen Sie einen Datensatz.
3. Klicken Sie Auf **Ausnahme Anfordern** .
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Bis	Wählen Sie das Datum aus, an dem der Status Zurückstellen abläuft und die Korrekturaufgabe erneut aktiviert wird. Wenn, nachdem der Datensatz übermittelt wurde E-Mail-Benachrichtigungen Sind definiert, Mitglieder von Vulnerability Response Gruppe erhält eine E-Mail, wenn das Ablaufdatum innerhalb einer Woche liegt. Wenn das Zurückstellungsdatum abläuft, wird die Korrekturaufgabe auf zurückgesetzt **Öffnen** Und eine zweite E-Mail-Benachrichtigung wird gesendet.
Grund	Geben Sie den Grund für die Zurückstellung des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Falsch positiv ○ Korrektur nicht verfügbar ○ Risiko akzeptiert ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Absenden**.
   Die Gruppe ist in Überprüfung markiert. A **Erneut Öffnen** Der zugehörige Link wird angezeigt. Das Datum und der Grund der erneuten Öffnung werden in Arbeitsnotizen unter angezeigt **Statusänderungsgenehmigungen** Registerkarte.

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe an

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe (VUL) an, bevor sie das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch eine Verlängerung über anfordern Vulnerability Response Arbeitsbereiche.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**an.
2. Öffnen Sie eine zurückgestellte Korrekturaufgabe.
3. Wählen Sie Aus **Verlängerung Anfordern** .
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, an dem der Status Zurückstellen abläuft und die Korrekturaufgabe erneut aktiviert wird.
Grund	Geben Sie den Grund für die Zurückstellung des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Risiko akzeptiert ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Änderungen an der Korrekturaufgabe auch auf die angreifbaren Elemente zurückgesetzt, die Teil der Korrekturaufgabe sind. Die angreifbaren Elemente müssen sich jedoch im Status „zurückgestellt“ und ihren aktuellen Status befinden, bis die Daten vor dem Datum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„aktualisiert bis“ liegen. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion durch den Genehmiger ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben nicht verfügbar, die als Teil einer Ausnahmeregel erstellt werden.
- Wenn eine zurückgestellte Korrekturaufgabe erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End.

Schließen Sie eine Korrekturaufgabe

Wenn Sie feststellen, dass das Problem, das einer Korrekturaufgabe zugeordnet ist, sofort ohne weitere Analyse geschlossen werden kann, können Sie verwenden **Schließen** Funktion. Ab v23.0 von Vulnerability Response, **Schließen** Schaltfläche wurde für eine Korrekturaufgabe entfernt, und das Schließen einer Korrekturaufgabe wird vom Scanner gesteuert.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

In Vulnerability Response Arbeitsbereiche, eine Korrekturaufgabe durchläuft dieselben status wie eine Korrekturaufgabe, die zuvor in früheren Versionen von durchgeführt wurde Vulnerability Response. Wenn alle angreifbaren Elemente (Vits) in einer Korrekturaufgabe geschlossen sind, wechselt die Korrekturaufgabe in den Status Inaktiv.

Wichtig:

Sie können Change-Anforderungen und Korrekturaufgaben manuell durch die status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist. Wenn das System jedoch registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder es aus einer Korrekturaufgabe entfernen, kann die Statussynchronisierung Ihren manuellen Eingriff möglicherweise überschreiben. Change-anforderungsstatus verschieben Korrekturaufgaben jedoch nicht automatisch aus dem Geschlossen Oder Zurückgestellt status.

Prozedur

1. Öffnen Sie den Datensatz, für den Sie eine Überprüfung anfordern möchten.
2. Wählen Sie aus **Schließen/Zurückstellen** Schaltfläche.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Status	Wählen Sie einen Status aus. Die Auswahlmöglichkeiten lauten wie folgt: ○ Zurückgestellt ○ Geschlossen
Bis	Nur in verfügbar **Zurückstellen** Popup-Fenster „status“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wählen Sie das Datum aus, an dem das **Zurückstellen** status läuft ab, und die Korrekturaufgabe wird erneut aktiviert. Wenn, nachdem der Datensatz übermittelt wurde E-Mail-Benachrichtigungen Sind definiert, Mitglieder von Vulnerability Response Gruppe erhält eine E-Mail, wenn das Ablaufdatum innerhalb einer Woche liegt. Wenn das Zurückstellungsdatum abläuft, wird das angreifbare Element auf zurückgesetzt **Öffnen** Und eine zweite E-Mail-Benachrichtigung wird gesendet.
Grund	Geben Sie den Grund für das Schließen des Problems ein.
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

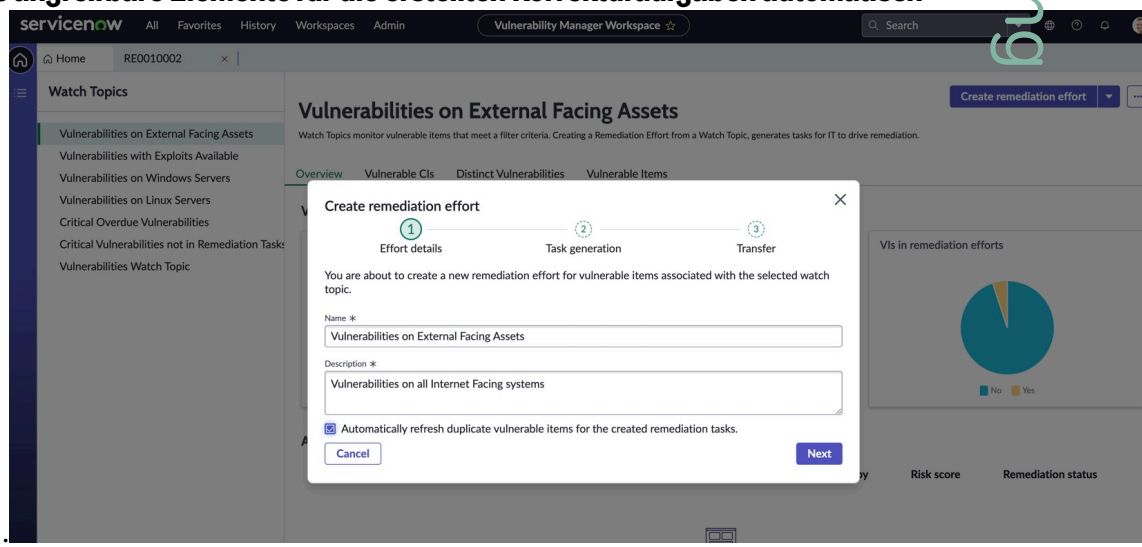
4. Wählen Sie **Absenden**.
   Die Korrekturaufgabe ist markiert **Geschlossen** .

Identifizierung doppelter angreifbarer Elemente aus mehreren Scannern

Wenn Sie mehrere Scanner für dasselbe Asset verwenden, um Schwachstellen zu erkennen, werden möglicherweise mehrere angreifbare Elemente (VIS) erstellt. Sie können diese doppelten VIS identifizieren, um sicherzustellen, dass die doppelten Schwachstellen nicht den Korrekturbesitzern zugewiesen werden.

Diese Lösung ist nur möglich, wenn dieselben Schwachstellen erkannt werden, z. B. dieselben Common Vulnerabilities and Exposures (CVEs). Die Schwachstellenkombination hängt von den verwendeten Scannern ab. Beispielsweise haben Qualys und Tenable ihren eigenen Schwachstellentyp, d. h. Drittparteieinträge (TPEs), und andere Scanner wie Microsoft Defender for Endpoint erkennen Schwachstellen basierend auf CVEs.

Ab Version 17.1 können Sie beim Erstellen einer Korrekturmaßnahme doppelte angreifbare Elemente für die erstellten Korrekturaufgaben automatisch aktualisieren. Um die doppelten angreifbaren Elemente automatisch zu aktualisieren, müssen Sie auswählen **Doppelte angreifbare Elemente für die erstellten Korrekturaufgaben automatisch aktualisieren**Option.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Doppelte VIS anzeigen : Identifizieren Sie doppelte angreifbare Elemente, die von mehreren Scannern im System gemeldet wurden. Sie können das doppelte VI als gelöst markieren. Weitere Informationen finden Sie unter Beheben Sie doppelte Schwachstellen automatisch. Doppelte Einträge werden nur angezeigt, wenn die Kombination von Schwachstellen mit CVEs erstellt wird. Weitere Informationen finden Sie unter Korrekturaufgabe für Vulnerability Response und status angreifbarer Elemente.

Potenzielle Duplikate werden für die folgenden Schwachstellenkombinationen identifiziert:

Scannerkombination	Typ der Schwachstelle
Scanner 1 und Scanner 2	CVE
Scanner 1 und Scanner 2	CVE und TPE

Beheben Sie doppelte Schwachstellen automatisch

Beginnt ab Vulnerability Response(VR) v17.1 können Sie doppelte Schwachstellen in einem Asset automatisch beheben.

Wenn ein Asset mit mehreren Scannern gescannt wird, besteht die Möglichkeit, dieselbe Schwachstelle wie Duplikate von den verschiedenen Scannern zu identifizieren. Wenn die Qualys- und Microsoft-Scanner beispielsweise dieselbe Schwachstelle identifizieren, können Sie die doppelte Schwachstelle automatisch beheben.

Beispielszenario

VR erstellt einen Datensatz, VI1, für Schwachstelle 1 aus dem Microsoft Defender for Endpoint-Scanner. Ein zweiter Datensatz, VI2, wird vom Qualys-Scanner für dieselbe Schwachstelle erstellt. Das Korrekturteam wendet die Patches an, die die VI1- und VI2-Datensätze lösen könnten. Wenn Sie den Qualys-Scan-Zeitplan über einen Tag hinaus konfigurieren, gibt Microsoft Defender bis zu diesem Zeitpunkt die Informationen zur behobenen Schwachstelle an, und VR schließt den VI1-Datensatz als „Geschlossen/behoben“.

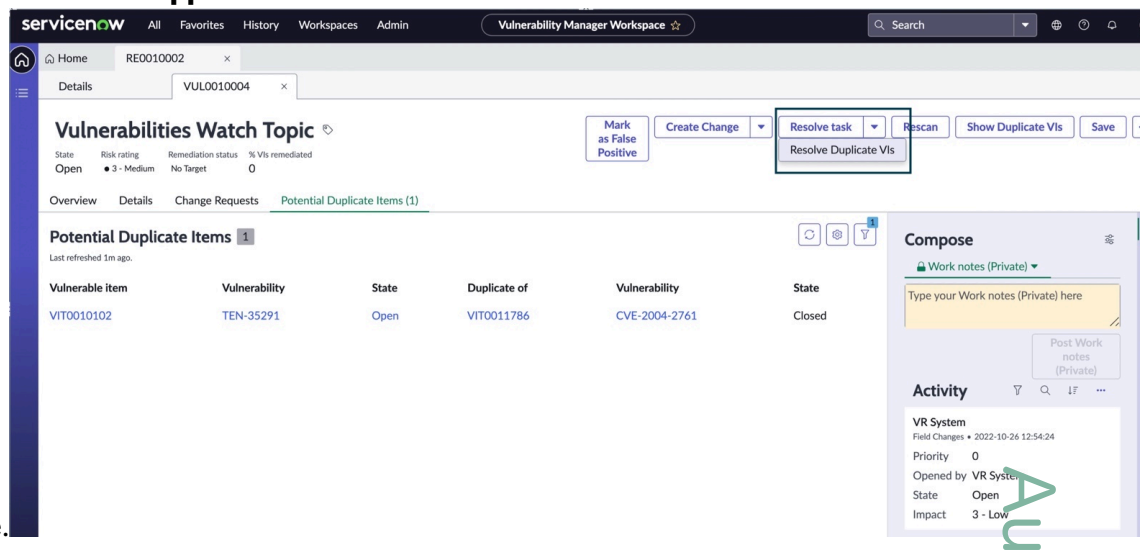
In diesem Szenario befindet sich der VI2-Datensatz noch im Status „Offen“, und VR wartet auf die Qualys-Scan-Ergebnisse. In dieser Situation bleiben VI-Datensätze vom zweiten Scanner im Status „Offen“, auch wenn der Patch angewendet wird und das VI vom anderen Scanner als behoben bestätigt wird.

Um diese Situation zu beheben, können Sie in Erwägung ziehen, den doppelten Schwachstellendatensatz basierend auf der Bedingung zu beheben, dass die Schwachstelle vom ersten Scanner geschlossen wird.

Beheben Sie Schwachstellen auf folgende Weise:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bei Bedarf: Wählen Sie aus **Doppelte VIS auflösen**UI-Aktion für die Korrekturaufgabe.



- Automatisiert: Aktivieren Sie die Systemeigenschaft `sn_vul.auto_resolve_duplicate_vit` Dient zum automatischen Lösen doppelter angreifbarer Elemente. Die tägliche geplante Aufgabe „Duplikate Vits bei Korrekturaufgabe aktualisieren und auflösen“ aktualisiert die doppelten Elemente automatisch.

Die doppelten VIS werden dann als gelöst markiert.

Hinweis:
Der Datensatz des gelösten Schwachstellenelements wird erneut geöffnet, wenn der Scanner ihn als identifiziert **Nicht Behoben** .

Erstellen und bearbeiten Sie eine Klassifizierungsgruppe

Erstellen Sie Gruppen, damit die zugrunde liegenden Regeln dieser Gruppe die Tabellendatensätze basierend auf den Bedingungen klassifizieren können. Die Regeln können verwendet werden, um ein beliebiges Feld in der entsprechenden Tabelle auszuwählen.

Vorbereitungen
Erforderliche Rolle: sn_vul.manage_classification_rule

Prozedur

1. Navigieren Sie zur Tabelle „Systemeigenschaften“.
2. In *`sn_sec_cmn.classificationTables`*Systemeigenschaft: Fügen Sie den Namen der Tabelle hinzu, für die Sie die Klassifizierungsgruppe erstellen möchten.
3. Erstellen Sie eine neue Business-Regel, indem Sie der Business-Regel in der in der Gruppe definierten Tabelle den folgenden Code-Fragment hinzufügen:
   ```
   VAR ClassificationCalc = New
   sn_vul.VulnerabilityCalculator(current,true,false,'sn_vul_classification_Group','sn_vul_classification_rule');
   classificationCalc.calculate();
   ```

   Hinweis:
   Geschäftsregeln werden bereitgestellt, um die Klassifizierung während der Erfassung für die Tabellen „erkannte Elemente“ und „Schwachstelleneintrag“ auszuführen. Für andere Tabellen müssen Sie die Business-Regeln hinzufügen, um die Klassifizierungsregeln bei der Erfassung zu haben.

4. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Klassifizierungsregeln**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie im Kontextmenü der Klassifizierungsgruppen auf **Neu** .
6. Füllen Sie im Formular die Felder aus.

Formular „Schwachstellenklassifizierungsgruppe“

Feld	Beschreibung
Name	Name der neuen Klassifizierungsgruppe.
Aktiv	Option zum Aktivieren der Gruppe.
Beschreibung	Beschreibung der neuen Klassifizierungsgruppe.
Tabelle	Tabelle, auf der die Regeln ausgeführt werden. **Hinweis:** Das Vulnerability Response-Basissystem enthält Klassifizierungsgruppen für erkannte Elemente und Schwachstellen.

Erstellen und bearbeiten Sie eine Klassifizierungsregel

Erstellen Sie Regeln, um die eingehenden Schwachstellen automatisch den richtigen Teams zur Behebung zuzuordnen.

Vorbereitungen
Erforderliche Rolle: sn_vul.manage_classification_rule

Warum und wann dieser Vorgang ausgeführt wird
Nach der Erstellung klassifizieren diese Regeln die Schwachstellen als Teil einer Plattform oder einer Anwendung. Sie können diese Regeln konfigurieren, um den Wert eines bestimmten Felds im Schwachstelleneintrag zu ersetzen.
Verwenden Sie diese Regeln, um die Berechnung vorgelagert in die Tabelle „Eintrag zu Schwachstellen von Drittparteien“ zu verschieben, um die Wiederverwendung von Inhalten zu ermöglichen.

Prozedur
1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Klassifizierungsregeln**an.
2. Um eine Klassifizierungsgruppe anzuzeigen, klicken Sie auf diese Gruppe.
3. Klicken Sie im Kontextmenü der Klassifizierungsregeln auf **Neu** .
4. Füllen Sie im Formular die Felder aus.

Formular „Schwachstellen-Klassifizierungsregel“

Feld	Beschreibung
Name	Name der neuen Klassifizierungsregel.
Aktiv	Option zum Aktivieren der Regel.
Beschreibung	Beschreibung der neuen Klassifizierungsregel.
Ausführungsreihenfolge	Reihenfolge, in der die Regel ausgeführt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erweiterte Ansicht	Option zum Anzeigen zusätzlicher Felder in den Abschnitten mit Registerkarten.
Wenn diese Bedingung erfüllt ist	
Bedingungstyp	Typ der Bedingung für die Regel. Die Auswahlmöglichkeiten lauten wie folgt: ○ **Filter** : Grundlegende Filterbedingungen zum Bestimmen, ob die Regel verwendet werden soll oder nicht. ○ **Filtergruppe** : Satz mehrerer Bedingungen, die zusammen verwendet werden. Die Regel wird basierend auf den in der Filtergruppe definierten Bedingungen ausgewertet. ○ **Skript** : Geskriptete Bedingung, die verwendet wird, um zu bestimmen, wann diese Regel angewendet werden soll. Dieses Feld wird nur angezeigt, wenn **Erweiterte Ansicht** Option ist ausgewählt.
Bedingung	Bedingung für die Regel. Definieren Sie Bedingungen basierend auf der Spalte, die in der Spalte „erforderlicher Schwachstelleneintrag“ ausgewählt ist. Sie können mehrere Bedingungen hinzufügen, um die Regel zu verfeinern. Dieses Feld wird nur angezeigt, wenn **Filter** Ist aus ausgewählt **Bedingungstyp** Feld. **Hinweis:** Wenn Sie mehrere Bedingungen oder Vorlagen definieren, können Sie nur aus einer übergeordneten und einer untergeordneten Tabelle auswählen. Sie können nicht aus zwei oder mehr untergeordneten Tabellen auswählen.
Filtergruppe	Gruppe von Filtern. Die Gruppe wird definiert, wenn eine Reihe von Bedingungen wiederholt an mehreren Orten verwendet wird. Klicken Sie auf die Suche mithilfe des Listensymbols ( ), um die Filtergruppe auszuwählen. Weitere Informationen finden Sie unter Erstellen und definieren Sie Filtergruppen in Security Operations . Dieses Feld wird nur angezeigt, wenn **Filtergruppe** Ist aus ausgewählt **Bedingungstyp** Feld.
Skript	Skript, das ausgewertet wird, um zu bestimmen, wann diese Regel angewendet werden soll. Sie können Ihren Code schreiben und die Antwort auf „wahr“ oder „falsch“ festlegen. Dieses Feld wird nur angezeigt, wenn **Skript** Ist aus ausgewählt **Bedingungstyp** Feld

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Diese Werte festlegen	
Klassifizierung	Klassifizierung der Regel. Um eine Option auszuwählen, klicken Sie auf das Glühlensymbol ( ). In der Liste werden die Optionen für Plattform und Anwendung angezeigt. Alternativ können Sie Ihre eigene Klassifizierung eingeben, die nicht in der Liste enthalten ist.
Klassifizierungstyp	Typ der Klassifizierung. Dieses Feld zeigt die gefilterte Liste der Klassifizierungstypen basierend auf Ihrem ausgewählten Wert für an **Klassifizierung** Feld.
Werttyp	Typ des Werts, der mithilfe dieser Regel zugewiesen wird. Die Auswahlmöglichkeiten lauten wie folgt: ○ **Vorlage**: Wählen Sie eine Vorlage. Sie können eine erforderliche Vorlage verwenden. ○ **Skript** : Wählen Sie ein bereits vorhandenes Skript aus, oder schreiben Sie Ihr eigenes anwenderdefiniertes Skript. Dieses Feld wird nur angezeigt, wenn **Erweiterte Ansicht** Option ist ausgewählt.
Vorlage	Eine andere Bedingung für die Regel außer **Klassifizierung** Und **Klassifizierungstyp** Felder. Wählen Sie eine Kombination aus Feldern und Werten aus, die Sie festlegen möchten, wenn die Regel ausgewertet wird. Dieses Feld wird nur angezeigt, wenn **Vorlage** Ist aus ausgewählt **Werttyp** Feld.
Skriptwert	Skript zum Festlegen von Werten für den aktuellen Datensatz. Dieses Feld definiert, welche Werte für die Felder in Schwachstelleneinträgen festgelegt werden sollen. Dieses Feld wird nur angezeigt, wenn **Skript** Ist aus ausgewählt **Werttyp** Feld.

5. Klicken Sie auf, um die neue Regel zu erstellen **Übermitteln** .

Example:
Verwenden Sie VR-Klassifizierungsregeln, um die Logik zu vorgelagerten Tabellen wie Schwachstelle und erkannte Elemente hinzuzufügen und zu berechnen. Sie können die Ausgabe mehrmals wiederverwenden, wodurch die Leistung von Regeln wie Zuweisungsregeln verbessert wird. Klassifizieren Sie beispielsweise den Drittpartei-Eintrag (TPE) als Java, und verwenden Sie die Ausgabe in den Zuweisungsregeln mehrmals. Beispiel für Zuweisungsregel:

```
VI.TPE.Classfication Type
        | IS | Java
```

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenden Sie eine Regel auf eine vorhandene Schwachstelle an

Wenn Sie eine Klassifizierungsregel ändern, führen Sie alle aktiven Regeln für alle Schwachstelleneinträge erneut aus. Sie können die vorhandenen Schwachstellen auch nachrüsten, indem Sie die neu erstellten Klassifizierungsregeln auf die vorhandenen Schwachstellen anwenden.

Vorbereitungen

Erforderliche Rolle: sn_vul.manage_classification_rule

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Schwachstellenklassifizierungsregeln**an.
2. Um eine Regel auszuwählen, aktivieren Sie das Kontrollkästchen neben der Regel.
3. Klicken Sie auf **Apply Changes (Änderungen übernehmen)**.
4. Klicken Sie Auf **Erneut Anwenden** .

Deaktivieren oder löschen Sie eine Klassifizierungsregel

Deaktivieren oder löschen Sie eine Klassifizierungsregel, wenn sie nicht mehr benötigt oder relevant ist.

Vorbereitungen

Erforderliche Rolle: sn_vul.manage_classification_rule

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Klassifizierungsregel deaktiviert oder gelöscht wird, die Daten, die in ausgefüllt wurden **Klassifizierung** Und **Classification_type** Felder der gelöschten Regel verbleiben in ihren jeweiligen Tabellen.

Wenn Sie diese Daten löschen möchten, erstellen Sie im eine Regel mit leeren Werten **Klassifizierung** Und **Classification_type** Felder und wenden Sie die Gruppe erneut an. Sobald diese neue Regel erneut angewendet wird, werden die Änderungen auf allen Datensätzen berücksichtigt, für die diese Regel gilt, basierend auf den Bedingungen der Regel.

Ab v24.0.6 von Vulnerability Response, Wenn eine Klassifizierungsregel gelöscht oder deaktiviert wird, wird sie nicht mehr auf das erkannte Element oder den Schwachstelleneintrag und die Daten in angewendet **Klassifizierung** Und **Classification_type** Felder werden gelöscht.

Prozedur

1. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Schwachstellenklassifizierungsregeln**an.
2. Um die Regel auszuwählen, die Sie löschen möchten, klicken Sie auf das Kontrollkästchen neben der Regel.
3. Um die Regel zu löschen, führen Sie einen der folgenden Schritte aus:
   - Klicken Sie in der Liste Aktion für ausgewählte Zeilen auf **Löschen** .
   - Wählen Sie die Regel aus, und klicken Sie auf **Löschen** Schaltfläche.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Apply Changes (Änderungen übernehmen)**.

Hinweis:
Wenn Sie nicht auf diese Schaltfläche klicken, befindet sich die Regel weiterhin im System. Schwachstellen, auf die von der Regel verwiesen wird, verweisen weiterhin auf sie.

Erstellen Sie eine Ausschlussregel

Erstellen Sie eine Regel, um die Konvertierung von Erkennungen in angreifbare Elemente (Vits) während der Erfassung zu filtern oder auszuschließen.

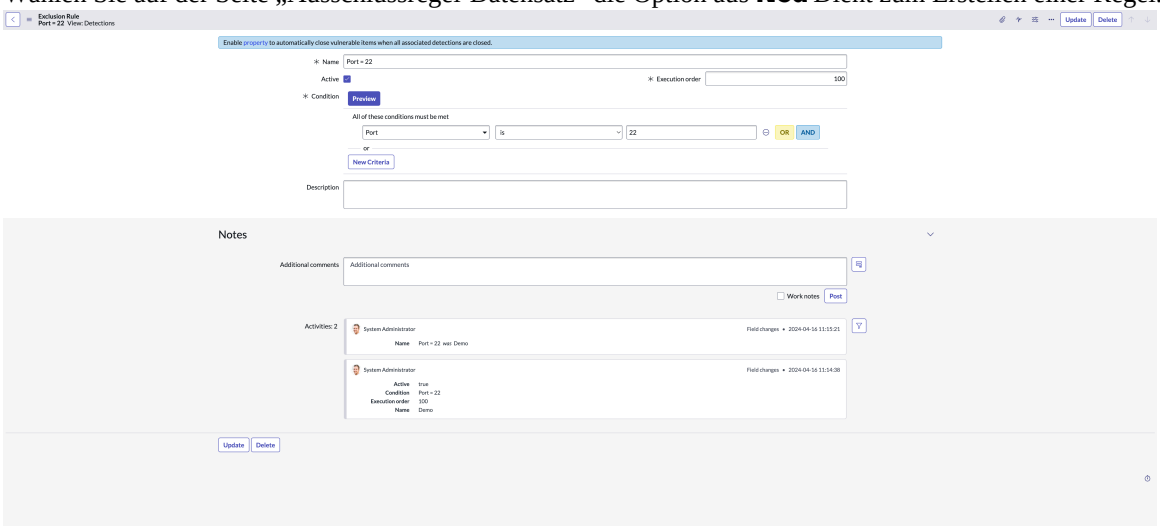
Vorbereitungen

Erforderliche Rolle: Schwachstellenadministrator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Ausschlussregeln**an.
2. Wählen Sie auf der Seite „Ausschlussregel-Datensatz“ die Option aus **Neu** Dient zum Erstellen einer Regel.



Die Meldung „Eigenschaft aktivieren, um angreifbare Elemente automatisch zu schließen, wenn alle zugehörigen Erkennungen geschlossen sind“ wird angezeigt. Standardmäßig ist die Eigenschaft inaktiv. Wählen Sie zum Aktivieren den Eigenschaftslink aus, und geben Sie den Wert als „wahr“ in ein **Wert** Feld.

3. Füllen Sie im Formular die Felder aus.

Formular „Ausschlussregel“

Feld	Beschreibung
Name	Name der Ausschlussregel.
Aktiv	Option zum Aktivieren der Ausschlussregel.
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausschlussregel.
Bedingung	Filterbedingungen für die Erkennungen, die während der Verarbeitung definiert werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Sie können keine Ausschlussregel oder Feldbedingungen für Schwachstellenelement auswählen.
Beschreibung	Beschreibung der Ausschlussregel.

4. Wählen Sie **Absenden**.
   Die Aktivität wird im System aufgezeichnet.

Hinweis:
Sobald eine Ausschlussregel erstellt wurde, wird sie ab der nachfolgenden Erfassung auf Erkennungen wirksam.

Change-Management Aufgaben für Vulnerability Response

Erstellen Sie von Korrekturaufgaben (RTS) aus Change-Anforderungen, ordnen Sie RTS vorhandenen Change-Anforderungen zu, oder teilen Sie Korrekturaufgaben in neue Aufgaben mit Teilmengen angreifbarer Elemente (VI) auf.

Erstellen und verwalten Sie Change-Anforderungen direkt aus einer Korrekturaufgabe, wenn ein manueller und kontrollierter Prozess jeglicher Art zum Ändern oder Entfernen unterstützter Konfigurationselemente (CIs) in Ihrer CMDB erforderlich ist. Durch das Erstellen und Verwalten von Change-Anforderungen direkt aus einem Datensatz können Sie Schwachstellen schnell untersuchen und beheben.

Siehe Change-Management für Vulnerability Response Für einen Überblick über die Funktionsweise des Change-Managements mit Vulnerability Response Anwendung und Systemanforderungen.

In den folgenden Themen erfahren Sie, wie Sie Change-Anforderungen erstellen, Korrekturaufgaben vorhandenen Change-Anforderungen zuordnen und Korrekturaufgaben aufteilen. Siehe Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben Informationen dazu, wie Statusfelder in Change-Anforderungen (CHG) automatisch Korrekturaufgaben lösen.

Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe

Erstellen Sie als IT-Korrekturbesitzer eine Change-Anforderung (CHG) direkt aus einer Korrekturaufgabe (VUL) für alle angreifbaren Elemente in der Gruppe. Erstellen Sie eine Change-Anforderung mit vorab ausgefüllten Informationen, die die bevorzugte Lösung enthalten, um Ihre Untersuchung auf Schwachstellen zu beschleunigen, die manuelles Eingreifen erfordern.

Vorbereitungen

Erforderliche Rollen: Zum Erstellen einer Change-Anforderung: Jeder Anwender mit der Rolle itil. Die Rolle „sn_vul.Remediation_owner“ wird ebenfalls automatisch zugewiesen, wenn die Rolle „itil“ einem Anwender zugewiesen wird.

Erforderliche Rolle: Zur Genehmigung von Change-Anforderungen: Anwender mit den Rollen itil, admin, sn_Change_write, Change_Manager.

Warum und wann dieser Vorgang ausgeführt wird

Informationen zum Erstellen einer Change-Anforderung aus dem Vulnerability Response Arbeitsbereiche, siehe Erstellen Sie eine Change-Anforderung in Arbeitsbereich für IT-Korrekturen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

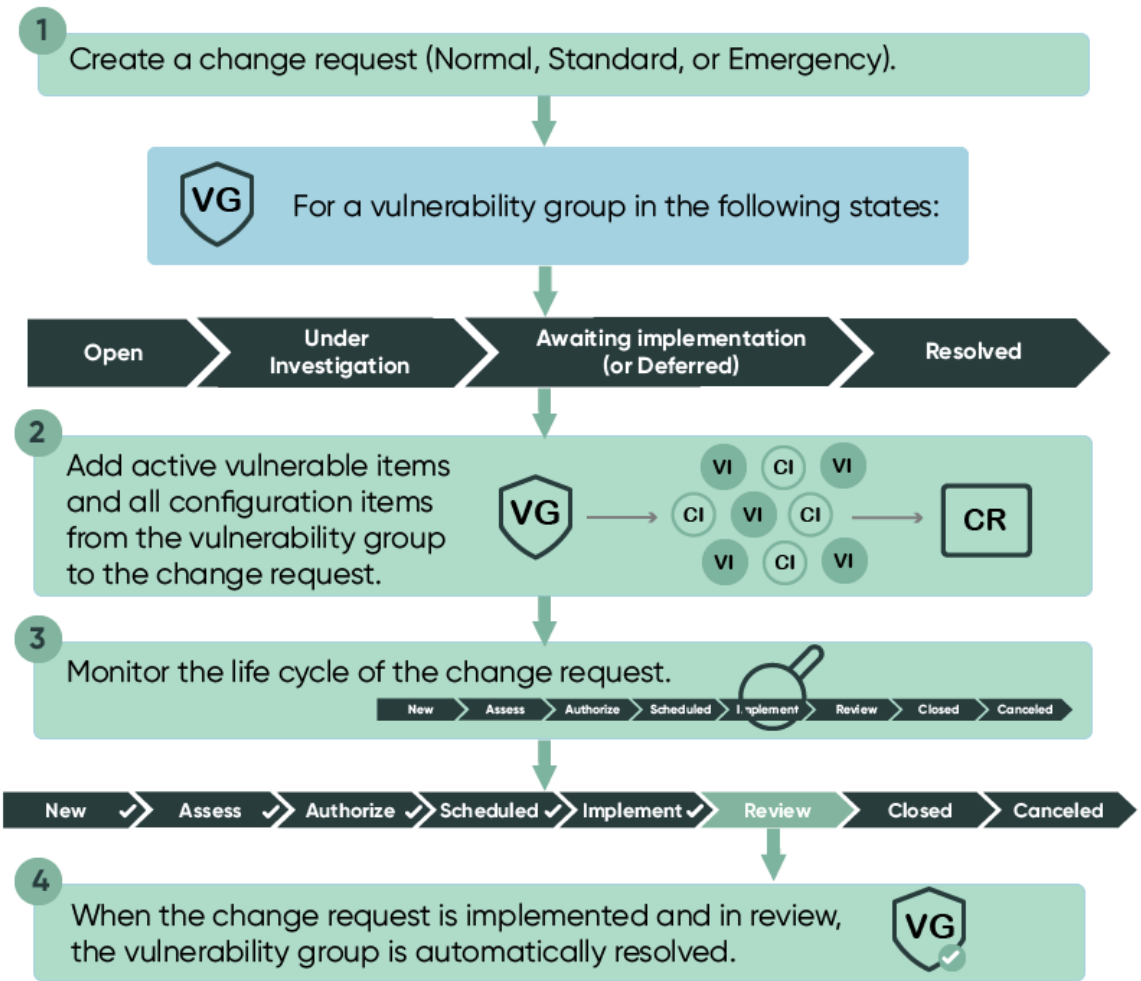
Um eine Change-Anforderung aus der klassischen Umgebung zu erstellen, führen Sie die unten aufgeführten Schritte aus.

Sie können Change-Anforderungen direkt aus einer Korrekturaufgabe erstellen, genehmigen, implementieren, überprüfen und schließen. Sie können drei Arten von Change-Anforderungen mit vorab ausgefüllten Informationen aus einer Korrekturaufgabe erstellen:

- Standard. Ein vorautorisierter Change, der ein geringes Risiko aufweist, relativ häufig ist und einem bestimmten Verfahren oder einer bestimmten Arbeitsanweisung folgt.
- Normal. Normale Change-Anforderungen folgen einem verbindlichen Prozess, der zwei Genehmigungsebenen erfordert, bevor sie implementiert, überprüft und geschlossen werden.
- Notfall. Ein Change zur Lösung eines schwerwiegenden Incident.

Die folgende Abbildung zeigt den grundlegenden Flow zum Erstellen einer Change-Anforderung aus einer ANGREIFBAREN Korrekturaufgabe. Die detaillierten Schritte für diesen Flow folgen dem Bild.

Der Korrekturaufgabendatensatz wird in den folgenden Abschnitten als UNGÜLTIG bezeichnet. In vorherigen Versionen von Vulnerability Response, Korrekturaufgaben wurden aufgerufen, Schwachstellen-Gruppen (VG) In den folgenden Bildern VG= Korrekturaufgabe oder ein ANGREIFBARER Datensatz.



Hinweis:

Wichtige Punkte zum Erstellen neuer Change-Anforderungen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie können neue Change-Anforderungen für jede Korrekturaufgabe (VUL) in einem anderen Status als erstellen Geschlossen .
- Stellen Sie sicher, dass Sie einen Genehmiger für andere Change-Anforderungen als „Standard“ (vorab genehmigt) haben, den Sie erstellen oder einer ÄNDERUNG zuordnen. Dadurch wird das Verschieben der ANGREIFBAREN Lösung beschleunigt. Weitere Informationen zum Hinzufügen von Anwendern finden Sie unter Fügen Sie der Vulnerability Response-Gruppe Anwender hinzu.
- Bevor eine Korrekturaufgabe gelöst werden kann, müssen alle Aufgaben für mindestens ein CHG abgeschlossen werden, das der ABLEHNUNG zugeordnet ist, damit die Change-Anforderung implementiert und in verschoben werden kann Überprüfen status.

Prozedur

1. Um eine vollständige Change-Anforderung aus einem vorhandenen Korrekturaufgabendatensatz zu erstellen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**an.
   Die Liste der Korrekturaufgaben, die Ihrer Zuweisungsgruppe zugewiesen sind, wird angezeigt.
2. **Wahlweise:** Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturübersicht** Um das Dashboard „Korrekturübersicht“ anzuzeigen und eine Ihnen oder Ihrer Zuweisungsgruppe zugewiesene ANFECHTBARE Person zu suchen.
3. Alternativ können Sie in der Spalte Nummer auf eine Korrekturaufgabe klicken, um den Datensatz zu öffnen und die Details anzuzeigen.
   Der Datensatz wird angezeigt.
4. Klicken Sie oben rechts im Datensatz auf den Datensatz, für den Sie die Change-Anforderung erstellen möchten **Erstellen Sie Einen Change** .
   Das Formular Change-Anforderung erstellen wird angezeigt.
5. Füllen Sie die Felder aus.

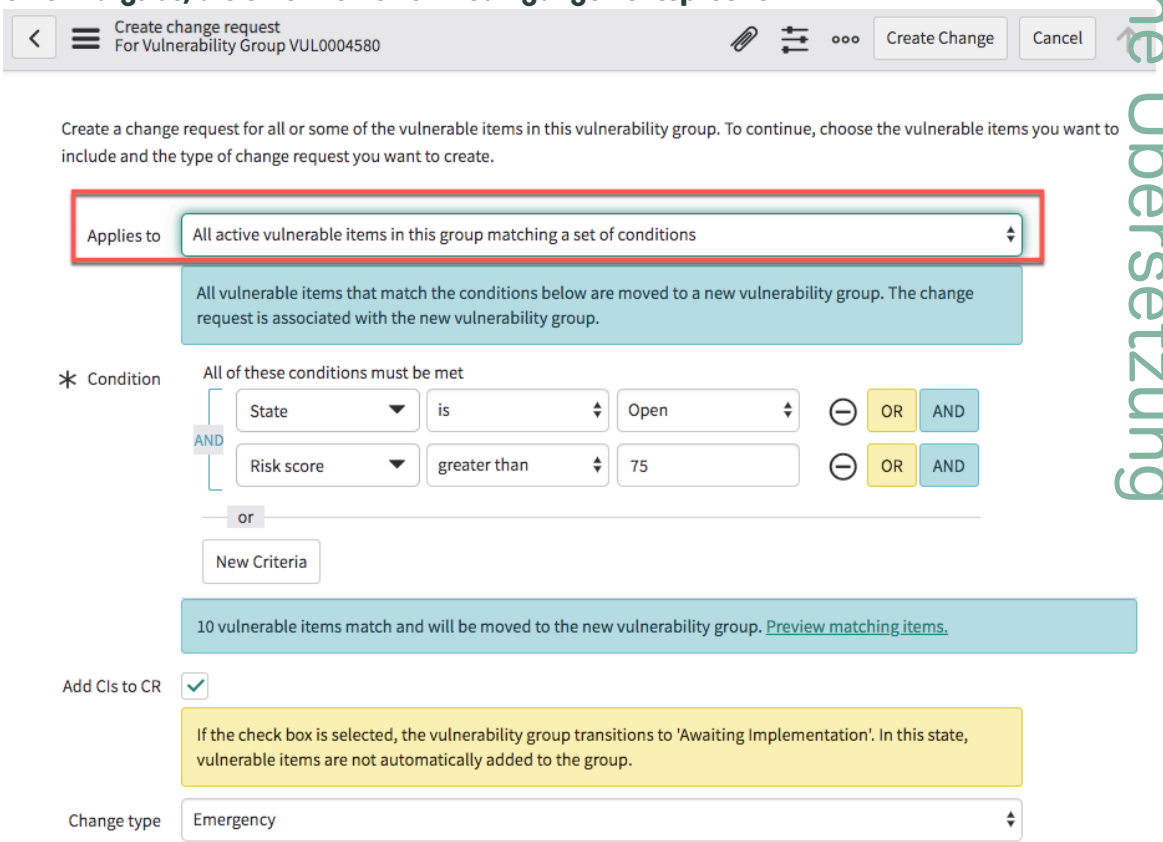
   a. Wählen Sie in der Auswahlliste des Felds „gilt für“ eine aus, um fortzufahren.

Option	Beschreibung
Alle aktiven angreifbaren Elemente in dieser Gruppe	Wenn diese Option ausgewählt ist, werden alle aktiven angreifbaren Elemente aus dieser Korrekturaufgabe mit einem anderen Status als „Geschlossen“ automatisch der Change-Anforderung hinzugefügt, nachdem Sie auf geklickt haben **Erstellen Sie Einen Change** .
Alle angreifbaren Elemente in dieser Gruppe, die einer Reihe von Bedingungen entsprechen	Wenn diese Option ausgewählt ist, wird der Bedingungsgenerator wie in der zweiten Abbildung unten angezeigt. Geben Sie Filterkriterien ein, um die angreifbaren Elemente zu identifizieren, die Sie für die neue Change-Anforderung benötigen. Ein Beispiel für einen Filter kann nur angreifbare Elemente enthalten, die bestimmten Suchkriterien entsprechen: **Status Ist Öffnen** Und **Risikopunktzahl Größer als 75** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Nachdem Sie Ihre Bedingungen eingegeben haben, wird eine Nachricht mit der Anzahl der VIS angezeigt, die Ihren Kriterien entsprechen (10). Ein Link (**Vorschau auf übereinstimmende Elemente anzeigen**), um eine Vorschau der übereinstimmenden Elemente anzuzeigen. Wenn keine Elemente Ihren Filterbedingungen entsprechen, wird unter dem Bedingungsgenerator eine Meldung angezeigt, die Sie anweist, Ihren Filter anzupassen. Nachdem Sie auf geklickt haben **Erstellen Sie Einen Change** , Alle angreifbaren Elemente, die diesem Bedingungsfilter entsprechen, werden in eine neue Korrekturaufgabe verschoben. Diese Change-Anforderung ist der neuen Korrekturaufgabe zugeordnet.

Erstellen Sie ein Change-Anforderungsformular für angreifbare Elemente in einer Aufgabe, die einer Reihe von Bedingungen entsprechen



b. Wahlweise: Wenn im Formular angezeigt, klicken Sie auf **Vorschau auf übereinstimmende Elemente anzeigen** Link für eine Liste der VIS, die Ihren Filterkriterien entsprechen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Vorschau der Korrekturaufgabenliste wird angezeigt. Sie können Elemente in dieser Vorschauliste auswählen und UI-Aktionen für sie ausführen. Diese Aktionen werden jedoch auch für die VUL ausgeführt. Wenn Sie beispielsweise ein VI aus der Vorschauliste löschen, wird dieses VI auch aus dem VUL gelöscht.

c. Nachdem Sie Ihre Vorschau abgeschlossen haben, schließen Sie das Browserfenster, um das Change-Anforderungsformular zurückzugeben.

d. Wählen Sie für das Kontrollkästchen CIs zu CR hinzufügen eine aus, um fortzufahren.

Option	Beschreibung
Kontrollkästchen „CIs zu CR hinzufügen“ aktiviert	Standard ist ausgewählt. Wenn das Kontrollkästchen aktiviert ist, werden alle Konfigurationselemente (Configuration Items, CI), die zu aktiven angreifbaren Elementen in dieser Korrekturaufgabe gehören, dieser Change-Anforderung hinzugefügt. Der Wert „UNGÜLTIG“ wird automatisch in verschoben Warten Auf Implementierung status.
Kontrollkästchen „CIs zu CR hinzufügen“ deaktiviert	Deaktivieren Sie das Kontrollkästchen, wenn die CIs aus den aktiven angreifbaren Elementen aus dieser Korrekturaufgabe nicht der neuen Change-Anforderung hinzugefügt werden sollen. Wenn diese Option deaktiviert ist, wird der Status der Change-Anforderung nicht mit dem Status „UNGÜLTIG“ synchronisiert, und der Status „UNGÜLTIG“ bleibt im aktuellen Status.

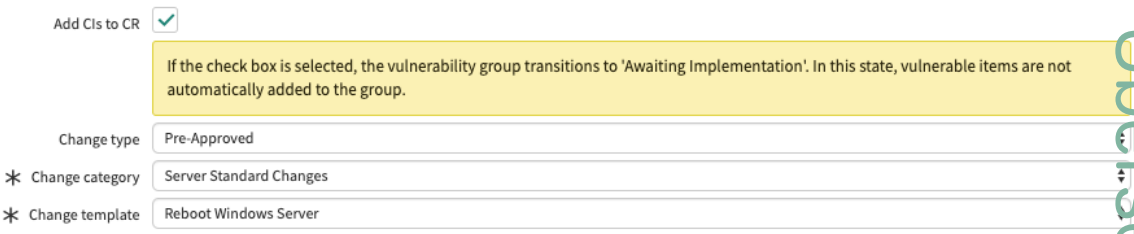
e. Wählen Sie in der Auswahlliste für das Feld Change-Typ einen aus, um fortzufahren.

Änderungstyp	Beschreibung
Notfall	Ein Change zur Lösung eines schwerwiegenden Incident.
Normal	Ein Change-Typ, der verwendet wird, um Changes an einem Service zu implementieren, bei denen es sich nicht um einen Standard- oder Notfall-Change handelt.
Standard	Eine vorautorisierte Change-Anforderung mit geringem Risiko, die häufig implementiert wird. Genehmigte Standard-Change-Anforderungen können in einem Vorlagenkatalog vordefiniert werden, um den Zugriff auf und die Anfrage eines Standard-Changes effizienter zu gestalten. Wenn diese Option ausgewählt ist, werden zwei Felder angezeigt, wie in der folgenden Abbildung gezeigt. Wählen Sie in jeder Auswahlliste eines aus, um diese Felder auszufüllen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Änderungstyp	Beschreibung
	▪ Change-Kategorie: Wählen Sie eine Kategorie für den Change aus Ihrem vorhandenen Katalog aus, z. B. Hardware , Server-Standard-Changes , Software . In diesem Beispiel Standard-Changes Werden Gepatcht Ist ausgewählt. ▪ Change-Vorlage: Wählen Sie eine verfügbare Vorlage für Change-Anforderungen mit vordefinierten Unterstützungsaufgaben aus Ihrem Katalog aus. In diesem Beispiel ist Monatlicher Microsoft-Patching-Zyklus Vorlage ist ausgewählt. Weitere Informationen zu ITSM Change-Anforderungskategorien, Vorlagen und Change-Typen finden Sie unter Change-Typen .

Die Funktion liest automatisch die Arten von Change-Anforderungen, die Sie in Ihrem Katalog in ITSM Change-Management eingerichtet haben. Wenn Sie beispielsweise den Namen für Ihre Standard-Change-Anforderungen in ITSM von ändern Standard Bis Vorab genehmigt , Ihr neuer Name wird automatisch in der Auswahlliste Change-Typ auf Change-Anforderung erstellen aus angezeigt, wie in der folgenden Abbildung gezeigt.



Die Felder im Abschnitt „Change-Anforderungsvorschau“ des Formulars sind vorab mit Informationen aus dem VUL ausgefüllt. Bei Bedarf können diese Feldwerte bearbeitet werden. Überprüfen Sie beispielsweise die Werte in den Feldern in der folgenden Abbildung:

Geplantes Enddatum

Dieses Datum (10. 2019) Ist derselbe Wert, der im Feld „Korrekturzieldatum“ des WIDERSPRUCHS angezeigt wird. Dieser Wert wird vom frühesten Korrekturzieldatum aus den angreifbaren Elementen abgeleitet, die zu der angreifbaren Elemente gehören. Wenn Sie eine Change-Anforderung für ein kritisches Problem erstellen, das ein früheres Korrekturdatum erfordert, können Sie diesen Wert und den Wert im Feld Priorität bearbeiten.

Begründung

Dieses Feld zeigt die Anzahl der CIs an, die dem CHG hinzugefügt werden. Wenn Sie zusätzliche Informationen hinzufügen möchten, möchten Sie diesen Text möglicherweise bearbeiten. Beispielsweise möchten Sie in diesem Feld eine Notiz zu dem Filter hinzufügen, den Sie zum Erstellen der neuen ÄNDERUNG verwendet haben, z. B. Risikopunktzahl größer als 75 . Dieser Text kann Ihnen helfen, Ihre neue Change-Anforderung und Korrekturaufgabe zu finden.

Implementierungsplan

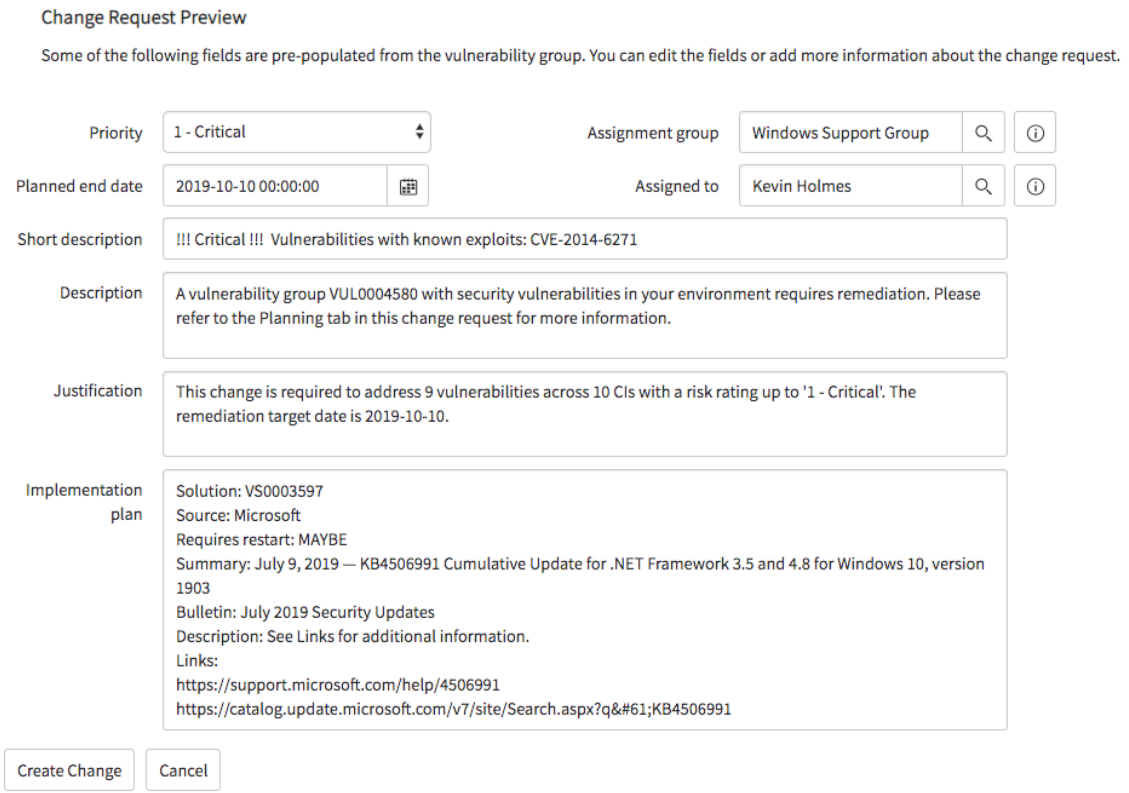
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

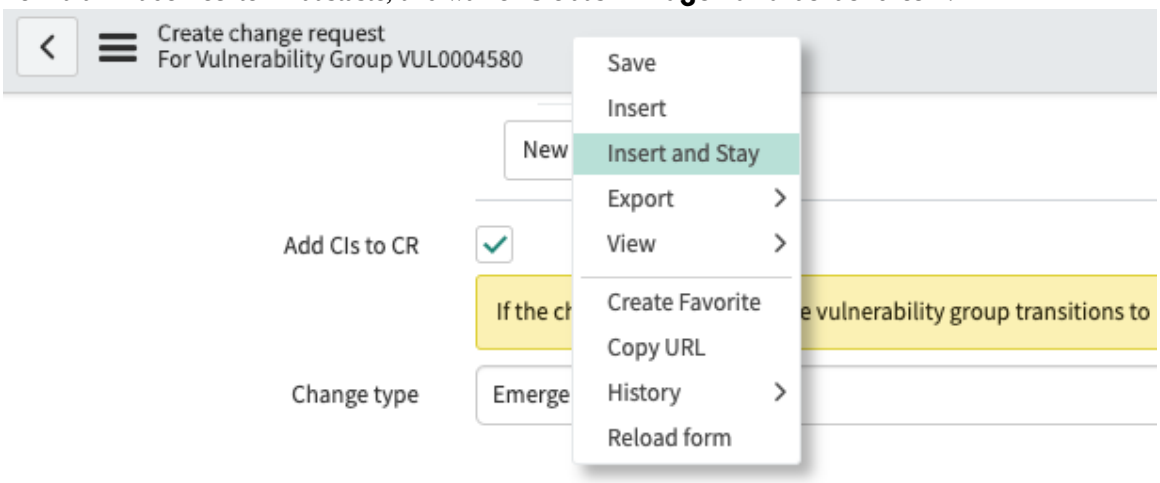
In diesem Feld wird die bevorzugte Lösung für die Schwachstelle angezeigt.

Zuweisungsgruppe und Zugewiesen an

Bearbeiten Sie diese Felder, um die Zuweisungsgruppe zu ändern oder diese Change-Anforderung einem Anwender in einer Ihrer Zuweisungsgruppen neu zuzuweisen.



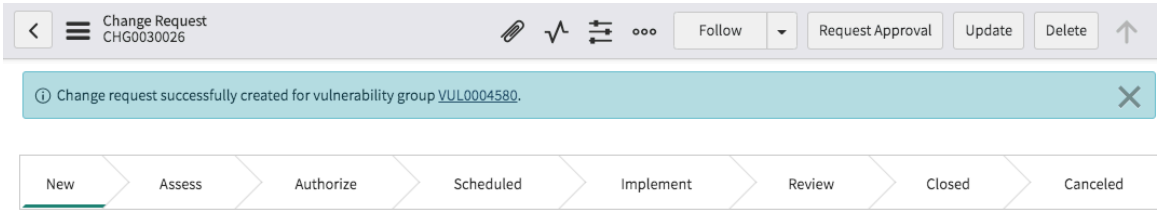
6. Fahren Sie mit der Vorschau der Felder fort, und bearbeiten Sie sie nach Bedarf.
7. Um Ihre Änderungen zu speichern und auf dieser Seite zu bleiben, klicken Sie im grauen Banner oben im Formular mit der rechten Maustaste, und wählen Sie aus **Einfügen und beibehalten** .



8. Nachdem Sie Ihre Änderungen abgeschlossen haben, wählen Sie eine aus, um fortzufahren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

Für eine Korrekturaufgabe in Öffnen status mit den Feldern Zuweisungsgruppe und Zugewiesen an nicht zugewiesen (leer) wird der aktuell angemeldete Anwender automatisch der Aufgabe zugewiesen, nachdem Sie auf geklickt haben **Erstellen Sie Einen Change** . Darüber hinaus muss das Kontrollkästchen CIs zu CR hinzufügen aktiviert sein. Oben auf der ABLEHNUNG wird eine blaue Bestätigungsnachricht angezeigt, die diese Zuweisung anzeigt.

Nächste Maßnahme

Überwachen Sie die Change-Anforderung und die Change-Aufgaben, um sicherzustellen, dass sie abgeschlossen sind und die Change-Anforderung implementiert ist. Nachdem dieses CHG implementiert und in verschoben wurde Überprüfen status: Wenn die Statussynchronisierung aktiviert ist, wird der STATUS „UNGÜLTIG“ automatisch in verschoben Gelöst . Weitere Informationen zur Statussynchronisierung finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu

Vermeiden Sie als IT-Korrekturbesitzer die Erstellung doppelter Change-Anforderungen (CHG), wenn Sie an der Lösung Ihrer Korrekturaufgaben arbeiten, indem Sie einer Change-Anforderung, die bereits in Ihrer Instanz verfügbar ist, eine Korrekturaufgabe (VUL) zuordnen.

Vorbereitungen

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: Jeder Anwender mit der Rolle itil. Die Rolle sn_vul.Remediation_owner wird auch automatisch einem Anwender zugewiesen, wenn die Rolle itil zugewiesen wird.

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Zuordnen einer Korrekturaufgabe zu einer vorhandenen Change-Anforderung finden Sie unter Erstellen Sie eine Change-Anforderung in Arbeitsbereich für IT-Korrekturen.

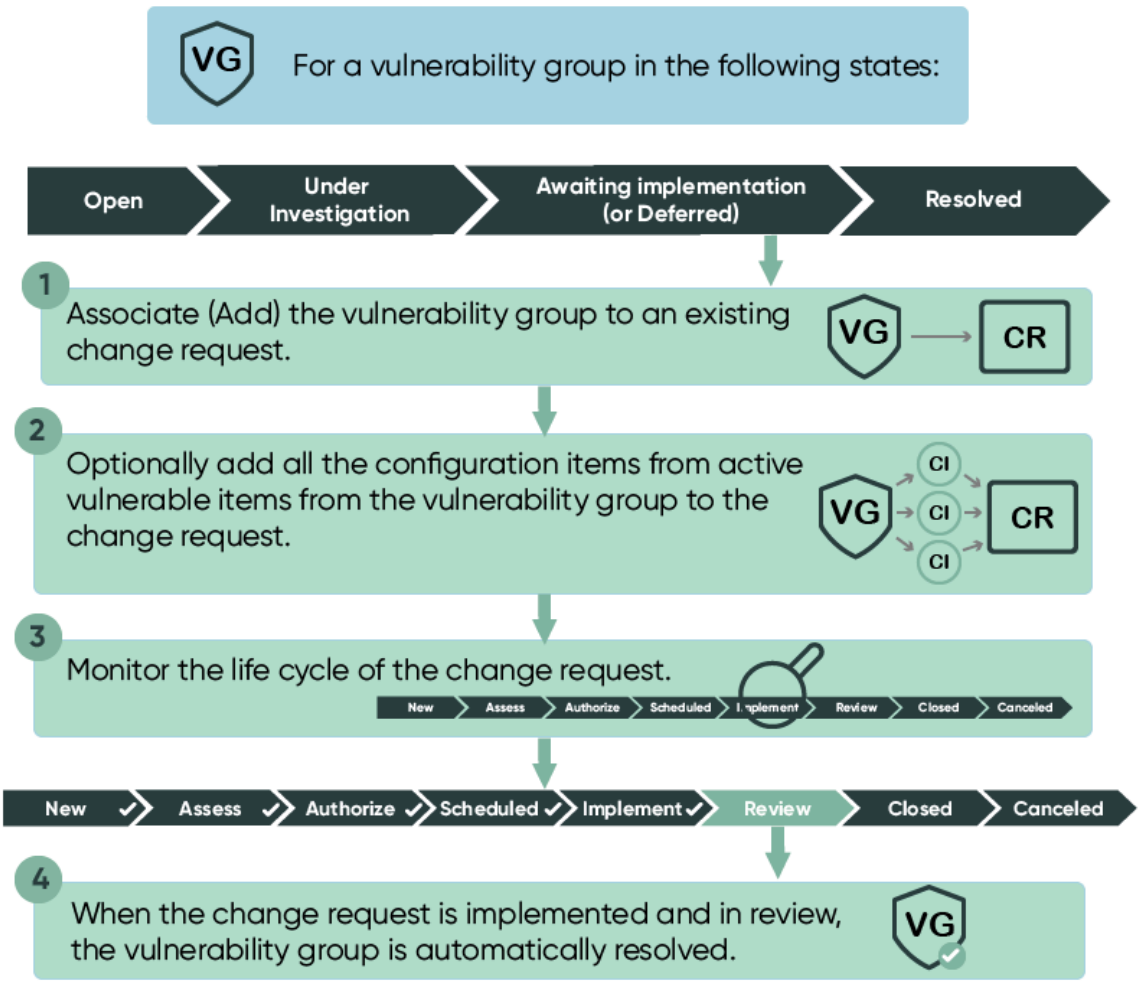
Der Korrekturaufgabendatensatz wird in den folgenden Abschnitten als UNGÜLTIG bezeichnet. In vorherigen Versionen von Vulnerability Response, Korrekturaufgaben wurden aufgerufen, Schwachstellen-Gruppen (VG). In den folgenden Bildern VG= Korrekturaufgabe oder ein ANGREIFBARER Datensatz.

Weitere Informationen zum Zuordnen einer Korrekturaufgabe zu einer vorhandenen Change-Anforderung finden Sie unter Erstellen Sie eine Change-Anforderung in Arbeitsbereich für IT-Korrekturen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Korrekturbesitzer können Sie Korrekturaufgaben, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen sind, vorhandenen Change-Anforderungen direkt aus den Korrekturaufgaben-Datensätzen zuordnen. Die folgende Abbildung zeigt den grundlegenden Flow zum Zuordnen einer Change-Anforderung zu einer vorhandenen ANGREIFBAREN Person (VG). Die detaillierten Schritte für diesen Flow folgen dem Bild.

Workflow zum Zuordnen einer Korrekturaufgabe zu einer vorhandenen Change-Anforderung



Hinweis:

Sie können eine vorhandene Change-Anforderung einem WIDERRUF in einem beliebigen Status zuordnen (Offen, wird untersucht, wartet auf Implementierung, Geschlossen und zurückgestellt). Wenn Sie eine Change-Anforderung einer vorhandenen ANGREIFBAREN Person zuordnen, werden der Change-Anforderung nur die aktiven VIS hinzugefügt.

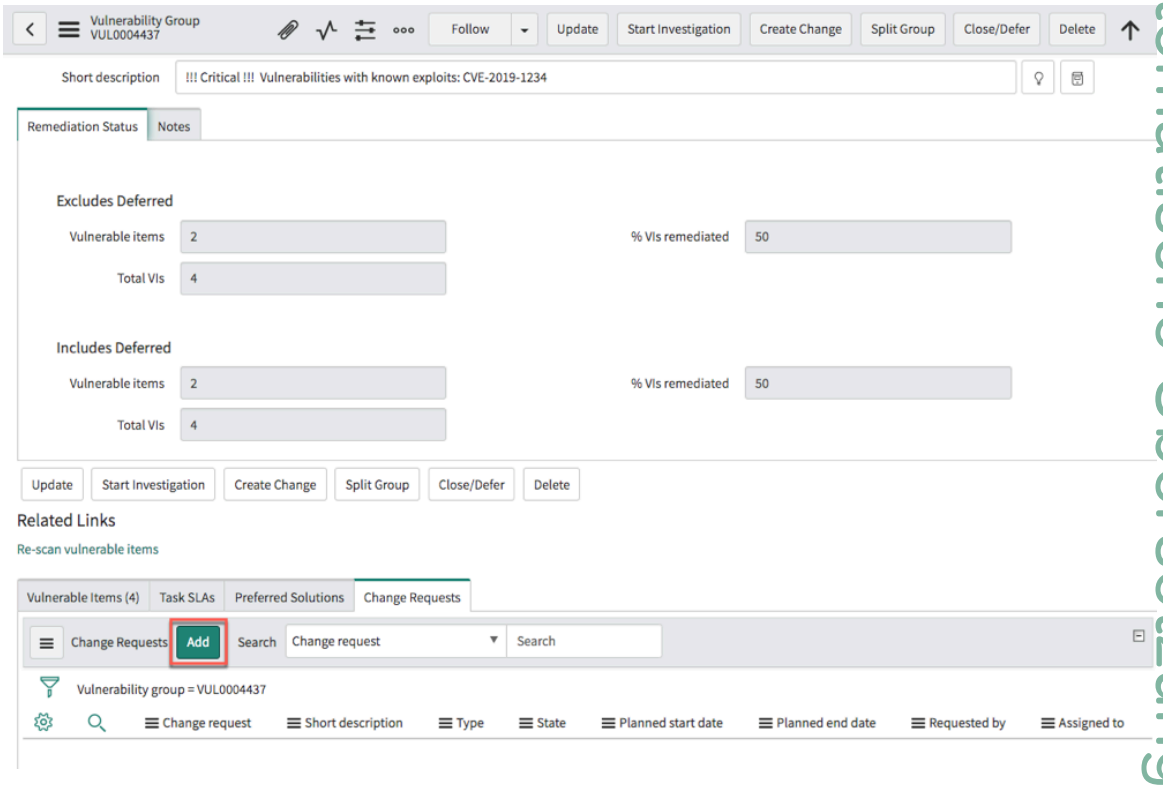
Um zu vermeiden, dass doppelte Change-Anforderungen erstellt werden, sollten Sie zunächst alle vorhandenen Change-Anforderungen anzeigen, die bereits einer ANGREIFBAREN Person zugeordnet sind. Informationen zum einfachen Nachverfolgen der Anzahl der Change-Anforderungen, die sich auf eine bestimmte ANFECHTUNG beziehen, finden Sie in der Spalte CR-Anzahl in der Liste „Korrekturaufgaben“. Wenn nicht angezeigt, klicken Sie auf das Einstellungssymbol ( ) Oben rechts. Verschieben Sie die Spalte „CR-Anzahl“ von „verfügbar“ in „ausgewählt“, und klicken Sie auf **OK** .

Um die neue Spalte automatisch auszufüllen, führen Sie für Kunden mit vorhandenen Daten in dieser Tabelle die geplante Aufgabe aus: Füllen Sie die neue Spalte „CR-Anzahl“ aus .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

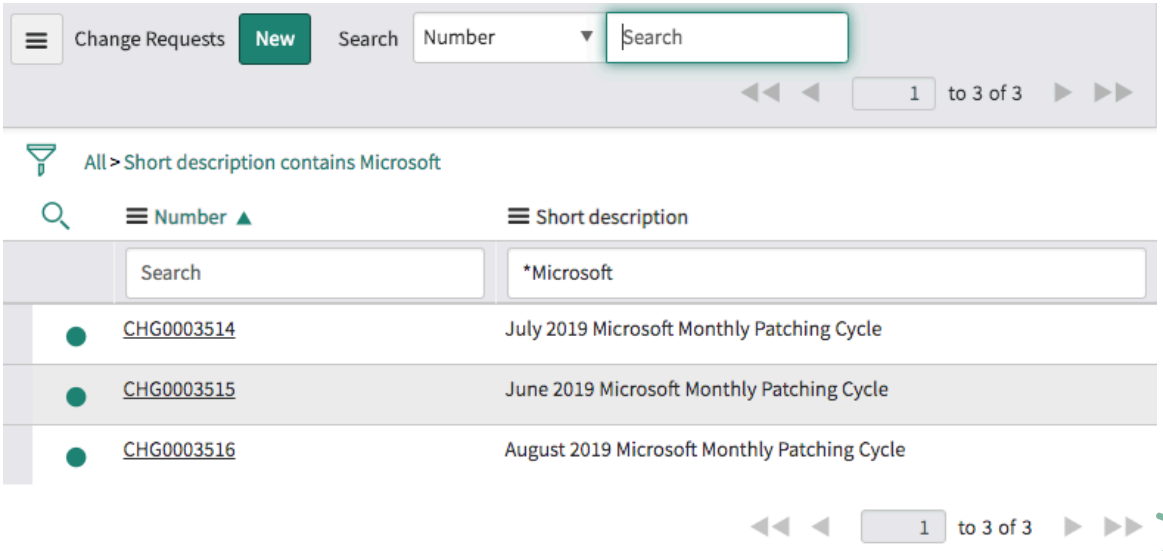
1. Um eine Korrekturaufgabe einer vorhandenen Change-Anforderung zuzuordnen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**an.
2. Suchen Sie die Korrekturaufgabe, mit der Sie arbeiten.
3. **Wahlweise:** Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturübersicht** Um das Dashboard „Korrekturübersicht“ anzuzeigen und eine Ihnen oder Ihrer Zuweisungsgruppe zugewiesene ANFECHTBARE Person zu suchen.
4. Klicken Sie in der Spalte Nummer auf einen UNGÜLTIGEN Datensatz, um ihn zu öffnen.
   Der UNGÜLTIGE Datensatz wird angezeigt.
5. Wenn der offene Datensatz angezeigt wird, scrollen Sie, falls er nicht bereits angezeigt wurde, zur zugehörigen Liste Change-Anforderungen, und wählen Sie ihn aus.
   Alle Change-Anforderungen, die der ABLEHNUNG zugeordnet sind, werden zusammen mit angezeigt **Hinzufügen** Schaltfläche. In der folgenden Abbildung sind dieser ÄNDERUNG bereits keine Change-Anforderungen zugeordnet.



6. Klicken Sie auf, um die ÄNDERUNG einer vorhandenen CHG zuzuordnen **Hinzufügen** .
   Das Formular vorhandene Change-Anforderung zu Korrekturaufgabe hinzufügen wird angezeigt.
7. Klicken Sie im Formular auf das Suchsymbol.
   Eine Listenansicht vorhandener Change-Anforderungen wird in einem neuen Fenster angezeigt, wie in der folgenden Abbildung dargestellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Wählen Sie ein Element aus der angezeigten Liste aus, oder klicken Sie alternativ auf den Filter ( ) Und geben Sie Bedingungen ein, um Ihre Suchergebnisse einzuschränken.
9. Wählen Sie für das Kontrollkästchen CIs zu CR hinzufügen eine aus, um fortzufahren.

Hinweis:
Dieses Kontrollkästchen wird nur für vorhandene Change-Anforderungen in angezeigt Neu status.

Option	Beschreibung
Kontrollkästchen „CIs zu CR hinzufügen“ aktiviert	Standard ist ausgewählt. Wenn das Kontrollkästchen aktiviert ist, werden alle Konfigurationselemente (Configuration Items, CI), die zu aktiven angreifbaren Elementen in dieser Korrekturaufgabe gehören, dieser Change-Anforderung hinzugefügt. Wenn diese Option ausgewählt ist, wird der Status der Change-Anforderung mit dem Status „UNGÜLTIG“ synchronisiert. Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.
Kontrollkästchen „CIs zu CR hinzufügen“ deaktiviert	Deaktivieren Sie das Kontrollkästchen, wenn die CIs aus den aktiven angreifbaren Elementen aus dieser Korrekturaufgabe nicht der neuen Change-Anforderung hinzugefügt werden sollen. Wenn diese Option deaktiviert ist, wird der Status der Change-Anforderung nicht mit dem Status „UNGÜLTIG“ synchronisiert, und der Status „UNGÜLTIG“ bleibt im aktuellen Status.

10. Klicken Sie mit der Nummer der Change-Anforderung, die Sie im Feld Suche nach Change-Anforderung anzeigen möchten, auf **Übermitteln** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Wert „UNGÜLTIG“ wird angezeigt. Oben im Datensatz wird die blaue Bestätigungsnachricht angezeigt, die angibt, dass die von Ihnen ausgewählte Change-Anforderung erfolgreich mit der ABLEHNUNG verknüpft ist.

Hinweis:
Für eine SCHWACHSTELLE in Öffnen status mit den Feldern „Zuweisungsgruppe“ und „Zugewiesen an“ nicht zugewiesen (leer) wird der aktuell angemeldete Anwender automatisch dem VUL zugewiesen, nachdem Sie auf geklickt haben **Hinzufügen** . Darüber hinaus muss das Kontrollkästchen CIs zu CR hinzufügen aktiviert sein. Oben auf der ABLEHNUNG wird eine blaue Bestätigungsnachricht angezeigt, die angibt, dass der aktuelle Anwender zugewiesen ist.

Nächste Maßnahme
Überprüfen Sie den UNGÜLTIGEN Datensatz. Klicken Sie in der Spalte „Change-Anforderung“ in der zugehörigen Liste „Change-Anforderungen“ auf den Link für das neue CHG, um den CR-Datensatz anzuzeigen. Im offenen CHG-Datensatz können Sie den Status der Change-Anforderung überwachen. Die betroffenen Konfigurationselemente (CI) und die Korrekturaufgaben werden in den zugehörigen Listen Betroffene CIs und Korrekturaufgaben angezeigt.

Teilen Sie eine Korrekturaufgabe auf

Identifizieren Sie als IT-Korrekturbesitzer über eine vorhandene Korrekturaufgabe (VUL) eine Teilmenge von angreifbaren Elementen (VI), die Sie in eine neue Gruppe verschieben möchten.

Vorbereitungen
Hinweis:

Anwendungsfälle zum Aufteilen von VIS aus vorhandenen VULs in neue Korrekturaufgaben können die folgenden Beispiele umfassen:

- Wenn Sie eine Change-Anforderung oder Change-Anforderungen für eine geteilte Aufgabe erstellen möchten.
- Wenn Sie eine aufgeteilte Gruppe einem anderen Anwender in Ihrer Zuweisungsgruppe neu zuweisen.
- Wenn Sie eine Zurückstellung oder Ausnahme für eine geteilte Aufgabe anfordern, da Sie wissen, dass einige Schwachstellen bei bestimmten Konfigurationselementen (Configuration Items, CI) in einem bestimmten Zeitrahmen nicht behoben werden können.

Erforderliche Rolle: Jeder Anwender mit der itil-Rolle zum Aufteilen eines WIDERSPRUCHS.

Hinweis:
Die Rolle „sn_vul.Remediation_owner“ wird ebenfalls automatisch zugewiesen, wenn die Rolle „itil“ einem Anwender zugewiesen wird.

Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen zum Aufteilen von Korrekturaufgaben in finden Sie in Vulnerability Response Arbeitsbereiche, siehe Teilen Sie eine Korrekturaufgabe in auf Arbeitsbereich für IT-Korrekturen.

Dient zum Aufteilen einer Korrekturaufgabe in der klassischen Umgebung oder für Versionen von Vulnerability Response.

Sie können vorhandene Korrekturaufgaben mit mehr als einem angreifbaren Element aufteilen, das sich in befindet Öffnen , status „wird untersucht“ oder „Warten auf Implementierung“. Indem Sie eine neue ABLEHNUNG mit angreifbaren Elementen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

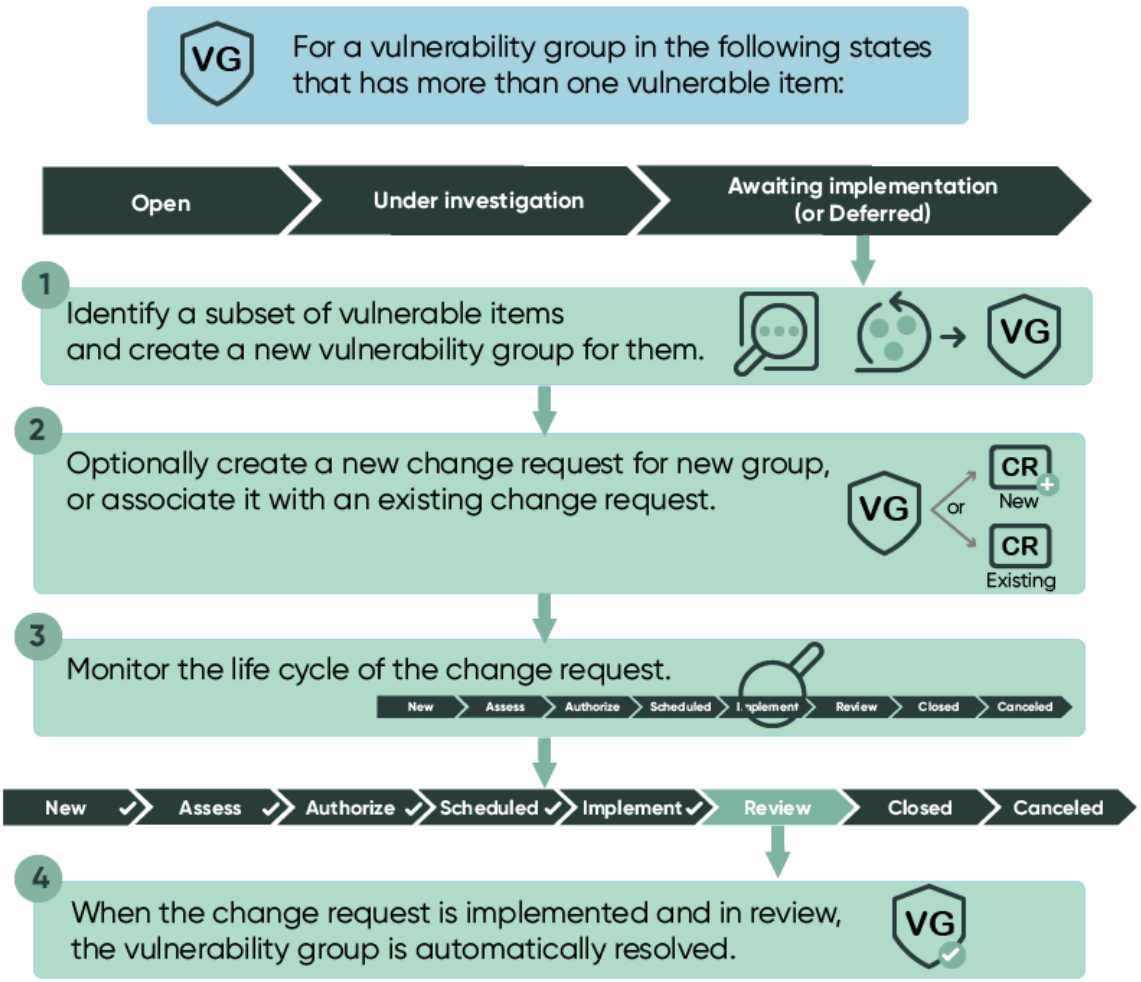
erstellen, die bestimmten Kriterien entsprechen, können Sie mit einer bestimmten Gruppe angreifbarer Elemente arbeiten, ohne die ursprüngliche Korrekturaufgabe zu beeinträchtigen.

Wenn Sie die Bedingungen für die angreifbaren Elemente angeben, die Sie mit dem Bedingungsgenerator in eine neue Korrekturaufgabe verschieben möchten, werden nur die aktiven VIS, die Ihren Kriterien entsprechen, in die neue Gruppe verschoben.

Sie müssen keine Change-Anforderungen (CHG) erstellen, wenn Sie eine ANGREIFBARE Komponente aufteilen. Sie haben die Möglichkeit, eine ABLEHNUNG gleichzeitig aufzuteilen, wenn Sie eine Change-Anforderung erstellen, oder Sie können eine ÄNDERUNG aufteilen, ohne eine Change-Anforderung zu erstellen. Die folgende Abbildung zeigt den grundlegenden Flow zum Aufteilen einer Korrekturaufgabe. Die detaillierten Schritte für diesen Flow folgen dem Bild.

Der Korrekturaufgabendatensatz wird in den folgenden Abschnitten als UNGÜLTIG bezeichnet. In vorherigen Versionen von Vulnerability Response, Korrekturaufgaben wurden aufgerufen, Schwachstellen-Gruppen (VG). In den folgenden Bildern VG= Korrekturaufgabe oder ein ANGREIFBARER Datensatz.

Workflow zum Aufteilen einer Korrekturaufgabe



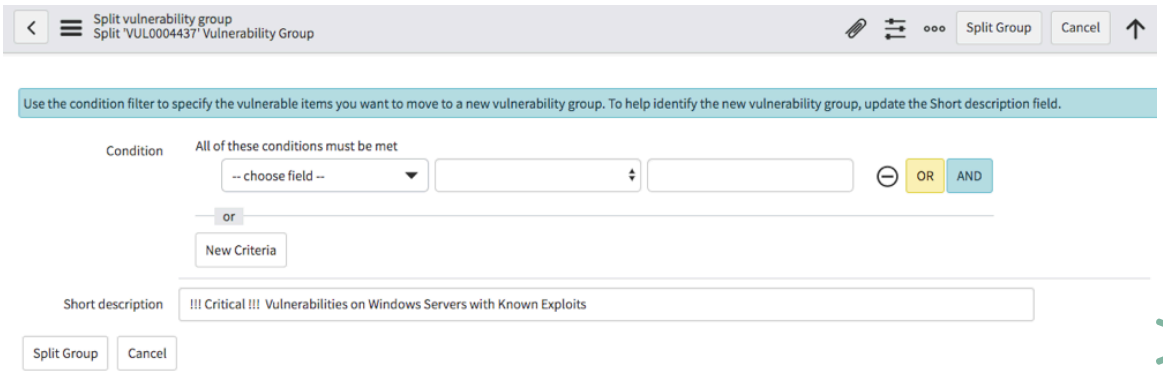
Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**an.
   Die Liste der Korrekturaufgaben wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

2. Klicken Sie in der Spalte Nummer auf einen Datensatz, um ihn zu öffnen.
   Der Datensatz wird angezeigt.
3. Klicken Sie oben rechts im Bereich DER ÄNDERUNG auf **Aufgabe Aufteilen** .
   Das Formular „Korrekturaufgabe aufteilen“ wird angezeigt.

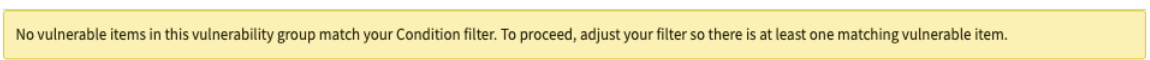


4. Geben Sie bei angezeigtem Bedingungsfilter die Bedingungen für die angreifbaren Elemente an, die Sie in eine neue Aufgabe verschieben möchten.
   Beispielsweise möchten Sie nur angreifbare Elemente herausfiltern, die den folgenden Bedingungen entsprechen:
   - In Öffnen status.
   - Risikopunktzahlen größer als 80 .
   - Konfigurationselemente, die „“ enthalten WINSV „.
   - Befindet sich in San Diego.

   Als Beispiel können Sie für Bedingungen Folgendes eingeben:
   - Status – ist – Offen
   - Risikopunktzahl: Ist größer als oder gleich 80
   - Konfigurationselement . Name – enthält – WINSV
   - Konfigurationselement . Standort – ist – San Diego

   Wenn angreifbare Elemente Ihrem Filter entsprechen, nachdem Sie die Bedingungen eingegeben haben, wird eine Nachricht mit der Anzahl der übereinstimmenden angreifbaren Elemente angezeigt.

   Hinweis:
   Wenn eine Meldung angezeigt wird, dass keine angreifbaren Elemente mit Ihrem Filter übereinstimmen, passen Sie die Bedingungen so an, dass mindestens ein angreifbares Element Ihren Filterkriterien entspricht.



5. **Wahlweise:** Passen Sie den Filter nach Bedarf an.
6. **Wahlweise:** Um Ihnen zu helfen, die neue ÄNDERUNG nach der Erstellung zu identifizieren, sollten Sie das Feld „Kurzbeschreibung“ aktualisieren.
   Wenn bearbeitet, verwenden Sie das Feld Kurzbeschreibung als Suchkriterien für die neue ÄNDERUNG, um sie nach der Erstellung zu finden, z. B. BEFINDET SICH IN SAN DIEGO .

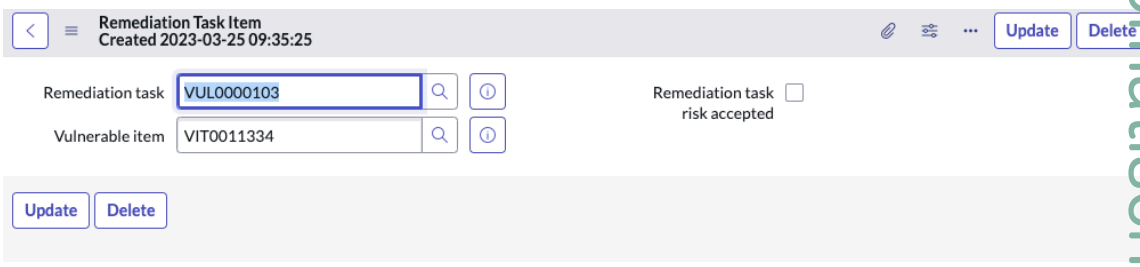
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. **Wahlweise:** Um eine Vorschau der Details zu den angreifbaren Elementen anzuzeigen, die Ihren Filterkriterien entsprechen, führen Sie die folgenden Schritte aus, bevor Sie auf klicken **Aufgabe Aufteilen** Um die neue ÄNDERUNG ZU erstellen.
   Diese Details umfassen vorhandene Change-Anforderungen, die dieser Teilmenge bereits zugeordnet sind, und VULs mit diesen angreifbaren Elementen. Wenn Sie diese Informationen in der Vorschau anzeigen, können Sie möglicherweise doppelte VULs nicht erstellen.

   a. Klicken Sie in der blauen Bestätigungsnachricht im Formular „Korrekturaufgabe aufteilen“ auf **Vorschau auf übereinstimmende Elemente anzeigen** .
   Die Liste „Korrekturaufgabenelement“ wird in einem neuen Fenster in Ihrem Browser mit einer Liste angreifbarer Elemente angezeigt, die Ihren Bedingungen entsprechen.

   b. Klicken Sie in der Spalte Nummer auf ein Element, um den Datensatz zu öffnen.

   c. Klicken Sie im Datensatz, der rechts neben der Schwachstellengruppe oder den Feldern des Schwachstellenelements angezeigt wird, auf das Informationssymbol für das angreifbare Element, um die Datensätze anzuzeigen.



   d. Klicken Sie im angezeigten Dialogfeld auf **Öffnen Sie Den Datensatz** .
   Informationen zum Korrekturzieldatum werden angezeigt. Klicken Sie im Abschnitt zugehörige Listen auf eine zugehörige Liste, um weitere Informationen zum VI anzuzeigen

8. Wenn Sie bereit sind, die neue ÄNDERUNG mit den VI zu erstellen, die Ihre Bedingungen erfüllen, schließen Sie das Vorschaufenster, um zum geteilten Aufgabenformular im anderen Fenster zurückzukehren, und klicken Sie oben im Formular auf **Aufgabe Aufteilen** .

   Hinweis:

   Bei weniger als 200 VIS wird der Aufteilungsvorgang synchron ausgeführt.

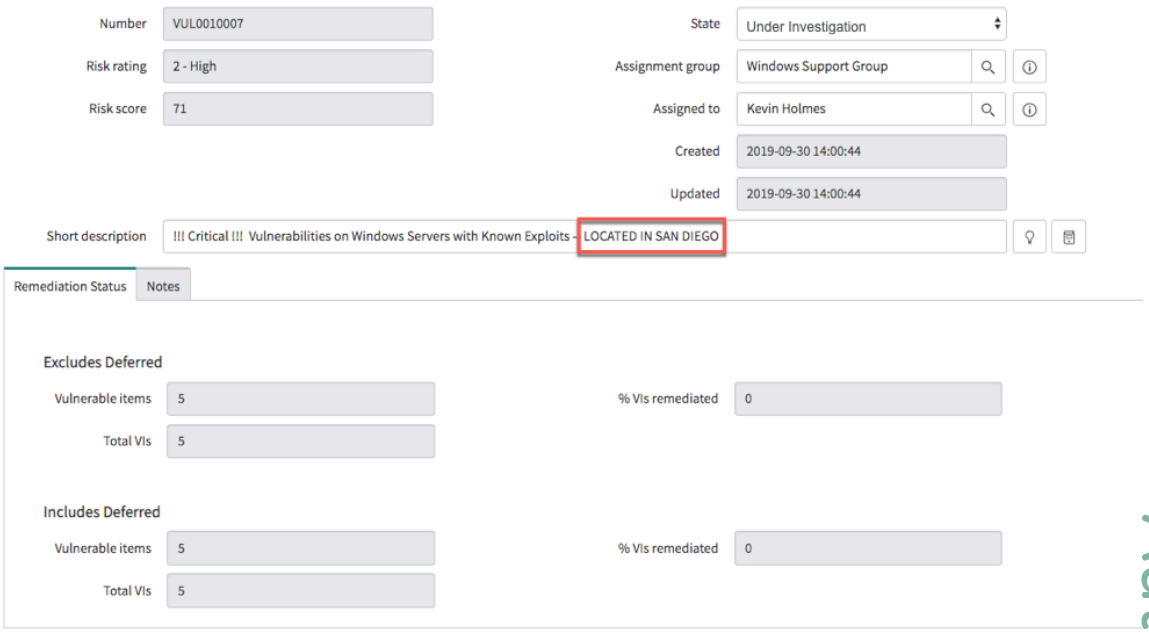
   Bei mehr als 200 VIS wird der Aufteilungsvorgang asynchron im Hintergrund ausgeführt, und es kann einige Sekunden dauern, bis die VIS in der neuen Gruppe angezeigt werden.

   Eine Bestätigungsnachricht wird angezeigt, die alle aktiven VIS anzeigt, die in die neue Gruppe verschoben werden. Die neue Nummer der Korrekturaufgabe wird ebenfalls angezeigt. Wenn nicht bereits in „wird untersucht“, wird die ANFECHTUNG in „wird untersucht“ verschoben. Überprüfen Sie das Feld Kurzbeschreibung auf den Text, den Sie für die neue ABLEHNUNG in eingegeben haben (BEFINDET SICH IN SAN DIEGO).

   Rollup-Berechnungen für die neue Gruppe werden durchgeführt, um die neue Risikopunktzahl, das Korrekturzieldatum und andere Feldwerte zu berechnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die angreifbaren Elemente, bevorzugten Lösungen und Change-Anforderungen werden in den zugehörigen Listen unten im Datensatz angezeigt. Verarbeiten und überwachen Sie diese neue Aufgabe wie bei jeder Korrekturaufgabe.

9. **Wahlweise:** Scrollen Sie zu **Notizen** Zugehörige Liste, und klicken Sie, um sie auszuwählen.
   Bestätigen Sie, dass die Anzahl der angreifbaren Elemente aus der ursprünglichen Korrekturaufgabe in die neue Gruppe im Aktivitätenstrom verschoben wurde.
10. **Wahlweise:** Um die VIS erneut aus der zugehörigen Liste „angreifbare Elemente“ auszuwählen und aufzuteilen, scrollen Sie zum Ende des Korrekturaufgabendatensatzes, und wählen Sie, wenn die VIS, die Sie verschieben möchten, in der Spalte „angreifbares Element“ der zugehörigen Liste „angreifbare Elemente“ ausgewählt sind, in der Auswahlliste „Aktionen für ausgewählte Zeilen“ aus **Aufgabe Aufteilen** .
    Das Formular „Korrekturaufgabe aufteilen“ wird angezeigt.
11. Um die Gruppe erneut aufzuteilen und die ausgewählten Elemente in eine neue Gruppe zu verschieben, klicken Sie auf **Aufgabe Aufteilen** .
    Die ausgewählten VIS werden in eine andere Korrekturaufgabe verschoben, die Bestätigungsnachricht wird angezeigt, und die neue Gruppe wird angezeigt.
12. Wählen Sie eine aus, um Ihre Untersuchung oder Korrektur fortzusetzen.

Nächste Maßnahme

Überwachen Sie den Status der neuen ANFECHTUNG, um ihre Lösung zu beschleunigen.

Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben

Es gibt eine synchronisierte Beziehung zwischen den Statusfeldern von Korrekturaufgaben (VULs) und den Statusfeldern von Change-Anforderungen (CHG) in Vulnerability Response Produkt. Während eine Change-Anforderung ihren Lebenszyklus durchläuft, verschiebt sie auch den Status aller zugehörigen Korrekturaufgaben automatisch.

Statussynchronisierung

Der Korrekturaufgabendatensatz wird in den folgenden Abschnitten als UNGÜLTIG bezeichnet. In vorherigen Versionen von Vulnerability Response, Korrekturaufgaben wurden aufgerufen, Schwachstellen-Gruppen (VG). In den folgenden Bildern VG= Korrekturaufgabe oder ein ANGREIFBARER Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Statussynchronisierung wird standardmäßig durch eine Systemeigenschaft (sn_vul.cr_State_synch) in Ihrer Instanz aktiviert, wenn Sie herunterladen Vulnerability Response Anwendung.

Wenn die Statussynchronisierung aktiviert ist, ändert das Feld CHG-Status das Feld Status der Korrekturaufgabe in den folgenden Fällen automatisch:

- Wenn eine neue CHG für eine Korrekturaufgabe erstellt wird (VUL), wenn sie sich nicht in befindet Warten Auf Implementierung , Der Status „UNGÜLTIG“ wird weiter zu verschoben Warten Auf Implementierung .
- Wenn ein vorhandenes CHG einem UNGÜLTIGEN ELEMENT zugeordnet ist, wenn es sich nicht in befindet Warten Auf Implementierung , Der Status „UNGÜLTIG“ wird weiter zu verschoben Warten Auf Implementierung .
- Nachdem die Aufgaben in einem CHG abgeschlossen sind (Implementiert), und das CHG wird in verschoben Überprüfen status, in den die ANNULLIERUNG verschoben wird Gelöst .

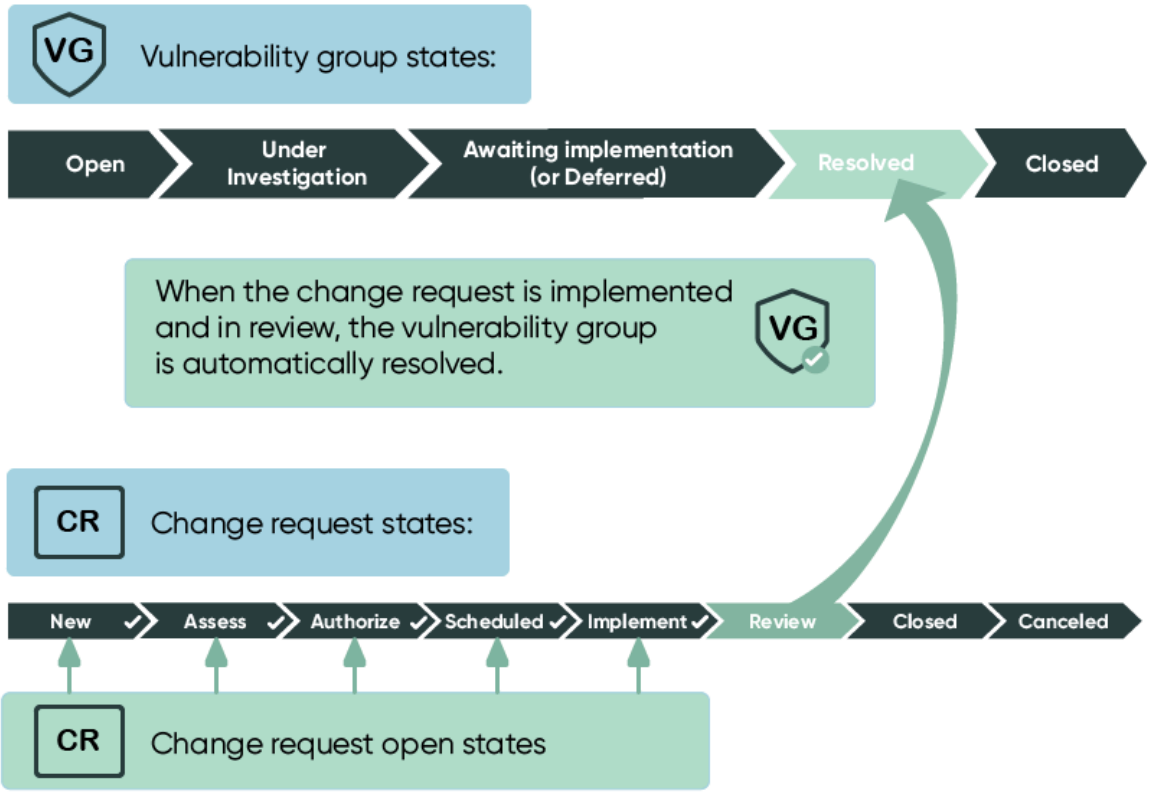
Weitere Informationen und Beispiele für die Statussynchronisierung finden Sie in den folgenden Abschnitten.

Hinweis:
Sie können CHG und VULs weiterhin manuell durch die status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist. Wenn das System jedoch registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder es aus einem UNGÜLTIGEN entfernen, kann die Statussynchronisierung Ihren manuellen Eingriff möglicherweise überschreiben. status von Change-Anforderungen verschieben jedoch nicht automatisch die ÄNDERUNG aus dem Geschlossen Oder Zurückgestellt status.

Statussynchronisierung weiterleiten

Die folgende Abbildung zeigt, wie CHG-status in einem Vorwärtslebenszyklus, also von, automatisch UNGÜLTIGE status verschieben Öffnen Bis Gelöst .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können neue Change-Anforderungen für jede Korrekturaufgabe in einem anderen Status als erstellen Geschlossen . Bei der Statussynchronisierung wird die ANGREIFBARE automatisch bidirektional durch verschoben Öffnen , Wird Untersucht , Warten Auf Implementierung , Und Gelöst status. Diese Bewegung basiert auf bestimmten Werten des Statusfelds in der Change-Anforderung. Die Statussynchronisierung zwischen der Change-Anforderung und der Korrekturaufgabe wird automatisch aufgerufen, sofern das Kontrollkästchen nicht aktiviert ist (Fügen Sie der CR CIs hinzu) Wird in einem Formular angezeigt, und Sie deaktivieren das Kontrollkästchen.

Die ABLEHNUNG wird nicht zu verschoben Gelöst Wenn sich ein CHG im status „Offen“ befindet. Alle CHG in status vor Überprüfen In seinem Lebenszyklus, z. B. Neu , Bewerten , Autorisieren , Geplant Oder Implementieren Wie in der vorherigen Abbildung gezeigt, gelten als offene status für das CHG. Offene status verschieben das Statusfeld nicht auf den Status, da Untersuchungen oder Aufgaben im CHG nicht abgeschlossen sind. Die Statussynchronisierung wird aufgerufen, wenn eine CHG für die ANGREIFBARE Beziehung erstellt oder zugeordnet wird oder sich der Status einer vorhandenen Beziehung im CHG ändert. Die abgeschlossenen CHG-status sind Überprüfen Und erfolgreich Geschlossen . Wenn ein CHG erfolgreich geschlossen wird, lauten seine geschlossenen Codes: Erfolgreich , Oder Erfolgreich mit Problemen , In diesem Fall wird die ABLEHNUNG zu verschoben Gelöst .

Statussynchronisierung rückwärts

Da ein CHG während seines Lebenszyklus verarbeitet wird, kann es irgendwann abgebrochen werden. In diesem Fall, wenn CHG lautet Abgebrochen , Oder Geschlossen (Mit dem Abschlusscode Nicht Erfolgreich), wird der WERT FÜR „UNGÜLTIG“ automatisch zurück zu verschoben Wird Untersucht . Die ANNULLIERUNG wird zurück zu verschoben Wird Untersucht , Da kein aktiver Plan zur Behebung der Schwachstelle vorhanden ist.

Wenn sich ein WIDERRUF in einem befindet Gelöst status, und Sie erstellen ein neues CHG oder ordnen es einem vorhandenen CHG in einem der anfänglichen offenen status zu, in den der STATUS „UNGÜLTIG“ automatisch zurückkehrt Warten Auf Implementierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

. Die ABLEHNUNG wird in diesen Status zurückversetzt, da dem CHG jetzt weitere Arbeit zugewiesen ist.

VULs mit mehr als einem CHG

Wenn ein WIDERRUF in ist Warten Auf Implementierung Hat mehr als ein CHG zugeordnet. Die Statussynchronisierung basiert auf dem Status des CHG im frühesten Status seines Lebenszyklus. Beispiel: Einem VUL sind vier CHG zugeordnet, CHG1, CHG2, CHG3 und CHG4, wie in der folgenden Tabelle dargestellt.

CHG-Nummer	CHG-Status
1	Implementieren
2	Abgebrochen
3	Geschlossen (Abschlusscode von Nicht Erfolgreich)
4	Geschlossen (Abschlusscode Erfolgreich)

Die Statussynchronisierung zwischen CHG und VUL in diesem Fall basiert auf CHG1, das sich im frühesten Status der vier CHG befindet, (Implementieren). In diesem Fall verbleibt der WIDERRUF in Warten Auf Implementierung .

In einem anderen Beispiel, wenn sich ein WIDERSPRUCH in befindet Gelöst status und hat ein vorhandenes CHG, das implementiert wurde und sich in befindet Überprüfen status, und ein neues CHG wird erstellt, von dem der WIDERRUF zurückverschoben wird Gelöst Bis Warten Auf Implementierung . Die Statussynchronisierung basiert auf dem CHG in der Neu status: Das CHG im frühesten Status.

CHG-Nummer	CHG-Status
1	Prüfung
2	Neu

Wenn VULs mehr als ein CHG haben, wird der Status der ANFECHTUNG in den folgenden Fällen automatisch übergehen:

- Wenn ein CHG vorwärts zu verschoben wird Überprüfen , Wenn sich alle anderen CHGs, die dem VUL zugeordnet sind, in befinden Überprüfen Oder Geschlossen status (mit erfolgreichem Abschlusscode),in den die ANFECHTUNG automatisch übergeht Gelöst . Alle anderen zugehörigen CHGs, die abgebrochen oder nicht erfolgreich geschlossen wurden, werden ignoriert.
- Wenn ein CHG zu verschoben wird Abgebrochen Oder Geschlossen (Abschlusscode von Nicht Erfolgreich), wenn sich alle anderen dem WIDERRUF zugeordneten CHGs im gleichen Status befinden, wird der WIDERRUF automatisch zurück zu verschoben Wird Untersucht .

Weitere Informationen zu den status der Korrekturaufgabe und zu den Aktionen in den einzelnen Status finden Sie unter Vulnerability Response status der Korrekturaufgabe und der angreifbaren Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewerten Sie Ihr Risiko für angreifbare Software

Sie können den Herausgeber und die Produktinformationen im Modul „Risikobewertung“ bereitstellen, um Ihr Zero-Day-Risiko (aktueller Tag) Ihrer Assets für angreifbare Software mit zu bewerten ITSM Software Asset Management(SAM) Grundlagenanwendung.

Wichtig:
Sie können die Risikobewertung nach Software und Common Vulnerabilities and Exposures (CVE) durchführen, um die zusätzlichen Fähigkeiten im Arbeitsbereich „Schwachstellenbewertung“ zu nutzen. Weitere Informationen finden Sie unter Arbeitsbereich für Schwachstellenbewertung kennenlernen.

Vorbereitungen

Erforderliche Rolle: Vulnerability admin (sn_Vulnerability_write)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Halten Sie die folgenden Informationen zur angreifbaren Software bereit, die Sie bewerten möchten:

- Herausgeber
- Version
- Produkt
- Edition

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zu Systemanforderungen finden Sie unter Konfigurieren Sie Schwachstelle Risikobewertung.

Zeigen Sie das Software-Risikobewertungsmodul an, und erstellen und bearbeiten Sie Risikobewertungsdatensätze bei Bedarf für angreifbare Software in Ihrem ServiceNow AI Platform® Instanz.

Sie verwalten die Vulnerability Response-Aktivitäten für einen großen Vorgang, der für viele Assets verantwortlich ist. Das Security Operations Center (SOC) in Ihrem Vorgang kontaktiert Sie über eine Version der Software, von der sie erfahren haben, dass sie angreifbar ist. Sie haben erkannt, dass ein Scan Ihrer Assets kürzlich abgeschlossen wurde und diese Schwachstelle nicht gefunden wurde. Das SOC-Team hat von dieser Schwachstelle aus einer zuverlässigen Quelle außerhalb der National Vulnerability Database (NVD), der Common Weakness Enumeration (CWE) oder anderen Drittparteibibliotheken in Ihrer Instanz erfahren, und Sie sind besorgt, dass Ihr Schwachstellen-Scanner das Plugin dafür noch nicht hinzugefügt hat.

Sie sind sicher, dass die Daten für diese Schwachstelle im NVD aktualisiert und bald importiert werden, damit Ihr Scanner diese Schwachstelle beim nächsten Scan erfassen kann. Da Sie jedoch über den Umfang Ihres potenziellen Risikos besorgt sind, möchten Sie heute bestimmen, ob Sie Assets in Ihrem Netzwerk haben, auf denen diese Software installiert ist.

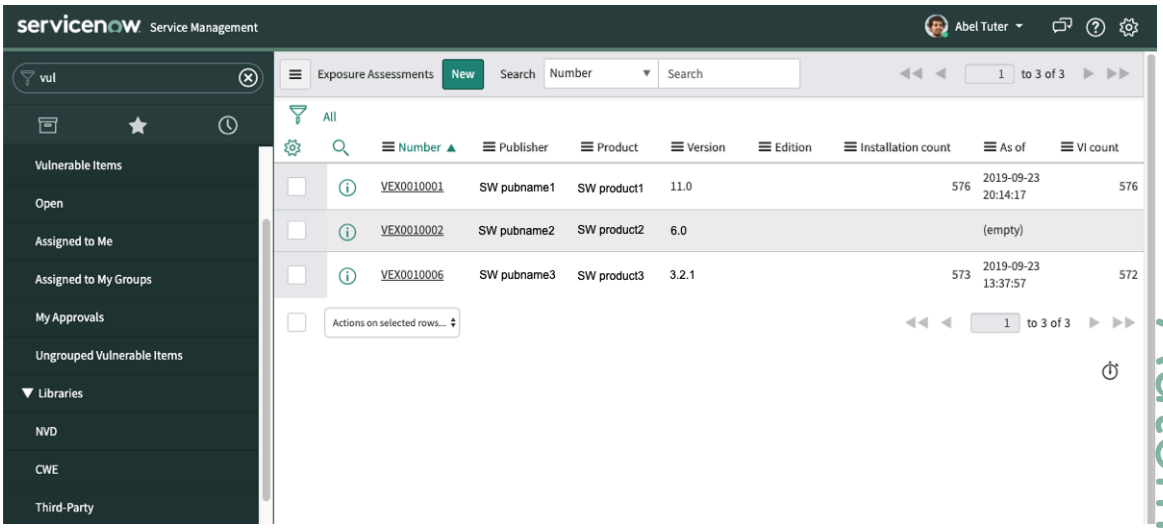
Ab v23.0 von Vulnerability Response, Wenn Sie das Pro- oder Enterprise-Abonnement haben, werden Sie zu weitergeleitet **Risikobewertung** Seite in den Arbeitsbereichen basierend auf Ihrer Rolle bei der Auswahl von **Risikobewertung** Link in **Alle** Menü. Weitere Informationen finden Sie unter Konfigurieren Sie Schwachstelle Risikobewertung.

Automatische Übersetzung

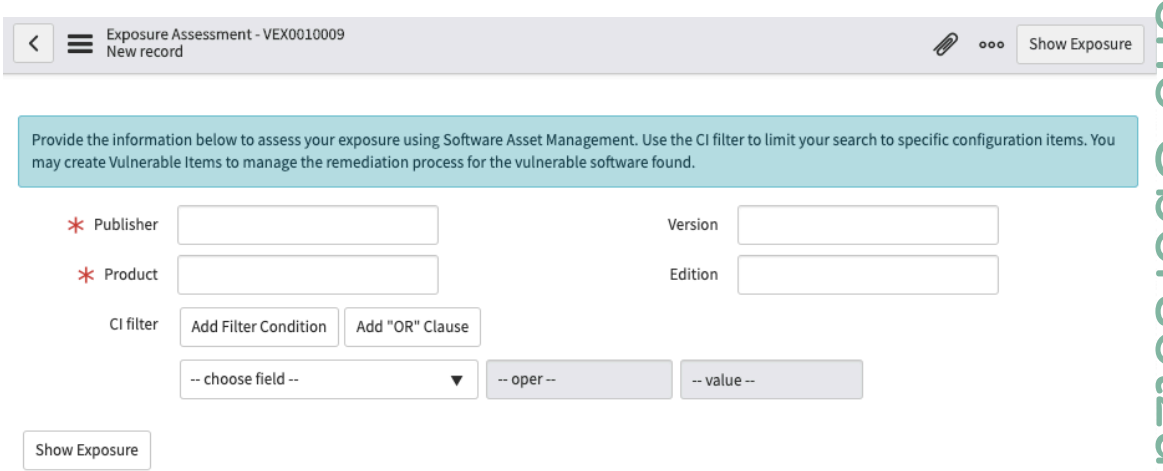
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Um eine neue Risikobewertung zu erstellen, navigieren Sie zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Bewertung des Gefahrenpotenzials**an.
   Die Liste Risikobewertungen wird angezeigt.



2. Wählen Sie **Neu**.
   Das Formular „Risikobewertung“ wird angezeigt.



3. Füllen Sie das Formular aus.

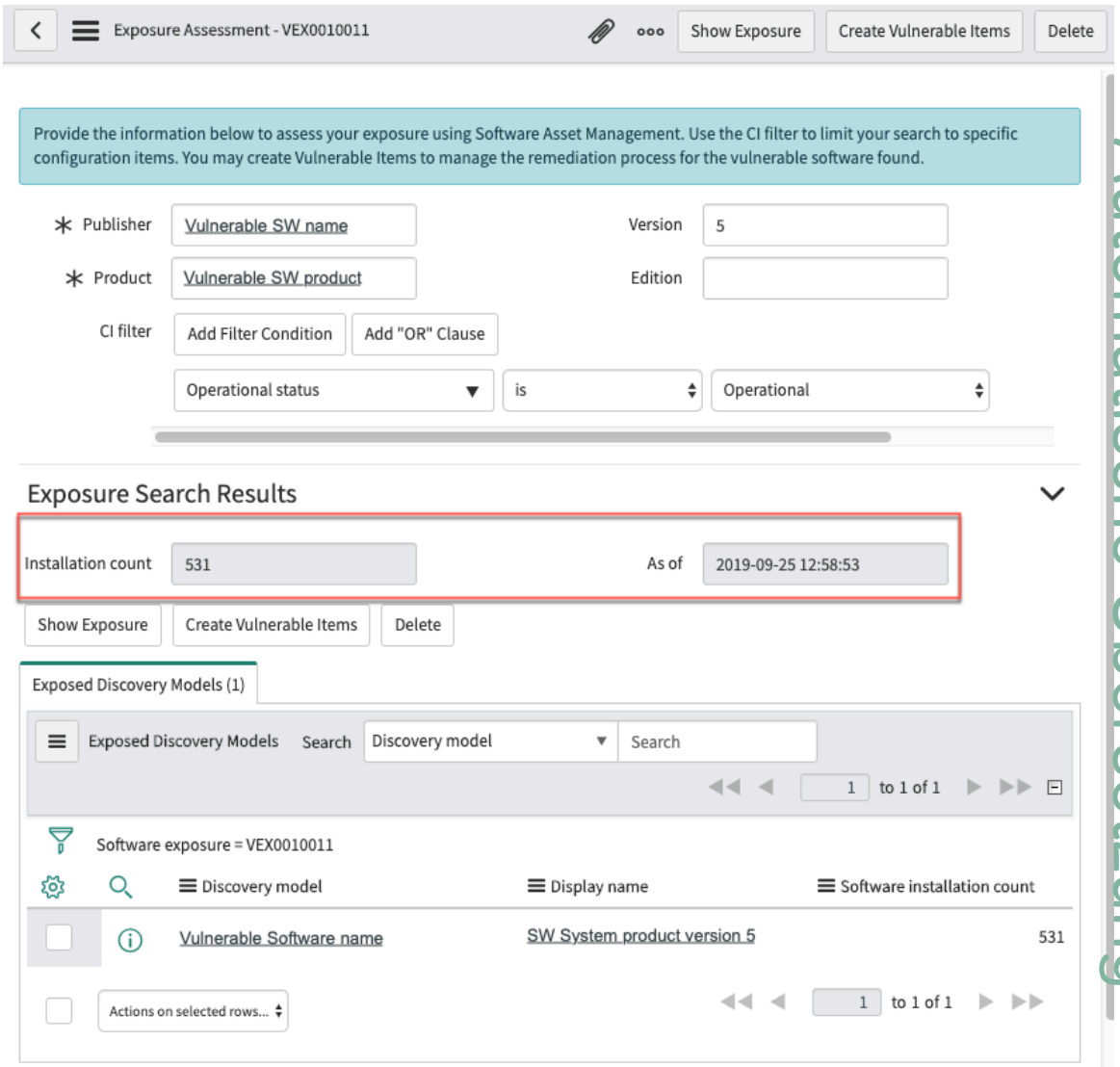
Feld	Beschreibung
Herausgeber	Name des Softwareherausgebers.
(Optional) Version	Geben Sie die Versionsnummer ein, um die Suche nach Ihren Assets einzugrenzen.
Produkt	Name des Softwareprodukts.
(Optional) Edition	Geben Sie die Edition ein, damit Sie die Suche nach Ihren Assets eingrenzen können.
CI-Filter	Verwenden Sie die Auswahllisten für den CI-Filter (Configuration Item), um Ihre Suche auf bestimmte Konfigurationselemente (Assets)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	zu beschränken. Sie können beispielsweise eine Abfrage nur für aktive Assets übermitteln, für die diese Software installiert sein kann: Betriebsstatus ist „betriebsbereit“

4. Wählen Sie Aus **Risiko Anzeigen** .
   Der Datensatz der Risikobewertung mit Ihrem Discovery-Modell und die Anzahl der Softwareinstallationen für Ihre Assets ab dem angegebenen Datum werden angezeigt.



5. Wählen Sie eine, um fortzufahren.

6. **Wahlweise:** Erstellen Sie ein angreifbares Element für Ihr Suchergebnis.

   Hinweis:
   Nachdem Sie angreifbare Elemente erstellt haben, können Sie die Suchkriterien für diesen Risikodatensatz nicht ändern.

7. Alternativ können Sie Ihre Filterbedingungen überarbeiten und Ihre Suchergebnisse weiter verfeinern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Führen Sie die folgenden Schritte aus, um angreifbare Elemente zu erstellen:

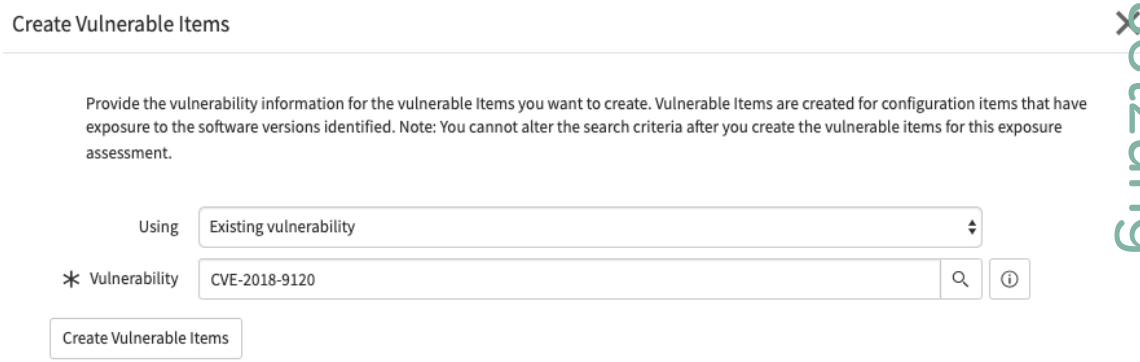
a. Wählen Sie Aus **Erstellen Sie Angreifbare Elemente** .
Das Dialogfeld Angreifbare Elemente erstellen wird angezeigt.

b. Füllen Sie die Felder aus.

Feld	Beschreibung
Arbeiten mit	Wählen Sie aus der Auswahlliste eine aus, um fortzufahren. ▪ **Vorhandene Schwachstelle** . Klicken Sie rechts neben dem Feld Schwachstelle auf das Suchsymbol. Wählen Sie in der angezeigten Liste die CVE-ID aus, oder geben Sie Suchkriterien ein, um die vorhandene CVE-ID zu finden, z. B. CVE 2018-9120. **Hinweis:** Dies kann eine CVE-ID aus einer anderen Schwachstellendatenbank als dem NVD sein. ▪ **Neue Schwachstelle** . Geben Sie die CVE-ID für Ihre neue Schwachstelle im Format xxxx-xxxx, xxxx-xxxxx oder xxxx-xxxxxx ein.
Schwachstellenzusammenfassung (nur für neue Schwachstelle)	Geben Sie eine Zusammenfassung für die neue Schwachstelle ein, z. B. Ein Angreifer kann ein Skript im Browser eines ahnungslosen Anwenders ausführen .

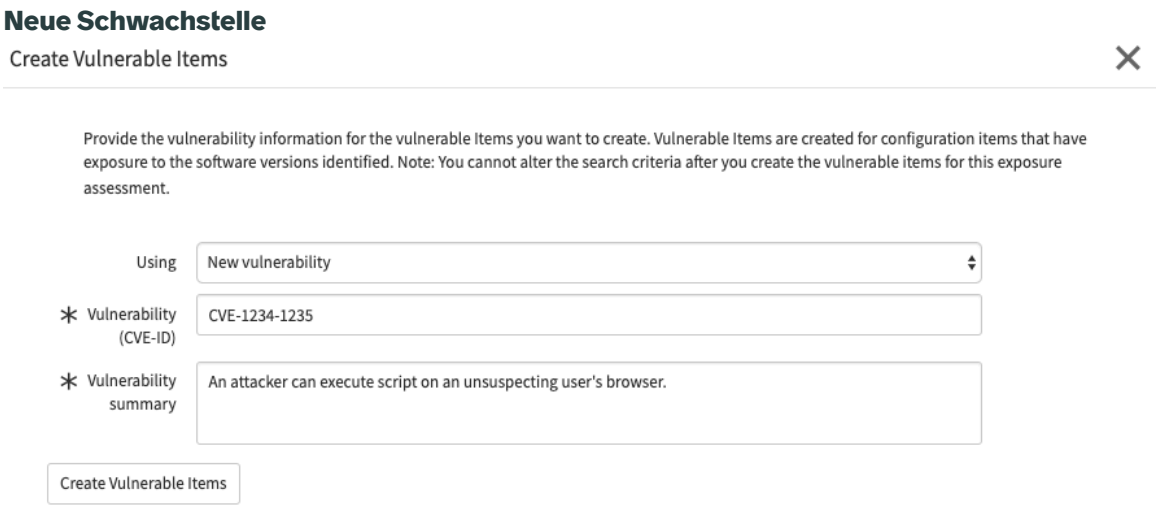
Die folgenden Bilder zeigen Beispiele für das ausgefüllte Formular für eine vorhandene Schwachstelle und eine neue Schwachstelle.

Vorhandene Schwachstelle



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



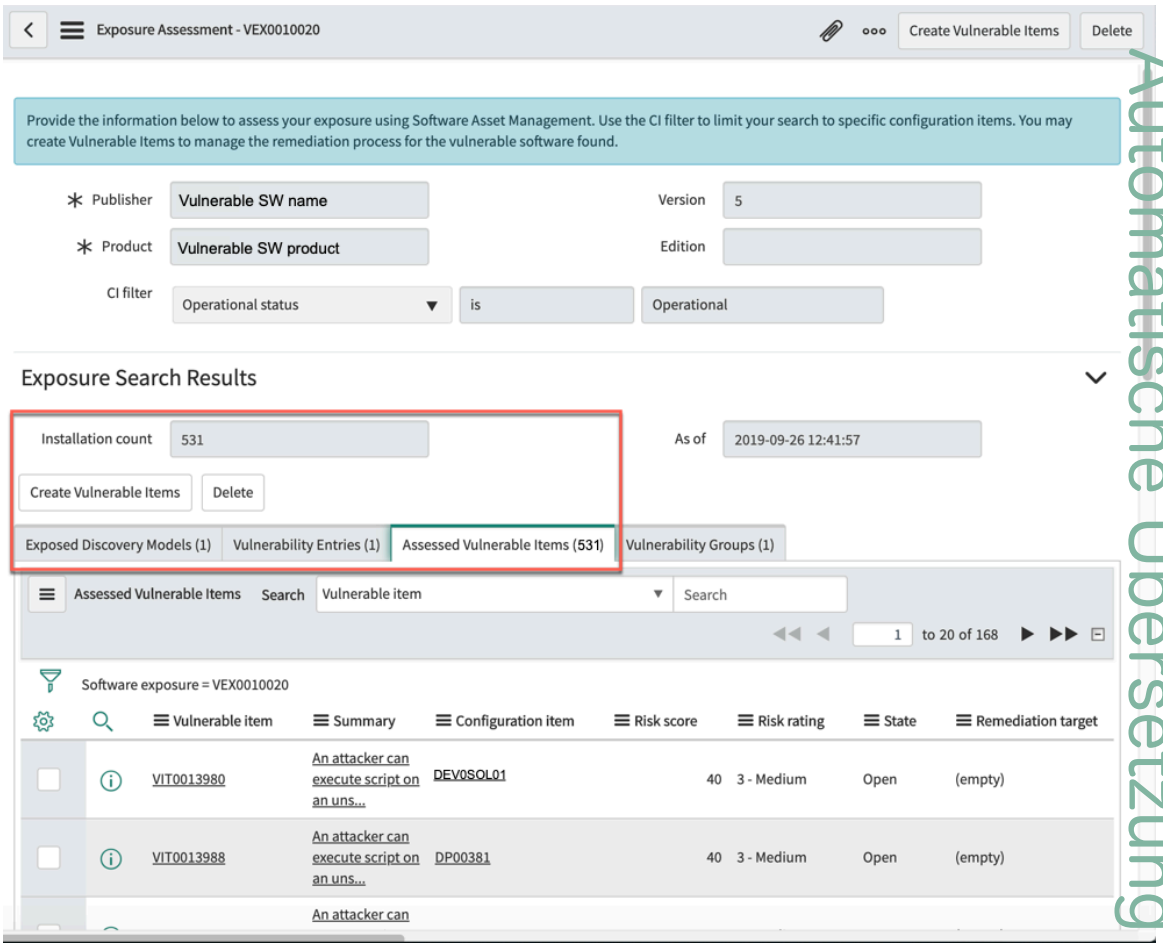
c. Wählen Sie Aus **Erstellen Sie angreifbare Elemente** .
Der Datensatz der Risikobewertung wird mit einer Statusmeldung angezeigt, die angreifbare Elemente erstellt werden.

d. Klicken Sie nach einigen Sekunden oben im Formular mit der rechten Maustaste auf das graue Banner, um die Seite neu zu laden.
Die neuen angreifbaren Elemente werden wie in der folgenden Abbildung auf der Registerkarte bewertete angreifbare Elemente (531) angezeigt. Die neue Korrekturaufgabe, die für diese angreifbaren Elemente erstellt wurde, wird auf der Registerkarte „Korrekturaufgabe“ (1) angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
In diesem Beispiel wird eine Korrekturaufgabe gemäß den Gruppenregeln und -Bedingungen aus der Korrekturaufgabenregel Schwachstelle erstellt. Diese Gruppenregel ist die standardmäßige Regel für Korrekturaufgaben, die mit dem Vulnerability Response-Produkt in Ihrem installiert wird ServiceNow AI Platform® Instanz. In diesem Beispiel haben die Bedingungen dieser Gruppenregel alle angreifbaren Elemente in einer einzigen Korrekturaufgabe platziert. Wenn Sie mehr als eine Korrekturaufgabe für die angreifbaren Elemente erstellen möchten, die Ihren Suchergebnissen der Risikobewertung entsprechen, sollten Sie zusätzliche Regeln für Korrekturaufgaben einrichten. Durch das Erstellen weiterer Korrekturaufgaben können Sie die Erstellung von Korrekturaufgaben mit einer großen Anzahl angreifbarer Elemente verhindern. Weitere Informationen zu Regeln für Korrekturaufgaben finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben Und Erstellen oder bearbeiten Vulnerability Response Regeln für Korrekturaufgaben.

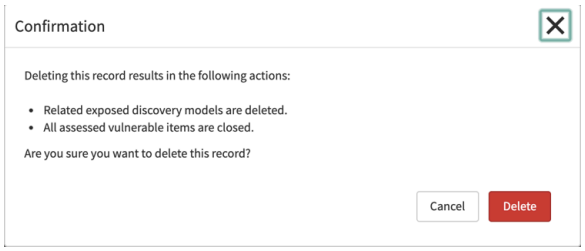


Automatische Übersetzung

9. Wählen Sie eine, um fortzufahren.

Option	Beschreibung
Korrekturaufgaben	Wenn die Registerkarte Korrekturaufgaben ausgewählt ist, klicken Sie in der Zahlenspalte auf , um den Datensatz zu öffnen und zu überprüfen und die Aufgabe zur Korrektur zuzuweisen. Weitere Informationen zu Zuweisungsgruppen finden Sie unter Creating groups .
Bewertete Schwachstellenelemente	Wenn die Registerkarte bewertete angreifbare Elemente ausgewählt ist, klicken Sie in der Spalte angreifbares Element auf , um die Datensätze

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	zu öffnen und einzelne angreifbare Elemente zu überprüfen und zuzuweisen.
Löschen	Löschen Sie den Risikobewertungsdatensatz. Ein Bestätigungsdialogfeld wird angezeigt. **Hinweis:** Wenn Sie den Risikodatensatz löschen, nachdem Sie angreifbare Elemente erstellt haben, werden alle angreifbaren Elemente, die Sie für diesen Datensatz erstellen, die nicht zu einem anderen Risikodatensatz gehören, automatisch in verschoben Geschlossen status. Der Grund für den Abschluss ist Abgebrochen .
	

Nächste Maßnahme

Reagieren Sie auf alle Zero-Day-Bedrohungen (aktueller Tag) basierend auf Ihrer Risikobewertung. Weitere Informationen zu Korrekturaufgaben und Change-Management für finden Sie Vulnerability Response, Siehe Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben Und Change-Management für Vulnerability Response.

Zuweisungsempfehlungen anzeigen

Eine Zuweisungsgruppe wird normalerweise mithilfe von Zuweisungsregeln einem angreifbaren Element zugewiesen. Diese Regeln werden vom Schwachstellenadministrator konfiguriert, um die richtigen Zuweisungsgruppen zuzuordnen, die auf den von Scannern von Drittparteien empfangenen Daten basieren.

Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Wenn eine übereinstimmende Zuweisungsgruppe nicht verfügbar oder falsch ist, können Sie verwenden Empfehlungen für die Zuweisung von Schwachstellen Dient zum Anzeigen alternativer Zuweisungsgruppen.

Verwenden Empfehlungen für die Zuweisung von Schwachstellen So führen Sie die folgenden Aktionen aus:

- Fordern Sie Empfehlungen für Zuweisungsgruppen für ein angreifbares Element an.
- Fordern Sie Empfehlungen für Zuweisungsgruppen für mehrere angreifbare Elemente an.
- Fordern Sie Empfehlungen für Zuweisungsgruppen für eine Korrekturaufgabe an.

Fordern Sie Empfehlungen für Zuweisungsgruppen für ein angreifbares Element an

Anforderung Empfehlungen für die Zuweisung von Schwachstellen Damit Sie Empfehlungen für Zuweisungsgruppen anzeigen können. Sie können Empfehlungen anfordern, wenn eine übereinstimmende Zuweisungsgruppe für ein angreifbares Element (VI) nicht verfügbar oder falsch ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_vul.Remediation_owner

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** Und öffnen Sie ein VI
   Das Element muss sich im Status Offen, zurückgestellt, wird untersucht oder wartet auf Implementierung befinden.
2. Klicken Sie auf das Empfehlungssymbol ( ) Neben **Zuweisungsgruppe** Feld für Zuweisungsvorschläge für dieses VI
3. Wählen Sie im Dialogfeld „Empfehlungen für Zuweisungsgruppe“ eine Empfehlung aus, die auf der Konfidenzpunktzahl basiert.
   Die Konfidenzpunktzahl sagt voraus, wie relevant die Übereinstimmung für das VI ist Weitere Informationen finden Sie unter Lösungen für maschinelles Lernen für Vulnerability Response.
4. Klicken Sie auf **Zuweisen**.

Ergebnisse
Die ausgewählte Gruppe wird in angezeigt **Zuweisungsgruppe** Und der Zuweisungstyp ändert sich in Empfehlung.

Fordern Sie Empfehlungen für Zuweisungsgruppen für mehrere angreifbare Elemente an

Verwenden Empfehlungen für die Zuweisung von Schwachstellen Dient zum Anzeigen der Zuweisungsgruppenempfehlungen für mehrere angreifbare Elemente (VIS) mithilfe einer Massenbearbeitung. Wenn mehrere VIS ausgewählt sind, wird eine Vorhersage für eine zufällige Stichprobe der ausgewählten VIS durchgeführt.

Vorbereitungen
Erforderliche Rolle: sn_vul.Remediation_owner

Warum und wann dieser Vorgang ausgeführt wird
Die Empfehlungen und ihre Konfidenzpunktzahlen können sich je nach Aufrufen geringfügig unterscheiden, basierend auf den Beispielen aus den ausgewählten VIS. Die Konfidenzpunktzahl bewertet, ob das System zuversichtlich ist, dass die empfohlene Zuweisungsgruppe zur Behebung der Schwachstelle geeignet ist. Verwenden Sie `Zuweisungsempfehlung_Batchsize` Systemeigenschaft zum Festlegen der Batchgröße bei Anforderung Empfehlungen für die Zuweisung von Schwachstellen Für Korrekturaufgaben (VULs) und VIS mit der Massenbearbeitungsoption. Der Standardwert dieser Systemeigenschaft ist für eine optimale Vorhersageleistung festgelegt.

Hinweis:
Wenn Sie den Standardwert erhöhen, die Antwortzeit für Empfehlungen für die Zuweisung von Schwachstellen Für diese Fälle kann sich ändern.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbares Element** Und wählen Sie mehrere VIS aus.
   Die Elemente müssen sich im Status Offen, wird untersucht oder wartet auf Implementierung befinden.
2. Klicken Sie Auf **Massenbearbeitung** .
3. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Angreifbare Massenelemente“

Feld	Beschreibung
Datensatzauswahl	Datensätze, die für die Massenbearbeitung ausgewählt werden sollen.
Zuweisungsgruppe	Zuweisungsgruppe, die für die ausgewählten angreifbaren Elemente festgelegt werden soll. Um die empfohlenen Zuweisungsgruppen anzuzeigen, klicken Sie auf das Empfehlungssymbol ( ) Neben dem Feld. Wählen Sie eine Empfehlung aus, die auf der Konfidenzpunktzahl basiert, und klicken Sie auf **Zuweisen** .
Arbeitsnotizen	Hinzuzufügende Notizen.

4. Klicken Sie auf **OK**.

Ergebnisse

Die ausgewählte Gruppe wird in angezeigt **Zuweisungsgruppe** Und der Zuweisungstyp ändert sich für alle ausgewählten AES in Empfehlung.

Fordern Sie Empfehlungen für Zuweisungsgruppen für eine Korrekturaufgabe an

Verwenden Empfehlungen für die Zuweisung von Schwachstellen Dient zum Anzeigen von Zuweisungsgruppenempfehlungen für eine Korrekturaufgabe (VUL).

Vorbereitungen

Erforderliche Rolle: sn_vul.Remediation_owner

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie Zuweisungsempfehlung_Batchsize Systemeigenschaft zum Festlegen der Batchgröße bei Anforderung Empfehlungen für die Zuweisung von Schwachstellen Für VULs und angreifbare Elemente (VIS) mit der Massenbearbeitungsoption. Der Standardwert dieser Systemeigenschaft ist für eine optimale Vorhersageleistung festgelegt.

Hinweis:
Wenn Sie den Standardwert erhöhen, die Antwortzeit für Empfehlungen für die Zuweisung von Schwachstellen Für diese Fälle kann sich ändern.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** Und wählen Sie eine ABLEHNUNG aus.
   Die Gruppe muss sich im Status Offen, wird untersucht oder wartet auf Implementierung befinden.
2. Klicken Sie auf das Empfehlungssymbol ( ) Neben **Zuweisungsgruppe** Feld für die Zuweisungsgruppenempfehlungen für die ausgewählte ABLEHNUNGSOPTION.
   Im Dialogfeld „Empfehlungen für Zuweisungsgruppe“ werden die empfohlenen Zuweisungsgruppen mit der durchschnittlichen Konfidenzpunktzahl für alle VIS in dieser Gruppe angezeigt.
3. Wählen Sie basierend auf der Konfidenzpunktzahl eine Empfehlung aus der Liste Zuweisungsgruppe aus.
   Die Konfidenzpunktzahl sagt voraus, wie relevant die Übereinstimmung für die ausgewählte ABLEHNUNG ist.
4. Klicken Sie auf **Zuweisen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die ausgewählte Gruppe wird in angezeigt **Zuweisungsgruppe** Feld.

5. Speichern Sie die Korrekturaufgabe mit den aktualisierten Informationen.

Ergebnisse

Alle VIS mit derselben Zuweisungsgruppe wie die ANGREIFBARE werden der ausgewählten Zuweisungsgruppe zugewiesen. Der Zuweisungstyp ändert sich in Empfehlung für den WIDERRUF sowie für alle geänderten VIS.

Ausnahme wird angefordert und genehmigt

Sie können anfordern, die Korrektur eines angreifbaren Elements oder einer Korrekturaufgabe für einen bestimmten Zeitraum zu verschieben. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist. Genehmiger, die Zugriff haben, können Anforderungen anderer Anwender genehmigen.

Sie können Ausnahmen von anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen.

- Fordern Sie eine Ausnahme für ein angreifbares Element an
- Fordern Sie eine Ausnahme für eine Korrekturaufgabe an
- Fordern Sie eine Massenausnahme an

Sie können auch Richtlinienausnahmen mit anfordern GRC: Richtlinien- und Compliance-Management:

- Fordern Sie eine Ausnahme mit an GRC: Richtlinien- und Compliance-Management
- Fordern Sie eine Massenausnahme mit an GRC: Richtlinien- und Compliance-Management

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des Ausnahmemanagements gesendet, die den Status und andere Details einer Anforderung angeben. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, die bestätigt, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail, in der angegeben wird, dass eine Ausnahme angefordert wurde.

Ab v21.0 von Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Fordern Sie eine Ausnahme für ein angreifbares Element an

Fordern Sie eine Ausnahme für ein angreifbares Element (VI) an, das nicht sofort behoben werden kann. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Vorbereitungen

Erforderliche Rolle: sn_vul.Remediation_owner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wichtig:
Sie können Ausnahmen über den Schwachstellenmanager und DIE IT-Korrekturarbeitsbereiche anfordern. Weitere Informationen finden Sie unter Fordern Sie Ausnahmen für Korrekturaufgaben und -Datensätze in an Arbeitsbereich des Schwachstellenmanagers und Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen.

Sie können auch Ausnahmen für VIS in der klassischen Umgebung anfordern.

Hinweis:

Ab v21.0 von Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente** > **Alle**an.
2. Wählen Sie das Element aus, für das Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element muss sich im Status „Offen“, „wird untersucht“ oder „Warten auf Implementierung“ befinden.
3. Klicken Sie im Formular Angreifbares Element auf **Ausnahme Anfordern** .
4. Wenn Vulnerability Response Ist im Bildschirm „Ausnahmemanagement“ ausgewählt. Füllen Sie die Felder im Formular „Ausnahme anfordern“ aus.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der in ausgewählten Dauer liegen **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmenverwaltung** Bildschirm. Wenn die Ausnahmeanforderung abläuft, kehrt die Gruppe in den Status Offen zurück.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Ab Version 18,0 von Vulnerability Response(VR): Wenn ein angreifbares Element zur Korrektur mithilfe der Ausnahmeverwaltungsfunktion zurückgestellt wurde, bleibt das für die Schwachstelle festgelegte Zurückstellungsdatum weiterhin bestehen, falls es vom Scanner erneut geöffnet wird. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft fest *sn_vul.auto_defer_vit_in_active_exception_win* „wahr“. Auch zurückgestellt **Bis** Das Datum wird auch nach dem Schließen des angreifbaren Elements oder dem Ablauf der Ausnahme beibehalten. Die erforderliche Rolle ist „sn_vul.Manage_Exception_Configuration“ für Lese- und Schreibvorgänge.
Grund	Grund für die Anforderung. Die Auswahlmöglichkeiten lauten wie folgt: ○ Risiko akzeptiert ○ Warten auf Wartungsfenster ○ Behebung nicht verfügbar ○ Ausgleichende Steuerung vorhanden ○ Sonstige Informationen zum Hinzufügen neuer Ursachenauswahlen finden Sie unter Definieren Sie die Zuordnung des Richtliniengrunds.
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Korrekturbesitzer aktualisiert werden.

5. Senden Sie die Ausnahmeanforderung, indem Sie auf klicken **Genehmigung Anfordern** .

Ergebnisse

Der Status des angreifbaren Elements ändert sich in „in Überprüfung“. Verwenden Sie **Genehmigung Der Statusänderung** Registerkarte zum Nachverfolgen des Status der Ausnahmeanforderung.

Fordern Sie eine Ausnahme für eine Korrekturaufgabe an

Fordern Sie eine Ausnahme an, um eine Korrekturaufgabe für einen angegebenen Zeitraum aufzuschieben, wenn sie nicht sofort gelöst werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Wichtig:

Sie können die Ausnahmen über die Arbeitsbereiche „Schwachstellenmanager“ und „IT-Korrektur“ anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.Remediation_owner

Sie können auch Ausnahmen für Korrekturaufgaben in der klassischen Umgebung anfordern.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Alle**an.
2. Wählen Sie die Gruppe aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählte Aufgabe muss sich im Status Offen, wird untersucht oder wartet auf Implementierung befinden.
3. Wählen Sie im Korrekturaufgabendatensatz (VUL) die Option aus **Ausnahme Anfordern** .
4. Füllen Sie im Formular die Felder aus.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der Ausnahmedauer liegen, die in der Konfiguration definiert ist.
Grund	Begründung für die Anforderung einer Ausnahme.
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer aktualisiert werden.

5. Klicken Sie auf **Genehmigungs-Engine**.

Fordern Sie eine Massenausnahme an

Verwenden Sie die Massenbearbeitungsoption, um eine Ausnahme für mehrere angreifbare Elemente (Vits) anzufordern, anstatt jedes Element manuell auszuwählen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_Analyst

Warum und wann dieser Vorgang ausgeführt wird

Wenn mehrere Vits ausgewählt sind, wird eine Korrekturaufgabe (VUL) mit diesen Elementen erstellt. Siehe Bearbeiten Sie angreifbare Elemente in Massenarbeit Vulnerability Response Weitere Informationen zum Bearbeiten mehrerer Vits.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Sie können eine Ausnahme anfordern für:

- Eine VIT aus der Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen.
- Mehrere Vits aus dem Arbeitsbereich des Schwachstellenmanagers. Weitere Informationen finden Sie unter Fordern Sie eine Massenausnahme im Vulnerability Manager-Arbeitsbereich an.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente** > **Alle** Und wählen Sie die Elemente aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählten Elemente müssen sich im Status Offen, wird untersucht oder wartet auf Implementierung befinden.
2. Klicken Sie Auf **Massenbearbeitung** .
3. Füllen Sie im Formular die Felder aus.

Formular „Massenbearbeitung angreifbarer Elemente“

Feld	Beschreibung
Datensatzauswahl	Datensätze, die Sie für eine Massenbearbeitung ausgewählt haben.
Status	Status des angreifbaren Elements. Wählen Sie den Status zurückgestellt aus, um eine Ausnahme für die ausgewählten Elemente anzufordern.
Grund	Substatus für den von Ihnen ausgewählten Status.
Kurzbeschreibung	Name der Korrekturaufgabe, die Sie erstellen.
Bis	Enddatum, das Sie für Ihre Ausnahmeanforderung angeben.
Zusätzliche Information	Weitere Details, die Sie erwähnen möchten, um den Genehmiger über die Gründe für Ihre Anforderung zu informieren.
Bevorzugte Lösung	Lösung, die darauf ausgerichtet ist, alle angreifbaren Elemente zu korrigieren, die Sie für eine Massenbearbeitung ausgewählt haben.
Zuweisungsgruppe	Zuweisungsgruppe für das VI Sie können eine Gruppe manuell auswählen oder Zuweisungsempfehlungen verwenden, wenn diese Funktion aktiviert ist.
Arbeitsnotizen	Hinzuzufügende Notizen.

4. Klicken Sie auf **OK**.
   Eine Korrekturaufgabe wird erstellt, die die von Ihnen ausgewählten VIS enthält. Diese Korrekturaufgabe wird zur Genehmigung übermittelt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fordern Sie eine Ausnahme mit an GRC: Richtlinien- und Compliance-Management

Fordern Sie Richtlinienausnahmen mit an GRC Fähigkeit zur Verwaltung von Richtlinienausnahmen in Richtlinien- und Compliance-Management Anwendung von innerhalb Vulnerability Response.

Vorbereitungen

Bevor Sie die Integration von Richtlinienausnahmen verwenden können, um Richtlinienausnahmen anzufordern, müssen Sie herunterladen GRC: Richtlinien- und Compliance-Management Anwendung aus dem ServiceNow Store.

Erforderliche Rolle: sn_vul.Remediation_owner

Sie können auch Ausnahmen in der klassischen Anwenderoberfläche anfordern:

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** (Oder **Korrekturaufgaben**)> **Alle** , Und öffnen Sie das Element oder die Gruppe, für das Sie eine Ausnahme anfordern möchten. Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie im ausgewählten Formular auf **Ausnahme Anfordern** .
3. Füllen Sie im Formular die Felder aus.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Richtlinie	Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft, und der Status des angreifbaren Elements oder der angreifbaren Gruppe von zurückgestellt in Offen ändert. **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf nicht überschreiten **Maximale Ausnahmedauer (Tage)** Die Sie für die Richtlinie in Richtlinie und Compliance festgelegt haben. Weitere Informationen finden Sie unter Erstellen Sie eine Richtlinie .
Grund	Grund für die Anforderung einer Ausnahme.
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Korrekturbesitzer ausgefüllt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.
   Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Korrekturbesitzer und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management .

Fordern Sie eine Massenausnahme mit an GRC: Richtlinien- und Compliance-Management

Wählen Sie eine Gruppe von angreifbaren Elementen aus, und übermitteln Sie eine Massenausnahme.

Vorbereitungen

Bevor Sie die Richtlinienausnahmeintegration verwenden können, um Massenausnahmen anzufordern, müssen Sie herunterladen GRC: Richtlinien- und Compliance-Management Anwendung aus dem ServiceNow Store.

Hinweis:
Um diese Funktion zu verwenden, müssen Sie ein Upgrade durchführen GRC: Richtlinien- und Compliance-Management Vor dem Upgrade Vulnerability Response. Wenn Sie bereits ein Upgrade durchgeführt haben Vulnerability Response Vor GRC: Richtlinien- und Compliance-Management Und möchten Sie diese Funktion verwenden, müssen Sie die Upgrade-Verfahren erneut in der richtigen Reihenfolge durchführen.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.Remediation_owner

Sie können auch Ausnahmen in der klassischen Umgebung in anfordern Vulnerability Response.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente** > **Alle** Und wählen Sie die Elemente aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählten Elemente müssen sich im Status „Offen“, „wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie Auf **Massenbearbeitung** .
3. Füllen Sie im Formular die Felder aus.

Formular „Massenbearbeitung angreifbarer Elemente“

Feld	Beschreibung
Datensatzauswahl	Datensätze, die Sie für eine Massenbearbeitung ausgewählt haben.
Status	Status des angreifbaren Elements. Wählen Sie den Status zurückgestellt aus, um eine Ausnahme für die ausgewählten Elemente anzufordern.
Kurzbeschreibung	Name der Aufgabe, die Sie erstellen.
Bevorzugte Lösung	Lösung, die Sie zum Beheben aller angreifbaren Elemente anvisieren, die Sie für die Massenbearbeitung ausgewählt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zuweisungsgruppe	Zuweisungsgruppe für das VI Sie können eine Gruppe manuell auswählen oder Zuweisungsempfehlungen verwenden, wenn diese Funktion aktiviert ist.
Arbeitsnotizen	Hinzuzufügende Notizen.

4. Klicken Sie auf **OK**.
   Eine Korrekturaufgabe wird mit den ausgewählten angreifbaren Elementen erstellt.
5. Füllen Sie im Formular die Felder aus.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Richtlinie	Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft, und der Status des angreifbaren Elements oder der angreifbaren Gruppe von zurückgestellt in Offen ändert. **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf nicht überschreiten **Maximale Ausnahmedauer (Tage)** Die Sie für die Richtlinie in festgelegt haben GRC: Richtlinien- und Compliance-Management. Weitere Informationen finden Sie unter Erstellen Sie eine Richtlinie .
Grund	Grund für die Anforderung einer Ausnahme.
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Korrekturbesitzer ausgefüllt werden.

6. Klicken Sie auf **Absenden**.
   Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Korrekturbesitzer und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management .

Genehmigen oder lehnen Sie eine Ausnahmeanforderung in ab Vulnerability Response

Genehmigen oder lehnen Sie die Ausnahmeanforderungen für angreifbare Elemente oder Korrekturaufgaben ab, die nicht sofort behoben werden können. Sie müssen diese

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen auf Risiko bewerten und sie dann zur Zurückstellung genehmigen, bis sie behoben werden können.

Wichtig:

Sie können die Ausnahmeanforderungen in genehmigen oder ablehnen Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle: sn_vul.Exception_Approver

Sie können Ausnahmeanforderungen auch in der klassischen Umgebung genehmigen.

Hinweis:

Ab v21.0 von Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Meine Genehmigungen**an.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Arbeiten mit einer Ausnahmeregel

Sie können eine Ausnahme für Schwachstellen, angreifbare Elemente (VIS) oder Konfigurationselemente (Configuration Items, CIs) anfordern, die nicht sofort behoben oder zurückgestellt werden können. Durch die Automatisierung des VI-Zurückstellungsprozesses können Sie die übereinstimmenden VIS basierend auf der Regel zurückstellen, wenn das System sie identifiziert.

Sie können die folgenden Aufgaben für eine Ausnahmeregel ausführen:

- Ausnahmeregel erstellen
- Antrag auf Ausnahmeregel genehmigen
- Ausnahmeregel aktivieren
- Öffnen Sie eine Ausnahmeregel erneut
- Aktualisieren Sie eine genehmigte Ausnahmeregel
- Ausnahmeregel löschen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Ab v21.0 von Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Ausnahmeregel erstellen

Erstellen Sie eine Regel, um automatisch eine Ausnahme für eine bestimmte Bedingung für eine Gruppe angreifbarer Elemente (VIS) anzufordern, z. B. eine Regel mit einer Bedingung, die auf dem Schwachstellenschweregrad dieser VIS basiert. Mit dieser Regel können Sie neue und vorhandene VIS automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Regel wird vom Datum „gültig ab“ bis zum Datum „gültig bis“ angewendet.
Die Korrekturaufgabe (VUL) wird erstellt, wenn die Regel genehmigt wird. Die Gruppierungsmethode für diese SCHWACHSTELLE wird als Ausnahmeregeln bezeichnet. Der WIDERRUF wird im Status zurückgestellt erstellt. Sie können diese ÄNDERUNG nicht schließen, erneut öffnen oder löschen. Neue und erneut geöffnete VIS werden vom Datum „gültig ab“ bis zum Datum „gültig bis“ zurückgestellt und diesem WIDERRUF hinzugefügt.

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des Workflows für Ausnahmeregeln gesendet. Diese E-Mails enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahmeregel angefordert wird, erhält die anfordernde Person eine E-Mail, die bestätigt, dass die Anforderung übermittelt wurde.

Hinweis:

Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann erneut zur Genehmigung übermitteln.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**an.
2. Klicken Sie auf der Seite „Ausnahmeregel – neuer Datensatz“ auf **Neu** Dient zum Erstellen einer Regel.
3. Füllen Sie im Formular die Felder aus.

Formular „Ausnahmeregel“

Feld	Beschreibung
Name	Name der Ausnahmeregel.
Gültig ab	Datum, ab dem diese Regel aktiv ist, um die VIS aufzuschieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Gültig bis	Datum, ab dem die Korrekturaufgabe keine neuen VIS mehr akzeptiert.
Grund	Grund für die Erstellung dieser Ausnahmeregel.
Zuweisungsgruppe	Gruppe, der die Korrekturaufgabe zugewiesen ist, die für die Nachverfolgung der zurückgestellten VIS erstellt wurde.
Zusätzliche Information	Zusätzliche Informationen, die die anfordernde Person dem Genehmiger bereitstellen möchte. Diese Informationen werden im Beschreibungsfeld der Korrekturaufgabe ausgefüllt.
Bedingung	Filterbedingung für die VIS, die bei der Verarbeitung der VIS definiert werden kann.
Für vorhandene Daten ausführen	Option, mit der Sie diese Regel bei der ersten Ausführung dieser Regel für vorhandene Daten ausführen können.
Workflow-Phase	Aktueller Genehmigungsstatus der Ausnahmeregel.
Status	Status der Ausnahmeregel.
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausnahmeregel.
Zurückgestellt bis	Datum, bis zu dem die VULs und VIS zurückgestellt werden. An diesem Datum wird die erstellte ÄNDERUNG geschlossen, alle VIS werden aus der Gruppe entfernt, und Gruppenregeln werden erneut angewendet.

4. Fügen Sie die Zuweisungsgruppe hinzu, wenn Sie die Regel erstellen.
5. Übermitteln Sie das Formular zur Genehmigung.
   Der Status der Anforderung ändert sich in „in Überprüfung“. Bis Sie die Ausnahmeregel übermitteln, bleibt sie im Status Entwurf.

Antrag auf Ausnahmeregel genehmigen

Bewerten Sie Ausnahmeregelanforderungen von Anwendern, damit Sie diese Anforderungen genehmigen oder ablehnen können.

Vorbereitungen

Erforderliche Rolle: sn_vul.Exception_Approver

Warum und wann dieser Vorgang ausgeführt wird

Die Mitglieder der Anwendergruppe „Ausnahmegenehmiger“ der Ebene 1 können die Anforderungen der Ausnahmeregel der Ebene 1 genehmigen. Ebenso können die Mitglieder der Anwendergruppe „Ausnahmegenehmiger“ der Ebene 2 die Anforderungen der Ausnahmeregel der Ebene 2 genehmigen. Beide Anwendergruppen erben standardmäßig die Ausnahmegenehmigerrolle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn Sie die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht zurück in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für das Ausnahmemanagement und falsch positive Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Meine Genehmigungen**an.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung mit ab, und erklären Sie, warum Sie die Anforderung genehmigt oder abgelehnt haben.
   Nachdem eine Ausnahmeregel genehmigt wurde, wird standardmäßig eine Korrekturaufgabe im Status zurückgestellt erstellt. Ab dem Datum „gültig ab“ wird diese Regel für alle erstellten VIS und auch für die VIS ausgeführt, die vom Status „Geschlossen“ in den Status „Offen“ verschoben werden. VIS, die den definierten Bedingungen entsprechen, werden der RT hinzugefügt und für den angegebenen Zeitraum zurückgestellt.

   Hinweis:
   Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann erneut zur Genehmigung übermitteln.

Ausnahmeregel aktivieren

Eine Regel wird am Datum „gültig ab“ aktiviert. Nach der Aktivierung wird der Ausnahmeprozess für angreifbare Elemente (VIS) automatisiert.

Die Ausnahmeregel folgt diesem Lebenszyklus:

1. Die neuen angreifbaren Elemente (VIS), die Sie erstellen oder erneut öffnen und die die angegebene Bedingung erfüllen, werden zurückgestellt. Wenn Sie die Option für vorhandene Daten ausführen aktivieren, wenn Sie die Ausnahmeregel zum ersten Mal ausführen, werden alle aktiven und nicht zurückgestellten VIS, die der Ausnahmeregelbedingung entsprechen, in die neu erstellte Korrekturaufgabe (RT) verschoben, und ihr Status wird in zurückgestellt geändert.
2. Wenn ein neu erstelltes VI der Ausnahmeregelbedingung entspricht, wird es in die zurückgestellte RT verschoben, die der Regel zugeordnet ist, und die Gruppenregel wird nicht dafür ausgeführt.
3. Am Datum „gültig ab“ werden vorhandene VIS hinzugefügt, wenn Sie die Option für vorhandene Daten ausführen aktivieren.
4. Die RT akzeptiert keine neuen VIS, wenn die Regel am Datum „gültig bis“ abläuft. Die RT bleibt bis zum Datum „zurückgestellt bis“ vorhanden.
5. Die Ausnahmeregel läuft am Datum „gültig bis“ ab.

Fordern Sie eine Verlängerung für eine Ausnahmeregel an

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor sie das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Exception_Approver

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch eine Verlängerung über anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Vulnerability Manager-Arbeitsbereich an.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Ausnahmeregeln**an.
2. Wählen Sie eine genehmigte Ausnahmeregel aus.
3. Wählen Sie Aus **Verlängerung Anfordern** .
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel erweitert werden muss.
Grund	Geben Sie den Grund für die Zurückstellung der Ausnahmeregel ein. Zur Auswahl stehen: ○ Risiko akzeptiert ○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Felder Zurückgestellt bis, Grund und zusätzliche Informationen für die Ausnahmeregel und die zugehörigen Korrekturaufgaben und angreifbaren Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktualisiert. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion durch den Genehmiger ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben nicht verfügbar, die als Teil einer Ausnahmeregel erstellt werden.
- Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End.
- Ab v21.0 von Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Öffnen Sie eine Ausnahmeregel erneut

Öffnen Sie eine Ausnahmeregel erneut, die abgelehnt wurde, Sie aber erneut übermitteln möchten. Durch erneutes Öffnen der Regel wird sie in den Status Entwurf versetzt.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Regel dann aktualisieren und erneut zur Genehmigung übermitteln.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**an.
2. Suchen Sie die Regel, die Sie erneut öffnen möchten, und klicken Sie auf **Erneut Öffnen** .
3. Aktualisieren Sie das Formular, und übermitteln Sie es erneut zur Genehmigung.

Aktualisieren Sie eine genehmigte Ausnahmeregel

Brechen Sie eine genehmigte Regel ab, um sie aktualisieren zu können. Bevor Sie beispielsweise Daten ändern oder einer genehmigten Regel eine Bedingung hinzufügen können, müssen Sie sie abbrechen, damit die Korrekturaufgabe (VUL) gelöscht wird und die angreifbaren Elemente (VIS) in den Status Offen versetzt werden.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Gruppenregeln werden erneut auf diese VIS angewendet. Übermitteln Sie die Regel, nachdem Sie die Änderungen vorgenommen haben, damit sie erneut den Genehmigungsprozess durchläuft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**an.
2. Öffnen Sie die Ausnahmeregel, die Sie abbrechen möchten, und klicken Sie auf **Abbrechen** .
3. Klicken Sie im Dialogfeld Abbruchregel auf **Abbruchregel** .
   Die Regel wird in den Status Entwurf zurückversetzt, und die zugehörige ANNULLIERUNG wird gelöscht. Die zugehörigen VIS werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen VIS angewendet.

Ausnahmeregel löschen

Löschen Sie eine Ausnahmeregel, die nicht mehr erforderlich ist. Sie können beispielsweise eine Regel löschen, wenn Sie ein angreifbares Element (VI) während der Erfassung nicht zurückstellen möchten.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Durch das Löschen einer Regel wird die zugehörige Korrekturaufgabe abgebrochen (VUL). Die zugehörigen VIS werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen VIS angewendet.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Ausnahmeregeln**an.
2. Öffnen Sie die Ausnahmeregel, die Sie löschen möchten, und klicken Sie auf **Löschen** .
3. Klicken Sie im Dialogfeld Regel löschen auf **Regel löschen** Zum Löschen der ausgewählten Regel.
   Die zugehörige Korrekturaufgabe wird ebenfalls gelöscht. Die zugehörigen VIS werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen VIS angewendet.

Markieren und genehmigen eines falsch positiven Elements

Angreifbare Elemente (VIS) und Korrekturaufgaben (VULs) können als falsch positive Ergebnisse markiert werden. Genehmiger mit Schreibzugriff können solche Anforderungen von anderen Anwendern genehmigen.

- Als falsch positiv markieren
- Massenbearbeitung für falsch positiv
- Genehmigen Oder lehnen Sie ab Falsch positiv

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des falsch positiven Workflows gesendet und geben den Status und andere Details einer Anforderung an. Wenn beispielsweise ein VI oder eine Korrekturaufgabe als falsch positiv markiert ist, erhält die anfordernde Person eine Bestätigungs-E-Mail. Gleichzeitig erhält der Genehmiger eine E-Mail, in der angegeben wird, dass ein VI oder eine Korrekturaufgabe als falsch positiv markiert wurde.

Ab v21.0 von Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Element in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Element oder die Korrekturaufgabe in den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Als falsch positiv markieren

Markieren Sie ein angreifbares Element (VI) oder eine Korrekturaufgabe (VUL) als falsch positiv, wenn die Warnung des Scanners nicht wirklich ein Problem ist. Wenn beispielsweise ein Konfigurationselement außer Betrieb genommen wurde, der Scanner jedoch weiterhin ein Problem damit auslöst, markieren Sie es als falsch positiv.

Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer

Sie können falsch positive Ergebnisse von anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie ein falsch positives Ergebnis für ein angreifbares Element oder eine Korrekturaufgabe an.

Sie können auch falsch positive Ergebnisse in der klassischen Umgebung anfordern:

Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente (oder Korrekturaufgaben)** > **Alle**an.
2. Öffnen Sie das VI oder DIE VUL-DATEI, das Sie als falsch positiv markieren möchten, und klicken Sie auf **Als falsch positiv markieren** .
   Das VI oder DAS VUL muss sich in einem befinden **Öffnen** status.
3. Geben Sie im Formular „falsch positiv“ Details in ein **Zusätzliche Informationen** Und klicken Sie auf **Genehmigung Anfordern** .
   Die Anforderung wird zur Genehmigung gesendet, und der Status des VI oder DER ANFECHTUNG ändert sich in **Wird Überprüft** .

Massenbearbeitung für falsch positiv

Verwenden Sie die Massenbearbeitung, um mehrere angreifbare Elemente (Vits) als falsch positiv zu markieren. Wenn mehrere Vits ausgewählt sind, wird eine Korrekturaufgabe mit diesen Elementen erstellt.

Wichtig:

Als Administrator oder Analyst können Sie die Massenbearbeitungsfunktion im Vulnerability Manager-Arbeitsbereich verwenden, um mehrere Vits als falsch positiv zu markieren. Weitere Informationen finden Sie unter Massenbearbeitung für falsch positive Werte im Vulnerability Manager-Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Sie können auch falsch positive Ergebnisse in der klassischen Umgebung anfordern:

Prozedur

1. Navigieren zu **Vulnerability Response** > **Angreifbare Elemente** > **Alle** Und wählen Sie die Elemente aus, die Sie als falsch positiv markieren möchten.
   Die ausgewählten Elemente müssen sich im Status „Offen“, „wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie Auf **Massenbearbeitung** .
3. Füllen Sie im Formular die Felder aus.

Formular „Massenbearbeitung angreifbarer Elemente“

Feld	Beschreibung
Datensatzauswahl	Datensätze, die für die Massenbearbeitung ausgewählt werden sollen.
Status	Status der angreifbaren Elemente. Wählen Sie „Geschlossen“ aus, um sie als falsch positiv zu markieren.
Grund	Substatus für den ausgewählten Status. Wenn Sie als Status Geschlossen ausgewählt haben, wählen Sie hier falsch positiv aus, um sie als falsch positiv zu markieren.
Zuweisung Aufheben	Senden Sie eine Anforderung zum Löschen der Felder Zugewiesen an und Zuweisungsgruppe.
Bevorzugte Lösung	Lösung, die auf die Korrektur aller angreifbaren Elemente ausgerichtet ist, die für die Massenbearbeitung ausgewählt wurden.
Zuweisungsgruppe	Zuweisungsgruppe für das VI Wählen Sie manuell oder mithilfe von Zuweisungsempfehlungen aus, wenn diese Option aktiviert ist.
Arbeitsnotizen	Hinzuzufügende Notizen.

4. Klicken Sie auf **OK**.
   Eine neue Korrekturaufgabe wird erstellt, die die ausgewählten VIS enthält, und diese Aufgabe wird zur Genehmigung gesendet.

Genehmigen Oder lehnen Sie ab Falsch positiv

Als falsch positiver Genehmiger können Sie falsch positive Anforderungen von anderen Anwendern genehmigen oder ablehnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

Als falsch positiver Genehmiger können Sie die falsch positiven Anforderungen in genehmigen oder ablehnen Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.false_positive_Approver für angreifbare Elemente
- sn_vul.App_false_positive_Approver für angreifbare Anwendungselemente

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellen** > **Meine Genehmigungen**an.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Hinweis:

Ein falsch positiver Wert kann zeitgebunden sein. Nur der Genehmiger kann das Enddatum festlegen.

Analytics- und Reporting-Lösungen für Vulnerability Response

Die Überwachung der Schwachstellenkorrektur umfasst die Anzeige von Trends, das Risikomanagement und die Überwachung von Zuweisungsgruppen. Sie können Probleme mit hohem Risiko, Arbeitsauslastungen von Zuweisungsgruppen, Zurückstellungen und wiederkehrende Schwachstellen überprüfen. Vulnerability Response Bietet Tools, Berichte und Verfahren, um diesen Prozess produktiver und effizienter zu gestalten.

Datenvisualisierungen in Vulnerability Response Arbeitsbereiche

Die Vulnerability Response Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie Ihren Korrekturfortschritt überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen, die aktualisiert werden, wenn sich Schwachstellendaten ändern. Siehe Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen erkunden Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen.

Schwachstellenanalysten können auch Standard verwenden Vulnerability Response Dashboards in **Alle** > **Vulnerability Response** > **Übersicht**an.

Wichtig:

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard kann auch in der neuen Experience-UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** Und klicken Sie auf **Dashboards** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Dashboards im Vulnerability Manager-Arbeitsbereich Und Dashboards im Arbeitsbereich „IT-Korrektur“ .

Hinweis:

Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Korrekturprozess

Die meisten Schwachstellenkorrekturen werden über den Korrekturaufgabendatensatz innerhalb von durchgeführt Vulnerability Response Arbeitsbereiche. Über die Korrekturaufgaben (RTS) im Status „wird untersucht“ können Sie mehrere Aufgaben ausführen.

- Erstellen Sie Change-Anforderungen.
- Fügen Sie Arbeitsnotizen und Beschreibungen von Schwachstellen innerhalb der Korrekturaufgabe hinzu.
- Verschieben Sie die Korrekturaufgabe und die darin enthaltenen angreifbaren Elemente auf ein späteres Datum.
- Schließen Sie die Korrekturaufgabe.
- Verfolgen Sie neue regulatorische Compliance-Verpflichtungen nach, die normalerweise zeitabhängig sind.

- Melden Sie sich bei der Vulnerability Response-Instanz an.
- Überprüfen Sie Ihre Schwachstellenmanagement- und Drittanbieter-Dashboards und -Berichte, um Problembereiche zu finden. Zeigen Sie beispielsweise Dashboards an, die die Fälligkeit von Korrekturaufgaben (RT) nach status oder angreifbaren Elementen mit hohem Risiko (VIS) nach ihrem Korrekturzieldatum anzeigen.
- Überprüfen Sie den Status der Korrekturaufgaben in der Reihenfolge des Risikos.
- Überarbeiten Sie die Priorisierung für die Aufgaben, indem Sie Ihre Risikopunktzahlrechner anpassen, wenn die Risikopunktzahl nicht korrekt berechnet wird, oder VIS oder RTS nach Bedarf zurückstellen. Siehe Vulnerability Response Rechner und Regeln für Schwachstellenrechner Oder Eine Korrekturaufgabe zurückstellen Weitere Informationen zu diesen Optionen.
- Überprüfen Sie zurückgestellte angreifbare Elemente, die kurz vor der erneuten Öffnung stehen, und ergreifen Sie bei Bedarf weitere Maßnahmen. Wenn Sie Change-Aktivitäten für Ihre Assets, Korrekturaufgaben und die entsprechenden angreifbaren Elemente initiieren und nachverfolgen möchten, finden Sie weitere Informationen unter Change-Management für Vulnerability Response Für weitere Aktionen.
- Überprüfen Sie das Feedback von IT Operations.

  Sobald Sie benachrichtigt werden, dass eine Change-Anforderung gelöst wurde, warten Sie auf den nächsten Scan. Scans werden automatisch durch den im Setup-Assistenten konfigurierten Importzeitplan einer Drittpartei ausgelöst.

- Wenn der Status nach einem Scan behoben ist, werden angreifbare Elemente während des Imports automatisch geschlossen. Die Gruppe wird geschlossen, wenn alle angreifbaren Elemente in der Gruppe behoben sind.
- Wenn der Status nach dem Scan nicht behoben ist, wird das VI automatisch wieder in „wird untersucht“ verschoben.

- Angreifbare Elemente, die in Ihrer Instanz auf „gelöst“ festgelegt sind, aber nicht von den Integrationsausführungen der Drittpartei in den Status „Geschlossen/behoben“ versetzt wurden, werden erneut geöffnet, wenn sie bei erneuten Scans erkannt werden.

  Für Qualys Erkennungen: Wenn der Scanner weiterhin VIS findet, die auf „gelöst“ festgelegt wurden, aber dann nicht durch nachfolgende Scans in „Geschlossen/behoben“ versetzt wurden, werden diese VIS wieder in „Offen“ verschoben, wenn das Datum der letzten Suche nach dem Datum der Lösung liegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Rapid7 Erkennungen ist jetzt eine Option auf der verfügbar Rapid7 Konfigurationsseite in Ihrer Instanz zum erneuten Öffnen gelöster VIS nach Alter. Wenn diese Option aktiviert ist, werden VIS auf „gelöst“ festgelegt, aber dann nicht auf „Geschlossen/behoben“ umgestellt, indem nachfolgende Scans nach der von Ihnen eingegebenen Anzahl von Tagen zurück zu „Offen“ übergehen.

Vulnerability Solution Management Bereitstellungsfortschritt

Umfassende Bereitstellungsmetriken für Korrekturaufgaben und Schwachstelleneinträge sind in enthalten Vulnerability Solution Management Unter **Korrekturstatus** In Schwachstellen, angreifbare Elemente. Identifizieren Sie einfach, welche Korrekturaufgabe oder Schwachstelle den Lösungsfortschritt verlangsamt. Details dazu, wie die Schwachstelle identifiziert wird oder welche Aspekte der betroffenen Assets das Korrekturproblem verursachen können. Aktualisieren Sie den Status Ihrer Metriken mit **Status aktualisieren** Zugehöriger Link in den Formularen für Schwachstellen, Lösungen und Korrekturaufgaben.

Wird standardmäßig verwendet Vulnerability Response Dashboards

Die Vulnerability Response Das Übersichts-Dashboard (Vulnerability Management) bietet einen Überblick über Schwachstellen und angreifbare Elemente, sodass der Schwachstellenadministrator Problembereiche schnell erkennen kann. Die Vulnerability Response Mit dem Korrektur-Dashboard (Schwachstellenkorrektur) kann sich ein Korrekturspezialist auf die Korrekturaufgaben und angreifbaren Elemente konzentrieren, die er besitzt.

Datenvisualisierungen in Vulnerability Response Arbeitsbereiche

Die Vulnerability Response Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie Ihren Korrekturfortschritt überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen, die aktualisiert werden, wenn sich Schwachstellendaten ändern. Siehe Vulnerability Response Arbeitsbereiche, Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen erkunden Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen.

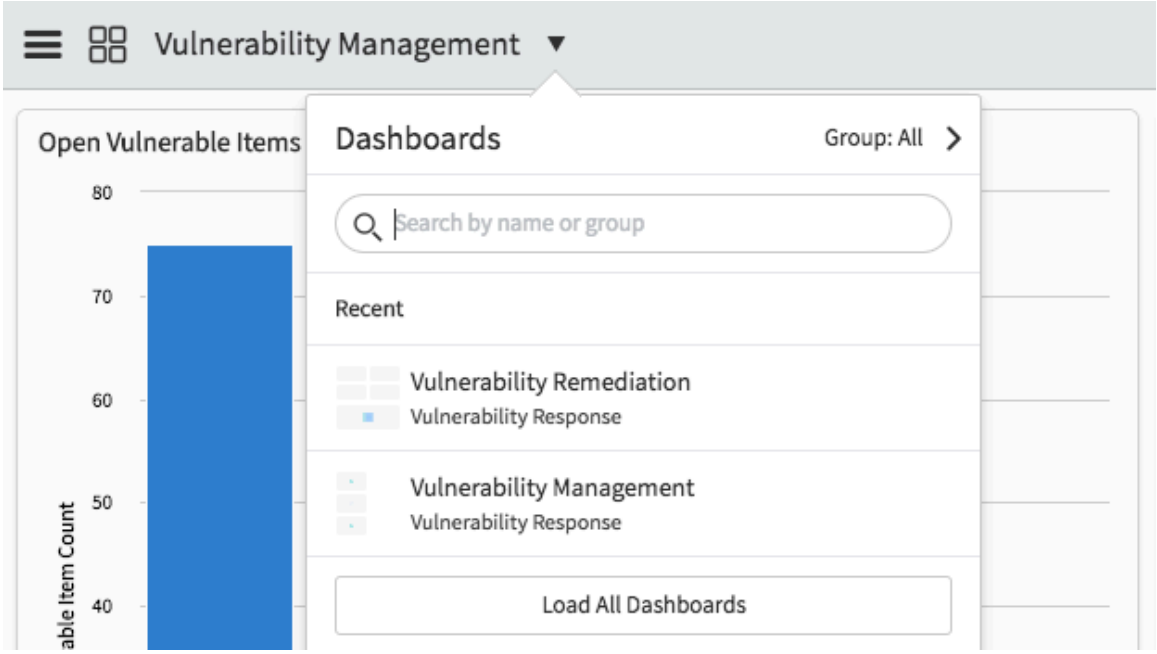
Schwachstellenanalysten können auch Standard verwenden Vulnerability Response Dashboards.

Erforderliche Rollen: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst und Anwender mit sn_vul.Vulnerability_read (oder die die Rolle sn_vul.Vulnerability_read erben) und PA_Viewer.

Der Standard Vulnerability Response Dashboards in der Legacy-Umgebung

Diese Berichte sind als Teil von enthalten Performance Analytics for Vulnerability Response Anwendung und erfordern kein separates Abonnement. Um eine zu öffnen, wählen Sie die Auswahlliste aus, um sie zu erweitern, und wählen Sie ein Dashboard aus. Alternativ können Sie den Namen eines Dashboards in das Suchfeld eingeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

Wenn Performance Analytics Inhaltspaket für Vulnerability Response Die Anwendung wird installiert und aktiviert. Das Dashboard „Vulnerability Management“ (PA) wird automatisch im Modul „Übersicht“ angezeigt. Dieses Dashboard enthält Berichte, die alle Phasen des Schwachstellenmanagement-Lebenszyklus abdecken.

Für Informationen zu den Berichten im Performance Analytics-Inhaltspaket für Vulnerability Response, Siehe Dashboard „Schwachstellenmanagement“ [PA] .

Informationen zum CISO-Dashboard und den Berichten zur Scan-Abdeckung finden Sie unter Schwachstellenmanagement-CISO-Dashboard .

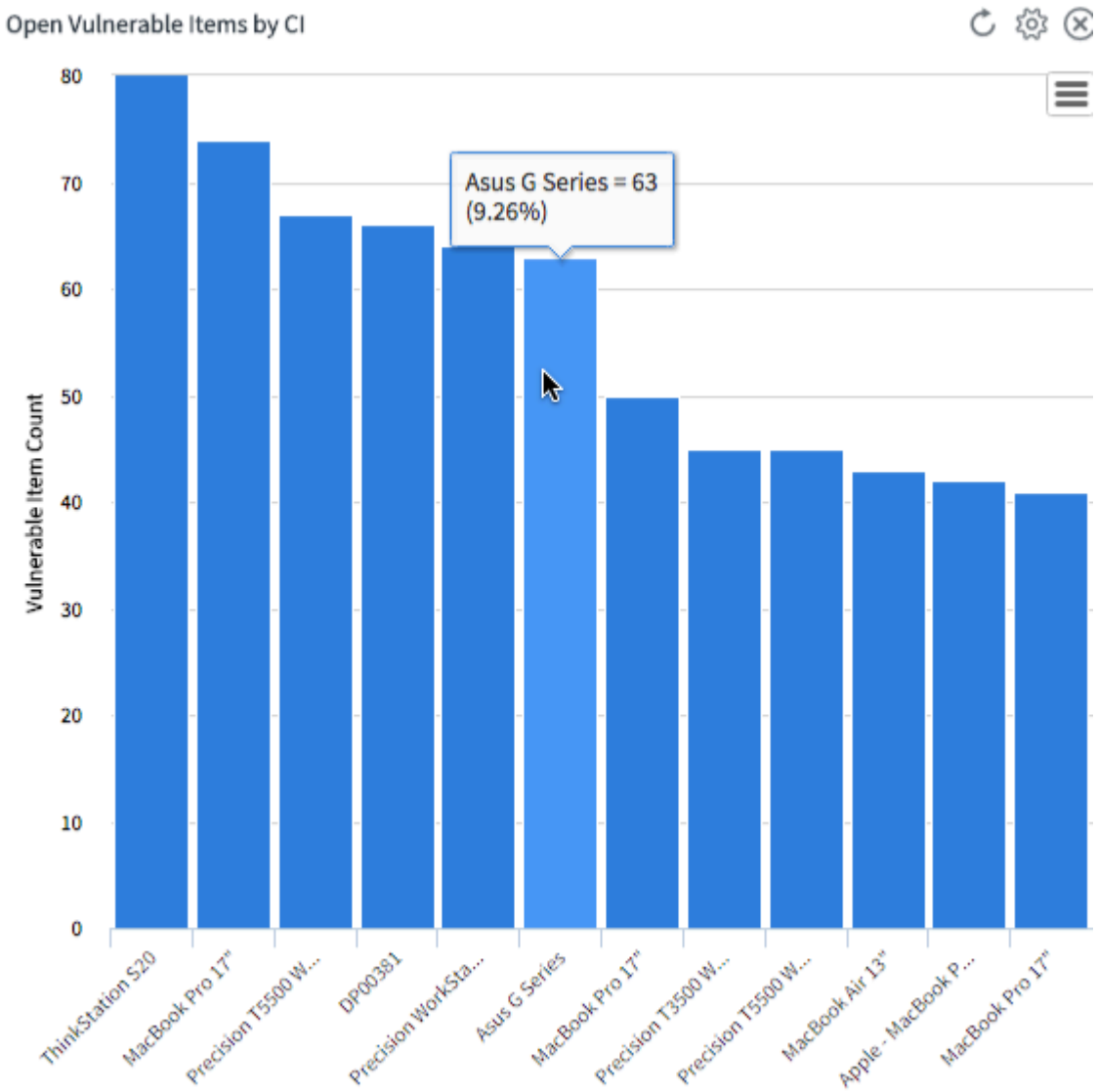
Dashboard „Schwachstellenmanagement“

In jedem Diagramm können Sie auf einen beliebigen Teil eines Diagramms zeigen (Balken, Kreis, Datenpunkt usw.), um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Wenn Sie auf einen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Hinweis:

Wenn anwenderdefinierte Dashboards erforderlich sind, finden Sie unter Erstellen und verwenden Sie Dashboards Weitere Informationen finden Sie unter .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Berichte zur Schwachstellenübersicht

Name	Visuell	Beschreibung
Offene angreifbare Elemente nach CI	Balkendiagramm	Zeigt die Anzahl der offenen angreifbaren Elemente an, die für jedes Konfigurationselement (CI) aufgezeichnet wurden, von den meisten bis zum wenigsten.
Angreifbare Elemente nach Korrekturzielstatus	Balkendiagramm	Zeigt die Anzahl der angreifbaren Elemente an, die sich dem Ziel, dem laufenden und dem veralteten Ziel nähern. **Hinweis:** Elemente im Status „zurückgestellt“, „gelöst“ oder „Geschlossen“ sind nicht enthalten.
Zurückgestellte angreifbare Elemente, die diese Woche ablaufen	Diagramm	Zeigt die Anzahl der zurückgestellten angreifbaren Elemente an, die innerhalb von sieben Tagen erneut aktiviert werden sollen.
Offene angreifbare Elemente nach Schwachstelle	Balkendiagramm	Zeigt die Anzahl der offenen angreifbaren Elemente für jede Schwachstelle an, von den meisten bis zu den geringsten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berichte zur Schwachstellenübersicht (Fortsetzung)

Name	Visuell	Beschreibung
Schwachstellen nach Modell	Balkendiagramm	Zeigt die Anzahl der angreifbaren Elemente an, die für jedes Modell (CI-Klasse) aufgezeichnet wurden, von den meisten bis zu den wenigsten.
Schwachstellen nach Woche	Trend	Zeigt die Anzahl der pro Woche aufgezeichneten Schwachstelleneinträge an.
Modelle mit den meisten Schwachstellen	Ring	Zeigt Modelle (CI-Klassen) mit den am stärksten angreifbaren Elementen an.
Schwachstellen nach Herausgeber	Balkendiagramm	Zeigt die Anzahl der für jeden Herausgeber aufgezeichneten angreifbaren Elemente an, von den meisten bis zu den wenigsten.
Schwachstellen nach Impact	Balkendiagramm	Zeigt die Anzahl der Schwachstelleneinträge für betroffene Netzwerktypen an.
Herausgeber mit den meisten Schwachstellen	Ring	Zeigt Herausgeber mit den am stärksten angreifbaren Elementen an.
CIs mit den meisten Schwachstellen	Ring	Zeigt CIs mit den am stärksten angreifbaren Elementen an.
Schwachstellen nach Punktzahl	Balkendiagramm	Zeigt die Anzahl der Schwachstelleneinträge nach Schwachstellenpunktzahlen an.
Erneut geöffnete angreifbare Elemente	Liste	Listet die erneut geöffneten angreifbaren Elemente und ihr Alter auf.
CIs mit den meisten Schwachstellen nach Klasse	Ring	Zeigt CIs mit den am stärksten angreifbaren Elementen an.
Alter des angreifbaren Elements	Liste	Listet die Anzahl der Tage auf, seit angreifbare Elemente zuletzt geöffnet wurden.
CIs mit Schwachstelle nach Datum	Liste	Listet Konfigurationselemente auf, die in den letzten 30 Tagen gescannt wurden.
CIs nicht gescannt	Liste	Listet Konfigurationselemente auf, die noch nie auf Schwachstellen gescannt wurden.

Dashboard für Schwachstellenkorrekturen

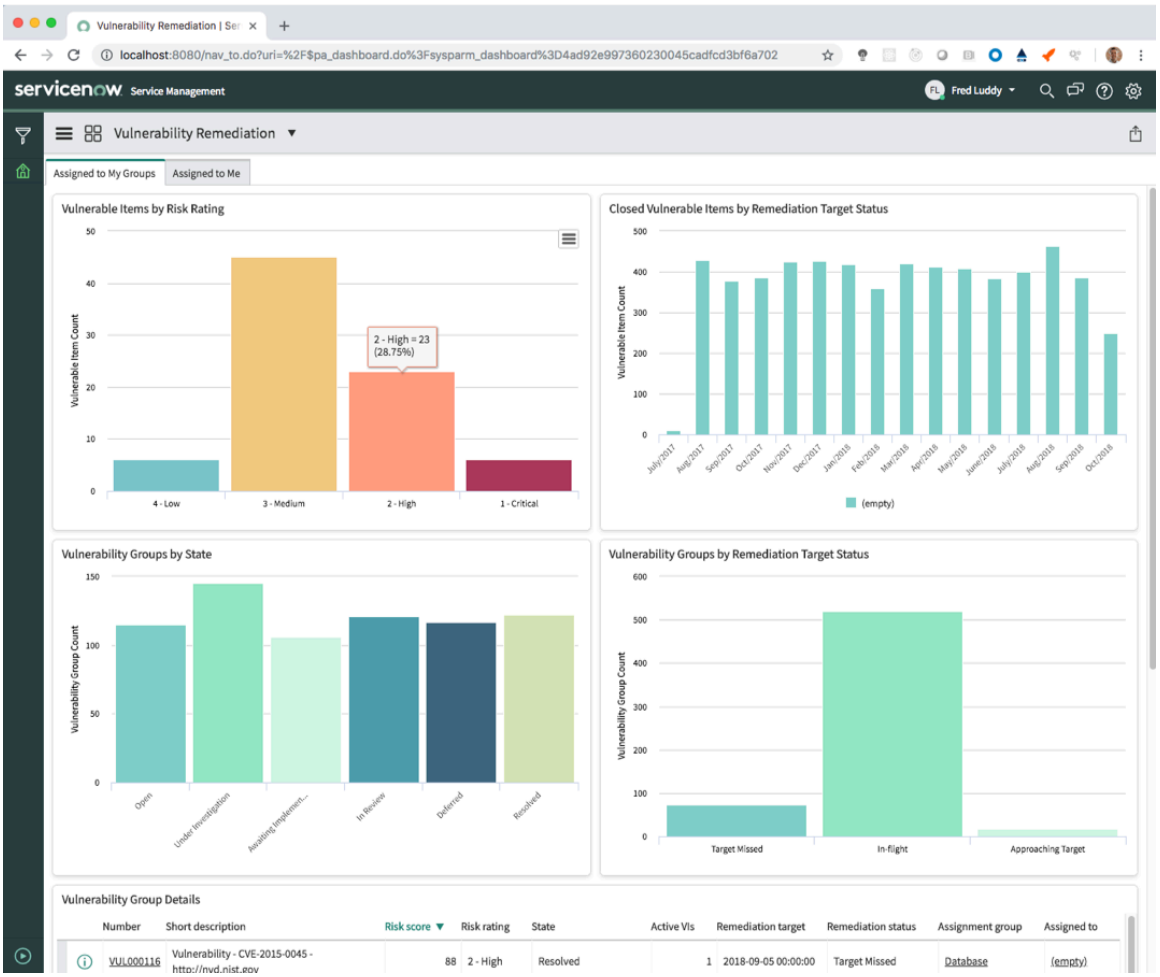
Ab Version 19,0 von Vulnerability Response, Dieses Dashboard ist in der neuen Experience-UI verfügbar.

Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Das Dashboard „Schwachstellenkorrektur“ enthält die folgenden Registerkarten: **Meinen Gruppen zugewiesen** , **Mir zugewiesen** , Und **Von mir angefordert** . Auf den Registerkarten „Zugewiesen an meine Gruppen“ und „mir zugewiesen“ werden dieselben Berichte angezeigt. Die erste Registerkarte berichtet nach den Zuweisungsgruppen, denen Sie angehören, und die Letztere nach angreifbaren Elementen oder Korrekturaufgaben, die Ihnen zugewiesen sind. Auf der Registerkarte „angefordert von mir“ werden die von Ihnen angeforderten falsch positiven Ergebnisse und Ausnahmen gemeldet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard für Schwachstellenkorrekturen



Automatische Übersetzung

Berichte

Meinen Gruppen zugewiesen und mir zugewiesen

Name	Visuell	Beschreibung
Angreifbare Elemente nach Risikobewertung	Balken	Anzahl der aktiven angreifbaren Elemente, gruppiert nach Risikobewertung für die ausgewählte Zeitspanne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Meinen Gruppen zugewiesen und mir zugewiesen (Fortsetzung)

Name	Visuell	Beschreibung
Geschlossene angreifbare Elemente nach Korrekturzielstatus	Balken	Anzahl der geschlossenen angreifbaren Elemente, gruppiert nach Nachbesserungszielstatus für die ausgewählte Zeitspanne.
Korrekturaufgaben nach Status	Balken	Anzahl der aktiven Korrekturaufgaben (RTS) gruppiert nach Status.
Korrekturaufgaben nach Status des Korrekturziels	Balken	Anzahl der aktiven RTS, gruppiert nach Korrekturzielstatus. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.
Details zur Korrekturaufgabe	Liste	Korrekturaufgaben-Datensatzdetails in einer Liste.

Angefordert von mir

Name	Visuell	Beschreibung
Status von Ausnahme- und falsch positiven Anforderungen	Balken	Anzahl der aktiven Anforderungen von Ihnen.
Ablaufende zurückgestellte und falsch positive Korrekturaufgaben	Balken	Anzahl der zurückgestellten und falsch positiven Korrekturaufgaben (RTS), gruppiert nach bis-Datum.

Dashboard „Schwachstellengenehmigungen“

Das Dashboard „Schwachstellengenehmigungen“ enthält die folgenden Berichte für Ausnahmen und falsch positive Genehmiger.

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard ist in der neuen Experience-UI verfügbar.

Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Name	Visuell	Beschreibung
Ausnahme- und falsch positive Anforderungen nach Alter meiner ausstehenden Genehmigungen	Balken	Anzahl der für Sie ausstehenden Genehmigungen, gruppiert nach Erstellungsdatum.
Meine Genehmigung und abgelehnte Ausnahme und falsch positive Anforderungen	Balken	Anzahl der genehmigten oder abgelehnten Genehmigungsanforderungen, gruppiert nach Genehmigungsstatus.
Alle Korrekturaufgaben nach Risikobewertung – Genehmigung ausstehend	Balken	Anzahl der Korrekturaufgaben mit ausstehender Genehmigung, gruppiert nach Risikobewertung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Visuell	Beschreibung
Alle ausstehenden und falsch positiven Genehmigungsanforderungen gruppiert nach Grund	Balken	Anzahl der ausstehenden Genehmigungsanforderungen, gruppiert nach Grund.

Platform Analytics-Lösungen Für Schwachstellenmanagement

Platform Analytics-Lösungen enthalten vorverpackte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen ServiceNow AI Platform-Produkten. Mit dieser Analytics- und Reporting-Lösung können Sie das Volumen, die Leistung und den Fortschritt von Schwachstellen nachverfolgen, von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur. Sie können Berichte nach Zuweisungsgruppe, Exploits, Risikobewertung oder Status filtern.

Die Performance Analytics for Vulnerability Response Inhaltspaket wird nicht automatisch mit installiert Vulnerability Response Anwendung. Sie ist im verfügbar ServiceNow Store Als separates Abonnement.

Performance Analytics for Vulnerability Response Enthält zwei Dashboards:

- Vulnerability Management (PA)-Dashboard
- Dashboard „Chief Information Security Officer (CISO)“ für Schwachstellenmanagement

Erforderliche Rollen, Installation und Anzeige der Dashboards

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet:

- ServiceNow AI Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Informationen zur Installation dieser Anwendung finden Sie unter Installieren und konfigurieren Sie die Anwendung Performance Analytics für Vulnerability Response [PA] .

Hinweis:
Richten Sie Analytics and Reporting-Lösungen in einer Instanz außerhalb der Produktion ein, und testen Sie sie, bevor Sie sie in der Produktion aktivieren.

Lösungen für Analytik und Berichterstellung bieten alle für die Analyse von Standardanwendungen erforderlichen Konfigurationsdatensätze. Passen Sie diese Datensätze zur Verwendung in Ihrer Produktionsumgebung an.

Navigieren Sie zum Anzeigen des Schwachstellen-Management-Dashboards (PA) zu **Vulnerability Response** > **Übersicht** > **an.**

Navigieren Sie zum Anzeigen des CISO-Dashboards für Schwachstellenmanagement zu **Vulnerability Response** > **CISO-Dashboard** > **an.**

Wichtige Begriffe

Performance Analytics (PA)

Lösung, die Verwaltungs-Dashboards erstellt, Berichte zu KPIs und Metriken erstellt und wichtige Geschäftsfragen beantwortet, um die Qualität zu erhöhen und Kosten zu senken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angreifbares Element (VI)

Eine von einem Schwachstellenscanner einer Drittpartei gemeldete Sicherheitslücke, die auf einem Konfigurationselement (Configuration Item, CI) vorhanden ist.

Nachbesserungsaufgabe

Korrekturaufgaben werden basierend auf der Gruppe, die den angreifbaren Elementen in einer Korrekturmaßnahme zugeordnet ist, erstellt und automatisch IT-Teams zugewiesen. IT-Teams und Korrekturbesitzer zeigen Korrekturaufgaben im Arbeitsbereich „IT-Korrektur“ an. Siehe Vulnerability Response Arbeitsbereiche Weitere Informationen finden Sie unter

an.

PA-Indikator

Definiert eine Leistungsmessung, die in regelmäßigen Abständen eines Business-Service, einer Aktivität oder eines Organisationsverhaltens durchgeführt wird, z. B. nicht zurückgestellte überfällige kritische angreifbare Elemente.

PA-Indikatorquelle

Datensätze, die Datensätze aus einer Tabellen- oder Datenbankansicht filtern, z. B. VI aktiv.

Zeigen Sie Datenvisualisierungen in Echtzeit an

Um zu sehen, was heute mit den wichtigsten Elementen in Ihrem passiert Vulnerability Response Anwendung können Sie bestimmte Berichte im Vulnerability Management (PA)-Dashboard in Echtzeit anzeigen. Durch die sofortige Anzeige dieser Berichte können Sie Ihre wichtigsten angreifbaren Elemente (VIS) verwalten und schnell beheben. Sie können die folgenden Berichte in Echtzeit anzeigen:

- Registerkarte „Übersicht“ – angreifbare Elemente nach Zuweisungsgruppe
- Registerkarte „angreifbare CIs“
  - Angreifbare Konfigurationselemente (CIs) ohne Besitzer
  - Außer Kraft gesetzte oder gestohlene CIs mit aktiven AEs
- Registerkarte „Ausnahmen“
  - Zurückgestellte angreifbare Elemente nach Grund
  - In Kürze ablaufende Zurückstellungsanforderungen
  - Zurückgestellte angreifbare Elemente vom CIO-Manager
- Registerkarte „Korrektur“: Nicht zugewiesene angreifbare Elemente

Weitere Informationen finden Sie unter Zeigen Sie Performance Analytics für Vulnerability Response [PA]-Berichte in Echtzeit an .

Vulnerability Management CISO Dashboard

Mit Vulnerability Management CISO Im Dashboard können Sie Daten wie Leistungskennzahlen (Key Performance Metrics, KPIs) für die Schwachstellenbeseitigung anzeigen, die höchsten Risiken anzeigen, die Scan-Abdeckung überprüfen und erfahren, wie Sie Risiken senken können.

Erforderliche ServiceNow AI Platform-Rollen

- sn_vul.Vulnerability_ciso zum Anzeigen des Dashboards.
- sn_vul.ciso_write zum Bearbeiten des Dashboards.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren des CISO-Dashboards

Um das CISO-Dashboard zu aktivieren, müssen Sie Performance Analytics für installieren Vulnerability Response Und aktivieren Sie den entsprechenden Performance Analytics-Auftrag. Weitere Informationen finden Sie unter Analytics- und Reporting-Lösungen für Vulnerability Response .

Anwendungsfälle

Anwender	Dashboard-Verwendung
Chief Information Security Officers (CISOs)	Chief Information Security Officers (CISOs) können das CISO-Dashboard verwenden, um Einblicke in das Schwachstellenmanagementprogramm für ihre Organisationen zu erhalten. Das Dashboard stellt Daten bereit, mit denen sie Daten auf einen Blick identifizieren können, wie sie die Schwachstellen in ihren Umgebungen verringern können.

Verwenden des CISO-Dashboards

Leitende Anwender, wie die Chief Information Security Officers (CISOs) in Ihrer Organisation, können das CISO-Dashboard für Vulnerability Response anzeigen, um zu verstehen, wie effektiv ihr Schwachstellenmanagementprogramm ist. Sie können das CISO-Dashboard anzeigen, indem Sie zu navigieren **Vulnerability Response** > **CISO-Dashboard**an. Verwenden Sie die Filter der obersten Ebene, um Berichte nach Risikobewertung, Altersbereich oder Internetverbindung zu filtern. Einige Berichte zeigen Trenddaten über einen bestimmten Zeitraum an. Sie können regelmäßig den Trend der wichtigen Metriken anzeigen, das allgemeine Geschäftssicherheitsrisiko analysieren und die Bereiche identifizieren, die verbessert werden müssen.

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard kann auch in der neuen Experience-UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** Und klicken Sie auf **Dashboards** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Dashboards im Vulnerability Manager-Arbeitsbereich Und Dashboards im Arbeitsbereich „IT-Korrektur“ .

Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Geplante Aufgaben werden ausgeführt

Führen Sie die geplanten Aufgaben in dieser Reihenfolge aus, um die Daten in den Berichten zu aktualisieren:

1. Aktualisieren Sie Dashboard-Tabellen
2. [PA VR] CISO-DASHBOARD

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgaben für das CISO-Dashboard

Name der geplanten Aufgabe	Beschreibung
Aktualisieren Sie Dashboard-Tabellen	Tägliche geplante Aufgabe, die Sie vor der Aufgabe [PA VR] CISO-Dashboard ausführen müssen, damit Sie die CISO-Daten erfassen können. Wenn Sie diese geplante Aufgabe ausführen, aktualisieren Sie die Berichte zur Scan-Abdeckung. Die aktualisierten Informationen umfassen die operativen Konfigurationselemente (CIs), die in den letzten 90 Tagen gescannt wurden, ihre Klassen und die Gesamtzahl der operativen CIs, die diesen Klassen entsprechen. Durch die Ausführung dieser geplanten Aufgabe werden die Berichte in aktualisiert **Empfohlene Aktionen** Auch Registerkarte. **Hinweis:** Operative CIs beziehen sich auf die CIs, die einen Betriebsstatus als haben Betriebsbereit .
[PA VR] CISO-DASHBOARD	Nachdem die geplante Aufgabe „Dashboard-Tabellen aktualisieren“ abgeschlossen ist, führen Sie diese geplante Aufgabe aus, um alle Berichte in auszufüllen **CISO-Übersicht** Registerkarte.

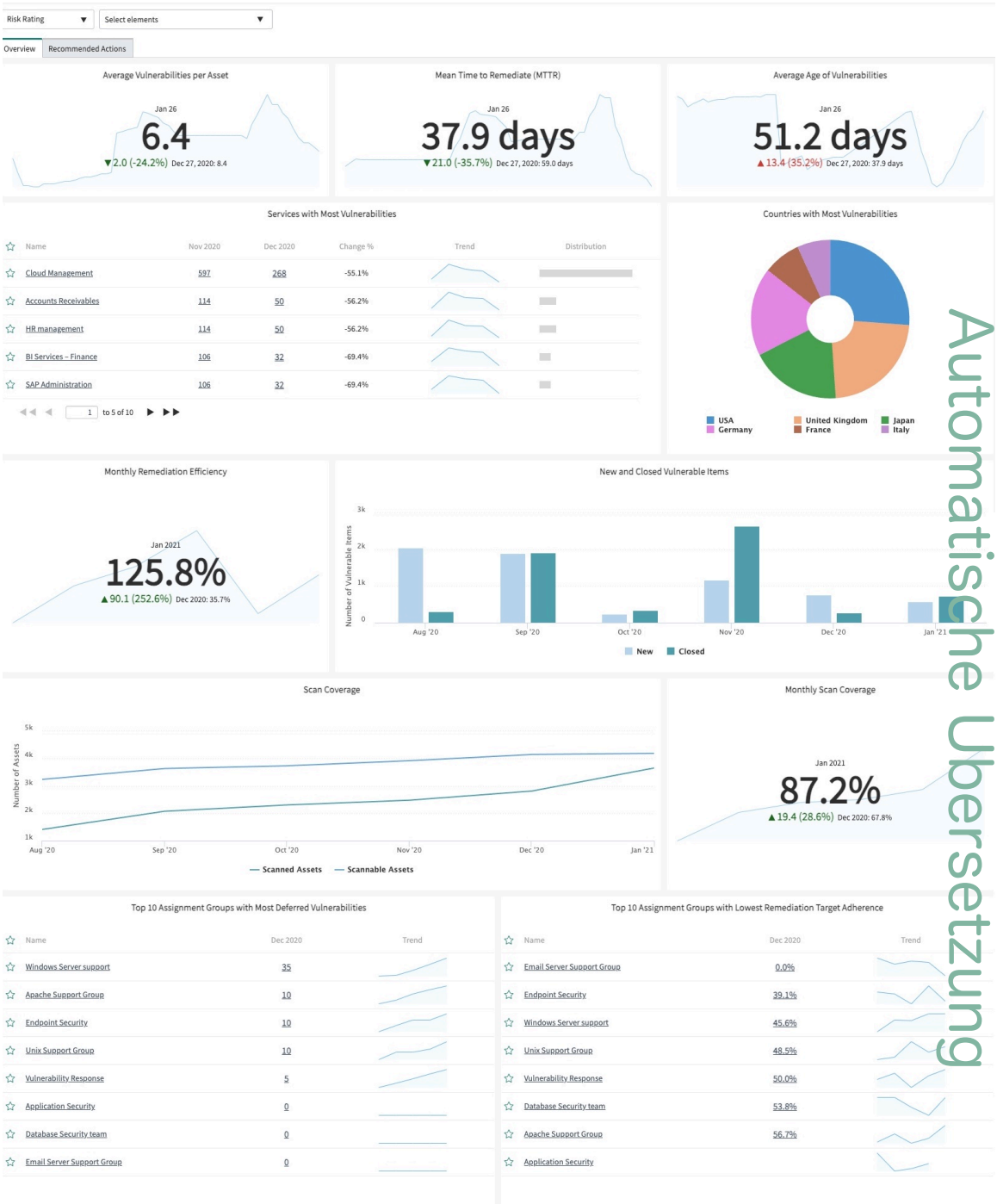
CISO-Dashboard-Registerkarten

Dieses Dashboard bietet einen Einblick in die Risiken im Schwachstellenmanagement. Sie können Schwachstellen und die zugehörigen Daten nach Region, Alter, Services und anderen Aufgliederungen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Übersicht“

Die Registerkarte Übersicht enthält Berichte, die die Sicherheitslage Ihrer Organisation auf einen Blick darstellen.



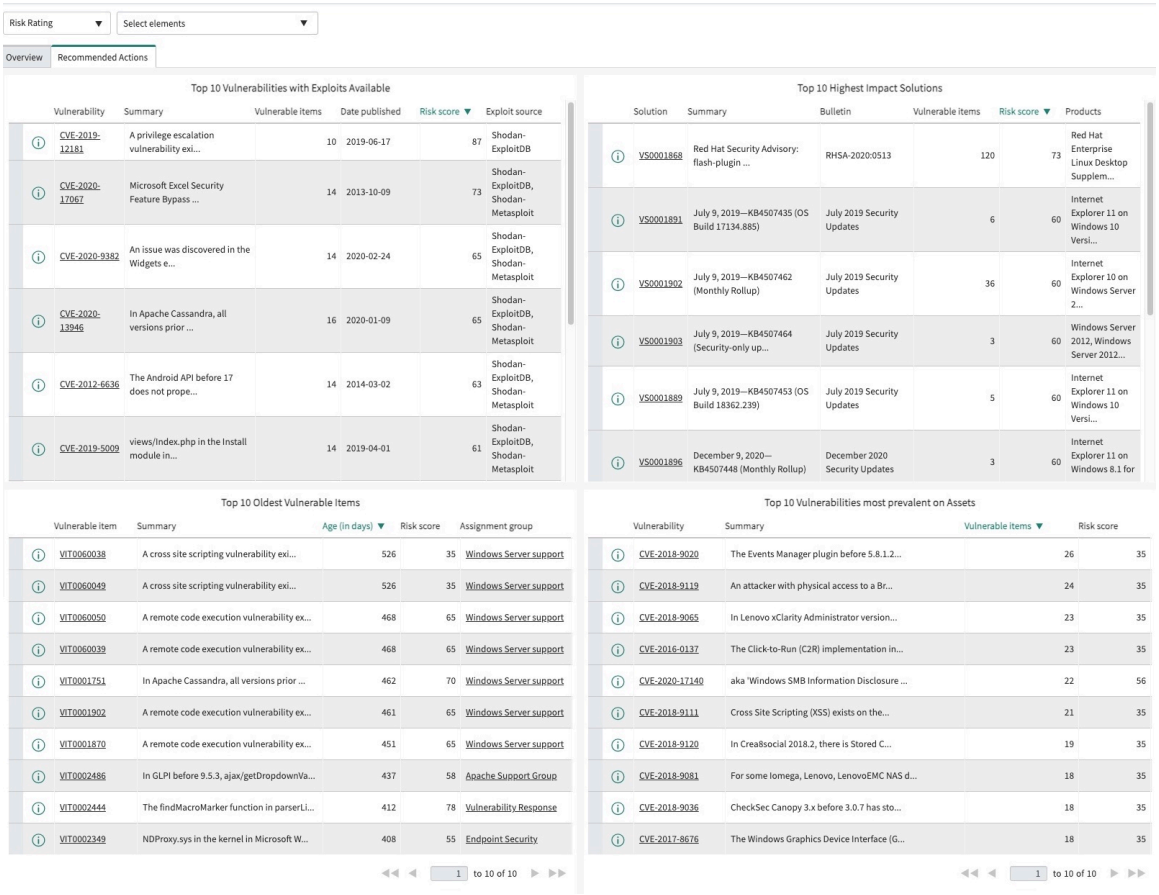
Automatische Übersetzung

Hinweis:
Der Filter der obersten Ebene kann nur für einige Berichte verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „empfohlene Aktionen“

Die Registerkarte empfohlene Aktionen enthält Berichte, die Einblicke in ausnutzbare, veraltete und weit verbreitete Schwachstellen bieten. Es enthält auch Lösungen, die Aktionen zur Reduzierung der Risiken empfehlen. Führen Sie aus **Aktualisieren Sie CISO-Dashboard-Tabellen** Geplante Aufgabe zum Aktualisieren der Berichte auf dieser Registerkarte.



Indikatoren

Um die Indikatoren anzuzeigen, navigieren Sie zu **Performance Analytics** > **Indikatoren**an.

1. Suchen Sie auf der Seite „Indikatoren“ in der Spalte Name nach dem erforderlichen Indikatornamen.
2. Klicken Sie auf den Indikatornamen, um den Datensatz zu öffnen und seine Details anzuzeigen.

   Die Indikatoren für das CISO-Dashboard erfassen standardmäßig keine Datensätze. Sie können Datensätze erfassen, indem Sie das Kontrollkästchen Datensätze sammeln aktivieren.

Summierte Dauer der geschlossenen angreifbaren Elemente

„Gesamtdauer geschlossener VIS“ wird täglich als Tage gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

Scannbare Assets

„Gescannte Assets“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

Services mit den meisten Schwachstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Services mit den meisten Schwachstellen werden täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

Durchschnittliche Schwachstellen pro Asset

[[Aktive angreifbare Elemente]] / [[Aktive angreifbare Konfigurationselemente]

Geschlossene angreifbare Elemente

„Geschlossene angreifbare Elemente“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

Durchschnittliche Zeit bis zur Fehlerkorrektur für angreifbare Elemente

[[Summierte Dauer der geschlossenen angreifbaren Elemente]]/[[Geschlossene angreifbare Elemente]]

Aktuelle Scan-Abdeckung

Berechnet die aktuelle Scan-Abdeckung als Prozentsatz.

Gescannte Assets

„Gescannte Assets“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

Geschlossene angreifbare Elemente (Ziel erfüllt)

„Geschlossene angreifbare Elemente (Ziel erfüllt)“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Maximierung der Punktzahl.

% der geschlossenen angreifbaren Elemente, die das Ziel erfüllt haben

[[Geschlossene angreifbare Elemente (Ziel erfüllt) / Nach Monat SUM]] / [[Geschlossene angreifbare Elemente / Nach Monat SUM]] *100

Aktive angreifbare Elemente

„Aktive angreifbare Elemente“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

Durchschnittliches Alter der angreifbaren Elemente

Das durchschnittliche Alter der aktiven VIS wird täglich als Einheit „Tage“ gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

Hinweis:
Die Anpassung der Berechnung von Alter und Alter geschlossener Elemente (VIS) kann zu einem starken Anstieg oder Rückgang der Performance Analytics (PA)-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung des Alters und des Alters, das für VIS geschlossen wird, finden Sie unter KB1703270 KB-artikel.

Aktive angreifbare Konfigurationselemente

„Aktive angreifbare CIs“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

Effizienz der monatlichen Fehlerbehebung

[Anzahl der während eines Monats geschlossenen angreifbaren Elemente] / [Anzahl neuer oder erneut geöffneter angreifbarer Elemente im selben Monat]

Neue angreifbare Elemente

„Neue angreifbare Elemente“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

Zurückgestellte angreifbare Elemente

„Zurückgestellte VIS“ wird täglich als numerische Einheit gemessen. Das Ziel dieses Indikators besteht in der Minimierung der Punktzahl.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgliederungen

- Zuweisungsgruppe: Gilt für einige VI-Berichte.
- Risikobewertung: Gilt für VI-Berichte.
- Altersbereich: Gilt für VI-Berichte.
- Alter geschlossen: Gilt für Berichte für geschlossene VIS.
- Mit Internetzugriff: Gibt an, ob das CI zur Hardwareklasse gehört und mit Internetzugriff verbunden ist.
- Region: Der verwendete CMDB-CI-Parameter ist Standort. Dieser Standort gibt das Ursprungsland des Konfigurationselements an.

Hinweis:
Die Anpassung der Berechnung von Alter und Alter geschlossener Elemente (VIS) kann zu einem starken Anstieg oder Rückgang der Performance Analytics (PA)-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung des Alters und des Alters, das für VIS geschlossen wird, finden Sie unter KB1703270 KB-artikel.

Datenvisualisierungen

Name	Typ	Beschreibung
Durchschnittliche Schwachstellen pro Asset	Einzelne Punktzahl	Durchschnittliche Anzahl aktiver angreifbarer Elemente pro Konfigurationselement.
Durchschnittliche Zeit bis zur Nachbesserung (MTTR)	Einzelne Punktzahl	Die durchschnittliche Zeit für die Nachbesserung (Schließung) eines angreifbaren Elements, angezeigt als laufender 30-Tage-Durchschnitt. **Hinweis:** Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum der letzten Öffnung und dem Datum und der Uhrzeit des Sammlungsauftrags.
Durchschnittliches Alter von Schwachstellen	Einzelne Punktzahl	Durchschnittliches Alter aktiver angreifbarer Elemente in Tagen.
Services mit den meisten Schwachstellen	Liste und Zeile	Monatlicher Durchschnitt der aktiven angreifbaren Elemente für Services in der Organisation. **Hinweis:** Informationen zum Definieren der Serviceklassifizierungen, die Sie in Vulnerability Response-Berichten und zugehörigen Listen anzeigen möchten, finden Sie auf der Registerkarte Services in Dashboard „Schwachstellenmanagement“ [PA] .
Länder mit den meisten Schwachstellen	Ring	Top-10-Länder mit der höchsten Anzahl angreifbarer Elemente.
Effizienz der monatlichen Fehlerbehebung	Einzelne Punktzahl	Prozentsatz der geschlossenen angreifbaren Elemente geteilt durch neue angreifbare Elemente im aktuellen Monat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Neue und geschlossene angreifbare Elemente	Balken	Anzahl der neuen importierten angreifbaren Elemente und Anzahl der in einem Monat geschlossenen angreifbaren Elemente.
Scan-Abdeckung	Linie	Anzahl der gescannten Assets im Vergleich zur Gesamtzahl der gescannten Assets, die im Laufe der Zeit angezeigt werden. Die im Widget enthaltenen CI-Klassen werden im Modul „Konfiguration der Scan-Abdeckung“ angegeben. Informationen zum Konfigurieren des Moduls „Scan-Abdeckung“ finden Sie unter Konfigurieren Sie die Berichte zur Scan-Abdeckung .
Monatliche Scan-Abdeckung	Einzelne Punktzahl	Prozentsatz der gescannten Assets geteilt durch die Gesamtzahl der gescannten Assets für den aktuellen Monat. Informationen zum Konfigurieren des Moduls „Scan-Abdeckung“ finden Sie unter Konfigurieren Sie die Berichte zur Scan-Abdeckung
Top 10 der Zuweisungsgruppen mit den meisten zurückgestellten Schwachstellen	Liste und Zeile	Top-10-Zuweisungsgruppen mit der höchsten Anzahl zurückgestellter angreifbarer Elemente, zurückgestellt basierend auf dem monatlichen Durchschnitt.
Top 10 der Zuweisungsgruppen mit den der niedrigsten Einhaltung des Nachbesserungsziels	Liste und Zeile	Top-10-Zuweisungsgruppen, deren angreifbare Elemente die geringste Einhaltung ihrer Korrekturziele aufweisen.

Empfohlene Aktionen

Name	Typ	Quelltabelle	Beschreibung
Top-10-Schwachstellen mit verfügbaren Exploits	Liste	Oberstes Schwachstellenelement [sn_vul_Analytics_Top_item]	Aktive Schwachstellen mit Exploits, die für alle Threat Intelligence-Anbieter verfügbar sind, die das VR-Exploit-Framework verwenden.
Top-10-Lösungen Mit Der Höchsten Auswirkung	Liste	Oberstes Schwachstellenelement [sn_vul_Analytics_Top_item]	Bevorzugte Lösungen oder Patches mit den höchsten Risikopunktzahlen für aktive angreifbare Elemente. Dieser Bericht verwendet die Fähigkeiten von Vulnerability Solution Management (VSM), das Patches von Microsoft und Red hat mit Schwachstellen in der Umgebung korreliert. VSM hilft bei der Identifizierung der bevorzugten Lösung für Schwachstellen.
Top 10 Der Ältesten Angreifbaren Elemente	Liste	Oberstes Schwachstellenelement [sn_vul_Analytics_Top_item]	Aktive angreifbare Elemente mit dem höchsten Alter. Lösen Sie diese Elemente, um das durchschnittliche Alter der Schwachstellen auf der Registerkarte Übersicht zu senken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Empfohlene Aktionen (Fortsetzung)

Name	Typ	Quelltabelle	Beschreibung
Die 10 häufigsten Schwachstellen für Assets	Liste	Oberstes Schwachstellenelement [sn_vul_Analytics_Top_item]	Aktive angreifbare Elemente, die für die höchste Anzahl von Assets verfügbar sind.

Konfigurieren Sie die Berichte zur Scan-Abdeckung

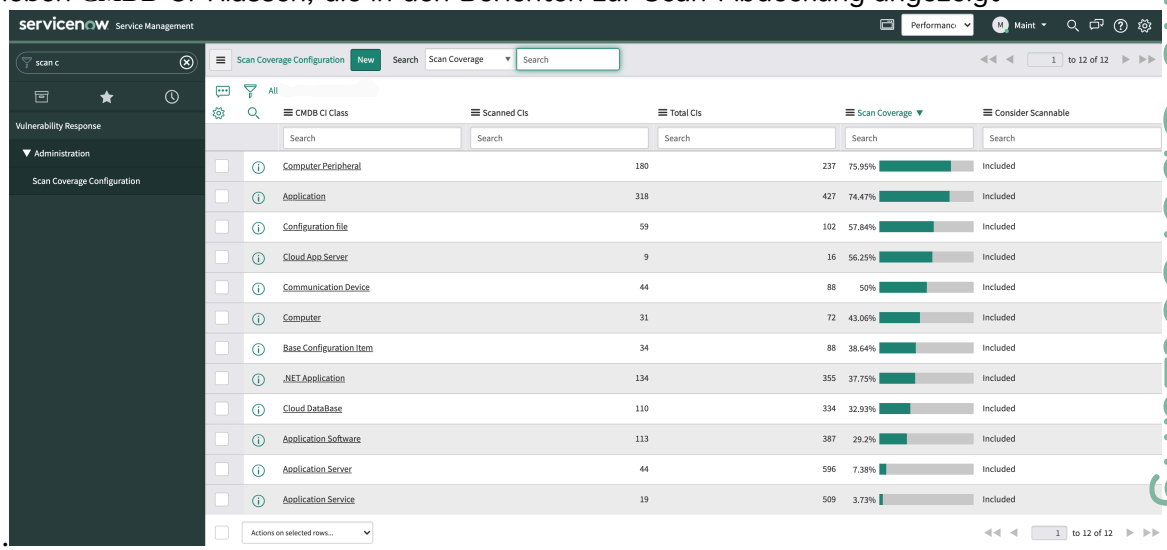
Ermöglichen Sie Ihren Anwendern, Scan-Abdeckungsberichte über das CISO-Dashboard auszuführen. Mit diesen Berichten können Ihre Anwender sehen, welche Scan-Abdeckung die Organisation über einen bestimmten Zeitraum hat.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Warum und wann dieser Vorgang ausgeführt wird

Die Scan-Abdeckung zeigt die Anzahl der Assets an, die in den letzten 90 Tagen von den Schwachstellen-Scannern für die verschiedenen Klassen gescannt wurden. Diese Assets werden mit der Anzahl der scanbaren Assets in verglichen Configuration Management Database (CMDB). Standardmäßig enthält das Modul „Konfiguration der Scan-Abdeckung“ CMDB CI-Klassen, mit denen mindestens ein gescanntes Asset abgeglichen wurde. Sie können eine CI-Klasse aus hinzufügen CMDB Zum Bericht „Scan-Abdeckung“, der im CISO-Dashboard angezeigt wird. Sie können ein- oder ausschließen CMDB CI-Klassen, die in den Berichten zur Scan-Abdeckung angezeigt werden.



Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Konfiguration der Scan-Abdeckung**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Konfiguration der Scanabdeckung“

Feld	Beschreibung
CMDB-CI-Klasse	CI-Klasse, die dem Scan-Abdeckungsbericht im CISO-Dashboard hinzugefügt werden muss. **Hinweis:** Wenn bereits eine CI-Klasse im Modul „Konfiguration der Scan-Abdeckung“ vorhanden ist, ist sie nicht in dieser Liste enthalten.
Als scannbar betrachten	Option zum Definieren, ob die CI-Klasse eingeschlossen werden muss oder nicht. Fügen Sie eine CI-Klasse hinzu, wenn ihre Daten den Scan-Abdeckungsberichten hinzugefügt werden sollen. Wenn ausgeschlossen, werden die Daten für diese CI-Klasse nicht hinzugefügt.

4. Klicken Sie auf **Absenden**.

Konfigurieren Sie die PA-Indikatoren für das CISO-Dashboard

Überwachen Sie die automatisierten und formulierten CISO-Indikatoren, damit Sie die Schwachstellendaten in Ihrer Instanz verwalten können.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Vulnerability Response Verfügt sowohl über automatisierte als auch über formulierte Indikatoren.

Wichtige Begriffe

Indikator

Definiert eine Leistungsmessung, die in regelmäßigen Abständen eines Business-Service, einer Aktivität oder eines Organisationsverhaltens durchgeführt wird. Ein Beispiel ist ein aktives angreifbares Element.

Indikatorquelle

Datensätze, die aus Datensätzen bestehen, die aus einer Tabelle oder Datenbankansicht gefiltert werden, um die Effizienz zu erhöhen. Ein Beispiel ist VI.Active (mit Internetverbindung).

Aufgliederungen

Aufgliederungen filtern und gruppieren Indikatorpunktzahlen mithilfe qualitativer Attribute wie Priorität, Kategorie und Zuweisungsgruppe.

Geplante Aufgaben

Geplante Aufgaben werden ausgeführt, um die Indikatorquellendaten auszufüllen. Die tägliche geplante Aufgabe [PA VR] CISO-Dashboard ist standardmäßig deaktiviert. Sie müssen sie aktivieren, um Indikatorpunktzahlen für das CISO-Dashboard zu erfassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Performance Analytics** > **Indikatoren** Und wählen Sie eine der folgenden Optionen aus:
   - Automatisierte Indikatoren
   - Formelindikatoren

   Weitere Informationen zu Indikatoren finden Sie unter Performance Analytics-Indikatoren .
2. Suchen Sie auf der Seite „Indikatoren“ in der Spalte Name nach dem erforderlichen Indikatornamen.
3. Klicken Sie auf den Indikatornamen, um den Datensatz zu öffnen und seine Details anzuzeigen.

   Die Indikatoren für das CISO-Dashboard erfassen standardmäßig keine Datensätze. Sie können Datensätze erfassen, indem Sie auswählen **Erfassen Sie Datensätze** Kontrollkästchen.

   Hinweis:
   Das Aktivieren von Datensatzsammlungen in einem Indikator kann Leistungsprobleme verursachen, z. B. dass viel mehr Zeit und Arbeitsspeicher benötigt werden, der zum Ausführen des Datensammlungsauftrags erforderlich ist.

   Die maximale Anzahl von Zeilen, die Sie für eine Indikatorquelle abrufen können, beträgt 1.000.000.

Dashboard „Integrität von SecOps Vulnerability Response“

Das Dashboard „Vulnerability Response-Integrität“ ist ein Tool, mit dem Unternehmen umfassende Einblicke in die Implementierung und Nutzung ihrer Vulnerability Response-Anwendungen erhalten können.

Die Gesamtintegritätsbewertung wird durch die Zusammenfassung verschiedener kritischer Faktoren über Konfiguration, Implementierung, Integration, Leistung, Daten, und -Prozess. Zeigen Sie das Aggregat-Dashboard für jede Kategorie für die folgenden Anwendungen an:

- Vulnerability Response
- Application Vulnerability Response
- Container Vulnerability Response
- Konfigurations-Compliance

Installieren des SecOps Vulnerability Response-Integritätsdashboards

Zum Installieren und Konfigurieren des SecOps Vulnerability Response-Integritätsdashboards für Vulnerability ResponseAnwendungen in Ihrem ServiceNow AI Platform-Instanz navigieren Sie zu ServiceNow® Store Und aktivieren Sie das Plugin SecOps Health Analytics (sn_sec_Analytics).

Erforderliche ServiceNow AI Platform-Rollen

Erforderliche Rollen: sn_sec_Analytics.admin, sn_sec_Analytics.read

Geplante Aufgabe

Um die geplante Aufgabe anzuzeigen, navigieren Sie zu **Alle** > **Systemzeitplaner** > **Geplante Aufgaben** > **Erfassen Sie Integritäts-Dashboard-Metriken**an. Die geplante Aufgabe „IntegritätsDashboard-Metriken erfassen“ wird täglich um 00:00 Uhr ausgeführt. Generiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Daten für das Dashboard „Integrität von SecOps Vulnerability Response“. Sie können die geplante Aufgabe auch manuell ausführen.

Anwendungsfälle

Beispiele dafür, wie Personen in Ihrer Organisation dieses Dashboard verwenden, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
Schwachstellenadministrator	Hilft Ihnen, die Integritätspunktzahl von zu verstehen Vulnerability Response Anwendungen. Es ist auch hilfreich, die Bereiche hervorzuheben, die verbessert werden müssen. Das Vulnerability Response-Integritäts-Dashboard befasst sich nur mit der Implementierungs- und Nutzungsintegrität. Es hilft nicht bei der Verwaltung von Schwachstellen oder Assets.
Supportadministrator	Hilft Ihnen, die Leistungs-, Anpassungs- und Konfigurationsprobleme mithilfe von KPIs zu identifizieren. Basierend auf der Integrität der Anwendung können Sie eine zusätzliche Analyse durchführen oder den Anwendern eine Empfehlung erteilen.
Implementierungspartner	Hilft Ihnen bei der Bewertung von Vulnerability Response Implementieren Sie die Integrität für Konfigurationen, Add-ons, Anpassungen und Integrationen, und stellen Sie den Anwendern Verbesserungsempfehlungen bereit.

Die Registerkarten des Security Ops Vulnerability Response-Integritätsdashboards

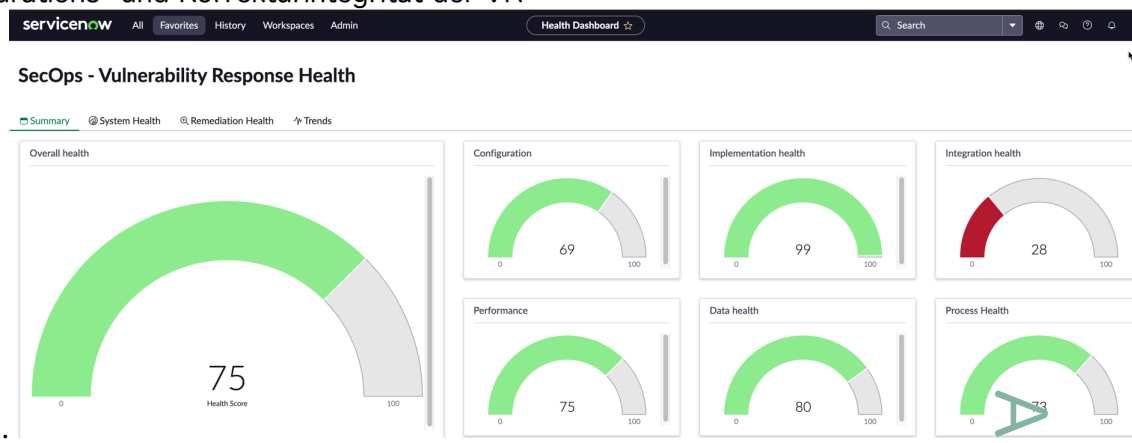
Um das Dashboard „Integrität von SecOps Vulnerability Response“ anzuzeigen, navigieren Sie zu **Security Operations-Integrität** > **Vulnerability Response-Integrität**an. Jede Farbe im Dashboard stellt Folgendes dar:

- Grün: Safe
- Gelb: Warnung
- Rot: Kritisch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

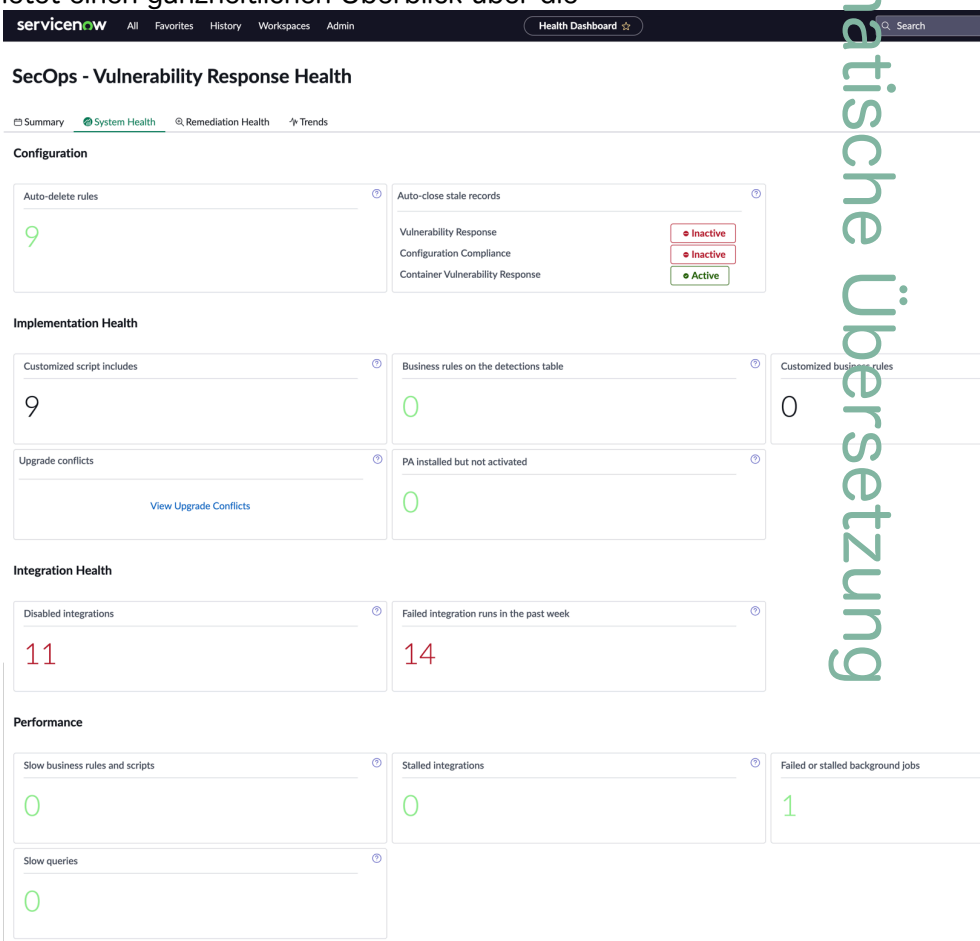
Registerkarte „Zusammenfassung“

Dieses Dashboard kommuniziert die Gesamtintegritätspunktzahl für die Konfigurations- und Korrekturintegrität der VR-Anwendungen.



Registerkarte „Systemintegrität“

Dieses Dashboard zeigt die Konfigurations- und Integrationsintegrität Ihrer Implementierung an. Sie bietet einen ganzheitlichen Überblick über die Implementierungsleistung.

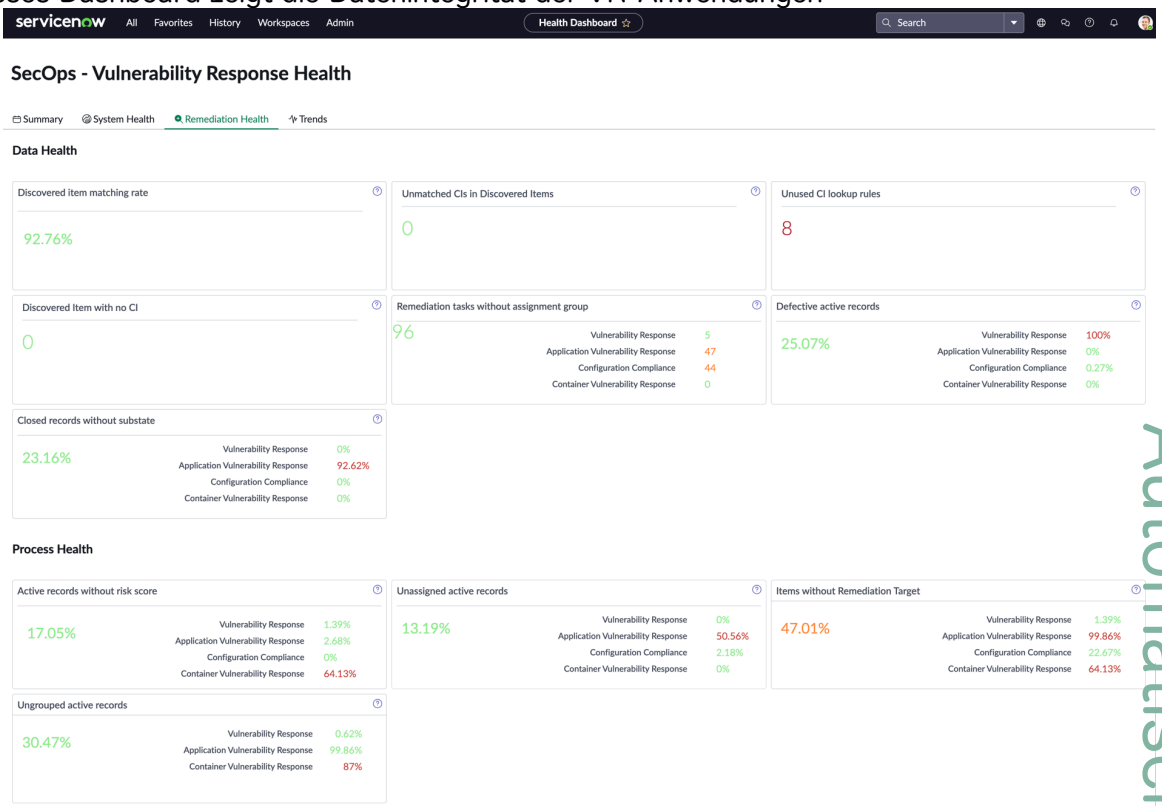


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Korrekturintegrität“

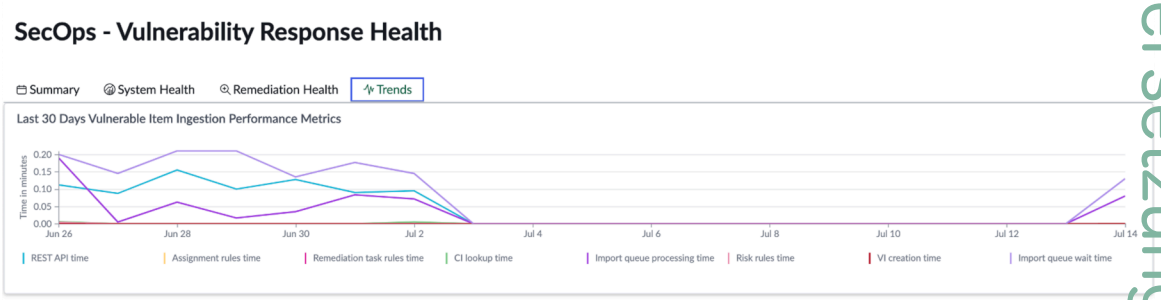
Dieses Dashboard zeigt die Datenintegrität der VR-Anwendungen



an.

Registerkarte Trends

Dieses Dashboard zeigt die Trends für die Leistungsmetriken der Erfassung angreifbarer Elemente für die letzten 30 Tage für die VR-Anwendungen



an.

Berichte

Hinweis:
Die Schwellenwerte sind Teil des Basissystems. Sie können die Werte basierend auf Ihren Anforderungen konfigurieren.

Zusammenfassung

Titel	Beschreibung
Integrität gesamt	Gesamtintegritätspunktzahl für die VR-Anwendungen. Weitere Informationen finden Sie in den Berichten für die Metriken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusammenfassung (Fortsetzung)

Titel	Beschreibung
Konfiguration	Gesamtkonfigurationsintegrität der VR-Anwendungen.
Implementierungsintegrität	Allgemeine Implementierungsintegrität der VR-Anwendungen.
Integrität der Integration	Gesamtintegrationsintegrationsintegrität der VR-Anwendungen.
Leistung	Gesamtleistungsintegritätspunktzahl der VR-Anwendungen.
Datenintegrität	Gesamtdatenintegrität der VR-Anwendungen.
Prozessintegrität	Gesamtpunktzahl der Prozessintegrität der VR-Anwendungen.

Systemintegrität

Titel	Beschreibung	Überlegungen zur Verbesserung der Leistung	Schwellenwertwarn	Schwellenwert kritisch
Konfiguration				
Regeln automatisch löschen	Zeigt die Anzahl der aktivierten Regeln zum automatischen Löschen an.	Überprüfen und lösen Sie die inaktiven Regeln zum automatischen Löschen.	3	1
Veraltete Datensätze automatisch schließen	Schließt automatisch veraltete Erkennungen. Weitere Informationen finden Sie unter dem Thema „veraltete Erkennungen in Vulnerability Response automatisch schließen“ in servicenow.com/docs.	Reduzieren Sie das Volumen veralteter Erkennungen. Aktivieren Sie diese Option, um die veralteten Erkennungen zu schließen, die nicht von den Scannern geschlossen werden.	3	1
Implementierungsintegrität				
Anwenderdefinierte Skripteinbindungen	Anzahl der angepassten „Skripteinbindungen“.	Minimieren Sie anwenderdefinierte Skripteinbindungen, um Upgrades zu erleichtern.	10	12

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemintegrität (Fortsetzung)

Titel	Beschreibung	Überlegungen zur Verbesserung der Leistung	Schwellenwertwarn	Schwellenwert kritisch
Business-Regeln in der Erkennungstabelle	Anzahl der anwenderdefinierten Business-Regeln in der Erkennungstabelle.	Minimieren Sie Geschäftsregeln, um Upgrades zu erleichtern.	4	8
Anwenderdefinierte Business-Regeln	Anzahl der anwenderdefinierten Business-Regeln vor der Erstellung von Datensätzen in der CMDB.	Verwenden Sie die standardmäßigen Business-Regeln für Datensätze.	5	8
Upgrade-Konflikte	Konflikte wie Geschäftsregeln und Skripts, die bei einem Upgrade identifiziert wurden.	Überprüfen und lösen Sie die Upgrade-Konflikte.	10	15
PA installiert, aber nicht aktiviert	Gibt an, ob das Performance Analytics-Dashboard nicht aktiviert ist.	Aktivieren Sie das PA-Dashboard.	10	15
Integrität der Integration				
Deaktivierte Integrationen	Anzahl der Integrationen, die deaktiviert wurden.	Überprüfen und aktivieren Sie die erforderlichen Integrationen.	6	9
Fehlgeschlagene Integrationsausführungen in der letzten Woche	Anzahl der Integrationsausführungen, die in der letzten Woche nicht erfolgreich waren.	Überprüfen und beheben Sie die Ursache der fehlgeschlagenen Integrationsausführungen.	9	12
Leistung				
Langsame Geschäftsregeln und Skripts	Business-Regeln und Skripts, deren durchschnittliche Ausführungszeit größer als 10 ms und die Ausführungsanzahl größer als 000 ist.	Überprüfen und lösen Sie die langsam laufenden Geschäftsregeln.	10	15
Festgestellte Integrationen	Anzahl der Integrationen, bei denen vor Abschluss eine	Überprüfen und beheben Sie die Ursache der blockierten Integrationen.	10	15

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemintegrität (Fortsetzung)

Titel	Beschreibung	Überlegungen zur Verbesserung der Leistung	Schwellenwertwarn	Schwellenwert kritisch
	Zeitüberschreitung aufgetreten ist.			
Fehlgeschlagene oder verzögerte Hintergrundaufträge	Fehlgeschlagene oder abgelaufene Hintergrundaufträge in der letzten Woche.	Überprüfen und beheben Sie die Ursache der fehlgeschlagenen Aufträge.	5	10
Langsame Abfragen	Abfragen, deren durchschnittliche Ausführungszeit größer als 10 ms und die Ausführungsanzahl größer als 000 ist.	Überprüfen und lösen Sie die langsam laufenden Geschäftsregeln.	10	15

Integrität der Korrektur

Titel	Beschreibung	Überlegungen zur Verbesserung der Leistung	Schwellenwertwarn	Schwellenwert kritisch
Datenintegrität				
Erkannte Übereinstimmungsrate des Elements	Anzahl der erkannten Elemente, die mit vorhandenen CIs abgeglichen sind.	Überprüfen Sie die Integrität Ihrer CMDB und die Logik der CI-Suchregeln.	50	20
Nicht abgeglichene CIs in erkannten Elementen	Erkannte Elemente im Status „nicht abgeglichen“.	Überprüfen Sie die Integrität Ihrer CMDB und die Logik der CI-Suchregeln.	9	12
Nicht verwendete CI-Suchregeln	CI-Suchregeln, die keinem erkannten Element zugeordnet sind.	Ändern Sie den Status der nicht verwendeten CI-Suchregeln in „Inaktiv“.	4	6
Erkanntes Element ohne CI	Erkanntes Element ohne Konfigurationselement.	Überprüfen Sie CI-Suchregeln, und wenden Sie sie erneut an.	9	12
Defekte aktive Datensätze	Datensätze ohne Konfigurationselement oder Schwachstelle.	Legen Sie die CIs mit der Option CMDB CI-Lebenszyklusmanagement außer Kraft.	40	60

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrität der Korrektur (Fortsetzung)

Titel	Beschreibung	Überlegungen zur Verbesserung der Leistung	Schwellenwertwarn	Schwellenwert kritisch
		Hinweis: Das direkte Löschen von CIs kann zu verwaisten Vits führen.		
Korrekturaufgaben ohne Zuweisungsgruppe	Aktive Korrekturaufgaben, deren Zuweisungsgruppe noch zugewiesen werden muss.	Weisen Sie einer Zuweisungsgruppe Korrekturaufgaben zu, und überprüfen Sie die vorhandenen Zuweisungsregeln.	40	60
Geschlossene Datensätze ohne Substatus	Datensätze, die ohne Substatus geschlossen werden.	Geben Sie beim Schließen der Datensätze Informationen im Feld Grund an.	40	50
Prozessintegrität				
Aktive Datensätze ohne Risikopunktzahl	Aktive Datensätze mit einer Risikopunktzahl von 0 oder ohne zugewiesene Risikopunktzahl.	Überprüfen und lösen Sie die Risikoregeln.	40	60
Nicht zugewiesene aktive Datensätze	Datensätze ohne Zuweisungsgruppe.	Weisen Sie den Datensätzen eine Gruppe zu, und überprüfen Sie die vorhandenen Zuweisungsregeln.	30	50
Elemente ohne Korrekturziel	Elemente ohne Korrekturzieldatum.	Überprüfen und lösen Sie die Korrekturzielregeln. Diese Regeln müssen alle Datensätze enthalten.	30	50
Nicht gruppierte aktive Datensätze	Datensätze, die nicht in einer Korrekturaufgabenrege enthalten sind.	Überprüfen Sie die Regeln für Korrekturaufgaben.	40	60

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trends

Titel	Beschreibung
Leistungsmetriken der Erfassung angreifbarer Elemente der letzten 30 Tage	Durchschnittliche Zeit für die Erfassung angreifbarer Elemente und die Verarbeitung mehrerer Regeln in den letzten 30 Tagen.

Schwellenwerte werden geändert

Sie können die Schwellenwerte für die Daten des SecOps VR-Integritätsdashboards basierend auf Ihren Einstellungen ändern.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Security Operations-Integrität** > **Konfiguration** > **Metriken**an.
2. Öffnen Sie auf der Seite „Integritäts-Dashboard-Daten“ den Datensatz, den Sie ändern möchten.
3. Aktualisieren Sie den Datensatz, und speichern Sie ihn.

Vulnerability Management(PA) Dashboard

Verfolgen Sie das Volumen, die Leistung und den Fortschritt von Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur. Sie können Berichte beispielsweise nach Zuweisungsgruppe, Exploits, Risikobewertung oder Status filtern. Erhalten Sie schnell Einblicke in Ihr Schwachstellenrisiko und die betroffenen Business-Services.

Erforderliche ServiceNow AI Platform-Rollen

Erforderliche Rolle: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst und Anwender mit sn_vul.Vulnerability_read (oder die die Rolle sn_vul.Vulnerability_read erben) und PA_Viewer.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
IT-Manager, IT-Analysten, Besitzer der Schwachstellenkorrektur	Helfen Sie Ihrer Organisation, mit zunehmenden Security Incidents aufgrund ausgenutzter Schwachstellen umzugehen, indem Sie effizient bestimmen, welche angreifbaren Elemente das meiste Risiko darstellen. Diese Dashboards bieten eine grafische Ansicht der Aktivität angreifbarer Elemente und helfen beim Entwerfen von Korrekturplänen und Statusfortschritten. Sie können sich auf die KPIs konzentrieren, die kritischen betroffenen Assets und Schwachstellen mit hoher Sichtbarkeit zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren Sie zum Anzeigen des Dashboard Vulnerability Management (PA) zu **Vulnerability Response** > **Übersicht**an.

Zeigen Sie Berichte an, die Trenddaten im Zeitverlauf anzeigen. Berichte mit Echtzeitdaten sind unten aufgeführt. Zeigen Sie Trends wichtiger Metriken in einem regelmäßigen Zeitplan an, um Ihre gesamten Geschäftsprozesse zu analysieren und Verbesserungsbereiche zu identifizieren.

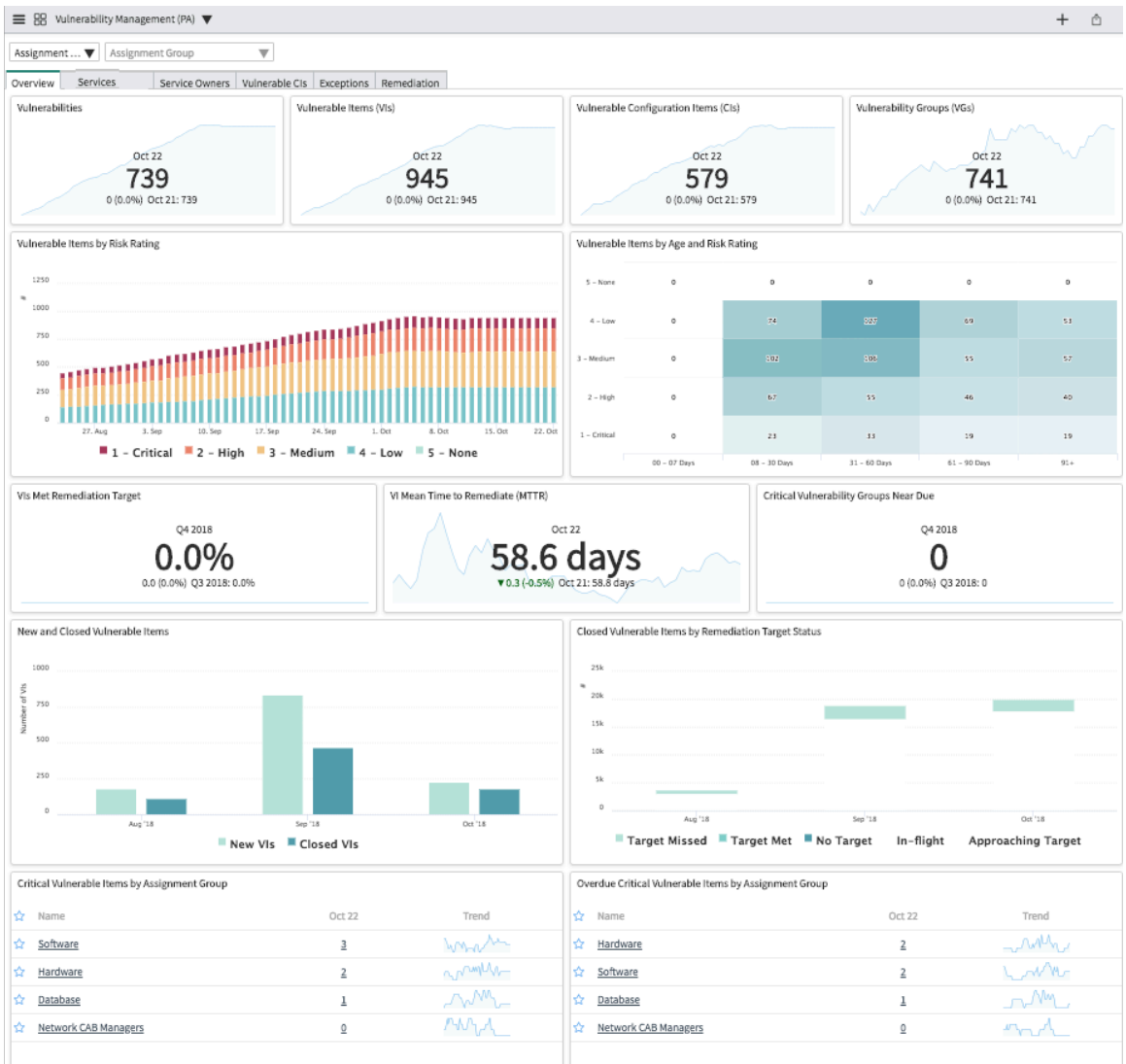
Weitere Informationen zum Anzeigen Ihrer PA-Berichte mit Echtzeitpunktzahlen finden Sie unter Zeigen Sie Performance Analytics für Vulnerability Response [PA]-Berichte in Echtzeit an .

Die Dashboard-Registerkarten für Schwachstellenmanagement [PA]

Registerkarte „Übersicht“

Dieses Dashboard kommuniziert KPIs für das Risiko und die Verbreitung von Schwachstellen, betroffene Assets, die Einhaltung von Korrekturzielen und den Korrekturfortschritt.

Auf der Registerkarte Übersicht können Sie den Bericht „kritische angreifbare Elemente nach Zuweisungsgruppe“ anzeigen, der basierend auf der geplanten Aufgabe ausgeführt wird.



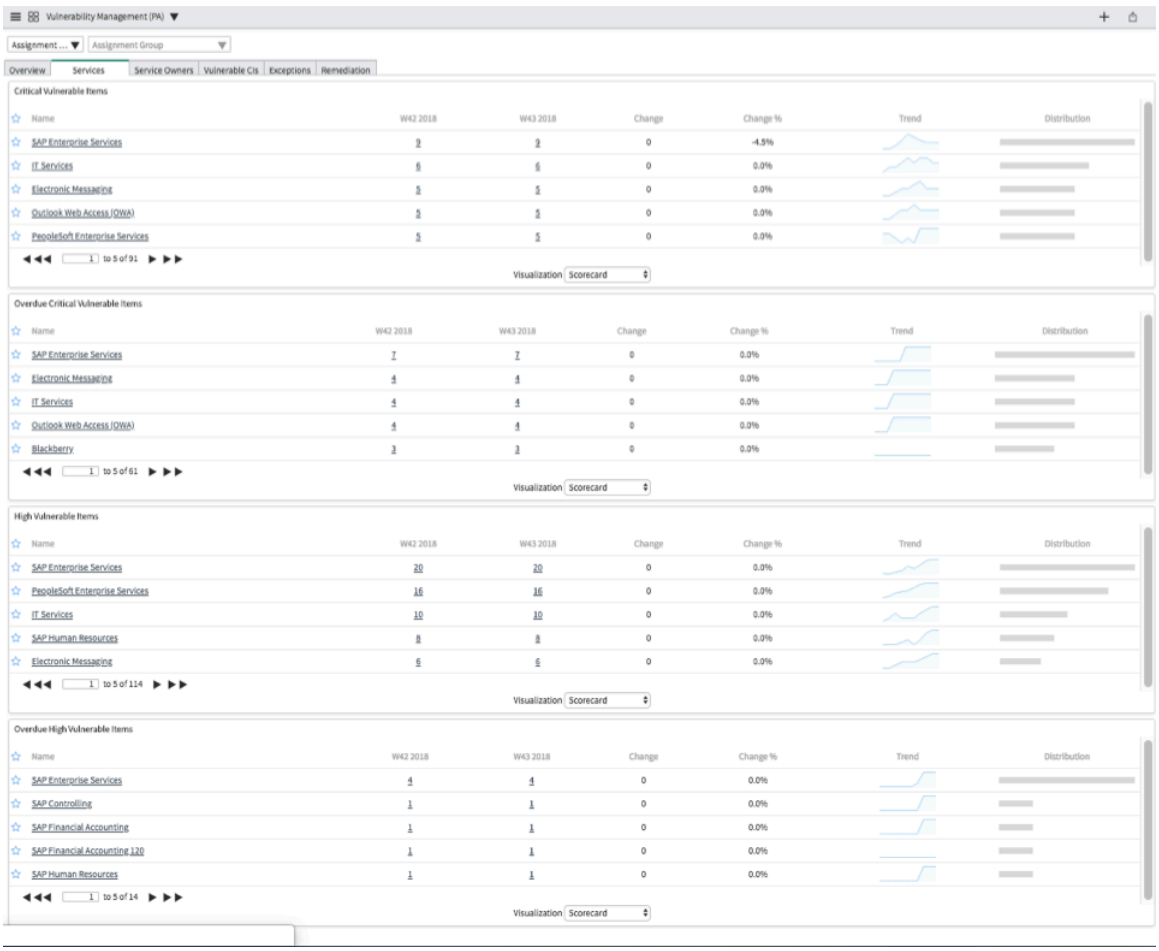
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Business-Services“

Dieses Dashboard stellt Schwachstellenrisiken auf Business-Service-Ebene dar. Die gemeinsame Nutzung dieser Informationen innerhalb der Organisation kann Servicemanagern helfen, Schwachstellen schnell und proaktiv zu beheben und die Organisation auf ein Modell für gemeinsame Verantwortlichkeit für die Informationssicherheit zu bringen.

Sie können die Serviceklasse mithilfe der Systemeigenschaft in technische Services oder Anwendungsservices ändern `sn_vul.service_classifications` .

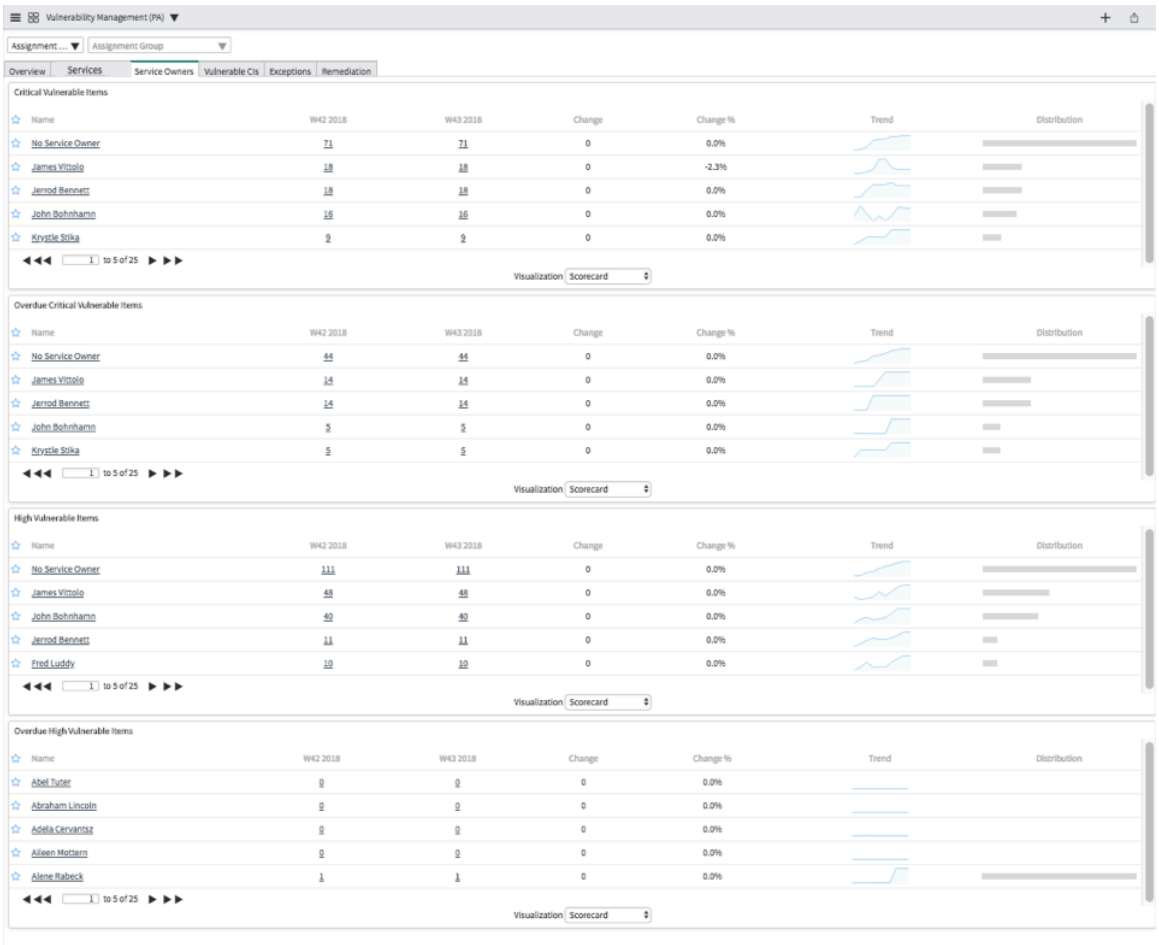


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Serviceverantwortliche“

In diesem Dashboard wird das Schwachstellenrisiko vom Business-Service-Level zu den Serviceverantwortlichen zusammengefasst – den Führungskräften, die für diese Business-Services verantwortlich sind. Es zeigt, welche Führungskräfte das größte Schwachstellenrisiko eingehen und welche möglicherweise die meiste Hilfe benötigen, um Korrekturmaßnahmen zu fördern.



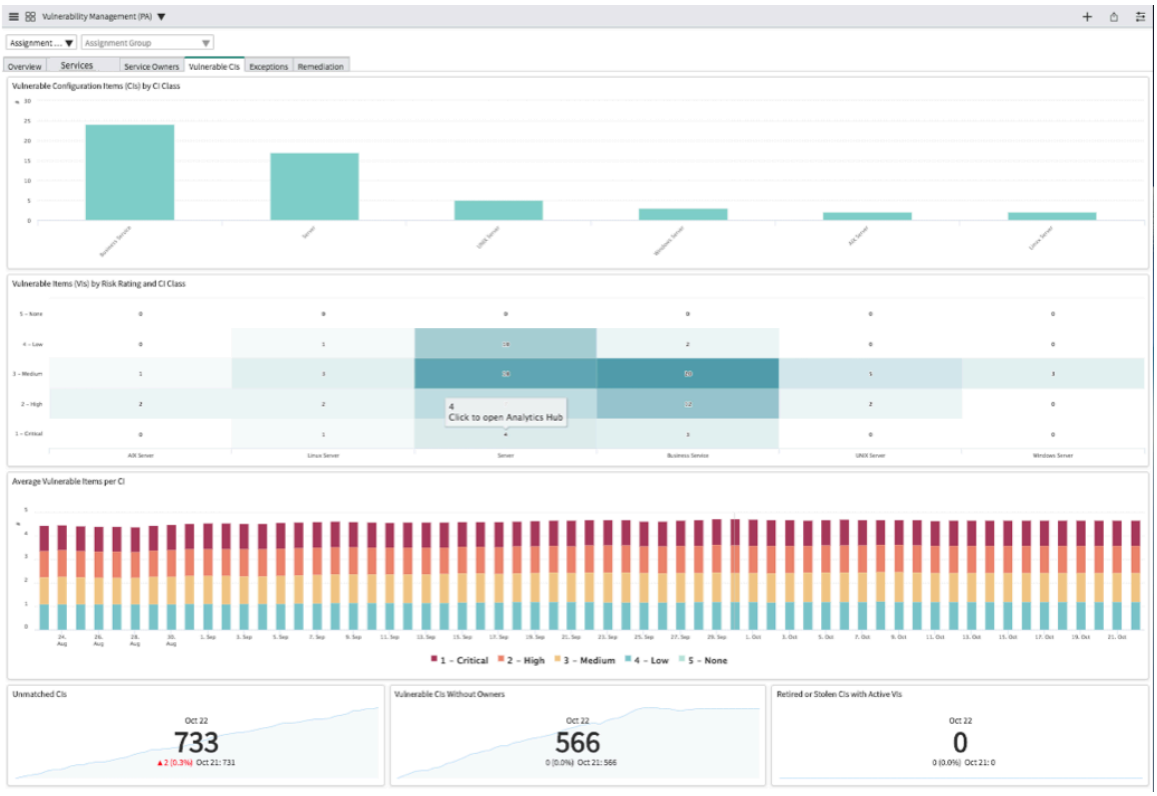
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „angreifbare CIs“

Dieses Dashboard zeigt den Umfang und die Zusammensetzung von CIs mit aktiven Schwachstellen und welche Kategorien von CIs die meiste Aufmerksamkeit erfordern. Identifizieren Sie außer Betrieb genommene Assets mit aktiven angreifbaren Elementen, und bestätigen Sie, dass die Assets außer Betrieb genommen wurden. Zeigen Sie die Anzahl der angreifbaren CIs an, denen keine Eigentumsinformationen fehlen, damit Sie die Besitzer für diese Assets proaktiv identifizieren können, bevor eine kritische Schwachstelle diese Systeme betrifft.

Auf der Registerkarte angreifbare CIs können Sie die angreifbaren CIs ohne Besitzer und stillgelegte oder gestohlene CIs mit Berichten zu aktiven VIS in Echtzeit anzeigen.

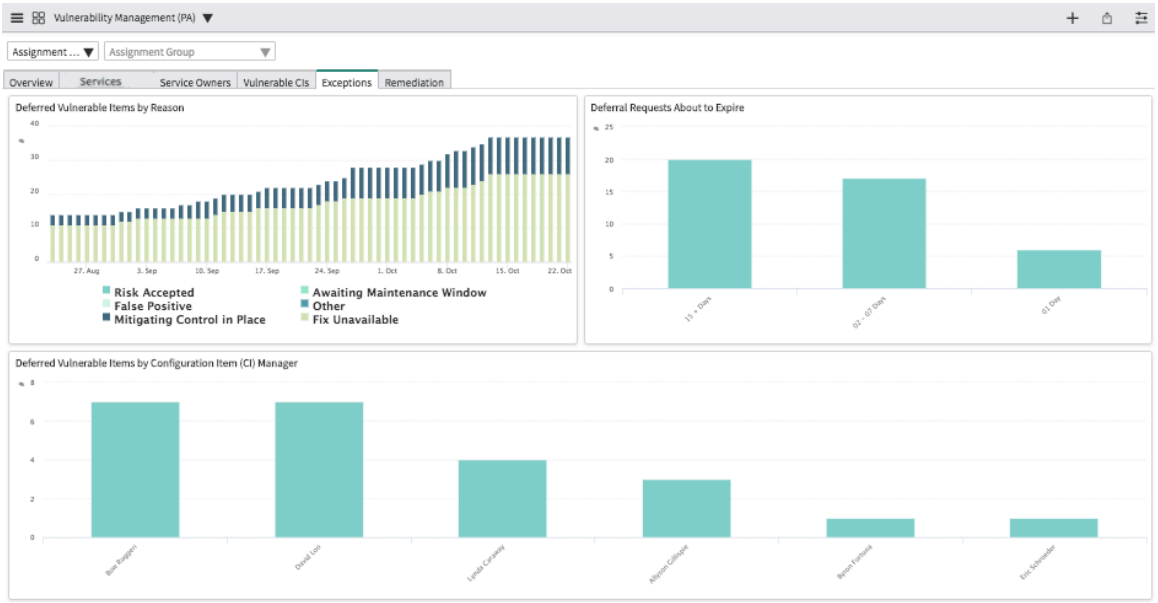


Registerkarte „Ausnahmen“

Dieses Dashboard hilft Ihnen, zu verstehen, wo Ihre Organisation aufgrund potenziell übermäßiger Zurückstellungen Risiken eingeht, und Korrekturoptionen zu überdenken.

Sie können Berichte „zurückgestellte angreifbare Elemente nach Grund“, „auslaufende Zurückstellungsanforderungen“, „Ausnahmen für kritische angreifbare Elemente nach Zuweisungsgruppe“ und „Ausnahmeanforderungen nach anfordernder Person“ anzeigen.

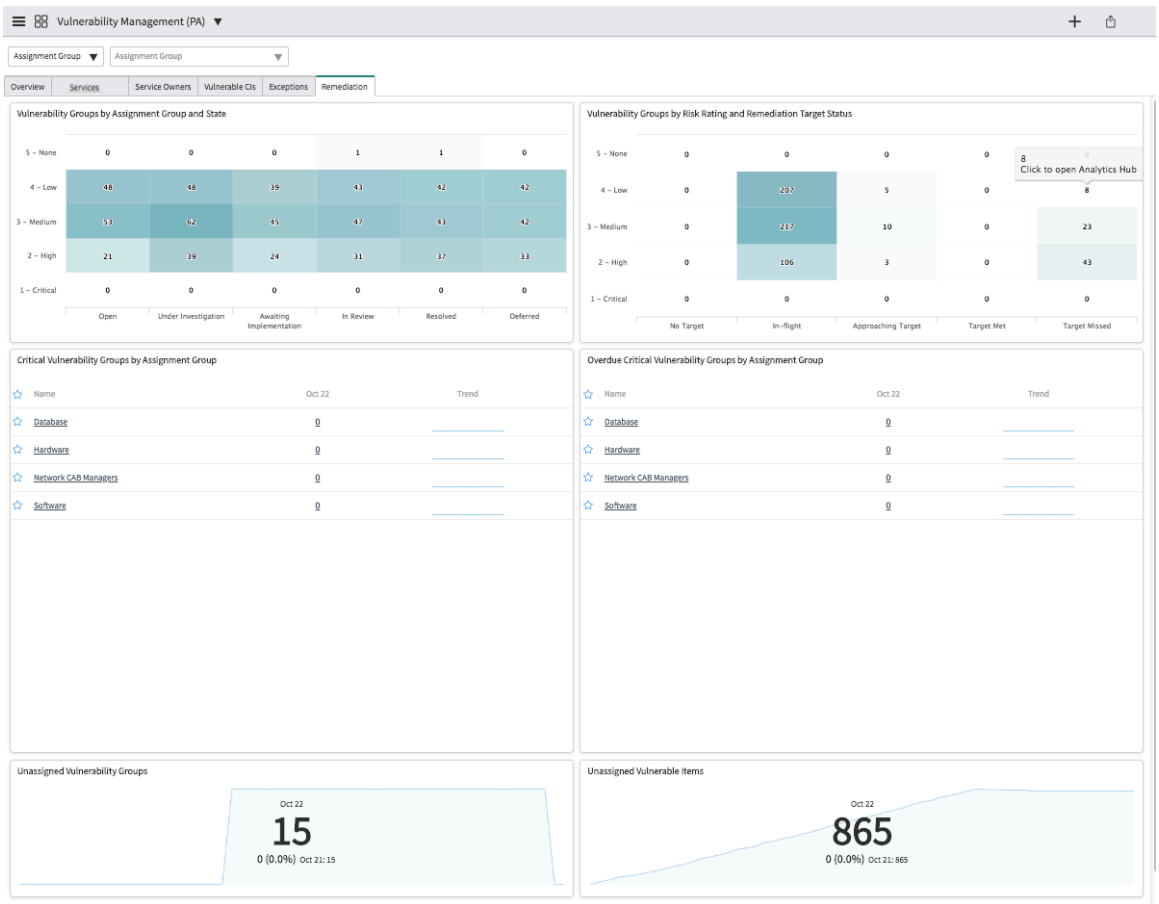
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Registerkarte „Remediation“

Dieses Dashboard hilft Ihnen, den Fortschritt Ihrer Korrekturaktionen zu verstehen und zu verstehen, welche Supportteams die meiste Unterstützung bei ihrem Abschluss benötigen.

Auf der Registerkarte „Korrektur“ können Sie den Bericht „nicht zugewiesene angreifbare Elemente“ in Echtzeit anzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Indikatoren

Vulnerability Response – Indikatoren

Es gibt eine Reihe von Indikatoren, die verwendet werden, um den Fortschritt Ihrer Schwachstellenbeseitigung in zu messen und nachzuverfolgen Vulnerability Response Anwendung.

Die Option „Datensätze sammeln“ für die -Indikatoren ist standardmäßig für deaktiviert Vulnerability Response Anwendung. Diese Option ist deaktiviert, damit bestimmte Berichte in Echtzeit angezeigt werden können. Trendinformationen, die von diesen Indikatoren verwendet werden, sind weiterhin verfügbar, wenn Sie die manuelle Erfassung von Datensätzen aktivieren und die Datensätze anzeigen möchten, aus denen die Punktzahlen bestehen.

Eindeutige Schwachstellen

Eindeutige Schwachstellen mit count_Active_VI > 0. Ziel ist die Minimierung.

Nicht zurückgestellte überfällige kritische angreifbare Elemente

Dies ist die Anzahl in der Datenquelle „AE.aktiv“, die die Tabelle sn_vul_vulnerable_item verwendet. Ziel ist die Minimierung.

% der angreifbaren Elemente mit erfülltem Korrekturziel

([[Geschlossene Angreifbare Elemente > Korrekturziel = Ziel Erfüllt]] / [[Geschlossene Angreifbare Elemente]]) * 100 . Ziel ist die Maximierung.

Nicht zugewiesene angreifbare Elemente

Alle aktiven angreifbaren Elemente, bei denen die Felder „Zuweisungsgruppe“ und „Zugewiesen an“ leer sind. Ziel ist die Minimierung.

Kritische angreifbare Elemente (Services)

Dies ist die Anzahl in der Datenquelle „aktive VIS (Services)“, die die Tabelle sn_vul_Analytics_Business_Services_VI verwendet. Ziel ist die Minimierung.

Weit überfällige angreifbare Elemente (Services)

Dies ist die Anzahl in der Datenquelle „aktive VIS (Services)“, die die Tabelle sn_vul_Analytics_Business_Services_VI verwendet. Ziel ist die Minimierung.

Nicht zugewiesene Korrekturaufgaben

Alle aktiven Korrekturaufgaben, bei denen sowohl die Felder Zuweisungsgruppe als auch Zugewiesen an leer sind. Ziel ist die Minimierung.

Kritische angreifbare Elemente

Dies ist die Anzahl in der Datenquelle „AE.aktiv“, die die Tabelle sn_vul_vulnerable_item verwendet. Ziel ist die Minimierung.

Angreifbare Elemente

Dies ist die Anzahl in der Datenquelle „AE.aktiv“, die die Tabelle sn_vul_vulnerable_item verwendet. Ziel ist die Minimierung.

Neue angreifbare Elemente

Dies ist die Anzahl in der Datenquelle „AE.Neu“, die die Tabelle sn_vul_vulnerable_item verwendet. Ziel ist die Minimierung.

Angreifbare Konfigurationselemente

Dies ist die eindeutige Anzahl in der Datenquelle „AE.aktiv“, die die Tabelle sn_vul_vulnerable_item verwendet. Ziel ist die Minimierung.

Summierte Dauer der geschlossenen angreifbaren Elemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dies ist die Summe in der Datenquelle „AE.Geschlossen“, die die Tabelle sn_vul_vulnerable_item verwendet. Ziel ist die Minimierung.

Nicht zurückgestellte Korrekturaufgaben

Dies ist die Anzahl in der Datenquelle „VG.aktiv“, die die Tabelle sn_vul_Vulnerability verwendet. Ziel ist die Minimierung.

Durchschnittliche Zeit bis zur Fehlerkorrektur für angreifbare Elemente

[[Summierte Dauer der geschlossenen angreifbaren Elemente]]/[[Geschlossene angreifbare Elemente]]

Kritische überfällige angreifbare Elemente (Services)

Dies ist die Anzahl in der Datenquelle „aktive VIS (Services)“, die die Tabelle sn_vul_Analytics_Business_Services_VI verwendet. Ziel ist die Minimierung.

Stillgelegte Konfigurationselemente

Dies ist die eindeutige Anzahl in der Datenquelle „AE.aktiv“, die die Tabelle sn_vul_vulnerable_item verwendet. Ziel ist die Minimierung.

Zurückstellungsanforderungen

Dies ist die Anzahl in der Datenquelle „aktive Zurückstellungsanforderungen“, die die Tabelle sn_vul_Change_Approval verwendet. Ziel ist die Minimierung.

Angreifbare Elemente nach Konfigurationselementen

Dies ist die Anzahl in Datenquellen-CIs mit aktiven VIS, die die Tabelle sn_vul_Analytics_VI_ci_class verwendet. Ziel ist die Minimierung.

Geschlossene angreifbare Elemente

„Geschlossene angreifbare Elemente“ wird täglich als numerische Einheit gemessen. Das Ziel besteht in der Maximierung.

Nicht abgeglichene Konfigurationselemente

Listet die Hosts auf, die von Schwachstellenscannern einer Drittpartei erkannt wurden und keinen vorhandenen CIs in der CMDB entsprechen.

Nicht zurückgestellte überfällige kritische Korrekturaufgaben

Dies ist die Anzahl in der Datenquelle „VG.aktiv“, die die Tabelle sn_vul_Vulnerability verwendet. Ziel ist die Minimierung.

Angreifbare Konfigurationselemente ohne Supportgruppe

Dies ist die Anzahl in der Datenquelle „AE.Offen“, die die Tabelle sn_vul_vulnerable_item verwendet. Ziel ist die Minimierung.

Nicht zurückgestellte kritische Korrekturaufgaben

Dies ist die Anzahl in der Datenquelle „VG.aktiv“, die die Tabelle sn_vul_Vulnerability verwendet. Ziel ist die Minimierung.

Zurückgestellte angreifbare Elemente

Dies ist die Anzahl in der Datenquelle „AE.aktiv“, die die Tabelle sn_vul_vulnerable_item verwendet. Ziel ist die Minimierung.

Hoch angreifbare Elemente (Services)

Dies ist die Anzahl in der Datenquelle „aktive VIS (Services)“, die die Tabelle sn_vul_Analytics_Business_Services_VI verwendet. Ziel ist die Minimierung.

Eindeutige Konfigurationselemente mit aktiven angreifbaren Elementen

Dies ist die eindeutige Anzahl in Datenquellen-CIs mit aktiven VIS, die die Tabelle sn_vul_Analytics_VI_ci_class verwendet. Ziel ist die Minimierung.

Durchschnittliche Anzahl angreifbarer Elemente pro Konfigurationselement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[[aktive angreifbare Elemente]] / [[angreifbare CIs]] . Ziel ist die Minimierung.

Korrekturaufgaben

Dies ist die Anzahl in der Datenquelle „VG.aktiv“, die die Tabelle sn_vul_Vulnerability verwendet. Ziel ist die Minimierung.

Kritische zurückgestellte angreifbare Elemente

Dies ist die Anzahl in der Datenquelle „AE.aktiv“, die die Tabelle sn_vul_vulnerable_item verwendet. Ziel ist die Minimierung.

Zurückstellungsanforderungen (erstellt)

Dies ist die Anzahl in der Datenquelle „Geschlossen.Anforderungen“, die die Tabelle sn_vul_Change_Approval verwendet. Ziel ist die Minimierung.

Aufgliederungen

Die folgenden Aufgliederungsnamen gelten für die Indikatoren im Dashboard:

- Alter
- Geschlossen mit Alter
- Zuweisungsgruppe
- CI-Klasse
- CI-Manager
- Zurückstellungsalter
- Aufschiebungsgrund
- Ausnahme für anfordernde Person
- Exploit-Angriffsvektor
- Exploit vorhanden
- Exploit-Kompetenzniveau
- Korrekturzielregel
- Nachbesserungszielstatus
- Nachbesserungszielstatus (geschlossen)
- Risikobewertung
- Service
- Servicerelevanz
- Servicebesitzer
- Schweregrad
- Status

Hinweis:
Die Anpassung der Berechnung von Alter und Alter geschlossener Elemente (VIS) kann zu einem starken Anstieg oder Rückgang der Performance Analytics (PA)-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung des Alters und des Alters, das für VIS geschlossen wird, finden Sie unter KB1703270 KB-artikel.

Aufgliederungsquelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zuweisungsgruppe: Gilt für VI- oder RT-Berichte
- Exploit vorhanden: Gilt für VI-Berichte.
- Exploit-Angriffsvektor: Gilt für VI-Berichte.
- Exploit-Kompetenzniveau: Gilt für VI-Berichte.
- Korrekturzielstatus: Gilt für VI- und RT-Berichte.
- Risikobewertung: Gilt für VI- und RT-Berichte.
- Status: Gilt für VI- und RT-Berichte.

Datenvisualisierungen

Titel	Typ	Beschreibung
Schwachstellen	Einzelne Punktzahl	Anzahl der Schwachstellen, die mit einem oder mehreren aktiven angreifbaren Elementen verknüpft sind.
Angreifbare Elemente (AEs)	Einzelne Punktzahl	Anzahl der aktiven (nicht geschlossenen) angreifbaren Elemente.
Angreifbare Konfigurationselemente (CIs)	Einzelne Punktzahl	Anzahl der Konfigurationselemente (CIs), die einem oder mehreren aktiven angreifbaren Elementen zugeordnet sind.
Korrekturaufgaben	Einzelne Punktzahl	Anzahl der aktiven (nicht geschlossenen) Korrekturaufgaben.
Angreifbare Elemente nach Risikobewertung	Balken	Anzahl der aktiven angreifbaren Elemente, gruppiert nach Risikobewertung für die ausgewählte Zeitspanne.
Angreifbare Elemente nach Alter und Risikobewertung	Heatmap	Anzahl der aktiven angreifbaren Elemente gruppiert nach Risikobewertung und Alter (in Tagen).
AEs mit erfülltem Korrekturziel	Einzelne Punktzahl	Prozentsatz der geschlossenen angreifbaren Elemente, die ihre Korrekturzieldaten im aktuellen und vorherigen Quartal erreicht haben. Korrekturziele werden aus dem Datum der letzten Öffnung plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet.
Durchschnittliche Zeit bis zur Korrektur (Mean Time to Remediation, MTTR) von VIS	Einzelne Punktzahl	Die durchschnittliche Zeit für die Nachbesserung (Schließung) eines angreifbaren Elements,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
		angezeigt als laufender 30-Tage-Durchschnitt. **Hinweis:** Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „Last_opened“ und dem Datum und der Uhrzeit des Sammlungsauftrags.
Kritische Korrekturaufgaben kurz vor der Fälligkeit	Einzelne Punktzahl	Anzahl der aktiven Korrekturaufgaben, die sich ihrem Korrekturzieldatum nähern. Das Korrekturzieldatum einer Korrekturaufgabe wird auf das nächste Fälligkeitsdatum festgelegt, das zu einem aktiven angreifbaren Element in der Gruppe gehört. Korrekturziele werden aus dem Datum der letzten Öffnung plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet. Dieser Bericht enthält keine zurückgestellten Korrekturaufgaben.
Neue und geschlossene angreifbare Elemente	Balken	Anzahl neuer und geschlossener angreifbarer Elemente über die ausgewählte Zeitspanne. **Hinweis:** Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „Last_opened“ und dem Datum und der Uhrzeit des Sammlungsauftrags.
Geschlossene angreifbare Elemente nach Korrekturzielstatus	Balken	Anzahl der geschlossenen angreifbaren Elemente, gruppiert nach Nachbesserungszielstatus für die ausgewählte Zeitspanne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
		Hinweis: Der Wert für „Alter geschlossen“ wird berechnet, wenn Daten erfasst werden. Der Wert ist die Differenz zwischen dem Datum „Last_opened“ und dem Datum und der Uhrzeit des Sammlungsauftrags.
Kritische angreifbare Elemente nach Zuweisungsgruppe	Liste und Zeile	Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, gruppiert nach Zuweisungsgruppe.
Überfällige kritische angreifbare Elemente nach Zuweisungsgruppe	Liste und Zeile	Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, deren Korrekturzieldaten überschritten wurden, gruppiert nach Zuweisungsgruppe. Korrekturziele werden aus dem Datum der letzten Öffnung plus der Anzahl der Tage (gemessen in 24-Stunden-Schritten) berechnet. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.

Business-Services

Name	Typ	Beschreibung
Kritische angreifbare Elemente	Liste, Position und Verteilungsleiste	Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, gruppiert nach Business-Service. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den beiden Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.
Überfällige kritische angreifbare Elemente	Liste, Position und Verteilungsleiste	Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, deren Korrekturzieldaten überschritten wurden, gruppiert nach Business-Service.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Business-Services (Fortsetzung)

Name	Typ	Beschreibung
		Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den beiden Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.
Hoch angreifbare Elemente	Liste, Position und Verteilungsleiste	Anzahl der aktiven angreifbaren Elemente mit hoher Risikobewertung, gruppiert nach Business-Service. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den beiden Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.
Überfällige hoch angreifbare Elemente	Liste, Position und Verteilungsleiste	Anzahl der aktiven angreifbaren Elemente mit einer hohen Risikobewertung, die ihre Korrekturzieldaten überschritten haben, gruppiert nach Business-Service. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den beiden Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.

Serviceverantwortliche

Name	Typ	Beschreibung
Kritische angreifbare Elemente	Liste, Position und Verteilungsleiste	Anzahl der aktiven angreifbaren Elemente mit kritischer Risikobewertung, gruppiert nach Business-Service-Besitzer. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den beiden Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.
Überfällige kritische angreifbare Elemente	Liste, Position und	Anzahl der aktiven angreifbaren Elemente mit einer kritischen Risikobewertung, die ihre Korrekturzieldaten überschritten haben, gruppiert nach Business-Service-Besitzer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Serviceverantwortliche (Fortsetzung)

Name	Typ	Beschreibung
	Verteilungsleiste	Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den beiden Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.
Hoch angreifbare Elemente	Liste, Position und Verteilungsleiste	Anzahl der aktiven angreifbaren Elemente mit hoher Risikobewertung, gruppiert nach Business-Service-Besitzer. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den beiden Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an.
Überfällige hoch angreifbare Elemente	Liste, Position und Verteilungsleiste	Anzahl der aktiven angreifbaren Elemente mit einer hohen Risikobewertung, die ihre Korrekturzieldaten überschritten haben, gruppiert nach Business-Service-Besitzer. Zeigt einen wöchentlichen Durchschnitt aus der aktuellen und der vorherigen Woche, die Differenz zwischen den beiden Wochen (in Anzahl und Prozent) und einen Trend an. Die Verteilungsleiste zeigt die Differenz zwischen allen Werten auf der aktuellen Seite der Bewertungsliste an. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.

Angreifbare CIs

Name	Typ	Beschreibung
Angreifbare Konfigurationselemente (CIs) nach CI-Klasse	Balken	Anzahlen der Konfigurationselemente mit aktiven Schwachstellen, gruppiert nach CI-Klasse in der CMDB.
Angreifbare Elemente (AEs) nach CI-Klasse	Baumübersicht	Anzahl der aktiven VIS, aufgeschlüsselt nach CI-Klasse.
Durchschnittliche angreifbare Elemente pro CI	Balken	Durchschnittliche Anzahl von angreifbaren Elementen, die zu einem Konfigurationselement gehören, gruppiert nach Risikobewertung.
Nicht abgeglichene CIs	Einzelne Punktzahl	Anzahl der importierten Konfigurationselemente, die keinem vorhandenen CI in der CMDB entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angreifbare CIs (Fortsetzung)

Name	Typ	Beschreibung
Angreifbare CIs ohne Supportgruppe	Einzelne Punktzahl	Anzahl der angreifbaren Konfigurationselemente, denen keine Supportgruppe zugewiesen ist.
Außer Kraft gesetzte oder gestohlene CIs mit aktiven AEs	Einzelne Punktzahl	Anzahl der markierten Konfigurationselemente **Stillgelegt** Oder **Gestohlen** In der CMDB mit aktiven angreifbaren Elementen.

Ausnahmen

Name	Typ	Beschreibung
Zurückgestellte angreifbare Elemente nach Grund	Balken	Anzahl der zurückgestellten angreifbaren Elemente, gruppiert nach Zurückstellungsgrund.
In Kürze ablaufende Zurückstellungsanforderungen	Balken	Anzahl der Zurückstellungsanforderungen, die Korrekturaufgaben oder angreifbaren Elementen zugeordnet sind und kurz davor stehen, zur Überprüfung erneut geöffnet zu werden. Sie werden nach der Anzahl der Tage gruppiert, die bis zur erneuten Öffnung verbleiben. Wenn E-Mail-Benachrichtigungen definiert sind, wird eine E-Mail gesendet.
Zurückgestellte angreifbare Elemente nach Configuration Item (CI) Manager	Balken	Anzahl der zurückgestellten angreifbaren Elemente, gruppiert vom Manager für das zugehörige Konfigurationselement.

Korrektur

Name	Typ	Beschreibung
Korrekturaufgaben nach Risikobewertung und Status	Heatmap	Anzahl der aktiven Korrekturaufgaben, gruppiert nach Risikobewertung und Status.
Korrekturaufgaben nach Risikobewertung und Status des Korrekturziels	Heatmap	Anzahl der aktiven Aufgaben, gruppiert nach Risikobewertung und Status des Korrekturziels. Dieser Bericht schließt zurückgestellte angreifbare Elemente aus.
Kritische Korrekturaufgaben nach Zuweisungsgruppe	Liste und Zeile	Anzahl der aktiven Korrekturaufgaben mit einer kritischen Risikobewertung, gruppiert nach Zuweisungsgruppe. Dieser Bericht enthält keine zurückgestellten Korrekturaufgaben.
Überfällige kritische Korrekturaufgaben nach Zuweisungsgruppe	Liste und Zeile	Anzahl der aktiven Korrekturaufgaben mit einer kritischen Risikobewertung, deren Korrekturzieldaten überschritten wurden, gruppiert nach Zuweisungsgruppe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrektur (Fortsetzung)

Name	Typ	Beschreibung
		Dieser Bericht enthält keine zurückgestellten Korrekturaufgaben.
Nicht zugewiesene Korrekturaufgaben	Einzelne Punktzahl	Anzahl der aktiven Korrekturaufgaben ohne einen Beauftragten oder eine Zuweisungsgruppe.
Nicht zugewiesene angreifbare Elemente	Einzelne Punktzahl	Anzahl der aktiven angreifbaren Elemente ohne einem Beauftragten oder einer Zuweisungsgruppe.

Anzeigen Performance Analytics for Vulnerability Response[PA] Berichte in Echtzeit

Um Ihre wichtigsten angreifbaren Elemente (VIS) zu verwalten und sie schnell zu beheben, zeigen Sie Berichte bei Bedarf in Echtzeit im Vulnerability Management (PA)-Dashboard an. Die Performance Analytics for Vulnerability Response Die Anwendung ist mit einem separaten Abonnement von verfügbar ServiceNow Store.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Um weitere Informationen zu den Berichten für zu zu erhalten Performance Analytics for Vulnerability Response, Siehe Dashboard „Schwachstellenmanagement“ [PA] .

Für weitere Informationen zum Setup und zur Installation von Performance Analytics for Vulnerability Response Anwendung, siehe Installieren und konfigurieren Sie Performance Analytics for Vulnerability Response[PA] Anwendung.

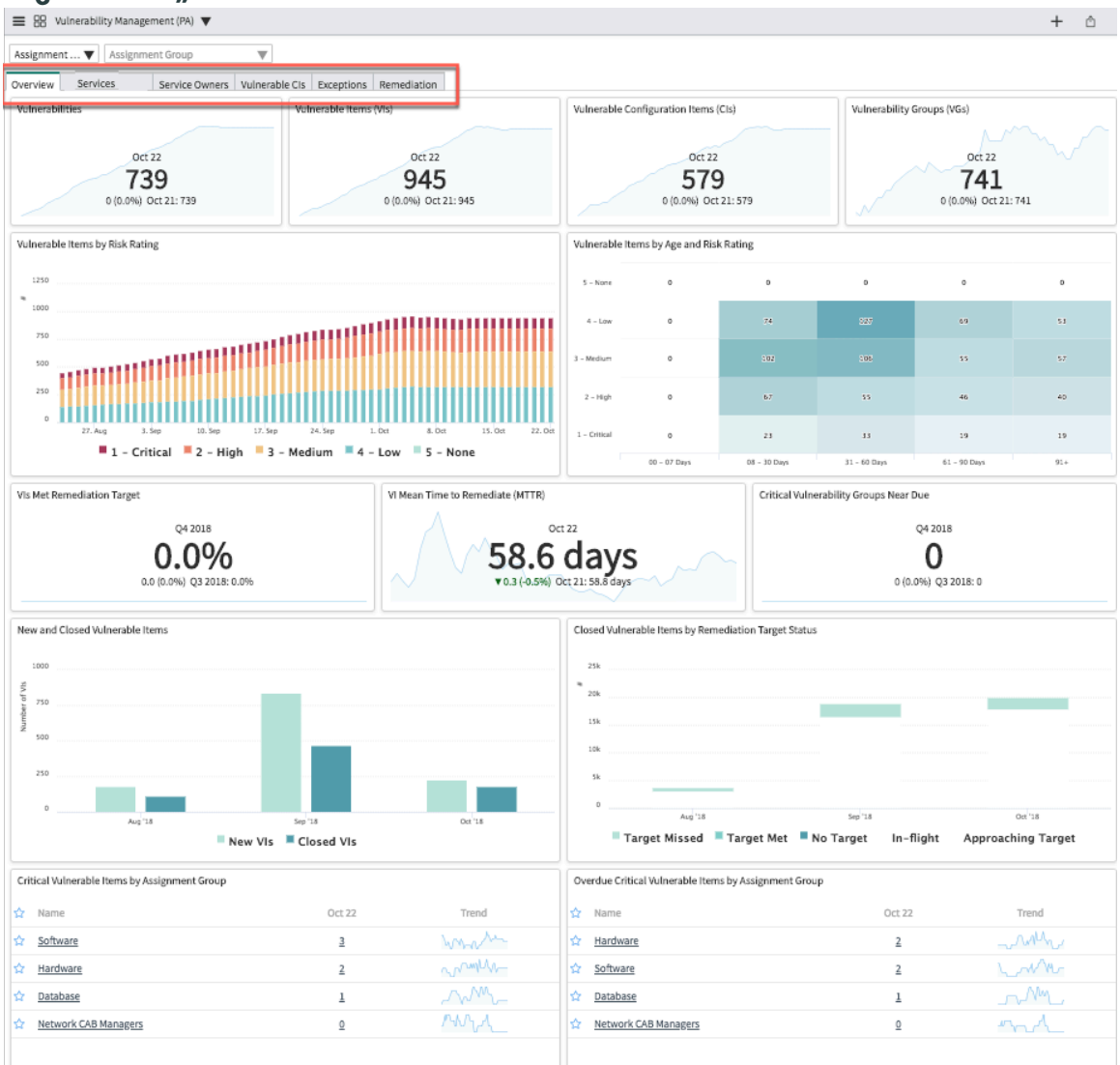
Wenn nicht angezeigt, navigieren Sie zum Anzeigen des Dashboards zu **Vulnerability Response** > **Übersicht**an. Oben im Dashboard werden die Berichtsregisterkarten angezeigt.

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard kann auch in der neuen Experience-UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** Und klicken Sie auf **Dashboards** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Dashboards im Vulnerability Manager-Arbeitsbereich Und Dashboards im Arbeitsbereich „IT-Korrektur“ .

Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Übersicht“



Zeigen Sie die folgenden Berichte auf den Registerkarten des Vulnerability Management (PA)-Dashboards in Echtzeit an.

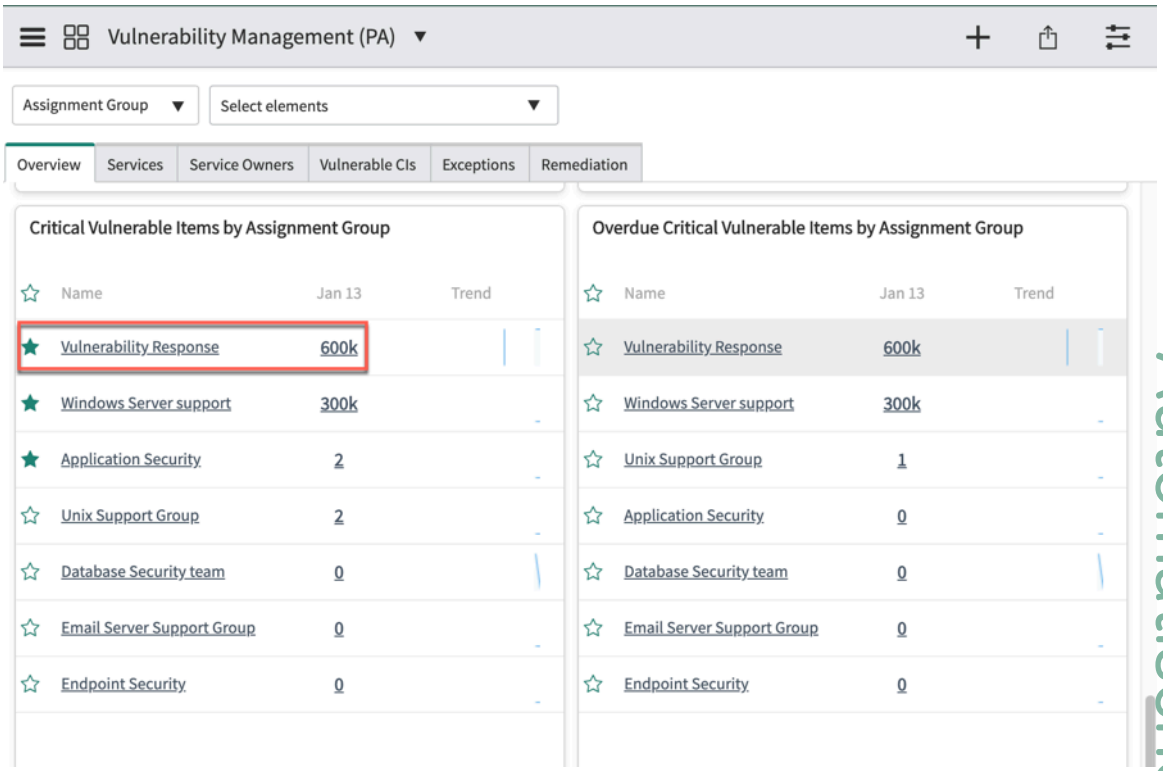
- Registerkarte „Übersicht“
  - Kritische angreifbare Elemente nach Zuweisungsgruppe
- Registerkarte „angreifbare CIs“:
  - Angreifbare CIs ohne Besitzer
  - Außer Kraft gesetzte oder gestohlene CIs mit aktiven AEs
- Registerkarte „Ausnahmen“:
  - Zurückgestellte angreifbare Elemente nach Grund
  - In Kürze ablaufende Zurückstellungsanforderungen
  - Zurückgestellte angreifbare Elemente vom CIO-Manager
- Registerkarte „Korrektur“:
  - Nicht zugewiesene angreifbare Elemente

Um Echtzeitpunktzahlen anzuzeigen, wenn eine der ausgewählten Registerkarten mit Echtzeitberichten ausgewählt ist, führen Sie die folgenden Schritte aus:

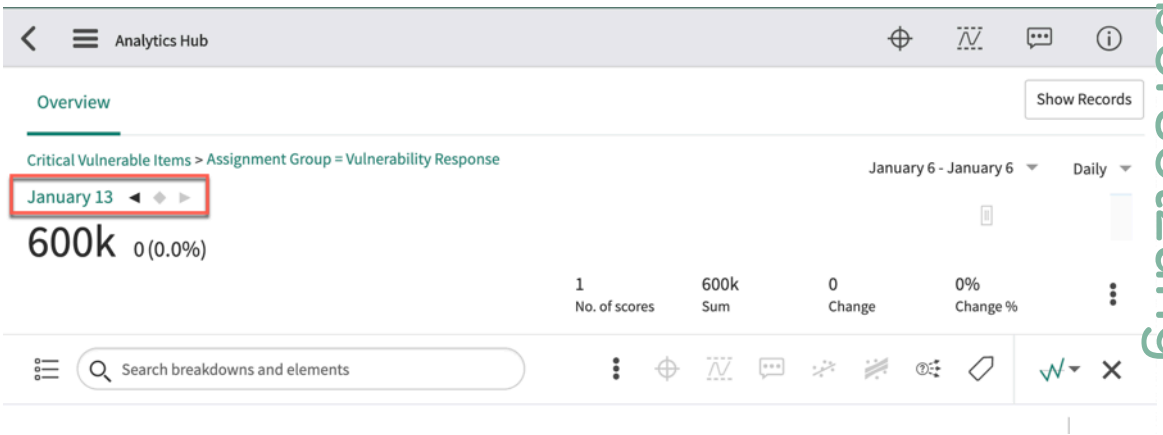
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie im Bericht, z. B. kritische angreifbare Elemente nach Zuweisungsgruppe, auf einen der angezeigten Links.



2. Klicken Sie im angezeigten Datensatz auf das Datum.

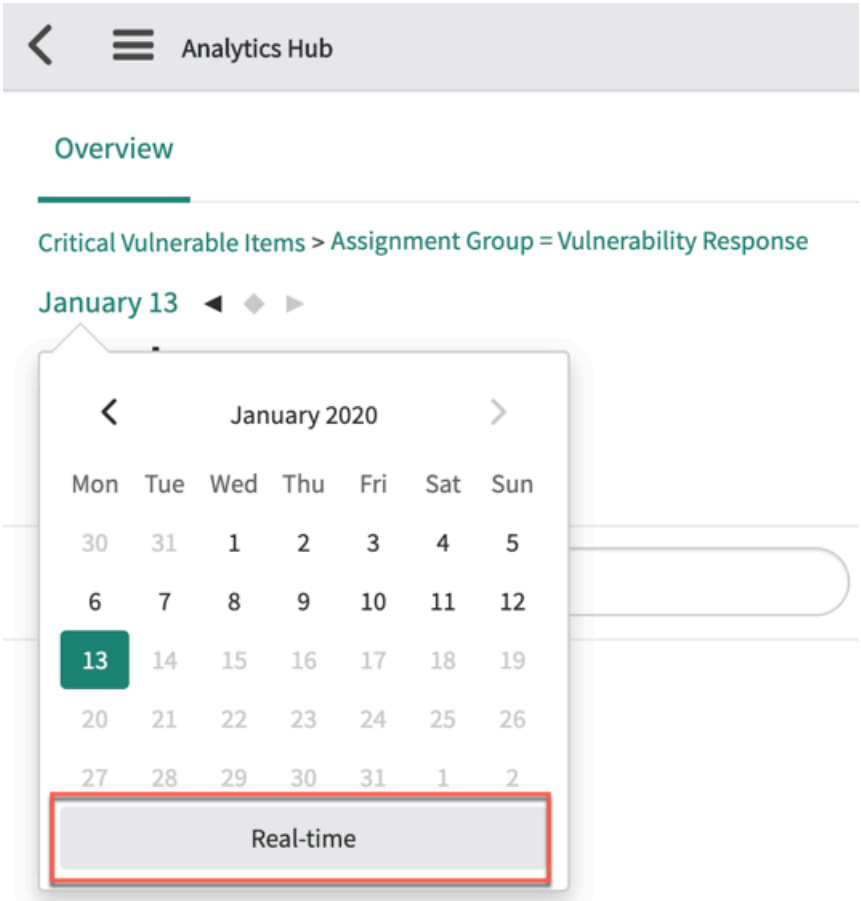


3. Klicken Sie im angezeigten Kalender auf Echtzeit.

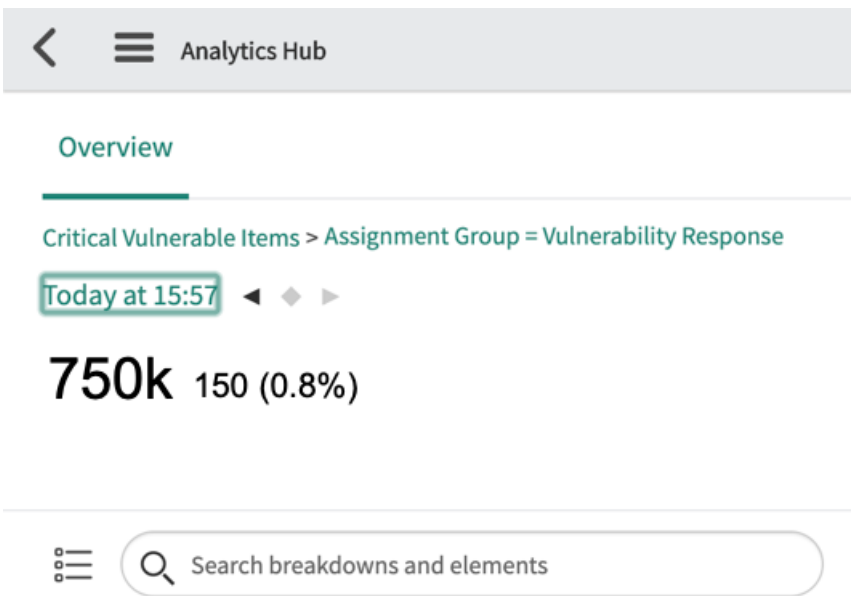
   Wenn ein Bericht keine Echtzeitpunktzahl unterstützt, wird die Echtzeitschaltfläche nicht im Kalender angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Es kann einige Minuten dauern, bis der Wert aktualisiert wird. Das aktuelle Datum, die Datensätze, die Anzahl der neuen Datensätze seit dem letzten Bericht und die prozentuale Änderung gegenüber dem letzten Bericht werden ebenfalls angezeigt.



4. **Wahlweise:** Um die Datensätze anzuzeigen, aus denen der Bericht besteht, und der Echtzeitbericht wird oben rechts angezeigt, klicken Sie auf **Datensätze anzeigen** .
Eine Liste der Datensätze, aus denen die Punktzahl besteht, wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie an Performance Analytics-Indikatoren für Vulnerability Response[PA]

Automatisiert und formuliert anzeigen Performance Analytics Indikatoren, die die Schwachstellendaten in Ihrer Instanz darstellen.

Vorbereitungen

Die Option Datensätze sammeln für die Indikatoren ist für die Anwendung Performance Analytics – Content Pack Vulnerability Response standardmäßig inaktiv. Diese Option ist deaktiviert, damit bestimmte Berichte in Echtzeit angezeigt werden können. Trendinformationen, die von diesen Indikatoren verwendet werden, sind weiterhin verfügbar, wenn Sie die manuelle Erfassung von Datensätzen aktivieren und die Datensätze anzeigen möchten, aus denen die Punktzahlen bestehen.

Hinweis:
Das Aktivieren von Datensätzen in einem Indikator kann sich auf Ihre Leistung auswirken und den für die Ausführung des Datensammlungsauftrags erforderlichen Zeit- und Arbeitsspeicher erheblich verlängern.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet) oder PA.Viewer

Warum und wann dieser Vorgang ausgeführt wird

Vulnerability Response Verfügt sowohl über automatisierte als auch über formulierte Indikatoren.

Wichtige Begriffe

PA-Indikator

Definiert eine Leistungsmessung, die in regelmäßigen Abständen eines Business-Service, einer Aktivität oder eines Organisationsverhaltens durchgeführt wird, z. B. nicht zurückgestellte überfällige kritische angreifbare Elemente.

PA-Indikatorquelle

Datensätze, die Datensätze aus einer Tabellen- oder Datenbankansicht filtern, z. B. VI aktiv.

Datensätze erfassen

Wenn diese Option aktiviert ist, werden Datensätze im Arbeitsspeicher gespeichert und Zugriff auf Analytics Hub gewährt.

Aufgliederungen

Aufgliederungen filtern und gruppieren gesammelte Datensätze. Aufgliederungen können die Speichernutzung erhöhen, insbesondere wenn ihre Anzahl und Vielfalt zunehmen.

Aufgliederungsausschlüsse

Ausschlüsse entfernen bestimmte Aufgliederungen, was den Arbeitsspeicherverbrauch reduzieren kann.

Prozedur

1. Navigieren Sie für automatisierte Indikatoren zu **Performance Analytics** > **Indikatoren** > **Automatisierte Indikatoren**an.
2. Navigieren Sie für formulierte Indikatoren zu **Performance Analytics** > **Formelindikatoren**an.

   Detaillierte Informationen zu Indikatoren finden Sie unter Performance Analytics-Indikatoren .
3. Suchen Sie in beiden Fällen nach **Anwendung** > **Performance Analytics**an.

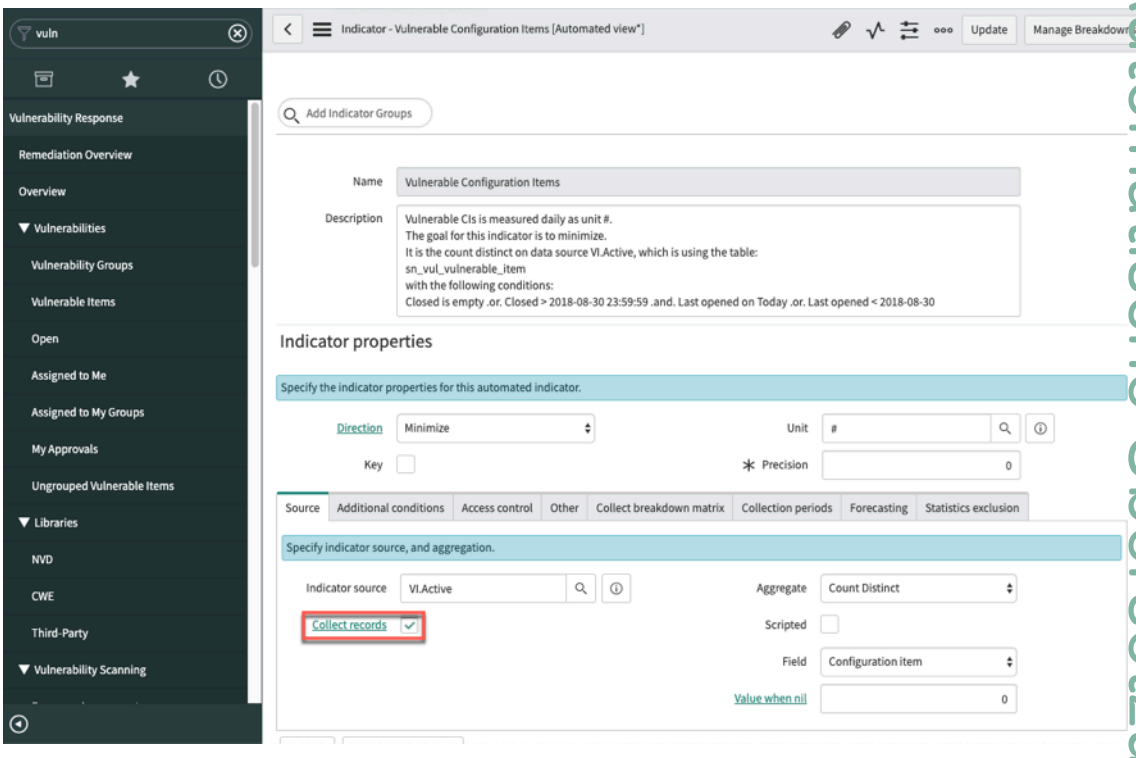
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn sie sich nicht in Ihrer Standardansicht befindet, fügen Sie hinzu **Anwendung** Spalte mit dem Zahnradsymbol ( ) In der oberen linken Ecke der Seite. Die Spalte Anwendung wird dann in Ihrem Dropdown-Menü „Suche“ angezeigt.

4. **Wahlweise:** Dient zum Aktivieren der Datensatzerfassung in einer Performance Analytics für Vulnerability Response Führen Sie die folgenden Schritte aus:

   a. Wenn die Liste der automatisierten Indikatoren angezeigt wird, klicken Sie in der Spalte Name auf den Indikator, für den Sie Datensatzerfassung aktivieren möchten.
   Der Indikatordatensatz wird angezeigt.

   b. Aktivieren Sie im Abschnitt Indikatoreigenschaften bei ausgewählter Registerkarte Quelle das Kontrollkästchen Datensätze sammeln.



   c. Wählen Sie eine, um fortzufahren.

Option	Beschreibung
Aktualisieren	Speichern Sie Ihre Änderungen, und kehren Sie zur Liste der Indikatoren zurück.
Aufgliederungen verwalten **Hinweis:** Wenn Sie Aufgliederungen der zweiten Ebene erneut aktivieren, können Sie Ihren Arbeitsspeicherverbrauch erheblich erhöhen und die Datensammlungsaufgabe verlangsamen.	Aktivieren Sie Aufgliederungen der zweiten Ebene für die aufgeführten Indikatoren erneut, oder bearbeiten Sie Aufgliederungen für andere Indikatoren. (Optional) Weitere Informationen zu Performance Analytics-Aufgliederungen

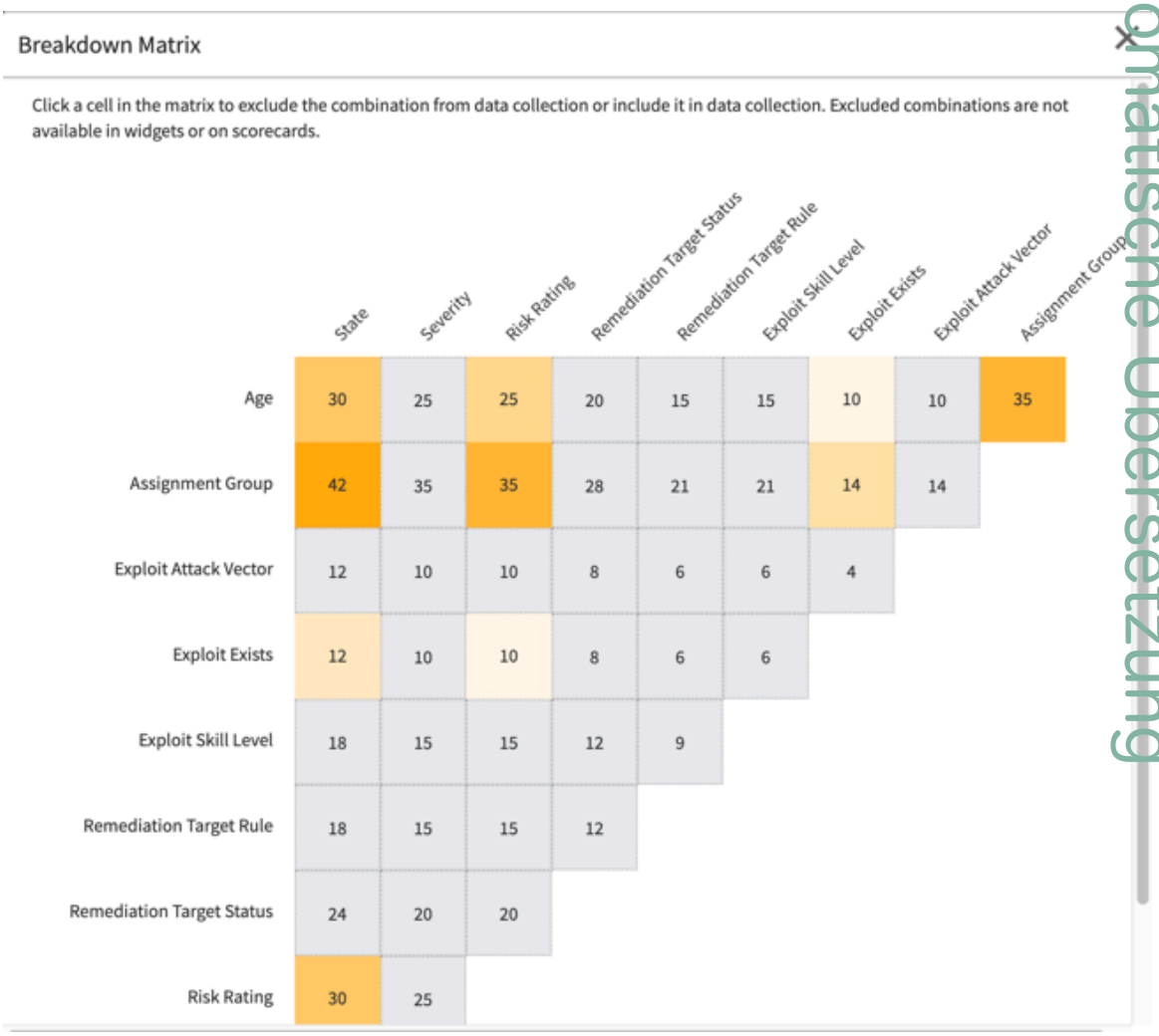
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Standardmäßig wurden Aufgliederungsausschlüsse der zweiten Ebene auf die folgenden Indikatoren angewendet: ▪ Angreifbare Konfigurationselemente ▪ Stillgelegte CIs ▪ Zurückgestellte AEs	finden Sie unter Performance Analytics-Aufgliederungen .

d. Klicken Sie auf **Aufgliederungen verwalten**.

e. Klicken Sie im angezeigten Formular auf **Konfigurieren Sie Die Aufgliederungsmatrix** .
Das Formular Aufgliederungsmatrix wird angezeigt. Ausgeschlossene Kombinationen werden ausgewählt und mit Farben angezeigt, wie in der folgenden Abbildung dargestellt.



f. Um den Ausschluss zu entfernen und eine ausgeschlossene Kombination zu reaktivieren, klicken Sie auf eine ausgewählte Zelle.

g. Klicken Sie oben rechts im Formular auf **Schließen** Um das Formular „Aufgliederung verwalten“ zurückzugeben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Klicken Sie auf den zurück-Pfeil, um zum Indikatordatensatz zurückzukehren.

i. Klicken Sie Auf **Aktualisieren** Um Ihre Änderungen zu speichern und zur Liste der Indikatoren zurückzukehren.

Framework für zusammengefasste Berichte

Mit dem Framework für zusammengefasste Berichte können Sie Berichte für die Daten erstellen, die komplexe und lang laufende On-the-fly-Abfragen umfassen, um die Leistung zu verbessern.

Das Framework für zusammengefasste Berichte verbessert die Leistung durch:

- Verwendung weniger Ressourcen und schnelleres Rendern von Berichten,
- Aggregieren der Daten und Wiederverwendung von Zusammenfassungen und Aufgliederungen (Gruppieren nach) und
- Die Abfragen in der Datenbank werden reduziert

Wenn Sie mehr als eine Million angreifbarer Elemente haben, verwenden Sie neben den Standardberichten das Framework für zusammengefasste Berichte, das in Vulnerability Response Common bereitgestellt wird.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- ServiceNow AI Platform Administrator (admin): Installiert und aktiviert Platform Analytics-Lösung und nimmt alle erforderlichen Änderungen an Systemeigenschaften vor.
- Performance Analytics Administrator (PA_admin): Überprüfen Sie die Zusammenfassungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.
- Administrator (sn_vul_cmn.admin): Zusammenfassungen erstellen.
- VR write(sn_vul_cmn.write): Bearbeiten Sie die Daten in den Zusammenfassungen und aggregierten Ergebnissen.
- VR-Lesen (sn_vul_cmn.read): Überprüfen Sie die Daten in den Zusammenfassungen und aggregierten Ergebnissen.
- Schwachstellenanalyst (sn_vul.Vulnerability_Analyst): Überprüfen Sie die zusammengefassten Ergebnisse.

Zugehörige Informationen

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Dient zum Analysieren der Leistung eines bestimmten Aspekts in einem Geschäftsprozess, der in einem aufgezeichnet wird ServiceNow Tabelle erstellen Sie eine für den Aspekt spezifische Zusammenfassung, und erstellen Sie einen Bericht für diese Zusammenfassung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_vul_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Zusammengefasste Berichte** > **Zusammenfassungsdefinitionen** > **Alle** Und klicken Sie auf **Neu** .
2. In **Name** Feld, geben Sie der Zusammenfassung einen beschreibenden Namen.
3. In **Beschreibung** Geben Sie eine kurze Beschreibung der Zusammenfassung an.
4. In **Quelle** Füllen Sie die Felder aus.

Felder auf der Registerkarte „Quelle“

Feld	Beschreibung
Tabelle	Tabelle, aus der Sie die Daten für den Bericht abrufen möchten. Diese Dropdown-Liste enthält nur die Tabellen „App sec Common“, „App-vul“, „App-vulc“, „App-vul-Container“ und „Anwendungsschwachstellen“.
Aggregatfunktion	Funktion, die auf die in ausgewählte Spalte angewendet werden soll **Feld** . ○ **Anzahl** : Anzahl der Datensätze. ○ **Summe** : Gesamtsumme der Werte in der in ausgewählten Spalte **Feld** . ○ **Durchschnitt** : Durchschnitt aller Werte in einer in ausgewählten Spalte **Feld** . ○ **Maximum** : Höchstwert in der in ausgewählten Spalte **Feld** . ○ **Minimum** : Mindestwert der in ausgewählten Spalte **Feld** . ○ **Eindeutige Anzahl** : Eindeutige Werte in der in ausgewählten Spalte **Feld** .
Feld	Spalte, auf die Sie die Funktion anwenden möchten. **Hinweis:** Dieses Feld wird nicht angezeigt, wenn Sie auswählen **Anzahl** In **Aggregatfunktion** Feld.

5. In **Zusätzliche Bedingungen** Registerkarte geben Sie die Bedingung in an **Bedingungen** Feld zum Auswählen eines bestimmten Satzes von Datensätzen, für die Sie die zusammengefassten Ergebnisse abrufen möchten.
6. In **Gruppieren Nach** Wählen Sie die Spalten der Tabelle aus, nach denen Sie die Daten gruppieren oder stapeln möchten.
   Sie können bis zu zwei Aufgliederungen auswählen.

   Wenn Sie auswählen **Datum** Spalte in einem beliebigen Feld „Gruppieren nach“, die **Trend nach** Feld wird angezeigt. Sie können die Zusammenfassungsergebnisse abrufen, die nach

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Woche, Tag, Minuten usw. kategorisiert sind, indem Sie die Optionen im auswählen **Trend nach** Feld.

7. In **Zeitplan** Wählen Sie auf der Registerkarte einen Zusammenfassungszeitplan aus, oder erstellen Sie einen Zusammenfassungszeitplan, der die Häufigkeit definiert, mit der Sie die Zusammenfassung ausführen können, um die Daten abzurufen.
   Informationen zum Erstellen eines Zusammenfassungszeitplans finden Sie unter Führen Sie mehrere Zusammenfassungen gleichzeitig aus.

   Hinweis:
   Sie können die Zusammenfassungsausführung für eine inaktive Zusammenfassungsdefinition nicht planen.

8. Klicken Sie Auf **Übermitteln** Um die Zusammenfassung zu erstellen.
   Die Zusammenfassung wird in der Zusammenfassungsliste angezeigt. Mit der vordefinierten Häufigkeit wird die Zusammenfassung ausgeführt, und für jede Ausführung wird ein Datensatz zusammen mit einem Ausführungsdatum und einer Ausführungszeit in der zugehörigen Liste „geplante Ausführungen“ erstellt.
9. Navigieren zu **Alle** > **Zusammengefasste Ergebnisse** Und öffnen Sie Ihre Zusammenfassung, um die zusammengefassten Ergebnisse und geplanten Ausführungen anzuzeigen.
   Die zusammengefassten Ergebnisse werden in aufgeführt **Zusammengefasste Ergebnisse** Zugehörige Liste. Wenn die Zusammenfassungsausführung fehlschlägt, finden Sie weitere Informationen unter **Notizen** Spalte in **Geplante Ausführungen** Zugehörige Liste für weitere Informationen.
10. **Wahlweise:** Wählen Sie Aus **Jetzt Ausführen** Dient zum Sammeln der Zusammenfassungsergebnisse unabhängig vom Zusammenfassungszeitplan.
    Wenn Sie die geplante Ausführung beenden, während sie ausgeführt wird, werden keine Änderungen an den aggregierten Ergebnissen vorgenommen. Sie können eine Zusammenfassung auch löschen oder deaktivieren.

Nächste Maßnahme
Erstellen Sie einen Bericht mithilfe Ihrer Zusammenfassung. Weitere Informationen zum Erstellen eines Berichts mithilfe einer Zusammenfassung finden Sie unter Erstellen Sie einen Bericht mithilfe einer Zusammenfassung.

Zugehörige Informationen

Framework für zusammengefasste Berichte

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Sie können die Ausführung mehrerer Zusammenfassungen mit einem einzigen Zusammenfassungszeitplan planen.

Vorbereitungen
Erforderliche Rolle: sn_vul_cmn.admin

Warum und wann dieser Vorgang ausgeführt wird
Angenommen, Sie möchten sechs Zusammenfassungen gleichzeitig ausführen. Erstellen Sie einen Zusammenfassungszeitplan, und fügen Sie ihm alle Zusammenfassungen hinzu. Diese Zusammenfassungen werden mit der definierten Häufigkeit und zum definierten Zeitpunkt ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Zusammengefasste Berichte** > **Zeitplan**an.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular „Zusammenfassungszeitplan“ aus.

Feld	Beschreibung
Zeitplanname	Name des Zusammenfassungszeitplans.
Aufgabe planen	Geplante Skriptausführung, die die Häufigkeit definiert, mit der die Zusammenfassungen ausgeführt werden müssen. Sie können eine geplante Aufgabe erstellen, indem Sie auswählen **Neu** Schaltfläche.

4. Wählen Sie **Absenden**.
   Der Zusammenfassungszeitplan wird in der Liste Zusammenfassungszeitplan angezeigt.
5. Öffnen Sie Ihren Zusammenfassungszeitplan.
6. Wählen Sie Aus **Bearbeiten** , Fügen Sie die Zusammenfassungen zu hinzu **Zusammenfassungsliste** , Und wählen Sie aus **Speichern** .
   Die ausgewählten Zusammenfassungen werden in der zugehörigen Liste „Zusammenfassungen“ angezeigt.

   Hinweis:
   Wenn Sie einem Zeitplan eine inaktive Zusammenfassung hinzufügen, wird die geplante Ausführung nicht gestartet.

7. Wählen Sie **Aktualisieren**.
   Diese Zusammenfassungen werden mit der im Zusammenfassungszeitplan definierten Häufigkeit ausgeführt.

Zugehörige Informationen

Framework für zusammengefasste Berichte

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Ein neuer Prozessor oder ein Hintergrundauftrag, Aggregated Reporting Framework Processor, wird mit dem Basissystem geliefert, das die geplanten Aufgaben ausführt, die sich auf die Tabelle „Framework für zusammengefasste Berichte“ beziehen. Dadurch kann das gesamte Subsystem im Hintergrund ausgeführt werden, und es ermöglicht eine bessere Auslastung der Systemressourcen, wenn sie verfügbar sind.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Hintergrundauftragskonfiguration – Common-Aggregation-Ergebnisrechner Für Vulnerability Response**an.
2. Definieren Sie die Anzahl der Zusammenfassungen, die Sie gleichzeitig in ausführen möchten **Max. Gleichzeitige Threads** Abgelegt und auswählen **Speichern** .
   Standardmäßig werden vier Zusammenfassungen gleichzeitig ausgeführt.
3. Navigieren Sie zur Liste Hintergrundauftrags-Prozessor-Pools, **sn_sec_cmn_background_Job_processor_Pool.list**, Und wählen Sie aus **Neu** Dient zum Erstellen eines Hintergrundauftrags-Prozessors für das Framework für zusammengefasste Berichte.
   Weitere Informationen zum Erstellen eines Hintergrundauftrags-Prozessorpools finden Sie unter Erweiterte parallele Verarbeitung für Hintergrundaufträge in Vulnerability Response .

Hinweis:
Die Anzahl der Hintergrundauftragsprozessoren muss der Anzahl der maximalen gleichzeitigen Threads entsprechen, die in angegeben werden **Hintergrundauftragskonfiguration – Common-Aggregation-Ergebnisrechner Für Vulnerability Response** Formular. Siehe Schritt 2 .

Zugehörige Informationen

Framework für zusammengefasste Berichte

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Um die spezifischen Daten für eine von Ihnen erstellte Zusammenfassung zu visualisieren und zu analysieren, generieren Sie einen Bericht, indem Sie im Bedingungsgenerator eine Bedingung für die Zusammenfassung angeben.

Vorbereitungen

Erforderliche Rolle: pa_admin

Prozedur

1. Navigieren zu **Alle** > **Berichte** > **Neu erstellen**an.
2. In **Daten** Füllen Sie die Felder aus.

Felder der Registerkarte „Daten“

Feld	Beschreibung
Berichtname	Name des Berichts.
Quelltyp	Typ der Quelle, aus der Daten abgerufen werden. Wählen Sie **Tabelle** aus.
Tabelle	Name der Tabelle, für die die Zusammenfassung erstellt wird. Wählen Sie die Tabelle „zusammengefasste Ergebnisse“ aus **Aggregiertes Ergebnis [sn_vul_cmn_aggregate_result]** .

3. Legen Sie im Bedingungsgenerator die Bedingung für Ihre Zusammenfassung fest, für die Sie einen Bericht generieren möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingung im Bedingungsgenerator

Teil	Beschreibung
Feld	Wählen Sie Aus **Zusammenfassung** .
Operator	Wählen Sie Aus **Ist** .
Wert	Name der Zusammenfassung.

4. In **Daten** Wählen Sie die Registerkarte aus **Als Nächstes** .
5. In **Typen** Wählen Sie die Registerkarte aus, wie Sie die Daten visualisieren möchten, und wählen Sie aus **Als Nächstes** .
   Weitere Informationen zu den Berichtstypen finden Sie unter Berichte Werden Erstellt .

   Die unterstützten Visualisierungen sind Balkendiagramm, Kreisdiagramm und Heatmap. Sie können die Liniendiagramme und andere Trendvisualisierungen ändern, um die unterstützten Visualisierungen mit aggregiertem Ergebnis zu verwenden, um dieselben Daten darzustellen. Listenansicht wird nicht unterstützt.
6. In **Konfigurieren** Füllen Sie die Felder aus.

Feld	Beschreibung
Gruppieren nach	Gruppiert die Daten nach dem ausgewählten Feld. Wählen Sie hier das Feld aus, das Sie in ausgewählt haben **Gruppiert nach 1** Feld in #unique_506_Connect_42_group-by Registerkarte der Zusammenfassung.
Stapeln nach	Organisiert Daten basierend auf dem ausgewählten Feld in Ebenen. Wählen Sie hier das Feld aus, das Sie in ausgewählt haben **Gruppiert nach 2** Feld in #unique_506_Connect_42_group-by Registerkarte der Zusammenfassung. **Hinweis:** Nur Balken- und horizontale Balkenberichte verwenden gestapelte Daten. Andere Berichtstypen ermöglichen nur die Gruppierung.
Aggregation	Anwenden **Minimum** Oder **Maximum** Funktion aktiviert **Wert** .

7. In **Stil** Füllen Sie die Felder entsprechend aus, und wählen Sie aus **Ausführen** .
   Für weitere Informationen zu den Feldern in **Konfigurieren** Und **Stil** Registerkarten, siehe Erstellen eines Berichts Video.
8. Legen Sie im Bedingungsgenerator die Bedingung für Ihre Zusammenfassung fest, für die Sie einen Bericht generieren möchten, und wählen Sie sie aus **Ausführen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

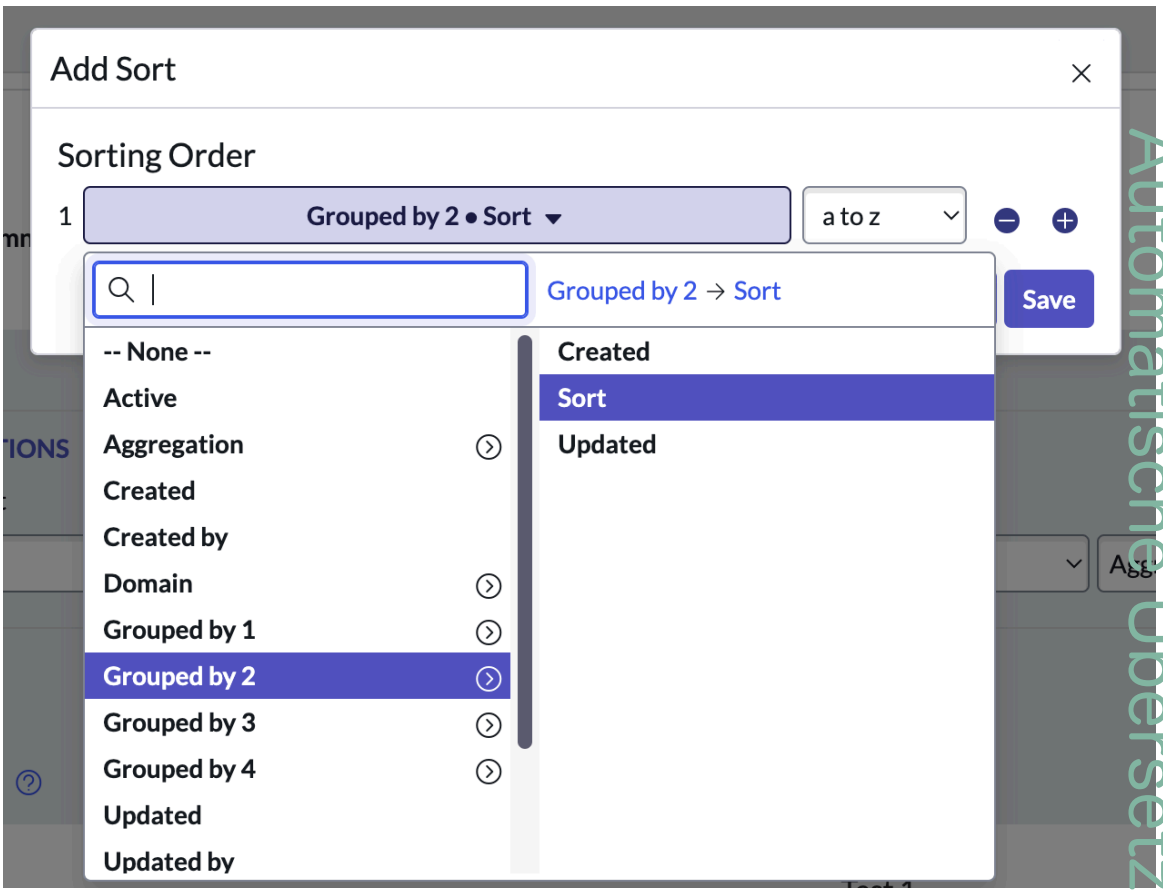
Der Bericht wird angezeigt.

9. Wählen Sie aus, um die Werte auf der X-Achse zu sortieren **Sortierung hinzufügen** .

   a. Geben Sie für Zeichenfolgen die Bedingung als an **Gruppiert nach > a–z oder z–a** Zum Sortieren der Zeichenfolgen in alphabetischer Reihenfolge.

   b. Geben Sie für die Datentypwerte „Ganzzahl“ und „Datum“ die Bedingung als an **Gruppiert nach.sort > a–z oder z–a** Zum Sortieren der Werte in aufsteigender bzw. absteigender Reihenfolge.

Ganzzahlen werden auf der X-Achse sortiert

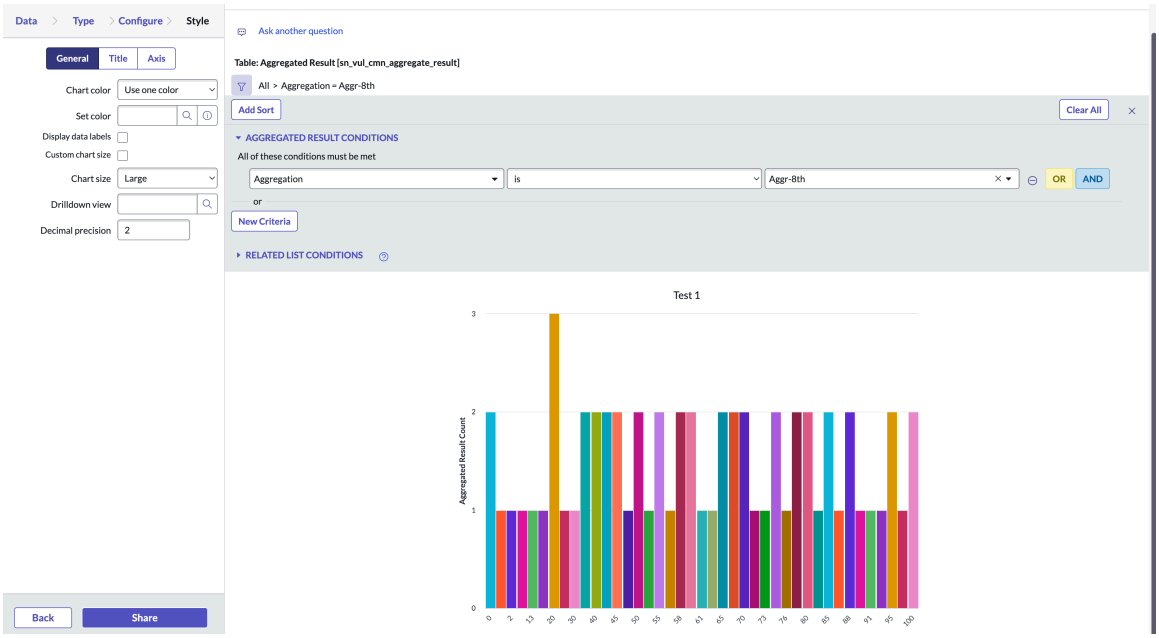


   c. Wählen Sie **Ausführen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Ganzzahl- und Datumswerte werden auf der X-Achse sortiert.



10. Wählen Sie Aus **Speichern** Um Ihren Bericht zu speichern.
    Der für eine Zusammenfassung generierte Bericht wird in angezeigt **Ergebnisse** Registerkarte des jeweiligen **Zusammenfassung** Formular.
11. **Wahlweise:** Fügen Sie Ihren Bericht einem Dashboard hinzu.
    Weitere Informationen zum Hinzufügen eines Berichts zu einem Dashboard finden Sie unter Fügen Sie einem reaktionsfähigen Dashboard einen Bericht hinzu .

    Die **Schwachstellenmanagement [Aggregiert]** Dashboard, das aus Berichten besteht, die mit dem zwischengespeicherten Reporting-Framework erstellt wurden, wird im Lieferumfang des Basissystems enthalten. Um dieses Dashboard anzuzeigen, navigieren Sie zu **Alle** > **Performance Analytics** > **Dashboards** > **Alle** > **Schwachstellenmanagement [Aggregiert]**an. Die aktiven Zusammenfassungen, die den Berichten in diesem Dashboard entsprechen, werden mit dem Basissystem geliefert.
12. Geben Sie Ihren Bericht für andere Anwender frei.
    Weitere Informationen zum Freigeben von Berichten finden Sie unter Berichte verteilen .

Zugehörige Informationen

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Framework für zusammengefasste Berichte

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Vulnerability Response Referenzinformationen

Die folgenden Themen enthalten neben Felddaten in den Formularen und Datensätzen in Links, Referenzinformationen, Problembehandlungen und Wissensartikel Vulnerability Response.

Unten finden Sie einige Links zu anderen Ressourcen, die Ihnen hilfreich sein könnten, beginnend mit einem Link zu den Knowledge Base-Links für Support und Problembehandlung VR/CC-artikel in der HI Knowledge Base.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Knowledge Base-Links für Support und Problembehandlung für VR/CC
- Weitere Informationen zu Anwendungen und Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema .
- Security Operations-Videos
- Entwicklerschulungen
- Entwicklerdokumentation
- Arbeiten Sie mit einem Implementierungsspezialisten zusammen, um Ihre gewünschten Geschäftsergebnisse mit zu erzielen Customer Success Center .
- Nehmen Sie an einem Vulnerability Response-Kurs Teil, um Fachwissen aufzubauen und den ROI schneller zu realisieren. Besuchen Sie zur Anmeldung die ServiceNow-Schulungs- und -Zertifizierungs-Website .
- Suchen Sie Komponenten, die mit einer Anwendung installiert sind
- Vulnerability Response Orchestration
- Tipps zum Schreiben von Integrationen
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Implementierungsprüfliste für Vulnerability Response Anwendung

Diese Prüfliste listet die Schritte auf, die für eine grundlegende Implementierung von erforderlich sind Vulnerability Response Anwendung auf Ihrem ServiceNow AI Platform® Instanz. Wenn Sie diese Aufgaben abgeschlossen haben, ist das Basissystem bereit für den Betrieb und die Verifizierung.

Vorbereitungen

Erforderliche Rollen: administrator zum Herunterladen und Aktivieren von Anwendungen und Zuweisen von Rollen, sn_vul.Vulnerability_admin zum Konfigurieren Vulnerability Response.

Prozedur

1. Erwägen Sie, eine PDF-Datei dieser Prüfliste zu erstellen und zu drucken, damit Sie Aufgaben beim Abschließen abchecken können.
2. Klicken Sie auf , um eine PDF-Datei zu generieren **Speichern Sie als PDF** Symbol ( ) Oben im Thema, und klicken Sie auf ausgewähltes Thema.

Vulnerability Response Prüflistenaufgaben für Basisimplementierungen für Administrator

Element	Beschreibung
☐	Stellen Sie als Anwender mit der Administratorrolle sicher, dass Sie über alle Berechtigungen verfügen und heruntergeladen haben (**Installieren**) Die folgenden Anwendungen aus dem ServiceNow® Store Auf Ihrem ServiceNow AI Platform Instanz: ○ Vulnerability Response ○ Vulnerability Response Integration mit der NIST National Vulnerability Database ○ Qualys Integration für Security Operations

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Beschreibung
	a. Um zu überprüfen, ob die Anwendungen in Ihrer Instanz verfügbar sind, navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** Und suchen Sie nach [sn_vul], [sn_vul_nvd] und [sn_vul_qualys]. **b.** Wenn Sie die Anwendungen nicht finden können, finden Sie unter Security Operations Und ServiceNow Store Weitere Informationen zum Abrufen von Berechtigungen und zum Herunterladen der Anwendungen.
☐	Navigieren Sie als Anwender mit der Administratorrolle **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung** Und aktivieren (**Installieren**) Der Vulnerability Response Anwendung zusammen mit ihren Abhängigkeiten von ServiceNow AI Platform Instanz. **Hinweis:** Während der Installation von Vulnerability Response Anwendung haben Sie die Möglichkeit, Demodaten zu installieren. Demodaten sind erforderlich, wenn Sie automatisierte Tests ausführen möchten, um sicherzustellen, dass Ihre Instanz nach der Installation funktioniert. Führen Sie Tests nur für Entwicklungs-, Test- und andere Instanzen außerhalb der Produktion aus, um Datenbeschädigung und -Ausfälle zu vermeiden. Wenn Demodaten oder Demoaccounts erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz in nicht-Produktion oder Produktion verwendet wird. Der Setup-Assistent für Vulnerability Response Wird automatisch zusammen mit der Anwendung installiert. Der Setup-Assistent ist erforderlich, um zu konfigurieren Vulnerability Response Anwendung. Darüber hinaus wird es zum Installieren und Konfigurieren von verwendet Qualys Integration für die Anwendung Security Operations, die in diesem Beispiel verwendet wird, sowie andere Anwendungen, die unterstützen und mit kompatibel sind Vulnerability Response. Weitere Informationen zur Installation von finden Sie Vulnerability Response Anwendung, siehe Vulnerability Response installieren.
☐	Navigieren Sie als Anwender mit der Administratorrolle im Setup-Assistenten zu **Alle** > **Vulnerability Response-Anwender und -Gruppen** Und weisen Sie Anwendern die erforderlichen zu Vulnerability Response Persona-Rollen. **a.** Zeigen Sie im Setup-Assistenten vorhandene Anwender und alle bereits zugewiesenen Rollen an, indem Sie auf klicken **Anwenderverwaltungsmodul** Link. **b.** Klicken Sie in der Liste auf einen Anwendernamen, um den Datensatz zu öffnen, und klicken Sie auf **Rollen** Zugehörige Liste. Alle diesem Anwender zugewiesenen Rollen werden angezeigt. **c.** Navigieren Sie zurück zu **Vulnerability Response-Anwender und -Gruppen** Befolgen Sie im Setup-Assistenten die Anweisungen, um die Rolle sn_vul.Vulnerability_admin zuzuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Beschreibung
	Hinweis: Die Rolle sn_vul.Vulnerability_admin ist erforderlich, um mit der Konfiguration fortzufahren. Alternativ können Sie mit der Konfiguration als Anwender mit der Administratorrolle fortfahren. (Optional) Sie können auch die Rollen Configuration Item (CI) Manager [sn_vul.ci_Manager] und Ausnahmegenehmiger [sn_vul.Exception_Approver] zuweisen, aber diese Personas sind für die verbleibenden Setup-Aufgaben nicht erforderlich. Weitere Informationen zum Zuweisen der Persona-Rollen mit dem Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zu Anwendern und zum Zuweisen von Rollen zu Anwendern und Gruppen finden Sie unter Anwenderverwaltung .
☐	**a.** Navigieren zu **Alle** > **Administration** > **Integrationen** Und verifizieren Sie **CWE – umfassende 2000-Integration** Ist aktiviert und führt die geplante Aufgabe aus, um Daten zu importieren. **b.** Navigieren Sie als Anwender mit der Administratorrolle zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** Und aktivieren (**Installieren**) Die Anwendung Vulnerability Response Integration mit NVD. Führen Sie die NVD- und CWE-Integrationen als Teil Ihres ersten Setups von aus Vulnerability Response Und vor dem Importieren von Schwachstellendaten in Ihre Instanz mit einem Scanner-Produkt eines Drittanbieters. Siehe Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken Und Konfigurieren und führen Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen aus Weitere Informationen zum Installieren, Konfigurieren und Anzeigen der NVD- und CWE-Bibliotheken.
☐	Navigieren Sie als Anwender mit der Administratorrolle **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung** Und aktivieren Sie Qualys Integration für Security Operations-Anwendung. Bevor Sie ein Scannerprodukt eines Drittanbieters wie installieren und ausführen Qualys Mit einer Bibliothek müssen Sie zuerst die NVD- und CWE-Integrationen installieren und ausführen, um Schwachstellendaten zu erfassen. Weitere Informationen finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.
☐	(Optional) als Anwender mit der Administratorrolle, wenn Sie Demodaten mit installiert haben Vulnerability Response-Anwendung können Sie ausführen Vulnerability Response ATF-Test-Suite, um zu überprüfen, ob die Anwendungen erfolgreich installiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Beschreibung
	Hinweis: Führen Sie Tests nur für Entwicklungs-, Test- und andere Instanzen außerhalb der Produktion aus, um Datenbeschädigung und -Ausfälle zu vermeiden. Weitere Informationen finden Sie unter Führen Sie die Test-Suite für Automated Test Framework (ATF) aus Vulnerability Response. Weitere Informationen zu automatisierten Tests finden Sie unter Automated Test Framework (ATF) .

3. Fahren Sie mit der Konfiguration der Anwendungen fort, beginnend im Abschnitt Einstellungen für Vulnerability Response.

Durch die Überprüfung dieser Einstellungen können Sie verstehen, wie es geht Vulnerability Response Funktioniert, wenn Sie mit der Einrichtung Ihrer Umgebung fortfahren. Für die in diesem Beispiel verwendete Scannerintegration müssen Sie die Einstellungen bearbeiten.

Die Konzepte, die Sie in diesem Konfigurationsbeispiel für verwenden Qualys Das Produkt gilt für andere Scanneranwendungen.

Ihr Qualys Zum Konfigurieren der Anwendung sind Anmeldeinformationen erforderlich. Stellen Sie sicher, dass Sie Accountnamen, Passwörter und andere Serviceinformationen haben, die für erforderlich sind Qualys Produkte, damit Sie Zugriff darauf haben.

Erforderliche Rollen: sn_vul.Vulnerability_admin oder alternativ admin.

Vulnerability Response Prüflistenaufgaben für Basisimplementierungen für Schwachstellenadministrator

Aufgabe	Beschreibung
☐	Überprüfen Sie die Zuweisungsregeln für Schwachstellen. Zuweisungsregeln weisen angreifbare Elemente (VIS) automatisch der entsprechenden Zuweisungsgruppe zu. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Weitere Informationen zum Konfigurieren von Vulnerability Response Verwenden Sie den Setup-Assistenten, siehe Wird Konfiguriert Vulnerability Response Mit dem Setup-Assistenten.
☐	Überprüfen Sie die Regeln für Korrekturaufgaben. Regeln für Korrekturaufgaben gruppieren angreifbare Elemente (VIS) automatisch, wenn sie basierend auf bestimmten Bedingungen importiert werden. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.
☐	Überprüfen Sie die Risikorechner. Risikorechner bewerten angreifbare Elemente für die Priorisierung. Sie können Rechner so konfigurieren, dass sie die Merkmale des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Konfigurationselements (CI), der Exploit-Verfügbarkeit und des Schwachstellenschweregrads berücksichtigen, die von Ihrem Lieferanten der Schwachstellenbewertung (Scanner) gemeldet wurden. Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln für Schwachstellenrechner.
☐	Überprüfen Sie die Korrekturzielregeln. Korrekturzielregeln definieren Korrekturzeitlinien für VIS und Korrekturaufgaben. Weitere Informationen finden Sie unter Vulnerability Response Korrekturzielregeln.
☐	Überprüfen Sie im Abschnitt „Integrationskonfiguration“ die Qualys Anwendungseinstellungen und definieren und planen Sie Ihre Datenimporte. **a.** Klicken Sie Auf **Scanner-Integrationen** . **b.** Klicken Sie auf der Seite „installierte Anwendungen“ auf **Bearbeiten** . **c.** Geben Sie Ihre Anmeldeinformationen ein und klicken Sie auf **Als Nächstes** . **d.** Lesen Sie die Beschreibungen für die Knowledgebase-Konfiguration. **e.** Überprüfen Sie die Seite „Konfiguration der Host-Erkennung“ auf Importeinstellungen, CI-Suchregeln und Importzeitpläne. **f.** Nachdem Sie mit den Einstellungen auf dieser Seite zufrieden sind, klicken Sie auf **Jetzt Ausführen** Zum Importieren von Daten. Klicken Sie auf **Zeigen Sie Details an** Link, der angezeigt wird, um den Ausführungsstatus der Schwachstellenintegration anzuzeigen. **g.** (Optional) Fahren Sie mit der Bearbeitung der Konfigurationseinstellungen fort. **h.** Klicken Sie Auf **Beenden** Um die Installation und Konfiguration im Setup-Assistenten abzuschließen. Weitere Informationen zum Konfigurieren von Qualys Anwendung, siehe Konfigurieren Sie Qualys Vulnerability Integration Mit dem Setup-Assistenten.

Nächste Maßnahme

Herzlichen Glückwunsch! Sie haben erfolgreich installiert Vulnerability Response Anwendung und konfigurierte sie und eine Scanneranwendung mit dem Setup-Assistenten. Das Basissystem ist jetzt betriebsbereit.

Um andere Anwendungen für herunterzuladen, zu installieren und zu konfigurieren Vulnerability Response, Führen Sie die gleichen Schritte und Konzepte aus, die Sie für die vorherige Prüfliste abgeschlossen haben. Weitere Informationen finden Sie in den spezifischen Themen, die für jede Anwendung bereitgestellt werden.

Weitere Informationen zu unterstützten Anwendungen, die für Sie über verfügbar sind ServiceNow Store Für Vulnerability Response, Siehe Installation von Vulnerability Response Und unterstützte Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für weitere Informationen zur Verwendung Vulnerability Response, Siehe Erkunden Sie Vulnerability Response Anwendung.

Vulnerability Response status der Korrekturaufgabe

Drittpartei-Integrationen importieren Erkennungsdaten für angreifbare Elemente, die neue angreifbare Elemente (Vits) erstellen oder vorhandene Vits aktualisieren. erkennungsstatus aktualisieren VIT-status, sofern sie „Offen“ oder „Geschlossen“ sind.

Weitere Informationen dazu, wie sich der Status einer Erkennung auf den Status einer VIT auswirkt, finden Sie unter Erkennungen, Korrekturaufgaben und status angreifbarer Elemente.

Mit Change-Management für Vulnerability Response, Es gibt eine synchronisierte Beziehung zwischen den Statusfeldern der Korrekturaufgaben und den Statusfeldern der Change Requests (CHG) im Vulnerability Response-Produkt. Während eine Change-Anforderung ihren Lebenszyklus durchläuft, verschiebt sie auch den Status aller zugehörigen Korrekturaufgaben automatisch. Nachdem eine Change-Anforderung implementiert wurde, wird die Korrekturaufgabe automatisch gelöst. Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

Hinweis:
Ab v23.0 von Vulnerability Response:

- Die **Statusgenehmigung Der Korrekturaufgabe** Workflow ist veraltet und wird im Flow Designer durch Flow-Korrekturaufgaben-Statusgenehmigung ersetzt.
- Die **Schließen** Schaltfläche wurde für eine Korrekturaufgabe entfernt, und das Schließen einer Korrekturaufgabe wird vom Scanner gesteuert.

In der folgenden Tabelle sind die status der Korrekturaufgabe und die Aktionen aufgeführt, die Sie für eine Korrekturaufgabe im jeweiligen Status ausführen können:

status der Korrekturaufgabe

Status	Beschreibung
Öffnen	Status bei Erstellung. In diesem Status können Sie: **Doppelte VIs anzeigen** Identifizieren Sie doppelte Vits, die von mehreren Scannern im System gemeldet wurden. Sie können die doppelte VIT als gelöst oder Geschlossen markieren. Doppelte Einträge werden nur angezeigt, wenn die Kombination von Schwachstellen mit erstellt wird Allgemeine Schwachstellen und Risiken (CVE) . Weitere Informationen finden Sie unter Vulnerability Response status der Korrekturaufgabe und der angreifbaren Elemente. **Untersuchung starten** Weisen Sie diese Korrekturaufgabe einer Person oder Gruppe zu, um mit der Untersuchung zu beginnen. **Als falsch positiv markieren** Markieren Sie ein Element oder eine Gruppe als falsch positiv, wenn der Scanner meldet, dass im System eine Schwachstelle vorhanden ist, in Wirklichkeit jedoch keine Schwachstelle vorhanden ist. **Ausnahme anfordern** Fordern Sie eine Ausnahme, ein Wiedereröffnungsdatum (bis), einen Grund an, und geben Sie optional zusätzliche Informationen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

status der Korrekturaufgabe (Fortsetzung)

Status	Beschreibung
	Verschiebt die Korrektur des Elements oder der Gruppe bis zum Datum, an dem eine Ausnahme angefordert wird. **Lösen** Markieren Sie als gelöst, um das Element oder die Gruppe in den Status „gelöst“ zu verschieben. **Change erstellen** Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. **Korrekturaufgabe aufteilen** Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Korrekturaufgabe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue Korrekturaufgabe verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe in auf Arbeitsbereich für IT-Korrekturen. **Zurückstellen** Wählen Sie den Status zurückgestellt, ein Datum der erneuten Öffnung und einen Grund aus, und geben Sie optional zusätzliche Informationen an. Verschiebt den Status der Korrekturaufgabe bis zum Datum der erneuten Öffnung. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Gruppe.
Wird untersucht	Ausgelöst durch **Untersuchung Starten** Schaltfläche. In diesem Status können Sie: **Security Incident** Weitere Informationen finden Sie unter Erstellen Sie einen Security Incident . **Change erstellen** Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. **Aufgabe teilen** Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Korrekturaufgabe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue Korrekturaufgabe verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

status der Korrekturaufgabe (Fortsetzung)

Status	Beschreibung
	Erstellen Sie eine Change-Anforderung Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe. **Warten auf Implementierung** Ändert den Status in Warten auf Implementierung. Dieser Status gibt an, dass Korrekturaufgaben außerhalb von verwiesen wurden Vulnerability Response. **Zurückstellen** Wählen Sie den Status zurückgestellt, ein Datum der erneuten Öffnung und einen Grund aus, und geben Sie optional zusätzliche Informationen an. Verschiebt den Status der Korrekturaufgabe bis zum Datum der erneuten Öffnung. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe.
Zurückgestellt	Ausgelöst durch **Ausnahme Anfordern** Schaltfläche. Als Teil des Genehmigungs-Workflows ist der Status „Zurückgestellt“ in Überprüfung und kann erst geschlossen werden, wenn genehmigt wurde. In diesem Status können Sie: **Change erstellen** Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. **Aufgabe teilen** Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Korrekturaufgabe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue VG verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe auf. **Security Incident** Weitere Informationen finden Sie unter Erstellen Sie einen Security Incident . **Erneut öffnen** Übergang zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe. Aufschubinformationen werden unter angezeigt **Schließen/ Zurückstellen** Registerkarte. Am Zurückstellungsdatum wird die Gruppe zur Korrektur erneut geöffnet.
Warten auf Implementierung	Ausgelöst durch **Warten Auf Implementierung** Schaltfläche. In diesem Status können Sie:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

status der Korrekturaufgabe (Fortsetzung)

Status	Beschreibung
	Security Incident Weitere Informationen finden Sie unter Erstellen Sie einen Security Incident . **Change erstellen** Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. **Aufgabe teilen** Verwenden Sie für eine Korrekturaufgabe mit mehr als einem angreifbaren Element eine Reihe von Bedingungen, um eine Teilmenge angreifbarer Elemente herauszufiltern und eine Korrekturaufgabe aufzuteilen. Die von Ihnen ausgewählten Elemente werden automatisch in eine neue Korrekturaufgabe verschoben. Weitere Informationen finden Sie unter Teilen Sie eine Korrekturaufgabe auf. **Erstellen Sie eine Change-Anforderung** Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe. **Zurückstellen** Wählen Sie den Status zurückgestellt, ein Datum der erneuten Öffnung und einen Grund aus, und geben Sie optional zusätzliche Informationen an. Verschiebt den Status der Korrekturaufgabe bis zum Datum der erneuten Öffnung. **Lösen** Fügen Sie Notizen hinzu. Der Status wird gelöst. Notizen werden unter angezeigt **Lösung** Registerkarte. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe.
Gelöst	Ausgelöst von **Lösen** Schaltfläche. In diesem Status können Sie: **Security Incident** Weitere Informationen finden Sie unter Erstellen Sie einen Security Incident . **Change erstellen** Erstellen Sie eine Change-Anforderung, oder ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe und Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu. **Erneut öffnen** Übergang zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

status der Korrekturaufgabe (Fortsetzung)

Status	Beschreibung
	Notizen werden unter angezeigt **Notizen** Registerkarte. Lösungsinformationen werden unter angezeigt **Lösung** Registerkarte.
Geschlossen	Ausgelöst Durch den Scanner. In diesem Status können Sie: **Security Incident** Weitere Informationen finden Sie unter Erstellen Sie einen Security Incident . **Erneut öffnen** Übergang zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe. Abschlussinformationen werden unter angezeigt **Schließen/ Zurückstellen** Registerkarte.

- Der Korrekturbesitzer kann nur ein angreifbares Element oder eine Korrekturaufgabe als gelöst markieren. Basierend auf der Bestätigung vom Scanner kann dieses gelöste Element oder diese Korrekturaufgabe als geschlossen oder erneut geöffnet markiert werden.
- Die **Löschen** Die Schaltfläche ist für den Administrator verfügbar, wenn mehrere angreifbare Elemente manuell erstellt wurden und diese geschlossen oder gelöscht werden müssen.
- Wenn Sie feststellen, dass die Elemente ein geringes Risiko sind, und auf ein Change-Fenster oder einen Patch warten, können Sie ihre Korrekturaufgabe in Zurückstellen ändern Rot status für einen definierten Zeitraum .Sie können mit eine Ausnahme anfordern **Ausnahme Anfordern** Option.

  Hinweis:
  Wenn Korrekturaufgaben zurückgestellt oder geschlossen werden, können Sie Lösungen angeben, um die Gründe dafür weiter zu definieren.

- Wenn eine VIT entweder manuell oder automatisch erneut geöffnet wird, geschieht Folgendes:
  - Der VIT-Status ändert sich in Offen. Der ursprüngliche Status der Korrekturaufgabe wird nicht aktualisiert.
  - Die VIT wird neu bewertet und in eine neue oder vorhandene Korrekturaufgabe aufgenommen, die auf den aktiven Regeln für Korrekturaufgaben basiert.

  Dadurch wird der Verlauf beibehalten, während gleichzeitig eine weitere Korrektur ermöglicht wird.

- Wenn eine Korrekturaufgabe erstellt (automatisch oder manuell) oder geteilt wird, wird sie aufgeteilt **Status** , **Grund** , Und **Bis** Felder werden ausgewertet. Im Falle der Aufteilungsaktion werden diese Felder sowohl für die alten als auch für die neuen Korrekturaufgaben ausgewertet. Wenn eine VIT aktualisiert wird, wird die aktualisiert **Status** , **Grund** , Und **Bis** Felder aller zugehörigen Korrekturaufgaben werden ausgewertet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn alle Vits in einer Korrekturaufgabe zurückgestellt werden und denselben Grund haben, ändert sich der Status der Korrekturaufgabe in **Zurückgestellt** Und der Grund der Vits wird der Korrekturaufgabe zugewiesen. Wenn sich die Vits im Grund unterscheiden, ändert sich der Grund der Korrekturaufgabe in **Keine** .
- Am nächsten **Bis** Datum aller Vits wird in aktualisiert **Bis** Feld der Korrekturaufgabe.
- Wenn Sie eine VIT erneut öffnen, ändert sich der Status der Korrekturaufgabe in **Öffnen** .

Diese Auswertung wird von durchgeführt *`Rollup vulnerability item values to vulnerability and group`*Geplante Aufgabe, die alle 15 Minuten ausgeführt wird.

Erkennungen, Korrekturaufgaben und status angreifbarer Elemente

Drittpartei-Integrationen rufen die Erkennungsdaten für angreifbare Elemente ab. Erkennungen sind eindeutige Vorkommen von Schwachstellen, wie von den Scannern gemeldet.

Erkennungsdaten werden mit angreifbaren Elementen (VIS, Vits) gekoppelt, und der VI-Status wird basierend auf dem Status der Erkennungen aktualisiert. Wenn kein VI gefunden wird, wird ein neues erstellt. Erkennungen werden nur von den Daten geöffnet oder geschlossen, die direkt von einem Scanner gefunden werden.

Wenn alle Erkennungen für ein angreifbares Element geschlossen sind, wird dieses angreifbare Element geschlossen. Im VI-Datensatz ist der Status Geschlossen/behoben. Wenn alle VIS für eine Korrekturaufgabe geschlossen sind, wird die Korrekturaufgabe geschlossen. Andernfalls bleibt der Status-Flow gleich.

Geschlossene VIS mit dem Substatus „behoben“ oder „veraltet“ werden erneut geöffnet, wenn eine neue Erkennung erstellt wird und die VIS mit der neuen Schwachstelle abgeglichen werden können.

Ab Version 20,0 von Vulnerability Response, Wenn eine Erkennung veraltet ist und sich das zugehörige VI im Status Geschlossen befindet, wechselt der Status des VI nicht in Geschlossen – Veraltet. Dadurch soll verhindert werden, dass das VI erneut geöffnet wird, wenn eine neue Erkennung identifiziert wird, sodass Sie vermeiden können, dass der gesamte falsch positive Anforderungs- und Genehmigungsprozess durchlaufen wird. Um dieses Verhalten umzukehren, deaktivieren Sie **Veraltete Erkennungen für geschlossene VIS ignorieren** Kontrollkästchen im Formular „Konfiguration automatisch schließen“. Weitere Informationen finden Sie unter Veraltete Erkennungen in automatisch schließen Vulnerability Response.

Gemäß der Skripteinbindung *`DetectionBase`*, Methode *`_shouldReOpenVI()`*, Wenn das VI zuvor mit dem Substatus „behoben“, „Veraltet“ oder „CI außer Betrieb genommen“ geschlossen wurde, wird es erneut geöffnet, und die Erkennung wird der vorhandenen VIT zugeordnet.

Nehmen wir beispielsweise an, dass das Abschlussdatum eines VIS nach dem Datum der letzten Entdeckung einer Erkennung liegt. Sie sollten davon ausgehen, dass diese VI-Datensätze geschlossen bleiben. Wenn Sie jedoch sehen, dass ein zuvor geschlossenes VI erneut geöffnet wurde, bedeutet dies, dass das VI durch eine frühere Erkennung geschlossen wurde und die Schwachstelle bei einem späteren Scan erneut gefunden wurde. Wenn eine neue Erkennung gefunden wird, die der geschlossenen VIT entspricht, die dieselbe Schwachstelle im Konfigurationselement des VI aufweist, wird das VI erneut geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturaufgaben und status angreifbarer Elemente

Korrekturaufgaben und status angreifbarer Elemente können sich gegenseitig beeinflussen. Meistens aktualisiert ein Korrekturaufgabenstatus den Status des angreifbaren Elements, wobei der Aufgabenstatus mit der höchsten Priorität zum Aktualisieren der angreifbaren Elemente in der Gruppe verwendet wird.

Die Statuspriorität lautet wie folgt.

Geschlossen > **Zurückgestellt** > **Gelöst** > **Wird überprüft** > **Warten auf Implementierung** > **Wird untersucht** > **Öffnen**

- Wenn sich eine Gruppe von angreifbaren Elementen in einer Korrekturaufgabe befindet und nicht auf einer einzelnen Ebene geändert wird, haben sie denselben Status wie ihre Korrekturaufgabe.
- Wenn die Korrekturaufgabe vom Status Offen in Warten auf Implementierung wechselt, werden alle VIS in der Korrekturaufgabe in den Status Warten auf Implementierung verschoben.
- Wenn die Korrekturaufgabe zurückgestellt wird, wird auch das VI zurückgestellt.
  Ab Version 16.5 können Sie nachverfolgen, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Container-Element oder eine Korrekturaufgabe zurückgestellt wird. Die geplante Aufgabe, `set deferral counts`, Wird täglich ausgeführt, um die Anzahl der Datensätze, die mehr als einmal zurückgestellt werden, in der Spalte „Anzahl der Zurückstellungen“ in den Modulen „mehrere Zurückstellungen“ für VR, AVR und CVR zu buchen. Alle Anzahlen für VIS, die einer Korrekturaufgabe zugeordnet sind, werden erfasst und veröffentlicht, wenn eine Korrekturaufgabe mehr als einmal zurückgestellt wird.

Angreifbare Elemente, die nur von Korrekturaufgaben aktualisiert wurden

Elemente entsprechen dem Status der Korrekturaufgabe, sofern sie nicht einzeln aktualisiert wurden, mit den folgenden Ausnahmen:

- Wenn sich der Status der Korrekturaufgabe in „Geschlossen“ ändert und ihre Lösung in „Abgebrochen“ oder „behoben mit Ausnahme“ geändert wird, ist das Element nicht betroffen und erhält den Status einer anderen Korrekturaufgabe, die es enthält. Wenn sich das angreifbare Element in keiner anderen Korrekturaufgabe befindet, wird es in den Status Offen zurückgesetzt.
- Wenn der Status des angreifbaren Elements „Geschlossen/behoben“ ist (aktualisiert durch einen Scan oder Import), bleibt das angreifbare Element im Status „Geschlossen/behoben“, wenn sich der Status der Korrekturaufgabe ändert. Diese Bedingung ist unabhängig davon, in welchem Status sich die Korrekturaufgabe befindet, „wahr“.

Angreifbare Elemente in status, die einzeln festgelegt sind

Angreifbare Elemente, die sich in einem für das Element aktualisierten Status befinden, z. B. die einzeln geschlossenen oder zurückgestellten Elemente, stimmen nicht automatisch mit dem Status der Korrekturaufgabe überein. Stattdessen vergleicht sie ihren Status mit allen zugehörigen Gruppen, um den Status mit der höchsten anzuwendenden Priorität zu finden.

Hinweis:
Der Status „Geschlossen/behoben“ ist ein Sonderfall. Wenn für die angreifbaren Elemente, die auf den Status Geschlossen/behoben gesetzt sind, alle angreifbaren Elemente innerhalb einer Korrekturaufgabe auf Geschlossen/behoben festgelegt sind, z. B. wenn ein Scanner feststellt, dass alle Schwachstellen behoben wurden, wird die Korrekturaufgabe automatisch als Geschlossen/behoben markiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturaufgaben enthalten leere Zuweisungsfelder

Wenn sich der Status der VIS in einer Korrekturaufgabe von gelöst in Offen ändert, wird der Status der Korrekturaufgabe auch von gelöst in wird untersucht aktualisiert.

Wenn jedoch beide verwendet werden **Zugewiesen an** Und **Zuweisungsgruppe** Felder in der Korrekturaufgabe sind leer, die Korrekturaufgabe verbleibt im Status „gelöst“ und wird nicht in „wird untersucht“ verschoben.

Zuweisungsgruppe für angreifbare Elemente wird nicht immer aktualisiert, wenn ihre Korrekturaufgabe aktualisiert wird

Wenn die Zuweisungsgruppe für ein VI im Status „Offen“ manuell aktualisiert wird, wird sie nicht erneut aktualisiert, wenn die Zuweisungsgruppe für ihre Korrekturaufgabe aktualisiert wird. Diese Informationen werden nicht überschrieben, da die Zuweisungsgruppe für das VI absichtlich aktualisiert wurde und Teil einer anderen Korrekturaufgabe sein kann.

Status-Rollup- und Rollup-Szenarien

Status-Rollup- und Rollup-Szenarien synchronisieren automatisch den Status von Korrekturaufgaben (RTS) und angreifbaren Elementen (Vits), wodurch Echtzeitaktualisierungen für beide sichergestellt werden. Diese dynamische Interaktion reduziert die manuelle Nachverfolgung, verbessert die Genauigkeit und bietet Anwendern eine aktuelle Ansicht des Fortschritts, wodurch das Schwachstellenmanagement effizienter wird und Anwender schnell fundierte Entscheidungen treffen können.

Rollup-Verhalten

Wenn sich der status von angreifbaren Elementen (VIT) ändern, können diese Änderungen bis zur Ebene der Korrekturaufgabe (RT) weitergegeben werden. Die folgende Tabelle fasst wichtige Rollup-Szenarien zusammen, in denen Änderungen des Status angreifbarer Elemente (VIT) den Status der zugehörigen Korrekturaufgabe (RT) beeinflussen können, basierend auf Abschlussbedingungen, Neuzuweisungen und Zurückstellungen.

Rollup-Szenarien

VIT-Status	RT-Status
Öffnen Sie > Wird Untersucht	Bleibt Offen
Offen > Geschlossen – Falsch Positiv	Bleibt Offen
Öffnen Sie > In Überprüfung	Bleibt Offen
Öffnen > zurückgestellt (beliebiger Substatus)	Öffnen Sie > Zurückgestellt
Öffnen > Gelöst	Bleibt Offen
Öffnen > Geschlossen – Abgebrochen	Bleibt Offen
Öffnen > Geschlossen – Behoben	Öffnen > Geschlossen – Behoben
Öffnen > Geschlossen – behoben mit Ausnahmen	Öffnen > Geschlossen
Geschlossen-Behoben > Offen	Bleibt Geschlossen – Behoben
Öffnen > Geschlossen-behoben; (nach dem nächsten Scan) > gelöst	Bleibt Offen
Öffnen > Geschlossen – Ungültig	Bleibt Offen
Öffnen > Geschlossen-Veraltet	Öffnen > Geschlossen – Abgebrochen
Geschlossen – Veraltet > Offen	Bleibt Geschlossen – Abgebrochen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollup-Szenarien (Fortsetzung)

VIT-Status	RT-Status
Öffnen > Geschlossen – Ergebnis Ungültig	Bleibt Offen
Öffnen > Geschlossen – Ungültig	Bleibt Offen
Öffnen > Closed-CI außer Betrieb genommen	Öffnen > Geschlossen – Abgebrochen
Öffnen Sie > Warten Auf Implementierung – Patch Geplant	Bleibt Offen
Öffnen > Warten Auf Implementierung – Patch Nicht Geplant	Bleibt Offen
Öffnen > Warten auf Implementierung – Patch geplant (fehlendes Zieldatum)	Bleibt Offen
Wird untersucht > Closed-CI außer Betrieb genommen	RT1: Wird untersucht > Geschlossen – Abgebrochen RT2: Wird untersucht > Geschlossen – Abgebrochen
Offen > gelöst; RT = gelöst; öffnet VIT erneut	Wenn zugewiesen, RT: Gelöst > wird untersucht; Sonst: Offen
VIT1: Geschlossen – behoben VIT2: Wird untersucht Wenn VIT2 erneut geöffnet wird und VIT1 gelöst bleibt.	RT1: Wird untersucht RT2: Geschlossen – behoben
VIT1: Geschlossen – veraltet VIT2: Closed-CI außer Betrieb genommen	Öffnen > Geschlossen – Abgebrochen
VIT1: Gelöst VIT2: Closed-CI außer Betrieb genommen	Bleibt Offen
VIT1: Geschlossen – behoben VIT2: Closed-CI außer Betrieb genommen	Öffnen > Geschlossen – Abgebrochen
VIT1: Geschlossen – behoben VIT2: Geschlossen – veraltet	Öffnen > Geschlossen – Behoben
VIT1: Closed-<any sub-state>	Öffnen Sie > Zurückgestellt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollup-Szenarien (Fortsetzung)

VIT-Status	RT-Status
VIT2: Zurückgestellt	Bis-Datum – vorwärts als VIT2 übertragen

Roll-down-Verhalten

Wenn sich der Status einer Korrekturaufgabe ändert, wird der Status häufig an die zugehörigen Vits weitergegeben, es sei denn, dies wird durch manuelle Updates oder bestimmte Ausnahmen überschrieben. Die folgende Tabelle fasst wichtige Rolldown-Szenarien zusammen, in denen Änderungen des Status der Korrekturaufgabe (RT) den Status des zugehörigen angreifbaren Elements (VIT) beeinflussen können, basierend auf Vorrangregeln und speziellen Bedingungen.

Rollup-Szenarien

RT-Status	VIT-Status
Öffnen Sie > Wird Untersucht	Öffnen Sie > Wird Untersucht
Offen > Geschlossen – Falsch Positiv	Offen > Geschlossen – Falsch Positiv
Öffnen Sie > In Überprüfung	Öffnen Sie > In Überprüfung
Öffnen > zurückgestellt (Substatus: Grund angegeben)	Öffnen > Zurückgestellt (Substatus: Grund Angegeben)
Öffnen > Gelöst	Öffnen > Gelöst
Öffnen > Geschlossen – Abgebrochen	Bleibt Offen
Öffnen > Geschlossen – behoben mit Ausnahmen	Bleibt Offen
RT1: Öffnen > wird untersucht RT2: Offen	Öffnen Sie > Wird Untersucht
RT1: Öffnen > wird untersucht > Warten auf Implementierung RT2: Wird untersucht	Öffnen Sie > Wird Untersucht > Wartet Auf Implementierung
RT1: Warten auf Implementierung > zurückgestellt RT2: Warten auf Implementierung	Warten Auf Implementierung > Zurückgestellt
RT1: Warten auf Implementierung > Geschlossen – Abgebrochen RT2: Wird untersucht	Warten Auf Implementierung> Wird Untersucht
Öffnen > Geschlossen – behoben mit Ausnahmen	VIT1: Offen > Geschlossen – behoben VIT2: Offen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollup-Szenarien (Fortsetzung)

RT-Status	VIT-Status
Abschließende Beobachtungen: VIT2 bleibt offen	
Öffnen > Gelöst Abschließende Beobachtungen: VIT2: Offen>gelöst	VIT1: Offen > Geschlossen – behoben VIT2: Offen
Öffnen > Gelöst Abschließende Beobachtungen: VIT2 wird erneut geöffnet; VIT1 bleibt gelöst; RT: Gelöst > Offen	VIT1: Offen > Geschlossen – behoben VIT2: Offen

Status der Korrekturaufgabe für angreifbare Elemente (Vits) in mehreren Gruppen

Wenn sich ein VIT in mehreren Korrekturaufgaben befindet (RT in den folgenden Tabellen) und sein eigener Status nicht festgelegt wurde, bestimmt der Status dieser VIT, wie in der folgenden Tabelle dargestellt.

Beispiele für angreifbare elementstatus

Status der Korrekturaufgabe	Status des angreifbaren Elements
RT 1: **Öffnen** > **Wird untersucht** RT 2: **Öffnen**	**Wird untersucht** Wenn RT 1 untersucht wird und RT 2 offen ist, ändert sich das VI in „wird untersucht“. Nach der Suche hat RT 1 und RT 2 den Status mit der höchsten Priorität.
RT 1: **Wird Untersucht** RT 2: **Öffnen** > **Wird untersucht**	**Wird untersucht** Wenn RT 2 untersucht wird und RT 1 untersucht wird, bleibt das VI als wird untersucht. Nach der Suche haben sie zwischen RT 1 und RT 2 den Status mit derselben Priorität.
RT 1: **Wird Untersucht** RT 2: **Wird untersucht** > **Warten auf Implementierung**	**Warten auf Implementierung** Wenn RT 2 auf Implementierung wartet und RT 1 untersucht wird, ändert sich das VI in „Warten auf Implementierung“. Nach der Suche hat RT 2 zwischen RT 1 und RT 2 den Status mit der höchsten Priorität.
RT 1: **Wird untersucht** > **Zurückgestellt** RT 2: **Warten auf Implementierung**	**Zurückgestellt** Wenn RT 1 zurückgestellt ist und RT 2 auf Implementierung wartet, ändert sich das VI in

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für angreifbare elementstatus (Fortsetzung)

Status der Korrekturaufgabe	Status des angreifbaren Elements
	zurückgestellt. Nach der Suche hat RT 1 und RT 2 den Status mit der höchsten Priorität.

Angreifbares Element in Sonderfällen mehrerer Gruppen

Status der Korrekturaufgabe	Status des angreifbaren Elements
RT 1: **Wird untersucht** RT 2: **Warten auf Implementierung** > **Geschlossen (behoben oder Abgebrochen)**	**Wird untersucht** Wenn RT 2 geschlossen/behoben oder geschlossen/abgebrochen ist und RT 1 untersucht wird, ändert sich das VI von „Warten auf Implementierung“ (zuvor höchste Priorität) zu „wird untersucht“ (derzeit höchste Priorität).
RT 1: Beliebiger Status RT 2: Beliebiger Status	Wenn der Quellstatus des angreifbaren Elements behoben ist (durch einen Scan oder Import aktualisiert), ändert sich der Status des angreifbaren Elements in Geschlossen/behoben, wenn die Gruppe ihren Status ändert. Diese Bedingung ist unabhängig davon, in welchen status sich die anderen zugeordneten Gruppen befinden. Die Suche nach angreifbaren Elementen nach dem Gruppenstatus findet nicht statt.

Wenn ein VI-Status einzeln festgelegt wird, wird sein Status bei der Bewertung der Priorität berücksichtigt, wie bei jeder anderen Korrekturaufgabe. Wenn ein VI zu mehr als einer Korrekturaufgabe gehört, werden in der folgenden Tabelle die vorgenommenen Aktualisierungen aufgeführt.

Status des angreifbaren Elements, der einzeln festgelegt wurde, Sonderfälle

Status des Schwachstellenelements innerhalb einer Gruppe	Endgültiger Status des angreifbaren Elements
RT 1-Status: **Wird untersucht** RT 2-Status: **Wird untersucht** > **Warten auf Implementierung** Ursprünglicher VI-Status: **Wird untersucht** > **(Im VI festgelegt)**	**Warten auf Implementierung** Wenn RT 2 zu „Warten auf Implementierung“ verschoben wurde und RT 1 weiterhin untersucht wurde, ändert sich das VI in „Warten auf Implementierung“ (höchste Priorität).
RT 1: **Wird untersucht** RT 2: **Wird untersucht** > **Warten auf Implementierung** Ursprünglicher VI-Status: **Zurückgestellt** > **(Im VI festgelegt)**	**Zurückgestellt** Wenn RT 2 zu „Warten auf Implementierung“ verschoben wurde und RT 1 weiterhin untersucht wurde, bleibt das VI im Status zurückgestellt (höchste Priorität).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Tabelle zeigt, dass der Status zurückgestellt wird, wenn zwei Korrekturaufgaben mit allgemeinen angreifbaren Elementen zurückgestellt werden, bis das späteste Datum erreicht ist.

Sonderfälle des zurückgestellten Status des angreifbaren Elements

Status des Schwachstellenelements innerhalb einer Gruppe	Endgültiger Status des angreifbaren Elements
RT 1-Status: **Wird überprüft (bis 10. April)** RT 2-Status: **Wird untersucht** > **Wird überprüft (bis April 30)** Ursprünglicher VI-Status: **Wird überprüft (bis 10. April)** > **(Im VI festgelegt)**	**Zurückgestellt (bis April 30)** Wenn RT 2 in zurückgestellt (bis April 30) verschoben wurde und RT 1 zurückgestellt bleibt (bis April 10), ändert sich das VI von zurückgestellt (bis April 05) in den Status zurückgestellt (bis April 30).
RT 1: **Wird überprüft (bis 15. Juli)** RT 2: **Wird untersucht** > **Wird überprüft (bis 10. Juli** Ursprünglicher VI-Status: **Zurückgestellt** > **(Bis 15. Juli)**	**Zurückgestellt (bis 15. Juli)** Wenn RT 2 in zurückgestellt verschoben wurde (bis Juli 10) und RT 1 zurückgestellt bleibt (Juli 15), bleibt das VI zurückgestellt (bis Juli 15).

Zusätzliche Einstellungen für Domänentrennung

Für eine genaue Ausführung und Ergebnisse sind die folgenden Vorsichtsmaßnahmen und Einstellungen für die Domänentrennung in erforderlich Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance.

Ändern Sie die Geschäftslogiken und -Prozesse in der globalen Domäne nicht, um Probleme zu vermeiden, sodass alle aktuellen Änderungen für jedes Upgrade aktualisiert werden. Duplizieren Sie alle Geschäftslogiken und -Prozesse in jeder Domäne separat, und stellen Sie sicher, dass sie in der globalen Domäne inaktiv sind. Andernfalls haben die Geschäftslogiken und -Prozesse in der globalen Domäne Vorrang vor der untergeordneten Domäne. Angenommen, Sie haben eine Risikoregel in einer untergeordneten Domäne erstellt und die globale Domäne hat auch eine ähnliche Risikoregel, dann hat die Regel der globalen Domäne Vorrang vor der Regel der untergeordneten Domäne.

Neubewertung von Rechnern und Regeln

Wenn Sie vor v20.0 Rechner oder Regeln erneut anwenden, wird die verwendet Erneut ausführen Die Kennzeichnung ist auf „wahr“ festgelegt, und eine Business-Regel wird ausgelöst, um eine geplante Aufgabe auszuführen, die die Rechner und Regeln erneut anwendet. Ab v20.0 müssen Sie nicht von abhängig sein Erneut ausführen Kennzeichnung. Wenn Sie auf klicken **Rechner Erneut Anwenden** Schaltfläche, wird ein Hintergrundauftrag ausgelöst, der die Rechner und Regeln erneut anwendet. Auf diese Weise können Sie Rechner und Regeln für alle Domänen erstellen.

Einstellungen für Rollup-Rechner

In einer Domäne darf nur ein Rollup-Rechner für eine Tabelle aktiv sein. Betrachten Sie beispielsweise die Tabelle „Korrekturaufgabe“, *sn_vul_vulnerability*Mit dem Rollup-Rechner **Korrekturaufgaben-Rollup** In der globalen Domäne. Wenn Sie diesen Rollup-Rechner duplizieren, indem Sie die Gewichtungen für dieselbe Tabelle in derselben Domäne ändern, gibt es Diskrepanzen in den Rollup-Berechnungen. Stellen Sie daher sicher, dass

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nur ein Rollup-Rechner aktiviert ist, wenn mindestens zwei Rollup-Rechner für eine Tabelle in derselben Domäne vorhanden sind.

Formularfelder „erkannte Elemente“

Assets werden automatisch mit Konfigurationselementen (CIs) in abgeglichen Configuration Management Database (CMDB) Wenn sie mithilfe der CI-Suchregeln importiert werden. Datensätze für nicht abgeglichene CIs werden während der Integrationsimporte von Drittanbietern automatisch erstellt und in erkannte Elemente eingeschlossen. Jedoch für Cloud-Assets, die in nicht vorhanden sind CMDB CL, der Datensatz wird in der Cloud-Ressourcenklasse erstellt.

Erkannte Elementfelder

Die Informationen in diesen Datensätzen werden aus den Datensätzen der Drittpartei erfasst und während des Imports klassifiziert.

Diese Felder befinden sich in Datensätzen, die in der Tabelle „erkannte Elemente“ [sn_sec_cmn_src_ci] aufgeführt sind.

Um importierte Daten in den in den folgenden Tabellen aufgeführten Feldern anzuzeigen, müssen Sie mindestens über die Rolle sn_vul.read_all verfügen.

Feld	Beschreibung
Anzahl	Bezeichner, der dem Datensatz zugewiesen ist.
Konfigurationselement	Konfigurationselement, das aus der Integration der Drittpartei-Quelle importiert wird. Ab v12.0 ist das Konfigurationselement das neueste CI aus der Liste der CIs, nachdem die außer Betrieb genommenen gefiltert wurden.
Klasse	Klasse, die dem CI während des Imports von zugewiesen ist Vulnerability Response.
Quelle	Quelle, die aus der Integration der Drittpartei-Quelle importiert wird.
CI-Übereinstimmungsregel	Die CI-Übereinstimmungsregel, die zum Erstellen des Elements verwendet wurde.
V18.0: Übereinstimmender Typ für den DI	Übereinstimmender Typ, der zum Erstellen des erkannten Elements verwendet wird. Die Optionen sind: • Erstellt von VR • Erstellt von IRE • Mit CI-Suche abgeglichen • Abgeglichen mit IRE • Manuell abgeglichen (beginnend mit v24.0.6 von Vulnerability Response, Sie können diese zusätzliche Option anzeigen. Diese Option wird automatisch festgelegt, wenn Sie ein CI im Formular „erkanntes Element“ manuell aktualisieren.) Diese Informationen sind nur für Daten verfügbar, die für ausgefüllt werden Vulnerability Response V18.0 und höher. Für vorhandene Daten enthält diese Spalte keinen Wert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn Sie die CI-Suchregeln erneut anwenden, werden möglicherweise einige CIs in DIS aktualisiert, was dazu führt, dass diese Spalte ausgefüllt wird.
Andere übereinstimmende CIs	Liste der anderen Konfigurationselemente, die der CI-Suchregel entsprechen.
Status	Status des CI, der während des Imports bestimmt wird. Die Auswahlmöglichkeiten lauten wie folgt: • **Übereinstimmend** : Ein übereinstimmendes Konfigurationselement wurde in der CMDB gefunden. • **Nicht Abgeglichen** : Es wurde keine Übereinstimmung in der CMDB gefunden. Ein Platzhalterdatensatz wird erstellt.
Erstellt	Datum, an dem der Datensatz des erkannten Elements erstellt wurde.
Aktualisiert	Datum, an dem der Datensatz des erkannten Elements aktualisiert wurde.
Aktualisiert von	Anwender, der die Daten aktualisiert hat.
Host-Tag	Host-Tags, die diesem erkannten Element während des Imports zugewiesen sind. Sie können bis zu 31 Host-Tags pro erkanntem Element haben.
Vollqualifizierter Domänenname	Daten, die diesem CI zugeordnet sind, wurden in der CMDB gefunden.
MAC-Adresse	Daten, die diesem CI zugeordnet sind, wurden in der CMDB gefunden.
Betriebssystem	Betriebssystem, das diesem CI zugeordnet ist.
NetBIOS	NetBIOS, das aus der Integration der Drittpartei-Quelle importiert wurde.
IP-Adresse	Daten, die diesem CI zugeordnet sind, wurden in der CMDB gefunden.
Quelldaten	Neueste Daten, die diesem CI aus der Quelle zugeordnet sind.
V16: Anfängliche Quelldaten	Anfängliche Daten, die diesem CI aus der Quelle zugeordnet sind.
V16: CI neu bewerten	Empfängt Daten vom Scanner. Wenn aktualisierte Daten vorhanden sind, wird der Wert auf „wahr“ festgelegt. **Hinweis:** Die Quelldatenwerte werden gemäß den neuesten Quelldaten neu berechnet. Wenn aktualisierte Daten vom Scanner abgerufen werden, werden die Quelldaten aktualisiert. Der vorhandene Quelldatenwert wird in das ursprüngliche Quelldatenfeld verschoben. Um die erkannten Elemente neu zu bewerten, aktivieren Sie Wenden Sie CI-Suchregeln erneut auf die geänderten erkannten Elemente an Geplante Aufgabe.
Agent ist vorhanden	Gibt An Wahr Wenn der Service Desk-Mitarbeiter auf dem Asset installiert ist. Wenn HostUID Und UUID Werte in der Spalte „Quelldaten“ sind leer. Dieser Wert wird als ausgefüllt Wahr . **Hinweis:** Dieses Feld wird ab v19.0 von angezeigt Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab v23.0 von Vulnerability Response, **Compliance von Testergebnissen in % (CI)** Die Spalte zeigt den Prozentsatz der Testergebnisse an, die für das entsprechende CI konform sind. Um diesen Wert zu erhalten, müssen Sie festlegen `CalcTRComplianceForCI` Bis `Wahr` In **Aktualisieren Sie Korrekturmetriken** Geplante Aufgabe.

Hinweis:
Die **Compliance von Testergebnissen in % (CI)** Wert wird nur für die erkannten Elemente ausgefüllt, die einen nicht leeren Wert in aufweisen **Datum des letzten Konfigurations-Compliance-Scans** Oder **Nicht-Infra-Datum des letzten Compliance-Scans** Spalten.

Ab Version 18,0 von Vulnerability Response, Qualys, Tenable for Vulnerability Response Und Rapid7 Scanner können die folgenden zusätzlichen Metadaten für Cloud-Assets erhalten.

Feld	Beschreibung
Cloud-Service-Provider	Name des Cloud-Service Providers, der Cloud Computing-Services anbietet. Beispiel: Amazon Web Services(AWS), Microsoft Azure Und Google Cloud Platform (GCP).
Cloud-Region	Standort, an dem die Ressource gehostet wurde.
Cloud-Account	Account, der von Cloud-Service Providern bereitgestellt wird, z. B. AWS, GCP, Usw., um auf Cloud-Computing-Services zuzugreifen.
Cloud-Ressourcentyp	Typen von Assets, die in der Cloud vorhanden sind, z. B. Amazon Elastic Compute Cloud (EC2)-Computer, AWS S3-Buckets usw.
Ressourcen-ID	Eindeutiger Bezeichner, der einer Ressource in einer Cloud-Computing-Umgebung zugewiesen ist. Diese ID wird verwendet, um die Ressource zu identifizieren und zu verwalten.
Ressourcenname	Anwenderdefinierter Name, der zum Identifizieren und Verwalten einer Ressource in einer Cloud-Computing-Umgebung verwendet wird.
Bild	Ein VM-Image oder ein Server-Image ist eine vorkonfigurierte virtuelle Maschine, die ein Betriebssystem, Anwendungen und andere Software enthält. Beispiel: Amazon-Computerbild.

Die neue CI-Suchregel „Cloud-Ressourcen-ID“ wurde eingeführt, um die Cloud-CIs basierend auf den Cloud-Metadaten abzugleichen.

Vulnerability Response Formularfelder für Schwachstellen

Schwachstellen werden automatisch erstellt, wenn Datensätze aus der National Vulnerability Database (NVD), der Common Weakness Enumeration (CWE) oder Integrationen von Drittparteien heruntergeladen und unter gespeichert werden **Bibliotheken** In Vulnerability Response.

NVD-Eingabefelder

Um importierte Daten in den in den folgenden Tabellen aufgeführten Feldern anzuzeigen, müssen Sie mindestens über die Rolle sn_vul.read_all verfügen.

Diese Felder befinden sich in Datensätzen, die in der Tabelle „National Vulnerability Database-Einträge“ [sn_vul_nvd_entry] aufgeführt sind.

Feld	Beschreibung
ID	Bezeichner für diesen Schwachstelleneintrag.
Risikobewertung	(Ausgeblendet, wenn der Schwachstelle keine Vits zugeordnet sind)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Quantifiziert **Risikopunktzahl** Trennung angreifbarer Elemente in „Kritisch“, „hoch“, „Mittel“, „Niedrig“ und „keine“. Weitere Informationen zu Risikobewertungen finden Sie unter Vulnerability Response Rechner und Regeln für Schwachstellenrechner. **Hinweis:** Diese Basis **Risikobewertung** Ist nicht mit dem Lösungsdatensatz identisch **Risikobewertung.**
Risikopunktzahl	(Ausgeblendet, wenn der Schwachstelle keine Vits zugeordnet sind) Berechnetes Risiko, das das angreifbare Element für Ihre Umgebung darstellt. **Hinweis:** Diese Basis **Risikopunktzahl** Ist nicht mit dem Lösungsdatensatz identisch **Risikopunktzahl.** Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln für Schwachstellenrechner.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle. Schweregradzuordnungen werden für NVD und mit bereitgestellt ServiceNow Drittpartei-Integrationen. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Erstellen Sie einen Vulnerability Response Schweregradzuordnung.
Exploit vorhanden	Ja, wenn dieser Schwachstelle mindestens ein Exploit zugeordnet ist.
Exploit-Kompetenzniveau	Niedrigstes Kompetenzniveau, das zum Ausnutzen dieser Schwachstelle erforderlich ist.
Exploit-Angriffsvektor	Der Angriffsvektor der Schwachstellen der Exploits für diese Schwachstelle. Verfügbar, wenn SAM NVD aktiviert ist.
Aktive AEs	(Ausgeblendet, wenn der Schwachstelle keine Vits zugeordnet sind) Anzahl der angreifbaren Elemente, die dieser Schwachstelle zugeordnet sind und sich nicht im Status „Geschlossen“ befinden. Wenn keine aktiven VIS für diese Schwachstelle vorhanden sind, **Risikobewertung** Und **Risikopunktzahl** Werden nicht angezeigt.
CWE-Eintrag	Verweis auf das Element „Allgemeine Schwachstellenaufzählung“, in das diese Schwachstelle am besten passt.
Veröffentlichungsdatum	Datum, an dem die Schwachstelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt geändert wurde.
Zusammenfassung	Beschreibung der Schwachstelle.
bedrohungsinformationen (beginnend mit Vulnerability Response Version 20.0)	Threat Intelligence bereitgestellt von Qualys. Mit diesen Daten können Sie die Motive, Ziele und Angriffsverhalten eines Bedrohungsakteurs verstehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schwachstellendetails	
CVSS v2	CVSS v2-Daten importiert
CVSS v3	Importierte CVSS v3-Daten, nicht verfügbar vor 2015.
Bevorzugte Lösung	(Ausgeblendet, wenn der Schwachstelle keine Vits zugeordnet sind) Lösung der höchsten Ersatzlösung in der Kette, abgeleitet von den in der Schwachstelle referenzierten Lösungen. Wenn in der Kette mehr als ein höchster Ersatz vorhanden ist, wird kein Wert festgelegt. Jeder manuell festgelegte Wert kann bei nachfolgenden Importen überschrieben werden. Das manuelle Festlegen dieses Werts sollte für das angreifbare Element erfolgen.
CISA-Exploit (Diese Registerkarte ist nur verfügbar, wenn die CISA-Anwendung installiert ist.)	
CISA-Fälligkeitsdatum	Frist zur Behebung der Schwachstelle.
Hinzugefügt am	Datum, an dem die Schwachstelle dem CISA-Katalog hinzugefügt wurde.
Produkt	Produkt, für das die Schwachstelle identifiziert wurde.
Lieferant/Projekt	Lieferant, der der identifizierten Schwachstelle zugeordnet ist.
Bekannte Ransomware Ab v21.0 von Vulnerability Response.	Ausgewählt, wenn das Feld **Bekannt für die Verwendung in Ransomware-Kampagnen** Wird aus dem CISA-Katalog „bekannte ausgenutzte Schwachstellen“ (KEVs) erfasst. Die Kennzeichnung wird auf der Ebene Common Vulnerabilities and Exposures (CVE) festgelegt und wird zum Drittparteieintrag (TPE) zusammengefasst.
Nachbesserungsstatus (Ausgeblendet, wenn der Schwachstelle keine VIS zugeordnet sind)	
Zurückgestellte sind ausgeschlossen	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
VIs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
%VIS korrigiert	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Beinhaltet Zurückgestellte	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle.
VIs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle.
%VIS korrigiert	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle.
Zugehörige Links	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zustand aktualisieren	Zeigt Datum und Uhrzeit der letzten Aktualisierung an. Aktualisiert Folgendes: • Status der Korrekturaufgabe • Risikopunktzahl und -Bewertung • Metriken wie aktive Vits, Gesamtvits aus dem Abschnitt „Korrekturstatus“
Zugehörige Listen	
Angreifbare Elemente	(Ausgeblendet, wenn der Schwachstelle keine Vits zugeordnet sind) Angreifbare Elemente, die dieser Schwachstelle zugeordnet sind.
Verwundbarkeitsreferenzen	Informationen über die Schwachstelle aus externen Quellen, zitiert von NVD.
Exploits	Exploits, die dieser Schwachstelle zugeordnet sind.
Lösungen	(Ausgeblendet, wenn der Schwachstelle keine Vits zugeordnet sind) Alle Vulnerability Solution Management Integrationslösungen, die dieser Schwachstelle zugeordnet sind.
Schwachstellen	Importiert **Schwäche** Daten, die einem Common Vulnerabilities and Exposures (CVE) zugeordnet sind.
Software mit Schwachstellen	(Ausgeblendet, wenn Software dem CVE zugeordnet ist) Importierte CPE-Daten (Common Platform Enumeration), die der Schwachstelle zugeordnet sind.
Schwachstellen-Malware-Kits	Malware, die aus verschiedenen Scannerquellen importiert wurde, für eine Schwachstelle.

CWE-Schwachstelleneintragsfelder

Diese Felder befinden sich in Datensätzen, die in der Tabelle „CWEs“ [sn_vul_cwe] aufgeführt sind.

Feld	Beschreibung
CWE-ID	Bezeichner für diesen Schwachstelleneintrag. Dieser Bezeichner wird sowohl für Kategorien als auch für Schwachstellen verwendet und ist zwischen den beiden Datensätzen eindeutig.
Name	Beschreibender Name, der dieser CWE-ID zugewiesen ist.
Wahrscheinlichkeit der Ausnutzung	Wie wahrscheinlich es ist, dass die Schwäche auf qualitativer Skala ausgenutzt wird. Einer der folgenden: • Unbekannt • Niedrig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Mittel • Hoch
Position in OWASP Top 10	Die numerische Position dieser Schwachstelle in der OWASP Top 10-Liste.
SANS bis Position 25	Die numerische Position dieser Schwachstelle in der SAN Top 25-Liste.
Klasse	Typ der Schwäche
Status	Einer der folgenden: • Unvollständig • Entwurf • Stabil • Überholt • Veraltet • Unstabil
Zusammenfassung	Einer der folgenden: • Variante • Klasse • Basis • Verbindung
Aktualisiert	Zeitpunkt der letzten Aktualisierung des Datensatzes in der Instanz.
Funktionsbereiche	Liste der betroffenen Funktionsbereiche. Beispiel: **Dateiverarbeitung** . Wird nur für 24/862 Schwachstellen ausgefüllt.
Betroffene Ressourcen	Liste der betroffenen Ressourcen. Beispiel: **Datei** Oder **Verzeichnis** . Wird nur für 51/863 Schwachstellen ausgefüllt.
URL	Knowledge Base-artikel, der dieser Schwachstelle zugeordnet ist.
Beschreibung	Beschreibung der Schwachstelle.
Integrationsausführung	Die Integrationsausführung, in die diese CWE importiert wurde.
Abschnitte	
Zusätzliche Details	Softwarekonzeptbeschreibungen, die die Schwachstelle weiter erklären. Beinhaltet: • Erweiterte Beschreibung • Hintergrunddetails • Notizen
Erkennungsmethoden	Details dazu, wie Sie diese Schwachstelle in einer Anwendung erkennen können.
Einführungsmodi	Die Phasen, in denen die Schwachstelle eingeführt wird, z. B. **Implementierung** , **Architektur und Design** , Und so weiter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Demo-Beispiele	Codebeispiele der Schwachstelle mit zugehörigen Beschreibungen.
Potenzielle Minderungen	Details dazu, wie die Schwachstelle verhindert werden kann, einschließlich der Phase des Anwendungslebenszyklus, in der sie auftritt, und der Effektivität der Minderung.
Zugehörige Listen	
Beziehungen	CWEs, die dieser Schwachstelle zugeordnet sind. Listet Beziehungen zwischen dieser CWE und anderen auf. Kann übergeordnetes/untergeordnetes Element, folgt/voran, required by/requires (für zusammengesetzte Schwachstellen), CanAlsoBe, PeerOf, Member von enthalten.
Beispiele für Beobachtung	Einige CVEs, die für diese Schwachstelle repräsentativ sind.
Häufige Konsequenzen	Konsequenzen eines erfolgreichen Exploits in Bezug auf Umfang und Auswirkung. Zum Beispiel: Umfang: Vertraulichkeit Impact: Anwendungsdaten Lesen
Mitgliedschaften	CWE-Mitgliedschaften mit dieser Schwachstelle.
Anwendbare Plattformen	Plattformen, die dieser Schwachstelle zugeordnet sind.
Anwendungsschwachstelleneinträge	Anderen Anwendungsschwachstelleneinträge, die einem zugeordnet sind.
Externe Referenzen	Informationen zur Schwachstelle aus externen Quellen.

Eingabefelder für Schwachstellen von Drittparteien

Diese Felder befinden sich in Datensätzen, die in der Tabelle „Drittanbieter-Schwachstelleneinträge“ [sn_vul_third_Party_entry] aufgeführt sind.

Feld	Beschreibung
ID	Bezeichner für diesen Schwachstelleneintrag.
Version 16.0: CVEs	Mehrere Common Vulnerability and Exposures (CVEs), die dieser Schwachstelle von Drittanbietern zugeordnet sind.
Quelle	Ursprung der Schwachstelle – ob Scanner oder physischer Test.
Risikobewertung	Quantifiziert **Risikopunktzahl** Trennung angreifbarer Elemente in „Kritisch“, „hoch“, „Mittel“, „Niedrig“ und „keine“. Weitere Informationen zu Risikobewertungen finden Sie unter . Vulnerability Response Rechner und Regeln für Schwachstellenrechner. **Hinweis:** Diese Basis **Risikobewertung** Ist nicht mit dem Lösungsdatensatz identisch **Risikobewertung**
Risikopunktzahl	Berechnetes Risiko, das das angreifbare Element für Ihre Umgebung darstellt, basierend auf der Risikopunktzahl.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Diese Basis **Risikopunktzahl** Ist nicht mit dem Lösungsdatensatz identisch **Risikopunktzahl.** Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln für Schwachstellenrechner.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle. Schweregradzuordnungen werden für NVD und mit bereitgestellt ServiceNow Drittpartei-Integrationen. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Erstellen Sie einen Vulnerability Response Schweregradzuordnung.
Exploit vorhanden	Ja, wenn dieser Schwachstelle mindestens ein Exploit zugeordnet ist.
Exploit-Kompetenzniveau	Niedrigstes Kompetenzniveau, das zum Ausnutzen dieser Schwachstelle erforderlich ist.
Exploit-Angriffsvektor	Der Angriffsvektor der Schwachstellen der Exploits für diese Schwachstelle.
Aktive AEs	Anzahl der angreifbaren Elemente, die dieser Schwachstelle zugeordnet sind und sich nicht im Status „Geschlossen“ befinden.
Kategorie	Von der Drittpartei-Integration bereitgestellte Klassifizierung. Hilft bei der Zuweisung.
Fehlerkorrekturtyp	Typen von Korrekturaktionen. • Patch • Konfigurationsänderung • Patch und Konfigurationsänderung • Gegenmaßnahme
CWE-Eintrag	Verweis auf das Element „Allgemeine Schwachstellenaufzählung“, in das diese Schwachstelle am besten passt.
PCI	Wenn das Kontrollkästchen aktiviert ist, wird die Schwachstelle als erhebliches Risiko für das Risiko von Zahlungsinformationen gekennzeichnet.
PCI-Schweregrad	Risikostufe für das Risiko von Zahlungsinformationen. [Nur Qualys.]
Veröffentlichungsdatum	Datum, an dem die Schwachstelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt geändert wurde.
Zusammenfassung	Beschreibung der Schwachstelle.
Schwachstellendetails	
CVSS v2	CVSS v2-Daten importiert
CVSS v3	Importierte CVSS v3-Daten, nicht verfügbar vor 2015.
Bedrohung	Beschreibung der Bedrohung durch diese Schwachstelle.
Bevorzugte Lösung	Lösung der höchsten Ersatzlösung in der Kette, abgeleitet von den in der Schwachstelle referenzierten Lösungen. Wenn in der Kette mehr als ein höchster Ersatz vorhanden ist, wird kein Wert festgelegt. Jeder manuell festgelegte Wert kann bei nachfolgenden Importen überschrieben werden. Das manuelle Festlegen dieses Werts sollte für das angreifbare Element erfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Korrekturhinweise	Beschreibung der vom Lieferanten abgerufenen Korrekturlösung.
Nachbesserungsstatus	
Zurückgestellte sind ausgeschlossen	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
VIs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
%VIS korrigiert	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Beinhaltet Zurückgestellte	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle.
VIs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle.
%VIS korrigiert	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle.
Zugehörige Links	
Zustand aktualisieren	Zeigt Datum und Uhrzeit der letzten Aktualisierung an. Aktualisiert Folgendes: • Status der Korrekturaufgabe • Risikopunktzahl und -Bewertung • Metriken wie aktive VIS, Gesamtanzahl VIS aus dem Abschnitt „Korrekturstatus“
Zugehörige Listen	
Angreifbare Elemente	Angreifbare Elemente, die dieser Schwachstelle zugeordnet sind.
Verwundbarkeitsreferenzen	Informationen über die Schwachstelle aus externen Quellen, zitiert von NVD.
CVEs	CVE-Datensatz (Common Vulnerability Enumeration), der dieser Schwachstelle zugeordnet ist.
Kategorien	Kategorien, die dieser Schwachstelle zugeordnet sind.
Exploits	Exploits, die dieser Schwachstelle zugeordnet sind.
Schwachstellen-Malware-Kits	Malware-Kits, die dieser Schwachstelle zugeordnet sind.
Lösungen (Rapid7)	Lösungsinformationen aus den Rapid7-Lösungsintegrationen. Wird angezeigt, wenn verfügbar.
Exploit-Frameworks	Exploit-Frameworks, die dieser Schwachstelle zugeordnet sind.
Lösungen	Vulnerability Solution Management Lösungen, die dieser Schwachstelle zugeordnet sind.
CISA-Exploit	
CISA ist vorhanden	CISA-Exploit ist für die Tabelle „Eintrag zu Schwachstellen von Drittparteien“ vorhanden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
CISA-Fälligkeitsdatum	Frist zur Behebung der Schwachstelle.

Formularfelder für Korrekturaufgabe

Mithilfe von Korrekturaufgaben kann der Analysten den Fortschritt überwachen und den Mediationsprozess effizienter steuern.

Diese Felder befinden sich in Datensätzen, die in der Tabelle „Korrekturaufgabe“ [sn_vul_Vulnerability] aufgeführt sind.

Um importierte Daten in den in den folgenden Tabellen aufgeführten Feldern anzuzeigen, müssen Sie mindestens über die Rolle sn_vul.read_all verfügen.

Felder für Korrekturaufgabe

Feld	Beschreibung
Anzahl	Die automatisch generierte VI-Nummer (angreifbare Elemente) für diesen Datensatz.
Risikobewertung	Rollup der Risikopunktzahlen für angreifbare Elemente, getrennt in Bereiche: Kritisch, hoch, Mittel, Niedrig und keine. Weitere Informationen zu Risikobewertungen finden Sie unter . Vulnerability Response Rechner und Regeln für Schwachstellenrechner. **Hinweis:** Diese Basis **Risikobewertung** Ist nicht mit dem Lösungsdatensatz identisch **Risikobewertung.**
Risikopunktzahl	Rollup der Risikopunktzahlen aller angreifbaren Elemente, die dieser Korrekturaufgabe zugeordnet sind. Risikoniveau, das die angreifbaren Elemente gemeinsam für Ihre Umgebung darstellen. **Hinweis:** Diese Basis **Risikopunktzahl** Ist nicht mit dem Lösungsdatensatz identisch **Risikopunktzahl.**
Korrekturziel	Datum, bis zu dem die angreifbaren Elemente behoben werden sollen, seit der ersten Identifizierung. Weitere Informationen zu Korrekturzielen finden Sie unter Vulnerability Response Korrekturzielregeln.
Korrekturstatus	Status der Korrektur für die Aufgabe. Sie wird durch das angreifbare Element mit dem nächsten Fälligkeitsdatum bestimmt. Zu den status offener Gruppen gehören: • In Ausführung • Ziel rückt näher • Ziel fehlt Zu den status geschlossener Gruppen gehören:

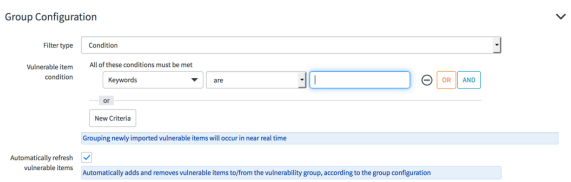
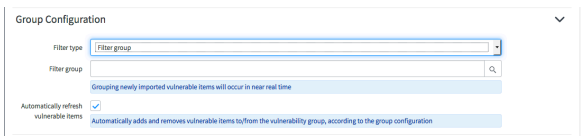
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für Korrekturaufgabe (Fortsetzung)

Feld	Beschreibung
	• Kein Ziel • Ziel erfüllt • Ziel fehlt Wenn die Aufgabe für berechnete Korrekturzieldaten geschlossen ist, wird der allgemeine Korrekturstatus aller geschlossenen angreifbaren Elemente in der Aufgabe angezeigt. Diese bestimmen, ob die Aufgabe ihr Datum erfüllt hat oder nicht. Der Korrekturstatus einer geschlossenen Aufgabe ist **Kein Ziel** Wenn keines der geschlossenen Elemente ein Korrekturzieldatum hatte. Ist es **Ziel Verfehlt** Wenn eines der geschlossenen Elemente sein Zieldatum verfehlt hat. Ist es **Ziel Erfüllt** Wenn mindestens ein geschlossenes VI sein Ziel erfüllt hat und keiner der anderen es verfehlt hat.
Status	Fortschrittsstatus der Aufgabe. Zu den Status gehören: • Öffnen • Wird untersucht • Warten auf Implementierung • Zurückgestellt • Wird überprüft • Gelöst • Geschlossen Weitere Informationen zu den Status finden Sie unter Vulnerability Response status der Korrekturaufgabe und der angreifbaren Elemente.
Bis-Datum für Risikominderung	Datum, an dem Ausgleichssteuerungen, die auf die Korrekturaufgabe angewendet werden, ablaufen. **Hinweis:** Dieses Feld wird nur angezeigt, wenn der Wert verfügbar ist.
Zuweisungsgruppe	Gruppe, die zur Bearbeitung dieser Korrekturaufgabe ausgewählt wurde.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an dieser Schwachstelle arbeitet.
Erstellt	Datum, an dem diese Korrekturaufgabe erstellt wurde.
Aktualisiert	Datum, an dem diese Korrekturaufgabe zuletzt aktualisiert wurde.
Schwachstelle	Schwachstelle, die für die Aufgabe gilt. (Sichtbar, wenn die Gruppe basierend auf einer einzelnen Schwachstelle gebildet wird.)
Kurzbeschreibung	Kurze Beschreibung dieser Korrekturaufgabe.

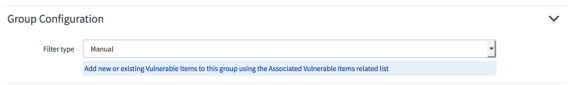
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für Korrekturaufgabe (Fortsetzung)

Feld	Beschreibung
Wird Überprüft (Sichtbar, wenn sich die RT im Status „in Überprüfung“ befindet)	
Angefordert von	Person, die die Zurückstellung beantragt hat.
Gewünschter Grund	Grund für Zurückstellung.
Gewünschter Zustand	Der vom Genehmiger angeforderte Status.
Gewünschter Substatus	Der vom Genehmiger angeforderte Grund.
Zurückstellung (Sichtbar, wenn sich die Aufgabe im Status „zurückgestellt“ befindet)	
Zurückgestellt von	Person, die die Aufgabe zurückgestellt hat.
Ablauf zurückstellen	Datum, an dem die Zurückstellung abläuft.
Grund für Zurückstellung	Grund für die Zurückstellung.
Lösung (Sichtbar, wenn sich die RT im Status „gelöst“ befindet)	
Gelöst von	Person, die die Korrekturaufgabe gelöst hat.
Lösungsdatum	Datum, an dem die Korrekturaufgabe gelöst wurde.
Lösungsnotizen	Zusätzliche Informationen.
Schließen (Sichtbar, wenn sich die RT im Status „Geschlossen“ befindet)	
Geschlossen von	Person, die die Korrekturaufgabe gelöst hat.
Geschlossen	Datum, an dem die Korrekturaufgabe geschlossen wurde.
Abschlussnotizen	Zusätzliche Informationen.
Gruppenkonfiguration (In allen status sichtbar)	
Filtertyp	Typ der Filterung, die zum Auswählen von Schwachstellen für die Gruppe verwendet wird: **Bedingung**  **Hinweis:** Wird einmal pro Stunde aktualisiert. **Filtergruppe**  **Hinweis:** Wird einmal pro Stunde aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für Korrekturaufgabe (Fortsetzung)

Feld	Beschreibung
	Manuell 
Nachbesserungsstatus	
Zurückgestellte sind ausgeschlossen	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente in dieser Aufgabe. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
VIs insgesamt	Gesamtzahl der angreifbaren Elemente in dieser Aufgabe. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
%VIS korrigiert	Abschluss in Prozent für die Korrektur angreifbarer Elemente in dieser Aufgabe. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Beinhaltet Zurückgestellte	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente in dieser Aufgabe.
VIs insgesamt	Gesamtzahl der angreifbaren Elemente in dieser Aufgabe.
%VIS korrigiert	Abschluss in Prozent für die Korrektur angreifbarer Elemente in dieser Aufgabe.
Notizen (In allen status sichtbar)	
Beschreibung	Beschreibung der Gruppe oder Korrekturaktionen.
Zusätzliche Anmerkungen	Zusätzliche Informationen.
Aktivitäten	Systemnotizen.
Zugehörige Links	
Angreifbare Elemente erneut scannen	Löst einen erneuten Scan der angreifbaren Elemente aus, um festzustellen, ob sie behoben wurden.
Aktualisierungsstatus	Zeigt Datum und Uhrzeit der letzten Aktualisierung an. Rollup der folgenden VIS in der Aufgabe: • Status der Korrekturaufgabe • Risikopunktzahlen und Risikobewertungen • Korrekturzieldatum und -Status (falls zutreffend) • Metriken wie aktive VIS, Gesamtanzahl VIS aus dem Abschnitt „Korrekturstatus“
Zugehörige Listen	
Angreifbare Elemente	Angreifbare Elemente in dieser Aufgabe.
Aufgaben-SLAs	Plattform-SLAs, die dieser Aufgabe zugeordnet sind.
Bevorzugte Lösungen	Bevorzugte Lösungen der angreifbaren Elemente in dieser Aufgabe.
Change-Anforderungen	Change-Anforderungen, die dieser Aufgabe zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder für Korrekturaufgabe (Fortsetzung)

Feld	Beschreibung
Angeforderte Genehmigungen	(Sichtbar, wenn sich die Aufgabe im Status „in Überprüfung“ befindet.) Liste der Genehmiger. Sobald die Zurückstellung genehmigt wurde, wird die Korrekturaufgabe in den Status zurückgestellt versetzt.

Formularfelder „Fragebogenkonfiguration“

Sie können einen eindeutigen Fragebogen für eine eindeutige Sammlung von Schwachstellen oder Korrekturaufgaben definieren, indem Sie die Schwachstellen bzw. Korrekturaufgaben im Abschnitt „Konfiguration des VR-Fragebogens“ des Formulars „Einstellungen für VR-Ausnahmemanagement“ filtern.

Das Formular „Fragebogenkonfiguration“ wird angezeigt, wenn Sie auswählen **Neu** Schaltfläche im Abschnitt „Konfiguration des VR-Fragebogens“ des Formulars „Einstellungen für VR-Ausnahmeverwaltung“.

Formularfelder „Fragebogenkonfiguration“

Feld	Beschreibung
Name	Name des Fragebogens.
Freigaberegel	Genehmigungsregel, für die der Fragebogen gilt. • **Ausnahmeanforderung für Schwachstellen-Gruppen** • **Ausnahmeanforderung für angreifbare Elemente** • **Falsch positiv für Schwachstellen-Gruppen** • **Falsch positiv für angreifbare Elemente** • **Fragebogen für Ausgleichssteuerungen für angreifbare Gruppen** Für Risikoreduzierungsanforderungen der Korrekturaufgabe. • **Fragebogen für Ausgleichssteuerungen für angreifbare Elemente** Für Anforderungen zur Risikominderung des angreifbaren Elements.
Beschreibung	Kurzbeschreibung für die Fragebogenkonfiguration.
Reihenfolge	Fragebogen mit der niedrigsten Reihenfolge wird während der Anforderungen angezeigt.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass der Fragebogen verwendet wird.
Tabelle	Tabelle, für die die Genehmigungsregel gilt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder „Fragebogenkonfiguration“ (Fortsetzung)

Feld	Beschreibung
	• Angreifbares Element [sn_vul_vulnerable_item für die Genehmigungsregeln im Zusammenhang mit angreifbaren Elementen. • Korrekturaufgabe [sn_vul_Vulnerability] für die Genehmigungsregeln im Zusammenhang mit Korrekturaufgaben.
Bedingung	Bedingung für die Datensätze, für die der Fragebogen angezeigt werden muss. Sie können die Bedingung auf alle Felder eines angreifbaren Elements und einer Korrekturaufgabe anwenden, mit Ausnahme **Grund** .
Fragebogen	Fragebogen, der angezeigt wird, wenn ein Korrekturbesitzer eine Ausnahme, ein falsch positives Ergebnis oder eine Risikominderung anfordert.

Zugehörige Informationen

Konfigurieren Sie das Ausnahmemanagement für Vulnerability Response

Konfigurieren Sie den Fragebogen für die Risikominderung

Vulnerability Response Formularfelder für angreifbare Elemente

Angreifbare Elemente werden während der Integrationsimporte von Schwachstellen von Drittparteien automatisch erstellt.

Felder für angreifbare Elemente

Um importierte Daten in den in den folgenden Tabellen aufgeführten Feldern anzuzeigen, müssen Sie mindestens über die Rolle sn_vul.read_all verfügen.

Diese Felder befinden sich in Datensätzen, die in der Tabelle „angreifbare Elemente“ [sn_vul_vulnerable_item] aufgeführt sind.

Wenn Sie SAM-NVD-Schwachstellen-Scan aktiviert haben, Die Datensätze werden mit der Software in verglichen Configuration Management Database (CMDB) Und-Übereinstimmungen werden bei angreifbarer Software oder Konfigurationselementen (Configuration Items, CIs) gefunden.

Feld	Beschreibung
Sicherheits-Tag auswählen	Sicherheits-Tag Um dem Datensatz Metadaten hinzuzufügen oder zu identifizieren, wer Zugriff auf diesen Security Incident-Datensatz haben soll. Dieses Feld wird erst angezeigt, nachdem das angreifbare Element gespeichert wurde.
Anzahl	Automatisch generierte angreifbare Elementnummer für diesen Datensatz.
Quelle	Scanner, der dieses angreifbare Element gefunden hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Risikobewertung	Quantifiziert **Risikopunktzahl** Trennung angreifbarer Elemente in „Kritisch“, „hoch“, „Mittel“, „Niedrig“ und „keine“. Weitere Informationen zu Risikobewertungen finden Sie unter Vulnerability Response Rechner und Regeln für Schwachstellenrechner. **Hinweis:** Diese Basis **Risikobewertung** Ist nicht mit dem Lösungsdatensatz identisch **Risikobewertung.**
Risikopunktzahl	Berechnetes Risiko, das das angreifbare Element für Ihre Umgebung darstellt. **Hinweis:** Diese Basis **Risikopunktzahl** Ist nicht mit dem Lösungsdatensatz identisch **Risikopunktzahl.** Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln für Schwachstellenrechner.
Schwachstelle	ID der Schwachstelle, die diesem angreifbaren Element zugeordnet ist.
Konfigurationselement	Betroffenes Asset.
Status	Dieses Feld ist standardmäßig auf festgelegt **Öffnen** , Aber Sie können es in ändern **Wird Untersucht** Wenn die Schwachstelle zur sofortigen Behebung bereit ist.
Bis-Datum für die Risikominderung	Datum, an dem Ausgleichssteuerungen, die auf das angreifbare Element angewendet werden, ablaufen. **Hinweis:** Dieses Feld wird nur angezeigt, wenn der ursprüngliche Risikopunktzahlwert verfügbar ist.
Zuweisungsgruppe	Gruppe, die zur Bearbeitung dieser Korrekturaufgabe ausgewählt wurde.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an dieser Schwachstelle arbeitet.
Erstellt	Datum, an dem dieses angreifbare Element in Ihrer Instanz erstellt wurde.
Zuletzt geöffnet	Datum, an dem das angreifbare Element zuletzt in Ihrer Instanz geöffnet wurde. Anfänglich entspricht dies dem Erstellungsdatum des angreifbaren Elements. Wenn es jedoch geschlossen wurde, dann erneut geöffnet, enthält das Datum und die Uhrzeit der erneuten Öffnung.
Aktualisiert	Datum des letzten Scans.
Alter	Dauer, für die das VI seit dem Datum der letzten Öffnung aktiv war. Wenn das VI geschlossen ist, wird der Wert des Felds Alter auf null festgelegt. Weitere Informationen zum Feld Alter finden Sie unter Berechnung und Anzeige des Alters angreifbarer Elemente. Weitere Informationen zum Anpassen der Berechnung der Altersdauer finden Sie unter KB1703270 artikel.
Schwachstelle	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zusammenfassung	Beschreibung der Schwachstelle.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle. Schweregradzuordnungen werden für NVD und mit bereitgestellt ServiceNow Drittpartei-Integrationen. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Erstellen Sie einen Vulnerability Response Schweregradzuordnung.
Schwachstellenpunktzahl (v3)	CVSS v3-Punktzahl.
Schwachstellenpunktzahl (v2)	CVSS v2-Punktzahl.
Exploit vorhanden	Ja, wenn mindestens ein Exploit den Schwachstellen zugeordnet ist, die diesem angreifbaren Element zugeordnet sind.
Exploit-Angriffsvektor	Der Angriffsvektor der Angreifer der Exploits für die Schwachstellen, die diesem angreifbaren Element zugeordnet sind.
Exploit-Kompetenzniveau	Niedrigstes Kompetenzniveau, das zum Ausnutzen der Schwachstellen erforderlich ist, die diesem angreifbaren Element zugeordnet sind.
Veröffentlichungsdatum	Datum, an dem die Schwachstelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt geändert wurde.
Bedrohung	Relevante Informationen zur Bedrohung. Aus dem Datensatz des angreifbaren Eintrags abgerufen. **Hinweis:** Alle hier vorgenommenen Änderungen aktualisieren den Datensatz des angreifbaren Eintrags.
Korrekturhinweise	Relevante Lösung für die Bedrohung, abgerufen aus dem Eintragsdatensatz für angreifbare Elemente.
Fehlerkorrektur Nur mit verfügbar Vulnerability Solution Management.	
Bevorzugte Lösung	Bevorzugte Lösung aus dem Schwachstellendatensatz importiert. **Hinweis:** Alle hier vorgenommenen manuellen Änderungen ändern den Schwachstellendatensatz nicht und bleiben bei nachfolgenden Importen im VI unverändert.
Zusammenfassung	Zusammenfassung aus dem Lösungsdatensatz importiert.
Lösungstyp	Potenzielle oder bevorzugte Lösung.
Erstmalige Erkennung	
DNS-Name	Name des Domänennamenservice-Namens. Wenn kein CI angegeben wird, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls vorhanden.
NetBIOS-Name	Name des NetBIOS. Wenn kein CI angegeben wird, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls vorhanden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
IP-Adresse	IPv4- oder IPv6-Adresse. Wenn kein CI angegeben wird, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls vorhanden.
Port	Adresse des Ports
Protokoll	Name des Protokolls.
SSL	Gibt an, ob SSL-Verschlüsselung verwendet wird oder nicht.
Erkennungen	
Status	Status der Erkennung.
Erste ermittelte	Datum, an dem die Drittparteiquelle die Erkennung für dieses Asset zuerst gefunden hat.
Zuletzt gefunden	Datum, an dem die Drittparteiquelle die Erkennung für dieses Asset zuletzt gefunden hat.
DNS-Name	Name des Domänennamenservice-Namens. Wenn kein CI angegeben wird, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls vorhanden.
NetBIOS-Name	Name des NetBIOS. Wenn kein CI angegeben wird, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls vorhanden.
IP-Adresse	IPv4- oder IPv6-Adresse. Wenn kein CI angegeben wird, wird dieses Feld verwendet, um nach einem übereinstimmenden CI zu suchen, falls vorhanden.
Port	Adresse des Ports
Protokoll	Name des Protokolls.
SSL	Gibt an, ob SSL-Verschlüsselung verwendet wird oder nicht.
Anzahl Ermittlungen	Gibt an, wie oft diese Schwachstelle in diesem Asset von der Drittparteiquelle erkannt wurde.
Integrationsausführung	Integrationsausführung, die die Erkennung importiert hat.
Schließen Verfügbar, sobald das angreifbare Element behoben und geschlossen wurde. Elemente in diesem Abschnitt sind schreibgeschützt.	
Geschlossen von	Wer das angreifbare Element geschlossen hat.
Geschlossen	Datum, an dem das angreifbare Element geschlossen wurde.
Abschlussnotizen	Informationen, die im Abschluss enthalten sind.
Alter der Schließung	Zeitraum, nach dem das VI geschlossen wurde. Wenn das VI erneut geöffnet wird, wird der Wert des Felds Alter geschlossen auf null festgelegt. Weitere Informationen dazu, wie das Feld Alter geschlossen wird, finden Sie unter Berechnung und Anzeige des Alters angreifbarer Elemente. Weitere Informationen zum Anpassen der Berechnung des Alters der geschlossenen Dauer finden Sie unter KB1703270 artikel.
Notizen	
Zusätzliche Kommentare/ Arbeitsnotizen	Alle relevanten Informationen. Aktivieren Sie das Kontrollkästchen, um zusätzliche Kommentare hinzuzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Beginnend mit Vulnerability Response V20.0 können Sie Arbeitsnotizen im Abschnitt „Notizen“ für ein zurückgestelltes angreifbares Element hinzufügen.
Aktivität	Wird nur angezeigt, wenn eine Arbeitsnotiz erstellt wurde.
Zugehörige Links	
Risikopunktzahl berechnen	Wenn entweder **Schwachstellenschweregrad** Oder **Risikopunktzahl** Rechner ist aktiviert, der **Risikopunktzahl** Feld wird aktualisiert.

Im Folgenden finden Sie die zugehörigen Listen für angreifbare Elemente.

Zugehörige Liste	Beschreibung
Korrekturaufgaben	Aufgaben, die diesem angreifbaren Element zugeordnet sind.
Betreffende Aufgaben	Aufgaben, die diesem angreifbaren Element zugeordnet sind.
Zugeordnete IP-Adressen	Verfügbar, wenn Qualys Vulnerability Integration Die Anwendung „Schwachstellenintegration“ ist installiert. IP-Adressen, die während der Deduplizierung gefunden werden.
Betroffene Services	Business-Services, die von diesem angreifbaren Element betroffen sind. Wird angezeigt, wenn diese Informationen in verfügbar sind cmdb Datensatz. Diese Informationen können manuell oder mit eingegeben werden ServiceNow® Service-Mapping Anwendung. Siehe Service-Mapping Weitere Informationen finden Sie unter . Wenn ein betroffenes CI, das dem angreifbaren Element zugeordnet ist, hinzugefügt oder aktualisiert wird, werden die Informationen in dieser zugehörigen Liste automatisch aktualisiert, wenn der Datensatz gespeichert wird.
Genehmigungen der Statusänderung	Status von Change-Anforderungen und anderen Genehmigungsinformationen, die der VIT zugeordnet sind.
Qualys-Tickets	Qualys Ticketintegrationsinformationen, die diesem angreifbaren Element zugeordnet sind.

Lösungsformularfelder

Lösungen werden automatisch erstellt, wenn Datensätze aus Lösungsintegrationen von Drittanbietern heruntergeladen und unter gespeichert werden **Lösungen** In Vulnerability Response.

Eingabefelder für Lösungsintegration

Die importierten Felder in dieser Tabelle sind schreibgeschützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anzahl	Bezeichner, der der Lösung zugewiesen ist.
Quelle	Ursprung der Lösung.
Quell-ID	Quellbezeichner für diese Lösung.
Risikobewertung	Trennt den Lösungsdatensatz **Risikopunktzahl** In Bereiche von kritisch bis keine. Für weitere Informationen zur Lösung **Risikobewertung** , Siehe Vulnerability Solution Management. **Hinweis:** Lösung **Risikobewertung** Ist nicht identisch mit **Angreifbares Element** , **Drittpartei-Schwachstelleneintrag** , Und **Korrekturaufgabe** Datensätze **Risikobewertung** .
Risikopunktzahl	Gewichtete Berechnung basierend auf **Risikopunktzahl** Und Anzahl der angreifbaren Elemente mit dieser Lösung als ihre **Bevorzugte Lösung** . Weitere Informationen zur Risikopunktzahl der Lösung finden Sie unter Vulnerability Solution Management. **Hinweis:** Lösungsdatensatz **Risikopunktzahl** Ist nicht identisch mit **Angreifbares Element** , **Drittpartei-Schwachstelleneintrag** , Und **Korrekturaufgaben** Datensätze **Risikopunktzahl** . Verfügbar, wenn SAM NVD aktiviert ist, aber wenn keine aktiven angreifbaren Elemente (VI) mit einer Schwachstelle verknüpft sind, die Lösung **Risikopunktzahl** Ist auf null festgelegt.
Höchste Ersetzung	Gibt an, dass keine Lösung sie ersetzt.
Lösungstyp	Welche Art von Lösung es ist. Die Auswahlmöglichkeiten lauten wie folgt: • Workaround • Mitigation • Lieferantenkorrektur • Patch • Rollup • Berechtigung • Wird nicht korrigiert • Keine verfügbar
Neustart erforderlich	Neustart erforderlich. Die Auswahlmöglichkeiten lauten wie folgt: • Ja • Nein • Vielleicht
Veröffentlichungsdatum	Datum, an dem die Schwachstelle nach Quelle veröffentlicht wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt von der Quelle geändert wurde.
Zusammenfassung	Korrekturzusammenfassung der Lösung.
Bulletin	Security Bulletin, das der Lösung zugeordnet ist.
Produktkategorien	Produktkategorien, für die die Lösung gilt.
Produkte	Produkte, für die die Lösung gilt.
Lösungsdetails	
Beschreibung	Wenn kein Inhalt aus der Lösungsquelle verfügbar ist, werden Sie zu einem anderen relevanten Abschnitt oder einer anderen Lösung weitergeleitet, um weitere Informationen zu erhalten.
Links	Importierte Internetressourcen, die der Lösung zugeordnet sind.
Schwachstellendetails	
Hinweise zu Schwachstellen	Zusammenfassung der von der Lösung korrigierten Schwachstellen.
Nachbesserungsstatus	
Bevorzugte Lösungsziele Korrekturstatus für angreifbare Elemente und ihre eindeutigen Konfigurationselemente (Configuration Items, CIs), für die dies die bevorzugte Lösung ist. **Hinweis:** Ein eindeutiges CI wird nur einmal gezählt, unabhängig davon, wie viele VIS es zugeordnet ist.	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
VIs insgesamt	Anzahl der aktiven und geschlossenen angreifbaren Elemente, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Behobene AEs in Prozent	Prozent abgeschlossen für Korrektur angreifbarer Elemente (VI). Gilt für VIS, für die diese Lösung bevorzugt wird. Diese Anzahl schließt zurückgestellte VIS aus.
Verbleibende CIs	Anzahl der eindeutigen CIs, die einem oder mehreren aktiven angreifbaren Elementen zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl schließt die CIs zurückgestellter angreifbarer Elemente aus.
CIs insgesamt	Anzahl der eindeutigen CIs, die einem oder mehreren aktiven und geschlossenen angreifbaren Elementen zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird. Diese Anzahl schließt die CIs zurückgestellter angreifbarer Elemente aus.
Behobene CIs in Prozent	Fertigstellungsgrad der eindeutigen korrigierten CIs (d. h. alle VIS für dieses CI und diese Lösung werden korrigiert). Wird durch die Anzahl der korrigierten CIs im Vergleich zu den insgesamt eindeutigen CIs bestimmt, die angreifbaren Elementen mit der bevorzugten Lösung zugeordnet sind. Diese Anzahl schließt die CIs zurückgestellter angreifbarer Elemente aus.
Bevorzugte Lösungsziele (Enthält Zurückgestellte)	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Korrekturstatus für angreifbare Elemente und ihre eindeutigen CIs, einschließlich zurückgestellt, für die dies die bevorzugte Lösung ist.	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung zur Korrektur bevorzugt wird.
VIs insgesamt	Anzahl der aktiven und geschlossenen angreifbaren Elemente, für die diese Lösung zur Korrektur bevorzugt wird.
Behobene AEs in Prozent	Prozent abgeschlossen für Korrektur angreifbarer Elemente (VI). Gilt für VIS, für die diese Lösung bevorzugt wird.
Verbleibende CIs	Anzahl der eindeutigen CIs, die einem oder mehreren aktiven angreifbaren Elementen zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird.
CIs insgesamt	Anzahl der eindeutigen CIs, die einem oder mehreren aktiven und geschlossenen angreifbaren Elementen zugeordnet sind, für die diese Lösung zur Korrektur bevorzugt wird.
Behobene CIs in Prozent	Fertigstellungsgrad der eindeutigen korrigierten CIs (d. h. alle VIS für dieses CI und diese Lösung werden korrigiert). Wird durch die Anzahl der korrigierten CIs im Vergleich zu den insgesamt eindeutigen CIs bestimmt, die angreifbaren Elementen mit der bevorzugten Lösung zugeordnet sind. Diese Anzahl schließt die CIs zurückgestellter angreifbarer Elemente aus.
Potenzielle Lösungsziele Korrekturstatus für angreifbare Elemente und ihre eindeutigen CIs mit einer Schwachstelle im Zusammenhang mit dieser Lösung.	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Verbleibende CIs	Anzahl der eindeutigen CIs, die einem oder mehreren aktiven angreifbaren Elementen zugeordnet sind, für die diese Lösung eine potenzielle Korrekturlösung ist. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Potenzielle Lösungsziele (Enthält Zurückgestellte) Korrekturstatus für angreifbare Elemente und ihre eindeutigen CIs, einschließlich zurückgestellt, mit einer Schwachstelle, die von dieser Lösung behoben werden kann, einschließlich der Anzahl der bevorzugten Lösungen.	
Angreifbare Elemente	Anzahl aktiver (nicht geschlossener) angreifbarer Elemente, für die diese Lösung eine potenzielle Lösung zur Korrektur darstellt.
Verbleibende CIs	Anzahl der eindeutigen CIs, die einem oder mehreren aktiven angreifbaren Elementen zugeordnet sind, für die diese Lösung eine potenzielle Korrekturlösung ist.
Notizen	
Interne Hinweise	Bearbeitbares Feld, das für den Korrekturspezialisten bereitgestellt wird.
Zugehörige Links	
Zustand aktualisieren	Datum und Uhrzeit der letzten Aktualisierung des Korrekturstatus. Aktualisiert Folgendes:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Status der Korrekturaufgabe • Risikopunktzahl und -Bewertung • Metriken aus dem Abschnitt „Korrekturstatus“
Zugehörige Listen	
Angreifbare Elemente	Angreifbare Elemente, die dieser Lösung als bevorzugte Lösung für die Korrektur zugeordnet sind.
Schwachstellen von Drittparteien	Schwachstellen von Drittparteien, die dieser Lösung zugeordnet sind.
CVEs	Common Vulnerability and Exposure (CVE)-Schwachstellen, die dieser Lösung zugeordnet sind.
Korrekturaufgaben	Korrekturaufgaben, die zugehörige angreifbare Elemente mit dieser Lösung enthalten, die für die Korrektur bevorzugt wird.
Vorhergehende Lösungen	Frühere Lösungen, die eine oder mehrere Schwachstellen dieser Lösung beheben.
Ersatzlösungen	Spätere Lösungen, die alle Schwachstellen dieser Lösung beheben. Diese Liste ist leer, wenn **Höchste Ersetzung** Kontrollkästchen ist aktiviert.

Genehmigungs-Workflow-Konfigurationen für Anforderung zum Aufheben der Zuweisung

Sie können den Genehmigungs-Workflow für das Entfernen von Zuweisungen aus angreifbaren Elementen (VIS, Vits), Korrekturaufgaben, angreifbaren Anwendungselementen (AVITs) und angreifbaren Containerelementen (CVITs) für Sie und Ihre Gruppe entwerfen.

VIT, Korrekturaufgabe, AVIT und CVIT haben jeweils eine standardmäßige Genehmigungsregel. Jede Genehmigungsregel verfügt über eine standardmäßige Genehmigungskonfiguration. Jede Genehmigungskonfiguration hat eine standardmäßige Genehmigerebene. Die Genehmigungsregeln für Vits, Korrekturaufgabe, AVIT und CVIT sind standardmäßig aktiviert. Als Administrator können Sie die folgenden Aktionen ausführen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Meine Genehmigungen** > **Freigaberegeln** Und Auswahl der entsprechenden Genehmigungsregel.

- Aktivieren oder deaktivieren Sie eine Genehmigungsregel.
- Erstellen und aktualisieren Sie eine Genehmigungskonfiguration.
- Definieren Sie Bedingungen für angreifbare Elemente und Korrekturaufgaben, für die die Genehmigungsregeln gelten.
- Erstellen und aktualisieren Sie mehrere Genehmigerebenen.

Die folgende Tabelle zeigt die standardmäßigen Genehmigungsregeln, Genehmigungskonfigurationen und Genehmigerebenen für VIT, Korrekturaufgabe, AVIT und CVIT, die im Lieferumfang des Basissystems enthalten sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßige Genehmigungsregeln, Genehmigungskonfigurationen und Genehmigerebenen

Typ	Genehmigungsregel	Genehmigungskonfigura	Genehmiger-Ebenen
VIT oder VI	Change-Anforderung für Feld zu angreifbarem Element	Change-Anforderung für Feld zu angreifbarem Element	Anforderung zum Aufheben der Zuweisung für VI auf Ebene 1
Nachbesserungsaufgabe	Schwachstellegruppenfeld Change-Anforderung	Change-Anforderung für Schwachstellenfeld	Ebene 1 – Anforderung der Zuweisungsaufhebung für SG
AVIT	Change-Anforderung für Feld zu angreifbaren Elementen der Anwendung	Change-Anforderung für Anwendungsschwachstellen Feld	Heben Sie die Zuweisung des App-Schwachstellenelements auf
CVIT	Genehmigung für Container-Verwaltung	Standardkonfiguration – CVIT-Zuweisung aufheben	CVIT-Zuweisung aufheben – Genehmigungsebene 1

Weitere Informationen zum Genehmigen von Anforderungen zum Aufheben der Zuweisung finden Sie unter Genehmigen oder lehnen Sie eine Anforderung zum Aufheben der Zuweisung in ab Vulnerability Response.

Vulnerability Response Beispiele für Regel für Korrekturaufgaben

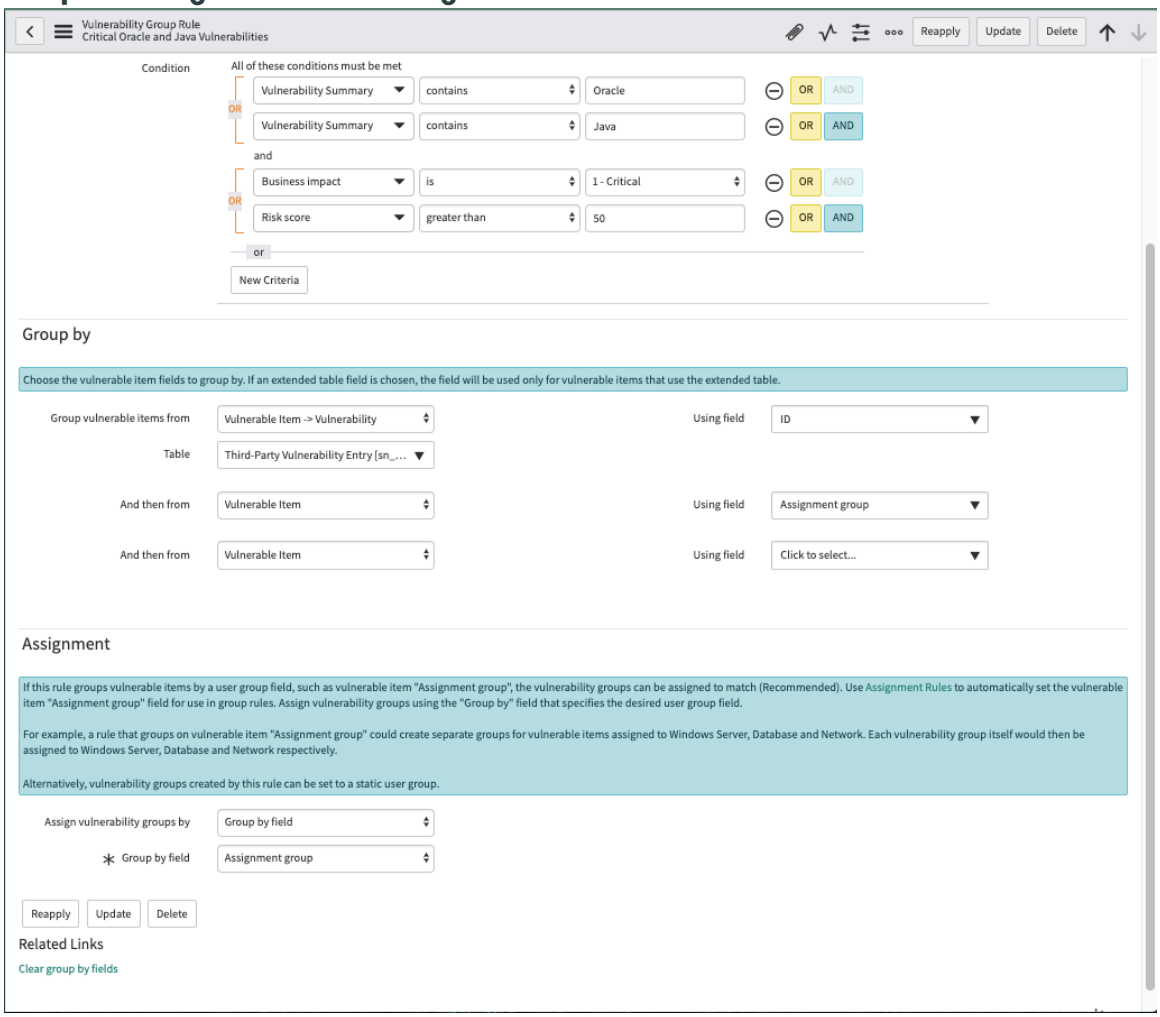
Beispiele für Regeln für Korrekturaufgaben, die Schwachstellen- und Risiko-, Impact- oder Konfigurationselement (Configuration Item, CI) verwenden.

Regel für Korrekturaufgaben zum Gruppieren angreifbarer Java- und Oracle-Elemente mit hohem Risiko

Dieses Beispiel zeigt einen Rundgang der Regel, die angreifbare Java- und Oracle-Elemente nach Schwachstelle gruppiert und sie ihren jeweiligen Supportgruppen zuweist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Regel für Korrekturaufgaben

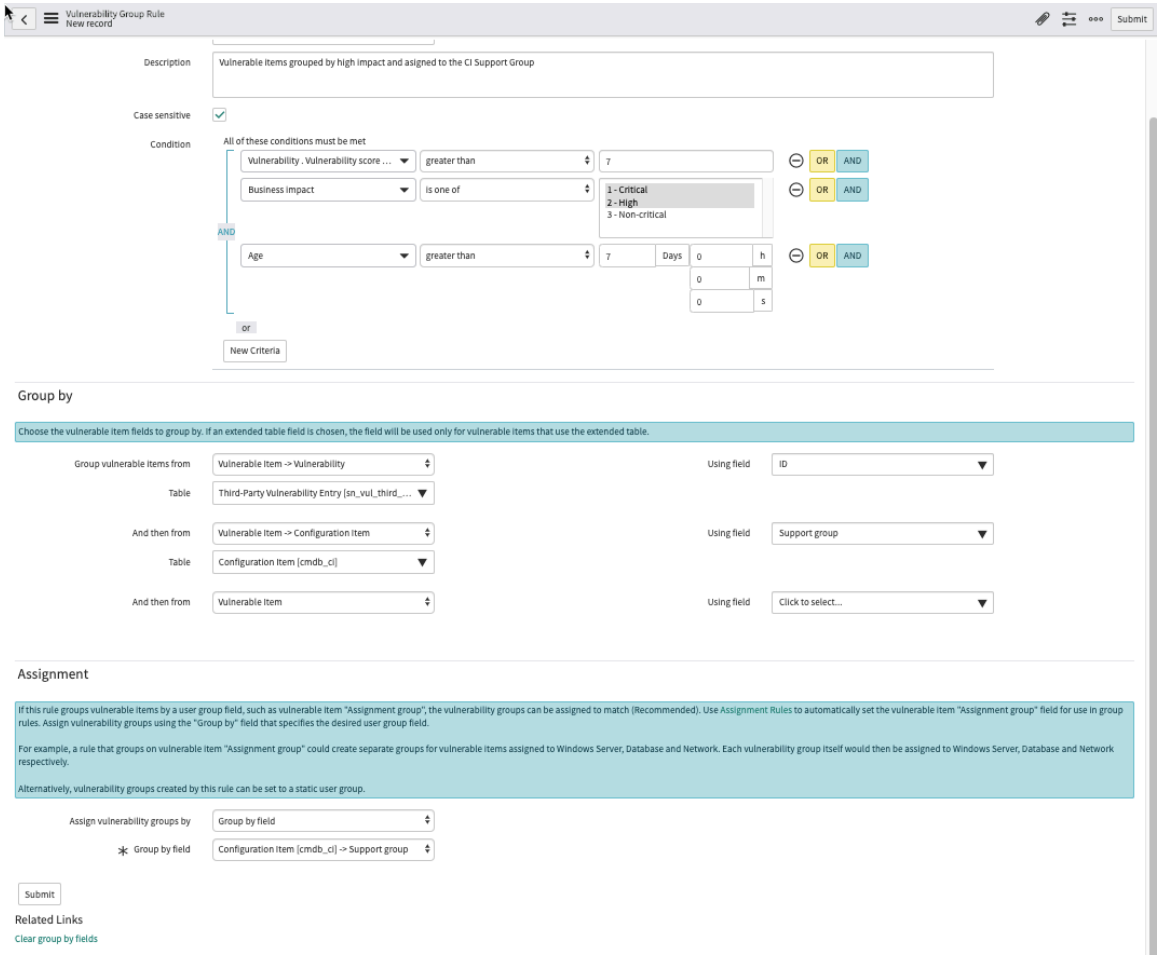


Klicken Sie mit der rechten Maustaste in den Header zu **Speichern** .

Regel für Korrekturaufgaben zum Gruppieren aller angreifbaren Elemente mit hoher Auswirkung nach Schwachstelle und CI-Supportgruppe

Dieses Beispiel zeigt die Formularfeldeinstellungen für eine Gruppenregel für angreifbare Elemente mit hoher Auswirkung, die sie der CI-Supportgruppe zuweist.

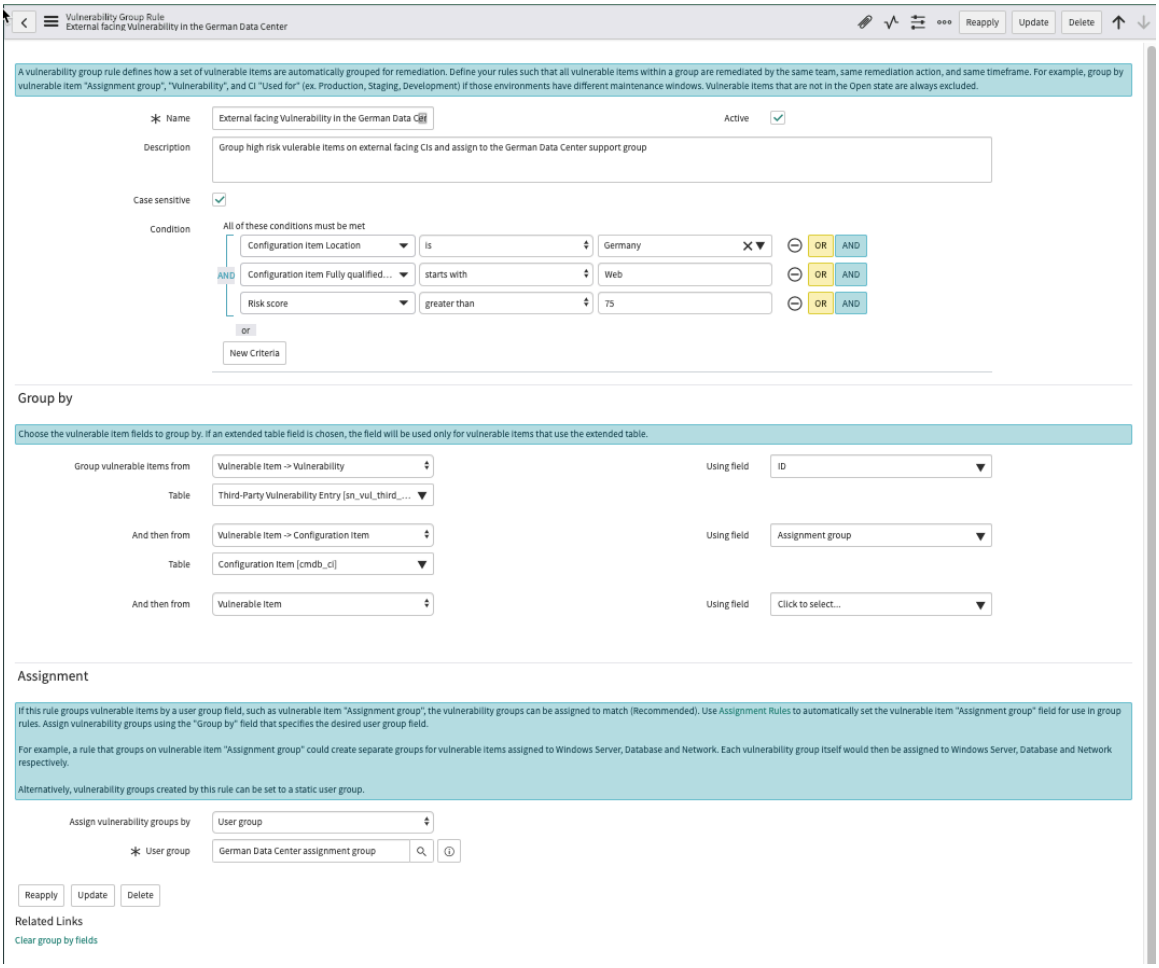
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Regel für Korrekturaufgaben zum Gruppieren aller Schwachstellen mit hohem Risiko für ein CI mit externer Ausrichtung in einem deutschen Rechenzentrum

Dieses Beispiel zeigt die Formularfeldeinstellungen für eine Gruppenregel für Schwachstellen mit hohem Risiko in externen CIs in einem deutschen Rechenzentrum. Sie sind der deutschen Rechenzentrumszuweisungsgruppe zugewiesen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beispiel zur Berechnung der Risikopunktzahl für Vulnerability Response

Sie können die Risikopunktzahlrechner bestimmen, um Risikopunktzahlen zu generieren, die die Schwachstellen- und Asset-Daten verwenden, die für Ihre Organisation spezifisch sind.

Beispiel für die Bestimmung der Punktzahlen von Risikoregelrechnern

Das folgende Beispiel zeigt, wie Punktzahlen für Risikoregelrechner bestimmt werden.

Angenommen, ein Risikoregelrechner ist mit den Feldern in dieser Tabelle konfiguriert:

Feld	Gewichtung	Gewichtungsaufgliederung
Schwachstelle.Schweregrad	50	Standard: 20 1 – Kritisch: 100 2 – Hoch: 80 3 – Mittel: 60 4 – Niedrig: 40 5 – Keine: 20
Vulnerability.Exploit Ist Vorhanden	50	Standard: 50

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Gewichtung	Gewichtungsaufgliederung
		Ja: 100 Nein: 0

Gehen Sie außerdem davon aus, dass die angreifbaren Elemente, die in dieser Tabelle angezeigt werden, im System vorhanden sind:

ID	Schwachstellenschweregrad	Schwachstellen-Exploit ist vorhanden
VIT00001	1 – Kritisch	1: Ja
VIT00002	2 – Hoch	1: Ja
VIT00003	3 – Mittel	2 – Nein
VIT00004	4 – Niedrig	2 – Nein
VIT00005	5 – Keine	2 – Nein

Die Berechnung der Risikopunktzahl für die angreifbaren Elemente wird basierend auf der folgenden Formel berechnet:

`Risikopunktzahl = (W(Schweregrad) * FV (Schweregrad). + W(exploitexists) * FV(Exploit vorhanden)) / 100`

Wo **W** Ist die Gewichtung und **FV** Ist der Gewichtungsprozentsatz des Feldwerts.

Die resultierende Risikopunktzahl für diese angreifbaren Elemente ist in dieser Tabelle beschrieben:

ID	Schwachstellenschwere (50 %)	Schwachstellen-Exploit vorhanden (50 %)	Resultierende Risikopunktzahl
VIT00001	1 – Kritisch (50 % x 100)	1 – Ja (50 % x 100)	100
VIT00002	2 – hoch (50 % x 80)	1 – Ja (50 % x 100)	90.0
VIT00003	3 – Mittel (50 % x 60)	2 – Nein (50 % x 0)	30
VIT00004	4 – Niedrig (50 % x 40)	2 – Nein (50 % x 0)	20
VIT00005	5 – keine (50 % x 20)	2 – Nein (50 % x 0)	10

Hinweis:
Da für VIT00005 der Wert des Schweregrads leer ist, wird für VIT00005 die Standardgewichtung angewendet.

Wenn der Gewichtungsprozentsatz für einen der Feldwerte geändert wird, finden Sie die Ergebnisse in dieser Tabelle:

Feld	Gewichtung	Gewichtungsaufgliederung
Schwachstelle.Schweregrad	50	• Standard: 20 • 1 – Kritisch: 100 • **2 – Hoch: 70**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Gewichtung	Gewichtungsaufgliederung
		*Überarbeiteter Wert • 3 – Mittel: 60 • 4 – Niedrig: 40
Vulnerability.Exploit Ist Vorhanden	50	• Standard: 50 • Ja: 100 • Nein: 0

Die Risikopunktzahl für die angreifbaren Elemente nach erneuter Anwendung des Rechners wird in dieser Tabelle angezeigt:

ID	Schwachstellenschwere (50 %)	Schwachstellen-Exploit vorhanden (50 %)	Resultierende Risikopunktzahl
VIT00001	1 – Kritisch (50 % x 100)	1 – Ja (50 % x 100)	100
VIT00002	**2 – hoch (50 % x 70)** *Überarbeiteter Wert	1 – Ja (50 % x 100)	**85** *Überarbeiteter Wert
VIT00003	3 – Mittel (50 % x 60)	2 – Nein (50 % x 0)	30
VIT00004	4 – Niedrig (50 % x 40)	2 – Nein (50 % x 0)	20
VIT00005	5 – keine (50 % x 20)	2 – Nein (50 % x 0)	10

Fehlerbehandlung für Erkennungen

Fehler werden beim Erstellen von Erkennungen oder beim Erstellen und Aktualisieren angreifbarer Elemente während der Verarbeitung der Anhänge protokolliert. Wenn ein Schwachstellenintegrationsprozess fehlschlägt, werden Fehler auf der Registerkarte „Protokoll der Schwachstellenintegrationen“ protokolliert.

Diese Fehler werden mit einer der folgenden Kategorien protokolliert.

Feld	Beschreibung
VI-Erstellung	Fehler beim Erstellen oder Aktualisieren der Erkennung.
Erkennung	Fehler beim Erstellen einer Erkennung.

Mobile Experience für Vulnerability Response

Wenn Sie für die Korrektur von Schwachstellen zuständig sind, können Sie mit Ihrem Android- oder iOS-Mobilgerät auf die Anwendung Vulnerability Response (VR) in Ihrer ServiceNow AI Platform®-Instanz zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Vulnerability Response

Informationen zu den Konzepten von Vulnerability Response und zu der Frage, wie dieses Produkt Ihrer Organisation helfen kann, finden Sie unter Vulnerability Response verstehen.

Hinweis:
Bevor Sie installieren Vulnerability Response Mobile-App Mobil , Machen Sie sich mit vertraut Mobile Agent an.

Übersicht

Als Anwender mit der Rolle „Korrekturbesitzer“ (sn_vul.Remediation_owner) Vulnerability Response Mobile-App Ermöglicht Ihnen das Anzeigen und Durchsuchen der Schwachstellen, Korrekturaufgaben und Zuweisungen in Ihrem ServiceNow AI Platform Instanz direkt von Android Oder iOS Mobilgerät.

Sie werden benachrichtigt, wenn Ihnen oder Ihrer Zuweisungsgruppe Korrekturaufgaben (RTS) oder VIS zugewiesen wurden. Diese App bietet einem Korrekturbesitzer die Flexibilität, Felder neu zuzuweisen, zu bearbeiten und mit der Korrektur zu beginnen, ohne an den Desktop gebunden zu sein.

Sie haben Zugriff auf Schwachstellen, Schwachstellenelemente, Module und alle Lösungen. Sie können die folgenden Aufgaben auf Ihrem Mobilgerät ausführen:

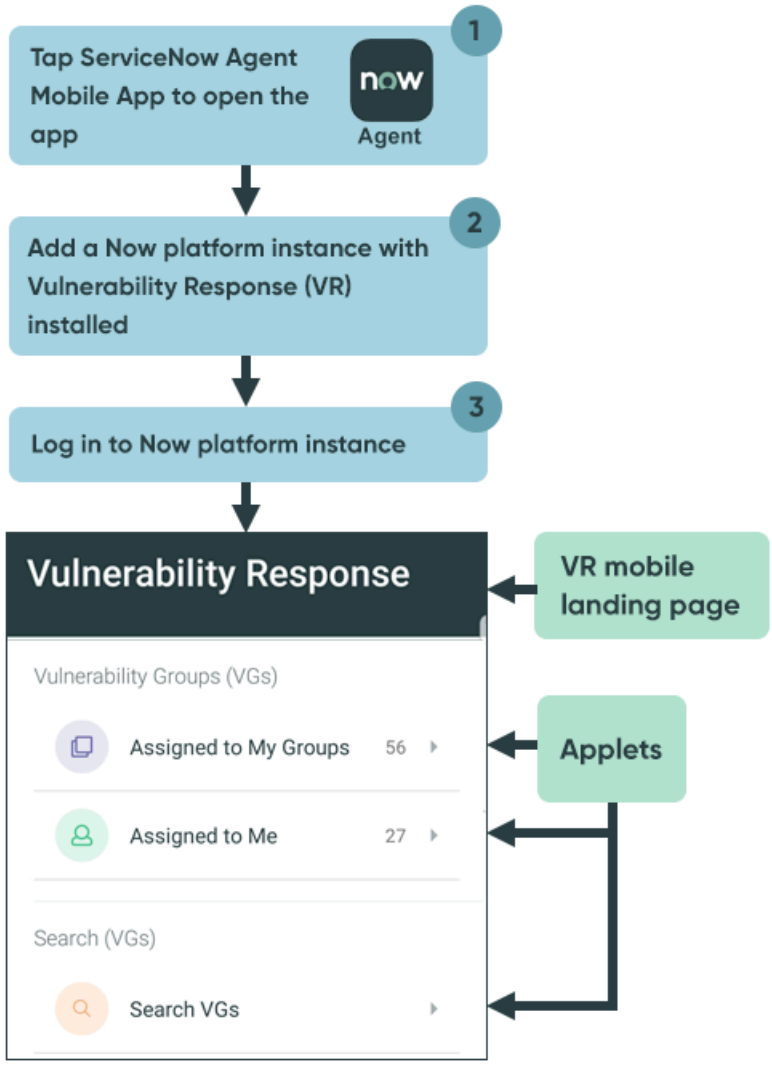
- Zeigen Sie Korrekturaufgaben an, und aktualisieren Sie sie.
- Zeigen Sie Change-Anforderungen an.
- Weisen Sie eine Korrekturaufgabe oder ein Schwachstellenelement einem anderen Mitglied einer Zuweisungsgruppe neu zu.
- Zeigen Sie Benachrichtigungen an, wenn Ihnen oder einer Ihrer Zuweisungsgruppen eine kritische Korrekturaufgabe zugewiesen ist.
- Bearbeiten Sie eine Teilmenge von Feldern in Korrekturaufgaben-Datensätzen.
- Suchen Sie nach Korrekturaufgaben, die bestimmten Suchkriterien entsprechen.

Die folgende Abbildung zeigt, wie Sie sich bei anmelden ServiceNow AI Platform Instanz von Ihrem Mobilgerät und dem Zielbildschirm von Vulnerability Response Mobile-App Das angezeigt wird, nachdem Sie sich angemeldet haben.

Für Schritt-für-Schritt-Anweisungen zur Einrichtung von ServiceNow AI Platform Instanz und installieren Sie Vulnerability Response Mobile-App, Siehe Richten Sie die Prüfliste für ein Vulnerability Response Mobile-App. Anweisungen zur Anmeldung finden Sie unter Melden Sie sich bei an Vulnerability Response Mobile-App.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Mobile-App



Anwendungen

-Anwendungen sind ServiceNow Softwarekomponenten wie Security Incident Response(SIR), Vulnerability Response(VR), Governance, Risk und Compliance(GRC) Und Sonstiges ServiceNow Produkte, die bestimmte Funktionen in Ihrem bieten ServiceNow AI Platform Instanz. Nachdem Sie Core-Anwendungen installiert haben, die mobile Apps auf Ihrem haben ServiceNow AI Platform Diese Anwendungen werden als Symbole unten auf Ihrem Mobilgerät angezeigt.

Vulnerability Response-Symbol auf Mobilgerät

Ordner

Jeweils ServiceNow® Mobile Die Anwendung enthält Ordner, die die Applets nach Kategorien trennen. Im vorherigen Bild sind Korrekturaufgaben und Suche (VGS) die Ordner für Vulnerability Response Mobile-App.

Applets

Applets sind die verschiedenen Optionen in der Anwendung. Im vorherigen Bild sind die Symbole unter Korrekturaufgaben und Suche (VGS) die verfügbaren Applets für Vulnerability Response Mobile-App.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Weitere Informationen zu den Applets von finden Sie in den folgenden Themen Vulnerability Response Mobile-App.

Richten Sie die Prüfliste für ein Vulnerability Response Mobile-App

Die folgende Prüfliste enthält die Setup-Aufgaben, die Sie in ausführen müssen ServiceNow AI Platform®-Instanz und auf Ihrem Mobilgerät vor der Verwendung von Vulnerability Response Mobile-App.

Vorbereitungen

Weitere Informationen folgen jedem Schritt in der rechten Spalte. Geschätzte Zeit bis zum Abschluss dieser Aufgabe: 15-20 Minuten.

Erforderliche Rollen: admin, sn_vul.Remediation_owner

Sie haben Ihr Mobilgerät erfolgreich für eingerichtet Vulnerability Response Mobile-App. Der nächste Schritt besteht darin, sich bei anzumelden Vulnerability Response Mobile-App Und fügen Sie ein hinzu ServiceNow AI Platform Instanz für Ihr Mobilgerät.

Prozedur

1. Drucken Sie diese Prüfliste optional aus, und verwenden Sie sie, um Sie durch die Aufgaben zu führen, die für die Installation von erforderlich sind Vulnerability Response Mobile-App.
2. Stellen Sie sicher, dass jedes Element in der Liste abgeschlossen ist, damit Sie sich bei anmelden können Vulnerability Response Mobile-App Und fügen Sie ein hinzu ServiceNow AI Platform Instanz.

Mobile Prüfliste

Element	Beschreibung
☐	Stellen Sie als Anwender mit der Administratorrolle sicher, dass Sie über verfügen Vulnerability Response Core-Anwendung auf installiert ServiceNow AI Platform Instanz. Dies ist der ServiceNow AI Platform Instanz, die Sie auf Ihrem Mobilgerät anzeigen. **Hinweis:** Die Vulnerability Response Core-Anwendung und ServiceNow AI Platform Instanz muss aus demselben Familien-Release stammen. **a.** Um zu überprüfen, ob die Kernanwendung auf Ihrer Instanz installiert ist, navigieren Sie zu **Plugins** Und suchen Sie nach Vulnerability Response. **b.** Wenn Vulnerability Response Core-Anwendung ist nicht bereits installiert. Klicken Sie auf **Installieren** Um es zu installieren. Weitere Informationen zur Installation von finden Sie Vulnerability Response Kernanwendung, siehe Vulnerability Response installieren. Weitere Informationen zum Abrufen von Vulnerability Response Kernanwendung auf der ServiceNow Store, Abrufen der Berechtigung, Installieren von Kernanwendungen und Aktivieren von Abhängigkeiten, siehe Security Operations Und ServiceNow Store.
☐	Stellen Sie als Anwender mit der Administratorrolle sicher, dass Sie über verfügen Vulnerability Response Mobile-App Auf installiert ServiceNow AI Platform Instanz, die Sie auf Ihrem Mobilgerät anzeigen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Beschreibung
	Hinweis: Die Vulnerability Response Mobile-App Und ServiceNow AI Platform Instanz muss aus demselben Familien-Release stammen. Die Vulnerability Response Mobile-App Und Vulnerability Response Anwendung muss kompatibel sein. Weitere Informationen zur Kompatibilität der Vulnerability Response-Anwendung finden Sie unter Kompatibilitätsmatrix für Vulnerability Response und Konfigurations-Compliance . Laden Sie herunter, und installieren Sie Vulnerability Response Mobile-App Von ServiceNow Store Auf Ihrem ServiceNow AI Platform Instanz. Wenn Sie installieren Vulnerability Response Mobile-App, Die Abhängigkeiten com.Glide.sg und com.Glide.sg.Agent_native_Client werden ebenfalls installiert. So überprüfen Sie, ob diese Abhängigkeiten installiert sind: **a.** Navigieren zu **Alle** > **Plugins**an. **b.** Suchen Sie nach den Plugin-IDs (com.Glide.sg und com.Glide.sg.Agent_native_Client). **c.** Wenn sie nicht aktiviert sind, aktivieren Sie diese Plugins. Diese Plugins sind für erforderlich Vulnerability Response Mobile-App. Weitere Informationen zum Abrufen von Vulnerability Response Mobile-App-Anwendung auf ServiceNow Store, Abrufen der Berechtigung, Installieren von Anwendungen und Aktivieren von Abhängigkeiten, siehe Security Operations Und ServiceNow Store.
☐	Als Anwender mit der Administratorrolle in Ihrem ServiceNow AI Platform Instanz überprüfen Sie, ob Sie mobile Anwender mit den erforderlichen zugewiesen haben ServiceNow AI Platform Rollen. **a.** Um die Rollen anzuzeigen, die einem Anwender zugewiesen sind, navigieren Sie zu **Alle** > **Administration** > **Anwender**an. **b.** Wählen Sie den Anwendernamen gefolgt von der zugehörigen Liste „Rollen“ aus. Alle diesem Anwender zugewiesenen Rollen werden angezeigt. **c.** Überprüfen Sie, ob ein Anwender zugewiesen ist, oder weisen Sie einen Anwender mit der Rolle „IT Infrastructure Library“ (itil) zu. Benutzer mit der Rolle itil können Change-Anforderungen und Korrekturaufgaben erstellen, öffnen, aktualisieren und schließen. Nur Anwendern mit der Rolle itil können Aufgaben zugewiesen werden. **d.** Überprüfen Sie, ob ein Anwender zugewiesen ist, oder weisen Sie einen Anwender mit der Rolle „Korrekturbesitzer“ (sn_vul.Remediation_owner) zu. Benutzer mit der Rolle „sn_vul.Remediation_owner“ können Schwachstellen- und Lösungsdatensätze lesen. Diese Rolle wird automatisch hinzugefügt, wenn Sie die Rolle itil zuweisen. **e.** Überprüfen Sie, ob Sie alle erforderlichen Zuweisungsgruppen erstellt und diesen Gruppen mobile Anwender zugewiesen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Beschreibung
	Hinweis: Wenn Sie eine große Anzahl von Anwendern für die mobile Anwendung haben, können Sie alternativ einer Gruppe die Rolle sn_vul.Remediation_owner zuweisen. Jeder Anwender, den Sie der Gruppe hinzufügen, erbt diese Rolle. Weitere Informationen zu Zuweisungsregeln und -Gruppen finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Weitere Informationen zu Anwendern und zum Zuweisen von Rollen zu Anwendern und Gruppen finden Sie unter Anwenderverwaltung .
☐	Laden Sie als Anwender mit der Rolle „Korrekturbesitzer“ (sn_vul.Remediation_owner) die aktuelle Version herunter ServiceNow® Agent-App auf Ihrem Mobilgerät. Die aktuelle Agent-App ist auf Apple verfügbar iOS App Store und Google Play Store.
☐	Stellen Sie als Benutzer mit der Rolle sn_vul.Remediation_owner sicher, dass Benachrichtigungen auf Ihrem Mobilgerät und in aktiviert sind ServiceNow AI Platform Instanz. Benachrichtigungen informieren Sie, wenn Ihnen oder Ihrer Zuweisungsgruppe kritische Korrekturaufgaben zugewiesen werden. Um Sie bei der rechtzeitigen Korrektur zu unterstützen, klicken Sie nach dem Aktivieren von Benachrichtigungen auf eine Benachrichtigung im Vulnerability Response Mobile-App Und navigieren Sie direkt zum Datensatz. Um Benachrichtigungen in zu aktivieren ServiceNow AI Platform Führen Sie die folgenden Schritte aus, damit sie auf Ihrem Mobilgerät angezeigt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Beschreibung
	a. Überprüfen Sie, ob Sie heruntergeladen und installiert haben Vulnerability Response Mobile-App Auf Ihrem ServiceNow AI Platform Instanz. **b.** In Systemeinstellungen in Ihrem ServiceNow AI Platform Stellen Sie unter Benachrichtigungen sicher, dass Sie aktiviert haben **ServiceNow Mobile-Anwendung** . Weitere Informationen zum Festlegen von Benachrichtigungen finden Sie unter Setting notification preferences in Core UI . ServiceNow AI Platform Benachrichtigungen werden auch auf dem Nachrichtenbildschirm auf Ihrem Mobilgerät angezeigt. Überprüfen Sie, ob Benachrichtigungen auch in den Einstellungen Ihres Mobilgeräts aktiviert sind.

Melden Sie sich bei an Vulnerability Response Mobile-App

Öffnen Sie die App Vulnerability Response Mobile, und fügen Sie ein hinzu ServiceNow AI Platform Instanz mit Vulnerability Response für Ihr Mobilgerät.

Vorbereitungen

Vergewissern Sie sich, dass Sie die in beschriebenen Setup-Schritte abgeschlossen haben Richten Sie die Prüfliste für ein Vulnerability Response Mobile-App.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Korrekturbesitzer (sn_vul.Remediation_owner)

Warum und wann dieser Vorgang ausgeführt wird

Zeit bis zum Abschluss dieser Aufgabe: 5-7 Minuten.

Prozedur

1. Tippen Sie auf Ihrem Mobilgerät auf **ServiceNow-Agent** App.

   Wenn Sie noch nicht bei angemeldet sind ServiceNow AI Platform Instanz wird der Bildschirm Instanzen angezeigt.

2. Wenn ServiceNow AI Platform Instanz mit Vulnerability Response Die Kernanwendung wurde Ihrem Mobilgerät nicht bereits hinzugefügt. Führen Sie die folgenden Schritte aus, um sie hinzuzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Tippen Sie im angezeigten Bildschirm „Instanzen“ auf das Plus-Symbol ( ).
Es wird ein Bildschirm angezeigt, der Sie auffordert, eine Adresse eines einzugeben und zu speichern ServiceNow AI Platform Instanz.

b. Füllen Sie die Felder aus.

Feldname	Beschreibung
Geben Sie die Instanzadresse ein, oder scannen Sie einen QR-Code.	Wählen Sie eine aus, um fortzufahren: ▪ Vor .service-now.com , Geben Sie den Namen Ihres ein ServiceNow AI Platform Beispiel: VrmobilenewyorkAgent . ▪ Geben Sie eine Adresse ein. Diese Adresse ist die URL Ihres ServiceNow AI Platform Instanz, die Sie auf Ihrem Mobilgerät anzeigen möchten. ▪ Scannen Sie einen QR-Code.
(Optional) Geben Sie den Kurznamen ein	Geben Sie einen Spitznamen für diese Instanz ein. Wenn dem Gerät mehrere Instanzen hinzugefügt wurden, können Kurznamen Ihnen helfen, schnell einen zu finden ServiceNow AI Platform Instanz.

c. Tippen Sie Auf **Speichern und anmelden**

3. Auf der ServiceNow Geben Sie den Anwendernamen und das Passwort für den -Anmeldebildschirm ein, der angezeigt wird ServiceNow AI Platform Instanz, die Sie hinzufügen möchten, und tippen Sie auf **Melden Sie Sich An** .
Der Zielbildschirm Vulnerability Response wird angezeigt. Sie haben sich erfolgreich bei angemeldet Vulnerability Response Mobile-App!

4. Überprüfen Sie nach der Anmeldung, ob Benachrichtigungen in aktiviert sind Vulnerability Response Mobile-App.

a. Tippen Sie auf dem Zielbildschirm unten auf **Benachrichtigung** .

b. Tippen Sie im Bildschirm Benachrichtigungen auf **Aktivieren Sie Benachrichtigungen** Wenn nicht aktiviert.
Benachrichtigungen von ServiceNow AI Platform Werden auf dem Bildschirm Benachrichtigungen in angezeigt Vulnerability Response Mobile-App.

5. Nachdem Sie sich bei einer Instanz auf Ihrem Mobilgerät angemeldet haben, ist dies der Standard ServiceNow AI Platform Instanz auf dem Gerät.
Wenn Sie eine weitere anzeigen möchten ServiceNow AI Platform Auf dem Gerät müssen Sie sich von der Standardinstanz abmelden. So melden Sie sich ab:

a. Tippen Sie auf **Einstellungen** Symbol.

b. Tippen Sie Auf **Melden Sie Sich Ab** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Bildschirm „Instanzen“ wird mit einem angezeigt ServiceNow AI Platform Instanzen, die Sie dem Mobilgerät hinzugefügt haben.

c. **Wahlweise:** Tippen Sie auf eine andere Instanz, um sich bei ihr anzumelden, oder führen Sie alternativ die vorherigen Schritte aus, um eine weitere Instanz hinzuzufügen.

Ergebnisse

Wenn der Bildschirm „Instanzen“ für den Vulnerability Response Mobile-App Wird nicht angezeigt, nachdem Sie auf getippt haben **ServiceNow-Agent** App verifizieren Sie auf Ihrem Gerät, dass **ServiceNow-Agent** Ist als vertrauenswürdige App auf Ihrem Gerät zulässig. Um den Zugriff als vertrauenswürdige App zuzulassen, navigieren Sie auf Ihrem Gerät zu den Einstellungen und allgemeiner Geräteverwaltung, und tippen Sie auf die Option (Trust-App usw.), um den Zugriff zu erlauben.

Wenn eine Fehlermeldung angezeigt wird, nachdem Sie Ihre Anmeldeinformationen auf dem Anmeldebildschirm eingegeben haben, überprüfen Sie, ob Ihr Anwendername und Ihr Passwort für den vorhanden sind ServiceNow AI Platform Instanz ist korrekt.

Wenn Sie Probleme beim Anzeigen des Zielbildschirms haben, überprüfen Sie Ihre Netzwerkverbindung.

Wenn Sie den Bildschirm Instanzen nicht anzeigen können, nachdem Sie auf getippt haben **ServiceNow-Agent** Versuchen Sie, die App von Ihrem Gerät zu deinstallieren. Überprüfen Sie, ob Sie über die aktuelle Version der App von Apple verfügen iOS App Store oder der Google Geben Sie den Store wieder, und versuchen Sie, ihn neu zu installieren.

Mit können Sie Korrekturaufgaben anzeigen, zuweisen und bearbeiten Vulnerability Response Mobile-App

Zeigen Sie die Felder in Korrekturaufgaben-Datensätzen (RT) an, weisen Sie sie zu, oder bearbeiten Sie sie. Navigieren Sie durch Schwachstellen, Schwachstellenelemente und Lösungsdatensätze und zugehörige Listen, um Lösungen, Bereitstellungsmetriken und zu behandelnde Elemente anzuzeigen.

Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer (sn_vul.Remediation_owner)

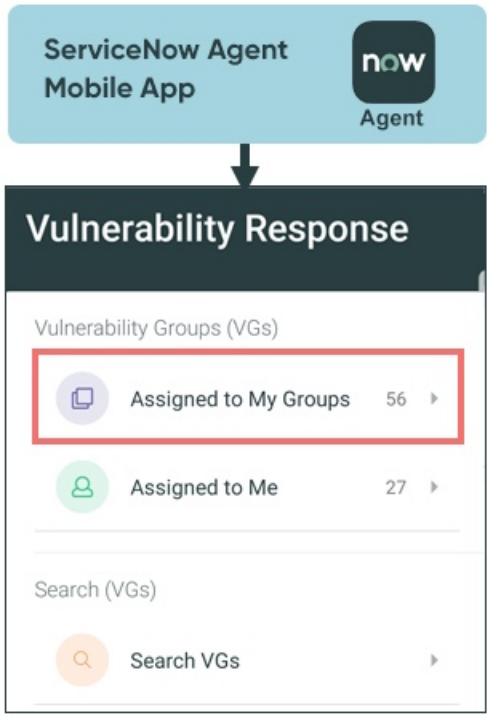
Warum und wann dieser Vorgang ausgeführt wird

Weisen Sie sich selbst RT-Datensätze (VUL) zu, oder weisen Sie sie einem anderen Mitglied Ihrer Gruppe zu. Alternativ können Sie die Details aktiver Korrekturaufgabendatensätze, angreifbarer Elemente (VI), NVD-Schwachstellen und Lösungen anzeigen, bevor Sie sie bearbeiten, zuweisen oder korrigieren. Zeit bis zum Abschluss dieser Aufgabe: 5-10 Minuten.

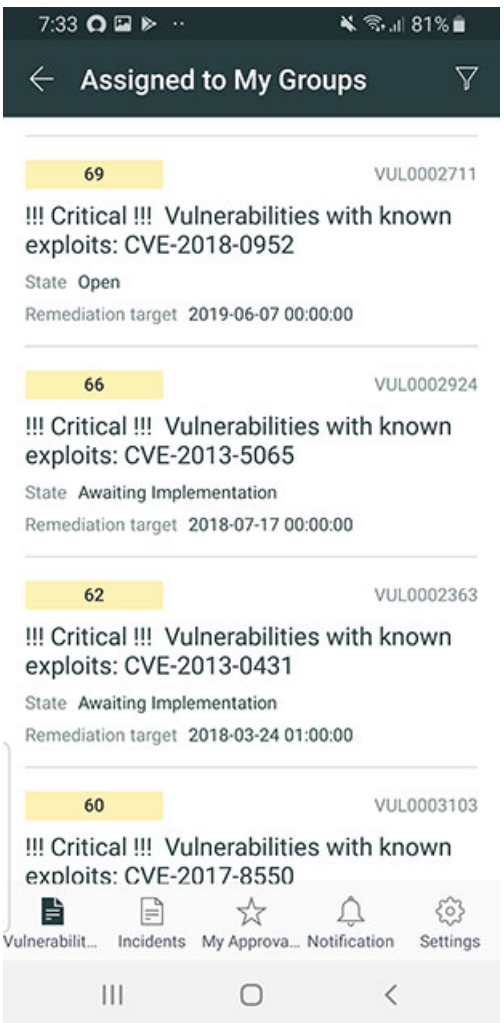
Prozedur

1. Wenn Sie nicht bei angemeldet sind ServiceNow AI Platform Instanz auf Ihrem Mobilgerät. Weitere Informationen finden Sie unter Melden Sie sich bei an Vulnerability Response Mobile-App.
2. Tippen Sie auf, während der Zielbildschirm Vulnerability Response angezeigt wird **Meinen Gruppen zugewiesen** .
   Wenn Sie weg von navigieren Vulnerability Response Mobile-App Nachdem Sie sich angemeldet haben, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

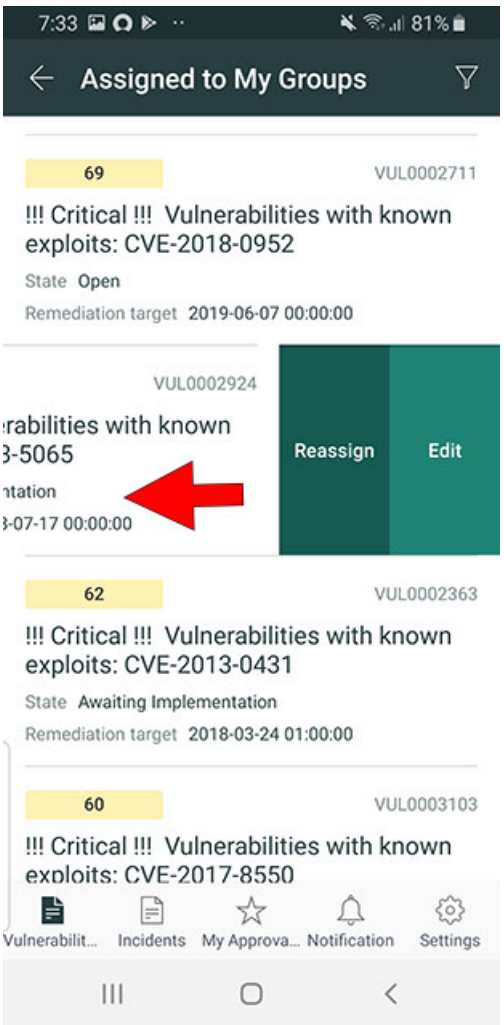


Die Liste der offenen Datensätze, die Ihrer Gruppe zugewiesen sind, wird angezeigt.



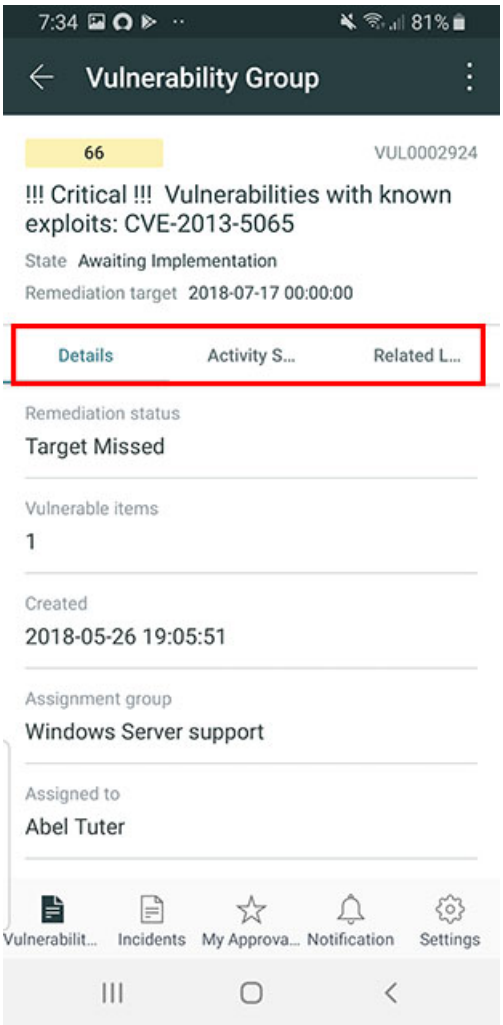
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Siehe Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App Um nach Datensätzen zu suchen, die bestimmten Kriterien entsprechen.
4. Alternativ mit dem Filtersymbol ( ) Angezeigt, Legen Sie Filter fest, um die Anzahl der Datensätze zu begrenzen In der Liste.
   Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator im ServiceNow AI Platform.
5. Um einen Datensatz direkt aus der Liste neu zuzuweisen oder zu bearbeiten, wobei die Liste der offenen Datensätze angezeigt wird, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.



6. Wählen Sie einen aus dem angezeigten Menü aus, um fortzufahren.
7. Alternativ können Sie auf einen Datensatz in der Liste tippen, um die Details eines offenen Schwachstellendatensatzes anzuzeigen und weitere zugeordnete Datensätze und zugehörige Listen anzuzeigen, wenn der Bildschirm meinen Gruppen zugewiesen angezeigt wird.
8. Wählen Sie im angezeigten Datensatz der offenen Korrekturaufgabe eine Option aus der folgenden Tabelle aus, um Arbeitsnotizen oder zugehörige Listen anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die folgende Abbildung zeigt den Navigationspfad vom Korrekturaufgabendatensatz zum bevorzugten Lösungsdatensatz für die ausgewählte Schwachstelle. Navigieren Sie durch die Datensätze und zugehörigen Listen, um Lösungen, Bereitstellungsmetriken und zu behandelnde Elemente anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigationspfad von der Korrekturaufgabe durch einen Lösungsdatensatz

9. Wählen Sie nach der Überprüfung, Bearbeitung oder Korrektur eine Option aus, um fortzufahren.

Zeigen Sie Korrekturaufgaben an, weisen Sie sie neu zu, und bearbeiten Sie sie mit dem Vulnerability Response Mobile-App

Zeigen Sie die Ihnen zugewiesenen Felder in Korrekturaufgaben-Datensätzen an, weisen Sie sie zu, oder bearbeiten Sie sie. Navigieren Sie durch Datensätze und zugehörige Listen, um Lösungen, Bereitstellungsmetriken und zu behandelnde Elemente anzuzeigen.

Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer (sn_vul.Remediation_owner)

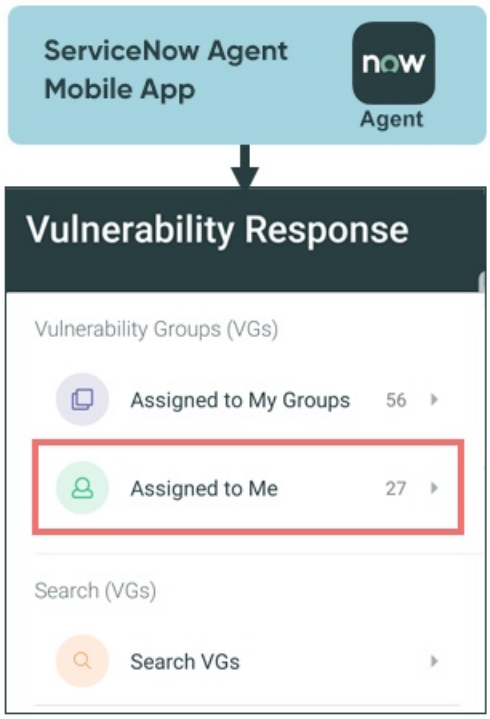
Warum und wann dieser Vorgang ausgeführt wird

Weisen Sie die Ihnen zugewiesenen Datensätze neu zu, oder bearbeiten Sie sie. Zeigen Sie die Details aktiver Korrekturaufgaben-Datensätze, Datensätze für angreifbare Elemente (VIS), Schwachstellen und Lösungen an, bevor Sie sie bearbeiten, zuweisen oder korrigieren. Zeit bis zum Abschluss dieser Aufgabe: 5-10 Minuten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

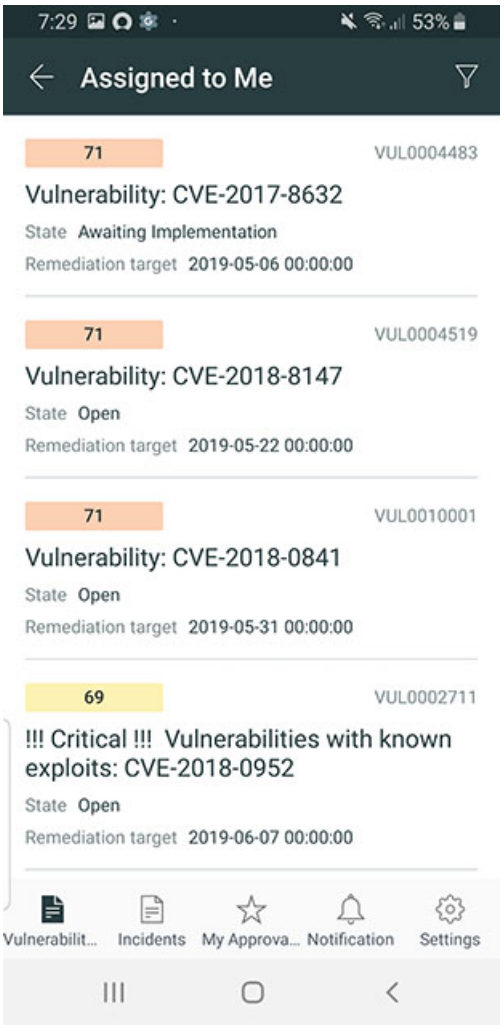
Prozedur

1. Wenn Sie nicht bei angemeldet sind ServiceNow AI Platform Instanz auf Ihrem Mobilgerät. Weitere Informationen finden Sie unter Melden Sie sich bei an Vulnerability Response Mobile-App.
2. Mit **Vulnerability Response** Zielbildschirm angezeigt, tippen Sie auf **Mir zugewiesen** .
   Wenn Sie weg von navigieren Vulnerability Response Mobile-App Nachdem Sie sich angemeldet haben, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



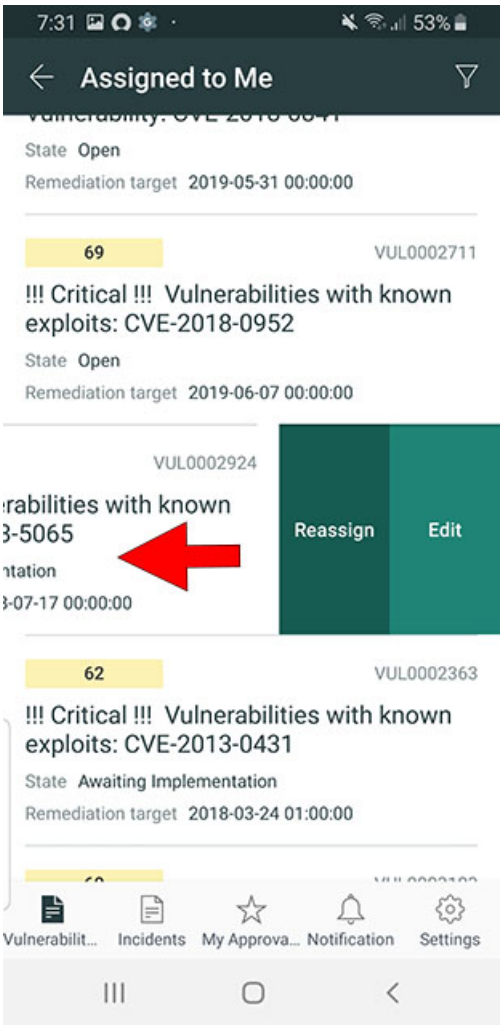
Die Liste der Datensätze der Korrekturaufgabe, die Ihnen zugewiesen sind, wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. **Wahlweise:** Siehe Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App Um nach Datensätzen zu suchen, die bestimmten Kriterien entsprechen.
4. Alternativ mit dem Filtersymbol ( ) Angezeigt, Legen Sie Filter fest, um die Anzahl der Datensätze zu begrenzen In der Liste.
   Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator im ServiceNow AI Platform.
5. Um den Datensatz direkt aus der Liste neu zuzuweisen oder zu bearbeiten, wobei der Bildschirm mir zugewiesen angezeigt wird, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.

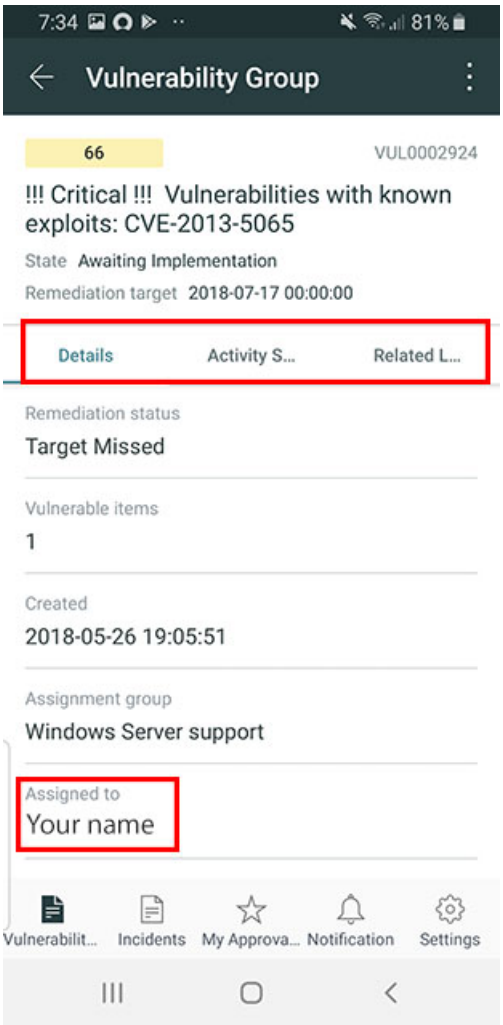
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie eine, um fortzufahren.

7. Alternativ können Sie auf einen Datensatz in der Liste tippen, um die Details eines offenen Datensatzes anzuzeigen und weitere zugehörige Datensätze und zugehörige Listen anzuzeigen, wobei der Bildschirm mir zugewiesen angezeigt wird.
8. Wählen Sie im angezeigten Datensatz der offenen Korrekturaufgabe eine Option aus der folgenden Tabelle aus, um Arbeitsnotizen oder zugehörige Listen anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die folgende Abbildung zeigt den Navigationspfad vom Korrekturaufgabendatensatz zum bevorzugten Lösungsdatensatz für die ausgewählte Schwachstelle. Navigieren Sie durch die Datensätze und zugehörigen Listen, um Lösungen, Bereitstellungsmetriken und zu behandelnde Elemente anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigationspfad von RT durch einen Lösungsdatensatz

9. Wählen Sie eine, um fortzufahren.

Automatische Übersetzung

Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App

Suchen Sie nach Korrekturaufgaben, die bestimmten von Ihnen ausgewählten Suchkriterien entsprechen.

Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer (sn_vul.Remediation_owner)

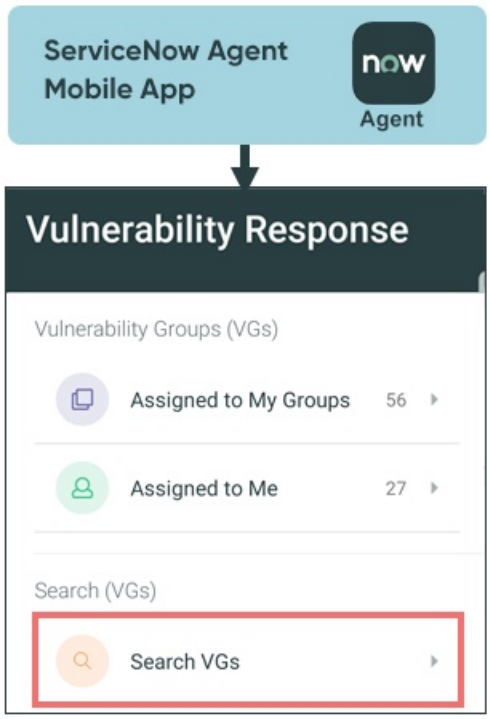
Warum und wann dieser Vorgang ausgeführt wird

Zeit bis zum Abschluss dieser Aufgabe: 5-7 Minuten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn Sie nicht bei angemeldet sind ServiceNow AI Platform Instanz auf Ihrem Mobilgerät. Weitere Informationen finden Sie unter Melden Sie sich bei an Vulnerability Response Mobile-App.
2. Mit **Vulnerability Response** Zielbildschirm angezeigt, tippen Sie auf **RTS durchsuchen** .
   Wenn Sie weg von navigieren Vulnerability Response Mobile-App Nachdem Sie sich angemeldet haben, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



3. Tippen Sie im angezeigten Suchbildschirm auf die Felder, und füllen Sie das Formular mit den gewünschten Suchkriterien aus.

   Befolgen Sie die Anweisungen nach der Tabelle, um Suchkriterien zu bearbeiten, Suchkriterien zu löschen oder eine Suche zu übermitteln.

Tippen Sie auf dieses Feld	Zum Hinzufügen eines Eintrags zu Android Geräte	Zum Hinzufügen eines Eintrags zu iOS Geräte
Anzahl	Tippen Sie auf den Bildschirm, und geben Sie eine RT-Nummer ein, z. B. (VUL0002372). Diese Zahl wird oben rechts im RT-Datensatz angezeigt. Tippen Sie auf das Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm RTS durchsuchen zurückzukehren. Tippen Sie auf das Schließen-Symbol (X), um Ihre Eingabe abzubrechen und zum Feld RTS durchsuchen zurückzukehren.	Geben Sie eine RT-Nummer ein, z. B. (VUL0002372). Diese Zahl wird oben rechts im RT-Datensatz angezeigt. Tippen Sie Auf **Fertig** Um zum Bildschirm „RTS durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen** Um den Eintrag zu löschen und zum Bildschirm „RTS durchsuchen“ zurückzukehren.
Risikobewertung	Tippen Sie auf ein oder mehrere Elemente gefolgt vom Häkchen-Symbol,	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tippen Sie auf dieses Feld	Zum Hinzufügen eines Eintrags zu Android Geräte	Zum Hinzufügen eines Eintrags zu iOS Geräte
	um Ihren Eintrag hinzuzufügen und den RTS-Bildschirm für die Suche zurückzugeben. Tippen Sie auf das Schließen-Symbol (X), um Ihre Eingabe abzubrechen und zum Feld RTS durchsuchen zurückzukehren.	oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie Auf **Fertig** Um zum Bildschirm „RTS durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen** Um den Eintrag zu löschen und zum Bildschirm „RTS durchsuchen“ zurückzukehren.
Korrekturstatus	Tippen Sie auf ein oder mehrere Elemente gefolgt vom Häkchen-Symbol, um Ihren Eintrag hinzuzufügen und den RTS-Bildschirm für die Suche zurückzugeben. Tippen Sie auf das Schließen-Symbol (X), um Ihre Eingabe abzubrechen und zum Feld RTS durchsuchen zurückzukehren.	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie Auf **Fertig** Um zum Bildschirm „RTS durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen** Um den Eintrag zu löschen und zum Bildschirm „RTS durchsuchen“ zurückzukehren.
Status	Tippen Sie auf ein oder mehrere Elemente gefolgt vom Häkchen-Symbol, um Ihren Eintrag hinzuzufügen und den RTS-Bildschirm für die Suche zurückzugeben. Tippen Sie auf das Schließen-Symbol (X), um Ihre Eingabe abzubrechen und zum Feld RTS durchsuchen zurückzukehren.	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie Auf **Fertig** Um zum Bildschirm „RTS durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen** Um den Eintrag zu löschen und zum Bildschirm „RTS durchsuchen“ zurückzukehren.
Grund	Tippen Sie auf ein oder mehrere Elemente gefolgt vom Häkchen-Symbol, um Ihren Eintrag hinzuzufügen und den RTS-Bildschirm für die Suche zurückzugeben. Tippen Sie auf das Schließen-Symbol (X), um Ihre Eingabe abzubrechen und zum Feld RTS durchsuchen zurückzukehren.	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie Auf **Fertig** Um zum Bildschirm „RTS durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen** Um den Eintrag zu löschen und zum Bildschirm „RTS durchsuchen“ zurückzukehren.
Zuweisungsgruppe	Wählen Sie einen aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein.	Wählen Sie einen aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tippen Sie auf dieses Feld	Zum Hinzufügen eines Eintrags zu Android Geräte	Zum Hinzufügen eines Eintrags zu iOS Geräte
	Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie für keinen Eintrag aus **Keine** .	Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie für keinen Eintrag aus **Keine** .
Zugewiesen an	Wählen Sie einen aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie für keinen Eintrag aus **Keine** .	Wählen Sie einen aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie für keinen Eintrag aus **Keine** .
Kurzbeschreibung	Tippen Sie auf den Bildschirm, und geben Sie Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalter (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie auf das Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm RTS durchsuchen zurückzukehren.	Geben Sie auf dem Bildschirm Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalter (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie Auf **Fertig** Um zum Bildschirm „RTS durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen** Um den Eintrag zu löschen und zum Bildschirm „RTS durchsuchen“ zurückzukehren.
Beschreibung	Tippen Sie auf den Bildschirm, und geben Sie Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalter (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie auf das Häkchensymbol, um Ihren Eintrag hinzuzufügen und zum Bildschirm RTS durchsuchen zurückzukehren.	Geben Sie auf dem Bildschirm Text ein. Die Funktion erkennt Textzeichenfolgen und Teiltextzeichenfolgen in diesem Feld, Platzhalter (*) werden jedoch nicht akzeptiert. Großbuchstaben sind nicht erforderlich. Tippen Sie Auf **Fertig** Um zum Bildschirm „RTS durchsuchen“ zurückzukehren. Tippen Sie im erweiterten Feld auf **Abbrechen** Um den Eintrag zu löschen und zum Bildschirm „RTS durchsuchen“ zurückzukehren.

Für Android Wählen Sie eines aus, um fortzufahren, wenn der Bildschirm „RTS durchsuchen“ angezeigt und alle Ihre Kriterien eingegeben werden.

4. Für iOS Wählen Sie eines aus, wenn der Bildschirm „RTS durchsuchen“ angezeigt wird, um fortzufahren.

5. **Wahlweise:** Wenn Ihre Suche mehrere Datensätze zurückgibt, können Sie dies tun Datensätze mit filtern Vulnerability Response Mobile-App Zum Verfeinern der Suchergebnisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensätze mit filtern Vulnerability Response Mobile-App

Legen Sie zusätzliche Filter fest, um die Anzahl der Datensätze zu begrenzen, die in einem Bildschirm angezeigt werden. Das Filtern von Datensätzen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der ServiceNow AI Platform.

Vorbereitungen
Erforderliche Rolle: Korrekturbesitzer (sn_vul.Remediation_owner)

Warum und wann dieser Vorgang ausgeführt wird
Zeit bis zum Abschluss dieser Aufgabe: 5 Minuten.

Prozedur

1. Um Ihre Suchergebnisse weiter zu verfeinern oder zusätzliche Filterkriterien in einer angezeigten Liste von Datensätzen einzugeben, tippen Sie auf das Filtersymbol ( ).
2. Wenn der Bildschirm Filter angezeigt wird, tippen Sie auf ein Feld, um es zu erweitern.
   Ein allgemeines Feld zum Eingeben von Suchkriterien für Korrekturaufgabendatensätze ist das Feld Status.
3. Tippen Sie in den angezeigten Optionen auf das Kontrollkästchen, oder tippen Sie auf ein Element für Ihren Filter.
   Für viele der Filter können Sie mehr als eine Option auswählen.
4. Tippen Sie auf das zurück-Symbol (Back) Oder **FERTIG** Um Ihre Änderungen in einem Feld zu speichern.
   Die von Ihnen ausgewählten Kriterien werden auf dem Bildschirm Filter angezeigt. Die Anzahl der Datensätze, die Ihren Kriterien entsprechen, wird ebenfalls oben im Bildschirm angezeigt. Tippen Sie Auf **ZURÜCKSETZEN** Um Filter zu entfernen und die Standardeinstellung wiederherzustellen.
5. **Wahlweise:** Wiederholen Sie die Schritte 1 bis 4 mit dem Bildschirm „Filter“, um mit der Festlegung Ihrer Filterkriterien fortzufahren.
6. Tippen Sie auf das Schnittungssymbol ( ) Zum Erstellen von UND-Bedingungen.
7. Tippen Sie alternativ auf das Schnittungssymbol ( ) Zum Erstellen von ODER-Bedingungen.
8. Nachdem Sie alle gewünschten Kriterien hinzugefügt haben, und der Bildschirm Filter angezeigt wird, tippen Sie auf **FERTIG** .
   Auf dem Bildschirm werden nur die Datensätze angezeigt, die Ihren Filterkriterien entsprechen.

Zugehörige Informationen

Suchen Sie mit nach Korrekturaufgaben Vulnerability Response Mobile-App

Vulnerability Response Orchestration

Mit Vulnerability Response Orchestration Workflows und Aktivitäten, mit denen Sie mithilfe der Workflow-Orchestration interagieren und Daten aus Windows- oder UNIX-basierten Systemen und Umgebungen abrufen können. Durch Anreicherung von Daten können Sie den Korrekturlebenszyklus verkürzen.

Weitere Informationen zum Bearbeiten von Workflows oder zum Erstellen anwenderdefinierter Workflows finden Sie unter Exploring flows .

Scan-Schwachstellen-Workflow

Die zugehörigen Listen namens **Vulnerability Response** > **Schwachstelle Scannen** Workflow scannt eine Korrekturaufgabe erneut.

Vorbereitungen
Erforderliche Rolle: keine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

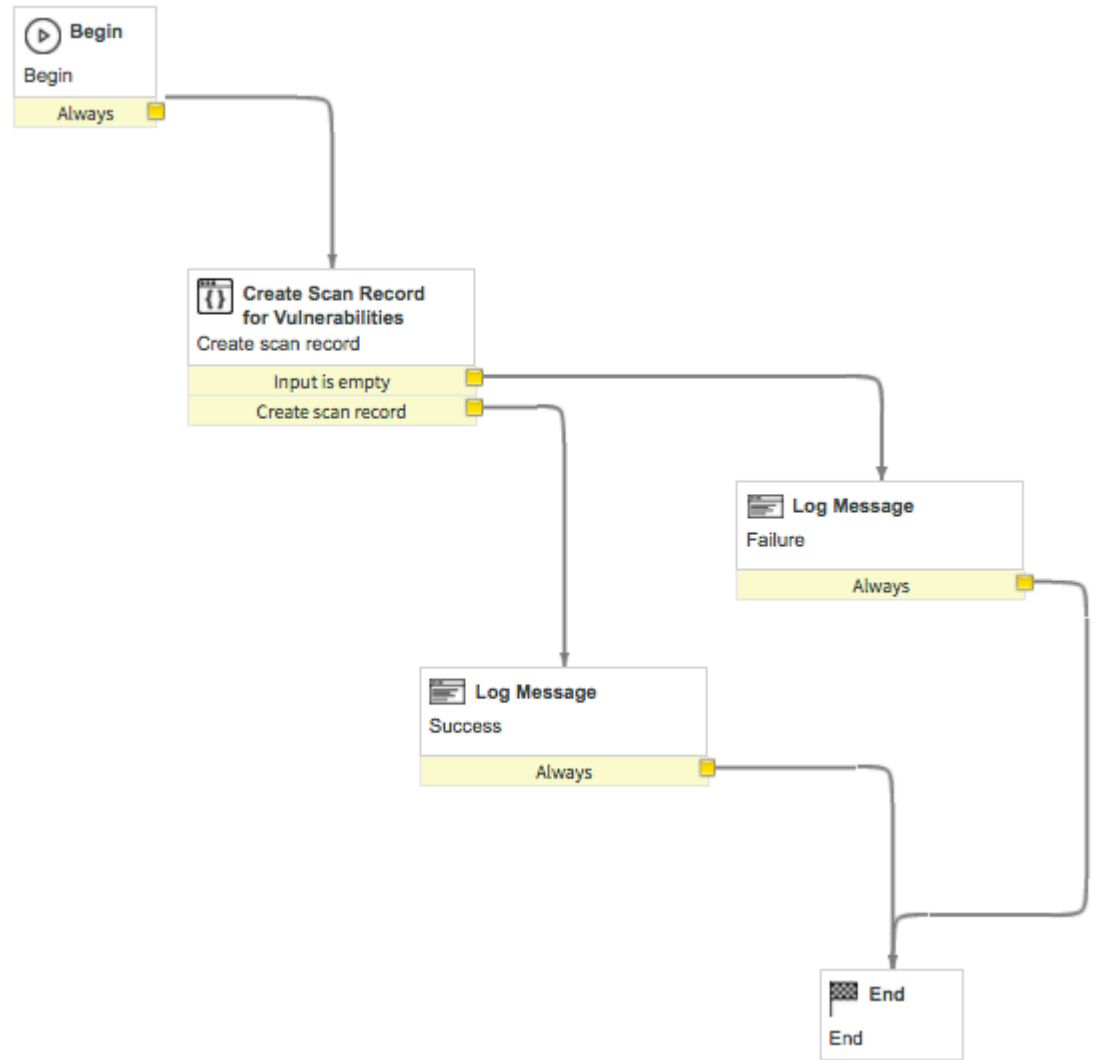
Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow wird durch ausgelöst **Angreifbare Gruppe erneut scannen** Während eines **Schließen/Ignorieren** Aktion.

Workflow-Prozessaktivitäten umfassen:

Variablen für Aktivität „Scan-Datensatz für Schwachstellen erstellen“

Protokollnachricht

Scan-Schwachstellen-Workflow



Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben**an.
2. Öffnen Sie einen Aufgabendatensatz (VUL).
3. Klicken Sie auf **Schließen**.
4. Wählen Sie Aus **Geschlossen** Für **Gewünschter Status** .
5. Wählen Sie Aus **Behoben** Für **Substatus** .
6. Wählen Sie Aus **Warten Sie auf die Bestätigung des nächsten Scans** Für **Jetzt schließen?**
   Für die Korrekturaufgabe und angreifbare Elemente, die **Status** Ändert sich in **Bestätigung Ausstehend** , **Substatus** Ändert sich in **Behoben** , Und ein erneutes Scannen wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Scan-Workflow für Schwachstellenelement

Die zugehörigen Listen namens**Angreifbare Antwort** > **Schwachstellenelement Scannen** Workflow scannt ein angreifbares Element erneut.

Vorbereitungen

Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird

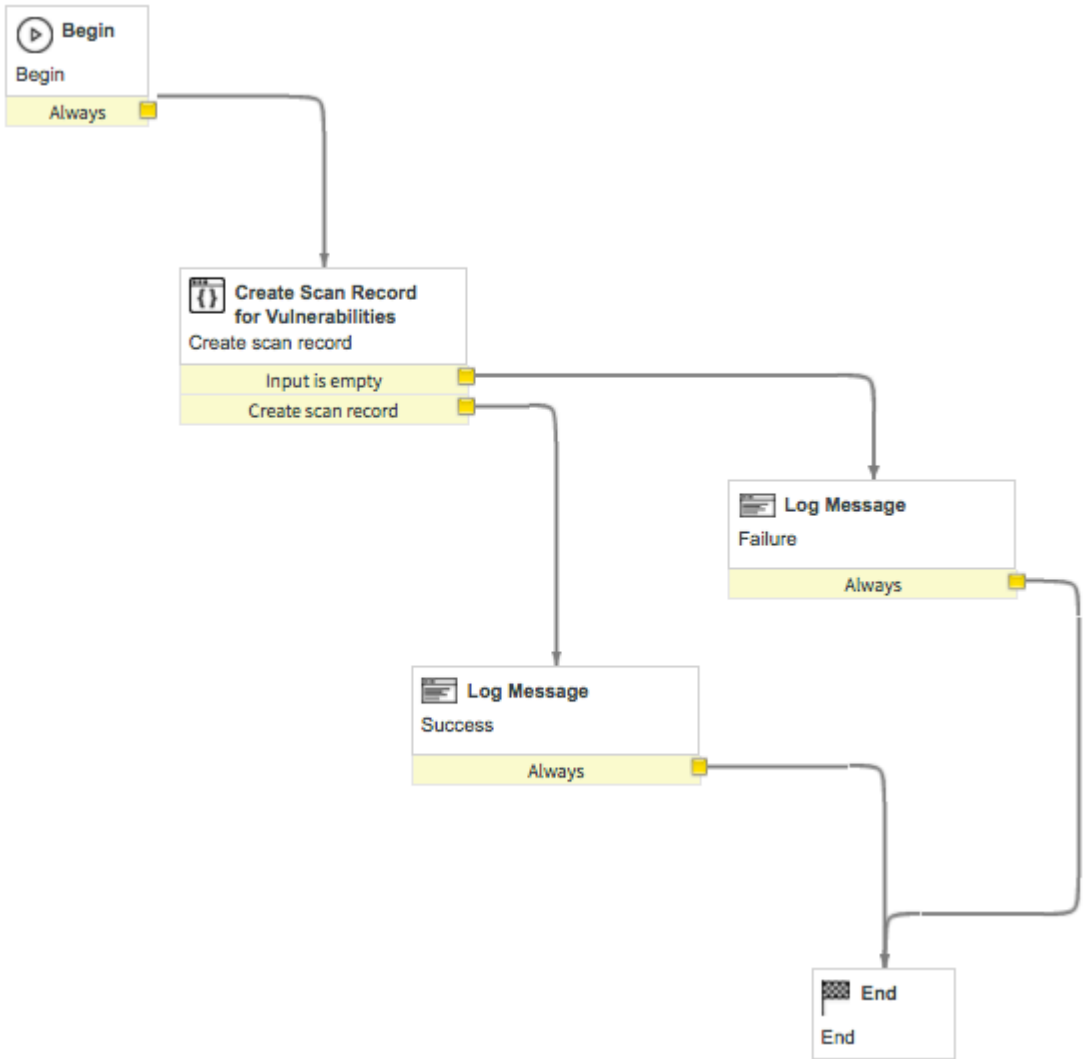
Dieser Workflow wird durch ausgelöst **Schwachstelle erneut scannen** , Während eines **Schließen/Ignorieren** Aktion.

Workflow-Prozessaktivitäten umfassen:

Variablen für Aktivität „Scan-Datensatz für Schwachstellen erstellen“

Protokollnachricht

Scan-Schwachstellen-Workflow



Prozedur

1. Navigieren zu **Schwachstelle** > **Schwachstellen** > **Angreifbare Elemente**an.
2. Öffnen Sie ein Schwachstellenelement.
3. Klicken Sie Auf **Schließen/Ignorieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

4. Wählen Sie Aus **Geschlossen** Für **Gewünschter Status** .
5. Wählen Sie Aus **Behoben** Für **Substatus** .
   Die **Status** Der Gruppe ändert sich in **Bestätigung Ausstehend** , **Substatus** Ändert sich in **Behoben** , Und ein erneutes Scannen wird ausgeführt.

Variablen für Aktivität „Scan-Datensatz für Schwachstellen erstellen“

Schwachstellen-Scans für einzelne oder mehrere angreifbare Elemente können mit ausgeführt werden **Erstellen Sie einen Scan-Datensatz für Schwachstellen** Im Basissystem enthaltene Workflow-Aktivität. Wenn die Eingabe an die Aktivität übergeben wird, wird ein Scan-Datensatz erstellt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Taskids [Zeichenfolge]	Eine Zeichenfolge von kommagetrennten sysIds, die die erwarteten Eingaben definieren. Dieses Feld ist ein Pflichtfeld.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
ScanResult [Boolesch]	Gibt „wahr“ zurück, wenn die Eingabe nicht leer ist. Für die taskIds wird ein Scan-Datensatz erstellt.

Application Vulnerability Response

Die Application Vulnerability Response(AVR)-Funktion von ServiceNow® Vulnerability Response Anwendung importiert angreifbare Anwendungselemente (AVITs) und ermöglicht Ihnen gemäß Regeln die Behebung von Anwendungsschwachstellen. Vulnerability Response Ist als separates Abonnement verfügbar.

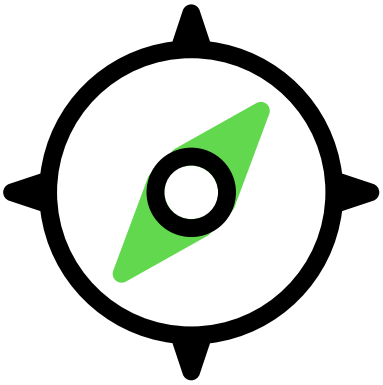
Ab AVR v19.0 wurden einige Schlüsseltabellen- und Spaltennamen aktualisiert. Daher werden in der Dokumentation Verweise auf die älteren und neueren Namen angezeigt. Eine vollständige Liste der aktualisierten Begriffe finden Sie unter Application Vulnerability Response-Produktübersicht.

Ab v19.0 von Vulnerability Response, Sie können Schwachstellendaten für Software Composition Analysis (SCA) und Software Bill of Materials (SBOM) erfassen, um Schwachstellen in Ihren Softwareanwendungen zu identifizieren. Weitere Informationen finden Sie unter Application Vulnerability Response erkunden und Veracode Vulnerability Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

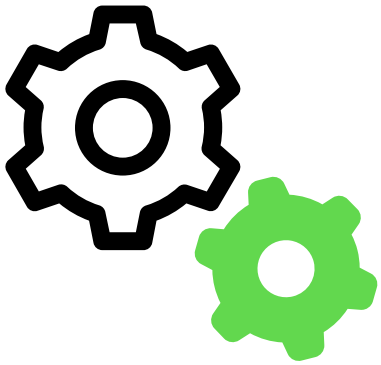
Application Vulnerability Response

Untersuchen



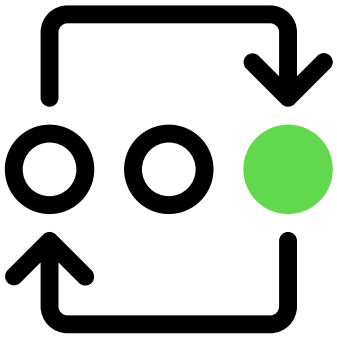
Erfahren Sie mehr über Konzepte und Funktionen von Application Vulnerability Response.

Konfigurieren



Konfigurieren Sie Application Vulnerability Response.

Integrieren

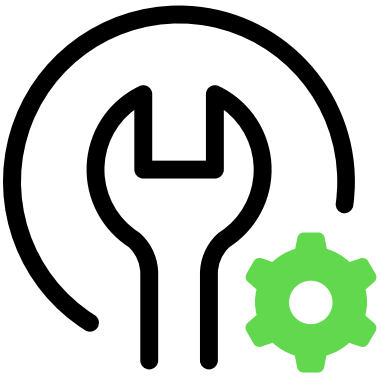


Erweitern Sie Application Vulnerability Response durch Integration mit anderen Anwendungen.

Verwenden Sie die Vulnerability Response-Arbeitsbereiche

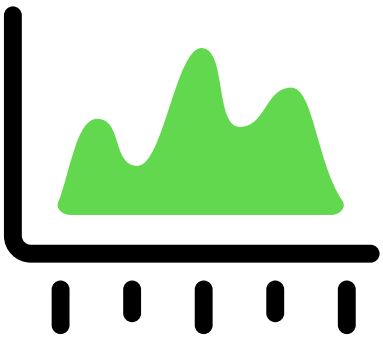
Erfahren Sie, wie Sie AVITs in den Arbeitsbereichen „Schwachstellenmanager“, „IT-Korrektur“ und „Schwachstellenbewertung“ überwachen, verwalten und beheben.

Beheben



Erfahren Sie, wie Sie Anwendungsschwachstellen beheben können.

Analytics Und Reporting



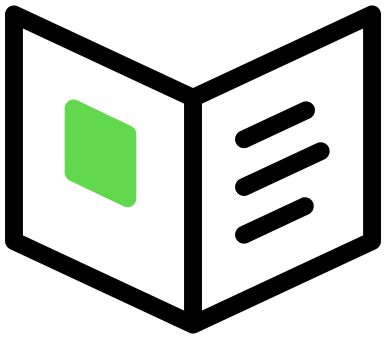
Zeigen Sie Analytics von Application Vulnerability Response an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Application Vulnerability Response (Fortsetzung)

Referenz



Rufen Sie Details zu Application Vulnerability Response-Komponenten wie Feldern, Tabellen und Eigenschaften ab.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Application Vulnerability Response erkunden

Anwendungsschwachstellen sind Schwachstellen in Ihren anwenderdefinierten Softwareanwendungen, die während des gesamten Entwicklungslebenszyklus der Anwendung gescannt werden.

Übersicht über Application Vulnerability Response Und verfügbare Versionen

Application Vulnerability Response(AVR) ist Teil von Vulnerability Response Anwendung, die Anwendungsschwachstellen verarbeitet.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response V23.0 Vulnerability Response V22.0 Vulnerability Response V21.0	Application Vulnerability Response release notes Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Versionen (Fortsetzung)

Freigabeversion	Release-Hinweise
Vulnerability Response V20.0 Vulnerability Response V19.0 Vulnerability Response V18.2	Kompatibilitätsmatrix und Änderungen am Release-Schema

Funktionsweise

Schwachstellendaten werden aus internen und externen Quellen importiert, z. B. der Common Weekness Enumeration (CWE) oder Integrationen von Drittparteien. Nachdem Daten importiert wurden, werden sie mit Anwendungsdaten in verglichen Configuration Management Database (CMDB) Und in verarbeitet Application Vulnerability Response Anwendung. Wenn zwischen importierten Anwendungsschwachstellendaten und Daten in Ihrer CMDB eine Übereinstimmung besteht, wird ein angreifbares Anwendungselement (AVIT) erstellt.

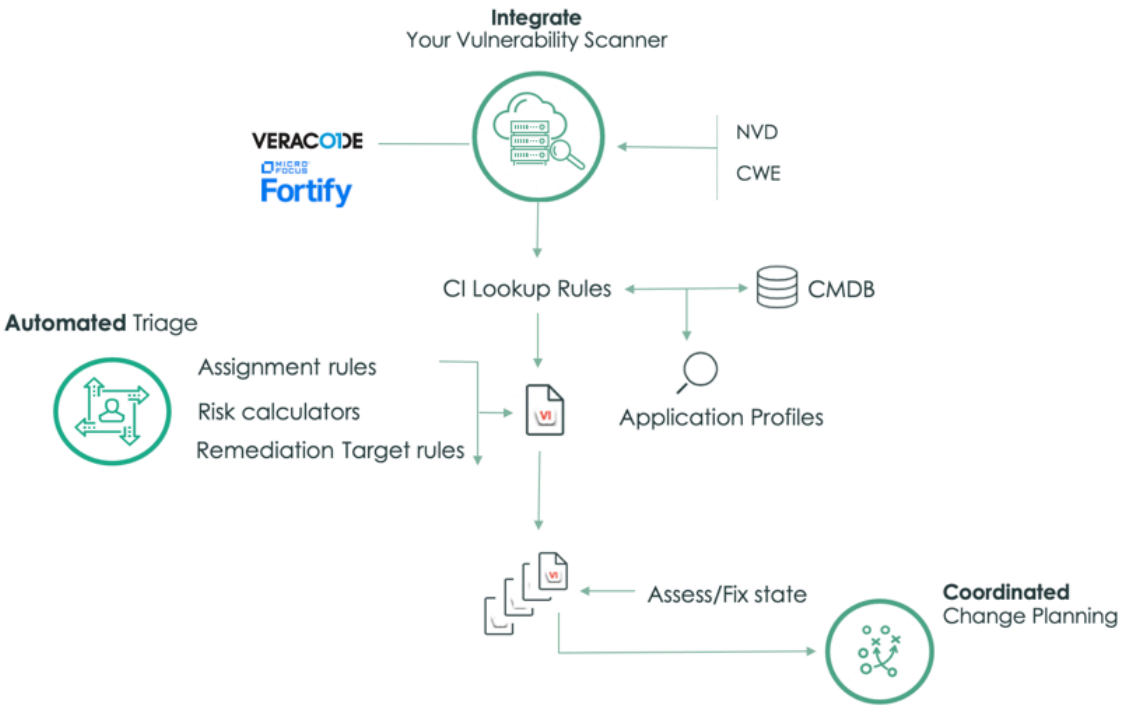
Die Application Vulnerability Response Enthält die folgenden wichtigen Funktionen:

- Integrieren Sie sie mit unterstützten Drittanbieterscannern, um Schwachstellendaten zu importieren.
- Vergleichen Sie Daten im Zusammenhang mit Anwendungsschwachstellen, und bestimmen Sie, ob Anwendungsschwachstellen in einer Anwendung gefunden werden.
- Priorisieren, korrigieren und verwalten Sie angreifbare Anwendungselemente (AVIT) Jede Anwendungsschwachstelle stellt einen Schwachstelleneintrag in der CWE- oder Drittparteibibliotheken dar.
- Ab Version 18,0 von Vulnerability Response, Sie können AVITs in überwachen und korrigieren Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen Entsprechend. Weitere Informationen finden Sie unter Arbeitsbereich des Schwachstellenmanagers und Arbeitsbereich für IT-Korrekturen.
- Korrelieren Application Vulnerability Response Daten mit Rechnern und Bibliotheken, die Sie bei der Ausführung der folgenden Aufgaben unterstützen.
  - Erstellen Sie angreifbare Anwendungselemente automatisch mit **CI-Suchregeln** . Während des Imports werden Schwachstellen von Drittanbietern einer CWE zugeordnet, um eine AVIT zu erstellen.
  - Erstellen Sie Zuweisungsregeln, um Zuweisungen angreifbarer Anwendungselemente zu automatisieren.
  - Verwenden Sie Rechnergruppen, um die Geschäftsauswirkung zu bestimmen, unterschiedliche Bedingungen mithilfe von Filtern anzugeben, einfache Berechnungen anzuwenden oder ein Skript zu verwenden.
  - Erstellen Sie Korrekturzielregeln, die den erwarteten Zeitrahmen für die Korrektur angreifbarer Anwendungselemente definieren, damit Sie bevorstehende Korrekturaktivitäten überwachen können.
- Verknüpfen Sie eine einzelne Schwachstelle einer Drittpartei mit mehreren CWE-Einträgen, und suchen Sie die primäre CWE für eine Schwachstelle, um Sie bei der Bestimmung des Risikos zu unterstützen. Weitere Informationen zu finden **Primäre CWE** , Siehe Anwendungsschwachstellen-Felder.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwenden Sie CWE-Datensätze, die aus der CWE-Datenbank heruntergeladen oder aus Drittanbieterintegrationen importiert werden, als Referenz, um zu entscheiden, ob Sie eine Schwachstelle eskalieren müssen. Jeder CWE-Datensatz enthält auch einen zugehörigen wissensartikel, der die Schwachstelle beschreibt.

Verwenden Application Vulnerability Response Um den Informationsfluss von der Integration über die Untersuchung und dann bis zur Lösung zu verfolgen.



Typen importierter Schwachstellendaten

Application Vulnerability Response Unterstützt die folgenden Typen importierter Anwendungsschwachstellendaten.

Hinweis:
Vor v19.0 wurden SAST-, SCA-, IAST- und Penetrationstestdaten nicht erfasst und können Unterschiede zwischen den darin angezeigten Elementen berücksichtigen Veracode, Fortify, Und Invicti Und was in angezeigt wird Application Vulnerability Response.

Dynamische Anwendungssicherheitstests (DAST)

DAST-Scans finden die Anwendung „Schwachstellen“, indem Eingaben an Ihre Anwendungen gesendet und deren Antworten überwacht werden, während sie ausgeführt werden. Dieser Ansatz könnte einen externen Angriff imitieren. Während des dynamischen Scans wird ein laufender Service (URL) auf Schwachstellen gescannt. Schwachstellenergebnisse enthalten einen URL-Speicherort einer erkannten Schwachstelle.

Statische Anwendungssicherheitstests (SAST)

SAST-Scans überprüfen den Quellcode von Anwendungen im Ruhezustand und helfen Ihnen, Schwachstellen in der Art und Weise zu finden, wie Sie Ihren Code geschrieben haben. Der SAST-Scan erfolgt für nicht kompilierten Quellcode und ist daher unabhängig von jedem Anwendungsservice vorhanden. Die zurückgegebenen Ergebnisse enthalten einen Datei- und Zeilennummernspeicherort einer erkannten Schwachstelle.

Interaktive Anwendungssicherheitstests (IAST)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IAST-Scans erkennen Softwareschwachstellen, indem sie während der Ausführung mit dem Programm interagieren. Menschliche Beobachtung, automatisierte Tests und Sensoren werden in Kombination verwendet, um mit der Anwendung zu interagieren, um Schwachstellen zu lokalisieren.

Software Composition Analysis (SCA)

Ab v19.0 von Vulnerability Response, Sie können Schwachstellen der Software Composition Analysis (SCA) erfassen. SCA-Schwachstellendaten, mit denen Sie Schwachstellen in der Open Source-Software identifizieren können, die in Ihren Softwareanwendungen verwendet wird.

Penetrationstests

Sie konfigurieren Penetrationstestbewertungsanforderungen in Application Vulnerability Response Damit Sie verstehen, wo sich Ihre Anwendungsschwachstellen befinden und wie Sie sie beheben können.

Software-Stückliste

Hochladen Software Bill of Materials(SBOM) Daten zur Identifizierung von Schwachstellen in Ihren Open Source-Komponenten. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Anwendungsfälle

Einige der folgenden DAST-Anwendungsfälle werden unterstützt:

- Verknüpfen Sie jede Schwachstelle aus Scan-Ergebnissen mit einer Art von cmdb_ci (untergeordnete Klasse).
- Verknüpfen Sie DAST-Scan-Ergebnisse mit einer vorhandenen Anwendung, wenn ein Datensatz in vorhanden ist CMDB Von Discovery Oder eine Drittpartei-Integration.
- Verknüpfen Sie das DAST-Scanergebnis mit einer neu eingefügten gescannten Anwendung, wenn zuvor keine neue Anwendung identifiziert und/oder in der CMDB gespeichert wurde.
- Speichern Sie DAST-Scan-Ergebnisse für eine CMDB, wenn Sie Ihre Anwendungen in einem anderen Produkt als verwalten ServiceNow®.
- Speichern Sie DAST-Scan-Ergebnisse für eine CMDB, wenn Sie zuvor für einen anderen Zweck angepasst haben.
- Erstellen Sie manuell eine Anwendung für das Quellcode-Repository.

Einige der unterstützten SAST-Anwendungsfälle werden unterstützt:

- Verknüpfen Sie jede Schwachstelle aus Scan-Ergebnissen mit einer Art von cmdb_ci (untergeordnete Klasse).
- Erstellen Sie manuell ein CI für das Quellcode-Repository.
- Speichern Sie SAST-Scan-Ergebnisse, die ohne zugehörigen Anwendungsservice sind.

[store-future: BEGIN review]Einige der folgenden IAST-Anwendungsfälle werden unterstützt:[End]

[store-future: BEGIN review]Einige der unterstützten SCA-Verwendungen werden unterstützt:[End]

Drittpartei-Integrationen

Die von unterstützten Drittpartei-Integrationen Application Vulnerability Response Sind als separate Anwendungen in verfügbar ServiceNow Store. Weitere Informationen finden Sie unter Integration von Application Vulnerability Response mit anderen Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselfunktionen

- Eine freigegebene API importiert DAST, SAST, IAST , Und SCA-Daten und Ergebnisse manueller Pen-Tests. Weitere Informationen finden Sie unter Penetrationstests.
- Eine separate API wird zum Importieren von SBOM-Daten verwendet. Weitere Informationen finden Sie unter Software Bill of Materials erkunden und Veracode Vulnerability Integration.

CI-Suchregeln

Anwendungsdaten automatisch nach Übereinstimmungen in durchsuchen Configuration Management Database (CMDB).

Zuweisungsregeln

Weisen Sie Anwendungsschwachstellen automatisch basierend auf Anwendergruppen, Anwendergruppenfeldern und Skripts zu.

Risikorechner

Priorisieren und bewerten Sie die Auswirkungen von AVITs automatisch mithilfe von Rechnern basierend auf beliebigen Kriterien mithilfe von Bedingungsfiltern.

Schweregradzuordnung

Berechnen Sie automatisch Anfangswerte für Felder in angreifbaren Anwendungselementen. Schwachstelleneinträge haben sowohl den Quellschweregrad als auch den normalisierten Schweregrad (basierend auf der Schweregradzuordnung). Der Schweregrad ist an die Common Sarkness Enumeration (CWE) gebunden.

Korrekturzielregeln

Definieren Sie den erwarteten Zeitrahmen für die Korrektur eines angreifbaren Anwendungselements.

Bericht

Erhalten Sie mit den kritischsten AVITs schnell Einblicke in Ihre Sicherheitslage, Korrekturtrends und Top-10-Anwendungen oder Geschäftsbereiche.

Der gemeinsame Punkt für beide Arten von Scans ist das Anwendungsrelease. Ein Anwendungs-Release, das einen definiert **Name** Zeichenfolge, ist der Bindepunkt zum Gruppieren gescannter Schwachstellenergebnisse auf der Scannerseite. Auf diese Weise weiß AVR, zu welchem Anwendungsrelease die Ergebnisse gehören, wenn Scan-Ergebnisse über die Integration importiert werden.

Eine untergeordnete Tabelle für Konfigurationselement [cmdb_ci], gescannte Anwendungen [sn_vul_App_Scanned_Application], wurde in erstellt Vulnerability Response Anwendung und Umfang. Diese Tabelle speichert die Anwendungsrelease-Abstraktion und bietet Servicediagrammerstellung über ihre CMDB-Beziehungen. Sie können über angezeigt werden **Alle** > **Application Vulnerability Response** > **Administration** > **Anwendungen** Modul. Die Listenansicht für gescannte Anwendungen enthält **Abteilung** Und **Supportgruppe** Während des Setups hinzugefügt.

Angreifbare Anwendungselemente (AVITs)

Bei Anwendungsschwachstellen bezieht AVR eine Schwachstelle mit einer Anwendung, um den Datensatz für angreifbare Anwendungselemente (AVIT) zu erstellen. Aufgrund der mehreren Definitionen dessen, was eine Anwendung in der CMDB ausmacht, Application Vulnerability Response Beschränkt Anwendungen auf gescannte Anwendungen. Gescannte Anwendungen sind die in Ihrer Umgebung gescannten Anwendungen, die von AVR als identifiziert werden **Name** Und **ID** . AVITs basieren bis zur Bestätigung auf der neuesten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Scan-Zusammenfassung **Behoben** Durch den Scanner. Wenn ein AVIT nicht mehr gefunden wird, bleibt er an die Scan-Zusammenfassung gebunden, in der er zuletzt gesehen wurde.

Angreifbare Anwendungselemente können über angezeigt werden **Alle** > **Application Vulnerability Response** > **Schwachstellen** > **Angreifbare Elemente** Modul.

Wenn eine Anwendung aus der CMDB entfernt wird, werden alle zugehörigen AVITs geschlossen.

Informationen zu AVIT-Formularfeldern finden Sie unter Felder für angreifbares Anwendungselement.

Anwendergruppen und -Rollen in Application Vulnerability Response

Oft arbeitet ein Team zusammen, um Anwendungsschwachstellen zu erstellen, zu verwalten und zu verwalten. Unter den Teammitgliedern gibt es strategische Rollen sowie operative Rollen. In den meisten Organisationen können Sie an mehr als einer Rolle teilnehmen und Rollen häufig mit anderen teilen. Application Vulnerability Response Verwendet drei Anwendergruppen mit granularen Rollen: App-Sec Manager, Application Security Champion und Developer. Siehe Application Vulnerability Response Anwendergruppen und Rollen Um weitere Informationen zu diesen Gruppen und Rollen zu erhalten.

Application Vulnerability Response status

Application Vulnerability Response Bietet ein Statusmodell für den Status Ihrer angreifbaren Anwendungselemente (AVITs) und hilft Ihnen, zu bestimmen, wann und wie Ihre AVITs korrigiert werden sollen.

Ein angreifbares Anwendungselement hat mehrere mögliche status, siehe status des angreifbaren Anwendungselements (AVI) Weitere Informationen finden Sie unter .

Vulnerability Response Anwendungen Und CSDM Tabellen

Die Vulnerability Response, Application Vulnerability Response, Integrationen von Schwachstellen von Drittparteien und Software Bill of Materials Anwendungen verwalten (Daten mittragen zu) CSDM Tabellen. Diese Anwendungen verwenden auch Daten aus CSDM Tabellen, die andere Anwendungen generieren. Mehrere ServiceNow Produkte profitieren daher von diesen und fügen ihnen einen Mehrwert hinzu Security Operations Anwendungen. Weitere Informationen finden Sie unter Vulnerability Response Anwendungen Und CSDM Tabellen.

Application Vulnerability Response konfigurieren

Bevor Sie ausführen Application Vulnerability Response In Ihrem ServiceNow AI Platform Instanz, müssen Sie sie konfigurieren.

Application Vulnerability Response konfigurieren

Führen Sie vor der Konfiguration die folgenden Setup-Schritte aus, damit Sie sicherstellen können, dass Ihre Konfiguration abgeschlossen ist.

Vorbereitungen

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Navigieren Sie zu , um zu überprüfen, ob es aktiviert ist **Abonnement-Management** >

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Abonnements In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren.
Überprüfen Sie, ob Performance Analytics for Vulnerability Response Ist installiert und aktiviert, um anzuzeigen Application Vulnerability Response Berichte.	Navigieren Sie zu , um zu überprüfen, ob es aktiviert ist **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Installieren und konfigurieren Sie Performance Analytics for Vulnerability Response[PA] Anwendung.
Überprüfen Sie, ob Veracode Vulnerability Integration Ist installiert, aktiviert und konfiguriert. (Führen Sie die Integrationen zu diesem Zeitpunkt nicht aus.)	Navigieren Sie zu , um zu überprüfen, ob es aktiviert ist **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Installieren Sie ServiceNow Vulnerability Response-Integration mit Veracode.
Version 14.0: Überprüfen Sie, ob Fortify Vulnerability Integration Ist installiert, aktiviert und konfiguriert. (Führen Sie die Integrationen zu diesem Zeitpunkt nicht aus.)	Navigieren Sie zu , um zu überprüfen, ob es aktiviert ist **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Installieren Sie ServiceNow Vulnerability Response-Integration mit Fortify Und Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integration.
Überprüfen Sie, ob die CWE 2000-Integration in ausgeführt wird Vulnerability Response.	Informationen zum Überprüfen der Integration finden Sie unter Überprüfen Sie, ob die geplante Aufgabe zum Aktualisieren von NVD-Datensätzen ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
[Optional] Überprüfen Sie, ob die NVD-Integration in ausgeführt wird Vulnerability Response.	Informationen zur Überprüfung finden Sie unter Überprüfen Sie, ob die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen ausgeführt wird.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Wenn nicht bereits zugewiesen, installiert der Anwender mit der Administratorrolle die Anwendung und weist Anwender den folgenden Anwendergruppen zu: App-SEC-Manager, Security Champion und Entwickler. Informationen zu Gruppenrollen finden Sie unter Application Vulnerability Response Anwendergruppen und Rollen. • Die App-SEC-Manager-Gruppe überwacht die Konfiguration und verifiziert die erwarteten Ergebnisse. **Hinweis:** Application Vulnerability Response Die Konfiguration ist über die Funktion des Setup-Assistenten in nicht verfügbar Vulnerability Response.

Erforderliche Rolle: App-Sec Manager-Anwendergruppe

Prozedur

1. Navigieren zu **Security Operations** > **CMDB** > **Suchregeln**an.
   Siehe Erstellen Sie eine CI-Suchregel Zum Erstellen oder Ändern von CI-Suchregeln für Ihre Umgebung.
2. Navigieren zu **Application Vulnerability Response** > **Administration**an.
3. Wählen Sie Aus **Zuweisungsregeln** .
   Siehe Erstellen oder bearbeiten Application Vulnerability Response Zuweisungsregeln Zum Erstellen oder Ändern von Anwendungszuweisungsregeln für Ihre Umgebung.
4. Wählen Sie Aus **Schwachstellenrechner** .
   Siehe Risiko in berechnen Application Vulnerability Response Automatisch Dient zum Erstellen oder Ändern von Anwendungsschwachstellen-Rechnern für Ihre Umgebung.
5. Wählen Sie Aus **Korrekturzielregeln** .
   Siehe Erstellen oder bearbeiten Sie Zielregeln für Anwendungskorrekturen Dient zum Erstellen oder Ändern von Anwendungskorrekturzielen für Ihre Umgebung.
6. Wählen Sie Aus **Normalisierte Schweregradzuordnungen** .
   Siehe Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu Dient zum Erstellen oder Ändern von Schweregradzuordnungen für Ihre Umgebung.
7. Navigieren Sie zu einer der beiden Optionen **Veracode Vulnerability Integration** > **Integrationen** oder **Fortify Vulnerability Integration** > **Integrationen**an.
8. Öffnen Sie die Integration der Veracode-Anwendungsliste oder die Fortify On Demand-Anwendungslistenintegration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wenn sie nicht bereits ausgeführt wurde, wählen Sie aus **Jetzt Ausführen** .

   Hinweis:
   Der andere Veracode Oder Fortify Integrationen sind standardmäßig inaktiv.

   Informationen zu Status der Integrationsausführung finden Sie unter Zeigen Sie an Veracode Status der Importausführung der Anwendungsschwachstellenintegration Oder Zeigen Sie an Fortify Vulnerability Integration Importausführungsstatus.

10. Nachdem die Integration der Anwendungsliste Veracode oder Fortify bei Bedarf abgeschlossen ist, navigieren Sie zu **Application Vulnerability Response** > **Administration** > **Anwendungen**an.

11. Geben Sie für jede Anwendung einen Wert für ein **Supportgruppe** (Wird von Zuweisungsregeln verwendet) und für **Abteilung** (In Berichterstellung verwendet).
    Informationen zum Aktualisieren mehrerer Einträge finden Sie unter Bearbeiten Sie mehrere Datensätze in einer Liste mit dem Listeneditor Um die Aufgabe in einem Massenvorgang abzuschließen.

    Hinweis:
    Um die automatisch aktualisierten anzuzeigen **Geschäftsbereich** , Aktualisieren Sie die Seite. Informationen zu gescannten Anwendungsformularfeldern finden Sie unter Gescannte Anwendungsfelder.

12. Kehren Sie zur Integrationsliste zurück, und aktivieren Sie die andere Veracode Oder Fortify Integrationen. Siehe Aktivieren Application Vulnerability Response Integrationen Zum Festlegen Ihrer Delta-Datenintegrationsimporte.

    Die Veracode Und Fortify Integrationen sind verkettet und werden nacheinander ausgeführt, wenn sie aktiviert sind.

13. **Wahlweise:** Navigieren zu **Application Vulnerability Response** > **Administration** > **Zuweisungsregeln**an.

    a. **Wahlweise:** Wenn Sie ausgewählt haben **Konfigurationselement: Supportgruppe** Für **Anwendergruppenfeld** Wenn Sie Ihre Zuweisungsregeln früher erstellt oder bearbeitet haben, können Sie jetzt die Werte verwenden, die Sie der Listenansicht „gescannte Anwendungen“ hinzugefügt haben. Ihre Zuweisungsregeln werden bearbeitet.

    b. Wählen Sie **Aktualisieren**.

    c. Wählen Sie in der Listenansicht Schwachstellenzuweisungsregeln die Option aus **Änderungen Anwenden** Um die Zuweisungsregeln erneut auf Ihre Avis anzuwenden.

Ergebnisse
Ihr Application Vulnerability Response Die Konfiguration ist jetzt abgeschlossen.

Nächste Maßnahme
Navigieren zu **Application Vulnerability Response** > **Übersicht** Und siehe Dashboard „Anwendungsschwachstellenmanagement“ [PA] Um Informationen zu Ihrer allgemeinen Sicherheitslage zu erhalten.

Überprüfen Sie, ob die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen ausgeführt wird

Verwenden Sie CWE-Datensätze (Common Weakness Enumeration), die aus der CWE-Datenbank heruntergeladen wurden, als Referenz, wenn Sie entscheiden, ob eine Schwachstelle eskaliert werden muss. Aktualisieren Sie regelmäßig geplante Datensätze zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

allgemeinen Schwachstellen aus der Datenbank „Allgemeine Schwachstellen-Aufzählung“. Sie können bei Bedarf auch das Standardskript aktualisieren oder eigene Skripts schreiben.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Jeder CWE-Datensatz enthält auch einen zugehörigen wissensartikel, der die Schwachstelle beschreibt.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Integrationen**an.
2. Wählen Sie aus **CWE – umfassende 2000-Integration** Geplante Aufgabe.
3. Stellen Sie sicher, dass die Checkbox **Aktiv** aktiviert ist.

Hinweis:
Die Einstellungen in diesem Formular werden von freigegeben Vulnerability Response Und Application Vulnerability Response. Das Ändern der Integrationseinstellungen erfordert Koordination mit und Fachwissen in Vulnerability Response Und ServiceNow.

4. Wenn das Kontrollkästchen aktiviert ist, sind Sie fertig.

Hinweis:
Wenn das Kontrollkästchen nicht aktiviert ist, muss diese Integration möglicherweise in konfiguriert werden Vulnerability Response. Siehe Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken Um weitere Informationen zu erhalten, bevor Sie sie auswählen.

Siehe nach Bedarf Schwachstellenbibliotheken anzeigen Um die importierten Einträge anzuzeigen.

Die **Primäre CWE** Feld enthält den CWE-Eintrag. Wenn einer Schwachstelle mehr als eine CWE zugeordnet ist, finden Sie weitere Informationen unter Anwendungsschwachstellen-Felder Informationen dazu, wie die primäre CWE bestimmt wird.

Überprüfen Sie, ob die geplante Aufgabe zum Aktualisieren von NVD-Datensätzen ausgeführt wird

Identifizieren Sie die Repositorys, die regelmäßig aktualisiert werden sollen. Sie können eine geplante Aufgabe ausführen, um die Datensätze der National Vulnerability Database (NVD) jede Nacht oder wöchentlich zu aktualisieren. Wenn er nicht bereits ausgeführt wird, können Sie den Auftrag aktivieren

Vorbereitungen

Erforderliche Rollen: App-Sec-Manager-Gruppe

Die NVD-Integration wird standardmäßig täglich montags um 00:00:00:00 als geplante Aufgabe ausgeführt.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Integrationen**an.
2. Wählen Sie aus **NIST National Vulnerability Database** Geplante Aufgabe.
3. Stellen Sie sicher, dass die Checkbox **Aktiv** aktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Einstellungen in diesem Formular werden von freigegeben Vulnerability Response Und Application Vulnerability Response. Das Ändern der Integrationseinstellungen erfordert Koordination mit und Fachwissen in Vulnerability Response Und ServiceNow.

4. Wenn das Kontrollkästchen aktiviert ist, sind Sie fertig.

Hinweis:
Wenn das Kontrollkästchen nicht aktiviert ist, muss diese Integration möglicherweise in konfiguriert werden Vulnerability Response. Siehe Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken Um weitere Informationen zu erhalten, bevor Sie sie auswählen.

Siehe nach Bedarf Schwachstellenbibliotheken anzeigen Um die importierten Einträge anzuzeigen.

Aktivieren Application Vulnerability Response Integrationen

Aktivieren Application Vulnerability Response Integrationen zum Durchführen regelmäßiger Updates.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
3. Aktivieren Sie die Checkbox **Aktiv**.
4. Wählen Sie **Aktualisieren**.
5. Wiederholen Sie den Vorgang bei Bedarf für jede Integration.
   Nach der ersten Ausführung werden die Integrationen verkettet, um Delta-Importe für nachfolgende Ausführungen durchzuführen.

Definieren Application Vulnerability Response E-Mail-Benachrichtigungen

Richten Sie E-Mail-Benachrichtigungen ein, um nützliche Informationen zu wichtigen Updates und Aktivitäten wie Genehmigung und Ablehnung falsch positiver Anforderungen zu teilen. Beim Erstellen einer E-Mail-Benachrichtigung wird angegeben, wann sie gesendet werden soll, wer sie erhält und was sie enthält.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **E-Mail-Vorlagen**an.
2. Wählen Sie **Neu**.

Detaillierte Anweisungen zum Erstellen von E-Mail-Benachrichtigungen finden Sie unter Create an email notification .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ab v21.0 von Vulnerability Response, Wenn ein Empfänger auf die Links in einer E-Mail-Benachrichtigung klickt, werden die Datensätze im geöffnet Arbeitsbereich des Schwachstellenmanagers Oder Arbeitsbereich für IT-Korrekturen Basierend auf ihrer Rolle.

- Links werden in geöffnet Arbeitsbereich des Schwachstellenmanagers Für die Anwender mit der Rolle sn_vul.App_sec_Manager .
- Links werden in geöffnet Arbeitsbereich für IT-Korrekturen Für Anwender mit Rollen: sn_vul.App_Security_Champion, Oder sn_vul.App_Developer.

Wenn der Empfänger keine der vorherigen Rollen hat, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Erstellen oder bearbeiten Sie Benachrichtigungen zu Korrekturzielen in Application Vulnerability Response

Schwachstellenadministratoren können die Korrekturzielbenachrichtigung bearbeiten oder neue hinzufügen, indem sie angeben, wann die Benachrichtigung gesendet werden soll, wer die Benachrichtigung erhält und welchen Inhalt die Benachrichtigung enthält.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Benachrichtigungen**an.
2. Wählen Sie den Benachrichtigungsdatensatz für das Korrekturziel aus, oder wählen Sie aus **Neu** .
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Create an email notification .
4. Wählen Sie Aus **Vorschau Der Benachrichtigung Anzeigen** Zum Anzeigen der Nachricht.

Ergebnisse

Ab v21.0 von Vulnerability Response, Wenn ein Empfänger auf die Links in einer E-Mail-Benachrichtigung klickt, werden die Datensätze im geöffnet Arbeitsbereich des Schwachstellenmanagers Oder Arbeitsbereich für IT-Korrekturen Basierend auf ihrer Rolle.

- Links werden in geöffnet Arbeitsbereich des Schwachstellenmanagers Für Anwender mit der Rolle: sn_vul.App_sec_Manager .
- Links werden in geöffnet Arbeitsbereich für IT-Korrekturen Für Anwender mit Rollen: sn_vul.App_Security_Champion, Oder sn_vul.App_Developer.

Wenn der Empfänger keine der vorherigen Rollen hat, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Ausnahmeverwaltung in Application Vulnerability Response

Wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Richtlinie nicht einhalten kann, können Sie eine Ausnahme anfordern. Das Ausnahmemanagement umfasst das anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Anwendungselement (AVIT), das nicht gemäß der Richtlinie korrigiert werden kann.

Einige Schwachstellen haben möglicherweise keinen Patch, eine Korrektur oder eine Lösung. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

akzeptieren, da Sie die Konsequenzen einer Nichtbeseitigung der Schwachstelle bestätigen und zustimmen.

Hinweis:

Ab v21.0 von Application Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Anwendungselement in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Anwendungselement oder die Korrekturaufgabe auf den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Lebenszyklus einer Ausnahme

Definition einer Ausnahme

Eine Ausnahme ist eine Anforderung zum Zurückstellen der Korrektur einer AVI für einen bestimmten Zeitraum. Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Ausnahme wird angefordert

Als Entwickler können Sie mit dem Ausnahmeverwaltungsprozess eine Ausnahme für ein AVI beantragen. Nachdem der Anwendungssicherheitsanalyst diese Anforderung genehmigt hat, wird AVI zu verschoben **Zurückgestellt** status.

Wichtig:
Sie können Ausnahmen für AVTIs und RTS über den Vulnerability Manager-Arbeitsbereich bzw. DEN IT-Korrekturarbeitsbereich anfordern. Weitere Informationen finden Sie unter Fordern Sie Ausnahmen für Korrekturaufgaben und -Datensätze in an Arbeitsbereich des Schwachstellenmanagers und Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen.

Ausnahmeregeln

Ab v20 können Sie Ausnahmeregeln erstellen, um vorhandene und neue angreifbare Anwendungselemente (AVI) automatisch für einen bestimmten Zeitraum aufzuschieben, wenn sie den Bedingungen der Regel entsprechen. Die Verwendung von Ausnahmeregeln zur automatischen Zurückstellung von Avis minimiert das Risiko fehlender Servicelevel-Vereinbarungen. Die Regeln können Ihnen helfen, mehrere Elemente zu verwalten, da Sie manuelle Eingriffe vermeiden. Siehe Ausnahmeregel erstellen.

Verlängerung für eine Ausnahmeregel wird angefordert

Ab v20 können Sie eine Anforderung für eine Verlängerung an senden **Zurückgestellt bis** Datum einer Ausnahmeregel. Sie können eine Erweiterung einer Regel anfordern, wenn Sie feststellen, dass eine große Anzahl von Datensätzen, die von der Regel erstellt wurden, nicht von gelöst wird **Zurückgestellt bis** Datum: Das Datum, an dem die Korrekturaufgabe keine neuen Avis mehr akzeptiert. Die Erweiterung aktualisiert die Ausnahmeregel, sodass das Zurückstellungsdatum für Ihre vorhandene Regel automatisch verlängert wird. Sie können Daten bis zu einem Jahr ab dem aktuellen Datum eingeben und müssen einen Grund für die Verlängerung angeben. Eine Verlängerungsanforderung erfordert eine zweistufige Genehmigung durch separate Genehmigungsgruppen.

Ausnahmeanforderung wird genehmigt

AVITs, die nicht sofort behoben werden können, werden von Anwendungssicherheitsanalysten überprüft, auf Risiko bewertet und für eine Zurückstellung genehmigt, bis sie behoben werden können. Das Genehmigen einer Ausnahmeanforderung kann ein Flow auf zwei Ebenen sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn nur der Genehmiger der ersten Ebene vorhanden ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger für hinzu Application Vulnerability Response.

Wichtig:
Sie können Ausnahmeanforderungen im Vulnerability Manager-Arbeitsbereich genehmigen oder ablehnen. Weitere Informationen finden Sie unter Genehmigen oder lehnen Sie Anforderungen in ab Arbeitsbereich des Schwachstellenmanagers.

Hinweis:

Nachdem eine Ausnahmeanforderung für ein AVIT genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Erneut öffnen
- Rufen Sie weitere Details ab

Nachverfolgung einer Ausnahmeanforderung

Nachdem Sie die Ausnahme ausgelöst haben, können Sie ihren Status mithilfe von nachverfolgen **Statusänderungsgenehmigungen** Registerkarte der AVIT.

Ablauf einer Ausnahmeanforderung und Anforderung einer Verlängerung einer Ausnahmeregel

Wenn eine Ausnahmeanforderung für eine bestimmte AVI abläuft, wird die betroffene AVI auf zurückgesetzt **Öffnen** status.

Ab v20 können Sie jedoch eine Anforderung zur Verlängerung von senden **Zurückgestellt bis** Datum in der Ausnahmeregel.

Konfigurieren Sie das Ausnahmemanagement für Application Vulnerability Response

Begrenzen Sie die Dauer einer angeforderten Ausnahme Und fügen Sie der Anforderung „Ausnahme“ oder „falsch positiv“ einen Fragebogen hinzu Verwenden des Moduls. Standardmäßig wird mit eine Ausnahme angefordert ServiceNow® Application Vulnerability Response Modul. Sie können auch eine Ausnahme mit anfordern GRC: Richtlinien- und Compliance-Management Integration.

Vorbereitungen
Erforderliche Rolle: sn_vul.App_Manage_Exception_Configuration

Warum und wann dieser Vorgang ausgeführt wird
Wenn Vulnerability Response Ist aktiviert, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ähnlich, wenn GRC: Richtlinien- und Compliance-Management Modul ist installiert. Sie können auswählen GRC: Richtlinien- und Compliance-Management Auf dem Konfigurationsbildschirm. Durch Aktivieren dieser Option können Sie eine Ausnahme anfordern, die das Richtlinien- und Kontrollziel von angibt GRC.

Wenn Sie einen Fragebogen hinzufügen, wird er an die Person gesendet, die die Ausnahme oder die falsch positive Anforderung stellt. Sie können entweder den Standardfragebogen verwenden oder einen basierend auf Ihren Anforderungen erstellen.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für die Anforderung der Ausnahme zu verstehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**an.
2. Wählen Sie im Formular „Konfiguration des Ausnahmemanagements“ aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option aus der Liste Ausnahmen verwalten mit auswählen.

   Hinweis:
   Beginnend mit Vulnerability Response Version 17.1. Sie können entweder auswählen Vulnerability Response Oder GRC: Richtlinien- und Compliance-Management. Sie müssen aktivieren GRC Zu verwendendes Plugin GRC: Richtlinien- und Compliance-Management Zum anfordern einer Ausnahme. Das Ändern der Konfiguration wirkt sich nicht auf die vorhandenen Daten aus.

3. Füllen Sie die Felder im Formular basierend auf der ausgewählten Option aus.
   - Wenn Sie ausgewählt haben Vulnerability Response Option, füllen Sie dann die Felder im Formular aus.

     Einstellungen für das Formular „VR-Ausnahmemanagement“

Feld	Beschreibung
Dauer	Zeitraum, für den eine Ausnahme angefordert werden kann.
Einheit	Zeiteinheit für den angegebenen Zeitraum.
Fragebogen aktivieren, um Ausnahme anzufordern	Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung.
Fragebogen, um Ausnahme anzufordern	Option zum Anzeigen des Fragebogens, den Sie zum anfordern einer Ausnahme ausgewählt haben. Standardmäßig wird der Ausnahmefragebogen angezeigt.
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur falsch positiven Anforderung, die ausgelöst wird.
Fragebogen, um falsch positive Meldung zu markieren	Option zum Anzeigen des von Ihnen ausgewählten Fragebogens als falsch positiv zu markieren. Der Fragebogen für falsch positive Anforderung wird standardmäßig angezeigt.

   - Wenn Sie ausgewählt haben GRC: Richtlinien- und Compliance-Management Option, füllen Sie dann die Felder im Formular aus.

     Einstellungen für das Formular „VR-Ausnahmemanagement“

Feld	Beschreibung
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur falsch positiven Anforderung, die ausgelöst wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Fragebogen, um falsch positive Meldung zu markieren	Option zum Anzeigen des von Ihnen ausgewählten Fragebogens zum Markieren als falsch positiv. Der Fragebogen für falsch positive Anforderung wird standardmäßig angezeigt.

4. Wählen Sie **Speichern**.

Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement

Beginnend mit Application Vulnerability Response V15.0: Verwenden Sie den Flow Designer, um Ausnahmeanforderungen für das Ausnahmemanagement, Ausnahmeregeln und die Verwaltung von falsch positiven Werten zu genehmigen. Wenn Sie bereitstellen Application Vulnerability Response(AVR) zum ersten Mal ist der Flow Designer standardmäßig aktiviert.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein vorhandener VR-Anwender sind, ist die Standardoption Workflow.
Wenn Sie bereitgestellt haben Application Vulnerability Response V15.0 oder höher, der Wert der Systemeigenschaft *sn_vul.flow_designer_activation*lst auf „wahr“ festgelegt. Dies bedeutet, dass der Flow Designer standardmäßig aktiviert ist.

Wenn Sie bereits verwenden Application Vulnerability Response Vor v15.0 ist der Wert dieser Systemeigenschaft auf „falsch“ festgelegt. Sie können den Flow Designer aktivieren, indem Sie den Wert in „wahr“ ändern.

Hinweis:
Sie können den Workflow nicht mehr verwenden, nachdem Sie den Flow Designer aktiviert haben. Einen detaillierten Vergleich zwischen Workflow und Flow Designer finden Sie unter Ausnahmemanagement-Workflow vs. Flow Designer.

Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmemanagement-Workflows konfigurieren.

- Ausnahmeanforderung für Korrekturaufgaben
- Ausnahmeanforderung für angreifbare Anwendungselemente
- Ausnahmeregel
- Falsch positiv für Korrekturaufgaben
- Falsch positiv für angreifbare Anwendungselemente

Hinweis:
Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den übereinstimmenden Genehmigungs-Workflow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Genehmigungsregeln**an.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie im Formular die Felder aus.

Formular „Genehmigungsregel“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.
Tabelle	Tabelle, auf die die Regel angewendet wird.
Anwendung	Der Standardwert ist Vulnerability Response.
Regeltyp	Gibt den Regeltyp an. Zum Beispiel Ausnahmeverwaltung, falsch positiv oder Ausnahmeregel.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird.
Beschreibung	Kurzbeschreibung der Genehmigungsregeln.
Genehmigung läuft ab y (Tage) Ab v21.0 von Application Vulnerability Response	Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann.
Genehmiger benachrichtigen (Tage) Ab v21.0 von Application Vulnerability Response	Datum, nach dem der Genehmiger benachrichtigt wird, Maßnahmen zu ergreifen.

4. Wählen Sie **Aktualisieren**.
   Auf der Registerkarte „Genehmigungskonfigurationen“ sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren.

Hinweis:
Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen.

Example:
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Schwachstellen definieren, die in verschiedenen Konfigurationselementen gefunden werden.

Zurückstellung der Korrektur in Application Vulnerability Response

Ab v20.0 können Sie die Korrektur mit zurückstellen **Warten Auf Implementierung** status, der für angreifbare Anwendungselemente (AVI) und Korrekturaufgaben verfügbar ist, während sie ihre Lebenszyklen durchlaufen. Sie können Datensätze nur manuell in diesen Status übergehen, indem Sie auswählen **Warten Auf Implementierung** Aus AVI- und Korrekturaufgabendatensätzen in der **Wird Untersucht** status.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfall

Als Korrekturspezialist können Sie einen Datensatz in verschieben **Warten Auf Implementierung** Um Ihrem Team mitzuteilen, dass Ihre Forschung und Arbeit an einer Aufgabe abgeschlossen ist. Sie können dieses Update auswählen, wenn Sie feststellen, dass eine Korrektur für die Implementierung bereit ist, aber nicht verfügbar ist. Ein Beispiel für eine nicht verfügbare Korrektur ist ein Software-Patch. Wenn das Wartungsfenster für einen Patch nicht verfügbar ist, wenn Sie Ihre Forschung abschließen, können Sie die Aufgabe nach verschieben **Warten Auf Implementierung** Bis der Patch bereitgestellt werden kann.

Pflichtfelder

Es gibt zwei erforderliche, bearbeitbare Felder in den Datensätzen der AVI- und Korrekturaufgaben, die sich im Status „Warten auf Implementierung“ befinden:

Datum der Korrekturzusage

Das geplante Korrekturdatum.

Korrekturplan

Die Beschreibung des Korrekturplans für die Korrektur. Dieser Text wird in den Notizen des Datensatzes angezeigt.

Felder und Systemeigenschaften

Es gibt zwei Systemeigenschaften, die auf festgelegt sind `Wahr` Standardmäßig für das modale Element, das beim Übergang eines Datensatzes zu angezeigt wird **Warten Auf Implementierung** . Wenn in den Standardeinstellungen beibehalten:

sn_vul.Remediation_fields

Legt Fest **Datum der Korrekturzusage** Und **Korrekturplan** Als Pflichtfelder. Wenn auf festgelegt `Falsch` , Diese Felder sind optional.

sn_vul.Warten_Implementierung

Zeigt das modale Element mit an **Datum der Korrekturzusage** , **Korrekturplan** Felder, nachdem Sie ausgewählt haben **Warten Auf Implementierung** In einem Datensatz. Wenn auf festgelegt `Falsch` , Sie können den Status eines AVI in „Warten auf Implementierung“ ändern, ohne dass Sie ein Zusagedatum oder einen Plan eingeben müssen.

Modul „Datum Der Verpassten Korrekturzusage“

Zeigen Sie alle Avis an, die ihre Daten der Korrekturzusage in verpasst haben **Datum Der Verpassten Korrekturzusage** Modul. Navigieren **Application Vulnerability Response** > **Angreifbare Elemente** > **Datum der Korrekturzusage vergangen** Zum Anzeigen der Liste.

Status-Rolldown von Korrekturaufgaben zu Avis

Die UI-Aktionsschaltfläche, in die ein Datensatz übertragen werden soll **Warten Auf Implementierung** Ist nur in Datensätzen für angreifbare Anwendungselemente und Korrekturaufgaben in sichtbar **Wird Untersucht** status. Für Status-Rollup im modalen Element, das angezeigt wird, wenn Sie auswählen **Warten Auf Implementierung** Für eine Korrekturaufgabe gibt es eine Option für **Vorhandene Avis überschreiben** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Wählen Sie Aus **Vorhandene Avis überschreiben** .	Wählen Sie diese Option aus, um die Daten der Korrekturzusage und die Korrekturpläne aller vorhandenen Avis in der Aufgabe zu überschreiben, die sich bereits in befinden **Warten Auf Implementierung** status. Wenn diese Option ausgewählt ist, wird für diese Funktion ein Rollup der Datums- und Plandaten der Korrekturaufgabe für Avis durchgeführt.
Verlassen **Vorhandene Avis überschreiben** Deaktiviert.	Lassen Sie die Option deaktiviert, um die Datums- und Planwerte für alle vorhandenen Avis in der Aufgabe, die sich bereits in der befinden, intakt zu halten **Warten Auf Implementierung** status. Wenn deaktiviert, ist Avis bereits in **Warten Auf Implementierung** Behalten Sie die vorhandenen Datums- und Plandaten bei und sind nicht vom Status-Rollup betroffen.

Rollup-Beispiele

Angenommen, Sie möchten eine Korrekturaufgabe von übergehen **Öffnen** Bis **Warten Auf Implementierung** Damit Sie das Zusagedatum und die Plandaten der Aufgabe für ein Softwarepatch-Wartungsfenster aktualisieren können. Angenommen, dass diese Aufgabe im eine AVI enthält **Warten Auf Implementierung** status, und Sie möchten das Datum der Zusage und die Plandaten aktualisieren, um sie der Korrekturaufgabe zu entsprechen.

Um die Avis-Datums- und Plandaten so zu überschreiben, dass sie mit der Korrekturaufgabe übereinstimmen, aktivieren Sie das Kontrollkästchen zu **Vorhandene Avis überschreiben** Wenn Sie dazu aufgefordert werden. Die Datums- und Planwerte des AVI werden zu den Plan- und Datumswerten, die Sie für die Aufgabe in der Eingabeaufforderung eingeben, wenn Sie auswählen **Warten Auf Implementierung** .

Wenn Sie in diesem Fall die Option Überschreiben nicht auswählen und ein AVI in vorhanden ist **Warten Auf Implementierung** , Die ursprünglichen Datums- und Plandaten im AVI bleiben intakt. Die Plan- und Datumswerte, die Sie für die Aufgabe in der Eingabeaufforderung eingeben, wenn Sie auswählen **Warten Auf Implementierung** Werden für keine Avis verwendet, die sich bereits in befinden **Warten Auf Implementierung** status in der Aufgabe.

Wenn sich ein AVI für eine Aufgabe in befindet **Gelöst** Oder **Geschlossen – behoben** Und Sie übergehen die Aufgabe zu **Warten Auf Implementierung** , Auswahl **Vorhandene Avis überschreiben** Ändert die Avis von nicht **Geschlossen – behoben** Und **Gelöst** Bis **Warten Auf Implementierung** Aufgrund eines höheren Statusvorrangs.

Wenn Überschreibung beim Verschieben der Aufgabe nach nicht ausgewählt ist **Warten Auf Implementierung** Und es gibt bereits eine AVI in **Warten Auf Implementierung** Und Sie verschieben die Aufgabe zurück zu **Öffnen** Oder **Wird Untersucht** , Die AVI verbleibt in **Warten Auf Implementierung** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie einen Ausnahmegenehmiger für hinzu Application Vulnerability Response

Fügen Sie den Genehmigergruppen Anwender hinzu, damit Sie eine Ausnahme anfordern können.

Vorbereitungen

Erforderliche Rolle: sn_vul.App_Exception_Approver

Warum und wann dieser Vorgang ausgeführt wird

Eine Ausnahmeanforderung für ein angreifbares Anwendungselement wird mit dem standardmäßigen zweistufigen Genehmigungs-Flow genehmigt. Die Anforderung kann von zwei Genehmigerebenen genehmigt werden. Das Hinzufügen von Anwendern zur Gruppe der ersten Ebene ist obligatorisch. Wenn auf der zweiten Ebene keine Anwender vorhanden sind, wird die Anforderung nach der Genehmigung auf der ersten Ebene genehmigt.

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**an.
2. Suchen Sie in der Spalte Name nach **Ausnahme** , Und klicken Sie auf **Genehmiger Für Anwendungsausnahme – Ebene 1** .

   Hinweis:
   Beginnt ab Application Vulnerability Response V12.8.1. Sie können die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahme oder falsch positive Anforderung über den Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** Und wählen Sie aus `sn_vul.app_exception_approver_L1`, `sn_vul.app_exception_approver_L2`, Oder `sn_vul.app_false_positive_approver_group`Zum Ändern des Eigenschaftswerts.

3. Klicken Sie im Formular Gruppenanwendungsausnahme – Ebene 1 auf die zugehörige Liste Gruppenmitglieder.
4. Klicken Sie Auf **Neu** Um eine Liste zu erstellen.
5. Füllen Sie im Formular die Felder aus.

Anwenderformular

Feld	Beschreibung
Anwender-ID	Eindeutiger Bezeichner für den Benutzer
Vorname	Vorname des Anwenders.
Nachname	Nachname des Anwenders.
Titel	Berufsbezeichnung des Benutzers Geben Sie einen Titel oder eine Stellenbeschreibung ein, oder wählen Sie eine aus der Liste aus.
Abteilung	Abteilung des Anwenders.
Passwort	Passwort, das dem Anwender zugewiesen ist. Dieses Passwort kann dauerhaft oder temporär sein.
Passwort muss zurückgesetzt werden	Option, mit der der Anwender das Passwort zurücksetzen können, um die Sicherheit zu gewährleisten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Gesperrt	Option zum Sperren des Anwenders aus der Instanz und zum Beenden aller aktiven Sitzungen des Anwenders. Das System verhindert, dass Anwender mit der Administratorrolle sich selbst sperren.
Aktiv	Option zum Aktivieren dieses Anwenders. Nur inaktive Anwender können in diesen Bereichen angezeigt werden: ○ Listen von Anwendern ○ Auswahlliste in Referenzfeldern (Lupensymbol) ○ Liste mit automatischer Vervollständigung, die angezeigt wird, wenn Sie in ein Referenzfeld eingeben
Nur Webservice-Zugang	Option, um diesen Anwender als nicht interaktiven Anwender zu bestimmen.
Interner Integrationsanwender	Option, um diesen Anwender als internen Integrationsanwender zu bestimmen.
E-Mail	E-Mail-Adresse des Anwenders.
Sprache	Bevorzugte Sprache des Anwenders.
Kalenderintegration	Kalender, der zum Verwalten des Arbeitszeitplans verwendet wird. Beispiel: Outlook.
Zeitzone	Zeitzone für den Standort dieses Anwenders.
Datumsformat	Bevorzugtes Format des Anwenders für Daten.
Telefon (geschäftlich)	Geschäftliche Telefonnummer des Anwenders.
Mobiltelefon	Mobiltelefon des Anwenders.
Foto	Foto, das Sie hochladen können, indem Sie auf klicken **Zum Hinzufügen klicken...** .

6. Klicken Sie auf **Absenden**.
7. **Wahlweise:** Wiederholen Sie die Schritte 1 bis 5, um einen Genehmiger für Anwendungsausnahmen auf Ebene 2 zu erstellen.
   Der Genehmiger muss zu navigieren **Anwendungsschwachstellenantwort** > **Meine Genehmigungen** Und genehmigen Sie Anforderungen.

Fordert und genehmigt eine Ausnahme in an Application Vulnerability Response

Sie können anfordern, die Korrektur eines angreifbaren Anwendungselements und einer Korrekturaufgabe für einen bestimmten Zeitraum zu verschieben.

Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist. Genehmiger, die Zugriff haben, können Anforderungen anderer Anwender genehmigen.

Sie können auch Ausnahmeregeln erstellen und eine Ausnahmereerweiterung für eine Ausnahmeregel anfordern. Standardmäßig sind für Zurückstellungen, Ausnahmeregeln und Ausnahmeerweiterungsanforderungen zwei Genehmigungsebenen erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum anfordern oder Genehmigen einer Ausnahme finden Sie unter:

- Fordern Sie eine Ausnahme für ein angreifbares Anwendungselement an
- Fordern Sie mit eine Ausnahme für Anwendungsschwachstellen an GRC: Richtlinien- und Compliance-Management
- Genehmigen Sie Ausnahmeregeln und Ausnahmeregelerweiterungsanforderungen in Application Vulnerability Response
- Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Application Vulnerability Response

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des Ausnahmemanagements gesendet, die den Status und andere Details einer Anforderung angeben. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, die bestätigt, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail, in der angegeben wird, dass eine Ausnahme angefordert wurde.

Ab v21.0 von Application Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Anwendungselement in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Anwendungselement oder die Korrekturaufgabe auf den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Fordern Sie eine Ausnahme für ein angreifbares Anwendungselement an

Fordern Sie eine Ausnahme für ein angreifbares Anwendungselement an, das nicht sofort behoben werden kann. Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Wichtig:
Sie können Ausnahmen für ein angreifbares Anwendungselement und eine Korrekturaufgabe über den Vulnerability Manager-Arbeitsbereich und DEN IT-Korrekturarbeitsbereich anfordern. Weitere Informationen finden Sie unter Fordern Sie Ausnahmen für Korrekturaufgaben und -Datensätze in an Arbeitsbereich des Schwachstellenmanagers und Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen.

Vorbereitungen
Erforderliche Rolle: Entwicklergruppe

Prozedur

1. Navigieren zu **Application Vulnerability Response** > **Angreifbare Anwendungselemente** > **Alle**
   Und wählen Sie das Element aus, für das Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element muss sich im Status „Offen“ oder „wird untersucht“ befinden.

   Hinweis:

   Ab v21.0 von Application Vulnerability Response, Der vorherige Status eines angreifbaren Anwendungselements wird in gespeichert **Backup_State** Feld.

2. Klicken Sie im Formular Angreifbares Anwendungselement auf **Ausnahme Anfordern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Abhängig davon, ob Vulnerability Response Ist oder ausgewählt GRC: Richtlinien- und Compliance-Management In **Application Vulnerability Response** > **Ausnahmenverwaltung** Bildschirm ändert sich das Formular „Ausnahme anfordern“. Wenn GRC: Richtlinien- und Compliance-Management, Siehe Fordern Sie mit eine Ausnahme für Anwendungsschwachstellen an GRC: Richtlinien- und Compliance-Management

3. Wenn Vulnerability Response Ist im Bildschirm „Ausnahmemanagement“ ausgewählt. Füllen Sie die Felder im Formular „Ausnahme anfordern“ aus.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der in ausgewählten Dauer liegen **Alle** > **Application Vulnerability Response** > **Administration** > **Ausnahmenverwaltung** Bildschirm. Wenn die Ausnahmeanforderung abläuft, kehrt die Gruppe zu zurück **Öffnen** status. **Hinweis:** Ab Version 18,0 von Application Vulnerability Response(AVR) kann ein zurückgestelltes angreifbares Anwendungselement von einem Scanner geschlossen und erneut geöffnet werden. Wenn das Element erneut geöffnet wird, bevor das Ausnahmefenster abläuft, wird der Status der AVIT in den Status zurückgestellt zurückgesetzt, entsprechend dem aktiven Ausnahmefenster. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft sn_vul.auto_defer_avit_in_active_exception_window auf „wahr“ fest. Außerdem wird das Datum „Zurückgestellt bis“ auch nach Abschluss der AVIT oder Ablauf der Ausnahme beibehalten. Die erforderliche Rolle ist „sn_vul.App_Manage_Exception_Configuration“ für Lese- und Schreibvorgänge.
Grund	Wählen Sie aus **Grund** . Die Auswahlmöglichkeiten lauten wie folgt: ○ Risiko akzeptiert ○ Warten auf Wartungsfenster ○ Behebung nicht verfügbar ○ Ausgleichende Steuerung vorhanden ○ Sonstige

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Informationen zum Hinzufügen neuer Ursachenauswahlen finden Sie unter Definieren Sie die Zuordnung des Richtliniengrunds.
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Korrekturbesitzer aktualisiert werden.

4. Klicken Sie Auf **Genehmigung Anfordern** Um die Ausnahmeanforderung zu übermitteln.
   Der Status des Anwendungs-Schwachstellenelements ändert sich in „in Überprüfung“. Verwenden Sie **Genehmigung Der Statusänderung** Registerkarte zum Nachverfolgen des Status der Ausnahmeanforderung.

Fordern Sie mit eine Ausnahme für Anwendungsschwachstellen an GRC: Richtlinien- und Compliance-Management

Fordern Sie Richtlinienausnahmen mit an GRC Fähigkeit zur Verwaltung von Richtlinienausnahmen in Richtlinien- und Compliance-Management Anwendung von innerhalb Application Vulnerability Response.

Vorbereitungen

Bevor Sie die Integration von Richtlinienausnahmen verwenden können, um Richtlinienausnahmen anzufordern, müssen Sie herunterladen GRC: Richtlinien- und Compliance-Management Anwendung aus dem ServiceNow Store.

Erforderliche Rolle: sn_vul.Remediation_ Besitzer

Sie können auch Ausnahmen in der klassischen Anwenderoberfläche anfordern:

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Anwendungselemente** (Oder **Korrekturaufgaben**)> **Alle** , Und öffnen Sie das Element oder die Gruppe, für das Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie im ausgewählten Formular auf **Ausnahme Anfordern** .
3. Wenn GRC: Richtlinien- und Compliance-Management Ist im Bildschirm „Ausnahmemanagement“ ausgewählt. Füllen Sie die Felder im Formular „Ausnahme anfordern“ aus.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Richtlinie	Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft, und der Status des angreifbaren Elements oder der angreifbaren Gruppe von zurückgestellt in Offen ändert. **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf nicht überschreiten **Maximale Ausnahmedauer (Tage)** Die Sie für die Richtlinie in Richtlinie und Compliance festgelegt haben. Weitere Informationen finden Sie unter Erstellen Sie eine Richtlinie .
Grund	Grund für die Anforderung einer Ausnahme.
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Pflichtfeld muss vom Korrekturbesitzer ausgefüllt werden.

a. Klicken Sie Auf **Genehmigung Anfordern** Um die Ausnahmeanforderung zu übermitteln.
Der Status der angreifbaren Elemente ändert sich in „in Überprüfung“, und eine Richtlinienausnahme wird erstellt. Verwenden Sie **Genehmigung Der Statusänderung** Registerkarte zum Nachverfolgen des Status der Ausnahmeanforderung.

b. Klicken Sie auf die zugehörige Liste Richtlinienausnahmen, um die Richtlinienausnahme anzuzeigen.

c. Klicken Sie auf die Nummer der Richtlinienausnahme.

d. In **Genehmiger** Wählen Sie den Namen des Genehmigers aus.

e. Klicken Sie auf die Registerkarte Quelle, und wählen Sie ein Kontrollziel aus **Kontrollziel** Feld.

f. Klicken Sie auf die Registerkarte Risikobewertung, und wählen Sie die Risikobewertung aus **Risikobewertung** Feld.

g. Speichern Sie das Formular.

h. Klicken Sie auf die Registerkarte Betroffene Steuerungen und dann auf Hinzufügen, um die Steuerungen hinzuzufügen.

i. Speichern Sie das Formular.

Hinweis:
Sie können eine Compliance-Überprüfung starten, indem Sie auf klicken **Compliance-Überprüfung anfordern** .

j. Das Genehmigungsformular wird an den Genehmiger gesendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

k. Als Genehmiger können Sie die Anforderung entweder genehmigen, indem Sie auf klicken **Genehmigen** Oder fordern Sie eine zusätzliche Genehmigung an, indem Sie auf klicken **Zusätzliche Genehmigung Anfordern** .
Der Datensatzstatus ändert sich in zurückgestellt. Der angegebene Grund ist der, den Sie beim Auslösen der Ausnahmeanforderung ausgewählt haben. Die Registerkarte Zurückstellung enthält zusätzliche Notizen zum Datensatz.

Hinweis:
Wenn die Anforderung abgelehnt wird, wird der Datensatz in den vorherigen Status verschoben.

4. Klicken Sie auf **Absenden**.
Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Korrekturbesitzer und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management .

Fordern Sie eine Ausnahme für eine Anwendungskorrekturaufgabe an

Fordern Sie eine Ausnahme an, um eine Anwendungskorrekturaufgabe für einen bestimmten Zeitraum aufzuschieben, wenn sie nicht sofort gelöst werden kann.

Vorbereitungen

Sie können Ausnahmen von anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Erforderliche Rollen: sn_vul.Remediation_owner, sn_vul.App_Security_Champion oder sn_vul_Container.Remediation_owner.

Sie können auch Ausnahmen für Anwendungskorrekturaufgaben in der klassischen Umgebung anfordern.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben** > **Alle**an.

2. Wählen Sie die Gruppe aus, für die Sie eine Ausnahme anfordern möchten.
Die ausgewählte Aufgabe muss sich im Status Offen, wird untersucht oder wartet auf Implementierung befinden.

3. Wählen Sie im Datensatz der Anwendungskorrekturaufgabe die Option aus **Ausnahme Anfordern** .

4. Füllen Sie im Formular die Felder aus.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der Ausnahmedauer liegen, die in der Konfiguration definiert ist.
Grund	Begründung für die Anforderung einer Ausnahme.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer aktualisiert werden.

5. Klicken Sie auf **Genehmigungs-Engine**.

Genehmigen Sie Ausnahmeregeln und Ausnahmeregelerweiterungsanforderungen in Application Vulnerability Response

Genehmigen Sie Ausnahmeanforderungen für angreifbare Anwendungselemente, die nicht sofort behoben werden können. Sie müssen diese Anforderungen auf Risiko bewerten und sie dann zur Zurückstellung genehmigen, bis sie behoben werden können.

Vorbereitungen
Erforderliche Rolle: sn_vul.App_Exception_Approver

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Meine Genehmigungen**an.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Definieren Sie die Zuordnung des Richtliniengrunds

Sie können die Ursachenauswahlen definieren, die jedem Anwender zur Verfügung stehen, der eine Ausnahme anfordert.

Vorbereitungen
Sie müssen die Anwendung GRC: Richtlinien- und Compliance-Management installiert haben. Diese Anwendung ist über verfügbar ServiceNow® Store Mit einem separaten Abonnement.

Weitere Informationen zu Systemanforderungen und Familienkompatibilität finden Sie in der Anwendungsliste auf der Website des ServiceNow Store .

Erforderliche Rolle: sn_vul.compliance.manager und sn_vul.Vulnerability_admin

Prozedur

1. Navigieren zu **Alle** > **Richtlinien und Compliance** > **Richtlinienausnahmen** > **Integrationsregistrierung**an.

   Hinweis:
   Sie können entweder einen Grund aus den Ursachenauswahlen auswählen, die in der Tabelle „Ursachenauswahlen“ verfügbar sind, oder einen neuen Grund hinzufügen.

2. Klicken Sie auf die Integrationsregistrierung für Ihre Anwendung, z. B. **Anwendungsschwachstellenantwort** , **Vulnerability Response** , Und so weiter.
3. Führen Sie die folgenden Schritte aus, um eine vorhandene Ursachenauswahl hinzuzufügen:
   a. Klicken Sie in der Liste Ursachenauswahlen auf **Neu** .
   b. Klicken Sie auf das Lupensymbol, um einen Grund auszuwählen.
4. Führen Sie die folgenden Schritte aus, um der Tabelle „Ursachenauswahlen“ neue Ursachenauswahlen hinzuzufügen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der Liste Ursachenauswahlen auf **Neu** .

b. Klicken Sie auf das Lupensymbol.

c. Klicken Sie auf **Neu**.

d. Füllen Sie im Formular die Felder aus.

Formular „Ursachenauswahlliste“

Feld	Beschreibung
Bezeichnung	Eindeutige Bezeichnung für diese Auswahl.
Wert	Eindeutiger Wert für diese Auswahl. Dieser Wert wird in der Tabelle „Zuordnungen des Grunds für Richtlinienausnahme“ für die jeweiligen Anwendungen zugeordnet. Um zu dieser Tabelle zu navigieren, geben Sie sn_vul_Policy_reason_Mapping.LIST im Filternavigator ein.
Reihenfolge	Reihenfolge für diese Auswahl. Gründe werden basierend auf dieser Nummer sortiert.
Standard	Option, die angibt, dass diese Ursachenauswahl immer verfügbar ist, wenn eine Richtlinienausnahme bei Bedarf angefordert wird. Wenn die Integrationsregistrierung keine anwendungsspezifischen Auswahlmöglichkeiten enthält, werden alle Ursachenauswahlen mit angegeben **Standard** Das ausgewählte Feld ist verfügbar.
Aktiv	Option zum Anzeigen der Auswahl in der Liste der Ursachenauswahlen.

5. Klicken Sie auf **Absenden**.

Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Application Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor sie das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rollen: App-SEC-Manager sn_vul.App_sec_Manager, Sicherheitsmeister sn_vul.App_Security_Champion.

Warum und wann dieser Vorgang ausgeführt wird

In einem Erweiterungsregeldatensatz können Sie eine Erweiterung für anfordern **Zurückgestellt Bis** Datum nur, wenn sich die Regel im befindet **Genehmigt** status. Sie können diese Erweiterung für eine Regel anfordern, wenn Sie feststellen, dass eine große Anzahl von Datensätzen, die von der Regel erstellt wurden, nicht von gelöst wird **Zurückgestellt bis** Datum: Das Datum, an dem die Korrekturaufgabe keine neuen Avis mehr akzeptiert. Die Erweiterung aktualisiert die Ausnahmeregel, sodass das Zurückstellungsdatum für Ihre vorhandene Regel automatisch verlängert wird.

Sie können auch eine Verlängerung über anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Vulnerability Manager-Arbeitsbereich an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Ausnahmeregeln**an.
2. Wählen Sie eine genehmigte Ausnahmeregel aus.
3. Wählen Sie Aus **Verlängerung Anfordern** .
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel erweitert werden muss.
Grund	Geben Sie den Grund für die Zurückstellung der Ausnahmeregel ein. Zur Auswahl stehen: ○ Risiko akzeptiert ○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Felder Zurückgestellt bis, Grund und zusätzliche Informationen für die Ausnahmeregel und die zugehörigen Korrekturaufgaben und angreifbaren Anwendungselemente aktualisiert. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion durch den Genehmiger ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben nicht verfügbar, die als Teil einer Ausnahmeregel erstellt werden.
- Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe in an Application Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe (VUL) an, bevor sie das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch eine Verlängerung über anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Vulnerability Manager-Arbeitsbereich an.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben**an.
2. Öffnen Sie eine zurückgestellte Korrekturaufgabe.
3. Wählen Sie Aus **Verlängerung Anfordern** .
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, an dem der Status Zurückstellen abläuft und die Korrekturaufgabe erneut aktiviert wird.
Grund	Geben Sie den Grund für die Zurückstellung des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Risiko akzeptiert ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Änderungen an der Korrekturaufgabe auch auf die angreifbaren Anwendungselemente zurückgesetzt, die Teil der Korrekturaufgabe sind. Die angreifbaren Anwendungselemente müssen sich jedoch im Status „zurückgestellt“ und ihren aktuellen Status befinden, bis die Daten vor dem Datum „aktualisiert bis“ liegen. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion durch den Genehmiger ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben nicht verfügbar, die als Teil einer Ausnahmeregel erstellt werden.
- Wenn eine zurückgestellte Korrekturaufgabe erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End.

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Anwendungselement in an Application Vulnerability Response

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Anwendungselement an, bevor es das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch eine Verlängerung über anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Vulnerability Manager-Arbeitsbereich an.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Elemente**an.
2. Öffnen Sie ein zurückgestelltes angreifbares Anwendungselement.
3. Wählen Sie Aus **Verlängerung Anfordern** .

   Hinweis:
   Die Schaltfläche „Verlängerung anfordern“ ist nur sichtbar, wenn der Status des angreifbaren Anwendungselements „Zurückgestellt“ lautet.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem das zurückgestellte angreifbare Anwendungselement zur Korrektur verlängert werden muss.
Grund	Geben Sie den Grund für die Zurückstellung des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Risiko akzeptiert ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei der Übermittlung der Anforderung und der nachfolgenden Aktion durch den Genehmiger wird eine E-Mail ausgelöst.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End.

6. Nachdem die Anforderung genehmigt wurde, werden „bis“, „Grund“ und „Zurückstellungshinweise“ aktualisiert.

Erstellen, löschen und brechen Sie eine Ausnahmeregel für ab Application Vulnerability Response

Erstellen Sie eine Regel, um automatisch eine Ausnahme für angreifbare Anwendungselemente (AVI) anzufordern, die bestimmte Bedingungen erfüllen.

Vorbereitungen

Beispielsweise können Sie eine Regel mit einer Bedingung erstellen, die auf einer bestimmten bekannten oder kritischen Schwachstelle basiert, die Sie wissen, dass Sie sie nicht sofort beheben können. Mit dieser Regel können Sie neue und vorhandene Avis automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

- Die Ausnahmeregel wird über angewendet **Gültig ab** Bis **Gültig bis** Datum, das Sie im Regeldatensatz eingeben.
- Die Korrekturaufgabe (AVUL) wird erstellt, nachdem die Regel für die Übereinstimmung mit Avis in genehmigt wurde **Zurückgestellt** status.
- Die Gruppierungsmethode für diese AVUL wird als Ausnahmeregeln bezeichnet.
- Sie können diese AVUL nicht schließen, erneut öffnen oder löschen. Neue und erneut geöffnete Avis werden zurückgestellt und dieser AVUL aus hinzugefügt **Gültig ab** Datum, bis die Gruppe am abläuft **Gültig bis** Datum.

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des Ausnahmeregel-Workflows gesendet. Diese E-Mails enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahmeregel angefordert wird, erhält die anfordernde Person eine E-Mail, die bestätigt, dass die Anforderung übermittelt wurde.

Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann erneut zur Genehmigung übermitteln.

Erforderliche Rollen: App sec-Manager sn_vul.App_sec_Manager und Sicherheitsmeister sn_vul.App_Security_Champion.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Ausnahmeregeln**an.
2. Wählen Sie auf der Seite „Ausnahmeregel – neuer Datensatz“ die Option aus **Neu** .
3. Füllen Sie die Felder aus.

Feld	Beschreibung
Name	Name der Ausnahmeregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Schreibgeschützt: Entwurf
Gültig ab	Datum, ab dem diese Regel aktiv ist, um Avis aufzuschieben.
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausnahmeregel. Ein niedrigerer Wert geht einem höheren voraus.
Gültig bis	Datum, an dem die Korrekturaufgabe die Annahme neuer Avis beendet.
Zurückgestellt bis	Datum, bis die Korrekturaufgaben und Avis zurückgestellt werden. An diesem Datum werden die AVULs geschlossen, und alle Avis werden aus den Aufgaben entfernt und erneut geöffnet. Gruppenregeln werden erneut auf diese Avis angewendet.
Grund	Grund für die Erstellung dieser Ausnahmeregel.
Zuweisungsgruppe	Gruppe, der die Korrekturaufgabe zugewiesen ist, um die zurückgestellten Avis nachzuverfolgen.
Zusätzliche Information	Zusätzliche Informationen, die die anfordernde Person dem Genehmiger bereitstellen möchte. Diese Informationen werden im Beschreibungsfeld der Korrekturaufgabe ausgefüllt.
Bedingung	Filterbedingungen, um anzugeben, welche Avis mit dieser Regel übereinstimmen.
Für vorhandene Daten ausführen	Option, mit der Sie diese Regel bei der ersten Ausführung dieser Regel für vorhandene Daten ausführen können. Wenn Sie diese Option deaktiviert lassen, wird Ihre Regel täglich von der geplanten Aufgabe ausgeführt *`Associate existing AVIs with Auto Exception Rule`*Beginnt mit neuen Daten. Wenn Sie die Option für vorhandene Daten ausführen aktivieren, wird eine geplante Aufgabe einmal für die vorhandenen Daten im ausgeführt **Gültig ab** Datum.

4. Fügen Sie die Zuweisungsgruppe hinzu, wenn Sie die Regel erstellen.
5. Wählen Sie eine aus.

Nachdem die Regel genehmigt wurde, wird sie in verschoben **Genehmigt** status. Ihre Regel wertet Avis mit aus *`Associate existing AVIs with Auto Exception Rule scheduled`*Auftrag. Wenn Sie ausgewählt haben **Für vorhandene Daten ausführen** , Wertet vorhandene Avis aus. Für die Regel wird automatisch eine Korrekturaufgabe erstellt, und alle übereinstimmenden Avis, die ihre Bedingungen erfüllen, werden der Aufgabe zugeordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die geplante Aufgabe führt die Ausnahmeregel einmal für vorhandene Daten aus. Die Regel wird für vorhandene Daten nicht erneut ausgeführt, auch wenn keine Avis gefunden werden. Es werden nur neue Daten ausgewertet, da die vorhandenen Avis, die der Regel entsprechen, bereits zurückgestellt wurden.

6. Um eine Regel zu löschen, wählen Sie aus **Löschen** Im Ausnahmeregeldatensatz.
   Die folgende Meldung wird angezeigt: Wenn Sie die Regel löschen, wird die zugehörige Korrekturaufgabe gelöscht, und die zugehörigen angreifbaren Elemente werden erneut geöffnet. Die Regeln für Korrekturaufgaben werden dann auf die einzelnen Avis angewendet, und die Ausnahmeregel wird gelöscht.
7. Wählen Sie Aus **Regel beibehalten** Zum Beenden von oder **Regel löschen** Um fortzufahren.
8. Wählen Sie aus, um eine Regel zu deaktivieren, sie aber in der Liste „Ausnahmeregeln“ zu behalten **Abbrechen** .
   Die folgende Meldung wird angezeigt: Wenn Sie diese Regel abbrechen, wird die zugehörige Korrekturaufgabe gelöscht, und die zugehörigen angreifbaren Elemente werden erneut geöffnet. Die Regeln für Korrekturaufgaben werden dann auf die einzelnen angreifbaren Elemente angewendet, und die Ausnahmeregel wird in den Entwurfsstatus verschoben.
9. Wählen Sie Aus **Regel beibehalten** Zum Beenden von oder **Abbrechen** Um die Regel nach zu verschieben **Entwurf** Und deaktivieren Sie es.

Application Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln

Konfigurieren Sie Korrekturaufgaben (AVULs), damit Analysten und Korrekturspezialisten angreifbare Anwendungselemente (AVI) organisieren und in großen Mengen analysieren können. Die Kriterien, nach denen Korrekturaufgaben erstellt werden, werden so konfiguriert, dass Avis automatisch Korrekturaufgaben zugewiesen werden. Mit Korrekturaufgaben können Sie den Fortschritt überwachen und den Korrekturprozess effizienter steuern.

Nachverfolgung der Anzahl der Zurückstellungen für angreifbare Anwendungselemente und Korrekturaufgaben

Verfolgen Sie, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Container-Element oder eine Korrekturaufgabe zurückgestellt wird. Die `set deferral counts`Die geplante Aufgabe wird täglich ausgeführt, um die Anzahl der Datensätze, die mehrmals zurückgestellt werden, in der Spalte „Anzahl der Zurückstellungen“ zu buchen. Datensätze werden in den Modulen „mehrere Zurückstellungen“ für VR, AVR und CVR angezeigt.

Regeln für Korrekturaufgaben verstehen

Mit Regeln für Korrekturaufgaben können Sie definieren, wie angreifbare Anwendungselemente automatisch gruppiert und zugewiesen werden. Eine Standardregel **Schwachstelle** Ist im Basissystem enthalten, das Avis basierend auf ihren Schwachstellen erfasst. Sie können jedoch nach jedem anderen Satz von Werten in Spalten gruppieren, auf die über AVI zugegriffen werden kann. Diese Werte können Konfigurationselement (Configuration Item, CI), Schwachstelleneintrag usw. enthalten.

Es gibt Aufgabenregeln für Application Vulnerability Response, die in enthalten sind Vulnerability Response Anwendung, die verfügbar ist, wenn Sie sie aktivieren.

Mit dem Bedingungsgenerator können Sie mehrere Bedingungen erstellen. Nachdem Sie ein Feldpaar festgelegt haben, wird im Abschnitt Gruppieren nach eine weitere Zeile angezeigt. Sie können bis zu sechs haben **Gruppieren nach** Auswahlen. Sie können auch die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppenzuweisung automatisieren. Siehe Weisen Sie angreifbare Anwendungselemente in zu Application Vulnerability Response Automatisch und Filtern in Vulnerability Response, um weitere Informationen zu erhalten.

Sie können Ihre angreifbaren Anwendungselemente beispielsweise nach dem Konfigurationselement oder nach dem Produktmodell gruppieren. Sie können eine Aufgabenregel für Schwachstellen mit niedrigem Schweregrad oder CIs mit niedrigem Risiko haben. Sie können eine andere Aufgabenregel für kritische Server und Schwachstellen haben, die das Unternehmen einem höheren Risiko aussetzen. Siehe Erstellen, bearbeiten und löschen Application Vulnerability Response Regeln für Korrekturaufgaben Um weitere Informationen zu den Optionen zu erhalten, die Ihnen zur Verfügung stehen.

Für angreifbare Anwendungselemente, die das Unternehmen einem höheren Risiko aussetzen, kann ein anderer Satz von Regeln verwendet werden. Der Name der Korrekturaufgabe wird an die Regel der Korrekturaufgabe angehängt **Gruppieren nach** Werte für die Kurzbeschreibung des neuen Datensatzes.

Wenn ein neues angreifbares Anwendungselement erstellt, importiert oder erneut geöffnet wird, nachdem es geschlossen wurde, werden die Regeln anhand dieses Elements ausgewertet. Eine AVI wird nur einmal automatisch ausgewertet, es sei denn, sie wird nach dem Schließen erneut geöffnet oder die Regeln werden manuell erneut angewendet.

Der folgende Prozess wird für jedes neue oder erneut geöffnete AVI verwendet:

- Für jede Korrekturaufgabenregel wird die AVI mit dem Korrekturaufgabenregelfilter verglichen.
- Für jede Regel, bei der die Regelbedingung für Korrekturaufgaben erfüllt ist, ruft die Regel die Daten aus dem ab **Gruppieren nach** Auswahlen im AVI. Erstellt einen Gruppennamen und ein Feld. In diesem Fall **Hohes Risiko: QID-32342:** *`Zusammenfassung von QID-3242`* (Name: Schwachstellen-ID: Schwachstellen-Zusammenfassung).

  Hinweis:
  Das Feld „Kurzbeschreibung“ ist auf 160 Zeichen beschränkt. Längere Schwachstellenzusammenfassungen werden gekürzt.

  Die Regel überprüft, ob eine Übereinstimmung vorhanden ist **Öffnen** Korrekturaufgabe, die derselben Zuweisungsgruppe wie die AVI zugewiesen ist.
  - Wenn die Aufgabe gefunden wird, wird die AVI der vorhandenen Aufgabe in hinzugefügt **Öffnen** status.
  - Wenn keine Aufgabe in **Öffnen** status wurde gefunden, die Regel erstellt einen **Hohes Risiko: QID-32342** Aufgabe, weist sie derselben Zuweisungsgruppe wie die AVI zu und platziert die AVI in der Korrekturaufgabe.

Es kann mehr als eine Regel für Korrekturaufgaben definiert werden, um verschiedene Arten von Schwachstellen zu gruppieren. Da jede Schwachstelle mit den Regelbedingungen für Korrekturaufgaben verglichen wird, bevor sie in eine Korrekturaufgabe eingefügt wird, können sich zu viele Regeln auf die Leistung auswirken. Richten Sie Ihre Aufgabenregeln so ein, dass die Bedingungen Ihnen helfen, doppelte Korrekturaufgaben zu vermeiden.

Standardmäßig verwenden Regeln für Korrekturaufgaben die vom festgelegte Zuweisungsgruppe **Zuweisungsregeln** In der AVI beim Gruppieren der Elemente und weist die Korrekturaufgabe entsprechend der Avis zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Teil der Standardaufgabenregel wird die Zuweisung dieser Korrekturaufgaben durch die Regeln in gesteuert **Zuweisungsregeln** Modul. Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln.

Wenn eine Aufgabenregel aus der Formular- oder Listenansicht gelöscht wird, haben Sie die Möglichkeit, alle zu löschen **Öffnen** Von dieser Regel erstellte Aufgaben. Aufgaben nicht in **Öffnen** status sind ausgeschlossen.

Regeln für Korrekturaufgaben werden erneut angewendet

Wenn Sie eine Korrekturaufgabenregel ändern möchten, verwenden Sie **Erneut Anwenden** Schaltfläche auf der Seite mit der Regel für Korrekturaufgaben, um die geänderte Regel für alle aktiven erneut auszuführen **Öffnen** Von dieser Regel erstellte Korrekturaufgaben. Korrekturaufgaben werden automatisch basierend auf der geänderten Regel gelöscht und neu erstellt.

Erneut Anwenden Überprüft nur vorhandene Korrekturaufgaben.

Nachdem Sie ausgewählt haben **Erneut Anwenden** , Die folgende Meldung wird angezeigt: Durch das erneute Anwenden dieser Korrekturaufgabenregel werden die Korrekturaufgaben für diese Regel gelöscht und neu erstellt. Korrekturaufgaben, die sich nicht im Status „Offen“ befinden, werden nicht gelöscht .

Korrekturaufgaben werden erstellt und Avis manuell hinzugefügt

Sie erstellen eine Anwendungskorrekturaufgabe (AVUL) aus einem anderen Anwendungskorrekturaufgabendatensatz und fügen angreifbare Anwendungselemente (AVITs) manuell hinzu. Weitere Informationen finden Sie unter Erstellen Sie eine Anwendungskorrekturaufgabe manuell in Application Vulnerability Response.

Regeln für Korrekturaufgaben und Erstellung und Aktualisierung von AVI

Wenn ein CI oder Produktmodell aus einem Scan einer bekannten Schwachstelle zugeordnet ist, wird ein AVI erstellt. Nach der Erstellung wird die AVI anhand der Bedingungen der Regeln für Korrekturaufgaben für eine Übereinstimmung ausgewertet. Wenn eine Übereinstimmung mit einer vorhandenen Korrekturaufgabe besteht, wird die AVI hinzugefügt. Wenn keine übereinstimmende Korrekturaufgabe gefunden wird, wird eine für das AVI erstellt.

Wenn eine Eigenschaft, die in den Filterbedingungen für Korrekturaufgaben erfasst wird, in einem AVI aktualisiert oder geändert wird, wird das aktualisierte AVI auch anhand der Regeln für Korrekturaufgaben für eine Übereinstimmung ausgewertet. Wenn eine Übereinstimmung mit einer vorhandenen Korrekturaufgabe besteht, wird die AVI hinzugefügt. Wenn keine übereinstimmende Korrekturaufgabe gefunden wird, wird eine für die AVI erstellt.

Status-Rollup und Rolldown

Wenn Sie eine Korrekturaufgabe auf „Offen“ oder von „Offen“ auf „wird untersucht“ aktualisieren, wird der neue Status auf alle zugehörigen Avis zurückgesetzt. Status-Rollup erfolgt unmittelbar nach dem Ändern des Status.

Status-Rollup von Avis zur Korrekturaufgabe findet nur statt, wenn sich alle Avis in der Aufgabe befinden **Zurückgestellt** Oder **Geschlossen: Behoben** status. Rollup wird mit durchgeführt *`Rollup application vulnerable item values to vulnerability and group`*Geplante Aufgabe, die alle 15 Minuten ausgeführt wird. Der Status wird erst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nach Ausführung des Auftrags als Rollup ausgeführt. Damit ein Rollup von der Avis zur Korrekturaufgabe erfolgt, müssen alle Avis denselben Status aufweisen.

Erstellen, bearbeiten und löschen Application Vulnerability Response Regeln für Korrekturaufgaben

Sie können Regeln erstellen, um angreifbare Anwendungselemente (AVI) basierend auf Filterbedingungen automatisch in Korrekturaufgaben (AVUL) zu gruppieren. Diese Regeln gruppieren Avis automatisch, wenn sie importiert oder manuell erstellt werden.

Vorbereitungen

Wenn Sie eine neue Regel erstellen, gilt sie nicht für vorhandene Daten. Nachdem Sie sie übermittelt haben, wird sie für neue Importe ausgeführt.

Erforderliche Rolle: sn_vul.App_sec_Manager

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Regeln für Korrekturaufgaben**an.
2. Öffnen Sie die Regel, oder wählen Sie aus **Neu** .
3. Füllen Sie die Felder im Formular aus, oder bearbeiten Sie sie.

Regel für Korrekturaufgaben

Feld	Beschreibung
Name	Name der Aufgabenregel.
Aktiv	Gibt an, ob die Aufgabe aktiv ist.
Beschreibung	Eine Beschreibung der Regel.
Groß-/ Kleinschreibung beachten	Bestimmt, ob bei einer Bedingung die Groß-/Kleinschreibung beachtet wird oder nicht. **Hinweis:** Beim Standardwert wird die Groß-/Kleinschreibung nicht berücksichtigt.
Bedingung	Optionale Filterbedingungen für die Regel. Standardmäßig (**Groß-/Kleinschreibung beachten** Kontrollkästchen nicht aktiviert), wird bei dem Suchtext, den Sie in den Bedingungsgenerator für Aufgabenregeldatensätze und -Formulare eingeben, die Groß-/Kleinschreibung nicht beachtet. Sie haben die Möglichkeit, Suchvorgänge mit Groß-/Kleinschreibung in Aufgabendatensätzen und -Formularen zu aktivieren. Eine Beispielbedingung ist **Schwachstelle** > **ist** > **VULNENT123451** (Bekannte importierte Schwachstelle). Alle Avis mit dieser Schwachstelle entsprechen dieser Bedingung.
Gruppieren nach (bis zu sechs Bedingungssätze sind verfügbar)	
Gruppieren Sie angreifbare Anwendungselemente aus	Die Tabelle, die die Regel zum Gruppieren von Avis verwendet. Wählen Sie die Elemente aus der Struktur aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ Angreifbares Anwendungselement [sn_vuln_vulnerable_item] ◦ Konfigurationselement für angreifbares Anwendungselement [cmdb_ci] ◦ Angreifbares Anwendungselement – Anwendungsschwachstelle [sn_vul_third_Party_entry] ◦ Angreifbares Anwendungselement – Produktmodell **Hinweis:** Wenn Sie eine erweiterte Tabelle auswählen, wird die **Feld wird verwendet** Wird nur für angreifbare Anwendungselemente angewendet, die diese erweiterte Tabelle verwenden.
Mit Feld	Feld in der Tabelle, das die Regel zum Gruppieren von Avis verwendet. Wählen Sie Bedingungen aus der Struktur aus. **Hinweis:** Sie können Gruppierungsbedingungen erstellen, damit nicht alle Avis, die Daten freigeben, derselben Korrekturaufgabe zugewiesen werden. Wenn Sie beispielsweise Zuweisungsgruppe und IP-Adresse als Felder verwenden auswählen und mehrere Avis der anfänglichen Filterbedingung entsprechen **Schwachstelle** , Diese Avis können mit den vielen Optionen im Abschnitt Gruppieren nach verschiedenen Zuweisungsgruppen zur Korrektur zugewiesen werden. Die Bedingungen für Gruppieren nach geben Ihnen die Flexibilität, verschiedene Korrekturaufgaben zu erstellen, die verschiedenen Gruppen zugewiesen werden können, auch wenn sie einige Daten teilen.
Zuweisung	
Korrekturaufgaben zuweisen nach	Wenn Korrekturaufgaben automatisch zugewiesen werden, wird zusätzlich zu die Zuweisungsauswahl verwendet **Gruppieren Nach** Auswahlmöglichkeiten zum Gruppieren der angreifbaren Elemente. Neue Aufgaben werden nach Bedarf erstellt, sodass jede AVI in einer Aufgabe mit einem übereinstimmenden Zuweisungsgruppensatz platziert wird. Um die Zuweisung von Aufgaben zu automatisieren, die basierend auf dieser Regel erstellt wurden, wählen Sie eine der verfügbaren Optionen aus. ◦ Feld „Gruppieren nach“: Wenn Sie ein Anwendergruppenfeld aus ausgewählt haben **Feld wird verwendet** Werte in **Gruppieren nach** Abschnitt, werden sie im Dropdown-Menü angezeigt. ◦ Anwendergruppe: Verwenden Sie die Suchliste, um eine statische Anwendergruppe auszuwählen.

Wenn Sie eine Regel entweder aus der Formular- oder Listenansicht löschen, haben Sie die Möglichkeit, alle zu löschen **Öffnen** Von dieser Regel erstellte Korrekturaufgaben. Gruppen nicht in **Öffnen** status sind ausgeschlossen.

4. Wählen Sie Aus **Übermitteln** Für neue Regeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie ausgewählt haben **Übermitteln** , Ihre Regel wird in der Liste Regeln für Korrekturaufgaben [sn_vul_grouping_rule] angezeigt. Die folgenden Situationen initiieren Ihre Regel.

- Wenn neue Avis erstellt werden.
- Wenn Sie auswählen **Erneut Anwenden** . Sie wählen aus **Erneut Anwenden** Dient zur Auswertung von Aufgabenregeln nur für vorhandene Korrekturaufgaben.
- Wenn Avis aktualisiert werden, entweder von Ihnen oder vom System.

  Wenn ein AVI aktualisiert wird, werden Aufgabenregeln auf Übereinstimmungen mit vorhandenen Korrekturaufgaben ausgewertet. Einige häufige Updates, die eine Regelprüfung initiieren, sind:

  - Wenn sich der Status von „Geschlossen“ in „Offen“ oder von „Geschlossen“ in „wird untersucht“ ändert.
  - Das Konfigurationselement (CI) wird geändert.
  - Die Schwachstelle wird geändert.

Das System überprüft alle Aufgabenregeln auf Übereinstimmungen mit dem aktualisierten AVI. Wenn die Bedingungen einer Regel den Bedingungen einer Korrekturaufgabe entsprechen, werden ihr übereinstimmende Avis zugewiesen.

Wenn keine Übereinstimmung gefunden wird, wird eine neue Korrekturaufgabe erstellt.

Weitere Informationen zum Status-Rollup von Avis zu Korrekturaufgaben und zum Status-Rollup von Korrekturaufgaben zu Avis finden Sie unter Application Vulnerability Response Übersicht über Korrekturaufgaben und Aufgabenregeln.

Ein Beispiel für eine Regel für Korrekturaufgaben finden Sie unter Application Vulnerability Response Beispiele für Regel für Korrekturaufgaben.

5. Um eine Aufgabenregel zu löschen, wählen Sie die Regel in der Liste Regeln für Korrekturaufgaben aus, und wählen Sie aus **Löschen** .
   Die folgende Meldung wird angezeigt: Die ausgewählte Regel für Korrekturaufgaben hat n Korrekturaufgaben erstellt. Von den Korrekturaufgaben befinden sich n im Status Offen. .

Option	Beschreibung
Kontrollkästchen deaktiviert (Standard).	Löschen Sie nur die Regel. Aufgaben nicht in **Öffnen** status sind ausgeschlossen.
Kontrollkästchen ausgewählt.	Schließen Sie die Korrekturaufgaben in ein **Öffnen** status, wenn Sie die Regel für Korrekturaufgaben löschen. Löschen Sie die Regel und alle Korrekturaufgaben in **Öffnen** status.

6. Wählen Sie eine Option aus, und wählen Sie aus **Löschen** .

Erstellen Sie eine Anwendungskorrekturaufgabe manuell in Application Vulnerability Response

Erstellen Sie eine Anwendungskorrekturaufgabe (AVUL) aus einem anderen Anwendungskorrekturaufgabendatensatz, und fügen Sie angreifbare Anwendungselemente (AVITs) manuell hinzu.

Vorbereitungen

Erforderliche Rolle: sn_vul.App_sec_Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben** > **Alle**an.
2. Wählen Sie oben rechts auf der Seite die Option aus **Neu** .
3. Wählen Sie auf der Registerkarte Gruppenkonfiguration für Gruppierungsmethode aus **Manuell** .
4. Wählen Sie **Absenden**.
5. Suchen Sie Ihren neuen Aufgabendatensatz (AVUL) in der Tabelle „Anwendungskorrekturaufgaben“ [sn_vul_App_Vulnerability].
   Der Datensatz wird in erstellt **Öffnen** status.
6. Öffnen Sie den Datensatz, und fügen Sie dieser Gruppe mithilfe der zugehörigen Liste angreifbare Anwendungselemente hinzu (**Bearbeiten** Oder **Hinzufügen**).
7. Wählen Sie Aus **Aktualisieren** Zum Speichern des Datensatzes oder anderer UI-Aktionen, um den Datensatz in einen anderen Status zu versetzen.

Erstellen Sie Regeln für das automatische Schließen

Verwenden Sie Regeln zum automatischen Schließen, um ältere AVITs basierend auf den von Ihnen festgelegten Filterbedingungen automatisch zu schließen.

Vorbereitungen

Erforderliche Rolle: sn_vul.App_Manage_Auto_close_rules

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Regeln für automatisches Schließen**an.
   Das Basissystem bietet die folgenden Regeln für das automatische Schließen:

   Zuletzt gescannte Anwendungsschwachstellen Schwachstellen, die in den letzten 90 Tagen nicht gemeldet wurden, werden auf umgestellt **Veraltet** status.
2. Wählen Sie Aus **Neu** Dient zum Erstellen einer neuen Regel zum automatischen Schließen.
3. Füllen Sie die Felder des Formulars aus.

Feld	Wert
Name	Name der Regel zum automatischen Schließen.
Aktiv	Option zum Aktivieren der Regel. Wenn diese Option aktiviert ist, werden alle Erkennungen, die den Filterkriterien entsprechen, automatisch geschlossen.
Ausführungsreihenfolge	Eindeutiger Wert für die Ausführung der Regel zum automatischen Schließen. Dieser Wert bestimmt die Reihenfolge der Ausführung. Der Standardwert ist 100.
Integrationstyp	Anwendungsschwachstellenintegration
Beschreibung	Beschreibung der Regel zum automatischen Schließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Bedingung	Filterbedingungen, die verwendet werden, um Erkennungen zu identifizieren, die geschlossen werden sollen.

4. Wählen Sie **Absenden**.

Die **Regelprozessor für automatisches Schließen** Die geplante Aufgabe wird jede Nacht ausgeführt. Identifiziert AVITs basierend auf den angegebenen Bedingungen und überträgt die übereinstimmenden zu **Veraltet** status. In Fällen, in denen AVITs mit dem Status „Geschlossen“ und „Veraltet“ vorhanden sind, wird die AVIT mit dem Substatus „Geschlossen“ als geschlossen **Behoben** .

Penetrationstests konfigurieren

Sie können die Sprint-Dauer und den geschätzten Aufwand für die Bewertungstypen von Penetrationstests konfigurieren. Dies bietet Anwendungsbesitzern die Planungsfunktion, die ihnen hilft, einen vorläufigen Zeitrahmen für ihre Penetrationstestbewertungsanforderungen zu bestimmen.

Vorbereitungen
Erforderliche Rolle: Ethical Hacker

Warum und wann dieser Vorgang ausgeführt wird
Das Konfigurieren der Einstellungen für die Penetrationstestbewertung für das Team für ethische Hacker hilft auch, die Gruppe und den Ansprechpartner zu bestimmen, die die Anforderung zur Penetrationstestbewertung erhalten.

Ab v19.0 von Vulnerability Response, Wenn Sie verwenden Veracode Vulnerability Integration, Die Penetrationstest-Tests in Veracode Vulnerability Integration Sind manuelle Ergebnisse von Veracode. Sie sind nicht mit Penetrationstestbewertungsanforderungen verknüpft, die Sie in konfigurieren Application Vulnerability Response. Für weitere Informationen zu Penetrationstestbewertungen von Veracode, Siehe Veracode Vulnerability Integration.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration**an.
2. Verwenden Sie den ersten Abschnitt, um die Zuweisungsgruppe zu konfigurieren.
3. Füllen Sie im Formular die Felder aus.

Formular „Penetrationstest-Konfiguration“

Feld	Beschreibung
Anwendergruppe des Penetrationstestteams	Gruppe, der die Anforderung zur Penetrationstest-Bewertung zugewiesen ist.
Standard-Beauftragter für Bewertungsanforderungen für Penetrationstests	Ansprechpartner für die Anforderung zur Bewertung des Penetrationstests.

4. Wählen Sie **Aktualisieren**.
5. Verwenden Sie den zweiten Abschnitt, um Sprints zu konfigurieren.
   Details finden Sie unter Konfigurieren Sie Sprints für Penetrationstests.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Verwenden Sie den dritten Abschnitt, um Bewertungstypen zu konfigurieren.
   Details finden Sie unter Konfigurieren Sie Bewertungstypen für Penetrationstests.

Konfigurieren Sie Sprints für Penetrationstests

Konfigurieren Sie die Sprint-Dauer und -Kapazität für das Team für ethische Hacker, damit es die Sprint-Kapazität für Penetrationstestbewertungen verwalten kann.

Vorbereitungen
Erforderliche Rolle: Ethical Hacking

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration**an.
2. Wählen Sie aus **Konfigurieren** Option für Konfigurieren von Sprints.
3. Füllen Sie im Formular die Felder aus.

Formular „Sprint-Konfiguration“

Feld	Beschreibung
Sprint-Dauer (Tage)	Anzahl der Tage in einem Sprint.
Startdatum	Startdatum für die Sprint-Dauer.
Anzahl der Sprints	Anzahl der Sprints, die basierend auf den Start- und Enddaten für den Sprint-Bereich generiert werden können.
Enddatum	Enddatum für die Sprint-Dauer.
Sprint-Kapazität	
Sprint-Kapazität (Stunden)	Kapazität eines Sprints in Stunden.

4. Wählen Sie Aus **Sprints Generieren** .
   Um die erstellten Sprints anzuzeigen, wählen Sie aus **Zeigen Sie Sprints An** .

Hinweis:
Nachdem die Sprints generiert wurden und in Bearbeitung sind, wenn Sie auswählen **Sprints Generieren** Für die gleiche Dauer wird der aktuelle Sprint wie gewohnt abgeschlossen. Die verbleibenden Sprints werden basierend auf der aktualisierten Sprint-Konfiguration neu berechnet.

Konfigurieren Sie Bewertungstypen für Penetrationstests

Konfigurieren Sie den geschätzten Aufwand für jede Art von Penetrationstestbewertung. Auf diese Weise können Sie die Kapazität jedes Sprints verwalten, indem Sie den für jeden Bewertungstyp erforderlichen Aufwand schätzen.

Vorbereitungen
Erforderliche Rolle: Ethical Hacking

Warum und wann dieser Vorgang ausgeführt wird
Jeder Sprint ist einer Penetrationstestanforderung zugewiesen. Basierend auf dem geschätzten Aufwand für den Bewertungstyp werden die Stunden angepasst, um die Saldostunden für den Sprint widerzuspiegeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration**an.
2. Ab v19.0 von Vulnerability Response, Wählen Sie aus **Konfigurieren** Zum Anzeigen von Bewertungstypen, Anwendungsgröße und geschätztem Aufwand.
3. **Wahlweise:** Wählen Sie einen Bewertungstyp-Datensatz aus, um die Felder nach Bedarf zu aktualisieren oder neue Datensätze zu erstellen.

   (Optional) Die Werte für die Anwendungsgröße bieten Ihnen weitere Optionen, mit denen Sie die Testzeit und den Aufwand genauer schätzen können. Sie können die Stunden für diese Datensätze bearbeiten oder auswählen **Neu** Um eigene Kombinationen zu erstellen.

   Sie können Bewertungstyp und Anwendungsgröße für Werte in vorhandenen Datensätzen von Penetrationstestanforderungen ändern, sodass Sie Tests entsprechend der Sprint-Kapazität planen können. Wenn Sie beispielsweise eine Testanforderung ausfüllen, wird die Anzahl der von Ihnen konfigurierten Sprints möglicherweise nicht angezeigt, da einige Sprints bereits für Tests verwendet wurden. Wenn die geschätzten Aufwandsstunden eines Sprints mit der für den Typ und die Größe eines Tests erforderlichen Kombination übereinstimmen, sind sie für neue Anforderungen nicht verfügbar.

   Sie können die Sprints, die Testanforderungen in Datensätzen in der Liste Penetrationstest-Sprints zugewiesen sind, unter anzeigen **Alle** > **Application Vulnerability Response** > **Administration** > **Penetrationstest-Konfiguration** > **Sprints konfigurieren**an. Siehe Konfigurieren Sie Sprints für Penetrationstests Weitere Informationen zum Konfigurieren von Sprints.

   Die Basiswerte für Bewertungstyp, Anwendungsgröße und geschätzter Aufwand sind:

   Formular zur Konfiguration des Bewertungstyps für Penetrationstests

Bewertungstyp	Anwendungsgröße	Geschätzter Aufwand (Stunden)
Fokussierter Test	Klein	20
Fokussierter Test	Mittel	30
Fokussierter Test	Groß	40
Fokussierter Test	Standard	40
Erneut Testen	Klein	10
Erneut Testen	Mittel	15
Erneut Testen	Groß	20
Erneut Testen	Standard	20
Vollständiger Penetrationstest	Klein	60
Vollständiger Penetrationstest	Mittel	70
Vollständiger Penetrationstest	Groß	80
Vollständiger Penetrationstest	Standard	80

4. Wählen Sie Aktualisieren aus, um Ihre Änderungen zu speichern, oder übermitteln Sie sie für einen neuen Datensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie vor v19.0 aus **Konfigurieren** Option für Konfigurieren von Bewertungstypen.
6. Aktualisieren Sie die Werte für die Bewertungstypen nach Bedarf.
   Basiswerte sind:

Formular zur Konfiguration des Bewertungstyps für Penetrationstests

Bewertungstyp	Geschätzter Aufwand (Stunden)
Fokussierter Test	40
Erneut Testen	20
Vollständiger Penetrationstest	80

7. Speichern Sie die Änderungen.

Integration von Application Vulnerability Response mit anderen Anwendungen

Vulnerability Response Enthält Unterstützung für Integrationen von Drittparteien.

Drittpartei-Integrationen

Integrationen von Anwendungsschwachstellen helfen, die Daten von Anwendungsschwachstellen in Ihrer Instanz zu ergänzen, indem Daten von externen Systemen und Lieferanten abgerufen werden. Weitere Informationen zu unterstützten Integrationen finden Sie in den folgenden Übersichtsthemen:

- Fortify Vulnerability Integration
- GitHub-Anwendungsschwachstellen-Integration
- Invicti-Schwachstellen-Integration
- Veracode Vulnerability Integration
- Vulnerability Response-Integration mit Black Duck
- Manuelle Erfassung von Schwachstellen für Application Vulnerability Response
- Atlassian-Jira-Integration

Wichtig:
Im Vulnerability Manager-Arbeitsbereich können Sie mit manuell ein Agile-Problem erstellen Listenaktion Und Formularaktion Um die Korrektur von AVITs und RTS nachzuverfolgen.

Hinweis:

Integrationen mit mehreren Quellen werden in nicht unterstützt Application Vulnerability Response. Drittpartei-Integrationen werden separat behandelt. Wenn in Ihrer Umgebung mehr als eine Drittanbieter-Integrationsanwendung verwendet wird, gibt es keine Deduplizierung von angreifbaren Anwendungselementen (AVI) über Integrationen hinweg.

Die folgende Tabelle enthält eine Liste von Application Vulnerability Response Von erstellte Integrationen ServiceNow® Und Partner, um Schwachstellen zu importieren und angreifbare Elemente zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response: Infrastrukturintegrationen

Lieferant	Lieferantenprodukt	Integrationszusammenfassung	Store-Link	Schlüsselfunktionen	Erzeugt von
Veracode	Dynamische Veracode-Analyse	Importieren Sie Test, Richtlinien, Ergebnisse Importieren Sie DAST-Ergebnisse Importieren Sie SAST-Ergebnisse Importieren Sie SCA-Ergebnisse			ServiceNow®
Qualys WAR					ServiceNow®
					ServiceNow®
					Partner
					ServiceNow®
					ServiceNow®
					Partner
					Partner
					Partner
					Partner
					Partner
					Partner
					Partner
					Partner
					Partner
					Partner
					Partner
					Partner
					Partner
					Partner
					Partner

Vulnerability Response Anwendungen Und CSDM Tabellen

Die Vulnerability Response, Application Vulnerability Response, Integrationen von Schwachstellen von Drittparteien und Software Bill of Materials Anwendungen verwalten (Daten mittragen zu) CSDM Tabellen. Diese Anwendungen verwenden auch Daten aus CSDM Tabellen, die andere

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen generieren. Mehrere ServiceNow Produkte profitieren daher von diesen und fügen ihnen einen Mehrwert hinzu Security Operations Anwendungen. Weitere Informationen finden Sie unter Vulnerability Response Anwendungen Und CSDM Tabellen.

Zusätzliche Hinweise für Integrationen

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Application Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Schwachstellenintegrationen für Application Vulnerability Response Sind für die geplante Ausführung konfiguriert. Sie können sie jedoch bei Bedarf manuell ausführen.

Erforderliche Rolle: sn_vul.App_read_Integrations

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Integrationen**an.
2. Öffnen Sie den Datensatz für die Integration, die Sie ausführen möchten.
3. Klicken Sie auf **Jetzt ausführen**.

Vulnerability Response-Integration mit Black Duck

Die Vulnerability Response Integration mit Vulnerability Response-Integration mit Black Duck Verwendet die Daten, die aus dem SCA-Tool (Black Duck Software Composition Analysis) importiert werden, um die Auswirkung und Priorität der Fehler in Ihrem Code zu bestimmen.

Integrationsübersicht

Mit Vulnerability Response-Integration mit Black Duck, Können Sie SCA erfassen und diese Daten für verfügbar machen ServiceNow AI Platform. Ab v22.0.5 von Vulnerability Response, Sie können die SCA-Schwachstellendaten in Ihre Instanz importieren, um die Schwachstellen in Ihren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Softwareanwendungen zu identifizieren. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Eine freigegebene API erfasst die SCA-Daten.

Hinweis:
Jeder Integrationsdatensatz hat einen konfigurierten Run-as-Anwender. Der Standardwert für diesen Anwender ist VR-System. Ändern Sie diesen Wert nicht.

Täglich rufen geplante Aufgaben die Integrationen automatisch in der Reihenfolge auf, in der sie aufgelistet sind. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Verfügbare Versionen

Black Duck-Integration – Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response-Integration mit Black Duck 1.0.5	Application Vulnerability Response release notes

Anwendergruppe und Rollen

Die Vulnerability Response-Integration mit Black Duck Wird von einem Anwender mit der Administratorrolle installiert und von einem Mitglied der App-Sec-Manager-Gruppe konfiguriert. Weitere Informationen finden Sie im Abschnitt Application Vulnerability Response Anwendergruppen und Rollen.

Informationen zu Status der Integrationsausführung finden Sie unter Zeigen Sie an Vulnerability Response-Integration mit Black Duck Importausführungsstatus

Informationen zum Anzeigen von Daten in den Schwachstellen von Drittparteien finden Sie unter Schwachstellenbibliotheken anzeigen.

Bereiten Sie Aufgaben vor der Integration für vor Vulnerability Response-Integration mit Black Duck

Planen und führen Sie die Aufgaben vor der Integration für aus Vulnerability Response-Integration mit Black Duck Damit Ihre Integration erfolgreich ist. Die Vulnerability Response-Integration mit Black Duck Es wird davon ausgegangen, dass Sie mit der Anwendung „Black Duck Software Composition Analysis“ (SCA) und den APIs vertraut sind.

Vorbereitungen
Bevor Sie installieren und konfigurieren Vulnerability Response-Integration mit Black Duck, Sie sollten die CWE-Integration (Common Weekness Enumeration) ausführen und installieren, die auch von verwendet wird Application Vulnerability Response. Die CWE-Integration wird mit installiert Vulnerability Response Standardmäßig.

Hinweis:
Obwohl die NIST Vulnerability Database (NVD)-Daten nicht erforderlich sind, um die Black Duck Application Vulnerability Integration zu installieren, wäre es nützlich, wenn Sie haben. Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jeder Integrationsdatensatz hat einen konfigurierten Run-as-Anwender. Der Standardwert für diesen Anwender ist VR.System. Ändern Sie diesen Wert nicht.

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen vor, die Ihren Anforderungen entsprechen.

Validieren Sie die Größenanpassung Ihrer Instanz anhand der Anzahl der angreifbaren Anwendungselemente, die Sie importieren möchten. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.

Die Vulnerability Response-Integration mit Black Duck Erfordert eine API-URL und ein API-Token.

Prozedur

Erstellen Sie das API-Token und die Schlüssel-Anmeldeinformationen.

a. Melden Sie sich bei der Black Duck-Plattform an.

b. Wechseln Sie zum Anwenderaccount-Menü, und wählen Sie aus **API-Anmeldeinformationen** .

c. Wählen Sie Aus **Generieren Sie API-Anmeldeinformationen** .

d. Zeichnen Sie Ihre Anmeldeinformationen zur späteren Verwendung auf.

Installieren Sie ServiceNow Vulnerability Response-Integration mit Black Duck

Bevor Sie die Integration in Ihrer Instanz ausführen, müssen Sie die Installations- und Konfigurationsschritte abschließen, damit das SCA-Tool (Black Duck Software Composition Analysis) ordnungsgemäß in integriert wird Application Vulnerability Response.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Sie müssen diese Setup-Aufgaben ausführen, damit das SCA-Tool (Black Duck Software Composition Analysis) ordnungsgemäß in integriert wird Application Vulnerability Response.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Setupaufgaben

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben (Fortsetzung)

Setupaufgaben	Beschreibung
	Wenn die Anwendung nicht installiert und aktiviert ist, finden Sie weitere Informationen unter Vulnerability Response installieren.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Wenn nicht bereits zugewiesen, installiert der Anwender mit der Administratorrolle die Anwendung und weist Anwender der App-Sec-Manager-Gruppe zu. Informationen zu Gruppenrollen finden Sie unter Application Vulnerability Response Anwendergruppen und Rollen. • Die App-SEC-Manager-Gruppe überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Dieses SCA-Tool ist als separates Abonnement verfügbar.

Prozedur

1. Melden Sie sich bei der Instanz an, die Sie installieren möchten Vulnerability Response-Integration mit Black Duck Ein.
2. Navigieren Sie zum ServiceNow Store.
3. In ServiceNow Store, Suchen Sie nach Vulnerability Response Integration mit der Black Duck-Anwendung.
4. Wählen Sie die Anwendungskachel aus.
   Die Details zur Anwendung, die Sie installieren, werden angezeigt.

   Hinweis:
   Lesen Sie ggf. die Abschnitte über weitere Anforderungen und Abhängigkeiten.

5. Wählen Sie Aus **App Anfordern** Und geben Sie ein Now Support Anmeldeinformationen.
6. Wählen Sie Aus **Abrufen** .
7. Geben Sie den Instanznamen und den Grund für die Instanz ein, und wählen Sie aus **Validieren Sie Die Instanz** .
8. Wählen Sie Aus **Anforderung** .
   Sie erhalten eine E-Mail mit den detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**an.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen Sie aus **Installieren** .
    Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Konfigurieren Sie Vulnerability Response-Integration mit Black Duck Für Ihre Umgebung. Siehe Konfigurieren Sie die Eigenschaften Vulnerability Response-Integration mit Black Duck

Konfigurieren Sie die Eigenschaften Vulnerability Response-Integration mit Black Duck

Bevor Sie ausführen Vulnerability Response-Integration mit Black Duck In Ihrer Instanz müssen Sie die Installations- und Konfigurationsschritte abschließen, damit das SCA-Tool (Black Duck Software Composition Analysis) ordnungsgemäß in integriert wird Application Vulnerability Response Anwendung.

Vorbereitungen

Erforderliche Rolle: App-Sec Manager-Anwendergruppe

Warum und wann dieser Vorgang ausgeführt wird

Die Vulnerability Response-Integration mit Black Duck Ist als separates Abonnement verfügbar.

Prozedur

1. Navigieren zu **Alle** > **Blackduck-Schwachstellenintegration** > **Konfiguration**an.
2. Wählen Sie den Typ Standardauthentifizierung aus.
   Für die Standardauthentifizierung ist ein erforderlich MID-Server Für Instanzen, die lokal sind. Sie können das API-Token, das für die Standardauthentifizierung erforderlich ist, aus Ihrem Black Duck-Account generieren.
3. Füllen Sie im Formular die Felder aus.
   Basic Authentication

Feld	Beschreibung
API-URL	Black Duck-API-URL für Enterprise- oder On-Premise-Instanzen. Die lokale Instanz ist Ihre Black Duck-Endpunkt-URL.
API-Token	Token, das Sie über Ihre Black Duck-Konsole generiert haben.
MID-Server	MID-Server Dies ist für Instanzen erforderlich, die für die Standardauthentifizierung lokal sind.
SCA einbeziehen	Schwachstellen aus SCA-Scans (Software Composition Analysis), die standardmäßig enthalten sind. SCA-Scans identifizieren die Schwachstellen in Open Source-Komponenten.
Wählen Sie die Option zum Verwalten falsch positiver Ergebnisse in ServiceNow aus	ServiceNow Option zum Verwalten falsch positiver Ergebnisse. Lassen Sie diese Option aktiviert, wenn Sie die importierten angreifbaren Anwendungselemente (Avis) mit selektieren möchten **Quelle** status, die als markiert sind **Falsch Positiv** Oder **Potenziell Falsch Positiv** . Avis mit diesen **Quelle** status, die normalerweise einem zugeordnet sind **Geschlossen** status in Ihrer Instanz sind zugeordnet **Öffnen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie können einen anfordern **Falsch positiv** Aus dem AVI-Datensatz. ○ Deaktivieren Sie eine oder beide Optionen, wenn Sie beibehalten möchten **Quelle** status, die von Ihrem Scanner importiert wurden. ○ Wenn deaktiviert, wird **Ausnahme anfordern** Und **Falsch Positiv** Aktionen sind in Avis nicht sichtbar.
Integrationsinstanz	Instanz, die Sie zum Importieren der Daten verwenden.

4. Wählen Sie Aus **Anmeldeinformationen speichern und testen** .
5. Führen Sie aus **Integration Der Black Duck-Projektliste** Bevor Sie andere Integrationen ausführen. Die anderen Black Duck-Integrationen, z. B. Black Duck Application List Integration und Black Duck Application Angreifbare Item Integration, hängen von den aktuellen Projekt- und Anwendungsdaten ab, die Sie aus der Projektlistenintegration importiert haben.

Zeigen Sie an Vulnerability Response-Integration mit Black Duck Importausführungsstatus

Überprüfen Sie den Erfolg Ihrer Integrationsausführungen, suchen Sie nach Problemen, und bestätigen Sie Ihre Korrekturentscheidungen, indem Sie die zugehörige Liste „Ausführungen der Schwachstellenintegration“ anzeigen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Blackduck-Schwachstellenintegration** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
3. Wählen Sie die zugehörige Liste Vulnerability Integration Ausführungen aus.
4. Überprüfen Sie, ob alle Importe erfolgreich waren.
   Problembehandlung:

   Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:

   ○ Netzwerkunterbrechung.

   ○ Ein Problem bei der Datenübertragung, das während einer Transformation zu beschädigten Daten führt.

   Wenn eine dieser Bedingungen auftritt, wählen Sie aus **Jetzt Ausführen** , Und führen Sie die Integration erneut aus.
5. Zeigen Sie die importierten Repositorys an, indem Sie zur Integrationsliste navigieren und den Black Duck-Integrationsdatensatz auswählen.
6. Wählen Sie die zugehörige Liste Vulnerability Integration wird ausgeführt, und öffnen Sie einen Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datentransformation für Vulnerability Response-Integration mit Black Duck

Nachdem Sie die Daten identifiziert haben, die Sie importieren möchten, werden die Daten aus dem abgerufen Vulnerability Response-Integration mit Black Duck, Wurde durch eine Reihe von Datenquellen verarbeitet und in Ihrer Instanz umgewandelt.

Vulnerability Response-Integration mit Black Duck

Die Daten aus der API werden zuerst in die Tabelle „Black Duck AppVul Item Import“ [sn_vul_blackduck_appvul_item_Import] geladen, und die Black Duck AppVul Item Transform wird zum Transformieren der importierten Informationen verwendet.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen** Und suchen Sie nach **Black Duck AppVul-Elementtransformation** . In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Transformationszuordnungsfelder für AppVul-Element „Black Duck“

Quellenfeld	Zielfeld	Beschreibung
app_id	Quell_App_ID	Anwendungs-ID.
Ausstellende ID	Source_avit_ID	AVIT-ID.
app_name	app_name	Anwendungsname.
Version	App_Version	Anwendungsversion.
Build_ID	Source_Scan_ID	Build-ID der Anwendung.
account_id	account_id	Account-ID.
Sandbox_ID	Sandbox_ID	Sandbox-ID.
Last_Update_time	Last_Scan_date	Zeitpunkt der letzten Aktualisierung.
App_Name + Last_Scan_date	Scan_Summary_Name	Scan-Zusammenfassung.
life_cycle_stage	Source_sdlc_Status	SDLC-Status der Quelle.
level	Source_severity	Quellenschweregrad.
Category_Name	Kategorie	Kategorie.
Source_severity	Source_severity	Quellenschweregrad.
Category_ID + „ CWE-“ + CweId	Source_entry_ID	Quelleintrags-ID.
Source_Vulnerability_summary	Source_Vulnerability_summary	Zusammenfassung der Quell-Schwachstelle.
Source_Recommendation	Source_Recommendation	Quellempfehlung.
Beschreibung	Beschreibung	Beschreibung aus der Quelle.
Beschreibung	Source_Vulnerability_explanation	Erklärung der Quell-Schwachstelle.
Mitigation_Status_desc	Source_Mitigation_Status	Quellminderungsstatus.
Remediation_Status	Source_Remediation_Status	Quellkorrekturstatus.
Zeile	Line_number	Position, in der der Fehler gefunden wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transformationszuordnungsfelder für AppVul-Element „Black Duck“ (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
Modul	Application_Module	Anwendungsmodul.
Quelldatei	Source_Notes	Quellnotizen.
Betrifft_Richtlinie_Compliance	Erfüllt_mit_Richtlinie	Werte können „Ja“ oder „Nein“ sein, je nachdem, ob die Quellinformationen „wahr“ oder „falsch“ sind.
Sourcefilepath + sourcefile	location	Standortzuordnung eines statischen Fehlers.
URL	location	Standortzuordnung für einen dynamischen Fehler.
Umfang, Typ, exploitLevel	Source_additional_info	Namenswertfeld, das mit den Werten aus der Quelle für statische Fehler ausgefüllt ist.

In der folgenden Tabelle sind die Transformationsskripts aufgeführt, die während des Transformationsprozesses ausgeführt werden.

Black Duck-Transformationszuordnungs-Skriptzeitpunkt und -Zweck

Black Duck-Transformationszuordnungsskript

Wenn das Skript ausgeführt wird	Zweck
Beim Start (Wenn ein Importsatz eine Transformation erstellt hat).	Skript, das verwendet wird, um den Datensatz zu verarbeiten und die Anzahl der erstellten, aktualisierten oder unveränderten Entitäten sowie der Entitäten zu aktualisieren, die als Teil dieser Integration importiert werden. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.
OnBefore (Bevor die Transformation eines Importsatzes abgeschlossen ist)	Skript, das zum Definieren des Verhaltens für Datensätze verwendet wird, die ungültig sind und ignoriert werden müssen. Wird auch verwendet, um das globale Objekt für die Datensatzverarbeitung zu definieren. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Black Duck-Integrationsstatuszuordnung

Die folgende Tabelle zeigt die quellstatus aus der Black Duck Vulnerability Integration und ihre zielstatus in Ihrer Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Black Duck-quellstatus und die entsprechenden ServiceNow AI Platform status

Black Duck-quellstatus	Beschreibung der quellstatus	Zielstatus in ServiceNow AI Platform
Neu	Schwachstelle betrifft diese Komponentenversion.	Öffnen
Benötigt Überprüfung	Es kann nicht bestimmt werden, ob eine Schwachstelle diese Komponentenversion betrifft.	Öffnen
Korrektur Erforderlich	Für diese Version ist eine Korrektur erforderlich.	Öffnen
Korrektur abgeschlossen	Die Korrektur für diese Schwachstelle ist abgeschlossen.	Geschlossen
Gemindert	Schwachstelle wurde gemindert.	Geschlossen
Gepatcht	Schwachstelle wurde gepatcht.	Geschlossen
Ignoriert	Schwachstelle wurde ignoriert.	Geschlossen

Importieren Sie die Projektinformationen aus der Black Duck-Integrationsinstanz

Importieren Sie die Projektinformationen aus der Black Duck-Integrationsinstanz, um sicherzustellen, dass die Schwachstellenintegrationen sequenziell ausgeführt werden. Eine erfolgreiche Integration hilft Ihnen, die angreifbaren Anwendungselemente (Avis) zu identifizieren und zu erfassen.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Sie können alle Projektinformationen aus importieren Vulnerability Response-Integration mit Black Duck In der Tabelle [sn_vul_blackduck_project] Black Duck Projects. Alle erforderlichen Attribute, z. B. Projekt-GUID, die zum Abfragen verschiedener Versionen des Projekts erforderlich sind, werden in der Tabelle [sn_vul_blackduck_project] Black Duck Projects erfasst.

Prozedur

1. Navigieren zu **Alle** > **Blackduck-Schwachstellenintegration** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
   Sie können beispielsweise auswählen **Integration Der Black Duck-Projektliste.**
3. Wählen Sie **Jetzt ausführen**.

Hinweis:
Jeweils Vulnerability Response-Integration mit Black Duck Soll den vollständigsten Datenabruf bieten. Wenn diese Integrationen nicht ordnungsgemäß ausgeführt werden, kann dies zu unvollständigen Daten führen und erfordert ServiceNow Und Application Vulnerability Response-Expertise.

Nachdem der Import abgeschlossen ist, können Sie die Projektdetails in der Tabelle [sn_vul_blackduck_project] Black Duck Projects anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Informationen zu Status der Integrationsausführung finden Sie unter Zeigen Sie an Vulnerability Response-Integration mit Black Duck Importausführungsstatus.
5. **Wahlweise:** Wenn Sie andere Integrationsparameter ändern möchten, müssen Sie zur Integrationsinstanz navigieren.

Importieren Vulnerability Response-Integration mit Black Duck Projektversionen der Tabelle „erkannte Anwendungen“

Importieren Sie die Vulnerability Response-Integration mit Black Duck-Projektversionen in die Tabelle „erkannte Anwendungen“ [sn_vul_Release], damit die Black Duck-Schwachstellenintegrationen sequenziell ausgeführt werden. Eine erfolgreiche Integration hilft Ihnen, die angreifbaren Anwendungselemente (Avis) zu identifizieren und zu erfassen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird
Sie können alle verschiedenen Versionen der Projekte hinzufügen und anzeigen (Details finden Sie in der Tabelle „Black Duck-Projekte“), die aus importiert wurden Vulnerability Response-Integration mit Black Duck In der Tabelle „erkannte Anwendungen“ [sn_vul_Release].

Prozedur
1. Navigieren zu **Alle** > **Blackduck-Schwachstellenintegration** > **Integrationen** an.
2. Wählen Sie eine Integration aus.
   Sie können beispielsweise auswählen **Integration Der Black Duck-Anwendungsliste** .
3. Wählen Sie **Jetzt ausführen**.

   Hinweis:
   Jede Projektversion der Integrationen soll einen möglichst vollständigen Datenabruf bieten. Wenn diese Integrationen nicht ordnungsgemäß ausgeführt werden, kann dies zu unvollständigen Daten führen und erfordert Fachwissen von ServiceNow und Application Vulnerability Response.

   Nachdem der Import abgeschlossen ist, können Sie die verschiedenen Versionen eines Projekts in der Tabelle „erkannte Anwendungen“ [sn_vul_Release] anzeigen. Wenn Sie CI-Suchregeln verwenden, sind diese erkannten Anwendungen mit der Tabelle „Konfigurationselement“ [cmdb_ci] verknüpft.
4. Zeigen Sie den Status Ihrer Integrationsausführungen an.
   Weitere Informationen finden Sie unter Zeigen Sie an Vulnerability Response-Integration mit Black Duck Importausführungsstatus.

Importieren Sie die angreifbaren Anwendungselemente aus dem Vulnerability Response-Integration mit Black Duck

Importieren Sie die angreifbaren Anwendungselemente (Avis) aus der Vulnerability Response-Integration mit Black Duck, damit die Integration sequenziell ausgeführt wird. Eine erfolgreiche Integration hilft Ihnen, Avis zu identifizieren und zu erfassen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird
Sie können die Scan-Ergebnisse in anzeigen Vulnerability Response-Integration mit Black Duck Fügen Sie Avis in Ihre Instanz ein, und reichern Sie Ihre Schwachstellendaten von Drittparteien an. Wenn sich der Scannerdatensatz im Status Geschlossen befindet, werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Avis standardmäßig nicht erstellt. Sie können vorhandene Avis mithilfe der Eigenschaft sn_vul_create_closed steuern.

Prozedur

1. Navigieren zu **Alle** > **Integration Von Black Duck-Schwachstellen** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
   Sie können beispielsweise auswählen **Black Duck-Anwendung – Integration Angreifbarer Elemente** .
3. Wählen Sie **Jetzt ausführen**.

Hinweis:
Die Vulnerability Response-Integration mit Black Duck Soll Ihnen den vollständigsten Datenabruf bieten. Wenn diese Integrationen nicht ordnungsgemäß ausgeführt werden, kann dies zu unvollständigen Daten führen und erfordert ServiceNow Und Application Vulnerability Response Fachwissen.

Nachdem Sie alle SCA-Schwachstellen aus importiert haben Vulnerability Response-Integration mit Black Duck, Sie können die Avis- und Schwachstellendaten von Drittparteien anzeigen.

Legen Sie die Importzeiten für fest Vulnerability Response-Integration mit Black Duck

Legen Sie die Startzeit für fest Vulnerability Response-Integration mit Black Duck Importe. Sie können die Integrationen im Voraus festlegen, um eine bessere Leistung und schnellere Importausführungen zu erzielen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird
Nach dem ersten Import führen die Black Duck-Schwachstellenintegrationen jedes Mal einen vollständigen Import durch.

Prozedur

1. Navigieren zu **Alle** > **Integration Von Black Duck-Schwachstellen** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
3. Legen Sie das neue fest **Startzeit** .
   Die Zeit wird als Stunden in Ortszeit berechnet. Die Standardzeit für die Black Duck Application List Integration-Importe ist 00:00:00. Die anderen Integrationen sind **Bei Bedarf** Und sind verkettet, was bedeutet, dass sie einer Sequenz folgen, die nach der Integration der Black Duck-Anwendungsliste ausgeführt wird. Ändern von **Startzeit** Erfordert Advanced ServiceNow Und Application Vulnerability Management Fachwissen.
4. Wählen Sie **Aktualisieren**.
   Die neue Zeit wird für den nächsten geplanten Import verwendet.

Schließen Sie geschlossene angreifbare Black Duck-Anwendungselemente ein

Schließen Sie geschlossene angreifbare Anwendungselemente (Avis) während der Black Duck-Integrationsimporte für angreifbare Elemente ein, da sie standardmäßig nicht während der Integrationsimporte erstellt werden. Wenn Sie sie erstellen möchten, müssen Sie die Systemeigenschaft ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass Vulnerability Response-Integration mit Black Duck Ist installiert und wird ausgeführt.

Erforderliche Rolle: Administrator

Prozedur

1. Geben Sie im Navigationsfilter sys_properties.list ein.
2. In **Name** Feld für die Liste eingeben sn_vul.create_closed .
3. Doppelklicken Sie auf **Wert** Feld und legen Sie es auf fest **Wahr**
4. Speichern Sie, indem Sie auf das grüne Häkchensymbol klicken .
   Die Datensätze im Status Geschlossen beim nächsten Black Duck-Import werden als Avis in erstellt Application Vulnerability Response.

Fortify Vulnerability Integration

Die Fortify Vulnerability Integration Verwendet Daten, die aus importiert wurden Fortify Produkt, mit dem Sie die Auswirkung und Priorität von Fehlern in Ihrem Code bestimmen können.

Fortify Vulnerability Integration

Die Fortify Das Produkt sammelt Scannerdaten und stellt diese Daten dem zur Verfügung ServiceNow AI Platform®. Es lässt sich problemlos in integrieren ServiceNow® Application Vulnerability Response Funktion von Vulnerability Response Dient zum Zuordnen von Schwachstellen von Drittparteien, um die Daten in Ihrer Instanz zu ergänzen.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Geplante Aufgaben rufen die Integrationen jeden Tag automatisch auf. Sobald alle Integrationen aktiviert sind, werden sie so verkettet, dass sie in der Reihenfolge ausgeführt werden. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Vulnerability Response-Integration mit Fortify V2.4 Fortify v2.3 Fortify v2.2 Fortify v2.1	Application Vulnerability Response release notes Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fortify Vulnerability Integration

Um anzuzeigen Fortify Vulnerability Integration, Navigieren Sie zu **Fortify-Schwachstellenintegration** > **Integrationen**an.

Die folgenden Integrationen sind im Basissystem enthalten. Diese Integrationen sind standardmäßig nicht alle aktiv.

Nach der ersten Ausführung werden täglich geplante Aufgaben verkettet, um die Integrationen automatisch in der Reihenfolge auszuführen. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Fortify Schwachstellenintegrationen

Integration	Beschreibung
Fortify Integration der Anwendungsliste bei Bedarf	Ruft Ab Fortify Anwendungsscannerdaten (Schwachstellen, Metadaten) und ergänzt Ihre Anwendungsdaten von Drittparteien. Diese Integration ist so festgelegt, dass sie täglich um 00:00:00 ausgeführt wird. Standardmäßig ist sie aktiv.
Fortify Zusammenfassungsintegration für Scan bei Bedarf	Ruft Scan-Datensätze von ab Fortify. Diese Integration ist so verkettet, dass sie nach ausgeführt wird Fortify Integration der Anwendungsliste bei Bedarf, wenn aktiviert. Standardmäßig ist er inaktiv.
Fortify Integration angreifbarer Elemente für Anwendungen bei Bedarf	Ruft Scan-Ergebnisse von ab Fortify, Fügt AVITs ein und ergänzt Ihre Schwachstellendaten von Drittparteien. Wenn sich der Scannerdatensatz in befindet **Geschlossen** status, AVITs werden nicht erstellt. Vorhandene AVITs werden noch aktualisiert. Zeigen Sie ab v2.3 Details an, z. B. Gesamtverarbeitungszeiten, durchschnittliche Zeiten für Prozesse vor und nach der Integrationsausführung und Berichte zu den Datensätzen der Integrationsausführung für die Integration angreifbarer Anwendungselemente. Diese Integration ist so verkettet, dass sie nach ausgeführt wird Fortify Zusammenfassungsintegration für Scan bei Bedarf, wenn aktiviert. Standardmäßig ist er inaktiv.

Informationen zu Status der Integrationsausführung finden Sie unter . Zeigen Sie an Fortify Vulnerability Integration Importausführungsstatus.

Informationen zum Anzeigen von Daten in Schwachstellen von Drittparteien finden Sie unter Schwachstellenbibliotheken anzeigen.

Vorbereitung für Fortify Vulnerability Integration

Ein erfolgreich Fortify Vulnerability Integration Erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die Fortify Vulnerability Integration Davon ausgegangen, dass Sie mit vertraut sind Fortify Produkt und API.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Die CWE-Integration (Common Weakness Enumeration) wird auch von verwendet Application Vulnerability Response Und sollten vor der Installation und Konfiguration von ausgeführt werden Fortify Vulnerability Integration.

Hinweis:
NIST Vulnerability Database (NVD)-Daten sind zum Installieren von nicht erforderlich Fortify Vulnerability Integration, Jedoch bieten sie Ergänzungen und wären nützlich.

Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Erforderliche Rolle: App-Sec-Manager

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Validieren Sie die Größenanpassung Ihrer Instanz basierend auf der Anzahl der angreifbaren Anwendungselemente, die Sie importieren möchten. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.

Die Fortify Vulnerability Integration Erfordert einen API-Schlüssel, ein API-Geheimnis und eine API-Stamm-URL, die über verfügbar sind Fortify Account bei Bedarf.

Prozedur

So erstellen Sie einen geheimen API-Schlüssel:

a. Melden Sie sich bei an Fortify On-Demand-Portal.

b. Navigieren zu **Alle** > **Administration** > **Einstellung** > **API**an.

c. Fügen Sie ServiceNow als Anwendung hinzu.

d. Klicken Sie Auf **Neues Geheimnis** Dient zum Generieren eines API-Geheimnisses.

e. Zeichnen Sie Ihr API-Geheimnis zur späteren Verwendung auf.

Installieren Sie ServiceNow® Vulnerability Response-Integration mit Fortify

Bevor Sie die Integration auf Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit die ausgeführt werden kann Fortify Produkt ist ordnungsgemäß in integriert Application Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist Anwender der App-Sec-Manager-Gruppe zu. Informationen zu Gruppenrollen finden Sie unter . Application Vulnerability Response Anwendergruppen und Rollen. • Die App-SEC-Manager-Gruppe überwacht die Konfiguration und verifiziert die erwarteten Ergebnisse.

Erforderliche Rolle: App-Sec-Manager

Prozedur

1. Melden Sie sich bei der Instanz an, die Sie installieren möchten Fortify Vulnerability Integration Ein.
2. Navigieren Sie zum ServiceNow Store.
3. In ServiceNow Store, Suchen Sie mit nach Vulnerability Response-Integration Fortify Anwendung.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Erwägen Sie, das zu lesen **Andere Anforderungen** Und **Abhängigkeiten** Abschnitte, falls zutreffend.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Nächste Maßnahme

Konfigurieren Sie Fortify Vulnerability Integration Für Ihre Umgebung. Weitere Informationen finden Sie unter Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integration.

Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integration

Bevor Sie die Integration auf Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit die ausgeführt werden kann Fortify Das Produkt ist ordnungsgemäß in integriert Application Vulnerability Response Funktion von Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Erforderliche Rollen: App-Sec-Manager

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.
Überprüfen Sie, ob Vulnerability Response Integration mit Fortify Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Installieren Sie ServiceNow Vulnerability Response-Integration mit Fortify.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	• Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die App und weist Anwender der App-Sec-Manager-Gruppe zu. • Der App-SEC-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.
Für Fortify Vulnerability Integration, Haben Sie **API-ID** Und **API-Schlüssel** Bereit.	Kontakt Fortify Um zu erhalten **API-ID** Und **API-Schlüssel** .

Prozedur

1. Melden Sie sich bei der Instanz an, die Sie installieren möchten Fortify Integrationen von Anwendungsschwachstellen auf.
2. Navigieren Sie zum ServiceNow Store.
3. In ServiceNow Store, Suchen Sie nach Vulnerability Response Integration mit Fortify Anwendung.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Erwägen Sie, das zu lesen **Andere Anforderungen** Und **Abhängigkeiten** Abschnitte, falls zutreffend.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**an.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.
11. Sobald die Installation abgeschlossen ist, navigieren Sie zu **Fortify-Schwachstellenintegration** > **FoD-Konfiguration**an.
12. Füllen Sie im Formular die Felder aus.

Fortify on Demand-Konfigurationsformular

Feld	Beschreibung
API-Stamm-URL	Fortify-Instanz-URL des Anwenders.
API Key	Eindeutiger Bezeichner an gesendet Fortify API.
Geheimer API-Schlüssel	Geheimer Clientschlüssel bereitgestellt von Fortify.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
DAST einbeziehen	Option zum Einbeziehen von Schwachstellen aus DAST-Scans. DAST-Scans identifizieren Schwachstellen im Verhalten Ihrer Gesamtanwendung.
SAST einbeziehen	Option zum Einbeziehen von Schwachstellen aus SAST-Scans. SAST-Scans identifizieren Schwachstellen im Code.
Selektierungsausnahmen und falsch positive Ergebnisse in ServiceNow (ab v20.0 von Vulnerability Response)	Wählen Sie Optionen aus, um die Ausnahmemanagement und falsch positiv für Avis mit zu verwalten ServiceNow Workflows automatisch beim Import. Diese Optionen sind standardmäßig aktiviert. Ein Beispiel für einen Anwendungsfall finden Sie unter Statuszuordnung für Zurückstellungen und falsch positive Ergebnisse in verwalten Application Vulnerability Response. **Verwalten Sie Ausnahmen in ServiceNow** Lassen Sie diese Option aktiviert, wenn Sie importierte Avis selektieren möchten, die für markiert sind **Zurückgestellt** status. Avis mit **Quelle** status, die normalerweise einem zugeordnet sind **Zurückgestellt** status in Ihrer Instanz werden stattdessen zugeordnet **Öffnen** . Sie **Fordern Sie eine Ausnahme an** Aus dem AVI-Datensatz. **Verwalten Sie falsch positive Ergebnisse in ServiceNow** Lassen Sie diese Option aktiviert, wenn Sie importierte Avis mit selektieren möchten **Quelle** status markiert als **Falsch Positiv** Oder **Potenziell Falsch Positiv** . Avis mit diesen **Quelle** status, die normalerweise einem zugeordnet sind **Geschlossen** status in Ihrer Instanz sind zugeordnet **Öffnen** . Sie fordern an **Falsch positiv** Aus dem AVI-Datensatz. ○ Deaktivieren Sie ein oder beide Kontrollkästchen, wenn Sie beibehalten möchten **Quelle** status, die von Ihrem Scanner importiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Diese Avis werden den status Ziel- und Zielgrund zugeordnet, wenn sie importiert werden, werden jedoch nicht von den Ausnahmen- und falsch positiven Workflows selektiert. Die **Ausnahme anfordern** Und **Falsch Positiv** Aktionen sind in Avis nicht sichtbar.
Selektierung in ServiceNow (vor v20.0 von Vulnerability Response)	Verwalten Sie Ihre Anwendungsschwachstellen-Selektierung in ServiceNow Instanz: ○ Aktivieren Sie das Kontrollkästchen, um die Avis in auszuwählen ServiceNow. Wenn diese Option ausgewählt ist, werden Avis im Status „Offen“ importiert. Sie können dann eine Ausnahme anfordern oder die AVI als falsch positiv markieren. ○ Um den Quellstatus beizubehalten, d. h. den vom Scanner importierten Status, stellen Sie sicher, dass das Kontrollkästchen nicht aktiviert ist. **Hinweis:** Die **Als falsch positiv markieren** Und **Ausnahme Anfordern** Optionen sind nur für Avis verfügbar, die innerhalb von selektiert werden ServiceNow.

13. Wählen Sie Aus **Anmeldeinformationen speichern und testen** .

Nächste Maßnahme

Wenn Ihre Umgebung domänengetrennte Importe erfordert, finden Sie weitere Informationen unter Erstellen Sie domänengetrennte Importe für eine Integration.

Informationen zur Erstinstallation finden Sie unter Application Vulnerability Response konfigurieren Für weitere Anweisungen.

Änderungen finden Sie nach der Erstinstallation unter Fortify Vulnerability Integration Änderung und Aktivitäten.

Zeigen Sie an Fortify Vulnerability Integration Importausführungsstatus

Verwenden Sie **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Korrekturentscheidungen zu unterstützen.

Vorbereitungen

Um anzuzeigen Fortify Importausführungsstatus:

- Die Vulnerability Response Und Fortify Vulnerability Integration Anwendungen müssen installiert und konfiguriert sein.
- Die Fortify Vulnerability Integration Importe müssen geplant und ausgeführt werden.

Erforderliche Rolle: App-Sec-Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Application Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur

1. Navigieren zu **Alle** > **Fortify-Schwachstellenintegration** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste.
4. Überprüfen Sie, ob alle Importe erfolgreich waren.
5. Zeigen Sie ab v2.3 Details an, z. B. Gesamtverarbeitungszeiten, durchschnittliche Zeiten für Prozesse vor und nach der Integrationsausführung und Berichte zu den Datensätzen der Integrationsausführung für die Integrationen angreifbarer Anwendungselemente.

Fortify Vulnerability Integration Änderung und Aktivitäten

Konfigurieren Sie optionale Änderungen speziell für Fortify Vulnerability Integration.

Hinweis:
Ändern anderer Fortify Vulnerability Integration Andere Einstellungen als die hier aufgeführten erfordern erweiterte Einstellungen ServiceNow Und Application Vulnerability Response Fachwissen und übersteigt den Umfang der Produktdokumentation.

Führen Sie ein Handbuch durch Fortify Import von Anwendungsschwachstellen

Wenn Ihr anfänglicher Import fehlgeschlagen ist oder Sie nicht auf den geplanten anfänglichen Import warten möchten, können Sie unabhängig von der täglichen geplanten Aufgabe einen vollständigen Datenimport durchführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager

Prozedur
1. Navigieren zu **Alle** > **Fortify-Schwachstellenintegration** > **Integrationen**an.
2. Wählen Sie eine Integration aus, z. B. die Fortify Integration Der Anwendungsliste.
3. Wählen Sie **Jetzt ausführen**.

> **Hinweis:**
> Führen Sie für einen vollständigen Datenabruf die Fortify-Anwendungsschwachstellenintegrationen in der Reihenfolge aus.

Importieren Sie Daten mit Fortify Vulnerability Integration

Importieren Sie Daten aus dem Fortify-Scanner, um angreifbare Anwendungselemente (Avis) zuzuordnen, und ergänzen Sie dadurch die Daten in Ihrer Instanz.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager

Warum und wann dieser Vorgang ausgeführt wird
Nach dem ersten Import Fortify Schwachstellenintegrationen führen bei jeder Ausführung einen Delta-Import durch, wobei die neuesten Daten abgerufen werden. Siehe Führen Sie ein Handbuch durch Fortify Import von Anwendungsschwachstellen Weitere Informationen zu vollständigen Importen.

Prozedur
1. Navigieren zu **Alle** > **Fortify-Schwachstellenintegration** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
3. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Name	Name der Integrationsausführung.
Aktiv	Option zum Aktivieren einer Integration.
Ausführen	Häufigkeit der Integrationsausführung.
Zeit	
Anwendung	Anwendung, die diesen Datensatz enthält.
Quellenintegration	Quellintegration für diese Integration.
Quellinstanz	Quellinstanz für diese Integration.
Nächste Integration	Next-in-Sequence-Integration, die nach der aktuellen Integrationsausführung ausgeführt werden soll.
Startzeit	Startdatum und -Uhrzeit der letzten erfolgreichen Integrationsausführung. Die Zeit wird als Stunden in Ortszeit berechnet. Die Standardzeit für die erste Ausführung ist 00:00:00.
Integrationsdetails	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Integrationsskript	Skripteinbindung, die erweitert `VulnerabilityIntegrationBase`Wird ausgeführt, wenn die Integration ausgeführt wird. Dieses Skript definiert, wie Daten aus einem Drittparteisystem abgerufen werden.
Integrationswerksskript	Skript, das definiert, wie die für das Integrationsskript ausgewählte Skripteinbindung erstellt wird.
Berichtsprozessorstrategie	Strategie, die Sie verwenden möchten, um die Daten zu verarbeiten, die vom Integrationsskript zurückgegeben werden, wenn die Integration ausgeführt wird.

4. Wählen Sie Aus **Jetzt Ausführen** Zum Ausführen der Integration.

Schließen Sie geschlossene angreifbare Fortify-on-Demand-Anwendungselemente ein

Standardmäßig **Geschlossen** Angreifbare Anwendungselemente (AVITs) werden während nicht erstellt Fortify Integrationsimporte für angreifbare Elemente. Wenn Sie sie erstellen möchten, müssen Sie eine Systemeigenschaft ändern.

Vorbereitungen

Die Fortify Vulnerability Integration Muss installiert sein und ausgeführt werden.

Erforderliche Rolle: App-Sec-Manager

Prozedur

1. In der linken Navigation **Filternavigator** Textfeld, Typ `sys_properties.list` .
2. In **Name** Suchfeld für die Liste eingeben `sn_vul.create_closed` .
3. Doppelklicken Sie auf **Wert** Feld und auf festgelegt **Wahr**
4. Klicken Sie auf das grüne Häkchensymbol Zum Speichern.
   Datensätze in **Geschlossen** status im nächsten Fortify Importe werden als AVITs in erstellt Application Vulnerability Response.

GitHub-Anwendungsschwachstellen-Integration

Die GitHub-Anwendungsschwachstellen-Integration Importiert SAST-Daten (Static Application Security Testing) und SCA-Daten (Software Composition Analysis), damit Sie Schwachstellen-Warnungen in den Repositorys in anzeigen können GitHub Umgebung.

GitHub-Anwendungsschwachstellen-Integration

Die GitHub-Anwendungsschwachstellen-Integration Sammelt Scannerdaten und stellt diese Daten dem zur Verfügung ServiceNow AI Platform®. Es lässt sich problemlos in integrieren ServiceNow® Application Vulnerability Response Funktion von Vulnerability Response Um Schwachstellen von Drittparteien und zuzuordnen GitHub Warnungen in Ihrer Instanz.

Die GitHub Die Umgebung unterstützt mehrere Organisationen. Diese Organisationen, sowohl lokal als auch Enterprise, können verschiedene Abteilungen enthalten, z. B. Engineering, Qualität, Dokumentation usw. Jede Organisation kann wiederum mehrere Repositorys unterstützen. Nachdem Sie Ihre Anwendungsdaten mit importiert haben GitHub

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Repositorys-Integration können Sie Schwachstellen- und Warnungsdaten aus diesen Repositorys importieren. Importierte Daten werden wie eine Anwendung in verarbeitet Application Vulnerability Response Anwendung. Wenn Scanner Schwachstellen erkennen und Warnungen für die Repositorys generieren, werden in Schwachstellen erstellt Application Vulnerability Response.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
GitHub-Anwendungsschwachstellen-Integration v1.2, v1.1, 1,0	Application Vulnerability Response release notes Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

GitHub-Integrationen

Integration	Beschreibung
GitHub Repository-Integration	Importieren Sie ab v1.1 alle Anwendungsdaten für Ihren GitHub Lokale und Cloud-Accounts (Enterprise). Die Integration importiert Anwendungen aus den Repositorys, die Sie für eine Organisation (lokal) oder aus Ihrer Enterprise-Umgebung (Cloud) konfiguriert haben. Führen Sie diese Integration aus, bevor Sie die andere ausführen GitHub Integrationen, da sie von den aktuellen Anwendungsdaten abhängen, die aus der Repositorenintegration importiert wurden.
GitHub CodeScan-Integration	Ruft Schwachstellen-Warnungen für Code-Scans von ab GitHub Repositorys für Sicherheitsschwachstellen und Codierungsfehler. Importierte Daten werden SAST-Ergebnissen in Ihrer Instanz zugeordnet.
GitHub Dependabot-Integration	Ruft abhängige Warnungen für Abhängigkeiten mit bekannten Schwachstellen aus Repositorys ab. Importierte Daten werden SCA-Ergebnissen in Ihrer Instanz zugeordnet.
GitHub Geheimnisscans	Ruft Geheimnisse aus dem Code Ihrer Organisation zusammen mit den Ergebnissen der Anwendungssicherheitstests ab. Die Daten werden SCA-Ergebnissen in Ihrer Instanz zugeordnet.
GitHub Speicherort Des Geheimen Scans	Ruft die Standort- und Zeilennummern für die gescannten Geheimnisse im Code Ihrer Organisation ab, um Ihre Entwickler bei der Korrektur zu unterstützen.

Wird Hochgeladen SBOM Dateien in ServiceNow AI Platform® Von Ihrem GitHub Repositorys

Bestimmen Sie, ob SBOM Dateien, die in Ihren CI/CD-Pipelines (kontinuierliche Integration und kontinuierliche Bereitstellung/-Bereitstellung) generiert wurden, wurden erfolgreich in der Warteschlange in Ihrer eingefügt ServiceNow AI Platform® Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schützen Sie Ihre Umgebungen während der Softwareentwicklungszyklen mit vor potenziell schädlichen Komponenten GitHub Aktionen, die Sie über initiieren GitHub Umgebung.
- Holen Sie alle erforderlichen ab GitHub Aktionen für SBOM Laden Sie in den GitHub Marketplace hoch.

Die SBOM Anwendungen müssen hochgeladen werden SBOM Dateien. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Importierte Daten werden angezeigt

Anwendungsdaten aus importiert GitHub Die Repository-Integration wird in der Tabelle „erkannte Anwendungen“ [sn_vul_App_Release] angezeigt. Führen Sie diese Integration zuerst aus.

Die Repos-Integration importiert Tags und Themen, die Sie für ein Repository in konfiguriert haben GitHub Account aus dem Menü „Einstellungen“. Alle anwenderdefinierten Eigenschaften befinden sich im Menü unter Ihrem Repository. Werte, die Sie für die Eigenschaften festlegen, werden als Schlüssel-Wert-Paare importiert. Weitere Informationen dazu, wo Sie diese Informationen in Ihrer Instanz anzeigen können, finden Sie unter Zeigen Sie an GitHub-Anwendungsschwachstellen-Integration Importausführungsstatus und importierte Repository-Daten.

Daten (Ergebnisse) aus importiert GitHub Die Dependabot-Integration wird in den folgenden Tabellen angezeigt.

- Erkannte Anwendungen [sn_vul_App_Release].
- Zusammenfassungen des Anwendungsschwachstellen-Scans [sn_vul_App_vul_Scan_summary].
- Angreifbare Anwendungselemente [sn_vul_App_vulnerable_item].
- Pakete [sn_vul_App_Package].

Importierte Daten aus der GitHub CodeScan-Integration werden in den folgenden Tabellen angezeigt.

- Erkannte Anwendungen [sn_vul_App_Release].
- Zusammenfassungen des Anwendungsschwachstellen-Scans [sn_vul_App_vul_Scan_summary].
- Anwendungsschwachstelleneinträge [sn_vul_App_vul_entry].
- Angreifbare Anwendungselemente [sn_vul_App_vulnerable_item].

Vorbereitung für GitHub-Anwendungsschwachstellen-Integration

Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die GitHub-Anwendungsschwachstellen-Integration Davon ausgegangen, dass Sie mit dem GitHub-Produkt und der API vertraut sind.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Erforderliche Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- administrator zum Herunterladen, Installieren und Aktivieren von Anwendungen und zum Zuweisen von Rollen.
- GitHub-Administrator zum Abrufen von Anmeldeinformationen und Generieren von Token in der GitHub-Konsole.
- administrator zum Einrichten von Verbindungen und Alias-Datensätzen in Ihrer Instanz.

Setupaufgaben

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.
Überprüfen Sie, ob GitHub-Anwendungsschwachstellen-Integration Ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Installieren Sie ServiceNow GitHub-Anwendungsschwachstellen-Integration.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die App und weist Anwender der Anwendergruppe „App-Sec Manager“ zu. • Der App-SEC-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. • sn_vul_github_config_Integration wird von der Anwendergruppe „App-Sec Manager“ geerbt. Diese Rolle enthält die Rollen connection_admin und oauth_admin.
Rufen Sie Ihre GitHub-Anmeldeinformationen und -Accountinformationen ab.	Account-Informationen sind in Datensätzen erforderlich, die Sie zur Authentifizierung erstellen. Siehe OAuth 2,0-Anmeldeinformationen für werden erstellt GitHub Apps: JWT für GitHub-Anwendungsschwachstellen-Integration Weitere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben (Fortsetzung)

Setupaufgaben	Beschreibung
	Informationen zu Details zu Ihrem Bedarf und zum Einrichten der erforderlichen Datensätze für die OAuth-Authentifizierung.
Überprüfen Sie, ob Sie CWE-Daten (Common Weakness Enumeration) importieren.	Die CWE-Integration (Common Weakness Enumeration) wird auch von verwendet Application Vulnerability Response Und sollten vor der Installation und Konfiguration der GitHub Vulnerability Integration ausgeführt werden. Es wird mit installiert Vulnerability Response, Standardmäßig. **Hinweis:** NIST Vulnerability Database (NVD)-Daten sind für die Installation der GitHub Vulnerability Integration nicht erforderlich, bieten jedoch eine Ergänzung und wären nützlich. Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken.

OAuth 2,0-Anmeldeinformationen für werden erstellt GitHub Apps: JWT für GitHub-Anwendungsschwachstellen-Integration

Führen Sie die folgenden Schritte aus, um Ihren zu integrieren GitHub Apps, die das JWT-Bearer-Token für verwenden GitHub-Anwendungsschwachstellen-Integration.

Erforderliche Rollen:

- sn_vul.App_sec_Manager und admin für Datensätze in Ihrem ServiceNow AI Platform.
- Für Aufgaben in Ihrem ist keine Instanzrolle erforderlich GitHub Account.
- Weitere Informationen zum Kontext der Schritte für dieses Setup finden Sie unter OAuth 2,0-Protokoll .

Erstellen und konfigurieren Sie GitHub App für GitHub-Anwendungsschwachstellen-Integration

Erstellen Sie eine anwenderdefinierte GitHub App aus Ihrem GitHub Account zum Aktivieren der OAuth 2,0-Authentifizierung mit Ihrem GitHub-Anwendungsschwachstellen-Integration In Ihrer Instanz.

Vorbereitungen

Erforderliche Rolle: Keine Instanzrolle erforderlich

Warum und wann dieser Vorgang ausgeführt wird

Führen Sie diese Schritte aus Ihrem aus GitHub Account. Siehe Gebäude GitHub Apps Auf der GitHub Entwickler-Website für Anweisungen zum Erstellen und Konfigurieren anwenderdefinierter Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Von Ihrem GitHub Account erstellen Sie Ihren GitHub App, indem Sie zu navigieren **Entwicklereinstellungen** > **GitHub-Apps**an.
2. In **Homepage-URL** Feld eingeben `https://<instance-name>.service-now.com` .
3. In **Rückruf-URL der Anwenderautorisierung** Feld eingeben `https://<instance-name>.service-now.com/oauth_redirect.do` .
4. In **Identifizieren und Autorisieren von Anwendern** Deaktivieren Sie den Abschnitt **Anwenderautorisierungstoken ablaufen lassen** Feld.
5. In **Webhook** Wählen Sie den Abschnitt aus **Aktiv** Feld.
6. In **Webhook-URL** Feld eingeben `https://instance-name>.service-now.com/` .
7. Lassen Sie die verbleibenden Felder leer (Standard).
8. In **Repository-Berechtigungen** Konfigurieren Sie die folgenden Einstellungen.

Code-Scan	Schreibgeschützt
Inhalte	Schreibgeschützt
Anwenderdefinierte Eigenschaften	Schreibgeschützt
Abhängige Warnungen	Schreibgeschützt
Metadaten	Schreibgeschützt

Hinweis:
Wenn Sie bereits eine GitHub-App verwenden und eine der Berechtigungen aktualisieren, müssen Sie diese Berechtigungen für Ihre GitHub-App überprüfen und akzeptieren. Sie können zu Ihrer App navigieren und auswählen **Konfigurieren > Anforderung überprüfen > neue Berechtigungen akzeptieren** .

9. Belassen Sie die verbleibenden Berechtigungen als `Kein Zugriff` (Standard).
10. In **Abonnieren Sie Ereignisse** Wählen Sie den Abschnitt aus **Bereitstellungsschutzregel** Option.
11. Klicken Sie mit der rechten Maustaste in den Header, um die Änderungen zu speichern.
12. Installieren Sie neu erstellte GitHub App in den Accounts Ihrer Wahl.
    a. Wählen Sie auf der Seite „GitHub-Apps-Einstellungen“ Ihre App aus.
    b. Wählen Sie in der linken Sidebar aus **Installieren Sie Die App** .
    c. Wählen Sie Aus **Installieren** Neben der Organisation oder dem persönlichen Account, das das richtige Repository enthält.
    d. Installieren Sie die App auf allen Repositorys, oder wählen Sie Repositorys aus. Weitere Informationen finden Sie unter GitHub-Apps werden installiert .
13. Wählen Sie nach der Installation die Einstellungen (Zahnradsymbol) für Ihre App aus, und notieren Sie sich die folgenden Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Details sind erforderlich, wenn Sie die Anwendungsregistrierung in erstellen ServiceNow AI Platform Instanz.

- App-ID
- Client-ID
- Geheimer Clientschlüssel.
- Beachten Sie das Token in der URL. Dies ist die Token-ID, die Sie in der Token-URL in Ihrer Instanz eingeben.

14. Scrollen Sie auf der Seite nach unten, generieren Sie einen neuen privaten Schlüssel, und speichern Sie ihn auf Ihrem Computer.

Generieren Sie das JKS-Zertifikat für GitHub-Anwendungsschwachstellen-Integration

Generieren Sie ein JKS-Zertifikat für die JWT-Authentifizierung für GitHub-Anwendungsschwachstellen-Integration.

Vorbereitungen

Sie müssen das Passwort notieren, das Sie zum Generieren der JKS-Datei (Schlüsselspeicher-Passwort) verwenden.

Erforderliche Rolle: sn_vul.App_sec_Manager

Prozedur

1. Erstellen Sie ein VON CA signiertes Zertifikat mit GitHub Privater App-Schlüssel:

```
openssl req -new -x509 -key <file-name>.pem -out <certificate-name>.pem -days 1095
```

2. Geben Sie die erforderlichen Details ein.
3. Erstellen Sie die PKCS 12-Datei mit GitHub Privater App-Schlüssel und VON CA signiertes Zertifikat:

```
openssl pkcs12 -export -in <certificate-name>.pem -inkey <file-name>.pem -certfile
 <certificate-name>.pem -out <PKCS-12-file-name>.p12
```

4. Geben Sie das Exportpasswort an.
5. JKS-Datei erstellen:

```
keytool -importkeystore -srckeystore <PKCS-12-file-name>.p12 -srcstoretype pkcs12
 -destkeystore <JKS-certificate-filename>.jks -deststoretype JKS
```

6. Geben Sie die Passwörter des Ziel- und Quellschlüsselspeichers an.

Hängen Sie an GitHub Java Key Store-Zertifikat an Ihre Instanz für GitHub-Anwendungsschwachstellen-Integration

Aktivieren Sie die JWT-Bearer-Token-Authentifizierung, indem Sie Ihr gültiges GitHub Java Keystore (JKS)-Zertifikat an Ihre Instanz anhängen.

Vorbereitungen

Ein gültiges Java-Schlüsselspeicher-Zertifikat.

Erforderliche Rolle: sn_vul.App_sec_Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Zertifikate**an.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die Felder aus.

X.509-Zertifikatformularfelder

Feld	Beschreibung
Name	Name zur eindeutigen Identifizierung des Datensatzes. Beispiel: Mein GitHub-App-Zertifikat für AVR .
Benachrichtigung bei Ablauf	Option zum Festlegen der Anwender, die benachrichtigt werden sollen, wenn das Zertifikat abläuft.
Tage vor Ablauf benachrichtigen	Anzahl der Tage, die eine Benachrichtigung gesendet werden soll, bevor das Zertifikat abläuft.
Aktiv	Option zum Aktivieren des Zertifikats.
Typ	Option zum Auswählen des Zertifikattyps. Wählen Sie Aus **Java-Schlüsselspeicher** .
Läuft in Tagen ab	Anzahl der Tage, bis das Zertifikat abläuft.
Schlüsselspeicher-Passwort	Passwort, das dem Zertifikat zugeordnet ist (Hinweis: Das zuvor erstellte Zielschlüsselspeicher-Passwort).
Kurzbeschreibung	Zusammenfassung des Zertifikats.

4. Wählen Sie das Anhangssymbol aus, und hängen Sie ein JKS-Zertifikat an.
5. Wählen Sie Aus **Validiert Speicher/Zertifikate** .
   Für gültige Zertifikatdateien wird eine gültige Nachricht „key_Store“ angezeigt.

Erstellen Sie einen JWT-Signaturschlüssel für GitHub JKS-Zertifikat für GitHub-Anwendungsschwachstellen-Integration

Erstellen Sie einen JSON-Webtoken-Signaturschlüssel (JWT), der Ihrem zugewiesen werden soll GitHub Java-Schlüsselspeicher-Zertifikat.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- sn_vul.App_sec_Manager

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **JWT-Schlüssel**an.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JWT-Schlüssel-Formularfelder

Feld	Beschreibung
Name	Name zur eindeutigen Identifizierung des JWT-Signaturschlüssels. Beispiel: Mein GitHub-App-JWT-Schlüssel für AVR .
Signatur-Schlüsselspeicher	Wählen Sie das gültige JKS-Zertifikat aus, das Sie in der vorherigen Aufgabe angehängt haben.
Schlüssel-ID	Lassen Sie dieses Feld leer.
Signaturalgorithmus	Belassen Sie diesen Wert als RSA 256.
Signaturschlüssel-Passwort	Passwort, das dem Signaturschlüssel zugeordnet ist. Dies ist das Passwort, das Sie zum Generieren der JKS-Datei verwendet haben.
Aktiv	Option zum Aktivieren des Schlüssels.

4. Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle im grauen Header der Seite, und wählen Sie aus **Speichern** .

Erstellen Sie einen JWT-Provider für Ihren GitHub Signaturschlüssel für GitHub-Anwendungsschwachstellen-Integration

Fügen Sie Ihrem einen JSON-Webtoken-Anbieter (JWT) hinzu ServiceNow Instanz für GitHub.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- sn_vul.App_sec_Manager

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **JWT-Anbieter**an.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formularfelder des JWT-Anbieters

Feld	Beschreibung
Name	Name zur eindeutigen Identifizierung des JWT-Providers. Beispiel: Mein GitHub-App-JWT-Anbieter für AVR .
Ablaufintervall (Sek.)	Anzahl in Sekunden zum Festlegen der Lebensdauer von JWT-Provider-Token. Sie können diese Einstellung als Standard belassen.
Signierkonfiguration	Wählen Sie den JWT-Schlüssel aus, den Sie in den vorherigen Schritten erstellt haben.

4. Klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie aus **Speichern** .
5. Geben Sie ein GitHub App **App-ID** Für den Wert von **iss** Anspruch in der zugehörigen Liste Standardansprüche.
   Dies ist die App-ID aus dem GitHub App in Ihrem GitHub Konsole, die Sie in den vorherigen Schritten erstellt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Verlassen **aud** Und **Untergeordnet** Werte leer (Standard).
7. Klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie aus **Speichern** .

Registrieren GitHub Als OAuth-Provider (JWT) für GitHub-Anwendungsschwachstellen-Integration

Verwenden Sie die während generierten Informationen GitHub Zu registrierende App-Account-Konfiguration GitHub Als OAuth-Provider und zulassen, dass die Instanz OAuth 2,0-Token anfordert.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- sn_vul.App_sec_Manager

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**an.
2. Wählen Sie **Neu**.
   Die **Welche Art von OAuth-Anwendung?** Nachricht wird angezeigt.
3. Wählen Sie **Verbindung zu einem fremden OAuth-Provider herstellen** aus.
4. Füllen Sie im Formular die Felder aus.

Formularfelder „Anwendungsregistrierung“

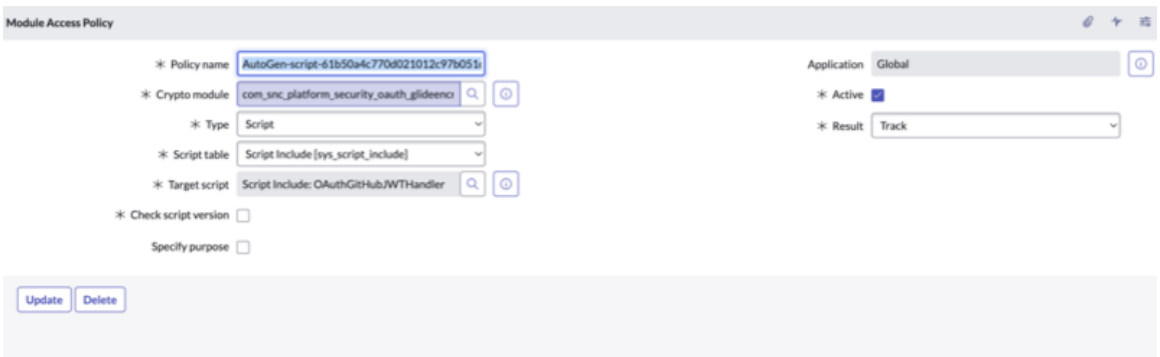
Feld	Beschreibung
Name	Name zur eindeutigen Identifizierung des Datensatzes. Geben Sie beispielsweise ein `Mein GitHub-App-Anbieter für AVR` .
Client-ID	Client-ID von GitHub App. Die Client-ID stammt aus dem GitHub Anwendung in Ihrem GitHub Konsole, die Sie in den vorherigen Schritten erstellt haben. Diese ID ist in verfügbar **Über** Abschnitt von GitHub App-Konfiguration in GitHub.
Zugänglich	Belassen Sie diese Einstellung im aktuellen Wert.
Geheimer Clientschlüssel	Geheimer Client-Schlüssel von GitHub App. Das geheime Clientgeheimnis stammt aus dem GitHub Anwendung in Ihrem GitHub Konsole, die Sie in den vorherigen Schritten erstellt haben. Diese ID ist in verfügbar **Über** Abschnitt von GitHub App-Konfiguration in GitHub.
Aktiv	Option zum Aktivieren des Schlüssels. Lassen Sie dies ausgewählt.
Autorisierungs-URL	Diese URL wird automatisch generiert.
Token-URL	Die Position des Tokenendpunkts, den die Instanz zum Abrufen und Aktualisieren von Token verwendet. Geben Sie das Token aus der URL in ein GitHub App. Dies ist das Token, das in der URL angezeigt wird, nachdem Ihre App in installiert wurde GitHub. Im Abschnitt App installieren in Ihrer GitHub-App-Konfiguration in GitHub, Wählen Sie das Zahnrad aus. Das Token wird in der Webseiten-URL angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

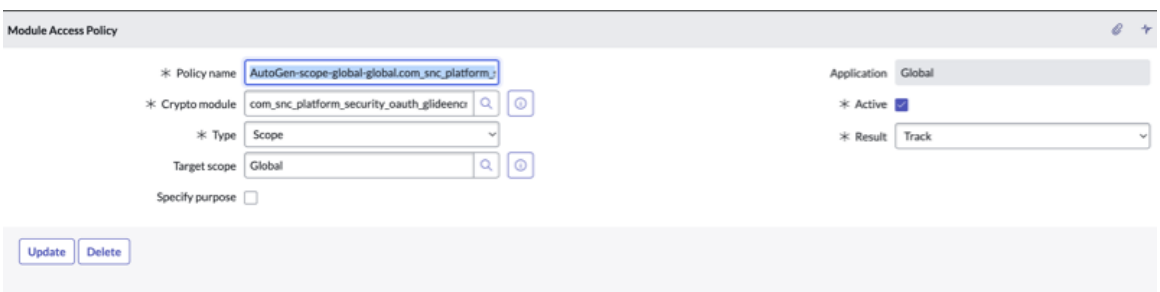
Feld	Beschreibung
	○ Für Cloud: https://api.github.com/app/installations/49374672/access_tokens . Installations-ID: 9374672. ○ Für lokal: https://github-372.secops-eng.com/api/v3/app/installations/7/access_tokens/api/v3 .
OAuth-API-Skript	Option, mit der Sie auf eine geänderte OAuthUtil-Skripteinbindung verweisen können. Wählen Sie Aus **OAuthGitHubJWTHandler** .
Standardgewährungstyp	Typ der Gewährung, die der Anwendungsregistrierung zugeordnet ist. Wählen Sie Aus **JWT-Bearer** .

5. Belassen Sie die restlichen Formularfelder als Standard.
6. Klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie aus **Speichern** .
7. Scrollen Sie zu **OAuth-Entitätsprofile** Zugehörige Liste, wählen Sie sie aus, und öffnen Sie das Standardprofil, das in der Liste erstellt wurde.
8. Füllen Sie aus **JWT-Anbieter** Feld mit dem zuvor erstellten JWT-Provider, und speichern Sie das Formular.
9. Kehren Sie zur Anwendungsregistrierungsdatei zurück, und speichern Sie sie.
10. Navigieren zu **Schlüsselverwaltung** > **Modulzugriffsrichtlinien** > **Alle**an.
11. Wählen Sie die Richtlinie so aus Com_snc_Platform_Security_oauth_Glideencrypter Wird als angezeigt **Krypto-Modul** Feldwert, und OAuthGitHubJWTHandler Ist die Skripteinbindung in **Zielskript** Feld.

    In der folgenden Abbildung Com_snc_Platform_Security_oauth_Glideencrypter Ist als Wert für ausgewählt **Krypto-Modul** Feld. Die **Skripttabelle** Feld wird angezeigt Die Skripteinbindung [sys_script_include] Tabelle, und **Zielskript** Feldwert ist OAuthGitHubJWTHandler .



12. Wählen Sie **Aktualisieren**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wie im vorherigen Bild gezeigt, der Wert in **Richtlinienname** Feldänderungen und **Skripttabelle** Und **Zielskript** Felder werden nicht mehr angezeigt.

13. Verifizieren Sie **Ergebnis** Feld ist auf festgelegt Nachverfolgen Und speichern Sie Ihre Änderungen.

Erstellen Sie Anmeldeinformationen und Verbindungen für GitHub-Anwendungsschwachstellen-Integration

Erstellen Sie einen Anmeldeinformationsdatensatz für GitHub App-Anbieter, der zuvor zum Autorisieren von Aktionen erstellt wurde.

Vorbereitungen

Erforderliche Rollen:

- Administrator
- sn_vul.App_sec_Manager

Prozedur

1. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Anmeldeinformationen**an.
2. Wählen Sie **Neu**.
3. Wählen Sie **OAuth 2.0-Anmeldeinformationen** aus.
4. Wählen Sie Aus **Neu** Und füllen Sie die Felder aus.
5. Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle im Header der Seite, und wählen Sie aus **Speichern** .
   Die Liste Anmeldeinformationen wird angezeigt.
6. Öffnen Sie den soeben erstellten Datensatz, und wählen Sie aus **OAuth-Token abrufen** Zugehöriger Link.
   Es wird eine Meldung angezeigt, dass das OAuth-Token erfolgreich importiert wurde.
7. Navigieren zu **Anmeldeinformationen und Verbindungen** > **Verbindungen**an.
8. Wählen Sie **Neu**.
9. Wählen Sie Aus **HTTP(s)-Verbindung** .
10. Wählen Sie Aus **Neu** Und füllen Sie die Felder aus.
11. Wählen Sie **Absenden**.
    Die Liste Aliasse für Verbindungen und Anmeldeinformationen wird angezeigt.
12. Öffnen Sie Ihren Datensatz, und wählen Sie auf der Registerkarte zugehörige Liste Verbindungen die Option aus **Neu** Und füllen Sie die Felder im HTTP-Verbindungsdatensatz aus.
13. Wählen Sie **Absenden**.
    Die Liste Aliasse für Verbindungen und Anmeldeinformationen wird angezeigt. Sie sind jetzt bereit, die Schritte bis abzuschließen Konfigurieren Sie die Eigenschaften GitHub-Anwendungsschwachstellen-Integration. Geben Sie im Feld Verbindung die Anmeldeinformationen ein, die Sie in den vorherigen Schritten erstellt haben.

Installieren Sie ServiceNow® GitHub-Anwendungsschwachstellen-Integration

Bevor Sie die Integration auf Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit die ausgeführt werden kann GitHub-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsschwachstellen-Integration Ist ordnungsgemäß in integriert Application Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei der Instanz an, die Sie installieren möchten GitHub-Anwendungsschwachstellen-Integration Ein.
2. Navigieren Sie zum ServiceNow Store.
3. In ServiceNow Store, Suchen nach GitHub-Anwendungsschwachstellen-Integration Anwendung.
4. Wählen Sie die Anwendungskachel aus.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Erwägen Sie, das zu lesen **Andere Anforderungen** Und **Abhängigkeiten** Abschnitte, falls zutreffend.

5. Wählen Sie Aus **App Anfordern** Und geben Sie ein Now Support Anmeldeinformationen.
6. Wählen Sie Aus **Abrufen** .
7. Geben Sie ein **Instanzname** Und **Grund für die Instanz** , Und wählen Sie aus **Validieren Sie Die Instanz** .
8. Wählen Sie Aus **Anforderung** .
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**an.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen Sie aus **Installieren** .
    Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Konfigurieren Sie die Eigenschaften GitHub-Anwendungsschwachstellen-Integration

Bevor Sie die Integration auf Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit das GitHub-Produkt ordnungsgemäß in integriert wird Application Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Erforderliche Rollen:

- App-SEC-Manager-Anwendergruppe
- sn_vul.App_sec_Manager für OAuth-Setup erforderlich

Prozedur

1. Navigieren zu **Alle** > **GitHub-Schwachstellenintegration** > **Konfiguration**an.
2. Wählen Sie Aus **Standardauthentifizierung** Oder **OAuth** Für Authentifizierungstyp.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Standardauthentifizierung erfordert einen MID-Server für lokale Instanzen. Generieren Sie das für die Standardauthentifizierung erforderliche API-Token von Ihrem GitHub Account.
- OAuth erfordert die OAuth-App, die Anmeldeinformationen und das Verbindungs-Setup, die in beschrieben werden OAuth 2,0-Anmeldeinformationen für werden erstellt GitHub Apps: JWT für GitHub-Anwendungsschwachstellen-Integration.

3. Füllen Sie die Felder basierend auf dem von Ihnen ausgewählten Typ aus.
Basic Authentication

Feld	Beschreibung
API-URL	Das entsprechende GitHub API-URL für Enterprise oder lokal. Die Standard-URL ist https://api.github.com . Lokal ist Ihr GitHub Endpunkt-URL.
API-Token	Token, das Sie aus generiert haben GitHub Konsole.
API-Typ	Wählen Sie eines aus: **Organisation** Wählen Sie diese Option aus, wenn Sie Daten für eine bestimmte Organisation nach Namen importieren möchten. Die GitHub Die Umgebung unterstützt mehrere Organisationen. Jede Organisation kann mehrere Repositorys unterstützen. Wenn Sie eine Organisation eingeben, werden nur Daten aus dieser Organisation importiert. **Enterprise** Die Enterprise-Umgebung unterstützt mehrere Organisationen. Wählen Sie diese Option aus, wenn Sie Schwachstellendaten aus allen Organisationen in Ihrer Enterprise-Umgebung (Cloud) importieren möchten.
Organisationsname	Name von GitHub Repository. Nur Daten aus der von Ihnen eingegebenen Organisation werden importiert.
MID-Server	Für lokale Instanzen für die Standardauthentifizierung ist ein MID-Server erforderlich.
Wählen Sie Optionen aus, um das Ausnahmemanagement und falsch positive Ergebnisse zu verwalten.	Wählen Sie Optionen aus, um das Ausnahmemanagement und das falsch positive für angreifbare Anwendungselemente (Avis) mit zu verwalten ServiceNow Workflows automatisch beim Import.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Verwalten Sie Ausnahmen in ServiceNow Lassen Sie diese Option aktiviert, wenn Sie importierte Avis selektieren möchten, die für markiert sind **Zurückgestellt** status. Avis mit **Quelle** status, die normalerweise einem zugeordnet sind **Zurückgestellt** status in Ihrer Instanz werden stattdessen zugeordnet **Öffnen** . Sie **Fordern Sie eine Ausnahme an** Aus dem AVI-Datensatz. **Verwalten Sie falsch positive Ergebnisse in ServiceNow** Lassen Sie diese Option aktiviert, wenn Sie importierte Avis mit selektieren möchten **Quelle** status markiert als **Falsch Positiv** Oder **Potenziell Falsch Positiv** . Avis mit diesen **Quelle** status, die normalerweise einem zugeordnet sind **Geschlossen** status in Ihrer Instanz sind zugeordnet **Öffnen** . Sie fordern an **Falsch positiv** Aus dem AVI-Datensatz. ○ Deaktivieren Sie ein oder beide Kontrollkästchen, wenn Sie beibehalten möchten **Quelle** status, die von Ihrem Scanner importiert wurden. ○ Wenn deaktiviert, wird **Ausnahme anfordern** Und **Falsch Positiv** Aktionen sind in Avis nicht sichtbar.
Integrationsinstanz	Instanz, in die Sie Daten importieren.

OAuth

Feld	Beschreibung
API-URL	Das entsprechende GitHub API-URL für Enterprise oder lokal. Die Standard-URL ist https://api.github.com . Lokal ist Ihr GitHub Endpunkt-URL.
Verbindung	Die von Ihnen erstellte Verbindung wurde in beschrieben OAuth 2,0-Anmeldeinformationen für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	werden erstellt GitHub Apps: JWT für GitHub-Anwendungsschwachstellen-Integration.
API-Typ	Wählen Sie eines aus: **Organisation** Wählen Sie diese Option aus, wenn Sie Daten für eine bestimmte Organisation nach Namen importieren möchten. Die GitHub Die Umgebung unterstützt mehrere Organisationen. Jede Organisation kann mehrere Repositorys unterstützen. Wenn Sie eine Organisation eingeben, werden nur Daten aus dieser Organisation importiert. **Enterprise** Die Enterprise-Umgebung unterstützt mehrere Organisationen. Wählen Sie diese Option aus, wenn Sie Schwachstellendaten aus allen Organisationen in Ihrer Enterprise-Umgebung (Cloud) importieren möchten. **Hinweis:** GitHub Apps unterstützen keine APIs auf Enterprise-Ebene.
Organisationsname	Organisationsname für Ihren GitHub Repositorys. Nur Daten aus den Repositorys in der von Ihnen eingegebenen Organisation werden importiert.
Wählen Sie Optionen aus, um das Ausnahmemanagement und falsch positive Ergebnisse zu verwalten.	Wählen Sie Optionen aus, um das Ausnahmemanagement und das falsch positive für angreifbare Anwendungselemente (Avis) mit zu verwalten ServiceNow Workflows automatisch beim Import. **Verwalten Sie Ausnahmen in ServiceNow** Lassen Sie diese Option aktiviert, wenn Sie importierte Avis selektieren möchten, die für markiert sind **Zurückgestellt** status. Avis mit **Quelle** status, die normalerweise einem zugeordnet sind **Zurückgestellt** status in Ihrer Instanz werden stattdessen zugeordnet **Öffnen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie **Fordern Sie eine Ausnahme an** Aus dem AVI-Datensatz. **Verwalten Sie falsch positive Ergebnisse in ServiceNow** Lassen Sie diese Option aktiviert, wenn Sie importierte Avis mit selektieren möchten **Quelle** status markiert als **Falsch Positiv** Oder **Potenziell Falsch Positiv** . Avis mit diesen **Quelle** status, die normalerweise einem zugeordnet sind **Geschlossen** status in Ihrer Instanz sind zugeordnet **Öffnen** . Sie fordern an **Falsch positiv** Aus dem AVI-Datensatz. ○ Deaktivieren Sie ein oder beide Kontrollkästchen, wenn Sie beibehalten möchten **Quelle** status, die von Ihrem Scanner importiert wurden. ○ Wenn deaktiviert, wird **Ausnahme anfordern** Und **Falsch Positiv** Aktionen sind in Avis nicht sichtbar.

4. Wählen Sie Aus **Anmeldeinformationen speichern und testen** .
5. Führen Sie aus GitHub Repository-Integration, bevor die anderen Integrationen ausgeführt werden. Der andere GitHub Integrationen hängen von aktuellen Anwendungsdaten ab, die aus der Repositorenintegration importiert wurden. Daten aus der Repositorintegration werden in der Tabelle „erkannte Anwendungen“ [sn_vul_App_Release] gespeichert. Weitere Informationen finden Sie unter Zeigen Sie an GitHub-Anwendungsschwachstellen-Integration Importausführungsstatus und importierte Repository-Daten.

Zeigen Sie an GitHub-Anwendungsschwachstellen-Integration Importausführungsstatus und importierte Repository-Daten

Verwenden Sie **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Korrekturentscheidungen zu unterstützen.

Vorbereitungen
Erforderliche Rolle: sn_vul.App_sec_Manager

Prozedur

1. Navigieren zu **Alle** > **GitHub-Schwachstellenintegration** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
3. Wählen Sie aus **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste.
4. Überprüfen Sie, ob alle Importe erfolgreich waren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trouble?

Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:

- Netzwerkunterbrechung.
- Ein Problem bei der Datenübertragung, das zu beschädigten Daten während der Transformation führt.

Wenn eine dieser Bedingungen auftritt, wählen Sie aus **Jetzt Ausführen** , Und führen Sie die Integration erneut aus.

5. Um importierte Repositorys anzuzeigen, navigieren Sie zurück zur Integrationsliste, und wählen Sie aus GitHub Datensatz der Repository-Integration.
6. Wählen Sie aus **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste und öffnen Sie einen Datensatz.
   Die Anzahl der Repositorys, die Sie mit einer Integrationsausführung importiert haben, wird in der Spalte importierte Elemente angezeigt.

   Alle Tags und Themen, die Sie für ein Repository in konfiguriert haben GitHub Accounts aus dem Menü „Einstellungen“ werden importiert. Alle importierten anwenderdefinierten Eigenschaften befinden sich im Menü unter Ihrem Repository.

   Tags, Themen und anwenderdefinierte Eigenschaften werden nur in Ihre Instanz importiert, wenn sie in konfiguriert sind GitHub Account.

   Wenn importiert, dies GitHub Informationen werden in Ihrer Instanz in der Spalte „zusätzliche Quellinformationen“ in der Tabelle „erkannte Anwendungen“ [sn_vul_App_Release] und in den zusätzlichen Quellinformationen angezeigt. Abschnitt in einem erkannten Anwendungsdatensatz. Anwenderdefinierte Eigenschaften werden als Schlüssel-Wert-Paare angezeigt, und Tags und Themen werden in Arrays angezeigt.

Anzeigen GitHub-Anwendungsschwachstellen-Integration Importsätze

Zeigen Sie Details für Importinformationen für an GitHub-Anwendungsschwachstellen-Integration.

Vorbereitungen

Erforderliche Rolle: sn_vul.App_sec_Manager

Prozedur

1. Navigieren Sie zu **GitHub-Schwachstellenintegration** > **Importsatztabellen**an.
2. Wählen Sie einen Datensatz für eine Integration aus.
3. Wählen Sie einen zugehörigen Link aus, um die folgenden Informationen anzuzeigen:
   - Importsätze
   - Transformationszuordnungen
   - Verlauf umwandeln

Invicti-Schwachstellen-Integration

Die Invicti-Schwachstellen-Integration Verwendet aus dem Invicti-Produkt importierte Anwendungsdaten, um die Auswirkung und Priorität von Fehlern in Ihrem Code zu bestimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Invicti-Schwachstellen-Integration

Die Invicti-Schwachstellen-Integration Sammelt Scannerdaten und stellt diese Daten dem zur Verfügung ServiceNow AI Platform®. Es lässt sich problemlos in integrieren ServiceNow® Application Vulnerability Response Funktion von Vulnerability Response Dient zum Zuordnen importierter Informationen zu Schwachstellen von Drittanbieteranwendungen in Ihre Instanz.

Die Integration importiert die folgenden Typen gescannter Daten.

- Dynamische Anwendungssicherheitstests (DAST)
- Interaktive Anwendungssicherheitstests (IAST)

Weitere Informationen zu DAST und IAST finden Sie unter Application Vulnerability Response erkunden.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Invicti-Schwachstellen-Integration v1.1 Invicti-Schwachstellen-Integration 1.0	Application Vulnerability Response release notes Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Integrationen

Die folgenden Integrationen sind im Basissystem enthalten. Die Integrationen sind verkettet, sodass nach erfolgreichem Abschluss einer Integration die nächste Integration initiiert wird. Die Integrationen werden in der in der folgenden Tabelle aufgeführten Reihenfolge ausgeführt.

Nach der ersten Ausführung werden täglich geplante Aufgaben verkettet, um diese Integrationen automatisch in der Reihenfolge auszuführen. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Integrationen von Invicti-Anwendungsschwachstellen

Integration	Beschreibung
Invicti-Anwendungslistenanwendung	Importiert von Invicti gescannte Anwendungen basierend auf der Tabelle „erkannte Anwendungen“ [sn_vul_App_Release] oder „gescannte Anwendung“ [sn_vul_App_scanned_Application] `sn_vul.use_product_model`Die Systemeigenschaft ist für die CI-Suchregeldatensätze festgelegt. • Wenn die Produktmodelleigenschaft auf „wahr“ festgelegt ist, wird eine Anwendung in die Tabelle „erkannte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen von Invicti-Anwendungsschwachstellen (Fortsetzung)

Integration	Beschreibung
	Anwendungsveröffentlichungen“ eingefügt. • Wenn die Produktmodelleigenschaft auf „falsch“ festgelegt ist, wird eine Anwendung in die Tabelle „gescannte Anwendung“ eingefügt. Sie können Suchregeln mit Konfigurationselementen (Configuration Items, CIs) als Suchziele aktivieren, indem Sie die Systemeigenschaft ändern. Wenn Sie sie ändern, sollten Sie auch CI-Suchregeln aktivieren, um dem Suchziel zu entsprechen. Weitere Informationen finden Sie unter: • Konfigurieren Sie die Eigenschaften Invicti-Schwachstellen-Integration • Erstellen Sie eine CI-Suchregel • CI-Suchregeln in werden erneut angewendet Application Vulnerability Response
Integration Der Invicti-Scan-Liste	Diese Integration wird initiiert, nachdem die Integration der Anwendungsliste erfolgreich abgeschlossen wurde. Diese Integration importiert Daten über das Datum und die Uhrzeit der Ausführung eines Scans.
Integration Von Angreifbaren Invicti-Anwendungselementen	Diese Integration wird initiiert, nachdem die Integration der Scan-Liste erfolgreich abgeschlossen wurde. Zeigen Sie ab v1.1 Details an, z. B. Gesamtverarbeitungszeiten, durchschnittliche Zeiten für Prozesse vor und nach der Integrationsausführung und Berichte zu den Datensätzen der Integrationsausführung für die Integration angreifbarer Anwendungselemente. Jede Schwachstelle in Invicti hat einen Typ, z. B. **DirectoryListing** . Dieser Typ wird in Ihrer Instanz als eindeutige ID zugeordnet und als Teil des Werts im Feld Schwachstelle im Datensatz des angreifbaren Anwendungselements (AVI) angezeigt: **Invicti-DirectoryListing** . Weitere Informationen zur Zuordnung finden Sie unter Invicti-Schwachstellen-Integration statuszuordnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Obergrenze für Elemente pro Seite für alle drei Integrationen beträgt 200.

Bereiten Sie sich auf den vor Invicti-Schwachstellen-Integration

Eine erfolgreiche Integration erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die Invicti-Schwachstellen-Integration Davon ausgegangen, dass Sie mit dem Invicti-Produkt und der API vertraut sind.

Die CWE-Integration (Common Weakness Enumeration) wird auch von verwendet Application Vulnerability Response Und sollten vor der Installation und Konfiguration der Invicti Vulnerability Integration ausgeführt werden.

Hinweis:
NIST Vulnerability Database (NVD)-Daten sind für die Installation der Integration nicht erforderlich, bieten jedoch eine Anreicherung der Schwachstellen und sind nützlich.

Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Hinweis:
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Validieren Sie die Größenanpassung Ihrer Instanz basierend auf der Anzahl der angreifbaren Anwendungselemente, die Sie importieren möchten. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support. Die Administratorrolle ist erforderlich, um Anwendungen auf Ihrem zu installieren und zu konfigurieren ServiceNow AI Platform Instanz.

Rufen Sie Ihre API-Anmeldeinformationen und das API-Token auf Ihrer Invicti-Konsole ab. Überprüfen Sie die Informationen, die auf der Invicti-Produkt-Website unter verfügbar sind API-Übersicht .

Installieren Sie ServiceNow® Vulnerability Response-Integration mit Invicti

Bevor Sie die Integration auf Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit die ausgeführt werden kann Invicti-Schwachstellen-Integration Die Anwendung ist ordnungsgemäß in integriert Application Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei der Instanz an, die Sie installieren möchten Invicti-Schwachstellen-Integration Ein.
2. Navigieren Sie zum ServiceNow Store.
3. In ServiceNow Store, Suchen Sie nach Invicti-Schwachstellen-Integration Anwendung.
4. Wählen Sie die Anwendungskachel aus.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Erwägen Sie, das zu lesen **Andere Anforderungen** Und **Abhängigkeiten** Abschnitte, falls zutreffend.

5. Wählen Sie Aus **App Anfordern** Und geben Sie ein Now Support Anmeldeinformationen.
6. Wählen Sie Aus **Abrufen** .
7. Geben Sie ein **Instanzname** Und **Grund für die Instanz** , Und wählen Sie aus **Validieren Sie Die Instanz** .
8. Wählen Sie Aus **Anforderung** .
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
10. Suchen Sie die Anwendung, wählen Sie sie aus, und wählen Sie aus **Installieren** Um es zu aktivieren.
    Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Konfigurieren Sie die Eigenschaften Invicti-Schwachstellen-Integration

Bevor Sie die Integration auf Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit die ausgeführt werden kann Invicti-Schwachstellen-Integration Funktioniert ordnungsgemäß mit Application Vulnerability Response Funktion von Vulnerability Response.

Vorbereitungen

Erforderliche Rollen:

- administrator zum Installieren und Aktivieren von Anwendungen
- App-SEC Manager-Anwendergruppe zum Konfigurieren der Integration

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.
Überprüfen Sie, ob Invicti-Schwachstellen-Integration Ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Installieren Sie ServiceNow Vulnerability Response-Integration mit Invicti.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die App und weist Anwender der App-Sec-Manager-Gruppe zu. • Der App-SEC-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.
Für die Inviciti Vulnerability Integration haben Sie Ihren **Anwender-ID** Und **API-Token** Bereit.	Wenden Sie sich an Ihren Invicti-Administrator, um die zu erhalten **Anwender-ID** Und **API-Token** Wenn Sie sie nicht kennen. Weitere Informationen finden Sie auf der Invicti-Produkt-Website unter API-Übersicht .

Prozedur

1. Navigieren zu **Alle** > **Invicti** > **Invicti-Konfiguration**an.
2. Füllen Sie die Felder aus.

Feld	Beschreibung
API-URL	Invicti-Instanz-URL des Anwenders. Dies sind die Informationen, die Sie von erhalten haben Bereiten Sie sich auf den vor Invicti-Schwachstellen-Integration.
Anwender-ID	Eindeutige Anwender-ID.
API-Token	API-Token, das Sie über Ihre Invicti-Konsole generiert haben. Dies sind die Informationen, die Sie von erhalten haben Bereiten Sie sich auf den vor Invicti-Schwachstellen-Integration.
Wählen Sie den Scan-Typ aus. Sie müssen mindestens einen auswählen.	
Importieren Sie DAST	Option zum Einbeziehen von Schwachstellen aus DAST-Scans. DAST-Scans suchen dynamisch Schwachstellen für eine Anwendung, während sie ausgeführt wird. Dieser Ansatz könnte einen externen Angriff imitieren.
Import IAST	Option zum Einbeziehen von Schwachstellen aus IAST-Scans. IAST-Scans erkennen Softwareschwachstellen, indem sie während der Ausführung mit dem Programm interagieren. Menschliche Beobachtung, automatisierte Tests und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sensoren werden in Kombination verwendet, um mit der Anwendung zu interagieren, um Schwachstellen zu lokalisieren.
Datumsformat	Parameter, der die Startzeit in das Format konvertiert, das von der Invicti-API unterstützt wird, die von der Invicti-Anwendungsintegration für angreifbare Elemente verwendet wird. Dieser Parameter muss dem Format entsprechen, das Sie in Ihrem Invicti-Account definiert oder ausgewählt haben, z. B. **tt/MM/JJJJ** . Überprüfen Sie, ob die Datums- und Uhrzeitformate in Ihrer Invicti-Konsole mit denen übereinstimmen, die Sie für das Datumsformat in eingeben ServiceNow AI Platform Instanz. So ändern Sie dieses Format in Ihrer Invicti-Konsole: **a.** Melden Sie sich unter an Invicti-Anmeldung . **b.** Wählen Sie Aus **Anwendername** Oben rechts. **c.** Navigieren zu **Anwendereinstellungen** > **Datums-/Uhrzeitformat**an. **Hinweis:** Fehlgeschlagene Importe können auftreten, wenn Sie ein ungültiges Datumsformat in eingeben ServiceNow AI Platform Instanz. Wenn Sie in Ihrer Instanz ein gültiges Format eingeben, das sich vom Datumsformat in Ihrer Invicti-Konsole unterscheidet, gibt Invicti eine leere Nutzlast zurück.
Ausnahmen in ServiceNow verwalten	Wählen Sie eines aus: **Aktiviert (ausgewählt)** Angreifbare Anwendungselemente (AVIT) aus Invicti mit status wie **Anwesend** Und **AcceptedRisk** Die in Ihrer Instanz möglicherweise zurückgestellt werden, werden stattdessen zugeordnet **Öffnen** Automatisch. **Deaktiviert (nicht ausgewählt)** quellstatus für aus Invicti importierte angreifbare Anwendungselemente (AVITs) werden beibehalten. Sie müssen Ausnahmen für diese AVITs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	aus AVIT-Datensätzen verwalten (zurückstellen). Weitere Informationen zu Invicti-quellstatus und -Zielfeldern finden Sie unter Invicti-Schwachstellen-Integration statuszuordnung.
Falsch positive Ergebnisse in ServiceNow verwalten	Wählen Sie eines aus: **Aktiviert (ausgewählt)** AVITs mit status von Invicti wie **Anwesend** Und **Falsch Positiv** Das könnte zu übergehen **Geschlossen** In Ihrer Instanz werden stattdessen zugeordnet **Öffnen** Automatisch. **Deaktiviert (nicht ausgewählt)** Aus Invicti importierte AVIT-status werden beibehalten. Sie müssen falsch positive oder potenzielle falsch positive Ergebnisse für diese AVITs aus AVIT-Datensätzen verwalten.

3. Wählen Sie Aus **Anmeldeinformationen speichern und testen** .
4. **Wahlweise:** Ändern Sie Ihre Suchregeln so, dass sie auf Konfigurationselementen basieren.

   (Optional) Standardmäßig ist **sn_vul.use_product_model** Systemeigenschaft ist aktiviert (auf festgelegt Wahr) Für Ihre Suchregeln, die basierend auf dem Produktmodell in der Tabelle [sn_sec_cmn_ci_Lookup_rule] aufgeführt sind. Wenn diese Regel aktiviert ist:

   - Diese Regel identifiziert Übereinstimmungen zwischen importierten Daten und den Daten in Configuration Management Database (CMDB) Basierend auf dem Produktmodell.
   - Datensätze werden in der Tabelle „erkannte Anwendungen“ [sn_vul_App_Release] erstellt oder aktualisiert.
   - Wenn Sie Ihre Suchregeln für Invicti erstellen oder bearbeiten, **Produktmodell** Wird in angezeigt **Suchziel** Feld im Regelformular.

   Um Ihre Regeln so zu ändern, dass sie auf Konfigurationselementen basieren, müssen Sie manuell deaktivieren (auf festlegen) Falsch) Der **sn_vul.use_product_model** Systemeigenschaft.

   a. Navigieren zu **Alle** > **Systemeigenschaften** Und suchen Sie **sn_vul.use_product_model** Zeichnen Sie auf, und legen Sie den Wert auf fest Falsch .

   b. Wählen Sie **Aktualisieren**.

   c. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **Suchregeln**an.

   d. Suchen Sie die Regeln für Anwendungsname und Quellanwendung-ID, die das Suchziel als haben **Konfigurationselement** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Aktivieren Sie das Kontrollkästchen aktiv für diese Regeln.

f. Wählen Sie **Aktualisieren**.
Wenn Sie Ihre Suchregeln für Invicti erstellen oder bearbeiten, beachten Sie dies **Konfigurationselement** Wird in angezeigt **Suchziel** Feld im Regelformular. Datensätze werden in der Tabelle „gescannte Anwendungen“ [sn_vul_App_Scanned_Application] erstellt oder aktualisiert.

Anzeigen von Invicti-Schwachstellen-Integration Importausführungsstatus und Datensätze

Verwenden Sie **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Korrekturentscheidungen zu unterstützen.

Importstatus, Importsätze und Datensätze werden angezeigt

Um den Status Ihrer Importe anzuzeigen, navigieren Sie als Anwender in der Anwendergruppe „App-Sec Manager“ zu **Alle** > **Invicti-Schwachstellenintegration** > **Integrationen** Und wählen Sie einen Integrationsdatensatz aus. Wählen Sie aus **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste.

Zeigen Sie ab v1.1 Details an, z. B. Gesamtverarbeitungszeiten, durchschnittliche Zeiten für Prozesse vor und nach der Integrationsausführung und Berichte zu den Datensätzen der Integrationsausführung für die Integration angreifbarer Anwendungselemente.

Um die Importsätze anzuzeigen, navigieren Sie zu **Alle** > **Invicti-Schwachstellenintegration** > **Integrationen** > **Importsatztabellen** Und wählen Sie eine Integration aus.

Die Anwendungslistenintegration erstellt oder aktualisiert Datensätze basierend auf dem Suchziel:

- Produktmodell: Tabelle „erkannte Anwendungen“ [sn_vul_App_Release]
- Konfigurationselement: Tabelle „gescannte Anwendungen“ [sn_vul_App_scanned_Application]

Die Integration der Scan-Liste erstellt oder aktualisiert Datensätze in der Tabelle „gescannte Anwendungen“ [sn_vul_App_Scan_summary].

Die Integration angreifbarer Anwendungselemente erstellt oder aktualisiert Datensätze in der Tabelle „angreifbare Anwendungselemente“ [sn_vul_App_vulnerable_item] und „CWEs“ [sn_vul_cwe].

Hinweis:
Jede Schwachstelle in Invicti hat einen „type“, z. B. „ProductDirectoryListing“. Dieser Typ wird als eindeutige ID in Ihre Instanz importiert und als Teil des Werts im Feld Schwachstelle im AVIT-Datensatz (Application Angreifbare Elemente) angezeigt. In diesem Beispiel ist der Wert Invicti-ProductDirectoryListing , Und dieser Wert wird auch als eindeutige ID im Datensatz „Anwendungsschwachstelleneintrag“ angezeigt. Invicti-AVITs unterstützen mehrere CWE-Einträge (Common Weakness Enumeration), daher werden CWEs nicht als eindeutige IDs verwendet. CWEs werden auch im AVIT-Datensatz angezeigt.

Wenn für Invicti AVITs doppelte Typen in Invicti für eine Schwachstelle vorhanden sind, wird das Wort „anwenderdefiniert“ in den Wert eingefügt, z. B. Invicti-custom-ProductDirectoryListing . Wenn Sie einen anwenderdefinierten Typ für Schwachstellen erstellen, ist die Schwachstellen-ID möglicherweise Invicti-Anwenderdefiniert- <title of vulnerability>.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue Felder: Für Scan-Typ = Invicti , Die betroffenen Parameter und die anwenderdefinierten Felder können Daten enthalten, die Ihnen helfen, die Schwachstelle zu verstehen und zu beheben. Wenn keine Daten vorhanden sind, werden diese Felder nicht im AVIT angezeigt.

Invicti-Schwachstellen-Integration statuszuordnung

Die folgenden quellstatus aus dem Invicti-Schwachstellen-Integration Und ihre zielstatus in Ihrer Instanz sind in der folgenden Tabelle aufgeführt.

Invicti-quellstatus und die entsprechenden ServiceNow AI Platform status

Invicti-quellstatus	Beschreibung der quellstatus	Zielstatus in ServiceNow AI Platform
Präsentieren	Das Problem wurde identifiziert.	Öffnen
Vorhanden, AcceptedRisk, überarbeitet	Das Problem wurde berücksichtigt und ist als Schwachstelle mit geringem Risiko markiert.	Zurückgestellt
Vorhanden, Falsch Positiv	Das Problem wurde berücksichtigt und ist als keine echte Schwachstelle markiert.	Geschlossen
Behoben Unbestätigt, behoben nicht bestätigt	Das Problem wurde behoben, aber nicht von Invicti Enterprise bestätigt.	Gelöst
Behoben (bestätigt), behoben Bestätigtbestätigt, behoben Bestätigtbestätigt, AcceptedRisk, behoben bestätigt, Falsch Positiv	Das Problem wurde von Invicti Enterprise behoben und bestätigt, und es sind keine weiteren Maßnahmen erforderlich.	Geschlossen
Behoben (Retest nicht möglich)	Das Problem wurde identifiziert, Invicti kann jedoch nicht erneut testen, um zu bestätigen, ob das Problem behoben wurde oder nicht.	Gelöst
Überarbeitet	Das Problem wurde in vorherigen Scans behoben, wurde jedoch erneut gefunden.	Öffnen
Zurückgestellt, Ignoriert	Das Problem wurde vom Anwender ignoriert. Um in Invicti Enterprise ein Problem zu ignorieren, aktualisiert ein Anwender seinen Status in „akzeptiertes Risiko“.	Risiko akzeptiert

Zuordnung des Anwendungs-Release

Quellfeld	Zielfeld auf ServiceNow AI Platform
ID	Quell_App_ID
CreatedAt	App_Creation_date
UpdatedAt	App_Updation_date

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	app_name
RootURL	Source_additional_info
Beschreibung	Beschreibung
Tags	Tags

Schwachstellenzuordnung

Quellfeld	Zielfeld auf ServiceNow AI Platform
Typ	Kategoriename
Schwachstellendetail	Zusammenfassung
Auswirkung	Bedrohung
Quellreferenzen	Webreferenzen
Quellempfehlung	Lösung
Typ	Source_entry_ID/ID
Schweregrad	Source_severity
Klassifizierung[„Cwe“]	CWE-Liste
CvssVectorZeichenfolge	CVVS v3-Felder

Scan-Zusammenfassungszuordnung

Quellenfeld	Zielfeld
Quelle	Quelle
Gesamtzahl der Schwachstellen	Detected_flaw_count
Datum der Initiierung	Dynamisches Scan-Datum
id	Source_Scan_ID

Zuordnung von angreifbaren Anwendungselementen (AVIT)

Quellfeld	Zielfeld auf ServiceNow AI Platform
Typ	Überprüfungstyp
Website-ID	Quell-App-ID
ID	AVIT-ID der Quelle
Datum der letzten Anzeige	Zuletzt gefunden
Datum der ersten Anzeige	Erste ermittelte
Datum der letzten Aktualisierung	Datum des letzten Scans
parameters	Betroffener Parameter
URL	Betroffene URL
Schweregrad	Quellenschweregrad

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

URL	Quell-Link
Schwachstellendetail	Zusammenfassung der Quell-Schwachstelle
Externe Referenzen	Quellreferenzen
Remedy + Remedy-Referenzen	Quellempfehlung
Status	Quellenkorrekturstatus
Auswirkung	Erklärung der Quell-Schwachstelle

Veracode Vulnerability Integration

Die Vulnerability Response Integration mit Veracode Die Anwendung verwendet Daten, die aus importiert wurden Veracode Produkt, mit dem Sie die Auswirkung und Priorität von Fehlern in Ihrem Code bestimmen können.

Veracode Vulnerability Integration

Die Veracode Das Produkt erfasst dynamische Anwendungssicherheitstests (Dynamic Application Security Testing, DAST), statische Anwendungssicherheitstests (Static Application Security Testing, SAST) und manuelle Scannerdaten und stellt diese Daten für bereit ServiceNow AI Platform®. Es lässt sich problemlos in integrieren Application Vulnerability Response Funktion von Vulnerability Response Dient zum Zuordnen von Schwachstellen von Drittparteien, um die Daten in Ihrer Instanz zu ergänzen.

Ab v19.0 von Vulnerability Response, Sie können Schwachstellen der Software Composition Analysis (SCA) und importieren Software Bill of Materials(SBOM) Schwachstellendaten, mit denen Sie Schwachstellen in Ihren Softwareanwendungen identifizieren können. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Eine gemeinsam genutzte API erfasst DAST-, SAST-, SCA-Daten und Ergebnisse manueller Penetrationstests.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Täglich rufen geplante Aufgaben die Integrationen automatisch in der Reihenfolge auf, in der sie aufgelistet werden. Sie können einzelne geplante Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Schwachstellenbeseitigung, indem die Instanz mit anderen Schwachstellenverwaltungssystemen synchronisiert wird.

Rufen Sie weitere Details von ab Veracode

Wählen Sie ab v4.2 aus **Rufen Sie Weitere Details Ab** Für angreifbare Anwendungselemente (AVITs) mit Veracode Als Quelle in der Tabelle „Angreifbares Anwendungselement“ [sn_vul_App_vulnerable_item] oder aus den Listenansichten in den Vulnerability Response-Arbeitsbereichen, um Folgendes anzuzeigen Veracode Daten.

- Details zu HTTP-Quellanforderungen und Quellantworten für DAST-Scans (Dynamische Anwendungssicherheitstests) werden in der zugehörigen Liste „HTTP-Anforderung/-Antwort“ angezeigt.
- Lösungsempfehlungen von Veracode werden in der zugehörigen Liste „Ergebnisse“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- HTTP-Quellanforderung, Quellantwort und Empfehlungen werden auf der Registerkarte Details in Vulnerability Response angezeigt Vulnerability Response Arbeitsbereiche.
- Die Spalte „Beschreibung“ wird in der Tabelle für angreifbare Elemente der Anwendung [sn_vul_app_vulnerable_item] unterstützt.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Veracode V4.3 Veracode V4.2 Veracode V4.1	Application Vulnerability Response release notes Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Anwendergruppe und Rollen

Die Veracode Vulnerability Integration Wird von einem Systemadministrator [admin] installiert und von einem Mitglied der App-Sec-Manager-Gruppe konfiguriert. Weitere Informationen finden Sie unter Application Vulnerability Response Anwendergruppen und Rollen.

Veracode Vulnerability Integration

Um anzuzeigen Veracode Schwachstellenintegrationen navigieren Sie zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**an.

Die folgenden Integrationen sind im Basissystem enthalten.

Veracode Vulnerability Integration

Integration	Beschreibung
Beginnend mit v4.1: Veracode Projektintegration verknüpfen	Diese Integration ist standardmäßig aktiviert. Ruft alle zugeordneten Projekte für jede Anwendung aus ab Veracode. Anwendungen können mehrere Projekte in haben Veracode Anwendung. Importierte Daten aus dieser Integration werden in den folgenden Datensätzen angezeigt: • **Datum des letzten SCA-Scans** , **App-Erstellungsdatum** , Und **App-Update-Datum** Sind in Datensätzen in aufgeführt **Erkannte Anwendungen** . • Bei Zusammenfassungsdatensätzen und angreifbaren Anwendungselementen (AVITs) des Anwendungsschwachstellen-Scans **SDLC-Status der Quelle** (Softwareentwicklungslebenszyklus) wird angezeigt. • **Ausnutzbarkeit der Quelle** Wird in Datensätzen von angreifbaren Anwendungselementen (AVI) angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Veracode Vulnerability Integration (Fortsetzung)

Integration	Beschreibung
Veracode Integration der Anwendungsliste (JSON)	Diese Integration ist standardmäßig inaktiv. Ruft Ab Veracode Anwendungsscannerdaten (Schwachstellen, Metadaten) und ergänzt Ihre Anwendungsdaten. Ruft Scan-Datensätze von ab VeracodeÜber eine JSON-basierte API.
Veracode Integration der Anwendungsliste (XML)	Diese Integration ist standardmäßig inaktiv. Die XML-basierte Version dieser Integration wurde deaktiviert (veraltet). Ruft Ab Veracode Anwendungsscannerdaten (Schwachstellen, Metadaten) und ergänzt Ihre Anwendungsdaten. Diese Integration ist so festgelegt, dass sie täglich um 00:00:00 ausgeführt wird. **Hinweis:** Eine JSON-basierte API von Veracode Wird verwendet, um die Liste der Anwendungen abzurufen. Diese API importiert das „Datum der letzten Richtlinien-Compliance-Prüfung“ für diese Anwendungen, das angibt, wann diese Anwendungen zuletzt von gescannt wurden Veracode.
Veracode Software Bill of Materials(SBOM) Integration	Version 4,3 von Veracode Vulnerability Integration Enthält die folgenden Erweiterungen von Veracode SBOM Dateien: • Wenn Sie SBOM Response installiert haben, haben Sie die Möglichkeit, von gefundene Schwachstellen einzubeziehen Veracode Für die SBOM-Dateien, die Sie hochladen. • Veracode Ist dem zugeordnet **Quelle** Feld für Datensätze in der Tabelle „Stückliste“ [sn_sbom_doc] für Veracode SBOM-Dateien. Diese Integration ist standardmäßig aktiviert. Ab v4.2 Importe Software Bill of Materials Von generierte Dateien im CycloneDX- und SPDX-Format Veracode Und stellt sie zur Analyse in Ihrer Instanz in die Warteschlange. Sie müssen haben Software-Stückliste Anwendungen, die installiert sind, um diese Daten zu importieren und anzuzeigen.
Veracode Integration der Scan-Zusammenfassung (JSON)	Diese Integration ist standardmäßig inaktiv. Ruft Scan-Datensätze von ab VeracodeÜber eine JSON-basierte API. Diese Integration ersetzt die XML-basierte API-Integration. Sie ist verkettet und folgt dem Veracode Integration der Anwendungsliste, wenn aktiviert.
Veracode Scan-Zusammenfassung (XML)	Diese Integration ist standardmäßig inaktiv. Die XML-basierte Version dieser Integration wurde deaktiviert (veraltet). Ruft Scan-Datensätze von ab Veracode. Diese Integration ist verkettet und folgt dem Veracode Integration der Anwendungsliste, wenn aktiviert. **Hinweis:** Folgt automatisch Veracode Integration der Anwendungsliste, wenn sie aktiviert ist. Mit dem Datum „Letzte Richtlinien-Compliance-Prüfung“ für die Anwendungen von Veracode, Diese Integration ruft nur Daten für die Anwendungen ab, die nach „delta_Start_time“ dieser Integration gescannt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Veracode Vulnerability Integration (Fortsetzung)

Integration	Beschreibung
Veracode JSON-Integration für angreifbares Anwendungselement	Zeigen Sie ab v4.2 Details an, z. B. Gesamtverarbeitungszeiten, durchschnittliche Zeiten für Prozesse vor und nach der Integrationsausführung und Berichte zu den Datensätzen der Integrationsausführung für die Integrationen angreifbarer Anwendungselemente. Diese Integration ist standardmäßig inaktiv. Ruft Scan-Ergebnisse mit mehr Schwachstellendaten ab als die XML-basierte Integration aus Veracode. Sie fügt Avis ein und ergänzt Ihre Schwachstellendaten von Drittparteien.
Veracode Integration angreifbarer Anwendungselemente (XML)	Zeigen Sie ab v4.2 Details an, z. B. Gesamtverarbeitungszeiten, durchschnittliche Zeiten für Prozesse vor und nach der Integrationsausführung und Berichte zu den Datensätzen der Integrationsausführung für die Integrationen angreifbarer Anwendungselemente. Diese Integration ist standardmäßig inaktiv. Ruft Scan-Ergebnisse von ab Veracode, Fügt angreifbare Anwendungselemente (AVITs) ein und reichert Ihre Schwachstellendaten von Drittparteien an. Standardmäßig, wenn sich der Scannerdatensatz im befindet **Geschlossen** status, AVITs werden nicht erstellt. Vorhandene AVITs werden noch aktualisiert. Diese Integration ist verkettet und folgt dem Veracode Integration der Scan-Zusammenfassung, wenn aktiviert. Die XML-basierte API ist für veraltet Veracode JSON-Integration der Scan-Zusammenfassung. **Hinweis:** Folgt automatisch Veracode Integration der Scan-Zusammenfassung. Mit dem Datum „Letzte Richtlinien-Compliance-Prüfung“ für die Anwendungen von Veracode, Diese Integration ruft nur Daten für die Anwendungen ab, die nach „delta_Start_time“ dieser Integration gescannt wurden.
Veracode Kategorieintegration	Diese Integration ist standardmäßig inaktiv. Ruft erweiterte Kategoriedaten von ab Veracode.
Veracode CWE-Integration	Diese Integration ist standardmäßig aktiviert. Ruft Ab Veracode–Spezifische CWE-Daten (Common Weakness Enumeration) für Bedrohungsinformationen und Korrekturempfehlungen. Diese Daten werden in Anwendungsschwachstelleneintragsdatensätzen ausgefüllt und aktualisiert. Diese CWE-Integration funktioniert unabhängig von der geplanten Aufgabe für die CWE Comprehensive 2000-Integration, die Sie für aktivieren Vulnerability Response Anwendung. Ihre Daten werden nicht dupliziert, wenn Sie über verfügen Veracode CWE-Integration und CWE Comprehensive 2000 Integration aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Veracode Vulnerability Integration (Fortsetzung)

Integration	Beschreibung
Veracode DevOps-Integration	Diese Integration ist standardmäßig inaktiv. Die Integration kann in der Liste Anwendungsschwachstellen-Integrationen in angezeigt werden Application Vulnerability Response. Wenn Sie über eine DevOps Change-Geschwindigkeit-Lizenz verfügen, ist diese Funktion so strukturiert, dass DevOps-Anwender keine SecOps-Lizenz benötigen, um Zusammenfassungsdetails für Schwachstellen-Scans von Drittanbietern anzuzeigen. Es gibt keine Auswirkung oder Änderung an Application Vulnerability Response.

Informationen zu Status der Integrationsausführung finden Sie unter . Zeigen Sie an Veracode Status der Importausführung der Anwendungsschwachstellenintegration.

Informationen zum Anzeigen von Daten in Schwachstellen von Drittparteien finden Sie unter Schwachstellenbibliotheken anzeigen.

Vorbereitung für Veracode Vulnerability Integration

Ein erfolgreich Veracode Vulnerability Integration Erfordert die Planung und Ausführung von Aufgaben vor der Integration. Bereiten Sie sich auf die Integration vor, indem Sie diese Aufgaben ausführen. Die Veracode Vulnerability Integration Davon ausgegangen, dass Sie mit vertraut sind Veracode Produkt und API.

Vorbereitungen

Die CWE-Integration (Common Weakness Enumeration) wird auch von verwendet Application Vulnerability Response Und sollten vor der Installation und Konfiguration von ausgeführt werden Veracode Vulnerability Integration. Es wird mit installiert Vulnerability Response, Standardmäßig.

Hinweis:
NIST Vulnerability Database (NVD)-Daten sind zum Installieren von nicht erforderlich Veracode Integration von Anwendungsschwachstellen, bieten jedoch Ergänzungen und wären nützlich. Informationen zu NVD finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender konfiguriert. Der Standardwert für diesen Anwender ist **VR.System** . Ändern Sie diesen Wert nicht.

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Nehmen Sie vor dem Ausführen der Integration alle erforderlichen Konfigurationsänderungen basierend auf Ihren Anforderungen vor.

Validieren Sie die Größenanpassung Ihrer Instanz basierend auf der Anzahl der angreifbaren Anwendungselemente, die Sie importieren möchten. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen, wenden Sie sich an Kundenservice und Support.

Die Veracode Vulnerability Integration Erfordert eine API-ID und einen API-Schlüssel.

Prozedur

So erstellen Sie die API-ID und die Schlüssel-Anmeldeinformationen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Melden Sie sich bei an Veracode Plattform.

b. Wechseln Sie zum Anwenderaccount-Menü, und wählen Sie aus **API-Anmeldeinformationen** .

c. Klicken Sie Auf **Generieren Sie API-Anmeldeinformationen** .

d. Zeichnen Sie Ihre Anmeldeinformationen zur späteren Verwendung auf.

Installieren Sie ServiceNow® Vulnerability Response-Integration mit Veracode

Bevor Sie die Integration auf Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit die ausgeführt werden kann Veracode Produkt ist ordnungsgemäß in integriert Application Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist Anwender der App-Sec-Manager-Gruppe zu. Informationen zu Gruppenrollen finden Sie unter . Application Vulnerability Response Anwendergruppen und Rollen. • Die App-SEC-Manager-Gruppe überwacht die Konfiguration und verifiziert die erwarteten Ergebnisse.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich bei der Instanz an, die Sie installieren möchten Veracode Vulnerability Integration Ein.
2. Navigieren Sie zum ServiceNow Store.
3. In ServiceNow Store, Suchen Sie mit nach Vulnerability Response-Integration Veracode Anwendung.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Erwägen Sie, das zu lesen **Andere Anforderungen** Und **Abhängigkeiten** Abschnitte, falls zutreffend.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Geben Sie **Instanzname** und den **Reason for the Instance** (Grund für die Instanz) ein und klicken Sie auf **Validate Instance** (Instanz validieren).
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**an.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Nächste Maßnahme

Konfigurieren Sie Veracode Vulnerability Integration Für Ihre Umgebung. Weitere Informationen finden Sie unter Konfigurieren Sie die Eigenschaften Veracode Vulnerability Integration.

Konfigurieren Sie die Eigenschaften Veracode Vulnerability Integration

Bevor Sie die Integration auf Ihrer Instanz ausführen, müssen die Installations- und Konfigurationsschritte abgeschlossen werden, damit die ausgeführt werden kann Veracode Produkt ist ordnungsgemäß in integriert Application Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Vulnerability Response Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.
Überprüfen Sie, ob Vulnerability Response Integration mit Veracode Anwendung ist installiert und aktiviert.	Um zu überprüfen, ob diese Anwendung aktiviert ist, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Installieren Sie ServiceNow Vulnerability Response-Integration mit Veracode.
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die App und weist Anwender der Anwendergruppe „App-Sec Manager“ zu. • Der App-SEC-Manager überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.
Für Veracode Integration von Anwendungsschwachstellen, haben Sie Ihren **API-ID** Und **API-Schlüssel** Bereit.	Kontakt Veracode Um zu erhalten **API-ID** Und **API-Schlüssel** . Weitere Informationen finden Sie unter Vorbereitung für Veracode Vulnerability Integration. Ab Version 4,0, wenn Sie verwenden Veracode Vulnerability Integration, Die Penetrationstest-Tests in Veracode Vulnerability Integration Sind manuelle Ergebnisse von Veracode. Diese Ergebnisse sind nicht mit Penetrationstestbewertungsanforderungen verknüpft, die Sie in konfigurieren Application Vulnerability Response. Weitere Informationen zu Penetrationstestanforderungen in finden Sie in Application Vulnerability Response, Siehe Penetrationstests konfigurieren.

Erforderliche Rolle: App-Sec Manager-Anwendergruppe

Prozedur

1. Navigieren zu **Alle** > **Veracode Vulnerability Integration** > **Konfiguration**an.
2. Füllen Sie aus **API-ID** Und **API-Schlüssel** Felder.
3. Wählen Sie Ihre Testergebnisse aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Version 4,0:	**a.** Wählen Sie Aus **DAST** Oder **SAST** Daten–typen, die in den Import aufgenommen werden sollen. **Hinweis:** Sie können eine oder die andere oder beide auswählen, müssen jedoch mindestens eine auswählen. **b.** Wählen Sie Aus **SCA** Dient zum Importie–ren von SCA-Schwachstellen (Software Composition Analysis). **c.** Wählen Sie Aus **Manuell Einschließen** Dient zum Importieren von Ergebnissen manueller Penetrationstests aus Veracode. Für diese Ergebnisse werden AVITs er–stellt.
Version 3.0	Wählen Sie Aus **DAST** Oder **SAST** Datentypen, die in den Import aufgenommen werden sollen. **Hinweis:** Sie können eine oder die andere oder beide auswählen, müssen jedoch mindestens eine auswählen.
Version 1,0:	Ergebnisse dynamischer Anwendungssi–cherheitstests sind standardmäßig ausge–wählt.

4. Fügen Sie hinzu Veracode **Schweregrad** Ebene zum Filtern Ihrer importierten Daten.
   Dieser Wert wird aus importiert Veracode. Sie können dem Feld mehrere Werte hinzufügen. Wenn ausgefüllt, werden beim Import nur Daten erfasst, die den von Ihnen hinzugefügten Schweregradstufen entsprechen.
5. Speichern und validieren Sie Ihre Auswahlmöglichkeiten.

Option	Bezeichnung
Version 3,0:	Klicken Sie Auf **Anmeldeinformationen spei chern und testen** . **Hinweis:** Die Konfiguration wurde erfolgreich abge-schlossen, es sei denn, eine Fehlermeldung wird angezeigt. Wenn während der Konfigura-tion eine Fehlermeldung angezeigt wird, geben Sie Ihre Daten erneut ein.
Version 1,0:	Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Überprüfen Sie die erfolgreiche Konfigura–tion, indem Sie auf klicken **Test-Anmeldein formationen** . **Hinweis:** Die Konfiguration wurde erfolgreich abge-schlossen, es sei denn, eine Fehlermeldung wird angezeigt. Wenn während der Konfigura-tion eine Fehlermeldung angezeigt wird, geben Sie Ihre Daten erneut ein.

6. Wählen Sie aus, wie Sie Ausnahmen und falsch positive Ergebnisse für AVITs beim Import verwalten möchten.
   Optionen zum Verwalten von AVITs beim Import mit ServiceNow Ausnahmemanagement und falsch positive Workflows sind standardmäßig aktiviert. Die Workflows werden basierend darauf ausgelöst, wie **Quelle** status in den AVITs werden in Ihrer Instanz zugeordnet. Ein Beispiel für einen Anwendungsfall finden Sie unter Statuszuordnung für Zurückstellungen und falsch positive Ergebnisse in verwalten Application Vulnerability Response.

7. Wählen Sie ab v4.3 die Einstellungen für die folgenden Parameter aus, oder überprüfen Sie sie.

8. Wählen Sie Aus **Anmeldeinformationen speichern und testen** .

Nächste Maßnahme
Wenn Ihre Umgebung domänengetrennte Importe erfordert, finden Sie weitere Informationen unter Erstellen Sie domänengetrennte Importe für eine Integration.

Informationen zur Erstinstallation finden Sie unter Application Vulnerability Response konfigurieren Für weitere Anweisungen.

Änderungen finden Sie nach der Erstinstallation unter Veracode Vulnerability Integration Änderungen und Aktivitäten.

Zeigen Sie an Veracode Status der Importausführung der Anwendungsschwachstellenintegration

Verwenden Sie **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste, um den Erfolg Ihrer Integrationsausführungen zu überprüfen, Probleme zu lokalisieren und Ihre Korrekturentscheidungen zu unterstützen.

Vorbereitungen
Um anzuzeigen Veracode Vulnerability Integration Importausführungsstatus:

- Application Vulnerability Response Und Veracode Vulnerability Integration Muss installiert und konfiguriert sein.
- Die Veracode Vulnerability Integration Importe müssen geplant und ausgeführt werden.

Erforderliche Rolle: App-Sec-Manager-Gruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Application Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur

1. [store-future: BEGIN review]Wenn Sie nicht verwenden Veracode Statusdiagramm der Integrationsausführung, [End] Navigieren Sie zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
3. Klicken Sie auf **Schwachstellenintegration Wird Ausgeführt** Zugehörige Liste.
4. Überprüfen Sie, ob alle Importe erfolgreich waren.

   Trouble?

   Die häufigsten Ursachen für eine fehlgeschlagene Ausführung sind:

   - Netzwerkunterbrechung.
   - Ein Problem bei der Datenübertragung, das zu beschädigten Daten während der Transformation führt.

   Wenn eine dieser Bedingungen auftritt, klicken Sie auf **Jetzt Ausführen** , Und führen Sie die Integration erneut aus.
5. Zeigen Sie ab v4.2 Details an, z. B. Gesamtverarbeitungszeiten, durchschnittliche Zeiten für Prozesse vor und nach der Integrationsausführung und Berichte zu den Datensätzen der Integrationsausführung für die Integrationen angreifbarer Anwendungselemente.
   Weitere Informationen zum Anzeigen zusätzlicher von importierter Details Veracode, Weitere Details finden Sie unter Veracode Vulnerability Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzeigen Veracode Scan-Zusammenfassungen

Zeigen Sie Details für Scan-Zusammenfassungsinformationen für an Veracode Schwachstellenintegration.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Prozedur

1. Navigieren Sie zur Tabelle „Anwendungsschwachstellen-Scan-Zusammenfassungen“ [sn_vul_App_vul_Scan_summary_list].
2. Wählen Sie einen Datensatz für ein aus Veracode Scannen.
3. Ab v19.0 von Vulnerability Response Und v4.0 der Veracode Vulnerability Integration verwenden Sie das Symbol „Liste personalisieren“ (Zahnradsymbol), um die folgenden Spalten anzuzeigen.
   - Größe des statischen Scans
   - Anzahl Bibliotheken von Drittparteien
   - Anzahl anfälliger Drittparteibibliotheken
   - Gesamtanzahl der Drittanbieterfehler nach Schweregrad
   - Anzahl Probleme von Drittparteibibliotheken
   - Anzahl Probleme von Drittparteilizenzen
   - Gemischte Fehleranzahl
   - Anzahl der geminderten Fehler
   - Anzahl nicht geminderter Fehler
   - Anzahl statischer Fehler nach Schweregrad
   - Anzahl neuer Fehler nach Schweregrad
   - Anzahl nicht geminderter Fehler nach Schweregrad
   - Gesamtanzahl der Fehler nach Schweregrad
   - Bewertung des letzten SCA-Scans
   - Datum des letzten SCA-Scans
   - Veröffentlichungsdatum des Scans
   - Tags

Datentransformation für Veracode Schwachstellenintegration

Nachdem Sie die Daten identifiziert haben, die Sie importieren möchten, werden die Daten aus dem abgerufen Veracode Anwendung, verarbeitet durch eine Reihe von Datenquellen und in Ihrer Instanz transformiert.

Veracode Integration Angreifbarer Anwendungselemente

Die Daten aus der API werden zuerst in geladen Veracode Tabelle „AppVul-Elementimport“ [sn_vul_veracode_appvul_item_Import], und Veracode AppVul-Elementtransformation wird verwendet, um die importierten Informationen zu transformieren.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu *System Import Sets > Transform Maps*Und suchen Sie nach Veracode AppVul-Elementtransformation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Veracode AppVul-Elementtransformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
app_id	Quell_App_ID	Anwendungs-ID.
Ausstellende ID	Source_avit_ID	AVIT-ID.
app_name	app_name	Anwendungsname.
Version	App_Version	Anwendungsversion.
Build_ID	Source_Scan_ID	Build-ID der Anwendung.
account_id	account_id	Account-ID.
Sandbox_ID	Sandbox_ID	Sandbox-ID.
Last_Update_time	Last_Scan_date	Zeitpunkt der letzten Aktualisierung.
App_Name + Last_Scan_date	Scan_Summary_Name	Scan-Zusammenfassung.
life_cycle_stage	Source_sdlc_Status	SDLC-Status der Quelle.
level	Source_severity	Quellenschweregrad.
Category_Name	Kategorie	Kategorie.
Source_severity	Source_severity	Quellenschweregrad.
Category_ID + „ CWE-“ + CweId	Source_entry_ID	Quelleintrags-ID.
Source_Vulnerability_summary	Source_Vulnerability_summary	Zusammenfassung der Quell-Schwachstelle.
Source_Recommendation	Source_Recommendation	Quellempfehlung.
Beschreibung	Beschreibung	Beschreibung aus der Quelle.
Beschreibung	Source_Vulnerability_explanation	Erklärung der Quell-Schwachstelle.
Mitigation_Status_desc	Source_Mitigation_Status	Quellminderungsstatus.
Remediation_Status	Source_Remediation_Status	Quellkorrekturstatus.
Zeile	Line_number	Position, in der der Fehler gefunden wird.
Modul	Application_Module	Anwendungsmodul.
Quelldatei	Source_Notes	Quellnotizen.
Betrifft_Richtlinie_Compliance	Erfüllt_mit_Richtlinie	Werte können „Ja“ oder „Nein“ sein, je nachdem, ob die Quellinformationen „wahr“ oder „falsch“ sind.
Sourcefilepath + sourcefile	location	Standortzuordnung im Fall von `static`Fehler.
URL	location	Standortzuordnung im Fall von `dynamic`Fehler.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Veracode AppVul-Elementtransformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
Umfang, Typ, exploitLevel	Source_additional_info	Namenswertfeld, das im Falle statischer Fehler mit den Werten aus der Quelle ausgefüllt wird.

Die folgenden Transformationsskripts werden während des Transformationsprozesses ausgeführt.

Veracode Zeitpunkt und Zweck des Transformationszuordnungsskripts

Wenn das Skript ausgeführt wird	Zweck
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist)	Skript, das verwendet wird, um die Datenquelle zu verarbeiten und die Anzahl der erstellten, aktualisierten oder unveränderten AVITs und der im Rahmen dieser Integration aus importierten AVITs zu aktualisieren Veracode. Dieses Skript ist zur internen Verwendung vorgesehen und darf nicht geändert oder gelöscht werden.

Veracode Vulnerability Integration Änderungen und Aktivitäten

Konfigurieren Sie optionale Änderungen speziell für Veracode Vulnerability Integration.

Anzeigen zusätzlicher Daten, die von importiert wurden Veracode Vulnerability Integration

Hinweis:
Ändern anderer Veracode Vulnerability Integration Andere Einstellungen als die hier aufgeführten erfordern erweiterte Einstellungen ServiceNow Und Application Vulnerability Response Fachwissen und übersteigt den Umfang der Produktdokumentation.

Rufen Sie weitere Details von ab Veracode

Wählen Sie ab v4.2 aus **Rufen Sie Weitere Details Ab** Für angreifbare Anwendungselemente (AVITs) mit Veracode Als Quelle in der Tabelle „Angreifbares Anwendungselement“ [sn_vul_App_vulnerable_item] oder aus den Listenansichten in den Vulnerability Response-Arbeitsbereichen, um Folgendes anzuzeigen Veracode Daten.

- Details zu HTTP-Quellanforderungen und Quellantworten für DAST-Scans (Dynamische Anwendungssicherheitstests) werden in der zugehörigen Liste „HTTP-Anforderung/-Antwort“ angezeigt.
- Lösungsempfehlungen von Veracode werden in der zugehörigen Liste „Ergebnisse“ angezeigt.
- HTTP-Quellanforderung, Quellantwort und Empfehlungen werden auf der Registerkarte Details in Vulnerability Response angezeigt Vulnerability Response Arbeitsbereiche.
- Die Spalte „Beschreibung“ wird in der Tabelle für angreifbare Elemente der Anwendung [sn_vul_app_vulnerable_item] unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ändern Veracode Integrationsinstanzparameter

Nach der Erstinstallation können Sie Parameter für ändern Veracode Integrationen in Veracode Integrationsinstanz.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Parameter für eine Integration von ihrer Instanz aus ändern, um zu bestimmen, welche Art von Daten Sie erfassen. Für einige dieser Einstellungen können Sie diese Parameter auch über die Konfigurationsseite der Integration ändern.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Integrationen**an.
2. Wählen Sie Aus **Veracode-Anwendungsschwachstelle** In der Spalte Quellinstanz für Veracode Integration, die Sie ändern möchten.
3. Wählen Sie aus **Integrationsinstanzparameter** Registerkarte und doppelklicken Sie auf ein Feld in der Wertspalte, um die Werte zu ändern.

   Ab v19.0 von Vulnerability Response Und v4.0 des Veracode Vulnerability Integration, Sie können die folgenden Parameter für konfigurieren Veracode Integrationen.

   Manuell importieren

   Geben Sie Ein Wahr Dient zum Importieren von Ergebnissen manueller Penetrationstests aus Veracode. Sie können diesen Wert auch über die Integrationskonfigurationsseite ändern.

   Die Penetrationstest-Tests in Veracode Vulnerability Integration Sind manuelle Ergebnisse von Veracode. Diese Ergebnisse sind nicht mit Penetrationstestbewertungsanforderungen verknüpft, die Sie in konfigurieren Application Vulnerability Response. Weitere Informationen zu Penetrationstestanforderungen in finden Sie in Application Vulnerability Response, Siehe Penetrationstests konfigurieren.

   Import_sca

   Geben Sie Ein Wahr Dient zum Importieren von SCA-Schwachstellen (Software Composition Analysis). Sie können diesen Wert auch über die Integrationskonfigurationsseite ändern.

   status

   Geben Sie Ein Öffnen Oder Geschlossen Um Ergebnisse für die gewünschten status zu importieren. Wenn Sie dieses Feld leer lassen, importieren die Integrationsergebnisse sowohl für den status „Offen“ als auch für den status „Geschlossen“.

   Policy_Sandbox

   Geben Sie ein Richtlinie Oder Sandbox Zum Importieren von Datensätzen, die einer Richtlinie oder einer Sandbox entsprechen. Diese Datensätze können sich darauf beziehen, wie Anwendungen in Ihrer Umgebung getestet werden.

   Policy_rule_pass

   Geben Sie Ein Wahr Oder Falsch Dient zum Importieren von Datensätzen, die eine Richtlinienregel bestanden haben. Diese Datensätze können sich darauf beziehen, wie Anwendungen in Ihrer Umgebung getestet werden.

4. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie ein Handbuch durch Veracode Import von Anwendungsschwachstellen

Wenn Ihr anfänglicher Import fehlgeschlagen ist oder Sie nicht auf den geplanten anfänglichen Import warten möchten, können Sie unabhängig von der täglichen geplanten Aufgabe einen vollständigen Datenimport durchführen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

Prozedur

1. Navigieren zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**an.
2. Wählen Sie und Integration aus, z. B. Veracode Integration Der Anwendungsliste.
3. Klicken Sie auf **Jetzt ausführen**.

   Hinweis:
   Jeder der Veracode Anwendungsschwachstellen-Integrationen sollen einen möglichst vollständigen Datenabruf bieten. Die Ausführung von außerhalb der Reihenfolge erfordert ServiceNow Und Application Vulnerability Response Kompetenz und kann zu unvollständigen Daten führen.

   Sobald der Import abgeschlossen ist, werden geplante Importe fortgesetzt.
4. Informationen zu Status der Integrationsausführung finden Sie unter . Zeigen Sie an Veracode Status der Importausführung der Anwendungsschwachstellenintegration.
5. Wenn Sie andere Integrationsparameter ändern möchten, müssen Sie zur Integrationsinstanz navigieren.

Festlegen Veracode Vulnerability Integration Importzeiten

Sie können die Startzeit für zurücksetzen Veracode Vulnerability Integration.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird
Nach dem ersten Import wird die Veracode Schwachstellenintegrationen führen bei jeder Ausführung einen vollständigen Import durch. Siehe Führen Sie ein Handbuch durch Veracode Import von Anwendungsschwachstellen Weitere Informationen zum Durchführen von Importen.

Prozedur

1. Navigieren zu **Alle** > **Veracode Vulnerability Integration** > **Integrationen**an.
2. Wählen Sie eine Integration aus.
3. Legen Sie das neue fest **Startzeit** .
   Die Zeit wird als Stunden in Ortszeit berechnet. Die Standardzeit für Veracode Importe der Anwendungslistenintegration ist 00:00:00. Die anderen Integrationen sind **Bei Bedarf** Und verkettet, um nach ausgeführt zu werden Veracode Integration Der Anwendungsliste. Ändern von **Startzeit** Für eines dieser Elemente ist Advanced erforderlich ServiceNow Und Application Vulnerability Management Fachwissen.
4. Klicken Sie auf **Aktualisieren**.
   Die neue Zeit wird für den nächsten geplanten Import verwendet.

Schließen Sie geschlossene angreifbare Elemente der Veracode-Anwendung ein

Standardmäßig **Geschlossen** Angreifbare Anwendungselemente (Avis) werden während nicht erstellt Veracode Integrationsimporte für angreifbare Elemente. Wenn Sie sie erstellen möchten, müssen Sie eine Systemeigenschaft ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Die Veracode Vulnerability Integration Muss installiert sein und ausgeführt werden.

Erforderliche Rolle: Administrator

Prozedur

1. In der linken Navigation **Filternavigator** Textfeld, Typ `sys_properties.list` .
2. In **Name** Suchfeld für die Liste eingeben `sn_vul.create_closed` .
3. Doppelklicken Sie auf **Wert** Feld und auf festgelegt **Wahr**
4. Klicken Sie auf das grüne Häkchensymbol Zum Speichern.
   Datensätze in **Geschlossen** status im nächsten Veracode Importe werden als Avis in erstellt Application Vulnerability Response.

Manuelle Erfassung von Schwachstellen für Application Vulnerability Response

Sicherheitsexperten und Anwendungstester können die Ergebnisse von Anwendungspenetrationstests im Penetrationstest-Arbeitsbereich erstellen und verwalten.

Die Penetrationstestformulare sind im Penetrationstest-Arbeitsbereich verfügbar, um die in den Kerngeschäftsanwendungen identifizierten Schwachstellen zu dokumentieren.

Sicherheitsexperten und Anwendungstester können mithilfe der bereitgestellten Vorlagen im Excel- oder CSV-Format Ergebnisse aus externen Quellen und Plattformen manuell importieren. Alle Schwachstellenergebnisse werden im Penetrationstests-Arbeitsbereich verfügbar gemacht.

Um auf die Vorlage zum Hochladen in den Penetrationstest-Arbeitsbereich zuzugreifen und sie herunterzuladen, navigieren Sie zu **Alle** > **Manuelle AVIT-Erfassung** > **Datei hochladen – UI**an.

Für jeden Datei-Upload für die jeweilige Anwendung wird ein neues Penetrationstest-Formular erstellt. Alle Schwachstellenergebnisse in diesem Upload sind demselben Penetrationstest-Formular zugeordnet. Der Anwendungsname muss mit den Datensätzen in der Tabelle übereinstimmen:

- Anwendungstabelle
- Geschäftsanwendungstabelle
- Gescannte Anwendungstabelle

Der Anwendungsname ist ein Pflichtfeld in der Vorlage zum Identifizieren der Schwachstellen in einer Anwendung, die einem Penetrationstest-Formular zugeordnet sind. Alle Datensätze ohne Anwendungsnamen werden während der Erstellung der Schwachstelle nicht verarbeitet und übersprungen.

Hinweis:
Pflichtfelder in der Vorlage sind für die Verarbeitung der Penetrationstestergebnisse erforderlich. Es muss sichergestellt werden, dass alle Felder in der Vorlage intakt sind, um Probleme bei der Verarbeitung von Penetrationstestergebnissen zu vermeiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Pflichtfelder, die als Teil der Vorlage für die Erstellung des Penetrationstestergebnisses erforderlich sind

Spaltenname	Obligatorisch	Beschreibung	Verfügbare Optionen/ max. Zeichen in Zeichenfolgen
Risikobewertung	Obligatorisch	Schweregrad des angreifbaren Anwendungselements	Kritisch Hoch Mittel Niedrig Keine (Standard)
Angefordert von	Obligatorisch	Angefordert von	151
CWE-Kategorie	Obligatorisch (nur eine Spalte ausfüllen)	CWE-ID	255
Schwachstellen-ID	Obligatorisch (nur eine Spalte ausfüllen)	Schwachstellen-ID	255
Anwendung	Obligatorisch	Anwendungsname	255
Zweck der Anwendung	Obligatorisch	Zweck der Anwendung	4000
Arten vertraulicher Daten	Obligatorisch	Listet die Arten sensibler Daten auf, auf die über die Anwendungen zugegriffen werden kann.	40
Liste der Compliance-Programme	Obligatorisch	Liste der Compliance-Programme	4000
Details des Technologiestapels	Obligatorisch	Details des Technologiestapels	4000
Anwendungsteam	Obligatorisch	Name des Anwendungsteams: Gruppe, die für die Entwicklung und Wartung von Softwareanwendungen verantwortlich ist	100
Zu testende URLs	Obligatorisch	Zu testende URLs	4000
Schritte zum Reproduzieren	Obligatorisch	Schritte zum Reproduzieren	1000
Technische Details	Obligatorisch	Technische Details	1000
Zugewiesen an	Obligatorisch	Zugewiesen an (Person, die für die Durchführung von Penetrationstests und die Generierung von Sicherheitsergebnissen verantwortlich ist)	151

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Pflichtfelder, die als Teil der Vorlage für die Erstellung des Penetrationstestergebnisses erforderlich sind (Fortsetzung)

Spaltenname	Obligatorisch	Beschreibung	Verfügbare Optionen/ max. Zeichen in Zeichenfolgen
Zuweisungsgruppe	Obligatorisch	Zuweisungsgruppe (Gruppe, die für die Durchführung von Penetrationstests und die Generierung von Sicherheitsergebnissen verantwortlich ist)	151

Laden Sie Anwendungsschwachstellen mithilfe einer Vorlagendatei hoch

Verwenden Sie eine Vorlagendatei, um die Anwendungsschwachstellen hochzuladen. Um auf die Vorlage zuzugreifen und sie herunterzuladen, navigieren Sie zu **Alle** > **Manuelle AVIT-Erfassung** > **Datei hochladen – UI**an.

Vorbereitungen

Erforderliche Rolle: Ethical Hacker **sn_vul.App_Pen_Tester**

Prozedur

1. Navigieren zu **Alle** > **Manuelle AVIT-Erfassung** > **Datei hochladen – UI**an.
2. Wählen Sie die Excel- oder CSV-Links aus, und laden Sie die Vorlage im entsprechenden Format herunter.
3. Geben Sie in der Vorlage die Schwachstellendaten in die Datensätze ein.
   Anweisungen zum Ausfüllen der Daten in der Vorlage finden Sie im Blatt „Beispiele“ in der Vorlage.
4. Wählen Sie Datei importieren, und laden Sie die aktualisierte Vorlage hoch.
5. Wählen Sie Absenden.

   Die Seite Schwachstellenintegration Push-Warteschlangen wird angezeigt. Sie können den Status nachverfolgen und Protokollnotizen im Zusammenhang mit den Übermittlungen anzeigen.

Hinweis:
Für auftretende Fehler:

- Ein **Fehlerprotokolldatei** Ist direkt an die zugehörige angehängt **Push-Warteschlange** Datensatz.
- Zusätzlich **Fehlerdetails** Kann auch in gefunden werden **Protokollnotizen** Abschnitt desselben Push-Warteschlangendatensatzes.
- Dieser Ansatz stellt sicher, dass ethische Hacker ihre Übermittlungen einfach überwachen und beheben können, ohne Zugriff auf tiefere Integrationsdetails auf Systemebene zu benötigen.

Überprüfen Sie die Integrationsausführung

Wenn die Integrationsausführung erfolgreich ist, überprüfen Sie die Anzahl der einzelnen Erkennungen und die erstellten oder aktualisierten Penetrationstestergebnisse.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Manuelle AVIT-Erfassung** > **Integrationen**an.
2. Wählen Sie den Namen der Integration basierend auf dem hochgeladenen Dateityp aus.
3. Wählen Sie die Registerkarte Ausführungen der Schwachstellenintegration aus.
4. Wählen Sie die Nummer der Integrationsausführung aus.
5. Wählen Sie die Registerkarte Elemente aus.
   Überprüfen Sie die Informationen auf der Registerkarte Elemente.

Ergebnisse

Registerkarte „Elemente“

Registerkarte/Feld	Beschreibung
Registerkarte „Elemente“	Zeigt die Gesamtzahl der importierten AVITs an.
Neue Elemente	Zeigt die Anzahl der angreifbaren Anwendungselemente an, die aus dieser Integrationsausführung erstellt werden.
Importierte Elemente	Zeigt die Summe aller Felder in diesem Abschnitt an.
Doppelte Elemente	Zeigt doppelte Elemente an. Dieses Feld ist nicht mehr ausgefüllt.
Unveränderte Elemente	Zeigt angreifbare Anwendungselemente an, die während der Integrationsausführung gefunden wurden und in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da keiner der relevanten Feldwerte geändert wurde.

Hinweis:
Nachdem Sie die erfolgreiche Integrationsausführung bestätigt haben, verfolgen Sie den Übermittlungsstatus, indem Sie zu navigieren **Push-Warteschlange** Datensatz. Der Datensatz „Push-Warteschlange“ enthält die folgenden Details:

- **Protokollnotizen** : Besteht aus Datensatzverarbeitungsinformationen.
- **Fehlerdateien** : Besteht aus Fehlerdetails, die während der Veröffentlichung aufgetreten sind.

Upload-Status überprüfen

Überprüfen Sie, ob die Ausführung der Schwachstellenintegration erfolgreich, teilweise erfolgreich oder ein Fehler war.

Vorbereitungen
Erforderliche Rolle: sn_vul.App_Pen_Tester

Prozedur

1. Navigieren zu **Alle** > **Manuelle AVIT-Erfassung** > **Verlauf hochgeladener Dateien**an.
2. **Überprüfen Sie den Upload-Status** : In **Push-Warteschlangen Für Anwendungsschwachstellenintegration** Tabelle: Überprüfen Sie die Spalte erstellt für den Zeitstempel des Uploads und die Spalte Status für den Upload-Status.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise: Überprüfen Sie Den Erfolg** : Zeigen Sie im Feld Notizen die Erfolgsmassage an, um sicherzustellen, dass alle Datensätze erfolgreich verarbeitet wurden.
4. **Fehlerbehandlung (Fehlgeschlagen/Teilweise Erfolgreich)**
   - Für Uploads mit dem Status „Fehlgeschlagen“ oder „Teilerfolg“ wird eine Fehlerprotokolldatei generiert.
   - Administratoranwender können diese Datei anzeigen, um die Gründe für den Upload-Fehler zu verstehen.
   - Benutzer mit der Rolle „App_Pen_Tester“ können die Datensätze der Push-Warteschlange und die zugehörigen Fehlerdetails anzeigen.
   - Die Fehlerprotokolldatei enthält nur die Ergebnisse, bei denen die Verarbeitung fehlgeschlagen ist, und enthält spezifische Informationen für die Korrektur und erneute Erfassung.
5. **Richtlinien zur erneuten Erfassung** :
   - Wenn Sie erfolgreich verarbeitete Ergebnisse erneut erfassen, werden doppelte Datensätze erstellt.
   - Um Duplikate zu vermeiden, erfassen Sie nur die in der Fehlerprotokolldatei aufgeführten Ergebnisse erneut.

Wird Korrigiert Application Vulnerability Response Schwachstellen

Die Überwachung von Fehlerkorrekturen ist ein Prozess, der mit der Überprüfung des Status beginnt und mit dem Schließen von angreifbaren Anwendungselementen (AVITs) endet. Application Vulnerability Response Bietet Tools und Verfahren, um diesen Prozess produktiver und effizienter zu gestalten.

Application Vulnerability Response Korrekturprozess

Die Korrektur angreifbarer Anwendungselemente wird manuell durchgeführt.

Eine Übersicht über den Prozess:

- Melden Sie sich bei der Application Vulnerability Response-Instanz an.
- Überprüfen Sie, ob Ihre Regeln (CI-Suche, Zuweisung) für angreifbare Anwendungselemente wie erwartet funktionieren. Informationen zum Überarbeiten von CI-Suchregeln finden Sie unter Identifizieren Sie Anwendungen in Application Vulnerability Response Automatisch. Informationen zu Zuweisungsregeln finden Sie unter Weisen Sie angreifbare Anwendungselemente in zu Application Vulnerability Response Automatisch.
- Überprüfen Sie, ob Ihre Korrekturziele korrekt sind. Siehe Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response Um Informationen zur Funktionsweise und Überarbeitung von Korrekturzielregeln zu erhalten. Zeigen Sie den Korrekturzielstatus eines angreifbaren Anwendungselements an.

  Hinweis:
  Korrekturzielregeln gehören zu AVITs. Diese Regeln werden ausgeführt, wenn AVIT importiert wird.

- Überprüfen Sie die Dashboards oder Berichte. Zeigen Sie beispielsweise Dashboards an, die AVITs-Alterung nach status anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn Performance Analytics for Vulnerability Response Die Anwendung „“ (com.snc.Vulnerability.Analytics) ist aktiviert. Anwender mit bestimmten Rollen können Daten anzeigen, die für Mitglieder der Gruppen „App-SEC Manager“ und „Security Champion“ von Interesse sind.

Für App-Sec-Manager, Performance Analytics for Vulnerability Response Enthält Application Vulnerability ResponseÜbersicht, die Ihnen bei der Überwachung von Problembereichen helfen kann. Siehe Analytics- und Reporting-Lösungen für Application Vulnerability Response Und Dashboard „Anwendungsschwachstellenmanagement“ [PA] .

Ab Version 13,0 von Vulnerability Response Anwendung: Für Security Champions, Performance Analytics for Vulnerability Response Enthält das Dashboard „meine Anwendungsschwachstellen“, mit dem Sie Ihre Problembereiche überwachen können. Siehe Dashboard „meine Anwendungsschwachstellen“ .

Ab Version 13,0 von Vulnerability Response Anwendung: Informationen zur Begrenzung der Menge der für Berichte oder zugehörige Listen gesammelten Daten finden Sie unter Definieren Sie Serviceklassifizierungen für Vulnerability Response Berichterstellung und zugehörige Listen.

- Überprüfen Sie den Status von AVITs in der Reihenfolge der Priorität, und suchen Sie nach Änderungen.
- Überarbeiten Sie das Risiko für die AVITs nach Bedarf. Weitere Informationen finden Sie unter Erstellen Sie einen Anwendungsschwachstellen-Rechner.
- Weisen Sie den AVIT bei Bedarf zur Korrektur einer Zuweisungsgruppe zu.
- Erneutes Scannen wird automatisch vom Importzeitplan der Drittpartei ausgelöst.
- Nach erneutem Scannen, wenn der Status lautet **Behoben** , AVITs werden während des Imports automatisch geschlossen.
- Nach dem Scan, wenn der Status nicht lautet **Behoben** , AVIT wird erneut geöffnet.

Rufen Sie weitere Details von ab Veracode

Wählen Sie Aus **Rufen Sie Weitere Details Ab** Für angreifbare Anwendungselemente (AVITs) mit Veracode Als Quelle in der Tabelle „Angreifbares Anwendungselement“ [sn_vul_App_vulnerable_item] oder aus den Listenansichten in den Vulnerability Response-Arbeitsbereichen, um Folgendes anzuzeigen Veracode Daten.

- Details zu HTTP-Quellanforderungen und Quellantworten für DAST-Scans (Dynamische Anwendungssicherheitstests) werden in der zugehörigen Liste „HTTP-Anforderung/-Antwort“ angezeigt.
- Lösungsempfehlungen von Veracode werden in der zugehörigen Liste „Ergebnisse“ angezeigt.
- HTTP-Quellanforderung, Quellantwort und Empfehlungen werden auf der Registerkarte Details in Vulnerability Response angezeigt Vulnerability Response Arbeitsbereiche.
- Die Spalte „Beschreibung“ wird in der Tabelle für angreifbare Elemente der Anwendung [sn_vul_app_vulnerable_item] unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellenbibliotheken anzeigen

Sie können Schwachstellendaten anzeigen, die aus der National Vulnerability Database (NVD), der Common Weakness Enumeration (CWE) oder Drittparteien importiert wurden, um zu entscheiden, ob eine Korrekturaufgabe eskaliert werden soll.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > Für **Bibliotheken** .

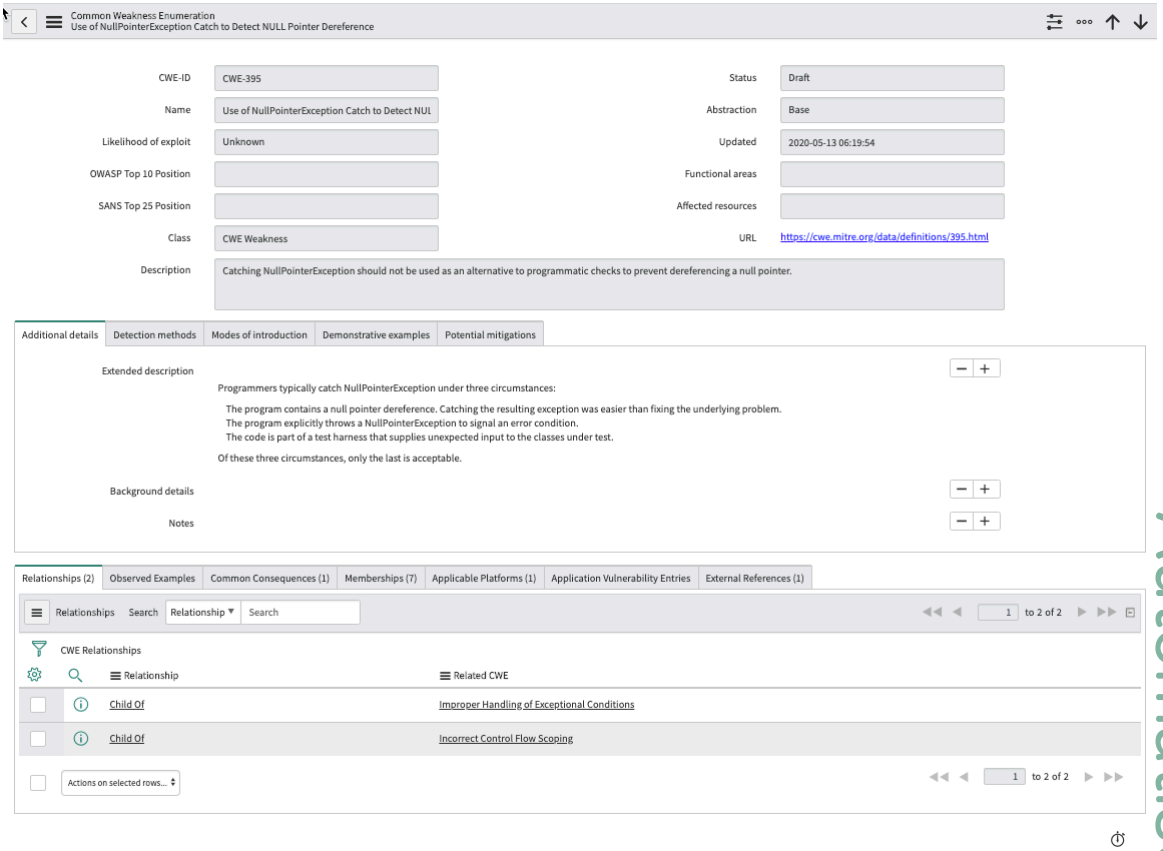
   Die folgenden Bibliotheken sind verfügbar:

Bibliotheken	Beschreibung
NVD	Liste der von NVD gefundenen Schwachstellen und enthält Sicherheitsprüflisten, sicherheitsbezogene Softwarefehler, Fehlkonfigurationen, Produktnamen und Auswirkungsmetriken einschließlich Exploits.
CWE	Liste der in der Community entwickelten Softwareschwächungstypen. Jeder CWE-Datensatz enthält auch einen zugehörigen wissensartikel, der die Schwachstelle beschreibt. Sie können eine Schwachstelle nicht über den Bildschirm „Allgemeine Schwachstellenaufzählungen“ eskalieren. Sie dient nur als Referenz.
Drittpartei	Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste zugehöriger Referenzen, angreifbarer Elemente, Exploits, CWEs und CVEs.

2. Wählen Sie eine Bibliothek aus, um Schwachstellen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Informationen zu bestimmten Feldern finden Sie unter Anwendungsschwachstellen-Felder.

Anwendungsschwachstellen-Felder

Schwachstellen werden automatisch erstellt, wenn Datensätze aus der National Vulnerability Database (NVD), der Common Weekness Enumeration (CWE) oder Integrationen von Drittanbietern heruntergeladen werden. NVD und CWE werden unter gespeichert **Bibliotheken** In Vulnerability Response Oder unter **Schwachstellen** In Application Vulnerability Response.

CWE-Schwachstelleneintragsfelder

Die Felder in dieser Tabelle sind schreibgeschützt.

Feld	Beschreibung
CWE-ID	Bezeichner für diesen Schwachstelleneintrag. Dieser Bezeichner wird sowohl für Kategorien als auch für Schwachstellen verwendet und ist zwischen den beiden Datensätzen eindeutig.
Name	Beschreibender Name, der dieser CWE-ID zugewiesen ist.
Wahrscheinlichkeit der Ausnutzung	Wie wahrscheinlich es ist, dass die Schwäche auf qualitativer Skala ausgenutzt wird. Einer der folgenden: • Niedrig • Mittel • Hoch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Position in OWASP Top 10	Die numerische Position dieser Schwachstelle in der OWASP Top 10-Liste.
SANS bis Position 25	Die numerische Position dieser Schwachstelle in der SAN Top 25-Liste.
Klasse	Typ der Schwäche
Status	Einer der folgenden: • Unvollständig • Entwurf • Stabil • Überholt • Veraltet • Unstabil
Zusammenfassung	Einer der folgenden: • Variante • Klasse • Basis • Verbindung
Aktualisiert	Zeitpunkt der letzten Aktualisierung des Datensatzes in der Instanz.
Funktionsbereiche	Liste der betroffenen Funktionsbereiche. Beispiel: **Dateiverarbeitung** . Wird nur für 24/862 Schwachstellen ausgefüllt.
Betroffene Ressourcen	Liste der betroffenen Ressourcen. Beispiel: **Datei** Oder **Verzeichnis** . Wird nur für 51/863 Schwachstellen ausgefüllt.
URL	Knowledge Base-artikel, der dieser Schwachstelle zugeordnet ist.
Beschreibung	Beschreibung der Schwachstelle.
Integrationsausführung	Die Integrationsausführung, in die diese CWE importiert wurde.
Abschnitte	
Zusätzliche Details	Softwarekonzeptbeschreibungen, die die Schwachstelle weiter erklären. Beinhaltet: • Erweiterte Beschreibung • Hintergrunddetails • Notizen
Erkennungsmethoden	Details dazu, wie Sie diese Schwachstelle in einer Anwendung erkennen können.
Einführungsmodi	Die Phasen, in denen die Schwachstelle eingeführt wird, z. B. **Implementierung** , **Architektur und Design** , Und so weiter.
Demo-Beispiele	Codebeispiele der Schwachstelle mit zugehörigen Beschreibungen.
Potenzielle Minderungen	Details dazu, wie die Schwachstelle verhindert werden kann, einschließlich der Phase des Anwendungslebenszyklus, in der sie auftritt, und der Effektivität der Minderung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zugehörige Listen	
Beziehungen	CWEs, die dieser Schwachstelle zugeordnet sind. Listet Beziehungen zwischen dieser CWE und anderen auf. Kann übergeordnetes/untergeordnetes Element, folgt/voran, required by/requires (für zusammengesetzte Schwachstellen), CanAlsoBe, PeerOf, Member von enthalten.
Beispiele für Beobachtung	Einige CVEs, die für diese Schwachstelle repräsentativ sind.
Häufige Konsequenzen	Konsequenzen eines erfolgreichen Exploits in Bezug auf Umfang und Auswirkung. Zum Beispiel: Umfang: Vertraulichkeit Impact: Anwendungsdaten Lesen
Mitgliedschaften	CWE-Mitgliedschaften mit dieser Schwachstelle.
Anwendbare Plattformen	Plattformen, die dieser Schwachstelle zugeordnet sind.
Anwendungsschwachstelleneinträge	Anwendungsschwachstelleneinträge, die einem zugeordnet sind.
Externe Referenzen	Informationen zur Schwachstelle aus externen Quellen.

Anwendungsschwachstellen-Eingabefelder

Die Felder in dieser Tabelle sind schreibgeschützt.

Feld	Beschreibung
ID	Bezeichner für diesen Schwachstelleneintrag.
Quelle	Ursprung der Schwachstelle – ob Scanner oder physischer Test.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle. Schweregradzuordnungen werden für NVD und mit bereitgestellt ServiceNow Drittpartei-Integrationen. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu.
Version 13.0: Primäre CWE Version 12.1: CWE-Eintrag	Verweis auf das Element „Allgemeine Schwachstellenaufzählung“, in das diese Schwachstelle am besten passt. Wenn der Schwachstelle mehr als eine CWE zugeordnet ist, wird die primäre CWE wie folgt bestimmt: • Ist die CWE den OWASP Top 10 zugeordnet. Wenn ja, verwenden Sie diese CWE. Wenn nicht, fahren Sie fort. • Ist die CWE den SANs Top 25 zugeordnet? Wenn ja, verwenden Sie diese CWE. Wenn nicht, fahren Sie fort. • Hat die CWE den höchsten Schweregrad? Wenn ja, verwenden Sie diese CWE. Wenn nicht, fahren Sie fort. • Wählen Sie die neueste aller CWEs aus. Die neueste CWE ist diejenige mit der neuesten **Aktualisiert** Feldwert im CWE-Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Kategoriename	Von der Drittpartei-Integration bereitgestellte Klassifizierung. Hilft bei der Zuweisung.
Schwachstellendetails	
Bedrohung	Beschreibung der Bedrohung durch diese Schwachstelle.
Beschreibung der Verringerung	Beschreibung der Schritte, die zur Minderung der Schwachstelle ausgeführt werden könnten.
Zugehörige Liste	
Version 13.0: CWEs	Liste der CWEs, die dieser Schwachstelle zugeordnet sind. Nicht zutreffend für Veracode Vulnerability Integration.

NVD-Eingabefelder

Die importierten Felder in dieser Tabelle sind schreibgeschützt.

Hinweis:

NVD-Daten werden in nicht verwendet Application Vulnerability Response Und -Einträge stellen dar Vulnerability Response Nur Daten.

CWEs, die in verwendet werden Application Vulnerability Response, Kann als Beispiele für eine Schwachstelle auf NVD-Einträge verweisen und werden hier nur zu Informationszwecken bereitgestellt.

Feld	Beschreibung
ID	Bezeichner für diesen Schwachstelleneintrag.
Risikobewertung	(Ausgeblendet, wenn nicht Vulnerability Response Angreifbare Elemente (VIS) sind der Schwachstelle zugeordnet.) Quantifiziert **Risikopunktzahl** Trennung von VIS in „Kritisch“, „hoch“, „Mittel“, „Niedrig“ und „keine“.
Risikopunktzahl	(Ausgeblendet, wenn der Schwachstelle keine VIS zugeordnet sind) Berechnetes Risiko, das das angreifbare Element für Ihre Umgebung darstellt.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle in Vulnerability Response. Schweregradzuordnungen werden für NVD und mit bereitgestellt ServiceNow Drittpartei-Integrationen. Application Vulnerability Response **Schweregrad** Wird von importiert abgeleitet **Quellenschweregrad** Und nicht NVD. Für Informationen zu Application Vulnerability Response Schweregradzuordnung, siehe Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu.
Exploit vorhanden	Ja, wenn dieser Schwachstelle mindestens ein Exploit zugeordnet ist.
Exploit-Kompetenzniveau	Niedrigstes Kompetenzniveau, das zum Ausnutzen dieser Schwachstelle erforderlich ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Exploit-Angriffsvektor	Der Angriffsvektor der Schwachstellen der Exploits für diese Schwachstelle.
Aktive AEs	(Ausgeblendet, wenn der Schwachstelle keine VIS zugeordnet sind) Anzahl der angreifbaren Elemente, die dieser Schwachstelle zugeordnet sind und sich nicht im Status „Geschlossen“ befinden. Wenn für diese Schwachstelle keine aktiven Avis vorhanden sind, **Risikobewertung** Und **Risikopunktzahl** Werden nicht angezeigt.
CWE-Eintrag	Verweis auf das Element „Allgemeine Schwachstellenaufzählung“, in das diese Schwachstelle gemäß NVD am besten passt.
Veröffentlichungsdatum	Datum, an dem die Schwachstelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt geändert wurde.
Zusammenfassung	Beschreibung der Schwachstelle.
Schwachstellendetails	
CVSS v2	CVSS v2-Daten importiert
CVSS v3	Importierte CVSS v3-Daten, nicht verfügbar vor 2015.
Bevorzugte Lösung	(Ausgeblendet, wenn der Schwachstelle keine VIS zugeordnet sind) Lösung der höchsten Ersatzlösung in der Kette, abgeleitet von den in der Schwachstelle referenzierten Lösungen. Wenn in der Kette mehr als ein höchster Ersatz vorhanden ist, wird kein Wert festgelegt. Jeder manuell festgelegte Wert kann bei nachfolgenden Importen überschrieben werden. Das manuelle Festlegen dieses Werts sollte für das angreifbare Element erfolgen.
Nachbesserungsstatus (Ausgeblendet, wenn der Schwachstelle keine VIS zugeordnet sind)	
Zurückgestellte sind ausgeschlossen	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Anwendungselemente mit dieser Schwachstelle. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
VIs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
%VIS korrigiert	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle. Diese Anzahl schließt zurückgestellte angreifbare Elemente aus.
Beinhaltet Zurückgestellte	
Angreifbare Elemente	Anzahl der aktiven angreifbaren Elemente mit dieser Schwachstelle.
VIs insgesamt	Gesamtanzahl der angreifbaren Elemente mit dieser Schwachstelle.
%VIS korrigiert	Abschluss in Prozent für die Korrektur angreifbarer Elemente mit dieser Schwachstelle.
Zugehörige Links	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Vor v13.0: Import von Software-Schwachstellen erzwingen **Hinweis:** In v13.0 entfernt	(Veraltet) Berechnet die Produktzuordnung mit neu ITSM Software Asset Management Basierend auf Informationen von NVD. Aktualisiert die Bibliothek der angreifbaren Software.
Zustand aktualisieren	Zeigt Datum und Uhrzeit der letzten Aktualisierung an. Aktualisiert Folgendes: • Status der Korrekturaufgabe • Risikopunktzahl und -Bewertung • Metriken wie aktive VIS, Gesamtanzahl VIS aus dem Abschnitt „Korrekturstatus“
Zugehörige Listen	
Angreifbare Elemente	(Ausgeblendet, wenn der Schwachstelle keine VIS zugeordnet sind) Angreifbare Elemente, die dieser Schwachstelle zugeordnet sind.
Verwundbarkeitsreferenzen	Informationen über die Schwachstelle aus externen Quellen, zitiert von NVD.
Exploits	Exploits, die dieser Schwachstelle zugeordnet sind.
Lösungen	(Ausgeblendet, wenn der Schwachstelle keine VIS zugeordnet sind) Alle Vulnerability Solution Management Integrationslösungen, die dieser Schwachstelle zugeordnet sind.
Version 13.0: Schwachstellen	Importierte CWE-Schwachstellendaten, die einem Common Vulnerabilities and Exposures (CVE) zugeordnet sind.
Version 13.0: Software mit Schwachstellen	(Ausgeblendet, wenn der Schwachstelle keine VIS zugeordnet sind) Importierte CPE-Daten (Common Platform Enumeration), die der Schwachstelle zugeordnet sind.

Identifizieren Sie Anwendungen in Application Vulnerability Response Automatisch

Wenn Daten aus einer Drittpartei-Integration importiert werden, Application Vulnerability Response Verwendet Anwendungsdaten automatisch, um nach Übereinstimmungen in zu suchen Configuration Management Database (CMDB). Dies geschieht mit **CI-Suchregeln** . Diese Regeln identifizieren Anwendungen für den Datensatz für angreifbare Anwendungselemente (AVI), um die Korrektur zu erleichtern.

Während Anwendungen importiert werden, wird eine Suche in der gescannten Anwendung durchgeführt [sn_vul_App_Scanned _Application] t Kann „Source_App_ID“ und „App_Name“ verwenden, um Übereinstimmungen mit Anwendungen aus früheren Importen zu finden. Wenn eine Übereinstimmung mit der Anwendungs-ID gefunden wird, werden ihre Werte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in verwendet **Anwendung** Und **App-Release** Felder im Datensatz des angreifbaren Anwendungselements.

Wenn keine Übereinstimmung gefunden wird oder das Feld „Anwendungs-ID“ leer ist, verwenden die Regeln die anderen Anwendungsinformationen, um zu versuchen, die Anwendung korrekt zu identifizieren. Wenn immer noch keine Übereinstimmung gefunden wird, wird nur mit ein Platzhalter gescannter Anwendungsdatensatz erstellt **Anwendungsname** Und **Anwendungs-ID** Felder.

Die **Quellanwendungs-Id** Und **Anwendungsname** Suchregeln sind im Lieferumfang enthalten Veracode Vulnerability Integration, Standardmäßig.

Hinweis:
Standard-CI-Suchregeln für Application Vulnerability Response Sind nur für verfügbar Veracode Schwachstellenintegration.

Beim Versuch einer Übereinstimmung werden die Suchregeln nach den niedrigsten Werten ausgewertet **Reihenfolge** Wert zuerst. Sie werden angehalten, wenn eine Regel ein einzelnes CI als Übereinstimmung zurückgibt.

Hinweis:
Wenn eine Regel so erstellt wird, dass sie mehr als ein CI zurückgibt, wird nur die erste Übereinstimmung verwendet.

Um das Auffinden übereinstimmender Probleme zu erleichtern, wird die CI-Suchregel, die zum Auffinden verwendet wird, hinzugefügt, wenn eine Übereinstimmung gefunden wird **CI-Übereinstimmungsregel** Feld für gescannte Anwendungen. Klicken Sie auf das Zahnrad personalisierte Liste aktualisieren Symbol oben in der Listenansicht der gescannten Anwendung, um sie der Ansicht hinzuzufügen.

Hinweis:
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

CI-Suchregeln können domänengetrennt sein und quellspezifisch sind. Wenn unterstützt, kann jede Quelle mehrere Bereitstellungen haben. Zum Beispiel die Veracode Schwachstellenintegration, kann mehrere Bereitstellungen von haben Veracode Schwachstellenintegration. Jede Bereitstellung verfügt über einen eigenen Satz von CI-Suchregeln.

Hinweis:
CI-Suchregeln werden von allen Bereitstellungen der Schwachstellenintegration freigegeben. Wenn eine Regel gelöscht oder geändert wird, wirken sich die Löschung oder Änderungen auf alle Bereitstellungen der Schwachstellenintegration aus.

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Iterieren und Durchführen des Abgleichs innerhalb von verwendet wird CMDB Kann zu längeren Verarbeitungszeiten führen. Um eine potenzielle Verschlechterung der Ressourcen oder Leistungskomplikationen zu vermeiden, testen Sie alle anwenderdefinierten CI-Suchregeln oder Änderungen an vordefinierten **CI-Suchregeln** . Siehe Verhindern Sie doppelte oder verwaiste Datensätze, nachdem Sie CI-Suchregeln für Application Vulnerability Response ausgeführt haben Weitere Informationen zum verhindern doppelter verwaister Datensätze, zum Löschen von Daten und zum Bereinigen von Daten.

Zugehörige Informationen

Konfigurationsverwaltung und die CMDB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine CI-Suchregel

Die **CI-Suchregeln** Das Modul enthält Regeln, die definieren, welche Felder übereinstimmende Daten in enthalten Configuration Management Database (CMDB). Diese Regeln werden verwendet, um Anwendungen und Anwendungs-Releases zu identifizieren und sie dem Datensatz für angreifbare Anwendungselemente (AVI) hinzuzufügen, um die Korrektur zu erleichtern.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Das Erstellen von CI-Suchregeln erfordert erweiterte Funktionen ServiceNow Und Application Vulnerability Management Fachwissen. Anstatt eine der vorhandenen Suchregeln zu ändern, sollten Sie sie kopieren und die Kopie ändern. Wenn Sie zufrieden sind, dass die neue Regel das tut, was Sie möchten, deaktivieren Sie die ursprüngliche.

Hinweis:
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen neuer Regeln.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **CMDB** > **CI-Suchregeln**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „CI-Suchregel“

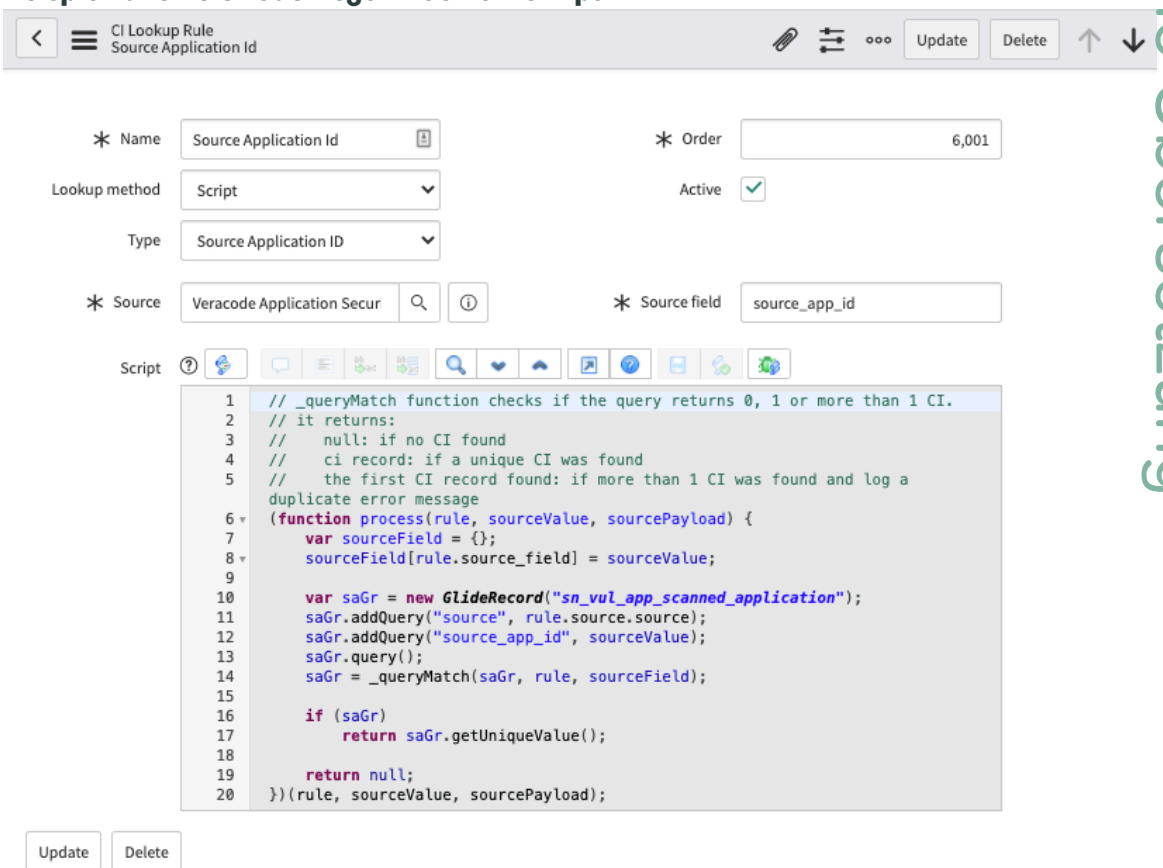
Feld	Beschreibung
Name	Name der Regel.
Suchmethode	Für den Abgleich verwendete Methode. Die Auswahlmöglichkeiten lauten wie folgt: ○ **Skript** : Vorgefertigtes oder anwenderdefiniertes Skript. ○ **Feldübereinstimmung** : Suche nach Tabelle oder Feld in der CMDB.
Typ	Mit dem Skript verwendeter Typ **Suchmethode** .
Reihenfolge	Rangfolge für die Regel. Übereinstimmungen mit der niedrigsten Reihenfolge werden zuerst ausgewertet.
Aktiv	Kontrollkästchen, um anzugeben, ob die Regel aktiv oder deaktiviert ist.
Quelle	Quelle, die als Eingabe für diese Regel verwendet wird. Nach der Auswahl werden Bedingungsfilter angezeigt.
Quellenfeld	Quellfeld, das als Eingabe für diese Regel verwendet wird. Felder müssen eine Zeichenfolge oder Zahl sein.
Beschreibung	Text, der die Regel beschreibt.
V19.0: Suchziel	Suchansatz, dem Sie folgen möchten. Wählen Sie aus: ○ Konfigurationselement ○ Produktmodell

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Skript	Bearbeitbares Beispielskript, basierend auf **Typ** , Wird angezeigt. Implementieren Sie das anwenderdefinierte Skript gemäß den Kommentaren, die in der Vorlage der Standardfunktion enthalten sind. **Hinweis:** Die Prozessfunktion hat drei Parameter: `rule`, `sourceValue`, Und `sourcePayload`
Suchen Sie nach CI Tabelle	Tabelle, die in der CMDB gesucht werden soll. Wird mit Feldübereinstimmung verwendet **Suchmethode** .
V19.0: Suchen Sie in der Produkttabelle	Wenn Sie das Produktmodell auswählen **Suchziel** , Der Standardwert ist Anwendungsmodell.
Suchen Sie nach CI Feld	Feld, das Informationen enthält, die zum Auffinden eines CI verwendet werden können. Wird mit der Feldübereinstimmung verwendet **Suchmethode** . Dieses Feld kann sich im CI-Datensatz oder in einem zugehörigen Datensatz wie einem Netzwerkadapter befinden.
V19.0: Suche nach Produktmodellfeld	Wenn Sie das Produktmodell auswählen **Suchziel** , Der Standardwert ist Name.

4. Klicken Sie auf **Absenden**.

Beispiel für eine CI-Suchregel mit einem Skript



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Felder für angreifbares Anwendungselement

CI-Suchregeln in werden erneut angewendet Application Vulnerability Response

Sie können Ihre Suchregeln für Konfigurationselemente (Configuration Item, CI) erneut anwenden, um vorhandene CIs (gescannte Anwendungen und Produktmodelle) in erkannten Anwendungsdatensätzen zu aktualisieren.

Suchregel wird erneut angewendet

Sie können Suchregeln für ausgewählte oder gefilterte Elemente in der Tabelle „erkannte Anwendungen“ erneut anwenden.

Wenn kein Filter angewendet wird, ist die Option erneut anwenden deaktiviert. Nach der erneuten Anwendung können Anwender eine Hintergrundauftrags-URL oder eine Fehlermeldung erhalten, wenn die Integration ausgeführt wird.

Um die Regeln erneut auf vorhandene erkannte Anwendungen anzuwenden, navigieren Sie zu **Alle** > **Security Operations** > **CMDB** > **Suchregeln**an.

Hinweis:
Ab v25.0.3 von Application Vulnerability Response, Wird eine neue Regel für das automatische Schließen „CI außer Betrieb genommen“ eingeführt, um die angreifbaren Elemente und Erkennungen im Zusammenhang mit außer Betrieb genommenen CIs zu schließen.

Das Suchziel wird festgelegt

Standardmäßig ist *sn_vul.use_product_model*Systemeigenschaft ist aktiviert (auf festgelegt **Wahr**). Je nachdem, wie die Systemeigenschaft für die Datensätze der CI-Suchregel festgelegt ist, werden erkannte Anwendungsdatensätze wie folgt aktualisiert:

- Wenn das Wertfeld auf festgelegt ist **Wahr** , Produktmodell ist das Suchziel für CI-Suchregeln, und erkannte Anwendungen werden mit den Produktmodellen aktualisiert.
- Wenn das Wertfeld auf festgelegt ist **Falsch** , Konfigurationselement (gescannte Apps) ist das Suchziel, und erkannte Anwendungen werden mit den Konfigurationselementen (gescannte Anwendungen) aktualisiert.

Zum Ändern von *sn_vul.use_product_model*Systemeigenschaft, damit Konfigurationselemente als Ziel verwendet werden:

1. Navigieren Sie als Anwender mit der Rolle sn_vul.App_sec_Manager zu **Alle** > **Systemeigenschaften** > **Alle**
2. Suchen *sn_vul.use_product_model*.
3. Öffnen Sie den Datensatz.
4. Legen Sie das Feld Typ auf fest **Falsch** .
5. Wählen Sie **Aktualisieren**.

Wenn Sie diese Systemeigenschaft zurücksetzen, müssen Sie Ihre Regeln so ändern, dass die Suchziele mit der Systemeigenschaftseinstellung übereinstimmen. Wenn Sie beispielsweise die Systemeigenschaft zurücksetzen, sodass Sie das Konfigurationselement als Ziel verwenden, suchen Sie nach den Regeln, die das Suchziel als Konfigurationselement haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Aktivieren Sie das Kontrollkästchen aktiv für diese Regeln, und wählen Sie aus **Aktualisieren** .
2. Suchen Sie die Regeln, die das Produktmodell als Ziel verwenden, und deaktivieren Sie sie, indem Sie das Kontrollkästchen aktiv deaktivieren und auswählen **Aktualisieren** .

Wenn Sie eine neue Suchregel erstellen, legen Sie das Suchziel für die Regel im Regelformular fest. Weitere Informationen finden Sie unter Erstellen Sie eine CI-Suchregel.

Verhindern Sie doppelte oder verwaiste Datensätze, nachdem Sie CI-Suchregeln für Application Vulnerability Response ausgeführt haben

Ergreifen Sie Schritte, um zu verhindern, dass doppelte oder verwaiste Datensätze durch Übereinstimmungen (Konfigurationselemente (CIs) innerhalb von entstehen CMDB.

Das Importieren von Schwachstellendaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Iterieren und Durchführen des Abgleichs in der CMDB verwendet wird, kann zu längeren Verarbeitungszeiten führen. Gründliches Testen und Debugging von Verarbeitungsskripts in den Regeln trägt dazu bei, das Potenzial von Problemen später im Prozess zu mindern.

Doppelte oder verwaiste Datensätze werden verhindert

- Verwenden Sie kleine Teilmengen von Daten, die für die getestete CI-Suchregel spezifisch sind.
  - Alle festlegen **CI-Suchregeln** , Anderer als der getestete, bis **Inaktiv** .
  - Analysieren Sie die importierten Anwendungen und Konfigurationselemente (Configuration Items, CIs), um sicherzustellen, dass Sie das erwartete Verhalten beobachten und die Übereinstimmung ordnungsgemäß erfolgt.
- Überprüfen Sie CI-status wie **Stillgelegt** .
- Entfernen Sie Testdaten. Sobald Sie mit der Beobachtung des richtigen oder erwarteten Verhaltens bei der CI-Übereinstimmung beginnen, beginnen Sie von vorn. Dies kann geschehen durch:
  - Löschen der für das Testen verwendeten Daten: (Siehe **Daten werden aus Tabellen gelöscht** Abschnitt)
    - Gescannte Anwendungen
    - Angreifbare Anwendungselemente (Avis)
  - Führen Sie die Integrationen manuell erneut aus.

an.

Daten werden aus Tabellen gelöscht

Manchmal haben Sie Daten importiert und stellen fest, dass etwas nicht stimmt. Wenn dies in einer Entwicklungs- oder Leistungsumgebung geschieht, könnten Sie sich von einer besseren Umgebung zurückziehen, aber das ist nicht immer eine Option.

Hinweis:
Das Ausführen dieser Aktionen erfordert erweiterte Schritte ServiceNow Fachwissen.

Es gibt vier Optionen zum Löschen von Daten aus Tabellen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwenden **Löschen Sie Alle Datensätze** Ein **Tabellenkonfiguration** .
- Konfigurieren Sie **Tabellenbereinigung** Indem Sie zu navigieren **Automatisch Entleeren** (sys_Auto_Flush.list) und erstellt eine neue **Automatisch leeren** Datensatz.
- Kürzen Sie gs.truncateTable mit einem Hintergrundskript.

Hinweis:
Niemals verwenden `truncateTable` In einer Produktionsumgebung. Wenden Sie sich an Ihren Support-Mitarbeiter, bevor Sie große Löschungen in Produktions- oder freigegebenen Umgebungen ausführen.

- Erstellen Sie eine Anforderung in HI, um die Daten zu löschen.

Weisen Sie angreifbare Anwendungselemente in zu Application Vulnerability Response Automatisch

Weisen Sie Anwendungsschwachstellen automatisch basierend auf Anwendungs-Tags oder einer der Zuweisungsgruppen im Konfigurationselement [cmdb_ci] oder Plattformzuweisungsgruppen zu, um die durchschnittliche Zeit bis zur Zuweisung zu reduzieren.

Angreifbare Anwendungselemente werden automatisch zugewiesen

Es gibt drei verschiedene Möglichkeiten, Avis mit zuzuweisen **Zuweisen mit** :

Hinweis:
Die Funktion „Zuweisungsempfehlung“ in Vulnerability Response Ist nicht verfügbar für Application Vulnerability Response.

- Anwendergruppe: Mit dieser Option können Sie eine der vorhandenen auswählen ServiceNow AI Platform® Anwendergruppen.
- Anwendergruppenfeld: Mit dieser Option können Sie ein beliebiges Zuweisungsgruppenfeld auswählen, das in der Tabelle „cmdb_ci“ verfügbar ist. Standardmäßig werden die folgenden drei Gruppenfelder im Listenmenü unter angezeigt **Anwendergruppenfeld** .
  - Keine: Gibt keinen Standardwert für dieses Pflichtfeld an
  - Konfigurationselement: Genehmigungsgruppe
  - Konfigurationselement: Zuweisungsgruppe
  - Konfigurationselement: Supportgruppe
- Skript: Mit dieser Option können Sie die Bedingungen mithilfe eines Skripts definieren. Diese Option erfordert Codierung oder erweitert ServiceNow Fachwissen.

Führen Sie zuerst Regeln mit hoher Priorität aus (Elemente, die eine besondere Behandlung erfordern, bei denen das Risiko kritisch ist oder eine AVI von regulatorischer Compliance behandelt werden sollte). Führen Sie als Nächstes Ihre allgemeinen Regeln aus, bei denen keine spezielle Behandlung erforderlich ist und Sie wissen, wer dafür verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um Avis der Gruppe zuzuweisen, die ermittelt, welcher Zuweisungsgruppe sie angehören soll. Diese Gruppe kann eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel würde zuletzt ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewertungsprozess für Zuweisungsregel

Wenn ein neues AVI erstellt, importiert oder nach dem Schließen erneut geöffnet wird, werden die Zuweisungsregeln darauf ausgewertet. Ein AVI wird nur einmal ausgewertet, es sei denn, es wird nach dem Schließen erneut geöffnet. Sie können Regeln nach Änderungen manuell erneut anwenden.

Der folgende Prozess wird für jedes neue, aktualisierte oder erneut geöffnete AVI verwendet:

- Für jede Schwachstellenzuweisungsregel wird AVI mit dem Zuweisungsfilter verglichen, wobei zuerst die Regel der niedrigsten Reihenfolge gilt.
- Wenn die Bedingung erfüllt ist, wird dem AVI eine Zuweisungsgruppe zugewiesen. Die Suche wird beendet.
- Wenn die Bedingungen keine Übereinstimmung zwischen allen anderen Regeln finden, wird die AVI der Standardzuweisungsgruppe zugewiesen, wenn eine Standardregel vorhanden ist.

Hinweis:
Wenn keine Standardregel vorhanden ist, bleibt die AVI nicht zugewiesen.

Zuweisungstyp , Ob **Manuell** Oder **Regel** Und **Zuweisungsregel** Ist über den Slushbucket „Formularlayout“ im Formular „Angreifbares Anwendungselement“ (AVI) verfügbar. Jede AVI, die ursprünglich von einer Regel zugewiesen wurde, später aber manuell neu zugewiesen wurde, enthält einen Verweis auf die ursprüngliche Regel. Verwenden **Zuweisungsregel** Und **Zuweisungstyp** Informationen zur Identifizierung von Fällen, in denen die Zuweisungsregeln keine richtige Übereinstimmung für den beabsichtigten Empfänger gefunden haben. Oder welche Regeln die meisten Neuzuweisungen hatten.

Hinweis:
Die Zuweisungsregeln bewerten manuell erstellte Zuweisungen nicht neu.

Zuweisungsregeln werden erneut angewendet

Wenn Sie eine Zuweisungsregel ändern, verwenden Sie **Änderungen Anwenden** Schaltfläche in der Listenansicht „Zuweisungsregeln“, um alle geänderten Regeln für alle aktiven offenen Avis (mit Ausnahme der manuell zugewiesenen) erneut auszuführen.

Hinweis:

Wenn *`Reapply all vulnerability assignment rules`*Die geplante Aufgabe wurde nicht vor der ersten Verwendung ausgeführt **Änderungen Anwenden** , Dann werden alle Zuweisungsregeln für alle offenen Avis ausgeführt, mit Ausnahme der manuell zugewiesenen Avis. Danach alle nachfolgenden Verwendungen von **Änderungen Anwenden** Führen Sie nur die geänderten Regeln und alle abhängigen Regeln erneut aus. Änderungen an einer Regel können dazu führen, dass eine AVI mit einer anderen unveränderten Regel übereinstimmt. [store-future: BEGIN review]Durch das erneute Anwenden von Zuweisungsregeln werden die angreifbaren Elemente nicht neu gruppiert.[End]

Die geplante Aufgabe [*`Reapply all assignment rules`*] Ist standardmäßig inaktiv. Wenn diese Option aktiviert ist, werden alle Regeln auf alle offenen Avis angewendet, mit Ausnahme der manuell zugewiesenen. Es kann ausgeführt werden **Täglich** , **Wöchentlich** , **Monatlich** , **Regelmäßig** , **Einmal** , Oder **Bei Bedarf** . Je nachdem, wie viele aktive Avis Sie in Ihrer Umgebung haben, denken Sie daran, festzulegen **Ausführen** Feld entsprechend nach der ersten Ausführung, um Leistungsauswirkungen zu vermeiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen oder bearbeiten Application Vulnerability Response Zuweisungsregeln

Sie können Regeln erstellen, um angreifbare Anwendungselemente (Avis) basierend auf Filterbedingungen automatisch zuzuweisen. Diese Regeln weisen Avis zu, da sie importiert oder manuell erstellt werden.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird

Mit Zuweisungsregeln definieren Sie die Zuweisungsbedingung und die Reihenfolge der Ausführung. Sobald ein AVI einer Regelbedingung entspricht, wird die Zuweisungssuche beendet. Weitere Informationen finden Sie unter Filtern in Application Vulnerability Management.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Zuweisungsregeln**an.
2. Klicken Sie auf **Neu**.
3. Wenn **Neu** Füllen Sie die Felder im Formular entsprechend aus.

Zuweisungsregel Für Anwendungsschwachstellen

Feld	Beschreibung
Name	Name der Gruppenregel.
Aktiv	Gibt an, ob die Zuweisungsregel aktiv ist.
Ausführungsreihenfolge	Reihenfolge, in der die Regeln ausgewertet werden. Regeln mit hoher Priorität, Elemente, die eine besondere Behandlung erfordern, bei denen das Risiko kritisch ist, oder AVI von regulatorischer Compliance behandelt werden sollte, um zuerst ausgeführt zu werden. Führen Sie als Nächstes Ihre allgemeinen Regeln aus, für die keine spezielle Behandlung gilt R Erfüllt, und Sie wissen, wer für sie verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um Avis der Gruppe zuzuweisen, die ermittelt, welcher Zuweisungsgruppe sie angehören soll. Diese Gruppe kann eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel würde zuletzt ausgeführt.
Beschreibung	Beschreibung der Zuweisungsregel.
Bedingung	
Bedingungsfelder	Bedingungen, die erfüllt werden müssen.
Neues Kriterium	Fügt weitere Bedingungsfilterfelder zur Auswahl hinzu.
Zuweisen mit	Um die Zuweisung von Gruppen zu automatisieren, die basierend auf dieser Regel erstellt wurden, wählen Sie eine der verfügbaren Optionen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Anwendergruppe: Wählen Sie eine Anwendergruppe aus der Suchtabelle aus. ○ Anwendergruppenfeld: Wählen Sie ein Anwendergruppenfeld aus dem Listenmenü aus. ○ Skript: Erstellen oder bearbeiten Sie ein Skript. **Hinweis:** Das Erstellen oder Bearbeiten eines Skripts erfordert ServiceNow Fachwissen.

4. Klicken Sie auf **Absenden**.
   Neue oder aktualisierte Regeln werden beim nächsten Import ausgewertet.

Zuweisungen werden aus entfernt Application Vulnerability Response Angreifbare Elemente und Korrekturaufgaben

Sie können löschen **Zugewiesen an** Und **Zuweisungsgruppe** Felder auf Application Vulnerability Response Angreifbare Elemente direkt aus den Datensätzen für angreifbare Anwendungselemente und Korrekturaufgaben, die Sie bestimmen, dass sie Ihnen oder Ihren Gruppen möglicherweise falsch zugewiesen sind.

Übersicht für den Workflow

Wenn Sie das bestimmen Application Vulnerability Response Angreifbare Elemente (AVITs) und Korrekturaufgaben (AVULs) liegen nicht in Ihrem Umfang für die Korrektur. Wenn Sie der Meinung sind, dass Datensätze Ihnen oder Ihren Gruppen falsch zugewiesen wurden, können Sie sich selbst oder Ihre Gruppen aus dem entfernen **Zugewiesen an** Und **Zuweisungsgruppe** Felder in AVIT- und AVUL-Datensätzen.

Der Workflow zum Aufheben der Zuweisung wird in den klassischen Ansichten und Arbeitsbereichsansichten für AVITs und AVULs unterstützt.

Sie haben die Möglichkeit, Anforderungen zum Löschen der Zuweisungsfelder zur Genehmigung zu senden. Weitere Informationen finden Sie unter Genehmigen oder lehnen Sie eine Anforderung zum Aufheben der Zuweisung in ab Vulnerability Response.

- Die **Zuweisung Aufheben** Die Schaltfläche wird in AVIT- und AVUL-Datensätzen in einem anderen Status als „Geschlossen“ oder „gelöst“ angezeigt.
- Nachdem die Anforderung zum Löschen der Felder genehmigt wurde, alle **Zugewiesen an** Und **Zuweisungsgruppe** Felder in den AVITs, die einer AVUL zugeordnet sind und dieselbe Zuweisungsgruppe haben, werden ebenfalls nicht zugewiesen. Wenn ein angreifbares Anwendungselement eine andere Zuweisungsgruppe hat als die zugehörige Korrekturaufgabe, wird die Zuweisung nicht aufgehoben. In den meisten Fällen wurden diese angreifbaren Anwendungselemente manuell zugewiesen. Weitere Informationen finden Sie unter Entfernen von Zuweisungen aus angreifbaren Elementen und Korrekturaufgaben.
- Alle Datensätze, die Sie entweder mit der UI-Aktion oder manuell aktualisieren, werden im Modul „nicht zugewiesen“ für angezeigt Application Vulnerability Response.
- Sie können die Zuweisungsfelder für mehrere AVITs in einer Liste löschen. Nachdem Sie die AVITs und dann ausgewählt haben **Massenbearbeitung** Wählen Sie im angezeigten Dialogfeld die aus **Zuweisung Aufheben** Kontrollkästchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Siehe Entfernen Sie Zuweisungen aus angreifbaren Elementen und Korrekturaufgaben Weitere Informationen zu den Schritten zum Löschen der Zuweisungsfelder.

Systemeigenschaften und Genehmigungsbenachrichtigungen

Wenn ein Korrekturbesitzer auswählt **Zuweisung Aufheben** In einem Datensatz löst standardmäßig die Systemeigenschaft sn_vul.unassign_vr.Approval_required den Genehmigungs-Flow aus und erstellt einen Datensatz für die Genehmigung einer Statusänderung im Status Überprüfen, und die Anforderung wird zur Genehmigung weitergeleitet. Die Anforderung wird in der Liste meine Genehmigungen für Anwender mit sn_vul_.unassign_Approver angezeigt.

Hinweis:
Als Schwachstellenadministrator [sn_vul.Vulnerability_admin] können Sie festlegen *`sn_vul.unassign_vr.approval_required`*Systemeigenschaft zu **Falsch** Zum Deaktivieren des Genehmigungsprozesses.

Darüber hinaus können Sie den Wert in ändern *`sn_vul.default_assignment_group`*Systemeigenschaft. Wenn die Zuweisungsfelder gelöscht werden, wird eine bestimmte Gruppe zugewiesen. Beispiel: Wenn ein Anwender auf klickt **Zuweisung Aufheben** In einem Datensatz, der zur Überprüfung an eine bestimmte Gruppe weitergeleitet werden soll, können Sie die System-ID für die Gruppe Ihrer Wahl im Feld Wert der Systemeigenschaft hinzufügen.

Hinweis:
Wenn Sie diesen Wert ändern, werden Benachrichtigungen für alle nicht zugewiesenen Vits, AVITs und CVITs an die von Ihnen angegebene Gruppe gesendet.

Siehe Entfernen von Zuweisungen aus angreifbaren Elementen und Korrekturaufgaben Weitere Informationen zum Ändern der Systemeigenschaften.

Risiko in berechnen Application Vulnerability Response Automatisch

Anwendungsschwachstellen-Rechner automatisieren die Berechnung anfänglicher Risikowerte für die Felder in angreifbaren Anwendungselementen (Avis). Risikoberechnungen bieten Einblicke in die Priorisierung von Fehlerkorrekturen. Die Bedingung für jeden Rechner wird in der Reihenfolge ausgewertet, und der erste übereinstimmende Rechner wird verwendet.

Anwendungsschwachstellen-Rechner

Die Application Vulnerability Response Das Basissystem enthält zwei Schwachstellenrechner, die die Basis festlegen **Risikopunktzahl** Für das angreifbare Anwendungselement.

- **Basisrisiko-Rechner**
- **Rechner für erweitertes Risikomanagement**

Anwendungsschwachstellen-Rechner können erstellt werden, um die Auswirkungen von Avis anhand beliebiger Kriterien mithilfe von Bedingungsfiltern zu priorisieren und zu bewerten. Unabhängig davon, ob es sich um die Geschäftsauswirkung der Schwachstelle, die Klasse des Konfigurationselements (Configuration Item, CI) oder das Alter der AVI handelt, können Sie zusätzliche Schwachstellenrechner erstellen, um andere Felder in Avis festzulegen. Oder Sie können die vorhandenen Schwachstellenrechner anpassen. Ein Rechner kann geschrieben werden, um einen beliebigen Satz von Prioritäten widerzuspiegeln. Weitere Informationen finden Sie unter Filtern in Application Vulnerability Management.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Avis enthalten **Risikopunktzahl** Wert, der von den Risikorechnern abgeleitet wird.

Hinweis:
Eine AVI wird angezeigt **Quellenschweregrad** Aber nicht normalisierter Schweregrad. Der normalisierte Schweregrad wird von den Rechnern zum Abrufen von verwendet **Risikopunktzahl** Wert, wird jedoch nicht in Avis angezeigt.

Jeder Rechner enthält eine Liste von Rechnerregeln mit einer Bedingung, die bestimmt, wann sie angewendet werden sollen. Wenn der Rechner ausgeführt wird, wird die Bedingung für jede Rechnerregel in der Reihenfolge ausgewertet, und die erste übereinstimmende Rechnerregel wird verwendet.

Alle aktivierten Schwachstellenrechner legen die ausgewählten Felder jedes Mal fest, wenn ein AVI erstellt wird, wenn sich ein zugehöriges CI oder eine Schwachstelle ändert.

Die **Grundlegendes Risiko** Rechner berechnet **Risikopunktzahl** Für Avis mit dem normalisierten Schwachstellenschweregrad.

Hinweis:
Nur ein Rechner pro Zielfeld (**Risikopunktzahl**) Kann gleichzeitig aktiv sein.

Die **Grundlegendes Risiko** Ist standardmäßig aktiviert. Die **Rechner Für Erweitertes Risiko** Ist standardmäßig inaktiv.

Regeln des Anwendungsschwachstellen-Rechners

Das Basissystem **Basisrisikorechner** Der Rechner enthält Rechnerregeln, die jedem Schweregrad (keine bis Kritisch) einen Wert (0–100) für zuweisen **Risikopunktzahl** Basierend auf Schweregrad. **Unbekannter Schweregrad** Wird automatisch eine Risikopunktzahl von 100 zugewiesen. Diese Werte können angepasst werden und z. B. **Rechner Für Erweitertes Risiko** , Neue Rechnerregeln oder neue Risikoregeln können erstellt werden.

Hinweis:
Ab v23.0 von Application Vulnerability Response, Immer wenn die Risikopunktzahl in einem AVIT aktualisiert wird, wird **Notizen** Abschnitt wird mit den folgenden Details aktualisiert:

- Rechnergruppenname
- Rechnername: Je nachdem, ob die Rechnerregel auf einer Vorlage oder einem Skript basiert, wird der Name mit den Details in Klammern angehängt. Um die Basis der Rechnerregel zu ändern oder anzuzeigen, wählen Sie eine beliebige Regel aus, und wählen Sie aus **Erweiterte Ansicht** Kontrollkästchen. Von **Werttyp** Wählen Sie im Dropdown-Feld die erforderliche Option aus. Wenn **Vorlage** Ist ausgewählt, wird die Risikopunktzahl gemäß der in der Regel angegebenen Bedingung aktualisiert. Wenn **Skript** Ist ausgewählt, können Sie das vorhandene Skript entweder hinzufügen oder aktualisieren. Die Systemeigenschaft `sn_sec_cmn.risk_score_changes_add_worknotes`Hilft beim Ausfüllen des Abschnitts „Arbeitsnotizen“. Ab v25.0.3 von Application Vulnerability Response, Die Systemeigenschaft `sn_sec_cmn.risk_score_changes_add_worknotes`Ist standardmäßig inaktiv. Wenn Sie sie aktivieren, können Sie nur im Abschnitt „Arbeitsnotizen“ alle Änderungen im Zusammenhang mit der Risikopunktzahl eines angreifbaren Anwendungselements anzeigen. Außerdem werden die Arbeitsnotizen nur aktualisiert, wenn sich die Risikopunktzahl ändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Basissystem **Rechner Für Erweitertes Risiko** Rechner enthält eine spezialisierte Schwachstellenrechnerregel namens **Standardrisikoregel** . Wird berechnet **Risikopunktzahl** Basierend auf mehreren Werten:

- Schwachstellenschweregrad
- OWASP Top 10
- SANS Top 25

Sie können die Kriterien für die Standardrisikoregel anpassen. Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel.

Sie können die Werte anpassen, die in verwendet werden sollen **Standardrisikoregel** Und wie viel Gewichtung jeder dieser Werte gegeben werden soll. Gewichtungen werden verwendet, um anzupassen, wie viel jedes Element beim Festlegen von zählt **Risikopunktzahl** .

Jede Regel hat einen **Reihenfolge** Wenn Sie jedoch die erste Einstellung festlegen, die den Bedingungen entspricht, wird aktualisiert **Risikopunktzahl** Feld in AVI. Nicht geskriptete Rechnerregeln verursachen normalerweise weniger Auswirkungen auf die Leistung als geskriptete Rechnerregeln.

Gewichtungen Der Schwachstellenrisikopunktzahl

Allen Schwachstellen wird eine Risikopunktzahl und eine Bewertung basierend auf Faktoren wie Schweregrad, Relevanz, Ausnutzungsinformationen usw. zugewiesen. Die Business-Regel `Update Risk Rating from Risk Score`In der Tabelle „angreifbare Elemente“ ist für die Berechnung der Risikobewertung verantwortlich. Wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Elemente ausgefüllt. Vor Version 17,1 von Vulnerability Response(VR)-Anwendung wurden die folgenden Risikobewertungen als Teil der Skripteinbindung bereitgestellt SchwachstellenUtils , Die hartcodiert waren.

Wert (Risikobewertung)	Gewichtung (Risikopunktzahl)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

Ab Version 18,0 von Vulnerability Response,

- Die Risikobewertungstypen werden in der Basistabelle als avr_Risk_Rating geliefert. Diese Typen werden als Teil der Business-Regel in jeder Tabelle übergeben, in der die Risikobewertung berechnet wird.
- Das Skript wird geändert, sodass Sie die Einträge in den Tabellenwerten für Risikopunktzahlgewichtungen für die Berechnung der Risikobewertung abfragen können.
- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, stellen Sie sicher, dass Sie die Bezeichnungen für die neue Risikobewertung hinzufügen und auch die zugehörigen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Skripts und Business-Regeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.

- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle mit Risikopunktzahlgewichtungen zugreifen, indem Sie sn_sec_cmn_Risk_Score_weight im Filternavigator eingeben.

Darüber hinaus wird die Risikopunktzahl in den folgenden Szenarien automatisch neu berechnet:

- Wenn sich ein Konfigurationselement (Configuration Item, CI) von nicht mit Internetzugriff zu Internetzugriff ändert.
- Wenn die zugehörigen Common Vulnerabilities and Exposures (CVEs) oder Drittparteieinträge (TPEs) in den Schwachstellen-Elementen (VIS) mit einer bekannten CVE-Exploit-Schwachstelle (KEV) verknüpft sind.

Definieren Sie Felder und Gewichtungen für die Risikoregel

Passen Sie die Parameter und Gewichtungen für die Risikoregel an, damit Sie Risikopunktzahlen generieren können, die die Schwachstellen- und Asset-Daten verwenden, die für Ihre Organisation spezifisch sind. Indem Sie die Felder auswählen, die in der Risikoregel enthalten sind, können Sie ein effektives Risikobewertungs-Framework definieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.App_Manage_Risk_Score_Configuration

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Schwachstellen-Rechner**an.
2. Klicken Sie auf der Seite „Schwachstellenrechner“ auf **Rechner Für Erweitertes Risiko** .
3. Navigieren zu **Seite „Schwachstellen-Rechner“** > **Registerkarte „Regeln des Schwachstellenrechners“** > **Standardrisikoregel**an.
4. **Wahlweise:** Legen Sie im Abschnitt „Risikorechnerkriterien“ der Seite „Schwachstellenrisikoregel“ die Gewichtung für jedes Kriterium entsprechend seiner Bedeutung bei der Berechnung der Gesamtrisikopunktzahl fest.
5. Um die Regel zu deaktivieren, müssen Sie löschen **Aktiv** Kontrollkästchen.
6. Um Risikoregelfelder zu den Kriterien des Risikorechners hinzuzufügen, klicken Sie auf **Fügen Sie Kriterien hinzu** .
7. Füllen Sie im Formular die Felder aus.

Formular „Risikoregelfeld“

Feld	Beschreibung
Referenztabelle auswählen	Tabelle, die Sie zum Definieren der Gewichtung der Risikopunktzahl verwenden. Sie können eine dieser Optionen auswählen: ○ **Angreifbares Anwendungselement** : Fügen Sie Felder hinzu, die direkt vom angreifbaren Element (VI) aus DOT-Walking-fähig sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Angreifbares Anwendungselement: Konfigurationselement** : Fügen Sie Dot-Walk-Felder hinzu, die Teil der Basistabellenerweiterungen sind, z. B. die Hardwaretabelle. Diese Felder sind nicht Teil der Basistabelle (cmdb_ci). ○ **Angreifbares Anwendungselement: Schwachstelle** : Fügen Sie Dot-Walk-Felder hinzu, die Teil der Tabellen sind, die die Basistabelle erweitern, z. B. Drittparteieintrag. Diese Felder sind nicht Teil der Basistabelle „Schwachstelleneintrag“. ○ **Referenztabelle Für Angreifbares Anwendungselement** : Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) sind, oder Tabellen, die einen Verweis auf das angreifbare Element haben. Diese Felder sind nicht direkt Dot-Walking-fähig vom VI ○ **Konfigurationselement-Referenztabelle** : Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von cmdb_ci sind, oder Tabellen, die einen Verweis auf cmdb_ci haben. Diese Felder sind nicht direkt Dot-Walking-fähig vom VI ○ **Referenztabelle Für Schwachstellen** : Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von sn_vul_entry sind, oder Tabellen, die einen Verweis auf sn_vul_entry haben. Diese Felder sind nicht direkt Dot-Walking-fähig vom VI ○ **Anwenderdefinierte Bedingungen** : Verwenden Sie diese Option, um der Regel Gewichtungen zuzuweisen, indem Sie die Bedingung auswerten. Beispielsweise bestimmt der Filter mit Internetzugriff, ob ein Konfigurationselement (Configuration Item, CI) extern oder intern ist.
Tabelle	Feld, das nur angezeigt wird, wenn eine der folgenden Optionen in der Referenztabelle auswählen ausgewählt ist: ○ **Angreifbares Anwendungselement -> Konfigurationselement** ○ **Angreifbares Anwendungselement -> Schwachstelle**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Referenztabelle für angreifbare Anwendungselemente** ○ **Referenztabelle für Konfigurationselemente** ○ **Referenztabelle für Schwachstellen**
Feld	Feld, das für die Berechnung der Risikopunktzahl für diese Regel verwendet werden soll.
Aggregation	Feld, das nur angezeigt wird, wenn eine Referenztabelle aus der Referenztabelle auswählen ausgewählt wird. Wählen Sie den Mindest- oder Höchstwert aus, der für Berechnungen berücksichtigt werden soll, wenn das Feld aus den zugehörigen Tabellen (m2m) ausgewählt wird.
Gewichtung	Gewichtung dieses Felds innerhalb der Risikoregel. Der Wert muss eine Ganzzahl von 0 bis 100 sein.
Definieren Sie Die Wertgewichtung	Komponente, um jedem Feldwert Gewichtungen zuzuweisen. Für numerische Felder können Feldwerte als Bereich definiert werden (z. B. 1–5). Die Gewichtungen müssen eine Ganzzahl zwischen 0 und 100 sein. **Hinweis:** Dieses Feld wird nicht angezeigt, wenn die Option Anwenderdefinierte Bedingungen in der Referenztabelle auswählen ausgewählt ist.
Bedingungstabelle	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenztabelle auswählen ausgewählt sind. Wählen Sie eine Bedingung aus der Liste aus.
Feldname	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenztabelle auswählen ausgewählt sind. Geben Sie einen Namen für die Risikokriterien ein.
Bedingung	Feld, das nur angezeigt wird, wenn Anwenderdefinierte Bedingungen in der Referenztabelle auswählen ausgewählt sind. Zeigen Sie eine Vorschau der Elemente in dieser Tabelle an, die den definierten Bedingungen entsprechen.

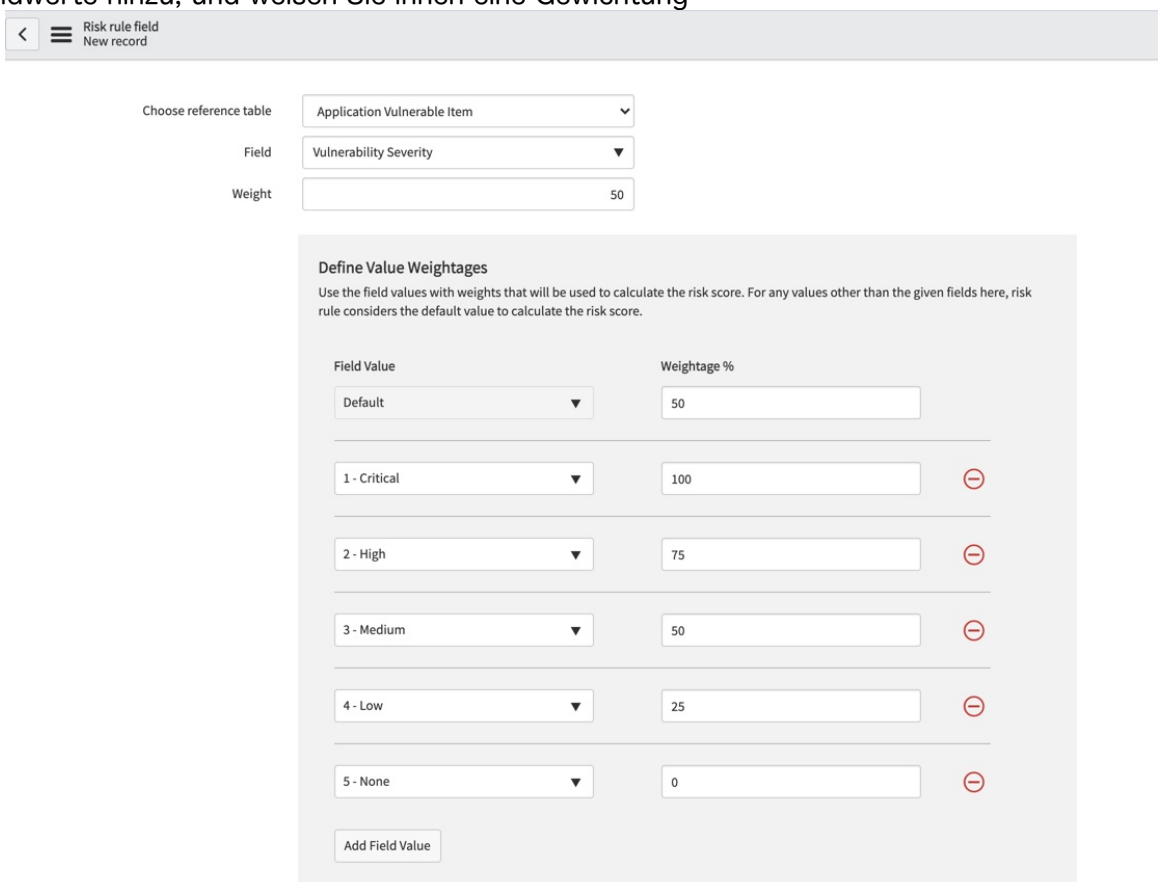
8. Klicken Sie auf **Absenden**.
9. Aktivieren Sie auf der Seite „Regel“ die Regel, und wenden Sie sie erneut an, um die Risikopunktzahl für die aktiven angreifbaren Elemente neu zu bewerten.

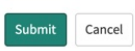
Example:
Fügen Sie den Quellschweregrad als Kriterium für eine Risikoregel hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfall: Drittpartei-Lieferanten wie Qualys und Tenable geben ihre eigenen Punktzahlen an. Diese Punktzahlen werden in ausgefüllt **Quellenschweregrad** Feld in der Tabelle „sn_vul_entry“. Verwenden Sie dieses Feld für Berechnungen der Risikopunktzahl. Um diese Punktzahl zur Berechnung der Risikopunktzahl zu verwenden, gehen Sie wie folgt vor:

1. Navigieren Sie zur Seite „Risikoregel“.
2. Um die Regel zu deaktivieren, löschen Sie **Aktiv** Kontrollkästchen.
3. Um Risikoregelfelder zu den Kriterien des Risikorechners hinzuzufügen, klicken Sie auf **Fügen Sie Kriterien hinzu** .
4. Wählen Sie in der Liste Referenztabelle auswählen die Option aus **Angreifbares Anwendungselement** .
5. Wählen Sie in der Feldliste aus **Schwachstelle.Schweregrad** .
6. In **Gewichtung** Feld die relative Wichtigkeit dieses Felds innerhalb der Risikoregel eingeben. Der Wert muss eine Ganzzahl von 0 bis 100 sein.
7. Fügen Sie im Abschnitt „Wertgewichtung definieren“ Feldwerte hinzu, und weisen Sie ihnen eine Gewichtung



zu. 

8. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Vulnerability Response-Rechner und Regeln für Schwachstellenrechner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Anwendungsschwachstellen-Rechner

Ein Anwendungsschwachstellen-Rechner ist eine vordefinierte Formel zum Berechnen eines Zielfelds, wenn bestimmte Kriterien erfüllt sind. Rechner, die das angreifbare Anwendungselement (AVI) berechnen **Risikopunktzahl** , Kann enthalten **Risikoregeln** . Risikoberechnungen bieten Einblicke in die Priorisierung von Fehlerkorrekturen.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

Hinweis:
Bei der Ausführung von Anwendungsschwachstellen-Rechnern, die Skripts enthalten, kann es zu einer Leistungsverschlechterung kommen.

Ordnen Sie Ihre Regeln an, um zuerst die einfachsten Regeln auszuführen. Führen Sie nur Skripts für die Elemente aus, die nicht mit einer Bedingung und einem Vorlagenwert oder einer Risikoregel behandelt werden können.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Schwachstellen-Rechner**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Formular „Schwachstellenrechner“

Feld	Beschreibung
Name	Der Name des Anwendungsschwachstellen-Rechners.
Tabelle	Automatisch mit dem Namen der AVI-Tabelle ausgefüllt.
Anwendung	Automatisch ausgefüllt mit Vulnerability Response.
Zielfeld	Zu berechnendes Feld.
Beschreibung	Textbeschreibung des Rechners.
Aktiv	Aktivieren oder deaktivieren Sie den Rechner.

4. Klicken Sie mit der rechten Maustaste in den Header zu **Speichern** .
   Die **Regeln Für Schwachstellenrechner** Abschnitt wird angezeigt.
5. Erstellen Sie eine Regel für den Rechner, indem Sie auf klicken **Neu** .

Hinweis:
Für **Neue Risikoregeln** Formular (nur verfügbar, wenn **Zielfeld** Ist **Risikopunktzahl**) Siehe Schritt 10.

6. Füllen Sie die Felder entsprechend aus.

Formular „Schwachstellen-Rechner-Regel“

Feld	Beschreibung
Name	Name der Rechnerregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Reihenfolge	Die Reihenfolge, in der der Schwachstellenrechner ausgeführt werden soll. Ein Rechner mit einer Auftragseingabe von 100 wird vor einem Rechner mit einer Auftragseingabe von 200 ausgeführt.
Rechner	Wird automatisch mit dem übergeordneten Rechner ausgefüllt.
Aktiv	Standardmäßig ist **Aktiv** Das Kontrollkästchen ist aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie dieses Kontrollkästchen deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt wurden.
Erweiterte Ansicht	Wenn diese Option ausgewählt ist, können geskriptete Bedingungen und geskriptete Werte aus ausgewählt werden **Bedingungstyp** Und **Werttyp** .

7. Füllen Sie die Felder im aus **Wenn diese Bedingung erfüllt ist** Registerkarte entsprechend.

Registerkarte „wenn diese Bedingung erfüllt ist“

Feld	Beschreibung
Bedingungstyp	Verfügbar, wenn Sie auswählen **Erweiterte Ansicht** . Zur Auswahl stehen: ○ Filter: Verwendet Filterbedingungen. ○ Filtergruppe: Siehe Erstellen und definieren Sie Filtergruppen Zum Definieren der Rechnerkriterien. ○ Skript: Skriptbedingung, die verwendet wird, um zu bestimmen, wann dieser Rechner angewendet werden soll. **Hinweis:** Bevor Sie Skripts schreiben, um zu bestimmen, wann die Rechner angewendet werden sollen, kehren Sie zu zurück **Anwendungsschwachstellen-Rechner** Liste. Erkunden Sie die mit dem Basissystem gelieferten Schwachstellenrechner-Datensätze.
Bedingung	Definiert grundlegende Filterbedingungen, um zu bestimmen, ob der Rechner verwendet werden soll oder nicht. Wählen Sie entweder aus **Filtergruppe** Oder **Skript** Bedingungstypen, blendet dieses Feld aus.

8. Klicken Sie auf **Legen Sie diese Werte fest** Registerkarte und füllen Sie die Felder im Formular entsprechend aus.

Legen Sie die Registerkarte diese Felder fest

Feld	Beschreibung
Werttyp	Verfügbar, wenn Sie auswählen **Erweiterte Ansicht** . Zur Auswahl stehen: ○ Vorlage: Definieren Sie die Werte, die für jedes Feld festgelegt werden sollen. ○ Skript: Wird verwendet, um die Werte für jedes Feld festzulegen.
Skriptwerte	Verfügbar, wenn Sie ausgewählt haben **Skript** Werttyp.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Definiert, auf welche Werte die Berechnungen angewendet werden sollen.
Vorlage	Wählen Sie die Felder und Werte aus, die Sie für den Rechner verwenden möchten. Wählen Sie entweder aus **Skript** Werttyp, blendet dieses Feld aus.

9. Wenn Sie alle Einträge abgeschlossen haben, klicken Sie auf **Übermitteln** .

Hinweis:
Wenn Sie einen vorhandenen Rechner bearbeiten und alle vorhandenen Punktzahlen aktualisieren möchten, können Sie verwenden **Rechner Erneut Anwenden** Schaltfläche. Er wird durch alle aktiven Avis ausgeführt. Wenn dieser Rechner zum Festlegen seines Werts verwendet würde, berechnet er den Wert für diese Avis neu. Da das erneute Anwenden eines Rechners lange dauern kann, wird er von einer geplanten Aufgabe verarbeitet.

10. Für **Neue Risikoregeln** Füllen Sie die Felder entsprechend aus.

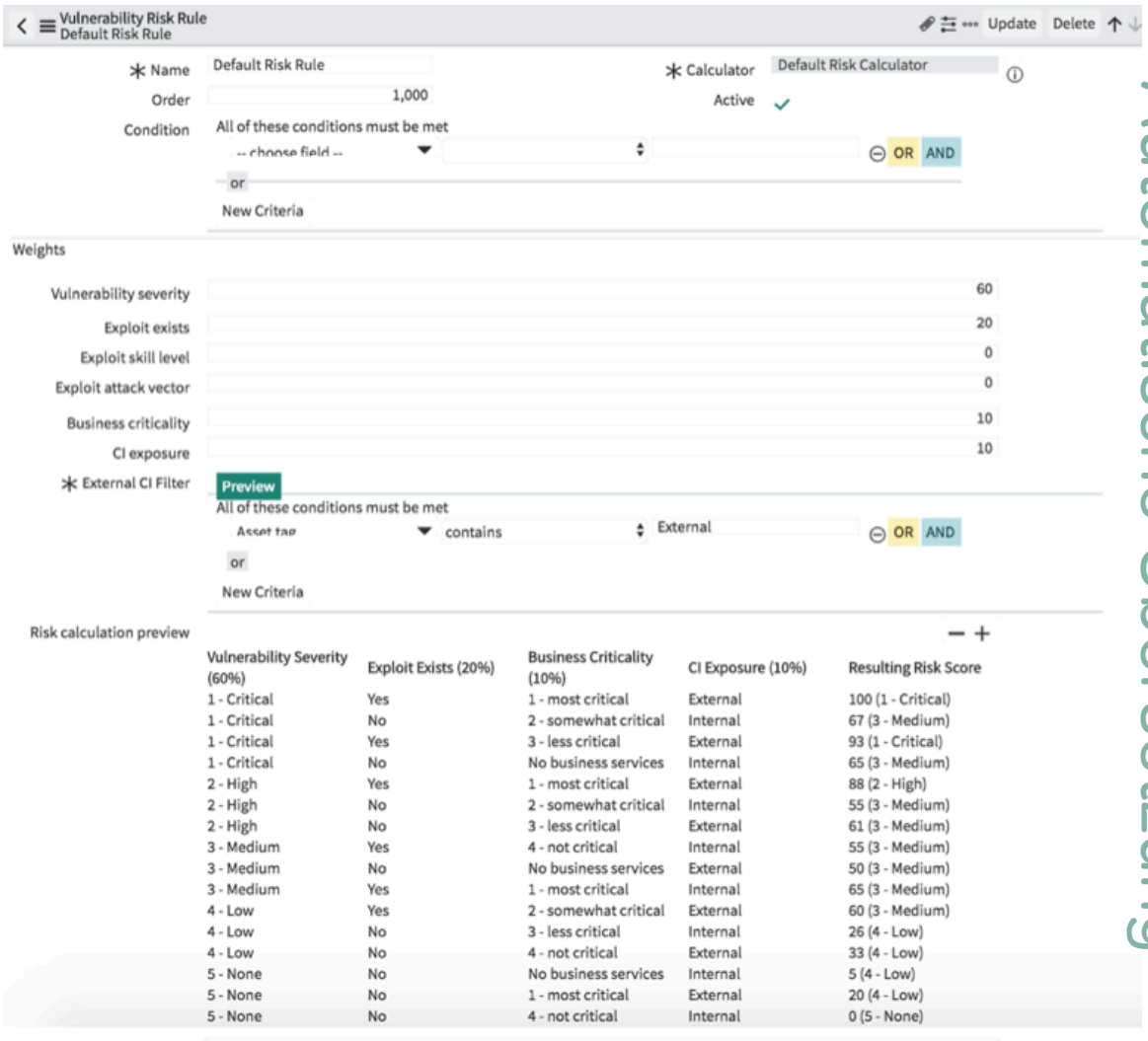
Legen Sie jede Gewichtung entsprechend dem Prozentsatz des Ergebnisses fest, der aus diesem Wert stammen soll. Legen Sie für alle Daten, die Ihr Scanner nicht bereitstellt, oder für Daten, die nicht Teil der Risikopunktzahl sein sollten, die Gewichtung auf null fest.

Während Sie die Gewichtungen aktualisieren, zeigen Szenarien die verbleibenden Gewichtungen sowie die erwarteten Gewichtungen an **Risikopunktzahl** Ergebnisse.

Feld	Beschreibung
Name	Name der Rechnerregel.
Reihenfolge	Die Reihenfolge, in der der Rechner ausgeführt werden soll. Ein Rechner mit einer Auftragseingabe von 100 wird vor einem Rechner mit einer Auftragseingabe von 200 ausgeführt.
Rechner	Wird automatisch mit dem übergeordneten Rechner ausgefüllt.
Aktiv	Standardmäßig ist **Aktiv** Das Kontrollkästchen ist aktiviert, was bedeutet, dass die Rechnerregel aktiv ist. Wenn Sie dieses Kontrollkästchen deaktivieren, gilt diese Regel nicht für neue angreifbare Elemente, die im System erstellt wurden.
Bedingung	Definiert grundlegende Filterbedingungen für die Bestimmung, ob der Rechner verwendet werden soll. Wählen Sie entweder aus **Filtergruppe** Oder **Skript** Bedingungstypen, blendet dieses Feld aus.
Gewichtungen	
Schwachstellenschweregrad	Prozentsatz des Ergebnisses, das aus dem Schweregrad stammt.
OWASP Top 10	Prozentsatz des Ergebnisses, das aus der Präsenz der Schwachstelle in der OWASP Top 10-Liste stammt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, legen Sie die Gewichtung auf null fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
SANS Top 25	Prozentsatz des Ergebnisses, das aus der Präsenz der Schwachstelle in der Liste der Top 25 der SANS stammt. Wenn diese Informationen in Ihren Schwachstellen nicht vorhanden sind, legen Sie die Gewichtung auf null fest.
Laufende Summe	Automatisch berechnete Prozentsätze insgesamt. Wenn dieser Wert 100 erreicht, werden in der Szenariovorschau Beispielrisikopunktzahlen in verschiedenen Szenarien angezeigt.
Beispielszenarien	Wenn alle Gewichtungen 100 % ergeben, werden Szenarien für Risikopunktzahlen angezeigt, die in einigen der möglichen Szenarien eine Vorschau der Risikopunktzahl bieten.



Automatische Übersetzung

11. Klicken Sie auf **Absenden**.

Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu

Application Vulnerability Response Die Schweregradzuordnung transformiert Schweregradfelder der Drittpartei-Quelle in erkennbare Felder in Vulnerability Response.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager-Gruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Application Vulnerability Response Drittpartei-Integrationen wie Veracode Vulnerability Integration Geben Sie bei der Installation Schweregradzuordnungen an. Diese Zuordnungen können angepasst werden, indem die Felder in vorhandenen Zuordnungen geändert werden.

Das Erstellen oder Bearbeiten einer Schweregradzuordnung ist nur für anwenderdefinierte oder nicht standardmäßige Zuordnungen von Drittparteien in Ihrer Umgebung vorgesehen und erfordert Application Vulnerability Response Und ServiceNow Fachwissen.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Normalisierte Schweregradzuordnung**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feldzuordnung

Feld	Beschreibung
Quelle	Der Name der Quelle für die Schweregradzuordnung.
Quellwert	Der Quellschweregradwert.
Zielwert	Der Wert des Zielschweregrads. Die Auswahlmöglichkeiten lauten wie folgt: ○ 1 – Kritisch ○ 2 – Hoch ○ 3 – Mittel ○ 4 – Niedrig ○ 5 – Keine

4. Wiederholen Sie Schritt 3 für jeden Quellenschweregrad.
5. Klicken Sie auf **Absenden**.

Filtern in Application Vulnerability Management

Rechner und Zuweisungsregeln verwenden Bedingungen während des Imports, die mit erstellt wurden **Bedingungsgenerator** . Änderungen an ihren Kriterien können sich auf die Leistung auswirken, da jeder Datensatz mit diesen Filtern ausgewertet wird.

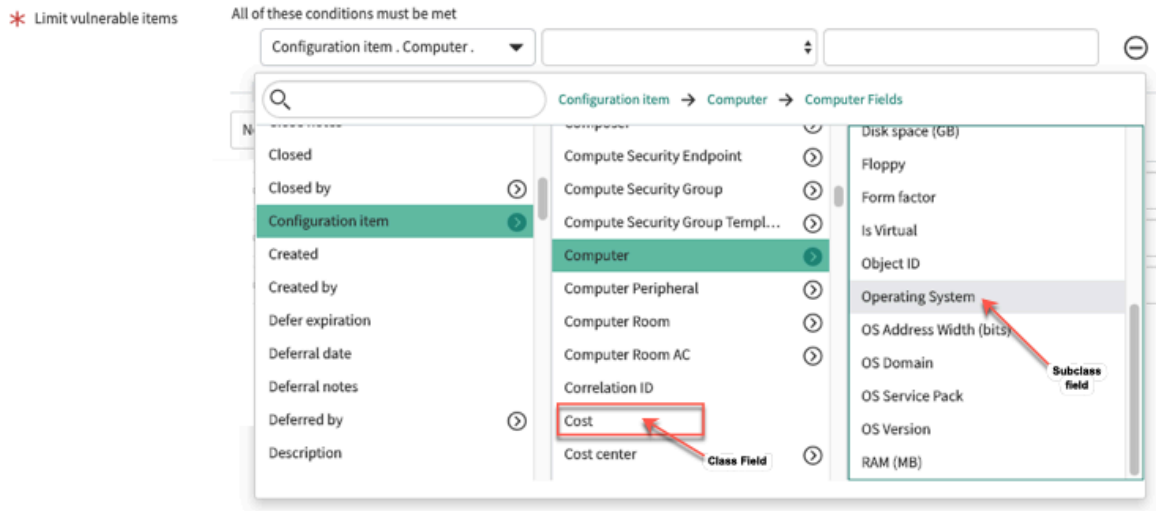
Die mit dem Basissystem gelieferten Regeln und Rechner sind für die Leistung optimiert. Das Bearbeiten oder Erstellen von Regeln oder Rechnern ist vorsichtig und erfordert möglicherweise beides ServiceNow Und Application Vulnerability Response Fachwissen. Dennoch sind einige Anleitungen verfügbar.

Vermeiden Sie das Filtern basierend auf Unterklassenfeldern

Einige Tabellen unterstützen Erweiterung. Ein Beispiel dafür ist die Tabelle „CMDB-CI“ [cmdb_ci]. Tabellen wie cmdb_ci_Hardware und cmdb_ci_Computer erweitern diese Tabelle. Wenn Sie basierend auf einem Feld filtern, das sich nicht in der übergeordneten Tabelle befindet, kann das Erstellen und Auswerten dieses Filters kostspielig sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dropdown-Menü „Bedingungsfilter“



Zum Beispiel Filtern nach **Konfigurationselement** > **Kosten**
Würde die Leistung nicht beeinträchtigen, da **Kosten** Ist ein Klassenfeld und kein Unterklassenfeld von **Konfigurationselement**.

Konfigurationselement > **Computer**, Ist jedoch eine Unterklasse, die einen Dot-Walk zu einem anderen Feld erfordert, in diesem Fall **Betriebssystem**. Dieser Prozess kann viele Millisekunden dauern, die sich schnell summieren, wenn Millionen von angreifbaren Elementen importiert werden, und die Leistung beeinträchtigen.

Hinweis:
Die Verwendung der Bedingung [enthält] ist wie eine Platzhaltersuche und kann Auswirkungen auf die Leistung haben. Die Verwendung von [ist] ist, wo immer möglich, effizienter.

Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response

Zielregeln für Anwendungskorrektur definieren den erwarteten Zeitrahmen für die Korrektur angreifbarer Anwendungselemente (Avis) und geben einen Zeitrahmen für die Behebung der Schwachstelle selbst an. Wenn beispielsweise ein angreifbares Anwendungselement eine kritische Risikobewertung enthält, muss die Schwachstelle für dieses Element innerhalb von 15 Tagen behoben werden.

App-SEC-Manager können Zielregeln für Anwendungskorrekturen erstellen, indem sie Folgendes definieren:

- Das Korrekturziel.
- Das Erinnerungsziel.
- [store-future: BEGIN review]Die Erinnerung und Benachrichtigungsempfänger – Wer soll benachrichtigt werden, wenn die Avis das Erinnerungsziel- oder Korrekturziel überschritten haben und nicht korrigiert wurden.[End]

App-SEC-Manager können das Korrekturzieldatum im AVI-Formular und in Listenansichten anzeigen, Daten werden jedoch nicht für Avis in aktualisiert **Zurückgestellt** , **Gelöst** , Oder **Geschlossen** status.

Die **Korrekturzieldatum** Ist in der AVI-Listenansicht wie folgt farbcodiert:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Avis, die ihr Benachrichtigungsdatum nicht erreicht haben, werden grün angezeigt.
- Avis, die sich dem Korrekturzieldatum nähern, werden orange angezeigt.
- Avis, die das Korrekturzieldatum überschritten haben, werden rot angezeigt.

[store-future: BEGIN review]Eine Zusammenfassungs-E-Mail gemäß der Anwendungskorrekturzielregel wird gesendet, wenn mindestens ein Avis sich dem Korrekturzieldatum nähert oder das Korrekturzieldatum überschritten ist.[End]

Standardregeln

Application Vulnerability Response Wird mit drei Standardregeln geliefert, die standardmäßig inaktiv sind:

- Regel für kritische Risikobewertung: Ein Korrekturziel mit **1 – Kritisch** Risikobewertung, ein Korrekturziel von 15 Tagen und eine Erinnerung an **7** Tage vor dem Zieldatum.
- Regel für mittlere bis hohe Risikobewertung: Ein Korrekturziel mit entweder einem **2 – Hoch** Oder **3 – Mittel** Risikobewertung ein Korrekturziel von 30 Tagen und eine Erinnerung an **7** Tage vor dem Zieldatum.
- Regel für weniger kritische Risikobewertung: Ein Korrekturziel mit **4 – Niedrig** Risikobewertung ein Korrekturziel von 45 Tagen und eine Erinnerung an **7** Tage vor dem Zieldatum.

Korrekturzielregeln können deaktiviert oder gelöscht werden

Wenn eine Regel deaktiviert ist, werden die aktuellen Korrekturzieldaten für die Avis gelöscht, auf die sie angewendet wurde. Wenn eine AVI eine aktive Regel erfüllt, wird diese Regel angewendet, andernfalls hat die AVI keine Regel oder kein Zieldatum, und ihr Status ist **Kein Ziel** .

Wenn Regeln gelöscht werden, wird **Korrekturziel** Datum und zugehörige Felder in geschlossenen Avis werden beibehalten. Die **Korrekturziel** Datum und zugehörige Felder in nicht geschlossenen Avis werden gelöscht, und alle abhängigen Regeln werden erneut angewendet.

Korrekturregelszenario

Wenn mehrere Korrekturzielregeln auf dieselbe AVI angewendet werden, wird die restriktivste Regel angewendet.

Beispiel: Wenn ein AVI die Bedingung für zwei Anwendungskorrekturzielregeln erfüllt:

Szenario: AVI zuletzt geöffnet am 01/2018 um 10:00:00.

- Anwendungskorrekturzielregel 1: Zuletzt geöffnet am 03/07/2018; Korrekturziel ist 15 Tage seit dem letzten Öffnen; berechnetes Korrekturzieldatum ist 03/16/2018 10:00:00.
- Anwendungskorrekturzielregel 2: Zuletzt geöffnet am 03/10/2018; Korrekturziel ist 10 Tage seit dem letzten Öffnen; berechnetes Korrekturzieldatum ist 03/11/2018 10:00:00.

In diesem Szenario gilt die Anwendungskorrekturzielregel 2 für AVI, da sie das restriktivere Datum hat. 10 Tage seit der ersten Identifizierung der AVI im Vergleich zu 15 Tagen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Anwendungskorrekturziele werden aus berechnet **Zuletzt Geöffnet** Datum plus Anzahl der Tage (gemessen in 24-Stunden-Schritten). Sie können dieses Feld dem AVI-Formular aus dem Formularlayout-Slushbucket hinzufügen. Dies ist das Datum, an dem die AVI zuletzt in Ihrer Instanz geöffnet wurde.

Ab V17.1 werden Korrekturziele aus berechnet **Ziel von (Datum)** . Der Standardwert bleibt erhalten **Datum der letzten Öffnung** .

Hinweis:
Sobald die Anwendungskorrekturzielregel definiert ist, werden die Korrekturzieldaten von berechnet `Evaluate remediation targets` Geplante Aufgabe oder **Änderungen Anwenden** Schaltfläche in der Listenansicht „Korrekturzielregeln“.

Über die geplante Aufgabe „Korrekturziele auswerten“

`Evaluate remediation targets` Wird einmal täglich um 16:00 Uhr ausgeführt.

`Evaluate remediation targets` Iteriert alle aktiven Schwachstellenregeln, beginnend mit diesen Regeln mit dem frühesten Korrekturzieldatum. Es werden alle Avis untersucht, die:

- Befinden sich nicht in **Geschlossen** , **Zurückgestellt** , Oder **Gelöst** status.
- Hat kein Korrekturzieldatum.
- Haben ein Korrekturzieldatum, das nach dem Datum in der Anwendungskorrekturzielregel liegt.

`Evaluate remediation targets` Fügt ein Korrekturzieldatum hinzu, wenn eines nicht vorhanden ist oder wenn diese Regel ein früheres Datum als das im Datensatz enthält, aktualisiert sie das vorhandene Zieldatum. Schließlich wird aktualisiert **Korrekturzieldatum** Und **Korrekturstatus** Felder im AVI-Formular. Für inaktive Regeln **Bewerten Sie Korrekturziele** Löscht die Korrekturfelder im AVI.

Korrekturzielregeln werden erneut angewendet

Wenn Sie eine Korrekturzielregel ändern, verwenden Sie **Änderungen Anwenden** Schaltfläche auf der Listenseite „Korrekturzielregeln“, um alle geänderten Regeln für alle aktiven offenen Avis mit Ausnahme der in erneut auszuführen **Geschlossen** , **Zurückgestellt** Oder **Gelöst** status.

Hinweis:

Wenn die geplante Aufgabe `Evaluate remediation targets`Wird ausgeführt, können Sie keinen Prozess zum erneuten Anwenden initiieren. Wenn jedoch bereits ein Prozess zur erneuten Anwendung ausgeführt wird und die geplante Aufgabe ausgelöst wird, werden sie parallel ausgeführt.

Prozesse in erneut anwenden Vulnerability Response Und Application Vulnerability Response Sind unabhängig und können parallel ausgeführt werden.

Erstellen oder bearbeiten Sie Zielregeln für Anwendungskorrekturen

Beschleunigen Sie die Behebung von Schwachstellen mit hohem Risiko rechtzeitig, indem Sie eine Korrekturzielregel auf Ebene von anwendungsangreifbaren Elementen (Application Angreifbare Elemente, AVI) einrichten.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Das Basissystem wird mit drei Korrekturzielregeln geliefert.

- Regel Für Kritische Risikobewertung
- Regel Für Weniger Kritische Risikobewertung
- Regel für mittlere bis hohe Risikobewertung

Diese Regeln sind standardmäßig inaktiv. Wenn Sie eine bearbeiten möchten, anstatt eine neue zu erstellen, überprüfen Sie die **Aktiv** Feld vor dem Speichern.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Administration** > **Korrekturzielregeln**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Name der Regel.
Ziel (Tage)	Geben Sie die Anzahl der Tage an, innerhalb derer Avis seit dem letzten Öffnen korrigiert werden soll.
V17.1: Ziel von (Datum)	Datum, ab dem die Ziel-SLAs berechnet werden. Sie können nur die Felder für Datum oder Datum und Uhrzeit angeben. Der Standardwert ist das Datum der letzten Öffnung. Informationen zum Anpassen der Werte für dieses Feld finden Sie unter KB1642413 .
Aktiv	Standardmäßig ist **Aktiv** Das Kontrollkästchen ist aktiviert, was bedeutet, dass die Korrekturzielregel aktiv ist. Wenn dieses Kontrollkästchen deaktiviert ist, gilt diese Regel nicht für neue Avis, die im System erstellt wurden.
Benachrichtigen (Tage vor dem Fälligkeitsdatum)	Anzahl der Tage vor der angestrebten Korrekturzeit, bis eine Erinnerung festgelegt werden soll. Das mit diesem Wert berechnete Benachrichtigungsdatum wird verwendet, um den Korrekturstatus und die Farbcodierung anzuzeigen. Wenn das Datum vor dem Benachrichtigungsdatum liegt, lautet der Korrekturstatus „in Flug“. Wenn das Benachrichtigungsdatum überschritten und vor dem Korrekturzieldatum liegt, wird der Status als näheres Ziel angezeigt. **Hinweis:** Wenn dieses Feld auf 0 festgelegt ist, wird nur ein festgelegt **Ziel Verfehlt** Benachrichtigung ist festgelegt.
Regel gilt für	Wählen Sie mit dem Bedingungsfilter die Kriterien für die Anwendung der Regel auf Avis aus. Um Auswirkungen auf die Leistung zu vermeiden, testen Sie Ihre Bedingungen im gesamten Produktionsbereich. Mit Tests können Sie bestimmen, wie lange der ist **Bewerten Sie Korrekturziele** Die Ausführung des Auftrags erfordert die Bedingungen und die Größe Ihres Configuration Management Database (CMDB).
Aktualisierungsverlauf	
Aktivitäten	Für die anfängliche Erstellung einer Regel nicht verwendet. Anschließend werden Systemarbeitsnotizen hier protokolliert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.
   Diese Regel tritt bei der nächsten Ausführung der geplanten Aufgabe in Kraft. `Evaluate remediation targets`. Dasselbe gilt, wenn eine vorhandene Regel aktualisiert wird oder wenn verwendet wird **Änderungen Anwenden** Schaltfläche in der Listenansicht „Korrekturzielregeln“. Dasselbe gilt, wenn eine vorhandene Regel aktualisiert wird. Für weitere Informationen zur geplanten Aufgabe und **Änderungen Anwenden** Siehe , Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response.

Zeigen Sie den Korrekturzielstatus eines angreifbaren Anwendungselements an

Wenn ein angreifbares Anwendungselement (AVI) sein Korrekturzieldatum fast erreicht (oder überschritten) hat, wie durch eine Korrekturzielregel definiert, wird der AVI-Datensatz mit einem Status aktualisiert. Diese Informationen können Ihnen helfen, bevorstehende Korrekturaktivitäten proaktiv zu überwachen.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager-Gruppe

Warum und wann dieser Vorgang ausgeführt wird
Die **Bewerten Sie Korrekturziele** Die geplante Aufgabe wird einmal pro Tag ausgeführt, um das aktuelle Datum mit dem Korrekturdatum für angreifbare Elemente zu vergleichen, das in der zugehörigen Korrekturzielregel angegeben ist. Wenn das aktuelle Datum innerhalb der Anzahl von Tagen liegt, bevor die Korrektur überfällig ist, wird dem Datensatz des angreifbaren Elements ein Korrekturstatus hinzugefügt.

Prozedur

Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Elemente**an.
Wenn das Korrekturdatum für das AVI innerhalb des Bereichs der in der Korrekturzielregel festgelegten Bedingungen liegt, überprüfen Sie die Spalten „Korrekturzielstatus“, die in der Listenansicht „angreifbare Elemente“ sichtbar sind. Wenn das Korrekturzieldatum für ein AVI verstrichen ist, wird im AVI-Formular eine Anmerkung angezeigt.

Hinweis:
Um die Anzahl der Avis anzuzeigen, die sind **Ziel Wird Erreicht** , **In Betrieb** Und **Vergangenes Ziel** , Siehe Dashboard „Anwendungsschwachstellenmanagement“ [PA] .

Zugehörige Informationen

Erstellen oder bearbeiten Sie Zielregeln für Anwendungskorrekturen

Schließen Sie eine Korrekturaufgabe

Wenn Sie feststellen, dass das Problem, das einer Anwendungskorrekturaufgabe zugeordnet ist, sofort ohne weitere Analyse geschlossen werden kann, können Sie verwenden **Schließen** Funktion. Ab v23.0 von Vulnerability Response, **Schließen** Schaltfläche wurde für eine Anwendungskorrekturaufgabe entfernt.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
In Vulnerability Response Arbeitsbereiche, eine Korrekturaufgabe durchläuft dieselben status wie eine Korrekturaufgabe, die zuvor in früheren Versionen von durchgeführt wurde Vulnerability Response. Wenn alle angreifbaren Elemente (Vits) in einer Korrekturaufgabe geschlossen sind, wechselt die Korrekturaufgabe in den Status Inaktiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Sie können Change-Anforderungen und Korrekturaufgaben manuell durch die status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist. Wenn das System jedoch registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder es aus einer Korrekturaufgabe entfernen, kann die Statussynchronisierung Ihren manuellen Eingriff möglicherweise überschreiben. Change-anforderungsstatus verschieben Korrekturaufgaben jedoch nicht automatisch aus dem Geschlossen Oder Zurückgestellt status.

Prozedur

1. Öffnen Sie den Datensatz, für den Sie eine Überprüfung anfordern möchten.
2. Wählen Sie aus **Schließen** Schaltfläche.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Status	Wählen Sie den Status als Geschlossen aus.
Grund	Geben Sie den Grund für das Schließen des Problems ein.
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

4. Wählen Sie **Absenden**.
   Die Korrekturaufgabe ist markiert **Geschlossen** .

Change-Management für Application Vulnerability Response

Erstellen Sie Change-Anforderungen aus Korrekturaufgaben in der Anwendung „Application Vulnerability Response“, um Ihre Untersuchung auf Anwendungsschwachstellen (AVIT) zu beschleunigen, die manuelles Eingreifen erfordern.

Erstellen Sie Change-Anforderungen mit vorab ausgefüllten Informationen für gescannte Anwendungen, die als Konfigurationselemente (Configuration Items, CI) klassifiziert sind, um Ihre Untersuchung auf Anwendungsschwachstellen (AVITs) zu beschleunigen, die manuelle Eingriffe erfordern.

- Der Change-Anforderungs-Workflow in Application Vulnerability ResponseÄhnelt dem in unterstützten Workflow Vulnerability Response.
- Weitere Informationen zu finden Vulnerability Response Change-Anforderungs-Workflow, siehe Change-Management für Vulnerability Response.

Erstellen Sie eine Change-Anforderung für die Anwendungskorrekturaufgabe

Als App-sec-Manager oder Security Champion können Sie Change-Anforderungen aus Korrekturaufgaben in der Anwendung Application Vulnerability Response erstellen.

Vorbereitungen
Erforderliche Rollen:

Aus Vulnerability Manager Manager Workspace: sn_vul.App_sec_Manager.

Aus ITRem-Besitzerarbeitsbereich: sn_vul.App_sec_Champion oder sn_vul.App_Developer und itil-Rolle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Um eine Change-Anforderung aus der klassischen Umgebung zu erstellen, führen Sie die unten aufgeführten Schritte aus.

Sie können Change-Anforderungen direkt aus einer Korrekturaufgabe erstellen, genehmigen, implementieren, überprüfen und schließen. Sie können drei Arten von Change-Anforderungen mit vorab ausgefüllten Informationen aus einer Korrekturaufgabe erstellen:

- Standard. Ein vorautorisierter Change, der ein geringes Risiko aufweist, relativ häufig ist und einem bestimmten Verfahren oder einer bestimmten Arbeitsanweisung folgt.
- Normal. Normale Change-Anforderungen folgen einem verbindlichen Prozess, der zwei Genehmigungsebenen erfordert, bevor sie implementiert, überprüft und geschlossen werden.
- Notfall. Ein Change zur Lösung eines schwerwiegenden Incident.

Hinweis:
Change-Anforderungen werden für Application Vulnerability Response nur unterstützt, wenn die erkannte Anwendung einem Konfigurationselement (Configuration Item, CI) zugeordnet ist. Dies tritt nur auf, wenn Sie „Produktmodell“ in der Systemeigenschaft „Produktmodell verwenden“ [sn_vul.use_product_model] auf „falsch“ festlegen.

Prozedur

1. Um eine vollständige Change-Anforderung aus einem vorhandenen Korrekturaufgabendatensatz zu erstellen, navigieren Sie zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**an.
   Die Liste der Korrekturaufgaben, die Ihrer Zuweisungsgruppe zugewiesen sind, wird angezeigt.
2. **Wahlweise:** Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturübersicht** Um das Dashboard „Korrekturübersicht“ anzuzeigen und eine Ihnen oder Ihrer Zuweisungsgruppe zugewiesene ANFECHTBARE Person zu suchen.
3. Alternativ können Sie in der Spalte Nummer auf eine Korrekturaufgabe klicken, um den Datensatz zu öffnen und die Details anzuzeigen.
   Der Datensatz wird angezeigt.
4. Wenn der APP-VUL-Datensatz angezeigt wird, für den Sie die Change-Anforderung erstellen möchten, klicken Sie oben rechts im Datensatz auf **Erstellen Sie Einen Change** .
   Das Formular Change-Anforderung erstellen wird angezeigt.
5. Füllen Sie die Felder aus.

   a. Wählen Sie in der Auswahlliste des Felds „gilt für“ eine aus, um fortzufahren.

Option	Beschreibung
Alle aktiven angreifbaren Anwendungselemente in dieser Gruppe	Wenn diese Option ausgewählt ist, werden alle aktiven angreifbaren Anwendungselemente aus dieser Korrekturaufgabe mit einem anderen Status als „Geschlossen“ automatisch der Change-Anforderung hinzugefügt, nachdem Sie auf geklickt haben **Erstellen Sie Einen Change** .
Alle angreifbaren Anwendungselemente in dieser Gruppe, die einer Reihe von Bedingungen entsprechen	Wenn diese Option ausgewählt ist, wird der Bedingungsgenerator wie in der zweiten Abbildung unten angezeigt. Geben Sie Filterkriterien ein, um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	die angreifbaren Elemente zu identifizieren, die Sie für die neue Change-Anforderung benötigen. Ein Beispiel für einen Filter kann nur angreifbare Elemente enthalten, die bestimmten Suchkriterien entsprechen: **Status Ist Öffnen** Und **Risikopunktzahl Größer als 75** . Nachdem Sie Ihre Bedingungen eingegeben haben, wird eine Nachricht mit der Anzahl der AVITs angezeigt, die Ihren Kriterien entsprechen (10). Ein Link (**Vorschau auf übereinstimmende Elemente anzeigen**), um eine Vorschau der übereinstimmenden Elemente anzuzeigen. Wenn keine Elemente Ihren Filterbedingungen entsprechen, wird unter dem Bedingungsgenerator eine Meldung angezeigt, die Sie anweist, Ihren Filter anzupassen. Nachdem Sie auf geklickt haben **Erstellen Sie Einen Change** , Alle angreifbaren Anwendungselemente, die diesem Bedingungsfilter entsprechen, werden in eine neue Korrekturaufgabe verschoben. Diese Change-Anforderung ist der neuen Korrekturaufgabe zugeordnet.

Erstellen Sie ein Change-Anforderungsformular für angreifbare Anwendungselemente in einer Aufgabe, die einer Reihe von Bedingungen entsprechen

b. **Wahlweise:** Wenn im Formular angezeigt, klicken Sie auf **Vorschau auf übereinstimmende Elemente anzeigen** Link für eine Liste der AVITs, die Ihren Filterkriterien entsprechen.
Die Vorschau der Korrekturaufgabenliste wird angezeigt. Sie können Elemente in dieser Vorschauliste auswählen und UI-Aktionen für sie ausführen. Diese Aktionen werden jedoch auch für die APP-VUL ausgeführt. Wenn Sie beispielsweise ein VI aus der Vorschauliste löschen, wird dieses AVIT auch aus der APP-VUL gelöscht.

c. Nachdem Sie Ihre Vorschau abgeschlossen haben, schließen Sie das Browserfenster, um das Change-Anforderungsformular zurückzugeben.

d. Wählen Sie für das Kontrollkästchen CIs zu CR hinzufügen eine aus, um fortzufahren.

Option	Beschreibung
Kontrollkästchen „CIs zu CR hinzufügen“ aktiviert	Standard ist ausgewählt. Wenn das Kontrollkästchen aktiviert ist, werden alle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Konfigurationselemente (Configuration Items, CI), die zu aktiven angreifbaren Elementen in dieser Korrekturaufgabe gehören, dieser Change-Anforderung hinzugefügt. Die APP-VUL wird automatisch zu verschoben Warten Auf Implementierung status.
Kontrollkästchen „CIs zu CR hinzufügen“ deaktiviert	Deaktivieren Sie das Kontrollkästchen, wenn die CIs aus den aktiven angreifbaren Anwendungselementen aus dieser Korrekturaufgabe nicht der neuen Change-Anforderung hinzugefügt werden sollen. Wenn diese Option deaktiviert ist, wird der Status der Change-Anforderung nicht mit der APP-VUL synchronisiert, und die APP-VUL bleibt im aktuellen Status.

e. Wählen Sie in der Auswahlliste für das Feld Change-Typ einen aus, um fortzufahren.

Änderungstyp	Beschreibung
Notfall	Ein Change zur Lösung eines schwerwiegenden Incident.
Normal	Ein Change-Typ, der verwendet wird, um Changes an einem Service zu implementieren, bei denen es sich nicht um einen Standard- oder Notfall-Change handelt.
Standard	Eine vorautorisierte Change-Anforderung mit geringem Risiko, die häufig implementiert wird. Genehmigte Standard-Change-Anforderungen können in einem Vorlagenkatalog vordefiniert werden, um den Zugriff auf und die Anfrage eines Standard-Changes effizienter zu gestalten. Wenn diese Option ausgewählt ist, werden zwei Felder angezeigt. Wählen Sie in jeder Auswahlliste eines aus, um diese Felder auszufüllen: ▪ Change-Kategorie: Wählen Sie eine Kategorie für den Change aus Ihrem vorhandenen Katalog aus, z. B. Hardware , Server-Standard-Changes , Software . In diesem Beispiel Standard-Changes Werden Gepatcht Ist ausgewählt. ▪ Change-Vorlage: Wählen Sie eine verfügbare Vorlage für Change-Anforderungen mit vordefinierten Unterstützungsaufgaben aus Ihrem Katalog aus. In diesem Beispiel ist Monatlicher Microsoft-Patching-Zyklus Vorlage ist ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Änderungstyp	Beschreibung
	Weitere Informationen zu ITSM Change-Anforderungskategorien, Vorlagen und Change-Typen finden Sie unter Change-Typen .

Die Funktion liest automatisch die Arten von Change-Anforderungen, die Sie in Ihrem Katalog in ITSM Change-Management eingerichtet haben. Wenn Sie beispielsweise den Namen für Ihre Standard-Change-Anforderungen in ITSM von ändern Standard Bis Vorab genehmigt , Ihr neuer Name wird automatisch in der Auswahlliste Change-Typ auf Change-Anforderung erstellen aus angezeigt, wie in der folgenden Abbildung gezeigt.

Die Felder im Abschnitt „Change-Anforderungsvorschau“ des Formulars sind vorab mit Informationen aus der APP-VUL ausgefüllt. Bei Bedarf können diese Feldwerte bearbeitet werden. Überprüfen Sie beispielsweise die Werte in den Feldern in der folgenden Abbildung:

Geplantes Enddatum

Dieses Datum (10. 2019) Ist derselbe Wert, der im Feld Korrekturzieldatum der APP-VUL angezeigt wird. Dieser Wert wird vom frühesten Korrekturzieldatum aus den angreifbaren Anwendungselementen abgeleitet, die zur APP-VUL gehören. Wenn Sie eine Change-Anforderung für ein kritisches Problem erstellen, das ein früheres Korrekturdatum erfordert, können Sie diesen Wert und den Wert im Feld Priorität bearbeiten.

Begründung

Dieses Feld zeigt die Anzahl der CIs an, die dem CHG hinzugefügt werden. Wenn Sie zusätzliche Informationen hinzufügen möchten, möchten Sie diesen Text möglicherweise bearbeiten. Beispielsweise möchten Sie in diesem Feld eine Notiz zu dem Filter hinzufügen, den Sie zum Erstellen der neuen APP-VUL verwendet haben, z. B. Risikopunktzahl größer als 75 . Dieser Text kann Ihnen helfen, Ihre neue Change-Anforderung und Korrekturaufgabe zu finden.

Implementierungsplan

In diesem Feld wird die bevorzugte Lösung für die Schwachstelle angezeigt.

Zuweisungsgruppe und Zugewiesen an

Bearbeiten Sie diese Felder, um die Zuweisungsgruppe zu ändern oder diese Change-Anforderung einem Anwender in einer Ihrer Zuweisungsgruppen neu zuzuweisen.

6. Fahren Sie mit der Vorschau der Felder fort, und bearbeiten Sie sie nach Bedarf.
7. Um Ihre Änderungen zu speichern und auf dieser Seite zu bleiben, klicken Sie im grauen Banner oben im Formular mit der rechten Maustaste, und wählen Sie aus **Einfügen und beibehalten** .
8. Nachdem Sie Ihre Änderungen abgeschlossen haben, wählen Sie eine aus, um fortzufahren.

Hinweis:

Für eine Korrekturaufgabe in Öffnen status mit den Feldern Zuweisungsgruppe und Zugewiesen an nicht zugewiesen (leer) wird der aktuell angemeldete Anwender automatisch der Aufgabe zugewiesen, nachdem Sie auf geklickt haben **Erstellen Sie Einen Change** . Darüber hinaus muss das Kontrollkästchen CIs zu CR hinzufügen aktiviert sein. Oben auf der ABLEHNUNG wird eine blaue Bestätigungsnachricht angezeigt, die diese Zuweisung anzeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Überwachen Sie die Change-Anforderung und die Change-Aufgaben, um sicherzustellen, dass sie abgeschlossen sind und die Change-Anforderung implementiert ist. Nachdem dieses CHG implementiert und in verschoben wurde Überprüfen status: Wenn die Statussynchronisierung aktiviert ist, wird die APP-VUL automatisch zu verschoben Gelöst .

Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu

Vermeiden Sie als Appsec-Manager oder Security Champion die Erstellung doppelter Change-Anforderungen (CHG), wenn Sie an der Lösung Ihrer Korrekturaufgaben arbeiten, indem Sie einer Change-Anforderung, die bereits in Ihrer Instanz verfügbar ist, eine Korrekturaufgabe (APP-VUL) zuordnen.

Vorbereitungen

Erforderliche Rollen:

Aus Vulnerability Manager Manager Workspace: sn_vul.App_sec_Manager.

Aus ITRem-Besitzerarbeitsbereich: sn_vul.App_sec_Champion oder sn_vul.App_Developer und itil-Rolle.

Warum und wann dieser Vorgang ausgeführt wird

Als Korrekturbesitzer können Sie Korrekturaufgaben, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen sind, vorhandenen Change-Anforderungen direkt aus den Korrekturaufgaben-Datensätzen zuordnen. Die folgende Abbildung zeigt den grundlegenden Flow zum Zuordnen einer Change-Anforderung zu einer vorhandenen APP-VUL (VG).

Hinweis:
Sie können eine vorhandene Change-Anforderung einer APP-VUL in einem beliebigen Status zuordnen (Offen, wird untersucht, wartet auf Implementierung, Geschlossen und zurückgestellt). Wenn Sie eine Change-Anforderung einer vorhandenen ANGREIFBAREN Person zuordnen, werden der Change-Anforderung nur die aktiven VIS hinzugefügt.

Um zu vermeiden, dass doppelte Change-Anforderungen erstellt werden, sollten Sie zunächst alle vorhandenen Change-Anforderungen anzeigen, die bereits einer APP-VUL zugeordnet sind. Informationen zum einfachen Nachverfolgen der Anzahl der Change-Anforderungen, die sich auf eine bestimmte APP beziehen, finden Sie in der Spalte „CR-Anzahl“ in der Liste „Korrekturaufgaben“. Wenn nicht angezeigt, klicken Sie oben rechts auf das Einstellungssymbol (). Verschieben Sie die Spalte „CR-Anzahl“ von „verfügbar“ in „ausgewählt“, und klicken Sie auf **OK** .

Um die neue Spalte automatisch auszufüllen, führen Sie für Kunden mit vorhandenen Daten in dieser Tabelle die geplante Aufgabe aus: Füllen Sie die neue Spalte „CR-Anzahl“ aus .

Prozedur

1. Um eine Korrekturaufgabe einer vorhandenen Change-Anforderung zuzuordnen, navigieren Sie zu **Alle** > **Application Vulnerability Response** > **Korrekturaufgaben**an.
2. Suchen Sie die Korrekturaufgabe, mit der Sie arbeiten.
3. **Wahlweise:** Navigieren zu **Alle** > **Application Vulnerability Response** > **Korrekturübersicht**
   Um das Dashboard „Korrekturübersicht“ anzuzeigen und eine APP-VUL zu suchen, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen ist.
4. Klicken Sie in der Spalte Nummer auf einen APP-VUL-Datensatz, um ihn zu öffnen.
   Der APP-VUL-Datensatz wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wenn der offene Datensatz angezeigt wird, scrollen Sie, falls er nicht bereits angezeigt wurde, zur zugehörigen Liste Change-Anforderungen, und wählen Sie ihn aus.
   Alle Change-Anforderungen, die der APP-VUL zugeordnet sind, werden zusammen mit angezeigt **Hinzufügen** Schaltfläche. In der folgenden Abbildung sind dieser APP-VUL bereits keine Change-Anforderungen zugeordnet.
6. Um die APP-VUL einem vorhandenen CHG zuzuordnen, klicken Sie auf **Hinzufügen** .
   Das Formular vorhandene Change-Anforderung zu Korrekturaufgabe hinzufügen wird angezeigt.
7. Klicken Sie im Formular auf das Suchsymbol.
   Eine Listenansicht vorhandener Change-Anforderungen wird in einem neuen Fenster angezeigt, wie in der folgenden Abbildung dargestellt.
8. Wählen Sie ein Element aus der angezeigten Liste aus, oder klicken Sie alternativ auf den Filter (), und geben Sie Bedingungen ein, um Ihre Suchergebnisse einzuschränken.
9. Wählen Sie für das Kontrollkästchen CIs zu CR hinzufügen eine aus, um fortzufahren.

Hinweis:
Dieses Kontrollkästchen wird nur für vorhandene Change-Anforderungen in angezeigt Neu status.

Option	Beschreibung
Kontrollkästchen „CIs zu CR hinzufügen“ aktiviert	Standard ist ausgewählt. Wenn das Kontrollkästchen aktiviert ist, werden alle Konfigurationselemente (Configuration Items, CI), die zu aktiven angreifbaren Elementen in dieser Korrekturaufgabe gehören, dieser Change-Anforderung hinzugefügt. Wenn diese Option ausgewählt ist, wird der Status der Change-Anforderung mit der APP-VUL synchronisiert. Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.
Kontrollkästchen „CIs zu CR hinzufügen“ deaktiviert	Deaktivieren Sie das Kontrollkästchen, wenn die CIs aus den aktiven angreifbaren Elementen aus dieser Korrekturaufgabe nicht der neuen Change-Anforderung hinzugefügt werden sollen. Wenn diese Option deaktiviert ist, wird der Status der Change-Anforderung nicht mit der APP-VUL synchronisiert, und die APP-VUL bleibt im aktuellen Status.

10. Klicken Sie mit der Nummer der Change-Anforderung, die Sie im Feld Suche nach Change-Anforderung anzeigen möchten, auf **Übermitteln** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die APP-VUL wird angezeigt. Oben im Datensatz wird die blaue Bestätigungsnachricht angezeigt, die angibt, dass die von Ihnen ausgewählte Change-Anforderung erfolgreich mit der APP-VUL verknüpft ist.

Hinweis:
Für eine APP-VUL in Öffnen status mit den Feldern Zuweisungsgruppe und Zugewiesen an nicht zugewiesen (leer) wird der aktuell angemeldete Anwender automatisch der APP-VUL zugewiesen, nachdem Sie auf geklickt haben **Hinzufügen** . Darüber hinaus muss das Kontrollkästchen CIs zu CR hinzufügen aktiviert sein. Oben in der APP-VUL wird eine blaue Bestätigungsnachricht angezeigt, die angibt, dass der aktuelle Anwender zugewiesen ist.

Nächste Maßnahme
Überprüfen Sie den APP-VUL-Datensatz. Klicken Sie in der Spalte „Change-Anforderung“ in der zugehörigen Liste „Change-Anforderungen“ auf den Link für das neue CHG, um den CR-Datensatz anzuzeigen. Im offenen CHG-Datensatz können Sie den Status der Change-Anforderung überwachen. Die betroffenen Konfigurationselemente (CI) und die Korrekturaufgaben werden in den zugehörigen Listen Betroffene CIs und Korrekturaufgaben angezeigt.

Penetrationstests

Penetrationstests in Application Vulnerability Response Ermöglicht Anwendungsbesitzern, die Sicherheitslage ihrer Anwendung zu bewerten. Es handelt sich um das manuelle Testen einer Anwendung durch das ethische Hacking-Team.

Erforderliche Rollen

Penetrationstests erfordern die folgenden Rollen:

App-Sec-Manager : Enthält Sicherheitsmanager und Anwendungsbesitzer, die die Bewertungsanforderungen für Penetrationstests verwalten. Es enthält die folgenden granularen Rollen:

- sn_vul.App_Manage_Pen_Test_Request
- sn_vul.App_read_all
- cmdb_read

Ethischer Hacker : Enthält Mitglieder des Teams für ethische Hacking, die Penetrationstests von Anwendungen durchführen. Sie enthält die folgenden granularen Rollen:

- sn_vul.App_Update_assignment_Group
- sn_vul.App_Update_assigned_to
- sn_vul.App_Manage_Manual_avits
- sn_vul.App_Manage_Pen_Test_Request_config
- ITIL
- sn_vul.App_read_all
- sn_vul.App_Manage_Pen_Test_Request
- sn_vul.App_Update_State

Weitere Informationen zu diesen Rollen finden Sie unter Application Vulnerability Response Anwendergruppen und Rollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab v19.0 von Vulnerability Response, Wenn Sie verwenden Veracode Vulnerability Integration, Die Penetrationstest-Tests in Veracode Vulnerability Integration Sind manuelle Ergebnisse von Veracode. Sie sind nicht mit Penetrationstestbewertungsanforderungen verknüpft, die Sie in konfigurieren Application Vulnerability Response. Für weitere Informationen zu Penetrationstestbewertungen von Veracode, Siehe Veracode Vulnerability Integration.

Lebenszyklus von Penetrationstests

Als Anwendungsbesitzer können Sie das Ethical Hacking-Team um eine Penetrationstestbewertung Ihrer Anwendung anfordern. Das ethische Hacking-Team reagiert auf diese Anforderung und erstellt Penetrationstestergebnisse. Diese Ergebnisse sind manuell erstellte angreifbare Anwendungselemente (Avis).

Der Penetrationstests-Workflow deckt den Lebenszyklus von Penetrationstests ab, von der Übermittlung der Testanforderung bis zur Lösung der Ergebnisse des Teams für ethische Hacking.

Penetrationstestbewertung wird angefordert

Ab v19.0 können Sie unter neue Anforderungen erstellen oder vorhandene Anforderungen kopieren **Alle** > **Anforderungen für Penetrationstestbewertung** > **Alle**an.

Vor v19.0 können Sie als Anwendungsbesitzer mithilfe des ITSM-Servicekatalogs eine Penetrationstestbewertung für Ihre Anwendung anfordern.

Überprüfung der Penetrationstestbewertungsanforderung

Das Ethical Hacking-Team überprüft und bewertet die Anwendung und den Umfang der Penetrationstestbewertungsanforderung und fügt sie dem vorhandenen Backlog hinzu.

Umgebung wird vorbereitet

Das ethische Hacking-Team sendet dann eine Anforderung an den Anwendungsbesitzer, eine Umgebung bereitzustellen, in der er mit dem Testen beginnen kann. Sobald die Umgebung bereit ist, informiert der Anwendungsbesitzer das ethische Hacking-Team.

Weitere Informationen zum Konfigurieren von Testanforderungen finden Sie unter Penetrationstests konfigurieren.

Tests und Berichterstellung der Penetrationstestergebnisse

Das Ethical Hacking-Team testet die Anwendung und meldet die Ergebnisse dem Anwendungsbesitzer. Das Ethical Hacking-Team definiert auch die Servicelevel-Vereinbarungen (Service Level Agreements, SLAs) für Penetrationstestergebnisse anhand des Korrekturzieldatums. Diese Ergebnisse sind die manuell erstellten Avis. Der Anwendungsbesitzer überprüft wiederum die vom ethischen Hacking-Team erstellten Avis. Sie planen die Korrekturen und weisen sie dem Anwendungsteam zu.

Hinweis:
Korrekturzielregeln gelten nicht für die Penetrationstestergebnisse.

Das Ethical Hacking-Team kann eine Bibliothek von Anwendungsschwachstelleneinträgen (Aves) erstellen und sie beim Melden der Avis wiederverwenden. Sie können auch den Status der Penetrationstestergebnisse nachverfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

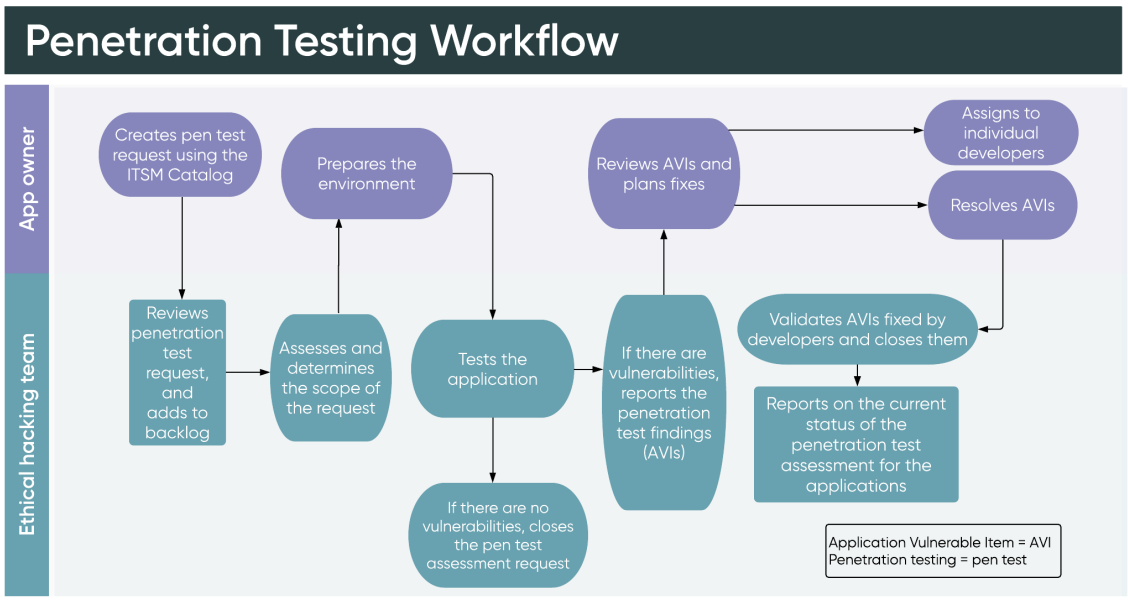
Korrektur und Validierung der Penetrationstestergebnisse

Nachdem die Ergebnisse des Penetrationstests vom Anwendungsteam behoben und gelöst wurden, werden die Korrekturen manuell validiert und vom Team für ethische Hacking geschlossen.

Application Vulnerability Management-Berichte

Verwenden Sie die in verfügbaren Berichte Application Vulnerability Management PA-Dashboard zum Nachverfolgen der Penetrationstestergebnisse.

Lebenszyklus von Penetrationstests



Penetrationstestbewertungsanforderung aus vorhandenen Anforderungen erstellen (v19.0)

Ab v19.0 erstellen Sie Penetrationstestbewertungsanforderungen direkt aus der Liste der vorhandenen Anforderungen. Sie können auch vorhandene Anforderungen im Status Geschlossen in dieser Liste kopieren, um Anforderungen zu erstellen.

Vorbereitungen

Erforderliche Rolle: App-Sec-Manager

Warum und wann dieser Vorgang ausgeführt wird

Ab v19.0 von Vulnerability Response, Wenn Sie verwenden Veracode Vulnerability Integration, Die Penetrationstest-Tests in Veracode Vulnerability Integration Sind manuelle Ergebnisse von Veracode. Sie sind nicht mit Penetrationstestbewertungsanforderungen verknüpft, die Sie in konfigurieren Application Vulnerability Response. Für weitere Informationen zu Penetrationstestbewertungen von Veracode, Siehe Veracode Vulnerability Integration.

Prozedur

1. Navigieren zu **Alle** > **Anforderungen für Penetrationstestbewertung** > **Alle**an.
2. **Wahlweise:** Alternativ können Sie eine Anforderung erstellen, indem Sie geschlossene Anforderungen replizieren.
   Alle Werte aus der ursprünglichen Anforderung werden im neuen Formular beibehalten. Aktive angreifbare Anwendungselemente (Avis) werden automatisch in die neue Anforderung kopiert. Wählen Sie Aus **Kopieren Und Anforderung Erstellen** Aus Datensätzen im Status „Geschlossen“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie Neu, und füllen Sie die Felder aus.

Formular „Bewertungsanforderung für Penetrationstests“

Feld	Beschreibung
Anzahl	Eindeutiger Bezeichner, der für die Anforderung zur Bewertung des Penetrationstests generiert wurde.
Status	Wählen Sie einen Wert basierend auf dem Status der Anforderung aus.
Angefordert von	Person, die die Bewertung der Anwendung anfordert.
Zuweisungsgruppe	Gruppe ausgewählt, um die Penetrationstestergebnisse zu bearbeiten. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden. Informationen zum Konfigurieren von Gruppen finden Sie unter Penetrationstests konfigurieren.
Anwendung	Wählen Sie mithilfe der Suchoption eine Anwendung aus.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an den Penetrationstestergebnissen arbeitet. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Anwendungstyp	Wählen Sie eine Option aus: ○ Webservice (bekannt als API vor v16.1) ○ Web-Anwendung ○ Thick Client ○ Mobil (wenn Sie auswählen **Mobil** , Die Registerkarte Mobile wird unten im Formular mit zusätzlichen Feldern angezeigt)
Sprint	Zeigt die Sprints mit verfügbarer Bandbreite an, um die Bewertungsanforderung basierend auf dem Feld „ausgewählter Bewertungstyp“ zu erfüllen. Siehe Konfigurieren Sie Sprints für Penetrationstests Und Konfigurieren Sie Bewertungstypen für Penetrationstests Weitere Informationen zum Ändern der Sprint-Kapazität und des Testumfangs.
V19.0: Anwendungsgröße	Wählen Sie die Größe der Anwendung aus, die Sie testen möchten. ○ Klein ○ Mittel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Groß ○ Standard (wählen Sie diese Option aus, wenn Sie sich über die Größe nicht sicher sind) Weitere Informationen Penetrationstests konfigurieren Weitere Informationen zum Ändern der Sprint-Kapazität und des Testumfangs mit Anwendungsgröße und Sprint-Kapazität.
Erstellt	Datum und Uhrzeit der Erstellung der Anforderung.
Bewertungstyp	Wählen Sie den Typ der Bewertung aus: ○ Vollständiger Penetrationstest ○ Fokussierter Test ○ Erneut testen Weitere Informationen zu Testkombinationen und Testumfang finden Sie unter Konfigurieren Sie Bewertungstypen für Penetrationstests.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung der Anforderung.
Demo-Datum	Datum, an dem diese Anwendung demonstriert werden kann.
Produktbereitstellung geplant am	Geplantes Datum für die Bereitstellung dieser Anwendung in der Produktion.
Anwendungsversion/-release für die Bereitstellung geplant	Version der Anwendung, die für die Produktionsbereitstellung geplant ist.
V19.0: Anwendung im Besitz eines Drittanbieters oder einer Joint-Venture-Registerkarte Wenn Sie für dieses Feld Ja auswählen, wird die Registerkarte Lieferanten-/Joint Venture-Informationen angezeigt. Füllen Sie die zusätzlichen Felder aus.	
Ist eine Klausel vorhanden, die es uns ermöglicht, Pen-Tests durchzuführen?	Der Begriff „Klausel“ kann sich auf Standards für Tests beziehen, die alle Vereinbarungen enthalten, die zwischen zwei oder mehr Parteien bestehen, die Sie hinzufügen möchten. Wenn Sie auswählen **Ja** , Fügen Sie die Klausel hinzu.
Die Klausel, die die Berechtigung zum Durchführen von Pen-Tests angibt	
Vollständiger offizieller Name und Adresse des Lieferanten	
Angriffserkennungssystem	
Technischer Kontakt des Lieferanten	
Wurden die protokollierten Informationen von böswilligen Aktivitäten überprüft?	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Wird die Anwendung von einem anderen Drittanbieter gehostet?	
Kontakt des Lieferanten, der den Pen-Test abzeichnet	
Registerkarte „Anwendungsdetails“	
Zweck der Anwendung	Beschreibung der Funktionalität der Anwendung.
Details des Technologiestapels	Komplettieren Sie den Technologiestapel vom Front-End zum Back-End, Datenbanken und andere Schlüsseltechnologien.
Ist Drittpartei-Anwendung?	Bestätigt, ob diese Anwendung im Besitz eines Drittlieferanten ist.
Listet die Arten sensibler Daten auf, auf die über die Anwendung zugegriffen werden kann.	Typen vertraulicher Daten, auf die über die Anwendung zugegriffen werden kann. Zum Beispiel personenbezogene Daten, PHI-Daten und Finanzdaten wie Kreditkartennummern.
Authentifizierungstyp	Gibt an, ob diese Anwendung LDAP-Authentifizierung, eine eigene native Authentifizierung oder andere Authentifizierungsformen verwendet.
Fällt die Anwendung unter ein Compliance-Programm?	Gibt an, ob sich diese Anwendung auf Compliance-Programme wie PCI auswirkt.
Kontakte im Anwendungsteam	Mitglieder des Anwendungsteams, die vom Team für ethische Hacker bei Fragen kontaktiert werden sollen.
Liste der Compliance-Programme	
Zugehörige Schnittstellen oder Anwendungen von Drittparteien	
IP-Adresse	
Ungefähre Anzahl der Anwender in der Produktion?	
Automatisiertes Skript vorhanden?	
Die Produktionsversion dieser App ist extern ausgerichtet?	
v 19.0: Geschäftsauswirkung	
Finanzieller Schaden	Wählen Sie einen aus der Liste aus.
Nichteinhaltung	Wählen Sie einen aus der Liste aus.
Reputationsschaden	Wählen Sie einen aus der Liste aus.
Datenschutzverletzung	Wählen Sie einen aus der Liste aus.
Registerkarte „Testdetails“	
Zu testende URLs	URLs, die in Penetrationstests einbezogen werden müssen.
Auszuschließende URLs	URLs, die von Penetrationstests ausgeschlossen werden müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Wurde diese Anwendung zuvor getestet?	Gibt an, ob diese Anwendung bereits Penetrationstests unterzogen wurde.
Grund für erneuten Test	Grund für die Anforderung einer Neubewertung des Penetrationstests, wenn die Anwendung zuvor getestet wurde.
Wann wurde die Anwendung getestet?	Zeitrahmen, in dem die Anwendung Penetrationstests durchgeführt wurde.
Details des Test-Accounts	Details des Test-Accounts, der vom Ethical Hacking-Team für Penetrationstests verwendet werden kann.
Anwendungsrollen	Rollen, die von der Anwendung für ihre Anwender unterstützt werden.
Meistverwendete Rollen	Am häufigsten verwendete Rollen in der Anwendung.
Registerkarte „zusätzliche Kommentare“	
Arbeitsnotizen	

4. Wählen Sie Aus **Speichern** Um Ihre Bearbeitungen oder zu speichern **Übermitteln** Um die Anforderung zu initiieren.

Penetrationstestbewertungsanforderung erstellen (vor v19.0)

Initiieren Sie eine Penetrationstestbewertungsanforderung für Ihre Webanwendungen oder APIs. Diese Anforderungen werden an das Ethical Hacking-Team übermittelt, das dann diese Anwendungen testen und die Ergebnisse der Penetrationstests manuell melden kann.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager

Warum und wann dieser Vorgang ausgeführt wird
Der Anwendungsbesitzer stellt eine Penetrationstestbewertungsanforderung, um seine Anwendung oder APIs manuell zu scannen. Das Ethical Hacking-Team testet die Anwendung und erstellt manuell Penetrationstestergebnisse. Diese Ergebnisse sind manuell erstellte angreifbare Anwendungselemente (Avis).

Die Standardzuweisungsgruppe für das Penetrationstestergebnis ist die Gruppe, die im Feld „Anwendungsteam“ der zugehörigen Penetrationstestbewertungsanforderung konfiguriert ist. Der Zuweisungstyp des Penetrationstestergebnisses ist manuell. Die Zuweisungsregeln können die Zuweisung dieser Penetrationstestergebnisse nicht überschreiben.

Ab v19.0 können Sie Penetrationstestbewertungsanforderungen direkt aus der Tabelle Penetrationstestbewertungsanforderungen [sn_vul_Pen_Test_assessment_Request_list] erstellen. Weitere Informationen finden Sie unter Penetrationstestbewertungsanforderung aus vorhandenen Anforderungen erstellen (v19.0).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie vor v19.0 Bis **Alle** > **Self-Service** > **Servicekatalog** > **Services** > **Anforderung für Penetrationstestbewertung**an.
2. **Wahlweise:** Alternativ können Sie eine Anforderung erstellen, indem Sie geschlossene Anforderungen replizieren.
   Alle Werte aus der ursprünglichen Anforderung werden beibehalten. Aktive angreifbare Anwendungselemente (Avis) werden automatisch in die neue Anforderung kopiert.
3. Füllen Sie im Formular die Felder aus.

Formular „Bewertungsanforderung für Penetrationstests“

Feld	Beschreibung
Anzahl	Eindeutiger Bezeichner, der für die Anforderung zur Bewertung des Penetrationstests generiert wurde.
Angefordert von	Person, die die Bewertung der Anwendung anfordert.
Übergeordnete Bewertungsanforderung	Ursprüngliche Anforderung zur Bewertung von Penetrationstests, die zum Erstellen der untergeordneten Anforderung verwendet wurde. Sie wird mithilfe einer geschlossenen Bewertungsanforderung erstellt. Nur im Formular „Anforderung für untergeordnete Bewertungen“ sichtbar.
Anwendung	Wählen Sie mithilfe der Suchoption eine Anwendung aus.
Anwendungstyp	Wählen Sie eine Option aus: ○ Webservice (bekannt als API vor v16.1) ○ Web-Anwendung ○ Thick Client ○ Mobil (wenn Sie mobil auswählen, wird die Registerkarte Mobile am unteren Rand des Formulars mit zusätzlichen Feldern angezeigt)
V19.0: Anwendungsgröße	Wählen Sie die Größe der Anwendung aus, die Sie testen möchten. ○ Klein ○ Mittel ○ Groß ○ Standard (wählen Sie diese Option aus, wenn Sie sich über die Größe nicht sicher sind)
Bewertungstyp	Wählen Sie den Typ der Bewertung aus: ○ Vollständiger Penetrationstest ○ Fokussierter Test ○ Erneut testen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Details finden Sie unter Konfigurieren Sie Bewertungstypen für Penetrationstests.
Zweck der Anwendung	Beschreibung der Funktionalität der Anwendung.
Details des Technologiestapels	Komplettieren Sie den Technologiestapel vom Front-End bis zum Back-End, Datenbanken und andere Schlüsseltechnologien.
Ist Drittpartei-Anwendung?	Bestätigt, ob diese Anwendung im Besitz eines Drittlieferanten ist.
Listet die Arten sensibler Daten auf, auf die über die Anwendung zugegriffen werden kann.	Typen vertraulicher Daten, auf die über die Anwendung zugegriffen werden kann. Zum Beispiel personenbezogene Daten, PHI-Daten und Finanzdaten wie Kreditkartennummern.
Authentifizierungstyp	Gibt an, ob diese Anwendung LDAP-Authentifizierung, eine eigene native Authentifizierung oder andere Authentifizierungsformen verwendet.
Fällt die Anwendung unter ein Compliance-Programm?	Gibt an, ob sich diese Anwendung auf Compliance-Programme wie PCI auswirkt.
Kontakte im Anwendungsteam	Mitglieder des Anwendungsteams, die vom Team für ethische Hacker bei Fragen kontaktiert werden sollen.
Demo-Datum	Datum, an dem diese Anwendung demonstriert werden kann.
Produktbereitstellung geplant am	Geplantes Datum für die Bereitstellung dieser Anwendung in der Produktion.
Anwendungsversion/-release für die Bereitstellung geplant	Version der Anwendung, die für die Produktionsbereitstellung geplant ist.
V19.0: Anwendung im Besitz eines Drittanbieters oder eines Joint Ventures	Wenn Sie für dieses Feld Ja auswählen, wird die Registerkarte Lieferanten-/Joint Venture-Informationen mit zusätzlichen Feldern angezeigt. Der Begriff „Klausel“ kann sich auf Standards für Tests beziehen, die alle Vereinbarungen zwischen zwei oder mehr Parteien umfassen.
Status	Wählen Sie einen Wert basierend auf dem Status der Anforderung aus.
Zuweisungsgruppe	Gruppe ausgewählt, um die Penetrationstestergebnisse zu bearbeiten. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an den Penetrationstestergebnissen arbeitet. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sprint	Zeigt die Sprints mit verfügbarer Bandbreite an, um die Bewertungsanforderung basierend auf dem Feld „ausgewählter Bewertungstyp“ zu erfüllen.
Erstellt	Datum und Uhrzeit der Erstellung der Anforderung.
Teststartdatum	Datum und Uhrzeit des Testbeginns.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung der Anforderung.
Testdetails	
Zu testende URLs	URLs, die in Penetrationstests einbezogen werden müssen.
Auszuschließende URLs	URLs, die von Penetrationstests ausgeschlossen werden müssen.
Wurde diese Anwendung zuvor getestet?	Gibt an, ob diese Anwendung bereits Penetrationstests unterzogen wurde.
Grund für erneuten Test	Grund für die Anforderung einer Neubewertung des Penetrationstests, wenn die Anwendung zuvor getestet wurde.
Wann wurde die Anwendung getestet?	Zeitrahmen, in dem die Anwendung Penetrationstests durchgeführt wurde.
Details des Test-Accounts	Details des Test-Accounts, der vom Ethical Hacking-Team für Penetrationstests verwendet werden kann.
Anwendungsrollen	Rollen, die von der Anwendung für ihre Anwender unterstützt werden.
Meistverwendete Rollen	Am häufigsten verwendete Rollen in der Anwendung.

4. Wählen Sie **Absenden**.
   Eine E-Mail-Benachrichtigung wird an das ethische Hacking-Team gesendet, dass die Anforderung für die entsprechende Anwendung erstellt wurde.

Replizieren Sie eine Penetrationstestanforderung im Status „Geschlossen“

Erstellen Sie eine Penetrationstestbewertungsanforderung, indem Sie eine Anforderung im Status Geschlossen replizieren. Aktive angreifbare Anwendungselemente (Avis) werden in die neue Anforderung kopiert.

Vorbereitungen
Erforderliche Rolle: Anwendungsteam

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Anforderungen für Penetrationstestbewertung** > **Alle**an.
2. Wählen Sie eine Anforderung im Status Geschlossen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie Aus **Kopieren und Anforderung erstellen** .
   Eine neue Anforderung wird erstellt, und die aktiven Avis werden mit aktualisierten Daten in diese Anforderung kopiert. Um den ursprünglichen Status der Avis aus der übergeordneten Anforderung anzuzeigen, navigieren Sie zu **Snapshot Der Penetrationstestergebnisse** Registerkarte.

Penetrationstestergebnisse basierend auf Bewertungsanforderungen erstellen (vor v19.0)

Erstellen Sie Penetrationstestergebnisse basierend auf der Anforderung zur Bewertung des Penetrationstests. Bei diesen Ergebnissen handelt es sich um manuell erstellte Anwendungsschwachstellenelemente (Application Vulnerability Items, Avis).

Vorbereitungen

Erforderliche Rolle: Ethical Hacker

Prozedur

1. Navigieren zu **Alle** > **Self-Service** > **Servicekatalog** > **Services** > **Anforderungen für Penetrationstestbewertung**an.
2. Um eine AVI für eine Penetrationstest-Bewertungsanforderung zu erstellen, wählen Sie die entsprechende Anforderung aus.
3. Wählen Sie im Abschnitt angreifbare Anwendungselemente die Option aus **Neu** .
4. Füllen Sie im Formular die Felder aus.

Formular „Angreifbares Anwendungselement“ (Penetrationstestansicht)

Feld	Beschreibung
Anzahl	Automatisch generierter AVI-Bezeichner für diesen Datensatz.
Bewertungsanforderung	Anforderung zur Bewertung des Penetrationstests, der diese AVI zugeordnet ist.
Schwachstelle	Schwachstelle, die in der Tabelle „Schwachstelleneinträge“ mithilfe der Suchoption ausgewählt wurde.
Risikobewertung	Quantifiziert **Risikopunktzahl** Trennung angreifbarer Elemente in „Kritisch“, „hoch“, „Mittel“, „Niedrig“ und „keine“. Weitere Informationen zu Risikobewertungen finden Sie unter Risiko in berechnen Application Vulnerability Response Automatisch. Ab V16.1 ist der Wert standardmäßig mit dem Schweregrad der Schwachstelle identisch.
Auswirkungen auf Compliance-Programme?	Bestätigt, ob sich dies auf ein Compliance-Programm auswirkt. Auswahlmöglichkeiten sind „Ja“ und „Nein“
Liste der betroffenen Compliance-Programme	Dieses Feld wird angezeigt, wenn der Wert des Felds „wirkt sich auf jedes Compliance-Programm aus“ auf festgelegt ist `Yes`. Listet die betroffenen Compliance-Programme auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Geplante(s) Release/Korrekturversion	Release bis, wann die Penetrationstestergebnisse gelöst werden müssen.
Status	Der Standardwert ist **Öffnen** Wenn die AVI erstellt wird. Siehe status des angreifbaren Anwendungselements (AVI) Für weitere Informationen zur Zuordnung von status.
Zuweisungsgruppe	Gruppe ausgewählt, um an dieser AVI zu arbeiten. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die für diese AVI arbeitet. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Korrekturziel	Datum, bis zu dem Avis korrigiert werden muss, seit der ersten Identifizierung. Dieses Feld wird nur angezeigt, wenn zutreffend. Weitere Informationen zu Korrekturzielen finden Sie unter Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response.
Erstellt	Zeitstempel, zu dem das angreifbare Anwendungselement (AVI) erstellt wurde.
Aktualisiert	Zeitstempel, zu dem das angreifbare Anwendungselement (AVI) aktualisiert wurde.
Geöffnet von	Anwender, der dieses Penetrationstest-Ergebnis erstellt hat.
Sicherheitsteamkontakt	Ansprechpartner im ethischen Hacking-Team.
Kurzbeschreibung	Kurze Erklärung des Penetrationstestergebnisses.
Details	
Technische Details	Technische Details des Penetrationstestergebnisses.
Auswirkung	Bewertung der Auswirkungen des Penetrationstestergebnisses.
Schritte zum Reproduzieren	Dokumentieren Sie die Schritte zum Reproduzieren und Überprüfen des Penetrationstestergebnisses.
Empfehlung	Zeichnen Sie die empfohlenen Aktionen in diesem Feld auf.
Notizen	
Arbeitsnotizen	Fügen Sie Notizen hinzu, um Informationen zu Statusübergängen und anderen Feldaktualisierungen zu kommunizieren.
V16.1: Betroffene URLs	Weitere Informationen zu den betroffenen URLs.
V16.1: Betroffene Parameter	Weitere Informationen zu den betroffenen Parametern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
V16.1: Betroffene Funktionalitäten	Weitere Informationen zu den betroffenen Funktionalitäten.

5. Wählen Sie aus, um das Formular zu speichern **Übermitteln** .

Erstellen Sie einen Anwendungsschwachstelleneintrag

Erstellen Sie einen Anwendungsschwachstelleneintrag für die Schwachstelle, die für das Penetrationstestergebnis angegeben ist. Anwendungsschwachstellen sind Schwachstellen in anwenderdefinierten Softwareanwendungen.

Vorbereitungen

Erforderliche Rolle: Ethical Hacker

Warum und wann dieser Vorgang ausgeführt wird

Application Vulnerability Response Bezieht eine Schwachstelle auf eine Anwendung, um das Penetrationstestergebnis zu erstellen. Diese Ergebnisse sind manuell erstellte angreifbare Anwendungselemente (Avis). Sie können während Penetrationstests einen vorhandenen Eintrag wiederverwenden oder manuell für jede Schwachstelle erstellen.

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Bibliotheken** > **Drittpartei**an.
2. Wählen Sie auf der Seite Anwendungsschwachstelleneinträge die Option aus **Neu** .
3. Füllen Sie im Formular die Felder aus.

Formular „Anwendungsschwachstellen-Eintrag“ (Penetrationstestansicht)

Feld	Beschreibung
ID	Bezeichner für diesen Schwachstelleneintrag.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle. Schweregradzuordnungen werden für NVD und mit ServiceNow-Drittanbieterintegrationen bereitgestellt. Weitere Informationen zum Erstellen oder Anpassen von Schweregradzuordnungen finden Sie unter Ordnen Sie den Schweregrad eines angreifbaren Anwendungselements automatisch zu.
Primäres CVE	Verweis auf das Element „Allgemeine Schwachstellenaufzählung“, in das diese Schwachstelle am besten passt.
Kategoriename	Von der Drittpartei-Integration bereitgestellte Klassifizierung. Hilft bei der Zuweisung.
Schwachstellendetails	
Angriffsvektor	Angriffsvektor für diese Schwachstelle.
Angriffskomplexität	Metrik, die die Bedingungen beschreibt, die außerhalb der Kontrolle des Angreifers liegen und vorhanden sein müssen, um die Schwachstelle auszunutzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Umfang	Metrik zur Messung der Fähigkeit einer Software-Schwachstelle, Ressourcen über ihre Mittel hinaus zu beeinflussen.
Integrität	Metrik zum Messen der Auswirkung auf die Integrität einer erfolgreich ausgenutzten Schwachstelle.
CVSS-Vektor	Öffnen Sie das Framework, um die Merkmale und den Schweregrad von Softwareschwachstellen zu erfassen.
Erforderliche Berechtigungen	Berechtigungsstufe, die ein Angreifer besitzen muss, bevor er die Schwachstelle erfolgreich ausnutzt.
Anwenderinteraktion	Anforderung für menschliche Interaktion, um eine Schwachstelle erfolgreich auszunutzen.
Vertraulichkeit	Auswirkung auf die Vertraulichkeit der Informationsressourcen aufgrund einer erfolgreich ausgenutzten Schwachstelle. Diese Ressourcen werden von einer Softwarekomponente verwaltet.
Verfügbarkeit	Auswirkung auf die Verfügbarkeit der betroffenen Komponente, die aus einer erfolgreich ausgenutzten Schwachstelle resultiert.
CVSS-Basispunktzahl	Numerische Darstellung (0–10) des Schweregrads eines Anwendungsschwachstelleneintrags.
Bedrohung	Beschreibung der Bedrohung durch diese Schwachstelle.
Beschreibung der Verringerung	Beschreibung der Schritte zum Minimieren der Schwachstelle.

4. Wählen Sie aus, um das Formular zu speichern **Übermitteln** .

Hinweis:
Aves werden in der Tabelle „Anwendungsschwachstelleneintrag“ (sn_vul_App_vul_entry) erstellt. Die Tabelle „Anwendungsschwachstelleneintrag“ ist ein untergeordnetes Element des Schwachstelleneintrags (`sn_vul_entry`) Tabelle. Daher werden die erstellten Aves auch der Tabelle „Schwachstelleneintrag“ hinzugefügt.

Penetrationstest-Arbeitsbereich

Der Arbeitsbereich für Penetrationstests in Application Vulnerability Response hilft Kunden, eine Penetrationstestbewertungsanforderung anzufordern und mithilfe des Workflows nachzuverfolgen. Damit können Anwendungsbesitzer die Sicherheitslage ihrer Anwendung bewerten. Es handelt sich um das manuelle Testen einer Anwendung durch das ethische Hacking-Team.

Erforderliche Rollen

Penetrationstests erfordern die folgenden Rollen:

sn_vul.App_Pen_Tester: Stellt einen Pen-Tester dar, der für die Erstellung von Pen-Testergebnissen im Rahmen der Anwendungspenetrationstests verantwortlich ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sn_vul.App_Pen_Test_Requester: Wählen Sie den Datensatz für die Aktion sn_vul.App_Pen_Test_Requester aus.

Lebenszyklus von Penetrationstests

Als Anwendungsbesitzer können Sie das Ethical Hacking-Team um eine Penetrationstestbewertung Ihrer Anwendung anfordern. Das ethische Hacking-Team reagiert auf diese Anforderung und erstellt Penetrationstestergebnisse. Diese Ergebnisse sind manuell erstellte angreifbare Anwendungselemente (Avis).

Der Penetrationstests-Workflow deckt den Lebenszyklus von Penetrationstests ab, von der Übermittlung der Testanforderung bis zur Lösung der Ergebnisse des Teams für ethische Hacking.

Neue Anforderung für Penetrationstestbewertung erstellen

Initiieren Sie eine Penetrationstestbewertungsanforderung für Ihre Webanwendungen, mobilen Anwendungen oder APIs. Diese Anforderungen werden an das Ethical Hacking-Team übermittelt, das dann diese Anwendungen testen und die Ergebnisse der Penetrationstests manuell melden kann.

Vorbereitungen
Erforderliche Rolle: App-Sec-Manager

Prozedur

1. Navigieren zu **Penetrationstest-Arbeitsbereich**an.
2. Auf der **Anforderung Zur Bewertung Von Penetrationstests** Füllen Sie die Felder aus.
3. Wählen Sie **Absenden**.
   Eine E-Mail-Benachrichtigung wird an das ethische Hacking-Team gesendet, dass die Anforderung für die entsprechende Anwendung erstellt wurde.
4. Sobald das Formular übermittelt wurde, kann das ethische Hacking-Team **Beginnen Sie Mit Der Umfangsdefinition** .
5. Nach der Umfangsdefinition bereitet der Anwendungsbesitzer die Testumgebung vor, und das ethische Hacking-Team kann es **Starten Sie den Test** .
6. Wenn Sie die Details in der Anforderung von überprüfen müssen, können Sie die Testphase als „Warten“ markieren, indem Sie auswählen **Auf Warten setzen** Schaltfläche.
7. Sobald die Tests abgeschlossen sind, können Sie die AVITs auf der Registerkarte Penetrationstesttestergebnisse anzeigen.

Hinweis:
Sie können eine Anforderung aus einer vorhandenen Anforderung duplizieren. Nach dem Duplizieren werden die an die übergeordnete Anforderung angehängten AVITs in die duplizierte Anforderung verschoben (nicht kopiert).

Erstellen Sie Penetrationstestergebnisse basierend auf einem Bewertungsfragebogen

Erstellen Sie Penetrationstestergebnisse, die Tests an den anerkannten Standards des MASVS-Fragebogens im Penetrationstest-Workflow ausrichten. Diese Ergebnisse sind manuell erstellte Anwendungs-Schwachstellenelemente (Avis).

Vorbereitungen
Erforderliche Rolle: App-sec Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Penetrationstest-Ergebnisse** Registerkarte
2. Wählen Sie den veröffentlichten Fragebogen basierend auf Ihrer Anwendung aus.
3. Überprüfen Sie die Tests, und markieren Sie die Testphase als abgeschlossen.
4. Schließen Sie die Anforderung nach Abschluss des obigen Schritts.

Hinweis:
Die vorherigen Schritte können von einem Mitglied des Teams für ethische Hacking ausgeführt werden.

Veröffentlichen Sie den Bewertungsfragebogen

Zum Testen einer mobilen Anwendung gibt es bestimmte Standards, die von der OAS-Community entwickelt wurden, um Testern zu helfen, die Fehler in ihren Produkten zu identifizieren. Navigieren Sie zum Bewertungsarbeitsbereich, um den Fragebogen Ihrer Wahl zu erstellen. Veröffentlichen Sie sie, um sie im Bewertungsanforderungsformular anzeigen zu können.

Vorbereitungen

Erforderliche Rolle: sn_vul.App_Pen_Test_Requester

Erforderliche Rollen für anfordernde Person und Tester von Penetrationstests:

sn_vul.App_Manage_Pen_Test_Request:

Enthält: sn_Smart_asmt.assessment_Reader sn_Smart_asmt:assessment_admin sn_Smart_asmt.actor.

sn_vul.App_Pen_Tester

Enthält: sn_Smart_asmt.assessment_Reader sn_Smart_asmt:actor.

Hinweis:
Als Teil der Funktion „Engine für intelligente Bewertungen“ haben wir die obigen Rollen hinzugefügt. Diese Rollen sind wichtig, damit die anfordernde Person und der Tester Penetrationstests die Fragebogen anzeigen und übermitteln können.

Prozedur

1. Navigieren zu **Bewertungsarbeitsbereich**an.
2. Jeder Fragebogen enthält Richtlinien. Überprüfen Sie die Fragebogen, und ändern Sie bei Bedarf, um die Testanforderungen Ihrer Organisation zu erfüllen. Anschließend können Sie die Tests abschließen.
   Der Fragebogen entspricht standardmäßig den MASVS-Standards. Weitere Informationen finden Sie unter:
3. Veröffentlichen Sie die Fragebogen, und wählen Sie den veröffentlichten Fragebogen aus der Liste im Abschnitt „Testdetails“ des Anforderungsformulars für Penetrationstests aus.

   Hinweis:
   Veröffentlichen Sie den Fragebogen, um ihn im Anforderungsformular zur Bewertung der Penetrationstestanforderung anzuzeigen.

4. Die Persona, die Tests durchführt, kann die Tests dann auf der Registerkarte „Bewertung“ des Formulars „Penetrationstest-Anforderung“ als bestanden oder fehlgeschlagen oder nicht zutreffend markieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie einen Bewertungsfragebogen

Nach der Erstellung des Bewertungsfragebogens können Sie diese Fragebogen zu Testzwecken verwenden.

Vorbereitungen

Erforderliche Rolle: sn_vul.App_Pen_Tester

Prozedur

1. Navigieren zu **Penetrationstestanforderung** Formular.
2. Befolgen Sie die im Formular genannten Richtlinien.
3. Wählen Sie ein aus **Penetrationstestanforderung** .
4. Navigieren Sie zu **Registerkarte „Bewertung“** .
5. Öffnen Sie die Registerkarte, beantworten Sie den Fragebogen und **Übermitteln** .

Hinweis:
Die Persona, die der Penetrationstestanforderung zugewiesen ist, kann sie übermitteln.

Penetrationstest-Dashboard

Verschaffen Sie sich in Ihrem persönlichen Penetrationstest-Dashboard einen Überblick über Ihre Penetrationstestanforderungen und manuellen Ergebnisse. Sie können den Fortschritt Ihres Teams mit im Penetrationstest-Arbeitsbereich anzeigen. Das Dashboard bietet Ihnen einen Überblick über Penetrationstestergebnisse. Sie können Tests anzeigen und priorisieren, die Ihre Aufmerksamkeit erfordern, Testergebnisse nachverfolgen und Zuweisungen anzeigen.

Der Pen-Test-Manager/Lead des Ethical Hacking-Teams kann die Schlüsselmetriken identifizieren und analysieren, z. B. die Überwachung der Penetrationstestanforderungen, und den Gesamtfortschritt seines Teams im Penetrationstest-Arbeitsbereich anzeigen. Der Pen-Test-Manager/Lead des Ethical Hacking-Teams kann auch die folgenden Einblicke anzeigen:

- Übersicht über manuelle Ergebnisse, kategorisiert nach Status und Bewertungstyp, um die strategische Entscheidungsfindung zu unterstützen.
- Verteilung der zugewiesenen Penetrationstests auf Einzelpersonen für eine bessere Kapazitätsplanung
- Priorisieren Sie überfällige Ergebnisse basierend auf ihrem Fortschritt, um die Lösungseffizienz zu verbessern.
- Machen Sie sich mit der Landschaft von Pen-Testergebnissen basierend auf der kritischen Verteilung vertraut.

Penetration-Dashboard-Komponenten

Analysieren Sie den Fortschritt und die Daten Ihres Teams visuell, und steigern Sie die Geschäftsergebnisse mithilfe der Komponenten in Ihrem persönlichen Dashboard.

Indikatoren für wichtige Elemente

Zeigen Sie das nicht zugewiesene Notfall-Release, das Übersichtsdatum der Tests, die nicht zugewiesenen Tests und alle ausstehenden kritischen Validierungen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Nicht zugewiesene Notfall-Release** : Gibt die Gesamtanzahl der nicht zugewiesenen Penetrationstestanforderungen für den Bewertungstyp „Notfall-Release“ an.
- **Tests Überfällig** : Gibt die Gesamtanzahl der Tests an, die das Fälligkeitsdatum überschritten haben.
- **Nicht zugewiesene Tests** : Gibt die Gesamtanzahl der nicht zugewiesenen Tests an, die dem Team zugewiesen sind.
- **Kritische Validierung Ausstehend** : Gibt die Gesamtanzahl der AVITs für alle Anforderungen im Status „Validierung ausstehend“ an.

Hinweis:
Wählen Sie jede Kachel aus, um die Liste der Elemente anzuzeigen und die erforderlichen Aufgaben auszuführen.

Penetrationstestanforderungen

Zeigen Sie die Testanforderungen nach Status, überfälligen Tests und Tests nach Release-Genehmigungen an.

- **Testanforderungen nach Status** : Gibt die Anzahl der Testanforderungen in diesen verschiedenen status des Penetrationstestzyklus an. Sie können die Liste der Testanforderungen in verschiedenen status anzeigen und zur Liste navigieren, indem Sie auf die einzelnen farbigen Kacheln klicken. Sie können den Status dieser Tests für die folgenden sechs Monate auch anzeigen, indem Sie den Monat aus der Filter-Dropdownliste im oberen rechten Abschnitt der Registerkarte auswählen. Im Folgenden finden Sie die verschiedenen testanforderungsstatus:
  - Offen: Anzahl der offenen Testanforderungen.
  - Umfangsdefinition wird ausgeführt:
  - Umfangsdefinition abgeschlossen:
  - Umgebungsvorbereitung:
  - Umgebung bereit zum Testen:
  - Test wird ausgeführt:
  - Vollständiger Penetrationstest:
  - Bug Bounty-Programme: Anreize für ethische Hacker mit Prämien, Sicherheitsschwachstellen zu finden und zu melden.
  - Fokussierter Test:
  - Interesse an Führungskräften: Bericht über die Einbindung der Geschäftsleitung und den Support für kritische Projekte innerhalb der Organisation.
  - Einmalige Überprüfungen: Bewerten Sie bestimmte Projekte außerhalb der regulären Entwicklungs- und Releasezyklen, um die Leistung zu bewerten und Verbesserungen zu implementieren.
  - Notfall-Release: Unterstützt Notfall-Releases, die für schnelle Software-Updates erforderlich sind, um kritische Probleme wie Sicherheitsschwachstellen zu beheben.
- **Überfällige Tests:** : Gibt den ausstehenden Test aus einem bestimmten Zeitraum an. Sie können die Zeitleiste auswählen, für die Sie die fälligen Tests anzeigen möchten. Die Dropdown-Optionen sind: **Gestern Fällig** , **Diese Woche fällig** , **Letzte Woche fällig** , **Letzten Monat fällig** , Und **Vor letztem Monat fällig** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Tests nach Release-Genehmigungen** : Gibt genehmigungsstatus für abgeschlossene Tests an, die zur Freigabe bereit sind. Überprüft außerdem, ob alle erforderlichen Prüfungen abgeschlossen sind, bevor neue Software bereitgestellt wird. Sie können den Status dieser Tests für die folgenden sechs Monate auch anzeigen, indem Sie den Monat aus der Filter-Dropdownliste im oberen rechten Abschnitt der Registerkarte auswählen.

Ergebnisse

Gibt die Anzahl der gemeldeten offenen Penetrationstestergebnisse (AVITs) zusammen mit der Anzahl der AVITs an, die validiert werden müssen. Sie können die Liste der Ergebnisse in verschiedenen status anzeigen und zur Liste navigieren, indem Sie die einzelnen farbigen Kacheln auswählen. Die folgenden Daten können Sie in diesem Abschnitt anzeigen:

- **Offene Ergebnisse (AVITs) nach Risikobewertung**
- **Validierung für Ergebnisse ausstehend (AVITs)**

Teamübersicht

Gibt die Tests an, die Teammitgliedern für die folgenden sechs Monate zugewiesen sind. Im Folgenden finden Sie die verschiedenen status:

- **Umfangsdefinition wird ausgeführt**
- **Offen**
- **Umfangsdefinition abgeschlossen**
- **Umgebung bereit zum Testen**
- **Test läuft**
- **Umgebungsvorbereitung**

Platform Analytics-Lösungen für Application Vulnerability Response

Platform Analytics-Lösungen Vorverpackt enthalten Platform Analytics Inhalt zur Verwendung mit anderen ServiceNow AI Platform Produkte. Dies Platform Analytics-Lösung Stellt wichtige Metriken für die Analyse Ihres Anwendungs-Schwachstellenmanagement-Prozesses bereit.

Übersicht

Das Inhaltspaket „Performance Analytics for Vulnerability Response“ ist im verfügbar ServiceNow® Store Als separates Abonnement. Die Anwendung wird nicht automatisch mit der Vulnerability Response-Anwendung installiert. Das Content Pack „Application Vulnerability Response“ ist Teil des Content Pack „Performance Analytics for Vulnerability Response“.

Weitere Informationen zum Einrichten, Installieren und Konfigurieren Ihrer Performance Analytics for Vulnerability Response-Anwendung finden Sie unter Installieren und konfigurieren Sie die Anwendung Performance Analytics für Vulnerability Response [PA] .

Wichtige Begriffe

Performance Analytics (PA)

Lösung, die Verwaltungs-Dashboards erstellt, Berichte zu KPIs und Metriken erstellt und wichtige Geschäftsfragen beantwortet, um die Qualität zu erhöhen und Kosten zu senken.

Angreifbares Anwendungselement (AVI)

Eine Anwendungsschwachstelle, die von einem Schwachstellen-Scanner einer Drittpartei gemeldet wurde und auf einem Konfigurationselement (Configuration Item, CI) vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PA-Indikator

Definiert eine Leistungsmessung, die in regelmäßigen Abständen einer Aktivität oder eines Organisationsverhaltens durchgeführt wird, z. B. Top 10-Anwendungen mit den kritischsten angreifbaren Anwendungselementen.

PA-Indikatorquelle

Datensätze, die Datensätze aus einer Tabellen- oder Datenbankansicht filtern, z. B. AVI aktiv.

- Das Dashboard „meine Anwendungsschwachstellen“ verfolgt das Volumen, die Leistung und den Fortschritt von Anwendungsschwachstellen von der ersten Analyse/Erkennung bis zur Eindämmung oder Korrektur.
- Zeigen Sie die Zielerreichungsraten der Korrektur an, und bestimmen Sie effizient, welche angreifbaren Anwendungselemente (Avis) das größte Risiko für Ihre Organisation darstellen.

Erforderliche Rollen

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet:

- ServiceNow AI Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Die folgenden Dashboards bieten eine grafische Ansicht der AVI-Aktivitäten, um Korrekturpläne und Statusfortschritte zu bestimmen. Sie können sich auf die KPIs konzentrieren, die kritischen betroffenen Anwendungen und Schwachstellen mit hoher Sichtbarkeit zugeordnet sind.

- Das Application Vulnerability Management (PA)-Dashboard kommuniziert KPIs für das Risiko und die Verbreitung von Schwachstellen, betroffene Anwendungen, Nachbesserungstrends und den Korrekturfortschritt. Der Standardwert für Trends ist drei Monate, kann jedoch in 7 Tage, einen Monat, 3 Monate, 6 Monate, seit Jahresbeginn geändert werden. 1 Jahr oder alle.
- Das Dashboard „meine Anwendungsschwachstellen“ verfolgt das Volumen, die Leistung und den Fortschritt von Anwendungsschwachstellen von der ersten Analyse/Erkennung bis zur Eindämmung oder Korrektur.

Hinweis:
Das Dashboard „meine Anwendungsschwachstellen“ ist eine Teilmenge des Übersichts-Dashboards und nur verfügbar, wenn sich ein Mitglied der Security Champion-Anwendergruppe bei einer Instanz anmeldet. Weitere Informationen zum Dashboard „meine Anwendungsschwachstellen“ finden Sie unter Dashboard „meine Anwendungsschwachstellen“ .

Application Vulnerability Management (PA)-Dashboard

Verfolgen Sie das Volumen, die Leistung und den Fortschritt von Anwendungsschwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfälle

Anwender	Dashboard-Verwendung
Schwachstellenmanager	Mit Application Vulnerability Management Dashboard, Schwachstellenmanagement kann bestimmen, welche angreifbaren Anwendungselemente (Avis) das größte Risiko für ihre Organisationen darstellen. Diese Dashboards bieten eine grafische Ansicht der AVI-Aktivitäten, damit sie Korrekturpläne und Statusfortschritte bestimmen können. Konzentrieren Sie sich auf die KPIs, die kritischen betroffenen Anwendungen und Schwachstellen mit hoher Sichtbarkeit zugeordnet sind.

Erforderlich ServiceNow AI Platform Rollen, Setup und Dashboard-Registerkarten

Das Application Vulnerability Management (PA)-Dashboard ist als Teil des Content Pack „Performance Analytics for Vulnerability Response“ enthalten. Das Inhaltspaket „Performance Analytics for Vulnerability Response“ wird nicht automatisch mit installiert Vulnerability Response Anwendung. Sie ist im verfügbar ServiceNow® Store Als separates Abonnement.

Weitere Informationen zum Einrichten, Installieren und Konfigurieren Ihrer Performance Analytics for Vulnerability Response-Anwendung finden Sie unter Installieren und konfigurieren Sie die Anwendung Performance Analytics für Vulnerability Response [PA] .

Navigieren Sie zum Anzeigen des Dashboards als Anwender, der Security Champion-, App-Sec-Manager- oder Entwickleranwendergruppen zugewiesen ist, zu **Application Vulnerability Response** > **Übersicht**an.

Hinweis:
Das Dashboard „meine Anwendungsschwachstellen“ ist eine Teilmenge des Übersichts-Dashboards und nur verfügbar, wenn sich ein Mitglied der Security Champion-Anwendergruppe bei einer Instanz anmeldet. Informationen zum Dashboard „meine Anwendungsschwachstellen“ finden Sie unter Dashboard „meine Anwendungsschwachstellen“.

Ab Version 19,0 von Application Vulnerability Response, Dieses Dashboard kann auch in der neuen Experience-UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** Und klicken Sie auf **Dashboards** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Seite „Dashboards“ in Arbeitsbereich des Schwachstellenmanagers und Seite „Dashboards“ in Arbeitsbereich für IT-Korrekturen.

Das Übersichts-Dashboard kommuniziert KPIs für das Risiko und die Verbreitung von Schwachstellen, betroffene Anwendungen, Nachbesserungstrends und Korrekturfortschritt. Der Standardwert für Trends ist drei Monate, kann jedoch in 7 Tage, einen Monat, 3 Monate, 6 Monate, seit Jahresbeginn geändert werden. 1 Jahr oder alle.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgliederung der Daten in Application Vulnerability Management Dashboard von **Scan-Typ** , **Anwendung** Oder **Geschäftsbereich** . Jede dieser Auswahlmöglichkeiten verfügt über einen zusätzlichen Filter. **Wählen Sie Elemente aus** , Um Ihre Auswahl zu verfeinern. Beginnt ab Application Vulnerability Response V15.0, Geschäfts- und CI-Anwendungen wurden den Auswahlmöglichkeiten für hinzugefügt **Anwendung** Filter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

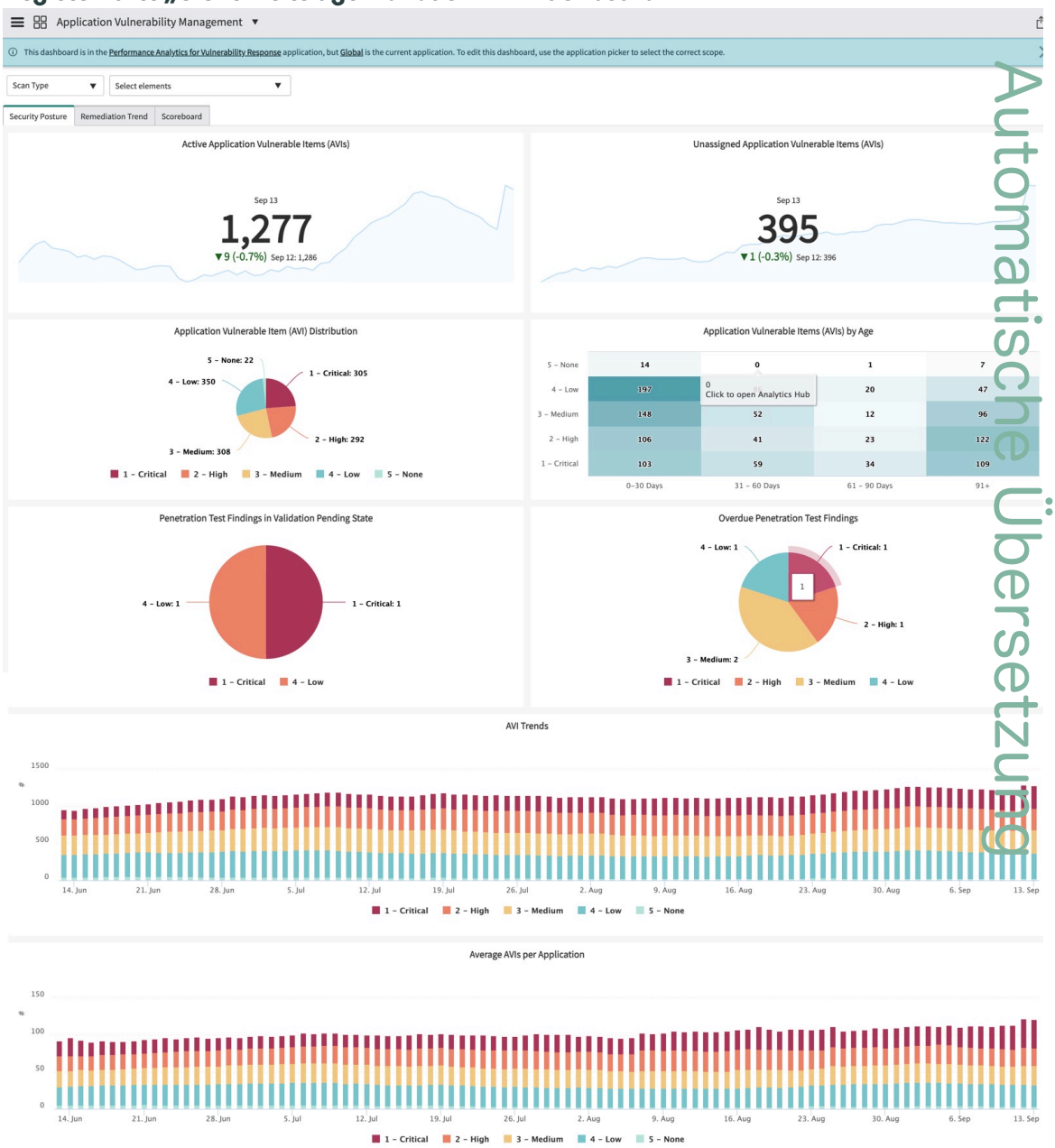
Registerkarte „Sicherheitslage“

Die Registerkarte Sicherheitslage hilft Ihnen, Ihre Sicherheitslage und den Fortschritt Ihrer Korrekturaktionen zu verstehen.

Beginnt ab Application Vulnerability Response V15.0 können Sie die Berichte zu Penetrationstestergebnissen anzeigen. Penetrationstestergebnisse sind angreifbare Anwendungselemente (Avis), die basierend auf den Anforderungen zur Penetrationstestbewertung manuell erstellt werden.

Hinweis:
Der Scan-Typ für diese Widgets ist manuell.

Registerkarte „Sicherheitslage“ für das AVM-Dashboard



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

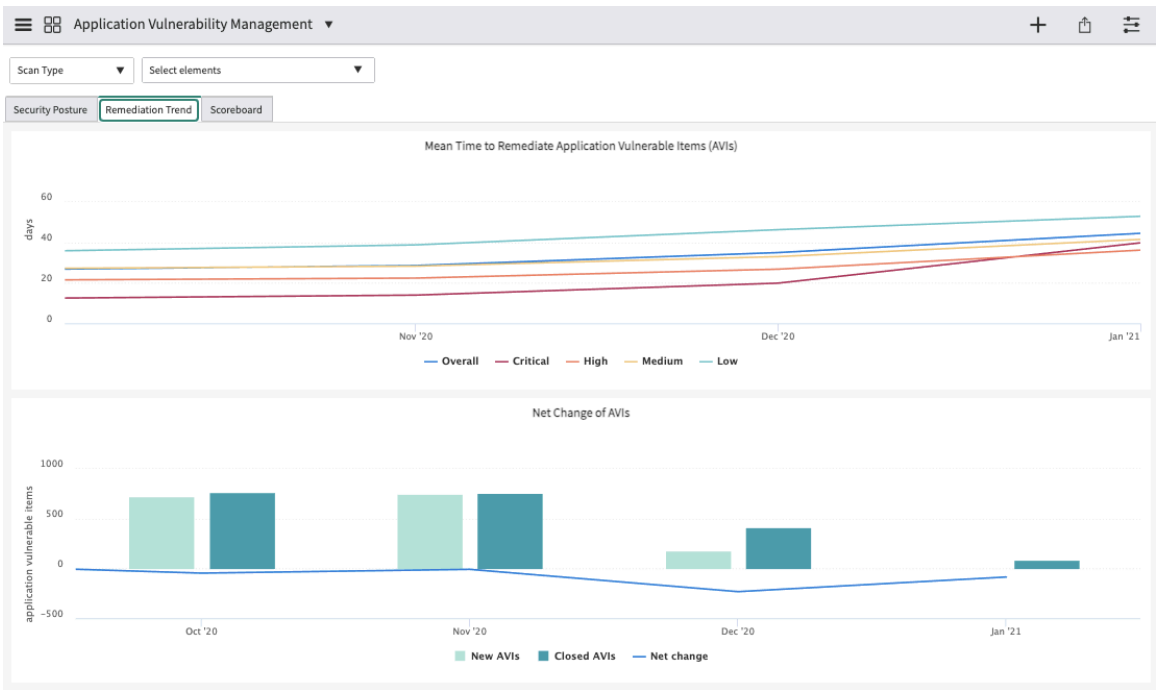
Registerkarte „Ausnahmen“

Dieses Dashboard hilft Ihnen zu verstehen, wo Ihre Organisation aufgrund potenziell übermäßiger Zurückstellungen Risiken eingeht, und hilft Ihnen, Korrekturoptionen zu überdenken.

Sie können zurückgestellte angreifbare Anwendungselemente nach Grund, auslaufende Zurückstellungsanforderungen für Avis, Ausnahmen für kritische angreifbare Anwendungselemente nach Zuweisungsgruppe, AVI-Ausnahmeanforderungen nach anfordernder Person anzeigen.

Registerkarte „Nachbesserungstrend“

Die Registerkarte „Nachbesserungstrend“ hilft Ihnen, den Fortschritt Ihrer Korrekturaktionen zu verstehen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

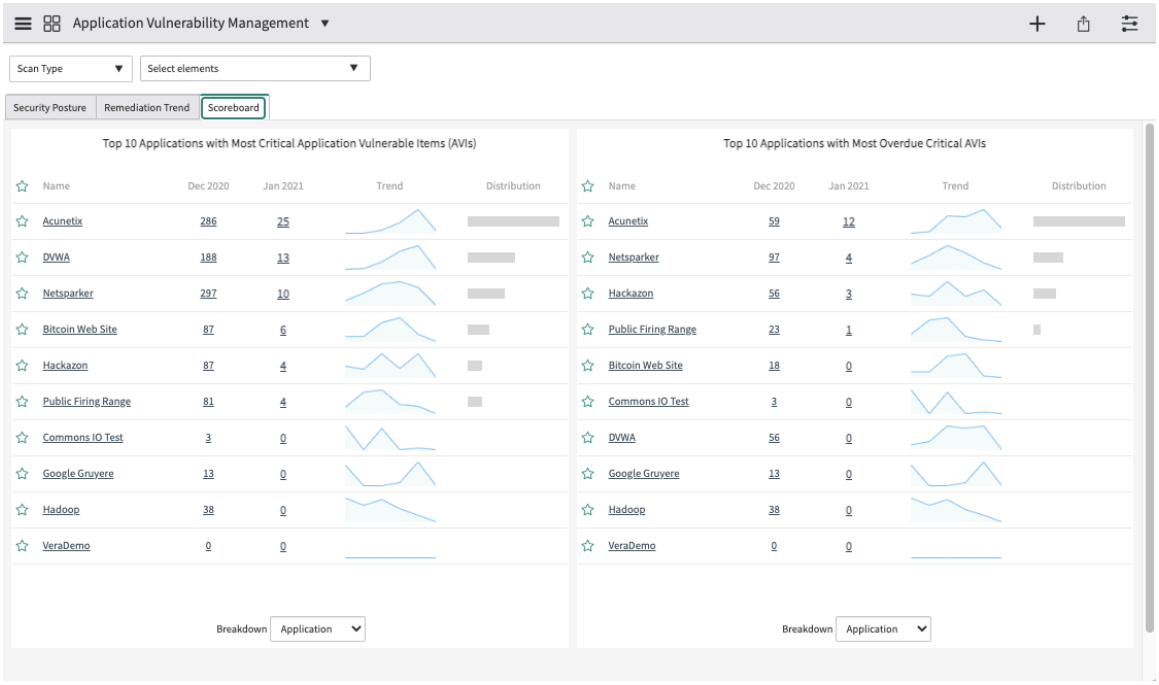
Registerkarte „Anzeigetafel“

Auf der Registerkarte „Anzeigetafel“ können Sie den Fortschritt Ihrer Korrekturaktionen verstehen und welche Avis bei ihrem Abschluss die meiste Unterstützung benötigen.

Scan-Typelemente:

- Dynamisch: Verwenden Sie nur Metriken aus dem dynamischen Datenimport
- Statisch: Verwenden Sie nur Metriken aus dem statischen Datenimport

Sie können entweder oder beide auswählen.



Indikatoren

Mittlere Zeit bis zur Fehlerkorrektur niedriger AVIs

[[summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 4 – Niedrig]] / [[geschlossene angreifbare Anwendungselemente > Risikobewertung = 4 – Niedrig]] . Ziel ist die Minimierung.

Anwendungsreleases

Dies ist die eindeutige Anzahl für Anwendungen von AVI.Active, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

Angreifbare Anwendungselemente

Dies ist die Anzahl in App-vul-Elementen „AVI.aktiv“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

Durchschnittliche AVIs pro Anwendung

[Aktive Angreifbare Anwendungselemente]] / [[Anwendungsveröffentlichungen]] . Ziel ist die Minimierung.

Nicht zugewiesene AEs

Dies ist die Anzahl in der Indikatorquelle „AVI.aktiv“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

Mittlere Zeit bis zur Fehlerkorrektur von AVIs

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[[summierte Dauer der geschlossenen angreifbaren Anwendungselemente]] / [[geschlossene angreifbare Anwendungselemente]] . Ziel ist die Minimierung.

Mittlere Zeit bis zur Korrektur hoher AVIs

[[summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 2 – hoch]] / [[geschlossene angreifbare Anwendungselemente > Risikobewertung = 2 – hoch]] . Ziel ist die Minimierung.

Geschlossene angreifbare Anwendungselemente

Dies ist die Anzahl in der Indikatorquelle „AVI.Geschlossen“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Maximierung.

Mittlere Zeit bis zur Fehlerkorrektur kritischer AVIs

[[summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 1 – Kritisch]] / [[geschlossene angreifbare Anwendungselemente > Risikobewertung = 1 – Kritisch]] . Ziel ist die Minimierung.

Neue angreifbare Anwendungselemente

Dies ist die Anzahl in der Indikatorquelle „AVI.Neu“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

Mittlere Zeit bis zur Fehlerkorrektur mittlerer AVIs

[[summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 3 – Mittel]] / [[geschlossene angreifbare Anwendungselemente > Risikobewertung = 3 – Mittel]] . Ziel ist die Minimierung.

Nettoänderung in AEs

[[Neue Angreifbare Anwendungselemente]] – [[Geschlossene Angreifbare Anwendungselemente]] . Ziel ist die Minimierung.

Summierte Dauer der geschlossenen angreifbaren Anwendungselemente

Dies ist die Anzahl in der Indikatorquelle „AVI.Geschlossen“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

Kritische überfällige angreifbare Anwendungselemente

Dies ist die Anzahl in der Datenquelle „AVI.aktiv“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

Kritische angreifbare Anwendungselemente

Dies ist die Anzahl in der Indikatorquelle „Anwendungen mit aktiven Avis“, die die Tabelle sn_vul_Analytics_App_ci_dept_bu verwendet. Ziel ist die Minimierung.

Aufgliederungen

- Alter
- Geschlossen mit Alter
- Anwendung
- Geschäftsbereich
- Risikobewertung
- Scantyp

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Anpassung der Berechnung von Alter und Alter der geschlossenen Elemente für angreifbare Anwendungselemente (Avis) kann zu einem starken Anstieg oder Rückgang der Performance Analytics (PA)-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung des Alters und des Alters, das für Avis geschlossen wurde, finden Sie unter KB1703270 KB-artikel.

Datenvisualisierungen

Sicherheitslage

Name	Typ	Beschreibung
V15.0: Penetrationstestergebnisse im Status „Validierung ausstehend“	Kreisdiagramm	Penetrationstestergebnisse im Status „gelöst“, aber mit ausstehender Validierung, gruppiert nach Risikobewertung.
V15.0: Überfällige Penetrationstestergebnisse	Kreisdiagramm	Kritische Penetrationstestergebnisse, deren Korrekturzieldatum verfehlt wurde, gruppiert nach Risikobewertung.
Aktive angreifbare Anwendungselemente (AVIs)	Einzelne Punktzahl	Anzahl der aktiven (nicht geschlossenen) angreifbaren Anwendungselemente (AVIs).
Nicht zugewiesene angreifbare Anwendungselemente (AVIs)	Einzelne Punktzahl	Anzahl der aktiven angreifbaren Anwendungselemente (AVIs) ohne eine Zuweisungsgruppe.
Verteilung des angreifbaren Anwendungselements (AVI)	Kreisdiagramm	Distribution aller aktiven angreifbaren Anwendungselemente (AVIs) sortiert nach Risikobewertung.
Angreifbare Anwendungselemente (AVIs) nach Alter	Heatmap	Anzahl der aktiven angreifbaren Anwendungselemente (Avis) gruppiert nach Risikobewertung und Alter (in Tagen). **Hinweis:** Die Anpassung der Berechnung von Alter und Alter der geschlossenen Elemente für angreifbare Anwendungselemente (Avis) kann zu einem starken Anstieg oder Rückgang der Performance Analytics (PA)-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung des Alters und des Alters, das für Avis geschlossen wurde, finden Sie unter KB1703270 KB-artikel.
AVI-Trends	Trend	Trend der aktiven angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung.
Durchschnittliche AVIs pro Anwendung	Trend	Trend der durchschnittlichen angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trend bei Korrekturen

Name	Typ	Beschreibung
Durchschnittliche Zeit bis zur Korrektur angreifbarer Anwendungselemente (Avis)	Linie	Trend der durchschnittlichen Nachbesserungszeit für angreifbare Elemente in einer Anwendung (AVIs) nach Risikobewertung.
Nettoänderung von Avis	Trend	Trend der erkannten neuen angreifbaren Anwendungselemente (Application Vulnerable Items, AVIs) im Vergleich zu den Schließungen pro Monat.

Anzeigetafel

Name	Typ	Beschreibung
Top-10-Anwendungen mit den kritischsten angreifbaren Anwendungselementen (AVIs)	Punktzahlkarte und Verteilungsleiste	Anwendungen mit der höchsten Anzah an kritischen angreifbaren Elementen in einer Anwendung (AVIs).
Top-10-Anwendungen mit den meisten überfälligen kritischen angreifbaren Anwendungselementen (Avis)	Punktzahlkarte und Verteilungsleiste	Anwendungen mit der meisten Anzahl aktiver angreifbarer Anwendungselemente (Avis), die ihre Korrekturzieldaten überschritten haben.

Dashboard „meine Anwendungsschwachstellen“

Dieses Dashboard enthält wichtige Metriken für die Analyse Ihres Anwendungs-Schwachstellenmanagement-Prozesses, z. B. die Anzeige der Korrekturzielerreichungsraten.

Erforderlich ServiceNow AI Platform Rollen und Anzeigen des Dashboards

Hinweis:

- Dieses Dashboard ist Teil des Inhaltspakets „Application Vulnerability Response“. Das Anwendungs-Vulnerability Response-Inhaltspaket ist Teil des Performance Analytics for Vulnerability Response-Inhaltspakets.
- Das Inhaltspaket „Performance Analytics for Vulnerability Response“ ist im verfügbar ServiceNow® Store Als separates Abonnement.
- Das Inhaltspaket „Performance Analytics for Vulnerability Response“ wird nicht automatisch mit der Anwendung „Vulnerability Response“ installiert.

Das Dashboard „meine Anwendungsschwachstellen“ ist nur verfügbar, wenn sich ein Mitglied der Security Champion-Anwendergruppe bei einer Instanz anmeldet. Informationen zum Dashboard „Übersicht“ finden Sie unter Dashboard „Anwendungsschwachstellenmanagement“ [PA] .

Navigieren Sie zum Anzeigen des Dashboards zu **Application Vulnerability Response** > **Meine Anwendungsschwachstellen**an.

Ab Version 19,0 von Application Vulnerability Response, Dieses Dashboard kann auch in der neuen Experience-UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** Und klicken Sie auf **Dashboards** Symbol. Abhängig von Ihrer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Seite „Dashboards“ in Arbeitsbereich des Schwachstellenmanagers und Seite „Dashboards“ in Arbeitsbereich für IT-Korrekturen.

Zeigen Sie Berichte an, die Trenddaten im Zeitverlauf anzeigen. Zeigen Sie Trends wichtiger Metriken in einem regelmäßigen Zeitplan an, um Ihre gesamten Geschäftsprozesse zu analysieren und Verbesserungsbereiche zu identifizieren.

Das Dashboard „meine Anwendungen – Schwachstellen“ ist im Content Pack „Performance Analytics for Vulnerability Response“ enthalten. Das Inhaltspaket „Performance Analytics for Vulnerability Response“ wird nicht automatisch mit installiert Vulnerability Response Anwendung. Sie ist im verfügbar ServiceNow® Store Als separates Abonnement.

Anwendungsfälle

Anwender	Dashboard-Verwendung
IT-Spezialisten, Korrekturbesitzer oder Analysten, die Schwachstellen beheben, die ihnen oder einer Gruppe zugewiesen sind, der sie angehören.	Ein Security Champion verwendet das Dashboard „meine Anwendungsschwachstellen“, um das Volumen, die Leistung und den Fortschritt der Korrektur von Anwendungsschwachstellen nachzuverfolgen. Ermitteln Sie effizient, welche angreifbaren Anwendungselemente (Avis) das größte Risiko für Ihre Organisation darstellen. Diese Dashboards bieten eine grafische Ansicht der AVI-Aktivitäten, um Korrekturpläne und Statusfortschritte zu bestimmen. Sie können sich auf die KPIs konzentrieren, die kritischen betroffenen Anwendungen und Schwachstellen mit hoher Sichtbarkeit zugeordnet sind. Erhalten Sie schnell Einblicke in Ihr Schwachstellenrisiko und Ihre Sicherheitslage. Verfolgen Sie von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur nach.

Dashboard-Registerkarten „meine Anwendungsschwachstellen“ [PA]

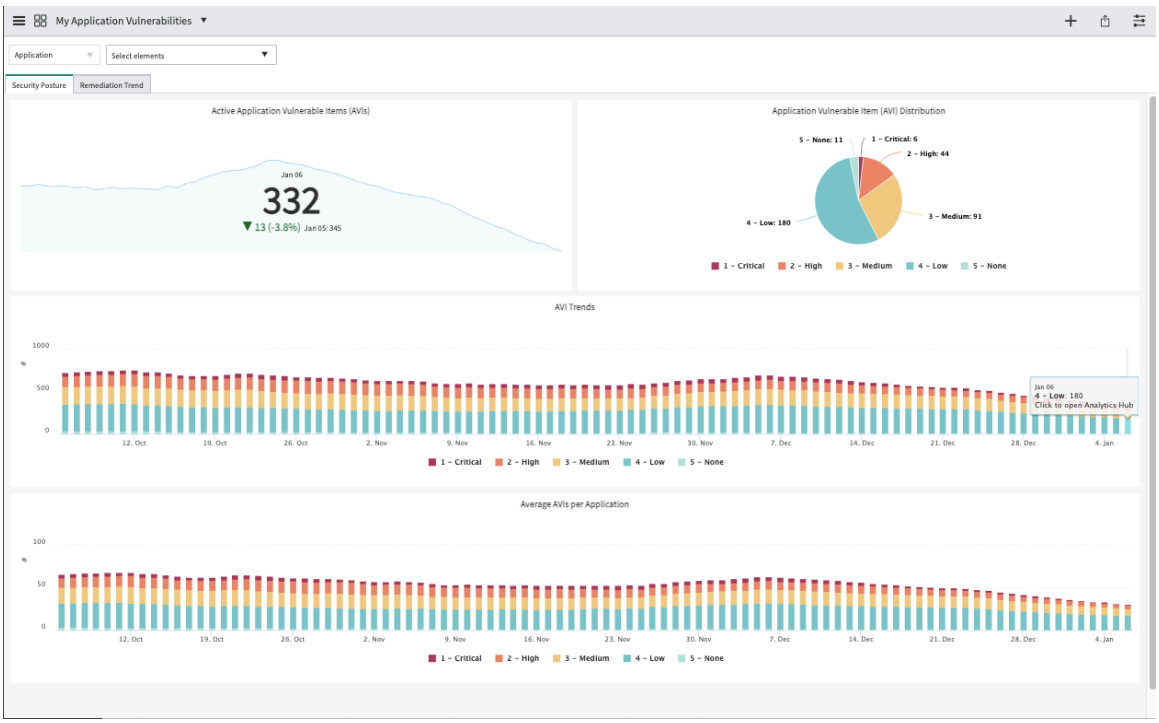
Das Dashboard „meine Anwendungsschwachstellen“ kommuniziert KPIs für das Risiko und die Verbreitung von Schwachstellen, betroffene Anwendungen, Korrekturtrends und Korrekturfortschritt. Der Standardwert für Trends ist drei Monate, kann jedoch in 7 Tage, einen Monat, 3 Monate, 6 Monate, seit Jahresbeginn geändert werden. 1 Jahr oder alle.

Daten werden im Dashboard nach aufgeschlüsselt **Anwendung** . Verwenden Sie **Wählen Sie Elemente aus** Liste, um Ihre Auswahl zu verfeinern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

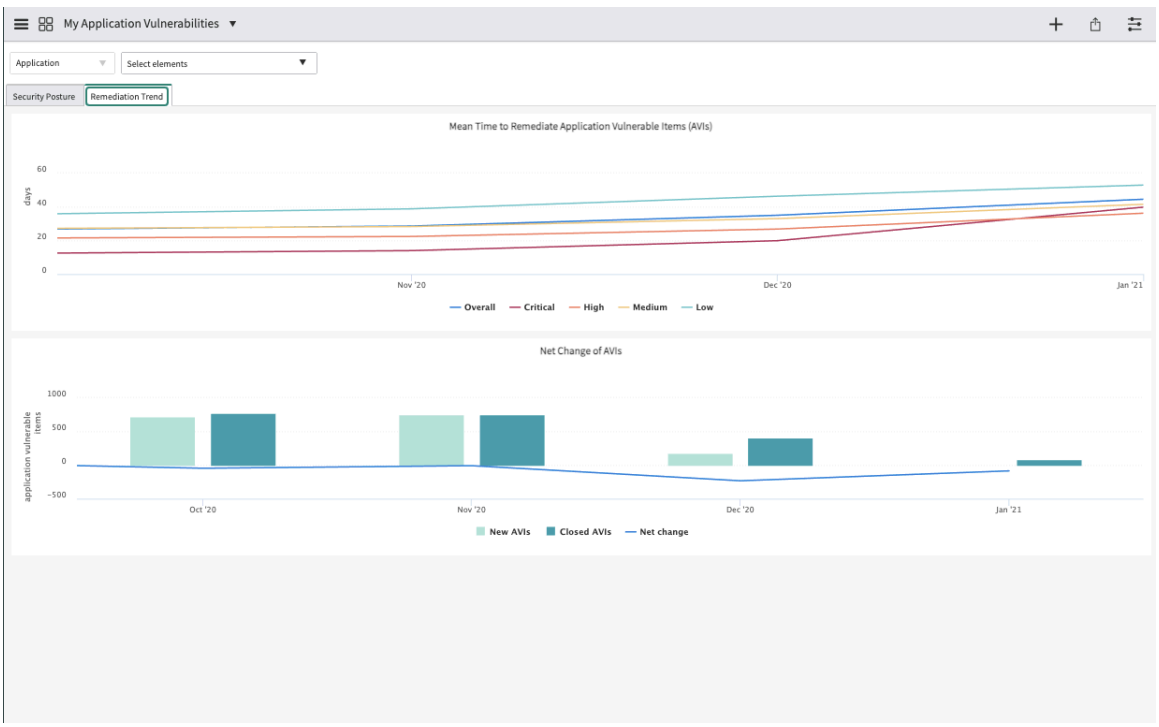
Registerkarte „Sicherheitslage“

Die Registerkarte Sicherheitslage hilft Ihnen, Ihre Sicherheitslage und den Fortschritt Ihrer Korrekturaktionen zu verstehen. Gliedern Sie die Daten im Dashboard „Anwendungsschwachstellenmanagement“ nach auf **Scan-Typ, Anwendung** Oder **Geschäftsbereich** . Jede dieser Auswahlmöglichkeiten verfügt über einen zusätzlichen Filter. **Wählen Sie Elemente aus** , Um Ihre Auswahl zu verfeinern.



Registerkarte „Nachbesserungstrend“

Die Registerkarte „Nachbesserungstrend“ hilft Ihnen, den Fortschritt Ihrer Korrekturaktionen zu verstehen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Indikatoren

Mittlere Zeit bis zur Fehlerkorrektur niedriger AVIs

[[summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 4 – Niedrig]] / [[geschlossene angreifbare Anwendungselemente > Risikobewertung = 4 – Niedrig]] . Ziel ist die Minimierung.

Anwendungsreleases

Dies ist die eindeutige Anzahl für Anwendungen von AVI.Active, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

Angreifbare Anwendungselemente

Dies ist die Anzahl in App-vul-Elementen „AVI.aktiv“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

Durchschnittliche AVIs pro Anwendung

[Aktive Angreifbare Anwendungselemente]] / [[Anwendungsveröffentlichungen]] . Ziel ist die Minimierung.

Nicht zugewiesene AEs

Dies ist die Anzahl in der Indikatorquelle „AVI.aktiv“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

Mittlere Zeit bis zur Fehlerkorrektur von AVIs

[[summierte Dauer der geschlossenen angreifbaren Anwendungselemente]] / [[geschlossene angreifbare Anwendungselemente]] . Ziel ist die Minimierung.

Mittlere Zeit bis zur Korrektur hoher AVIs

[[summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 2 – hoch]] / [[geschlossene angreifbare Anwendungselemente > Risikobewertung = 2 – hoch]] . Ziel ist die Minimierung.

Geschlossene angreifbare Anwendungselemente

Dies ist die Anzahl in der Indikatorquelle „AVI.Geschlossen“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Maximierung.

Mittlere Zeit bis zur Fehlerkorrektur kritischer AVIs

[[summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 1 – Kritisch]] / [[geschlossene angreifbare Anwendungselemente > Risikobewertung = 1 – Kritisch]] . Ziel ist die Minimierung.

Neue angreifbare Anwendungselemente

Dies ist die Anzahl in der Indikatorquelle „AVI.Neu“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

Mittlere Zeit bis zur Fehlerkorrektur mittlerer AVIs

[[summierte Dauer der geschlossenen angreifbaren Anwendungselemente > Risikobewertung = 3 – Mittel]] / [[geschlossene angreifbare Anwendungselemente > Risikobewertung = 3 – Mittel]] . Ziel ist die Minimierung.

Nettoänderung in AEs

[[Neue Angreifbare Anwendungselemente]] – [[Geschlossene Angreifbare Anwendungselemente]] . Ziel ist die Minimierung.

Summierte Dauer der geschlossenen angreifbaren Anwendungselemente

Dies ist die Anzahl in der Indikatorquelle „AVI.Geschlossen“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kritische überfällige angreifbare Anwendungselemente

Dies ist die Anzahl in der Datenquelle „AVI.aktiv“, die die Tabelle sn_vul_App_vulnerable_item verwendet. Ziel ist die Minimierung.

Kritische angreifbare Anwendungselemente

Dies ist die Anzahl in der Indikatorquelle „Anwendungen mit aktiven Avis“, die die Tabelle sn_vul_Analytics_App_ci_dept_bu verwendet. Ziel ist die Minimierung.

Aufgliederungen

- Alter
- Geschlossen mit Alter
- Anwendung
- Geschäftsbereich
- Risikobewertung
- Scantyp

Hinweis:
Die Anpassung der Berechnung von Alter und Alter der geschlossenen Elemente für angreifbare Anwendungselemente (Avis) kann zu einem starken Anstieg oder Rückgang der Performance Analytics (PA)-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung des Alters und des Alters, das für Avis geschlossen wurde, finden Sie unter KB1703270 KB-artikel.

Datenvisualisierungen

Sicherheitslage

Name	Typ	Beschreibung
Aktive angreifbare Anwendungselemente (AVIs)	Einzelne Punktzahl	Anzahl der aktiven (nicht geschlossenen) angreifbaren Anwendungselemente (AVIs).
Verteilung des angreifbaren Anwendungselements (AVI)	Kreisdiagramm	Distribution aller aktiven angreifbaren Anwendungselemente (AVIs) sortiert nach Risikobewertung.
AVI-Trends	Trend	Trend der aktiven angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung.
Durchschnittliche AVIs pro Anwendung	Trend	Trend der durchschnittlichen angreifbaren Elemente in Anwendungen (AVIs), gruppiert nach Risikobewertung.

Trend bei Korrekturen

Name	Typ	Beschreibung
Durchschnittliche Zeit bis zur Korrektur angreifbarer Anwendungselemente (Avis)	Linie	Trend der durchschnittlichen Nachbesserungszeit für angreifbare Elemente in einer Anwendung (AVIs) nach Risikobewertung.
Nettoänderung von Avis	Trend	Trend der erkannten neuen angreifbaren Anwendungselemente (Application Vulnerable Items, AVIs) im Vergleich zu den Schließungen pro Monat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Framework für zusammengefasste Berichte für Application Vulnerability Response

Mit dem Framework für zusammengefasste Berichte können Sie Berichte für die Daten erstellen, die komplexe und lang laufende On-the-fly-Abfragen umfassen, um die Leistung zu verbessern.

Das Framework für zusammengefasste Berichte verbessert die Leistung durch:

- Verwendung weniger Ressourcen und schnelleres Rendern von Berichten,
- Aggregieren der Daten und Wiederverwendung von Zusammenfassungen und Aufgliederungen (Gruppieren nach) und
- Die Abfragen in der Datenbank werden reduziert

Wenn Sie mehr als eine Million angreifbarer Anwendungselemente (AVITs) haben, verwenden Sie neben den Standardberichten das Framework für zusammengefasste Berichte.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- ServiceNow AI Platform Administrator (admin): Installiert und aktiviert Platform Analytics-Lösung und nimmt alle erforderlichen Änderungen an Systemeigenschaften vor.
- Performance Analytics Administrator (PA_admin): Überprüfen Sie die Zusammenfassungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.
- Administrator (sn_vul_cmn.admin): Zusammenfassungen erstellen.
- VR write(sn_vul_cmn.write): Bearbeiten Sie die Daten in den Zusammenfassungen und aggregierten Ergebnissen.
- VR-Lesen (sn_vul_cmn.read): Überprüfen Sie die Daten in den Zusammenfassungen und aggregierten Ergebnissen.
- Schwachstellenanalyst (sn_vul.Vulnerability_Analyst): Überprüfen Sie die zusammengefassten Ergebnisse.

Zugehörige Informationen

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Application Vulnerability Response Referenzen

Referenzthemen mit Informationen zu Tabellen, Rollen und Eigenschaften, die mit installiert sind Application Vulnerability Response Anwendung.

Details finden Sie unter:

- Application Vulnerability Response Anwendergruppen und Rollen
- Mit Application Vulnerability Response installierte Komponenten
- status des angreifbaren Anwendungselements (AVI)
- Gescannte Anwendungsfelder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Felder für angreifbares Anwendungselement
- Anwendungsschwachstellen-Felder
- penetrationsteststatus

Application Vulnerability Response Anwendergruppen und Rollen

Bevor Sie Schwachstellen erfolgreich mit beheben können Application Vulnerability Response(AVR) müssen Sie Anwender Anwendergruppen zuweisen.

Rollen definieren, was Sie und Ihre Gruppen in sehen und tun können Application Vulnerability Response, Performance Analytics for Vulnerability Response, Und Drittpartei-Integrationen mit Application Vulnerability Response.

Anwendergruppen

Im Folgenden sind die Standardanwendergruppen aufgeführt Unterstützung Application Vulnerability Response:

- App-SEC-Manager: Enthält Sicherheitsmanager. Beginnt ab Application Vulnerability Response V15.0 enthält auch Anwendungsbesitzer, die die Penetrationstestbewertungsanforderungen verwalten.
- Security Champion: Enthält Verbindungen zwischen der Entwicklungsgruppe und Sicherheitsmanagern.
- Entwickler: Enthält einzelne Beitragende.
- V15.0: Ethischer Hacker: Enthält Mitglieder des Teams für ethische Hacker, die Penetrationstests von Anwendungen durchführen.

Die Systemadministratorrolle [admin] ist erforderlich, um Anwender dem zuzuweisen Application Vulnerability Response Standardanwendergruppen, die das Modul Anwenderadministration verwenden,

Hinweis:

Zuweisen von AVR-Anwendern zu Application Vulnerability Response Anwendergruppen für Application Vulnerability Response Ist in nicht verfügbar Vulnerability Response Setup-Assistent-Funktion. Nur Vulnerability Response Dort werden Rollen zugewiesen.

In der folgenden Tabelle sind die verfügbaren aufgeführt Application Vulnerability Response Anwendergruppen und die ihnen zugeordneten Rollen. Verwenden Sie diese Tabelle, um zu bestimmen, welche Anwender welchen Gruppen zugewiesen werden sollen.

Anwendergruppe	Rollen in dieser Gruppe
Security Champion Mitglieder dieser Gruppe können:	• sn_vul.App_read_assigned • sn_vul.App_write_assigned • sn_vul.App_Update_assignment_Group

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendergruppe	Rollen in dieser Gruppe
• Lesen und schreiben Sie angreifbare Anwendungselemente (Avis), die Ihnen zugewiesen sind. • Weisen Sie eine Ihnen zugewiesene AVI einer anderen Person oder Gruppe zu. • V20.0: Ausnahmeregeln erstellen, aktualisieren, löschen und abbrechen (deaktivieren).	• sn_vul.App_Update_assigned_to • sn_vul.App_Manage_Auto_Exception_rule
App-Sec-Manager Mitglieder dieser Gruppe können: • V20.0: Ausnahmeregeln erstellen, aktualisieren, löschen und abbrechen (deaktivieren). • Lesen, schreiben, löschen und alle Vorgänge für Regeln für Anwendungskorrekturaufgaben. • Alle Avis lesen und schreiben. • Konfigurieren Sie AVR, indem Sie Regeln, Rechner und Schweregradzuordnungen erstellen und verwalten. • Konfigurieren Sie Integrationen. • Löschen Sie Avis. • Weisen Sie AVI Einzelpersonen oder Gruppen zu. • Verwalten Sie Anwendungen. • Ermöglicht den Zugriff auf das Anwendungsmodul. • Integration planen, konfigurieren, ausführen. • Integrationen lesen und ausführen. • Zeigen Sie AVR an Performance Analytics Dashboards und Berichte. • V15.0: Penetrationstestbewertungsanforderungen verwalten.	• sn_vul.App_Manage_Auto_Exception_rule • sn_vul.App_Manage_Group_rules • sn_vul.App_read_all • sn_vul.App_write_all • sn_vul.App_Update_assignment_Group • sn_vul.App_Update_assigned_to • sn_vul.App_configure_Integrations **Hinweis:** Standardmäßig enthält diese Rolle granulare Rollen für die Konfiguration der Drittpartei-Integration. Informationen zum Definieren oder Bearbeiten einer App-Sec Manager-Anwendergruppe nach einzelnen oder bestimmten Integrationen finden Sie unter Vulnerability Response Personas und granulare Rollen. • sn_vul.App_Manage_assignment_rules • sn_vul.App_Manage_Remediation_target_rules • sn_vul.App_Manage_Risk_Score_configurations • sn_vul.App_Manage_Applications • sn_vul.App_Manage_App_vul_permissions • sn_vul.App_Manage_normalized_severity • Version 13.0: sn_vul.App_Manage_App_sc • Nur Version 12,0: sn_vul.App_read_Application_Release [Entfernt in v12.1. Nicht verwenden] • sn_sec_int.admin • Version 13.0: pa_Power_user • pa_viewer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendergruppe	Rollen in dieser Gruppe
	Hinweis: Beginnend mit Vulnerability Response V13.0, PA_Viewer ist in PA_Power_user enthalten und wird nicht mehr von sich selbst benötigt. • V15.0: sn_vul.App_Manage_Pen_Test_Request • V15.0: sn_vul.App_Update_State • V15.0: cmdb_read
Entwickler Mitglieder dieser Gruppe können: • Lesen und schreiben Sie AVR-Datensätze, die Ihnen zugewiesen sind. • Weisen Sie eine Ihnen zugewiesene AVI einer anderen Person oder Gruppe zu.	• sn_vul.App_read_assigned • sn_vul.App_write_assigned • sn_vul.App_Update_assignment_Group • sn_vul.App_Update_assigned_to • sn_vul.App_PA_sc_View
V15.0: Ethischer Hacker Mitglieder dieser Gruppe können: • Konfigurieren Sie die Standardzuweisungsgruppe und den Beauftragten für Penetrationstestbewertungsanforderungen. • Verwalten Sie Penetrationstestergebnisse. • Verwalten Sie Penetrationstestbewertungsanforderungen. • Zeigen Sie angreifbare Anwendungselemente an. • Aktualisieren Sie die Zuweisung für angreifbare Anwendungselemente.	• V15.0: sn_vul.App_Update_State • V15.0: sn_vul.App_Manage_Pen_Test_Request • V15.0: itil • V15.0: sn_vul.App_read_all • V15.0: sn_vul.App_Manage_Pen_Test_Request_config • V15.0: sn_vul.App_Manage_Manual_avits • V15.0: sn_vul.App_Update_assigned_to • V15.0: sn_vul.App_Update_assignment_Group

Weisen Sie Anwender Anwendergruppen in zu Application Vulnerability Response

Weisen Sie mithilfe des Moduls „Anwenderverwaltung“ in Ihrer Instanz Anwender Gruppen zu.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

So weisen Sie einen Anwender einer Gruppe zu oder entfernen ihn:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Administration** > **Gruppen**an.

b. Suchen und öffnen Sie die entsprechende Gruppe, z. B. **App-Sec-Manager** .
Der Gruppendatensatz wird angezeigt.

c. Wählen Sie die Registerkarte **Gruppenmitglieder** aus.
Die aktuellen Mitglieder der Gruppe werden angezeigt.

d. Klicken Sie auf **Bearbeiten**.
Das Formular Mitglieder bearbeiten wird angezeigt.

e. Von **Sammlung** Wählen Sie Anwender aus, die der Gruppe hinzugefügt oder aus ihr entfernt werden sollen.

f. Sobald alle Anwender zu hinzugefügt wurden **Liste Der Gruppenmitglieder** Oder entfernt, klicken Sie auf **Speichern** .
Sie kehren zu zurück **Gruppenmitglieder** Registerkarte.

g. Klicken Sie Auf **Aktualisieren** Um Ihre Änderungen zu speichern und zur Gruppenliste zurückzukehren.

Zugehörige Informationen

Mit Application Vulnerability Response installierte Komponenten

Mit Application Vulnerability Response installierte Komponenten

Bei der Aktivierung von werden verschiedene Arten von Komponenten installiert Application Vulnerability Response Funktion, einschließlich Tabellen, Anwenderrollen und geplanten Aufgaben.

Ab v24.0.6 von Application Vulnerability Response, Die am häufigsten verwendeten Systemeigenschaften sind jetzt innerhalb von zugänglich Application Vulnerability Response Anwendung. Um diese Systemeigenschaften anzuzeigen, navigieren Sie zu **Alle**Application Vulnerability Response**Eigenschaften**an.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Installierte Rollen

Granulare Rollen in Application Vulnerability Response Sind standardmäßig bestimmten Anwendergruppen zugewiesen.

Hinweis:
Die Verwendung granularer Rollen außerhalb dieser Anwendergruppen erfordert Codierung und erweiterte Funktionen Application Vulnerability Response Oder ServiceNow Fachwissen.

Rollentitel [Name]	Beschreibung	Enthält Rollen
V20.0: sn_vul.App_Manage_Auto_Exception_rule	Ausnahmeregeln erstellen, aktualisieren, löschen und abbrechen (deaktivieren).	sn_vul.App_read_Auto_Excep

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul.App_Manage_Group_rules	Lesen, schreiben, löschen und alle Vorgänge für Regeln für Anwendungskorrekturaufgaben.	• sn_vul.App_read_all • sn_vul.App_read_Grou
V20.0: sn_vul.App_Exception_Approver	Genehmigt Ausnahmeregeln und Ausnahmeregelerweiterungsanforderungen. Ab v20.0 wurde die granulare Rolle sn_vul.App_read_all für diese Rolle entfernt, damit Sie auf die angreifbaren Anwendungselemente und Korrekturaufgaben zugreifen können, die Ihnen und Ihrer Gruppe zugewiesen sind, anstatt auf alle angreifbaren Anwendungselemente und Korrekturaufgaben.	• sn_vul.App_read_Auto • sn_vul.View_Manager_
sn_vul.App_false_positive_Approver	Genehmigt oder lehnt falsch positive Anforderungen ab.	sn_vul.View_Manager_Work
sn_vul.App_read_assigned	Zeigen Sie angreifbare Anwendungselemente (Avis) an, die Ihnen entweder in der klassischen Anwenderoberfläche und zugewiesen sind Arbeitsbereich für IT-Korrekturen. **Wichtig:** Ab v24.0 von Vulnerability Response, Die Rolle „sn_vul.App_read_assigned“ hat die Berechtigung zum Zugriff auf Arbeitsbereich für IT-Korrekturen.	sn_vul.View_ren Workspace
sn_vul.App_read_all	Zeigen Sie alle Avis und zugehörigen Informationen entweder in der klassischen Anwenderoberfläche oder an Arbeitsbereich des Schwachstellenmanagers. **Wichtig:** Ab v24.0 von Vulnerability Response, Die Rolle „sn_vul.App_read_all“ hat die Berechtigung zum Zugriff auf Arbeitsbereich des Schwachstellenmanagers.	sn_vul.View_Manager_Work
sn_vul.App_write_assigned	Aktualisieren Sie die Ihnen zugewiesenen Avis.	
sn_vul.App_write_all	Aktualisieren Sie alle Avis und zugehörigen Informationen.	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul.App_Update_assignment_Group	Aktualisieren Sie die AVI-Zuweisungsgruppe.	**Hinweis:** Bei Verwendung außerha Standardanwendergruppe oder sn_vul.App_write_a
sn_vul.App_Update_assigned_to	Aktualisieren Sie den AVI-Beauftragten.	**Hinweis:** Bei Verwendung außerha Standardanwendergruppe oder sn_vul.App_write_a
sn_vul.App_configure_Integrations	Konfigurieren Sie Drittpartei-Integrationen.	sn_vul.App_read_all sn_vul.App_read_Integra sn_sec_int.admin sn_vul_veracode.configu sn_vul.configure_nvd_Ad [store-future: BEGIN review]sn_vul_fortify.con **Hinweis:** Informationen zum Defin einer App-Sec Manager- einzelnen oder bestimmte Sie unter Vulnerability R granulare Rollen.
sn_vul.App_read_Integrations	Zeigen Sie alle Integrationen von Drittparteien an.	
sn_vul_veracode.configure_Integration	Veracode-Integrationen definieren, aktualisieren und löschen.	
sn_vul.App_Manage_assignment_rules	Definieren, aktualisieren und löschen Sie AVI-Zuweisungsregeln.	sn_vul.App_read_all sn_vul.App_read_assignr
sn_vul.App_read_assignment_rules	Zeigen Sie Zuweisungsregeln an.	
sn_vul.App_Manage_Remediation_target_rules	Definieren, aktualisieren und löschen Sie AVI-Korrekturzielregeln.	sn_vul.App_read_all sn_vul.App_read_Remed
sn_vul.App_Manage_Risk_Score_configurations	Definieren, aktualisieren und löschen Sie AVR-Rechner und Risikoregeln.	sn_vul.App_read_all sn_vul.App_read_Risk_Sc sn_sec_cmn.calc.write

Automatisierte Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul.App_read_Risk_Score_Configuration	Zeigen Sie AVR-Rechner und Risikoregeln an.	
sn_vul.App_Manage_Applications	Anwendungsdatensätze anzeigen, aktualisieren und löschen.	
sn_vul.App_Manage_App_sc	Gibt einem Sicherheitsmeister die Möglichkeit, sich selbst der zugehörigen Liste „gescannte Anwendung“ hinzuzufügen oder daraus zu entfernen.	
sn_vul.App_PA_sc_View	Bietet dem spezifischen Security Champion eine relevante Ansicht.	
sn_vul.App_Manage_App_vul_permissions	[Intern] wird von sn_vul.App_Manage_Applications verwendet.	
sn_vul.App_Manage_normalized_severity	Aktualisieren Sie die Zuordnung auf den normalisierten Schweregrad.	sn_vul.App_read_normalized_
sn_vul.App_read_normalized_severity [Entfernt in v12.1. Nicht verwenden.]	Zeigen Sie Datensätze des normalisierten Schweregrads an.	
sn_vul.App_read_Application_Release	Zeigen Sie Anwendungsrelease-Datensätze an.	
sn_sec_int.admin	Bietet Zugriff auf Integrationen.	
pa_power_user	Bietet Zugriff auf Berichte	pa_viewer
sn_vul.App_sec_Manager	Priorisiert und verwaltet angreifbare Anwendungselemente.	
sn_vul.App_Developer	Entwickler, der für die Behebung der Anwendungsschwachstellen verantwortlich ist.	
sn_vul.App_create_watch_topic	Erstellen Sie Überwachungsthemen für Anwendungsschwachstellen.	
sn_vul.App_read_watch_topic	Lesen Sie Überwachungsthemen für Anwendungsschwachstellen.	
sn_vul.App_Edit_watch_topic	Bearbeiten Sie Überwachungsthemen für Anwendungsschwachstellen.	
sn_vul_blackduck.configure_Integration	Konfigurieren Sie Drittpartei-Integrationen.	sn_vul_blackduck.configure_

Automatische Übersetzung

Installierte geplante Aufgaben

Für Vulnerability Response Freigegebene geplante Aufgaben siehe, Mit Vulnerability Response installierte Komponenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
Ordnen Sie vorhandene Avis der automatischen Ausnahmeregel zu	Wertet angreifbare Anwendungselemente auf Übereinstimmungen mit Ausnahmeregeln aus.
Füllen Sie Eintrag und CVE M2M aus	Macht vorhandene Datensätze mit mehreren CWE-Datensätzen konsistent. Einmal nach dem Upgrade ausführen, um auszufüllen und dann zu deaktivieren.
Primäre CWE neu synchronisieren	Für anwenderdefinierte primäre CWE-Berechnungen. Einmal nach dem Upgrade ausführen, um erneut zu synchronisieren und dann zu deaktivieren.
Rollup der Werte angreifbarer Anwendungselemente für Schwachstelle und Gruppe	Berechnet Schwachstellen und Gruppen-Rollups für angreifbare Anwendungselemente. **Hinweis:** Ab v23.0 von Application Vulnerability Response, Die geplante Aufgabe wird erweitert, um Hintergrundaufträge mit Multithreading-Fähigkeiten zu erstellen. Dieses Upgrade umfasst die Segmentierung des Auftrags in mehrere kleinere untergeordnete Aufträge, die entweder parallel oder gleichzeitig ausgeführt werden. Diese Änderung ermöglicht die gleichzeitige Verarbeitung mehrerer Datensätze, wodurch die Gesamtaufgabe erheblich beschleunigt wird.
Integration Der Black Duck-Projektliste	Ruft Daten in die Tabelle „Black Duck-Projekte“ ab und erfasst sie.
Integration Der Black Duck-Anwendungsliste	Importiert Anwendungen in die Tabelle „erkannte Anwendungen“ für alle Projektversionen, die mit Black Duck Integration in der Projekttabelle verfügbar sind.
Black Duck-Anwendung – Integration Angreifbarer Elemente	Erfasst angreifbare Elemente basierend auf den Schwachstellen, die von Scannern für jede erkannte Anwendung im System erkannt werden.

Installierte Tabellen

Tabelle	Beschreibung
Anwendungs-Release [sn_vul_App_Release]	Enthält Informationen zur Anwendungsversion.
Version 13.0: Anwendungssicherheits-Champions [sn_vul_App_m2m_App_sc]	Enthält Application Vulnerability Response Datensätze der Security Champion-Gruppe.
Anwendungsschwachstelleneintrag [sn_vul_App_vul_entry]	Enthält Anwendungsschwachstellen-Einträge.
Anwendungsschwachstellenintegration	Enthält Application Vulnerability Response Integrationsdatensätze.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_vul_App_Integration]	
Ort für Anwendungsschwachstellen-Scan [sn_vul_App_vul_Scan_location]	Enthält Informationen zum Scan-Standort von Drittparteien.
Zusammenfassung von Anwendungsschwachstellen-Scan [sn_vul_App_vul_Scan_summary]	Enthält Zusammenfassungsinformationen zu Drittpartei-Scans.
Angreifbares Anwendungselement [sn_vul_App_vulnerable_item]	Enthält AVI-Datensätze. Ab v19.0 werden die folgenden Spalten für Software-Stücklisten hinzugefügt: • sn_sbm_config_rule • sn_sbom_component • vex_Begründung • vex_Detail • vex_response • vex_State • sca_type (SBOM-SCA)
Gescannte Anwendung [sn_vul_App_scanned_Application]	Enthält Anwendungsinformationen.
Statuszuordnung [sn_vul_App_State_Map]	Enthält die Statuszuordnung von Drittpartei-Integrationen zu status angreifbarer Anwendungselemente (AVI).
Schwachstellen-CWEs [sn_vul_m2m_entry_cwe]	Verknüpft CVE-Daten mit Einträgen für angreifbare Anwendungen.
Anwendungskorrekturaufgabe – Manifest sn_vul_App_rt_Manifest	Alle Aktualisierungen der Korrekturaufgabe werden mithilfe dieser Manifesttabelle nach geplanten Aufgaben vorgenommen.
Anwendungskorrekturaufgabe sn_vul_App_Vulnerability	Enthält Anwendungskorrekturaufgaben.
Anwendungskorrekturaufgabenelement sn_vul_App_m2m_vul_Group_item	M2M-Tabelle zwischen AVI- und Anwendungskorrekturaufgaben.
Version 21.0: Angreifbare Anwendungselemente	Enthält AVI-Datensätze.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_vul_App_vulnerable_item	
Version 21.0: Paket [sn_vul_App_Package]	Enthält Anwendungspaketdetails.
Version 21.0: Lizenzen sn_vul_App_license	Enthält Anwendungslizenzen.
Version 21.0: Anwendungskorrekturaufgaben sn_vul_App_Vulnerability	Enthält Anwendungskorrekturaufgaben.
sn_vul_blackduck_config	Enthält Details zur Konfiguration der Black Duck-Integration.
sn_vul_blackduck_project	Enthält Details zu den Projekten von Black Duck.
sn_vul_blackduck_project_Import	Importsatztabelle für die Black Duck-Projekterfassung.
sn_vul_blackduck_App_Import	Importsatztabelle für die Black Duck-Anwendungserfassung.
sn_vul_blackduck_avit_Import	Importsatztabelle für die Black Duck AVIT-Erfassung.

status des angreifbaren Anwendungselements (AVI)

Application Vulnerability Response Bietet jederzeit ein Statusmodell für den Status Ihrer angreifbaren Anwendungselemente (Avis). Wenn Sie wissen, wie sich die einzelnen Status zueinander beziehen und sich gegenseitig beeinflussen, können Sie bestimmen, wann und wie Sie Ihre Avis korrigieren können.

status des angreifbaren Anwendungselements

Das Verständnis der Funktionsweise von status hilft beim Erstellen oder Bearbeiten von AVI-Regeln (Application Angreifbare Element). Avis haben mehrere mögliche status, die dem importierten Korrekturstatus aus der Drittpartei-Integration zugeordnet werden. In einem AVI die **Status** Feld ist schreibgeschützt.

Application Vulnerability Response status-Flow-Diagramm

Status	Beschreibung
Öffnen	Status bei Erstellung. In diesem Status können Sie: **V16: Weitere Details abrufen** Rufen Sie die folgenden Informationen zu einem aus Fortify importierten AVI ab: • Schwachstellenzusammenfassung • Erklärung der Schwachstelle • Empfehlung • Referenzen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Application Vulnerability Response status-Flow-Diagramm (Fortsetzung)

Status	Beschreibung
	• Anforderung • Antwort **V16: Als falsch positiv markieren** Markieren Sie ein Element als falsch positiv, wenn der Scanner meldet, dass im System eine Schwachstelle vorhanden ist, in Wirklichkeit jedoch keine Schwachstelle vorhanden ist. **V16: Ausnahme anfordern** Fordern Sie eine Ausnahme, ein Wiedereröffnungsdatum (bis), einen Grund an, und geben Sie optional zusätzliche Informationen an. Verschiebt die Korrektur des Elements bis zu dem Datum, bis zu dem eine Ausnahme angefordert wird. **V15: Schließen** Wählen Sie im Dialogfeld „Angreifbares Element schließen“ den Status Geschlossen aus, und geben Sie zusätzliche Informationen an. Schließt das AVI. **V15: Lösen** Markieren Sie ein offenes AVI als gelöst, um es in den Status gelöst zu verschieben. Sie müssen Lösungshinweise im Dialogfeld Angreifbares Anwendungselement lösen hinzufügen.
Zurückgestellt	**V15:** Dies wird durch ausgelöst **Ausnahme Anfordern** Option. Als Teil des Genehmigungs-Workflows ist der Status „Zurückgestellt“ in Überprüfung und kann erst nach Genehmigung geschlossen werden. In diesem Status können Sie: **V16: Weitere Details abrufen** Rufen Sie die folgenden Informationen zu einem aus Fortify importierten AVI ab: • Schwachstellenzusammenfassung • Erklärung der Schwachstelle • Empfehlung • Referenzen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Application Vulnerability Response status-Flow-Diagramm (Fortsetzung)

Status	Beschreibung
	• Anforderung • Antwort **Erneut öffnen** Versetzt eine geschlossene oder gelöste AVI zurück in den Status Offen. **Schließen** Wählen Sie den Status „Geschlossen“ und einen Grund aus, und geben Sie zusätzliche Informationen an. Schließt das AVI.
Wird untersucht	Wählen Sie diese Option aus dem aus **Status** Liste. In diesem Status können Sie: **V20.0** Führen Sie einen manuellen Übergang einer Korrekturaufgabe oder eines AVI-Datensatzes zu durch **Warten Auf Implementierung** . **V16: Weitere Details abrufen** Rufen Sie die folgenden Informationen zu einem aus Fortify importierten AVI ab: • Schwachstellenzusammenfassung • Erklärung der Schwachstelle • Empfehlung • Referenzen • Anforderung • Antwort **V16: Als falsch positiv markieren** Markieren Sie ein Element als falsch positiv, wenn der Scanner meldet, dass im System eine Schwachstelle vorhanden ist, in Wirklichkeit jedoch keine Schwachstelle vorhanden ist. **V16: Ausnahme anfordern** Fordern Sie eine Ausnahme, ein Wiedereröffnungsdatum (bis), einen Grund an, und geben Sie optional zusätzliche Informationen an. Verschiebt die Korrektur des Elements bis zu dem Datum, bis zu dem eine Ausnahme angefordert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Application Vulnerability Response status-Flow-Diagramm (Fortsetzung)

Status	Beschreibung
	V15: Schließen Wählen Sie im Dialogfeld „Angreifbares Element schließen“ den Status Geschlossen aus, und geben Sie zusätzliche Informationen an. Schließt das AVI. **V15: Lösen** Markieren Sie ein offenes AVI als gelöst, um es in den Status gelöst zu verschieben. Sie müssen Lösungshinweise im Dialogfeld Angreifbares Anwendungselement lösen hinzufügen.
Warten auf Implementierung	Sie können Datensätze nur manuell in diesen Status übergehen, indem Sie „Warten auf Implementierung“ aus AVI und Korrekturaufgabendatensätze im Status „wird untersucht“ auswählen. In diesem Status können Sie: **Öffnen** Wechselt AVI zurück in den Status „Offen“. **Wird untersucht** Rufen Sie weitere Informationen zur Lösung ab. Wechselt zu „wird untersucht“. **Lösen** Markieren Sie ein offenes AVI als gelöst, um es in den Status gelöst zu verschieben. Sie müssen Lösungshinweise im Dialogfeld Angreifbares Anwendungselement lösen hinzufügen. **Schließen** Wählen Sie im Dialogfeld „Angreifbares Element schließen“ den Status Geschlossen aus, und geben Sie zusätzliche Informationen an. Schließt das AVI. Wechseln Sie in diesem Status einen Datensatz in „Warten auf Implementierung“, wenn Ihre Forschung und Arbeit an einer Aufgabe abgeschlossen sind und obwohl eine Korrektur zur Implementierung bereit ist, sie noch nicht verfügbar ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Application Vulnerability Response status-Flow-Diagramm (Fortsetzung)

Status	Beschreibung
	Legen Sie fest **Datum der Korrekturzusage** Und **Korrekturplan** Felder. Nach der Implementierung lösen oder schließen Sie die Datensätze.
Gelöst	Wird über die Schaltfläche „Lösen“ ausgelöst. In diesem Status können Sie: **V16: Weitere Details abrufen** Rufen Sie die folgenden Informationen zu einem aus Fortify importierten AVI ab: • Schwachstellenzusammenfassung • Erklärung der Schwachstelle • Empfehlung • Referenzen • Anforderung • Antwort **Erneut öffnen** Wechselt zurück zu **Öffnen** status. **Schließen** Wählen Sie aus **Geschlossen** status, einen Grund, und geben Sie zusätzliche Informationen an. Schließt die Gruppe. Hinweise und Lösungsinformationen werden unter angezeigt **Notizen** Registerkarte.
Geschlossen	Wird über die Schaltfläche „Schließen“ ausgelöst. In diesem Status können Sie: Erneut öffnen: Wechselt in den Status „Offen“ zurück.

Hinweis:
Weitere Informationen finden Sie unter Integration Von Application Vulnerability Response Mit anderen Anwendungen zum Verständnis verschiedener Integrationen, die die AVI bezogen haben.

status der Anwendungskorrekturaufgabe

Von der Erstellung bis zum Abschluss einer Anwendungskorrekturaufgabe durchläuft die Anwendungskorrekturaufgabe während des gesamten Korrekturprozesses verschiedene status.

Die Statuspriorität lautet wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geschlossen > **Zurückgestellt** > **Gelöst** > **Wird überprüft** > **Warten auf Implementierung** > **Wird untersucht** > **Öffnen**

Der Statusübergang geschieht, wenn Sie verschiedene Aktionen ausführen, z. B. Zurückstellen, Öffnen, Schließen usw.

Die Aktionen, die Sie für eine Anwendungskorrekturaufgabe in einem bestimmten Status ausführen können, ähneln denen einer Host-Korrekturaufgabe. Daher finden Sie weitere Informationen unter Vulnerability Response status der Korrekturaufgabe Und Status-Rollup- und Rollup-Szenarien In Vulnerability Response Dokumentation.

Hinweis:
Ab v23.0 von Vulnerability Response, **Schließen** Schaltfläche wurde entfernt, um sicherzustellen, dass das Schließen der Korrekturaufgabe vom Scanner gesteuert wird.

Application Vulnerability Response Beispiele für Regel für Korrekturaufgaben

Ein Beispiel für eine Regel für Korrekturaufgaben mit dem Bedingungsgenerator.

Eine Regel für Korrekturaufgaben mit Schwachstelle, Produktmodell, IP-Adresse und Zuweisungsgruppe

1. Legen Sie im Bedingungsgenerator für einen neuen Datensatz die Bedingung als fest **Schwachstelle** > **ist** Und geben Sie eine bekannte Schwachstelle ein.

   Schwachstellen werden aus den Integrationen Nation Vulnerability Database (NVD) und Common Weakness Enumeration (CWE) importiert, wie in beschrieben Application Vulnerability Response konfigurieren.

2. Wählen Sie im Abschnitt Gruppieren nach die Option aus **Angreifbares Anwendungselement** Für **Gruppieren Sie angreifbare Anwendungselemente aus** Feld.
3. Wählen Sie im Feld Verwenden die Option aus **Zuweisungsgruppe** .

   Verwenden Sie Zuweisungsregeln, um automatisch festzulegen **Zuweisungsgruppe** Feld zur Verwendung in Ihrer Korrekturaufgabenregel. Sie können eine mit der Anwendung bereitgestellte Regel verwenden oder eigene Zuweisungsregeln einrichten. Weitere Informationen finden Sie unter Weisen Sie angreifbare Anwendungselemente in zu Application Vulnerability Response Automatisch.

4. Wählen Sie eine andere Bedingung aus, z. B. Konfigurationselement für angreifbare Anwendungselemente im **Angreifbares Anwendungselement von gruppieren** Feld und IP-Adresse oder Produktmodell in **Verwenden** Feld.
5. Wählen Sie im Abschnitt „Zuweisung“ für Feld „Korrekturaufgabe zuweisen“ die Option aus **Feld „Gruppieren nach“** .
6. Wählen Sie im Feld Gruppieren nach die Option aus **Zuweisungsgruppe** .

   Wie in diesem Abschnitt beschrieben, weist diese Auswahl angreifbare Elemente verschiedenen Gruppen basierend auf den Bedingungen zu, die Sie im Abschnitt „Gruppieren nach“ festgelegt haben. Obwohl Avis die Schwachstelle gemeinsam nutzen, werden sie basierend auf dem CI-Produktmodell oder nach IP-Adresse verschiedenen Gruppen zugewiesen.

7. Wählen Sie Aus **Übermitteln** Um Ihre Regel zu speichern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gescannte Anwendungsfelder

Anwendungen werden während des Imports unter gespeichert **Administration** > **Erkannte Anwendungen** in Application Vulnerability Response.

Gescannte Anwendungsfelder

Die importierten Felder in dieser Tabelle sind schreibgeschützt, sofern nicht anders angegeben. **Abteilung** Und **Supportgruppe** Einträge können manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.

Feld	Beschreibung
Name	Importierter Name der Anwendung.
Version	Importierte Version der Anwendung, falls zutreffend.
Betriebsstatus	Importierter Betriebsstatus der Anwendung.
Abteilung	Importierte Abteilung, zu der die Anwendung gehört. Wenn leer, kann es manuell hinzugefügt werden.
Geschäftsbereich	Importierter Geschäftsbereich, zu dem die Abteilung gehört. Wenn **Abteilung** Feld ausgefüllt ist, wird dieses Feld automatisch mit dem Geschäftsbereich ausgefüllt, zu dem die Abteilung gehört. Andernfalls wird er leer und schreibgeschützt gelassen.
Support-Gruppe	Importierte Supportgruppe, zu der die Anwendung gehört. Wenn leer, kann es manuell hinzugefügt werden.
Beschreibung	Importierte Beschreibung der Anwendung.
Letzte Compliancеprüfung der Richtlinie am	Datum, an dem die Anwendung zuletzt von Veracode zur Richtlinienkonformität gescannt wurde. Es wird in den verketteten Integrationen der Anwendungslistenintegration verwendet, wo Unterstützung für die Delta-Erfassung für Anwendungen verfügbar ist, indem dieses Datum mit der Delta-Startzeit der jeweiligen Integrationen verglichen wird. **Hinweis:** Daten werden abgerufen, damit Anwendungen aus Veracode abgerufen werden, dessen Wert „Datum der letzten Richtlinien-Compliance-Prüfung“ größer oder gleich der „Startzeit“ (delta_Start_time) der verketteten Integrationen ist.
Zugehörige Liste (nur für einen App-Sec-Manager oder Security Champion sichtbar)	
Security Champion	Listet die Anwendungen auf, die einem Security Champion zugeordnet sind. App-SEC-Manager können Mitglieder zur Liste hinzufügen oder daraus entfernen.

Felder für angreifbares Anwendungselement

Angreifbare Anwendungselemente (AVITs) werden während der Importe von Schwachstellenintegrationen aus Drittteilen automatisch erstellt.

Felder für angreifbare Anwendungselemente

Mit Ausnahme von **Zuweisungsgruppe** , **Zugewiesen an** Felder und **Notizen** , Alle anderen Felder in AVIT sind schreibgeschützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anzahl	Automatisch generierter AVIT-Bezeichner für diesen Datensatz.
Überprüfungstyp	Typ des Scanners, der diesen AVIT gefunden hat. Die Auswahlmöglichkeiten lauten wie folgt: • Dynamisch • Statisches Objekt • SCA
Risikobewertung	Quantifiziert **Risikopunktzahl** Trennung angreifbarer Elemente in „Kritisch“, „hoch“, „Mittel“, „Niedrig“ und „keine“. Weitere Informationen zu Risikobewertungen finden Sie unter . Risiko in berechnen Application Vulnerability Response Automatisch.
Risikopunktzahl	Berechnetes Risiko, das die AVI für Ihre Umgebung darstellt. Weitere Informationen finden Sie unter Risiko in berechnen Application Vulnerability Response Automatisch.
Datum der Korrekturzusage	Das Datum, an dem AVITs nach dem Verschieben in korrigiert werden sollen **Wird Untersucht** . Dieses Feld wird nur angezeigt, wenn sich der AVIT in befindet **Wird Untersucht** .
Korrekturziel	Datum, bis zu dem die AVITs korrigiert werden sollen, seit der ersten Identifizierung. Wird nur angezeigt, wenn zutreffend. Weitere Informationen zu Korrekturzielen finden Sie unter Automatisieren Sie die Nachverfolgung von Korrekturzielen in Application Vulnerability Response.
Korrekturstatus	Status der Korrektur für AVIT. Sie wird vom AVIT mit dem nächsten Fälligkeitsdatum bestimmt, falls zutreffend. Zu den Status gehören: • In Ausführung • Ziel rückt näher • Vergangenes Ziel
Kategoriename	Name der Kategorie der Schwachstelle.
Schwachstelle	ID der Schwachstelle, die diesem angreifbaren Anwendungselement zugeordnet ist.
Anwendungs-Release	Version der Anwendung.
Anwendungsmodul	Betroffene Anwendung im DAST-Scan. Für SAST-Scans ausgeblendet.
Standort Version 14.0: SAST	DAST: URL-Speicherort der Schwachstelle in der Anwendung. SAST: Dateipfad und Zeilennummer der Schwachstelle in der Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Dieses Feld ist standardmäßig auf festgelegt **Öffnen** Bei der Erstellung. Siehe status des angreifbaren Anwendungselements (AVI) Für weitere Informationen zur Zuordnung von status.
Grund	[Nur sichtbar, wenn sich der AIV im befindet **Geschlossen** status.] Erklärung des Status.
Zuweisungsgruppe	Gruppe ausgewählt, um an dieser AVIT zu arbeiten. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die für diese AVI arbeitet. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden
Erste ermittelte	Datum, an dem die Drittparteiquelle das angreifbare Anwendungselement zuerst gefunden hat.
Zuletzt gefunden	Datum, an dem die Drittparteiquelle das angreifbare Anwendungselement zuletzt gefunden hat.
Geschlossen	[Nur sichtbar, wenn sich die AVIT im befindet **Geschlossen** status.] Datum, an dem die AVI geschlossen wurde.
Geschlossen von	[Nur sichtbar, wenn sich die AVIT im befindet **Geschlossen** status.] Entität, die den AVIT geschlossen hat.
Zusammenfassung	Importierte Beschreibung der Schwachstelle.
Ergebnisse Schreibgeschützte Daten, die aus der Integration von Drittparteien importiert wurden.	
AVIT-ID der Quelle	Importierter Bezeichner für die Quell-AVIT.
Quellenschweregrad	Schweregrad aus der Quellanwendung importiert.
Zieldatum für Quellenkorrektur	Importdatum, bis zu dem die Quelle die Korrektur des AVIT erwartet.
Quellenminderungsstatus	Hat den Minderungsstatus aus der Quellanwendung importiert.
Quellenkorrekturstatus	Korrekturstatus aus der Quellanwendung importiert.
Quellermittlungsstatus	[Nur sichtbar, wenn ausgefüllt] Problemstatus aus der Quellanwendung importiert.
SDLC-Status	Lebenszyklusstatus der Softwareentwicklung importiert.
Entspricht der Richtlinie	Compliance-Status importiert. Wenn kein Status angegeben ist, wird dieses Feld auf festgelegt **Nicht Zutreffend** .
Quell-Link	URL zur Quell-AVIT.
Quellhinweise	Importierte Notizen aus der Quelle.
Schwachstellenzusammenfassung	Zusammenfassung aus der Quelle importiert.
Erklärung der Schwachstelle	Erklärung aus der Quelle importiert.
Empfehlung	Empfehlung aus der Quelle importiert.
Referenzen	Referenzen aus der Quelle importiert.
HTTP-Anforderung/-Antwort (nur für DAST-Scans sichtbar)	
Quellenanforderung	HTTP-Anforderung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quellenantwort	HTTP-Antwort
Notizen	
Korrekturplan	Details dazu, wie die AVITs korrigiert werden. Der Plan sollte von implementiert werden **Datum der Korrekturzusage** . Dieses Feld wird nur angezeigt, wenn sich der AVIT in befindet **Wird Untersucht** .
Zusätzliche Kommentare/ Arbeitsnotizen	Alle relevanten Informationen. Wählen Sie das Textfeld für Arbeitsnotizen aus, um Informationen hinzuzufügen. Beginnend mit Vulnerability Response V20.0 können Sie Arbeitsnotizen im Abschnitt „Notizen“ für ein zurückgestelltes angreifbares Anwendungselement hinzufügen.

Altersberechnungen für eine AVIT:

- Die Spalte Alter in der AVIT-Liste zeigt die Dauer (Format: Tage HH:MM:SS) an, für die ein AVIT aktiv ist. Der Alterswert ist null für einen geschlossenen AVIT.
- Die Spalte Alter geschlossen in der AVIT-Liste zeigt die Dauer (Format: Tage HH:MM:SS) an, für die ein AVI aktiv ist, bevor es geschlossen wird. Für AVITs, die sich nicht im Status „Geschlossen“ befinden, ist der Wert „Alter geschlossen“ null.

Weitere Informationen zum Anpassen der Berechnung des Alters und der Dauer der geschlossenen Zeiten finden Sie unter KB1703270 artikel.

penetrationsteststatus

Anwendungsbesitzer können eine Penetrationstestbewertung für ihre Anwendungen anfordern und den Fortschritt des Teams für ethische Hacker überwachen, bis die Anforderung gelöst ist.

Die Penetrationstest-Bewertungsanforderung durchläuft die folgenden übergangsstatus, bis sie gelöst ist.

Phasen der Anforderung zur Bewertung des Penetrationstests

Feld	Beschreibung
penetrationsteststatus	
Öffnen	Status, wenn die Bewertungsanforderung vom Anwendungsbesitzer erstellt wird.
Umfangsdefinition	Das Ethical Hacking-Team bewertet die Anforderung und den Umfang der Anwendung.
Vorbereitung der Umgebung	Der Anwendungsbesitzer erstellt eine Umgebung mit Rollen und anderen Informationen und stellt sie dem ethischen Hacking-Team zum Testen zur Verfügung.
Tests	Das Ethical Hacking-Team testet die Anwendung manuell, um die Ergebnisse des Penetrationstests zu identifizieren.
V16.1: Test wird ausgeführt	Das ethische Hacking-Team gibt an, dass derzeit Tests durchgeführt werden. Wenn dieser Status ausgewählt ist, wird **Test Angehalten** Option wird im Formular verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Phasen der Anforderung zur Bewertung des Penetrationstests (Fortsetzung)

Feld	Beschreibung
V16.1: Test angehalten	Dieses Feld wird nur angezeigt, wenn der Status „Test wird ausgeführt“ ausgewählt ist. Das Ethical Hacking-Team steuert die Servicelevel-Vereinbarungen (Service Level Agreements, SLAs) der Penetrationstestbewertungsanforderungen, indem dieser Status bei Bedarf ausgewählt wird. Dadurch wird sichergestellt, dass genaue SLAs gemeldet werden.
V16.1: Tests werden überprüft	Das ethische Hacking-Team gibt an, dass die Tests abgeschlossen sind und von einem Fachexperten überprüft werden.
Geschlossen	Das ethische Hacking-Team schließt die Anforderungen zur Bewertung von Penetrationstests, nachdem die Ergebnisse des Penetrationstests gemeldet wurden. **Hinweis:** Ab V16.1 können Sie verwenden **Kopieren und Anforderung erstellen** Option im Formular, um die Anforderung im Status „Geschlossen“ zu replizieren und eine neue Anforderung zu erstellen. Details finden Sie unter Replizieren Sie eine Penetrationstestanforderung im Status „Geschlossen“.
V16.1: Abgebrochen	Der Anwendungsbesitzer bricht die Anforderung zur Bewertung des Penetrationstests ab.
V16.1: Entwurf	Der Anwendungsbesitzer erstellt eine Anforderung und speichert sie als Entwurf, bevor er die Anforderung übermittelt.
status des angreifbaren Anwendungselements	
Öffnen	Wenn das ethische Hacking-Team die Ergebnisse des Penetrationstests identifiziert und erstellt, lautet sein Status „Offen“.
Gelöst	Wenn das Anwendungsteam die Ergebnisse des Penetrationstests löst, wird ihr Status in gelöst verschoben. **Hinweis:** Wenn das Ergebnis des Penetrationstests gelöst wurde, aber noch vom ethischen Hacking-Team validiert werden muss, lautet der Substatus `Validation Pending`.
Geschlossen	Das ethische Hacking-Team validiert, dass die Penetrationstestergebnisse gelöst wurden, und verschiebt den Status in „Geschlossen“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Statuszuordnung für Zurückstellungen und falsch positive Ergebnisse in verwalten Application Vulnerability Response

Sie können verwalten, wie der **Quelle** status für angreifbare Anwendungselemente (Avis), die von importiert wurden Veracode Vulnerability Integration Und Fortify Vulnerability Integration Werden nach dem Import in Ihrer Instanz zugeordnet.

Ab v20.0 von Vulnerability Response, Sie haben weitere Optionen zum Selektieren Ihrer importierten Avis mit ServiceNow Workflows.

Wenn Sie Konfigurieren Sie die Eigenschaften Fortify Vulnerability Integration Oder Konfigurieren Sie die Eigenschaften Veracode Vulnerability Integration, Die Integrationskonfigurationsseiten bieten zwei Optionen, mit denen Sie Ausnahmen und falsch positive Ergebnisse in Ihrer Instanz verwalten können.

- Verwalten Sie Ausnahmen in ServiceNow
- Verwalten Sie falsch positive Ergebnisse in ServiceNow

Erforderliche Rolle: App-Sec-Manager.

Anwendungsfall für Ausnahmemanagement

Avis werden aus diesen Integrationen mit importiert **Quelle** status. Beim Import werden diese Status zugeordnet **Ziel** Und **Zielgrund** status in Ihrer Instanz, da es in einigen Fällen keine genauen Übereinstimmungen zwischen den quellstatus Ihres Scanners und den von Ihrer Instanz verwendeten status gibt.

Zum Beispiel quellstatus wie **Wird Nicht Korrigiert** , **Korrektur Zurückgestellt** , **Risiko Akzeptiert** , Und **Risiko Gemindert** Von Fortify Vulnerability Integration Sind dem zugeordnet **Zurückgestellt** status mit einem Substatus von **Risiko Akzeptiert** Oder **Ausgleichende Kontrolle vorhanden** In Ihrer Instanz.

Sie haben auf den Konfigurationsseiten für diese Integrationen die folgenden Optionen:

Option	Kontrollkästchen ausgewählt	Beschreibung
Verwalten Sie Ausnahmen in ServiceNow	Y (standardmäßig)	Wenn Sie diese Option ausgewählt lassen, müssen Sie Ausnahmen aus AVI-Datensätzen anfordern. Importierte Avis für markiert **Zurückgestellt** status werden mit selektiert ServiceNow Ausnahmemanagement-Workflow. Avis mit **Quelle** status, die normalerweise einem zugeordnet sind **Zurückgestellt** status werden dem zugeordnet **Zielstatus der Selektierung** In **Öffnen** status.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Kontrollkästchen ausgewählt	Beschreibung
	N	Wenn Sie das Kontrollkästchen deaktivieren, behalten Sie bei **Quelle** status, die von Ihrem Scanner importiert wurden. Diese Avis sind dem zugeordnet **Zielstatus** Als **Zurückgestellt** , Und bis **Zielgrund** status in Ihrer Instanz. Sie werden vom Ausnahme-Workflow nicht selektiert, da sie nicht dem zugeordnet sind **Zielselektierung** status und **Zielgrund für Selektierung** status. Die **Ausnahme Anfordern** UI-Aktion ist für den AVI-Datensatz nicht verfügbar, da der Datensatz bereits in enthalten ist **Zurückgestellt** Zielstatus.

Anwendungsfall für falsch positiv

Für falsch positive Ergebnisse von Veracode Vulnerability Integration Beispiel: quellstatus wie **Falsch Positiv** Oder **Potenziell Falsch Positiv** Sind dem zugeordnet **Geschlossen Zielstatus** Mit einem Substatus von **Falsch Positiv** .

Option	Kontrollkästchen ausgewählt	Beschreibung
Verwalten Sie falsch positive Ergebnisse in ServiceNow	Y (standardmäßig)	Wenn Sie diese Option ausgewählt lassen, müssen Sie eine anfordern **Falsch Positiv** Aus AVI-Datensätzen. Importierte Avis für markiert **Falsch Positiv** Oder **Potenziell Falsch Positiv** status werden mit selektiert ServiceNow Ausnahmemanagement-Workflow. Avis mit **Quelle** status, die normalerweise einem zugeordnet sind **Geschlossen Zielstatus** Sind einem zugeordnet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Kontrollkästchen ausgewählt	Beschreibung
		Zielselektierung status in **Öffnen** . Die **Falsch Positiv** Die UI-Aktion ist für den AVI-Datensatz verfügbar.
	N	Wenn Sie das Kontrollkästchen deaktivieren, behalten Sie bei **Quelle** status, die von Ihrem Scanner importiert wurden. Diese Avis sind dem zugeordnet **Zielstatus** Als **Geschlossen** Und ein **Zielgrund** status in **Falsch Positiv** In Ihrer Instanz. Sie werden nicht durch den falsch positiven Workflow selektiert. Die **Falsch Positiv** Die UI-Aktion ist für den AVI-Datensatz nicht verfügbar, da sich der Datensatz bereits in befindet **Geschlossen** Zielstatus.

Application Vulnerability Response Referenzen

Die folgenden Begriffe werden in verwendet Application Vulnerability Response.

Angreifbare Anwendungselemente (Avis)

Paarungen von Schwachstelleneinträgen und potenziell angreifbaren Anwendungen in Ihrer Unternehmensumgebung.

Zuweisungsregeln

Regeln, die zum Zuweisen von Avis basierend auf Ihren definierten Kriterien verwendet werden.

Common Platform Enumeration (CPE)

Ein strukturiertes NIST NVD-Benennungsschema für IT-Systeme, Software und Pakete.

Common Vulnerabilities and Exposures (CVE)

Wörterbuch der öffentlich bekannten Schwachstellen und Risiken im Bereich der Informationssicherheit.

Common Weakness Enumeration (CWE)

Liste der in der Community entwickelten Softwareschwächungstypen.

Integrationen

Geplante Aufgaben, die Berichtsdaten aus CWE oder einem Drittparteisystem abrufen, z. B. Veracode, Um Schwachstellendaten abzurufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn die Integration der NIST National Vulnerability Database in erfolgt Vulnerability Response Ist aktiviert und konfiguriert, CVE-Ergänzung ist für CWEs verfügbar, aber nicht erforderlich. Informationen zur Integration der NIST National Vulnerability Database finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken.

National Vulnerability Database (NVD)

Repository von standardbasierten Schwachstellenverwaltungsdaten der US-Regierung, dargestellt mit dem Security Content Automation Protocol (SCAP).

Nachbesserungszielregeln

Regeln, die verwendet werden, um Avis-Zieldaten für die Korrektur basierend auf Ihren definierten Kriterien zuzuweisen.

Schwachstellen-Rechner

Rechner, die verwendet werden, um Anwendungsschwachstellen basierend auf Ihren definierten Kriterien zu priorisieren und zu kategorisieren.

Beispiel für Ausnahmeregel für Application Vulnerability Response

Eine Beispielregel, die auf einer bekannten Schwachstelle für eine Ausnahmeregel basiert.

Feld	Beschreibung
Name	Ein eindeutiger Name, der Ihnen hilft, den Zweck zu identifizieren und die Regel leicht zu finden, z. B. `Veracode-1 cwe-22-Ausnahme` .
Status	Schreibgeschützt: Entwurf
Gültig ab	Datum, an dem diese Regel aktiv ist, um Avis zurückzustellen.
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausnahmeregel. Ein niedrigerer Wert geht einem höheren voraus.
Gültig bis	Datum, an dem die Korrekturaufgabe keine neuen VIS mehr akzeptiert.
Zurückgestellt bis	Datum, bis zu dem die Korrekturaufgaben und Avis zurückgestellt werden. An diesem Datum wird die AVUL geschlossen, alle Avis werden aus der Aufgabe entfernt und erneut geöffnet. Gruppenregeln werden erneut auf diese Avis angewendet.
Grund	Grund für die Erstellung dieser Ausnahmeregel. Wählen Sie einen aus der Liste aus, z. B. **Korrektur Nicht Verfügbar** .
Zuweisungsgruppe	Gruppe, die für die Nachverfolgung der zurückgestellten VIS zugewiesen ist, z. B. APP SEC Manager.
Zusätzliche Information	Zusätzliche Informationen, die die anfordernde Person dem Genehmiger bereitstellen möchte. Diese Informationen werden im Beschreibungsfeld der Korrekturaufgabe ausgefüllt. In diesem Beispiel `Avis mit der Schwachstelle zurückstellen – Veracode-1-22`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bedingung	Filterbedingungen, um anzugeben, welche Avis mit dieser Regel übereinstimmen. In diesem Beispiel Schwachstelle ist Veracode-1-22 .
Für vorhandene Daten ausführen	Option, mit der Sie diese Regel bei der ersten Ausführung dieser Regel für vorhandene Daten ausführen können. Wenn Sie diese Option deaktiviert lassen, wird Ihre Regel täglich von der geplanten Aufgabe ausgeführt *`Associate existing AVIs with Auto Exception Rule`*Beginnt mit neuen Daten. Wenn Sie die Option für vorhandene Daten ausführen aktivieren, wird eine geplante Aufgabe einmal für die vorhandenen Daten im ausgeführt **Gültig ab** Datum.

Application Vulnerability Response-Produktübersicht

Das Produkt Application Vulnerability Response (AVR) erfasst die von Ihren Tools für Anwendungssicherheitstests erkannten Schwachstellen und Schwachstellen und bietet eine zentrale Übersicht, um die Sicherheitslage aller Anwendungen in Ihrer Umgebung zu verstehen.

Mit AVR können Sie die Risiken mit den Korrektur-Workflows reduzieren. Das Ziel dieser Produktansicht besteht darin, Ihnen zu helfen, zu verstehen, wie wichtige AVR-Entitäten mit dem zentralen CSDM-Framework funktionieren.

Aktualisierte Terminologie

Ab AVR v19.0 wurden die folgenden Schlüsseltabellen- und Spaltennamen aktualisiert. Daher werden in der Dokumentation Verweise auf die älteren und neueren Namen angezeigt.

Aktualisierte Liste der Begriffe, Tabellen- und Feldnamen für AVR

Vor AVR v19.0	Ab AVR v19.0
CI-Suchregeln	Suchregeln
Formular „CI-Suchregel“	Suchregelformular
CI-Übereinstimmungsregel	Übereinstimmungsregel
Tabelle durchsuchen	CI-Tabelle durchsuchen
Feld durchsuchen	CI-Feld durchsuchen
Anwendungs-Release	Erkannte Anwendungen
Anwendungs-Release-Tabelle	Erkannte Anwendungstabelle
Business-Relevanz	Geschäftsrelevanz – Quelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Installieren Sie die neuesten Versionen der folgenden Anwendungen:

- Security Support Common
- Vulnerability Response
- Sicherheits-Integrations-Framework
- Orchestration Des Sicherheitssupports
- Scanner-Integrationen wie Veracode und Fortify

AVR und CSDM 4,0

Vor AVR v19.0 wurde bei der Erfassung von Anwendungsschwachstellen die Anwendung, für die die Schwachstellen erfasst wurden, mithilfe der CI-Suchregeln anhand der gescannten Anwendungen (sn_vul_App_scanned_Application) gesucht. Wenn der Anwendungsnamensdatensatz nicht vorhanden ist, wird ein Eintrag vorgenommen.

Ab AVR v19.0 werden zur Ausrichtung an das CSDM 4,0-Framework die Produktmodelltabellen anstelle der Tabelle „gescannte Anwendungen“ verwendet. Wenn die Anwendung über die Version verfügt, erfolgt die Suche anhand der Tabelle „Softwaremodell“. Wenn keine Version vorhanden ist, erfolgt die Suche anhand der Tabelle „Anwendungsmodell“. Sowohl Anwendungsmodell als auch Softwaremodell sind untergeordnete Tabellen der Tabelle „Produktmodell“, d. h. der Basistabelle in CMDB. Der folgende Screenshot erläutert das Produktmodell.

Systemeigenschaft

Legen Sie die Systemeigenschaft fest, um den auf dem CSDM 4,0-Produktmodell basierenden Suchprozess zu verwenden `sn_vul.use_product_model`Bis `true`.

Überlegungen zu Systemeigenschaften

Name der Systemeigenschaft	Systemeigenschaftswert	Zielwert suchen	Überlegungen
sn_vul.use_product_model	wahr	Wählen Sie den Wert aus **Produktmodell**	Neue Anwender sollten den Wert auswählen **Produktmodell** Dient zur Verwendung der Suchregeln für Produktmodelle des CSDM 4,0-Frameworks.
	falsch	Wählen Sie den Wert aus **Konfigurationselement**	Vorhandene Anwender können den CI-Suchprozess und den vorhandenen weiterhin verwenden **CI-Suchregeln** .

Hinweis:
Um den Suchzielwert festzulegen, navigieren Sie zu **Suchregel** Seite > **[AVR-Integrationssuchregel]** > **Suchziel** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchregeln in AVR

Im CSDM 4,0-Framework werden produktmodellbasierte Suchregeln anstelle von CI-Suchregeln verwendet, um Einträge in den jeweiligen Produktmodellklassen zu erstellen. Ebenso können Sie für Skripts die Suchregeln im Framework des CSDM 4,0-Modells definieren.

Ab AVR v19.0 müssen Sie beim Erstellen einer Suchregel definieren, ob Sie den Konfigurationselement- oder Produktmodellansatz mit verwenden möchten **Suchziel** Feld. Weitere Informationen finden Sie unter Erstellen Sie eine CI-Suchregel.

Erkannte Anwendungen

Navigieren zu **Alle** > **Erkannte Anwendungen**an. In der Tabelle „erkannte Anwendungen“ werden die von den Scannern erfassten Anwendungen angezeigt. Wenn die Systemeigenschaft `sn_vul.use_product_model`Ist auf festgelegt `true`, Sie können die entsprechenden Produktmodelle für die -Anwendungen anzeigen.

Überlegungen zu AVR

Vorhandensein doppelter CI- oder Produktmodell-Datensätze

Überprüfen Sie, ob die Systemeigenschaft vorhanden ist `sn_vul.use_product_model`Wurde für den Suchvorgang ordnungsgemäß konfiguriert. Stellen Sie sicher, dass Sie entweder auswählen **Konfigurationselement** Oder **Produktmodell** Als Suchziel beim Konfigurieren des Suchregelformulars.

Container Vulnerability Response

Die ServiceNow® Container Vulnerability Response Anwendung importiert angreifbare Container-Elemente (CVITs) Und gemäß den Regeln können Sie Container-Schwachstellen beheben. Schwachstellendaten werden aus internen und externen Quellen abgerufen, z. B. aus der National Vulnerability Database (NVD) oder Integrationen von Drittparteien.

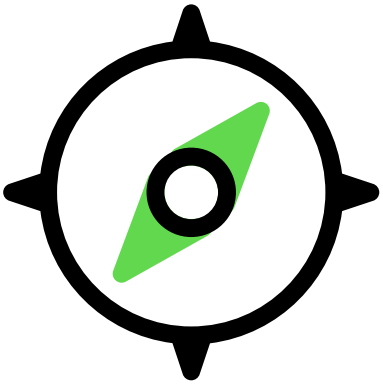
Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

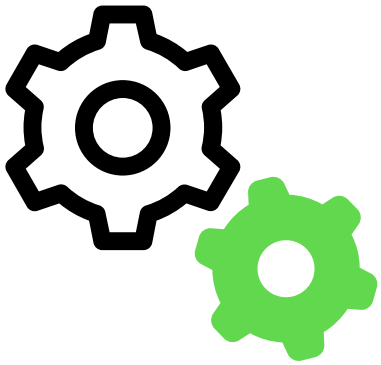
Container Vulnerability Response

Untersuchen



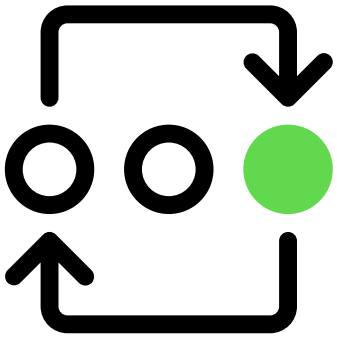
Erfahren Sie mehr über Container Vulnerability Response-Konzepte und -Funktionen.

Konfigurieren



Konfigurieren Sie Container Vulnerability Response.

Integrieren

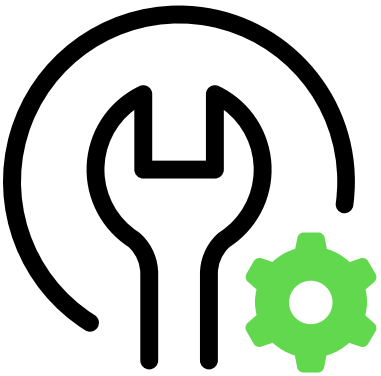


Erweitern Sie Container Vulnerability Response durch Integration mit anderen Anwendungen.

Verwenden Sie die Vulnerability Response-Arbeitsbereiche

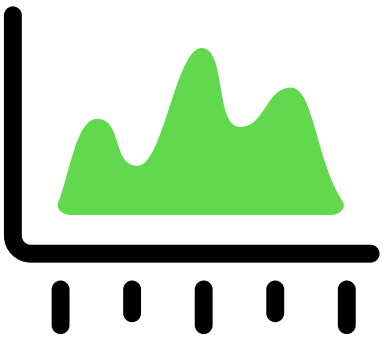
Erfahren Sie, wie Sie CVITs in den Arbeitsbereichen „Schwachstellenmanager“, „IT-Korrektur“ und „Schwachstellenbewertung“ überwachen, verwalten und beheben.

Beheben



Erfahren Sie, wie Sie Container-Schwachstellen beheben können.

Analytics Und Reporting

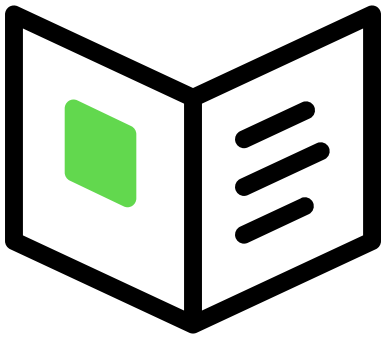


Zeigen Sie Analysen von Container Vulnerability Response an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenz



Rufen Sie Details zu Container Vulnerability Response-Komponenten wie Feldern, Tabellen und Eigenschaften ab.

Vorteile

Die Container Vulnerability Response Die Anwendung bietet die folgenden Vorteile:

- Integration in Container-Sicherheitsprodukte von Drittanbietern, z. B. Prisma Cloud Compute von Palo Alto Networks.
- Importiert Schwachstellendaten für die Images, die zur Laufzeit bereitgestellt werden, und ergänzt die Schwachstellendaten mit Kontextinformationen zur Laufzeit (Hosts, Kubernetes-Cluster, Services und Namespaces).
- Stellt eine Liste der Referenzen bereit, die aus Schwachstellen auf die relevanten Kubernetes-Entitäten in erstellt wurden Configuration Management Database (CMDB) Verwenden ServiceNow Kubernetes-Discovery.
- Bietet ein umfassendes Reporting-Dashboard, das Einblicke in Schwachstellen- und Korrekturtrends bietet.

Schlüsselfunktionen

Die Container Vulnerability Response Die Anwendung verwaltet Schwachstellen, die in den Containern erkannt werden. Es bietet die folgenden Funktionen:

- Zeigen Sie auf das Quell-Docker-Image aus CVITs, anstatt Container auszuführen.
- Konfigurieren Sie die Granularität von CVITs, um sie auf Image-, Kubernetes-Cluster-, Namespace- oder Servicelevel nachzuverfolgen.
- Verfolgen Sie neue Image-Versionen, um behobene Schwachstellen zu identifizieren. Alle in älteren Versionen gemeldeten Schwachstellen werden automatisch in gelöst ServiceNow Wenn neue Image-Versionen zur Laufzeit bereitgestellt werden.
- Verfolgen Sie CVITs in Basis-Images getrennt von Anwendungs-Images, um eine unabhängige Korrektur zu ermöglichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie Ausnahmeanforderungen oder falsch positive Anforderungen, die über einen mehrstufigen Genehmigerprozess überprüft werden können.
- Definieren Sie Ausnahmeregeln, um CVITs automatisch zurückzustellen.

Anwendungsfälle

Container sind eine großartige Möglichkeit, Anwendungen in mehreren Umgebungen mit weniger Overhead und erhöhter Portabilität bereitzustellen und zu skalieren. Schwachstellen in Container-Images können jedoch ein Risiko für den zugrunde liegenden Host und letztendlich für die Infrastruktur darstellen, in der Container von diesen Images gestartet wurden. Es gibt zwar viele Container-Sicherheitsprodukte, die Container-Images auf Schwachstellen scannen, aber es gibt einige Überlegungen und Probleme im Zusammenhang mit der Behebung der Schwachstellen. Container Vulnerability Response Kann bei der Lösung verschiedener Probleme oder Anwendungsfälle helfen, die bei der Behebung von Container-Image-Schwachstellen auftreten. Erkunden Sie, wie Sie die Vorteile von nutzen können Container Vulnerability Response Modul:

Laufzeitkontext

Schwachstellen in Container-Images können erkannt werden, indem das Image in den folgenden Phasen des Anwendungslebenszyklus gescannt wird.

- Phase 1: Wenn Images in der CI/CD-Pipeline erstellt werden.
- Phase 2: Wenn Bilder in der Registrierung veröffentlicht werden
- Phase 3: Wenn Images zur Laufzeit bereitgestellt werden.

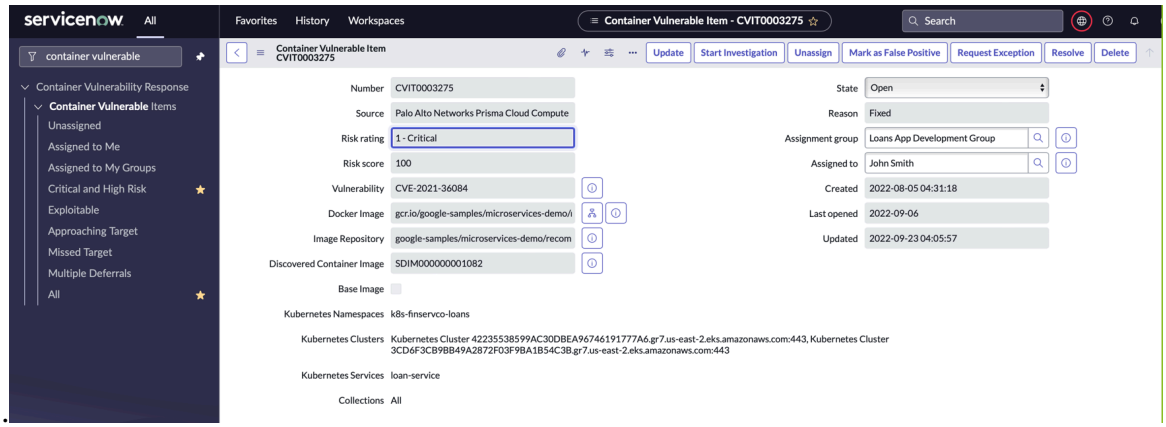
Es ist zwar wichtig, Schwachstellen in Phase 1 und Phase 2 so früh wie möglich zu identifizieren, aber die Durchführung eines Scans für die Images, die in einer Laufzeitumgebung bereitgestellt werden, ist ebenso wichtig. Es bietet die folgenden Vorteile:

- Identifizierung neuer allgemeiner Schwachstellen und Risiken (CVEs), die veröffentlicht wurden.
- Bietet einen genauen Einblick in die Risikosituation bereitgestellter Anwendungen.
- Priorisierung von Schwachstellen, die gelöst werden müssen. Der Laufzeitkontext in Bezug auf die Anwendungsservices oder Business-Services, die aufgrund einer Schwachstelle betroffen sind, kann bei der Priorisierung helfen.

Container Vulnerability Response Integration mit Containersicherheitsprodukten wie Prisma Cloud Compute aus Palo Alto Networks Dient zum Abrufen der Schwachstellendaten für die Images, die zur Laufzeit bereitgestellt werden, und ergänzt die Schwachstellendaten mit den Kontextinformationen zur Laufzeit, z. B. Hosts, Kubernetes-Cluster, Services und Namespaces, auf denen diese Container-Images bereitgestellt werden. Kunden, die verwenden ServiceNow Die Kubernetes-Discovery kann die aus Schwachstellen erstellten Verweise auf die relevanten Kubernetes-Entitäten in ihren anzeigen Configuration Management Database (CMDB). Zusätzlich zur Ergänzung der Metadaten ServiceNow Bietet außerdem ein umfassendes Reporting-Dashboard,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um Einblicke in die Trends bei Schwachstellen und Fehlerkorrekturen zu erhalten.



Identifizieren Sie den Besitz

Voraussetzungen

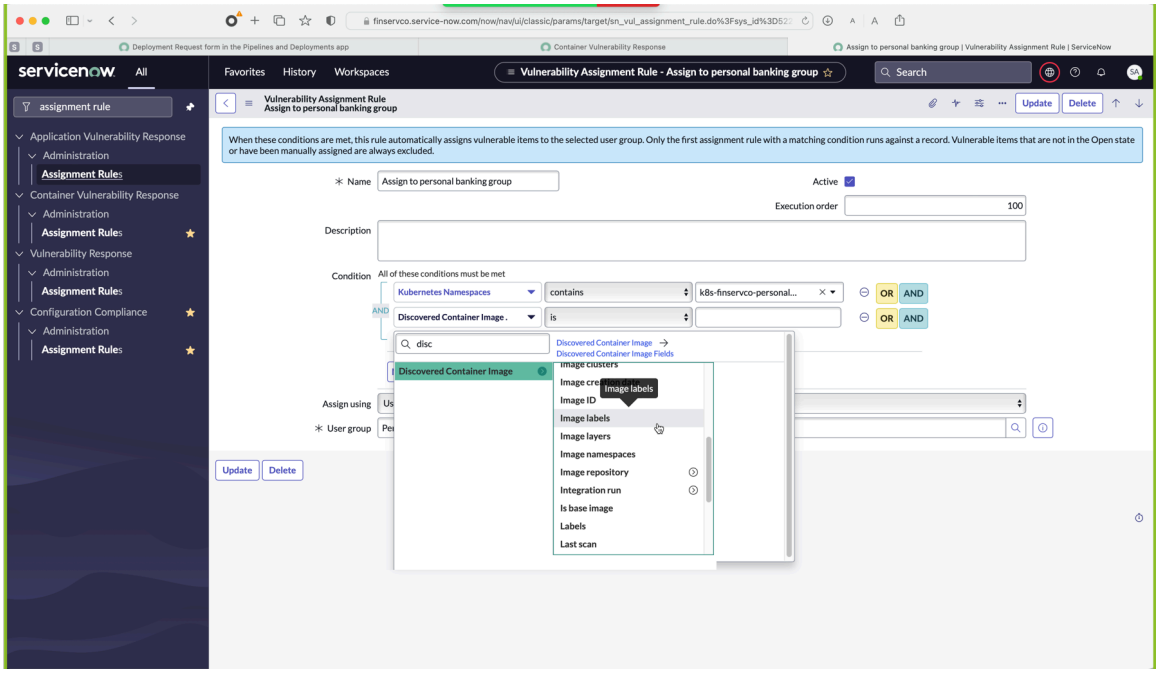
- **Kubernetes-Metadaten und -Referenzen** : Für Container Vulnerability Response Zum Ausfüllen von Kubernetes-Metadaten (Namespace, Cluster usw.) und Verweisen auf Configuration Management Database (CMDB) Einträge, müssen Sie die Kubernetes-Discovery aus implementieren Information Technology Operations Management(ITOM). Die Kubernetes-Discovery füllt das Docker-Image, die ausgeführten Docker-Container, Pods, Kubernetes-Cluster usw. im aus CMDB. Container Vulnerability Response Identifiziert das Docker-Image in CMDB Basierend auf der Image-ID identifiziert und dann die zugehörigen Kubernetes-Entitäten und füllt die Verweise auf diese Entitäten aus angreifbaren Elementen aus.
- **Cloud-Metadaten und Docker-Image-Bezeichnungen** : Container Vulnerability Response Füllt auch Docker-Image-Bezeichnungen, Cloud-Account-IDs und Regionen aus, in denen ein Image bereitgestellt wird. Diese Daten werden im Datensatz „erkanntes Container-Image“ verwaltet, der dem angreifbaren Element zugeordnet ist. Es sind keine Voraussetzungen zum Ausfüllen dieser Daten vorhanden. Container Vulnerability Response Verwendet die Daten, die von Containersicherheitsprodukten (z. B. Palo Alto Prisma Cloud Compute) zurückgegeben werden, um diese Einträge auszufüllen.

Der Besitz für das Patchen einer Schwachstelle in einem Container-Image kann von Organisation zu Organisation variieren. Diese Informationen können an verschiedenen Orten erfasst werden. Einige Organisationen verwenden Docker-Image-Bezeichnungen, um die Anwendungsteams zu identifizieren, die ein bestimmtes Container-Image besitzen, während andere Organisationen den Kubernetes-Namespace oder den Cloud-Account verwenden, in dem ein Container-Image bereitgestellt wird, um den richtigen Besitzer zu identifizieren.

Container Vulnerability Response Stellt die erforderlichen Datenmodellelemente bereit, um die Docker-Image-Bezeichnungen, Kubernetes-Cluster-/Service-/Namespace-Metadaten oder die Cloud-Account-Metadaten (Cloud-Account-ID, Region, Provider usw.) im Modul „Zuweisungsregeln“ erfassen und verwenden zu können und Schwachstellen automatisch dem richtigen Anwendungsteam basierend auf den Metadaten des Image oder der Laufzeitumgebung zuzuweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Verfolgen Sie Schwachstellen in den Basis-Images nach

Voraussetzungen

Für die Eigenschaft „Basisbild“, die in ausgefüllt werden soll Container Vulnerability Response, Basis-Images müssen explizit in konfiguriert werden Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Konsole. Weitere Informationen zum Konfigurieren von Basis-Images in Prisma Cloud finden Sie unter https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-admin- Compute/Vulnerability_Management/Base_images.

Container Vulnerability Response Ermöglicht die Erstellung separater Schwachstellendatensätze für eine Basisebene, damit sie einem anderen Team zugewiesen werden können.

Verfolgen Sie Schwachstellen, die in einem Basis-BS-Image wie Alpine identifiziert wurden, anhand der Schwachstellen, die in anderen Ebenen des Container-Image erkannt wurden. Viele Organisationen verfügen über dedizierte Teams, die dafür verantwortlich sind, Basis-BS-Images zu patchen und für alle Anwendungsteams verfügbar zu machen.

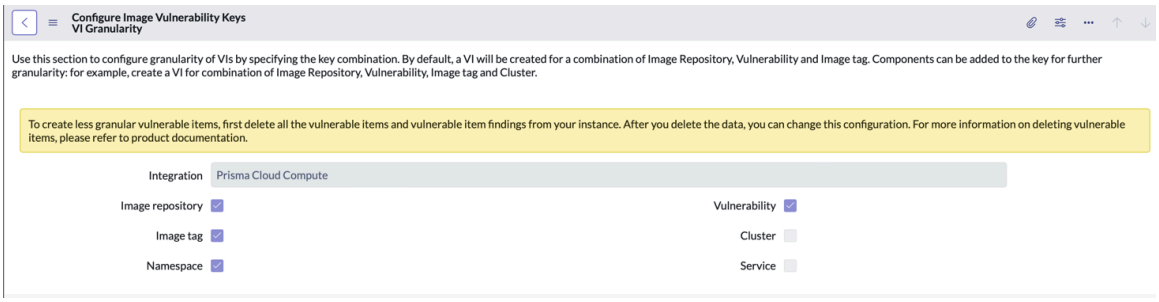
Definieren Sie die Granularität für angreifbare Elemente

Automatische Übersetzung

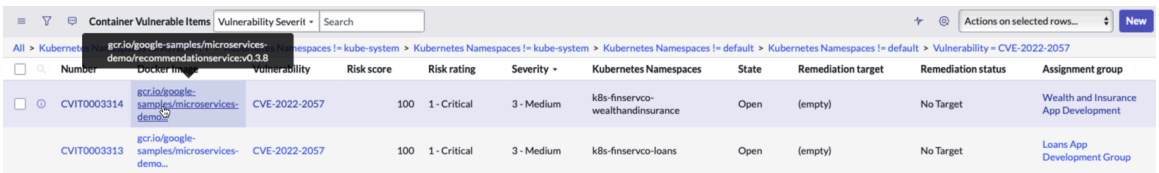
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Konfigurieren Sie die Granularität von CVITs, indem Sie zu navigieren **Alle** > **Container Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**an.



Standardmäßig wird für jede eindeutige Kombination von CVE und Docker-Image-Version (Referenz + Tag) ein angreifbares Element erstellt. Einige Docker-Images können jedoch in mehr als einem Kubernetes-Namespace bereitgestellt werden, und jeder Namespace kann verschiedenen Geschäftsbereichen oder Teams gehören. Jedes Team kann seinem eigenen Rhythmus folgen, um neue Versionen von Container-Images bereitzustellen, um Schwachstellen zu beheben. Um dieses Szenario zu berücksichtigen, Container Vulnerability Response Ermöglicht Ihnen, die Granularität für angreifbare Elemente zu definieren: Ob ein angreifbares Element für jeden Kubernetes-Namespace/Cluster/Service erstellt werden soll, auch für jede eindeutige Kombination aus Docker-Image-Version und Schwachstelle.



Im Beispiel können Sie zwei angreifbare Elemente sehen, die für dieselbe Kombination aus Docker-Image und CVE erstellt wurden. Einer für den Kubernetes-Namespace „k8s-finservco-Darlehen“ und der andere für „k8s-finservco-WealthandInsurance“.

Identifizieren Sie betroffene Services mithilfe der Tag-basierten Service-Identifizierung

Voraussetzungen

- Identifizieren Sie verschiedene Services in Ihrer Anwendung, und definieren Sie die Tags/Schlüssel-Wert-Paare, die diese Services darstellen.
- Stellen Sie Docker-Images und Kubernetes-Pods mit diesen Tags oder Bezeichnungen bereit.
- ITOM-Kubernetes-Discovery bereitstellen Definieren Sie „Tag-basierte Services“ mit den richtigen Tags oder Bezeichnungen.
- Stellen Sie ITOM Kubernetes Discovery bereit
- Definieren Sie „Tag-basierte Services“ mit den richtigen Tags oder Schlüssel-Wert-Paaren.
- Importieren Sie Schwachstellendaten in ServiceNow Verwenden Container Vulnerability Response

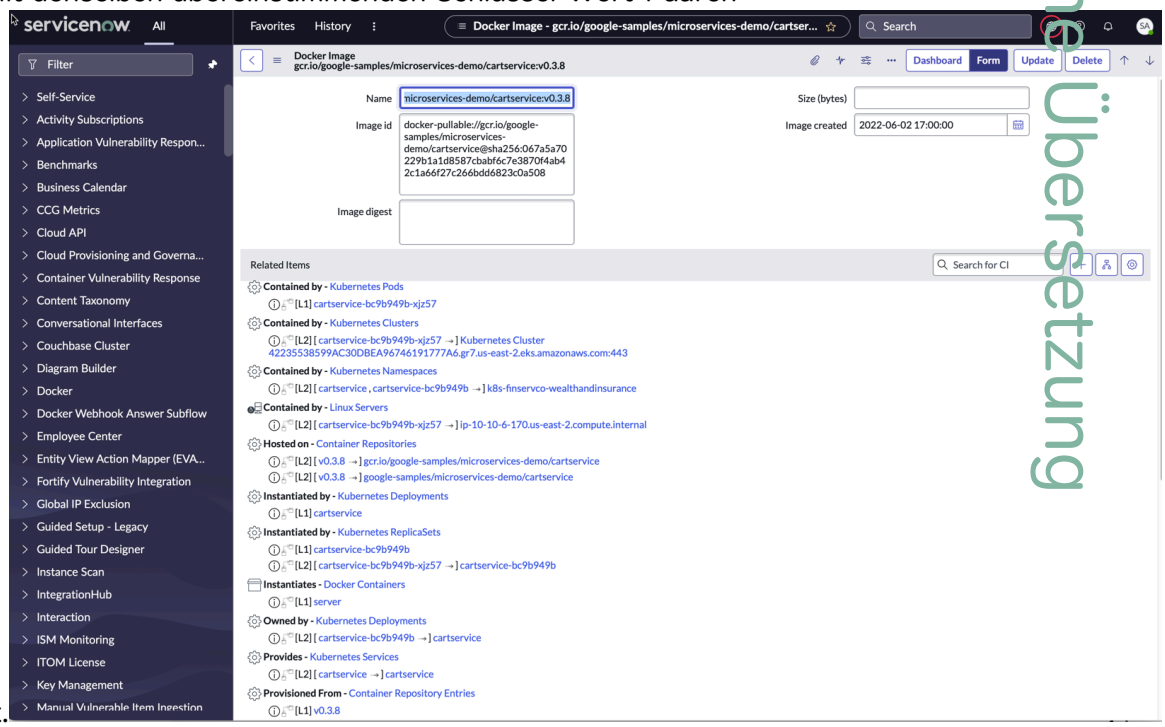
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Risikoberechnung für angreifbare Elemente kann durchgeführt werden, indem das CI (Docker-Image) und die Relevanz der zugehörigen Services in betrachtet werden CMDB. Um jedoch die Identifizierung betroffener Services zu erleichtern, Container Vulnerability Response Bietet Tag-basierte Service-Identifizierung.

Wenn Kubernetes-Pods oder -Entitäten mit Schlüsselwerten oder Bezeichnungen veröffentlicht werden, die den in einem beliebigen Tag-basierten Service in definierten Schlüsselwerten entsprechen ServiceNow, Container Vulnerability Response Stellt automatisch die Beziehung zwischen einem Docker-Image und dem betroffenen Anwendungsservice her und verwendet die Relevanz dieses Anwendungsservice bei der Risikoberechnung.

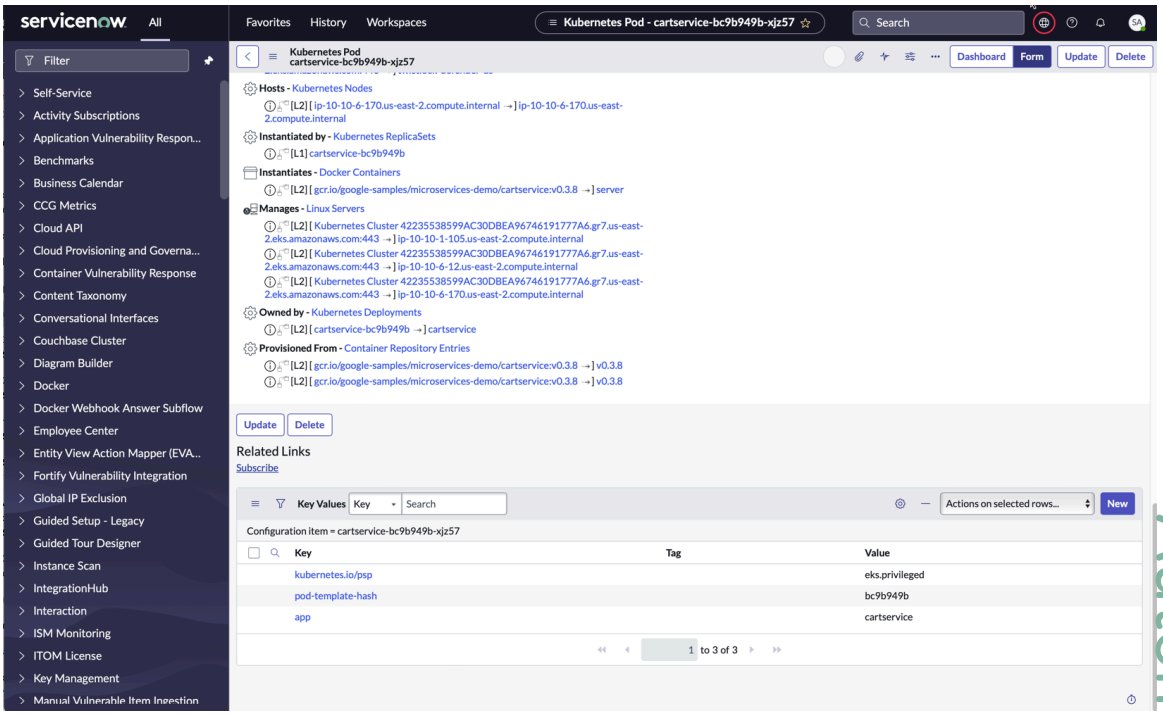
Der Flow lautet wie folgt:

1. Container Vulnerability Response Importiert Schwachstellendaten aus dem Container-Sicherheitsprodukt.
2. Für jedes angreifbare Container-Element Container Vulnerability Response Füllt das Docker-Image aus CMDB Das hat die Schwachstelle.
3. Container Vulnerability Response Betrachtet dann die Docker-Image-Bezeichnungen oder die Bezeichnungen/Schlüsselwerte, die mit Kubernetes-Pods veröffentlicht wurden, auf denen dieses Image bereitgestellt wird. Dieses Bild ist in verfügbar CMDB Wenn die Kubernetes-Discovery ausgeführt wird.
4. Container Vulnerability Response Sucht dann in nach „Tag-basierte Services“ CMDB Mit denselben übereinstimmenden Schlüssel-Wert-Paaren definiert.

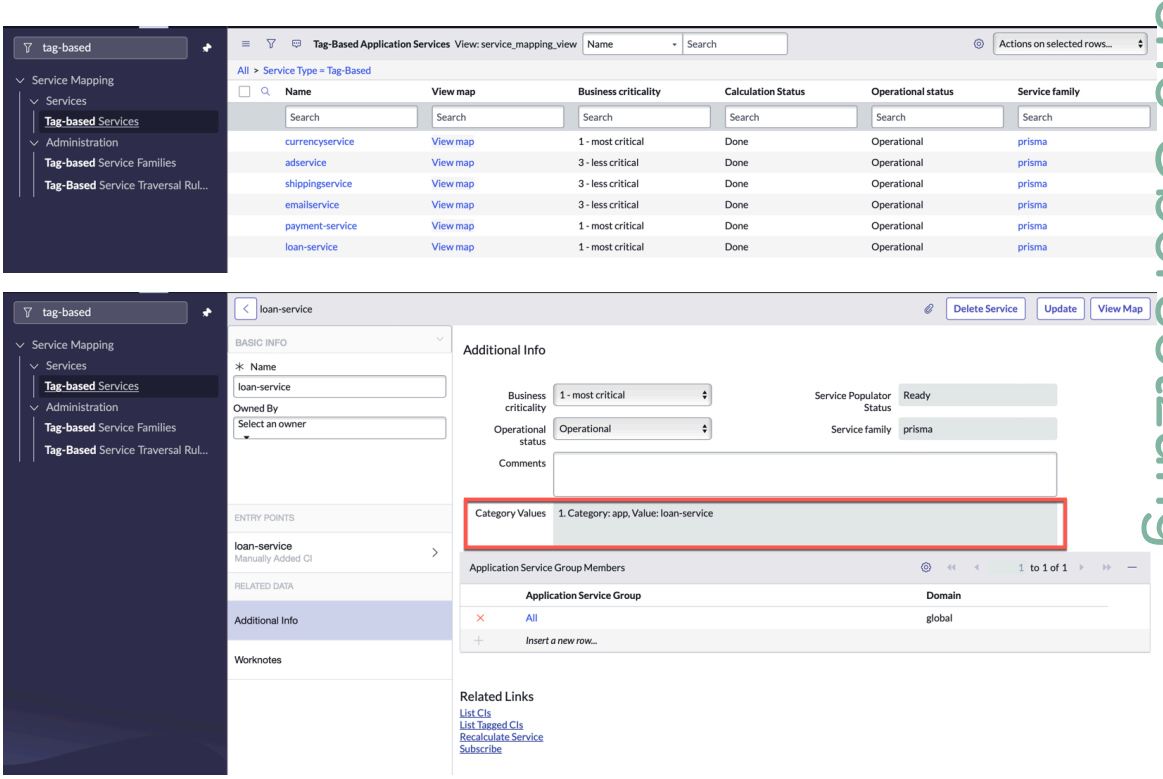


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Container Vulnerability Response Verwendet die „Geschäftsrelevanz“ des übereinstimmenden „Tag-basierten Service“ (falls vorhanden), um das Risiko eines angreifbaren Containerelements zu berechnen.



Automatische Übersetzung

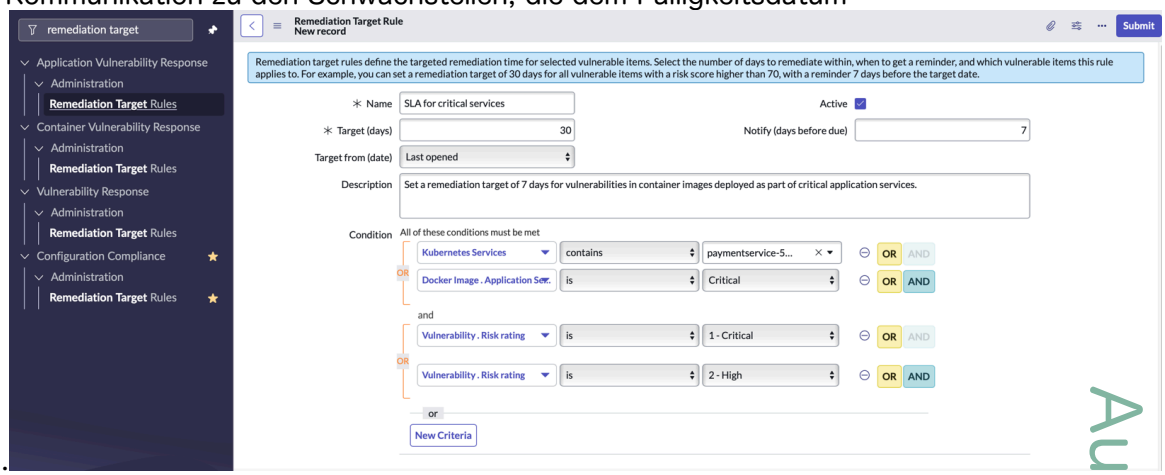
Nachverfolgung Von Schwachstellen

Korrekturziele werden festgelegt

ServiceNow Ermöglicht Schwachstellenmanagern die Definition von „Korrekturzielregeln“, um Servicelevel-Vereinbarungen (Service Level Agreements, SLAs) zur Behebung von Schwachstellen in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Container-Images zu definieren. Das Korrekturzieldatum kann basierend auf einer Bedingung/einem Kriterium für Bildmetadaten oder Schwachstelleninformationen definiert werden. Korrekturbesitzer erhalten E-Mail-Kommunikation zu den Schwachstellen, die dem Fälligkeitsdatum nähern.



Identifizierung behobener Schwachstellen

Im Gegensatz zu Host-Schwachstellen, die durch das Anwenden eines Patches auf einem Host behoben werden können, können Container-Schwachstellen nicht gepatcht werden. Neue Versionen von Container-Images müssen erstellt und bereitgestellt werden, um die älteren Versionen zu ersetzen. Die neuen Versionen haben einen anderen Bezeichner (Image-ID) als die vorherigen Versionen, was es schwierig macht, nachzuverfolgen, welche Schwachstellen bereits behoben wurden.

ServiceNow Identifiziert Schwachstellen, die in den vorherigen Versionen der Container-Images gemeldet wurden, aber in der neuesten Version des Image gelöst wurden, und verschiebt diese Schwachstellen automatisch in den Status „Geschlossen/behoben“, damit Sicherheitsteams immer genaue Einblicke in die aktuelle Risikolage haben.

Ausnahmen verwalten

Anwendungsteams oder Korrekturbesitzer für die Schwachstellen benötigen möglicherweise die Möglichkeit, aus den folgenden Gründen eine Ausnahme anzufordern.

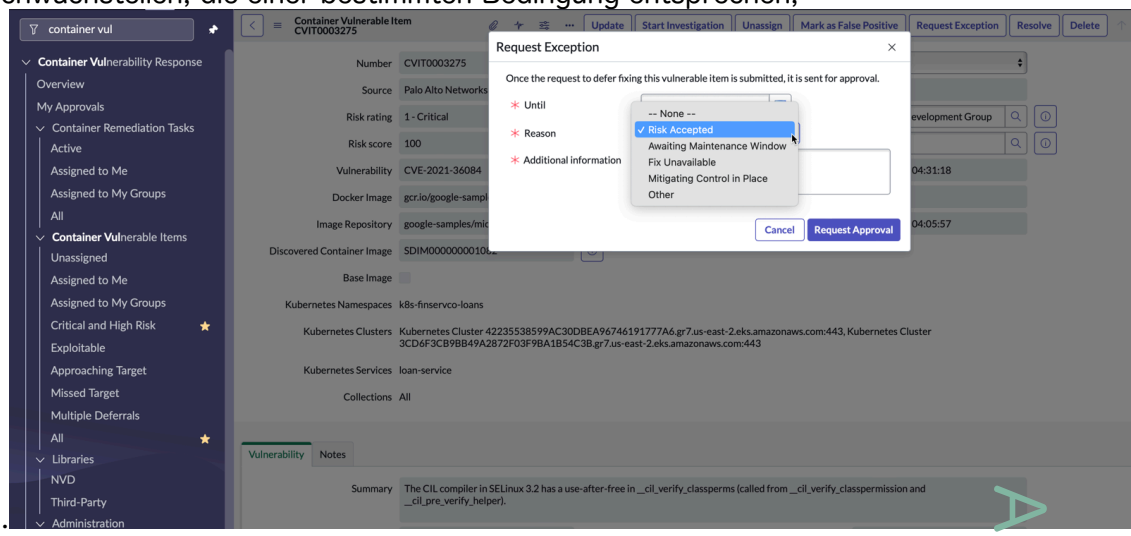
- Eine Minderungssteuerung ist bereits vorhanden
- Risiko akzeptiert
- Warten auf Wartungsfenster, um die Korrektur zu verschieben.

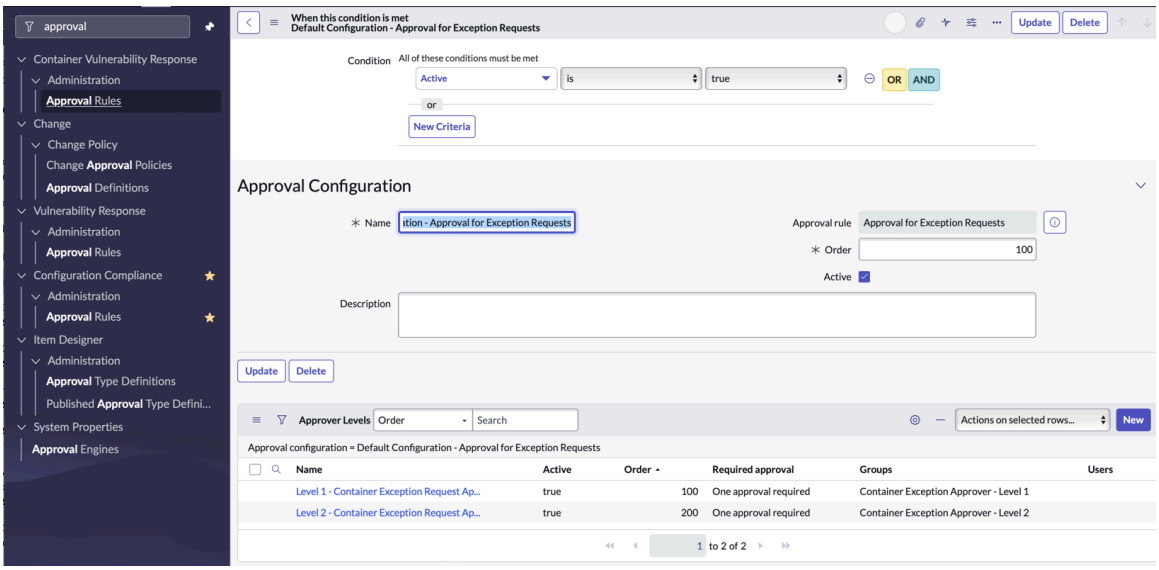
ServiceNow Ermöglicht Sicherheitsadministratoren das Definieren mehrerer Genehmigerebenen für Ausnahmeanforderungen. Sie können auch automatische Ausnahmeregeln definieren, die verwendet werden können, um

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

automatisch Schwachstellen, die einer bestimmten Bedingung entsprechen, aufzuschieben.





Neuigkeiten

Um mehr darüber zu erfahren, was in neu ist und was geändert wurde Yokohama, Siehe Yokohama Versionshinweise.

Erste Schritte

- Für eine Übersicht über Security Operations In Ihrem ServiceNow AI Platform Instanz, siehe Erläuterungen Zu Security Operations .
- Für Informationen zu allen Security Operations Anwendungen, die über heruntergeladen werden können ServiceNow Store, Siehe Security Operations und ServiceNow Store .

Container Vulnerability Response erkunden

Die Container Vulnerability Response Anwendung importiert angreifbare Container-Elemente (CVITs). Gemäß den Regeln können Sie mit der Funktion die Container-Schwachstellen beheben. Container Vulnerability Response Ist über ein separates Abonnement verfügbar.

Im Gegensatz zu herkömmlichen Anwendungen paketieren Container alle Anwendungsquellcodes zusammen mit ihren Abhängigkeiten in einer Binärdatei, die als Container-Image bezeichnet wird. Das Image wird in einer Registrierung veröffentlicht, um

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Option zur Ausführung dieses Image als Anwendung oder Containerinstanz auf einer beliebigen Plattform bereitzustellen. Die Phasen in einem Container-Lebenszyklus vor der Bereitstellung lauten wie folgt:

1. Container-Image verfassen: Das Container-Image wird erstellt und verweist auf einen Quellcode oder eine abhängige Bibliothek.
2. Containerimage erstellen
3. Container-Image veröffentlichen: Die Container-Image-Datei wird in einer Registrierung veröffentlicht. Jedes Bild hat eine eigene eindeutige ID basierend auf dem Inhalt des Bilds. Diese Images werden nach der Bereitstellung aus der Registrierung in die Laufzeitumgebung abgerufen. Die Images werden dann als Containerinstanzen auf dem Host in der Produktionsumgebung ausgeführt.

Container-Images werden gescannt

Ein Container-Image kann entweder vor oder nach der Bereitstellung auf Schwachstellen gescannt werden. Wenn Container-Images während der Phase vor der Bereitstellung gescannt werden, erhalten Sie möglicherweise viele Schwachstellenwarnungen, die möglicherweise nicht sofort Ihre Aufmerksamkeit erfordern. Das Scannen auf Schwachstellen während der Phase nach der Bereitstellung bietet jedoch größere Vorteile, z. B. die folgenden:

- Transparenz des mit den bereitgestellten Anwendungen verbundenen Risikos.
- Bietet eine fokussierte Ansicht nur auf die Images in der Produktionsumgebung.
- Identifizierung und Priorisierung der Schwachstellen, auf die sofort reagiert werden muss.
- Gruppierung und Zuweisung von Schwachstellen basierend auf den Metadaten des Bilds. Zum Beispiel können ein Bild-Repository, eine Image-Bezeichnung und andere Attribute im Zusammenhang mit dem Container-Image für Gruppierungs- und Zuweisungsregeln verwendet werden.

Jedes Container-Image enthält die folgenden Schlüsselkomponenten:

- Container oder Image-Repository: Stellt das Docker-Image mit einem bestimmten Repository oder Namen dar. Er hostet alle Versionen des Image.
- Docker-Image: Stellt eine bestimmte Version des Build-Docker-Images dar.
- Docker-Container: Stellt eine laufende Instanz des Docker-Images dar. Jede Version hat eine eindeutige ID und mehrere Instanzen der Container, die in der Produktionsumgebung ausgeführt werden.

Container Vulnerability Response Module

Die Container Vulnerability Response Das Modul enthält Details zu folgenden Themen:

Angreifbare Container-Elemente

Die angreifbaren Container-Elemente (CVITs) werden basierend auf Zuweisung, Relevanz, Ausnutzbarkeit und Korrekturstatus gruppiert und aufgelistet.

Bibliotheken

Erhalten Sie Zugriff auf die National Vulnerability Database (NVD) und Bibliotheken von Drittanbietern. Während die NVD-Bibliothek Informationen enthält, die auf die ID des Schwachstellenelements beschränkt sind, enthält die Drittparteibibliothek die meisten Details zu einem Schwachstellenelement. Informationen im NVD-Bildschirm werden nur ausgefüllt, wenn die NVD-Integration ausgelöst wird.

Administration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Administrationsmodul enthält Informationen zu den Zuweisungsregeln der angreifbaren Elemente, Korrekturzielregeln und Container-Schwachstellenintegrationen. Darüber hinaus können Sie auch die Dauer konfigurieren, nach der ein angreifbares Element automatisch geschlossen werden soll. Sie können den Abschnitt VI-Granularität konfigurieren verwenden, um die Granularität von CVITs zu konfigurieren, indem Sie die Schlüsselkombinationen angeben. Standardmäßig wird ein CVIT für eine Kombination aus einem Image-Repository, einem Image-Tag und einer Schwachstelle erstellt. Sie können dem Schlüssel zusätzliche Komponenten hinzufügen, um eine weitere Granularität zu erzielen. Sie können beispielsweise ein CVIT für eine Kombination aus Image-Repository, Image-Tag, Schwachstelle und Cluster erstellen.

Verfügbare Versionen

Freigabeversion	Release-Hinweise
Container Vulnerability Response v2.1 Container Vulnerability Response v 2,06 Container Vulnerability Response V2.0.4	Release-Hinweise für Container Vulnerability Response Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema .

Container Vulnerability Response status der Korrekturaufgabe und des angreifbaren Containerelements

Mit Container Vulnerability Response Anwendung können Sie das Statusmodell verwenden, um den Status einer Korrekturaufgabe jederzeit anzuzeigen. Wenn Sie wissen, wie sich die einzelnen Status zueinander beziehen und sich gegenseitig auswirken, können Sie bestimmen, wann und wie Sie Ihre angreifbaren Container-Elemente (CVITs) beheben können.

status der Korrekturaufgabe

Komplexe Anwendungsfälle können manchmal dazu führen, dass sich ein angreifbares Container-Element in einem anderen Status befindet als seine Korrekturaufgabe. Das Verständnis der Funktionsweise von status hilft bei der Erklärung dieses Verhaltens und kann beim Erstellen von Korrekturaufgaben und beim Erstellen oder Bearbeiten von Regeln für Korrekturaufgaben helfen.

Korrekturaufgaben haben viele mögliche status, wie im folgenden Diagramm dargestellt.

Container Vulnerability Response-Status-Flow

Hinweis:

- Angreifbare Container-Elemente können nicht manuell geschlossen werden.
- Jedes Aufgabenformular enthält **Folgen** Und **Aktualisieren** Schaltflächen, die Standard für sind ServiceNow Aufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturaufgabe und CVIT-Statusübergang und Rangfolge

Korrekturaufgaben und status angreifbarer Elemente können sich gegenseitig beeinflussen. Meistens aktualisiert ein Korrekturaufgabenstatus den Status des angreifbaren Elements, wobei der Aufgabenstatus mit der höchsten Priorität zum Aktualisieren der angreifbaren Elemente in der Gruppe verwendet wird.

Von der Erstellung bis zum Abschluss einer Container-Korrekturaufgabe durchläuft sie während des gesamten Korrekturprozesses verschiedene status.

Die Statuspriorität lautet wie folgt:

Geschlossen > **Zurückgestellt** > **Gelöst** > **Wird überprüft** > **Warten auf Implementierung** > **Wird untersucht** > **Öffnen**

Der Statusübergang geschieht, wenn Sie verschiedene Aktionen ausführen, z. B. Zurückstellen, Öffnen, Schließen usw.

Die Aktionen, die Sie für eine Container-Korrekturaufgabe in einem bestimmten Status ausführen können, ähneln denen einer Host-Korrekturaufgabe. Daher finden Sie weitere Informationen unter Vulnerability Response status der Korrekturaufgabe Und Status-Rollup- und Rollup-Szenarien In Vulnerability Response Dokumentation.

Container Vulnerability Response konfigurieren

Bevor Sie ausführen Container Vulnerability Response In Ihrem ServiceNow AI Platform Instanz, müssen Sie sie konfigurieren.

Vulnerability Response und Configuration Compliance für Container installieren

Bevor Sie ausführen Vulnerability Response und Configuration Compliance für Container Anwendung in Ihrem ServiceNow AI Platform Instanz müssen Sie die Berechtigung abrufen und die Anwendung aus herunterladen ServiceNow Store. Installieren Sie die Anwendung auf Ihrem ServiceNow AI Platform Und führen Sie einige Installationsschritte im Setup-Assistenten aus.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob die Anwendung installiert und aktiviert ist.	Navigieren Sie zu , um zu überprüfen, ob sie aktiviert ist **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Wenn die Anwendung nicht installiert und aktiviert ist, siehe , Vulnerability Response installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen, die Ihrer Instanz zugewiesen sind.	Die Administratorrolle ist für die Installation erforderlich. Wenn nicht bereits zugewiesen, weist der Systemadministrator [admin] auch die Rolle Schwachstellenadministrator, sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)] zu.

Erforderliche Rolle: Administrator

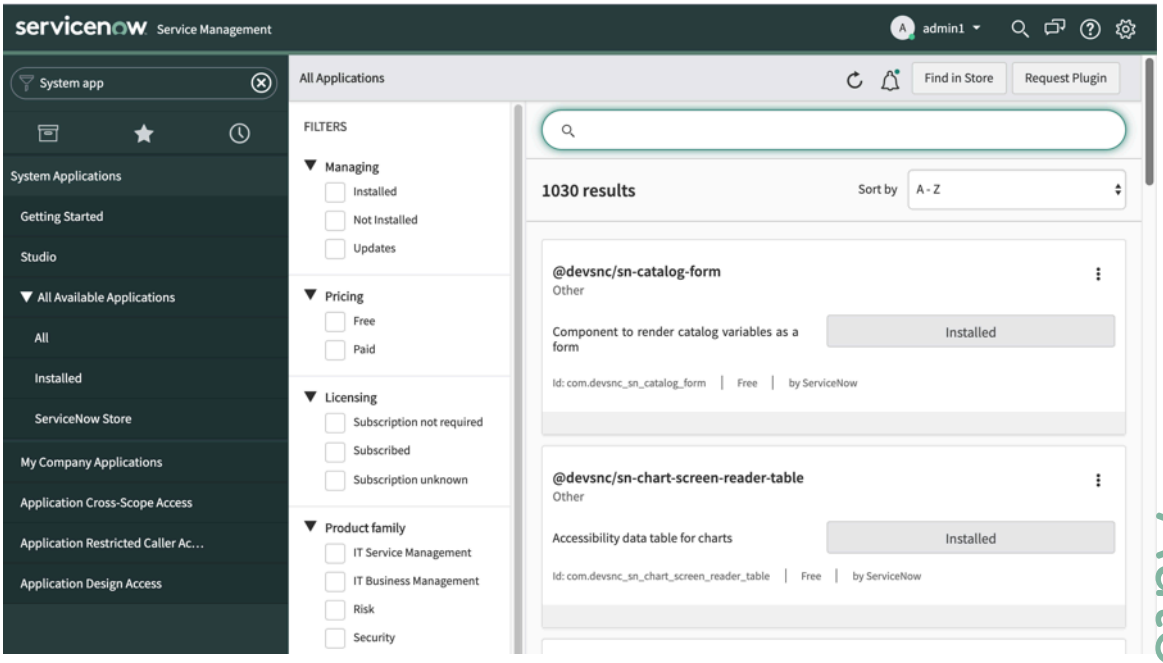
Prozedur

1. Um die Berechtigung abzurufen und herunterzuladen Vulnerability Response und Configuration Compliance für Container Anwendung, navigieren Sie zu ServiceNow Store.
2. Klicken Sie oben rechts auf der Seite auf **Melden Sie Sich An** .
3. Geben Sie in der Suchleiste ein Vulnerability Response und Configuration Compliance für Container.
4. Klicken Sie unter Apps und Lösungen auf Vulnerability Response und Configuration Compliance für Container Kachel.

5. Klicken Sie auf **Installation anfordern**.
6. Melden Sie sich bei an ServiceNow AI Platform Instanz, in der Sie installieren möchten Vulnerability Response und Configuration Compliance für Container Anwendung auf.
7. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Suchen Sie in den aufgeführten Anwendungen nach Vulnerability Response und Configuration Compliance für Container Anwendung, wählen Sie eine Version aus der Liste aus, und klicken Sie auf **Installieren** . Das Dialogfeld Anwendungsinstallation wird angezeigt. Alle installierten Abhängigkeiten werden angezeigt.
9. Klicken Sie auf **Schließen**.

Definieren Container Vulnerability Response E-Mail-Benachrichtigungen

Richten Sie E-Mail-Benachrichtigungen ein, um nützliche Informationen zu wichtigen Updates und Aktivitäten wie Genehmigung und Ablehnung falsch positiver Anforderungen zu teilen. Beim Erstellen einer E-Mail-Benachrichtigung wird angegeben, wann sie gesendet werden soll, wer sie erhält und was sie enthält.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **E-Mail-Vorlagen**an.
2. Wählen Sie **Neu**.

   Detaillierte Anweisungen zum Erstellen von E-Mail-Benachrichtigungen finden Sie unter Create an email notification .

Ergebnisse

Ab v21.0 von Vulnerability Response, Wenn ein Empfänger auf die Links in einer E-Mail-Benachrichtigung klickt, werden die Datensätze im geöffnet Arbeitsbereich des Schwachstellenmanagers Oder Arbeitsbereich für IT-Korrekturen Basierend auf ihrer Rolle.

- Links werden in geöffnet Arbeitsbereich des Schwachstellenmanagers Für Anwender mit den Rollen: sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin .
- Links werden in geöffnet Arbeitsbereich für IT-Korrekturen Für Anwender mit Rollen: sn_vul_Container.Remediation_owner .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Empfänger keine der vorherigen Rollen hat, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Erstellen oder bearbeiten Sie Benachrichtigungen zu Korrekturzielen

Schwachstellenadministratoren können die Korrekturzielbenachrichtigung bearbeiten oder neue hinzufügen, indem sie angeben, wann die Benachrichtigung gesendet werden soll, wer die Benachrichtigung erhält und welchen Inhalt die Benachrichtigung enthält.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Benachrichtigungen**an.
2. Wählen Sie den Benachrichtigungsdatensatz für das Korrekturziel aus, oder wählen Sie aus **Neu** .
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Create an email notification .
4. Wählen Sie Aus **Vorschau Der Benachrichtigung Anzeigen** Zum Anzeigen der Nachricht.

Ergebnisse
Ab v21.0 von Vulnerability Response, Wenn ein Empfänger auf die Links in einer E-Mail-Benachrichtigung klickt, werden die Datensätze im geöffnet Arbeitsbereich des Schwachstellenmanagers Oder Arbeitsbereich für IT-Korrekturen Basierend auf ihrer Rolle.

- Links werden in geöffnet Arbeitsbereich des Schwachstellenmanagers Für die Anwender mit den Rollen: sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin .
- Links werden in geöffnet Arbeitsbereich für IT-Korrekturen Für Anwender mit Rollen: sn_vul_Container.Remediation_owner .

Wenn der Empfänger keine der vorherigen Rollen hat, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Konfigurieren Sie das Ausnahmemanagement für Container Vulnerability Response

Begrenzen Sie die Dauer einer angeforderten Ausnahme Und fügen Sie der Anforderung „Ausnahme“ oder „falsch positiv“ einen Fragebogen hinzu Mit Container Vulnerability Response Modul. Standardmäßig wird mit eine Ausnahme angefordert ServiceNow® Container Vulnerability Response Modul. Sie können auch eine Ausnahme mit anfordern GRC: Richtlinien- und Compliance-Management Integration.

Vorbereitungen
Erforderliche Rolle: sn_vul_Container.Manage_Exception_Configuration

Warum und wann dieser Vorgang ausgeführt wird
Wenn Container Vulnerability Response Ist aktiviert, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ähnlich, wenn GRC: Richtlinien- und Compliance-Management Modul ist installiert. Sie können auswählen GRC: Richtlinien- und Compliance-Management Auf dem Konfigurationsbildschirm. Durch Aktivieren dieser Option können Sie eine Ausnahme anfordern, die das Richtlinien- und Kontrollziel von angibt GRC.

Wenn Sie einen Fragebogen hinzufügen, wird er an die Person gesendet, die die Ausnahme oder falsch positive Anforderung stellt. Sie können entweder den Standardfragebogen verwenden oder einen basierend auf Ihren Anforderungen erstellen. .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für die Anforderung der Ausnahme zu verstehen.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmenverwaltung**an.
2. Auf der **Ausnahmeverwaltungskonfiguration** Wählen Sie aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option aus dem auswählen **Verwalten Sie Ausnahmen mit** Liste.
   Sie können entweder auswählen Vulnerability Response Oder GRC: Richtlinien- und Compliance-Management.
3. Wenn Sie ausgewählt haben Vulnerability Response Option: Geben Sie die folgenden Informationen ein:

Vulnerability Response Felder

Feld	Beschreibung
Dauer	Zeitraum, für den eine Ausnahme angefordert werden kann.
Einheit	Zeiteinheit für den angegebenen Zeitraum.
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur falsch positiven Anforderung, die ausgelöst wird.
Fragebogen aktivieren, um Ausnahme anzufordern	Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung.
Fragebogen, um Ausnahme anzufordern	Zeigt den von Ihnen ausgewählten Fragebogen an, um eine Ausnahme anzufordern. Standardmäßig wird der Ausnahmefragebogen angezeigt.

Hinweis:
Wenn Sie auswählen GRC: Richtlinien- und Compliance-Management, Die Felder Dauer und Einheit werden als ausgeblendet Governance, Risk und Compliance Verarbeitet diesen Flow.

4. Wählen Sie **Speichern**.

Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement

Beginnend mit Vulnerability Response V15.0: Verwenden Sie den Flow Designer, um Ausnahmeanforderungen für das Ausnahmemanagement, Ausnahmeregeln und die Verwaltung von falsch positiven Werten zu genehmigen. Wenn Sie bereitstellen Vulnerability Response(VR) zum ersten Mal ist der Flow Designer standardmäßig aktiviert.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmemanagement-Workflows konfigurieren.

- Ausnahmeanforderung für Korrekturaufgaben
- Ausnahmeanforderung für angreifbare Container-Elemente
- Ausnahmeregel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Falsch positiv für Korrekturaufgaben
- Falsch positiv für angreifbare Container-Elemente

Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den übereinstimmenden Genehmigungs-Workflow.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Genehmigungsregeln**an.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie im Formular die Felder aus.

Formular „Genehmigungsregel“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.
Tabelle	Tabelle, auf die die Regel angewendet wird.
Anwendung	Der Standardwert ist Vulnerability Response.
Regeltyp	Gibt den Regeltyp an. Zum Beispiel Ausnahmeverwaltung, falsch positiv oder Ausnahmeregel.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird.
Beschreibung	Kurzbeschreibung der Genehmigungsregeln.
Genehmigung läuft ab y (Tage) Ab v2.5 von Container Vulnerability Response	Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann.
Genehmiger benachrichtigen (Tage) Ab v2.5 von Container Vulnerability Response	Datum, nach dem der Genehmiger benachrichtigt wird, Maßnahmen zu ergreifen.

4. Wählen Sie **Aktualisieren**.
   Auf der Registerkarte „Genehmigungskonfigurationen“ sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren. Weitere Informationen finden Sie unter Erstellen Sie Konfigurationen für eine Genehmigungsregel.

Hinweis:
Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen. Weitere Informationen finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement.

Example:
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Schwachstellen definieren, die in verschiedenen Konfigurationselementen gefunden werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schnellstarttests für Container Vulnerability Response

Überprüfen Sie, ob Container Vulnerability Response immer noch funktioniert, nachdem Sie eine Konfigurationsänderung vorgenommen haben, z. B. Anwendung eines Upgrades oder Entwickeln einer Anwendung. Kopieren Sie diese Schnellstarttests und passen Sie sie an, um sie bei der Verwendung Ihrer instanzspezifischen Daten zu übergeben.

Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder Demoaccounts erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz in nicht-Produktion oder Produktion verwendet wird. Siehe Führen Sie die Test-Suite für Automated Test Framework (ATF) aus Vulnerability Response Weitere Informationen zum Einrichten und Ausführen der Test-Suite für Container Vulnerability Response.

Container Vulnerability Response-Schnellstarttests erfordern die Aktivierung der Anwendung Container Vulnerability Response (sn_vul_container).

Container Vulnerability Response-Tests

Test	Beschreibung	Release-Version
CVR: Zuweisungsregeln	Ermittelt, ob angreifbare Elemente in Containern mit einem Mustersatz von Zuweisungsregeln zur Korrektur erfolgreich automatisch einer Zuweisungsgruppe zugewiesen werden können.	Vancouver
CVR: Ausnahmeregel	Testet Ausnahmeregeln.	Vancouver
CVR: Flow „Als falsch positiv markieren“	Testet, ob der Flow „Als falsch positiv markieren“ für das angreifbare Container-Element funktioniert.	Vancouver
CVR: Korrekturzielregeln	Erstellt eine Fehlerkorrektur-Zielregel.	Vancouver
CVR: Flow „Ausnahmeanforderung“	Testet, ob der Flow „Ausnahmeanforderung“ wie erwartet funktioniert.	Vancouver
CVR: Schwachstellen-Rechner	Testen Sie die Schwachstellen-Rechner des Containers.	Vancouver

Zugehörige Informationen

Schnellstarttests

Führen Sie die Test-Suite für Automated Test Framework (ATF) aus Container Vulnerability Response

Führen Sie die Testsuite Automated Test Framework (ATF) aus, nachdem Sie installiert oder aktualisiert haben Container Vulnerability Response Anwendung.

Vorbereitungen

Bestätigen Sie eine erfolgreiche Installation und dass Ihre Instanz wie geplant funktioniert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Testausführungseigenschaft ist standardmäßig deaktiviert, um zu verhindern, dass Tests auf einem Produktionssystem ausgeführt werden. Führen Sie Tests nur für Entwicklungs-, Test- und andere Nicht-Produktionsinstanzen aus. Wenn Demodaten oder Demoaccounts erstellt werden, sollten alle Demodaten entfernt werden, bevor die Instanz in nicht-Produktion oder Produktion verwendet wird.

- Führen Sie die folgenden Schritte aus, um den Test zu aktivieren:
  1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Administration** > **Eigenschaften**an.
  2. Wenn nicht ausgewählt, wählen Sie aus **Aktivieren Sie die Ausführung der Test-/Test-Suite** Kontrollkästchen.
  3. Klicken Sie auf **Speichern**.
  4. Wenn der Bereich nicht auf festgelegt ist **Container Vulnerability Response** Klicken Sie im Header oder im Header nicht der Bereich angezeigt wird, auf das Einstellungssymbol.
  5. Klicken Sie im Fenster Systemeinstellungen auf **Entwickler** .
  6. Wenn nicht ausgewählt, klicken Sie auf **Anwendungsauswahl im Header anzeigen** Und schließen Sie das Fenster.
  7. In der Liste, die neben angezeigt wird Systemadministrator , Klicken Sie auf **Container Vulnerability Response** Für das Feld.

Erforderliche Rolle: admin oder atf_test_admin

Prozedur

1. Navigieren zu **Alle** > **Automated Test Framework (ATF)** > **Tests**an.
2. Suchen Sie in der Paketliste nach **Vulnerability Response und Konfigurations-Compliance für Container** .
3. Wählen Sie einen Test aus, um den Datensatz zu öffnen.
4. Wählen Sie im offenen Datensatz die aus **Aktiv** Kontrollkästchen.
5. Wählen Sie in der zugehörigen Liste Testschritte in der Spalte aktiv die Option wahr aus.
6. Klicken Sie auf **Aktualisieren**.
7. Öffnen Sie den Test erneut, und klicken Sie auf **Aktivieren Sie hier Tests und Test-Suite-Ausführung** .
8. Aktivieren Sie Test-/Test-Suite-Eigenschaften und Test-Debugging-Eigenschaften.
9. Klicken Sie auf **Speichern**.
10. Wenn **Test Ausführen** Schaltfläche wird nicht angezeigt. Aktualisieren Sie Ihren Bildschirm, öffnen Sie den Datensatz erneut, und klicken Sie auf **Test Ausführen** Um den Test zu starten.
    Nach einigen Minuten zeigt das Dialogfeld Test ausführen einen erfolgreichen Test an. Klicken Sie Auf **Wechseln Sie zum Ergebnis** Weitere Informationen finden Sie unter .

Nächste Maßnahme

Herzlichen Glückwunsch! Sie können mit der Konfiguration von fortfahren Container Vulnerability Response.

Um weitere Informationen zu automatisierten Tests für zu erhalten Container Vulnerability Response Und automatisierte Tests, Test-Suites und das Erstellen automatisierter Tests finden Sie unter Automated Test Framework (ATF) .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration von Container Vulnerability Response mit anderen Anwendungen

Erweitern Sie die Fähigkeiten von Container Vulnerability Response Durch Integration mit anderen Anwendungen.

Container Vulnerability Response Ist in Container-Sicherheitsprodukte integriert, um Schwachstellendaten für die Images abzurufen, die zur Laufzeit bereitgestellt werden. Anschließend werden die Schwachstellendaten mit kontextbezogenen Informationen zur Laufzeit wie Hosts, Kubernetes-Cluster, Services und Namespaces ergänzt, auf denen diese Container-Images bereitgestellt werden. Mit der Kubernetes-Discovery von ServiceNow können Sie die aus Schwachstellen erstellten Verweise auf die relevanten Kubernetes-Entitäten in anzeigen Configuration Management Database (CMDB). Neben der Ergänzung der Metadaten bietet ServiceNow auch ein umfassendes Reporting-Dashboard, das Einblicke in Schwachstellen- und Korrekturtrends bietet.

Container Vulnerability Response Bietet Integrationen mit den folgenden Anwendungen:

- Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute-Integration
- Verstehen von Atlassian Jira Integration mit Vulnerability Response
- Verständnis der Tenable-Schwachstellenintegration

- **Wichtig:**
  Im Vulnerability Manager-Arbeitsbereich können Sie mit manuell ein Agile-Problem erstellen Listenaktion Und Formularaktion Um die Korrektur von CVITs und RTS nachzuverfolgen.

Zusätzliche Hinweise für Integrationen

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter.
Um diese Fehlkommunikation zu vermeiden, ab Version 2.1.2 von Container Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute-Integration

Mit der Prisma Cloud Compute-Integration können Sie Container-Images scannen, um Schwachstellen zu erkennen.

Ab Version 23,0 von Vulnerability Response, Können Sie verwenden Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute In Container Vulnerability Response Anwendung zum Importieren von Schwachstellen auf den ausgeführten Hosts. Die Prisma-Host-APIs ermöglichen das Abrufen umfassender Schwachstelleninformationen für einen bestimmten Host und bieten auch einen Snapshot der Host-Schwachstellen zu einem bestimmten Zeitpunkt. Diese API ermöglicht die regelmäßige Synchronisierung zwischen Prisma- und ServiceNow-Instanz. Da Prisma sowohl als SaaS-Lösung (Software as a Service) als auch als lokale Lösung angeboten wird, ist die Verwendung eines MID-Servers erforderlich, um Prisma-APIs von der ServiceNow-Instanz aus aufzurufen.

Ab Version 16,1 von Vulnerability Response, Können Sie verwenden Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute In Container Vulnerability Response Anwendung zum Importieren von Container-Image-Schwachstellendaten für bereitgestellte Container. Sie können dann Berichte zu Schwachstellen und angreifbaren Elementen im anzeigen Vulnerability Response Dashboards. Diese Schwachstellen können dann priorisiert und behoben werden.

Wenn Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Produkt und Ihr ServiceNow AI Platform Instanz befindet sich nicht in derselben Umgebung, Sie müssen einen MID-Server verwenden. Weitere Informationen finden Sie unter Systemanforderungen des MID-Servers .

Integrationen werden angezeigt

Sie können die Integrationen anzeigen, die Teil von sind Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Um die Integrationen anzuzeigen, navigieren Sie zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Integrationen**an.

Die folgenden Integrationen sind verfügbar.

Ausführungssequenz	Zeitplan	Integration	Beschreibung
1	Täglich	Integration Von Prisma Cloud Compute Base Images	Ruft die Schwachstellen für Basis-Images aus der Prisma-API ab und meldet die Basis-Images-Schwachstellen separat. Außerdem werden Image-Ergebnisse und angreifbare Elemente erstellt, die auf die Basis-Images verweisen.
2	Täglich	Integration Von Prisma Cloud Compute-Schwachstellen	Ruft Container-Schwachstellen ab. Erstellt Ergebnisse und angreifbare Container-Elemente (CVITs) und erkannte Container-Images.
3	Bei Bedarf	Integration Der Anzahl Der Prisma-Cloud-Compute-Container	Ruft die Containeranzahlen für jedes nicht-Basis-Image ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausführungssequenz	Zeitplan	Integration	Beschreibung
4	Täglich	Integration Der Prisma-Cloud-Compute-Registrierung	Ruft statische Bildergebnisse ab, die aus dem Prisma-Registrierungsscan abgerufen wurden, und erfasst sie in Container Vulnerability Response.

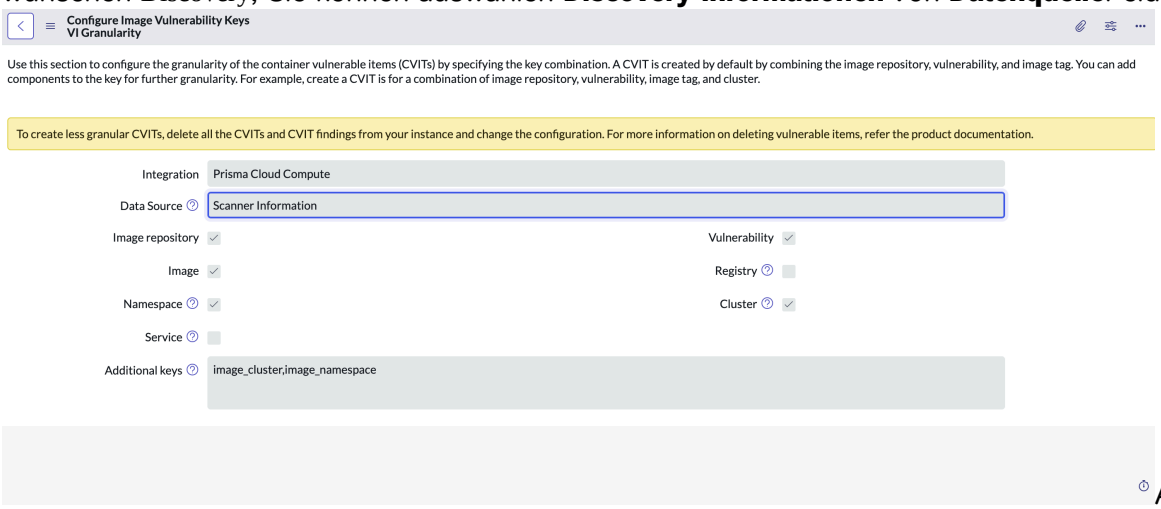
Basis-Image-Konfiguration in Prisma

In der Prisma-Konsole können Sie die Registrierung konfigurieren und dann die Basis-Images aus diesen Registrierungen konfigurieren. Wenn im Basis-Image eine Schwachstelle vorhanden ist, wird bei der Ausführung der Prisma Cloud Compute Base Images-Integration die verwendet **Basis-Image** Das Kontrollkästchen ist aktiviert, um anzugeben, dass die Schwachstellen im Basis-Image vorhanden sind.

Konfigurieren Sie die CVR-basierte VI-Granularität

Um die Granularität von CVITs zu konfigurieren, navigieren Sie zu **Alle** > **Prisma-Cloud-Computing-Integration** > **CVS-basierte-VI-Granularität konfigurieren** Und geben Sie die Schlüsselkombinationen an. Standardmäßig wird ein CVIT für eine Kombination aus Image-Repository, Image und Schwachstelle erstellt. Sie können dem Schlüssel zusätzliche Komponenten hinzufügen, um eine weitere Granularität zu erzielen. Sie können beispielsweise ein CVIT für eine Kombination aus Image-Repository, Image, Schwachstelle und Cluster erstellen.

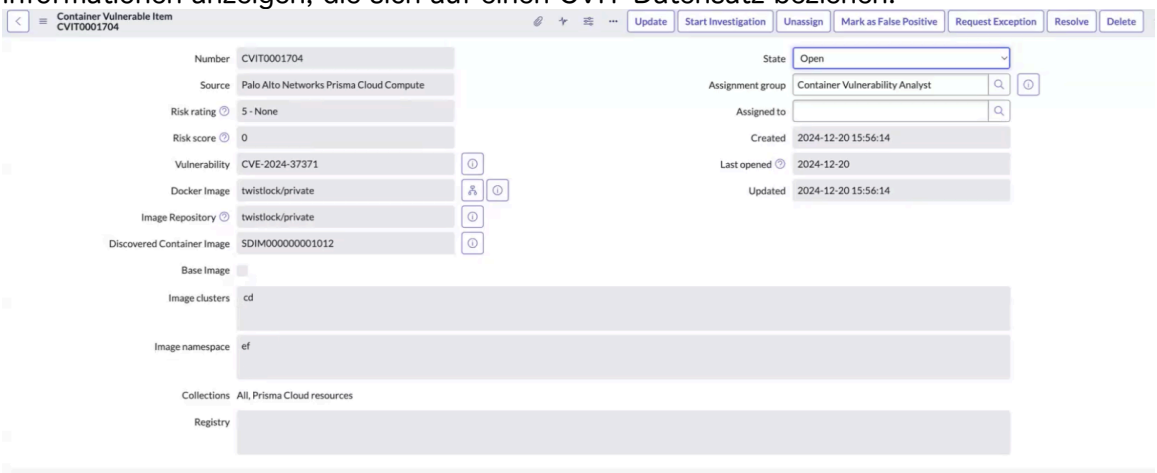
Ab v2.12.1 von Container Vulnerability Response, Sie können auch die Granularität von angreifbaren Container-Elementen (CVITs) mithilfe von Registrierungsinformationen und Datenquellen konfigurieren. Der Namespace und die Clusterinformationen werden sowohl vom Scanner als auch empfangen Discovery. Wenn Sie diese Informationen nur von wünschen Discovery, Sie können auswählen **Discovery-Informationen** Von **Datenquelle**Feld.



Abhängig von der ausgewählten Datenquelle können Sie entweder Bild- oder Kubernetes-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen anzeigen, die sich auf einen CVIT-Datensatz beziehen.



Wenn **Scannerinformationen** Ist ausgewählt, wird der CVIT-Datensatz angezeigt **Image-Cluster** Und **Image-Namespace** Felder.

Wenn **Discovery-Informationen** Ist ausgewählt, wird der CVIT-Datensatz angezeigt **Kubernetes-Cluster** Und **Kubernetes-Namespace** Felder.

Prisma-Integrationsprozess

Wenn Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Wird ausgeführt, überprüft es, ob in der Tabelle National Vulnerability Database (NVD) eine Common Vulnerability and Exposure (CVE) vorhanden ist. Wenn sie bereits vorhanden ist, werden die vorhandenen Informationen verwendet. Wenn das CVE jedoch nicht gefunden wird, werden Platzhalterdatensätze in der NVD-Tabelle generiert. Beim Erstellen dieser Platzhalter-NVD-Datensätze werden anfänglich nur das CVE und sein Name ausgefüllt. Andere Details werden nicht mit der Annahme ausgefüllt, dass die NVD-Integration diese Details später ausfüllt. Wenn der Parameter der Integrationsinstanz *update_nvd*lst auf „wahr“ festgelegt, werden die Platzhalter-NVD-Datensätze aktualisiert. Standardmäßig ist der Instanzparameter auf „falsch“ festgelegt. Mindestens bis die NVD-Integration ausgeführt wird und diese Details ausfüllt, ist jedoch ein gewisses Verständnis des CVE erforderlich, z. B. seinen Schweregrad oder andere Details zum Problem. Um diese Anforderung zu erfüllen, die Felder **Exploit ist vorhanden** Und **Korrekturnotizen** Werden mit den aus Prisma erhaltenen Details ausgefüllt. Darüber hinaus kann diese Konfiguration angepasst werden, sodass Sie basierend auf den von Prisma bereitgestellten Informationen andere Felder angeben können, die Sie im NVD-Eintrag ausfüllen möchten.

Vorbereitung für Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute

Sie können sich auf vorbereiten Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Durch Ausführen von Setup-Aufgaben.

Bevor Sie beginnen

Zum Installieren und Konfigurieren von Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung können Sie die folgende Prüfliste drucken. Vergewissern Sie sich, dass die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und die Schwachstellendaten in importieren ServiceNow AI Platform® Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für Integrationsvorbereitung

Aufgabe	Beschreibung
☐	Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen: • API-Basis-URL • Anwendername und Passwort. Diese Anmeldeinformationen werden verwendet, um die Schwachstellen aus der Prisma Cloud Compute-Integration abzurufen. Weitere Informationen finden Sie unter https://pan.dev/compute/api/ **Hinweis:** Mid-Server ist optional. Die für die Prisma Cloud Compute-Integration verwendeten Anwenderanmeldeinformationen benötigen die Berechtigung zum Überwachen der Images. Siehe folgenden Code: `{"permission":"monitorImages","saas":true,"self-hosted":true}`
☐	Wenn nicht bereits installiert und aktiviert, installieren Sie Vulnerability Response Anwendung, bevor Sie die Drittanbieteranwendung installieren. Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe Vulnerability Response installieren. Diese Integration erfordert Version 16,1 von Vulnerability Response Oder später.
☐	Rufen Sie Berechtigungen ab, und laden Sie herunter Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung auf Ihrem ServiceNow AI Platform® Instanz.
☐	Schätzen Sie die Anzahl der angreifbaren Elemente, die Sie importieren möchten. Überprüfen Sie, ob Ihre Instanz die Anzahl der angreifbaren Elemente akzeptieren kann, die Sie importieren möchten. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an ServiceNow Technischer Support.
☐	Stellen Sie sicher, dass Sie über die folgenden Gruppen oder Anwender verfügen, um die Integrationen zu verwalten und die angreifbaren Elemente zu beheben: **Administrator** Installieren Sie die Anwendung Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute. Wenn nicht zugewiesen, weist der Administrator den Container-Schwachstellenadministrator (sn_vul_Container.Vulnerability_admin) und andere Rollen zu. **sn_vul_Container.Vulnerability_admin** Schließt die Konfiguration der Prisma Cloud Compute-Integration ab. Diese Rolle hat vollständigen Zugriff auf Container

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für Integrationsvorbereitung (Fortsetzung)

Aufgabe	Beschreibung
	Vulnerability Response(CVR)-Anwendung und ihre Datensätze. Dieser Administrator konfiguriert Integrationen und Regeln in Container Vulnerability Response. **Vulnerability Response-Gruppe** Standardmäßig ist die Vulnerability Response-Gruppe verfügbar. Anwender, die der Vulnerability Response-Gruppe zugewiesen sind, erben sn_vul.read_all, sn_vul_Container.read_all. **Besitzergruppe Für Container-Korrektur** Standardmäßig ist die Besitzergruppe Container-Korrektur verfügbar. Anwender, die dieser Gruppe zugewiesen sind, erben sn_vul_Container.Remediation_owner. Der Besitzer der Container-Korrektur korrigiert Container-Schwachstellen, die ihm oder einer Gruppe zugewiesen sind, zu der er gehört. **Schwachstellenanalyst** Anwender, die der Container-Schwachstellenanalyst-Gruppe zugewiesen sind, erben sn_vul.Vulnerability_Analyst. Der Schwachstellenanalyst überwacht die Nachbesserung aller angreifbaren Elemente. Wenn Sie noch nicht erstellt haben, können Sie zusätzliche Gruppen erstellen und Anwender mit dem Modul „Anwenderverwaltung“ in Ihrer Instanz hinzufügen. Weitere Informationen finden Sie unter Erstellen Sie eine Anwendergruppe .
☐	Installieren Sie Vulnerability Response Integration mit NVD und Ausführen der NIST National Vulnerability Database Integration – API (nur CVE).

Sie sind bereit für Konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung.

Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute installieren

Bevor Sie die Integration in Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte aus, damit das Prisma Cloud Compute-Produkt ordnungsgemäß in integriert wird Vulnerability Response Und Container Vulnerability Response. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich bei der Instanz an, die Sie installieren möchten Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Ein.
2. Navigieren Sie zum ServiceNow Store.
3. In ServiceNow Store, Suchen nach Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung.
4. Klicken Sie auf die Anwendungskachel.
   Über die Anwendung, die Sie installieren, werden detaillierte Informationen angezeigt.

   Hinweis:
   Lesen Sie **Andere Anforderungen** Und **Abhängigkeiten** Abschnitte, falls erforderlich.

5. Klicken Sie auf **App anfordern** und geben Sie Ihre Now Support-Anmeldeinformationen ein.
6. Klicken Sie auf **Abrufen**.
7. Aktualisieren Sie **Instanzname** Und **Grund für die Instanz** Felder, und klicken Sie auf **Validieren Sie Die Instanz** .
8. Klicken Sie auf **Anforderung**.
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
9. Navigieren zu **Systemanwendungen** > **Anwendungen**an.
10. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.

Ergebnisse
Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Nächste Maßnahme
Konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Für Ihre Umgebung. Weitere Informationen finden Sie unter Konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung.

Konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung

Installieren und konfigurieren Sie Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute Anwendung. Importieren Sie Daten aus Prisma Cloud Compute. Sie können die importierten Daten verwenden, um Schwachstellen für Ihre Docker-Images und -Hosts zu priorisieren und zu beheben.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie die E-Mail von ServiceNow Die Sie über die Integration erhalten haben.
2. Melden Sie sich als Administrator bei Ihrer Instanz an.
3. Befolgen Sie die Anweisungen in der E-Mail, um den zu erhalten Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute.
4. Navigieren zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Administration** > **Konfiguration**an.
   Füllen Sie die Felder im Formular „Prisma-Cloud-Compute-Konfiguration“ aus. Weitere Informationen finden Sie unter Formular „Konfiguration von Prisma-Cloud-Computing“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie in der Liste Projekte eine der Optionen aus **Alle Projekte** Oder **Bestimmte Projekte** Um entweder alle Projekte oder ausgewählte Projekte zu konfigurieren.
   Wenn Sie auswählen **Bestimmte Projekte** , Sie können die Projekte aus der Liste verfügbar auswählen.
6. Schließen Sie die Konfiguration ab, indem Sie eine der Optionen auswählen **Beenden** Oder **Anmeldeinformationen speichern und testen** .
   - Wenn Sie ein Projekt konfiguriert haben, wählen Sie aus **Beenden** .
   - Wenn Sie kein Projekt konfiguriert haben, wählen Sie aus **Anmeldeinformationen speichern und testen**
7. Zeigen Sie die neu erstellte Instanz an, indem Sie zu navigieren **Prisma-Cloud-Computing-Integration** > **Administration** > **Integrationsinstanzen**an.
8. Zeigen Sie die Projekte an, die Sie zuvor konfiguriert haben, indem Sie auswählen **Integrationsinstanzparameter** .
9. Führen Sie die neu erstellte Integrationsinstanz aus, um die folgenden Daten zu importieren:
   - Docker-Images: Listet die Docker-Images auf, die mit einer Identifizierungs- und Abgleichsmodul (IRE) erstellt werden. Jedes Docker-Image enthält auch Informationen zur Beziehung zwischen den Repositorys und den installierten Versionen.
   - Erkannte Container-Images: Das Modul „erkannte Container-Images“ stellt Informationen zur Image-ID, zum Docker-Image und zum Image-Repository bereit. Außerdem werden die Ebeneninformationen gespeichert und dem erkannten Image zugeordnet. Sie können hier auch die Projekte und die Containeranzahl anzeigen. Für ein erkanntes Container-Image können Sie Cloud-Metadaten wie Cloud-Provider, Cloud-Region, Cloud-Account-ID und Cloud-Ressourcen-IDs anzeigen.
   - Container-Image-Pakete: Stellt Informationen zu den Paketen bereit, in denen die Schwachstellen vorhanden sind. Die Binärpaketdetails werden auch als kommagetrennter Wert bereitgestellt.
   - Container-Image-Ebenen: Auf diesem Bildschirm wird der Datensatz für jede Image-Ebene angezeigt.
   - Container-Image-Ergebnisse: Auf diesem Bildschirm wird die Liste der Ergebnisse zusammen mit Informationen zu den zugehörigen Schwachstellen, der Image-Ebene, dem Docker-Image, dem Image-Repository und dem erkannten Image angezeigt. Derzeit sind die Informationen zu Schwachstellen nur auf die ID beschränkt. Zusätzliche Informationen werden ausgefüllt, wenn National Vulnerability Database (**NVD**) Integration wird ausgelöst.
   - Angreifbare Container-Elemente: Jedes Ergebnis weist eine entsprechende Schwachstelle auf. Die CVITs werden basierend auf der Granularität weiter erstellt.
10. Konfigurieren Sie die Granularität eines angreifbaren Elements.

    a. Navigieren zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Image-Schwachstellenschlüssel konfigurieren**

    b. Konfigurieren Sie die Granularität der CVITs, indem Sie die erforderlichen Kontrollkästchen aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die angreifbaren Elemente werden basierend auf den beim nächsten Import ausgewählten Schlüsseln erstellt.

Hinweis:
Standardmäßig wird ein CVIT für eine Kombination aus Image-Repository, Schwachstelle und Image-Tag erstellt. Sie können dem Schlüssel Komponenten hinzufügen, um eine weitere Granularität zu erzielen. Sie können beispielsweise ein CVIT für eine Kombination aus Image-Repository, Schwachstelle, Image-Tag und Cluster erstellen. Sobald die Ergebnisse angreifbarer Elemente oder angreifbarer Elemente erstellt wurden, können die Kontrollkästchen nicht mehr bearbeitet werden.

Erkunden Sie Wiz Container-Schwachstellenintegration

Importieren Sie Container-Schwachstellendaten mit Wiz Container-Schwachstellenintegration, die in enthalten ist Wiz Vulnerability Response Integration.

Wiz Container-Schwachstellenintegration Übersicht

Die Wiz Container Vulnerability Integration importiert Container-Image-Schwachstellen, die von identifiziert werden Wiz Schwachstellenscanner. Importieren Sie Daten, damit Sie Container-Schwachstellen mit den automatisierten Workflows der KI-Plattform-Instanz von ServiceNow identifizieren, priorisieren und zuweisen können.

Ergebnisse werden angreifbaren Container-Elementen (CVITs) zugeordnet, um Selektierung, Risikopriorisierung und gezielte Korrektur-Workflows für containerbasierte Arbeitsauslastungen zu unterstützen.

Um weitere Informationen zu den anderen Integrationen zu erhalten, die in enthalten sind Wiz Vulnerability Response Schritte zur Integration, Installation und Konfiguration finden Sie unter Verstehen von Wiz Vulnerability Response Integration.

Container-Schwachstellen werden behoben

Die Überwachung der Fehlerkorrektur ist ein Prozess, der mit der Überprüfung des Status beginnt und mit dem Schließen angreifbarer Container-Elemente (CVITs) endet. Container Vulnerability Response Bietet Tools und Verfahren, um diesen Prozess produktiver und effizienter zu gestalten.

Container Vulnerability Response Rechnerregeln

Schwachstellenrechner automatisieren die Berechnung der Anfangswerte für die Felder in angreifbaren Containerelementen. Die Bedingung für jeden Rechner wird in der Reihenfolge ausgewertet, und der erste übereinstimmende Rechner wird verwendet.

Navigieren Sie zu , um Schwachstellen-Rechner anzuzeigen und zu erstellen **Alle** > **Container Vulnerability Response** > **Administration** > **Schwachstellen-Rechner**an.

Die Container Vulnerability Response Das Basissystem enthält zwei Schwachstellenrechner, die die Basis-Risikopunktzahl für das angreifbare Container-Element festlegen. Die folgenden Rechnergruppen sind im Basissystem verfügbar:

- Schwachstellenschweregrad: Berechnet die Risikopunktzahl für angreifbare Elemente anhand des normalisierten Schwachstellenschweregrads.
- Standard-Risikorechner: Basiert auf der Risikoregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab Version 2,10 von Container Vulnerability Response, Im Fall von:

- **Standardrisikorechner** Regel: Wenn sich die Risikopunktzahl für ein angreifbares Container-Element (CVIT) ändert, werden die folgenden Details im Abschnitt „Notizen“ des CVIT dokumentiert:
  - Rechnergruppenname
  - Rechnername
  - Feldwerte mit einer Gewichtung größer als 1 und ihrem Beitrag zur Risikopunktzahl.
  - Endgültige Risikopunktzahl
- **Schwachstellenschweregrad** Risikoregel: Immer wenn die Risikopunktzahl für ein CVIT aktualisiert wird, wird die aktualisiert **Notizen** Abschnitt wird mit den folgenden Details aktualisiert:
  - Rechnergruppenname
  - Rechnername: Je nachdem, ob die Rechnerregel auf einer Vorlage oder einem Skript basiert, wird der Name mit den Details in Klammern angehängt. Um die Basis der Rechnerregel zu ändern oder anzuzeigen, wählen Sie eine beliebige Regel aus, und wählen Sie aus **Erweiterte Ansicht** Kontrollkästchen. Von **Werttyp** Wählen Sie im Dropdown-Feld die erforderliche Option aus. Wenn **Vorlage** Ist ausgewählt, wird die Risikopunktzahl gemäß der in der Regel angegebenen Bedingung aktualisiert. Wenn **Skript** Ist ausgewählt, können Sie das vorhandene Skript entweder hinzufügen oder aktualisieren. Die Systemeigenschaft *sn_sec_cmn.risk_score_changes_add_worknotes*Hilft beim Ausfüllen des Abschnitts „Arbeitsnotizen“. Ab v2.12.2 von Container Vulnerability Response, Die Systemeigenschaft *sn_sec_cmn.risk_score_changes_add_worknotes*Ist standardmäßig inaktiv. Wenn Sie sie aktivieren, können Sie nur im Abschnitt „Arbeitsnotizen“ alle Änderungen im Zusammenhang mit der Risikopunktzahl eines angreifbaren Containerelements anzeigen. Außerdem werden die Arbeitsnotizen nur aktualisiert, wenn sich die Risikopunktzahl ändert.

Gewichtungen Der Schwachstellenrisikopunktzahl

Allen Schwachstellen wird eine Risikopunktzahl und eine Bewertung basierend auf Faktoren wie Schweregrad, Relevanz, Ausnutzungsinformationen usw. zugewiesen. Die Business-Regel *Update Risk Rating from Risk Score*In der Tabelle „angreifbare Container-Elemente“ ist für die Berechnung der Risikobewertung verantwortlich. Wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Container-Elemente ausgefüllt. Vor Version 17,1 von Vulnerability Response(VR)-Anwendung wurden die folgenden Risikobewertungen als Teil der Skripteinbindung bereitgestellt SchwachstellenUtils , Die hartcodiert waren.

Wert (Risikobewertung)	Gewichtung (Risikopunktzahl)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab Version 18,0 von Vulnerability Response,

- Die Risikobewertungstypen werden in der Basistabelle „Risikopunktzahlgewichtungen“ [sn_sec_cmn_Risk_Scorew_weight] als cvr_Risk_Rating geliefert. Diese Typen werden als Teil der Business-Regeln oder Skripteinbindungen in jeder Tabelle übergeben, in der die Risikobewertung berechnet wird.
- Das Skript wird geändert, sodass Sie die Einträge in den Tabellenwerten für Risikopunktzahlgewichtungen für die Berechnung der Risikobewertung abfragen können.
- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, stellen Sie sicher, dass Sie die Bezeichnungen für die neue Risikobewertung hinzufügen und auch die zugehörigen Skripts und Business-Regeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.
- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle mit Risikopunktzahlgewichtungen zugreifen, indem Sie sn_sec_cmn_Risk_Score_weight im Filternavigator eingeben.

Darüber hinaus wird die Risikopunktzahl in den folgenden Szenarien automatisch neu berechnet:

- Wenn sich ein Konfigurationselement (Configuration Item, CI) von nicht mit Internetzugriff zu Internetzugriff ändert.
- Wenn die zugehörigen Common Vulnerabilities and Exposures (CVEs) oder Drittparteieinträge (TPEs) in den Schwachstellen-Elementen (VIS) mit einer bekannten CVE-Exploit-Schwachstelle (KEV) verknüpft sind.

Weitere Informationen finden Sie unter Vulnerability Response Rechner und Regeln für Schwachstellenrechner.

Container Vulnerability Response Zuweisungsregeln

Definieren Sie die Kriterien, nach denen angreifbare Container-Elemente automatisch einer Zuweisungsgruppe zur Korrektur zugewiesen werden.

Um Zuweisungsregeln für angreifbare Container-Elemente zu erstellen und anzuzeigen, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Administration** > **Zuweisungsregeln**an. Wenn Sie eine Zuweisungsregel erstellen, können Sie die Bedingungen festlegen. Wenn diese Bedingungen erfüllt sind, weist die Regel die angreifbaren Container-Elemente automatisch der ausgewählten Anwendergruppe zu. Nur die erste Zuweisungsregel mit einer übereinstimmenden Bedingung wird für einen Datensatz ausgeführt. Siehe Vulnerability Response Übersicht über Zuweisungsregeln Weitere Informationen zu Zuweisungsregeln.

Erforderliche Rollen: sn_vul_Container.manage_assignment_rules zum Definieren und Aktualisieren von Regeln und sn_vul_Container.Container_reapply zum erneuten Anwenden von Regeln.

Ab Version 2,13 wurden den Datensätzen in der Tabelle „erkanntes Container-Image“ [sn_vul_Container_image] Felder für Scannerinformationen hinzugefügt. Sie können die folgenden Werte als Bedingungen verwenden, wenn Sie Ihre Zuweisungsregeln für angreifbare Container-Image-Elemente (CVITs) erstellen oder aktualisieren, damit Sie den Besitz in Ihren Container-Umgebungen nachverfolgen können.

- Cloud-Account-IDs
- Image-Namespaces

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Registry
- Hosts
- Bezeichnungen
- Status (Lieferantenstatus für eine gelöste Schwachstelle)

Hinweis:
Dieser Wert in der Tabelle „Container-Image-Ergebnis“ [sn_vul_Container_image_results] bezieht sich auf die Version, in der eine Schwachstelle gelöst wurde, z. B. Behoben in 6.2.1 . Dieser Wert wird aus importiert Vulnerability Response Integration with Palo Alto Networks Prisma Cloud Compute-Integration.

Hinweis:
Angreifbare Container-Elemente (CVITs), die sich nicht im Status „Offen“ befinden oder manuell zugewiesen wurden, werden immer von Zuweisungsregeln ausgeschlossen. Wenn Sie Ihren Zuweisungsregeln Werte für diese Scannerfelder hinzufügen und Ihre Regeln erneut ausführen, werden angreifbare Elemente nur neu zugewiesen, wenn der Zuweisungstyp lautet Regel . Elemente mit Typ Manuell Werden von den Zuweisungsregeln nicht berücksichtigt.

Wichtig:
Als Schwachstellenadministrator und -Analyst können Sie die neuesten Zuweisungen für ausgewählte CVITs in abrufen Arbeitsbereich des Schwachstellenmanagers. Diese Methode ist effizienter als die erneute Anwendung der Zuweisungsregeln für alle CVITs im klassisch UI, die ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Arbeitsbereich des Schwachstellenmanagers.

Container Vulnerability Response Korrekturzielregeln

Korrekturzielregeln definieren den erwarteten Zeitrahmen für die Korrektur eines angreifbaren Container-Elements (CVIT). Diese Regeln ähneln der Art, wie SLAs einen Zeitrahmen für die Behebung der Schwachstelle selbst bereitstellen.

Um Korrekturzielregeln für Container-Schwachstellen zu erstellen und anzuzeigen, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Administration** > **Korrekturzielregeln**an.

Die Korrekturzielregeln definieren die Zielkorrekturzeit für ausgewählte angreifbare Container-Elemente (CVITs). Legen Sie eine Frist für die Behebung der Schwachstelle fest, indem Sie die Anzahl der Tage für die Behebung auswählen. Legen Sie eine Erinnerung für die Korrektur fest, und legen Sie die angreifbaren Container-Elemente fest, für die die Regel gilt. Sie können ein Korrekturziel für die Tage festlegen, innerhalb derer es korrigiert werden muss, und auch eine Erinnerung festlegen, bevor Sie sich dem Zieldatum nähern. Weitere Informationen finden Sie unter Vulnerability Response Korrekturzielregeln.

Wichtig:
Als Schwachstellenadministrator und -Analyst können Sie das neueste Korrekturzieldatum für ausgewählte CVITs in abrufen Arbeitsbereich des Schwachstellenmanagers. Diese Methode ist effizienter als die Ausführung der Korrekturzielregeln für alle CVITs in klassisch UI, die ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Arbeitsbereich des Schwachstellenmanagers.

Ausnahmeverwaltung in Container Vulnerability Response

Wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Richtlinie nicht einhalten kann, können Sie eine Ausnahme anfordern. Das Ausnahmemanagement umfasst das anfordern, Überprüfen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigen oder Ablehnen von Ausnahmen für ein angreifbares Container-Element (CVIT), das nicht gemäß der Richtlinie korrigiert werden kann.

Einige Container-Schwachstellen (CVIT) haben möglicherweise keinen Patch, eine Korrektur oder eine Lösung. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko akzeptieren, da Sie die Konsequenzen einer Nichtbeseitigung der Schwachstelle bestätigen und zustimmen.

Lebenszyklus einer Ausnahme

Definition einer Ausnahme

Eine Ausnahme ist eine Anforderung zum Zurückstellen der Korrektur eines CVIT oder RT für einen bestimmten Zeitraum. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Ausnahme wird angefordert

Als Korrekturbesitzer können Sie mithilfe des Ausnahmeverwaltungsprozesses eine Ausnahme für ein CVIT oder RT beantragen. Nachdem der Ausnahmegenehmiger diese Anforderung genehmigt hat, wird CVIT oder RT zu einem verschoben **Zurückgestellt** status.

Ausnahmeanforderung wird genehmigt

CVIT oder RTS, die nicht sofort behoben werden können, werden von Schwachstellenanalysten überprüft, auf Risiko bewertet und für eine Zurückstellung genehmigt, bis sie behoben werden können. Das Genehmigen einer Ausnahmeanforderung kann ein Workflow auf zwei Ebenen sein. Wenn nur der Genehmiger der ersten Ebene vorhanden ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger hinzu.

Hinweis:

Beginnt ab Vulnerability Response V15.0: Wenn Sie die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht zurück in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für das Ausnahmemanagement und falsch positive Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Sobald eine Ausnahmeanforderung für ein CVIT oder RT genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Erneut öffnen
- Löschen
- Aktualisieren Sie **Zuweisung an** Oder **Zuweisungsgruppen** Felder

Nachverfolgung einer Ausnahmeanforderung

Nachdem Sie die Ausnahme ausgelöst haben, können Sie ihren Status mithilfe von nachverfolgen **Statusänderungsgenehmigungen** Registerkarte des CVIT oder RT. Wenn eine Aktion für eine RT ausgeführt wird, können Sie den Status der einzelnen CVITs in dieser RT nicht nachverfolgen.

Ablauf einer Ausnahmeanforderung

Wenn eine Ausnahmeanforderung für ein bestimmtes CVIT oder RT abläuft, wird das betroffene CVIT oder RT auf zurückgesetzt **Öffnen** status.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein einzelnes CVIT oder alle CVITs in einer RT beim nächsten Scan übergeben werden, werden die CVITs und gegebenenfalls die RT übergeben **Status** Feld ändert sich in **Geschlossen** Mit dem Substatus **Behoben** .

Konfigurieren Sie Genehmigungsregeln

Zeigen Sie Genehmigungsregeln an, und konfigurieren Sie sie, indem Sie zu navigieren **Alle** > **Container Vulnerability Response** > **Administration** > **Genehmigungsregeln**an. Fordern Sie eine Ausnahme für die CVITs an, die nicht sofort behoben oder zurückgestellt werden kann, indem Sie die betroffenen Schwachstellen, Konfigurationselemente (Configuration Items, CIs) oder CVITs identifizieren. Automatisieren Sie den CVIT-Zurückstellungsprozess. Verschieben Sie die übereinstimmenden CVITs basierend auf diesen Regeln, wenn das System diese CVITs identifiziert.

Die folgenden Genehmigungsregeln werden standardmäßig ausgeliefert:

- Genehmigung für Ausnahmeanforderungen: Im Basissystem wird eine Standardkonfiguration mit zwei Genehmigungsebenen bereitgestellt. Immer wenn für ein angreifbares Element eine Ausnahmeanforderung vorhanden ist, wird die Genehmigungsanforderung an die Anwender oder Gruppen gesendet, die auf Ebene 1 vorhanden sind. Nach der Genehmigung durch Genehmiger der Ebene 1 wird es an die Genehmiger der Ebene 2 gesendet.

  Hinweis:
  Sie können die Standardebenen ändern und nach Bedarf bearbeiten. Beginnt ab Container Vulnerability Response V2.0.6. Sie können die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahme oder falsch positive Anforderung über den Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** Und wählen Sie aus *`sn_vul_container.container_exception_approver_L1`*, *`sn_vul_container.container_exception_approver_L2`*, Oder *`sn_vul_container.container_false_positive_approver_group`*Zum Ändern des Eigenschaftswerts.

- Genehmigung für Ausnahmeregeln: Sie verfügt nicht über eine Konfiguration, sondern über zwei Genehmigungsebenen.
- Genehmigung für falsch positive Ergebnisse: Sie verfügt über eine Konfiguration mit einer Genehmigungsebene.

Hinweis:
Ab v2.5 von Container Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Container-Element in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Container-Element oder die Korrekturaufgabe auf den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Fordert und genehmigt eine Ausnahme in an Container Vulnerability Response

Sie können anfordern, die Korrektur eines angreifbaren Container-Elements (CVIT) für einen bestimmten Zeitraum zu verschieben. Beispielsweise können Sie als Entwickler eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist. Genehmiger, die Zugriff haben, können Anforderungen anderer Anwender genehmigen.

Informationen zum anfordern oder Genehmigen einer Ausnahme finden Sie unter:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fordern Sie eine Ausnahme für ein angreifbares Container-Element an
- Fordern Sie eine Ausnahme für Container-Schwachstellen mit an GRC: Richtlinien- und Compliance-Management

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des Ausnahmemanagements gesendet, die den Status und andere Details einer Anforderung angeben. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, die bestätigt, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail, in der angegeben wird, dass eine Ausnahme angefordert wurde. Ab v2.5 von Container Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Container-Element in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Container-Element oder die Korrekturaufgabe auf den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Fordern Sie eine Ausnahme für ein angreifbares Container-Element an

Fordern Sie eine Ausnahme für ein angreifbares Container-Element (CVIT) an, das nicht sofort behoben werden kann. Beispielsweise können Sie als Korrekturbesitzer eine Ausnahme anfordern, wenn für einen Computer kein Patch verfügbar ist.

Vorbereitungen

Erforderliche Rolle: Entwicklergruppe

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Ausnahme für mehrere CVITs gleichzeitig anfordern, indem Sie die Massenbearbeitungsfunktion in verwenden Arbeitsbereich des Schwachstellenmanagers. Weitere Informationen finden Sie unter Fordern Sie eine Massenausnahme im Vulnerability Manager-Arbeitsbereich an.

Prozedur

1. Navigieren zu **Container Vulnerability Response** > **Angreifbare Container-Elemente** > **Alle**an.
2. Wählen Sie das Element aus, für das Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element muss sich im Status „Offen“ oder „wird untersucht“ befinden.
3. Klicken Sie im Formular Angreifbares Container-Element auf **Ausnahme Anfordern** .
   [store-future: BEGIN review]

   Hinweis:

   Abhängig davon, ob Vulnerability Response Oder GRC: Richtlinien- und Compliance-Management Ist in ausgewählt **Container Vulnerability Response** > **Ausnahmenverwaltung** Bildschirm ändert sich das Formular „Ausnahme anfordern“.

   [End]
4. [store-future: BEGIN review]Wenn Vulnerability Response Im Bildschirm „Ausnahmemanagement“ ausgewählt ist, gehen Sie dann wie folgt vor.[End]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Füllen Sie im Formular die Felder aus.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der in ausgewählten Dauer liegen **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmenverwaltung** Bildschirm. Wenn die Ausnahmeanforderung abläuft, kehrt die Gruppe in den Status „Offen“ zurück. **Hinweis:** Ab Version 1,2 von Container Vulnerability Response, Wenn ein angreifbares Element zur Korrektur mithilfe der Ausnahmeverwaltungsfunktion zurückgestellt wurde, bleibt das für die Schwachstelle festgelegte Zurückstellungsdatum weiterhin bestehen, falls es vom Scanner erneut geöffnet wird. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft fest *sn_vul.container.auto_defer_cvit_in_active_e* „wahr“. Außerdem wird das Datum „Zurückgestellt bis“ auch nach dem Schließen des CVIT oder dem Ablauf der Ausnahme beibehalten. Die erforderliche Rolle ist „sn_vul_Container.Manage_Exception_Configuration“ für Lese- und Schreibvorgänge.
Grund	Grund für die Ausnahme. Die Auswahlmöglichkeiten lauten wie folgt: ▪ Risiko akzeptiert ▪ Warten auf Wartungsfenster ▪ Behebung nicht verfügbar ▪ Ausgleichende Steuerung vorhanden ▪ Sonstige Informationen zum Hinzufügen neuer Ursachenauswahlen finden Sie unter Definieren Sie eine Richtlinienursachenzuordnung.
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer aktualisiert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Senden Sie die Ausnahmeanforderung, indem Sie auf klicken **Genehmigung Anfordern** . Der Status des angreifbaren Containerelements ändert sich in „in Überprüfung“. Verwenden Sie **Genehmigung Der Statusänderung** Registerkarte zum Nachverfolgen des Status der Ausnahmeanforderung.

Fordern Sie eine Ausnahme für eine Container-Korrekturaufgabe an

Fordern Sie eine Ausnahme an, um eine Container-Korrekturaufgabe für einen angegebenen Zeitraum aufzuschieben, wenn sie nicht sofort gelöst werden kann.

Vorbereitungen

Sie können Ausnahmen von anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen.

Erforderliche Rolle:

sn_vul.Remediation_owner, sn_vul.App_Security_Champion oder sn_vul_Container.Remediation_owner.

Sie können auch Ausnahmen für Container-Korrekturaufgaben in der klassischen Umgebung anfordern.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Korrekturaufgaben** > **Alle**an.
2. Wählen Sie die Gruppe aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählte Aufgabe muss sich im Status Offen, wird untersucht oder wartet auf Implementierung befinden.
3. Wählen Sie im Datensatz der Container-Korrekturaufgabe die Option aus **Ausnahme Anfordern** .
4. Füllen Sie im Formular die Felder aus.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der Ausnahmedauer liegen, die in der Konfiguration definiert ist.
Grund	Begründung für die Anforderung einer Ausnahme.
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer aktualisiert werden.

5. Klicken Sie auf **Genehmigungs-Engine**.

Fordern Sie eine Ausnahme für Container-Schwachstellen mit an GRC: Richtlinien- und Compliance-Management

Fordern Sie Richtlinienausnahmen mit an GRC Fähigkeit zur Verwaltung von Richtlinienausnahmen in Richtlinien- und Compliance-Management Anwendung von innerhalb Container Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Bevor Sie die Integration von Richtlinienausnahmen verwenden können, um Richtlinienausnahmen anzufordern, müssen Sie herunterladen GRC: Richtlinien- und Compliance-Management Anwendung aus dem ServiceNow Store.

Erforderliche Rolle: sn_vul.Remediation_owner

Sie können auch Ausnahmen in der klassischen Anwenderoberfläche anfordern:

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente** (Oder **Korrekturaufgaben**)> **Alle** , Und öffnen Sie das Element oder die Gruppe, für das Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie im ausgewählten Formular auf **Ausnahme Anfordern** .

   Hinweis:
   Wenn GRC: Richtlinien- und Compliance-Management Ist im Bildschirm „Ausnahmemanagement“ ausgewählt, füllen Sie dann die Felder im Formular „Ausnahme anfordern“ aus. Weitere Informationen zu den Formularfeldern finden Sie unter Formular „Ausnahme anfordern“.

   a. Senden Sie die Ausnahmeanforderung, indem Sie auf klicken **Genehmigung Anfordern** .
   Der Status der angreifbaren Elemente ändert sich in „in Überprüfung“, und eine Richtlinienausnahme wird erstellt. Verwenden Sie **Genehmigung Der Statusänderung** Registerkarte zum Nachverfolgen des Status der Ausnahmeanforderung.

   b. Zeigen Sie die Richtlinienausnahme an, indem Sie auf die zugehörige Liste Richtlinienausnahmen klicken.

   c. Klicken Sie auf die Nummer der Richtlinienausnahme.

   d. In **Genehmiger** Wählen Sie den Namen des Genehmigers aus.

   e. Klicken Sie auf die Registerkarte Quelle, und wählen Sie ein Kontrollziel aus **Kontrollziel** Feld.

   f. Klicken Sie auf die Registerkarte Risikobewertung, und wählen Sie die Risikobewertung aus **Risikobewertung** Feld.

   g. Speichern Sie das Formular.

   h. Klicken Sie auf **Betroffene Steuerungen** Registerkarte.

   i. Fügen Sie die Steuerungen hinzu, indem Sie auf klicken **Hinzufügen** .

   j. Speichern Sie das Formular.

   Hinweis:
   Sie können eine Compliance-Überprüfung starten, indem Sie auf klicken **Compliance-Überprüfung anfordern** .

   Das Genehmigungsformular wird an den Genehmiger gesendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Genehmiger kann die Anforderung entweder genehmigen, indem er auf klickt **Genehmigen** Oder fordern Sie eine zusätzliche Genehmigung an, indem Sie auf klicken **Zusätzliche Genehmigung Anfordern** .

Der Datensatzstatus ändert sich in zurückgestellt. Der angegebene Grund ist der, den Sie beim Auslösen der Ausnahmeanforderung ausgewählt haben. Die **Zurückstellung** Die Registerkarte enthält zusätzliche Notizen zum Datensatz.

Hinweis:
Wenn die Anforderung abgelehnt wird, wird der Datensatz in den vorherigen Status verschoben.

3. Klicken Sie auf **Absenden**.
   Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Korrekturbesitzer und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management .

Definieren Sie eine Richtlinienursachenzuordnung

Definieren Sie Ursachenauswahlen, die jedem Anwender zur Verfügung stehen, der eine Ausnahme anfordert.

Vorbereitungen

Erforderliche Rolle: sn_vul.compliance.manager und sn_vul_Container.Manage_Exception_Configuration

Prozedur

1. Navigieren zu **Alle** > **Richtlinien und Compliance** > **Richtlinienausnahmen** > **Integrationsregistrierung**an.

   Hinweis:
   Sie können entweder einen Grund aus den Ursachenauswahlen auswählen, die in der Tabelle „Ursachenauswahlen“ verfügbar sind, oder einen neuen Grund hinzufügen.

2. Klicken Sie auf die Integrationsregistrierung Container Vulnerability Response – CVIT.
3. Klicken Sie in der Liste Ursachenauswahlen auf **Neu** .
4. Klicken Sie auf das Lupensymbol.
5. Fügen Sie eine vorhandene Ursachenauswahl hinzu, um einen neuen zu erstellen.
   - Wenn Sie eine vorhandene Ursachenauswahl hinzufügen möchten, wählen Sie einen Grund aus.
   - Wenn Sie der Tabelle „Ursachenauswahlen“ eine neue Ursachenauswahl hinzufügen möchten, klicken Sie auf **Neu** Und füllen Sie die Felder im Formular aus.

Formular „Ursachenauswahlliste“

Feld	Beschreibung
Bezeichnung	Eindeutige Bezeichnung für diese Auswahl.
Wert	Eindeutiger Wert für diese Auswahl. Dieser Wert wird in der Tabelle „Richtliniengrund-Zuordnung“ für die jeweiligen Anwendungen zugeordnet. Um zu dieser Tabelle zu navigieren, geben Sie ein sn_vul_Policy_reason_Mapping.LIST Im Filternavigator.
Reihenfolge	Reihenfolge für diese Auswahl. Gründe werden basierend auf dieser Nummer sortiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Standard	Option, die angibt, dass diese Ursachenauswahl immer verfügbar ist, wenn eine Richtlinienausnahme bei Bedarf angefordert wird. Wenn die Integrationsregistrierung keine anwendungsspezifischen Auswahlmöglichkeiten enthält, werden alle Ursachenauswahlen mit angegeben **Standard** Das ausgewählte Feld ist verfügbar.
Aktiv	Option zum Anzeigen der Auswahl in der Liste der Ursachenauswahlen.

6. Klicken Sie auf **Absenden**.

Ergebnisse
Die Auswahl für den Grund wird hinzugefügt. Die Auswahl für den Grund ist in verfügbar **Grund** Feld des Anforderungsformulars für Richtlinienausnahme für die ausgewählte Anwendung.

Genehmigen Sie eine Ausnahmeanforderung in Container Vulnerability Response

Genehmigen Sie Ausnahmeanforderungen für angreifbare Container-Elemente oder Korrekturaufgaben, die nicht sofort behoben werden können. Sie müssen diese Anforderungen auf Risiko bewerten und sie dann zur Zurückstellung genehmigen, bis sie behoben werden können.

Vorbereitungen
Erforderliche Rolle: sn_vul.Exception_Approver

Warum und wann dieser Vorgang ausgeführt wird
Sie können die Ausnahme und falsch positive Anforderungen in genehmigen Arbeitsbereich des Schwachstellenmanagers.

Sie können Ausnahmeanforderungen auch in der klassischen Umgebung genehmigen:

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Meine Genehmigungen**an.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Verschieben Sie ein angreifbares Container-Element in Container Vulnerability Response

Wenn Sie feststellen, dass das Problem, das einem angreifbaren Container-Element (CVIT) zugeordnet ist, ein geringes Risiko aufweist und sofort ohne weitere Analyse zurückgestellt werden kann, können Sie verwenden **Zurückstellen** Funktion.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)
Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Warum und wann dieser Vorgang ausgeführt wird
Eine geplante Aufgabe wird jeden Tag ausgeführt, um nach zurückgestellten angreifbaren Elementen zu suchen, die ihr Wiedereröffnungsdatum erreicht haben. An dem Tag, an dem die Zurückstellung des CVIT abläuft, wird der Datensatz erneut geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente**an.
2. Öffnen Sie ein angreifbares Element.
3. Klicken Sie Auf **Ausnahme Anfordern** .
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Bis	Wählen Sie das Datum aus, an dem der Status zurückgestellt abläuft und die Korrekturaufgabe erneut aktiviert wird. **Hinweis:** Ab Version 18,0 von Container Vulnerability Response Wenn ein zurückgestelltes angreifbares Container-Element (CVIT) vor Ablauf des Ausnahmefensters von einem Scanner geschlossen und erneut geöffnet wird, wird der Status des CVIT in den zurückgestellten Status zurückgesetzt, entsprechend dem aktiven Ausnahmefenster. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft fest *sn_vul.container.auto_defer_cvit_in_active_ex* „wahr“. Darüber hinaus wird das Datum „Zurückgestellt bis“ auch nach dem Schließen des angreifbaren Elements oder dem Ablauf der Ausnahme beibehalten. Die erforderliche Rolle ist „sn_vul_Container.Manage_Exception_Configuration“ für Lese- und Schreibvorgänge. Wenn, nachdem der Datensatz übermittelt wurde E-Mail-Benachrichtigungen Sind definiert, Mitglieder von Container Vulnerability Response Gruppe erhält eine E-Mail, wenn das Ablaufdatum innerhalb einer Woche liegt. Wenn das Zurückstellungsdatum abläuft, wird das angreifbare Element auf „Offen“ zurückgesetzt, und eine zweite E-Mail-Benachrichtigung wird gesendet.
Grund	Geben Sie den Grund für die Zurückstellung des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Falsch positiv ○ Korrektur nicht verfügbar ○ Risiko akzeptiert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Klicken Sie auf **Absenden**.
   Die Gruppe ist markiert **Wird Überprüft** . A **Erneut Öffnen** Der zugehörige Link wird angezeigt. Das Datum und der Grund der erneuten Öffnung werden in Arbeitsnotizen unter angezeigt **Statusänderungsgenehmigungen** Registerkarte.

   Beginnend mit Container Vulnerability Response v2.3 können Sie relevante Informationen im Feld Arbeitsnotizen im Abschnitt „Notizen“ für ein zurückgestelltes angreifbares Container-Element hinzufügen.

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Container-Element an

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Container-Element an, bevor es das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch eine Verlängerung über anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Vulnerability Manager-Arbeitsbereich an.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente**an.
2. Öffnen Sie ein zurückgestelltes angreifbares Container-Element.
3. Wählen Sie Aus **Verlängerung Anfordern** .

   Hinweis:
   Die Schaltfläche „Verlängerung anfordern“ ist nur sichtbar, wenn der Status des angreifbaren Containerelements „Zurückgestellt“ lautet.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem das zurückgestellte angreifbare Container-Element zur Korrektur erweitert werden muss.
Grund	Geben Sie den Grund für die Zurückstellung des Problems ein. Zur Auswahl stehen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Risiko akzeptiert ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei der Übermittlung der Anforderung und der nachfolgenden Aktion durch den Genehmiger wird eine E-Mail ausgelöst.

   Hinweis:
   - Die Anforderung durchläuft zwei Genehmigungsebenen.
   - Wenn ein zurückgestelltes angreifbares Container-Element erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End.

6. Nachdem die Anforderung genehmigt wurde, werden „bis“, „Grund“ und „Zurückstellungshinweise“ aktualisiert.

Arbeiten mit einer Ausnahmeregel in Container Vulnerability Response

Sie können eine Ausnahme für angreifbare Container-Elemente (CVITs) anfordern, die nicht sofort behoben oder zurückgestellt werden können. Durch die Automatisierung des VI-Zurückstellungsprozesses können Sie die übereinstimmenden CVITs basierend auf der Regel zurückstellen, wenn das System sie identifiziert.

Sie können die folgenden Aufgaben für eine Ausnahmeregel ausführen:

- Erstellen Sie eine Ausnahmeregel in Container Vulnerability Response
- Genehmigen Sie eine Ausnahmeregelanforderung in Container Vulnerability Response
- Ausnahmeregel in wird aktiviert Container Vulnerability Response
- Öffnen Sie eine Ausnahmeregel in erneut Container Vulnerability Response
- Aktualisieren Sie eine genehmigte Ausnahmeregel in Container Vulnerability Response
- Löschen Sie eine Ausnahmeregel in Container Vulnerability Response
- Verschieben Sie ein angreifbares Container-Element in Container Vulnerability Response

Hinweis:
Ab v2.5 von Container Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Container-Element in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Container-Element oder die Korrekturaufgabe auf den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Ausnahmeregel in Container Vulnerability Response

Erstellen Sie eine Regel, um automatisch eine Ausnahme für eine bestimmte Bedingung für eine Gruppe angreifbarer Container-Elemente (CVITs) anzufordern, z. B. eine Regel mit einer Bedingung, die auf dem Schwachstellenschweregrad dieser CVITs basiert. Mit dieser Regel können Sie neue und vorhandene CVITs automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Regel wird vom Datum „gültig ab“ bis zum Datum „gültig bis“ angewendet.
Die Korrekturaufgabe (VUL) wird erstellt, wenn die Regel genehmigt wird. Die Gruppierungsmethode für diese SCHWACHSTELLE wird als Ausnahmeregeln bezeichnet. Der WIDERRUF wird im Status zurückgestellt erstellt. Sie können diese ÄNDERUNG nicht schließen, erneut öffnen oder löschen. Neue und erneut geöffnete CVITs werden vom Datum „gültig ab“ bis zum Datum „gültig bis“ zurückgestellt und diesem WIDERRUF hinzugefügt.

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des Workflows für Ausnahmeregeln gesendet. Diese E-Mails enthalten den Status und andere Details einer Anforderung. Wenn beispielsweise eine Ausnahmeregel angefordert wird, erhält die anfordernde Person eine E-Mail, die bestätigt, dass die Anforderung übermittelt wurde.

Hinweis:
Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann erneut zur Genehmigung übermitteln.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**an.
2. Klicken Sie auf der Seite „Ausnahmeregel – neuer Datensatz“ auf **Neu** Dient zum Erstellen einer Regel.
3. Füllen Sie die Felder im Formular „Ausnahmeregel“ aus.

   Hinweis:
   Weitere Informationen zu den Formularfeldern finden Sie unter Formular „Ausnahmeregel“.

4. Fügen Sie die Zuweisungsgruppe hinzu, wenn Sie die Regel erstellen.
5. Übermitteln Sie das Formular zur Genehmigung.
   Der Status der Anforderung ändert sich in „in Überprüfung“. Bis Sie die Ausnahmeregel übermitteln, bleibt sie im Status Entwurf.
6. So zeigen Sie eine Gruppe zum Verwalten von Ausnahmeregeln an und erstellen sie sie:

   a. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**an.

   b. Klicken Sie in einer Ausnahmeregel auf **Angeforderte Genehmigungen** Registerkarte zum Anzeigen des Status der Anforderung.
   Täglich wird eine geplante Aufgabe ausgeführt, die die Ausnahmeregeln für vorhandene Daten ausführt. Alle angreifbaren Elemente, die der Bedingung entsprechen, werden in den Status zurückgestellt verschoben verschoben. Wenn eine genehmigte Ausnahmeregel gelöscht wird, werden alle zurückgestellten angreifbaren Elemente in ihren vorherigen Status zurückgesetzt. Weitere Informationen finden Sie unter Arbeiten mit einer Ausnahmeregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigen Sie eine Ausnahmeregelanforderung in Container Vulnerability Response

Bewerten Sie Ausnahmeregelanforderungen von Anwendern, damit Sie diese Anforderungen genehmigen oder ablehnen können.

Vorbereitungen

Erforderliche Rolle: sn_vul.Exception_Approver

Warum und wann dieser Vorgang ausgeführt wird

Die Mitglieder der Anwendergruppe „Ausnahmegenehmiger“ der Ebene 1 können die Anforderungen der Ausnahmeregel der Ebene 1 genehmigen. Ebenso können die Mitglieder der Anwendergruppe „Ausnahmegenehmiger“ der Ebene 2 die Anforderungen der Ausnahmeregel der Ebene 2 genehmigen. Beide Anwendergruppen erben standardmäßig die Ausnahmegenehmigerrolle.

Hinweis:

Wenn Sie die VR-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht zurück in Workflow ändern. Informationen zum Konfigurieren von Genehmigungsregeln für das Ausnahmemanagement und falsch positive Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Meine Genehmigungen**an.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen oder lehnen Sie die Anforderung mit ab, und erklären Sie, warum Sie die Anforderung genehmigt oder abgelehnt haben.
   Nachdem eine Ausnahmeregel genehmigt wurde, wird standardmäßig eine Korrekturaufgabe im Status zurückgestellt erstellt. Ab dem Datum „gültig ab“ wird diese Regel für alle erstellten CVITs und auch für diejenigen ausgeführt, die vom Status „Geschlossen“ in den Status „Offen“ verschoben werden. CVITs, die den definierten Bedingungen entsprechen, werden der RT hinzugefügt und für den angegebenen Zeitraum zurückgestellt.

   Hinweis:
   Wenn die Regel abgelehnt wird, können Sie sie im Status Entwurf erneut öffnen, aktualisieren und dann erneut zur Genehmigung übermitteln.

Ausnahmeregel in wird aktiviert Container Vulnerability Response

Eine Regel wird am Datum „gültig ab“ aktiviert. Nach der Aktivierung wird der Ausnahmeprozess für angreifbare Container-Elemente (CVITs) automatisiert.

Die Ausnahmeregel folgt diesem Lebenszyklus:

1. Die neuen CVITs, die Sie erstellen oder erneut öffnen und die die angegebene Bedingung erfüllen, werden zurückgestellt. Wenn Sie die Option für vorhandene Daten ausführen aktivieren, wenn Sie die Ausnahmeregel zum ersten Mal ausführen, werden alle aktiven und nicht zurückgestellten CVITs, die der Ausnahmeregelbedingung entsprechen, in die neu erstellte Korrekturaufgabe (RT) verschoben, und ihr Status wird in zurückgestellt geändert.
2. Wenn ein neu erstelltes CVIT der Ausnahmeregelbedingung entspricht, wird es in die zurückgestellte RT verschoben, die der Regel zugeordnet ist, und die Gruppenregel wird nicht dafür ausgeführt.
3. Am Datum „gültig ab“ werden vorhandene CVITs hinzugefügt, wenn Sie die Option für vorhandene Daten ausführen aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Die RT akzeptiert keine neuen CVITs, wenn die Regel am Datum „gültig bis“ abläuft. Die RT bleibt bis zum Datum „zurückgestellt bis“ vorhanden.
5. Die Ausnahmeregel läuft am Datum „gültig bis“ ab.

Öffnen Sie eine Ausnahmeregel in erneut Container Vulnerability Response

Öffnen Sie eine Ausnahmeregel erneut, die abgelehnt wurde, Sie aber erneut übermitteln möchten. Durch erneutes Öffnen der Regel wird sie in den Status Entwurf versetzt.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Regel dann aktualisieren und erneut zur Genehmigung übermitteln.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**an.
2. Suchen Sie die Regel, die Sie erneut öffnen möchten, und klicken Sie auf **Erneut Öffnen** .
3. Aktualisieren Sie das Formular, und übermitteln Sie es erneut zur Genehmigung.

Aktualisieren Sie eine genehmigte Ausnahmeregel in Container Vulnerability Response

Brechen Sie eine genehmigte Regel ab, um sie aktualisieren zu können. Bevor Sie beispielsweise Daten ändern oder einer genehmigten Regel eine Bedingung hinzufügen können, müssen Sie sie abbrechen, damit die Korrekturaufgabe (VUL) gelöscht wird und die angreifbaren Container-Elemente (CVITs) in den Status Offen versetzt werden.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Gruppenregeln werden erneut auf diese CVITs angewendet. Übermitteln Sie die Regel, nachdem Sie die Änderungen vorgenommen haben, damit sie erneut den Genehmigungsprozess durchläuft.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**an.
2. Öffnen Sie die Ausnahmeregel, die Sie abbrechen möchten, und klicken Sie auf **Abbrechen** .
3. Klicken Sie im Dialogfeld Abbruchregel auf **Abbruchregel** .
   Die Regel wird in den Status Entwurf zurückversetzt, und die zugehörige ANNULLIERUNG wird gelöscht. Die zugehörigen CVITs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen CVITs angewendet.

Löschen Sie eine Ausnahmeregel in Container Vulnerability Response

Löschen Sie eine Ausnahmeregel, die nicht mehr erforderlich ist. Sie können beispielsweise eine Regel löschen, wenn Sie ein angreifbares Container-Element (CVIT) während der Erfassung nicht zurückstellen möchten.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

Durch das Löschen einer Regel wird die zugehörige Korrekturaufgabe abgebrochen (VUL). Die zugehörigen CVITs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen CVITs angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**an.
2. Öffnen Sie die Ausnahmeregel, die Sie löschen möchten, und klicken Sie auf **Löschen** .
3. Klicken Sie im Dialogfeld Regel löschen auf **Regel löschen** Zum Löschen der ausgewählten Regel.
   Die zugehörige Korrekturaufgabe wird ebenfalls gelöscht. Die zugehörigen CVITs werden erneut geöffnet, und Gruppenregeln werden auf die einzelnen CVITs angewendet.

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe in an Container Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe (VUL) an, bevor sie das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch eine Verlängerung über anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Vulnerability Manager-Arbeitsbereich an.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Korrekturaufgaben**an.
2. Öffnen Sie eine zurückgestellte Korrekturaufgabe.
3. Wählen Sie Aus **Verlängerung Anfordern** .
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, an dem der Status Zurückstellen abläuft und das angreifbare Container-Element erneut aktiviert wird.
Grund	Geben Sie den Grund für die Zurückstellung des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Risiko akzeptiert ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei Genehmigung der Anforderung werden die Änderungen an der Korrekturaufgabe auch auf die angreifbaren Container-Elemente zurückgesetzt, die Teil der Korrekturaufgabe sind. Die angreifbaren Container-Elemente müssen sich jedoch im Status „zurückgestellt“ und ihren aktuellen Status befinden, bis die Daten vor dem Datum „aktualisiert bis“ liegen. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion durch den Genehmiger ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben nicht verfügbar, die als Teil einer Ausnahmeregel erstellt werden.
- Wenn eine zurückgestellte Korrekturaufgabe erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End.

Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Container Vulnerability Response

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor sie das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Exception_Approver

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch eine Verlängerung über anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Vulnerability Manager-Arbeitsbereich an.

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Ausnahmeregeln**an.
2. Wählen Sie eine zurückgestellte Ausnahmeregel aus.
3. Wählen Sie Aus **Verlängerung Anfordern** .
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel erweitert werden muss.
Grund	Geben Sie den Grund für die Zurückstellung der Ausnahmeregel ein. Zur Auswahl stehen: ○ Risiko akzeptiert ○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Felder Zurückgestellt bis, Grund und zusätzliche Informationen für die Ausnahmeregel und die angreifbaren Container-Elemente aktualisiert. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion durch den Genehmiger ausgelöst.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben nicht verfügbar, die als Teil einer Ausnahmeregel erstellt werden.
- Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End.

Markieren und genehmigen eines falsch positiven Container-Schwachstellenelements

Angreifbare Container-Elemente (CVITs) und Korrekturaufgaben (VULs) können als falsch positive Werte markiert werden. Genehmiger mit Schreibzugriff können solche Anforderungen von anderen Anwendern genehmigen.

- Markieren Sie in als falsch positiv Container Vulnerability Response
- Genehmigen Sie ein falsch positives Ergebnis

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des falsch positiven Workflows gesendet und geben den Status und andere Details einer Anforderung an. Wenn beispielsweise ein CVIT oder eine Korrekturaufgabe als falsch positiv markiert ist, erhält die anfordernde Person eine Bestätigungs-E-Mail. Gleichzeitig erhält der Genehmiger eine E-Mail, in der angegeben wird, dass ein CVIT oder eine Korrekturaufgabe als falsch positiv markiert wurde. Ab v2.5 von Container Vulnerability Response, Sie können die Zeitrahmen für die Genehmigung von falsch positiven Ergebnissen und Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das angreifbare Container-Element in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das angreifbare Container-Element oder die Korrekturaufgabe auf den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Wichtig:
Als Schwachstellenanalyst und Korrekturbesitzer können Sie falsch positive Ergebnisse von anfordern und genehmigen Vulnerability Manager-Arbeitsbereich Und IT-Korrekturarbeitsbereich Entsprechend.

Markieren Sie in als falsch positiv Container Vulnerability Response

Markieren Sie ein angreifbares Container-Element (CVIT) oder eine Korrekturaufgabe als falsch positiv, wenn die vom Scanner gegebene Warnung kein Problem darstellt. Wenn beispielsweise ein CVIT außer Betrieb genommen wurde, der Scanner jedoch weiterhin ein Problem damit aufwirft, markieren Sie es als falsch positiv.

Wichtig:
Als Schwachstellenanalyst und Korrekturbesitzer können Sie falsch positive Ergebnisse von anfordern Vulnerability Manager-Arbeitsbereich Und IT-Korrekturarbeitsbereich Entsprechend.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Korrekturbesitzer

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response (oder Korrekturaufgaben)** > **Alle**an.
2. Öffnen Sie das CVIT, das Sie als falsch positiv markieren möchten, und klicken Sie auf **Als falsch positiv markieren** .
   Das CVIT muss sich in befinden **Öffnen** status.
3. Geben Sie im Formular „falsch positiv“ Details in ein **Zusätzliche Informationen** Und klicken Sie auf **Genehmigung Anfordern** .
   Die Anforderung wird zur Genehmigung gesendet, und der Status des CVIT ändert sich in **Wird Überprüft** . Sowohl die anfordernde Person als auch der Genehmiger werden per E-Mail benachrichtigt.

Genehmigen Sie ein falsch positives Ergebnis

Als falsch positiver Genehmiger können Sie falsch positive Anforderungen von anderen Anwendern genehmigen.

Wichtig:
Sie können falsch positive Anforderungen in genehmigen oder ablehnen Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle: False_positive_Approver
Sie können Ausnahmen und falsch positive Anforderungen auch in der klassischen Umgebung genehmigen:

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Meine Genehmigungen**an.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Hinweis:
Ein falsch positiver Wert kann zeitgebunden sein. Nur der Genehmiger kann das Enddatum festlegen.

Übersicht über Container Vulnerability Response-Korrekturaufgaben und Aufgabenregeln

Konfigurieren Sie Korrekturaufgaben (CVULs), damit Analysten und Korrekturspezialisten angreifbare Container-Elemente (CVIT) organisieren und in Massenanalysen analysieren können. Die Kriterien, nach denen Korrekturaufgaben erstellt werden, werden so konfiguriert, dass CVITs automatisch Korrekturaufgaben zugewiesen werden. Mit Korrekturaufgaben können Sie den Fortschritt überwachen und den Korrekturprozess effizienter steuern.

Entfernen von Zuweisungen aus angreifbaren Containerelementen und Korrekturaufgaben

Ab Version 2,13 können Sie löschen **Zugewiesen an** Und **Zuweisungsgruppe** Felder in angreifbaren Container-Elementen (CVITs) direkt aus den CVIT- und Korrekturaufgaben-Datensätzen, die Sie bestimmen, dass sie Ihnen oder Ihren Gruppen möglicherweise falsch zugewiesen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Siehe Entfernen von Zuweisungen aus angreifbaren Containerelementen und Korrekturaufgaben und Entfernen Sie Zuweisungen aus angreifbaren Elementen und Korrekturaufgaben, um weitere Informationen zu erhalten.

Nachverfolgung der Anzahl der Zurückstellungen für angreifbare Container-Elemente und Korrekturaufgaben

Verfolgen Sie, wie oft ein angreifbares Element, ein angreifbares Anwendungselement, ein angreifbares Container-Element oder eine Korrekturaufgabe zurückgestellt wird. Die geplante Aufgabe „Anzahl der Zurückstellungen festlegen“ wird täglich ausgeführt, um die Anzahl der Datensätze, die mehrmals zurückgestellt werden, in der Spalte „Anzahl der Zurückstellungen“ zu buchen. Datensätze werden in den Modulen „mehrere Zurückstellungen“ für VR, AVR und CVR angezeigt.

Regeln für Korrekturaufgaben verstehen

Mit Regeln für Korrekturaufgaben können Sie definieren, wie angreifbare Container-Elemente automatisch gruppiert und zugewiesen werden. Eine Standardregel **Schwachstelle** Ist im Basissystem enthalten, das CVITs basierend auf ihren Schwachstellen erfasst. Sie können jedoch nach jedem anderen Satz von Werten in Spalten gruppieren, auf die über das CVIT zugegriffen werden kann. Diese Werte können Konfigurationselement (Configuration Item, CI), Schwachstelleneintrag usw. enthalten.

Es gibt Aufgabenregeln für Container Vulnerability Response, die in der Vulnerability Response-Anwendung enthalten sind, die verfügbar ist, wenn Sie sie aktivieren.

Mit dem Bedingungsgenerator können Sie mehrere Bedingungen erstellen. Nachdem Sie ein Feldpaar festgelegt haben, wird im Abschnitt Gruppieren nach eine weitere Zeile angezeigt. Sie können bis zu sechs haben **Gruppieren nach** Auswahlen. Sie können auch die Gruppenzuweisung automatisieren.

Sie können Ihre angreifbaren Container-Elemente beispielsweise nach dem Konfigurationselement oder nach dem Produktmodell gruppieren. Sie können eine Aufgabenregel für Schwachstellen mit niedrigem Schweregrad oder CIs mit niedrigem Risiko haben. Sie können eine andere Aufgabenregel für kritische Server und Schwachstellen haben, die das Unternehmen einem höheren Risiko aussetzen. Siehe Erstellen, bearbeiten und löschen Sie Regeln für Container Vulnerability Response-Korrekturaufgaben Um weitere Informationen zu den Optionen zu erhalten, die Ihnen zur Verfügung stehen.

Für angreifbare Container-Elemente, die das Unternehmen einem größeren Risiko aussetzen, kann ein anderer Satz von Regeln verwendet werden. Der Name der Korrekturaufgabe wird an die Regel der Korrekturaufgabe angehängt **Gruppieren nach** Werte für die Kurzbeschreibung des neuen Datensatzes.

Wenn ein neues angreifbares Container-Element erstellt, importiert oder nach dem Schließen erneut geöffnet wird, werden die Regeln anhand dieses Elements ausgewertet. Ein CVIT wird nur einmal automatisch ausgewertet, es sei denn, es wird nach dem Schließen erneut geöffnet, oder die Regeln werden manuell erneut angewendet.

Der folgende Prozess wird für jedes neue oder erneut geöffnete CVIT verwendet:

- Für jede Korrekturaufgabenregel wird das CVIT mit dem Regelfilter für Korrekturaufgaben verglichen.
- Für jede Regel, bei der die Regelbedingung für Korrekturaufgaben erfüllt ist, ruft die Regel die Daten aus dem ab **Gruppieren nach** Auswahlen im CVIT. Erstellt einen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppennamen und ein Feld. In diesem Fall **Hohes Risiko: QID-32342: Zusammenfassung von QID-3242** (Name: Schwachstellen-ID: Schwachstellen-Zusammenfassung).

Hinweis:
Das Feld „Kurzbeschreibung“ ist auf 160 Zeichen beschränkt. Längere Schwachstellenzusammenfassungen werden gekürzt.

Die Regel überprüft, ob eine Übereinstimmung vorhanden ist **Öffnen** Korrekturaufgabe, die derselben Zuweisungsgruppe wie CVIT zugewiesen ist.

- Wenn die Aufgabe gefunden wird, wird das CVIT der vorhandenen Aufgabe in hinzugefügt **Öffnen** Status.
- Wenn keine Aufgabe in **Öffnen** status wurde gefunden, die Regel erstellt einen **Hohes Risiko: QID-32342** Aufgabe, weist sie derselben Zuweisungsgruppe wie CVIT zu und platziert das CVIT in der Korrekturaufgabe.

Es kann mehr als eine Regel für Korrekturaufgaben definiert werden, um verschiedene Arten von Schwachstellen zu gruppieren. Da jede Schwachstelle mit den Regelbedingungen für Korrekturaufgaben verglichen wird, bevor sie in eine Korrekturaufgabe eingefügt wird, können sich zu viele Regeln auf die Leistung auswirken. Richten Sie Ihre Aufgabenregeln so ein, dass die Bedingungen Ihnen helfen, doppelte Korrekturaufgaben zu vermeiden.

Standardmäßig verwenden Regeln für Korrekturaufgaben die vom festgelegte Zuweisungsgruppe **Zuweisungsregeln** In CVIT beim Gruppieren der Elemente und weist die Korrekturaufgabe zu, um sie den CVITs zu entsprechen.

Als Teil der Standardaufgabenregel wird die Zuweisung dieser Korrekturaufgaben durch die Regeln in gesteuert **Zuweisungsregeln** Modul. Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response-Zuweisungsregeln – Übersicht.

Wenn eine Aufgabenregel aus der Formular- oder Listenansicht gelöscht wird, haben Sie die Möglichkeit, alle offenen Aufgaben zu löschen, die von dieser Regel erstellt wurden. Aufgaben nicht in **Öffnen** Status sind ausgeschlossen.

Regeln für Korrekturaufgaben werden erneut angewendet

Wenn Sie eine Korrekturaufgabenregel ändern möchten, verwenden Sie **Erneut Anwenden** Schaltfläche auf der Seite mit der Regel für Korrekturaufgaben, um die geänderte Regel für alle aktiven erneut auszuführen **Öffnen** Von dieser Regel erstellte Korrekturaufgaben. Korrekturaufgaben werden automatisch basierend auf der geänderten Regel gelöscht und neu erstellt.

Erneut Anwenden Überprüft nur vorhandene Korrekturaufgaben.

Nachdem Sie ausgewählt haben **Erneut Anwenden** , Die folgende Meldung wird angezeigt: Durch erneutes Anwenden dieser Korrekturaufgabenregel werden die Korrekturaufgaben für diese Regel gelöscht und neu erstellt. Korrekturaufgaben, die sich nicht im Status „Offen“ befinden, werden nicht gelöscht.

Wichtig:
Als Schwachstellenadministrator und -Analyst können Sie die Regeln für Korrekturaufgaben für ausgewählte angreifbare Elemente in auswerten Arbeitsbereich des Schwachstellenmanagers. Diese Methode ist effizienter als die erneute Anwendung der Regeln für Korrekturaufgaben in der klassischen Anwenderoberfläche, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Arbeitsbereich des Schwachstellenmanagers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regeln für Korrekturaufgaben und CVIT-Erstellung und -Aktualisierung

Wenn ein CI aus einem Scan einer bekannten Schwachstelle zugeordnet ist, wird ein CVIT erstellt. Nach der Erstellung wird das CVIT anhand der Bedingungen der Regeln für Korrekturaufgaben für eine Übereinstimmung ausgewertet. Wenn eine Übereinstimmung mit einer vorhandenen Korrekturaufgabe besteht, wird das CVIT hinzugefügt. Wenn keine übereinstimmende Korrekturaufgabe gefunden wird, wird eine für das CVIT erstellt.

Wenn eine Eigenschaft, die in den Filterbedingungen für Korrekturaufgaben erfasst wird, in einem CVIT aktualisiert oder geändert wird, wird die aktualisierte AVI auch anhand der Regeln für Korrekturaufgaben für eine Übereinstimmung ausgewertet. Wenn eine Übereinstimmung mit einer vorhandenen Korrekturaufgabe besteht, wird das CVIT hinzugefügt. Wenn keine übereinstimmende Korrekturaufgabe gefunden wird, wird eine für das CVIT erstellt.

Status-Rollup und Rolldown

Wenn Sie eine Korrekturaufgabe auf „Offen“ oder von „Offen“ auf „wird untersucht“ aktualisieren, wird der neue Status auf alle zugehörigen CVITs zurückgesetzt. Status-Rollup erfolgt unmittelbar nach dem Ändern des Status.

Status-Rollup von CVITs zur Korrekturaufgabe findet nur statt, wenn sich alle CVITs in der Aufgabe befinden **Zurückgestellt** Oder **Geschlossen: Behoben** status. Rollup wird mit den Werten des angreifbaren Containerelements in Vulnerability und einer geplanten Gruppenaufgabe durchgeführt, die alle 15 Minuten ausgeführt wird. Der Status wird erst nach Ausführung des Auftrags als Rollup ausgeführt. Damit ein Status-Rollup von den CVITs zur Korrekturaufgabe erfolgt, müssen sich alle CVITs im gleichen Status befinden.

Erstellen, bearbeiten und löschen Sie Regeln für Container Vulnerability Response-Korrekturaufgaben

Sie können Regeln erstellen, um angreifbare Container-Elemente (CVIT) basierend auf Filterbedingungen automatisch in Korrekturaufgaben (CVUL) zu gruppieren. Diese Regeln gruppieren CVITs automatisch, wenn sie importiert oder manuell erstellt werden.

Vorbereitungen

Wenn Sie eine neue Regel erstellen, gilt sie nicht für vorhandene Daten. Nachdem Sie sie übermittelt haben, wird sie für neue Importe ausgeführt.

Erforderliche Rolle: App-Sec-Manager

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Administration** > **Regeln Für Korrekturaufgaben.**an.
2. Öffnen Sie die Regel, oder wählen Sie aus **Neu** .
3. Füllen Sie die Felder im Formular aus, oder bearbeiten Sie sie.

Regel für Korrekturaufgaben

Feld	Beschreibung
Name	Name der Aufgabenregel.
Aktiv	Gibt an, ob die Aufgabe aktiv ist.
Beschreibung	Eine Beschreibung der Regel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Groß-/Kleinschreibung beachten	Bestimmt, ob bei einer Bedingung die Groß-/Kleinschreibung beachtet wird oder nicht. **Hinweis:** Beim Standardwert wird die Groß-/Kleinschreibung nicht berücksichtigt.
Bedingung	Optionale Filterbedingungen für die Regel. Standardmäßig (**Groß-/Kleinschreibung beachten** Kontrollkästchen nicht aktiviert), wird bei dem Suchtext, den Sie in den Bedingungsgenerator für Aufgabenregeldatensätze und -Formulare eingeben, die Groß-/Kleinschreibung nicht beachtet. Sie haben die Möglichkeit, Suchvorgänge mit Groß-/Kleinschreibung in Aufgabendatensätzen und -Formularen zu aktivieren. Eine Beispielbedingung ist **Schwachstelle** > **ist** > **VULNENT123451** (Bekannte importierte Schwachstelle). Alle CVIT mit dieser Schwachstelle entsprechen dieser Bedingung.
Gruppieren nach (bis zu sechs Bedingungssätze sind verfügbar)	
Gruppieren Sie angreifbare Container-Elemente aus	Die Tabelle, die die Regel zum Gruppieren von CVITs verwendet. Wählen Sie die Elemente aus der Struktur aus: ○ Angreifbares Container-Element [sn_vuln_vulnerable_item] ○ Angreifbares Container-Element: Docker-Image ○ Angreifbares Container-Element: Container-Schwachstelle **Hinweis:** Wenn Sie eine erweiterte Tabelle auswählen, wird die **Feld wird verwendet** Wird nur für angreifbare Anwendungselemente angewendet, die diese erweiterte Tabelle verwenden.
Mit Feld	Feld in der Tabelle, das die Regel zum Gruppieren von CVITs verwendet. Wählen Sie Bedingungen aus der Struktur aus.
Zuweisung	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Korrekturaufgaben zuweisen nach	Wenn Korrekturaufgaben automatisch zugewiesen werden, wird zusätzlich zu die Zuweisungsauswahl verwendet **Gruppieren Nach** Auswahlmöglichkeiten zum Gruppieren der angreifbaren Elemente. Neue Aufgaben werden nach Bedarf erstellt, sodass jedes CVIT in einer Aufgabe mit einem übereinstimmenden Zuweisungsgruppensatz platziert wird. Um die Zuweisung von Aufgaben zu automatisieren, die basierend auf dieser Regel erstellt wurden, wählen Sie eine der verfügbaren Optionen aus. ○ Feld „Gruppieren nach“: Wenn Sie ein Anwendergruppenfeld aus ausgewählt haben **Feld wird verwendet** Werte in **Gruppieren nach** Abschnitt, werden sie im Dropdown-Menü angezeigt. ○ Anwendergruppe: Verwenden Sie die Suchliste, um eine statische Anwendergruppe auszuwählen.

Hinweis:
Wenn Sie eine Regel entweder aus der Formular- oder Listenansicht löschen, haben Sie die Möglichkeit, alle offenen Korrekturaufgaben zu löschen, die von dieser Regel erstellt wurden. Gruppen, die sich nicht im Status „Offen“ befinden, werden ausgeschlossen.

4. Wählen Sie Aus **Übermitteln** Für neue Regeln.
Nachdem Sie ausgewählt haben **Übermitteln** , Ihre Regel wird in der Liste Regeln für Korrekturaufgaben [sn_vul_grouping_rule] angezeigt. Die folgenden Situationen initiieren Ihre Regel.
   - Wenn neue CVITs erstellt werden.
   - Wenn Sie auswählen **Erneut Anwenden** . Sie wählen aus **Erneut Anwenden** Dient zur Auswertung von Aufgabenregeln nur für vorhandene Korrekturaufgaben.
   - Wenn CVITs aktualisiert werden, entweder von Ihnen oder vom System.

     Wenn ein CVIT aktualisiert wird, werden Aufgabenregeln auf Übereinstimmungen mit vorhandenen Korrekturaufgaben ausgewertet. Einige häufige Updates, die eine Regelprüfung initiieren, sind:
     - Wenn sich der Status von „Geschlossen“ in „Offen“ oder von „Geschlossen“ in „wird untersucht“ ändert.
     - Das Konfigurationselement (CI) wird geändert.
     - Die Schwachstelle wird geändert.

   Das System überprüft alle Aufgabenregeln auf Übereinstimmungen mit dem aktualisierten CVIT. Wenn die Bedingungen einer Regel den Bedingungen einer Korrekturaufgabe entsprechen, werden ihr übereinstimmende CVITs zugewiesen.

   Wenn keine Übereinstimmung gefunden wird, wird eine neue Korrekturaufgabe erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Status-Rollup von CVITs zu Korrekturaufgaben und zum Status-Rollup von Korrekturaufgaben zu CVITs finden Sie unter Übersicht über Container Vulnerability Response-Korrekturaufgaben und Aufgabenregeln.

Ein Beispiel für eine Regel für Korrekturaufgaben finden Sie unter Anwendungsschwachstellen-Antwort-Korrekturaufgaben-Regelbeispiele.

5. Um eine Aufgabenregel zu löschen, wählen Sie die Regel aus der Liste Regeln für Korrekturaufgaben aus, und wählen Sie Löschen.
Die folgende Meldung wird angezeigt: Die ausgewählte Regel für Korrekturaufgaben hat n Korrekturaufgaben erstellt. Von den Korrekturaufgaben befinden sich n im Status Offen.

Option	Beschreibung
Kontrollkästchen deaktiviert (Standard).	Löschen Sie nur die Regel. Aufgaben, die sich nicht im Status „Offen“ befinden, werden ausgeschlossen.
Kontrollkästchen ausgewählt.	Schließen Sie die Korrekturaufgaben in den Status Offen ein, wenn Sie die Regel für Korrekturaufgaben löschen. Löschen Sie die Regel und alle Korrekturaufgaben im Status Offen.

6. Wählen Sie eine Option aus, und wählen Sie aus **Löschen** .

Erstellen Sie Regeln zum automatischen Schließen für Container Vulnerability Response

Verwenden Sie Regeln zum automatischen Schließen, um ältere angreifbare Container-Elemente (CVITs) basierend auf den von Ihnen festgelegten Filterbedingungen automatisch zu schließen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Container_Manage_Auto_close_stale_VI

Prozedur

1. Navigieren zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente** > **Regeln für automatisches Schließen**an.

   Das Basissystem bietet die folgenden Regeln für das automatische Schließen: **Zuletzt gescannte Container-Schwachstellen** : Schwachstellen, die in den letzten 90 Tagen nicht gemeldet wurden, werden in den Status „Veraltet“ versetzt.

2. Wählen Sie Aus **Neu** Dient zum Erstellen einer Regel zum automatischen Schließen.
3. Füllen Sie die Felder des Formulars aus.

Feld	Wert
Name	Name der Regel zum automatischen Schließen.
Aktiv	Option zum Aktivieren der Regel. Wenn diese Option aktiviert ist, werden alle Erkennungen, die den Filterkriterien entsprechen, automatisch geschlossen.
Ausführungsreihenfolge	Eindeutiger Wert für die Ausführung der Regel zum automatischen Schließen. Dieser Wert bestimmt die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	Reihenfolge der Ausführung. Der Standardwert ist 100.
Integrationstyp	Integration von Container-Schwachstellen **Hinweis:** Um Host-Schwachstellen mit der Prisma Cloud Compute-Integration zu scannen, wählen Sie aus **Integration Des Schwachstellen-Scanners** .
Beschreibung	Beschreibung der Regel zum automatischen Schließen.
Bedingung	Filterbedingungen, die verwendet werden, um Erkennungen zu identifizieren, die geschlossen werden sollen.

4. Wählen Sie **Absenden**.
   Die **Automatisch Schließen** Regeln geplante Aufgaben werden täglich ausgeführt. Identifiziert CVITs basierend auf den angegebenen Bedingungen und überträgt die übereinstimmenden zu **Veraltet** status. In Fällen, in denen CVITs mit dem Status „Geschlossen“ und „Veraltet“ vorhanden sind, wird das CVIT mit dem Substatus „behoben“ geschlossen.

Entfernen von Zuweisungen aus angreifbaren Containerelementen und Korrekturaufgaben

Sie können löschen **Zugewiesen an** Und **Zuweisungsgruppe** Felder in angreifbaren Containerelementen direkt aus den Datensätzen für angreifbare Container-Elemente und Korrekturaufgaben, die Sie bestimmen, dass sie Ihnen oder Ihren Gruppen möglicherweise falsch zugewiesen sind.

Übersicht für den Workflow

Wenn Sie feststellen, dass angreifbare Container-Elemente (CVITs) und Korrekturaufgaben (CVULs) nicht in Ihrem Korrekturbereich liegen, oder wenn Sie der Meinung sind, dass Datensätze Ihnen oder Ihren Gruppen falsch zugewiesen wurden, können Sie sich selbst oder Ihre Gruppen aus dem entfernen **Zugewiesen an** Und **Zuweisungsgruppe** Felder in CVIT- und CVUL-Datensätzen.

Der Workflow zum Aufheben der Zuweisung wird in Arbeitsbereichen und in klassischen Ansichten und Arbeitsbereichsansichten für CVITs und CVULs unterstützt.

Sie haben die Möglichkeit, Anforderungen zum Löschen der Zuweisungsfelder zur Genehmigung zu senden. Siehe Genehmigen oder lehnen Sie eine Anforderung zum Aufheben der Zuweisung in ab Vulnerability Response und Entfernen von Zuweisungen aus angreifbaren Elementen und Korrekturaufgaben, um weitere Informationen zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die **Zuweisung Aufheben** Die UI-Aktion wird in CVIT- und CVUL-Datensätzen in einem anderen Status als „Geschlossen“ oder „gelöst“ angezeigt.

  Hinweis:
  Nachdem die Anforderung zum Löschen der Felder für eine CVUL genehmigt wurde, alle **Zugewiesen an** Und **Zuweisungsgruppe** Felder in CVITs, die dieselbe Zuweisungsgruppe haben, sind nicht zugewiesen. Wenn ein CVIT in einem CVUL eine andere Zuweisungsgruppe als das zugehörige CVUL hat, wird die Zuweisung nicht aufgehoben. In den meisten Fällen wurden diese CVITs manuell zugewiesen. Siehe Übersicht über Container Vulnerability Response-Korrekturaufgaben und Aufgabenregeln und Entfernen von Zuweisungen aus angreifbaren Elementen und Korrekturaufgaben, um weitere Informationen zu erhalten.

- Alle Datensätze, die Sie entweder mit der UI-Aktion oder manuell aktualisieren, werden im Modul „nicht zugewiesen“ für Container Vulnerability Response angezeigt.

Siehe Entfernen Sie Zuweisungen aus angreifbaren Elementen und Korrekturaufgaben Weitere Informationen zu den Schritten zum Löschen der Zuweisungsfelder.

Systemeigenschaften und Genehmigungsbenachrichtigungen

Wenn ein Korrekturbesitzer auswählt **Zuweisung Aufheben** In einem Datensatz löst standardmäßig die Systemeigenschaft sn_vul.unassign_vr.Approval_required den Genehmigungs-Flow aus und erstellt einen Datensatz für die Genehmigung einer Statusänderung im Status Überprüfen, und die Anforderung wird zur Genehmigung weitergeleitet. Die Anforderung wird in der Liste meine Genehmigungen für Anwender mit sn_vul_Container.unassign_Approver angezeigt.

Hinweis:
Als Schwachstellenadministrator [sn_vul.Vulnerability_admin] können Sie festlegen *`sn_vul.unassign_vr.approval_required`*Systemeigenschaft zu **Falsch** Zum Deaktivieren des Genehmigungsprozesses.

Darüber hinaus können Sie den Wert in ändern *`sn_vul.default_assignment_group`*Systemeigenschaft. Wenn die Zuweisungsfelder gelöscht werden, wird eine bestimmte Gruppe zugewiesen. Beispiel: Wenn ein Anwender auf klickt **Zuweisung Aufheben** In einem Datensatz, der zur Überprüfung an eine bestimmte Gruppe weitergeleitet werden soll, können Sie die System-ID für die Gruppe Ihrer Wahl im Feld Wert der Systemeigenschaft hinzufügen.

Hinweis:
Wenn Sie diesen Wert ändern, werden Benachrichtigungen für alle nicht zugewiesenen Vits, AVITs und CVITs an die von Ihnen angegebene Gruppe gesendet.

Schließen Sie eine Korrekturaufgabe

Wenn Sie feststellen, dass das Problem, das einer Anwendungskorrekturaufgabe zugeordnet ist, sofort ohne weitere Analyse geschlossen werden kann, können Sie verwenden **Schließen** Funktion. Ab v2.10 von Container Vulnerability Response, **Schließen** Schaltfläche wurde für eine Container-Korrekturaufgabe entfernt.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
In Vulnerability Response Arbeitsbereiche, eine Korrekturaufgabe durchläuft dieselben status wie eine Korrekturaufgabe, die zuvor in früheren Versionen von durchgeführt wurde

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response. Wenn alle angreifbaren Elemente (Vits) in einer Korrekturaufgabe geschlossen sind, wechselt die Korrekturaufgabe in den Status Inaktiv.

Wichtig:
Sie können Change-Anforderungen und Korrekturaufgaben manuell durch die status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn die Statussynchronisierung aktiviert ist. Wenn das System jedoch registriert, dass ein CHG seinen Status geändert hat, oder Sie ein CHG hinzufügen oder es aus einer Korrekturaufgabe entfernen, kann die Statussynchronisierung Ihren manuellen Eingriff möglicherweise überschreiben. Change-anforderungsstatus verschieben Korrekturaufgaben jedoch nicht automatisch aus dem Geschlossen Oder Zurückgestellt status.

Prozedur

1. Öffnen Sie den Datensatz, für den Sie eine Überprüfung anfordern möchten.
2. Wählen Sie aus **Schließen** Schaltfläche.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Status	Wählen Sie den Status als aus *Geschlossen* .
Grund	Geben Sie den Grund für das Schließen des Problems ein.
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

4. Wählen Sie **Absenden**.
   Die Korrekturaufgabe ist markiert **Geschlossen** .

IT Operations Management Und Muster-Discovery

Wenn die Discovery aktiviert ist, werden Informationen vom empfangen Information Technology Operations Management(ITOM)-Team. Wenn ITOM Discovery ist aktiviert. Sie können Kubernetes-Namespaces, Kubernetes-Cluster und Kubernetes-Services anzeigen, wenn Sie ein angreifbares Container-Element (CVIT) öffnen. Andernfalls können Sie Informationen zur Prisma-Nutzlast anzeigen.

Die Image-Bezeichnungen aus den Prisma-Nutzlasten werden als Schlüssel-Wert-Paare unter dem Docker-Image gespeichert. Die Bezeichnungen in einer Prisma-Nutzlast werden in der Tabelle „cmdb_key_value“ gespeichert. Um diese Funktion zu aktivieren, wird vom ITOM-Team eine Identifizierungsregel für cmdb_ci_Docker_image verschickt. Öffnen Sie das Docker-Bild, um die Liste der zugehörigen Elemente anzuzeigen. Die meisten Elemente werden von ausgefüllt ITOM Team. Der Identifizierungseintrag für ein Docker-Image wird geliefert, um die Werte als Schlüssel-Wert-Paare anzuzeigen.

Die Geschäftsrelevanz wird basierend auf den Service-Relevanzinformationen bestimmt, die von empfangen wurden ITOM Team. Eine geplante Aufgabe wird ausgeführt, um Daten aus allen Services abzurufen, die einem Image zugeordnet sind. Berechnet die Geschäftsrelevanz basierend auf der Servicezuordnung. Da die Risikopunktzahl von der Geschäftsrelevanz abhängen kann, wird auch die Risikopunktzahl basierend darauf berechnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Analytics- und Reporting-Lösungen für Container Vulnerability Response

Dies Platform Analytics-Lösung Enthält vorverpackt Platform Analytics Inhalt zur Verwendung mit anderen ServiceNow AI Platform Produkte. Dies Platform Analytics-Lösung Stellt ein Risiko dafür bereit, wie Schwachstellen über die verschiedenen Diagramme verwaltet werden.

Erforderliche Rollen

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet:

- ServiceNow AI Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Platform Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Container Vulnerability Response-Dashboard

Analytics- und Reporting-Lösungen enthalten vorpaketierte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen ServiceNow AI Platform-Produkten. Dies Platform Analytics-Lösung Ermöglicht Ihnen, das Volumen, die Leistung und den Fortschritt von Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur nachzuverfolgen. Sie können Berichte nach Zuweisungsgruppe, Exploits, Risikobewertung oder Status filtern.

Erforderliche ServiceNow AI Platform-Rollen

- ServiceNow AI Platform-Administrator (admin): Installieren und aktivieren Sie diese Analytics- und Reporting-Lösung und nehmen Sie alle erforderlichen Änderungen an den Systemeigenschaften vor.
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Zugriff auf das Dashboard von Container Vulnerability Response

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Container Vulnerability Response** > **Übersicht**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

Ab Version 2,2 von Container Vulnerability Response, Dieses Dashboard kann auch in angezeigt werden Next Experience UI. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** Und wählen Sie aus **Dashboards** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, wählen Sie die Dropdown-Liste neben dem Dashboard-Namen aus. Weitere Informationen finden Sie unter Seite „Dashboards“ in Arbeitsbereich des Schwachstellenmanagers und Seite „Dashboards“ in Arbeitsbereich für IT-Korrekturen.

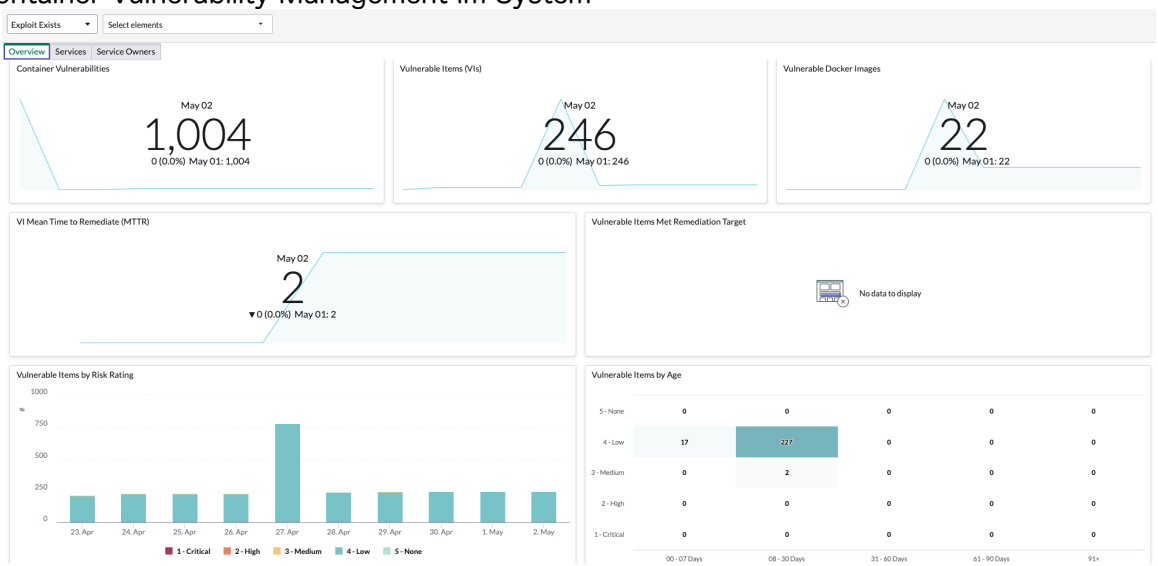
Hinweis:

- Wenn Sie ein neuer Anwender sind, können Sie die Dashboards nur über die Arbeitsbereiche anzeigen.
- Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Container Vulnerability Management-Registerkarten

In diesem Dashboard können Sie die Schwachstellen anzeigen, die in Containern vorhanden sind. Sie können die Schwachstellen und die zugehörigen Daten nach Region, Alter, Services und anderen Aufgliederungen anzeigen.

Die **Übersicht**Die Registerkarte stellt den Gesamtstatus von Container Vulnerability Management im System

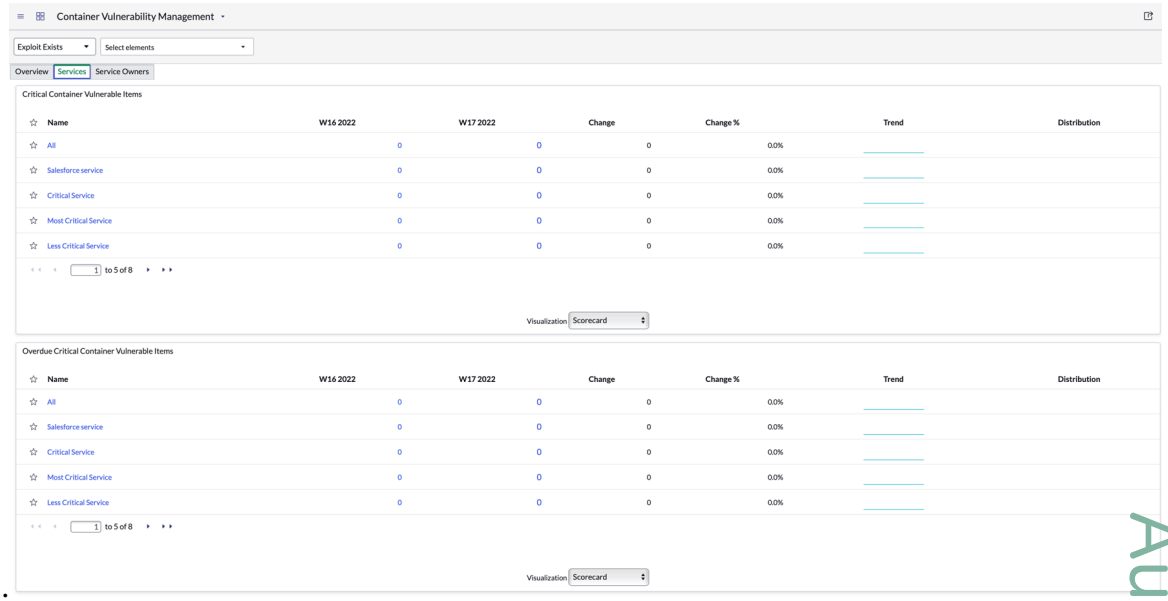


bereit.

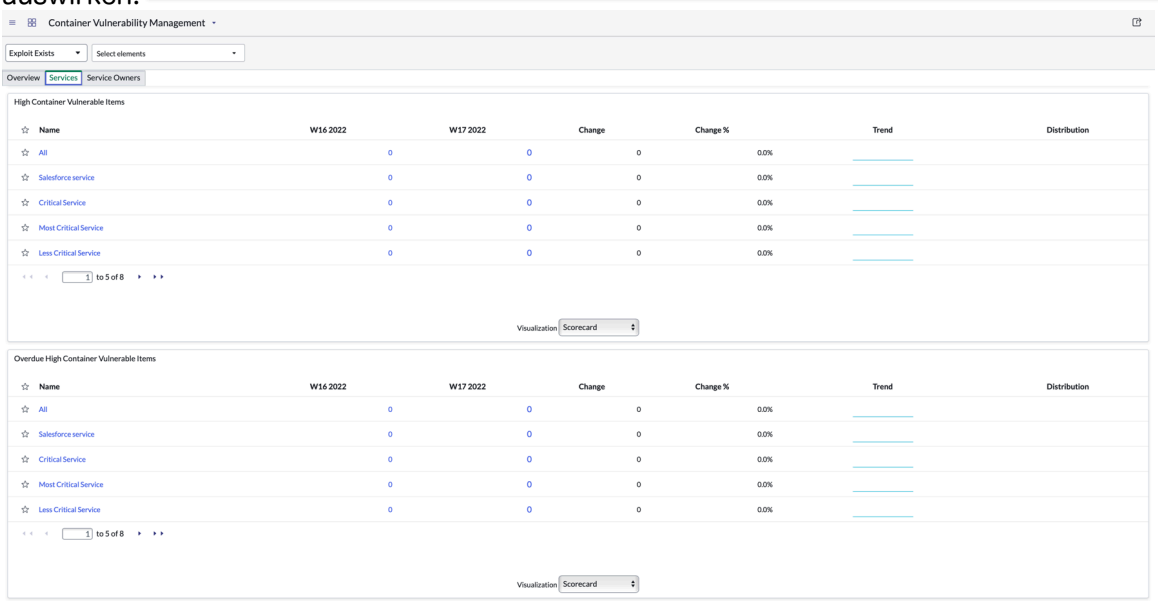
Die **Services**Auf der Registerkarte werden angreifbare Container-Elemente angezeigt, die sich auf Anwendungsservices

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



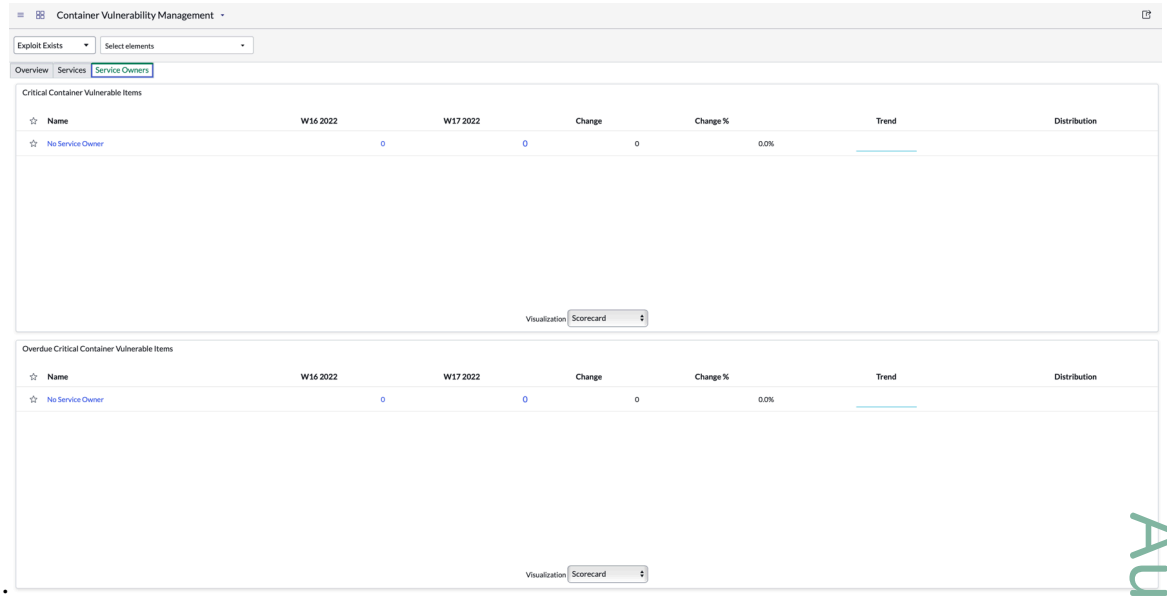
auswirken.



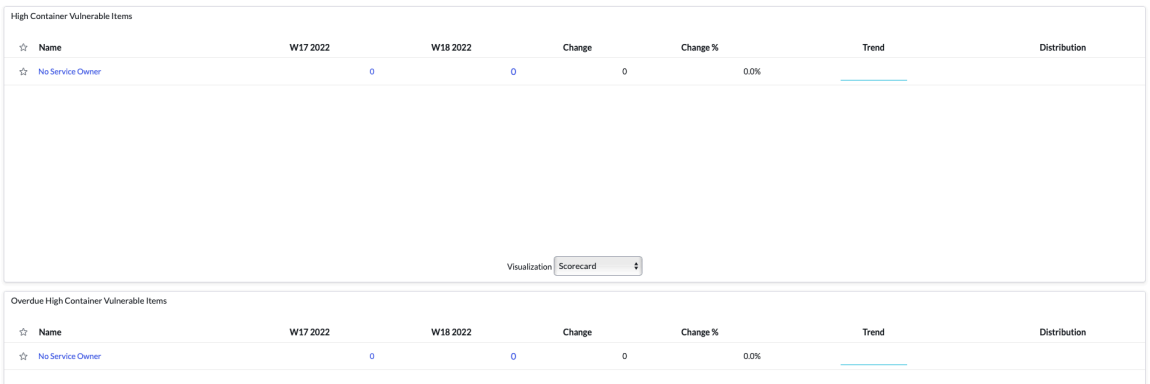
Die **Serviceverantwortliche**Auf der Registerkarte werden angreifbare Container-Elemente angezeigt, die sich auf Serviceverantwortliche

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



auswirken.



Aufgliederungen

- Exploit vorhanden
- Exploit-Angriffsvektor
- Exploit-Kompetenzniveau
- Nachbesserungszielstatus
- Risikobewertung
- Status
- Zuweisungsgruppe

Automatische Übersetzung

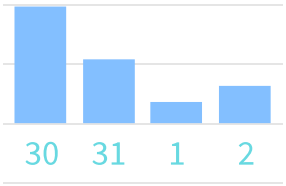
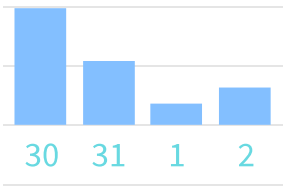
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenvisualisierungen

Name	Typ	Beschreibung
Container-Schwachstellen	Einzelwert	Anzahl der Container-Schwachstellen, die mit einem oder mehreren aktiven angreifbaren Container-Elementen verknüpft sind.
Angreifbare Elemente (AEs)	Einzelwert	Anzahl der aktiven (nicht geschlossener) angreifbaren Containerelemente.
Angreifbare Docker-Images	Einzelwert	Anzahl der Docker-Images, die mit aktiven angreifbaren Container-Elementen verknüpft sind.
Durchschnittliche VI-Zeit bis zur Korrektur (MTTR)	Einzelwert	Die durchschnittliche Zeit für die Nachbesserung (Schließung) eines angreifbaren Elements, angezeigt als laufender 30-Tage-Durchschnitt.
Angreifbare Elemente mit erfülltem Korrekturziel	Einzelwert	Prozentsatz der geschlossenen angreifbaren Container-Elemente, die ihre Korrekturzieldaten im aktuellen und vorherigen Quartal erreicht haben. Korrekturziele werden aus dem Datum der letzten Öffnung plus der Anzahl der Tage berechnet.

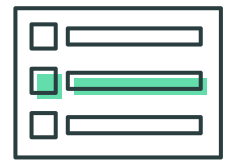
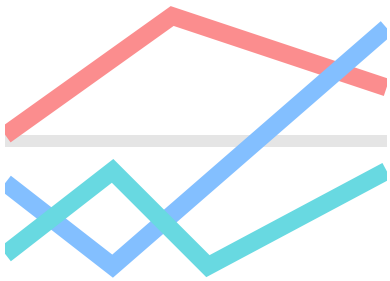
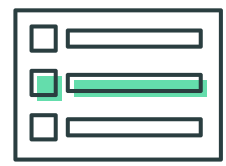
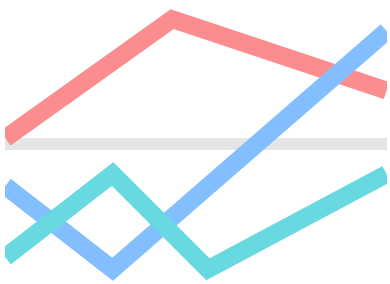
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Angreifbare Elemente nach Risikobewertung	Balken 	Anzahl der aktiven angreifbaren Container-Elemente, gruppiert nach Risikobewertung für die ausgewählte Zeitspanne.
Angreifbare Elemente nach Alter	Balken 	Anzahl der aktiven angreifbaren Container-Elemente gruppiert nach Risikobewertung und Alter (in Tagen). **Hinweis:** Das Anpassen der Berechnung von Alter und Alter der geschlossenen Elemente für angreifbare Container-Elemente (CVIS) kann zu einem starken Anstieg oder Rückgang der Performance Analytics (PA)-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung des Alters und des Alters, das für CVIS geschlossen wurde, finden Sie unter KB1703270 KB-artikel.

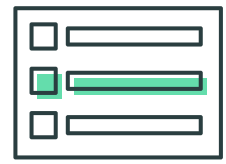
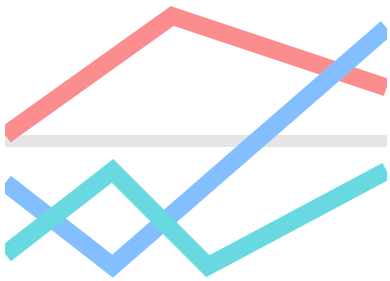
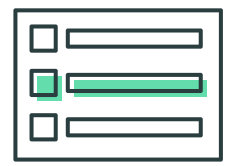
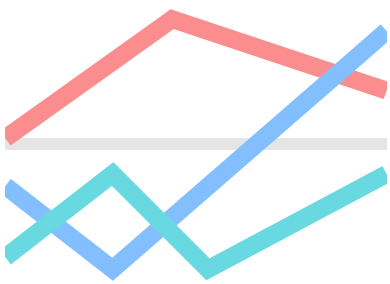
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Kritische angreifbare Container-Elemente	Liste und Zeile  	Anzahl der aktiven angreifbaren Container-Elemente mit kritischer Risikobewertung, gruppiert nach Service.
Überfällige kritische angreifbare Container-Elemente	Liste und Zeile  	Anzahl der aktiven angreifbaren Container-Elemente mit einer kritischen Risikobewertung, die ihre Korrekturzieldaten überschritten haben, gruppiert nach Service.

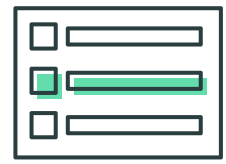
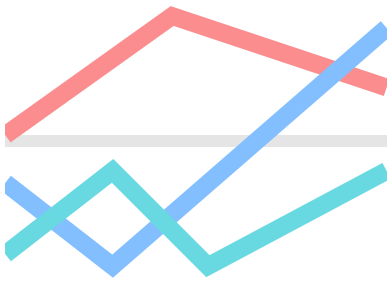
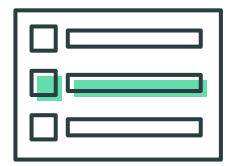
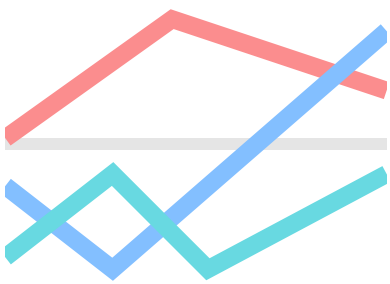
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Hoch angreifbare Container-Elemente	Liste und Zeile  	Anzahl der aktiven angreifbaren Container-Elemente mit hoher Risikobewertung, gruppiert nach Service.
Überfällige, hoch angreifbare Container-Elemente	Liste und Zeile  	Anzahl der aktiven angreifbaren Elemente mit einer hohen Risikobewertung, die ihre Korrekturzieldaten überschritten haben, gruppiert nach Service.

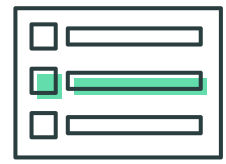
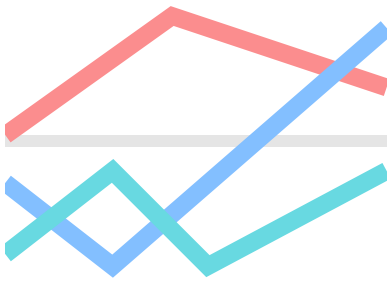
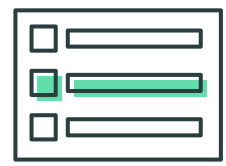
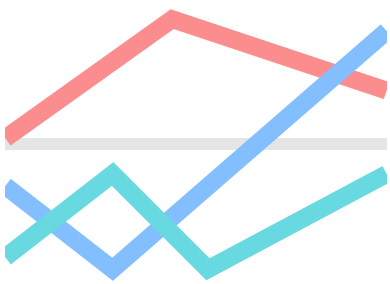
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Kritische angreifbare Container-Elemente	Liste und Zeile  	Anzahl der aktiven angreifbaren Container-Elemente mit kritischer Risikobewertung, gruppiert nach Serviceverantwortlicher.
Überfällige kritische angreifbare Container-Elemente	Liste und Zeile  	Anzahl der aktiven angreifbaren Container-Elemente mit einer kritischen Risikobewertung, die ihre Korrekturzieldaten überschritten haben, gruppiert nach Serviceverantwortlicher.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Hoch angreifbare Container-Elemente	Liste und Zeile  	Anzahl der aktiven angreifbaren Container-Elemente mit hoher Risikobewertung, gruppiert nach Serviceverantwortlicher.
Überfällige, hoch angreifbare Container-Elemente	Liste und Zeile  	Anzahl der aktiven angreifbaren Elemente mit einer hohen Risikobewertung, die ihre Korrekturzieldaten überschritten haben, gruppiert nach Serviceverantwortlicher.

Framework für zusammengefasste Berichte für Container Vulnerability Response

Mit dem Framework für zusammengefasste Berichte können Sie Berichte für die Daten erstellen, die komplexe und lang laufende On-the-fly-Abfragen umfassen, um die Leistung zu verbessern.

Das Framework für zusammengefasste Berichte verbessert die Leistung durch:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwendung weniger Ressourcen und schnelleres Rendern von Berichten,
- Aggregieren der Daten und Wiederverwendung von Zusammenfassungen und Aufgliederungen (Gruppieren nach) und
- Die Abfragen in der Datenbank werden reduziert

Wenn Sie mehr als eine Million angreifbare Container-Elemente (CVITs) haben, verwenden Sie das Framework für zusammengefasste Berichte neben den Standardberichten.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- ServiceNow AI Platform Administrator (admin): Installiert und aktiviert Platform Analytics-Lösung und nimmt alle erforderlichen Änderungen an Systemeigenschaften vor.
- Performance Analytics Administrator (PA_admin): Überprüfen Sie die Zusammenfassungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.
- Administrator (sn_vul_cmn.admin): Zusammenfassungen erstellen.
- VR write(sn_vul_cmn.write): Bearbeiten Sie die Daten in den Zusammenfassungen und aggregierten Ergebnissen.
- VR-Lesen (sn_vul_cmn.read): Überprüfen Sie die Daten in den Zusammenfassungen und aggregierten Ergebnissen.
- Schwachstellenanalyst (sn_vul.Vulnerability_Analyst): Überprüfen Sie die zusammengefassten Ergebnisse.

Zugehörige Informationen

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Container Vulnerability Response – Referenz

Referenzthemen mit Informationen zu Tabellen, Rollen und Eigenschaften, die mit installiert sind Container Vulnerability Response.

Mit Container Vulnerability Response installierte Komponenten

Bei der Aktivierung der Anwendung Container Vulnerability Response werden mehrere Arten von Komponenten installiert, z. B. Tabellen, Benutzerrollen und regelmäßige Aufgaben.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Ab v2.11 von Container Vulnerability Response, Die am häufigsten verwendeten Systemeigenschaften sind jetzt innerhalb von zugänglich Container Vulnerability Response Anwendung. Um diese Systemeigenschaften anzuzeigen, navigieren Sie zu **Alle**Container Vulnerability Response**Eigenschaften**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Container Vulnerability Response installierte Rollen

Rollen werden bei der Aktivierung von Container Vulnerability Response hinzugefügt.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender und Gruppen in sehen und tun können Vulnerability Response Anwendung. Informationen zur ersten Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent. Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Hinweis:

Wenn Sie ein Upgrade-Kunde sind, hat sich der Zugriff für die Anwender und Gruppen, die Sie mit den Berechtigungen sn_vul.Vulnerability_read und sn_vul.Vulnerability_write vor v10.3 zugewiesen haben, nicht geändert. Benutzern und Gruppen bleiben diese Rollen zugewiesen, bis Sie sie ändern. Ab v10.3 können Sie jedoch granulare Rollen zuweisen, um mehr Kontrolle darüber zu erhalten, was Anwender und Gruppen im tun und sehen können Vulnerability Response Anwendung. Eine Übersicht und weitere Informationen zur Verwaltung dieser Rollen finden Sie unter Vulnerability Response Personas und granulare Rollen Und Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Rollentitel [Name]	Beschreibung
V2.10: sn_vul_container.delete	Löscht Quelldatensätze. Enthält die Rollen sn_vul_cmn.delete und sn_vul_container.delete_vi.
sn_vul_Container.ci_Manager	Verwaltet die Neuklassifizierung abgeglichener Konfigurationselem (Configuration Items, CIs).
sn_vul_Container.configure_Integrations	Konfiguriert Container-Integratio
sn_vul_Container.configure_VI_granularity	Konfiguriert die Granularität des Containerelements.
sn_vul_Container.create_VI	Kann angreifbare Container-Elem erstellen.
sn_vul_container.delete_vi	Kann manuell erstellte angreifbar Elemente löschen.
sn_vul_Container.Exception_Approver	Genehmigt Ausnahmen, Zurücks und Abschlüsse von angreifbaren Containerelementen. Enthält die Rolle „sn_vul.View_Manager_Wor Ab v2.3 wurde die granular sn_vul_Container.read_all fü Rolle entfernt, damit Sie au angreifbaren Container-Ele und Korrekturaufgaben zug können, die Ihnen und Ihrer zugewiesen sind, anstatt au

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung
	angreifbaren Container-Ele Korrekturaufgaben.
sn_vul_Container.false_positive_Approver	Genehmigt oder lehnt das Schlie Container-Elemente als falsch po Enthält die Rolle sn_vul.View_Manager_Worl
sn_vul_Container.Manage_assignment_rules	Definiert und aktualisiert Zuweis angreifbare Container-Elemente.
sn_vul_Container.Manage_Auto_close_stale_VI	Konfigurieren Sie das automatisc veralteter angreifbarer Container-
sn_vul_Container.Manage_Auto_Exception_rule	Verwalten (erstellen/lesen/aktual Ausnahmeregeln
sn_vul_Container.Manage_normalized_severity	Kann die Zuordnung aktualisiere Schweregrad zu normalisieren.
sn_vul_Container.Manage_permissions	Kann Anwendern Container-Sch Antwortrollen zuweisen.
sn_vul_Container.Manage_Remediation_targ…	Definiert und aktualisiert Zielreg Container-Korrekturmaßnahmen.
sn_vul_Container.Manage_Risk_Score_confi...	Definiert und aktualisiert Risikobewertungsrechner, Risiko Schwachstellen-Rollup-Rechner Container-Elemente.
sn_vul_Container.read_all	Kann alle angreifbaren Container zugehörigen Informationen anzei Enthält die Rolle sn_vul.View_Manager_Worl
sn_vul_Container.read_assigned	Kann angreifbare Container-Elem die Ihnen oder Ihren Gruppen zug entweder in der klassischen Anw oder Arbeitsbereich für IT-Korre Enthält die Rolle sn_vul.View_rem_Workspac **Wichtig:** Ab v24.0 von Vulnerability Rolle „sn_vul_Container.rea hat die Berechtigung zum Z Arbeitsbereich für IT-Korre
sn_vul_Container.read_assignment_rules	Kann Zuweisungsregeln für angr Container-Elemente anzeigen.
sn_vul_Container.read_Auto_Exception_rule	Lesen Sie Ausnahmeregeln
sn_vul_Container.read_detected_image	Kann erkannte Elemente anzeige

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung
sn_vul_Container.read_Integrations	Kann Ergebnisse von Integration anzeigen.
sn_vul_Container.read_normalized_severity	Kann die normalisierte Schwereg anzeigen.
sn_vul_Container.read_Remediation_target...	Kann Korrekturzielregeln anzeig
sn_vul_Container.read_Risk_Score_configu...	Kann Risikopunktzahlrechner, R Schwachstellen-Rollup-Rechner Container-Elemente anzeigen.
sn_vul_Container.Remediation_owner	Liest und schreibt angreifbare Co Elemente, die ihnen zugewiesen Schwachstellendatensätze könne einem Anwender mit dieser Rolle werden.
sn_vul_Container.Update_assigned_to	Kann die Zuweisung angrei Container-Elemente aktualis Erfordert sn_vul_container. oder sn_vul_Container.write
sn_vul_Container.Update_assignment_Group	Kann Zuweisungsgruppe fü Container-Elemente aktualis Erfordert sn_vul_container. oder sn_vul_Container.write
sn_vul_Container.Update_State	Kann status angreifbarer E aktualisieren. Erfordert sn_vul_container. oder sn_vul_Container.write
sn_vul_Container.Vulnerability_admin	Konfiguriert alle Regeln, Integrat den Container Vulnerability Resp
sn_vul_Container.Vulnerability_Analyst	Überwacht die Nachbesserung al Container-Elemente.
sn_vul_Container.write_all	Kann alle angreifbaren Container Korrekturaufgaben aktualisieren.
sn_vul_Container.write_assigned	Kann angreifbare Container-Elem Korrekturaufgaben aktualisieren, meinen Gruppen zugewiesen sind
sn_vul_Container.read_watch_topic	Kann Überwachungsthemen für C Schwachstellen lesen.
sn_vul_Container.create_watch_topic	Kann Überwachungsthemen für C Schwachstellen erstellen.
sn_vul_Container.Edit_watch_topic	Kann Überwachungsthemen für C Schwachstellen bearbeiten.

Automatisierte Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung
sn_vul_Container.Manage_Exception_Configuration	Kann Ausnahmeverwaltungskonf verwalten.

Mit Container Vulnerability Response installierte Tabellen

Tabellen werden bei Aktivierung von hinzugefügt Container Vulnerability Response(CVR).

Tabelle	Beschreibung
Container-Image-Ergebnis sn_vul_Container_image_results	Speichert Informationen zu den zugehörigen Schwachstellen, der Image-Ebene, dem Docker-Image, dem Image-Repository und dem erkannten Image. Ab v2.11.3 von Container Vulnerability Response, Sie können auch den Pfad anzeigen, in dem das Ergebnis angezeigt wird.
Container-Image-Ebene sn_vul_Container_image_Layer	Enthält die Informationen jeder Bildebene. Ein Image ist eine statische Datei mit ausführbarem Code, die einen Container auf einem Computersystem erstellen kann.
Container-Image-Paket sn_vul_Container_image_Package	Stellt Informationen zu den Paketen bereit, in denen die Schwachstellen vorhanden sind. Die Binärpaketdetails werden auch als kommagetrennter Wert bereitgestellt. Ab v2.11.3 von Container Vulnerability Response, Sie können auch die Paket-URL (PURL) anzeigen.
Angreifbares Container-Element sn_vul_Container_image_vulnerable_item	Enthält Details zu jedem Ergebnis und der entsprechenden Schwachstelle. Ab v2.11.3 von Container Vulnerability Response, Sie können auch Informationen zum Datum des letzten Scans eines Bildes anzeigen, das als Container ausgeführt wird.
Schwachstelleneintrag (v2.11.3) sn_vul_entry	Stellt Informationen zum Schweregrad eines CVE und alle zusätzlichen Informationen bereit, die von Prisma gesendet werden.
Erkanntes Container-Image sn_vul_Container_image	Stellt Informationen zur Image-ID, zum Docker-Image und zum Image-Repository bereit. Außerdem werden die Ebeneninformationen gespeichert und dem erkannten Image zugeordnet. Ab v2.11.3 von Container Vulnerability Response, Enthält auch Informationen zum Image-Digest eines Docker-Images und zum Datum des letzten Scans eines Images, das als Container und Registrierung ausgeführt wird.
Ergebniszuordnungen sn_vul_Container_Finding_m2m_vul_item	M2M-Beziehung der Container-Image-Ergebnisse und der angreifbaren Container-Elemente (CVITs).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Angreifbare Elemente automatisch schließen sn_vul_Container_image_Auto_close_config	Enthält Informationen zum Schließen der veralteten Container-Image-Ergebnisse und zum Rollup des Status zu den CVITs.
Container-Image-Schwachstellenschlüssel sn_vul_Container_image_Vulnerability_Keys	Enthält die Granularität-Konfiguration für die Erstellung von CVITs aus den Container-Image-Ergebnissen.
Docker-bezogene Services sn_vul_Container_m2m_ci_Services	Enthält alle Business-Services im Zusammenhang mit einem Container-Image.
Anzahlen der VR-Container sn_vul_Container_vr_Container_count	Enthält den gleitenden Durchschnitt der Containerinstanzen, die in den letzten 90 Tagen aus einem Container-Image abgeleitet wurden.
Element der Container-Korrekturaufgabe sn_vul_Container_m2m_vul_Group_item	M2M-Tabelle zwischen CVIT- und Container-Korrekturaufgaben.
Container-Korrekturaufgabe sn_vul_Container_Vulnerability	Enthält Container-Korrekturaufgaben.
Container-Korrekturaufgabe – Manifest sn_vul_Container_rt_Manifest	Alle Aktualisierungen der Korrekturaufgabe werden mithilfe dieser Manifesttabelle nach geplanten Aufgaben durchgeführt.

Mit Container Vulnerability Response installierte regelmäßige Aufgaben

Regelmäßige Aufgaben werden bei der Aktivierung von Container Vulnerability Response hinzugefügt.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Geplante Aufgabe	Beschreibung
Ordnen Sie vorhandene Container-VIS der automatischen Ausnahmeregel zu	Ordnet die automatische Ausnahmeregel automatisch vorhandenen angreifbaren Containerelementen (CVITs) zu.
Überprüfen Sie Den Ablauf Der Zurückstellung Für Angreifbare Container-Elemente	Sendet Benachrichtigungen, wenn angreifbare Container-Elemente oder Container-Schwachstellen abgelaufen sind (und wenn sie in einer Woche ablaufen).
Anzahl der Vulnerability Response-Container (Anwendung –	Wird täglich ausgeführt, um die Tabelle „sn_vul_Container_vr_Container_count“ auszufüllen, die den gleitenden 90-Tage-Durchschnitt für Container berechnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
Vulnerability Response und Konfigurations-Compliance für Container)	
CVITs automatisch schließen	Schließt automatisch angreifbare Container-Elemente, die der in der Konfiguration für das automatische Schließen definierten Bedingung entsprechen. Ihr Status wird in „behoben“ geändert.
Geschäftsrelevanz für CVIT berechnen	Verarbeitet alle aktiven CVITs und aktualisiert das Feld Geschäftsrelevanz basierend auf den betroffenen Services des Docker-Images des CVIT.
Schließen Sie CVITs abbrechen, denen kein Docker-Image zugeordnet ist	Läuft automatisch CVITs ab, denen kein CI zugeordnet ist. Ihr Status wird auf „Geschlossen“ und der Substatus auf „Abgebrochen“ festgelegt.
Berechnen Sie die zugehörigen VI-Anzahlen für die Container-Korrekturaufgabe	Berechnet die Anzahl der Datensätze der Container-Korrekturaufgabe.
Rollup der Werte angreifbarer Container-Elemente zu Schwachstelle und Gruppe	Berechnet Schwachstellen und Gruppen-Rollups für angreifbare Container-Elemente. **Hinweis:** Ab v2.10 von Container Vulnerability Response, Die geplante Aufgabe wird erweitert, um Hintergrundaufträge mit Multithreading-Fähigkeiten zu erstellen. Dieses Upgrade umfasst die Segmentierung des Auftrags in mehrere kleinere untergeordnete Aufträge, die entweder parallel oder gleichzeitig ausgeführt werden. Diese Änderung ermöglicht die gleichzeitige Verarbeitung mehrerer Datensätze, wodurch die Gesamtaufgabe erheblich beschleunigt wird.

Container Vulnerability Response Glossar

Erfahren Sie mehr über Begriffe und Konzepte, die einzigartig für sind Container Vulnerability Response.

Wichtige Begriffe

Behälter

Eine Softwareeinheit, die den Code und alle seine Abhängigkeiten so verpackt, dass die Anwendung nahtlos und zuverlässig von einer Computerumgebung in eine andere ausgeführt wird.

Container-Image

Eine statische Datei mit ausführbarem Code, die einen Container auf einem Computersystem erstellen kann. Ein Container-Image kann nicht geändert werden und kann daher konsistent in jeder Umgebung bereitgestellt werden.

Cluster

Eine Reihe von Worker-Computern, als Knoten bezeichnet, die containerisierte Anwendungen ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Docker

Software zum Erstellen, Bereitstellen und Verwalten von Anwendungscontainern auf Servern und in der Cloud.

Docker-Bild

Eine Vorlagendatei, die Code, erforderliche Bibliotheken, Konfigurationen usw. enthält. Die Datei wird zum Starten von Containerinstanzen verwendet. Sie besteht aus einer vereinigung von Dateisystemen mit Ebenen.

Dockerdatei

Eine Textdatei mit Anweisungen zum Erstellen von Container-Images durch Hinzufügen mehrerer Ebenen. Zum Beispiel Layering von Basis-Ubuntu, Nginx und App-Code.

Docker Verfassen

Ein Tool zum Definieren und Ausführen komplexer Anwendungen mit Docker. Mit Verfassen können Sie eine Anwendung mit mehreren Containern in einer einzelnen Datei definieren.

Docker-Container

Ein Docker-Container ist eine Laufzeitinstanz, die über ein Docker-Image gestartet wird.

Image-Ebene

Eine Ebene ist eine Änderung an einem Bild. Sie wird durch eine Anweisung in der Dockerdatei dargestellt. Ebenen werden sequenziell auf das Basisbild angewendet, um das endgültige Bild zu erstellen.

Image-Repository

Eine Sammlung von Docker-Images mit verschiedenen Tags oder Versionen.

Bildbezeichnungen

Eine Reihe von Schlüssel-Wert-Paaren, die mit dem Bild als Metadaten gespeichert sind.

Namespace

Eine von Kubernetes verwendete Abstraktion, um die Isolierung von Ressourcengruppen in einem einzelnen Cluster zu unterstützen.

Pod

Eine Reihe ausgeführter Container (eine andere Abstraktion oben auf einem Container).

Registry

Ein gehosteter Service, der Repositorys von Images enthält.

Service

Eine abstrakte Möglichkeit, eine Anwendung, die auf einer Reihe von Pods ausgeführt wird, als Netzwerkservice verfügbar zu machen.

Tag

Ein Tag ist eine Bezeichnung, die auf ein Docker-Image in einem bestimmten Image-Repository angewendet wird. Tags geben an, wie verschiedene Images in einem Repository voneinander unterschieden werden.

Formularfelder für angreifbares Container-Element

Angreifbare Container-Elemente (CVITs) werden während der Importe von Schwachstellenintegrationen aus Drittteilen automatisch erstellt.

Formularfelder für angreifbares Container-Element

Mit Ausnahme von **Zuweisungsgruppe** , **Zugewiesen an** Felder und **Notizen** , Alle anderen Felder im CVIT sind schreibgeschützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anzahl	Automatisch generierter CVIT-Bezeichner für diesen Datensatz.
Quelle	Scanner, der die Schwachstelle identifiziert hat.
Risikobewertung	Quantifiziert **Risikopunktzahl** Trennung angreifbarer Elemente in „Kritisch“, „hoch“, „Mittel“, „Niedrig“ und „keine“.
Risikopunktzahl	Berechnetes Risiko, das das CVIT für Ihre Umgebung darstellt.
Korrekturzielregel	Korrekturzielregel, nach der das Korrekturzieldatum berechnet wird.
Korrekturziel	Datum, bis zu dem die CVITs korrigiert werden sollen, seit der ersten Identifizierung. Wird nur angezeigt, wenn zutreffend.
Korrekturstatus	Status der Korrektur für das CVIT.
Schwachstelle	ID der Schwachstelle, die diesem angreifbaren Anwendungselement zugeordnet ist.
Docker-Bild	Vorlagendatei, die Code, erforderliche Bibliotheken, Konfigurationen usw. enthält. Die Datei wird zum Starten von Containerinstanzen verwendet. Sie besteht aus einer vereinigung von Dateisystemen mit Ebenen.
Erkanntes Container-Image	Eindeutiger Datensatz für jede Bild-ID.
Basis-Image	Ein grundlegendes Image, das zum Erstellen containerisierter Anwendungen verwendet wird und das wichtige Betriebssystem und die wichtigsten Bibliotheken enthält. Es dient als Ausgangspunkt für die Erstellung und Anpassung von Anwendungen in Umgebungen wie Docker.
Image-Cluster	Gruppen zugehöriger Images, die in verschiedenen Kontexten verwendet werden, z. B. Clustering ähnlicher Images in maschinellem Lernen oder Container-Images in einem Repository.
Image-Namespace	Wird verwendet, um Container-Images innerhalb einer Registrierung zu organisieren und zu isolieren, sodass verschiedene Teams oder Projekte separate Sammlungen verwalten können.
Status	Dieses Feld ist standardmäßig auf festgelegt **Öffnen** Bei der Erstellung. Siehe status des angreifbaren Anwendungselements (AVI) Für weitere Informationen zur Zuordnung von status.
Zuweisungsgruppe	Gruppe ausgewählt, um an diesem CVIT zu arbeiten.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die für dieses CVIT arbeitet. Kann manuell von einem App-Sec-Manager hinzugefügt oder bearbeitet werden.
Erstellt	Datum und Uhrzeit der Erstellung eines CVIT.
Zuletzt Geöffnet	Spätestes Datum und späteste Uhrzeit, zu der das CVIT erneut geöffnet wird.
Aktualisiert	Datum und Uhrzeit der letzten Änderung des CVIT.
Zuerst gefunden (v2.12.1)	Datum, an dem die Schwachstelle erstmals gefunden wurde. Ab v2.12.1 können Sie das genaue Datum und die Uhrzeit der ersten Erkennung anzeigen, um Klarheit zu gewährleisten und verschiedene Zeitzonen zu berücksichtigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Um die Details zum Datum und zur Uhrzeit der ersten Suche auszufüllen, muss die Integration erneut ausgeführt werden.
Zuletzt gefunden (v2.12.1)	Datum, an dem die Schwachstelle zuletzt gefunden wurde. Ab v2.12.1 können Sie das genaue Datum und die Uhrzeit der letzten Entdeckung anzeigen, um Klarheit zu gewährleisten und verschiedene Zeitzonen zu berücksichtigen. Um die Details zum Datum und zur Uhrzeit der letzten Suche auszufüllen, muss die Integration erneut ausgeführt werden.
Lösungsdatum (v2.12.1)	Datum, an dem die Schwachstelle gelöst wurde. Ab v2.12.1 können Sie das genaue Datum und die Uhrzeit der Lösung anzeigen, um Klarheit zu gewährleisten und verschiedene Zeitzonen zu berücksichtigen. Das Lösungsdatum wird ausgefüllt, wenn das CVIT als Teil des Workflows gelöst wird.
Zuletzt geöffnet (v2.12.1)	Datum, an dem die Schwachstelle zuletzt geöffnet wurde. Ab v2.12.1 können Sie das genaue Datum und die Uhrzeit der letzten Öffnung anzeigen, um Klarheit zu gewährleisten und verschiedene Zeitzonen zu berücksichtigen. Die geplante Aufgabe *`Add default values for last_opened_dt_tm from last _opened`*Füllt die Daten in diesem Feld aus. Sie darf nur einmal bei Bedarf ausgeführt werden.
Schwachstelle	
Zusammenfassung	Beschreibung der Schwachstelle.
Schweregrad	Normalisierter Schweregrad dieser Schwachstelle. Schweregradzuordnungen werden für die National Vulnerability Database (NVD) und für Integrationen von ServiceNow-Drittparteien bereitgestellt.
Schwachstellenpunktzahl (v3)	V3-Punktzahl des Common Vulnerability Scoring System (CVSS).
Schwachstellenpunktzahl (v2)	CVSS v2-Punktzahl.
Exploit vorhanden	Ja, wenn mindestens ein Exploit den Schwachstellen zugeordnet ist, die diesem angreifbaren Element zugeordnet sind.
Exploit-Angriffsvektor	Der Angriffsvektor der Angreifer der Exploits für die Schwachstellen, die diesem angreifbaren Element zugeordnet sind.
Exploit-Kompetenzniveau	Niedrigstes Kompetenzniveau, das zum Ausnutzen der Schwachstellen erforderlich ist, die diesem angreifbaren Element zugeordnet sind.
Veröffentlichungsdatum	Datum, an dem die Schwachstelle veröffentlicht wurde.
Zuletzt geändert	Datum, an dem die Schwachstelle zuletzt geändert wurde.
Bedrohung	Relevante Informationen zur Bedrohung. Aus dem Datensatz des angreifbaren Eintrags abgerufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Alle hier vorgenommenen Änderungen aktualisieren den Datensatz des angreifbaren Eintrags.
Korrekturhinweise	Relevante Lösung für die Bedrohung, abgerufen aus dem Eintragsdatensatz für angreifbare Elemente.
Notizen	
Arbeitsnotizen	Alle relevanten Informationen. Wählen Sie das Textfeld für Arbeitsnotizen aus, um Informationen hinzuzufügen.
Bildergebnisse	Ergebnisse des Scans von Container-Images auf Schwachstellen.
Angeforderte Genehmigungen	Genehmigungsanforderung für CVIT ausgelöst.
Genehmigungen der Statusänderung	Anforderung für Statusänderungsgenehmigungen für CVIT gestellt.

Altersberechnungen eines CVIT:

- Die Spalte Alter in der Liste der CVITs zeigt die Dauer (Format: Tage HH:MM:SS) an, für die ein CVIT aktiv ist. Der Alterswert ist für ein geschlossenes CVIT null.
- Die Spalte Alter geschlossen in der CVITs-Liste zeigt die Dauer (Format: Tage HH:MM:SS) an, für die ein CVIT aktiv ist, bevor es geschlossen wird. Für CVITs, die sich nicht im Status Geschlossen befinden, ist der Wert für Alter Geschlossen Null.

Weitere Informationen zum Anpassen der Berechnung des Alters und der Dauer der geschlossenen Zeiten finden Sie unter KB1703270 artikel.

Formular „Konfiguration von Prisma-Cloud-Computing“

Auf das Formular „Prisma-Cloud-Compute-Konfiguration“ wird innerhalb des Moduls „Prisma-Cloud-Compute-Integration“ zugegriffen.

Navigieren Sie zum Anzeigen des Formulars „Prisma-Cloud-Compute-Konfiguration“ zu **Alle** > **Prisma-Cloud-Computing-Integration** > **Administration** > **Konfiguration**an.

Konfiguration des Prisma-Cloud-Computings

Feld	Beschreibung
Integrationsinstanz	Name der neuen Integrationsinstanz. Sie können eine Instanz erstellen oder auf das Suchsymbol klicken, um eine vorhandene Instanz auszuwählen.
API-Basis-URL	URL zur Integration mit Prisma Cloud Compute.
Anwendername	Anwendername für den Zugriff auf Prisma Cloud Compute.
Passwort	Passwort für den Zugriff auf Prisma Cloud Compute.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration des Prisma-Cloud-Computings (Fortsetzung)

Feld	Beschreibung
MID-Server	Eine Java-Anwendung, die als Windows-Service oder UNIX-Daemon auf einem Server in Ihrem lokalen Netzwerk ausgeführt wird. Der MID-Server ermöglicht die Kommunikation und das Verschieben von Daten zwischen ServiceNow Instanz und externe Anwendungen, Datenquellen und Services.
Projekte verwenden	Option zum Konfigurieren der Projekte. Wenn Sie das Kontrollkästchen aktivieren, können Sie Projekte auf der Konfigurationsseite auswählen und die Integrationen basierend auf den Projekten ausführen, die zum Ausfüllen projektspezifischer Details konfiguriert sind. **Hinweis:** Wenn dieses Kontrollkästchen aktiviert ist, wird **Konfigurieren Sie Projekte** Registerkarte ist aktiviert. Klicken Sie Auf **Als Nächstes** Um mit der Konfiguration der Projekte fortzufahren.

Formular „Ausnahme anfordern“

Fordern Sie Richtlinienausnahmen mit an GRC Fähigkeit zur Verwaltung von Richtlinienausnahmen in Richtlinien- und Compliance-Management Anwendung von innerhalb Container Vulnerability Response.

Navigieren Sie zum Anzeigen des Formulars „Prisma-Cloud-Compute-Konfiguration“ zu **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente** (Oder **Korrekturaufgaben**)> **Alle** , Und öffnen Sie das Element oder die Gruppe, für das Sie eine Ausnahme anfordern möchten.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Richtlinie	Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft und der Status des angreifbaren Elements oder der angreifbaren Gruppe von zurückgestellt in Offen geändert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Ausnahme anfordern“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf nicht überschreiten **Maximale Ausnahmedauer (Tage)** Die Sie für die Richtlinie in Richtlinie und Compliance festgelegt haben. Weitere Informationen finden Sie unter Erstellen Sie eine Richtlinie .
Grund	Grund für die Anforderung einer Ausnahme.
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer ausgefüllt werden.

Formular „Ausnahmeregel“

Erstellen Sie eine Regel, um automatisch eine Ausnahme für eine bestimmte Bedingung für eine Gruppe angreifbarer Container-Elemente (CVITs) anzufordern, z. B. eine Regel mit einer Bedingung, die auf dem Schwachstellenschweregrad dieser CVITs basiert. Mit dieser Regel können Sie neue und vorhandene CVITs automatisch zurückstellen, wenn sie der genehmigten Regelbedingung entsprechen.

Um das Formular „Ausnahmeregel“ anzuzeigen, navigieren Sie zu **Alle** > **Container Vulnerability Response** > **Administration** > **Ausnahmeregeln**an.

Formular „Ausnahmeregel“

Feld	Beschreibung
Name	Name der Ausnahmeregel.
Gültig ab	Datum, ab dem diese Regel aktiv ist, um die CVITs aufzuschieben.
Gültig bis	Datum, ab dem die Korrekturaufgabe keine neuen CVITs mehr akzeptiert.
Grund	Grund für die Erstellung dieser Ausnahmeregel.
Zuweisungsgruppe	Gruppe, der die Korrekturaufgabe zugewiesen ist, die zur Nachverfolgung der zurückgestellten CVITs erstellt wurde.
Zusätzliche Information	Zusätzliche Informationen, die die anfordernde Person dem Genehmiger bereitstellen möchte. Diese Informationen werden im Beschreibungsfeld der Korrekturaufgabe ausgefüllt.
Bedingung	Filterbedingung für die CVITs, die bei der Verarbeitung der CVITs definiert werden kann.
Für vorhandene Daten ausführen	Option, mit der Sie diese Regel bei der ersten Ausführung dieser Regel für vorhandene Daten ausführen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Ausnahmeregel“ (Fortsetzung)

Feld	Beschreibung
Workflow-Phase	Aktueller Genehmigungsstatus der Ausnahmeregel.
Status	Status der Ausnahmeregel.
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausnahmeregel.
Zurückgestellt bis	Datum, bis zu dem die VULs und CVITs zurückgestellt werden. An diesem Datum wird die erstellte ÄNDERUNG geschlossen, alle CVITs werden aus der Gruppe verschoben, und Gruppenregeln werden erneut angewendet.

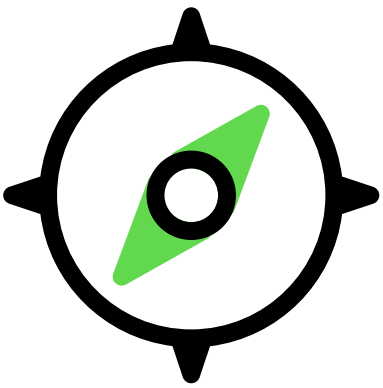
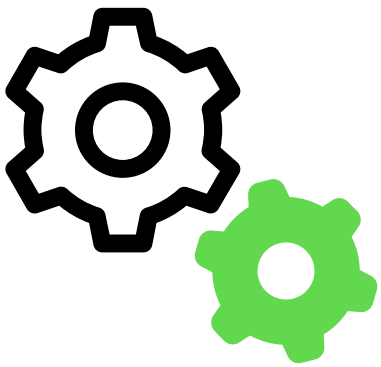
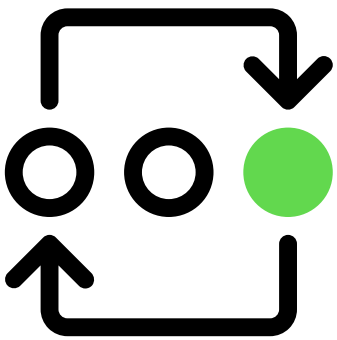
Konfigurations-Compliance

Die ServiceNow® Konfigurations-Compliance Die Anwendung ist eine SCA-Anwendung (Secure Configuration Assessment), die Scan-Ergebnisse aus Integrationen mit Konfigurations-Scan-Anwendungen von Drittanbietern zusammenfasst. Sie können Konfigurations-Compliance-Probleme mit priorisieren Configuration Management Database (CMDB). Konfigurations-Compliance Ist eng in den IT-Change-Management-Prozess integriert, um nicht konforme Konfigurationen zu beheben.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Konfigurations-Compliance

Untersuchen	Einrichten, Installieren und Konfigurieren	Integrieren
		
Erfahren Sie mehr über Konfigurations-Compliance-Konzepte und -Funktionen	Konfigurieren Sie Konfigurations-Compliance	Erweitern Sie die Konfigurations-Compliance, indem Sie sie mit anderen Anwendungen integrieren

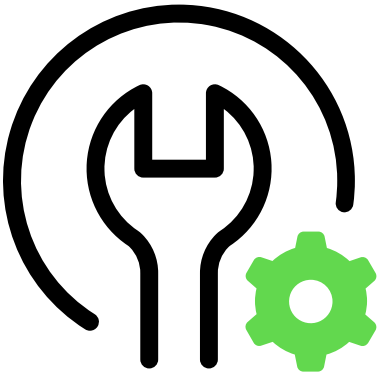
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance (Fortsetzung)

Verwenden Sie die Vulnerability Response-Arbeitsbereiche

Erfahren Sie, wie Sie Konfigurationsprobleme in den Arbeitsbereichen „Schwachstellenmanager“, „IT-Korrektur“ und „Schwachstellenbewertung“ überwachen, verwalten und beheben können.

Beheben

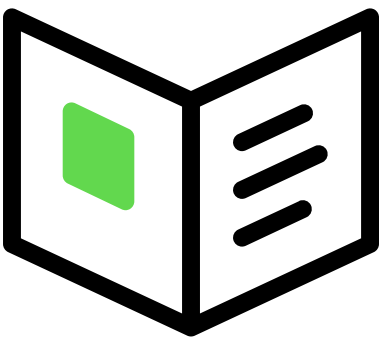


Erfahren Sie, wie Sie Ihre nicht konformen Assets mit Configuration Compliance beheben können

Analytics Und Berichte

Zeigen Sie Berichte und Dashboards in Konfigurations-Compliance an

Referenz



Rufen Sie Details zu Configuration Compliance-Komponenten wie Feldern, Tabellen und Eigenschaften ab

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Konfigurations-Compliance erkunden

Verwenden Sie Testergebnisse aus SCA-Integrationen (Secure Configuration Assessment) von Drittanbietern, um die Compliance mit Sicherheits- oder Unternehmensrichtlinien zu überprüfen. Identifizieren, priorisieren und korrigieren Sie nicht konforme Konfigurationselemente.

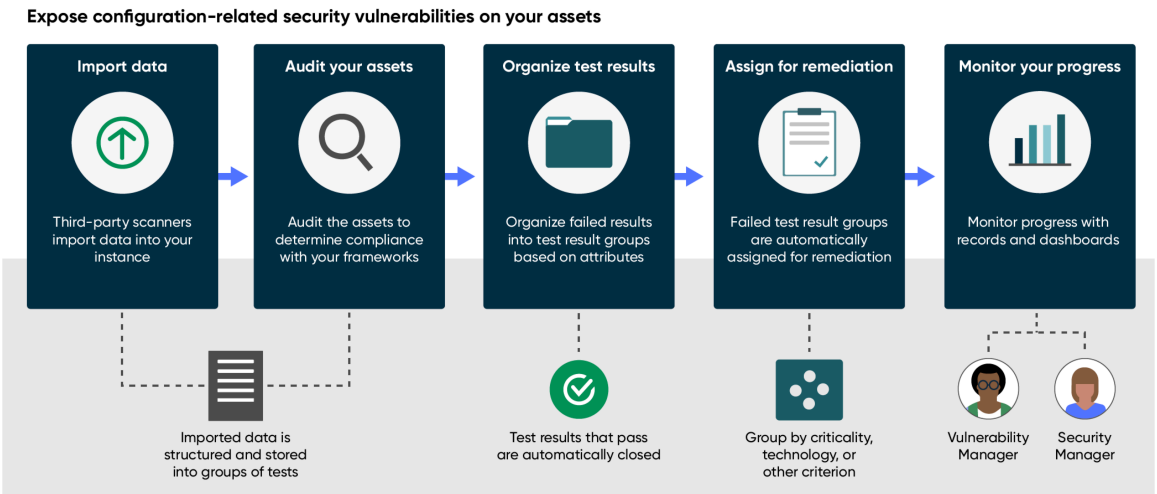
Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Konfigurations-Compliance – Beschreibung

Die ServiceNow® Konfigurations-Compliance Mit der Anwendung können Sie die kritischsten konfigurationsbezogenen Schwachstellen in Ihrer Umgebung schnell und effizient priorisieren und beheben. Konfigurations-Compliance Ist nach Abonnement in verfügbar ServiceNow® Store.



Schlüsselfunktionen von Konfigurations-Compliance

Verwenden Sie Configuration Management Database (CMDB) In Ihrem ServiceNow AI Platform® Damit Sie Ihre kritischsten konfigurationsbezogenen Sicherheitsschwachstellen offenlegen und beheben können. Konzentrieren Sie Ihre Korrekturressourcen auf Aktivitäten mit der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

größten Risikominderung. Optimieren Sie den Korrekturprozess für die Stakeholder in den Bereichen Sicherheit, IT und Geschäftsprozess. Die Konfigurations-Compliance Die Anwendung enthält die folgenden wichtigen Funktionen:

- Mit unterstützten Drittanbieterintegrationen können Richtlinien, Tests, autorisierende Quellen und Technologien automatisch importiert werden. Siehe Konfigurations-Compliance-Integrationen Weitere Informationen zu unterstützten Integrationen.
- Korrelieren Sie Richtlinien und Tests mit Konfigurationselementen (Assets), um konfigurationsbezogene Schwachstellen zu identifizieren und sicherzustellen, dass Ihre Assets Ihren Richtlinien und Steuerungen entsprechen.
- Vereinheitlichen Sie die Konfigurationsbewertung, -Zuweisung und -Korrektur für alle Ihre Assets.
- Inhalte von Konfigurations-Scans können aus führenden SCA-Integrationsanwendungen (Secure Configuration Assessment) des Ökosystems importiert werden.
- Konfigurationsergebnisse und Testfehler können basierend auf den Kompetenzen und Verantwortungsbereichen von Korrekturspezialisten automatisch gruppiert und weitergeleitet werden. Intelligente Workflows und eine enge Integration mit Change-Management sorgen für reibungslose Aufgabenübergaben zwischen Gruppen.
- Bei Verwendung mit ServiceNow Governance, Risk und Compliance(GRC) Anwendung, Konfigurationstests in Konfigurations-Compliance Kann zu den entsprechenden GRC-Steuerungen zusammengefasst werden.
- Mit verbessertem Change-Management können Sie vorab ausgefüllte Change-Anforderungen für IT direkt aus erstellen Konfigurations-Compliance Um Sie bei Ihren Korrekturaufgaben zu unterstützen, die zusätzliche Ressourcen erfordern.
- Zeigen Sie mit Dashboards Korrekturstatusmetriken für Korrekturaufgaben, Compliance-Tests und Richtliniendatensätze an.

Konfigurations-Compliance – Benutzer

Konfigurations-Compliance Aktivitäten können viele Verwaltungsebenen umfassen.

- Systemadministratoren
- Schwachstellenadministratoren
- Schwachstellenmanager
- Schwachstellenanalysten
- Compliance-Administratoren

Konfigurations-Compliance Aufgaben umfassen die folgenden Rollen.

- sn_vulc.admin – kann lesen, schreiben, löschen
- sn_vulc.write – kann lesen und schreiben
- sn_vulc.Remediation_owner – kann zugewiesene Datensätze lesen und aktualisieren

> **Hinweis:**
> Die Rolle sn_vulc.Remediation_owner wird ebenfalls automatisch zugewiesen, wenn einem Anwender die Rolle itil zugewiesen wird.

- sn_vulc.read – kann lesen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance und Security Operations

Wenn Qualys Vulnerability Integration Und Tenable Vulnerability Integration Sind installiert, Zugriff auf Vulnerability Response Wird verfügbar. Sie können mehrere Bereitstellungen dieser Integrationen haben. Daten, die aus jeder Bereitstellung stammen, werden identifiziert und in einer einzigen Instanz von verfügbar gemacht GRC.

Verfügbare Versionen für Yokohama

Freigabeversion	Release-Hinweise
Konfigurations-Compliance V15.4	Versionshinweise zur Konfigurations-Compliance . Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema Siehe Einrichten, Installieren und Konfigurieren von Konfigurations-Compliance Anwendung Weitere Informationen zum Aktivieren der Anwendung.

Konfigurations-Compliance Daten importiert

Die Konfigurations-Compliance Die Anwendung importiert Richtlinien, Tests, autorisierende Quellen und Testergebnisse aus Integrationen von Drittparteien und speichert sie zur Anzeige in Modulen.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Unterstützte Integrationen

Drittpartei-Integrationen importieren Konfigurationsbewertungsergebnisse, Testgruppen, Tests, Technologien, autoritative Quellen, und Testergebnisse in Konfigurations-Compliance Anwendung. Schwachstellenmanager oder Schwachstellenanalysten können diese Daten verwenden, um konfigurationsbezogene Schwachstellen in Ihren Assets zu identifizieren und darauf zu reagieren.

Weitere Informationen zu unterstützten Integrationen finden Sie unter Konfigurations-Compliance-Integrationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Testgruppen

Testgruppen beziehen sich auf autorisierende Dokumente und Testdatensätze. Eine Gruppe von Konfigurationstests definiert Testgruppen. Testgruppen richten sich normalerweise an einer Technologieklasse aus, z. B. Windows, Oracle-Datenbanken, Cisco IOS, und werden häufig vom primären Industriestandard abgeleitet. Testgruppen können geändert werden, um die Anforderungen der Organisation zu erfüllen. Ein einzelner Konfigurationstest kann mehreren Testgruppen angehören.

Integration	Beschreibung
Qualys Vulnerability Integration	Testgruppen werden abgerufen, und Kontroll-IDs werden von der geplanten Aufgabe ausgefüllt. **Qualys-PC-Richtlinien** Um 1:00 Uhr. Sie können die geplante Aufgabe anzeigen, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **Qualys-PC-Richtlinien**an. **Hinweis:** Wenn Sie die Integration manuell ausführen möchten, führen Sie aus **Qualys-PC-Richtlinien** Zuerst.
Tenable Vulnerability Integration	Die geplante Aufgabe Tenable.io Compliance-Ergebnisintegration importiert Richtlinien. Wenn Sie die Integrationen manuell ausführen möchten, führen Sie die Integrationen in der folgenden Reihenfolge aus, bis Sie ignorierte Assets mit Bewertungsdaten abgleichen: • Tenable.io Asset-Integration • Tenable.io Integration Von Compliance-Ergebnissen • Tenable.io Integration Der Compliance-Ergebnisse Im Backfill • Tenable.io Asset-Integration • Tenable.io Integration Der Compliance-Ergebnisse Im Backfill Um den Richtliniendatensatz anzuzeigen, navigieren Sie zu **Alle** > **Konfigurations-Compliance** > **Testgruppen**an. Um die Testgruppendatensätze korrekt zu identifizieren und zu erstellen, werden Audit-Informationen für Testgruppen importiert und in angezeigt **Kurzbeschreibung** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tests

Tests sind Bibliotheken von Datensätzen, die Scans von Computing-Assets organisieren. Konfigurationstests definieren, wie eine Klasse von Technologie-Assets gesteuert werden soll.

A Konfigurations-Compliance„Test“ ist der Mechanismus, den Drittanbieter-Integrationsanwendungen verwenden, um Assets nach Schwachstellentyp zu gruppieren. Einige VA-Scanlösungen von Drittanbietern wie Qualys verfügen über sehr große Testbibliotheken (bis zu 8.000), die Richtlinien und Frameworks von autorisierenden Quellen zugeordnet sind.

Ein Test kann viele Werte haben, eins-zu-viele, erwartete vs. Tatsächliche usw. Ein Test ist alles, was verwendet werden kann, um eine nicht konforme Software- oder Hardware-Asset-Klasse zu identifizieren. Zum Beispiel eine Release- oder Hardwarekummer.

Integration	Beschreibung
Qualys Vulnerability Integration	Die geplante Aufgabe, **Qualys-PC-Steuerungen** , Ruft die Tests ab. Sie können die geplante Aufgabe anzeigen, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **Qualys-PC-Steuerungen**an. **Hinweis:** Wenn Sie die Integration manuell ausführen möchten, führen Sie aus **Qualys-PC-Steuerungen** Nach **Qualys-PC-Richtlinien** .
Tenable Vulnerability Integration	Die geplante Aufgabe Tenable.io Integration von Compliance-Ergebnissen importiert Konfigurationstests (Tests). Wenn Sie die Integrationen manuell ausführen möchten, führen Sie die Integrationen in der folgenden Reihenfolge aus, bis Sie ignorierte Assets mit Bewertungsdaten abgleichen: • Tenable.io Asset-Integration • Tenable.io Integration Von Compliance-Ergebnissen • Tenable.io Integration Der Compliance-Ergebnisse Im Backfill • Tenable.io Asset-Integration • Tenable.io Integration Der Compliance-Ergebnisse Im Backfill Navigieren Sie zum Anzeigen des Konfigurationstestdatensatzes zu **Konfigurations-Compliance** > **Tests**an. Im Datensatz werden importierte Daten in angezeigt **Kurzbeschreibung** Registerkarten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
	„Feld und Korrekturstatus“, „Beschreibung“ und „Korrektur“. Daten werden auch im angezeigt **Bezugsvermerke** , **Richtlinien** , Und **Testergebnisse** Zugehörige Links.

Technologien

Eine der Techniken, die von Drittanbieter-Schwachstellen-Scannern zum Erstellen von Testgruppen von Software- und Hardware-Konfigurationselementen für die Analyse verwendet werden, besteht darin, sie nach Technologie zu organisieren. Technologien sind eine importierte Bibliothek von Betriebssystemen, Netzwerkgeräten, Datenbanken und Apps, die Richtlinien zugeordnet sind. Tests haben mehrere Implementierungen für verschiedene Technologien. Die Korrektur ist ebenfalls technologiespezifisch.

Sie können Zeigen Sie die entsprechenden Technologien an Um für einen Test besser zu verstehen, auf welche Arten von Software- oder Hardware-Assets die Steuerung angewendet werden kann. Beispiele für Technologien, die auf Steuerungen angewendet werden können, sind CentOS 7.x, Windows 8,1, Windows 2016 Server usw. Die Liste der Technologien ist schreibgeschützt und entspricht den in definierten Technologien Qualys Cloud Platform Anwendung.

Technologien werden nur für datenbankbezogene Konfigurationsbewertungen importiert. Die *db_type*(Wenn nicht leer) im Import wird zum Erstellen einer Technologie verwendet. Zeigen Sie Technologien an, die im Abschnitt Technologien in Konfigurationstesterdatensätzen, Testergebnisdatensätzen, Richtliniendatensätzen und in ausgefüllt sind **Konfigurations-Compliance** > **Unterstützungsdaten** > **Technologien**an.

Autorisierende Quellen

Konfigurations-Compliance Verwendet autoritative Quellen und Zitate beim Generieren von Schwachstellenwarnungen für Tests. Autoritative Quellen werden normalerweise Abschnitten veröffentlichter Branchenstandards zugeordnet, z. B. „NIST 800-53 Version 3 (2009) 3: 2009, SA-4“.

Hinweis:
In Qualys Vulnerability Integration, Diese Kombination wird als Framework bezeichnet.

Autorisierende Quellen und Zitate (auch als Mandate bezeichnet) werden aus den Schwachstellen-Scannern von Drittanbietern importiert.

Autorisierende Quelldatensätze enthalten Verweise auf Informationen zu bekannten Software- und Hardwarekonfigurationsproblemen von Experten im Bereich der Computersicherheit. Sie definieren Anforderungen für Sicherheitsrichtlinien und -Verfahren. Konfigurationstests können durch Bezugsvermerke auf mehrere autorisierende Quellen verweisen. Autorisierende Quellen können zur Vorbereitung eines Audits Berichte über Compliance für einen bestimmten Standard erstellen.

Integration	Beschreibung
Qualys Vulnerability Integration	Die geplante Aufgabe, **Qualys-PC-Richtliniendetail** , Ruft die autorisierenden Quellen und Bezugsvermerke ab. Sie können diese geplante Aufgabe anzeigen, indem Sie zu navigieren **Qualys Schwachstellenintegration**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
	> **Primäre Integrationen** > **Qualys-PC-Richtliniendetail**an. **Hinweis:** Wenn Sie die Integration manuell ausführen möchten, führen Sie aus **Qualys-PC-Richtliniendetail** Nach **Qualys-PC-Richtlinien** .
Tenable Vulnerability Integration	Die geplante Aufgabe Tenable.io Integration von Compliance-Ergebnissen importiert autorisierende Quellen als Teil von Zitatdaten. Wenn Sie die Integrationen manuell ausführen möchten, führen Sie die Integrationen in der folgenden Reihenfolge aus, bis Sie ignorierte Assets mit Bewertungsdaten abgleichen: • Tenable.io Asset-Integration • Tenable.io Integration Von Compliance-Ergebnissen • Tenable.io Integration Der Compliance-Ergebnisse Im Backfill • Tenable.io Asset-Integration • Tenable.io Integration Der Compliance-Ergebnisse Im Backfill Daten werden auf angezeigt **Bezugsvermerke** Zugehöriger Link zu Konfigurationstestdatensätzen.

Testergebnisse

Konfigurations-Compliance Berechnet die Testergebnisse nicht, importiert sie jedoch als Teil einer Drittpartei-Integration. Sobald sie in angezeigt werden können Konfigurations-Compliance, Werden sie mit korrigiert **Korrekturaufgaben** . Weitere Informationen finden Sie unter Konfigurations-Compliance Korrelation.

Integration	Beschreibung
Qualys Vulnerability Integration	Sie können die Testergebnisse auf eine der folgenden Arten abrufen: Die geplante Aufgabe, **Qualys-PC-Ergebnisse** , Ruft die Testergebnisse ab. Sie können diese geplante Aufgabe anzeigen, indem Sie zu navigieren **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **Qualys-PC-Ergebnisse**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
	Hinweis: Wenn Sie die Integration manuell ausführen möchten, führen Sie aus **Qualys-PC-Ergebnisse** Nach **Qualys-PC-Richtlinien** Und **Qualys-PC-Richtliniendetail** . Die **Qualys-PC-Ergebnisse** Beim Import wird verwendet *`Start Time`*Parameter in **Integrationsdetails** Registerkarte . Alle anderen Konfigurations-Compliance Importe beziehen alle verfügbaren Daten unabhängig von ein *`Start Time`*. Wenn **Qualys-PC-Ergebnisse** Import ist abgeschlossen, ein Ereignis wird ausgelöst, um Berechnungen für das Ende des Imports auszulösen. Weitere Informationen finden Sie unter Konfigurations-Compliance status. Alternativ können Sie ab V14.5 auch die folgenden Integrationen ausführen, um die Testergebnisse abzurufen: • Qualys PCRS-Richtlinienhostintegration: Ruft die Host-IDs für jede Richtlinie ab. Um diese geplante Aufgabe anzuzeigen, navigieren Sie zu Qualys Vulnerability Integration > Primäre Integrationen > Qualys PCRS Policy Host Integration. **Hinweis:** Wenn Sie die Integration manuell ausführen möchten, führen Sie die Qualys PCRS-Richtlinienhostintegration nach Qualys PC-Richtlinien und Qualys PC-Richtliniendetails aus. Nachdem diese geplante Aufgabe abgeschlossen ist, wird automatisch die Qualys PCRS-Testergebnisintegration ausgelöst. • Qualys Integration von PCRS-Testergebnissen: Ruft die Testergebnisse für jede Host-ID ab. Um diese geplante Aufgabe anzuzeigen, navigieren Sie zu Qualys Vulnerability Integration > Primary Integrations > Qualys PCRS Test Results Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
	Hinweis: Wenn Sie die Integration manuell ausführen möchten, führen Sie die Qualys PCRS-Testergebnisintegration nach Qualys PC-Richtlinien, Qualys PC-Richtliniendetails und Qualys PCRS-Richtlinienhostintegration aus. Diese Integration verwendet den Parameter Startzeit auf der Registerkarte Integrationsdetails.
Tenable Vulnerability Integration	Die geplante Aufgabe Tenable.io Integration von Compliance-Ergebnissen importiert Testergebnisse. Wenn Sie die Integrationen manuell ausführen möchten, führen Sie die Integrationen in der folgenden Reihenfolge aus, bis Sie ignorierte Assets mit Bewertungsdaten abgleichen: • Tenable.io Asset-Integration • Tenable.io Integration Von Compliance-Ergebnissen • Tenable.io Integration Der Compliance-Ergebnisse Im Backfill • Tenable.io Asset-Integration • Tenable.io Integration Der Compliance-Ergebnisse Im Backfill Navigieren Sie zum Anzeigen des Konfigurationstestdatensatzes zu **Konfigurations-Compliance** > **Testergebnisse**an. Im Datensatz werden importierte Daten in angezeigt **Testen** , Und **Konfigurationselement** Felder. Daten werden auch im angezeigt **Erwartete Werte** , **Ist-Werte** , Und **Korrektur** Registerkarten. Die **Korrekturaufgaben** Und **Testergebnisverlauf** Zugehörige Links werden ausgefüllt.

Erkennung von Konfigurations-Compliance

Konfigurations-Compliance Daten werden aus SCA-Scanneranwendungen von Drittanbietern importiert. Sie strukturieren Gruppen von Software- und Hardwaretests in Datensätzen, um die Durchführung von Bewertungen zu beschleunigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Wenn ein Import abgeschlossen ist, wird ein Ereignis gesendet, um Aktionen für das Ende des Imports anzuzeigen. Für jede aktive Korrekturaufgabe werden die folgenden Aktionen ausgeführt:

- Gelöste Korrekturaufgaben mit fehlgeschlagenen Ergebnissen werden an zurückgegeben **Warten Auf Implementierung** status.
- Korrekturaufgaben, bei denen alle Ergebnisse bestanden wurden, sind **Geschlossen** .
- Der Status der Testergebnisse in aktiven Korrekturaufgaben wird aktualisiert.
- Die Kennzeichnung, die angibt, ob ein Ergebnis Teil einer aktiven Korrekturaufgabe ist, wird aktualisiert.

Konfigurations-Compliance Korrelation

Konfigurations-Compliance Bietet Priorisierung und Gruppierung von Testergebnissen (in Korrekturaufgabe), um Probleme mit Nichteinhaltung zu beheben.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Asset-Zentrierte Priorisierung

Konfigurations-Scans können eine große Anzahl von Ergebnissen erzeugen. Priorisieren Sie die Ergebnisse, um die größte Risikominderung zu erzielen. Die Priorität umfasst sowohl die Relevanz von Konfigurationstests als auch die Asset-Relevanz. Die Priorität des Konfigurationstestergebnisses wird als Risikopunktzahl einer Skala von 0 bis 100 ausgedrückt. Rechnergruppen berechnen die Risikopunktzahl und können angepasst werden.

Wenn der Drittparteiimport abgeschlossen ist, Konfigurations-Compliance Sendet ein Ereignis, um Aktionen für das Ende des Imports anzugeben. Für jede aktive Ergebnisgruppe werden die folgenden Aktionen ausgeführt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Gelöste Korrekturaufgaben mit fehlgeschlagenen Ergebnissen werden an zurückgegeben **Warten auf Implementierung** status.
- Korrekturaufgaben, bei denen alle übergebenen Ergebnisse sind **Geschlossen** .
- Der Status der Testergebnisse, die sich in aktiven Korrekturaufgaben befinden, wird aktualisiert.
- Die Kennzeichnung, die angibt, ob ein Ergebnis Teil einer aktiven Korrekturaufgabe ist, wird aktualisiert.

Reihenfolge der Korrekturaufgaben

Wenn Testergebnisse zu mehr als einer Gruppe gehören, wird die **Status** Eines Testergebnisses wird gemäß einer Rangfolge abgeleitet.

Die **Status** Und **Lösung** Felder in **Konfigurationstest** Formular und **Ergebnis** Feld in **Testergebnis** Formular, werden gemäß dieser Rangfolge berechnet.

Hinweis:

Die Gruppenmitgliedschaftspriorität gilt nur für Elemente, bei denen das Element den Konfigurationstest nicht bestanden hat. **Bestanden** Elemente befinden sich immer im **Geschlossen – Behoben** status.

Die **Ergebnis** Wert bestimmt den Status. Wir ignorieren Korrekturaufgaben in **Geschlossen – Behoben** Und **Geschlossen – Abgebrochen** status. Der Elementstatus wird aus den status aller anderen Korrekturaufgaben berechnet, zu denen er gehört oder auf festgelegt ist **Öffnen** , Wenn für das Element keine andere Gruppe vorhanden ist.

Order of Precedence for Test Results belonging to multiple Test Result Groups						
Group A	**Group B**					
	Open	**Under Investigation**	**Awaiting Implementation**	**Resolved**	**Deferred**	**Closed-Invalid**
Open	Open	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Under Investigation	Under Investigation	Under Investigation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Awaiting Implementation	Resolved	Deferred	Closed-Invalid
Resolved	Resolved	Resolved	Resolved	Resolved	Deferred	Closed-Invalid
Deferred	Deferred	Deferred	Deferred	Deferred	Deferred	Closed-Invalid
Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid	Closed-Invalid

Erstellung von Korrekturaufgaben

Konfigurations-Compliance Korrekturaufgaben werden manuell erstellt.

Es gibt zwei Möglichkeiten zum Erstellen und Ausfüllen **Korrekturaufgaben** .

- Von **Korrekturaufgaben** Modul und mit Filtern, die automatisch ausfüllen **Testergebnisse** Registerkarte.

  Dies ist gut, wenn Sie wissen, welche Filterung Sie verwenden möchten. Zum Beispiel werden alle fehlgeschlagenen Testergebnisse erfasst, die eine moderate und höhere Relevanz haben, sich auf die Windows-basierte Infrastruktur auswirken und nur für die SAP-Lieferkettenanwendung gelten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Indem Sie Testergebnisse in auswählen **Testergebnisse** Führen Sie eine Korrekturaufgabe auf, und erstellen Sie sie aus **Aktionen für ausgewählte Zeilen...** Menü.

  Diese Methode eignet sich für Ergebnisse, die nicht leicht gefiltert werden können, oder Situationen, in denen Sie Testergebnisse zur Korrektur angeben möchten. Zum Beispiel Ausreißer, die nichts gemeinsam haben.

Hinweis:
Wenn Sie eine Korrekturaufgabe aus erstellen **Testergebnisse** Liste und Sie entscheiden sich später, einen Filter für diese Korrekturaufgabe zu verwenden. Ihre ursprünglichen Einträge werden entfernt und durch die Filterergebnisse ersetzt.

Nicht Gruppierte Testergebnisse

Nicht Gruppierte Testergebnisse Enthält alle nicht bestandenen Testergebnisse, die nicht Mitglieder eines aktiven (nicht- **Geschlossen**) Korrekturaufgabe. Dieses Modul wird nach jedem Import und immer dann aktualisiert, wenn Testergebnisse einer Korrekturaufgabe hinzugefügt oder daraus entfernt werden.

Erkannte Elemente für Konfigurations-Compliance

Assets werden mithilfe von CI-Suchregeln automatisch mit Konfigurationselementen (Configuration Items, CIs) abgeglichen, wenn sie mithilfe der Host- und Testergebnisintegrationen importiert werden. Erkannte Elemente geben Ihnen Einblick, wie die Asset-Identifizierung CIs in zugeordnet wird CMDB.

Erkannte Elemente werden berücksichtigt **Übereinstimmend** , **Nicht Abgeglichen** , Oder **Neu Klassifiziert** . Identifizierte CIs befinden sich in **Übereinstimmend** status.

Um das Auffinden potenzieller Übereinstimmungsprobleme zu erleichtern, wird die CI-Suchregel, die dem CI entspricht, in angezeigt **CI-Übereinstimmungsregel** Feld.

Hinweis:
CI-Übereinstimmungsregel Außenunterstützung ist nur für verfügbar Qualys Integration.

Wenn keine Übereinstimmung gefunden wurde, wird ein CI in erstellt *`Nicht abgeglichenes CI`* Klasse `[sn_sec_cmn_unmatched_ci]` , `[cmdb_ci_Unclassed_Hardware]` , Oder `[cmdb_ci_unvollständig_ip]` Von CMDB. Wenn das ursprüngliche nicht abgeglichene CI neu klassifiziert wurde, werden erkannte Elementdatensätze aktualisiert, um diesen Status widerzuspiegeln. Weitere Informationen finden Sie unter Nicht abgeglichene CIs Und Zeigen Sie nicht abgeglichene Konfigurationselemente an, und klassifizieren Sie sie erneut Weitere Informationen finden Sie unter .

Standardmäßig berechnet der geplante Job **Security Operations** > **CMDB** > **Erkannte Elemente** Modul listet nicht übereinstimmende Konfigurationselemente auf. Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Eine Beschreibung der Felder in erkannten Elementen finden Sie unter Formularfelder „erkannte Elemente“ .

CI-Changes für erkannte Elemente für Konfigurations-Compliance

Der Standardwert der Eigenschaft `sn_sec_cmn.Update_on_ci_Change` Ist `Wahr` . Wenn also das Konfigurationselement (Configuration Item, CI) für ein erkanntes Element aktualisiert wird, werden auch die Testergebnisse aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Die externe ID für das Testergebnis wird aktualisiert, und die Risikopunktzahl, Zuweisungsregeln, Regeln für Korrekturaufgaben und Korrekturzielregel werden neu bewertet. Wenn ein Testergebnis mit demselben Test und CI vorhanden ist, werden die Testergebnisse mit dem vorhandenen Testergebnis aktualisiert, und das aktuelle Testergebnis wird mit dem Substatus geschlossen Ungültiges CI . Arbeitsnotizen werden entsprechend hinzugefügt.

Wenn Sie das CI für das vorhandene Testergebnis nicht aktualisieren möchten, legen Sie die Eigenschaft auf „falsch“ fest. Wenn sich in diesem Fall ein CI ändert, wird ein neues Testergebnis erstellt, und das vorhandene wird als geschlossen Ungültiges CI .

Nicht übereinstimmende erkannte Elemente für abgleichen Konfigurations-Compliance

Erstellen Sie eine geplante Aufgabe, um nicht übereinstimmende erkannte Elemente abzugleichen. Wenn ein Testergebnis erstellt wird, ist das Konfigurationselement (Configuration Item, CI), das ihm zum Zeitpunkt der Erstellung hinzugefügt wurde, möglicherweise veraltet.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn sich die Informationen in der CMDB ändern, werden nicht übereinstimmende CI-Informationen nicht abgeglichen. Wenden Sie zum Abgleich CI-Suchregeln auf die Testergebnisse an, die sich in einem nicht abgeglichenen Status befinden, wenn die CMDB mit den neuesten CIs aktualisiert wird.
Eine geplante Aufgabe wird bei Bedarf ausgeführt, um die CI-Übereinstimmungsregel für die erkannten Elemente in einem nicht abgeglichenen Status erneut anzuwenden. Wenn sich das CI nach erneuter Anwendung der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Betroffene Testergebnisse werden ebenfalls aktualisiert. Details finden Sie unter CI-Changes für erkannte Elemente für Konfigurations-Compliance.

Hinweis:

Beginnend mit Konfigurations-Compliance v24 können Sie die erneute Anwendung von CI-Suchregeln für erkannte Elemente mit dem Substatus „CI außer Betrieb genommen“ überspringen, indem Sie die Systemeigenschaft aktivieren *sn_sec_cmn.skipItemsWithCIDecommissioned*.

Prozedur

1. Navigieren zu **Alle** > **Security Operations > Nicht Abgeglichene Erkannte Elemente Abgleichen**an.
2. Klicken Sie auf der Seite Hintergrundaufträge auf **Erstellen Sie einen Abgleichsauftrag** .
3. Füllen Sie im Formular die Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können nur das Feld Parameter bearbeiten.

Hintergrundauftrag

Feld	Beschreibung
Anzahl	Eindeutige Auftragsnummer.
Erstellt von	Anwender, der den Auftrag erstellt hat.
Parameter	Parameter zum Abgleichen der nicht übereinstimmenden erkannten Elemente: ○ Grenzwert: Maximale Anzahl erkannter Elemente, die abgeglichen werden sollen. Wenn Sie keinen Wert eingeben, werden 10.000 erkannte Elemente abgeglichen. ○ FirstDiscovereditem: Erstes erkanntes Element, das abgeglichen werden muss. Wenn Sie keinen Wert eingeben, beginnt der Abgleichsprozess mit dem ersten erkannten Element.
Status	Aktueller Status des Hintergrundauftrags.
Statusbeschreibung	Beschreibung des aktuellen Status des Hintergrundauftrags.
Auftragstyp	Typ des Auftrags. Der Wert ist **Nicht übereinstimmende erkannte Elemente abgleichen** .
Gestartet um	Zeit, zu der der Auftrag gestartet wurde.
Endete um	Zeit, zu der der Auftrag abgeschlossen wurde.
Auftragsdauer	Gesamtzeit, die für den Abschluss des Auftrags benötigt wurde.
Substatus	Substatus für den ausgewählten Status.
Notizen	Anzahl der verarbeiteten Datensätze.

4. Klicken Sie auf **Absenden**.

Hinweis:
- Um die Ausführung des Auftrags zu beenden, klicken Sie auf **Abbrechen** .
- Sie können nicht übereinstimmende CIs nicht abgleichen oder CI-Suchregeln beim Importieren von Hosts oder Testergebnissen nicht erneut anwenden.

Wenden Sie CI-Suchregeln erneut auf ausgewählte erkannte Elemente für an Konfigurations-Compliance

Wenden Sie Suchregeln für Konfigurationselemente (Configuration Item, CI) erneut auf ausgewählte erkannte Elemente aus den Auswahlaktionen der Listenansicht „erkannte Elemente“ an. Der Administrator muss möglicherweise eine Suchregel aus mehreren Gründen bearbeiten oder aktualisieren. Wenn sich die Suchregel ändert, können sie sie erneut auf die erkannten Elemente anwenden.

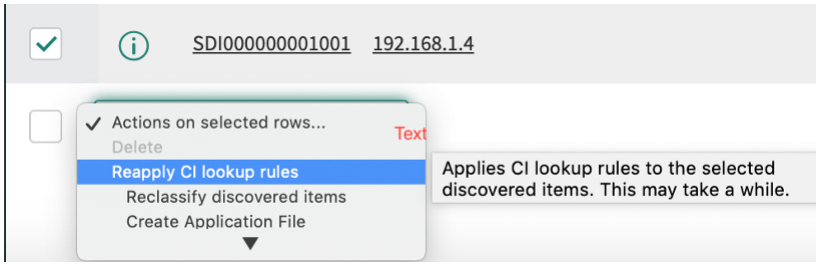
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rollen:

Warum und wann dieser Vorgang ausgeführt wird
Wenn sich das CI ändert, nachdem die CI-Suchregeln erneut angewendet wurden, werden die erkannten Elemente mit dem neuen CI und den Testergebnissen aktualisiert. Weitere Informationen finden Sie unter CI-Changes für erkannte Elemente für Konfigurations-Compliance.

Prozedur

1. Navigieren zu **Alle** > **Sicherheitsvorgänge** > **CMDB** > **Erkannte Elemente**an.
2. Wählen Sie die erforderlichen erkannten Elemente aus, und klicken Sie auf **Aktion für ausgewählte Zeilen** .



3. Wählen Sie Aus **Wenden Sie die CI-Suchregeln erneut an** Aus der Liste.

Die Regeln werden auf diese erkannten Elemente erneut angewendet.

Hinweis:

Beginnend mit Konfigurations-Compliance v15.1.5. Sie können die erneute Anwendung von CI-Suchregeln auf erkannte Elemente mit dem Substatus „CI außer Betrieb genommen“ überspringen, indem Sie die Systemeigenschaft aktivieren *sn_sec_cmn.skipItemsWithCIDecommissioned*.

Die Tenable Vulnerability Integration Mit Konfigurations-Compliance

Die Tenable.io Produkt von Tenable Vulnerability Integration Importiert Richtlinien, Steuerungen (Testergebnisse) und Konfigurationstests zur Verarbeitung in Konfigurations-Compliance Anwendung.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Tenable.io

Die Tenable Vulnerability Integration Wird unterstützt.

Sie können importierte Daten verwenden, um:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

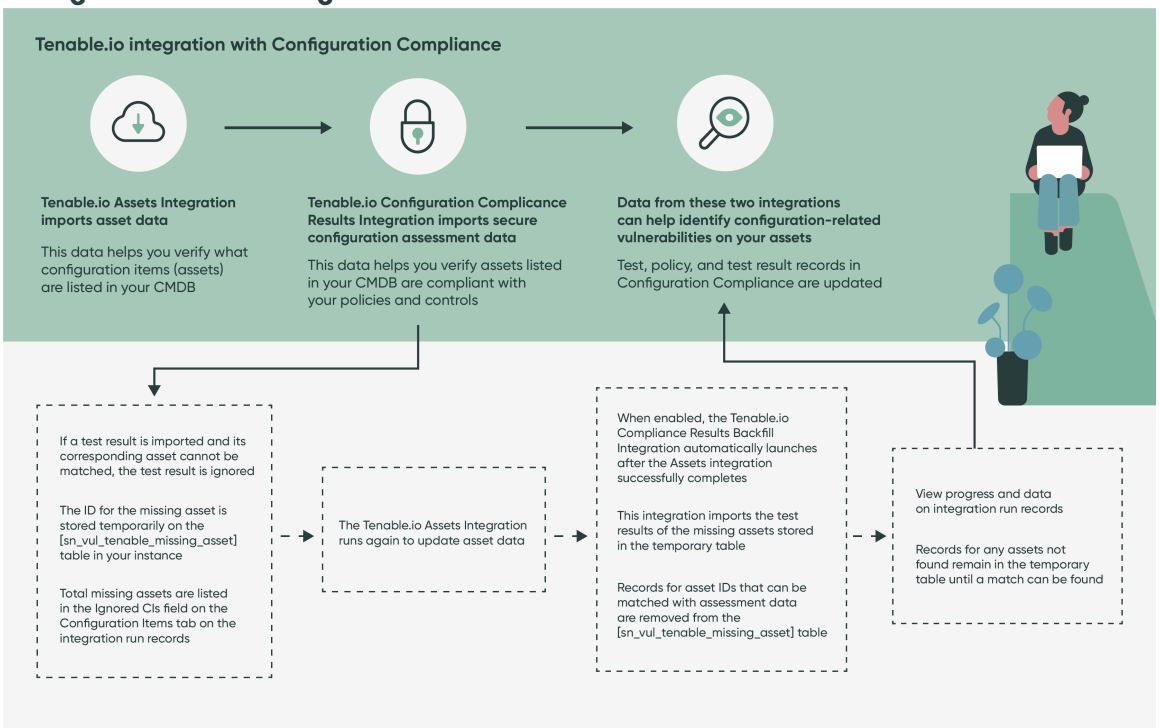
- Identifizieren Sie konfigurationsbezogene Schwachstellen in Ihren Assets, die in aufgeführt sind Configuration Management Database (CMDB)
- Überprüfen Sie, ob Ihre Assets Ihren Richtlinien und Steuerungen entsprechen.

Assets-Daten, Richtlinien, Steuerungen (Testergebnisse) und Konfigurationstests werden mit den folgenden Integrationen importiert:

- Tenable.io Asset-Integration
- Tenable.io Integration Von Compliance-Ergebnissen
- Tenable.io Integration Der Compliance-Ergebnisse Im Backfill

Die folgende Abbildung zeigt, wie die Integrationen zusammenarbeiten, um Asset- und Konfigurationsbewertungsdaten zu importieren und ignorierte CIs abzugleichen, die während eines Imports übersehen werden.

Importieren Sie den Flow für die Ergebnisse der sicheren Konfigurationsbewertung



Daten werden importiert, aktualisiert und in den Testergebnis-, Richtlinien- und Konfigurationstestdatensätzen in angezeigt Konfigurations-Compliance Anwendung.

In einigen Fällen unterscheidet sich die Anzahl der importierten Konfigurationselemente (Configuration Items, CIs) für Tenable.io Asset-Integration und Tenable.io Integration Von Compliance-Ergebnissen. In diesem Fall werden temporäre Datensätze für die ignorierten Asset-IDs erstellt und gespeichert. Diese Datensätze können später mit importierten Bewertungsdaten abgeglichen werden, indem Importe aus der Compliance-Ergebnisse-Backfill-Integration importiert werden.

Angenommen, die Asset-Integration importiert 80 Assets bei einer Integrationsausführung, die Compliance-Ergebnisintegration hingegen 100.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können die Anzahl der ignorierten CIs bei Integrationsausführungen überprüfen, indem Sie zu navigieren **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**an. Klicken Sie auf den Namen einer Integration, um den Datensatz zu öffnen. Auf der **Schwachstellenintegration Wird Ausgeführt** Zugehöriger Link, öffnen Sie einen Datensatz für die Integrationsausführung, und wählen Sie aus **Elemente** Registerkarte, um den Wert in anzuzeigen **Ignorierte CIs** Feld. Dieses Feld verfolgt die Gesamtzahl der ignorierten (fehlenden) Assets aus dem Import.

Durch Vergleich von Werten in **Ignorierte CIs** Felder in jedem Datensatz der Integrationsausführung gibt es einen Unterschied von 20 ignorierten CIs. Daher wird die Auffüllungsintegration automatisch ausgeführt, wie im vorherigen Bild gezeigt. Diese Integration importiert die Konfigurationsbewertungsinformationen für die zusätzlichen 20 Assets, die von der Compliance-Ergebnisintegration gefunden wurden, aber von der Asset-Integration verfehlt wurden. Da Bewertungsdaten für fehlende Assets nicht importiert werden, wird Tenable.io Compliance-Ergebnisse Backfill-Integrationsimporte bis zu 200 Asset-IDs pro Integrationsausführung, um die fehlenden Assets mit den entsprechenden Bewertungsdaten abzugleichen. Alle Datensätze, die für fehlende oder ignorierte Assets erstellt und in der temporären Tabelle aufgeführt wurden, werden gelöscht, nachdem diese Assets und ihre Daten abgeglichen wurden.

Hinweis:
Es können mehrere Ausführungen dieser Integrationen erforderlich sein, um alle ignorierten Assets zu importieren.

Weitere Informationen zum Aktivieren und Konfigurieren von Tenable.io Asset-Integration, siehe Konfigurieren Sie die Tenable-Schwachstellenintegration mit dem Setup-Assistenten. Siehe Verständnis der Tenable-Schwachstellenintegration Um weitere Informationen zur Integration zu erhalten.

Die Tenable.io Integration von Compliance-Ergebnissen und der Tenable.io Compliance-Ergebnisse – Backfill-Integration ist standardmäßig inaktiv.

So aktivieren Sie sie:

1. Navigieren zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**an.
2. Klicken Sie in der Liste Tenable-Integrationen auf einen Integrationsnamen, um den Datensatz zu öffnen, und wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren. Möglicherweise möchten Sie die Zeitplaneinstellungen in ihren Standardwerten belassen, damit diese Integrationen beginnen.

CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Konfigurations-Compliance Integrationen von Schwachstellen von Drittparteien

Wenn Daten aus einer Drittpartei-Integration importiert werden, Konfigurations-Compliance Verwendet automatisch Hostdaten, um nach Übereinstimmungen in zu suchen Configuration Management Database (CMDB). Dies geschieht mit **CI-Suchregeln** . Diese Regeln werden verwendet, um Konfigurationselemente (Configuration Items, CIs) zu identifizieren und dem Testergebnisdatensatz hinzuzufügen, um die Korrektur zu erleichtern.

Wenn Assets importiert werden, wird zuerst eine Suche für durchgeführt **Erkannte Elemente** Listen Sie mithilfe von Drittpartei-IDs auf, um Übereinstimmungen mit Konfigurationselementen (Configuration Item, CIs) aus vorherigen Importen zu finden. Wenn eine Host-ID-Übereinstimmung gefunden wird, wird sie als verwendet **Konfigurationselement** Feld im Testergebnisdatensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können mit sehen, wie importierte Assets CIs zugeordnet werden **Erkannte Elemente** Liste. Wenn keine Übereinstimmung gefunden wird oder das Feld cmdb_ci leer ist, verwenden die Regeln die anderen Hostinformationen, um zu versuchen, das CI korrekt zu identifizieren. Wenn immer noch keine Übereinstimmung gefunden wird, wird ein Platzhalter-CI erstellt und als festgelegt **Nicht abgeglichenes CI** . Siehe Nicht abgeglichene CIs Um weitere Informationen zur Behandlung dieser CIs zu erhalten.

Ein neues erkanntes Element wird erstellt und diesem CI zugeordnet.

Hinweis:
CI-Suchregeln sind nur für verfügbar Qualys Integration für Security Operations.

CI-Suchregeln können domänengetrennt sein und quellspezifisch sind. Jede Quelle kann mehrere Bereitstellungen haben. Qualys kann mehrere Bereitstellungen der Qualys-Integration haben. Jede Bereitstellung verfügt über einen eigenen Satz von CI-Suchregeln.

Hinweis:
CI-Suchregeln werden von allen Bereitstellungen der Schwachstellenintegration freigegeben. Wenn eine Regel gelöscht oder geändert wird, wirken sich die Löschung oder Änderungen auf alle Bereitstellungen der Schwachstellenintegration aus.

Beim Versuch einer Übereinstimmung besteht der erste Schritt in einer Lieferanten-ID-Suche nach einer genauen Übereinstimmung für Quelle, Source_instance und Lieferanten-ID. Dann werden Suchregeln in der Reihenfolge von der niedrigsten bis zur höchsten ausgeführt und beendet, wenn eine Regel nur ein einzelnes CI als Übereinstimmung zurückgibt. Wenn eine Regel so erstellt wird, dass sie mehr als ein CI zurückgibt, wird nur die erste Übereinstimmung verwendet.

Hinweis:
Um einen Abgleich bei Netzwerkelementen auf niedriger Ebene zu vermeiden, wenn ein übereinstimmendes CI einer von ist `Dscy_switchport` , `cmdb_ci_Network_Adapter` , `cmdb_ci_nic` , Oder `cmdb_ci_ip_address` , Das übergeordnete CI wird zurückgegeben.

Eine Systemeigenschaft zum Ausschließen von CI-Klassen ist verfügbar. Diese Eigenschaft ist mit Upgrade nicht verfügbar. Siehe Ignorieren Sie CI-Klassen Für Upgrade-Informationen und Anweisungen zum Festlegen der Eigenschaft.

Um das Auffinden übereinstimmender Probleme zu erleichtern, wird die CI-Suchregel, die zum Auffinden verwendet wird, dem Datensatz „erkanntes Element“ in hinzugefügt **CI-Übereinstimmungsregel** Feld. Suchregeln werden nach den niedrigsten Werten ausgewertet **Reihenfolge** Wert zuerst.

Einige von Qualys CI-Suchregeln, die im Lieferumfang des Basissystems enthalten sind:

- QUALYS-HOST-ID
- FQDN
- NetBIOS
- DNS
- IP

Einige der im Lieferumfang des Basissystems enthaltenen Microsoft Defender-CI-Suchregeln sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- S3-Bucket
- Name
- Ressourcen-ID

Einige der im Lieferumfang des Basissystems enthaltenen Palo Alto Prisma Cloud-CI-Suchregeln sind:

- S3-Bucket
- Name
- Ressourcen-ID

Das Importieren von Testergebnisdaten kann eine Instanz belasten, und Leistungsprobleme mit Ressourcen können auftreten, wenn Regeln nicht sorgfältig erstellt werden. Die Logik, die zum Iterieren und Durchführen des Abgleichs innerhalb von verwendet wird CMDB Kann zu längeren Verarbeitungszeiten führen. Um eine potenzielle Verschlechterung der Ressourcen oder Leistungskomplikationen zu vermeiden, testen Sie alle anwenderdefinierten CI-Suchregeln oder Änderungen an vordefinierten **CI-Suchregeln** . Siehe Schritte zur Verhinderung doppelter oder verwaister Datensätze nach der Ausführung Vulnerability Response CI-Suchregeln Weitere Informationen zum verhindern doppelter verwaister Datensätze, zum Löschen von Daten und zum Bereinigen von Daten.

Aktualisierte CI-Suchregeln werden erneut angewendet

Wenn Sie eine CI-Suchregel ändern, klicken Sie auf **Änderungen Anwenden** Auf der Listenseite „CI-Suchregeln“, um alle Regeln für die erkannten Elemente erneut auszuführen, die:

- Wurden mit den aktualisierten Regeln abgeglichen
- Werden von keiner Regel abgeglichen

Wenn sich das Konfigurationselement (Configuration Item, CI) nach erneuter Anwendung der Suchregeln ändert, werden die erkannten Elemente mit dem neuen CI aktualisiert. Die Testergebnisse werden ebenfalls aktualisiert. Weitere Informationen finden Sie unter CI-Changes für erkannte Elemente für Konfigurations-Compliance.

Vorhandene Konfigurationselemente für werden dedupliziert Konfigurations-Compliance

Die Nachbesserung von CI-Duplikaten für Deduplizierungsaufgaben wird mit aktualisiert `sn_sec_cmn_src_ci.cmdb_ci` Eigenschaft.

Wenn eine Deduplizierungsaufgabe zum Aktualisieren der Konfigurationselemente (Configuration Items, CIs) verwendet wird, werden auch die erkannten Elemente aktualisiert, die sich auf diese CIs beziehen. Daher werden die Testergebnisse mit dem CI aktualisiert. Details finden Sie unter CI-Changes für erkannte Elemente für Konfigurations-Compliance.

CIs für werden erstellt Konfigurations-Compliance Mit der Identifizierungs- und Abgleichsmodul

Beginnend mit Konfigurations-Compliance11.1. Sie können Konfigurationselemente (Configuration Items, CIs) in erstellen Configuration Management Database (CMDB) Mit der Ire-API (Identification and Reconciliation Engine). Wenn Sie die IRE-API zum Erstellen von CIs verwenden, können Sie verhindern, dass doppelte CIs erstellt werden, und Sie können CI-Attribute abgleichen, indem Sie zulassen, dass nur autorisierende Datenquellen in schreiben CMDB.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine CI-Klasse (Tabelle) ist der ursprüngliche Tabellenname in der Instanzdatenbank. CMDB Enthält Basissystemklassen, die Daten zu CIs speichern.

IRE für die CI-Erstellung verwenden

Vor Version 11.1, wenn kein übereinstimmendes CI in der Liste erkannter Elemente oder gefunden wurde CMDB, Ein CI wurde in der nicht abgeglichenen CI-Klasse (`sn_sec_cmn_Unmatched_ci`).

Weitere Informationen finden Sie unter Nicht abgeglichene CIs .

Ab Version 11.1 können Sie die IRE-API verwenden, um CIs in zu erstellen CMDB. Anstatt die nicht abgeglichene CI-Klasse zu verwenden, wird ein CI in der Klasse „nicht klassifizierte Hardware“ oder „unvollständig durch IP identifiziertes Gerät“ erstellt.

CMDB CI-Klassen

Hinweis:
Um die neuen Klassen zu verwenden, aktivieren Sie CMDB CI-Klassenmodelle-Plugin. Andernfalls werden CIs in der nicht abgeglichenen CI-Klasse erstellt.

Ab Version 11.1: Wenn der Host, den Sie von einem Scanner einer Drittpartei importiert haben, nicht in der Liste erkannter Elemente oder gefunden werden kann CMDB, Wird in einem der folgenden neuen gespeichert CMDB CI-Klassen.

CMDB CI-Klassen

CMDB CI-Klasse	Beschreibung
Unvollständiges IP-identifiziertes Gerät (`cmdb_ci_Inclusive_ip`)	Das CI wird in dieser Tabelle erstellt, wenn in den vom Scanner empfangenen Hostinformationen nur die IP-Adresse verfügbar ist.
Nicht Klassifizierte Hardware (`cmdb_Unclassed_Hardware_ci`)	CI wird in dieser Tabelle erstellt, wenn in den vom Scanner empfangenen Hostinformationen eine der folgenden Informationen verfügbar ist: • Hostname • IP-Adresse • DNS • NETBIOS • MAC-Adresse **Hinweis:** Wenn die MAC-Adresse verfügbar ist, wird der Netzwerkadaptereintrag erstellt und mit dem nicht klassifizierten Hardware-CI verknüpft. Wenn sowohl die IP- als auch die MAC-Adresse verfügbar sind, wird auch das IP-Adressen-CI erstellt und mit dem nicht klassifizierten Hardware-CI verknüpft.

Das System verwendet automatisch eine nicht abgeglichene CI-Klasse, wenn einer der folgenden Fälle eintritt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die CMDB CI-Klassen-Plugin ist nicht aktiviert.
- IRE löst beim Erstellen eines neuen CI eine Ausnahme aus.

Zugehörige Informationen

Store-App „CMDB CI Class Models“

Identification and Reconciliation Engine (IRE)

Konfigurations-Compliance Übersicht über Zuweisungsregeln

Definieren Sie die Kriterien, nach denen Testergebnisse automatisch einer Zuweisungsgruppe zur Korrektur zugewiesen werden.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Eine standardmäßige Zuweisungsregel, **Der CI-Supportgruppe zuweisen** , Ist im Basissystem enthalten, das Testergebnisse dem zuweist **CI-Supportgruppe** . Standardmäßig inaktiv.

Die von den Zuweisungsregeln festgelegten Zuweisungsgruppen werden von verwendet **Regeln Für Korrekturaufgaben** Zum Zuweisen von Besitzern zu Korrekturaufgaben (RTS).

Automatische Zuweisung von Testergebnissen

Es gibt drei verschiedene Möglichkeiten, Testergebnisse mit zuzuweisen **Zuweisen mit** :

- Zuweisungsgruppe: Mit dieser Option können Sie eine der vorhandenen auswählen ServiceNow AI Platform® Anwendergruppen.
- Zuweisungsgruppenfeld: Mit dieser Option können Sie ein beliebiges Zuweisungsgruppenfeld auswählen, das in der Tabelle „cmdb_ci“ verfügbar ist. Standardmäßig werden die folgenden drei Gruppenfelder angezeigt:
  - Keine: Gibt keinen Standardwert für dieses Pflichtfeld an
  - Konfigurationselement: Genehmigungsgruppe
  - Konfigurationselement: Zuweisungsgruppe
  - Konfigurationselement: Supportgruppe
- Skript: Mit dieser Option können Sie die Bedingungen mithilfe eines Skripts definieren. Diese Option erfordert Codierung oder erweitert ServiceNow® Fachwissen.

Siehe Erstellen oder bearbeiten Konfigurations-Compliance Zuweisungsregeln Weitere Informationen zum Erstellen von Zuweisungsregeln.

Mit der Rolle sn_vulc.Remediation_owner können Sie Testergebnisse und Korrekturaufgaben anzeigen und aktualisieren, die ihnen oder ihren Zuweisungsgruppen zugewiesen sind. Um die Module anzuzeigen, navigieren Sie zu **Alle** > **Konfigurations-Compliance** > **Testergebnisse**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

> **Meine offenen Testergebnisse**, Oder **Konfigurations-Compliance** > **Korrekturaufgaben** > **Meine offenen Aufgaben**an.

Die Rolle „sn_vulc.Remediation_owner“ kann einem Anwender direkt zugewiesen werden, oder sie wird automatisch zugewiesen, wenn Sie einem Anwender die Rolle „itil“ zuweisen.

Bewertungsprozess für Zuweisungsregel

Wenn ein neues Testergebnis importiert oder nach dem Schließen erneut geöffnet wird, werden die Zuweisungsregeln anhand dieses Ergebnisses ausgewertet. Die Zuweisungsregeln werden nach CI-Abgleich und Berechnungen der Risikopunktzahl ausgewertet. Ein Testergebnis wird nur beim ersten Import und wenn eine Regel geändert wird, automatisch ausgewertet, es sei denn, es wird nach dem Schließen erneut geöffnet. Sie können Regeln nach Änderungen manuell erneut anwenden.

Der folgende Prozess wird für jedes neue oder erneut geöffnete Testergebnis verwendet:

- Für jede Zuweisungsregel für Testergebnisse wird das Testergebnis mit dem Zuweisungsfilter verglichen, wobei zuerst die Regel für die niedrigste Reihenfolge gilt.
- Wenn die Bedingung erfüllt ist, wird dem Testergebnis eine Zuweisungsgruppe zugewiesen. Die Suche wird beendet.
- Wenn die Bedingungen keine Übereinstimmung zwischen allen Regeln finden, bleibt das Testergebnis nicht zugewiesen.

Zuweisungsregeln werden erneut angewendet

Wenn Sie eine Zuweisungsregel ändern, verwenden Sie **Änderungen Anwenden** Schaltfläche auf der Listenseite „Zuweisungsregeln“, um alle geänderten Regeln für alle aktiven offenen Testergebnisse erneut auszuführen, mit Ausnahme der manuell zugewiesenen.

Hinweis:
Die Zuweisungsregeln bewerten manuell erstellte Zuweisungen nicht neu.

Die geplante Aufgabe [`Reapply all assignment rules`] Ist standardmäßig inaktiv. Wenn diese Option aktiviert ist, werden alle offenen Testergebnisse anhand aller aktiven Regeln mit Ausnahme der manuell zugewiesenen ausgewertet. Sie kann täglich, wöchentlich, monatlich, regelmäßig, einmal oder bei Bedarf ausgeführt werden.

Wichtig:
Als Administrator und Analyst können Sie die neuesten Zuweisungen für ausgewählte Testergebnisse in abrufen Arbeitsbereich des Schwachstellenmanagers. Diese Methode ist effizienter als die erneute Anwendung der Zuweisungsregeln für alle Testergebnisse in klassisch UI, die ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Arbeitsbereich des Schwachstellenmanagers.

Zuweisungsregeln und Zuweisung von Korrekturaufgaben

Normalerweise weisen Sie Ihre Korrekturaufgabe (RT) derselben Zuweisungsgruppe wie die darin enthaltenen Testergebnisse zu. Das tun die Regeln für Korrekturaufgaben standardmäßig.

Wenn Ihre RT beispielsweise nach Konfigurationselementklasse gruppiert, kann die erstellte Korrekturaufgabe durch die verschiedenen Zuweisungsgruppen getrennt werden. Eine Oracle Database TRG kann Gruppe 1 und eine Oracle Database TRG Gruppe 2 zugewiesen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Zuweisungsgruppe auf Ebene der Korrekturaufgabe geändert wird, werden alle Testergebnisse in dieser Korrekturaufgabe, die dieselbe Zuweisungsgruppe haben, auf die neue Zuweisungsgruppe aktualisiert. Die Testergebnisse werden als manuell zugewiesen markiert und sind nicht für eine weitere Regelauswertung berechtigt.

Zuweisungen werden aus entfernt Konfigurations-Compliance Korrekturaufgaben

Sie können löschen **Zugewiesen an** Und **Zuweisungsgruppe** Felder in Korrekturaufgaben und den zugehörigen Testergebnissen direkt aus den Testergebnisdatensätzen und Korrekturaufgaben, die Sie bestimmen, dass sie Ihnen oder Ihren Gruppen möglicherweise falsch zugewiesen sind.

Übersicht über den Workflow

Korrekturbesitzer können Datensätze für die Neuzuweisung mit aktualisieren **Zuweisung Aufheben** Schaltfläche.

Anwendungsfall für sn_vulc.Remediation_owner

Wenn Sie feststellen, dass RTS und die zugehörigen Testergebnisse nicht in Ihrem Korrekturbereich liegen oder wenn Sie der Meinung sind, dass Datensätze Ihnen oder Ihren Gruppen falsch zugewiesen wurden, können Sie sich selbst oder Ihre Gruppen aus dem entfernen **Zugewiesen an** Und **Zuweisungsgruppe** Felder in diesen Korrekturaufgaben-Datensätzen.

Heben Sie die Zuweisung des Moduls auf

Die **Zuweisung Aufheben** Die Schaltfläche wird in den Korrekturaufgaben- und Testergebnisdatensätzen in einem anderen Status als „Geschlossen“ oder „gelöst“ angezeigt.

Wenn Sie auswählen **Zuweisung Aufheben** , Sie werden aufgefordert, alle der Korrekturaufgabe zugeordneten Testergebnisse neu zuzuweisen und zu übergehen **Nicht Zugewiesen** Zuweisungstyp.

Hinweis:
Wenn ein Testergebnis einer Korrekturaufgabe eine andere Zuweisungsgruppe als die Korrekturaufgabe hat, wird die Zuweisung nicht aufgehoben. In den meisten Fällen wurden diese Testergebnisse manuell zugewiesen.

Alle Datensätze, die Sie entweder über die UI-Schaltfläche oder manuell aktualisieren, werden im Modul „nicht zugewiesen“ unter angezeigt Konfigurations-Compliance.

Für die Schritte zum Neuzuweisen von Datensätzen mit *Unassigned*UI-Aktion, siehe Entfernen Sie Zuweisungen aus Korrekturaufgaben für Sie oder Ihre Gruppen.

Systemeigenschaft und Benachrichtigungen

Wenn Sie ein Administrator mit der Rolle sn_vulc.Vulnerability_admin sind, wenn Sie auswählen **Zuweisung Aufheben** In einem Datensatz standardmäßig die Systemeigenschaft *sn_vulc.unassign_test_result_group.approval_required*Löst den Datensatz „Genehmigung der Statusänderung“ und den Datensatz „angeforderte Genehmigung“ aus. Außerdem wird die Anforderung in der Liste meine Genehmigungen des Genehmigers angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Als Schwachstellenadministrator können Sie festlegen `sn_vulc.unassign_test_result_group.approval_required`Systemeigenschaft zu **Falsch** Zum Deaktivieren des Genehmigungsprozesses.

- Wenn der Genehmiger Ihre Anforderung genehmigt, wird standardmäßig Folgendes ausgeführt: Die Systemeigenschaft `sn_vulc.default_assignment_group`Löscht die Felder Zugewiesen an und Zuweisungsgruppe und füllt das Feld Zuweisungstyp mit aus **Nicht Zugewiesen** . Als Schwachstellenadministrator können Sie den Wert in ändern `sn_vulc.default_assignment_group`Systemeigenschaft, damit die Zuweisungsfelder gelöscht werden und dann eine bestimmte Gruppe zugewiesen wird. Beispiel: Wenn ein Anwender auswählt **Zuweisung Aufheben** Für einen Datensatz, der zur Überprüfung an eine bestimmte Gruppe weitergeleitet werden soll, können Sie im Feld Wert der Systemeigenschaft eine System-ID für die Gruppe Ihrer Wahl hinzufügen.
- Wenn der Genehmiger Ihre Anforderung ablehnt, wird der Grund für die Ablehnung in angezeigt **Notizen** Registerkarte.

Alternativ, wenn `sn_vulc.default_assignment_group`lst nicht für eine bestimmte Gruppe konfiguriert. Standardmäßig werden Anwender, die Sie der Anwendergruppe „Benachrichtigung aufheben“ hinzufügen, benachrichtigt, wenn die Zuweisung von Datensätzen aufgehoben wird. Die Systemeigenschaft `sn_vulc.default_notification_group`Bestimmt die Benachrichtigungen an diese Gruppe.

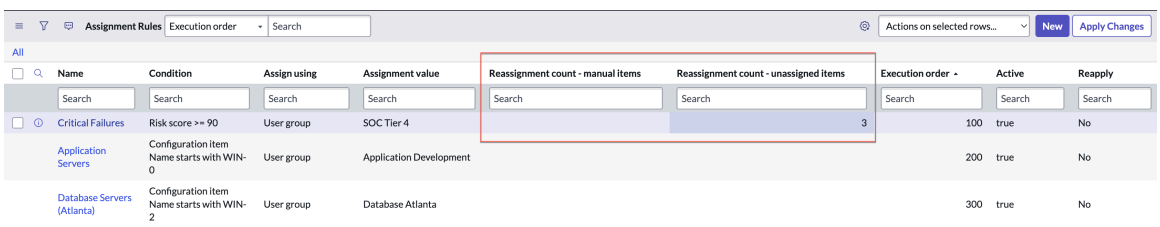
Der Zuweisungstyp, unabhängig davon **Manuell** , **Regel** , Oder **Nicht Zugewiesen** , Ist in den RT-Datensätzen und der Listenansicht verfügbar. Die **Nicht Zugewiesen** Der Zuweisungstyp wird nach angezeigt **Zugewiesen an** Und **Zuweisungsgruppe** Felder werden von der Systemeigenschaft der Funktion gelöscht.

Überwachen Sie Ihre Zuweisungsregeln mit der geplanten Aufgabe für diese Funktion

Eine tägliche geplante Aufgabe zählt die Datensätze, wenn sie zum wechseln **Nicht Zugewiesen** Zuweisungstyp. Mit dieser Anzahl können Schwachstellenanalysten alle Zuweisungsregeln überwachen und anpassen, die möglicherweise nicht gut funktionieren, basierend auf Zuweisungsregeln, die eine höhere Anzahl nicht zugewiesener RTS aufweisen.

Die `Reassignment count for assignment rules`Die geplante Aufgabe wird täglich ausgeführt und veröffentlicht die Gesamtzahl der RTS, die von dieser Funktion für eine bestimmte Zuweisungsregel nicht zugewiesen werden.

Der Auftrag zählt auch alle Datensätze, die manuell nicht zugewiesen wurden. Sowohl die manuellen Anzahlen als auch die von dieser Funktion gesammelten Anzahlen werden in der Liste „Schwachstellenzuweisungsregeln“ in zwei Spalten angezeigt: `Reassignment count - manual items`Und `Reassignment count - unassigned items`.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Als Schwachstellenadministrator können Sie diese Anzahlen anzeigen, indem Sie zu navigieren **Konfigurations-Compliance** > **Administration** > **Zuweisungsregeln**an.
2. Wählen Sie das Zahnradsymbol oben rechts in der Liste, und wählen Sie aus **Anzahl der Neuzuweisungen: Manuelle Elemente** , Und **Anzahl der Neuzuweisungen: Nicht zugewiesene Elemente** Zur Anzeige.
3. Jede RT, die ursprünglich von einer Regel zugewiesen wurde, später jedoch automatisch oder manuell neu zugewiesen wurde, enthält einen Verweis auf die ursprüngliche Regel in der Listenansicht.

Konfigurations-Compliance Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben

Erstellen Sie automatisch Korrekturaufgaben (RTS), um Ergebnisse mithilfe von Regeln für Korrekturaufgaben in einem Massenprozess zu analysieren. Die Kriterien, nach denen Aufgaben erstellt werden, sind so konfiguriert, dass Sie Testergebnisse nicht manuell zu Korrekturaufgaben zuweisen müssen.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Verständnis von Korrekturaufgaben

Korrekturaufgaben stellen eine Reihe von zu korrigierenden Testergebnissen dar. Die Gruppierung von Testergebnissen hat viele Vorteile. Sie können Testergebnisse durch die korrekturstatus verschieben, sie als untersucht markieren, zurückstellen und sie als Massenlösung markieren, indem Sie Gruppen verwenden. Sie können Bedingungen erstellen, um alle Ergebnisse mit angegebenen Ergebnissen, Technologien, Risikopunktzahlen und anderen Daten im Zusammenhang mit den Testergebnissen automatisch zu gruppieren. Testergebnisse können zu mehr als einer Korrekturaufgabe gehören, wodurch Sie die Flexibilität haben, aktiv mit einer Korrekturaufgabe zu arbeiten und eine andere zu überwachen. Alles hängt von Ihren organisatorischen Anforderungen ab. Sie können beispielsweise nach Zuweisung gruppieren und auch eine Gruppe erstellen, die Technologien enthält.

Korrekturaufgaben werden wie folgt erstellt.

- Manuell mit einer von zwei Optionen, um der Gruppe Testergebnisse hinzuzufügen.
  - **Manuell** : Erstellt eine Korrekturaufgabe ohne Einträge. Testergebnisse müssen manuell hinzugefügt werden.
  - **Filter** : Erstellt eine Korrekturaufgabe und verwendet Bedingungen, um dieser Korrekturaufgabe automatisch Testergebnisse hinzuzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Manuell hinzugefügte Testergebnisse werden nicht automatisch durch Regeln für Korrekturaufgaben oder Bedingungen für Korrekturaufgaben aus Korrekturaufgaben entfernt.

- Automatisch mithilfe von Regeln für Korrekturaufgaben. Diese Option ist die einfachste Option. Nach der Konfiguration erstellen die Regeln für Korrekturaufgaben alle gewünschten Korrekturaufgaben.

Von einer Korrekturaufgabe aus kann die Gruppe von Testergebnissen einem Anwender zugewiesen, bis zu einem späteren Zeitpunkt zurückgestellt und zum Erstellen von verwendet werden **Change-Anforderung** , Und so weiter.

Hinweis:

Mit der Rolle sn_vulc.Remediation_owner können Sie Testergebnisse und Korrekturaufgaben anzeigen und aktualisieren, die Ihnen oder Ihren Zuweisungsgruppen zugewiesen sind. Um die Module anzuzeigen, navigieren Sie zu **Alle** > **Konfigurations-Compliance** > **Testergebnisse** > **Meine offenen Testergebnisse**, Oder **Konfigurations-Compliance** > **Korrekturaufgaben** > **Meine offenen Aufgaben**an.

Wenn festgestellt wird, dass einer Korrekturaufgabe ein neues Testergebnis hinzugefügt werden kann, wird das Testergebnis in eingeschlossen **Testergebnisse** Zugehörige Liste der Korrekturaufgabe.

Beim Aktualisieren des Status einer Korrekturaufgabe kann der Status der zugehörigen Testergebnisse entsprechend dieser Korrekturaufgabe aktualisiert werden. Weitere Informationen zu Statusänderungen finden Sie unter Konfigurations-Compliance status.

Regeln für Korrekturaufgaben verstehen

Mit Regeln für Korrekturaufgaben können Sie definieren, wie Testergebnisse automatisch gruppiert und zugewiesen werden. Eine Standardregel, **Zuweisungsgruppe, Test** , Ist in der Basissystemgruppierung von Testergebnissen basierend auf einem Testergebnis enthalten **Zuweisungsgruppe** Und **Testen** Feld. Diese Regel ist standardmäßig deaktiviert. Sie können nach jedem anderen Satz von Werten in Spalten gruppieren, auf die über das Testergebnis zugegriffen werden kann. Sie können bis zu sechs Schlüssel und eine beliebige Anzahl von Bedingungen verwenden. Weitere Informationen finden Sie unter Erstellen oder bearbeiten Konfigurations-Compliance Regeln für Korrekturaufgaben.

Wichtig:
Als Administrator und Analyst können Sie die Regeln für Korrekturaufgaben für ausgewählte Testergebnisse im Vulnerability Manager-Arbeitsbereich auswerten. Diese Methode ist effizienter als die erneute Anwendung der Regeln für Korrekturaufgaben in der klassischen Anwenderoberfläche, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Arbeitsbereich des Schwachstellenmanagers.

Sie können Ihre Testergebnisse beispielsweise nach Zuweisungsgruppe oder Technologie und Konfigurationselement (CI) gruppieren. Für Testergebnisse, die das Unternehmen einem höheren Risiko aussetzen, kann ein anderer Satz von Regeln verwendet werden. Sie können eine Regel für Korrekturaufgaben für CIs mit niedrigem Schweregrad oder niedrigem Risiko haben. Siehe Anzeigen Konfigurations-Compliance Testergebnisse Für weitere Informationen zu verfügbaren Feldern.

Wenn ein neues Testergebnis importiert oder nach dem Schließen erneut geöffnet wird, werden die Regeln für Korrekturaufgaben darauf ausgewertet. Ein Testergebnis wird nur einmal ausgewertet, es sei denn, es wird nach dem Schließen erneut geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regeln für Korrekturaufgaben werden nach CI-Abgleich, Berechnungen der Risikopunktzahl und Zuweisungsregeln ausgewertet.

Der folgende Prozess wird für jedes neue oder erneut geöffnete Testergebnis verwendet:

- Für jede Korrekturaufgabenregel wird das Testergebnis mit dem Bedingungsfilter verglichen.
- Für jede Regel, bei der die Regelbedingung erfüllt ist, werden die Daten aus den Gruppenschlüsselspalten im Testergebnis abgerufen. Die Regel überprüft, ob eine Übereinstimmung vorhanden ist **Öffnen** Korrekturaufgabe, die derselben Zuweisungsgruppe wie das Testergebnis zugewiesen ist.

  Wenn die Korrekturaufgabe gefunden wird, wird das Testergebnis der vorhandenen Korrekturaufgabe in hinzugefügt **Öffnen** status.

- Wenn keine Korrekturaufgabe in vorhanden ist **Öffnen** status ist gefunden, die Regel erstellt eine Korrekturaufgabe und weist sie basierend auf zu **Anwendergruppe** Oder **Schlüssel** Wert in der Regel und platziert das Testergebnis darin.

Es kann mehr als eine Testergebnisregel definiert werden, um verschiedene Arten von Ergebnissen zu gruppieren. Da jedes Ergebnis mit den Regelbedingungen verglichen wird, bevor es in eine Korrekturaufgabe eingefügt wird, können zu viele Regeln Auswirkungen auf die Leistung haben.

Wenn eine Korrekturaufgabenregel gelöscht wird, haben Sie die Möglichkeit, alle offenen Aufgaben zu löschen, die von der Regel erstellt wurden. Dies gilt sowohl für die Regelformularansicht als auch für die Listenansicht.

Wenn eine Korrekturaufgabenzuweisung vorgenommen oder geändert wird, wird **Zuweisungsgruppe** Und **Zugewiesen an** Felder führen ein Rollup zu allen Testergebnissen durch, mit Ausnahme der, bei denen das Testergebnis eine andere Zuweisungsgruppe als die RT hat. Weitere Informationen zu Zuweisungsregeln finden Sie unter Konfigurations-Compliance Übersicht über Zuweisungsregeln. Diese Zuweisungen werden beim nächsten Import automatisch für diese Gruppe verwendet.

Verfolgen Sie die Anzahl der Zurückstellungen für Testergebnisse und Korrekturaufgaben

Verfolgen Sie ab v14.3, wie oft ein Testergebnis oder eine Korrekturaufgabe im Modul „mehrere Zurückstellungen“ zurückgestellt wird. Eine geplante Aufgabe, **Legen Sie die Anzahl der Zurückstellungen fest** , Wird täglich ausgeführt, um Anzahlen für Datensätze zu buchen, die mehr als einmal in der Spalte „Anzahl der Zurückstellungen“ in den Datensätzen, die im Modul „mehrere Zurückstellungen“ aufgeführt sind, zurückgestellt werden.

Konfigurieren von Rechnergruppen und Rechnern für Konfigurations-Compliance

Konfigurations-Compliance-Rechner werden verwendet, um Datensatzwerte zu aktualisieren, wenn vordefinierte Bedingungen erfüllt sind. Die Rechner werden basierend auf den Kriterien gruppiert, die verwendet werden, um zu bestimmen, wie die Datensätze aktualisiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Konfigurations-Compliance-Rechner

Die Anwendung Konfigurations-Compliance enthält zwei Arten von Rechnern, Risikorechner und Risikopunktzahl-Rollup-Rechner. Diese Rechnergruppen sind standardmäßig aktiviert.

Die Gruppe des Risikopunktzahlrechners wurde in Risikorechner umbenannt.

Die Rollup-Rechner für Risikopunktzahl enthält Rollup-Rechner für Konfigurationstests und Korrekturaufgaben.

Die Konfiguration von Risiko- und Rollup-Rechnern für die Korrektur von Testergebnissen und Korrekturaufgaben umfasst die folgenden Aufgaben:

- Erstellen Sie einen Risikorechner
- Erstellen Sie einen Rollup-Rechner für die Risikopunktzahl

Nachdem Sie einen Risikorechner erstellt haben, ist er für Berechnungen mit der nächsten Datenerfassung verfügbar. Nachdem Sie sie erstellt haben, können Sie sie auch bei Bedarf anwenden.

Weitere Informationen zu Rechnern und Rechnergruppen finden Sie unter Konfigurations-Compliance Rechnergruppen.

Konfigurations-Compliance Ausnahmemanagement – Übersicht

Wenn Ihre Organisation eine veröffentlichte Schwachstellenmanagement- oder Sicherheitsrichtlinie, einen Standard oder eine Richtlinie nicht einhalten kann, können Sie eine Ausnahme anfordern. Das Ausnahmemanagement umfasst das anfordern, Überprüfen, Genehmigen oder Ablehnen von Ausnahmen für eine Korrekturaufgabe, die nicht gemäß der Richtlinie korrigiert werden kann.

Wichtig:
Ausnahmeverwaltung wird in unterstützt Vulnerability Manager-Arbeitsbereich Und IT-Korrekturarbeitsbereich .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Einige Schwachstellen haben möglicherweise keinen Patch, eine Korrektur oder eine Lösung. Wenn eine Ausnahme genehmigt wird, bedeutet dies auch, dass Sie ein Risiko akzeptieren, da Sie die Konsequenzen bestätigen und akzeptieren, die sich daraus ergeben, dass die konfigurationsbezogene Schwachstelle nicht behoben wird.

Lebenszyklus einer Ausnahme

Eine Ausnahme ist eine Anforderung zum Zurückstellen der Korrektur einer Korrekturaufgabe für einen bestimmten Zeitraum.

Der Lebenszyklus einer Ausnahme sieht wie folgt aus:

- Ausnahme wird angefordert
- Ausnahmeanforderung wird genehmigt
- Nachverfolgung einer Ausnahmeanforderung
- Ablauf einer Ausnahmeanforderung

Ausnahme wird angefordert

Als Korrekturbesitzer können Sie mit dem Ausnahmeverwaltungsprozess eine Ausnahme für eine Korrekturaufgabe beantragen. Während des Genehmigungsprozesses verbleibt die Korrekturaufgabe in **Wird überprüft** status. Nachdem der Ausnahmegenehmiger diese Anforderung genehmigt hat, wird die Korrekturaufgabe zu einem verschoben **Zurückgestellt** status.

Wichtig:
Sie können eine Ausnahme im IT-Korrekturarbeitsbereich anfordern. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen.

Ausnahmeanforderung wird genehmigt

Korrekturaufgaben, die nicht sofort behoben werden können, werden überprüft, auf Risiko bewertet und zur Zurückstellung genehmigt, bis sie behoben werden können. Das Genehmigen einer Ausnahmeanforderung kann ein Workflow auf zwei Ebenen sein. Wenn nur der Genehmiger der ersten Ebene vorhanden ist, kann die Ausnahme angefordert und genehmigt werden. Wenn jedoch kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Weitere Informationen finden Sie unter Fügen Sie einen Ausnahmegenehmiger für hinzu Konfigurations-Compliance.

Wichtig:
Sie können eine Ausnahmeanforderung im Vulnerability Manager-Arbeitsbereich genehmigen oder ablehnen. Weitere Informationen finden Sie unter Fordern Sie Ausnahmen für Korrekturaufgaben und -Datensätze in an Arbeitsbereich des Schwachstellenmanagers.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Beginnt ab Konfigurations-Compliance V13.0: Wenn Sie die CC-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht zurück in Workflow ändern.

Sobald eine Ausnahmeanforderung für eine Korrekturaufgabe genehmigt wurde, können Sie die folgenden Aktionen ausführen:

- Erneut öffnen
- Löschen

Hinweis:

Ablehnungskommentare werden in den Arbeitsnotizen für eine Korrekturaufgabe angezeigt. Wenn eine Ausnahmeanforderung abgelehnt wird, wird diese Korrekturaufgabe in ihren vorherigen Status zurückgesetzt.

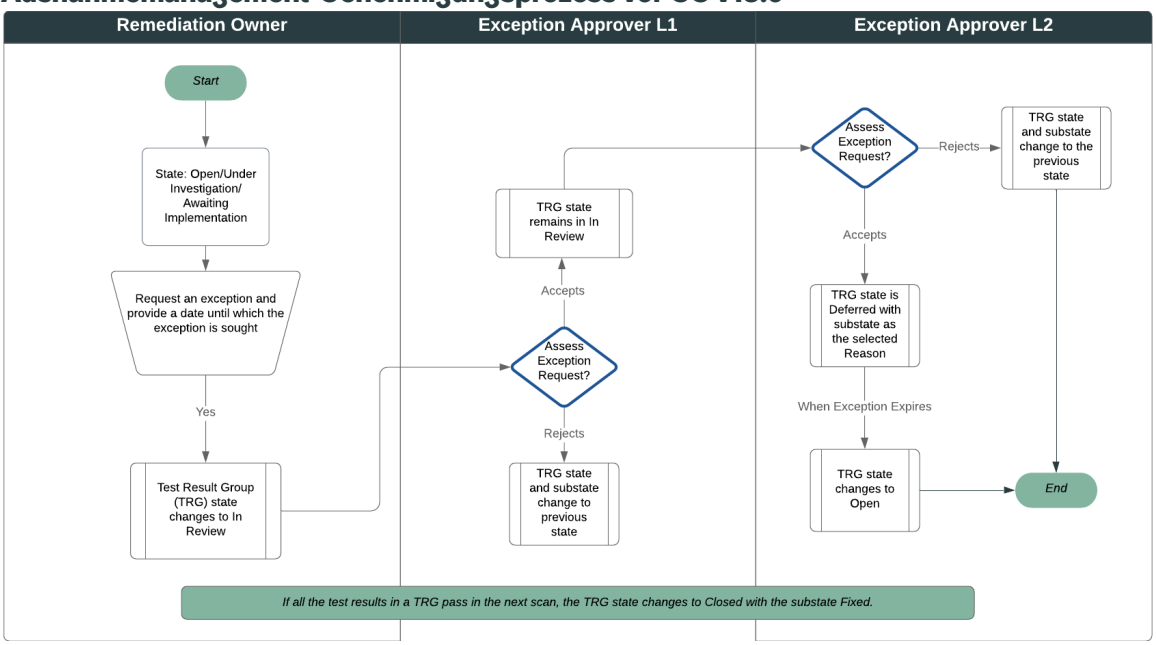
Nachverfolgung einer Ausnahmeanforderung

Nachdem Sie die Ausnahme ausgelöst haben, können Sie ihren Status mithilfe von nachverfolgen **Statusänderungsgenehmigungen** Registerkarte der Korrekturaufgabe. Wenn eine Aktion für eine Korrekturaufgabe ausgeführt wird, können Sie den Status der einzelnen Testergebnisse in dieser Korrekturaufgabe nicht nachverfolgen.

Ablauf einer Ausnahmeanforderung

Wenn eine Ausnahmeanforderung für eine Korrekturaufgabe abläuft, wird die Korrekturaufgabe auf zurückgesetzt **Öffnen** status.

Ausnahmemanagement-Genehmigungsprozess vor CC v13.0



Konfigurations-Compliance Change-Management

Als IT-Korrekturbesitzer können Sie Change-Anforderungen (CHG) direkt aus Korrekturaufgaben (RTS) in erstellen und verwalten Konfigurations-Compliance Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Change-Anforderungen und Konfigurations-Compliance Workflow

Change-Anforderungen und Change-Management sind Teil des Korrekturprozesses von Konfigurations-Compliance Workflow. Während dieser Korrekturphase können Sie Change-Anforderungen verwenden, um Testergebnisse zu priorisieren, nachzuverfolgen und zu korrigieren.

Die Konfigurations-Compliance Die Anwendung funktioniert mit ServiceNow AI Platform® IT-Change-Management-Prozess, mit dem Sie nicht konforme Software und Technologien in Ihrer Umgebung beheben können.

Mit Change-Management in Konfigurations-Compliance Anwendung können Sie Testergebnisse vorhandenen Change-Anforderungen zuordnen oder eine Korrekturaufgabe aufteilen und nur für ausgewählte Testergebnisse eine neue Korrekturaufgabe erstellen.

Weitere Informationen finden Sie unter Change-Anforderung in Konfigurations-Compliance erstellen.

Wichtige Begriffe

Tests

Tests sind Bibliotheken von Datensätzen, die Scans von Computing-Assets organisieren. Konfigurationstests definieren, wie eine Klasse von Technologie-Assets gesteuert werden soll. Ein Test ist alles, was verwendet werden kann, um eine Softwareklasse oder ein Hardware-Asset zu identifizieren, das nicht konform ist.

Testergebnisse

Testergebnisse werden von Drittpartei-Integrationen importiert. Sobald sie in angezeigt werden können Konfigurations-Compliance, Werden sie mit korrigiert **Korrekturaufgaben** . Gruppen werden gemäß Zuweisungsregeln zur Korrektur zugewiesen.

Hinweis:
Ab Version 14,9 von Konfigurations-Compliance, Testergebnis ist beschriftet, *Ergebnis* .

Nachbesserungsaufgabe

Testergebnisse werden gemäß Zuweisungsregeln in Korrekturaufgaben gruppiert und automatisch den Korrekturbesitzern zur Korrektur zugewiesen.

Hinweis:
Ab Version 14,9 von Konfigurations-Compliance, Testergebnis ist gekennzeichnet *Korrekturaufgabe* .

Testgruppen

Testgruppen beziehen sich auf autorisierende Dokumente und Testdatensätze. Eine Gruppe von Konfigurationstests definiert Testgruppen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Change-Anforderungen

Change-Anforderungen helfen Ihnen, kontrollierte Prozesse für die Korrektur zu implementieren. Sie können Change-Anforderungen mit Korrekturaufgaben in verwenden Konfigurations-Compliance Damit Sie nicht konforme Assets (Konfigurationselemente) identifizieren, nachverfolgen und lösen können, die zusätzliche Ressourcen erfordern oder für die Sie eine Zurückstellung anstreben könnten.

Weitere Informationen zu Testergebnissen und Korrekturaufgaben finden Sie unter Konfigurations-Compliance Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.

Wann Change-Anforderungen in verwendet werden sollen Konfigurations-Compliance

Change-Anforderungen helfen Ihnen, Korrekturaktivitäten für Ihre Testergebnisse zu initiieren und nachzuverfolgen. Wenn Korrekturbesitzer eine große Anzahl nicht korrigierter Test- oder Konfigurationselemente haben, können sie Change-Anforderungen verwenden, um Testergebnisse für die Zurückstellung zu identifizieren. Alternativ können sie Testergebnisse und Konfigurationselemente identifizieren und neu gruppieren, die mehr Ressourcen erfordern, als ursprünglich in der ursprünglichen Korrekturaufgabe identifiziert wurden.

Erstellen Sie Change-Anforderungen aus einer Korrekturaufgabe

Erstellen Sie eine Change-Anforderung direkt aus einer Korrekturaufgabe für alle Testergebnisse in der Korrekturaufgabe, oder verwenden Sie Filterung, um nur Testergebnisse zu identifizieren, die bestimmten Kriterien entsprechen. Erstellen Sie eine Change-Anforderung mit vorab ausgefüllten Informationen, um Ihre Untersuchung auf Testergebnisse zu beschleunigen, die manuelles Eingreifen erfordern.

Teilen Sie eine Korrekturaufgabe auf

Identifizieren Sie in einer vorhandenen Korrekturaufgabe eine Teilmenge von Testergebnissen, die Sie in eine neue Korrekturaufgabe verschieben möchten. Durch Erstellen einer neuen TRG können Sie mit einer bestimmten Gruppe von Testergebnissen arbeiten, ohne die ursprüngliche Korrekturaufgabe zu beeinträchtigen.

Ordnen Sie Testergebnisse einer vorhandenen Change-Anforderung zu

Ordnen Sie Testergebnisse vorhandenen Aufgaben zu, um zu vermeiden, dass bei der Lösung Ihrer Korrekturaufgaben doppelte Change-Anforderungen erstellt werden. Durch die Zuordnung einer Korrekturaufgabe zu einer Change-Anforderung, die bereits in Ihrer Instanz verfügbar ist, können Sie eine vorhandene Aufgabenliste verwenden.

Typen von Change-Anforderungen für eine Korrekturaufgabe

Sie können Change-Anforderungen direkt aus Korrekturaufgaben erstellen, genehmigen, implementieren, überprüfen und schließen, die Ihnen zugewiesen sind. Sie können drei Arten von Change-Anforderungen mit vorab ausgefüllten Informationen aus einer Korrekturaufgabe erstellen:

- Standard. Ein vorautorisierter Change, der ein geringes Risiko aufweist, relativ häufig ist und einem bestimmten Verfahren oder einer bestimmten Arbeitsanweisung folgt.
- Normal. Normale Change-Anforderungen folgen einem verbindlichen Prozess, der zwei Genehmigungsstufen erfordert, bevor sie implementiert, überprüft und geschlossen werden.
- Notfall. Ein Change zur Lösung eines schwerwiegenden Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einrichten, Installieren und Konfigurieren von Konfigurations-Compliance Anwendung

Bevor Sie die Anwendung in ausführen ServiceNow AI Platform®-Instanz müssen Sie zuerst herunterladen und installieren Konfigurations-Compliance Anwendung aus dem ServiceNow® Store. Diese Anwendung ist als separates Abonnement verfügbar.

Führen Sie vor der Installation die folgenden Schritte der Setup-Prüfliste aus, die in der folgenden Tabelle aufgeführt sind. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Weitere Informationen zu veröffentlichten Versionen von finden Sie Konfigurations-Compliance Anwendung sowie Drittpartei und ServiceNow Anwendungen, die damit kompatibel sind, finden Sie unter Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema [KB0856498] artikel in der HI Knowledge Base.

Weitere Informationen zum Abrufen von Berechtigungen für Store-Apps finden Sie unter Security Operations Und ServiceNow Store.

Richten Sie Prüflistenaufgaben ein

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist die Konfigurations-Compliance-Administratorrolle [sn_vulc.admin] zu. • Der Konfigurations-Compliance-Administrator [sn_vulc.admin] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. • Der Korrekturbesitzer [sn_vulc.Remediation_owner] liest und aktualisiert zugewiesene Datensätze. Die Rolle sn_vulc.Remediation_owner wird ebenfalls automatisch zugewiesen, wenn einem Anwender die Rolle itil zugewiesen wird.
Unterstützte Integrationen	Bevor Sie verwenden können Konfigurations-Compliance Um Konfigurationselemente zu korrigieren, müssen Sie eine Scannerintegration von Drittanbietern installieren und mindestens einen Netzwerkscan durchführen. Überprüfen Sie, ob Vulnerability Response Die Anwendung wird installiert und aktiviert, bevor unterstützte Integrationen von Drittanbietern konfiguriert werden. Weitere

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie Prüflistenaufgaben ein (Fortsetzung)

Setupaufgaben	Beschreibung
	Informationen finden Sie unter Vulnerability Response installieren. Um zu überprüfen, ob Integrationsanwendungen installiert und aktiviert sind, navigieren Sie zu **Abonnement-Management** > **Abonnements** In Ihrer Instanz. In der Liste werden die Abonnements angezeigt, die Ihr Unternehmen erworben hat. Weitere Informationen zu Integrationen von Drittparteien und eine Liste der unterstützten Produkte finden Sie unter Konfigurations-Compliance-Integrationen.

Qualys Vulnerability Integration

- Wenn Qualys Vulnerability Integration Ist bereits auf Ihrem System installiert, und Ihre API-Anmeldeinformationen unterscheiden sich von denen, für die Sie verwenden möchten Konfigurations-Compliance, Wechseln Sie zu Setup-Assistent (in Vulnerability Response) Und weisen Sie sie jedem zu **Qualys-PC** Integration.
- Navigieren zu **Qualys Schwachstellenintegration** > **Primäre Integrationen** Und bearbeiten Sie **Qualys-API-Anmeldeinformationen** Feld unter **Qualys-REST-Details** Registerkarte.

Für detailliertere Informationen zum Qualys Vulnerability Integration, Siehe Qualys Vulnerability Integration verstehen.

Sie sind jetzt bereit, die zu installieren Konfigurations-Compliance Anwendung. Weitere Informationen finden Sie unter Konfigurations-Compliance installieren.

Konfigurations-Compliance installieren

Bevor Sie ausführen Konfigurations-Compliance In Ihrem ServiceNow AI Platform®-Instanz müssen Sie zuerst herunterladen und installieren Konfigurations-Compliance Anwendung aus dem ServiceNow Store. Diese Anwendung ist als separates Abonnement verfügbar.

Vorbereitungen

Schließen Sie die Setup-Prüfliste ab, die in beschrieben ist Einrichten, Installieren und Konfigurieren von Konfigurations-Compliance Anwendung Vor der Installation. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Erforderliche Rolle: Administrator

Prozedur

1. Zum Aktivieren von ServiceNow-Produkte befolgen Sie die Schritte in Opt in to the ServiceNow Store products .
2. Zum Installieren einer Anwendung, die Sie über erworben haben ServiceNow Store, Befolgen Sie die Schritte in Install a ServiceNow Store application .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Alternativ, wenn Sie Ihre Berechtigung für verwalten möchten Konfigurations-Compliance Anwendung für andere ServiceNow AI Platform Führen Sie die Schritte in aus Manage entitlements from your ServiceNow instance .
4. Wenn Sie bereits installiert haben Konfigurations-Compliance Anwendung und Sie aktualisieren sie, siehe Install an update to a ServiceNow Store application .
5. Installieren Sie unterstützte Anwendungen.

   Separate Drittanbieteranwendungen erfassen und transformieren Daten in Konfigurations-Compliance. Bevor Sie verwenden können Konfigurations-Compliance Um Konfigurationselemente zu korrigieren, müssen Sie eine Scannerintegration von Drittanbietern installieren und mindestens einen Netzwerkscan durchführen.

   Informationen zum Installieren von Drittpartei-Integrationen für Konfigurations-Compliance, Siehe Konfigurations-Compliance-Integrationen.

Erstellen oder bearbeiten Konfigurations-Compliance Zuweisungsregeln

Erstellen Sie Regeln, um Testergebnisse basierend auf Filterbedingungen automatisch zuzuweisen. Diese Regeln weisen Testergebnisse beim Importieren zu.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Das Basissystem wird mit einem geliefert Konfigurations-Compliance Zuweisungsregel, **Der CI-Supportgruppe zuweisen** , Die Testergebnisse derselben Zuweisungsgruppe wie die CI-Supportgruppe zuweist. Diese Regel ist standardmäßig inaktiv. Sie können mit Filterbedingungen ändern. Mit Zuweisungsregeln definieren Sie eine oder mehrere Zuweisungsbedingungen und die Reihenfolge der Ausführung. Sobald ein Testergebnis mit einer Regelbedingung übereinstimmt, wird die Zuweisungssuche beendet.

Hinweis:
Neue oder aktualisierte Regeln werden beim nächsten Import automatisch oder manuell mithilfe von ausgewertet **Änderungen Anwenden** Schaltfläche in der Liste Zuweisungsregeln.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Zuweisungsregeln**an.
2. Öffnen Sie **Der CI-Supportgruppe zuweisen** Regel oder klicken Sie auf **Neu** .
3. Bearbeiten Sie **Der CI-Supportgruppe zuweisen** Regel, oder wenn **Neu** Füllen Sie die Felder im Formular entsprechend aus.

Konfigurations-Compliance-Zuweisungsregel

Feld	Beschreibung
Name	Der Name der Zuweisungsregel
Ausführungsreihenfolge	Reihenfolge, in der die Regeln ausgewertet werden. Die niedrigste Zahl wird zuerst ausgewertet. Regeln mit hoher Priorität, Testergebnisse, die eine spezielle Behandlung erfordern, wenn das Risiko kritisch ist, oder ein Testergebnis, das von der Compliance mit behördlichen Vorschriften behandelt werden sollte, sollten zuerst ausgeführt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	werden. Führen Sie als Nächstes Ihre allgemeinen Regeln aus, bei denen keine spezielle Behandlung erforderlich ist und Sie wissen, wer dafür verantwortlich sein sollte. Erstellen Sie abschließend eine Standardregel, um der Gruppe Testergebnisse zuzuweisen, die ermittelt, welcher Zuweisungsgruppe sie angehören soll. Diese Gruppe kann eine weitere Regel hinzufügen, um ihre Entscheidungen abzudecken. Diese Standardregel würde zuletzt ausgeführt.
Aktiv	Gibt an, ob die Zuweisungsregel aktiv ist.
Bedingung	
Bedingungsfelder	Bedingungen, die erfüllt werden müssen. Die Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird in diesem Datensatz oder Formular nicht unterstützt.
Neues Kriterium	Fügt weitere Bedingungsfilterfelder zur Auswahl hinzu.
Beschreibung	Text, der die Zuweisungsregel beschreibt.
Zuweisen mit	Um die Zuweisung von Gruppen zu automatisieren, die basierend auf dieser Regel erstellt wurden, wählen Sie eine der verfügbaren Optionen aus. ○ Anwendergruppe: Wählen Sie eine Anwendergruppe aus der Suchtabelle aus ○ Anwendergruppenfeld: Wählen Sie ein Anwendergruppenfeld aus dem Dropdown-Menü aus. ○ Skript: Erstellen oder bearbeiten Sie ein Skript. **Hinweis:** Das Erstellen oder Bearbeiten eines Skripts erfordert ServiceNow Fachwissen.
Anwendergruppenfeld	Wählen Sie die Anwendergruppe aus, die für die Korrektur von Tests verantwortlich ist, die den Bedingungen der Zuweisungsregeln entsprechen.

4. Klicken Sie auf **Absenden**.

Konfigurations-Compliance Korrekturzielregeln

Mit Korrekturzielregeln können Sie die erwarteten Zeitrahmen für die Korrektur von Testergebnissen festlegen. Sie können Benachrichtigungen an Anwender und Gruppen senden, wenn Zieldaten näher rücken und überfällig sind.

Wichtig:
Als Configuration Compliance-Administrator oder -Analyst können Sie das neueste Korrekturzieldatum für einen bestimmten Satz von Testergebnissen im Vulnerability Manager-Arbeitsbereich abrufen. Diese Methode ist effizienter als die Ausführung der Korrekturzielregeln für alle Testergebnisse in der klassischen Anwenderoberfläche, was ein zeitaufwändiger Prozess ist. Weitere Informationen finden Sie unter Bewerten Sie die Korrektureigenschaften der Datensätze in neu Arbeitsbereich des Schwachstellenmanagers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rollen: Konfigurations-Compliance-Administrator (sn_vulc_admin) oder ein Manager mit der Rolle sn_vulc.Manage_Remediation_target_rules.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

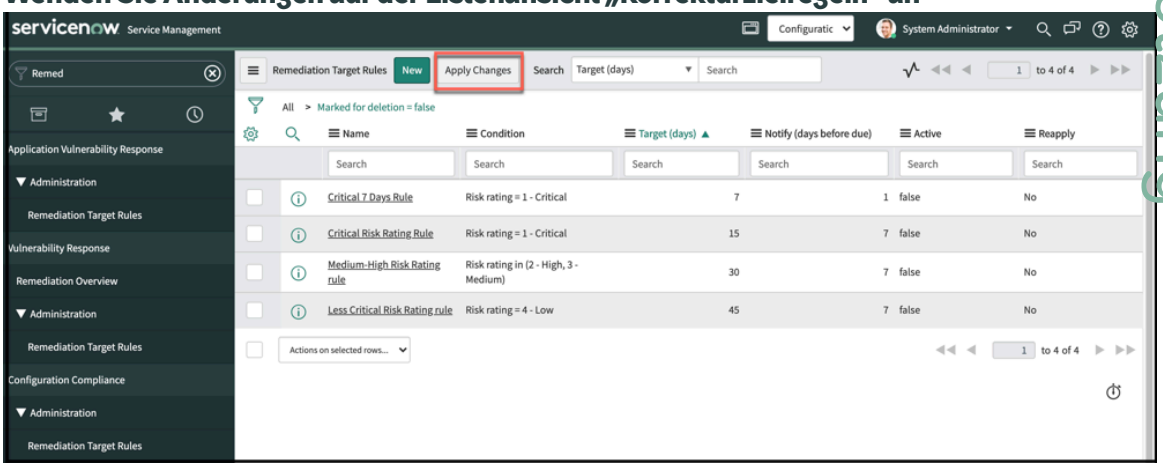
Korrekturzielregeln

Eine geplante Aufgabe, *`Evaluate and notify remediation targets`*, Wird täglich ausgeführt und verwendet aktive Korrekturzielregeln, um aktive Testergebnisdatensätze auszuwerten. Immer wenn Testergebnisdatensätze, die Korrekturaufgaben zugeordnet sind, aktualisiert oder geändert werden, werden die geänderten Werte von den Zielregeln ausgewertet, und Änderungen werden zusammengefasst und für zugehörige Korrekturaufgaben angezeigt.

Sie können vorhandene Korrekturzielregeln bearbeiten, deaktivieren oder löschen und neue erstellen. Wenn Sie eine Regel ändern, deaktivieren oder neu erstellen, haben Sie die Möglichkeit, auf zu klicken **Änderungen Anwenden** In der Listenansicht „Korrekturzielregeln“ und wenden Sie die Änderungen, die Sie vor der nächsten geplanten Aufgabe eingeführt haben, manuell an. Mit dieser Option können Sie Ihre Testergebnisdatensätze neu bewerten, ohne warten zu müssen. Wenn Sie Ihre Änderungen nicht manuell anwenden, werden Ihre Änderungen bei der nächsten täglichen geplanten Aufgabe erfasst und angewendet.

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Korrekturzielregeln** Zum Anzeigen von Korrekturzielregeln.

Wenden Sie Änderungen auf der Listenansicht „Korrekturzielregeln“ an



2. Klicken Sie auf eine Regel in der Spalte Name, um den zugehörigen Datensatz zu öffnen.
3. Wählen Sie aus **Aktiv** Kontrollkästchen im Datensatz der Korrekturzielregel zum Aktivieren von (Wahr) Alle deaktivierten Regeln (Falsch).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jedes Mal, wenn Sie eine Zielregel ändern oder hinzufügen, unabhängig davon, ob Sie die Änderungen manuell anwenden oder auf die nächste geplante Aufgabe warten, werden Ihre Änderungen verwendet, um alle aktiven Testergebnisse zusammen mit anderen Zielregeln auszuwerten, die von Ihren Änderungen betroffen sind. Wenn Sie die Änderungen manuell anwenden, kann diese Auswertung einige Zeit dauern, wenn Sie eine große Menge aktiver Testergebnisse haben, da alle von Ihren Änderungen betroffenen Regeln für eine Auswertung verwendet werden.

Der Standardwert für gezielte Korrekturtage ist beispielsweise 30. Wenn Sie eine neue Regel erstellen, die auch 30 für gezielte Korrekturtage enthält, werden diese Regel und alle Zielregeln mit 30 Tagen oder mehr als Zieldaten jeweils auf Ihre Testergebnisse angewendet.

Zielregeln deaktiviert und gelöscht

Wenn eine Regel aktiv ist, Wahr Wird in der Spalte aktiv in der Listenansicht Korrekturzielregeln angezeigt. Nachdem eine Regel deaktiviert wurde (Falsch), wird sie nicht mehr auf neue Testergebnisse angewendet. Die geplante Aufgabe verfolgt jedoch weiterhin alle vorhandenen Testergebnisse, auf die die Regel angewendet wurde. Wenn die deaktivierte Regel oder die deaktivierten Regeln anschließend erneut aktiviert werden, werden alle Testergebnisse mit leerem angezeigt **Korrekturzieldatum** Feld wird anhand der erneut aktivierten Regeln ausgewertet. Dies umfasst Testergebnisse, die erstellt wurden, während die Regeln deaktiviert wurden.

Wenn Regeln gelöscht werden, wird **Korrekturzieldatum** Und zugehörige Felder in geschlossenen Testergebnissen werden beibehalten. Die **Korrekturzieldatum** Und zugehörige Felder in nicht geschlossenen Testergebnissen werden gelöscht, und alle abhängigen Regeln werden erneut angewendet.

Um eine Regel zu deaktivieren, deaktivieren Sie im Datensatz der Korrekturzielregel das Kontrollkästchen aktiv, und klicken Sie auf **Aktualisieren** . Falsch Wird in der Spalte aktiv in der Listenansicht Korrekturzielregeln angezeigt.

Klicken Sie auf, um eine Regel zu löschen **Löschen** Wählen Sie im Formular oder alternativ in der Listenansicht die Regel oder Regeln aus, und klicken Sie auf **Löschen** Von **Aktionen für Zeilen** Liste. Die Regel wird nicht mehr in der Liste angezeigt, und die nächste Regel in der Reihenfolge des Vorgangs ersetzt die gelöschte Regel.

Wenn Sie eine Regel deaktivieren oder löschen und Ihre Änderungen vor der nächsten geplanten Aufgabe anwenden, wird die Regelreferenz aus dem Feld gelöscht, das Korrekturdatum und die Statusdaten bleiben jedoch erhalten. Wenn Sie Ihre Änderungen nicht manuell anwenden, wird die Regelreferenz mit der nächsten geplanten Aufgabe aus dem Feld gelöscht.

Informationen zu Zielregeln und der geplanten Aufgabe „Korrekturziele bewerten und benachrichtigen“

Die *`Evaluate and notify remediation targets`*Die geplante Aufgabe wird einmal täglich um 16:30 Uhr ausgeführt. Es greift alle aktiven Korrekturzielregeln auf und wertet alle aktiven Testergebnisse ab, beginnend mit den Testergebnissen mit dem frühesten Korrekturzieldatum. Es werden alle Testergebnisse ausgewertet, die die folgenden Kriterien erfüllen:

- Befinden sich nicht in **Geschlossen** status.
- Hat kein Korrekturzieldatum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Haben Korrekturzieldaten, die nach den Daten in den Korrekturzielregeln liegen.
- Werden erstellt, nachdem ein Scannerimport abgeschlossen wurde. Die geplante Aufgabe nimmt alle neuen Testergebnisse auf, die als Ergebnis eines Imports erstellt werden, und wertet sie aus.

Nachdem eine Zielregel definiert wurde, werden Korrekturzieldaten von berechnet *`Evaluate and notify remediation targets`*Geplante Aufgabe. Die geplante Aufgabe fügt ein Korrekturzieldatum hinzu, wenn kein vorhanden ist, oder wenn diese Regel ein früheres Datum als das im Datensatz enthält, aktualisiert sie das vorhandene Zieldatum.

Alle abgelaufenen Datensätze und Erinnerungsdaten, die den Zielregeln entsprechen, werden vom Auftrag abgerufen, und Benachrichtigungen werden gesendet. Bei deaktivierten Regeln löscht der Auftrag die Korrekturfelder in Testergebnisdatensätzen und beendet das Senden von Benachrichtigungen.

Die Eigenschaft „sn_sec_cmn.Evaluate_targetmissing_Records“ verhindert, wenn diese Option aktiviert ist *`Evaluate and notify remediation targets`*Geplante Aufgabe aus der Auswertung der verpassten Testergebnisse des Ziels. Diese Eigenschaft ist standardmäßig aktiviert.

Zieldaten und -Status in den Listen- und Formularansichten anzeigen

Konfigurations-Compliance Manager können das Korrekturzieldatum sowohl im Testergebnisformular als auch in Listenansichten anzeigen. Korrekturzielregeln werden auch nach einem Scannerimport ausgeführt und erneut ausgeführt, wenn ein Testergebnis erneut geöffnet wird.

Die geplante Aufgabe aktualisiert den **Korrekturziel** Und **Korrekturstatus** In der Listenansicht der Testergebnisse, und **Korrekturzielregel** , **Korrekturziel** , Und **Korrekturstatus** Felder im Testergebnisformular.

Hinweis:
Standardmäßig ist **Korrekturziel** Und **Korrekturstatus** Spalten werden in der Listenansicht Testergebnisse nicht angezeigt. Um diese Spalten anzuzeigen, müssen Sie sie auch der Listenansicht hinzufügen. Fügen Sie auf ähnliche Weise hinzu **Korrekturzielregel** , **Korrekturziel** , Und **Korrekturstatus** Felder zum Testergebnisformular.

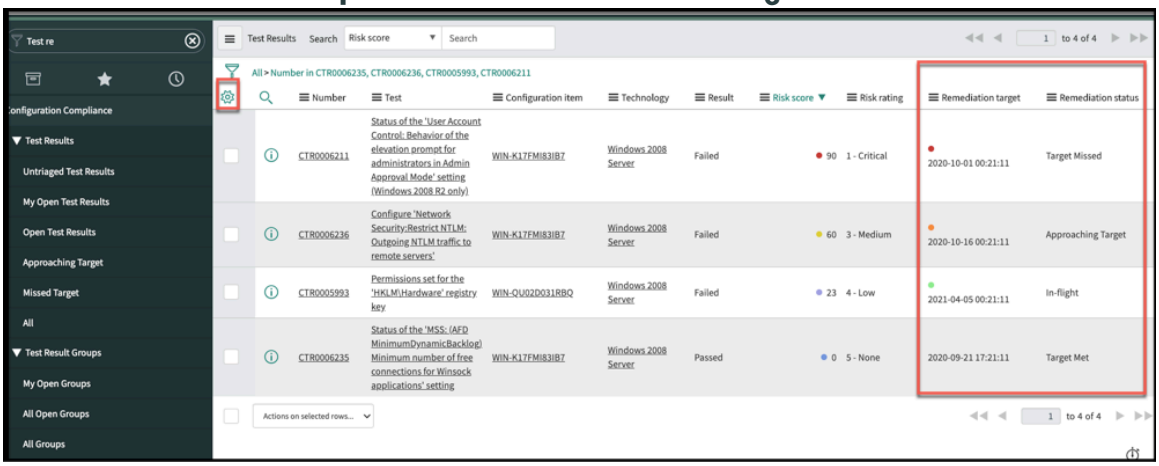
Verwenden Sie die Slushbuckets in den Menüs Einstellungen und zusätzliche Aktionen, wie in den folgenden Bildern gezeigt, um diese Spalten und Felder anzuzeigen. Klicken Sie für das zusätzliche Aktionsmenü im Testergebnisdatensatz auf das Menüsymbol, gefolgt von **Konfigurieren** Und **Formularlayout** Um den Slushbucket anzuzeigen und die Felder aus zu verschieben **Verfügbar** Bis **Ausgewählt** .

Das Korrekturzieldatum wird in der Listenansicht Testergebnisse als farbige Punkte codiert:

- Testergebnisse, die ihr Benachrichtigungsdatum nicht erreicht haben, werden grün angezeigt.
- Testergebnisse, die sich dem Korrekturzieldatum nähern, werden orange angezeigt.
- Testergebnisse nach dem Korrekturzieldatum werden rot angezeigt.

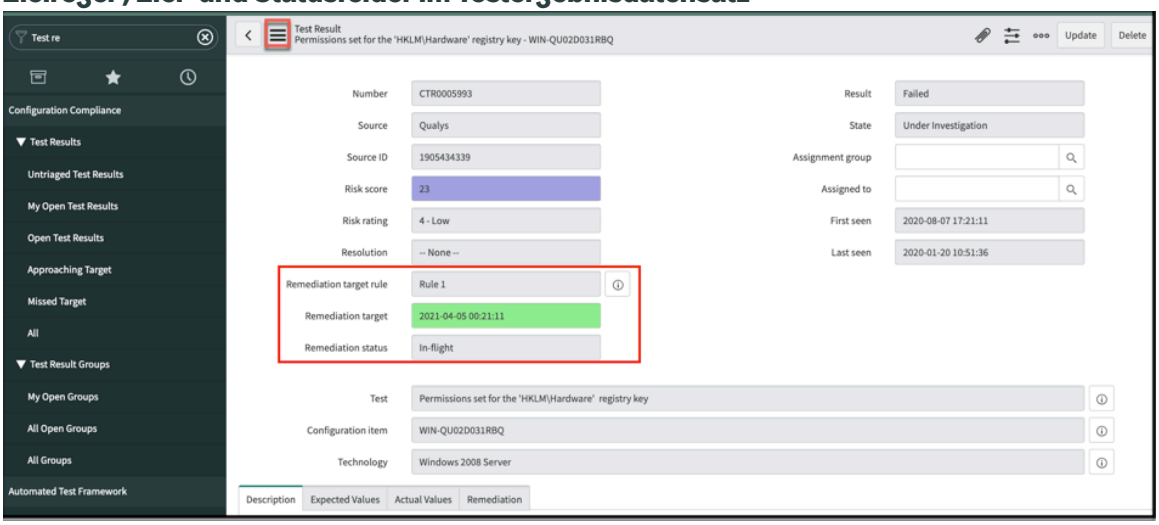
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturziel- und Statusspalten in der Listenansicht Testergebnisse



- Ziel Verfehlt : Das Zieldatum ist überfällig
- In Betrieb : Das Testergebnis wird ausgeführt

Zielregel-, Ziel- und Statusfelder im Testergebnisdatensatz



Testergebnisdatensätze werden auch visuell auf der angezeigt Konfigurations-Compliance Dashboard. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Übersicht** Und überprüfen Sie den Status des Dashboards. Die Übersicht enthält vorhandene Widgets und den Korrekturstatus. Die Farben der Diagramme entsprechen den Farben, die in der Listenansicht Testergebnisse und im Testergebnisdatensatz angezeigt werden.

Korrekturzielregel-Szenario

Wenn mehrere Korrekturzielregeln auf dasselbe Testergebnis angewendet werden, wird die restriktivste Regel angewendet.

Beispiel: Wenn ein am 01/2018 erstmals identifiziertes Testergebnis die Bedingungen für zwei Korrekturzielregeln erfüllt:

- Korrekturzielregel 1: Definiert am 03/07/2018; Korrekturziel ist 15 Tage seit der ersten Anzeige; berechnetes Korrekturzieldatum ist 03/16/2018 10:00:00.
- Korrekturzielregel 2: Definiert am 03/10/2018; Korrekturziel ist 10 Tage seit der ersten Anzeige; berechnetes Korrekturzieldatum ist 03/11/2018 10:00:00.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Korrekturziele werden aus berechnet **Zuletzt gesehen** Datum plus Anzahl der Tage (gemessen in 24-Stunden-Schritten).

Ab V14.5 werden Korrekturziele aus berechnet **Ziel von (Datum)** . Der Standardwert bleibt erhalten **Zuletzt Gesehen** . Ab v14.12 ist der Standardwert **Letzter Durchgang** .

In diesem Szenario gilt die Korrekturzielregel 2 für das Testergebnis, da es das restriktivere Datum aufweist: 10 Tage seit der ersten Identifizierung des Testergebnisses vs. 15 Tage.

Erstellen oder ändern Sie Zielregeln, und wenden Sie Änderungen erneut an

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Korrekturzielregeln** Zum Anzeigen, Bearbeiten und Erstellen neuer Korrekturzielregeln.
2. Klicken Sie in der Spalte Name auf eine Regel, um eine Zielregel zu öffnen und den Datensatz zu bearbeiten, oder klicken Sie alternativ auf **Neu** Um eine neue Zielregel zu erstellen.
3. Füllen Sie das Formular aus, um den erwarteten Korrekturzeitrahmen zu definieren, anzugeben, für welche Testergebnisse diese Regel mit Bedingungen gilt, und festzulegen, wann Erinnerungen an Anwender oder Gruppen oder beides gesendet werden sollen.

Formular „Korrekturzielregel“

Feld	Beschreibung
Name	Name für Ihre Regel.
Aktiv	Aktivieren oder deaktivieren Sie die Regel. Die Regel ist standardmäßig automatisch aktiviert (wahr) und wird auf Ihre Testergebnisse angewendet, wenn Sie Änderungen manuell oder nach der nächsten geplanten Aufgabe anwenden möchten.
Ziel (Tage)	Legen Sie das angestrebte Fristdatum für die Korrektur in Tagen fest. Der Standardwert für gezielte Korrekturtage ist 30. Wenn Sie beispielsweise eine neue Regel erstellen, die auch 30 für einen Zielwert hat, werden Ihre neue Regel und alle anderen vorhandenen Regeln, die ebenfalls 30 Tage oder länger als Zieldaten haben, auf Ihre Testergebnisse angewendet.
Ziel ab (Datum)	Datum, ab dem die Zieldaten berechnet werden. Sie können nur die Felder für Datum oder Datum und Uhrzeit angeben. Ab v14.12, Der Standardwert ist *Letzter Durchgang* . Wählen Sie eine der folgenden Optionen aus: ○ Zuletzt gesehen ○ Zuerst gesehen ○ Erstellt ○ Letzte Übergabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn der letzte Durchgang leer ist, wird das Erstellungsdatum für die Berechnung des Korrekturziels berücksichtigt. ○ Zuletzt Geöffnet Informationen zum Anpassen der Werte für dieses Feld finden Sie unter KB1642413 .
Benachrichtigen (Tage vor dem Fälligkeitsdatum)	Legen Sie eine Anzahl von Tagen vor dem Fristdatum fest, um Anwender und Gruppen zu erinnern.
Beschreibung	Kurzbeschreibung der Regel.
Bedingung	Verwenden Sie den Bedingungsgenerator, um die Testergebnisse anzugeben, für die diese Regel gilt. Legen Sie beispielsweise ein Korrekturzieldatum von 30 Tagen für alle Testergebnisse mit Risikopunktzahlen größer als 70 fest. Senden Sie Erinnerungen sieben Tage vor dem Korrekturdatum an Anwender oder Gruppen oder beide. Die Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird in diesem Datensatz oder Formular nicht unterstützt. Vor V 12.0 wird die Groß-/Kleinschreibung für den Suchtext unterstützt, den Sie im Bedingungsgenerator eingeben.
Anwender und Anwendergruppen oder beide	Wählen Sie Anwender oder Gruppen oder beide aus, um Benachrichtigungen über die bevorstehenden und überfälligen Zieldaten zu senden, die Sie festgelegt haben.

4. Klicken Sie auf **Absenden**. Alternativ können Sie auf klicken, um bearbeitete Regeln zu speichern **Aktualisieren** .

   Die Listenansicht wird mit Ihrer aktualisierten oder neuen Regel angezeigt. Regeln in der Liste werden sortiert und ab der Regel mit dem niedrigsten Korrekturzieldatum ausgeführt. Wenn Sie eine Regel deaktivieren oder löschen, ersetzt die nächste Regel in der Reihenfolge die inaktive oder gelöschte Regel.

5. Um Ihre neuen Änderungen jetzt anzuwenden, klicken Sie auf **Änderungen Anwenden** .

Konfigurations-Compliance Rechnergruppen

Konfigurations-Compliance Rechner werden verwendet, um Datensatzwerte zu aktualisieren, wenn vordefinierte Bedingungen erfüllt sind. Die Rechner werden basierend auf den Kriterien gruppiert, die verwendet werden, um zu bestimmen, wie die Datensätze aktualisiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Konfigurations-Compliance Rechnergruppen

Im Datensatz „Standard-Risikorechner“ können Rechnerregeln bei Bedarf auf alle betroffenen Testergebnisse und Sammlungen angewendet werden. Schwachstellenmanager können diese Funktion verwenden, um ihre Konfiguration des Risikorechners anzupassen. Möglicherweise experimentieren sie bereits zu Beginn ihrer Bereitstellung mit mehreren Priorisierungsschemata und wenden diese Änderungen bei Bedarf an, um anzuzeigen, wie sie sich auf Importergebnisse auswirken.

Die Gruppe des Risikopunktzahlrechners wurde in Risikorechner umbenannt.

Risikopunktzahl-Rollup-Rechner sind in enthalten Konfigurations-Compliance. Es gibt zwei Arten von einzelnen Rollup-Rechnern:

Konfigurationstest-Risiko-Rollup

Rechner, die Risikopunktzahlen für alle Testergebnisse mit demselben Konfigurationstest zusammenfassen, um eine Gesamtrisikopunktzahl für den Konfigurationstest bereitzustellen. Der Rollup-Wert wird in den Feldern „Risikopunktzahl“ angezeigt.

Rollup der Korrekturaufgaben-Risikobewertung

Diese Rechner fassen Risikopunktzahlen für alle Testergebnisse in einer Korrekturaufgabe zusammen, um eine Gesamtrisikopunktzahl für diese Korrekturaufgabe bereitzustellen. Der Rollup-Wert wird in den Feldern „Risikopunktzahl“ angezeigt.

Sowohl die Gruppe der Risikopunktzahlrechner als auch die Gruppe der Risikopunktzahl-Rollup-Rechner sind standardmäßig aktiviert.

Weitere Informationen finden Sie in den folgenden Schlüsselbegriffen für Konfigurations-Compliance Rechner:

Testergebnis

Ein Testergebnis ist das Ergebnis des Konfigurationstests für ein Konfigurationselement (Configuration Item, CI) und die zugehörige Technologie. Testergebnisse mit den status „Fehlgeschlagen“, „Fehler“ und „Unbekannt“ identifizieren Hardware, Software und Assets, die nicht Ihren Richtlinien entsprechen.

Nachbesserungsaufgabe

Testergebnisse werden zum Zeitpunkt des Datenimports basierend auf den vordefinierten Regeln für Korrekturaufgaben gruppiert. Diese Korrekturaufgaben ähneln den Schwachstellengruppen in Vulnerability Response. Korrekturaufgaben organisieren Testergebnisse für Massenanalysen in Gruppen und stellen eine Reihe von zu korrigierenden Elementen dar.

Risikopunktzahl in einem Testergebnis

Ein von Risikopunktzahlrechnern berechneter Wert, der auf dem Geschäftskontext eines Assets und dem Schweregrad des zugehörigen Tests

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

basiert. Dies ist der Durchschnitt der Geschäftsrelevanz des betroffenen Assets, wie in der CMDB definiert, und der vom Scanner kommunizierte Schweregrad des Tests.

Jedem Asset können mehrere Services zugeordnet sein. Die Geschäftsrelevanz eines Assets wird durch den Service mit der höchsten Relevanz bestimmt.

Der berechnete Wert wird in den Feldern „Risikopunktzahl“ der Testergebnisse angezeigt. Die Punktzahlen zeigen Werte im Bereich von 0 bis 100 an. Felder sind auch farbcodiert, um Ihnen den Schweregrad auf einen Blick anzuzeigen.

Risikopunktzahl in Korrekturaufgabe

Diese Punktzahl wird im Datensatz der Korrekturaufgabe angezeigt und ist der Rollup-Wert der Risikopunktzahlen für alle aktiven Testergebnisse in einer Korrekturaufgabe. Diese Punktzahl ändert sich, wenn Testergebnisse in der Korrekturaufgabe korrigiert werden.

Risikopunktzahl im Konfigurationstest

Diese Punktzahl wird in Konfigurationstests angezeigt und ist der Rollup-Wert der Risikopunktzahlen für alle aktiven Testergebnisse mit diesem Konfigurationstest. Diese Punktzahl ändert sich, wenn die Testergebnisse, die diesem Konfigurationstest zugeordnet sind, korrigiert werden.

Risikobewertung

Das Ausmaß des Risikos, das ein fehlgeschlagenes Testergebnis für Ihr System darstellt. Sie basiert auf einer Reihe von Risikopunktzahlen auf einer numerischen Skala von 1-5, die Risiken als kritisch (1) bis keine (5) bewertet. Die Punktzahl basiert auf einem Bereich von Risikopunktzahlen und wird in Risikobewertungsfeldern angezeigt.

Risikobewertungsbereiche

Risikobewertung	Risikopunktzahl
1 – Kritisch	90 bis 100
2: Hoch	70 bis 89
3: Mittel	40 bis 69
4: Niedrig	1 bis 39
5: Keine	0

Rollup-Rechner für Risikopunktzahl

Es gibt zwei Arten von Rollup-Rechnern:

- Konfigurationstestrisiko-Rollup: Diese Rechner führen Risikopunktzahlen für alle Testergebnisse mit demselben Konfigurationstest zusammen, um eine Gesamtrisikopunktzahl für den Konfigurationstest bereitzustellen. Der Rollup-Wert wird in den Feldern „Risikopunktzahl“ angezeigt. Sie können die Skriptwerte für Gewichtung und Punktzahl für diese Rechner bearbeiten.
- Rollup der Risikopunktzahl für Korrekturaufgaben: Diese Rechner führen Risikopunktzahlen für alle Testergebnisse in einer Korrekturaufgabe zusammen, um eine Gesamtrisikopunktzahl für diese Korrekturaufgabe bereitzustellen. Der Rollup-Wert wird in den Feldern „Risikopunktzahl“ angezeigt. Sie können die Skriptwerte für Gewichtung und Punktzahl für diese Rechner bearbeiten. Ein Beispiel für einen Rollup-Rechner für Risikopunktzahlen und wie er Punktzahlen berechnet, finden Sie unter Beispiel für die Berechnung des Risiko-Rollups für Konfigurations-Compliance(Vor v15.0).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Historische Risikopunktzahl

Die inhärente Risikopunktzahl für alle bestandenen Tests führt zu einer Korrekturaufgabe. Dieses Feld zeigt das Ausmaß des Risikos an, das von einer Testgruppe korrigiert wurde, und wird erst angezeigt, nachdem sich eine Testgruppe im Status „Geschlossen“ befindet und die Risikopunktzahl null ist.

Punktzahlen werden berechnet, wenn sich die Risikopunktzahl ändert oder wenn Testergebnisse einer Korrekturaufgabe hinzugefügt oder daraus entfernt werden.

Hinweis:
Um ordnungsgemäß zu funktionieren, erfordert dieses Skript Service-Mapping Plugin. Service-Mapping Ist als separates Abonnement verfügbar und erfordert die Aktivierung durch ServiceNow Personal.

Erstellen Sie einen Konfigurations-Compliance Rechnergruppe

Konfigurations-Compliance Rechnergruppen werden verwendet, um Rechner basierend auf ihrer Verwendung zu gruppieren.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird
Die Konfigurations-Compliance Das Basissystem enthält eine Rechnergruppe: **Risikopunktzahl** . Wenn Sie andere Rechner erstellen, können Sie sie dieser Gruppe hinzufügen oder andere Gruppen und Rechner erstellen. Innerhalb jeder Gruppe wird der erste Rechner ausgeführt, der dem Testergebnis entspricht.

Es gibt zwei Rechnergruppen, die in enthalten sind Konfigurations-Compliance Anwendung:

- Risikorechner
- Rollup-Rechner für Risikopunktzahl

Risikorechner berechnen die Risikopunktzahl und die Risikobewertung eines Testergebnisses.

Risikopunktzahl-Rollup-Rechner führen Risikopunktzahlen für alle Testergebnisse und Korrekturaufgaben mit demselben Konfigurationstest zusammen, um eine Gesamtrisikopunktzahl bereitzustellen.

Sie erstellen auch neue Rechner direkt aus diesen Gruppen.

Prozedur

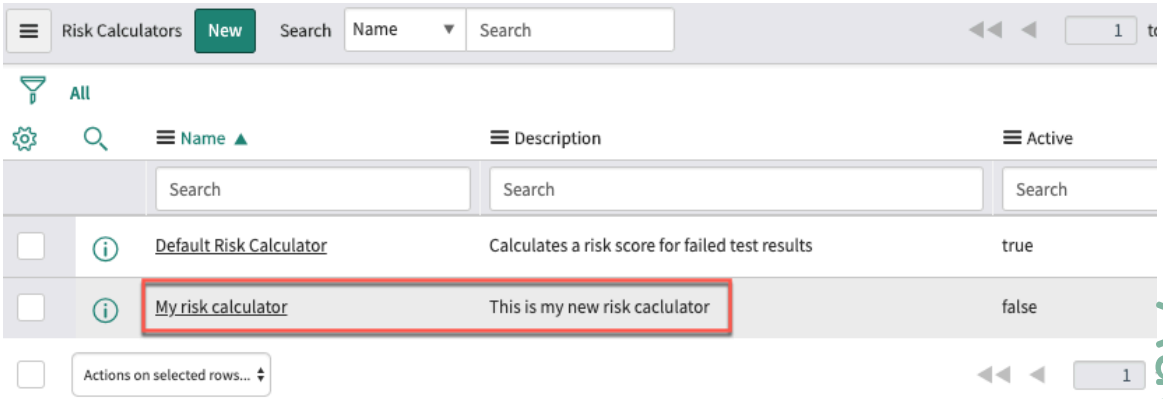
1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Rechnergruppen**an.
2. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** Und wählen Sie aus **Risikorechner** Oder **Risikopunktzahl-Rollup-Rechner** .
3. Klicken Sie auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name des Rechners.
Beschreibung	Eine Beschreibung dieser Rechnergruppe.
Aktiv	Aktivieren oder deaktivieren Sie die Rechnergruppe.

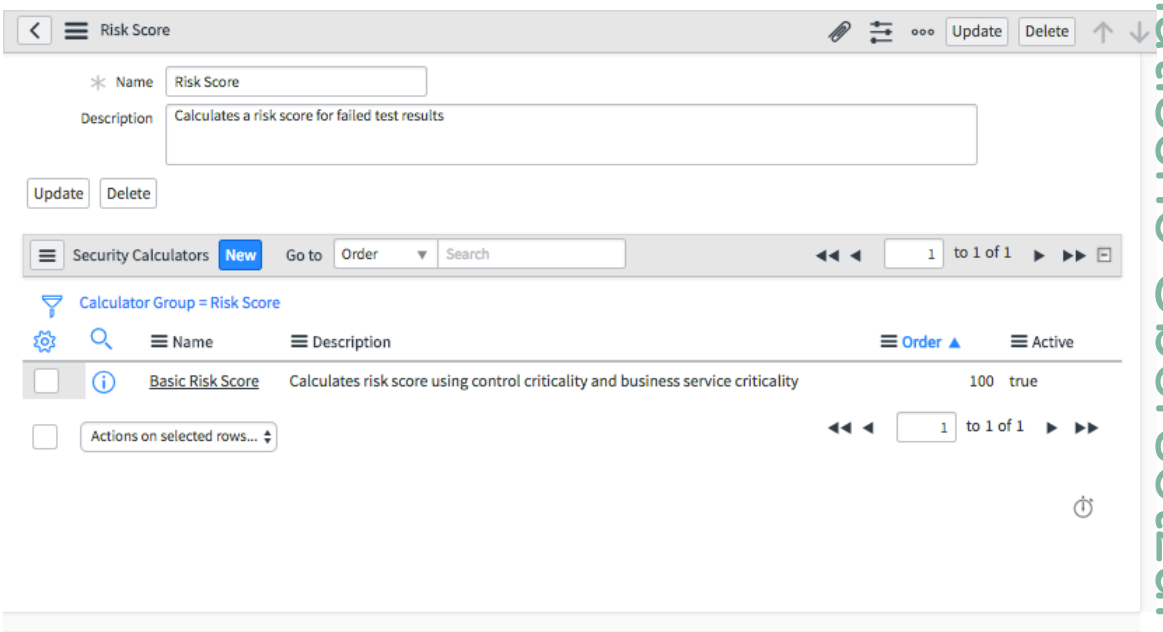
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Rechtsklick **Speichern** In der Formularüberschrift, oder klicken Sie auf **Übermitteln** .
   Die neue Rechnergruppe wird in der Gruppenliste mit den anderen Rechnern angezeigt. Klicken Sie auf den Namen der neuen Rechnergruppe, um den Datensatz zu öffnen. Siehe Erstellen, bearbeiten und wenden Sie Risikorechner für an Konfigurations-Compliance Weitere Informationen zum Festlegen von Bedingungen und angezeigten Werten und zum erneuten Anwenden von Rechnern.



Die **Sicherheitsrechner** Zugehörige Liste wird angezeigt.



6. Klicken Sie Auf **Neu** Um Rechner zusammen mit ihren Bedingungen zur Gruppe hinzuzufügen.

   Die Groß-/Kleinschreibung für den Suchtext, den Sie im Bedingungsgenerator eingeben, wird in diesem Datensatz oder Formular nicht unterstützt.

Konfigurations-Compliance Rechner und Rechnerregeln

Konfigurations-Compliance Automatisieren Sie die Berechnung der Anfangswerte für die Felder in Testergebnissen. Die Bedingung für jeden Rechner wird in der Reihenfolge ausgewertet, und der erste übereinstimmende Rechner wird verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance Rechner

Das Konfigurations-Compliance-Basissystem enthält einen Konfigurations-Compliance-Rechner (**Standardrisikorechner**), die die Basis festlegt **Risikopunktzahl** Im Testergebnis. Konfigurations-Compliance-Rechner können erstellt werden, um die Auswirkung von Testergebnissen basierend auf beliebigen Kriterien mithilfe von Bedingungsfiltern zu priorisieren und zu bewerten. Unabhängig davon, ob es sich um die Geschäftsauswirkung der Schwachstelle, die Klasse des Konfigurationselements (Configuration Item, CI) handelt, können Sie zusätzliche Konfigurations-Compliance-Rechner erstellen, um andere Felder in Testergebnissen festzulegen, oder Sie können die vorhandenen Konfigurations-Compliance-Rechner anpassen. Ein Rechner kann geschrieben werden, um einen beliebigen Satz von Prioritäten widerzuspiegeln.

Jeder Rechner enthält eine Liste von Rechnerregeln mit einer Bedingung, die bestimmt, wann sie angewendet werden sollen. Wenn der Rechner ausgeführt wird, wird die Bedingung für jede Rechnerregel in der Reihenfolge ausgewertet, und die erste übereinstimmende Rechnerregel wird verwendet.

Alle aktivierten Konfigurations-Compliance-Rechner legen die ausgewählten Felder jedes Mal fest, wenn ein Testergebnis erstellt wird, wenn sich ein zugehöriges CI oder ein Konfigurationstest ändert oder wenn sich ändert **Berechnen Sie Die Risikopunktzahl** Zugehöriger Link in einem Testergebnis wird verwendet. Beispielsweise wird die Risikopunktzahl in Testergebnisdatensätzen automatisch aktualisiert, wenn der Wert „Control.Relevality“ für ein importiertes Testergebnis aktualisiert wird. Nachdem ein Testergebnisimport eine Testergebnispunktzahl aktualisiert hat, können Sie die Risikopunktzahl der Testergebnisse neu berechnen, indem Sie auswählen **Rechner Erneut Anwenden** Schaltfläche.

Wenn Sie aus einem vorhandenen Testergebnis auswählen **Berechnen Sie Die Risikopunktzahl** Zugehöriger Link und einer der Rechner ist aktiviert. Das Feld „Risikopunktzahl“ im Testergebnis wird aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Die **Berechnen Sie Die Risikopunktzahl** Der zugehörige Link ist nur sichtbar, wenn mindestens ein Konfigurations-Compliance-Rechner aktiviert ist.
- Ab v22.0 von Vulnerability Response, Sie können die Risikopunktzahl für ein Testergebnis im Vulnerability Manager-Arbeitsbereich und IM IT-Korrekturarbeitsbereich aktualisieren, indem Sie auswählen **Berechnen Sie Die Risikopunktzahl** Schaltfläche in der Datensatzansicht.
- Ab Version 14,13 von Konfigurations-Compliance Wenn sich die Risikopunktzahl eines Testergebnisses ändert, werden die folgenden Details im Abschnitt „Notizen“ des Testergebnisses dokumentiert:
  - Rechnergruppenname
  - Rechnername: Je nachdem, ob die Rechnerregel auf einer Vorlage oder einem Skript basiert, wird der Name mit den Details in Klammern angehängt. Um die Basis der Rechnerregel zu ändern oder anzuzeigen, wählen Sie eine beliebige Regel aus, und wählen Sie aus **Erweiterte Ansicht** Kontrollkästchen. Von **Werttyp** Wählen Sie im Dropdown-Feld die erforderliche Option aus. Wenn **Vorlage** Ist ausgewählt, wird die Risikopunktzahl gemäß der in der Regel angegebenen Bedingung aktualisiert. Wenn **Skript** Ist ausgewählt, können Sie das vorhandene Skript entweder hinzufügen oder aktualisieren.
  - Feldwerte mit ihrer Gewichtung und ihrem Beitrag zur Risikopunktzahl
  - Endgültige Risikopunktzahl
  - Die Systemeigenschaft `sn_sec_cmn.risk_score_changes_add_worknotes`Hilft beim Ausfüllen des Abschnitts „Arbeitsnotizen“. Ab v15.2.1 von Konfigurations-Compliance, Die Systemeigenschaft `sn_sec_cmn.risk_score_changes_add_worknotes`Ist standardmäßig inaktiv. Wenn Sie sie aktivieren, können Sie nur im Abschnitt „Arbeitsnotizen“ alle Änderungen im Zusammenhang mit der Risikopunktzahl eines Testergebnisses anzeigen. Außerdem werden die Arbeitsnotizen nur aktualisiert, wenn sich die Risikopunktzahl ändert.

Konfigurations-Compliance Rechnerregeln

Standardmäßig ein Basissystem **Standardrisikorechner** Ist angegeben. Wenn Sie eine Risikoregel für diesen Rechner erstellen möchten, müssen Sie das Zielfeld von festlegen **Standardrisikorechner** Bis **Risikopunktzahl** . Wählen Sie aus **Neue Risikoregel** Schaltfläche zum Erstellen einer neuen Risikoregel . Dies Erstellt eine spezialisierte Regel für den Testergebnisrechner mit der Bezeichnung **Risikoregel** , Die wiederum Berechnet **Risikopunktzahl** Basiert auf mehreren Werten. Standardmäßig Die folgenden Werte für die Berechnung der Risikopunktzahl Werden berücksichtigt :

- Business-Relevanz
- Relevanz

Sie können die Werte anpassen, die in verwendet werden sollen **Standardrisikoregel** Und wie viel Gewichtung jeder dieser Werte gegeben werden soll. Gewichtungen werden verwendet, um anzupassen, wie viel jedes Element beim Festlegen der Basis zählt **Risikopunktzahl** .

Beginnend mit Konfigurations-Compliance Version 13.0. Sie können die Kriterien für die Standardrisikoregel anpassen. Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuweisen eines Gewichtungsprozentsatzes

Sie können den Gewichtungsprozentsatz (0–100) auch auf der Feldwertebene zuweisen. Sie können beispielsweise jeder Schweregradstufe einen Gewichtungsprozentsatz zuweisen (keine zu Kritisch). Wenn die Relevanzgewichtung für die Risikoregel 50 beträgt und die folgenden Gewichtungswerte für die Relevanzstufe zugewiesen werden:

Gewichtungsprozentsatz zuweisen

Relevanz	Risikopunktzahl
Kritisch	100
Hoch	50
Mittel	20
Keine	0

Wenn die Relevanz kritisch ist, beträgt die entsprechende Gewichtung 50. Wenn die Relevanz hoch ist, beträgt die Gewichtung 25, und wenn die Relevanz Mittel ist, beträgt die Gewichtung 10. Wenn die Relevanz keine ist, ist die entsprechende Gewichtung 0. Weitere Informationen finden Sie unter . Siehe Beispiel für die Berechnung der Risikopunktzahl für Konfigurations-Compliance.

Jede Regel hat einen **Reihenfolge** Wenn Sie jedoch die erste Einstellung festlegen, die den Bedingungen entspricht, wird aktualisiert **Risikopunktzahl** Feld im Testergebnis. Nicht geskriptete Rechnerregeln verursachen normalerweise weniger Auswirkungen auf die Leistung als geskriptete Rechnerregeln.

Das Basissystem Konfigurations-Compliance Der Rechner enthält Rechnerregeln, die jeder Kritikalitätsebene (keine bis Kritisch) einen Wert (0–100) für zuweisen **Risikopunktzahl** Basierend auf Schweregrad. Unbekannter Schweregrad wird automatisch eine Risikopunktzahl von 100 zugewiesen. Diese Werte können angepasst werden, z. B. Standardrisikorechner, neue Rechnerregeln oder neue Risikoregeln können erstellt werden.

Gewichtungen Der Schwachstellenrisikopunktzahl

Allen Schwachstellen wird eine Risikopunktzahl und eine Bewertung basierend auf Faktoren wie Schweregrad, Relevanz, Ausnutzungsinformationen usw. zugewiesen. Die Business-Regel *`Update Risk Rating from Risk Score`*ln der Tabelle „angreifbare Elemente“ ist für die Berechnung der Risikobewertung verantwortlich. Wenn sich die Risikopunktzahl ändert, wird die Risikobewertung berechnet und für die angreifbaren Elemente ausgefüllt. Vor Version 17,1 von Vulnerability Response(VR)-Anwendung wurden die folgenden Risikobewertungen als Teil der Skripteinbindung bereitgestellt SchwachstellenUtils , Die hartcodiert waren.

Wert (Risikobewertung)	Gewichtung (Risikopunktzahl)
1	90–100
2	70–89
3	40–69
4	1–39
5	0

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab Version 18,0 von Vulnerability Response,

- Die Risikobewertungstypen werden in der Basistabelle als cc_Risk_Rating geliefert. Diese Typen werden als Teil der Business-Regel in jeder Tabelle übergeben, in der die Risikobewertung berechnet wird.
- Das Skript wird geändert, sodass Sie die Einträge in den Tabellenwerten für Risikopunktzahlgewichtungen für die Berechnung der Risikobewertung abfragen können.
- Fügen Sie zusätzliche Einträge für einen vorhandenen Typ hinzu, oder erstellen Sie einen neuen Typ. Wenn Sie einen neuen Typ erstellen, stellen Sie sicher, dass Sie die Bezeichnungen für die neue Risikobewertung hinzufügen und auch die zugehörigen Skripts und Business-Regeln ändern. Sie müssen auch einen neuen Stil für die neue Risikopunktzahl hinzufügen.
- Ändern Sie das Skript, um die Datensätze in der Basistabelle abzufragen.

Sie können auf die Tabelle mit Risikopunktzahlgewichtungen zugreifen, indem Sie sn_sec_cmn_Risk_Score_weight im Filternavigator eingeben.

Darüber hinaus wird die Risikopunktzahl in den folgenden Szenarien automatisch neu berechnet:

- Wenn sich ein Konfigurationselement (Configuration Item, CI) von nicht mit Internetzugriff zu Internetzugriff ändert.
- Wenn die zugehörigen Common Vulnerabilities and Exposures (CVEs) oder Drittparteieinträge (TPEs) in den Schwachstellen-Elementen (VIS) mit einer bekannten CVE-Exploit-Schwachstelle (KEV) verknüpft sind.

Definieren Sie Felder und Gewichtungen für die Risikoregel

Passen Sie die Parameter und Gewichtungen für die Risikoregel an, damit Sie Risikopunktzahlen generieren können, die die Test- und Asset-Daten verwenden, die für Ihre Organisation eindeutig sind. Indem Sie die Felder auswählen, die in der Risikoregel enthalten sind, können Sie ein effektives Risikobewertungs-Framework definieren.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Risikorechner**an.
2. Klicken Sie Auf **Standardrisikorechner** .
3. Wählen Sie das Zielfeld als aus **Risikopunktzahl** .
   Die **Neue Risikoregel** Die Schaltfläche wird in der Tabelle „Rechnerregel“ angezeigt.
4. Klicken Sie auf **Neue Risikoregel** Schaltfläche zum Navigieren zu **Konfigurations-Compliance-Risikoregel** Formular.
5. Legen Sie im Abschnitt „Kriterien des Risikorechners“ die Gewichtung für jedes Kriterium entsprechend seiner Bedeutung bei der Berechnung der Gesamtrisikopunktzahl fest.
6. Löschen Sie **Aktiv** Kontrollkästchen zum Deaktivieren der Regel.
7. Klicken Sie Auf **Fügen Sie Kriterien Hinzu** Zum Hinzufügen von Risikoregelfeldern zu den Kriterien des Risikorechners.
8. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Risikoregelfeld“

Feld	Beschreibung
Referenztabelle auswählen	Die Tabelle, die Sie zum Definieren der Gewichtung der Risikopunktzahl verwenden. Wählen Sie unter den folgenden Optionen aus: ○ Testergebnis: Fügen Sie Felder hinzu, zu denen Sie direkt DOT-Walk aus dem Testergebnis (TR) aus durchführen können. ○ Testergebnis – Konfigurationselement: Fügen Sie Dot Walk-fähige Felder hinzu, die Teil der Basistabellenerweiterungen sind, z. B. die Hardwaretabelle. Diese Felder sind nicht Teil der Basis-Tabelle „cmdb_ci“. ○ Testergebnis – Test: Fügen Sie Dot-Walking-Felder hinzu, die Teil der Tabellen sind, die die Basistabelle erweitern, z. B. „Drittparteieintrag“. Diese Felder sind nicht Teil der Konfigurationstestbasistabelle. ○ Testergebnis-Referenztabelle: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) sind, oder Tabellen, die einen Verweis auf das Testergebnis haben. Diese Felder können nicht direkt aus dem Testergebnis aus durch Dot-Walking übernommen werden. ○ Konfigurationselement-Referenztabelle: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von cmdb_ci sind, oder Tabellen, die einen Verweis auf cmdb_ci haben. Diese Felder können nicht direkt vom TR aus DOT-Walking durchgeführt werden. ○ Testreferenztabelle: Fügen Sie Felder hinzu, die Teil der zugehörigen Tabellen (m2m) von sn_vulc_Test sind, oder Tabellen, die einen Verweis auf sn_vulc_Test haben. Diese Felder können nicht direkt vom TR aus DOT-Walking durchgeführt werden. ○ Anwenderdefinierte Bedingungen: Verwenden Sie diese Option, um der Regel Gewichtungen zuzuweisen, indem Sie die Bedingung auswerten. Beispielsweise bestimmt der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Filter mit Internetzugriff, ob ein Konfigurationselement (Configuration Item, CI) extern oder intern ist.
Feld	Das Feld, das für die Berechnung der Risikopunktzahl für diese Regel verwendet wird.
Gewichtung	Gewichtung dieses Felds innerhalb der Risikoregel. Der Wert muss eine Ganzzahl von 0 bis 100 sein.
Tabelle	○ Testergebnis > Konfigurationselement ○ Testergebnis > Test ○ Test-Ergebnisreferenztabelle ○ Referenztabelle für Konfigurationselemente ○ Test-Referenztabelle Dieses Feld wird nur angezeigt, wenn eine der aufgeführten Optionen im Feld Referenztabelle auswählen ausgewählt ist.
Aggregation	Wählen Sie den Mindest- oder Höchstwert aus, der für Berechnungen berücksichtigt werden soll, wenn das Feld aus den zugehörigen Tabellen (m2m) ausgewählt wird. Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle auswählen eine Referenztabelle ausgewählt ist.
Definieren Sie die Wertgewichtung	Komponente, um jedem Feldwert Gewichtungen zuzuweisen. Definieren Sie für numerische Felder Feldwerte als Bereich (z. B. 1–5). Der Wert muss eine Ganzzahl zwischen 0 und 100 sein. Dieses Feld wird nicht angezeigt, wenn die Option Anwenderdefinierte Bedingungen im Feld Referenztabelle auswählen ausgewählt ist.
Bedingungstabelle	Wählen Sie eine Bedingung aus der Liste aus. Dieses Feld wird nur angezeigt, wenn die Option Anwenderdefinierte Bedingungen im Feld Referenztabelle auswählen ausgewählt ist.
Feldname	Geben Sie einen Namen für die Risikokriterien ein. Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle auswählen anwenderdefinierte Bedingungen ausgewählt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bedingung	Zeigen Sie eine Vorschau der Elemente in dieser Tabelle an, die den definierten Bedingungen entsprechen. Dieses Feld wird nur angezeigt, wenn im Feld Referenztabelle auswählen anwenderdefinierte Bedingungen ausgewählt sind.

9. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Aktivieren Sie auf der Seite „Regel“ die Regel, und wenden Sie sie erneut an, um die Risikopunktzahl für das aktive Testergebnis neu zu bewerten.

Bearbeiten Sie Risiko-Rollup-Rechner für Konfigurations-Compliance

Bearbeiten Sie einen vorhandenen Risiko-Rollup-Rechner.

Vorbereitungen
Erforderliche Rolle: Erforderliche Rolle: sn_vulc.admin

Prozedur
1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** Und wählen Sie aus **Risikopunktzahl-Rollup-Rechner** .
2. Wenn die Liste der Rollup-Rechner für Risikopunktzahl angezeigt wird, klicken Sie auf einen Rechner, um den Datensatz zu öffnen und das Formular zu bearbeiten.

Feld	Beschreibung
Name	Der Name des Rollup-Rechners für Konfigurationstests oder Korrekturaufgaben.
Beschreibung	Eine Beschreibung für den Risiko-Rollup-Rechner.
Tabelle	Tabelle, auf die der Rollup-Rechner angewendet wird.
Zurückstellung einschließen	Enthält zurückgestellte Testergebnisse während des Rollups der Risikopunktzahl.

3. Definieren Sie die Gewichtungen auf eine der folgenden Arten:
   - Weisen Sie im Abschnitt „Rollup-Gewichtungen“ Gewichtungen für Folgendes zu:

Rollup-Gewichtungen

Feld	Beschreibung	Standardgewichtung
Maximale Risikopunktzahl	Maximale Risikopunktzahl der berücksichtigten Testergebnisse.	85
Durchschnittliche Risikopunktzahl	Zusammenfassung der Risikopunktzahlen aller berücksichtigten Testergebnisse.	0
Anzahl der Testergebnisse	Anzahl der Testergebnisse.	15

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wählen Sie aus **Erweiterte Ansicht** Kontrollkästchen und in der **Skriptwerte** Bearbeiten Sie die Werte im Skript nach Bedarf.

  Hinweis:
  Das Bearbeiten des Skripts erfordert fortgeschrittene Kenntnisse des ServiceNow AI Platform Und Konfigurations-Compliance Anwendung.

4. Klicken Sie Auf **Aktualisieren** Um Ihre Änderungen zu speichern.

Rollup-Rechner sind geplante Aufgaben, die stündlich ausgeführt werden, um Änderungen zu erfassen. Diese geplanten Aufgaben umfassen auch Gesamtrisikopunktzahlen für Konfigurationstests und Korrekturaufgaben. Die Rollup-Werte werden in den Feldern „Risikopunktzahl“ angezeigt.

Ein Beispiel dafür, wie ein Risiko-Rollup-Rechner Punktzahlen bestimmt, finden Sie unter Beispiel für die Berechnung des Risiko-Rollups für Konfigurations-Compliance(Vor v15.0).

Erstellen, bearbeiten und wenden Sie Risikorechner für an Konfigurations-Compliance

Rechnerregeln können bei Bedarf auf alle betroffenen Testergebnisse und Sammlungen angewendet werden. Schwachstellenmanager können diese Funktion verwenden, um ihre Konfiguration des Risikorechners anzupassen und Änderungen bei Bedarf anzuwenden, um Ergebnisse zu importieren.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Prozedur

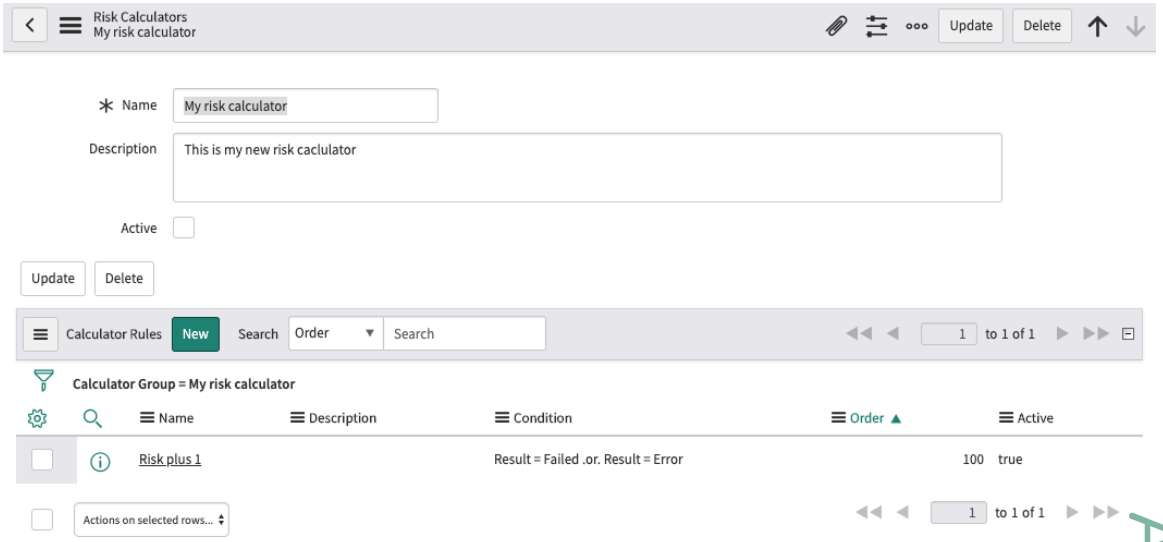
1. Führen Sie die folgenden Schritte aus, um einen neuen Risikorechner zu erstellen.

   a. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** Und wählen Sie aus **Risikorechner** .

   b. Klicken Sie in der Liste Risikorechner auf **Neu** .

   c. Geben Sie einen Namen und eine Beschreibung für Ihren neuen Rechner ein, und klicken Sie auf **Übermitteln** .
   Der neue Rechner wird in der Liste Risikorechner angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Klicken Sie in der Liste auf den neuen Rechner, um die Bedingungen zu erstellen, unter denen der Rechner ausgeführt wird, und geben Sie die Felder und Werte an, die in Testergebnisdatensätzen und Korrekturaufgaben angezeigt werden sollen.

e. Klicken Sie im angezeigten Datensatz auf **Neu** .

f. Füllen Sie die Felder auf den Registerkarten entsprechend aus.

Registerkarte	Beschreibung
Wenn diese Bedingung erfüllt ist	Verwenden Sie den Bedingungsgenerator, um die Bedingungen zu erstellen, unter denen der Rechner ausgeführt wird. Ein Beispiel ist: Ergebnis ist „Fehlgeschlagen“ oder Ergebnis ist „Fehler“ .
Diese Werte festlegen	Verwenden Sie die Vorlage, um die Felder und Werte auszuwählen, die angezeigt werden sollen.

g. Klicken Sie auf **Absenden**.
Der Datensatz wird mit den neuen Rechnerregeln und der Gruppe angezeigt, zu der er gehört.

2. Führen Sie die folgenden Schritte aus, um einen vorhandenen Rechner erneut auf Testergebnisse anzuwenden oder die Regeln und angezeigten Werte für einen vorhandenen Risikorechner zu bearbeiten.

a. Wählen Sie in den Listen Risikorechner oder Risiko-Rollup-Rechner den Rechner aus, den Sie bearbeiten möchten.

b. Um einen Risikorechner erneut auf Ihre vorhandenen Testergebnisdaten aus dem Datensatz anzuwenden, klicken Sie auf **Rechner Erneut Anwenden** .
Alle Testergebnisse, die die Bedingungen des Rechners erfüllen, werden aktualisiert.

Hinweis:
Abhängig von der Anzahl der Testergebnisse kann dieses Update einige Zeit dauern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Um die Bedingungen und Werte zu bearbeiten, klicken Sie unten links in der Spalte Name auf den Namen des Rechners.
Für Risikorechner der Datensatz und die **Wenn diese Bedingung erfüllt ist** Und **Legen Sie diese Werte fest** Registerkarten werden angezeigt.

d. Füllen Sie das Formular entsprechend aus.

Registerkarte	Feldbeschreibung
Wenn diese Bedingung erfüllt ist	Verwenden Sie den Generator für Filterbedingungen, um die Bedingungen zu erstellen, unter denen der Rechner ausgeführt werden soll.
Diese Werte festlegen	Wählen Sie eine, um fortzufahren. ▪ Werttyp: Vorlage. Wählen Sie Felder aus der Liste und die entsprechenden Werte aus. ▪ Skript: Geben Sie Ihre Änderungen mit dem Editor ein. **Hinweis:** Das Bearbeiten des Skripts erfordert fortgeschrittene Kenntnisse des ServiceNow AI Platform Und Konfigurations-Compliance Anwendung.

3. **Wahlweise:** Um die neuen Regeln bei Bedarf auf Ihre vorhandenen Testergebnisdaten anzuwenden, führen Sie die folgenden Schritte aus.

   a. Wenn die Liste Risikorechner angezeigt wird, klicken Sie auf einen Rechner, den Sie anwenden möchten. Der Datensatz wird angezeigt.

   b. Klicken Sie Auf **Rechner Erneut Anwenden** Um Ihre Änderungen bei Bedarf zu testen und auf Ihre Importergebnisse anzuwenden.

4. Zeigen Sie Ihre Änderungen an Testergebnissen an, und bearbeiten Sie Ihre Rechner nach Bedarf.

Beispiele für Konfigurations-Compliance Berechnung der Risikopunktzahl

Beginnend mit v13.0 von Konfigurations-Compliance, Sie können die Kriterien für die Standardrisikoregel anpassen. Verwenden Sie Risikopunktzahlen, die von Drittparteien wie Qualys und Tenable für die Berechnung der Risikopunktzahl bereitgestellt werden.

Drittpartei-Lieferanten wie Qualys und Tenable geben ihre eigenen Punktzahlen an. Diese Punktzahlen werden im Feld Relevanz in der Tabelle „sn_vulc_Test“ ausgefüllt. Verwenden Sie dieses Feld für Berechnungen der Risikopunktzahl. Um diese Punktzahl zur Berechnung der Risikopunktzahl zu verwenden, gehen Sie wie folgt vor:

Fügen Sie Quellenrelevanz als Kriterium für eine Risikoregel hinzu

Verwenden Sie Punktzahlen basierend auf der Relevanz, die von Drittparteien bereitgestellt wurde, um Risikopunktzahlen zu berechnen.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

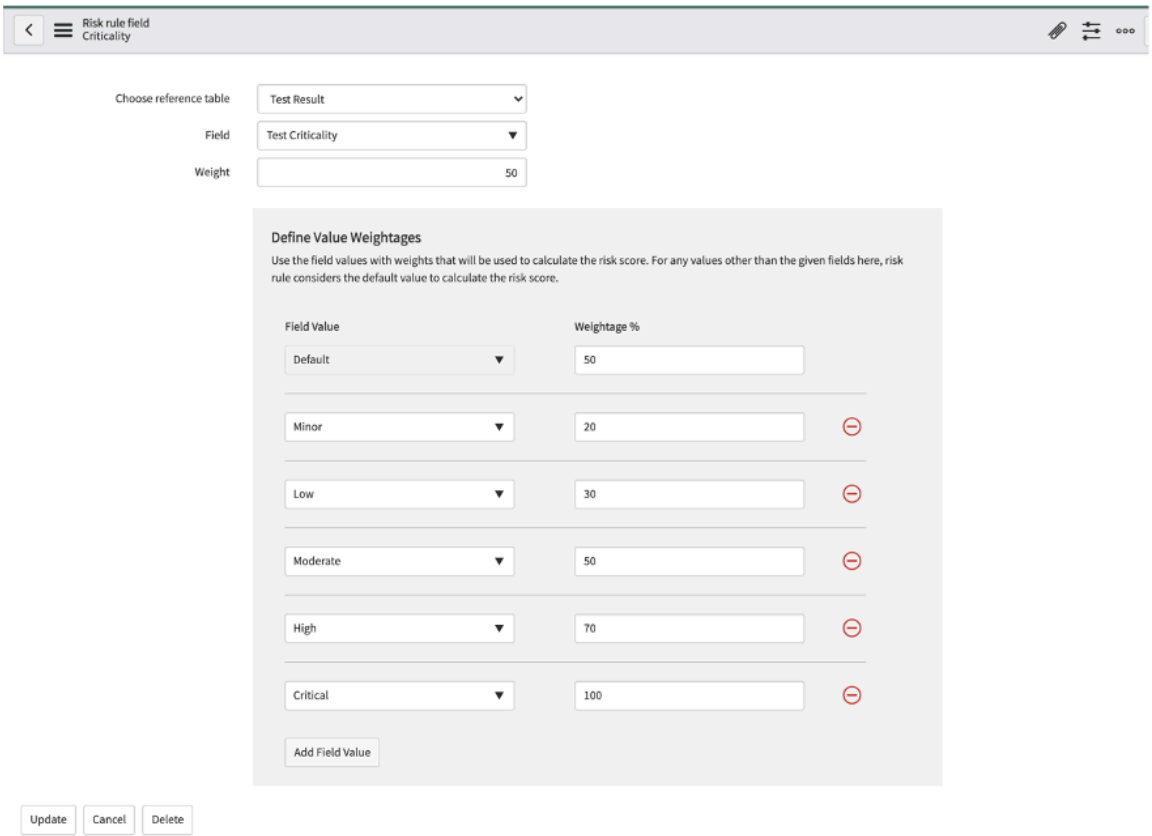
Warum und wann dieser Vorgang ausgeführt wird
Drittpartei-Lieferanten wie Qualys und Tenable stellen ihre eigenen Risikopunktzahlen bereit. Diese Punktzahlen werden im Feld Relevanz in der Tabelle „sn_vulc_Test“ ausgefüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie dieses Feld für Berechnungen der Risikopunktzahl und die Berechnung der Risikopunktzahl.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Risikorechner**an.
2. Navigieren Sie zum Formular „Risikoregel“.
3. Löschen Sie **Aktiv** Kontrollkästchen zum Deaktivieren der Regel.
4. Klicken Sie Auf **Fügen Sie Kriterien Hinzu** .
5. Von **Wählen Sie die Referenztabelle aus** Liste, wählen Sie aus **Testergebnis** .
6. Von **Feld** Liste, wählen Sie aus **Test.Relevanz** .
7. In **Gewichtung** Feld die relative Wichtigkeit dieses Felds angeben.
   Der Wert muss eine Ganzzahl von 0 bis 100 sein.
8. In **Definieren Sie Wertgewichtungen** Fügen Sie Feldwerte hinzu, und weisen Sie den Feldern einen Gewichtungsprozentsatz zu.



9. Klicken Sie auf **Absenden**.

Fügen Sie Geschäftsrelevanz als Kriterium für eine Risikoregel hinzu

Geben Sie einen Relevanzwert für Business-Services an, und verwenden Sie die Geschäftsrelevanz, um die Risikopunktzahlen zu berechnen.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Vorausgesetzt, Ihre Organisation verfügt über viele Business-Services, und ein Configuration Item (CI) wird von den folgenden Services verwendet:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Relevanz der Business-Services

Business-Service	Relevanz
Cloud-Management	1 – Sehr kritisch
E-Commerce	2 – Kritisch
Client-Services	3 – Weniger kritisch
Reise und Ausgaben	4 – Nicht kritisch

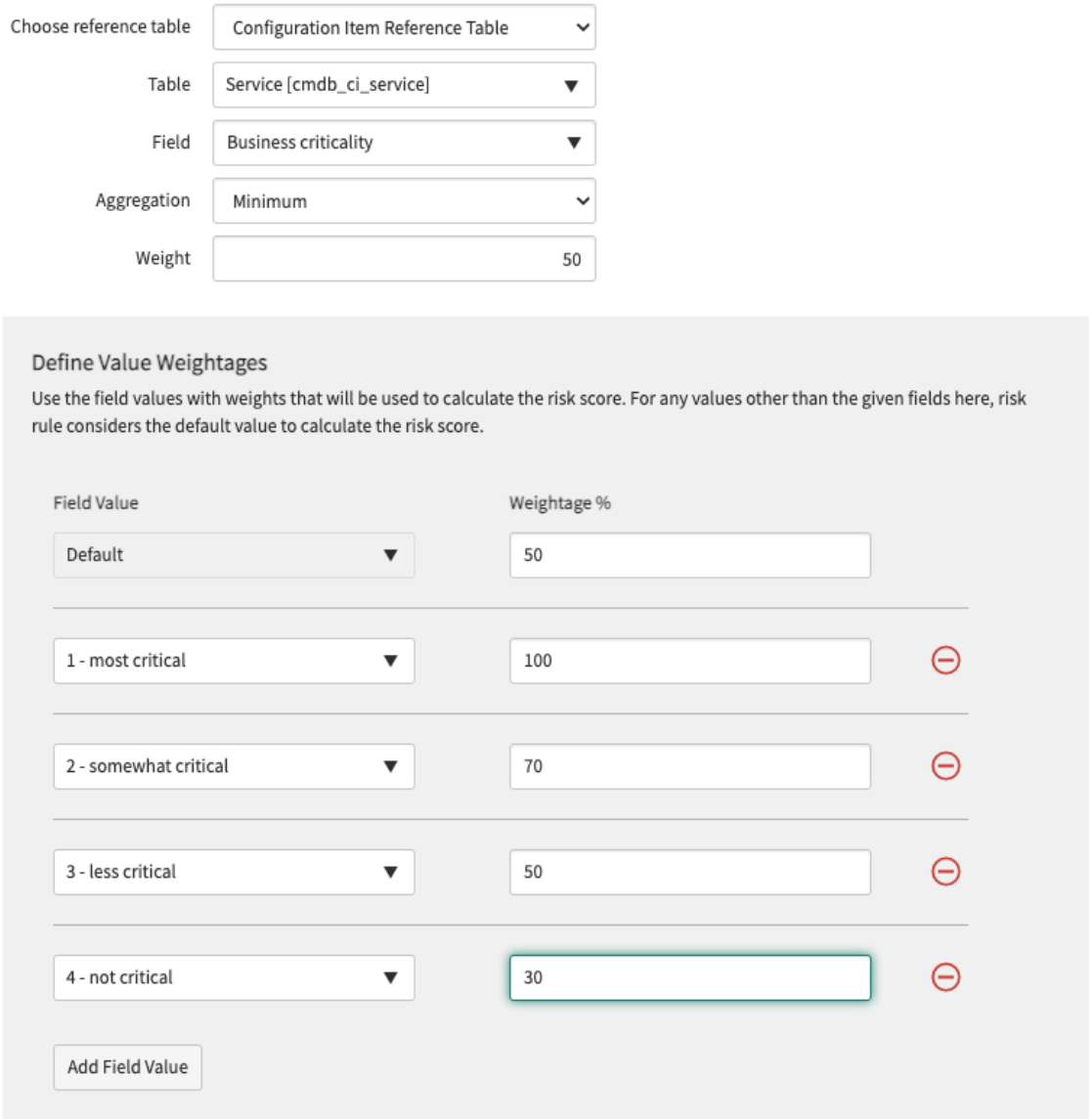
Die Zuordnung zwischen CI und Services wird in der Tabelle „Services“ [cmdb_ci_Services] gespeichert. Wenn ein CI keinen Konfigurationstest besteht, wird ein Testergebnis (TR) erstellt. Sie können den Wert der Geschäftsrelevanz aus den betroffenen Services verwenden, um die Risikopunktzahl für diese TR zu berechnen. Befolgen Sie das Verfahren, um den Relevanzwert dieser Services zur Berechnung der Risikopunktzahl zu verwenden.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Risikorechner**an.
2. Navigieren Sie vom zum Formular „Risikoregel“ **Rechnerregeln** Abschnitt.
3. Löschen Sie **Aktiv** Kontrollkästchen zum Deaktivieren der Regel.
4. Klicken Sie Auf **Fügen Sie Kriterien Hinzu** .
5. Von **Wählen Sie die Referenztabelle aus** Liste, wählen Sie aus **Konfigurationselement-Referenztabelle** .
6. Von **Tabelle** Liste, wählen Sie aus **Service [cmdb_ci_Service]** .
7. Von **Feld** Liste, wählen Sie aus **Geschäftsrelevanz** .
8. In **Zusammenfassung** Feld auswählen **Minimum** Um den kritischsten Service für diesen Anwendungsfall abzurufen (1 – kritischster Wert) oder **Maximum** Dient zum Abrufen des am wenigsten kritischen Service für diesen Anwendungsfall (4 – nicht kritischer Wert).
9. In **Gewichtung** Feld die relative Wichtigkeit dieses Felds angeben.
   Der Wert muss eine Ganzzahl von 0 bis 100 sein.
10. In **Definieren Sie Wertgewichtungen** Fügen Sie Feldwerte hinzu, und weisen Sie Gewichtungen zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwenderdefinierte Gewichtung der Geschäftsrelevanz-Risikoregel



Automatische Übersetzung

11. Klicken Sie auf **Absenden**.

Fügen Sie dem Risikorechner ein bedingtes Kriterium hinzu

Verwenden Sie anwenderdefinierte Bedingungen für die Risikoregel für die Berechnung der Risikopunktzahl.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Angenommen, Ihre Organisation verfügt über mehrere Konfigurationselemente (Configuration Items, CIs), von denen nur einige von einem externen Anwender aufgerufen werden können. Benutzer können Risikopunktzahlgewichtungen für diese nach außen gerichteten CIs hinzufügen.

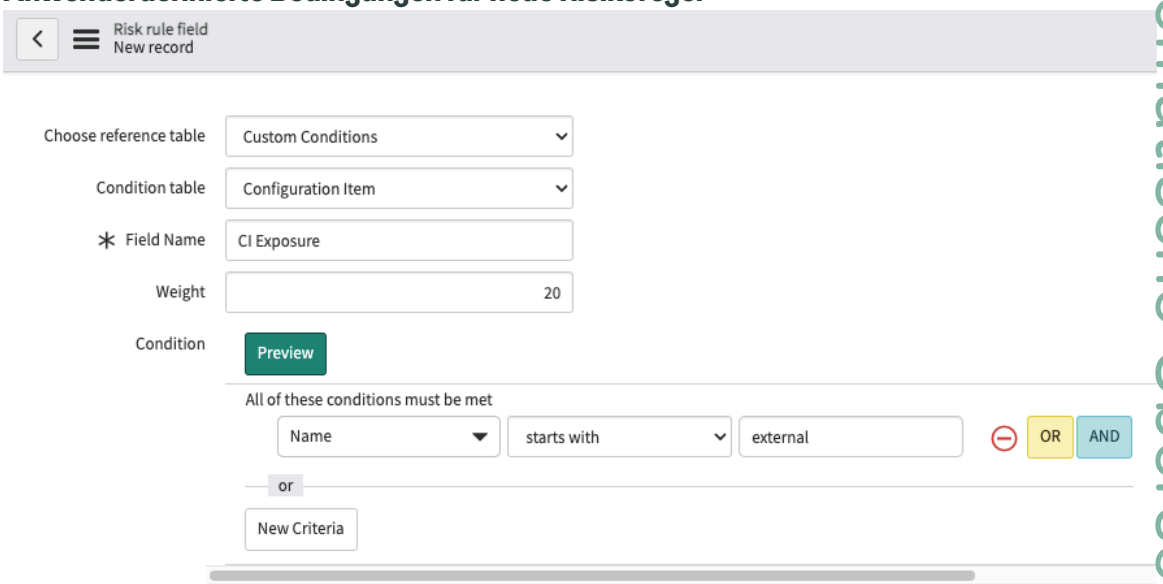
Hinweis:
Sie können diese CIs anhand ihres Namens identifizieren. Die Namen beginnen mit „extern“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Risikorechner**an.
2. Navigieren Sie zum Formular „Risikoregel“.
3. Löschen Sie **Aktiv** Kontrollkästchen zum Deaktivieren der Regel.
4. Klicken Sie Auf **Fügen Sie Kriterien Hinzu** .
5. Von **Wählen Sie die Referenztabelle aus** Liste, wählen Sie aus **Anwenderdefinierte Bedingungen** .
6. Von **Bedingungstabelle** Liste, wählen Sie aus **Konfigurationselement** .
7. In **Feldname** Feld eingeben `CI-Risiko` .
8. In **Gewichtung** Feld die relative Wichtigkeit dieses Felds angeben.
   Der Wert muss eine Ganzzahl von 0 bis 100 sein.
9. In **Bedingung** Feld auswählen **Name > beginnt mit** , Geben Sie den Wert als an `Extern` .

Anwenderdefinierte Bedingungen für neue Risikoregel



10. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Konfigurations-Compliance-Rechnergruppen

Beispiel zur Berechnung der Risikopunktzahl für Konfigurations-Compliance

Bestimmen Sie die Risikopunktzahlrechner, um Risikopunktzahlen zu generieren, die die für Ihre Organisation spezifischen Test- und Asset-Daten verwenden.

Beispiel für die Bestimmung der Punktzahlen von Risikoregelrechnern

Das folgende Beispiel zeigt, wie Punktzahlen für Risikoregelrechner bestimmt werden. Angenommen, ein Risikoregelrechner ist mit den Feldern in dieser Tabelle konfiguriert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bestimmen Sie die Punktzahlen des Risikoregelrechners

Feld	Gewichtung	Gewichtungsaufgliederung
Steuerung.Relevanz	50	Standard: 0 Minderjährig: 20 Niedrig: 30 Mittel: 50 Hoch: 70 Kritisch: 100
Business_Relevanz	50	Standard: 0 Minderjährig: 20 Niedrig: 30 Mittel: 50 Höhe: 70 Kritisch: 100

Davon ausgehen, dass die Testergebnisse, die in dieser Tabelle angezeigt werden, im System vorhanden sind.

Testergebniszuordnung

ID	Business-Relevanz	Steuerungsrelevanz
CTR0000001	1: Am Kritischsten	Kleiner
CTR0000002	1: Am Kritischsten	Niedrig
CTR0000003	2: Etwas Kritisch	Kleiner
CTR0000004	2: Etwas Kritisch	Mittel
CTR0000005	3 – Weniger Kritisch	Niedrig

Die Berechnung der Risikopunktzahl für das Testergebnis wird basierend auf der folgenden Formel berechnet:

Risikopunktzahl = (W(Control.Relevanz) * FV (Control.Relevanz). + W(Business_Relevality) * FV(Business_Relevality)) / 100, wobei W die Gewichtung und FV der Gewichtungsprozentsatz des Feldwerts ist.

Die resultierende Risikopunktzahl für diese Testergebnisse ist wie in dieser Tabelle beschrieben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risikopunktzahl basierend auf Testergebnissen

ID	Geschäftsrelevanz (50 %)	Steuerungsrelevanz (50 %)	Resultierende Risikopunktzahl
CTR0000001	1 – am kritischsten (50 % x100)	Gering (50 % x 20)	60
CTR0000002	1 – am kritischsten (50 % x100)	Niedrig (50 % x 30)	65
CTR0000003	2 – etwas kritisch (50 % x 70)	Gering (50 % x 30)	45
CTR0000004	2 – etwas kritisch (50 % x 70)	Mittel (50 % x 50)	60
CTR0000005	3 – weniger kritisch (50 % x 50)	Niedrig (50 % x 30)	40

Wenn der Gewichtungsprozentsatz für einen der Feldwerte geändert wird, finden Sie die Ergebnisse in dieser Tabelle:

Ergebnisse für geänderten Gewichtungsprozentsatz

Feld	Gewichtung	Gewichtungsaufgliederung
Steuerung.Relevanz	50	Standard: 0 Minderjährig: 20 Niedrig: 30 Mittel: 60 Höhe: 70 Kritisch: 100
Business_Relevanz	50	Standard: 50 1 – Äußerst Kritisch: 100 2 – Etwas Kritisch: 70 3 – Weniger Kritisch: 20 4 – Nicht Kritisch: 30

Die Risikopunktzahl für die Testergebnisse nach erneuter Anwendung des Rechners wird in dieser Tabelle angezeigt:

Risikopunktzahl für TR bei erneuter Anwendung des Rechners

ID	Geschäftsrelevanz (50 %)	Steuerungsrelevanz (50 %)	Resultierende Risikopunktzahl
CTR0000001	1 – am kritischsten (50 % x100)	Gering (50 % x 20)	60

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risikopunktzahl für TR bei erneuter Anwendung des Rechners (Fortsetzung)

ID	Geschäftsrelevanz (50 %)	Steuerungsrelevanz (50 %)	Resultierende Risikopunktzahl
CTR0000002	1 – am kritischsten (50 % x100)	Niedrig (50 % x 30)	65
CTR0000003	2 – etwas kritisch (50 % x 70)	Gering (50 % x 30)	45
CTR0000004	2 – etwas kritisch (50 % x 70)	Mittel (50 % x 60) *Überarbeiteter Wert	65 *Überarbeiteter Wert
CTR0000005	3 – weniger kritisch (50 % x 20) *Überarbeiteter Wert	Niedrig (50 % x 30)	25 *Überarbeiteter Wert

Beispiel für die Berechnung des Risiko-Rollups für Konfigurations-Compliance(Vor v15.0)

Das folgende Beispiel zeigt, wie Punktzahlen für Risiko-Rollup-Rechner bestimmt werden.

Für den folgenden Korrekturaufgaben-Rollup-Rechner lautet die Formel für die Berechnung der Risikopunktzahl der Korrekturaufgabe:

(Maximale Risikopunktzahl/100) * 85 + (Faktor * 15).

Der Faktor in der vorherigen Gleichung wird durch die Anzahl der Testergebnisse bestimmt, wie in der folgenden Tabelle gezeigt.

Anzahl Testergebnisse	Faktor
< 10	0,2
10-99	0,4
100-1000	0,6
1001-9999	0,8
>10000	1

Für die folgende Korrekturaufgabe TRG0003066 mit drei Testergebnisrisikopunktzahlen beträgt die maximale Punktzahl 90.

Anzahl	Risikopunktzahl	Nachbesserungsaul	Ergebnis	Status
CTR000123	90.0	TRG0003066	Fehlgeschlagen	Öffnen
CTR000124	70	TRG0003066	Fehlgeschlagen	Öffnen
CTR000125	40	TRG0003066	Fehlgeschlagen	Öffnen

Für die Korrekturaufgabe TRG0003066:

Die Risikopunktzahl beträgt 79, (90/100) * 85 + 0,2 * 15 = Math.Floor (76,5 +3) =79.

Die historische Risikopunktzahl ist null, da die Korrekturaufgabe noch „Offen“ ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der Datenerfassung werden die Testergebnisse „bestanden“, und die Korrekturaufgabe wechselt wie in der folgenden Tabelle gezeigt zu „Geschlossen“.

Anzahl	Risikopunktzahl (vor v15.0)	Nachbesserungsaul	Ergebnis	Status
CTR000123	0	TRG0003066	Bestanden	Geschlossen
CTR000124	0	TRG0003066	Bestanden	Geschlossen
CTR000125	0	TRG0003066	Bestanden	Geschlossen

Der Testergebnisverlauf wird in der folgenden Tabelle angezeigt.

Anzahl	Risikopunktzahl	Neuestes Ergebnis	Ergebnis
CTRH000111	90.0	CTR000123	Fehlgeschlagen
CTRH000112	70	CTR000124	Fehlgeschlagen
CTRH000113	40	CTR000125	Fehlgeschlagen

Die Risikopunktzahl ist null, da die Korrekturaufgabe keine aktiven Testergebnisse enthält.

Für die Korrekturaufgabe TRG0003066:

Die historische Risikopunktzahl beträgt 79: (90/100) * 85 + 0,2 * 15 = Math.Floor (76,5 +3) =79.

Beispiel für die Berechnung des Risiko-Rollups für Konfigurations-Compliance(V15.0 und höher)

Das folgende Beispiel zeigt, wie Punktzahlen für Risiko-Rollup-Rechner bestimmt werden.

Für den folgenden Korrekturaufgaben-Rollup-Rechner lautet die Formel für die Berechnung der Risikopunktzahl der Korrekturaufgabe:

(Maximale Risikopunktzahl* 80/100) + (durchschnittliche Risikopunktzahl* 5/100) + (Faktor * 15)

Wobei die Gewichtungen wie folgt lauten:

- Maximale Risikopunktzahl: 80
- Durchschnittliche Risikopunktzahl: 5
- Faktor: 15

Die Standardgewichtung der durchschnittlichen Risikopunktzahl ist 0. Weitere Informationen zum Festlegen der Gewichtungen finden Sie unter Bearbeiten Sie Risiko-Rollup-Rechner für Konfigurations-Compliance.

Der Faktor in der vorherigen Gleichung wird durch die Anzahl der Testergebnisse bestimmt, wie in der folgenden Tabelle gezeigt.

Anzahl Testergebnisse	Faktor
< 10	0,2
10-99	0,4

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzahl Testergebnisse	Faktor
100-1000	0,6
1001-9999	0,8
>10000	1

Für die folgende Korrekturaufgabe TRG0003066 mit drei Testergebnisrisikopunktzahlen beträgt die maximale Risikopunktzahl 90 und die durchschnittliche Risikopunktzahl 66.67.

Anzahl	Risikopunktzahl	Nachbesserungsaul	Ergebnis	Status
CTR000123	90.0	TRG0003066	Fehlgeschlagen	Öffnen
CTR000124	70	TRG0003066	Fehlgeschlagen	Öffnen
CTR000125	40	TRG0003066	Fehlgeschlagen	Öffnen

Für die Korrekturaufgabe TRG0003066:

Die Risikopunktzahl ist 81, (90* 80/100) + (66,67* 5/100) + (0,2 * 15) = Math.Floor (78,3 +3) = 81.

Die historische Risikopunktzahl ist null, da die Korrekturaufgabe noch „Offen“ ist.

Nach der Datenerfassung werden die Testergebnisse „bestanden“, und die Korrekturaufgabe wechselt wie in der folgenden Tabelle gezeigt zu „Geschlossen“. Ab v15.0 von Konfigurations-Compliance, Die Risikopunktzahl eines bestandenen Testergebnisses wird ausgefüllt, um das verringerte Risiko zu bestimmen.

Anzahl	Risikopunktzahl	Nachbesserungsaul	Ergebnis	Status
CTR000123	90.0	TRG0003066	Bestanden	Geschlossen
CTR000124	70	TRG0003066	Bestanden	Geschlossen
CTR000125	40	TRG0003066	Bestanden	Geschlossen

Der Testergebnisverlauf wird in der folgenden Tabelle angezeigt.

Anzahl	Risikopunktzahl	Neuestes Ergebnis	Ergebnis
CTRH000111	90.0	CTR000123	Fehlgeschlagen
CTRH000112	70	CTR000124	Fehlgeschlagen
CTRH000113	40	CTR000125	Fehlgeschlagen

Die Risikopunktzahl der Korrekturaufgabe ist null, da die Korrekturaufgabe keine aktiven Testergebnisse enthält.

Für die Korrekturaufgabe TRG0003066:

Die historische Risikopunktzahl beträgt 81: (90* 80/100) + (66.67* 5/100) + (0,2 * 15) = Math.Floor (78,3 +3) = 81.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen oder bearbeiten Konfigurations-Compliance Regeln für Korrekturaufgaben

Sie können Regeln erstellen, um Testergebnisse automatisch basierend auf Filterbedingungen zu gruppieren. Diese Regeln gruppieren Testergebnisse automatisch, wenn sie importiert werden. Verwenden Sie den Filter, um die nach dieser Regel gruppierten Testergebnisse einzugrenzen, z. B. alle Testergebnisse mit Exploits auszuwählen.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Das Basissystem wird mit einer Korrekturaufgabenregel geliefert. **Zuweisungsgruppe, Test** , Welche Testergebnisse nach Zuweisungsgruppe gruppiert (vorab ausgefüllt aus **Zuweisungsregeln**) Und das Testergebnis **Testen** Feld. Diese Regel kann mithilfe von Filterbedingungen und Gruppenschlüsseln geändert werden. Gruppenschlüssel sind Spalten in der Testergebnistabelle. Wählen Sie bis zu sechs Schlüssel aus, um anzugeben, welche Werte zum Gruppieren der Testergebnisse verwendet werden sollen.

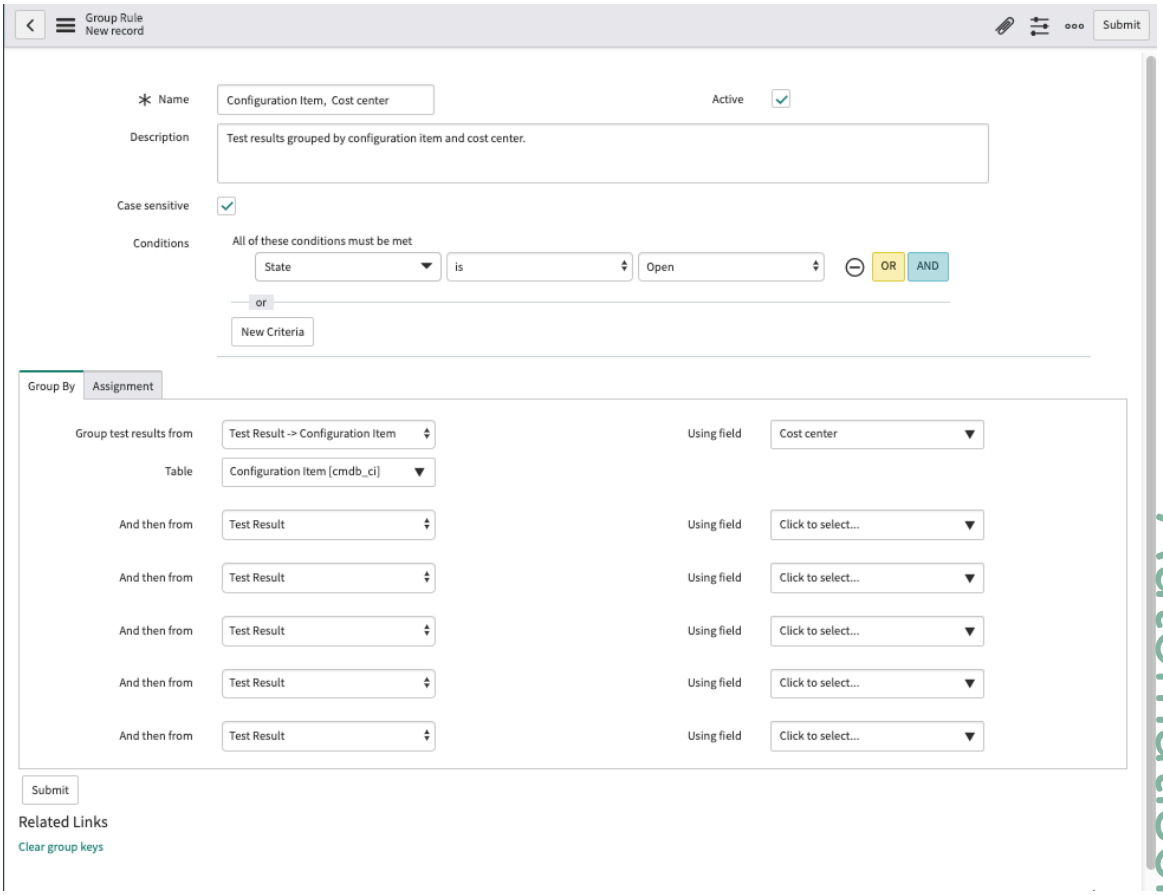
Ab Version 14,7 von Konfigurations-Compliance, **Zuweisungsgruppe, Test** Die Regel für Korrekturaufgaben ist für neue Implementierungen deaktiviert.

Hinweis:
Neue oder aktualisierte Regeln werden beim nächsten Import automatisch oder manuell mithilfe von ausgewertet **Erneut Anwenden** Schaltfläche im Formular „Regel für Korrekturaufgaben“.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Regeln für Korrekturaufgaben**an.
2. Öffnen Sie **Zuweisungsgruppe, Test** Regel oder klicken Sie auf **Neu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wenn **Neu** Füllen Sie die Felder im Formular entsprechend aus.

Konfigurations-Compliance Regel Für Korrekturaufgaben

Feld	Beschreibung
Name	Name der Korrekturaufgabenregel.
Aktiv	Gibt an, ob die Regel für Korrekturaufgaben aktiv ist.
Beschreibung	Textbeschreibung dieser Korrekturaufgabenregel.
Groß-/ Kleinschreibung beachten	Bestimmt, ob bei der Regelübereinstimmung die Groß-/Kleinschreibung beachtet wird oder nicht. **Hinweis:** Beim Standardwert wird die Groß-/Kleinschreibung nicht berücksichtigt.
Bedingungen	Bedingungen, die erfüllt werden müssen. Standardmäßig (**Groß-/Kleinschreibung beachten** Kontrollkästchen deaktiviert) wird bei dem Suchtext, den Sie im Bedingungsgenerator für Datensätze und Formulare für Korrekturaufgaben-Regeln eingeben, die Groß-/Kleinschreibung nicht beachtet. Sie haben die Möglichkeit, Suchvorgänge mit Groß-/Kleinschreibung in Gruppendatensätzen und -Formularen zu aktivieren.
Gruppieren nach	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Testergebnisse gruppieren von	Automatisieren Sie die Erstellung von Gruppen basierend auf dieser Regel. Wählen Sie eine der verfügbaren Optionen aus. ○ Testergebnis | mit Feld ○ Testergebnis->Konfigurationselement | Tabelle | mit Feld Wenn erweitert **Tabelle** Feld ist ausgewählt. Testergebnisse, die nicht die entsprechende erweiterte Tabelle verwenden, werden in einer separaten Korrekturaufgabe gruppiert.
Zuweisung	
Weisen Sie Testergebnisgruppen nach zu	Automatisieren Sie die Zuweisung von Gruppen, die basierend auf dieser Regel erstellt wurden. Wählen Sie eine der verfügbaren Optionen aus. ○ Gruppen-Key Wenn diese Option ausgewählt ist, wird ein Schlüsselwertfeld angezeigt. Verfügbare Felder werden in einem Dropdown-Menü aufgelistet. ○ Anwendergruppe Wenn diese Option ausgewählt ist, wird ein Suchfeld für Anwendergruppen angezeigt.

4. Klicken Sie auf **Absenden**.

Hinweis:
Das Löschen Der Gruppierung Nach Schlüsseln Der zugehörige Link entfernt die Gruppenschlüssel aus der Registerkarte Gruppieren nach im Formular.

Geben Sie die Dauer einer für eine Korrekturaufgabe angeforderten Ausnahme an

Verwenden Sie Systemeigenschaften, um die Dauer zu begrenzen, für die eine Ausnahme für eine Korrekturaufgabe angefordert wird. Die Korrektur der Korrekturaufgabe wird für den angegebenen Zeitraum zurückgestellt.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird
Die sn_vulc.Exception_max_Request_days Die Eigenschaft wird verwendet, um die maximale Anzahl von Tagen anzugeben, für die eine Ausnahme für eine Korrekturaufgabe angefordert werden kann. Der Standardwert ist 365 Tage.

Hinweis:
Sie können verwenden sn_vulc.Exception_Approval_required Eigenschaft zum Deaktivieren des Workflows für die Ausnahmegenehmigung für die Korrekturaufgabe, wenn dies nicht erforderlich ist. Standardmäßig ist diese Eigenschaft aktiviert, und ihr Wert ist Wahr .

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen Sie auf der Seite „Systemeigenschaften“ nach sn_vulc.Exception_max_Request_days .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf den Eigenschaftsnamen, um den Systemeigenschaftsdatensatz zu öffnen.
4. Um diesen Datensatz bearbeiten zu können, stellen Sie sicher, dass Konfigurations-Compliance Ist als aktuelle Anwendung ausgewählt.
5. Geben Sie einen positiven Wert ein **Wert** Und klicken Sie auf **Aktualisieren** .
   Der Datensatz wird aktualisiert und gespeichert.

Konfigurieren Sie das Ausnahmemanagement für Konfigurations-Compliance

Begrenzen Sie die Dauer einer angeforderten Ausnahme Und fügen Sie der Ausnahme einen Fragebogen hinzu Mit Konfigurations-Compliance Modul. Standardmäßig wird mit eine Ausnahme angefordert ServiceNow® Vulnerability Response Modul. Sie können auch eine Ausnahme mit anfordern GRC: Richtlinien- und Compliance-Management Integration.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Vulnerability Response Ist aktiviert, können Sie die Dauer begrenzen, für die eine Ausnahme angefordert werden kann. Ähnlich, wenn GRC: Richtlinien- und Compliance-Management Modul ist installiert. Sie können auswählen GRC: Richtlinien- und Compliance-Management Auf dem Konfigurationsbildschirm. Durch Aktivieren dieser Option können Sie eine Ausnahme anfordern, die das Richtlinien- und Kontrollziel von angibt GRC.

Wenn Sie einen Fragebogen hinzufügen, wird er an die Person gesendet, die die Ausnahme oder die falsch positive Anforderung stellt. Sie können entweder den Standardfragebogen verwenden oder einen basierend auf Ihren Anforderungen erstellen.

Für den Ausnahmegenehmiger ist es nützlich, den Grund für die Anforderung der Ausnahme zu verstehen.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Ausnahmenverwaltung**an.
2. Wählen Sie im Formular „Konfiguration des Ausnahmemanagements“ aus, wie Sie eine Ausnahme verwalten möchten, indem Sie eine Option aus der Liste Ausnahmen verwalten mit auswählen.
   - Vulnerability Response

     Hinweis:
     Ab 22,0 von Vulnerability Response, Sie können einen Fragebogen für falsch positive Anforderungen für einrichten Vulnerability Response Option auch.

   - GRC: Richtlinien- und Compliance-Management

     Hinweis:
     Sie müssen aktivieren GRC Zu verwendendes Plugin GRC: Richtlinien- und Compliance-Management Zum anfordern einer Ausnahme.

   Hinweis:
   Das Ändern der Konfiguration wirkt sich nicht auf die vorhandenen Daten aus.
3. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstellungen für das Formular „CC-Ausnahmeverwaltung“

Feld	Beschreibung
Dauer	Zeitraum, für den eine Ausnahme angefordert werden kann.
Einheit	Zeiteinheit für den angegebenen Zeitraum.
Fragebogen aktivieren, um Ausnahme anzufordern	Option zum Hinzufügen eines Fragebogens zur ausgelösten Ausnahmeanforderung.
Fragebogen, um Ausnahme anzufordern	Option zum Anzeigen des Fragebogens, den Sie zum anfordern einer Ausnahme ausgewählt haben. Standardmäßig wird der Ausnahmefragebogen angezeigt.
Fragebogen aktivieren, um falsch positive Meldung zu markieren	Option zum Hinzufügen eines Fragebogens zur falsch positiven Anforderung, die ausgelöst wird.
Fragebogen, um falsch positive Meldung zu markieren	Option zum Anzeigen des von Ihnen ausgewählten Fragebogens als falsch positiv zu markieren. Der Fragebogen für eine falsch positive Anforderung wird standardmäßig angezeigt.

4. Wählen Sie **Speichern**.

Fügen Sie einen Ausnahmegenehmiger für hinzu Konfigurations-Compliance

Fügen Sie den Genehmigergruppen Anwender hinzu, damit Sie in eine Ausnahme für eine Korrekturaufgabe anfordern können Konfigurations-Compliance.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Eine Ausnahmeanforderung für eine Korrekturaufgabe wird mit dem standardmäßigen zweistufigen Genehmigungs-Workflow genehmigt. Das Hinzufügen von Anwendern zur Gruppe der ersten Ebene ist obligatorisch. Wenn auf der zweiten Ebene keine Anwender vorhanden sind, wird die Anforderung nach der Genehmigung auf der ersten Ebene automatisch genehmigt.

Hinweis:
Wenn kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden.

Hinweis:
Bis Zu Konfigurations-Compliance V13.0: Wenn kein Genehmiger der ersten Ebene vorhanden ist, kann keine Ausnahme angefordert werden. Jedoch ab Konfigurations-Compliance V13.0: Wenn Sie die CC-Anwendung zum ersten Mal bereitstellen, ist der Flow Designer für das Ausnahmemanagement standardmäßig aktiviert. Wenn Sie den Workflow bereits verwenden, können Sie auf den Flow Designer aktualisieren. In beiden Fällen können Sie sie nicht zurück in Workflow ändern.

Prozedur

1. Navigieren zu **Alle** > **Systemsicherheit** > **Anwender und Gruppen** > **Gruppen**an.
2. Suchen Sie in der Spalte Name nach **Ausnahme** , Und klicken Sie auf **Ausnahmegenehmiger – Ebene 1 CC** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Beginnt ab Konfigurations-Compliance V14.7.5. Sie können die im Basissystem bereitgestellten Systemeigenschaften für Ausnahmegenehmigungen über den Workflow in der Tabelle „Systemeigenschaften“ [sys_properties] verwenden. Wenn also eine Ausnahmeanforderung über einen Workflow ausgelöst wird, wird sie zur Genehmigung an die in der Systemeigenschaft definierten Gruppen-IDs gesendet. Navigieren zu **Alle** > **Systemeigenschaften** Und wählen Sie aus `sn_vulc.exception_approver_L1_CC`Oder `sn_vulc.exception_approver_L2_CC`Zum Ändern des Eigenschaftswerts.

3. Navigieren Sie im Formular Gruppenausnahmegenehmiger – Ebene 1 CC zu **Gruppenmitglieder** > **Neu** (Oder **Bearbeiten**).
4. Füllen Sie im Formular die Felder aus.

Anwenderformular

Feld	Beschreibung
Anwender-ID	Eindeutiger Bezeichner für den Benutzer
Vorname	Vorname des Anwenders.
Nachname	Nachname des Anwenders.
Titel	Berufsbezeichnung des Benutzers Geben Sie einen Titel oder eine Stellenbeschreibung ein, oder wählen Sie eine aus der Liste aus.
Abteilung	Abteilung des Anwenders.
Passwort	Passwort, das dem Anwender zugewiesen ist. Dieses Passwort kann dauerhaft oder temporär sein.
Passwort muss zurückgesetzt werden	Option, mit der der Anwender das Passwort zurücksetzen können, um die Sicherheit zu gewährleisten.
Gesperrt	Option zum Sperren des Anwenders aus der Instanz und zum Beenden aller aktiven Sitzungen des Anwenders. Das System verhindert, dass Anwender mit der Administratorrolle sich selbst sperren.
Aktiv	Option zum Aktivieren dieses Anwenders. Nur inaktive Anwender können in diesen Bereichen angezeigt werden: ○ Listen von Anwendern ○ Auswahlliste in Referenzfeldern (Lupensymbol) ○ Liste mit automatischer Vervollständigung, die angezeigt wird, wenn Sie in ein Referenzfeld eingeben
Nur Webservice-Zugang	Option, um diesen Anwender als nicht interaktiven Anwender zu bestimmen.
Interner Integrationsanwender	Option, um diesen Anwender als internen Integrationsanwender zu bestimmen.
E-Mail	E-Mail-Adresse des Anwenders.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sprache	Bevorzugte Sprache des Anwenders.
Kalenderintegration	Kalender, der zum Verwalten des Arbeitszeitplans verwendet wird. Beispiel: Outlook.
Zeitzone	Zeitzone für den Standort dieses Anwenders.
Datumsformat	Bevorzugtes Format des Anwenders für Daten.
Telefon (geschäftlich)	Geschäftliche Telefonnummer des Anwenders.
Mobiltelefon	Mobiltelefon des Anwenders.
Foto	Foto, das Sie hochladen können, indem Sie auf klicken **Zum Hinzufügen klicken...** .

5. Klicken Sie auf **Absenden**.
6. **Wahlweise:** Wiederholen Sie die Schritte 1–5, um einen Ausnahmedämmengenehmiger der Ebene 2 CC zu erstellen.

   Hinweis:
   Wählen Sie beim Erstellen eines Genehmigers der zweiten Ebene aus **Ausnahmegenehmiger – Ebene 2 CC**

7. **Wahlweise:** Wenn Sie auswählen **Bearbeiten** , Verschieben Sie Anwender aus dem **Sammlung** Zu **Gruppenmitglieder** Bereich und klicken Sie auf **Speichern** .
   Der Genehmiger muss zu navigieren **Alle** > **Konfigurations-Compliance** > **Meine Genehmigungen** Und genehmigen Sie Anforderungen.

Erstellen Sie einen Konfigurations-Compliance Relevanzzuordnung

Konfigurations-Compliance Die Relevanzzuordnung bietet eine Transformationszuordnung für Relevanzfelder von Drittparteien zu erkennbaren Feldern in Konfigurations-Compliance Schweregrad.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Relevanz-Zuordnung**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feldzuordnung

Feld	Beschreibung
Quelle	Der Name der Quelle für die Relevanzzuordnung.
Quellwert	Der Quellenrelevanzwert.
Zielwert	Der Zielwert. Auswahlmöglichkeiten: **Kritisch** Das Konfigurationsproblem, das der Steuerung zugeordnet ist, verursacht eine Unterbrechung eines oder mehrerer geschäftskritischer CIs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hoch Das Konfigurationsproblem, das der Steuerung zugeordnet ist, ist eine Bedrohung, verursacht jedoch nicht das Herunterfahren kritischer Netzwerkressourcen. **Mittel** Das Konfigurationsproblem, das der Steuerung zugeordnet ist, ist ein Risiko, aber keine unmittelbare Bedrohung. **Niedrig** Das Konfigurationsproblem, das der Steuerung zugeordnet ist, ist eine Bedrohung auf niedriger Ebene und kann zugunsten von CIs ignoriert werden, die einem höheren Risiko ausgesetzt sind. **Kleiner** Das Konfigurationsproblem, das der Steuerung zugeordnet ist, ist ein geringfügiges Risiko und kann bei Bedarf ignoriert werden.

4. Klicken Sie auf **Absenden**.

Erstellen Sie E-Mail-Benachrichtigungen

Schwachstellenadministratoren können die Benachrichtigung bearbeiten oder neue hinzufügen, indem sie angeben, wann die Benachrichtigung gesendet werden soll, wer die Benachrichtigung erhält und welchen Inhalt die Benachrichtigung enthält.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können E-Mail-Vorlagen für verschiedene Arten von E-Mail-Benachrichtigungen erstellen. Weitere Informationen zum Erstellen von E-Mail-Vorlagen finden Sie unter Definieren Vulnerability Response E-Mail-Vorlagen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Benachrichtigungen**an.
2. Wählen Sie den Benachrichtigungsdatensatz für das Korrekturziel aus, oder wählen Sie aus **Neu** .
3. Füllen Sie die entsprechenden Felder im Formular aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Create an email notification .
4. Wählen Sie Aus **Vorschau Der Benachrichtigung Anzeigen** Zum Anzeigen der Nachricht.

Ergebnisse

Ab v14.11 von Konfigurations-Compliance, Wenn ein Empfänger auf die Links in einer E-Mail-Benachrichtigung klickt, werden die Datensätze im geöffnet Arbeitsbereich des Schwachstellenmanagers Oder Arbeitsbereich für IT-Korrekturen Basierend auf ihrer Rolle.

- Links werden in geöffnet Arbeitsbereich des Schwachstellenmanagers Für die Anwender mit der Rolle sn_vulc.admin.
- Links werden in geöffnet Arbeitsbereich für IT-Korrekturen Für die Anwender mit der Rolle sn_vulc.Remediation_owner.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Empfänger keine der vorherigen Rollen hat, werden die Links in einer E-Mail-Benachrichtigung in der klassischen Anwenderoberfläche geöffnet.

Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement in Konfigurations-Compliance

Verwenden Sie den Flow Designer, um Ausnahmeanforderungen für das Ausnahmemanagement und Ausnahmeregeln zu genehmigen. Wenn Sie bereitstellen Konfigurations-Compliance Zum ersten Mal ist der Flow Designer standardmäßig aktiviert.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Der Wert der Systemeigenschaft *sn_vulc.flow_designer_activation*lst auf „wahr“ festgelegt. Dies bedeutet, dass der Flow Designer standardmäßig aktiviert ist.

Hinweis:
Sie können den Workflow nicht mehr verwenden, nachdem Sie den Flow Designer aktiviert haben. Einen detaillierten Vergleich zwischen Workflow und Flow Designer finden Sie unter Ausnahmeverwaltungs-Workflow vs. Flow Designer in Konfigurations-Compliance.

Um den Flow Designer zu verwenden, erstellen Sie Regeln mit dem Modul „Genehmigungsregeln“. Mit diesem Modul können Sie Genehmigungsregeln für jeden der folgenden Ausnahmemanagement-Workflows konfigurieren.

- Ausnahmegenehmigungsregeln für Korrekturaufgabe
- Genehmigungsregel für automatische Ausnahmeregeln

Hinweis:
Sie können auch Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den übereinstimmenden Genehmigungs-Workflow. Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement in Konfigurations-Compliance.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Genehmigungsregeln** > **Ausnahmegenehmigungsregeln für Korrekturaufgabe**an.
2. Wählen Sie auf der Seite „Genehmigungsregeln“ die Gruppe aus, für die Sie die Genehmigungsregel festlegen möchten.
3. Füllen Sie im Formular die Felder aus.

Formular „Genehmigungsregel“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.
Tabelle	Tabelle, auf die die Regel angewendet wird.
Anwendung	Der Standardwert ist Konfigurations-Compliance.
Regeltyp	Gibt den Regeltyp an. Zum Beispiel Ausnahmeverwaltung oder Ausnahmeregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsregel verwendet wird.
Beschreibung	Kurzbeschreibung der Genehmigungsregeln.
Genehmigung läuft ab y (Tage)	Datum, bis zu dem der Genehmiger die Anforderung genehmigen kann.
Genehmiger benachrichtigen (Tage)	Datum, nach dem der Genehmiger benachrichtigt wird, Maßnahmen zu ergreifen.

4. Wählen Sie **Aktualisieren**.
   Auf der Registerkarte „Genehmigungskonfigurationen“ sind standardmäßig zwei Ebenen von Genehmigern eingerichtet. Sie können eine Regel auswählen, um die Bedingungen basierend auf verschiedenen Anwendungsfällen innerhalb einer Regel zu definieren. Weitere Informationen finden Sie unter Erstellen Sie Konfigurationen für eine Genehmigungsregel in Konfigurations-Compliance.

   Hinweis:
   Auf jeder Konfigurationsseite können Sie mehrere Genehmigungsebenen erstellen. Weitere Informationen finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement in Konfigurations-Compliance.

Example:
Basierend auf verschiedenen Anwendungsfällen können Sie verschiedene Genehmigungsprozesse für dieselben Testergebnisse definieren, die für verschiedene Korrekturaufgaben gefunden wurden.

Erstellen Sie Konfigurationen für eine Genehmigungsregel in Konfigurations-Compliance

Definieren Sie die Bedingungen, um übereinstimmende Korrekturaufgaben für eine Genehmigungsebene herauszufiltern.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird
Im Modul „Genehmigungskonfigurationen“ können Sie mehrere Genehmigungsebenen für verschiedene Konfigurationen konfigurieren. Definieren Sie bedingungsbasierte Regeln, wobei jede Regel mehrere Genehmigungsebenen enthält.

Hinweis:
Verwenden Sie das Modul „Genehmigungsregeln“, um Genehmigungsregeln für die Ausnahmemanagement-Workflows zu konfigurieren. Informationen zum Konfigurieren von Genehmigungsregeln finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement in Konfigurations-Compliance.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Genehmigungsregeln**an.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zu **Genehmigungskonfigurationen** Registerkarte.
3. Wählen Sie eine Konfiguration aus.
4. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Genehmigungskonfiguration“

Feld	Beschreibung
Name	Name der Genehmigungskonfiguration.
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel.
Reihenfolge	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Auftragseintrag von 100 vor einer Konfiguration mit einem Auftragseintrag von 200 ausgeführt.
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungskonfiguration verwendet wird.
Beschreibung	Kurzbeschreibung der Genehmigungskonfigurationsebenen.

5. Legen Sie eine Bedingung für die Testergebnisse oder Korrekturaufgaben auf eine der folgenden Arten fest:

Feld	Beschreibung
Bedingung	Identifiziert die übereinstimmenden Testergebnisse oder Korrekturaufgaben.
Erweiterte Bedingung	Skript, das die Bedingung für die Testergebnisse oder Korrekturaufgaben definiert. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie auswählen **Erweitert** Kontrollkästchen.

6. Wählen Sie **Aktualisieren**.
   Sie können Bedingungen definieren, die mehrere Genehmigungsebenen innerhalb einer Regel enthalten. Der Flow Designer erbt automatisch die in diesem Modul erstellten Regeln und verarbeitet den übereinstimmenden Genehmigungs-Workflow. Informationen zum Konfigurieren von Genehmigungsebenen finden Sie unter Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement in Konfigurations-Compliance.

Example:
Sie können verschiedene Genehmigungspfade für verschiedene Arten von Korrekturaufgaben definieren.

Erstellen Sie Genehmigungsebenen für das Ausnahmemanagement in Konfigurations-Compliance

Definieren Sie die Ebenen der Anwender und Anwendergruppen, die die Ausnahmeanforderungen genehmigen.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Genehmigungsregeln**an.
2. Wählen Sie eine Genehmigungsregel aus, und navigieren Sie zu **Genehmigungskonfigurationen** Registerkarte.
3. Wählen Sie eine Konfiguration aus.
4. In **Genehmigerebenen** Wählen Sie eine Genehmigerebene aus.
5. Füllen Sie im Formular die Felder aus.

Formular auf Genehmigerebene

Feld	Beschreibung
Name	Name der Genehmigungsebene.
Erforderliche Genehmigung	Wählen Sie aus, wie viele Genehmigungen für die ausgewählte Ebene erforderlich sind: ○ Ein Genehmiger erforderlich ○ Alle Anwender müssen genehmigen
Aktiv	Standardmäßig aktiviert, was bedeutet, dass die Genehmigungsebene verwendet wird.
Reihenfolge	Ausführungsreihenfolge verschiedener Konfigurationen innerhalb einer Regel. Beispielsweise wird eine Konfiguration mit einem Auftragseintrag von 100 vor einer Konfiguration mit einem Auftragseintrag von 200 ausgeführt.
Freigaberegel	Enthält die Tabellen- und Typdetails für die Genehmigungsregel. Dieses Feld ist schreibgeschützt.
Genehmigungskonfiguration	Enthält die Genehmigungskonfigurationen. Dieses Feld ist schreibgeschützt.
Zuweisen mit	Wählen Sie eine Option aus: ○ Anwender und Anwendergruppe ○ Genehmigungstabellenfeld ○ Skript
Gruppen	Genehmigerebenengruppe, die aus mehreren Anwendern besteht. Der Anwender muss über eine der folgenden Rollen für das Ausnahmemanagement und Ausnahmeregeln verfügen: ○ sn_vulc.Exception_Approver ○ sn_vulc.read ○ sn_vulc.read_Auto_Exception_rule
Anwender	Bearbeiten Sie die in den Gruppen aufgeführten Anwender.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie aus, um die Änderungen zu speichern **Aktualisieren** .

Hinweis:
Vor v13.0 ist der Workflow-Prozess funktionsfähig, wenn Anwender nur in Ausnahmebene 1 vorhanden sind. Ab v13.0 muss jedoch mindestens ein Anwender auf jeder Ebene vorhanden sein.

Vor v13.0 wurde die Korrekturaufgabe im Workflow zurückgestellt, wenn auf der zweiten Ebene kein Anwender vorhanden war. Ab v13.0 wird die Genehmigungsanforderung jedoch automatisch abgelehnt, wenn auf der zweiten Ebene kein Anwender vorhanden ist.

Example:
Es kann verschiedene Genehmigungsebenen für Korrekturaufgaben für Linux- und Windows-Server geben.

Ausnahmeverwaltungs-Workflow vs. Flow Designer in Konfigurations-Compliance

Beginnend mit Konfigurations-Compliance(CC) v13.0: Wenn Sie CC zum ersten Mal bereitstellen, ist der Flow Designer für die Genehmigung von Ausnahmeanforderungen im Ausnahmemanagement standardmäßig aktiviert. Wenn Sie ein vorhandener CC-Anwender sind, ist die Standardoption Workflow.

Workflow versus Flow Designer

Überlegungen	Workflow	Flow Designer
Version	Vor v13.0 von CC.	Ab v13.0 von CC.
Standardoption	Standardoption, wenn Sie ein vorhandener CC-Anwender sind.	Standardoption für neue CC-Anwender ab v13.0.
Festlegen des Genehmigungsprozesses	Die Ausnahmemanagement umfasst Ausnahmeanforderungen zusammen mit Ausnahmeregeln.	Umfasst das Definieren verschiedener Ebenen und das Hinzufügen verschiedener Genehmiger für verschiedene Anwendungsfälle. Einfacher zu implementieren als der Workflow. Die Ausnahmemanagement umfasst Ausnahmeanforderungen zusammen mit Ausnahmeregeln.
Upgrade auf Flow Designer	Sie können ein Upgrade auf Flow Designer über den Workflow durchführen. Vorhandene Anforderungen können jedoch nur mit dem Workflow genehmigt werden.	Flow Designer ist standardmäßig aktiviert.
Systemeigenschaft `sn_vulc.flow_designer_activation`	Wenn Sie den Workflow für das Ausnahmemanagement vor v13.0 verwendet haben, wird die Systemeigenschaft auf „falsch“ festgelegt. Um den Flow Designer zu aktivieren, legen Sie diese Eigenschaft auf „wahr“ fest.	Wenn Sie CC zum ersten Mal für v13.0 oder höher verwenden, wird der Systemeigenschaftswert standardmäßig auf „wahr“ festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow versus Flow Designer (Fortsetzung)

Überlegungen	Workflow	Flow Designer
	Hinweis: Sie können den Workflow nicht mehr verwenden, nachdem Sie den Flow Designer aktiviert haben.	
Genehmigungsregelmodul	Nachdem Sie die Systemeigenschaft auf „wahr“ festgelegt haben, wird der **Aktivieren Sie Modulgenehmigungsregeln** Die geplante Aufgabe wird innerhalb von 24 Stunden ausgeführt. Mit dieser geplanten Aufgabe wird aktiviert **Genehmigungsregeln** Modul. Um dieses Modul sofort zu aktivieren, führen Sie diesen Auftrag manuell aus.	Wenn Sie CC zum ersten Mal aus CC v13.0 bereitgestellt haben, ist dieses Modul standardmäßig verfügbar.
Genehmigungsstufen	Bietet die Option, nur zwei Ebenen von Genehmigern festzulegen.	Bietet mehrere Optionen, z. B. das Festlegen einer beliebigen Anzahl von Konfigurationen, Genehmigerebenen und das dynamische Hinzufügen von Genehmigern für jede Regel.

Konfigurations-Compliance-Integrationen

Drittpartei-Integrationen importieren Konfigurationsbewertungsergebnisse, Richtlinien, Tests, Technologien, autorisierende Quellen, testet Ergebnisse zusammen mit anderen Schwachstellendaten in Konfigurations-Compliance Anwendung.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Die Konfigurations-Compliance Die Anwendung unterstützt die folgenden Drittanbieterintegrationen:

- Beginnen Sie ab v14.11 die Korrektur von Sicherheitslücken in Ihren Enterprise-Assets, die von der Anwendung „Sicherheitsstatus-Steuerung“ identifiziert wurden, indem Sie Ergebnisse als Testergebnisse in veröffentlichen Konfigurations-Compliance Anwendung. Die Anwendung „Sicherheitsstatus-Steuerung“ und die unterstützten Anwendungen sind mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

separaten Abonnements von verfügbar ServiceNow® Store. Weitere Informationen finden Sie unter Sicherheitsstatus-Überwachung.

- Microsoft Defender for Cloud Integration für Security Operations
- Palo Alto Prisma Cloud Vulnerability Integration
- Integration von Konfigurations-Compliance in Qualys
- Die Tenable.io Produkt von Tenable-Schwachstellenintegration

Zusätzliche Hinweise für Integrationen

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter.
Um diese Fehlkommunikation zu vermeiden, ab Version 14.8.5 von Konfigurations-Compliance, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Microsoft Defender for Cloud Integration für Security Operations

Die Microsoft Defender for Cloud Integration Produkt ist ein Infrastruktursicherheitsmanagementsystem, das die Sicherheitslage Ihrer Cloud-Umgebungen verbessert.

Microsoft Defender for Cloud IntegrationFür Security Operationsist in integriert Konfigurations-Compliance Anwendung zum Zuordnen von Tests zu Konfigurationselementen (Configuration Items, CIs), um Testergebnisse zu erstellen. Es erkennt kontinuierlich neue Cloud-Ressourcen, die über Arbeitsauslastungen hinweg bereitgestellt werden, und bestimmt, ob sie gemäß Sicherheitsstandards wie dem Center for Internet Security (CIS) konfiguriert sind.

Ab Version 2,2 wird Microsoft Azure Security Center in umbenannt Microsoft Defender for Cloud Integration Für Security Operations.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Versionen

Anwendung	Version
Microsoft Defender for Cloud Integration Für Security Operations	2.3
Konfigurations-Compliance	14.3
Security Support Common	13.2
Vulnerability Response	16,2

Mehrere Bereitstellungen von Microsoft Defender for CloudPlattform

Wenn Sie mehrere Bereitstellungen von haben Microsoft Defender for CloudPlattformanwendung können Sie für jede Bereitstellung eine Integration hinzufügen. Ressourcen, die von mehreren Drittanbieterbereitstellungen identifiziert werden, werden konsolidiert und mit abgeglichen Configuration Management Database (CMDB). Diese Konsolidierung findet auch dann statt, wenn sich Scan-Prozesse zwischen mehreren Bereitstellungen überschneiden.

ServiceNow Microsoft Defender for Cloud Integrationen

Die Microsoft Defender for Cloud IntegrationFür Security Operations Ergänzt die Compliance-Daten in Ihrer Instanz, indem Daten von abgerufen werden Microsoft Defender for Cloud. Eine Reihe geplanter Aufgaben ruft die Integrationen automatisch auf. Sie können diese geplanten Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Nachbesserung von Testergebnissen, indem die Instanz mit synchronisiert wird Microsoft Defender for Cloud.

Für jeden Integrationsdatensatz ist ein „Run-as“-Anwender mit dem Standardwert konfiguriert **VR.System** . Dieser Wert muss gleich bleiben.

Hinweis:
Wenn Sie keinen gültigen „Ausführen als“-Anwender festlegen, werden doppelte oder mehrere Datenabrufanhänge für die Datenquellendatensätze erstellt. Die Anzahl der Anhänge erhöht sich jedes Mal, wenn die Integration ausgeführt wird. Dies erhöht die Verarbeitungszeit, was zu inkonsistenten Transformationsergebnissen führt.

Microsoft Defender for Cloud Plattformintegrationsaufgaben umfassen die folgenden Rollen.

- sn_vul_asc.configure_Integration: Fähigkeit zum Lesen, Schreiben und Löschen von Datensätzen.
- sn_vul_asc.read_Integration: Fähigkeit zum Lesen von Datensätzen.

Anzeigen von Microsoft Defender for CloudIntegrationen

Zeigen Sie die Integrationen an, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Integrationen**an.

Die folgenden Integrationen sind im Basissystem enthalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration	Beschreibung
Integration Der Richtliniendefinition	Ruft Richtlinien ab und erstellt Richtlinieneinträge in Ihrer Instanz.
Integration Von Bewertungsmetadaten	Ruft Bewertungsmetadaten ab und erstellt Tests in Ihrer Instanz.
Integration Von Compliance-Standards Und -Steuerungen	Ruft Standards und Steuerungen ab und erstellt die Autorisierungsquelle und Bezugsvermerke. Dann werden sie mit den erstellten Tests verknüpft.
Bewertungsintegration	Ruft Bewertungen ab und verarbeitet sie in Ihrer Instanz. Die Ausgabe dieser Integration ist Testergebnisse.

Erstellen Sie CIs mit der Identifizierungs- und Abgleichsmodul

Verwenden Sie die Identification and Reconciliation Engine (IRE), um CIs zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann, der von einem Scanner einer Drittpartei importiert wurde.

Wenn ein CI in der CMDB nicht übereinstimmt, wird ein CI in erstellt *cmdb_ci_cmp_resource*Klasse. Wenn eine Discovery später dasselbe CI findet, wird das CI angereichert oder ein anderes erstellt.

Hinweis:
Der automatische Abgleich findet für Cloud-Ressourcen nicht statt.

Installieren und konfigurieren Microsoft Defender for Cloud Integration Für Security Operations

Installieren und konfigurieren Sie Microsoft Defender for Cloud Integration Für Security Operations, Damit Sie die Daten verwenden können, die aus importiert werden Microsoft Defender for CloudUm Fehlkonfigurationen für Ihre Assets zu priorisieren und zu beheben.

Vorbereitungen

Erstellen Sie eine neue App-Registrierung in Azure Active Directory für Microsoft Defender for Cloud Integration. Weitere Informationen zum Registrieren einer neuen Anwendung in Azure Active Directory finden Sie unter Microsoft-Produktdokumentation Website. Weitere Informationen zu Azure-Rollen finden Sie unter Azure-Rollen .

Erforderliche Rolle: sn_vulc.admin

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**an.
2. Suchen Sie in der Suchleiste nach Microsoft Defender for Cloud Integration for Security Operations .
3. Wählen Sie **Installieren** aus.

   Alle Abhängigkeiten, die installiert werden, werden angezeigt.
4. Navigieren zu **Alle** > **Microsoft Defender für Cloud-Integration** > **Administration** > **Konfiguration** > **Microsoft Defender für Cloud-Konfiguration**an.
5. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Defender for Cloud Konfigurationsformular

Feld	Beschreibung
API-URL	Ressourcen-URL der Instanz. Beispiel: https://management.azure.com (Öffentliche Azure-Cloud)
Mandanten-ID	Mandantenidentität Ihrer Organisation.
Integrationsinstanz	Standardinstanz. Sie können auch eine Instanz erstellen, um die Daten aus mehreren Microsoft-Dateien zu übertragen Defender Mandanten oder Abonnements.
Client-ID	Client-Identität, die nach generiert wird Microsoft Defender for Cloud Integration Anwendung ist registriert.
Geheimer Clientschlüssel	Geheimer Clientschlüssel, der nach generiert wird Microsoft Defender for Cloud IntegrationAnwendung ist registriert.
Importieren Sie Ergebnisse aus	Ressourcen und Bewertungen, die den ausgewählten Verwaltungsgruppen-IDs und Abonnement-IDs entsprechen, die abgerufen werden sollen.
Verwaltungsgruppen-IDs	Ressourcen und Bewertungen, die den Managementgruppen-IDs entsprechen, die abgerufen werden sollen. **Hinweis:** Dieses Feld wird nur angezeigt, wenn Sie auswählen **Bestimmte Verwaltungsgruppen** Von **Importieren Sie Ergebnisse aus** Feld.
Abonnement-IDs	Identifikationsnummern der Abonnements, für die die Ressourcen und Bewertungen abgerufen werden sollen. **Hinweis:** Dieses Feld wird nur angezeigt, wenn Sie auswählen **Bestimmte Abonnements** Von **Importieren Sie Ergebnisse aus** Feld.
Validierungsstatus	Gibt an, ob die angegebenen Anmeldeinformationen und Abonnement-ID gültig sind.

6. Konfigurieren oder führen Sie die Integrationen aus, indem Sie auswählen **Speichern und testen** .

Konfigurations-Compliance Daten für importiert Microsoft Defender for Cloud Integration

Konfigurations-Compliance Importiert Richtlinien, Tests, autorisierende Quellen und Testergebnisse aus Drittpartei-Integrationen und speichert sie zur Anzeige in Modulen.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Testgruppen

Eine Gruppe von Konfigurationstests stellt eine Testgruppe dar. Testgruppen beziehen sich auf autorisierende Dokumente und Testdatensätze und können entsprechend den Anforderungen Ihrer Organisation geändert werden. Ein Konfigurationstest kann mehreren Testgruppen angehören.

Wenn Microsoft Defender for Cloud Integrationlst installiert, werden Testgruppen abgerufen und durch die geplante Aufgabe ausgefüllt, **Integration Von Richtliniendefinitionen** . Sie können die geplante Aufgabe anzeigen, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Administration** > **Integrationen** > **Integration Von Richtliniendefinitionen**an.

Hinweis:
Wenn Sie die Integration manuell ausführen möchten, führen Sie aus **Integration Von Richtliniendefinitionen** Zuerst.

Tests

Tests sind Bibliotheken von Datensätzen, die Scans von Computing-Assets organisieren. Konfigurationstests definieren, wie Assets gesteuert werden müssen.

A Konfigurations-Compliance„Test“ ist der Mechanismus, den Drittanbieter-Integrationsanwendungen verwenden, um Assets nach Testergebnistyp zu gruppieren.

Wenn Microsoft Defender for Cloud Integration Ist installiert, die geplante Aufgabe, **Integration Von Bewertungsmetadaten** , Ruft die Tests ab. Sie können die geplante Aufgabe anzeigen, indem Sie zu navigieren **Integration** > **Primäre Integrationen** > **Integration Von Bewertungsmetadaten**an.

Hinweis:
Wenn Sie die Integration manuell ausführen möchten, führen Sie aus **Integration Von Bewertungsmetadaten** Nach **Integration Von Richtliniendefinitionen** .

Ab v15.0 von Konfigurations-Compliance, Die Testgruppe, zu der ein Test gehört, wird in ausgefüllt **Testgruppen** Spalte der Testliste.

Autorisierende Quellen

Konfigurations-Compliance Verwendet autoritative Quellen und Zitate beim Generieren von Schwachstellenwarnungen für Tests. Autorisierende Quellen werden normalerweise Abschnitten veröffentlichter Branchenstandards zugeordnet, z. B. **ISO 27001** Und **PCI DSS 3.2.1** .

Diese Quelldatensätze enthalten Verweise auf Informationen zu bekannten Software- und Hardwarekonfigurationsproblemen von Experten im Bereich der Computersicherheit. Sie definieren Anforderungen für Sicherheitsrichtlinien und -Verfahren.

Wenn Microsoft Defender for Cloud Integration Ist installiert, die geplante Aufgabe, **Compliance-Standards Und -Steuerungen** , Ruft die autorisierenden Quellen und Bezugsvermerke ab. Sie können diese geplante Aufgabe anzeigen, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Integrationen** > **Integration Von Compliance-Standards Und -Steuerungen**an.

Hinweis:
Wenn Sie die Integration manuell ausführen möchten, führen Sie aus **Integration Von Compliance-Standards Und -Steuerungen** Nach **Integration Von Bewertungsmetadaten** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Assets

Die **Bewertungsintegration** Stellt wichtige Informationen wie Ressourcen-Tags und Cloud-Attribute bereit. Diese Informationen werden im Formular „erkanntes Element“ angezeigt. #Wird hauptsächlich zum Filtern verwendet Konfigurations-Compliance Regeln für Zuweisungs- und Korrekturaufgaben.

- Ressourcen-Tags: Alle Cloud-Ressourcen-Tags werden als Teil von als Host-Tags importiert **Bewertungsintegration** . Die Cloud-Tags für jeden Cloud-Ressourcentyp werden hier gespeichert, unabhängig davon, ob die Ressource ein Host ist oder nicht.
  - Beim Tag-Speicher wird die Groß-/Kleinschreibung nicht beachtet. Wenn ein#Tokyo-#Tag erstellt wird, wird ein erstellt **TOKIO** #Tag kann nicht in der Host-Tag-Tabelle gespeichert werden. **Tokio** Und **TOKIO** Werden als dasselbe Host-Tag betrachtet. Das Tag, das importiert wurde, gewinnt zuerst.
  - Die Verwendung von Host-Tags als Gruppenschlüssel in einer Gruppenregel kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Cloud-Attribute für Assets: Im Folgenden sind die Cloud-Attribute aufgeführt, aus denen die Integrationen abgerufen werden Microsoft Defender for Cloud:
  - Cloud-Account
  - Cloud-Region
  - Cloud-Ressourcentyp
  - Cloud-Service-Provider

Testergebnisse

Konfigurations-Compliance Berechnet die Testergebnisse nicht, importiert sie jedoch als Teil einer Drittpartei-Integration. Sobald sie in angezeigt werden können Konfigurations-Compliance, Werden sie mit korrigiert **Korrekturaufgaben** .

Wenn Microsoft Defender for CloudIntegration ist installiert, die geplante Aufgabe, **Bewertungsintegration** , Ruft die Testergebnisse ab. Sie können diese geplante Aufgabe anzeigen, indem Sie zu navigieren **Alle** > **Microsoft Defender für Cloud-Integration** > **Integrationen** > **Bewertungsintegration**an.

Die **Bewertungsintegration** Import ist die einzige Integration, die verwendet *`Start Time`*Parameter in **Integrationsdetails** Registerkarte. Alle anderen Konfigurations-Compliance Importe beziehen alle verfügbaren Daten unabhängig von ein *`Start Time`*.

Wenn **Bewertungsintegration** Import ist abgeschlossen, ein Ereignis wird gestartet, um Berechnungen für das Ende des Imports auszulösen.

Die **Bewertungsintegration** Ruft die Datenbewertungen standardmäßig nur ab, wenn eine Statusänderung gegenüber der letzten erfolgreichen Integrationsausführung für den letzten Tag vorliegt. Wenn die Bewertung in den letzten Tagen kontinuierlich fehlschlägt, ruft die Integration die Bewertung nicht ab, da für die Bewertung keine Statusänderung erfolgt. Um die Testergebnisse mit den Defender-Bewertungen auf dem neuesten Stand zu halten, eine neue **Umfassende Bewertungsintegration** Wird hinzugefügt, wodurch die Daten aus den letzten sieben Tagen abgerufen werden. Er wird wöchentlich ausgeführt und ruft alle Testergebnisse ab, die nicht bestanden wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Suchregeln zum Identifizieren von CIs aus Microsoft Defender for CloudIntegrationen

Wenn Daten aus einer Drittpartei-Integration importiert werden, Konfigurations-Compliance Verwendet automatisch Ressourcendaten, um nach Übereinstimmungen in zu suchen Configuration Management Database (CMDB), Mithilfe von CI-Suchregeln. Diese Regeln werden verwendet, um die Konfigurationselemente (Configuration Items, CIs) zu identifizieren und dem Testergebnisdatensatz hinzuzufügen, um die Korrektur zu erleichtern. Basissystem-CI-Suchregeln sind für Ressourcen-ID, Name und S3-Bucket verfügbar. Weitere Informationen zu CI-Suchregeln finden Sie unter CI-Sperrregeln für Microsoft Defender for Cloud Integration for Security Operations .

Vulnerability Response Integration with Palo Alto Prisma Cloud verstehen

Prisma Cloud ist eine API-basierte Sicherheitslösung für die Cloud-Infrastruktur. Es stellt eine Verbindung zu Ihrer Cloud-Umgebung her und überwacht die in den öffentlichen Cloud-Umgebungen bereitgestellten Ressourcen, z. B. Amazon Web Services(AWS), Microsoft Azure, Und so weiter. Sie erhalten vollständige Transparenz und Kontrolle über Risiken in Ihrer öffentlichen Cloud-Infrastruktur.

Die Vulnerability Response Integration with Palo Alto Prisma Cloud Die Anwendung erleichtert die Erfassung von Richtlinien und Warnungen aus Prisma Cloud als Tests bzw. Testergebnisse im Konfigurations-Compliance Anwendung. Mit der richtigen Konfiguration können die Testergebnisse nahtlos verwaltet werden, indem entsprechende Risikopunktzahlen zugewiesen und sie relevanten Anwendern und Gruppen gruppiert und zugewiesen werden.

Verfügbare Versionen

In der Tabelle werden die Anwendungen aufgelistet, die Vulnerability Response Integration with Palo Alto Prisma Cloud Hängt von zusammen mit der Version der Anwendung ab.

Anwendung	Version
Prisma-Cloud-Integration für Security Operations	2.3
Konfigurations-Compliance	14.7
Security Support Common	13,5
Vulnerability Response	18,0

ServiceNow Prisma-Cloud-Integrationen

Die Vulnerability Response Integration with Palo Alto Prisma Cloud Die Anwendung hilft beim Importieren der Prisma-Daten in Ihren ServiceNow Instanz zum Anreichern Ihrer Instanz für eine bessere Verwaltung. Eine Reihe geplanter Aufgaben ruft die Integrationen automatisch auf. Sie können diese geplanten Aufgaben auch manuell ausführen. Geplante Aufgaben vereinfachen den Lebenszyklus der Nachbesserung von Testergebnissen, indem die Instanz aktualisiert wird, indem regelmäßig Daten aus Prisma Cloud abgerufen werden.

Prisma Cloud-Integrationsaufgaben umfassen die folgenden Rollen.

- sn_vul_prismacloud.configure_Integration: Fähigkeit zum Lesen, Schreiben und Löschen von Datensätzen.
- sn_vul_prismacloud.read_Integration: Fähigkeit zum Lesen von Datensätzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationen werden angezeigt

Sie können die Integrationen anzeigen, die Teil von sind Vulnerability Response Integration with Palo Alto Prisma Cloud Indem Sie zu navigieren **Prisma-Cloud-Integration** > **Integrationen**an.

Die folgenden Integrationen sind im Basissystem verfügbar.

Ausführungssequenz	Zeitplan	Integration	Beschreibung
1	Wöchentlich	Prisma-Richtlinienintegration	• Ruft Richtlinien aus Prisma Cloud ab und erstellt Testeinträge in Ihrer Instanz. • Es bietet keinen inkrementellen Support. Wenn Sie die Integration in den letzten 10 Tagen ausführen, wird auch das Ergebnis für vorherige Integrationsausführungen angezeigt.
2	Täglich	Integration Von Prisma-Warnungen	• Ruft Warnungen aus Prisma Cloud ab und erstellt Testergebniseinträge in Ihrer Instanz. • Bietet inkrementellen Support. Die Integration wird täglich nach der letzten Ausführungszeit der Integration ausgeführt.

Vorbereitung der Installation von Vulnerability Response Integration with Palo Alto Prisma Cloud

Bereiten Sie die Installation von vor Vulnerability Response Integration with Palo Alto Prisma Cloud Durch Ausführen von Setup-Aufgaben.

Bevor Sie beginnen

Um Vulnerability Response mit Palo Alto Prisma Cloud zu integrieren, muss Ihnen in Prisma eine Berechtigungsgruppe zugewiesen sein, die schreibgeschützten Zugriff auf Richtlinien- und Warnungsdaten bietet. Weitere Informationen zu Berechtigungsgruppen finden Sie unter Prisma-Cloud-Administratorrollen .

Detaillierte Informationen zu den Rollen, die verschiedenen Berechtigungsgruppen zugewiesen sind, finden Sie auf der Seite Prisma Cloud-Administratorberechtigungen .

Darüber hinaus müssen Zugriffsschlüssel erstellt werden, um das Lesen der Warnungen zu ermöglichen. Weitere Informationen zum Erstellen von Zugriffsschlüsseln finden Sie unter Erstellen und verwalten Sie Zugriffsschlüssel .

Zum Installieren und Konfigurieren von Vulnerability Response Integration with Palo Alto Prisma Cloud, Verwenden Sie die folgende Prüfliste. Vergewissern Sie sich vor der Installation der Anwendung, dass die aufgeführten Elemente abgeschlossen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für Integrationsvorbereitung

Aufgabe	Beschreibung
☐	Stellen Sie sicher, dass Sie über die folgenden Informationen verfügen: • API-Basis-URL • Zugangsschlüssel-ID • Geheimer Schlüssel • Anwendername und Passwort für den Zugriff auf Prisma Cloud. Diese Anmeldeinformationen werden verwendet, um eine Verbindung mit der Prisma Cloud-Instanz über herzustellen ServiceNow AI Platform® Instanz. Die Zugriffsschlüssel-ID und der geheime Schlüssel müssen nach der Registrierung aus dem Prisma Cloud-Portal generiert werden.
☐	Wenn nicht bereits installiert und aktiviert, installieren Sie Vulnerability Response Anwendung, bevor Sie installieren Vulnerability Response Integration with Palo Alto Prisma Cloud Anwendung. Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe Vulnerability Response installieren. Diese Integration erfordert Version 15.2.0 Von Vulnerability Response Oder später.
☐	Wenn Sie die Anwendung noch nicht in Ihrer Instanz haben, rufen Sie Berechtigungen ab, und laden Sie herunter Vulnerability Response Integration with Palo Alto Prisma Cloud Anwendung für Ihren ServiceNow AI Platform® Instanz. Weitere Informationen finden Sie unter .
☐	Stellen Sie sicher, dass Sie die folgenden Plugins installiert haben, um eine reibungslose Integrationsausführung zu gewährleisten: • Vulnerability Response • Konfigurations-Compliance • Vulnerability Response Integration with Palo Alto Prisma Cloud Die folgenden Plugins sind optional, können jedoch nützlich sein: • Cloud Provisioning and Governance • Muster für Discovery und Service-Mapping
☐	Schätzen Sie die Anzahl der Testergebnisse, die Sie importieren möchten. Überprüfen Sie, ob Ihre Instanz die Anzahl der Testergebnisse akzeptieren kann, die Sie importieren möchten. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an ServiceNow Technischer Support.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste für Integrationsvorbereitung (Fortsetzung)

Aufgabe	Beschreibung
☐	Stellen Sie sicher, dass Sie über einen Administrator verfügen, der die Integrationen verwaltet und die Testergebnisse korrigiert: Der -Administrator installiert Vulnerability Response Integration with Palo Alto Prisma Cloud Anwendung. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.Vulnerability_admin) und andere Rollen zu.

Sie sind bereit für Installieren und konfigurieren Sie Vulnerability Response Integration with Palo Alto Prisma Cloud Anwendung.

Installieren und konfigurieren Sie Vulnerability Response Integration with Palo Alto Prisma Cloud Anwendung

Installieren Sie Vulnerability Response Integration with Palo Alto Prisma Cloud Anwendung zur Verwendung der aus Prisma Cloud importierten Daten. Verwenden Sie diese Daten, um Fehlkonfigurationen für Ihre Assets zu priorisieren und zu beheben.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Systemdefinition** > **Plugins**an.
2. Suchen Sie in der Suchleiste nach Vulnerability Response-Integration mit Palo Alto Prisma Cloud .
3. Klicken Sie auf **Installieren**.

   Alle Abhängigkeiten, die installiert werden, werden angezeigt.
4. Navigieren zu **Alle** > **Prisma-Cloud-Integration** > **Administration** > **Konfiguration** > **Prisma-Cloud-Konfiguration**an.
5. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Integrationsinstanz	Name der neuen Integrationsinstanz. Sie können eine Instanz erstellen oder auf das Suchsymbol klicken, um eine vorhandene Instanz auszuwählen.
API-URL	URL zur Integration in die Prisma-Cloud.
Zugangsschlüssel-ID	Eindeutiger Schlüssel zur Authentifizierung der Zugriffsanforderung bei der Prisma Cloud. **Hinweis:** Sie müssen den Schlüssel generieren, nachdem Sie sich beim Prisma Cloud-Portal angemeldet haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Geheimer Schlüssel	Privater Schlüssel zur Authentifizierung der Zugriffsanforderung bei der Prisma Cloud. **Hinweis:** Sie müssen den geheimen Schlüssel generieren, nachdem Sie sich beim Prisma Cloud-Portal angemeldet haben.

6. Klicken Sie Auf **Speichern und testen** .

Nächste Maßnahme
Navigieren Sie nach Abschluss der Installation zu **Prisma-Cloud-Integration** > **Konfiguration** Um mit der Konfiguration fortzufahren.

Konfigurieren Sie Vulnerability Response Integration with Palo Alto Prisma Cloud Anwendung

Konfigurieren Sie Vulnerability Response Integration with Palo Alto Prisma Cloud Anwendung. Verwenden Sie die aus Prisma Cloud importierten Daten, um Fehlkonfigurationen für Ihre Assets zu priorisieren und zu beheben.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur
1. Navigieren zu **Prisma-Cloud-Integration** > **Konfiguration**an.
2. Füllen Sie im Formular die Felder aus.

Prisma-Cloud-Konfiguration

Feld	Beschreibung
Integrationsinstanz	Name der neuen Integrationsinstanz. Sie können eine Instanz erstellen oder auf das Suchsymbol klicken, um eine vorhandene Instanz auszuwählen.
API-URL	URL zur Integration in Prisma Cloud.
Zugangsschlüssel-ID	Ein eindeutiger Schlüssel zur Authentifizierung der Zugriffsanforderung bei der Prisma Cloud. Sie müssen den Schlüssel generieren, nachdem Sie sich beim Prisma Cloud-Portal angemeldet haben.
Geheimer Schlüssel	Ein privater Schlüssel zur Authentifizierung der Zugriffsanforderung bei der Prisma Cloud.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie müssen den geheimen Schlüssel generieren, nachdem Sie sich beim Prisma Cloud-Portal angemeldet haben.

3. Klicken Sie Auf **Speichern und testen** .

Nächste Maßnahme
Nachdem Sie die Konfiguration abgeschlossen haben, navigieren Sie zu **Prisma-Cloud-Integration** > **Integrationen** Um sicherzustellen, dass die Integrationsausführung erfolgreich ist.

Verifizieren Sie Vulnerability Response Integration with Palo Alto Prisma Cloud Importausführungsstatus

Verwenden Sie Vulnerability Response Integration with Palo Alto Prisma Cloud Importieren Sie den Ausführungsstatus, um den Erfolg Ihrer Integrationsausführungen zu überprüfen und Probleme zu identifizieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter.
Um diese Fehlkommunikation zu vermeiden, ab Version 14.8.5 von Konfigurations-Compliance, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur

1. Navigieren zu **Prisma-Cloud-Integration** > **Integrationen**an.
2. Klicken Sie Auf **Integration Von Prisma-Richtlinien** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Jetzt ausführen**.
   Wenn diese Integration ausgeführt wird, werden die folgenden Tabellen in dieser Reihenfolge ausgefüllt:
   a. sn_vulc_Test.list (Konfigurationstests)
   b. sn_vulc_auth_src (autorisierende Quelle
   c. sn_vulc_Zitat (Zitate)
4. Unter **Elemente** Auf der Registerkarte die Anzahl der neuen Tests anzeigen, die erstellt, aktualisiert und ignoriert wurden, indem Sie auf die Ausführung der Schwachstellenintegration klicken.

   Hinweis:
   Richtlinien werden in Prisma Cloud für die ausgewählte Cloud-Instanz definiert. Die Instanz wird basierend auf den definierten Richtlinien gescannt.

5. Klicken Sie Auf **Integration Von Prisma-Warnungen** .
6. Klicken Sie auf **Jetzt ausführen**.
   Die folgenden Tabellen werden basierend auf der Integration ausgefüllt:
   - Testergebnisse
   - Erkannte Elemente: Wenn die Konfigurationselemente im System nicht verfügbar sind, werden sie erstellt. Die Klasse ist immer Cloud-Ressource. Auf der Seite „erkanntes Element“ werden drei neue Felder erstellt: **Cloud-Ressourcentyp** , **Cloud-Service Provider** , Und **Asset-Kategorie** .

     Unter **Elemente** Klicken Sie auf die Registerkarte Schwachstellen-Integrationsausführung, um die Anzahl der importierten, aktualisierten und ignorierten neuen Testergebnisse anzuzeigen. Die **Konfigurationselemente** Die Registerkarte wird auch basierend auf der Anzahl der erstellten Testergebnisse ausgefüllt.

Datenzuordnung

Die Daten aus Prisma Cloud werden in importiert Konfigurations-Compliance Modul von ServiceNow Instanz.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Die Daten aus Prisma Cloud werden mit einem anderen Namen in importiert Konfigurations-Compliance Wie in der Tabelle erwähnt.

Zuordnung von Prisma-Cloud-Daten in Konfigurations-Compliance

Prisma-Cloud	Konfigurations-Compliance
Richtlinie	Test

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnung von Prisma-Cloud-Daten in Konfigurations-Compliance (Fortsetzung)

Prisma-Cloud	Konfigurations-Compliance
Warnung	Testergebnis
Compliance-Standard	Autorisierende Quelle
Abschnitte	Bezugsvermerk
Asset	Discovery-Element/Konfigurationselement (CI)

Tests

Eine Richtlinie in Prisma Cloud wird als Test in importiert Konfigurations-Compliance. Richtlinien beziehen sich auf autorisierende Dokumente und Testdatensätze und können entsprechend den Anforderungen Ihrer Organisation geändert werden. Sie können die Tests anzeigen, indem Sie zu navigieren **Konfigurations-Compliance** > **Tests**an.

Wenn **Vulnerability Response-Integration mit Palo Alto Prisma Cloud** Ist installiert, der Integrationsauftrag, *`Prisma Policy Integration`*Ruft die Tests ab. Sie können diesen Integrationsauftrag anzeigen, indem Sie zu navigieren **Alle** > **Prisma-Cloud-Integrationen** > **Prisma-Richtlinienintegration**an.

Testergebnisse

Eine Warnung in Prisma Cloud wird als Testergebnis in importiert Konfigurations-Compliance. Warnungen werden mit korrigiert **Korrekturaufgaben** . Sie können die Testergebnisse anzeigen, indem Sie zu navigieren **Konfigurations-Compliance** > **Testergebnisse**an.

Die Konfigurations-Compliance Importiert Testergebnisse als Teil einer Drittpartei-Integration. Nachdem sie in angezeigt werden können Konfigurations-Compliance Anwendung, werden sie mithilfe von Korrekturaufgaben korrigiert.

Wenn **Vulnerability Response-Integration mit Palo Alto Prisma Cloud** Ist installiert, der Integrationsauftrag **Prisma-Warnungsintegration** Ruft die Testergebnisse ab. Sie können diesen Integrationsauftrag anzeigen, indem Sie zu navigieren **Alle** > **Prisma-Cloud-Integration** > **Integrationen** > **Prisma-Warnungsintegration**an.

Die **Prisma-Warnungsintegration** Ist ein Integrationsauftrag, der täglich ausgeführt wird und die Testergebnisse mit Statusänderung nach der in definierten Zeit abruft **Startzeit** Feld in **Integration** Registerkarte.

Hinweis:
Wenn Sie den Integrationsauftrag ausführen, **Prisma-Warnungsintegration** Führen Sie sie manuell aus, nachdem Sie den Integrationsauftrag ausgeführt haben. **Prisma-Richtlinienintegration** .

Wenn **Prisma-Warnungsintegration** Schließt den Import der Daten ab. Ein Ereignis wird gestartet, um Berechnungen für das Ende des Imports auszulösen. Wenn die Warnung in den letzten Tagen kontinuierlich fehlschlägt, ruft die Integration die Warnungen nicht ab, da für die Warnung keine Statusänderung erfolgt. Um die Testergebnisdaten mit den Prisma-Warnungen auf dem neuesten Stand zu halten, wird ein neuer Integrationsauftrag **Umfassende Prisma-Warnungsintegration** Wird hinzugefügt, wodurch die Warnungen abgerufen werden, die in den letzten sieben Tagen aktualisiert wurden. Er wird wöchentlich ausgeführt und ruft alle Testergebnisse ab, die nicht bestanden wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Autoritative Quellen

Konfigurations-Compliance Verwendet autoritative Quellen und Zitate beim Generieren von Schwachstellenwarnungen für Tests. Autorisierende Quellen werden normalerweise Abschnitten veröffentlichter Branchenstandards zugeordnet, z. B. ISO 27001 und PCI DSS 3,2.1.

Diese Quelldatensätze enthalten Verweise auf Informationen zu bekannten Software- und Hardwarekonfigurationsproblemen von Experten im Bereich der Computersicherheit. Die Referenzen definieren Anforderungen für Sicherheitsrichtlinien und -Verfahren. Navigieren zu **Konfigurations-Compliance** > **Autoritative Quellen** Zum Anzeigen der autoritativen Quellen.

Assets

Wenn Vulnerability Response Integration with Palo Alto Prisma Cloud Ist installiert, die geplante Aufgabe *`Prisma Alerts Integration`*Erfasst die warnungsbezogenen Informationen im Modul oder in der Tabelle „erkannte Elemente“. Sie können diese geplante Aufgabe anzeigen, indem Sie zu navigieren **Prisma-Cloud-Integration** > **Integrationen**an.

Die Integration von Prisma-Warnungen importiert zusätzliche Informationstypen, z. B. Ressourcen-Tags und Cloud-Attribute, die in Tabellen gespeichert sind. Diese Informationen werden im Formular „erkannte Elemente“ angezeigt.

- Host-Tags: Eine Ressource kann mehrere Tags haben. Die Host-Tags sind im Schlüssel-Wert-Paarformat verfügbar. Beispielsweise ist das Betriebssystem Windows 10 und die Java-Version 1,8.
- Cloud-Attribute für Assets: Die folgenden Cloud-Attribute sind verfügbar:
  - Cloud-Account: Stellt die Account-ID aus der Integration bereit. Die Informationen werden aus der Tabelle „Cloud-Accounts“ [sn_sec_cmn_Cloud_Account.LIST] ausgefüllt.
  - Cloud-Region: Gibt den Standort an, an dem die Ressource gehostet wurde. Die Informationen werden aus der Tabelle „Cloud-Regionen“ [sn_sec_cmn_Region.LIST] ausgefüllt.
  - Cloud-Ressourcentyp: Stellt Informationen zum Typ der Ressource bereit, z. B. ob es sich um eine virtuelle Maschine oder eine Datenbankinstanz handelt usw. Die Informationen werden aus der Tabelle „Cloud-Ressourcentyp“ [sn_sec_cmn_Cloud_resource_type.LIST] ausgefüllt.
  - Cloud-Service Provider: Stellt Informationen zum Cloud-Service Provider bereit, unabhängig davon, ob es sich um Amazon Web Services (AWS), Oracle Cloud usw. handelt. Die Informationen werden aus der Tabelle „Cloud-Service Provider“ [sn_sec_cmn_Cloud_Service_Provider.LIST] ausgefüllt.
  - Cloud-Account-Gruppen: Stellt Informationen zu den Account-Gruppen bereit. Die Informationen werden aus der Tabelle „Cloud-Account-Gruppen“ [sn_vul_prismacloud_Account_Group.list] ausgefüllt.

Hinweis:
Das Attribut „Cloud-Account-Gruppen“ ist nur für Prisma verfügbar.

CI-Suchregeln

Die CI-Suchregeln des Basissystems sind für Ressourcen-ID, Name und S3-Bucket verfügbar. Weitere Informationen zu den CI-Suchregeln finden Sie unter CI-Suchregeln für Microsoft Defender for Cloud Integration Für Security Operations Und Palo Alto Prisma Cloud.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prisma-Cloud-REST-Nachrichten

Prisma-REST-Nachrichten werden verwendet, um Aufrufe an die Prisma Application Programming Interface (API) zum Abrufen der Compliance-Daten zu tätigen.

Die folgenden REST-Nachrichten werden mit dem Basissystem geliefert.

Prisma-Cloud-Integrationen

Alle Prisma Cloud-Integrationen verwenden das JSON Web Token (JWT) für Authentifizierung und Autorisierung.

REST-Nachricht für Prisma-Anmeldung

Endpunkt	Beschreibung	Methode	Textkörper	API-Dokumentationslink
/Login	Ruft das JWT-Token zur Verwendung in allen nachfolgenden Integrationen ab.	*POST*	{ "username": <<access key id >>, "password": <<secret access key>>}	https://pan.dev/prisma-cloud/api/cspm/app-login/

REST-Nachricht für Prisma-Aktualisierungstoken

Endpunkt	Beschreibung	Methode	Textkörper	API-Dokumentationslink
/Auth_Token/extend	Verlängert das JWT-Token automatisch nach Ablauf. Die Standarddauer für den Token-Ablauf beträgt 60 Minuten.	*GET*	NA	https://pan.dev/prisma-cloud/api/cspm/extend-session/

REST-Nachricht der Prisma-Richtlinie

Endpunkt	Beschreibung	Methode	Textkörper	API-Dokumentationslink
/V2/Policy	Ruft alle Richtliniendaten aus Prisma ab.	*GET*	NA	https://pan.dev/prisma-cloud/api/cspm/get-policies/

REST-Nachricht für Prisma-Warnung

Endpunkt	Beschreibung	Methode	Textkörper	API-Dokumentationslink
/V2/Alert	Ruft alle Warnungen aus Prisma ab.	*POST*	{ "detailed": "false", "filters": [{ "name": "timeRange.type", "operator": "=", "value": "ALERT_STATUS_UPDATED"	https://pan.dev/prisma-cloud/api/cspm/post-alerts/

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachricht für Prisma-Warnung (Fortsetzung)

Endpunkt	Beschreibung	Methode	Textkörper	API-Dokumentationslink

			}
			],
			"sortBy": [
			"resource.id"
			],
			"pageToken": "",
			"offset": 0,
			"limit": 2000,
			"timeRange": {
			"type": "absolute",
			"value": {
			"startTime": <<Import since at integration level>>,
			"endTime": << Current integration run time>>
			}
			}
			}	

Für die Integration von Prisma-Verständniswarnungen müssen die Filter im obigen POST-Text wie folgt ersetzt werden:

```
"filters": [
{
            "name": "alert.status",
            "operator": "=",
            "value": "open"
        },
        {
            "name": "alert.status",
            "operator": "=",
            "value": "dismissed"
        },
        {
            "name": "alert.status",
            "operator": "=",
            "value": "snoozed"
        },
        {
            "name": "alert.status",
            "operator": "=",
            "value": "pending_resolution"
        },
        {
            "name": "timeRange.type",
            "operator": "=",
            "value": "ALERT_UPDATED"
        }

  ],
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration von Konfigurations-Compliance in Qualys

Die Qualys Richtlinien-Compliance erfasst die Daten und sendet sie automatisch an Qualys Anwendung, die die Informationen kontinuierlich analysiert und korreliert. Es lässt sich problemlos als integrieren Qualys Integration für Security Operations, um Konfigurationsergebnisse CIs und Business-Services zuzuordnen, um die Auswirkung und Priorität potenzieller Fehlkonfigurationen zu bestimmen.

Wenn Sie mehrere Bereitstellungen von haben Qualys Cloud Platform Anwendung können Sie für jede Bereitstellung eine Integration hinzufügen. Assets, die durch mehrere Drittanbieterbereitstellungen identifiziert werden, und ihre Schwachstellen werden konsolidiert und mit Ihrer CMDB abgeglichen. Diese Konsolidierung erfolgt auch dann, wenn sich Scanprozesse zwischen mehreren Bereitstellungen überschneiden. Daten, die aus jeder Bereitstellung stammen, werden identifiziert und in einer einzigen Instanz von verfügbar gemacht Vulnerability Response.

Hinweis:
Sie können die ursprüngliche Schwachstellenintegration nicht löschen, aber deaktivieren. Integrationen, die aus inaktiven Vorlagen erstellt wurden, sind standardmäßig deaktiviert.

Host-Tags

Alle Host-Tags werden als Teil von importiert Qualys Integration der Hostliste. Host-Tags werden hauptsächlich zum Filtern verwendet Vulnerability Response Regeln für Zuweisungs- und Korrekturaufgaben. Sie werden im Formular „erkanntes Element“ angezeigt.

Hinweis:
Die Qualys Die Integration der Host-Liste sollte vor dem Erstellen der Zuweisungs- oder Korrekturaufgabenregeln in ausgeführt werden Vulnerability Response Damit alle Tags in den Regeln vorhanden sein können und bevor angreifbare Elemente importiert und gruppiert werden.

- Beim Tag-Speicher wird die Groß-/Kleinschreibung nicht beachtet. Wenn ein **San Diego** Tag wird erstellt, dann ein **SAN DIEGO** Tag kann nicht in der Host-Tag-Tabelle gespeichert werden. „San Diego“ und „SAN DIEGO“ werden als dasselbe Host-Tag betrachtet. Das Tag, das importiert wurde, gewinnt zuerst.
- Die Verwendung von Host-Tags als Gruppenschlüssel in einer Regel für Korrekturaufgaben kann zu unerwarteten Ergebnissen führen. Host-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Host-Tags werden von der globalen Systemeigenschaft gesteuert **sn_vul.Import_Host_Tags** . Diese Eigenschaft ist standardmäßig auf „wahr“ festgelegt. Durch das Deaktivieren von Tags werden sie für alle Instanzen deaktiviert.

Host-Tags (auch als Asset-Tags bezeichnet) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Host-Assets Tags zuweisen. Beim Starten von Scans können Sie dann Tags auswählen, die den Hosts zugeordnet sind, die Sie scannen möchten. Mit dem Modul Host-Tags können Sie Host-Tag-Daten aus herunterladen Qualys Zu Ihrer Instanz auf einer geplanten Basis.

Zuordnen eines Tests zu seiner Testgruppe

Um das Feld Testgruppe in einem Testformular auszufüllen, aktivieren Sie *sn_vulc.add_policy_as_key*Systemeigenschaft. Weitere Informationen darüber, wie ein Test seiner Testgruppe zugeordnet ist, über die Auswirkungen der Aktivierung dieser Systemeigenschaft und über Nachanforderungen finden Sie unter KB1644268 artikel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung:
Sie können nicht deaktivieren `sn_vulc.add_policy_as_key`Systemeigenschaft, sobald sie aktiviert ist. Überprüfen Sie daher den Abschnitt „Auswirkung“ in KB1644268 artikel, bevor Sie diese Systemeigenschaft aktivieren.

Wenn Sie diese Systemeigenschaft aktivieren, wird nach der nächsten Erfassung die aktiviert **Testgruppe** Das Feld wird der Testtabelle hinzugefügt und füllt die Testgruppe aus, zu der ein Test gehört. Daher können Sie ganz einfach:

- Identifizieren Sie die Testgruppe, zu der ein Testergebnis gehört, durch Dot-Walking von Test zu Testgruppe.
- Unterscheiden Sie Testdatensätze mit derselben Test-ID, die verschiedenen Testgruppen zugeordnet sind.

Integration Qualys Mit ServiceNow® Konfigurations-Compliance Anwendung

Wenn Qualys Vulnerability Integration Ist bereits auf Ihrem System installiert, und Ihre API-Anmeldeinformationen unterscheiden sich von denen, für die Sie verwenden möchten Konfigurations-Compliance, Wechseln Sie zu Setup-Assistent (in Vulnerability Response) Und weisen Sie sie jedem zu **Qualys-PC** Integration.

Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Primäre Integrationen** Und bearbeiten Sie **Qualys-API-Anmeldeinformationen** Feld unter **Qualys-REST-Details** Registerkarte.

Konfigurieren Sie die PCRS-Parameter

Ab v12.6.3 von Qualys Integration for Security Operations, Können Sie verwenden Qualys PCRS-Richtlinie Host-Integration und Qualys PCRS-Testergebnisintegration zum Importieren von Testergebnissen mit neuen Sätzen von Qualys APIs. Diese Integrationen benötigen eine Gateway-URL, aus der Informationen abgerufen werden können Qualys.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie installieren Qualys Integration for Security Operations Für Vulnerability Response, Sie können konfigurieren **Gateway_url** Für die neuen PCRS-Integrationen in Konfigurations-Compliance. Weitere Informationen zur Suche nach der Gateway-URL für Ihre API-URL finden Sie unter Identifizieren Sie Ihre Qualys-Plattform .

Die Gateway-URL muss in hinzugefügt werden ServiceNow Instanz.

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Integrationsinstanzen**an.

   Hinweis:
   Stellen Sie sicher, dass der Bereich, in dem Sie sich befinden, Qualys für Security Operations ist.

2. Öffnen Sie die Instanz, die von den PCRS-Integrationen verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Fügen Sie auf der Registerkarte Integrationsinstanzparameter die Gateway-url für hinzu **Gateway_url** Konfiguration.

Hinweis:
Die Integration von Qualys PCRS-Testergebnissen ist von der Qualys PCRS-Richtlinienhostintegration abhängig. Wenn Sie also die Qualys PCRS-Testergebnisse der Integration zurückdatieren, müssen Sie sie möglicherweise erneut in derselben Reihenfolge ausführen.

Mit Qualys Integration for Security Operations installierte Komponenten

Die folgenden Rollen, geplanten Aufgaben und Tabellen werden mit Qualys Integration for Security Operations installiert.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Zeigen Sie gefilterte Listen für Komponenten an, die mit einer Anwendung installiert wurden

Filtern Sie die Tabelle „Anwendungsdateien“ so, dass nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert werden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, sollte installiert werden, damit ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Führen Sie die folgenden Schritte aus, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im Filternavigator ein **sys_metadata.list** Um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) aus, und wählen Sie, **Anwendung** > **ist** Gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**an.
3. Wählen Sie im Bedingungsgenerator aus, um einen zweiten Filter hinzuzufügen **UND** , Und wählen Sie dann aus, **Klasse** > **ist ein** Und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle** , **Geplante Aufgabe** , Oder **Tabelle** .
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die von Ihnen ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul_qualys.read	Hat Lesezugriff auf Qualys Vulnerability Integration Datensätze.	
sn_vul_qualys.user	Anwender für Qualys Vulnerability Integration. Kann Datensätze lesen und schreiben	sn_vul_qualys.read

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_vul_qualys.admin	Administrator für Qualys Vulnerability Integration. Sie können beispielsweise Startdaten der Integration ändern und einige erweiterte Konfigurationseinstellungen vornehmen.	• sn_vul_qualys.user • sn_vul.vulnerability_analyst
sn_vul.configure_qualys_Integration	Kann konfigurieren Qualys Vulnerability Integration	sn_vul_qualys.admin

Geplante Aufgaben Installiert

Regelmäßige Aufgabe	Beschreibung
Qualys PC-Richtlinien	Ruft Richtlinien von ab Qualys. Die Ausgabe wird in der Tabelle „sn_vulc_Policy“ gespeichert. Die in dieser Integration verwendete API unterstützt keine Paginierung, daher werden alle Richtlinien auf einer einzigen Seite heruntergeladen.
Qualys PC-Richtliniendetail	Ruft die vollständigen Richtliniendetails ab, z. B. Technologien und Abschnitte.
Qualys PC-Steuerungen	Ruft Informationen zu Compliance-Steuerungen für verschiedene Steuerungs-IDs ab Qualys.
Qualys PC-Ergebnisse	Ruft Compliance-Statusdatensätze von ab Qualys. Die Ausgabe dieser Integration ist Testergebnisse. Standardmäßig werden die Parameterdetails übergeben, um Hostinformationen, Daten/Uhrzeiten der letzten Scans, Steuerungs-ID und Nachweisinformationen zu importieren.
Qualys Umfassende PC-Ergebnisse	Ruft Compliance-Statusdatensätze von ab Qualys Basierend auf dem letzten Bewertungsdatum für die nicht bestandenen Testergebnisse. Dieser Auftrag wird einmal pro Woche ausgeführt. Die Ausgabe dieser Integration ist Testergebnisse. Standardmäßig werden die Parameterdetails übergeben, um die Hostinformationen, Daten/Uhrzeiten der letzten Scans, die Steuerungs-ID und Nachweisinformationen zu importieren.
Qualys PCRS-Richtlinienhostintegration	Ruft Ab Hostdaten Von Qualys Und verarbeitet sie in Ihrer Instanz. Die Ausgabe dieser Integration ist Richtlinienhost-IDs. Die Qualys Host Daten Wird in diese Integration importiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
	Hinweis: • Diese geplante Aufgabe wird nur angezeigt, wenn Konfigurations-Compliance Ist installiert. • Konfigurieren Sie die Instanzparameter Gateway_url und pcrs_page_size, bevor Sie diese Integration ausführen. Diese beiden Integrationen sind OOB inaktiv. Wenn Sie eine dieser Integrationen aktivieren, werden die PC-Ergebnisintegrationen deaktiviert. Diese beiden Integrationen werden basierend auf den neuen Streaming-APIs von Qualys hinzugefügt.
Qualys Integration von PCRS-Testergebnissen	Ruft die Testergebnisse für jede Host-ID ab. Diese Integration verwendet den Parameter Startzeit auf der Registerkarte Integrationsdetails. **Hinweis:** • Diese geplante Aufgabe wird nur angezeigt, wenn Konfigurations-Compliance Ist installiert. • Konfigurieren Sie die Instanzparameter Gateway_url und pcrs_page_size, bevor Sie diese Integration ausführen. • Wenn Sie die Integration manuell ausführen möchten, führen Sie aus Qualys Integration von PCRS-Testergebnissen nach Qualys PC-Richtlinien, Qualys PC-Richtliniendetail und Qualys PCRS-Richtlinienhostintegration.

Hinweis:
Die Qualys PCRS-Richtlinienhost und Qualys PCRS-Testergebnisintegrationen sind standardmäßig inaktiv. Diese beiden Integrationen basieren auf den neuen Streaming-APIs von Qualys. Wenn Sie eine dieser Integrationen aktivieren, wird die PC-Ergebnisintegration deaktiviert und umgekehrt.

Tabellen Installiert

Tabelle	Beschreibung
Qualys PC-Ergebnisimport sn_vul_qualys_pc_result_Import	Tabelle, die die Importsatzzeile erweitert. Die Transformation der Feldzuordnungen wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Richtlinien-Host-ID sn_vul_qualys_Policy_Host_ID	Tabelle, in der die Zuordnung zwischen der Richtlinie und dem Host gespeichert wird, für den diese Richtlinie gescannt wurde. Diese Tabelle wird in der neuen verwendet Qualys PCRS-Integration. **Hinweis:** Diese Tabelle wird nur angezeigt, wenn Konfigurations-Compliance Ist installiert.
Qualys Import des PCRS-Richtlinienhosts sn_vul_qualys_pcrs_Policy_Host_Import	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet. **Hinweis:** Diese Tabelle wird nur angezeigt, wenn Konfigurations-Compliance Ist installiert.
Qualys PC-Richtlinienimport sn_vul_qualys_pc_Policy_Import	Tabelle, die die Importsatzzeile erweitert. Die Feldzuordnungstransformation wird übersprungen, und der Antwortanhang wird direkt mit dem onComplete-Skript verarbeitet.

Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartition-Bezeichner für die Qualys-Integration

Erstellen Sie eindeutige Konfigurationselemente (Configuration Items, CIs) für Assets in Ihrer Umgebung, die IP-Adressen teilen. Identifizieren Sie die eindeutigen Assets in Ihrer Umgebung, und aktualisieren Sie die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen automatisch, um Ihnen weitere Details zu Ihren Schwachstellen zu geben.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig in Vulnerability Response Anwendung. Eine Möglichkeit, Ihre Assets zu identifizieren, ist die IP-Adresse. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, werden jedoch als ein CI in Ihrer CMDB gespeichert.

Wie in den folgenden Tabellen dargestellt, können mehrere Assets (CI) in Ihrer Umgebung IP-Adressen teilen, haben jedoch eindeutige Netzwerk- und Repository-IDs. Standardmäßig werden diese Assets jedoch als einzelnes CI identifiziert und gespeichert (CI 1) Während der IP-Adresssuche.

Standard-IP-Suche und CI-Erstellung

Quelle	IP-Adresse	NETWORK_ID	Konfigurationselement
Qualys Vulnerability Integration: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	03712	CI 1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-IP-Suche und CI-Erstellung (Fortsetzung)

Quelle	IP-Adresse	NETWORK_ID	Konfigurationselement
	123.12.12.141	03713	CI 1

Quelle	IP-Adresse	REPOSITORY_ID	Konfigurationselement
Qualys Vulnerability Integration: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Sie können einzelne CIs für Assets mit derselben IP-Adresse erstellen, um sie als eindeutige Assets zu identifizieren. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartition-Bezeichners [Network_Partition_Identifier], indem Sie die geplante Aufgabe ausführen. *`Update existing discovered items with network partition identifier`*.

Diese geplante Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Integrationen von Assets und behobenen und offenen Schwachstellen für Qualys Vulnerability Integration Im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.

Wenn diese geplante Aufgabe aktiviert ist, wird der Netzwerkpartition-Bezeichner [Network_Partition_Identifier] zu vorhandenen CI-Datensätzen aus importierten Daten hinzugefügt. Vorhandene CIs, die von der IRE erstellt wurden, werden ebenfalls aktualisiert. Die geplante Aufgabe erstellt auch CIs, die ab dem nächsten Import den Netzwerkpartition-Bezeichner enthalten. Alternativ können Sie den Auftrag bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

Ab v14.0 von Vulnerability Response Und v12.1 des Qualys Vulnerability Integration Schwachstellenintegration, die CMDB-CI-Klassenmodelle (1,0.21.) Wird unterstützt. Die Klassenmodelle haben den Netzwerkpartition-Bezeichner [Network_Partition_Identifier] in den Identifizierungsregeln für Identification and Reconciliation (IRE).

Option	Beschreibung
Führen Sie die geplanten Aufgaben bei Bedarf aus.	Aktualisieren Sie Ihre vorhandenen erkannten Elemente. CIs für Ihre vorhandenen Qualys Vulnerability Integration Daten werden erstellt oder aktualisiert, um die Granularität des Netzwerkpartition-Bezeichners einzubeziehen. Erkannte Elemente, angreifbare Elemente und Erkennungsdatensätze werden alle mit den neuen CIs aktualisiert.
Warten Sie auf Importe neuer Daten aus den Integrationen mit den nächsten geplanten Aufgaben.	Erstellen Sie CIs für jedes neue Asset mithilfe des Netzwerkpartition-Bezeichners, beginnend mit der nächsten geplanten Aufgabe. CI-, angreifbare Element- und Erkennungsdatensätze werden alle aktualisiert, um die neue Granularität einzubeziehen.

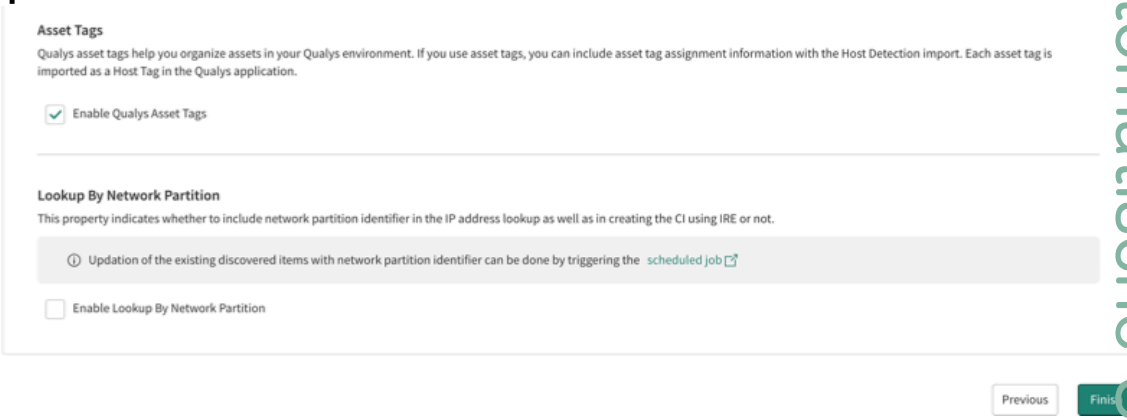
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Option	Beschreibung
	Neue CIs werden erstellt, wenn keine genaue Übereinstimmung gefunden wird.

Prozedur

1. Navigieren zu **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**an.
2. Wählen Sie Aus Qualys Vulnerability Integration.
3. **Bearbeiten** Die erforderliche Integration.
4. Wählen **Hosterkennungskonfiguration**an.
5. Wählen **Suche nach Netzwerkpartition aktivieren** Kontrollkästchen in **Suche nach Netzwerkpartition**



Abschnitt.

6. Klicken Sie auf **Fertigstellen**.

Netzwerkpartition-Bezeichner „NETWORK_ID“ und „REPOSITORY_ID“, die in der IP-Suche und CI-Erstellung enthalten sind

Quelle	IP-Adresse	NETWORK_ID	CI für Assets ohne Netzwerkpartition-Bezeichner	CIs-Assets mit Netzwerkpartition-Bezeichner
Qualys Vulnerability Integration: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

Quelle	IP-Adresse	REPOSITORY_ID	CI für Assets ohne Netzwerkpartition-Bezeichner	CIs-Assets mit Netzwerkpartition-Bezeichner
Qualys: Assets und Integrationen	123.12.12.141	12	CI 1	CI 1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quelle	IP-Adresse	REPOSITORY_ID	CI für Assets ohne Netzwerkpartition-Bezeichner	CIs-Assets mit Netzwerkpartition-Bezeichner
behobener und offener Schwachstellen				
	123.12.12.141	13	CI 1	CI 2

Die Suchregeln für die IP-Adresse und die CI-Identifizierung der unvollständigen IP-Adresse enthalten automatisch das Attribut des Netzwerkpartition-Bezeichners für einen Datenimport aus den Integrationen „Assets“ und „Feste und offene Schwachstellen“ für Qualys Vulnerability Integration.

Nachdem Sie die geplante Aufgabe aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartition-Bezeichner enthalten, indem Sie geplante Aufgaben bei Bedarf starten. Die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen werden automatisch aktualisiert.

Legen Sie zusätzliche Filterparameter für fest Qualys Importe

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit an Qualys Vulnerability Integration Damit Sie die Schwachstellendaten weiter verfeinern können, die Sie mit dem importieren Qualys Integrationen.

Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, damit Sie nur bestimmte Schwachstellendetails überprüfen können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die nach bestimmten IPs oder IP-Bereichen gefiltert sind. Oder Sie möchten nur Computer importieren, die sich in Ihrem Bereich befinden, z. B. nur Computer in Ihrem Unternehmensnetzwerk, die keine externen Geräte sind.

Um Ihnen beim Sammeln dieser Daten zu helfen, können Sie hinzufügen Qualys Parameter, die Ihnen beim Importieren der spezifischen Schwachstellendetails helfen, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder -Codierung können Sie mit dieser Funktion Ihre HTTP-Anforderungsinformationen anpassen Qualys Parameter in Ihrem ServiceNow AI Platform. Sie ändern oder fügen diese Werte Ihrem HTTP-Methodendatensatz unter der REST-Methode für die unterstützte hinzu Qualys Integrationen von Qualys Vulnerability Integration.

Erforderliche Rolle: sn_vul.Vulnerability_admin

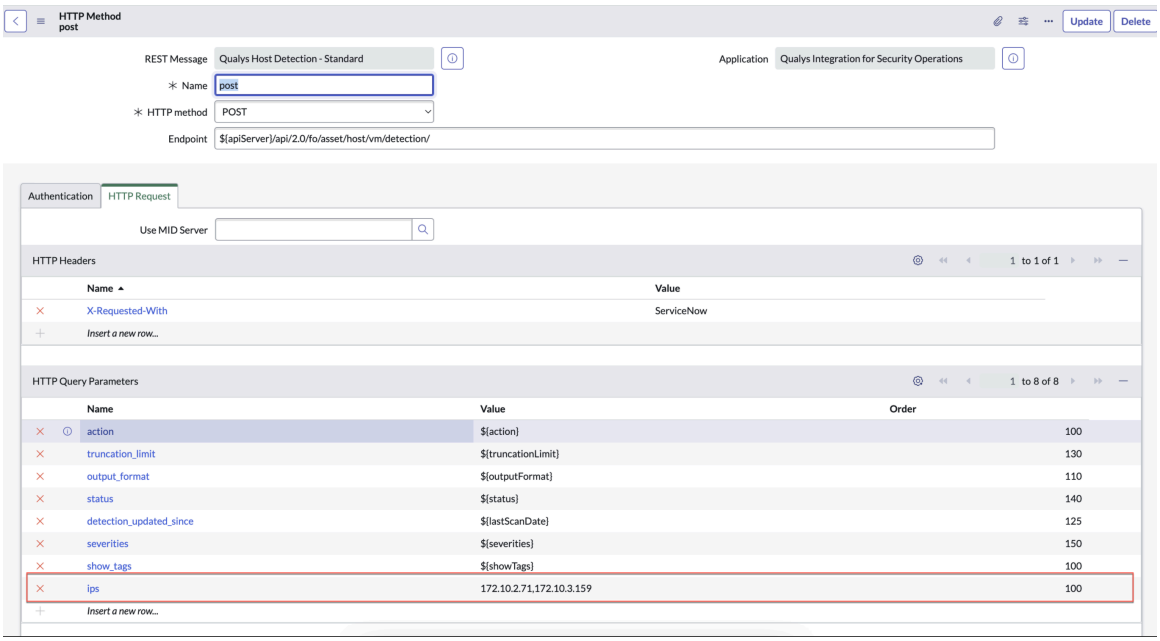
Prozedur

1. Suchen Sie die von unterstützten Parameter Qualys Produkt auf der Entwicklerwebsite, das Sie für Ihre Filterung verwenden möchten.
   Parameter und Werte, die Sie aus eingeben Qualys Produkte werden nur auf Integrationsinstanzebene in unterstützt ServiceNow AI Platform. Alle Qualys Integrationen unterstützen das Filtern mithilfe von Abfrageparametern.
2. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**an.
3. Auf der Qualys Integrationslistenseite klicken Sie auf den Datensatz für die Integration, die Sie öffnen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Mit Qualys Registerkarte „REST-Details“ ausgewählt. Suchen und klicken Sie auf das Informationssymbol (I) für die REST-Methode gefolgt von **Öffnen Sie Den Datensatz** Zum Öffnen des HTTP-Methodendatensatzes.
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Fügen Sie in den HTTP-Abfrageparametern für den Anforderungstext die Werte hinzu, die Sie von erhalten haben Qualys Entwickler-Site.

   In der folgenden Abbildung als Beispiel der Parameter, der nur bestimmte IP-Adressen/-Bereiche erfasst, *ips={value}*Wurde hinzugefügt. In diesem Fall **Wert** Ist mindestens eine von Ihnen angegebene IPs/Bereiche. Mehrere Einträge sind durch Kommas getrennt, 172.10.2,71, 172.10.3.159 , Und ein Bereich wird mit einem Bindestrich angegeben, 10.10.10.1-10.10.10.100 . Weitere Informationen finden Sie unter Qualys Entwickler-Website für weitere Informationen.



   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie unter Qualys Dokumentation für weitere Informationen zur Trennung der einzelnen Werte.

   Hinweis:
   Sie sollten sich Ihrer API-Anforderungen bewusst sein. Möglicherweise müssen Sie diese API-Eigenschaften den Abfrageparametern oder dem Textkörper hinzufügen.

   Einige andere Parameter, die Sie möglicherweise in nützlich finden Qualys Entwickler-Site:

   - *ag_ids* – IDs der abzurufenden Asset-Gruppenliste. Dieser Parameter stellt sicher, dass nur Computer in Ihrem Bereich einbezogen werden.
   - *qids* – Dieser Parameter beschränkt die Ergebnisse auf bestimmte Schwachstellen (QID in der Tabelle „Drittpartei-Eintrag“). Diese Einstellung verhindert, dass Ihr System mit Informationsdatensätzen überflutet wird.
7. Klicken Sie auf **Aktualisieren**.

Granularität von Qualys-Testergebnissen konfigurieren

Konfigurieren Sie die Granularität der Qualys-Testergebnisse, um sicherzustellen, dass das System Ergebnisse auf einer detaillierteren Ebene basierend auf Ihren ausgewählten Konfigurationsschlüsseln importiert. Zusätzlich zu den Standardschlüsseln können Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zusätzliche Schlüssel basierend auf Ihren Anforderungen konfigurieren, um die Granularität zu erhöhen. Granulare Importe ermöglichen es Teams, ihre jeweiligen Assets unabhängig zu verwalten und zu verhindern, dass Daten überschrieben werden, wenn mehrere Datensätze gemeinsame Bezeichner verwenden.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin

Prozedur

1. Navigieren zu **Alle** > **Granularität von Qualys-Testergebnissen konfigurieren**an.
2. Bestätigen Sie im Formular „Schlüsselkonfiguration“ Folgendes:
   - **Quellintegration** Ist `Qualys Cloud-Plattform` .
   - **Tabelle** Ist auf festgelegt `Testergebnis` .
3. In **Konfigurationsschlüssel** Wählen Sie das Feld aus, für das Sie eindeutige Testergebnisse erstellen möchten.
   Wählen Sie beispielsweise aus `instance`Erstellt eindeutige Testergebnisse für jede Instanz in einer Datenbank.

   Hinweis:
   Verwenden Sie diese Funktion mit Vorsicht. Jeder zusätzliche Konfigurationsschlüssel erhöht die Integrationszeit. Um eine optimale Leistung zu gewährleisten, beschränken Sie Ihre Verwendung auf nicht mehr als drei zusätzliche Schlüssel.

4. Geben Sie Ein *Wahr* Neben `instance`Zum Aktivieren der Granularität, oder *Falsch* Um sie zu deaktivieren.
5. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.

[store-future: BEGIN review]

Ordnen Sie ein zu Qualys Testergebnis mit seiner Testgruppe in Konfigurations-Compliance

Erstellen Sie Tests und Testergebnisse in Konfigurations-Compliance Mit Zuordnung zu Qualys Testgruppe.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Qualys Verwaltet eine Standardbibliothek von Richtlinien und Steuerungen und ermöglicht gleichzeitig die Erstellung anwenderdefinierter Richtlinien und Steuerungen. Diese Steuerungen können einer Richtlinie zugeordnet werden und bieten ein umfassendes Framework für die Bewertung der Sicherheitslage von IT-Assets. Bei Auswertung für ein Asset wird die Richtlinie generiert Qualys Haltungen, die in in in Testergebnisse umgewandelt werden Konfigurations-Compliance. Eine Steuerung, die einem zugeordnet ist Qualys Richtlinie unterscheidet sich von der Standardsteuerung in Qualys Bibliothek. Dies ermöglicht die Flexibilität, Attribute wie Relevanz, Status (aktiv oder inaktiv) und Technologie für die Steuerung auf Richtlinienebene zu definieren.

Zuvor in Konfigurations-Compliance, Die Tests werden normalerweise für erstellt Qualys Bibliothekssteuerungen anstelle der Steuerungen, die dem zugeordnet sind Qualys Richtlinien. Die Testergebnisse beziehen sich auf die Tests ohne Testgruppenzuordnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daher gibt es möglicherweise weniger Testergebnisse in Konfigurations-Compliance Im Vergleich zu Positionen in Qualys.

Zum Erstellen von Tests und Testergebnissen in Konfigurations-Compliance Mit der Zuordnung zur Testgruppe wurde auf Testebene eine neue Spalte „Testgruppe“ hinzugefügt. Die Ausfüllung dieser Spalte wird von der Systemeigenschaft gesteuert *sn_vulc.add_policy_as_key*. Sobald diese Systemeigenschaft aktiviert ist, Konfigurations-Compliance Erstellt Tests für Bibliothekssteuerungen (Testgruppe ist leer) und Steuerungen, die den Richtlinien zugeordnet sind (Testgruppe ist Richtlinien-ID). Die Testergebnisse beziehen sich auf die Tests mit Richtlinienzuordnung.

So stellen Sie sicher, dass alle Testergebnisse mit der Testgruppenzuordnung zu den neuen Tests migriert werden:

Prozedur

1. Aktivieren Sie die Systemeigenschaft sn_vulc.add_Policy_as_key.
   a. Geben Sie im Filternavigator sys_properties.list ein, um die Liste der Systemeigenschaften für Ihre Instanz anzuzeigen.
   b. Suchen Sie nach sn_vulc.Add_Policy_as_key Systemeigenschaft und öffnen Sie sie.
   c. Wählen Sie den Link in der Warnmeldung aus, um die Systemeigenschaft zu bearbeiten.
   d. Legen Sie fest **Wert** Feld bis Wahr Zum Aktivieren von sn_vulc.Add_Policy_as_key Systemeigenschaft.
2. **Wahlweise:** Für Kunden mit vorhandenen Daten (Tests und Testergebnisse) in Configuration Compliance:
   a. Löschen Sie **Startzeit** Feld für sn_vulc.Add_Policy_as_key Systemeigenschaft.
   b. Führen Sie die Integrationen in der folgenden Reihenfolge aus:
      - Qualys-PC-Richtlinien
      - Qualys-PC-Steuerungen
      - Qualys-PC-Richtliniendetail
      - Integration von Qualys PC-Ergebnissen/Qualys PCRS-Testergebnissen
3. Überprüfen Sie Folgendes:
   - Überprüfen Sie nach der Ausführung von Qualys PC-Richtlinien, ob neue Tests mit Testgruppenreferenz erstellt werden.
   - Stellen Sie nach der Ausführung der Qualys PC Results/Qualys PCRS Test Results Integration sicher, dass alle Testergebnisse auf einen neuen Test mit einer ausgefüllten Testgruppenreferenz verweisen.

Ergebnisse

- Neue Tests werden mit einem Verweis auf die Testgruppe erstellt. Die zugehörige Liste „Testgruppe“ ist für die neuen Tests nicht ausgefüllt. Die neuen Tests basieren auf den Steuerungen, die Richtlinien in zugeordnet sind Qualys, Die die Relevanz, den Status (aktiv oder inaktiv) und die Technologie der Steuerung auf Richtlinienebene widerspiegeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Test ohne Testgruppenreferenz spiegelt die Steuerungen in wider Qualys Bibliothek.
- Alle Testergebnisse verweisen auf die neuen Tests mit Testgruppenzuordnung. Eine Testgruppe für ein Testergebnis kann durch Dot-Walking zum zugehörigen Test identifiziert werden.

[End]

Wird Aufgelöst Qualys Schwachstellenintegrationsprobleme

Einige häufig aufgetretene Probleme werden zusammen mit Problemumgehungen besprochen.

Anhänge werden nach dem Import nicht angezeigt

Wenn Anhänge nach Importen von Drittparteien-Integrationen nicht wie erwartet für Datenquellen oder in einem Security Incident angezeigt werden, überprüfen Sie Ihre IP-Einschränkungen.

IP-Zugriffsbeschränkungen können verhindern, dass Anhänge angezeigt werden, es sei denn, Sie sind über eine sichere IP angemeldet. Da bei jedem Import ein neuer Anhang hinzugefügt wird, kann dies zu Duplikaten führen, die Sie entfernen müssen.

Wenn Sie beispielsweise eine Host-Importintegration einer Drittpartei ausführen und keine Anhänge in Ihren Datenquellen sehen, überprüfen Sie Ihre IP-Einschränkungen, und fügen Sie der Safe-Liste Anwender hinzu, bevor Sie den Import durchführen.

Ändern Sie Transformationszuordnungen

Transformationszuordnungen werden mit Basiskonfigurationen bereitgestellt und sind normalerweise ausreichend. Sie können Transformationszuordnungen je nach Bedarf Ihrer Organisation ändern.

Vorbereitungen

Erforderliche Rolle: sn_vul_qualys.admin + Import_admin

Prozedur

1. Navigieren zu **Alle** > **System-Importsätze** > **Administration** > **Transformationszuordnungen** Zum Anzeigen der REST-Nachrichten.
2. Filtern Sie die resultierende Liste nach Anwendung, und beschränken Sie die Liste auf **Qualys-Schwachstellenintegration** Anwendung.
3. Ändern Sie die Transformationszuordnungen entsprechend den Kundenanforderungen.

   Details zu den von der Qualys-API bereitgestellten Daten finden Sie unter Qualys-API-Dokumentation .

Überprüfen Sie die Größe der XML-Anhangseigenschaft

Überprüft, ob die XML-Anhangseigenschaft für große Dateien ausreicht.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Import Export**an.
2. Scrollen Sie nach unten zu **Importeigenschaften** > **XML-Format** Unten auf der Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Ändern Sie bei Bedarf den Wert in 250, und klicken Sie auf **Speichern** .

Zugehörige Informationen

Verfügbare Systemeigenschaften

Einschränkungen des Datenabrufs

Standardmäßig gibt es keine Einschränkungen beim Abrufen von Daten aus Qualys. Viele Datensätze können auf Schwachstellen mit niedrigem Schweregrad zurückzuführen sein, die ein Kunde nicht mit seinem Vulnerability Response-Prozess beheben möchte. Durch das Aktualisieren der entsprechenden REST-Nachrichten-/Methodenparameter kann dieses Verhalten geändert werden.

Die für dieses Update verantwortliche REST-Nachricht/Methode ist **Qualys-Host-Erkennung: Standard/Post** . Um die Werte zu aktualisieren, fügen Sie der Post-Methode einen neuen HTTP-Abfrageparameter mit den folgenden Werten hinzu:

- Name: Schweregrade
- Wert: 3-5 (oder ein beliebiger geeigneter Schweregrad)

Qualys Knowledge Base-Integration schlägt fehl

Lösen Qualys Fehler bei der Knowledge Base-Integration durch Reduzierung der von empfangenen Nutzlastanhangsgröße Qualys Bis zum angegebenen Grenzwert.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Stellen Sie sicher, dass die Nutzlast-Anhangsgröße innerhalb des angegebenen Grenzwerts liegt.
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**an.
   b. Wählen Sie aus **Integrationsinstanzparameter** Registerkarte.
   c. Wählen Sie Aus **max_delta_days** Und ändern Sie den Standardwert in 3.
2. Wenn die Integration weiterhin fehlschlägt, führen Sie die folgenden Schritte aus:
   a. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Primäre Integrationen**an.
   b. Wählen Sie Aus **Qualys Knowledge Base** .
   c. Wählen Sie aus **Integrationsdetails** Registerkarte.
   d. In **Startzeit** Wählen Sie das aktuelle Datum aus, um die Ausführung der Ausführung für diesen Tag zu überspringen.
   e. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Integrationsinstanzen**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Wählen Sie aus **Integrationsinstanzparameter** Registerkarte.

g. Wählen Sie Aus **kb_Backfill_Full_Import** Und ändern Sie den Standardwert in „wahr“.

Ergebnisse

Durch die Ausführung der Qualys Knowledge Base Backfill-Integration werden alle Drittparteieinträge (TPEs) im System aktualisiert. Während die Qualys Host Detection-Integration einen Platzhaltereintrag erstellt, aktualisiert die Qualys Knowledge Base Backfill-Integration ihn.

Qualys Statusdiagramm der Integrationsausführung

Die Qualys Das Modul „Integrationsausführungsstatus“ ist eine grafische Ansicht des Status von Qualys Integrationsausführungen.

Um den Status von Integrationsausführungen anzuzeigen, navigieren Sie zu **Qualys Schwachstellenintegration** > **Status der Integrationsausführung**an.

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard ist in der neuen Experience-UI verfügbar.

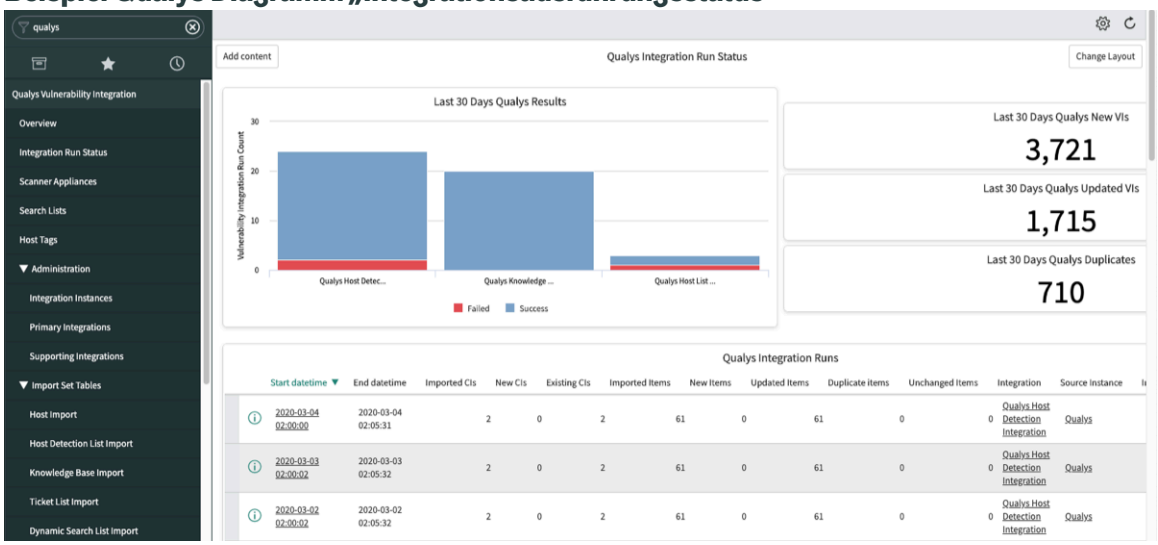
Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Zeigen Sie im Diagramm auf ein beliebiges Teil (Balken, Kreis, Datenpunkt usw.), um allgemeine Daten anzuzeigen, die für dieses Teil spezifisch sind. Wenn Sie auf einen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Die Qualys Status der Integrationsausführung zeigt den Ausführungsstatus der Schwachstellenintegration für die letzten 30 Tage an. Die aktualisierte VIS-Anzahl von Qualys[qualys] gibt die Anzahl aller eindeutigen Erkennungen im selben Asset an. Das VI wird dann mit der neuen Erkennung aktualisiert.

Hinweis:
Die Anzahl der Ausführungen der Schwachstellenintegration wird nur für die Integrationen angezeigt, die auf den Status „aktiv“ gesetzt sind. Navigieren zu **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen** Und legen Sie den Status auf aktiv fest.

Beispiel Qualys Diagramm „Integrationsausführungsstatus“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Werte in der Spalte importierte Elemente stellen die Gesamtzahl der Datensätze dar Die aus einer Integrationsausführung erstellt wurden.
- In der Spalte neue Elemente wird die Anzahl der Datensätze angezeigt Die aus einer Integrationsausführung erstellt wurden.
- Die Spalte „doppelte Elemente“ ist nicht mehr ausgefüllt. Möglicherweise möchten Sie diese Spalte aus der Anzeige entfernen.
- In der Spalte „aktualisierte Elemente“ wird die Anzahl der Datensätze angezeigt Werden während einer Integrationsausführung aktualisiert. Dieser Wert ist nicht die Anzahl der eindeutigen Datensätze Die aktualisiert wurden. Wenn zum Beispiel ein Datensatz Wird während der Integrationsausführung zweimal aktualisiert, wird sie zweimal gezählt und als angezeigt 2 Aktualisierte Elemente.
- In der Spalte „unveränderte Elemente“ werden Datensätze angezeigt Während der Integrationsausführung gefunden, die bereits in der Datenbank vorhanden sind, aber nicht aktualisiert wurden, da sich keiner der relevanten Feldwerte geändert hatte.

Hinweis:
Integrationsausführungen mit null Ergebnissen für alle vier der folgenden Werte: **Neue CIs** , **Vorhandene CIs** , **Neue Elemente** , Und **Aktualisierte Elemente** Werden aus gefiltert **Qualys-Integration Wird Ausgeführt** Liste.

Qualys Statusdiagrammberichte der Integrationsausführung

Name	Beschreibung
Letzte 30 Tage Qualys Ergebnisse	Die Anzahl der für jede Integration abgeschlossenen Integrationsausführungen. Zeigt sowohl erfolgreiche als auch fehlgeschlagene Ausführungen an. In einer Balkenvisualisierung ausführen.
Letzte 30 Tage Qualys Neue VIS	Die Anzahl der neuen Datensätze In den letzten 30 Tagen importiert. Wird als Ganzzahl angezeigt.
Letzte 30 Tage Qualys Aktualisierte VIS	Die Anzahl der aktualisierten Datensätze In den letzten 30 Tagen importiert. Wird als Ganzzahl angezeigt.
Letzte 30 Tage Qualys Duplikate	Die Anzahl der doppelten Datensätze In den letzten 30 Tagen importiert. Wird als Ganzzahl angezeigt.
Qualys Integrationsausführungen	Die Datensätze der Integrationsausführung in einer Liste. **Hinweis:** **V16.1:** Um die Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit ServiceNow Erkennungsdaten in `sn_vul_detection`Tabelle. Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennung oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „bis datumsanzahl“ in der Instanz nach Abschluss der Integrationsausführung an.
Letzte 30 Tage Qualys Leistungsmetriken Der Erfassung Angreifbarer Elemente	Tägliche Leistungsmetriken für angreifbare Elemente im Vergleich zu den letzten 30 Tagen.
Letzte 30 Tage Qualys Leistungsdurchsatz Der	Täglicher Durchsatz der Erfassung angreifbarer Elemente, gemessen für Qualys Integration der Host-Erkennung für die letzten 30 Tage.

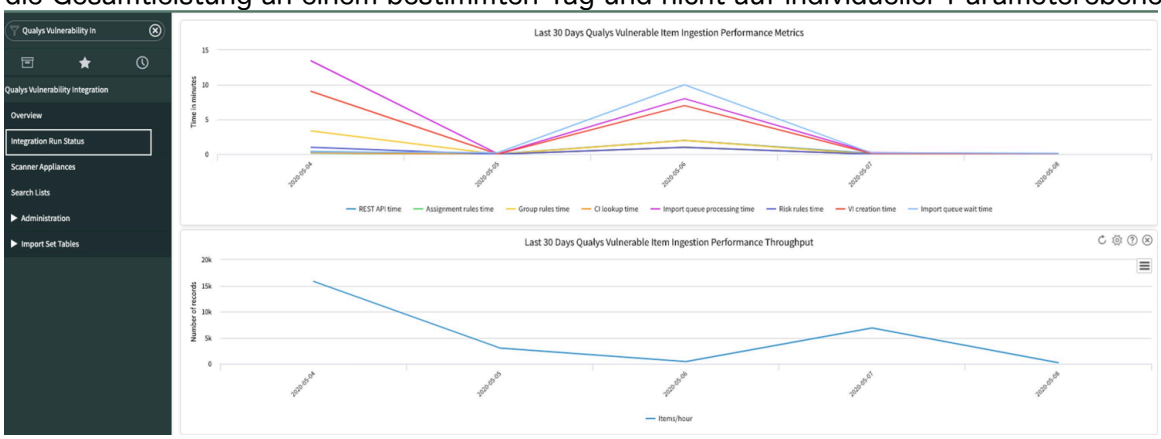
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Qualys Statusdiagrammberichte der Integrationsausführung (Fortsetzung)

Name	Beschreibung
Erfassung Angreifbarer Elemente	

Mehrere Faktoren können sich auf die Leistung der Integrationsausführung auswirken, z. B. die Datenmenge und die Zeit, die für die Verarbeitung dieser Daten benötigt wird. Zwei Diagramme vergleichen die Leistungsmetriken:

- Qualys Leistungsmetriken der Erfassung angreifbarer Elemente: Tägliche Leistungsmetriken für Zuweisungsregeln, Gruppenregeln, Risikoregeln, Warteschlangenwartezeit, Warteschlangenverarbeitungszeit, und andere Statistiken für angreifbare Elemente in den letzten 30 Tagen, um die Ursache für Leistungsabweichungen zu identifizieren. Die Leistung wird basierend auf der für jede Aktivität benötigten Zeit berechnet. Diese Parameter werden auf Ebene der Integrationsausführung berechnet und zugeordnet. Jeder Parameter ist zur einfachen Identifizierung farbcodiert.
- Qualys Leistungsdurchsatz der Erfassung angreifbarer Elemente: Vergleichen Sie den täglichen Erfassungsdurchsatz angreifbarer Elemente für Qualys Integration der Host-Erkennung. Der Durchsatz wird in Elementen pro Stunde gemessen. Dieser Bericht zeigt die Gesamtleistung an einem bestimmten Tag und nicht auf individueller Parameterebene.



Qualys-REST-Nachrichten

Qualys-REST-Nachrichten werden verwendet, um Anrufe an Qualys zu tätigen API Zum Abrufen der Compliance-Daten.

Die folgenden Rest-Nachrichten werden mit dem Basissystem geliefert.

REST-Nachricht für Qualys-PC-Richtlinien

Die REST-Nachricht Qualys PC-Richtlinien ruft Richtliniendaten von Qualys ab. Die Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die Anforderung an Qualys aus, Richtlinieninformationen abzurufen.

REST-Nachrichtenparameter für Qualys-PC-Richtlinien

Parametername	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachrichtenparameter für Qualys-PC-Richtlinien (Fortsetzung)

Parametername	Wert	Beschreibung
details	Alle	Gibt die Detailstufe an, die für abgerufene Richtlinien angezeigt wird. Ist es Sicher Zum Ändern gemäß Ihren Anforderungen.

REST-Nachricht für Qualys PC Controls

Die Rest-Nachricht Qualys PC Controls ruft Informationen zu Compliance-Steuerungen für verschiedene Steuerungs-IDs von Qualys ab.

Qualys PC steuert REST-Nachrichtenparameter

Parametername	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter.
details	Alle	Gibt die Detailstufe an, die für abgerufene Steuerungen angezeigt wird. Ist es Sicher Zum Ändern gemäß Ihren Anforderungen.

Qualys PC-Richtlinien – REST-Nachricht im Detail

Die REST-Nachricht Qualys PC-Richtliniendetail ruft die vollständigen Richtliniendetails ab, z. B. Technologien und Abschnitte.

Qualys-PC-Richtlinien – Details zu REST-Nachrichtenparametern

Parameter	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter.
Show_user_Controls	Boolean	• Legen Sie den Wert auf 1 fest, um anwenderdefinierte Steuerungen (UDCs) in die XML-Ausgabe aufzunehmen. • Wenn nicht angegeben, sind UDCs nicht enthalten. Dies ist ein optionaler Parameter. Ist es Sicher Zum Ändern gemäß Ihren Anforderungen.
Show_appAppendix	Boolean	(Optional) auf 1 festlegen, um den Abschnitt „Anhang“ in der XML-Ausgabe anzuzeigen. Wenn nicht angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachricht für Qualys-PC-Ergebnisse

Die Rest-Nachricht Qualys PC-Ergebnisse ruft Compliance-Statusdatensätze von Qualys ab.

REST-Nachrichtenparameter für Qualys-PC-Ergebnisse

Quellfeld	Wert	Beschreibung
Aktion	Liste	Gibt den Typ des angeforderten Vorgangs an. Erforderlicher Parameter. Änderungen werden nicht empfohlen.
Show_extended_evidence	Boolean	• Legen Sie diese Option auf 1 fest, um die erweiterten Nachweisinformationen in der Ausgabe anzuzeigen. • Legen Sie den Wert auf 0 fest, oder wenn nicht angegeben, werden die erweiterten Nachweisinformationen nicht in der Ausgabe angezeigt. **Hinweis:** • Sie können nicht angeben `Show_extended_evidence=1` In derselben Anforderung wie `Hide_evidence=1` . Dies führt zu einem Fehler. Der erweiterte Nachweis ist Teil der Nachweisdaten und wird nur angezeigt, wenn Nachweisdaten angezeigt werden. • Dieser Parameter ist nicht im Lieferumfang des Basissystems enthalten.
Ursache_des_Fehlers	Boolean	Wenn Sie „1“ bestehen, gibt Qualys die Fehlerursache zurück. Wenn Sie „0“ übergeben, gibt Qualys diese Attribute nicht zurück. **Hinweis:** Dieser Parameter ist nicht im Lieferumfang des Basissystems enthalten.
policy_id		Zeigt Datensätze mit Informationen zur Compliance-Situation für eine angegebene Richtlinie an. Eine gültige Richtlinien-ID ist erforderlich.
details	Alle	Gibt die Detailstufe an, die für angezeigt wird Haltungen Abgerufen. Es ist sicher, Änderungen gemäß Ihren Anforderungen vorzunehmen.
Show_Remediation_info		(Optional) auf 1 festlegen, um Korrekturinformationen in der XML- oder CSV-Ausgabe anzuzeigen. Standardmäßig enthält die Ausgabe keine Korrekturinformationen. Wenn nicht angegeben, sind die Korrekturinformationen nicht in der Ausgabe enthalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

REST-Nachricht der Qualys PCRS-Richtlinie Host-Integration

Die Qualys PCRS-Richtlinienhostintegration ruft Hostdaten von Qualys ab und verarbeitet sie in Ihrer Instanz.

REST-Nachrichtenparameter der Qualys-PCRS-Richtlinienhostintegration

Parametername	Wert	Beschreibung
policyId	${lastRunDatetime}	Richtlinien-IDs für die Compliance-Bewertung.

Integration von Qualys PCRS-Testergebnissen

Die Tabelle zeigt die gesendeten Anforderungsparameter.

REST-Nachrichtenparameter der Qualys PCRS-Testergebnisintegration

Parametername	Wert	Beschreibung
Nachweisangefordert	${lastRunDatetime}	• Der Standardwert ist 0, was angibt, dass Nachweisdaten für die Host-Situation nicht abgerufen werden. • Legen Sie den Wert auf 1 fest, um die Nachweisdaten abzurufen. **Hinweis:** Wenn Sie den Wert in 1 ändern, wird die Zeit erhöht, die zum Abrufen von Positionsdaten erforderlich ist.
Komprimierenangefordert		• Der Standardwert ist 1, was angibt, dass die Ausgabe komprimiert wird. • Legen Sie den Wert auf 0 fest, wenn die Daten nicht komprimiert werden sollen. **Hinweis:** Wenn die Daten nicht komprimiert werden, erhöht sich die Zeit, die zum Abrufen von Positionsdaten erforderlich ist.

Verständnis der Tenable-Schwachstellenintegration

Die Vulnerability Response Integration with Tenable Anwendung entwickelt von ServiceNow Engineering für die Tenable-Schwachstellenintegration verwendet Daten, die aus importiert wurden Tenable.io, Tenable.sc, Und Tenable.cs Produkte, mit denen Sie Schwachstellen für Ihre Assets priorisieren und beheben können. Die Anwendung ist mit einem separaten Abonnement als verfügbar ServiceNow® Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

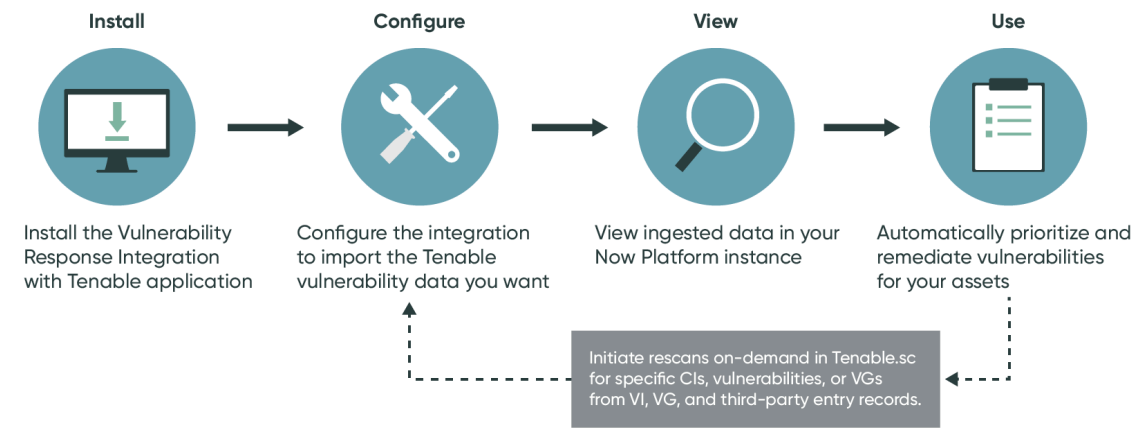
Die Tenable-Schwachstellenintegration verwendet drei Tenable-Integrationen, Tenable.io, Tenable.sc Und Tenable.cs, Um Scannerdaten von Drittparteien zu Ihren Assets und Schwachstellen zu importieren. Die Vulnerability Response Integration with Tenable Die Anwendung unterstützt Tenable.sc Produkt ab Version 5,13 und Tenable.cs Produkt ab Version 5,0.1.

- Tenable.io Ist eine cloudbasierte Enterprise-Integration.
- Tenable.sc Ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn der verwendet wird Tenable.sc Produkt und Ihr ServiceNow AI Platform Instanz befindet sich in derselben Umgebung.
- Wenn Tenable.sc Produkt und Ihr ServiceNow AI Platform Instanz befindet sich nicht in derselben Umgebung, Sie müssen einen MID-Server verwenden.
- Tenable.cs Ist eine cloudbasierte Enterprise-Integration.

Die Vulnerability Response Integration with Tenable Anwendung ist auf verfügbar ServiceNow Store Mit einem separaten Abonnement.

Für Listen und Beschreibungen der Integrationen in Tenable Vulnerability Integration, Siehe Tenable.io Integrationen mit Vulnerability Response Und Konfigurations-Compliance Anwendungen Und Tenable.sc Integrationen mit Vulnerability Response Anwendung.

Tenable-Schwachstellen-Integration



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfügbare Versionen für Yokohama

Freigabeversion	Release-Hinweise
Vulnerability Response Integration with Tenable V3.13.1, v4.1, v5.0.1	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema

Begriffe und wichtige Funktionen der Integrationen

Angreifbare Elemente und Schwachstellen

Ein angreifbares Element wird in erstellt ServiceNow AI Platform Instanz, wenn:

- Eine importierte Schwachstelle von einem Scanner eines Drittanbieters wird mit einem vorhandenen Asset (einem Konfigurationselement in Ihrem) abgeglichen CMDB). Das Tenable-Produkt bezieht sich auf diese Übereinstimmungen als **Schwachstellen** .
- Eine importierte Schwachstelle von einem Scanner eines Drittanbieters wird nicht mit einem vorhandenen Asset in Ihrem abgeglichen CMDB. In diesem Fall wird auch ein nicht übereinstimmendes CI zusammen mit einem angreifbaren Element erstellt.

  Für nicht abgeglichene CIs können Sie auch die Identification and Reconciliation Engine (IRE) verwenden, um CIs in zwei neuen Klassen zu erstellen, wenn ein vorhandenes CI nicht mit einem Host abgeglichen werden kann. Andernfalls werden nicht abgeglichene CIs in den nicht abgeglichenen CI-Klassen erstellt. Weitere Informationen finden Sie unter CIs für werden erstellt Vulnerability Response Verwenden der Identifizierungs- und Abgleichsmodul.

Einträge und Plugins von Drittanbietern für Schwachstellen

Einträge für Schwachstellen von Drittparteien werden aus Scannern von Drittparteien importiert und in der Tabelle „Schwachstelleneinträge von Drittparteien“ in aufgeführt ServiceNow AI Platform Instanz. Ab v24.0 von Vulnerability Response, Die Spalte Software in der Tabelle „Drittanbieter-Schwachstelleneinträge“ füllt die CPEs (Common Platform Enumerations, CPEs) aus, die einer Drittpartei zugeordnet sind Eintrag . Einträge von Drittpartei-Schwachstellen aus Tenable werden in erfasst Vulnerability Response Und mit vorhandenen Assets abgeglichen, die in aufgeführt sind CMDB. Tenable bezieht sich auf Einträge von Drittpartei-Schwachstellen als **Plugins** .

Konfigurationselement bzw. Configuration Item (CI)

Konfigurationselemente sind die vorhandenen Assets, die in aufgeführt sind CMDB.

Erkanntes Element

Assets, die aus dem Import von Tenable-Assets erfasst werden, werden mit vorhandenen Konfigurationselementen in abgeglichen CMDB. Importierte Assets werden aktualisiert.

Wenn keine Übereinstimmung gefunden wird, wird ein CI in der nicht abgeglichenen CI-Klasse von erstellt CMDB. Wenn das Plugin „CMDB CI-Klassenmodelle“ aktiviert ist, erstellt die Identification and Reconciliation Engine (IRE) CIs mit neuen Klassen. Weitere Informationen finden Sie unter CIs für werden erstellt Vulnerability Response Verwenden der Identifizierungs- und Abgleichsmodul.
Wenn das ursprüngliche, nicht abgeglichene CI neu klassifiziert wird, werden erkannte Elementdatensätze entsprechend dem Status aktualisiert. Erkannte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elemente geben Ihnen Einblick, wie Assets identifiziert und CIs in zugeordnet werden CMDB.

CI-Suchregeln

Wenn Daten aus einer Drittpartei-Integration importiert werden, verwendet Vulnerability Response automatisch Host-(Asset-)Daten, um nach Übereinstimmungen in der Configuration Management-Datenbank zu suchen (CMDB). CI-Suchregeln werden verwendet, um CIs zu identifizieren und sie VI-Datensätzen hinzuzufügen, wenn Vits erstellt werden, um Sie bei der Korrektur zu unterstützen.

Erneut scannen und Korrekturscan

Sie können einen gezielten erneuten Scan-Befehl für ein bestimmtes Konfigurationselement, eine Korrekturaufgabe oder einen Drittparteieintrag direkt aus den Datensätzen für angreifbare Elemente, Korrekturaufgaben und Schwachstelleneinträge von Drittparteien in Ihrem initiieren ServiceNow AI Platform Instanz. Tenable bezieht sich auf diesen erneuten Scan als **Korrekturscan** .

Schließen Sie ältere VIS automatisch

Mit dem Modul „veraltete angreifbare Elemente automatisch schließen“ in Ihrem ServiceNow AI Platform, Sie können ältere, veraltete angreifbare Elemente (VI) bereinigen, die kürzlich von Ihren Drittpartei-Integrationen nicht gefunden wurden. Diese VIS werden nach verschoben **Geschlossen** Hilft Ihnen, die Anzahl der aktiven angreifbaren Elemente und Korrekturaufgaben zu reduzieren und Assets in abzugleichen CMDB. Sie können alle Integrationen mit verwenden Vulnerability Response Integration with Tenable Dient zum automatischen Schließen veralteter VIS.

Instanz

Dieser Begriff bezieht sich auf ein eindeutiges Vorkommen von ServiceNow AI Platform® Anwendung.

Integration

Eine -Integration ist eine produktspezifische Referenz zu einer -Integration, z. B. Tenable.io Assets-Integration oder Tenable.sc Plugin-Integration. Dies sind die separaten Integrationen, die zu bestimmten Tenable-Produkten in der Tenable-Schwachstellenintegration in Ihrer Instanz gehören.

Integrationsinstanz

Dieser Begriff bezieht sich auf die separaten Tenable-Integrationen, die nach aufgeführt sind Tenable.io Und Tenable.sc Produkte.

Bereitstellung

Wenn eine Integration mehrere Quellen unterstützt, wird eine einzelne, eindeutige Integration als Bereitstellung Ihrer Integration bezeichnet. Der Begriff wird verwendet, um auf die Integrationen und Produkte in Ihrer Umgebung zu verweisen. Beispielsweise können Sie mehrere Bereitstellungen verschiedener Integrationen von haben Tenable.io Und Tenable.sc Produkte in Ihrer Umgebung.

Die Tenable.io, Tenable.sc, Und Tenable.cs Integrationen umfassen auch die folgenden wichtigen Funktionen:

- Konfigurationsbewertungsergebnisse, d. h. Testergebnisse zusammen mit Richtlinien, Konfigurationstests (Steuerungen) und Bezugsvermerke mit autorisierenden Quellen können in importiert werden Konfigurations-Compliance Anwendung mit Tenable.io Produkt. Siehe Tenable.io Integrationen mit Vulnerability Response Und Konfigurations-Compliance Anwendungen Und Konfigurations-Compliance erkunden Um weitere Informationen zur Funktionsweise dieser Integration mit zu erhalten Konfigurations-Compliance Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ab v2.1 des Tenable Vulnerability Integration, Erstellen Sie eindeutige Konfigurationselemente (Configuration Items, CIs), die verschiedene Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung enthalten, die dieselbe IP-Adresse verwenden. Identifizieren Sie die eindeutigen Assets in Ihrer Umgebung, und aktualisieren Sie die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen, um Ihnen weitere Details zu Ihren Schwachstellen zu geben.
- Sie können planen, wann die Aufträge für alle ausgeführt werden sollen Tenable.io, Tenable.sc Und Tenable.cs Integrationen. Sie können geplante Aufgaben auch bei Bedarf manuell ausführen.
- Für Asset-Importe mit Tenable.io, Sie können Asset-Tags aktivieren, um die in aufgeführten Assets zu organisieren und nachzuverfolgen CMDB In Tenable.io Umgebung.
- Die Tenable.io, Tenable.sc Und Tenable.cs Integrationen ermöglichen es Ihnen, CI-Suchregeln zu konfigurieren, um zu definieren, wie Asset-Daten aus Drittparteiquellen zur Identifizierung von Konfigurationselementen (Configuration Items, CIs) in verwendet werden ServiceNow AI Platform CMDB.
- Die Tenable.io, Tenable.sc Und Tenable.cs Mit Integrationen können Sie Importfilter für den Schwachstellenimport festlegen, sodass Sie nur die gewünschten Schwachstellen aus Tenable importieren. Für Tenable.io, Sie haben die Möglichkeit zum Importieren **Behoben** Schwachstellen aus Tenable mit dem Schwachstellenimport.
- Für Tenable.sc, Sie haben die Möglichkeit, bei Bedarf erneut scans direkt aus einem angreifbaren Element, einer Korrekturaufgabe und Drittpartei-Eintragsdatensätzen in zu initiieren ServiceNow AI Platform Instanz. Wenn VIS auf geändert wurden **Geschlossen/ Behoben** Wurden in Ihrer Instanz jedoch noch nicht aktualisiert, können Sie überprüfen, ob Schwachstellen in bestimmten Konfigurationselementen behoben wurden. Weitere Informationen finden Sie unter Initiieren Sie einen erneuten Scan für Tenable.sc Integration.

Die folgenden Abschnitte enthalten weitere Details zu den Tenable-Integrationen.

Erforderliche ServiceNow AI Platform-Rollen

Die Integrationsaufgaben erfordern die folgenden Rollen in Ihrem ServiceNow AI Platform Instanz.

Administrator

Der Systemadministrator verwendet den Setup-Assistenten, um zu installieren Vulnerability Response Integration with Tenable Anwendung. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.Vulnerability_admin) und andere Rollen im Setup-Assistenten zu.

sn_vul.vulnerability_admin

Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der Tenable-Integrationen im Setup-Assistenten ab. Diese Rolle hat vollständigen Zugriff auf Vulnerability Response(VR)-Anwendung und ihre Datensätze. Der Schwachstellenadministrator konfiguriert alle VR-Anwendungen und -Regeln für installierte Drittanbieterintegrationen.

sn_vul_Tenable.configure_Integration

Diese Rolle enthält die granulare Rolle sn_vul_Tenable.read_Integration, und Anwender mit dieser Rolle können konfigurieren Vulnerability Response Integration with Tenable Anwendung.

sn_vul_Tenable.read_Integration

Benutzer mit diesen Rollen können Datensätze von anzeigen (lesen), aber nicht bearbeiten Vulnerability Response Integration with Tenable Anwendung.

Vulnerability Response-Gruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Anwender, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen sn_vul.read_all und sn_vul.Remediation_owner automatisch.

Angreifbare Elemente

Angreifbare Elemente werden gemäß den Regeln für Korrekturaufgaben in Korrekturaufgaben gruppiert und basierend auf Ihren Zuweisungsregeln zur Korrektur zugewiesen. Weitere Informationen finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben und Vulnerability Response Übersicht über Zuweisungsregeln.

Suchregeln für Konfigurationselement (Configuration Item, CI)

CI-Suchregeln identifizieren CIs und bestimmen, wann sie einem angreifbaren Element hinzugefügt werden sollen. Weitere Informationen zur Funktionsweise von CI-Suchregeln finden Sie unter CI-Suchregeln zum Identifizieren von Konfigurationselementen aus Vulnerability Response Integrationen von Schwachstellen von Drittparteien.

Hinweis:
Regeln können nach dem Entfernen nicht wiederhergestellt werden. Anstatt vorhandene Regeln zu entfernen, deaktivieren Sie sie beim Erstellen von Regeln.

Folgendes Tenable.io Suchregeln sind im Lieferumfang des Basissystems enthalten.

- MAC_ADDRESS
- FQDN
- NetBIOS
- HostName
- DNS
- IP

Hinweis:
Die Tenable.io CI-Suchregeln priorisieren und füllen die nicht leeren Netzwerkschnittstellenwerte (FDQN, IPV4 und MacAddress) gegenüber den regulären FDQN-, IPV4- und MacAddress-Werten für ein erkanntes Element aus. Wenn diese Netzwerkschnittstellenwerte leer sind, werden die regulären FDQN-, IPV4- und MacAddress-Werte für ein erkanntes Element ausgefüllt.

Folgendes Tenable.sc Suchregeln sind im Lieferumfang des Basissystems enthalten.

- MAC_ADDRESS
- FQDN
- NetBIOS
- IP

Hinweis:
Für ein Asset werden mehrere Werte für ip_address, mac_address, fqdns und Network_Interfaces verwendet. Alle Werte werden in CI-Suchregeln für den Abgleich berücksichtigt. Alle Werte werden verwendet, um mehrere Netzwerkadapter mit IRE zu erstellen.

Die Tenable.cs Suchregel „Cloud-Ressourcen-ID“ wird mit dem Basissystem geliefert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zum Konfigurieren der Kategorisierung nicht übereinstimmender Cloud-Ressourcen in Ihrer bevorzugten CI-Klasse finden Sie unter CI-Klasse für nicht abgeglichene Cloud-Assets wird aktualisiert.

Neue Eigenschaften zum Ignorieren von IP-Adressen

In Tenable.io, Es sind zwei Eigenschaften verfügbar, wenn Sie mehrere IP-Adressen oder mehrere Mac-Adressen als Teil Ihrer CI-Suchregeln ignorieren möchten:

IgnoreIPAddress

Eine Liste von IP-Adressen, die für die CI-Suche und die CI-Erstellung ignoriert werden sollen.

IgnoreMacAddress

Eine Liste von MAC-Adressen, die bei der CI-Suche oder CI-Erstellung ignoriert werden sollen.

Erkannte Elemente

Dieses Modul listet Konfigurationselemente auf, die während des Imports aus den Tenable-Integrationen für angreifbare Elemente und den Tenable-Asset-Integrationen erkannt wurden.

Hinweis:
Der Standardfilter für diese Liste ist auf festgelegt Nicht Abgeglichen . Sie können alle erkannten Elemente aus einem Import anzeigen, indem Sie den Filter entfernen.

Weitere Informationen zum Modul „erkannte Elemente“ finden Sie unter Erkannte Elemente.

Asset-Tags

Asset-Tags (auch als Host-Tags bezeichnet) werden zum Organisieren und Nachverfolgen der Assets in Ihrer Organisation verwendet. Sie können Ihren Assets Tags zuweisen. Beim Starten der Scans können Sie dann Tags auswählen, die den Assets zugeordnet sind, die Sie scannen möchten. Mit dem Modul „Asset-Tags“ können Sie Asset-Tag-Daten aus herunterladen Tenable.io Zu Ihrer Instanz auf einer geplanten Basis. Asset-Daten, die Asset-Tags enthalten, werden aus abgerufen Tenable.io Und mit transformiert Tenable.io-Asset-Transformation Integrationstransformationszuordnungen.

Alle Asset-Tags werden als Teil von importiert Tenable.io Asset-Integration. Asset-Tags werden zum Filtern verwendet Vulnerability Response Zuweisungsregeln und Regeln für Korrekturaufgaben. Die Tags werden im Formular „erkanntes Element“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Führen Sie aus Tenable.io Asset-Integration vor dem Erstellen Vulnerability Response Zuweisungsregeln oder Regeln für Korrekturaufgaben in Vulnerability Response Anwendung, damit alle Tags für diese Regeln verfügbar sind, bevor angreifbare Elemente importiert und gruppiert werden. Beachten Sie auch die folgenden Punkte zu Tags:

- Beim Tag-Speicher wird die Groß-/Kleinschreibung nicht beachtet. Wenn Sie beispielsweise ein Tag erstellen, um Assets an Ihrem San Diego-Standort zu beschreiben, und erstellen Sie `San Diego` Tag, können Sie nicht auch erstellen `SAN DIEGO` Kennzeichnen und in der Asset-Tag-Tabelle speichern. `San Diego` Und `SAN DIEGO` Werden vom System als dasselbe Asset-Tag betrachtet. Welches Tag zuerst importiert wird, ist das Tag, das gespeichert und in Zukunft erkannt wird.
- Die Verwendung von Asset-Tags als Gruppenschlüssel in einer Korrekturaufgabenregel kann zu unerwarteten Ergebnissen führen. Asset-Tags sind nur zur Verwendung im Bedingungsgenerator vorgesehen.
- Asset-Tags werden von der globalen Systemeigenschaft sn_vul.Import_Asset_Tags gesteuert. Diese Eigenschaft ist auf festgelegt `Wahr` Standardmäßig. Durch das Deaktivieren von Tags werden sie für alle deaktiviert ServiceNow AI Platform® Instanzen.

Datenabruffilter

Mit den Einstellungen für den Datenabruf können Sie insbesondere den Typ und den Umfang der Daten bestimmen, die Sie aus der Tenable-Anwendung in importieren möchten ServiceNow AI Platform® Instanz. Eine Liste der am häufigsten verwendeten Einstellungen finden Sie unter Datenabrufeinstellungen für die Tenable-Schwachstellenintegration.

Schwachstellenprioritätsbewertung (VPR)

Die Vulnerability Priority Rating (VPR) ist ein Attribut aus dem Tenable-Produkt, das importiert und mit einem neuen Standardrisikorechner in verwendet wird Vulnerability Response. Die Tenable-Risikoregel wird mit installiert Vulnerability Response Integration with Tenable Anwendung als Teil des Standardrisikorechners in den Schwachstellenrechnern von Vulnerability Response.

Diese Risikoregel ist standardmäßig inaktiv.

Durch Aktivieren der Tenable-Risikorechnerregel werden die importierten VPR-Werte zur Berechnung der Risikopunktzahl für angreifbare Elemente verwendet. Die Standardgewichtungsverteilung für diesen Risikorechner: VPR = 70 %, Asset = 15 % und Geschäftsrelevanz = 15 %. Das Aktivieren dieser Tenable-Risikorechner-Regel kann sich auf Ihre Leistung der Datenerfassung auswirken. Weitere Informationen zu finden Vulnerability Response Rechner und die Tenable-Risikorechnerregel finden Sie unter Vulnerability Response Rechner und Regeln für Schwachstellenrechner.

Installation und Konfiguration

Nachdem Sie heruntergeladen haben Vulnerability Response Integration with Tenable Von ServiceNow® Store, Installation und Konfiguration werden vom Setup-Assistenten in unterstützt Vulnerability Response. Weitere Informationen finden Sie unter Wird Konfiguriert Vulnerability Response Mit dem Setup-Assistenten.

Tenable.io Integrationen mit Vulnerability Response Und Konfigurations-Compliance Anwendungen

Die Tenable.io Integrationen in Vulnerability Response Integration with Tenable-Anwendungen sind in verfügbar Vulnerability Response Und Konfigurations-Compliance Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste von Tenable.io Integrationen

Mehrere Quellen werden für alle unterstützt Tenable.io Und Tenable.sc Integrationen. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in hinzufügen und bereitstellen Vulnerability Response. Sie installieren und konfigurieren auch Vulnerability Response Integration with Tenable Anwendung aus Setup-Assistent.

Tenable.io Ist eine cloudbasierte Enterprise-Integration. In der folgenden Tabelle finden Sie die Namen und Beschreibungen der unterstützten Integrationen für Tenable.io Produkt.

Die Tenable.io Integration von Compliance-Ergebnissen und der Tenable.io Compliance-Ergebnisse – Backfill-Integration ist standardmäßig inaktiv.

So aktivieren Sie sie:

1. Navigieren zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**an.
2. Klicken Sie in der Liste Tenable-Integrationen auf einen Integrationsnamen, um den Datensatz zu öffnen, und wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren. Möglicherweise möchten Sie die Zeitplaneinstellungen in ihren Standardwerten belassen, damit diese Integrationen beginnen.

Tenable.io-Integrationen

Integration	Beschreibung
Tenable.io Asset-Integration	• Ruft alle Asset-Daten, einschließlich Asset-Tags, aus dem ab Tenable.io Produkt und verarbeitet es in Ihrer Instanz. • Ab v3.0, wenn Tenable.io Die Integration von Compliance-Ergebnissen ist aktiviert. Sie können sichere Konfigurationsbewertungsdaten zusammen mit importierten Asset-Daten importieren. Diese Daten können Ihnen helfen, die konfigurationsbezogenen Schwachstellen in Ihren Assets zu identifizieren und darauf zu reagieren. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die dieselbe IP-Adresse haben. • Koordiniert die REST-Nachrichtenaufrufe an die Asset-API. • Die Ausgabe dieser Integration ist erkannte Elemente. • Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_Chunk_Status] gespeichert. Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. • Ab v2.2, `Last Scan Time`Wird nur für Assets mit Schwachstellen importiert und aktualisiert.
Tenable.io Integration Von Compliance-Ergebnissen	• Ab v3.0 können Sie mit importierten sicheren Konfigurationsbewertungsdaten aus der Compliance-Ergebnisintegration zusammen mit importierten Daten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	aus der Asset-Integration die konfigurationsbezogenen Schwachstellen in Ihren Assets identifizieren und darauf reagieren. • Wenn diese Option aktiviert ist, werden allgemeine sichere Konfigurationsbewertungsdaten abgerufen und in verarbeitet ServiceNow AI Platform Instanz. Importierte Daten umfassen Testergebnisse zusammen mit Richtlinien, Konfigurationstests (Steuerungen) und Bezugsvermerke mit autorisierenden Quellen. • Bewertungsdaten für fehlende Assets oder Assets ohne Asset-IDs werden nicht importiert. • Wenn ein Testergebnis importiert wird und das entsprechende Asset nicht in Ihrer Instanz abgeglichen werden kann, wird das Testergebnis ignoriert, und die ID für das fehlende Asset wird in einem temporären Datensatz in der Tabelle [sn_vul_tenable_missing_Asset] gespeichert. • Der Gesamtwert der ignorierten (fehlenden) Assets wird in aufgeführt **Ignorierte CIs** Feld auf der **Konfiguration** Registerkarte im Datensatz der Integrationsausführung für diese Integration.
Tenable.io Integration Der Compliance-Ergebnisse Im Backfill	• Wenn diese Option aktiviert ist, wird diese Integration automatisch ausgeführt, nachdem die Asset-Integration als Teil einer verketteten Integrationsausführung erfolgreich abgeschlossen wurde. Diese Integration stimmt Konfigurationsbewertungsdaten mit fehlenden Assets ab, die in der Tabelle [sn_vul_TENABLE_missing_Asset] aufgeführt sind. • Importiert bis zu 200 Asset-IDs für alle fehlenden Assets, die in der Instanz erkannt oder vorhanden sind, nachdem der Import der Asset-Integration erfolgreich abgeschlossen wurde. • Entfernt die temporären Datensätze aus der Tabelle [sn_vul_TENABLE_missing_Asset], wenn Assets mit entsprechenden Konfigurationsbewertungsdaten abgeglichen werden können.
Tenable.io Integration Von Anmeldeinformationen Scannen	• Diese Integration ruft die in konfigurierten Scan-Anmeldeinformationen ab Tenable.io. • Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API. • Die Ausgabe dieser Integration ist Scan-Anmeldeinformationen, die in der Tabelle [sn_vul_Tenable_Scan_credential] ausgefüllt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	• Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scananforderungen von initiiert werden ServiceNow AI Platform. • Diese Integration wird wöchentlich ausgeführt.
Tenable.io Vorlagenintegration	Ein Vorlagendatensatz wird an gesendet Tenable.io Während des erneuten Scans. Diese Integration ruft verfügbare ab Tenable.io Anmeldeinformationen, die für erneute Scans verwendet werden sollen. Anmeldeinformationen sind instanzspezifisch, und ein einzelner Vorlagendatensatz wird importiert und vorübergehend sicher in der Tabelle [sn_vul_Tenable_io_template] gespeichert.
Tenable.io Plugin-Integration	• Ruft die Plugin-Daten aus dem ab Tenable.io Produkt. Abgerufene Daten basieren auf dem Datum, an dem die Plugins zuletzt von einem aktualisiert wurden Tenable.io Integrationsausführung. • Dieser Import stellt sicher, dass die Tenable.io Bezeichner (zehn IDs) sind aktuell. • Koordiniert die REST-Nachrichtenaufrufe an die Plugin-API. • Die Ausgabe dieser Integration ist Schwachstellen von Drittparteien.
Tenable.io Integration Behobener Schwachstellen	• Ruft Schwachstellendaten basierend auf Schweregradfiltern aus ab Tenable.io Produkt und verarbeitet es in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich in befinden **Öffnen** Und **Erneut Geöffnet** status, da diese Datensätze eine Korrektur erfordern. Vorhandene angreifbare Elemente werden von Vulnerability Response aktualisiert, wenn Erkennungen sind **Behoben** , Aber angreifbare Elemente werden für nicht erstellt **Behoben** Erkennungen standardmäßig, da Tenable berücksichtigt **Behoben** Schwachstellen **Gemindert** . • Wenn die Kennzeichnung **Erstellen Sie Zeiten für Schwachstellen für Erkennungen behobener Schwachstellen** Ist im Setup-Assistenten aktiviert, neue VIS werden in erstellt **Behoben** geben sie den status an, damit Sie Einblick in die Erkennungen haben, die sie erstellt haben. Da VIS für erstellt werden **Behoben** Erkennungen, die in Ihrer Instanz nicht bereits vorhanden sind, können sich negativ auf Ihre Importleistung auswirken. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, damit dies möglich ist **Behoben**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	Erkennungen aktualisieren nur die status vorhandener angreifbarer Elemente. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die dieselbe IP-Adresse haben. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration ist **Geschlossen/Behoben** Angreifbare Elemente (VIS). Außerdem werden Assets und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind. • Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_Chunk_Status] gespeichert. Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. Diese Integrationsausführung ist geplant. Es handelt sich um eine verkettete Integration, d. h. nach erfolgreichem Abschluss einer Ausführung wird die unten beschriebene Integration offener Schwachstellen ausgelöst. Ab Tenable v3.3 können Sie die folgenden Informationen für die Ausführungen der Schwachstellenintegration anzeigen: • **Blöcke insgesamt:** Gesamtanzahl der Blöcke, die von Tenable generiert werden • **Verfügbare Blöcke:** Anzahl der Blöcke, die für heruntergeladen werden können ServiceNow
Tenable.io Integration Offener Schwachstellen	• Diese Integration wird nach erfolgreichem Abschluss von ausgelöst Tenable.io Integration Behobener Schwachstellen. • Ruft Schwachstellendaten basierend auf den Schweregradfiltern aus ab Tenable.io Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die dieselbe IP-Adresse haben. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration ist **Neu/Erneut Geöffnet** Angreifbare Elemente (VIS). Außerdem werden Konfigurationselemente und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind. Tenable berücksichtigt aktive Schwachstellen **Kumulativ** (Aktuell).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io-Integrationen (Fortsetzung)

Integration	Beschreibung
	• Daten werden in Blöcken importiert und in der Tabelle [sn_vul_tenable_Chunk_Status] gespeichert. Tabellenbereinigung entfernt gespeicherte Daten automatisch nach 30 Tagen aus dieser Tabelle. Ab Tenable v3.3 können Sie die folgenden Informationen für die Ausführungen der Schwachstellenintegration anzeigen: • **Blöcke insgesamt:** Gesamtanzahl der Blöcke, die von Tenable generiert werden • **Verfügbare Blöcke:** Anzahl der Blöcke, die für heruntergeladen werden können ServiceNow
Tenable.io/Scan-Metadatenintegration	Diese Integration ruft Metadaten vom Endpunkt „/Scans“ ab. Ruft Scan-Informationen basierend auf der Last_schedule_ID aus den vorhandenen Asset-Daten in ab Tenable.io. Die Integration des Endpunkts „/scans“ aus Tenable.io Umfasst die folgenden Implementierungsschritte: • **Tabellenerstellung** : Eine neue anwenderdefinierte Tabelle, **sn_vul_Tenable_Scan** , Wird erstellt, um Scan-Metadaten zu speichern, die aus abgerufen wurden Tenable.io/Scans-Endpunkt. Dies umfasst Details wie Scan-ID, Name, Status, Startzeit, Endzeit, und Scan-Typ. • **Datenzuordnung** : Ein Referenzfeld wird zwischen erkannten Elementen (Konfigurationselementen oder Schwachstellen) und dem entsprechenden aktuellen Scan-Datensatz in eingerichtet **sn_vul_Tenable_Scan** Tabelle. Mit dieser Verknüpfung können Sie: ◦ Zeigen Sie die neuesten Scan-Informationen an, die jedem erkannten Element zugeordnet sind. ◦ Verbessern Sie den Kontext für Entscheidungen zur Selektierung und Korrektur von Schwachstellen. ◦ Verbessern Sie die Auditierbarkeit und Berichterstellungsfunktionen, indem Sie einen Verlaufsdatensatz von Scan-Aktivitäten pflegen.

Tenable.sc Integrationen mit Vulnerability Response Anwendung

Die Tenable.sc Integrationen in Vulnerability Response Integration with Tenable Anwendung.

Beginnend mit Vulnerability Response V20.0: Wenn ein Asset von einem Service Desk-Mitarbeiter gescannt wird, wird in der Spalte „Agent vorhanden“ in der Liste „erkannte Elemente“ der Wert „wahr“ angezeigt. Dies gibt an, dass der Scan authentisch ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste von Tenable.sc Integrationen

Mehrere Quellen werden für alle unterstützt Tenable.io Und Tenable.sc Integrationen. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in hinzufügen und bereitstellen Vulnerability Response. Sie können auch installieren und konfigurieren Vulnerability Response Integration with Tenable Anwendung aus Setup-Assistent.

- Tenable.sc Ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn der verwendet wird Tenable.sc Produkt und Ihr ServiceNow AI Platform Instanz befindet sich in derselben Umgebung.
- Wenn Tenable.sc Produkt und Ihr ServiceNow AI Platform Instanz befindet sich nicht in derselben Umgebung, Sie müssen einen MID-Server verwenden.

Tenable.sc-Integrationen

Integration	Beschreibung
Tenable.sc Asset-Integration	Um die Erstellung doppelter erkannter Elemente mit importierten Asset-Daten zu vermeiden, wird die Asset-Integration von verwendet Tenable.sc Das Produkt besteht aus zwei Integrationen. **Die Tenable.scÖffnen Sie Die Asset-Integration** Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable berücksichtigt **Kumulativ** (Aktuell), oder **Öffnen** . Die angreifbaren Elemente (VIS), die in Ihrer Instanz mit diesen importierten Asset-Daten erstellt werden, gelten als offen, d. h. in **Öffnen** status. Diese angreifbaren Elemente erfordern eine Untersuchung und müssen möglicherweise behoben werden. **Die Tenable.sc Integration Von Anlagegütern** Diese Integration importiert Schwachstellendaten zu Ihren Assets, die Tenable berücksichtigt **Gemindert** (Nicht mehr angreifbar) oder **Behoben** . Die angreifbaren Elemente für diese Assets werden aus dem übergehen **Öffnen** status zu **Geschlossen/Behoben** status in Ihrer Instanz, da die Ergebnisse von Scans zeigen, dass sie nicht mehr angreifbar sind. • Ruft alle Asset-Daten aus dem ab Tenable.sc Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die eine IP-Adresse teilen. • Koordiniert die REST-Nachrichtenaufrufe an die Assets-API. • Die Ausgabe dieser Integration ist erkannte Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
	• Der Tenable-Abfragefilter, den Sie im Setup-Assistenten auswählen, gilt auch für Tenable.sc Asset-Integration. Nur die Assets mit den Schwachstellen, die den Bedingungen des Abfragefilters entsprechen, werden importiert.
Tenable.sc Plugin-Integration	• Ruft die Plugin-Daten aus dem ab Tenable.sc Produkt. Abgerufene Daten basieren auf dem Datum, an dem die Plugins zuletzt von einem aktualisiert wurden Tenable.sc Integrationsausführung. • Dieser Import stellt sicher, dass die Tenable.sc Bezeichner (zehn IDs) sind aktuell, und nur aktive Schwachstellen werden importiert. • Koordiniert die REST-Nachrichtenaufrufe an die Plugins-API. • Die Ausgabe dieser Integration ist Schwachstellen von Drittparteien.
Tenable.sc Integration Behobener Schwachstellen	• Ruft Schwachstellendaten basierend auf Schweregradfiltern aus ab Tenable.sc Produkt und verarbeitet es in Ihrer Instanz. Angreifbare Elemente werden für Erkennungsdatensätze erstellt, die sich in befinden **Öffnen** Und **Erneut Geöffnet** status, da diese Datensätze eine Korrektur erfordern. Vorhandene angreifbare Elemente werden von Vulnerability Response aktualisiert, wenn Erkennungen sind **Behoben** , Aber angreifbare Elemente werden für nicht erstellt **Behoben** Erkennungen standardmäßig, da Tenable berücksichtigt **Behoben** Schwachstellen **Gemindert** . • Wenn die Kennzeichnung **Erstellen Sie Zeiten für Schwachstellen für Erkennungen behobener Schwachstellen** Ist im Setup-Assistenten aktiviert, erstellt es VIS in **Behoben** geben sie den status an, damit Sie Einblick in die Erkennungen haben, die sie erstellt haben. AS VIS werden für erstellt **Behoben** Erkennungen, die in Ihrer Instanz nicht vorhanden sind. Dies kann sich negativ auf Ihre Importleistung auswirken. Möglicherweise möchten Sie diese Funktion deaktiviert lassen, damit dies möglich ist **Behoben** Erkennungen aktualisieren nur die status vorhandener angreifbarer Elemente. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die eine IP-Adresse teilen. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
	Die Ausgabe dieser Integration ist **Geschlossen/Behoben** Angreifbare Elemente (VIS). Außerdem werden Assets und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind. Diese Integrationsausführung ist eine geplante Ausführung. Es handelt sich um eine verkettete Integration, was bedeutet, dass nach erfolgreichem Abschluss einer Ausführung die verwendet wird Tenable.sc„Integration offener Schwachstellen“, die als Nächstes beschrieben wird, wird ausgelöst. **Hinweis:** Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen.
Tenable.sc Integration Offener Schwachstellen	• Diese Integration wird nach erfolgreichem Abschluss von ausgelöst Tenable.sc Integration Behobener Schwachstellen. • Ruft Schwachstellendaten basierend auf den in ausgewählten Abfragefiltern ab Tenable.sc Produkt und verarbeitet es in Ihrer Instanz. • Erstellt entsprechende angreifbare Elemente für aktive Schwachstellen. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs mit dem Attribut Netzwerkpartition-Bezeichner für Assets in Ihrer Umgebung, die eine IP-Adresse teilen. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. • Die Ausgabe dieser Integration ist **Aktualisieren/ Neu erstellen** Angreifbare Elemente (VIS), wenn sie nicht vorhanden sind. Außerdem werden Konfigurationselemente und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind. **Hinweis:** Standardmäßig sind die Familien-IDs 0 und 39 von dieser Integration ausgeschlossen.
Tenable.sc Integration Von Anmeldeinformationen Scannen	• Diese Integration ruft die in konfigurierten Scan-Anmeldeinformationen ab Tenable.sc. • Koordiniert die REST-Nachrichtenaufrufe an die Anmeldeinformations-API. • Die Ausgabe dieser Integration ist Scan-Anmeldeinformationen, die in der Tabelle [sn_vul_Tenable_Scan_credential] ausgefüllt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.sc-Integrationen (Fortsetzung)

Integration	Beschreibung
	• Die importierten Anmeldeinformationen werden für den Zugriff auf den Scanner verwendet, wenn Scananforderungen von initiiert werden ServiceNow AI Platform. • Diese Integration wird wöchentlich ausgeführt.
Tenable.sc Integration Von Schwachstellen Auffüllen	• Diese Backfill-Integration importiert alle offenen und behobenen Schwachstellen, die während eines Imports möglicherweise nicht berücksichtigt wurden. • Diese Integration importiert sowohl offene als auch behobene Schwachstellen aus den letzten sieben Tagen, um Ihre Erkennungen und angreifbaren Elemente zu aktualisieren. • Diese Integration kann sich auf Ihre Leistung auswirken. • Diese Integration ist standardmäßig inaktiv. • Um Ihre Schwachstellendaten zu aktualisieren und potenzielle Leistungsprobleme zu vermeiden, ziehen Sie es möglicherweise vor, die Tenable.sc-Integrationen für behobene Schwachstellen und offene Schwachstellenintegrationen so zu planen, dass sie ausgeführt werden, wenn keine anderen Scans ausgeführt werden. • Die Ausgabe dieser Integration lautet: ○ **Geschlossen/Behoben** Angreifbare Elemente (VIS). Außerdem werden Assets und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind. ○ Bis **Aktualisieren/Neu erstellen** Angreifbare Elemente (VIS), wenn sie nicht vorhanden sind. Außerdem werden Konfigurationselemente und Drittparteieinträge erstellt, wenn sie nicht vorhanden sind.

Anwenderauthentifizierung und Tenable.sc

Die Anwenderauthentifizierung wird von unterstützt ServiceNow AI Platform® Instanz und Version 5,13 von Tenable.sc Produkt. Anwenderauthentifizierung ist erforderlich, wenn Sie Version 5,12 und früher von verwenden Tenable.sc Produkt.

Wenn Sie Anwenderauthentifizierung für auswählen Tenable.sc Integrationen, Token laufen möglicherweise ab und werden während der Integrationsausführungen ersetzt. In der Spalte Notizen im Datensatz Vulnerability Integration Run (VIN) wird die folgende Meldung für einen Prozess angezeigt, wenn ein Token abläuft: Fehler: Token-Validierung ist fehlgeschlagen . Wenn diese Nachricht angezeigt wird, ist keine Aktion erforderlich. Abgelaufene Token werden automatisch im Hintergrund aktualisiert, und die Meldung weist nicht auf eine Pause oder einen Fehler beim Integrationsprozess hin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Integrationen mit Vulnerability Response Und Container Vulnerability Response Anwendung

Die Tenable.cs Integrationen in Vulnerability Response Integration with Tenable-Anwendungen sind in Vulnerability Response und verfügbar Container Vulnerability Response Anwendungen.

Ab v20.0 Vulnerability Response, Wenn ein Asset von einem Service Desk-Mitarbeiter gescannt wird, wird in der Spalte „Service Desk-Mitarbeiter vorhanden“ in der Liste „erkannte Elemente“ „wahr“ angezeigt, was angibt, dass der Scan authentisch ist.

Liste von Tenable.cs Integrationen

Mehrere Quellen werden für alle unterstützt Tenable.io, Tenable.sc, Und Tenable.cs Integrationen. Sie können mehrere Instanzen der folgenden Integrationen in Ihrer Umgebung über den Setup-Assistenten in hinzufügen und bereitstellen Vulnerability Response. Sie können auch installieren und konfigurieren Vulnerability Response Integration with Tenable Anwendung aus Setup-Assistent.

Tenable.cs Ist eine cloudbasierte Enterprise-Integration. In der folgenden Tabelle finden Sie die Namen und Beschreibungen der unterstützten Integrationen für Tenable.cs Produkt.

Tenable.cs-Integrationen

Integration	Beschreibung
Tenable.cs Integration Von Cloud-Container-Assets	• Ruft alle Container-Asset-Daten aus dem ab Tenable.cs Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs. Koordiniert die REST-Nachrichtenaufrufe an die Asset-API. Die Ausgabe dieser Integration ist erkannte Container-Images, Docker-Images und Container-Repositorys.
Tenable.cs Öffnen Sie Die Integration Von Cloud-Container-Schwachstellen	Wenn diese Option aktiviert ist, wird diese Integration automatisch ausgeführt, nachdem die Integration der Container-Assets als Teil einer verketteten Integrationsausführung erfolgreich abgeschlossen wurde. • Ruft Container-Schwachstellendaten basierend auf den Schweregradfiltern aus ab Tenable.cs Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. Die Ausgabe dieser Integration ist neue/erneut geöffnete angreifbare Container-Elemente (CVIS). Wenn sie nicht vorhanden sind, werden auch erkannte Container-Images, Docker-Images, Container-Repositorys, Image-Ergebnisse, Drittparteieinträge erstellt. und Common Vulnerabilities and Exposures (CVE).
Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container	Diese Integration wird nach erfolgreichem Abschluss von ausgelöst Tenable.csÖffnen Sie Die Integration Von Cloud-Container-Schwachstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs-Integrationen (Fortsetzung)

Integration	Beschreibung
	• Ruft Container-Schwachstellendaten basierend auf den Schweregradfiltern aus ab Tenable.cs Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. Die Ausgabe dieser Integration ist neue/erneut geöffnete angreifbare Container-Elemente (CVIS). Wenn sie nicht vorhanden sind, werden auch Discovery-Container-Images, Docker-Images, Container-Repositorys, Image-Ergebnisse, Drittparteieinträge erstellt. und CVEs. Bildergebnisse werden im Status „Geschlossen“ erstellt.
Tenable.cs Öffnen Sie Die Integration Von Cloud-Host-Schwachstellen	• Ruft Schwachstellendaten basierend auf den Schweregradfiltern aus ab Tenable.cs Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. Die Ausgabe dieser Integration ist neue/erneut geöffnete angreifbare Elemente (VIS). Wenn sie nicht vorhanden sind, werden auch Konfigurationselemente, Drittparteieinträge und CVEs erstellt. Schwachstellenerkennungen werden im Status „Offen“ erstellt.
Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen	Diese Integration wird nach erfolgreichem Abschluss von ausgelöst Tenable.csÖffnen Sie Die Integration Von Cloud-Host-Schwachstellen. • Ruft Schwachstellendaten basierend auf den Schweregradfiltern aus ab Tenable.cs Produkt und verarbeitet es in Ihrer Instanz. • Erstellt eindeutige CIs für nicht abgeglichene Assets oder aktualisiert vorhandene CIs. • Koordiniert die REST-Nachrichtenaufrufe an die Schwachstellen-API. Die Ausgabe dieser Integration lautet „angreifbare Elemente schließen“ (VIS). Wenn sie nicht vorhanden sind, werden auch Konfigurationselemente, Drittparteieinträge und CVEs erstellt. Schwachstellenerkennungen werden im Status „Geschlossen“ erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwenderauthentifizierung und Tenable.sc

Die Anwenderauthentifizierung wird von unterstützt ServiceNow AI Platform® Instanz und Version 5,13 von Tenable.sc Produkt. Anwenderauthentifizierung ist erforderlich, wenn Sie Version 5,12 und früher von verwenden Tenable.sc Produkt.

Wenn Sie Anwenderauthentifizierung für auswählen Tenable.sc Integrationen, Token laufen möglicherweise ab und werden während der Integrationsausführungen ersetzt. In der Spalte Notizen im Datensatz Vulnerability Integration Run (VIN) wird die folgende Meldung für einen Prozess angezeigt, wenn ein Token abläuft: Fehler: Token-Validierung ist fehlgeschlagen . Wenn diese Nachricht angezeigt wird, ist keine Aktion erforderlich. Abgelaufene Token werden automatisch im Hintergrund aktualisiert, und die Meldung weist nicht auf eine Pause oder einen Fehler beim Integrationsprozess hin.

Vorbereitung auf die Tenable-Schwachstellenintegration

Bereiten Sie sich auf den vor ServiceNow® Tenable-Schwachstellenintegration durch Ausführen der folgenden Setup-Aufgaben.

Bevor Sie beginnen

Eine erfolgreiche Integration erfordert die Planung und sorgfältige Ausführung von Aufgaben vor der Integration. Für eine reibungslose Installation und Konfiguration von Vulnerability Response Integration with Tenable Anwendung möchten Sie möglicherweise die folgende Prüfliste drucken und überprüfen, ob die aufgeführten Elemente abgeschlossen sind, bevor Sie die Anwendung installieren und Schwachstellendaten in importieren ServiceNow AI Platform® Instanz.

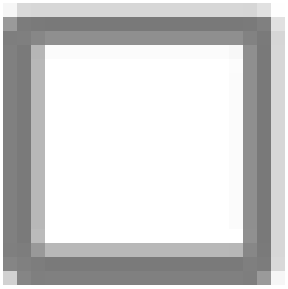
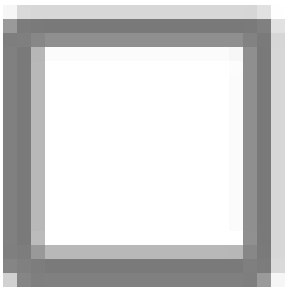
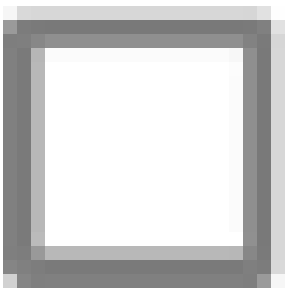
Hinweis:
Wenn Sie Daten mit der Tenable-Build-Integration importiert haben und mit der Verwendung von beginnen möchten ServiceNow® Vulnerability Response-Integration mit Tenable, siehe

Für aktuelle Datenbereinigung und -Migration von der Tenable-Build-Integration zur von erstellten Integration ServiceNow, Siehe Richtlinien für die Migration von der Tenable Vulnerability Response-Integration zur ServiceNow Vulnerability Response-Integration mit Tenable [KB0960667] artikel.

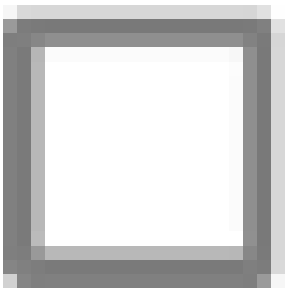
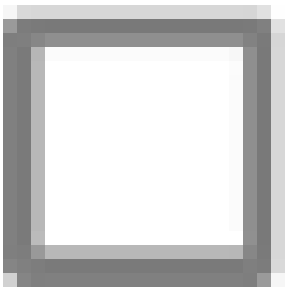
Erforderliche Rolle: Administrator zum Herunterladen und Installieren der Anwendung.

Aufgabe	Beschreibung
	(Optional) wenn Sie nicht bereits installiert und aktiviert sind, möchten Sie möglicherweise installieren Vulnerability Response Anwendung vor der Installation der Drittanbieteranwendung. Weitere Informationen zum Installieren und Aktivieren von Vulnerability Response Anwendung, siehe, Vulnerability Response installieren. Diese Integration erfordert Version 12,1 von Vulnerability Response Oder später.

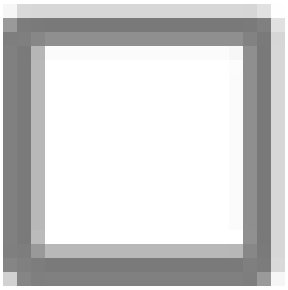
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Wenn Sie es noch nicht in Ihrer Instanz haben, rufen Sie Berechtigungen ab, und laden Sie herunter Vulnerability Response Integration with Tenable Anwendung für Ihren ServiceNow AI Platform® Instanz. Die Vulnerability Response Integration with Tenable Die Anwendung unterstützt Tenable.sc Produkt ab Version 5,13 Und Tenable.cs Produkt ab Version 5,0.1. .
	Schätzen Sie die Anzahl der angreifbaren Elemente, die Sie importieren möchten. Überprüfen Sie, ob Ihre Instanz die Anzahl der angreifbaren Elemente akzeptieren kann, die Sie importieren möchten. Eine unterdimensionierte Instanz kann zu langen Ladezeiten führen. Wenn Sie die Größe Ihrer Instanz nicht kennen oder Hilfe benötigen, wenden Sie sich an ServiceNow® Technischer Support.
	Stellen Sie sicher, dass Sie Gruppen oder Anwender haben, um die Integrationen zu verwalten und angreifbare Elemente zu korrigieren. **Administrator** Der Systemadministrator verwendet den Setup-Assistenten, um zu installieren Vulnerability Response Integration with Tenable Anwendung. Wenn nicht zugewiesen, weist der Administrator den Schwachstellenadministrator (sn_vul.Vulnerability_admin) und andere Rollen im Setup-Assistenten zu. **sn_vul.vulnerability_admin** Nach der Zuweisung schließt der Schwachstellenadministrator die Konfiguration der Tenable-Integrationen ab. Diese Rolle hat vollständigen Zugriff auf Vulnerability Response(VR)-Anwendung und ihre Datensätze. Konfiguriert alle VR-Anwendungen und -Regeln und konfiguriert Integrationen von Drittparteien. **sn_vul_Tenable.configure_Integration** Kann die Tenable-Schwachstellenintegration konfigurieren. Diese Rolle enthält die granulare Rolle sn_vul_Tenable.read_Integration. **sn_vul_Tenable.read_Integration** Kann Datensätze der Tenable-Schwachstellenintegration anzeigen (lesen). **Vulnerability Response-Gruppe** Standardmäßig ist die Vulnerability Response-Gruppe im Setup-Assistenten verfügbar. Anwender, die der Vulnerability Response-Gruppe zugewiesen sind, erben die Rollen sn_vul.read_all und sn_vul.Remediation_owner automatisch. Der Systemadministrator führt die anfängliche Zuweisung von Rollen an Anwender und Gruppen im Setup-Assistenten für die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Integration durch. Standardmäßig ist die Vulnerability Response-Gruppe verfügbar. Wenn Sie noch nicht erstellt haben, können Sie zusätzliche Gruppen erstellen und Anwender mit dem Modul „Anwenderverwaltung“ in Ihrer Instanz hinzufügen, bevor Sie den Setup-Assistenten verwenden. Siehe Erstellen Sie eine Anwendergruppe . Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender in der Vulnerability Response-Anwendung tun und sehen können. Informationen zur anfänglichen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.
	Um eine verbesserte Leistung für Ihren ersten Import heraufzustufen, sollten Sie möglicherweise bestimmte Funktionen, Regeln oder Aufträge in Ihrer Instanz deaktivieren. • Deaktivieren Sie Schwachstellen-Rechner, wenn Sie sie nicht verwenden. Diese Rechner sowie alle von Ihnen definierten Rechner werden jedes Mal ausgeführt, wenn ein Datensatz für angreifbare Elemente erstellt oder aktualisiert wird. Siehe Deaktivieren Sie Schwachstellen-Rechner . • Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln dazu führen, dass viele Benachrichtigungen generiert werden, was sich auf die Leistung auswirkt. Vor dem ersten Import sollten Sie benachrichtigungsbezogene Geschäftsregeln deaktivieren, wie in beschrieben Importieren Sie Änderungen für die Tenable-Schwachstellenintegration.
	Stellen Sie sicher, dass Sie alle Funktionen, Regeln, Abhängigkeits-Plugins oder Aufträge in Ihrer Instanz aktiviert haben, die für die Integration erforderlich sind. • Tenable.sc Ist eine lokale Integration, die Ihnen die Möglichkeit gibt, einen MID-Server zu verwenden, wenn der verwendet wird Vulnerability Response Integration with Tenable Produkt und Ihr ServiceNow AI Platform Instanz befindet sich in derselben Umgebung. Wenn Tenable.sc Produkt und Ihr ServiceNow AI Platform Instanz befindet sich nicht in derselben Umgebung, Sie müssen einen MID-Server verwenden. Weitere Informationen zu MID-Servern in Ihrer Instanz finden Sie unter MID-Server . • Überprüfen Sie, ob das IntegrationHub-Plugin installiert und aktiviert ist. Dieses Plugin ermöglicht es Basissystemkomponenten, externe Systeme mithilfe von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Integrations-APIs aufzurufen, und aktiviert Protokollschritte wie REST. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** Und suchen Sie das Plugin. Wenn nicht in Ihrer Instanz installiert, installieren und aktivieren Sie sie.
	Tenable-Anmeldeinformationen abrufen. Stellen Sie sicher, dass Sie Accountnamen, Passwörter und andere Serviceinformationen haben, die für Ihre Tenable-Produkte erforderlich sind, damit Sie Zugriff darauf haben. Tenable.io Erfordert Administratorzugriff mit einem Berechtigungsattribut größer oder gleich 64. Tenable.sc Erfordert Sicherheitsanalysten oder -Manager-Zugriff. **Hinweis:** Ab v3.8 von Vulnerability Response Integration with Tenable, Zugriff auf Tenable.io Benötigt keine Administratorrechte mehr. Ein Standardanwender mit einem Berechtigungsattribut von 16 kann auch auf das Produkt zugreifen.

Sie sind bereit für Installieren Sie Vulnerability Response Integration with Tenable Anwendung mit Setup-Assistent.

Installieren Sie Vulnerability Response Integration with Tenable Anwendung mit Setup-Assistent

Bevor Sie ausführen ServiceNow® Tenable-Schwachstellenintegration müssen Sie herunterladen Vulnerability Response Integration with Tenable Anwendung aus dem ServiceNow Store Und installieren und konfigurieren Sie es mit dem Setup-Assistenten in Vulnerability Response Anwendung.

Vorbereitungen

Bevor Sie die Tenable-Anwendung installieren, überprüfen Sie, ob Sie alle Elemente in der Prüfliste in abgeschlossen haben Vorbereitung auf die Tenable-Schwachstellenintegration.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

Erforderliche Rollen: administrator für die anfängliche Zuweisung der Rolle „sn_vul.Vulnerability_admin“ und die Installation der Tenable-Anwendung im Setup-Assistenten. Schwachstellenadministrator (sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet), um die Anwendung im Setup-Assistenten nach der Installation zu konfigurieren.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent** > **Installation der Integrationsanwendung**an.

   Nach einigen Minuten werden die Anwendungen angezeigt, die für die Installation in Ihrer Instanz verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Suchen Sie nach **Tenable (Tenable-Plattform)** Kachel und klicken Sie auf **Installieren** .

   Mit dieser Aktion wird installiert Vulnerability Response Integration with Tenable Anwendung, die Sie aus heruntergeladen haben ServiceNow Store.

3. Befolgen Sie die Anweisungen im Setup-Assistenten, um mit der Installation fortzufahren.

4. Weitere Informationen zum Installieren von Anwendungen mit dem Setup-Assistenten finden Sie unter Installieren Vulnerability Response Drittanbieteranwendungen mit Setup-Assistent.

Nächste Maßnahme

Nachdem Sie die Installation im Setup-Assistenten abgeschlossen haben, navigieren Sie zu **Integrationskonfiguration>Scannerintegrationen** In Setup-Assistent, um mit der Konfiguration fortzufahren. Weitere Informationen zur Ergänzung der im Setup-Assistenten bereitgestellten Hinweismeldungen finden Sie unter Konfigurieren Sie die Tenable-Schwachstellenintegration mit dem Setup-Assistenten.

Datenabrufeinstellungen für die Tenable-Schwachstellenintegration

Die folgenden Datenabrufeinstellungen helfen Ihnen, den Typ und den Umfang der Daten zu bestimmen, die Sie aus importieren möchten ServiceNow® Tenable-Schwachstellenintegration für Ihren ServiceNow AI Platform® Instanz.

Die in den folgenden Abschnitten beschriebenen Einstellungen helfen Ihnen, die Daten zu steuern, die Sie importieren möchten. Darüber hinaus können Sie die Werte dieser Filter in Integrationsinstanzen festlegen. Um Integrationsinstanzen anzuzeigen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Integrationsinstanzen** Und wählen Sie Ihre Integration aus, Tenable.io, Tenable.sc, Oder Tenable.cs.

Wählen Sie auf der angezeigten Seite „Integrationsinstanz“ die Integrationsinstanzparameter aus, um eine Liste von Parametern anzuzeigen, oder die Registerkarten Schwachstellenintegrationen für einen Zeitplan, REST-Details, Integrationsdetails, Datenquellen und Informationen zur Integrationsausführung.

Allgemeine Schweregrad- und Abrufeinstellungen und Filter für Tenable.io, Tenable.sc Und Tenable.cs In Ihrem ServiceNow AI Platform Instanz

Die folgenden Einstellungen sind für verfügbar Tenable.io, Tenable.sc, Und Tenable.cs Integrationen in Ihrem ServiceNow AI Platform Instanz. Diese und andere Konfigurationseinstellungen werden auf der Seite „Integrationsinstanz“ von angezeigt ServiceNow AI Platform Instanz. Möglicherweise möchten Sie diese Einstellungen für die ersten Integrationsausführungen in ihren Standardeinstellungen belassen.

Tenable.io

INSERT_fixed

Wenn Sie aktivieren **INSERT_fixed** Kennzeichnung im Setup-Assistenten für die Integration des Schwachstellenimports. Neue VIS werden für Erkennungen in erstellt **Behoben** status, der in Ihrer Instanz nicht vorhanden ist.

Schweregrad_Critical

Dieser Filter ist standardmäßig aktiviert (wahr), um Schwachstellen mit Schweregrad „Kritisch“ von zu empfangen Tenable.ioÖffnen Sie Schwachstellen und Tenable.io Integrationen Behobener Schwachstellen.

Schweregrad_hoch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Filter ist standardmäßig aktiviert (wahr), um Schwachstellen mit hohem Schweregrad von zu empfangen Tenable.ioÖffnen Sie Schwachstellen und Tenable.io Integrationen Behobener Schwachstellen.

Schweregrad_Medium

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit mittlerem Schweregrad von zu empfangen Tenable.ioÖffnen Sie Schwachstellen und Tenable.io Integrationen Behobener Schwachstellen.

Schweregrad_Info

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit Schweregrad auf Informationsebene von zu erhalten Tenable.ioÖffnen Sie Schwachstellen und Tenable.io Integrationen Behobener Schwachstellen.

Schweregrad_niedrig

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit niedrigem Schweregrad von zu empfangen Tenable.ioÖffnen Sie Schwachstellen und Tenable.io Integrationen Behobener Schwachstellen.

size

Diese Einstellung definiert die Anzahl der Plugin-Datensätze, die in den Ergebnissatz von aufgenommen werden sollen Tenable.io Plugins-Integration. Muss im int32-Format vorliegen. Der Standardwert ist 1.000. Die maximale Größe beträgt 000.

num_Assets

Die maximale Anzahl von Schwachstellen pro exportiertem Block aus Tenable.io Schwachstellen behoben und Tenable.ioÖffnen Sie Schwachstellen-Integrationen. Der Standardwert beträgt 50.

chunk_size

Gibt die Anzahl der Assets pro exportiertem Block von an Tenable.io Asset-Integration. Der Standardwert ist 1.000.

Tenable.sc

Async_Request

Dieser Parameter ist standardmäßig inaktiv (falsch). Aktivieren oder deaktivieren Sie diesen Parameter, um asynchrone oder synchrone API-Aufrufe mit durchzuführen Tenable.sc Entsprechend. Wenn bei synchronen Anrufen eine Zeitüberschreitung von 30 Sekunden auftritt, wenden Sie sich an den Support für das Tenable-Produkt, um die Box zu optimieren. Dieser Parameter gilt nach der Aktivierung für alle Integrationen von Tenable.sc. Für Bestandskunden, die asynchrone Aufrufe verwenden, ist ein Korrekturskript verfügbar, das dem vorhandenen einen neuen Parameter „async_Request“ hinzufügt Tenable.sc Integrationsinstanzen. Um die Korrekturskripts anzuzeigen, navigieren Sie zu **Systemdefinition** > **Korrekturskripts**an.

INSERT_fixed

Wenn Sie aktivieren **INSERT_fixed** Kennzeichnung im Setup-Assistenten für die Integration des Schwachstellenimports. Neue VIS werden für Erkennungen in erstellt **Behoben** status, der in Ihrer Instanz nicht vorhanden ist.

Offset

Gibt die Anzahl der Assets, Plugins und Schwachstellen an, die in einer Integrationsausführung importiert wurden.

Abfragefilter

Abfragefilter werden in der Tenable-Konsole konfiguriert. Diese Abfragefilter haben IDs, die im Setup-Assistenten oder auf der Seite „Integrationsinstanzen“ in ausgewählt werden können ServiceNow AI Platform Instanz. Diese Filter werden beim Abrufen der Daten aus angewendet Tenable.sc Integrationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs

Compute_severity_Critical

Dieser Filter ist standardmäßig aktiviert (wahr), um Schwachstellen mit Schweregrad „Kritisch“ von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Host-Schwachstellen und Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen.

Compute_severity_High

Dieser Filter ist standardmäßig aktiviert (wahr), um Schwachstellen mit hohem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Host-Schwachstellen und Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen.

Compute_severity_Medium

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit mittlerem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Host-Schwachstellen und Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen.

Compute_severity_info

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit Schweregrad auf Informationsebene von zu erhalten Tenable.csÖffnen Sie die Integration von Cloud-Host-Schwachstellen und Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen.

Compute_severity_low

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit niedrigem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Host-Schwachstellen und Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen.

Container_severity_Critical

Dieser Filter ist standardmäßig aktiviert (wahr), um Container-Schwachstellen mit Schweregrad „Kritisch“ von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container.

Container_severity_High

Dieser Filter ist standardmäßig aktiviert (wahr), um Container-Schwachstellen mit hohem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container.

Container_severity_Medium

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Container-Schwachstellen mit mittlerem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container.

Container_Schweregrad_Info

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Schwachstellen mit Schweregrad auf Informationsebene von den Container-Schwachstellen von zu erhalten Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container.

Container_severity_low

Dieser Filter ist standardmäßig inaktiv (falsch). Aktivieren Sie diesen Filter, um Container-Schwachstellen mit niedrigem Schweregrad von zu empfangen Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container.

Asset_page_limit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Einstellung definiert die Anzahl der Container-Asset-Datensätze, die in den Ergebnissatz von aufgenommen werden sollen Tenable.cs Integration Von Cloud-Container-Assets. Der Standardwert ist 1.000. Die maximale Größe beträgt 1.000.

Vuln_page_limit

Diese Einstellung definiert die Anzahl der Schwachstellendatensätze, die in den Ergebnissatz von aufgenommen werden sollen Tenable.cs Integration Offener Cloud-Host-Schwachstellen, Tenable.cs Integration Von Behobenen Cloud-Host-Schwachstellen, Tenable.csÖffnen Sie die Integration von Cloud-Container-Schwachstellen, und Tenable.cs Integration Von Schwachstellen Für Behobene Cloud-Container. Der Standardwert ist 1.000. Die maximale Größe beträgt 000.

REST-Nachrichten für die Tenable-Schwachstellenintegration

Die ServiceNow® Tenable Vulnerability Integration REST-Nachrichten werden verwendet, um Aufrufe an die Tenable-API zu tätigen.

Tenable.io Asset-REST-Nachricht

Die Tenable.io Die Asset-REST-Nachricht ruft Asset-Informationen für ab Tenable.io Asset-Integration. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die an gestellten Anforderungen aus Tenable.io Dient zum Abrufen von Asset-Informationen. Der Exportauftrag für Assets wird mit den folgenden Filtern übermittelt:

- „Is_deleted“: Falsch
- „Is_license“: Wahr

Tenable.io Plugins-REST-Nachricht

Die Tenable.io DIE Plugins-REST-Nachricht ruft Plugin-Informationen für ab Tenable.io Plugin-Integration. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die an gestellten Anforderungen aus Tenable.io Zum Abrufen von Plugins-Informationen.

Tenable.io REST-Nachricht für Schwachstellen

Die Tenable.io DIE REST-Nachricht „Schwachstellen“ ruft Schwachstelleninformationen für offene und geschlossene Schwachstellen aus dem ab Tenable.io Schwachstellenintegration. Änderungen am Datensatz der REST-Nachrichtenmethode wirken sich auf die an gestellten Anforderungen aus Tenable.io Zum Abrufen von Informationen zu Schwachstellen.

Tenable.sc fragt DIE REST-Nachricht ab

Die Rest-Nachricht Tenable.sc Queries ruft die Abfragefilterinformationen für die Tenable.sc Asset-Integration und Tenable.sc-Schwachstellenintegration ab, bei der der Abfragefilter konfiguriert ist.

Tenable.sc Plugins-REST-Nachricht

Die Tenable.sc Die Plugin-REST-Nachricht ruft Plugin-Informationen für ab Tenable.sc Plugins-Integration. Änderungen am Datensatz der REST-Nachricht „Plugins abrufen“ wirken sich auf die an gestellten Anforderungen aus Tenable.sc Zum Abrufen von Plugins-Informationen.

Parametername	Wert	Beschreibung
type	aktiv	Gibt an, dass das Quell-Tenable Daten aus abruft. Verwendet von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Wert	Beschreibung
		Code. Änderungen werden nicht empfohlen.
Felder	id, Beschreibung, cvssVector,cvssV3Vector, cvssV3TemporalVector, synopsis, cvssVector, baseScore,temporalScore, cvssV3Vector,cvssV3BaseScore, cvssV3TemporalScore, Name, vprScore, vprContext, pluginPubDate, pluginModDate, xrefs, Familie, Risikofaktor, cpe, seeAlso, Lösung, exploitAvailable, exploitFrameworks, type, Copyright, Version, sourcefile, Abhängigkeiten, requidPorts, requidUDPPorts, srcPort, dstPort,Protocol, checkType, cvssVectorBF, stigSeverity, patchPubDate, patchModDate, vulnPubDate, modifiedTime, md5	Gibt die Liste der aus Tenable importierten Felder an.

Tenable.sc REST-Nachricht für Schwachstellen

Die Tenable.sc DIE REST-Nachricht „Schwachstellen“ ruft Schwachstelleninformationen aus dem ab Tenable.sc Integration. Änderungen an der REST-Nachricht „Schwachstellen abrufen“ oder „gepatchte Schwachstellen abrufen“ oder ab v14.0 Vulnerability Response Und v2.2 der Tenable-Schwachstellenintegration, Datensatz „Schwachstellen im Backfill abrufen“ wirkt sich auf die Anforderungen aus, an die gestellt wird Tenable.sc Zum Abrufen von Informationen zu Schwachstellen.

Tenable.sc REST-Nachricht „Anmeldeinformationen scannen“

Tenable.sc REST-Nachricht der Richtlinie

Die Tenable.sc Die POST-REST-Nachricht der Richtlinie fügt eine Richtlinie für angeforderte Plugins hinzu. Generierte Richtlinie wird in verwendet Tenable.sc Scan-Anforderungen.

Tenable.sc REST-Nachricht scannen

Die Nachricht Tenable.sc Scan NACH REST fügt einen Scan hinzu, der von dem Zugriff und der Berechtigung abhängig ist, die im Anforderungstext der Rest-Nachricht definiert sind. Es verwendet Richtlinie, Plugin-ID und IP(s) im Anforderungstext für die Scan-Anforderung.

Tenable.sc REST-Nachricht des Scan-Ergebnisses

Die Tenable.sc Die Meldung „Scan-Ergebnis ABRUFEN“ enthält Scan-Details des Scans, der mithilfe der Scan-REST-Nachricht generiert wurde. Es verwendet die scanResultId in der Antwort der Scan-REST-Nachrichten und ruft Scan-Details für den ausgelösten Scan ab.

Tenable.sc Scan-Anmeldeinformationen

Die Tenable.sc Die REST-Nachricht „Anmeldeinformationen scannen“ ruft die Anmeldeinformationen von ab Tenable.sc. Änderungen am Datensatz der REST-Nachricht mit der Methode „Import“ wirken sich auf die an gestellten Anforderungen aus Tenable.sc Zum Abrufen der Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Wert	Beschreibung
Felder	id,Name,Beschreibung,Typ	Gibt die Liste der aus importierten Felder an Tenable.sc
Filter	Verwendbar	Gibt an, dass die Integration nur nutzbare Anmeldeinformationen von abruft Tenable.sc Änderungen an einem der Parameter werden nicht empfohlen.

Tenable.cs GraphQL-REST-Nachricht: Die Tenable.cs Die GraphQL-REST-Nachricht ruft Container-Asset-Informationen, Host- und Container-Schwachstelleninformationen für ab Tenable.cs Integration. Änderungen am Datensatz der REST-Nachricht „Container-Assets abrufen“, „Container-Schwachstellen abrufen“, „Schwachstellen berechnen“ abrufen wirken sich auf die an gestellten Anforderungen aus Tenable.cs Zum Abrufen von Asset- und Schwachstelleninformationen.

Datentransformation für die Tenable-Schwachstellenintegration

Nachdem Sie die zu importierenden Daten identifiziert haben, werden sie aus dem Tenable-Produkt abgerufen und über eine Reihe von Datenquellen und Transformationen in Ihrer Instanz verarbeitet.

Während der Installation werden normalisierte Schweregradzuordnungen im Modul „normalisierte Schweregradzuordnung“ installiert. Diese Zuordnungen transformieren importierte Tenable-Schweregrade in Standardschweregrade zur Verarbeitung in Ihrer Instanz. Informationen zum Erstellen von Schweregradzuordnungen finden Sie unter Zuordnung des Schweregrads von Vulnerability Response erstellen in Vulnerability Response Dokumentation.

Tenable.io-Asset-Import

Importierte Asset-Daten werden zuerst in die Tabelle „Tenable.io-Asset-Import“ [sn_vul_Tenable_io_Asset_Import] geladen.

Die Transformationszuordnung Tenable.io Asset Integration wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Import von Tenable-Assets verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach Tenable.io-Asset-Transformation .

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Tenable.io Asset-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_id	source_id	Tenable stellt eine eindeutige ID für Assets bereit und ordnet dem erkannten Elementdatensatz zu und wird für die CI-Suche verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.io Asset-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_ipv4s	ip_address	Ordnet den ersten ip-Wert dem Feld ip_address im erkannten Elementdatensatz zu.
u_mac_address	mac_address	Ordnet den ersten mac_address-Wert dem mac-Adressfeld im erkannten Elementdatensatz zu.
u_fqdns	fqdn	Ordnet den ersten fqdn-Wert dem fqdn-Feld im erkannten Elementdatensatz zu.
u_netbios_names	netbios	Ordnet den ersten netbios-Wert dem Feld netbios im erkannten Elementdatensatz zu.
u_Operating_Systems	os	Ordnet den ersten BS-Wert dem Feld „betriebssystem“ im erkannten Elementdatensatz zu.
(Vor v14.0 Vulnerability Response Und v2.2 der Tenable-Schwachstellenintegration) u_Last_Scan_time	Last_Scan_date	Ordnet das Feld Last_Scan_date im erkannten Elementdatensatz zu.
u_Last_authenticated_Scan_date	Last_auth_Scan_date	Ordnet das Feld Last_auth_Scan_date im erkannten Elementdatensatz zu.
[Skript]	name	Ordnet den Hostnamen anhand der Logik des Skripts zu.
u_tags		Die Tags werden in sn_sec_cmn_Host_Tag gespeichert. Die Zuordnung von Tags zu Assets wird in sn_sec_cmn_m2m_src_ci_Tag gespeichert.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Tenable.io Asset-Transformationsskript für Zeitplan und Zweck der Zuordnung

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Initialisiert die Werte in Import_Set für den Integrationsprozess. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Aktualisiert Werte im Host und überprüft, ob der Host vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einem Import_Set. Dieses Skript ist zur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
	internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Legt die Werte von neu erstellten CIs und von CIs fest, die aktualisiert und ignoriert wurden.dieses Skript ist für die interne Verwendung vorgesehen, und das Ändern oder Löschen dieser CIs wird nicht empfohlen.

Tenable.io-Plugins-Integration

Die Transformationszuordnung Tenable.io-Plugins wird verwendet, um Plugins zu transformieren, die aus Tenable.io importiert wurden.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern die Verarbeitung von Daten, die von den Tenable-Plugins empfangen werden.

Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach der Tenable.io-Plugin-Transformation.

Die Nutzlast des Tenable.io-Plugins enthält alle Felder in der Spalte u_attributes der Tabelle „sn_vul_Tenable_io_Plugin_Import“. Das Attributfeld wird analysiert und den Datensätzen der Drittpartei-Eintragstabelle zugeordnet, wie in der folgenden Tabelle aufgeführt.

Quellenfeld	Zielfeld	Beschreibung
id	id	Ordnet die ID aus der Quelle zu und fügt ihr das TEN-Präfix hinzu. Wenn die empfangene ID beispielsweise 12345 lautet, lautet die ID in der Zieltabelle TEN-12345.
Beschreibung	Zusammenfassung	Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu.
[Skript]	Quelle	Die Quelle für den importierten Drittparteieintrag (TPE) ist Tenable.io.
[Skript]	Source_instance	Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert.
Familie	Kategorie	Ordnet die Familie des Plugins der Kategoriespalte zu
Plugin_Modification_date	Last_modified	Ordnet Plugin_modify_date dem Feld „zuletzt geändert“ zu.
Plugin_publication_date	date_published	Ordnet Plugin_publication_date dem Veröffentlichungsdatum zu.
Has_Patch	Remediation_type	Ordnet den Korrekturtyp aus dem Wert „has_Patch“ zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
synopsis	Bedrohung	Ordnet die Bedrohungsinformationen zu dieser Schwachstelle zu.
cvss_Base__Score	Punktzahl	Ordnet die Basispunktzahl des Common Vulnerability Scoring System (CVSS) der Punktzahlspalte in der Drittpartei-Eintragstabelle zu.
Lösung	Lösung	Ordnet die vom Scanner bereitgestellte Lösung der Lösungsspalte in der Drittpartei-Eintragstabelle zu.
Exploit_available	Exploit	Ordnet die vom Scanner bereitgestellte Exploit_available der Exploit-Spalte in der Drittpartei-Eintragstabelle zu.
vpr.Punktzahl	Source_Risk_Score	Ordnet die vom Scanner bereitgestellte vpr-Punktzahl der Tabelle „Source_Risk_Score“ in der Drittpartei-Eintragsdatei zu.
[Skript]	Source_Risk_Rating	Ordnet die vpr-Punktzahl der Standard-Risikobewertung basierend auf den Punktzahlbereichen zu: • 9–10: Kritisch • 7–9: Hoch • 4–7: Mittel • 0–4: Niedrig
vpr.Driver.age_of_vuln	Age_of_vuln	Ordnet das Alter der Schwachstelle vom Scanner der Spalte „age_of_vuln“ in der Tabelle „Drittpartei-Eintrag“ zu.
vpr.drivers.Exploit_Code_Reife	Exploit_Code_Reife	Ordnet die Exploit-Code-Reife vom Scanner Exploit_Code_Reife in der Drittpartei-Eintragstabelle zu.
vpr.drivers.product_coverage	Product_Coverage	Ordnet die Produktabdeckung vom Scanner zu „Product_Coverage“ in der Drittpartei-Eintragstabelle zu.
vpr.Treiber.Threat_sources_last28	Threat_sources	Ordnet Bedrohungsquellen der letzten 28 Tage vom Scanner den Threat_sources in der Drittpartei-Tabelle zu.
vpr.Treiber.Threat_Intensity_last28	Threat_Intensity	Ordnet die Bedrohungsintensität in den letzten 28 Tagen aus dem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		Scanner Threat_Intensity in der Drittpartei-Eintragstabelle zu.
vpr.Treiber.Threat_recency	Threat_recency	Ordnet die Bedrohungsaktualisierungsinformationen aus dem Scanner Threat_recency in der Drittpartei-Eintragstabelle zu.
vpr.drivers.cvss3_Impact_Score	V3_Impact_subscore	Ordnet die cvss3-Auswirkungspunktzahl der Spalte v3_impact_subscore in der Drittpartei-Eintragstabelle zu.
cvss_temporal_Punktzahl	cvss_temporal_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v2 zu.
cvss_v3_temporal_Score	V3_temporal_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v3 zu.
risk_factor	Source_severity	Wird dem Quellschweregrad in der Drittpartei-Eintragstabelle zugeordnet.
name	name	Ordnet den Namen des Plugins dem Namen in der Drittpartei-Eintragstabelle zu.
stig_severity	stig_severity	Ordnet die vom Scanner bereitgestellte vpr-Punktzahl der Quelle_Risk_Score in der Tabelle „Drittpartei-Eintrag“ zu.
Plugin_type	Check_type	Ordnet den Plugin-Typ Check_type in der Drittpartei-Eintragstabelle zu.
Nicht supported_by_Vendor	Nicht supported_by_Vendor	Ordnet das Feld nicht supported_by_Vendor der Spalte nicht supported_by_Vendor zu.
[Skript]	Exploit_Attack_Vector	Die Spalte „Exploit_Attack_Vector“ in der Drittpartei-Eintragstabelle wird basierend auf den Spalten „Exploit_available“ und „v3_Attack_Vector“ der ausgefüllt.

Zusätzlich zu den direkten Feldern werden anderen Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

Quellenfeld	Beschreibung
cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dieselben Common Vulnerabilities and Exposures (CVE) in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden werden, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie in sn_vul_m2m_entry_cve.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Beschreibung
bid	Die Liste der Fehlertraqs wird als Referenz hinzugefügt.
Siehe_auch	Die Liste der URLs wird als Referenz hinzugefügt.
xrefs	Die Liste der X-REF wird als Referenz hinzugefügt.
[Skript]	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das anwendbare Exploit-Framework und Plugin in sn_vul_m2m_Framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Initialisiert die Werte in Import_Set für den Integrationsprozess. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Aktualisiert die Werte im Drittparteieintrag und überprüft, ob der Drittparteieintrag vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einem Drittparteieintrag. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Legt die Werte der neu erstellten CIs und der CIs fest, die aktualisiert und ignoriert wurden. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Die Skripteinbindung TenableIOPluginsImportProcessor wird aus dem onBefore-Transformationsskript aufgerufen. Es verwendet die Ausgabe der Integration von Tenable.io-Plugins und wandelt sie in um ServiceNow AI Platform Einträge zu Schwachstellen von Drittparteien. Alle Änderungen an dieser Skripteinbindung können die Transformation von Tenable.io-Plugins-Daten in der Drittpartei-Eintragstabelle ändern.

Import von Tenable.io-Schwachstellen

Die Transformationszuordnung Tenable.io für angreifbare Elemente wird verwendet, um Informationen zu offenen und behobenen Schwachstellen zu transformieren, die aus Tenable.io importiert wurden.

Hinweis:
Änderungen an dieser Transformationszuordnung ändern, wie Daten aus dem Import von Tenable-Schwachstellen verarbeitet werden.

Dieselbe Transformationszuordnung wird sowohl für die Tenable.io-Integration von behobenen Schwachstellen als auch für die Tenable.io-Integration offener Schwachstellen verwendet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach Transformationszuordnung für angreifbares Tenable.io-Element .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_Asset.uuID	id	UUID wird dem ID-Feld des cmdb_ci-Datensatzes zugeordnet.
u_Asset.ipv4	ip_address	Das Feld ipv4 wird dem ip-Adressfeld des cmdb_ci-Datensatzes zugeordnet.
u_Asset.Last_authenticated_results	Last_auth_Scan_date	Das Datum des letzten authentifizierten Scans wird dem Datum des letzten Authentifizierungsscans des cmdb_ci-Datensatzes zugeordnet.
u_Asset.mac_addess	mac_address	Die Mac-Adresse wird dem Feld „Host-mac-Adresse“ des cmdb_ci-Datensatzes zugeordnet.
u_asset.netbios_name	netbios	NetBIOS wird dem Feld netbios des Datensatzes „cmdb_ci“ zugeordnet.
u._Plugin.cvss3_Base_score	V3_Base_Score	Die CVSS v3-Basispunktzahl wird der v3-Basispunktzahl des Drittpartei-Eintragsdatensatzes zugeordnet.
u._Plugin.cvss3_temporal_Score	V3_temporal_Punktzahl	Die temporäre CVSS v3-Punktzahl wird der temporären v3-Punktzahl im Drittparteieintragsdatensatz zugeordnet.
u._Plugin.cvss_Base_Score	Punktzahl	CVSS-Basispunktzahl wird dem Punktzahlfeld des Drittparteieintragsdatensatzes zugeordnet.
u._Plugin.cvss_temporal_Score	Temporal_Punktzahl	Die temporäre Punktzahl wird der temporären Punktzahl im Drittparteieintragsdatensatz zugeordnet.
u_plugin.description	Zusammenfassung	Die Beschreibung wird dem Zusammenfassungsfeld im Drittparteieintragsdatensatz zugeordnet.
u_Plugin.family	Kategorie	Ordnet die Familie des Plugins der Kategoriespalte des Drittpartei-Eintragsdatensatzes zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_Plugin.Modification_date	Last_modified	Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Drittpartei-Eintragsdatensatz zugeordnet.
u_Plugin.publication_date	date_published	Das Veröffentlichungsdatum wird dem Feld Veröffentlichungsdatum des Drittpartei-Eintragsdatensatzes zugeordnet.
u_Plugin.Risk_factor	Source_severity	Der Risikofaktor wird dem Feld „Source_severity“ des Drittpartei-Eintragsdatensatzes zugeordnet.
u_Plugin.Lösung	Lösung	Die Lösung wird dem Lösungsfeld des Drittpartei-Eintragsdatensatzes zugeordnet.
u_Plugin.Synopse	Bedrohung	Die Synopse wird dem Bedrohungsfeld des Drittpartei-Eintragsdatensatzes zugeordnet.
u_Schweregrad_ID	Priorität	Priorität wird der Schweregrad-ID aus der Nutzlast zugeordnet. Der Standardwert ist 5.
u_Plugin.Exploit_available	Exploit	Ordnet die vom Scanner bereitgestellte Exploit_available der Exploit-Spalte in der Drittpartei-Eintragstabelle zu.
vpr.Punktzahl	Source_Risk_Score	Ordnet die vom Scanner bereitgestellte vpr-Punktzahl der Quelle_Risk_Score in der Tabelle „Drittpartei-Eintrag“ zu.
[Skript]	Source_Risk_Rating	Ordnet die vpr-Punktzahl der Standard-Risikobewertung basierend auf den Punktzahlbereichen zu: • 9–10: Kritisch • 7–9: Hoch • 4–7: Mittel • 0–4: Niedrig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_Plugin.vpr.drivers.age_of_vuln	Age_of_vuln	Ordnet das Alter der Schwachstelle aus dem Scanner Age_of_vuln in der Drittpartei-Eintragstabelle zu.
u_Plugin.vpr.drivers.Exploit_Code_Reife	Exploit_Code_Reife	Ordnet die Exploit-Code-Reife vom Scanner Exploit_Code_Reife in der Drittpartei-Eintragstabelle zu.
u_plugin.vpr.drivers.product_coverage	Product_Coverage	Ordnet die Produktabdeckung vom Scanner zu „Product_Coverage“ in der Drittpartei-Eintragstabelle zu.
u_Plugin.vpr.Treiber.Threat_sources_last28	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner Threat_sources in der Drittpartei-Eintragstabelle zu.
u_Plugin.vpr.Treiber.Threat_Intensity_last28	Threat_Intensity	Ordnet die Bedrohungsintensität in den letzten 28 Tagen aus dem Scanner Threat_Intensity in der Drittpartei-Eintragstabelle zu.
u_Plugin.vpr.Driver.Threat_recency	Threat_recency	Ordnet die Bedrohungsaktualisierungsinformationen aus dem Scanner Threat_recency in der Drittpartei-Eintragstabelle zu.
u_Plugin.vpr.drivers.cvss3_Impact_Score	V3_Impact_subscore	Ordnet die CVSS3 v3-Auswirkungspunktzahl der Spalte v3_Impact_subscore in der Drittpartei-Eintragstabelle zu.
u_Plugin.type	Check_type	Ordnet den Plugin-Typ Check_type in der Drittpartei-Eintragstabelle zu.
u_Plugin.Unsupported_by_Vendor	Nicht supported_by_Vendor	Ordnet das Feld nicht supported_by_Vendor im Plugin der Spalte nicht supported_by_Vendor zu.
[Skript]	Exploit_Attack_Vector	Die Spalte „Exploit_Attack_Vector“ in der Drittpartei-Eintragstabelle wird basierend auf den Spalten „Exploit_available“ und „v3_Attack_Vector“ der ausgefüllt.
u_Plugin.Family_ID	Family_ID	Ordnet die Plugin-Familien-ID der Spalte „Family_ID“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		in der Tabelle „Drittpartei-Eintrag“ zu.
port	port	Port wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.
protocol	protocol	Protokoll wird dem Protokollfeld des Datensatzes für angreifbare Elemente zugeordnet.
u_first_found	first_found	„Zuerst gefunden“ wird dem Feld „zuerst gefunden“ des Datensatzes des angreifbaren Elements zugeordnet.
u_Last_found	Last_found	„Zuletzt gefunden“ wird dem Feld „zuletzt gefunden“ des Datensatzes für angreifbare Elemente zugeordnet.
u_state	Status	Status wird dem Feld Status im Datensatz des angreifbaren Elements zugeordnet
[Skript]	Quelle	Die Quelle der Integration ist ausgefüllt. Die aus dieser Integration erstellten angreifbaren Elemente haben Tenable.io als Quelle.
[Skript]	Integration_instance	„Integration_instance“ ist der Name der Instanz, aus der das angreifbare Element importiert wird.
u_plugin.name	name	Ordnet den Namen des Plugins dem Namen in der Drittpartei-Eintragstabelle zu.
u_Plugin.stig_severity	stig_severity	Ordnet den stig-Schweregrad des Plugins der stig-Schweregrad-Spalte in der Drittpartei-Eintragstabelle zu

Zusätzlich zu den direkten Feldern werden anderen Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

Quellenfeld	Beschreibung
cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung finden Sie in sn_vul_m2m_entry_cve.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Beschreibung
bid	Die Liste der Fehlertraqs wird als Referenz hinzugefügt.
Siehe_auch	Die Liste der URLs wird als Referenz hinzugefügt.
xrefs	Die Liste der X-REF wird als Referenz hinzugefügt.
[Skript]	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das anwendbare Exploit-Framework und Plugin in sn_vul_m2m_Framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Tenable-E/A-Schwachstellenprozessor löst aus, der mithilfe des Importsatzes Daten aus Tenable.io importiert und jeden Datensatz in die CMDB-CI-Tabelle, die Tabelle „angreifbare Elemente“ und die Tabelle „Schwachstellen“ von Drittanbietern lädt. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Überprüft, ob der Drittparteieintrag und die Erkennungen vorhanden sind. Wenn nicht, werden diese Datensätze in ihren jeweiligen Tabellen erstellt. isn’tDieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Aktualisiert die Anzahl der CIs, Vits und Erkennungen wie aus Tenable.io importiert. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Tenable.sc-Asset-Import

Asset-Daten, die aus Tenable.sc importiert wurden, werden zuerst in die Tabelle „Tenable.sc Asset-Import“ (sn_vul_Tenable_sc_Asset_Import) geladen. Die Transformationszuordnung Tenable.sc Asset Integration wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Import von Tenable-Assets verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach Tenable.sc Asset-Transformation .

Quellenfeld	Zielfeld	Beschreibung
u_uuid	id	Die UUID wird nicht aus der Tenable-API ausgefüllt, daher wird das Attribut „u_uniqueness“ verwendet, um ein eindeutiges UUID-Feld für Assets zu erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		und dem cmdb_ci-Datensatz zuzuordnen.
u_ip	ip_address	Ordnet das ip-Feld aus der API dem Feld ip_address in einem cmdb_ci-Datensatz zu.
u_macaddress	mac_address	Ordnet das mac-Adressfeld aus der API dem Adressfeld im cmdb_ci-Datensatz zu.
u_dnsname	fqdn	Ordnet das dnsname-Feld aus der API dem fqdn-Feld im cmdb_ci-Datensatz zu.
u_netbiosname	netbios	Ordnet das netbios-Feld aus der API dem netbios-Feld im cmdb_ci-Datensatz zu.
u_Oscpe	os	Die BS-Informationen werden aus dem Oszillosattribut in der Nutzlast extrahiert und dem Feld „betriebssystem“ im cmdb_ci-Datensatz zugeordnet.
u_lastauthrun	Last_auth_Scan_date	Ordnet das Feld lastauthrun aus der API dem Feld Last_auth_Scan_date im erkannten Elementdatensatz zu.
u_lastauthrun und u_lastunauthrun	Last_Scan_date	Der lastauthrun wird aus der Tenable-API oder lastunauthrun extrahiert. Das Feld Last_Scan_date im erkannten Elementdatensatz wird basierend auf dem Wert ausgefüllt, der in der Nutzlast angezeigt wird.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Initialisiert die Werte in Import_Set für den Integrationsprozess. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Aktualisiert die Werte im Host und überprüft, ob der Host vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einem Import_Set. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Legt die Werte der neu erstellten CIs und der CIs fest, die aktualisiert und ignoriert wurden. Dieses Skript

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
	ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Import von Tenable.sc-Plugins

Plugins-Daten, die aus Tenable.sc importiert werden, werden zuerst in die Tabelle „Plugins-Import“ (sn_vul_Table_sc_Plugin_Import) von Tenable.sc geladen. Die Tenable.sc-Plugin-Transformationszuordnung wird verwendet, um die importierten Plugin-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem Tenable-Plugin-Import verarbeitet werden. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach Tenable.sc-Plugin-Transformationszuordnung .

Quellenfeld	Zielfeld	Beschreibung
u_id	id	Ordnet die ID aus der Quelle zu und fügt das TEN-Präfix hinzu. Wenn die empfangene ID beispielsweise 12345 lautet, lautet die ID in der Zieltabelle TEN-12345.
u_description	Zusammenfassung	Ordnet die Beschreibung des Plugins der Zusammenfassungsspalte zu.
[Skript]	Quelle	Aus dieser Integration importierte TPE hat Tenable.sc als Quelle.
[Skript]	Source_instance	Verweis auf die Tenable-Bereitstellung, die diesen Datensatz importiert.
u_Family	Kategorie	Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte zu.
u_Plugin_Modification_date	Last_modified	Ordnet Plugin_modify_date dem Feld „zuletzt geändert“ zu.
u_Plugin_publication_date	date_published	Ordnet Plugin_publication_date dem Veröffentlichungsdatum zu.
u_has_Patch	Remediation_type	Ordnet den Korrekturtyp aus dem Wert „has_Patch“ zu.
u_Synopse	Bedrohung	Ordnet die Bedrohungsinformationen zu dieser Schwachstelle zu.
u_cvss_Base_Score	Punktzahl	Ordnet die CVSS-Basispunktzahl der Punktzahlspalte in der Drittpartei-Eintragstabelle zu.
u_Solution	Lösung	Ordnet die vom Scanner bereitgestellte Lösung der Spalte „Lösung“ in der Tabelle „Drittpartei-Einträge“ zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_cvss_temporal_Punktzahl	cvss_temporal_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v2 zu.
u_cvss_v3_temporal_Score	V3_temporal_Punktzahl	Ordnet die temporäre Punktzahl für CVSS v3 zu.
u_Risk_factor	Quellenschweregrad	Wird dem Quellschweregrad in der Drittpartei-Eintragstabelle zugeordnet.
u_cvss_v3_Base_Score	V3_Base_Score	Ordnet die CVSS-Basispunktzahl in der Drittpartei-Eintragstabelle zu.
u_Exploit_available	Exploit	Ordnet das vom Scanner bereitgestellte exploitAvailable der Exploit-Spalte in der Tabelle „Drittpartei-Eintrag“ zu.
u_vpr_Punktzahl	Source_Risk_Score	Ordnet die VPR-Punktzahl aus dem Scanner der Quell-Risikopunktzahl in der Drittpartei-Eintragstabelle zu.
[Skript]	Source_Risk_Rating	Ordnet die vpr-Punktzahl der Standard-Risikobewertung basierend auf den Punktzahlbereichen zu: • 9–10: Kritisch • 7–9: Hoch • 4–7: Mittel • 0–4: Niedrig
u_vpr_context[ID=age_of_vuln]	Age_of_vuln	Ordnet das Alter der Schwachstelle aus dem Scanner Age_of_vuln in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID=Exploit_Code_Reife]	Exploit_Code_Reife	Ordnet die Exploit-Code-Reife vom Scanner Exploit_Code_Reife in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID=Product_Coverage]	Product_Coverage	Ordnet die Produktabdeckung vom Scanner zu „Product_Coverage“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID="Threat_sources_last_28"]	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28 Tagen vom Scanner zu Threat_sources in der Drittparteitabelle zu.
u_vpr_context[ID="Threat_Intensity_last_28"]	Threat_Intensity	Ordnet die Bedrohungsintensität in den letzten 28 Tagen aus dem Scanner Threat_Intensity in der Drittpartei-Eintragstabelle zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_vpr_context[ID=”Threat_recency”]	Threat_recency	Ordnet die Bedrohungsaktualisierungsinformationen aus dem Scanner Threat_recency in der Eintragstabelle des dritten Teils zu.
u_vpr_context[ID=cvssV3_impactScore]	V3_Impact_subscore	Ordnet die CVSS v3-Auswirkungsbewertung aus dem Scanner v3_impact_subscore in der Drittpartei-Eintragstabelle zu.
u_name	name	Ordnet den Namen des Plugins der Namensspalte in der Drittpartei-Eintragstabelle zu.
u_stig_severity	stig_severity	Ordnet das Feld „stig_severity“ im Plugin „stig_severity“ in der Drittpartei-Eintragstabelle zu.
u_Check_type	Check_type	Ordnet den Prüftyp Check_type in der Drittpartei-Eintragstabelle zu.
u_family.ID	Family_ID	Ordnet das Plugin „Family_ID“ der „family_ID“ in der Drittpartei-Eintragstabelle zu.
[Skript]	Exploit_Attack_Vector	Die Spalte „Exploit_Attack_Vector“ in der Drittpartei-Eintragstabelle wird basierend auf den Spalten „Exploit_available“ und „v3_Attack_Vector“ der ausgefüllt.

Zusätzlich zu den direkten Feldern werden anderen Informationen als zugehörige Listen zu Drittparteieinträgen hinzugefügt.

Quellenfeld	Beschreibung
u_cpe	Die Liste der CPEs wird als Referenz hinzugefügt.
u_See_auch	Die Liste der URLs wird als Referenz hinzugefügt.
u_Exploit_Frameworks	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das anwendbare Exploit-Framework und Plugin in sn_vul_m2m_Framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Diese Transformation wird verwendet, um die Werte in Import_Set für den Integrationsprozess zu initialisieren. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Skript ausgeführt wird	Zweck
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Funktion, die verwendet wird, um die Werte im Drittparteieintrag zu aktualisieren und zu überprüfen, ob der Drittparteieintrag vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einem Drittparteieintrag. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Diese Transformation wird verwendet, um die Werte von Plugins festzulegen, die erstellt und ignoriert wurden. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Die Skripteinbindung TenableSCPluginsImportProcessor wird aus dem onBefore-Transformationsskript aufgerufen. Es übernimmt die Ausgabe aus der Plugin-Integration Tenable.sc und wandelt sie in um ServiceNow Einträge zu Schwachstellen von Drittparteien. Alle Änderungen an dieser Skripteinbindung können die Transformation von Tenable.sc-Plugins-Daten in der Drittpartei-Eintragstabelle ändern.

Import von Tenable.sc-Schwachstellen

Die Transformationszuordnung Tenable.sc offene Schwachstellen wird verwendet, um importierte Daten aus der Tenable.sc-Integration offener Schwachstellen zu transformieren, und die Transformationszuordnung Tenable.sc und behobene Schwachstellen werden verwendet, um importierte Daten aus der Tenable.sc-Integration für behobene Schwachstellen zu transformieren.

Hinweis:
Änderungen an diesen Transformationszuordnungen ändern, wie Daten aus dem Import von behobenen/offenen Tenable-Schwachstellen verarbeitet werden.

Um auf die Transformationszuordnungen Tenable.sc offene und behobene Schwachstellen zuzugreifen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationsinstanzen** > **Tenable.sc – Integration von behobenen/offenen Schwachstellen** > **Datenquellen** > **Tenable.sc offene/behobene Schwachstellen** > **Transformationen**an.

Quellenfeld	Zielfeld	Beschreibung
u_Pluginid	ID	Wird als Bezeichner für das Plugin verwendet. Dieses Feld ist der Plugin-ID im Drittpartei-Eintragsdatensatz zugeordnet.
u_risikofaktor	Source_severity	Dieses Feld ist Source_severity im Drittpartei-Eintragsdatensatz zugeordnet.
u_severity	Priorität	Das Prioritätsfeld wird dem Schweregrad zugeordnet. Der Standardwert ist 5.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
u_hasbeengemindert	Status	Wurde gemindert ist dem Statusfeld des Schwachstellendatensatzes zugeordnet. Für die Integration behobener Schwachstellen befinden sich alle VIS im Status „Geschlossen“.
u_ip	ip_address	Die IP-Adresse wird dem Host-ip-Feld der Tabelle „cmdb_ci“ zugeordnet.
u_Port	port	Port wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.
u_protocol	protocol	Das Protokoll wird dem Portfeld des Datensatzes des angreifbaren Elements zugeordnet.
u_firstSeen	first_found	Der erste sichtbare Wert wird dem Feld zuerst gefunden des VI-Datensatzes zugeordnet.
u_lastSeen	Last_found	Der zuletzt gesehene Wert wird dem Feld zuletzt gefunden des VI-Datensatzes zugeordnet.
u_exploitAvailable	Exploit	ExploitAvailable wird dem Exploit-Feld im Drittpartei-Eintragsdatensatz zugeordnet.
u_Synopse	Bedrohung	Die Synopse wird dem Bedrohungsfeld im Drittparteieintragsdatensatz zugeordnet.
u_description	Zusammenfassung	Die Beschreibung wird dem Zusammenfassungsfeld im Drittparteieintragsdatensatz zugeordnet.
u_Solution	Lösung	Die Lösung wird dem Lösungsfeld im Drittpartei-Eintragsdatensatz zugeordnet.
u_basescore	Punktzahl	BaseScore wird dem Punktzahlfeld im Drittparteieintragsdatensatz zugeordnet.
u_temporalScore	Temporal_Punktzahl	Die temporäre Punktzahl wird der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		temporären Punktzahl im Drittparteieintragsdatensatz zugeordnet.
u_cvssv3basescore	V3_Base_Score	Cvssv3basescore wird der v3-Basispunktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u_cvsstemporalPunktzahl	V3_temporal_Punktzahl	Die temporäre Cvssv3Punktzahl wird der temporären v3-Punktzahl im Drittpartei-Eintragsdatensatz zugeordnet.
u_Pluginpubdate	date_published	Das Veröffentlichungsdatum des Plugins wird dem Veröffentlichungsdatum des Plugins im Drittpartei-Eintragsdatensatz zugeordnet.
u_Pluginmoddate	Last_modified	Das Datum der letzten Änderung wird dem Datum der letzten Änderung des Plugins im Drittpartei-Eintragsdatensatz zugeordnet.
u_dnsname	fqdn	DnsName wird dem FQDN-Feld des cmdb_ci-Datensatzes zugeordnet.
u_macaddress	mac_address	MacAddress wird dem Feld „mac_address“ des Datensatzes „cmdb_ci“ zugeordnet.
u_netbiosName	netbios	NetbiosName wird dem Feld „NETBIOS“ des cmdb_ci-Datensatzes zugeordnet.
u_ip	ip	IP ist dem IP-Feld des cmdb_ci-Datensatzes zugeordnet.
hostUniqueness	uuid	Die Hosteindeutigkeit ist keinem Feld zugeordnet, wird jedoch verwendet, um die UUID für den Host zu bestimmen.
u_Family	Kategorie	Ordnet das Namensfeld im Familienobjekt des Plugins der Kategoriespalte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		des Drittpartei-Eintragsdatensatzes zu.
u_plugintext	Nachweis	Plugin-Text wird dem Nachweis im tpe-Datensatz zugeordnet.
[Skript]	Quelle	Die Quelle der Integration ist ausgefüllt. Die aus dieser Integration erstellten angreifbaren Elemente haben Tenable.sc als Quelle.
[Skript}	Integration_instance	„Integration_instance“ ist der Name der Instanz, aus der das angreifbare Element importiert wird.
u_vpr_Punktzahl	Source_Risk_Score	Ordnet die VPR-Punktzahl aus dem Scanner der Quell-Risikopunktzahl in der Drittpartei-Eintragstabelle zu.
[Skript]	Source_Risk_Rating	Ordnet die vpr-Punktzahl der Standard-Risikobewertung basierend auf den Punktzahlbereichen zu: • 9 Bis 10: Kritisch • 7–9: Hoch • 4–7: Mittel • 0–4: Niedrig
u_vpr_context[ID=age_of_vuln]	Age_of_vuln	Ordnet das Alter der Schwachstelle aus dem Scanner Age_of_vuln in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID=Exploit_Code_Reife]	Exploit_Code_Reife	Ordnet die Exploit-Code-Reife vom Scanner Exploit_Code_Reife in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID=Product_Coverage]	Product_Coverage	Ordnet die Produktabdeckung vom Scanner zu „Product_Coverage“ in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID="Threat_sources_Last_28]	Threat_sources	Ordnet Bedrohungsquellen in den letzten 28

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Zielfeld	Beschreibung
		Tagen vom Scanner Threat_sources in der Drittparteitabelle zu.
u_vpr_context[ID="Threat_Intensity_Last_28]	Threat_Intensity	Ordnet die Bedrohungsintensität in den letzten 28 Tagen aus dem Scanner Threat_Intensity in der Drittpartei-Eintragstabelle zu.
u_vpr_context[ID=”Threat_recency”]	Threat_recency	Ordnet die Bedrohungsaktualisierungsinformationen aus dem Scanner Threat_recency in der Eintragstabelle des dritten Teils zu.
u_vpr_context[ID=cvssV3_impactScore]	V3_Impact_subscore	Ordnet die CVSS v3-Auswirkungsbewertung aus dem Scanner v3_impact_subscore in der Drittpartei-Eintragstabelle zu.
u_pluginname	name	Ordnet den Namen des Plugins der Namensspalte in der Eintragstabelle von Drittparteien zu.
u_stigseverity	stig_severity	Ordnet das Feld „stig_severity“ im Plugin „stig_severity“ in der Eintragstabelle von Drittparteien zu.
u_checktype	Check_type	Ordnet den Prüftyp Check_type in der Drittpartei-Eintragstabelle zu.
u_family.ID	Family_ID	Ordnet das Plugin „Family.ID“ der „family_ID“ in der Drittpartei-Eintragstabelle zu.
[Skript]	Exploit_Attack_Vector	Die Spalte „Exploit_Attack_Vector“ in der Tabelle „Third_Party_entry“ wird basierend auf den Spalten „Exploit_available“ und „v3_Attack_Vector“ ausgefüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quellenfeld	Beschreibung
u_cve	Fügt CVE-bezogene Daten in die Referenztabelle (sn_vul_nvd_entry) ein. Wenn dasselbe CVE in der NVD-Eintragstabelle (sn_vul_nvd_entry) gefunden wird, wird die aktuelle Schwachstelle dem NVD-Eintrag zugeordnet. Die Zuordnung befindet sich in sn_vul_m2m_entry_cve.
u_bid	Die Liste der Fehlertraqs wird als Referenz hinzugefügt.
u_cpe	Die Liste der CPEs wird als Referenz hinzugefügt.
u_seeauch	Die Liste der URLs wird als Referenz hinzugefügt.
u_xrefs	Die Liste der X-Referenzen wird als Referenz hinzugefügt.
u_exploitFrameworks	Die Liste der Exploits für dieses Plugin und fügt die Zuordnung für das anwendbare Exploit-Framework und Plugin in sn_vul_m2m_Framework_vul ein.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Diese Transformation wird verwendet, um die Werte in Import_Set für den Integrationsprozess zu initialisieren. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Funktion, die verwendet wird, um die Werte in der Schwachstelle zu aktualisieren und zu überprüfen, ob die Schwachstelle vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einer Tabelle für angreifbare Elemente. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Diese Transformation wird verwendet, um die Werte neuer erstellter VIS und von VIS festzulegen, die aktualisiert und ignoriert wurden. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Tenable.cs Container-Asset-Import

Importierte Asset-Daten werden zuerst in geladen Tenable.cs Container-Asset-Import [sn_vul_TENABLE_cs_Container_Asset_Import] Tabelle.

Die Tenable.cs Die Container-Asset-Transformationszuordnung wird verwendet, um die importierten Asset-Informationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem geändert werden Tenable.cs Container-Asset-Import wird verarbeitet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

System-Importsätze > Transformationszuordnungen. Suchen Sie nach Tenable.cs Container-Asset-Transformation.

In den folgenden Tabellen werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Tenable.cs Container-Asset-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_Digest	Image_ID	Tenable bietet einen eindeutigen Digest für die Container-Assets und ordnet dem erkannten Container-Image und dem Docker-Image-Datensatz zu und wird für die CI-Suche verwendet.
u_Digest	Image_Digest	Tenable bietet einen eindeutigen Digest für die Container-Assets und ordnet dem erkannten Container-Image und dem Docker-Image-Datensatz zu und wird für die CI-Suche verwendet.
u_name	name	Ordnet dem Namensfeld des Docker-Image-Datensatzes zu.
u_repositoryuri	name	Ordnet dem Container-Repository-Datensatz zu
u_repositoryuri	Repository	Ordnet dem erkannten Container-Image-Datensatz zu.
u_virtualMachines	Host_list	Ordnet dem erkannten Container-Image-Datensatz zu
u_Bezeichnungen	Image_Bezeichnungen	Ordnet den ersten BS-Wert dem bs-Feld des erkannten Elementdatensatzes zu.
u_Cluster	Image_Cluster	Ordnet dem erkannten Container-Image-Datensatz zu
u_imagetags	tags	Ordnet dem erkannten Container-Image-Datensatz zu
u_cloudProvider	Cloud_Provider	Ordnet dem erkannten Container-Image-Datensatz zu
u_accountid	Cloud_Account_IDs	Ordnet dem erkannten Container-Image-Datensatz zu
u_region	Cloud_Regions	Ordnet dem erkannten Container-Image-Datensatz zu
u_operatingsystem	os	Ordnet dem erkannten Container-Image-Datensatz zu
u_Scantime	Last_Scan_date	Ordnet dem erkannten Container-Image-Datensatz zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Tenable.cs Zeitplan und Zweck der Container-Asset-Transformationszuordnung

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Diese Transformation wird verwendet, um die Werte in Import_Set für den Integrationsprozess zu initialisieren. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Eine Funktion, mit der Werte im Host aktualisiert und überprüft werden, ob der Host vorhanden ist. Ändert basierend auf den Ergebnissen die Werte in einem Import_Set. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Diese Transformation wird verwendet, um die Werte von neu erstellten CIs und CIs festzulegen, die aktualisiert und ignoriert wurden. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Tenable.cs Import Von Container-Schwachstellen

Importierte Container-Schwachstellendaten werden zuerst in geladen Tenable.cs Container-Schwachstellenimport [sn_vul_TENABLE_cs_Container_vuln_Import] Tabelle.

Die Tenable.cs Die Container-Schwachstellen-Transformationszuordnung wird verwendet, um die importierten Container-Schwachstelleninformationen zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem geändert werden Tenable.cs Container-Schwachstellenimport wird verarbeitet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **Transformationszuordnungen**an. Suchen Sie nach Tenable.cs Container-Schwachstellen-Transformation.

In den folgenden Tabellen werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
[Skript]	Image_ID	Digest wird aus dem Feld „Resource.ID“ aus der API extrahiert und dem Feld „image_ID“ des erkannten Container-Image- und Docker-Image-Datensatzes zugeordnet.
[Skript]	Image_Digest	Digest wird aus dem Feld „Resource.ID“ aus der API extrahiert und dem Feld

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
		„image_Digest“ des erkannten Container-Image- und Docker-Image-Datensatzes zugeordnet.
[Skript]	name	Repository-Informationen werden aus dem Namensfeld extrahiert und dem Docker-Image- und Container-Repository-Datensatz zugeordnet.
[Skript]	Repository	Repository-Informationen werden aus dem Namensfeld extrahiert und zugeordnet, um den Container-Image-Datensatz zu erkennen.
u_resource.Bezeichnungen	Image_Bezeichnungen	Ordnet dem erkannten Container-Image-Datensatz zu
u_resource.CloudProvider	Cloud_Provider	Ordnet dem erkannten Container-Image-Datensatz zu
u_resource. AccountId	Cloud_Account_IDs	Ordnet dem erkannten Container-Image-Datensatz zu
u_resource.Region	Cloud_Regions	Ordnet dem erkannten Container-Image-Datensatz zu
u_Vulnerability. ID	id	Ordnet die ID aus der Quelle zu und fügt das TEN-Präfix hinzu. Wenn die empfangene ID beispielsweise 12345 lautet, lautet die ID in der Tabelle „Drittpartei-Eintrag“ TEN-12345.
u_Vulnerability. Beschreibungs-Id	Zusammenfassungs-ID	Wird dem Drittpartei-Eintragsdatensatz zugeordnet. Oder CVE-Datensatz.
u_Vulnerability.Schweregrad	v4_Base_severity	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.VprScore	Source_Risk_Score	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.VprSchweregrad	Source_severity	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.AttackVector	v4_Attack_Vector	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.ExploitReife	v4_Exploit_Reife	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
[Skript]	Quelle	Die Quelle für importierte TPE ist Tenable.cs.
u_Vulnerability.ID	name	Ordnet dem Datensatz der Schwachstellenreferenzen zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_Vulnerability. Links	URL	Ordnet dem Datensatz der Schwachstellenreferenzen zu
	Schwachstelle	Verweis auf TPE oder CVE im Datensatz der Schwachstellenreferenzen
u_Software.Name	name	Ist dem Container-Image-Paket-Datensatz zugeordnet
u_Software.Version	Version	Ist dem Container-Image-Paket-Datensatz zugeordnet
u_Software.Typ	Package_type	Ist dem Container-Image-Paket-Datensatz zugeordnet
u_softwarepfade	path	Ist dem Container-Image-Paket-Datensatz zugeordnet
u_gelöst	status	Ordnet dem Container-Image-Ergebnisdatensatz zu
u_firstscantime	first_found	Ordnet dem Container-Image-Ergebnisdatensatz zu
u_resource.ScanTime	Last_found	Ordnet dem Container-Image-Ergebnisdatensatz zu
u_Vulnerability.Description	Nachweis	Ordnet dem Container-Image-Ergebnisdatensatz zu
u_gelöst	Status	Ordnet dem Datensatz des angreifbaren Containerelements zu
u_firstscantime	first_found	Ordnet dem Datensatz des angreifbaren Containerelements zu
u_resource.ScanTime	Last_found	Ordnet dem Datensatz des angreifbaren Containerelements zu
[Skript]	Quelle	Die Quelle für den Datensatz des angreifbaren Containerelements ist Tenable.cs.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Tenable.cs Zeitplan und Zweck der Container-Schwachstellen-Transformationszuordnung

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Löst den TenableCS Container Vulnerabilities Processor aus, der Daten aus importiert Tenable.cs Mithilfe des Importsatzes und lädt jeden Datensatz in die CMDB-CI-Tabelle, die Tabelle „Angreifbares Element“, die Tabelle „Drittanbieter-Schwachstelleneintrag“, die Referenztabelle für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Zeitplan und Zweck der Container-Schwachstellen-Transformationszuordnung (Fortsetzung)

Wenn das Skript ausgeführt wird	Zweck
	Schwachstellen, das Container-Image-Paket, das Container-Image-Ergebnis und das angreifbare Container-Element. Das Ändern oder Löschen wird nicht empfohlen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist)	Überprüft, ob der Drittparteieintrag und die Bildergebnisse vorhanden sind. Wenn nicht, werden diese Datensätze in ihren jeweiligen Tabellen erstellt. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist)	Aktualisiert die Anzahl der CIs, Vits und Ergebnisse wie aus importiert Tenable.cs. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Tenable.cs Vulnerability-Import Berechnen

Importierte Host-Schwachstellendaten werden zuerst in geladen Tenable.cs Tabelle „Import von Compute-Schwachstellen“ [sn_vul_TENABLE_cs_Compute_vuln_Import].

Die Tenable.cs Die Transformationszuordnung „Schwachstellen berechnen“ wird verwendet, um die importierten Informationen zur Host-Schwachstelle zu transformieren. Änderungen an dieser Transformation ändern, wie Daten aus dem geändert werden Tenable.cs Import von Compute-Schwachstellen wird verarbeitet. Um auf diese Transformationszuordnung zuzugreifen, navigieren Sie zu **System-Importsätze** > **System-Importsätze**an. Suchen Sie nach Tenable.cs Transformation Für „Schwachstellen Berechnen“.

In der folgenden Tabelle werden die Transformationszuordnungsfelder nach Integration aufgelistet.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_resource.ID	object_id	Wird dem CMDB-CI-Datensatz zugeordnet.
u_resource.Name	name	Wird dem CMDB-CI-Datensatz zugeordnet.
	Asset_category	Cloud ist im erkannten Elementdatensatz als Asset-Kategorie zugeordnet.
U_resource.CloudProvider	Cloud_Service_Provider	Wird dem erkannten Elementdatensatz zugeordnet
u_resource.Region	Cloud_Region	Wird dem erkannten Elementdatensatz zugeordnet
u_resource.AccountId	cloud_account	Wird dem erkannten Elementdatensatz zugeordnet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_resource. CloudProvider	Cloud_resource_type	Wird dem erkannten Elementdatensatz zugeordnet
u_resource.ID	resource_id	Wird dem erkannten Elementdatensatz zugeordnet
u_resource.Name	resource_name	Wird dem erkannten Elementdatensatz zugeordnet
u_Vulnerability.ID	id	Ordnet die ID aus der Quelle zu und fügt das TEN-Präfix hinzu. Wenn die empfangene ID beispielsweise 12345 lautet, lautet die ID in der Tabelle „Drittpartei-Eintrag“ TEN-12345. Ordnet die ID auch CVEs zu.
u_Vulnerability. Beschreibung	Zusammenfassung	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.Schweregrad	v4_Base_severity	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.VprScore	Source_Risk_Score	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.VprSchweregrad	Source_severity	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.AttackVector	v4_Attack_Vector	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
u_Vulnerability.ExploitReife	v4_Exploit_Reife	Wird dem Drittpartei-Eintragsdatensatz zugeordnet.
[Skript]	Quelle	Die Quelle für importierte TPE ist Tenable.cs.
u_Vulnerability.ID	name	Ordnet dem Datensatz der Schwachstellenreferenzen zu
u_Vulnerability.Links	URL	Ordnet dem Datensatz der Schwachstellenreferenzen zu
	Schwachstelle	Verweis auf TPE oder CVE im Datensatz der Schwachstellenreferenzen
u_gelöst	status	Ordnet dem Erkennungsdatensatz für angreifbare Elemente zu
u_firstscantime	first_found	Ordnet dem Erkennungsdatensatz für angreifbare Elemente zu
u_resource.ScanTime	Last_found	Ordnet dem Erkennungsdatensatz für angreifbare Elemente zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
u_softwarepfade	Nachweis	Ordnet dem Erkennungsdatensatz für angreifbare Elemente zu
u_softwareresolutionVersionen	Solution_Summary	Ordnet dem Erkennungsdatensatz für angreifbare Elemente zu
u_gelöst	Status	Ist dem Datensatz des angreifbaren Elements zugeordnet
u_firstscantime	first_found	Ist dem Datensatz des angreifbaren Elements zugeordnet
u_resource.ScanTime	Last_found	Ist dem Datensatz des angreifbaren Elements zugeordnet
[Skript]	Quelle	Die Quelle für den Datensatz für angreifbare Elemente ist Tenable.cs.

Während des Transformationsprozesses werden drei Transformationsskripts ausgeführt. In der folgenden Tabelle werden die Ausführung jedes Skripts und sein Zweck aufgeführt.

Tenable.cs Zeitplan und Zweck der Konvertierungszuordnung für „Schwachstellen berechnen“

Wenn das Skript ausgeführt wird	Zweck
OnStart (wenn die Transformation eines Importsatzes gestartet wurde)	Löst Tenable CS Compute Vulnerabilities Processor aus, der Daten aus importiert Tenable.cs Mithilfe des Importsatzes und lädt jeden Datensatz in die CMDB-CI-Tabelle, die Tabelle „angreifbare Elemente“ und die Tabelle „Schwachstellen von Drittparteien“. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnBefore (bevor die Transformation eines Importsatzes abgeschlossen ist).	Überprüft, ob der Drittparteieintrag und die Erkennungen vorhanden sind. Wenn nicht, werden diese Datensätze in ihren jeweiligen Tabellen erstellt. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.
OnComplete (wenn die Transformation eines Importsatzes abgeschlossen ist).	Aktualisiert die Anzahl der CIs, Vits und Erkennungen wie aus importiert Tenable.cs. Dieses Skript ist zur internen Verwendung vorgesehen, und es wird nicht empfohlen, sie zu ändern oder zu löschen.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder

Quellenfeld	Zielfeld	Beschreibung
u_Digest	Image_ID	Ein eindeutiger Digest, der von Tenable für die Container-Assets

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tenable.cs Container-Schwachstellen-Transformationszuordnungsfelder (Fortsetzung)

Quellenfeld	Zielfeld	Beschreibung
		bereitgestellt wird. Er wird dem erkannten Container-Image und dem Docker-Image-Datensatz zugeordnet und für die CI-Suche verwendet.
u_name	name	Ordnet dem Namensfeld des Docker-Image-Datensatzes zu.

Legen Sie zusätzliche Filterparameter für fest Tenable.io Importe

Passen Sie die Filterparameter für Ihre geplanten Abfragen mit an Tenable Vulnerability Integration Damit Sie die mit importierten Schwachstellendaten weiter verfeinern können Tenable.io Produkt.

Vorbereitungen

Anwendungsfälle: Als Schwachstellenmanager oder Analyst möchten Sie möglicherweise Daten aus Ihren Abfragen herausfiltern, damit Sie nur bestimmte Schwachstellendetails überprüfen können. Angenommen, Sie möchten importierte Schwachstellen anzeigen, die gefiltert werden `cidr_range`, `num_assets`, `indexed_at`, Und `plugin_family`. Oder sagen Sie, Sie möchten eine ausführen Tenable.io Integration so, dass eine Ausführung alle vier Stunden nur kritische Schwachstellen importiert und eine andere alle 24 Stunden ausgeführt wird, um alle anderen nicht kritischen Schwachstellen abzurufen.

Um Ihnen beim Sammeln dieser Daten zu helfen, können Sie Tenable-unterstützte Parameter hinzufügen, damit Sie die spezifischen Schwachstellendetails importieren können, die Sie benötigen.

Ohne zusätzliche API-Aufrufe oder Codierung können Sie mit dieser Funktion Ihre HTTP-Anforderungsinformationen mit Tenable-Parametern in anpassen ServiceNow AI Platform. Folgendes Tenable.io Integrationen unterstützen das Filtern durch Bereitstellung von JSON-Inhalten im Anforderungstext:

- Asset-Integration
- Integration Von Behobenen Schwachstellen
- Integration Offener Schwachstellen

Sie sollten wissen, wie Sie verwenden JSON Zeichenfolgen für diese Funktion.

Erforderliche Rolle: sn_vul.Vulnerability_admin

Prozedur

1. Suchen Sie die von unterstützten Parameter Tenable.io Produkt auf der Entwicklerwebsite, das Sie für Ihre Filterung verwenden möchten.

   Parameter und Werte, die Sie aus eingeben Tenable.io Produkte werden nur auf Integrationsinstanzebene unterstützt.

2. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**an.
3. Klicken Sie auf der Listenseite Tenable-Integrationen auf den Datensatz für Tenable.io Integration, die Sie öffnen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wenn die Registerkarte Tenable-REST-Methoden ausgewählt ist, klicken Sie auf das Informationssymbol (I) für REST-Methode gefolgt von **Öffnen Sie Den Datensatz** .
5. Wählen Sie die Registerkarte **HTTP-Anforderung** aus.
6. Um den Datensatz zu bearbeiten, klicken Sie oben auf der Seite auf den Link in . um den Datensatz zu bearbeiten, klicken Sie auf **Hier** .
7. Geben Sie im Datensatz „REST-Methode“ im Feld Inhalt den JSON-Inhalt ein, den Sie als Teil des Anforderungstexts verwenden möchten.

   Beispielsweise können Sie den Schweregradparameter für importierte Schwachstellen als festlegen: `{"filters": {"severity": ["critical"]}}`Für Tenable.io Asset-Integration, sodass nur kritische Schwachstellen importiert werden (CVSS-Punktzahl von 10,0).

   Wenn Sie mehr als einen Parameter eingeben möchten, finden Sie unter Tenable.io Dokumentation für weitere Informationen zur Trennung der einzelnen Werte.
8. Klicken Sie auf **Aktualisieren**.

Tenable-Schwachstellenintegration – Berichterstellung

Zeigen Sie Berichte zu Schwachstellen und angreifbaren Elementen in an Vulnerability Response Dashboards.

Datenvisualisierungen in Vulnerability Response Arbeitsbereiche

Die Vulnerability Response Arbeitsbereiche enthalten Datenvisualisierungen, mit denen Sie Ihren Korrekturfortschritt überwachen können. Sie können die Bedrohungsstufe für Ihre Organisation bestimmen, indem Sie die Anzahl und den Schweregrad der aktiven Schwachstellen anzeigen, die für Ihre Organisation wichtig sind, in dynamischen Datenvisualisierungen, die aktualisiert werden, wenn sich Schwachstellendaten ändern. Siehe Vulnerability Response Arbeitsbereiche, Arbeitsbereich des Schwachstellenmanagers erkunden Und Arbeitsbereich für IT-Korrekturen erkunden Weitere Informationen zu den verfügbaren dynamischen Datenvisualisierungen.

Vorherige Versionen von Vulnerability Response

Das Dashboard „Vulnerability Response-Übersicht“ (Vulnerability Management) bietet einen Überblick über Schwachstellen und angreifbare Elemente, sodass der Schwachstellenadministrator Problembereiche schnell erkennen kann. Mit dem Vulnerability Response-Remediation-Dashboard (Vulnerability Remediation) kann sich ein Korrekturspezialist auf die Korrekturaufgaben und angreifbaren Elemente konzentrieren, die er besitzt.

Weitere Informationen finden Sie unter Wird standardmäßig verwendet Vulnerability Response Dashboards.

Erforderliche Rolle: Korrekturbesitzer.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender in der Vulnerability Response-Anwendung tun und sehen können. Informationen zur anfänglichen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.

Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren Sie zum Anzeigen des Dashboards zu **Vulnerability Response** > **Korrekturübersicht**an.

Statusdiagramm der Integrationsausführung für die Tenable-Schwachstellenintegration

Das Modul Tenable-Integrationsausführungsstatus bietet Ihnen eine grafische Ansicht des Status von Tenable-Integrationsausführungen.

Zeigen Sie im Diagramm auf einen beliebigen Teil des Diagramms, um eine Zusammenfassung der für diesen Teil spezifischen Daten anzuzeigen. Wenn Sie auf ein Teil im Balkendiagramm klicken, wird eine Liste geöffnet, die detailliertere Informationen enthält.

Erforderliche Rolle: Schwachstellenadministrator.

Persona und granulare Rollen sind verfügbar, um zu verwalten, was Anwender in der Vulnerability Response-Anwendung tun und sehen können. Informationen zur anfänglichen Zuweisung der Persona-Rollen im Setup-Assistenten finden Sie unter Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent.

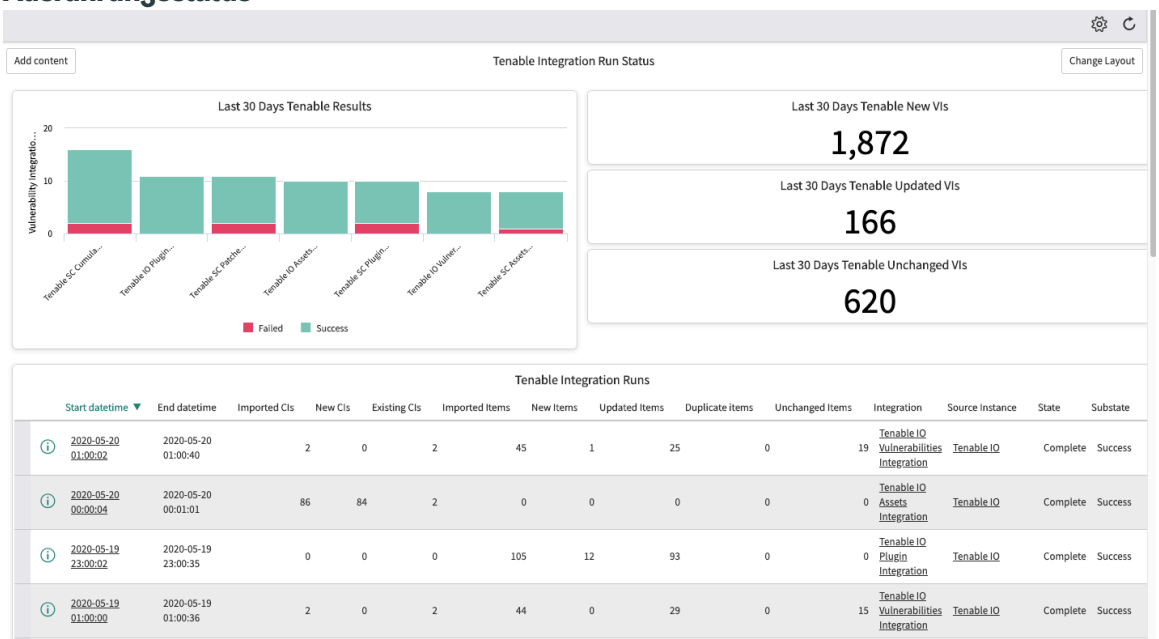
Weitere Informationen zum Verwalten granularer Rollen finden Sie unter Verwalten Sie Persona und granulare Rollen für Vulnerability Response.

Um die Daten anzuzeigen, navigieren Sie zu **Alle** > **Tenable-Schwachstellen-Integration** > **Status der Integrationsausführung**an.

Ab Version 19,0 von Vulnerability Response, Dieses Dashboard ist in der neuen Experience-UI verfügbar.

Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

Ausführungsstatus



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

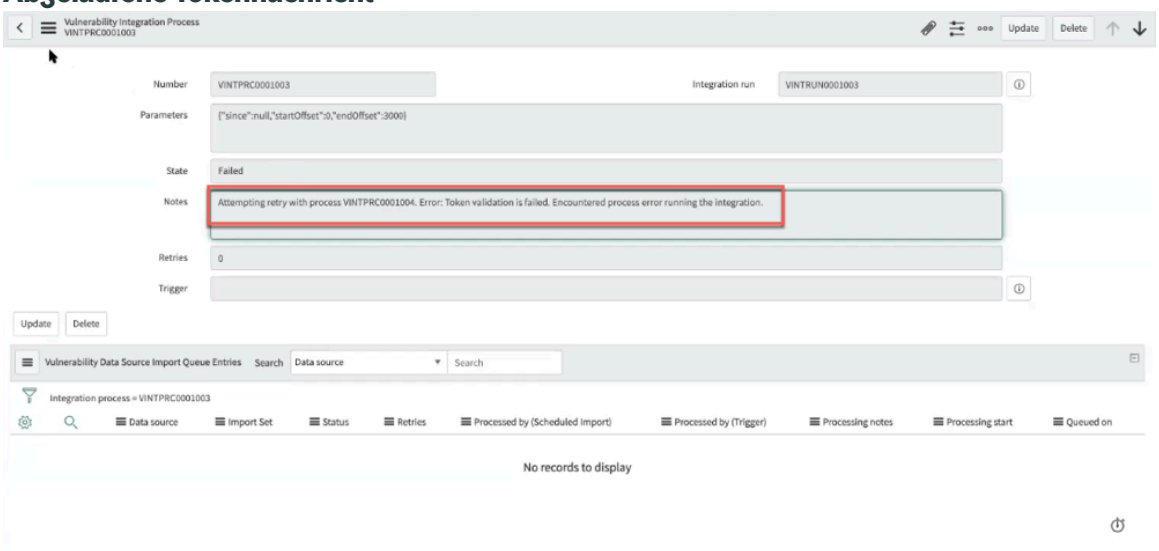
Statusdiagrammberichte der Tenable-Integrationsausführung

Name	Beschreibung
Tenable-Ergebnisse der letzten 30 Tage	Die Anzahl der für jede Integration abgeschlossenen Integrationsausführungen. Zeigt sowohl erfolgreiche als auch fehlgeschlagene Ausführungen an. Jede Ausführung wird als Balken im Diagramm angezeigt.
Neue Tenable-AEs der letzten 30 Tage	Die Anzahl der neuen angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Aktualisierte Tenable-AEs der letzten 30 Tage	Die Anzahl der aktualisierten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Unveränderte Tenable-AEs der letzten 30 Tage	Die Anzahl der doppelten angreifbaren Elemente, die in den letzten 30 Tagen importiert wurden. Wird als Ganzzahl angezeigt.
Tenable-Integrationsausführungen	Die Datensätze der Integrationsausführung in einer Liste. **Hinweis:** **V16.1:** Um die Erkennungen für diese Integration zu überprüfen, vergleichen Sie die Erkennungen oder Ergebnisse mit ServiceNow Erkennungsdaten in `sn_vul_detection`Tabelle. Während die Integration ausgeführt wird, kann sich die Anzahl der Erkennung oder Ergebnisse ändern. Dieser Bericht zeigt die Anzahl der Erkennungen in der Spalte „bis datumsanzahl“ in der Instanz nach Abschluss der Integrationsausführung an.

Ablauf der Token-Validierung

Wenn eine Tenable.sc-Integrationsausführung aus irgendeinem Grund fehlschlägt, läuft das Authentifizierungstoken für Tenable.sc automatisch ab, und im Datensatz des Schwachstellenintegrationsprozesses wird eine Meldung angezeigt.

Abgelaufene Tokennachricht



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für den nächsten Integrationsprozess wird automatisch ein neues Token generiert. Alle Integrationsprozesse, fehlgeschlagen und erfolgreich, werden auf der Registerkarte Prozess der Schwachstellenintegration im Datensatz „Prozess der Schwachstellenintegration“ angezeigt.

Initiieren Sie einen erneuten Scan für Tenable.sc Integration

Stellen Sie sicher, dass Ihre angreifbaren Elemente zwischen den geplanten Scanzyklen behoben wurden, indem Sie erneutes Scannen in der Tenable-Plattform initiieren. Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für initiieren Tenable.sc Produkt aus Ihrem ServiceNow AI Platform® Instanz.

Vorbereitungen

Erforderliche Rollen: sn_vul.write_all oder sn_vul.write_assigned

Hinweis:

Tenable.sc Unterstützt nicht das Starten eines erneuten Scans auf Agent-basierten Computern.

Vergewissern Sie sich, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**an.

Warum und wann dieser Vorgang ausgeführt wird

Informationen zum Initiieren eines erneuten Scans über die Arbeitsbereiche finden Sie unter Erneut Scannen Tenable.io Und Tenable.sc Angreifbare Elemente aus dem Vulnerability Response Arbeitsbereiche.

Führen Sie die unten aufgeführten Schritte aus, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

Um den Overhead und das Volumen für geplante, vollständige Scans, Korrekturbesitzer, IT-Spezialisten, Schwachstellenanalysten zu reduzieren, oder Schwachstellenmanager können bei Bedarf gezielte erneute Scans für bestimmte Schwachstellen in Assets (Konfigurationselementen) in ihren Umgebungen initiieren. Sie können erneutes Scans aus angreifbaren Elementen (VI), Korrekturaufgaben (RT), Drittparteieinträgen (TPE) oder erkannten Elementdatensätzen aus Ihrem initiieren ServiceNow AI Platform Instanz.

Erneutes Durchsuchen erlauben Ihren Korrekturbesitzer und Schwachstellenanalysten Um sicherzustellen, dass Ihre Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben haben.

Beispielsweise wird Ihre gesamte Umgebung alle drei Wochen einmal gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, aber Sie haben gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Ihrem aus initiieren ServiceNow AI Platform Für Tenable.sc Angreifbare Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie einen erneuten Scan von Ihrem anfordern ServiceNow AI Platform® Instanz auswählen Vulnerability Response Integration with Tenable Anmeldeinformationen sind optional. Die ServiceNow® Tenable.sc Die Integration von Scan-Anmeldeinformationen importiert und aktualisiert Scanner-Anmeldeinformationen aus dem Tenable.sc Produkt in Ihrer Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationsdaten zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten. Die ServiceNow® Tenable.sc Integration von Scan-Anmeldeinformationen ist aktiviert (Aktiv) Automatisch aus dem Setup-Assistenten in Ihrer Instanz heraus, wenn Sie konfigurieren Tenable.sc Integrationen von Schwachstellen (Tenable.sc Integrationen offener und behobener Schwachstellen).

Beachten Sie die folgenden Informationen zu den Anmeldeinformationen, die Sie importieren, damit Ihre Anwender sie nach Bedarf von Ihrem aus sehen können ServiceNow AI Platform Instanz:

- Anmeldeinformationen, die mit erstellt wurden Tenable.sc Die Administratoranwenderrolle steht Anwendern in allen Ihren Organisationen zur Verfügung.
- Anmeldeinformationen, die mit erstellt wurden Tenable.sc Die Rolle „Organisationsanwender“ ist nur für Anwender innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden nicht in importiert ServiceNow AI Platform Für Anwender außerhalb der Organisation des Erstellers, es sei denn, sie sind für den Account des Anwenders freigegeben, der für die Verbindung mit der Instanz verwendet wird.

Siehe Tenable.sc Dokumentationswebsite für weitere Informationen.

Siehe Konfigurieren Sie die Tenable-Schwachstellenintegration mit dem Setup-Assistenten Weitere Informationen zum Konfigurieren von Tenable.sc Anwendung. Um weitere Informationen zur Integration von Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Alle** > **Tenable-Schwachstellen-Integration** > **Integrationen** > **Tenable.sc – Integration von Scan-Anmeldeinformationen**an.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- *sn_sec_cmn.record_threshold_heartbeat*: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- *sn_sec_cmn.maximum_heartbeat_delay*: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**an.
2. Suchen Sie den Datensatz des angreifbaren Elements, aus dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   Hinweis:
   Sie können erneutes Scannen für VIS nur mit initiieren Tenable.sc Als Quelle. Verifizieren Tenable.sc Wird in angezeigt **Quelle** Spalte in den VI-Listenansichten oder in **Quelle** Felder in einzelnen Datensätzen. Sie können den Bedingungsgenerator verwenden, um VIS nach Quelle zu gruppieren. Oder wenn die Spalte Quelle in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf **Liste Personalisieren** Symbol (Zahnradsymbol), und verwenden Sie zum Verschieben den Slushbucket **Quelle** Von **Verfügbar** Bis **Ausgewählt** .

3. Alternativ navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** Für die Korrekturaufgaben- bzw. Drittpartei-Eintragsdatensätze, die Sie für den erneuten Scan verwenden möchten.

   Abhängig von Ihrer Auswahl, die **Erneut Scannen** Die Schaltfläche ist für die folgenden Datensätze verfügbar:

   - In einem einzelnen VI-Datensatz muss das VI aus dem stammen Tenable.sc Produkt und in einem anderen Status als **Geschlossen** . Bei mehreren VI-Datensätzen müssen alle VIS aus dem Tenable.sc-Produkt stammen und einen anderen Status als aufweisen **Geschlossen** .
   - In einem RT-Datensatz kann sich die Korrekturaufgabe in einem anderen Status als befinden **Geschlossen** , Und alle zugeordneten VIS müssen aus dem stammen Tenable.sc Produkt.
   - In einem Drittpartei-Eintrag-Datensatz (TPE) muss der Datensatz mindestens einen zugehörigen VI-Datensatz aus dem aufweisen Tenable.sc Produkt in einem anderen Status als **Geschlossen** .

4. Klicken Sie oben rechts im Datensatz auf **Erneut Scannen** .
   Sie werden aufgefordert, die Scanner-Anmeldeinformationen auszuwählen, um auf den Scanner zuzugreifen. Dies sind die Anmeldeinformationen, die von importiert wurden Tenable.sc Integration Von Anmeldeinformationen Scannen.
5. Wählen Sie im Dialogfeld die gewünschten Filter und Anmeldeinformationstypen aus.
6. Klicken Sie Auf **Scan Anfordern** .

   Eine Nachricht wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird. Der Status für alle erneuten Scans kann jederzeit unter den zugehörigen Scan-Listen in den VI-, RT- und TPE-Datensätzen gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht auf **Zeigen Sie Details an** Zum Anzeigen des Status des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erneuten Scans und zum Anzeigen anderer erneutes Scans, die aus einem bestimmten Datensatz gestartet wurden.

Das Feld Status im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Das untergeordnete Element scannt Importdaten. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans.

Ihr ServiceNow AI Platform® Die Instanz verfolgt den Status des erneuten Scans, bis er erfolgreich abgeschlossen ist, oder bis der festgelegte Nachverfolgungszeitraum abgelaufen ist, je nachdem, was zuerst geschieht. Durch die Zeitüberschreitung wird der Scan nicht beendet. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, an dem der ServiceNow AI Platform® Die Nachverfolgung des Status des erneuten Scans wurde beendet, nicht wenn der tatsächliche erneute Scan beendet wurde. Alle VIS, die in übergegangen sind oder übergehen werden **Geschlossen/Behoben** Werden mit dem nächsten geplanten Import der Tenable.sc-Integration für behobene Schwachstellen importiert.

Initiieren Sie einen erneuten Scan für Tenable.io Integration

Überprüfen Sie, ob Ihre angreifbaren Elemente zwischen den geplanten Scanzyklen behoben wurden, indem Sie erneutes Scannen in der Tenable-Plattform initiieren. Sie können bei Bedarf einen erneuten Scan für angreifbare Elemente für initiieren Tenable.io Produkt aus Ihrem ServiceNow AI Platform® Instanz.

Vorbereitungen

Erforderliche Rollen: sn_vul.write_all oder sn_vul.write_assigned

Vergewissern Sie sich, dass Ihr Scanner aktiviert ist, bevor Sie beginnen. Navigieren zu **Vulnerability Response** > **Schwachstellenscan** > **Scanner**an.

Warum und wann dieser Vorgang ausgeführt wird

- Siehe und Scannen Sie Datensätze und Korrekturaufgaben in erneut Arbeitsbereich des Schwachstellenmanagers Und Scannen Sie angreifbare Elemente und Korrekturaufgaben in erneut Arbeitsbereich für IT-Korrekturen Dient zum Initiieren eines erneuten Scans in den Vulnerability Response-Arbeitsbereichen.
- Führen Sie die unten aufgeführten Schritte aus, um einen erneuten Scan in der klassischen Umgebung zu initiieren.

Hinweis:
Tenable.io Unterstützt nicht das Starten eines erneuten Scans auf Agent-basierten Computern.

Um den Overhead und das Volumen geplanter, vollständiger Scans zu reduzieren, können Sie als Korrekturbesitzer, IT-Spezialist, Schwachstellenanalyst oder Schwachstellenmanager bei Bedarf gezielte erneute Scans initiieren. Sie können in Ihren Umgebungen nach bestimmten Schwachstellen für Assets (Konfigurationselemente) suchen. Sie können erneutes Scannen aus Datensätzen für angreifbare Elemente (VI), Korrekturaufgaben (VUL), Drittparteieintrag (TPE) oder erkannte Elemente (SDI) von Ihrem initiieren ServiceNow AI Platform Instanz. Durch erneutes Scannen können Sie verifizieren, ob Ihre Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie einen erneuten Scan von Ihrem anfordern ServiceNow AI Platform® Instanz auswählen Vulnerability Response Integration with Tenable Anmeldeinformationen sind optional. Die ServiceNow® Tenable.io Die Integration von Scan-Anmeldeinformationen importiert und aktualisiert Scanner-Anmeldeinformationen aus dem Tenable.io Produkt in Ihrer Instanz. Diese Integration wird wöchentlich ausgeführt, um Ihre Tenable-Anmeldeinformationsdaten zu importieren und sicher zu speichern.

Beachten Sie, dass diese importierten Daten keine Tenable-Passwörter oder andere vertrauliche Tenable-Account-Informationen enthalten.

Die folgenden Informationen beschreiben die Anmeldeinformationen, die Sie importieren, damit Ihre Anwender sie nach Bedarf von Ihrem aus sehen können ServiceNow AI Platform Instanz:

- Anmeldeinformationen, die mit erstellt wurden Tenable.io Die Administratoranwenderrolle steht Anwendern in allen Ihren Organisationen zur Verfügung.
- Anmeldeinformationen, die mit erstellt wurden Tenable.io Die Rolle „Organisationsanwender“ ist nur für Anwender innerhalb dieser Organisation verfügbar. Diese Anmeldeinformationen werden nicht in importiert ServiceNow AI Platform Für Anwender außerhalb der Organisation des Erstellers, es sei denn, sie sind für den Account des Anwenders freigegeben, der für die Verbindung mit der Instanz verwendet wird.

  Siehe Tenable.io Dokumentationswebsite für weitere Informationen.

- Die Tenable.io Vorlagenintegration und Tenable.io Die Integration von Scan-Anmeldeinformationen muss aktiviert werden, bevor erneute Scans initiiert werden. Um weitere Informationen zur Integration von Scan-Anmeldeinformationen anzuzeigen, navigieren Sie zu **Tenable-Schwachstellen-Integration** > **Integrationen** > **Tenable.io-Scan-Anmeldeinformationsintegration**an.

  Standardmäßig sind die Integrationen für Vorlagen und Scan-Anmeldeinformationen deaktiviert. Wenn Sie Ihre Anmeldeinformationen für eingeben Tenable.io, Alle Tenable.io Integrationen werden automatisch aktiviert. So aktivieren oder deaktivieren Sie diese Integrationen manuell:

  1. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**an.
  2. Suchen Sie in der angezeigten Liste nach Tenable.io Gewünschte Integrationsdatensätze.
  3. Öffnen Sie jeden Datensatz, und wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren der Integration.
  4. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.
  5. Kehren Sie zum Setup-Assistenten zurück, um mit Ihrer Konfiguration für fortzufahren Tenable Vulnerability Integration Mit Vulnerability Response.

Siehe Konfigurieren Sie die Tenable-Schwachstellenintegration mit dem Setup-Assistenten Weitere Informationen zum Konfigurieren von Tenable.io Und Tenable.sc Produkte.

Angenommen, Ihre gesamte Umgebung wird alle drei Wochen einmal gescannt. Der letzte vollständige Scan wurde vor einer Woche abgeschlossen, aber Sie haben gestern einen Patch angewendet, um eine kritische Schwachstelle zu beheben. Aufgrund der Art dieser Schwachstelle können Sie nicht zwei Wochen auf den nächsten geplanten Scan warten, um sicherzustellen, dass sie behoben wurde. Um sicherzustellen, dass Ihr Patch eine kritische

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstelle erfolgreich behoben hat, die bei einem früheren Scan erkannt wurde, können Sie einen gezielten erneuten Scan von Ihrem aus initiieren ServiceNow AI Platform Für Tenable.io Angreifbare Elemente.

Sie können aktualisierte Ergebnisse in den Datensätzen anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration von behobenen Schwachstellen initiiert haben.

Während der Ausführung der Integration werden mehrere Prozesse generiert, und Daten werden in Form von Seiten empfangen. Jeder Prozess kann einen oder mehrere Importwarteschlangeneinträge mit angehängten Daten auf Seiten enthalten. Diese Einträge müssen die Daten innerhalb der Frist von einer Stunde verarbeiten. Wenn die Nutzlastgröße jedoch groß ist, kann die Verarbeitungszeit eine Stunde überschreiten oder hängen bleiben, was zu einem Fehler bei der Integrationszeitüberschreitung führt. Die Integration verarbeitet die Daten trotz des Zeitüberschreitungsfehlers weiter. Um diese Fehlkommunikation zu vermeiden, ab Version 18.2.4 von Vulnerability Response, Zeitstempel (Heartbeat) werden regelmäßig gesendet, um anzugeben, ob die Warteschlange aktiv ist und Daten verarbeitet. Die **Letzter Verarbeiteter Datensatz** Das Feld auf der Seite „Warteschlangeneintrag importieren“ wird basierend auf der Anzahl der Datensätze aktualisiert, die die Importwarteschlange erstellt oder aktualisiert. Wenn ein Importwarteschlangeneintrag die Zeitgrenze von einer Stunde überschreitet, überprüft das System **Letzter Verarbeiteter Datensatz** Feld, um zu sehen, ob es auch älter als eine Stunde ist. Wenn dies der Fall ist, weist dies darauf hin, dass der Importwarteschlangeneintrag feststeckt, und es wird eine Zeitüberschreitung überschritten, um weitere Verzögerungen bei der Verarbeitung zu vermeiden.

Hinweis:
Die **Letzter Verarbeiteter Datensatz** Das Feld wird basierend auf dem aktualisiert, was in den folgenden Systemeigenschaften definiert ist:

- `sn_sec_cmn.record_threshold_heartbeat`: Definiert die Anzahl der verarbeiteten Datensätze, nach denen der Heartbeat (Zeitstempel) an den Importwarteschlangeneintrag gesendet wird.
- `sn_sec_cmn.maximum_heartbeat_delay`: Definiert die Zeit, nach der der Importwarteschlangeneintrag abgelaufen sein muss.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Angreifbare Elemente**an.
2. Suchen Sie den Datensatz des angreifbaren Elements, aus dem Sie einen erneuten Scan auslösen möchten, und öffnen Sie ihn.

   Hinweis:
   Wenn Sie verwenden Tenable.io Scanner, können Sie nur mit erneutes Scannen für VIS initiieren Tenable.io Als Quelle. Verifizieren Tenable.io Wird in angezeigt **Quelle** Spalte in den VI-Listenansichten oder in **Quelle** Felder in einzelnen Datensätzen. Sie können den Bedingungsgenerator verwenden, um VIS nach Quelle zu gruppieren. Oder wenn die Spalte Quelle in der VI-Listenansicht nicht angezeigt wird, klicken Sie oben links in der Liste auf **Liste Personalisieren** Symbol (Zahnradsymbol), und verwenden Sie zum Verschieben den Slushbucket **Quelle** Von **Verfügbar** Bis **Ausgewählt** .

3. Alternativ navigieren Sie zu **Alle** > **Vulnerability Response** > **Korrekturaufgaben** oder **Vulnerability Response** > **Bibliotheken** > **Drittpartei** Für die Datensätze, die Sie für den erneuten Scan verwenden möchten.

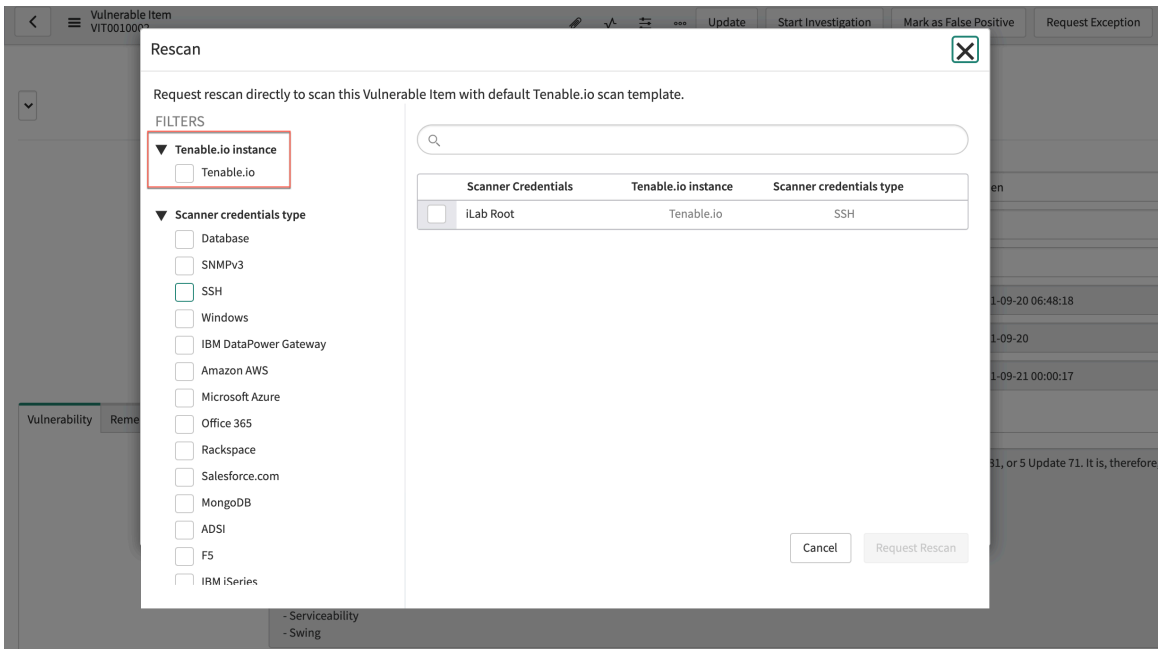
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängig von Ihrer Auswahl, die **Erneut Scannen** Die Schaltfläche ist für die folgenden Datensätze verfügbar:

- In einem einzelnen VI-Datensatz muss sich das VI in einem anderen Status als befinden **Geschlossen** . Bei mehreren VI-Datensätzen müssen alle VIS aus dem stammen Tenable.io Produkt und in einem anderen Status als **Geschlossen** .
- Für Korrekturaufgabendatensätze nur Korrekturaufgaben in einem anderen Status als **Geschlossen** Werden unterstützt. Alle zugeordneten VIS müssen sich in einem anderen Status als befinden **Geschlossen** Und verwenden Tenable.io Als Quelle.
- In einem Drittpartei-Eintrag-Datensatz (TPE) muss der Datensatz mindestens einen zugehörigen VI-Datensatz aus dem aufweisen Tenable.io Produkt in einem anderen Status als **Geschlossen** .
- Bei Datensätzen erkannter Elemente muss dem Datensatz mindestens ein VI-Datensatz aus dem zugeordnet sein Tenable.io Produkt in einem anderen Status als **Geschlossen** .
- In der Liste angreifbare Elemente können Sie einzelne angreifbare Elemente auswählen, die Sie erneut scannen möchten. Verwenden Sie das Menü Aktionen für ausgewählte Zeilen unten links im Bildschirm, um den erneuten Scan zu starten. Sie werden aufgefordert, Ihre Anmeldeinformationen einzugeben.

4. Klicken Sie oben rechts in einem Datensatz auf **Erneut Scannen** .
   Sie werden aufgefordert, die Instanz oder Instanzen für den erneuten Scan und die Scanner-Anmeldeinformationen auszuwählen, die Sie für den Zugriff auf den Scanner verwenden möchten. Die angezeigten Anmeldeinformationen sind die, die von importiert wurden Tenable.io Integration Von Anmeldeinformationen Scannen.
5. Wählen Sie im Dialogfeld die Instanz und/oder Instanzen und die Anmeldeinformationstypen aus, die Sie verwenden möchten.

   Im folgenden Bild eine Integrationsinstanz, Tenable.io Wird angezeigt. Wenn Sie mehr als einen haben Tenable.io-Instanz werden sie alle unter angezeigt Tenable.io Abschnitt im Formular.



6. Klicken Sie Auf **Erneutes Scannen Anfordern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Meldung wird angezeigt, die angibt, dass Ihr Scan verarbeitet wird und ein übergeordneter Scan-Datensatz erstellt wird. Der Status für alle untergeordneten Scans kann jederzeit unter den zugehörigen Scan-Listen in den VI-, Korrekturaufgabe-, TPE- und SDI-Datensätzen gefunden werden, die Sie zum Starten der erneuten Scans verwendet haben. Klicken Sie in der Nachricht auf **Zeigen Sie Details an** Zum Anzeigen des Status des erneuten Scans und zum Anzeigen anderer erneutes Scans, die aus einem bestimmten Datensatz gestartet wurden.

Das Feld Status im übergeordneten Scan-Datensatz wird als abgeschlossen markiert, nachdem alle untergeordneten Scans erfolgreich abgeschlossen wurden. Das untergeordnete Element scannt Importdaten. Jeder Scan unterstützt eine eindeutige Kombination aus Integrationsinstanz, TPE, IP und Netzwerk-ID. Möglicherweise werden mehrere untergeordnete Scans in einem übergeordneten Scan-Datensatz angezeigt. Beispielsweise beträgt die maximale Anzahl von IP-Adressen, die ein untergeordneter Scan unterstützen kann, 1000. Wenn für ein angreifbares Element 1002 IPs vorhanden sind, werden zwei untergeordnete Scans erstellt und in der zugehörigen Liste „Scans“ aufgeführt, um die Anforderung zu unterstützen. Der übergeordnete Scan-Datensatz ist ein Container für die untergeordneten Scans, und sein Status spiegelt den Status der untergeordneten Scans wider.

Ihr ServiceNow AI Platform® Die Instanz verfolgt den Status des erneuten Scans, bis er erfolgreich abgeschlossen ist, oder bis der festgelegte Nachverfolgungszeitraum abgelaufen ist, je nachdem, was zuerst geschieht. Durch die Zeitüberschreitung wird der Scan nicht beendet. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, an dem der ServiceNow AI Platform® Die Nachverfolgung des Status des erneuten Scans wurde beendet, nicht wenn der tatsächliche erneute Scan beendet wurde. Alle VIS, die in übergegangen sind oder übergehen werden **Geschlossen/Behoben** Werden mit dem nächsten geplanten Import von importiert Tenable.io Integration Behobener Schwachstellen.

Für Scans, die fehlerhaft sind, können Sie die untergeordneten Scans im übergeordneten Scan-Datensatz überprüfen. Zeigen Sie den Fehler in der Antwortnutzlast des untergeordneten Scans an.

Sie können aktualisierte Ergebnisse in den Datensätzen anzeigen, aus denen Sie die Scans nach dem nächsten geplanten Import der Integration von behobenen Schwachstellen initiiert haben.

Aktualisieren Sie Konfigurationselemente mit dem Netzwerkpartition-Bezeichner für Tenable Vulnerability Integration

Erstellen Sie eindeutige Konfigurationselemente (Configuration Items, CIs) für Assets in Ihrer Umgebung, die IP-Adressen teilen. Identifizieren Sie die eindeutigen Assets in Ihrer Umgebung, und aktualisieren Sie die CIs in Ihren vorhandenen erkannten Elementen, angreifbaren Elementen und Erkennungsdatensätzen automatisch, um Ihnen weitere Details zu Ihren Schwachstellen zu geben.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig in Vulnerability Response Anwendung. Eine Möglichkeit, Ihre Assets zu identifizieren, ist die IP-Adresse. In bestimmten Fällen können Assets IP-Adressen gemeinsam nutzen, werden jedoch als ein CI in Ihrer CMDB gespeichert.

Wie in den folgenden Tabellen dargestellt, können mehrere Assets (CI) in Ihrer Umgebung IP-Adressen teilen, haben jedoch eindeutige Netzwerk- und Repository-IDs. Standardmäßig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden diese Assets jedoch als einzelnes CI identifiziert und gespeichert (CI 1) Während der IP-Adresssuche.

Standard-IP-Suche und CI-Erstellung

Quelle	IP-Adresse	Netzwerk_ID	Konfigurationselement
Tenable.io: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	03712	CI 1
	123.12.12.141	03713	CI 1

Quelle	IP-Adresse	Repository_ID	Konfigurationselement
Tenable.sc: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	12	CI 1
	123.12.12.141	13	CI 1

Sie können einzelne CIs für Assets mit derselben IP-Adresse erstellen, um sie als eindeutige Assets zu identifizieren. Ausgehend von einem neuen Datenimport können Sie Ihre vorhandenen CIs mit mehr Granularität aktualisieren, einschließlich des Netzwerkpartition-Bezeichners [Network_Partition_Identifier], indem Sie die geplante Aufgabe ausführen. *`Update existing discovered items with network partition identifier`*.

Diese geplante Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese Funktion für die Assets und die Integrationen für behobene und offene Schwachstellen für Tenable.io Und Tenable.sc Produkte im Setup-Assistenten, um diesen Bezeichner in Ihren Datensätzen anzuzeigen.

Wenn diese geplante Aufgabe aktiviert ist, wird der Netzwerkpartition-Bezeichner [Network_Partition_Identifier] zu vorhandenen CI-Datensätzen aus importierten Daten hinzugefügt. Vorhandene CIs, die von der IRE erstellt wurden, werden ebenfalls aktualisiert. Die geplante Aufgabe erstellt auch CIs, die ab dem nächsten Import den Netzwerkpartition-Bezeichner enthalten. Alternativ können Sie den Auftrag bei Bedarf starten, um Ihre vorhandenen Daten zu aktualisieren.

Wenn Sie ein Upgrade ab v14.0 von durchführen Vulnerability Response Und v2.2 der Tenable-Schwachstellenintegration, der CMDB-CI-Klassenmodelle (1,0.21.) Wird unterstützt. Die Klassenmodelle haben den Netzwerkpartition-Bezeichner [Network_Partition_Identifier] in den Identifizierungsregeln für Identification and Reconciliation (IRE).

Option	Beschreibung
Führen Sie die geplanten Aufgaben bei Bedarf aus.	Aktualisieren Sie Ihre vorhandenen erkannten Elemente. CIs für Ihre vorhandenen Tenable-Daten werden erstellt oder aktualisiert, um die Granularität des Netzwerkpartition-Bezeichners einzubeziehen. Erkannte Elemente, angreifbare Elemente und Erkennungsdatensätze werden alle mit den neuen CIs aktualisiert.

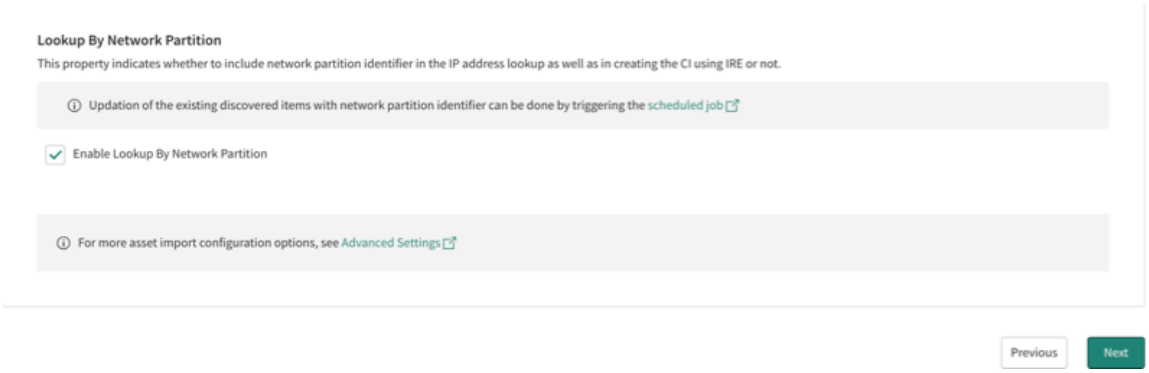
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Option	Beschreibung
Warten Sie auf Importe neuer Daten aus den Integrationen mit den nächsten geplanten Aufgaben.	Erstellen Sie CIs für jedes neue Asset mithilfe des Netzwerkpartition-Bezeichners, beginnend mit der nächsten geplanten Aufgabe. CI-, angreifbare Element- und Erkennungsdatensätze werden alle aktualisiert, um die neue Granularität einzubeziehen. Neue CIs werden erstellt, wenn keine genaue Übereinstimmung gefunden wird.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Setup-Assistent** > **Integrationskonfiguration** > **Scannerintegrationen**an.
2. Wählen Sie Aus Tenable.io Integrationen oder Tenable.sc Integrationen.
3. **Bearbeiten** Die erforderliche Integration.
4. Auswahlvorgang **Konfiguration des Asset-Imports**an.
5. Auswahlvorgang **Suche nach Netzwerkpartition aktivieren** Kontrollkästchen in **Suche nach Netzwerkpartition aktivieren** Abschnitt.



6. Klicken Sie auf **Next (Weiter)**.

Netzwerkpartition-Bezeichner „NETWORK_ID“ und „REPOSITORY_ID“ sind enthalten, und aktualisieren Sie vorhandene CIs, oder erstellen Sie CIs mit der nächsten geplanten Aufgabe.

Attribut des Netzwerkpartition-Bezeichners, das in der IP-Suche und CI-Erstellung enthalten ist

Quelle	IP-Adresse	NETWORK_ID	CI für Assets ohne Netzwerkpartition-Bezeichner	CIs-Assets mit Netzwerkpartition-Bezeichner
Tenable.io: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	03712	CI 1	CI 1
	123.12.12.141	03713	CI 1	CI 2

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quelle	IP-Adresse	REPOSITORY_ID	CI für Assets ohne Netzwerkpartition-Bezeichner	CIs-Assets mit Netzwerkpartition-Bezeichner
Tenable.sc: Assets und Integrationen behobener und offener Schwachstellen	123.12.12.141	12	CI 1	CI 1
	123.12.12.141	13	CI 1	CI 2

Bei der nächsten geplanten Aufgabe enthalten die Suchregeln für die IP-Adresse und die CI-Identifizierung der unvollständigen IP-Adresse automatisch das Attribut Netzwerkpartition-Bezeichner für einen Datenimport aus den Assets und Integrationen für behobene und offene Schwachstellen für Tenable.io Und Tenable.sc Produkte.

Nachdem Sie die Systemeigenschaft aktiviert und die Datensätze gespeichert haben, können Sie alternativ Ihre vorhandenen erkannten Elemente mit CIs aktualisieren, die den Netzwerkpartition-Bezeichner enthalten, indem Sie die geplanten Aufgaben bei Bedarf starten.

Importieren Sie Änderungen für die Tenable-Schwachstellenintegration

Konfigurieren Sie optionale Änderungen, und optimieren Sie einige der Daten speziell für die Importintegration von Tenable-Schwachstellen in ServiceNow® Tenable-Schwachstellenintegration.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Dieser Satz von Aufgaben erfordert Codierung und fortgeschrittenes Wissen über ServiceNow AI Platform.

Führen Sie die folgenden Schritte aus, um domänengetrennte Importe für die Tenable-Schwachstellenintegrationen zu erstellen. Das folgende Beispiel bezieht sich auf die Integration von Tenable.io Open Vulnerabilities, dieser Inhalt gilt jedoch für die anderen Tenable-Integrationen.

Prozedur

1. Erstellen Sie eine Domäne.
2. Erstellen Sie für jede von Ihnen erstellte Domäne einen Anwender, und weisen Sie den Anwender dieser Domäne zu.

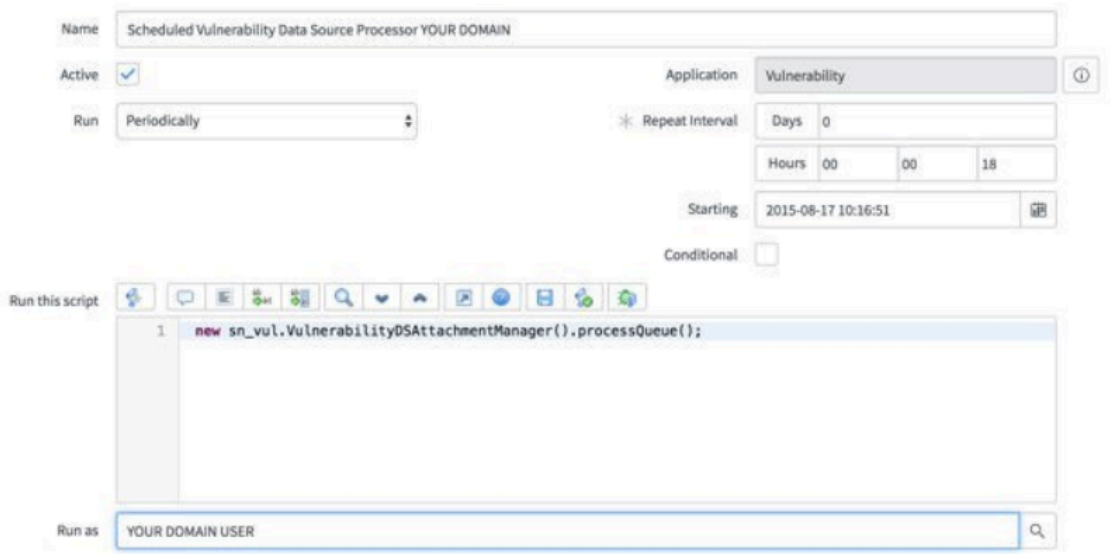
   Stellen Sie sich diesen Anwender als Run_as-Platzhalter für die Domäne in Tenable.io vor.
3. Integration Offener Schwachstellen.
   Der Anwender entspricht dem VR.System-Anwender in der globalen Domäne und muss über die folgenden Rollen verfügen: sn_vul.Tenable_configure_Integration, Import_admin und sn_vul.Vulnerability_write. Dieser Anwender benötigt Zugriff auf Datenquellen, Transformationszuordnungen und Schwachstellendaten.

   Hinweis:
   Betrachten Sie diesen Anwender als spezifisch für diese Rolle. Der Anwender darf keinen anderen Zweck haben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Erstellen Sie in jeder Domäne eine geplante Aufgabe, indem Sie den unter gefundenen Datenquellenprozessor für geplante Schwachstellen kopieren **Systemdefinition** > **Geplante Aufgaben**an.
5. Hängen Sie die Domäne an den Namen an, um die geplante Aufgabe zu identifizieren.
6. Ändern Sie den Run_as-Anwender in den Anwender, den Sie im vorherigen Schritt erstellt haben.

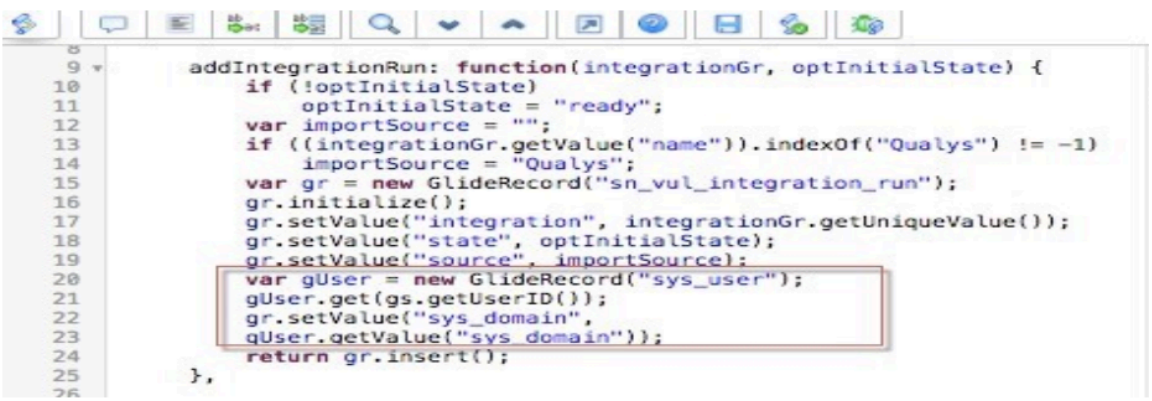
Hinweis:
Bearbeiten Sie die folgende UI-Aktion, damit die Integration in der Anwenderdomäne „Run_as“ ausgeführt wird.



7. Bearbeiten Sie die UI-Aktion Now ausführen in der Tenable.io Open Vulnerabilities Integration, um diesen Codeblock oben in der Datei hinzuzufügen.
```
//sys id below is of Tenable.io integration if(current.sys_id ==
"4df3f18d53730010d7f1ddeeff7b12a9"){ current.run_as = gs.getUserID(); }
```

Hinweis:
Bearbeiten Sie die folgenden Skripteinbindungen, damit die Integration in der Anwenderdomäne „Run_as“ ausgeführt wird.

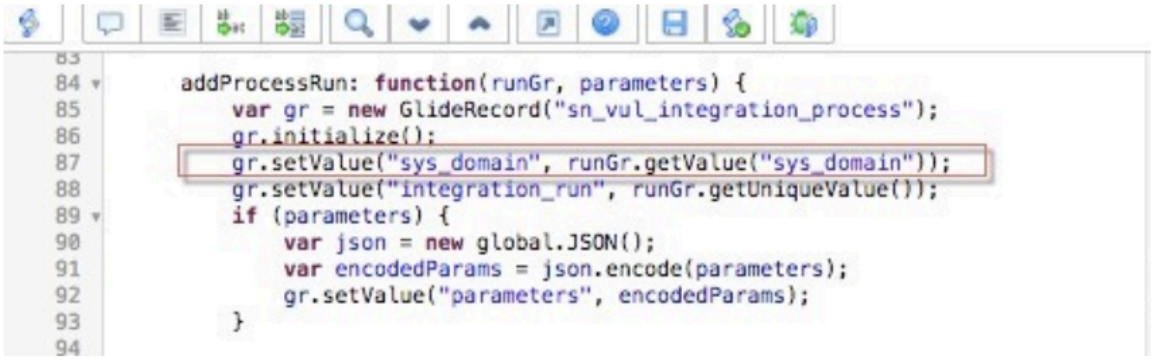
8. Bearbeiten Sie die Skripteinbindungsmethode „VulnerabilityIntegrationUtils“ addIntegrationRun, um den hervorgehobenen Code hinzuzufügen.



```
addIntegrationRun: function(integrationGr, optInitialState) {
    if (!optInitialState)
        optInitialState = "ready";
    var importSource = "";
    if ((integrationGr.getValue("name")).indexOf("Qualys") != -1)
        importSource = "Qualys";
    var gr = new GlideRecord("sn_vul_integration_run");
    gr.initialize();
    gr.setValue("integration", integrationGr.getUniqueValue());
    gr.setValue("state", optInitialState);
    gr.setValue("source", importSource);
    var gUser = new GlideRecord("sys_user");
    gUser.get(gs.getUserID());
    gr.setValue("sys_domain",
    gUser.getValue("sys_domain"));
    return gr.insert();
},
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Bearbeiten Sie die Skripteinbindungsmethode „VulnerabilityIntegrationUtils“ addProcessRun, um den hervorgehobenen Code hinzuzufügen.



```
addProcessRun: function(runGr, parameters) {
    var gr = new GlideRecord("sn_vul_integration_process");
    gr.initialize();
    gr.setValue("sys_domain", runGr.getValue("sys_domain"));
    gr.setValue("integration_run", runGr.getUniqueValue());
    if (parameters) {
        var json = new global.JSON();
        var encodedParams = json.encode(parameters);
        gr.setValue("parameters", encodedParams);
    }
```

10. Bearbeiten Sie die DataSourceVulnReportRefreshProcessor-Skripteinbindungsmethode _processFromDataSourceGroups, um diesen ursprünglichen Code zu ändern: Ursprünglicher _processFromDataSourcesGroups-Code in bearbeiteter _processFromDataSourcesGroups-Code.
11. Bearbeiten Sie die Skripteinbindungsmethode VulnerabilityDSAttachmentManager, QueueItem, um die folgenden hervorgehobenen Codeblöcke QueueItem, _getNext, _processQueueEntry hinzuzufügen.

Sie sind bereit für domänengetrennte Host-Erkennungsimporte.

Deaktivieren Sie Rechner vor dem Import

Führen Sie die folgenden Schritte aus, um den Standardrechner zu deaktivieren, wenn er nicht verwendet wird. Wenn Sie keine Schwachstellenrechner verwenden, sollten Sie die Standardrechner zusätzlich zu allen anderen von Ihnen definierten Rechnern deaktivieren. Schwachstellenrechner werden jedes Mal ausgeführt, wenn auf einen Datensatz für angreifbare Elemente zugegriffen wird, und können sich auf die Instanzleistung auswirken.

Erforderliche Rolle: sn_vul.Vulnerability_admin.

12. Navigieren zu **Alle** > **Schwachstelle** > **Administration** > **Schwachstellen-Rechner**an.
13. Öffnen Sie die Gruppe Schwachstellenauswirkung.
14. Öffnen Sie den Punktzahl- und servicebasierten Auswirkungsrechner.
15. Deaktivieren Sie das Feld aktiv, um den Rechner zu deaktivieren.
16. Klicken Sie auf Aktualisieren.

Sie haben den Standardrechner deaktiviert.

Deaktivieren Sie benachrichtigungsbasierte Business-Regeln vor dem ersten Import

Führen Sie die folgenden Schritte aus, um die Benachrichtigungsbezogenen Geschäftsregeln vor dem ersten Datensatzimport zu deaktivieren. Während des ersten Imports von Datensätzen können bestimmte benachrichtigungsbezogene Geschäftsregeln viele Benachrichtigungen generieren, die sich auf die Leistung auswirken. Diese Business-Regeln sollten geändert werden, um sie während des Imports zu deaktivieren.

Erforderliche Rolle ist sn_vul.Vulnerability_admin.

17. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**an.
18. Suchen Sie nach betroffenen ci-Benachrichtigungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

19. Öffnen Sie die Business-Regel, und fügen Sie die folgende Bedingung ein: `current.sys_class_name != “sn_vul_vulnerable_item"`.
20. Klicken Sie auf **Aktualisieren**.
21. Wiederholen Sie diesen Vorgang für die folgenden Business-Regeln:
    - Benachrichtigungen über betroffene Kostenstellen
    - Benachrichtigungen der betroffenen Gruppe
    - Benachrichtigungen zu betroffenen Standorten

Hinweis:
Nach Abschluss des ersten Datensatzimports haben Sie die Möglichkeit, diese Business-Regeln erneut zu aktivieren. Erwägen Sie jedoch, sie deaktiviert zu lassen. Sie können eine große Anzahl von Benachrichtigungen generieren und sich auf die Leistung Ihrer Instanz auswirken.

Ändern Sie ein anfängliches Startdatum

Führen Sie die folgenden Schritte aus, um ein anfängliches Startdatum zu ändern. Während der Installation mit dem Setup-Assistenten legen Sie ein erstes Startdatum für die Tenable-Integrationen fest. Sie können dieses Startdatum im Setup-Assistenten oder über die primäre Integration zurücksetzen, wie in den folgenden Schritten gezeigt.

22. Navigieren zu **Alle** > **Tenable-Schwachstellen-Integration** > **Administration** > **Integrationen**an.
23. Klicken Sie auf eine beliebige Integration.
24. Klicken Sie Auf Integrationsdetails.
25. Legen Sie das Feld Startzeit auf einen Wert in der Vergangenheit fest, damit alle seit dieser Zeit gescannten und erkannten Schwachstellen erkannt werden.

    Wenn Sie Tenable mit dem Setup-Assistenten konfiguriert haben, wird das Feld Startzeit vorab ausgefüllt, zunächst drei Monate vor dem heutigen Datum und anschließend bis zum heutigen Datum. Hinweis: Erwägen Sie, den Wert auf maximal einen Monat in der Vergangenheit festzulegen. Dadurch wird verhindert, dass große Datenmengen die Beschränkungen der Tenable-API-Rate überschreiten und Ausführungszeitüberschreitungen auslösen.

26. Klicken Sie auf **Absenden** oder **Aktualisieren**.
27. **Wahlweise:** Klicken Sie Auf **Jetzt Ausführen** Zur sofortigen Ausführung.

Teilen Sie Tenable-Erkennungen basierend auf der Schwachstelleninstanz auf, um angreifbare Elemente aufzuteilen

ServiceNow® Vulnerability Response ermöglicht die Aufteilung von Erkennungen von Tenable-Scannern, wodurch für jede erkannte Schwachstelleninstanz ein eindeutiges angreifbares Element (VIT) erstellt werden kann. Diese Aufteilung ermöglicht die Zuweisung von Vits an verschiedene Korrekturteams, wodurch die Verwaltung und Nachverfolgung von Schwachstellen verbessert wird.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Nutzlast des Tenable-Scanners enthält Erkennungsdaten, wobei jeder Pfad innerhalb des Nachweises zum Aufteilen der Erkennungen verwendet wird. Das Ausgabe-Tag in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Nutzlast identifiziert den Standort der Schwachstelle und erleichtert die genaue Identifizierung und Verwaltung von Schwachstellen gemäß ihren spezifischen Pfaden.

Prozedur

1. Legen Sie in der Tabelle „Drittpartei-Integrationen“ [sn_sec_int_Integration] fest **Nachweis in VI-Schlüssel einschließen** Spaltenwert auf „wahr“ für Tenable.io, Tenable.sc, Und Tenable.cs.
2. Navigieren zu **Alle** > **Vulnerability Response** > **Administration** > **VI-Granularität konfigurieren**an.
3. Für Tenable.cs Produkt, navigieren Sie zu **Erkennungsschlüsselkonfiguration** Tabelle [sn_vul_Detection_key_config], wählen Sie aus Tenable.cs Aufzeichnen und aktualisieren,
4. Wählen Sie im Formular „Port einbeziehen“ die aus **Port einschließen** Aktivieren Sie das Kontrollkästchen, und aktivieren Sie das **Klicken Sie hier** Link (gilt nur für Tenable.io und Tenable.sc).
5. Wählen Sie in der Liste Nachweis zu VI-Schlüsseln hinzufügen die Option aus **Neu** .
6. Im Formular „Nachweis zum VI-Schlüssel hinzufügen – neuer Datensatz“ im **Schwachstelle** Fügen Sie die Tenable-ID hinzu, für die Sie den Nachweis einschließen möchten.

   Hinweis:
   Sie können die Erkennungen nur basierend auf Pfadinformationen oder durch Kombination von Pfad- und Versionsdetails aufteilen. Weitere Informationen finden Sie im Abschnitt „Erkennungen von Tenable-Scannern aufteilen“ auf dieser Seite.

7. In **Regulärer Ausdruck zum Aufteilen von Tenable-Vits** Feld:
   - Teilen Sie die Erkennung nur basierend auf dem Pfad auf, indem Sie Pfad eingeben\s+:\s+([A\n]+).
   - Teilen Sie die Erkennung basierend auf Pfad und installierten und festen Versionen auf, indem Sie Pfad\s+:\s+([A\n]+)\n\s+Installed\s+Version\s+:\s+([A\n]+)\n\s+Fixed\s+Version\s+:\s+([A\n]+) eingeben.
8. Wählen Sie **Absenden**.

Example: Trennung von Erkennungen von Tenable-Scannern

Die folgende Erkennung von einem Tenable-Scanner zeigt einen Nachweis im Ausgabe-Tag, der sowohl Pfad- als auch Versionsinformationen enthält.

```
    "results":


            "asset":
                "agent_uuid": *92124caabdb9459baa9d053186df48b9",
               "bios_uuid": "ec2cbbfd-dc9e-efbf-acdd-485daZe8c7df"
               "device_ type": "aws-ec2-instance",
                "fqdn": "ip-ac0a0004. secops.com",
                "hostname": "ip-ac0a0004",
        "uuid": "486acb3b-674f-477a-bc37-660a7bba37b3",
                "ipv4": "18.220.145.158",
                "last_authenticated_results": "2024-05-17T03:34:04.424Z",

                "mac_address": "0a:3e:8b:ed:63:e6",
               "netbios name": "IP-AC0A0094".
               "operating_system": [
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                    "Microsoft Windows Server 2019 Datacenter Build 17763"

                  "network_id": "00000000-0000-0000-0000-000000000008",

                 "tracked": true

          "output": "In                    C: 11 Program Files (x86) \ \Common
Files\\0racle\\Java\\javapath_target_119044062511\n Installed version : 1.8.0_361.9\n Fixed
version
                                                                    Path
          "plugin":
               "bid":
                    123456

               "checks_for_default_account": false,
              "checks_for malware": false,

                "coe":
               "cpe:/a:notepad-plus-plus:notepad%5c%2b15ck2b"

                "cvSs3_base_score": 7.8,
               "cvss3 temporal score": 7.0,

               "cvss3_temporal_vector": {
                     "exploitability": "Proof-of-Concept",
                     "remediation level": "Official Fix",
                      "report_confidence": "Confirmed",
                      "raw": "E: P/RL:0/RC: C"
```


Erkunden Sie Integrationen von Wiz-Testergebnissen und -Problemen mit Konfigurations-Compliance

Importieren Sie Cloud-Konfigurationsdaten mit Integrationen von Wiz-Testergebnissen und -Problemen mit Konfigurations-Compliance Die in enthalten sind Wiz Vulnerability Response Integration.

Wiz Integration Von Testergebnissen

Importieren Sie Konfigurationstestergebnisse aus Wiz Um nicht konforme Cloud-Konfigurationen zu erkennen und Sicherheitsrichtlinien und -Standards in Ihrer Cloud-Umgebung durchzusetzen.

Ergebnisse werden Cloud-Testergebnissen (CTRs) in zugeordnet Konfigurations-Compliance Anwendung.

Hinweis:
Hostkonfigurationen von Wiz Werden nicht importiert.

Wiz Probleme Bei Der Integration

Importieren Sie Problemdaten aus Wiz Damit Schwachstellenmanager, Analysten sowie Cloud-Sicherheits- und -Risikoteams Kombinationen von Schwachstellen identifizieren können, die einen potenziellen Angriffspfad in Ihrer Cloud-Infrastruktur offenlegen könnten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Ergebnisse werden auch CTRs mit zugeordnet Wiz-Probleme Als Quelle in gekennzeichnet Konfigurations-Compliance Anwendung, mit der Sie Assets nachverfolgen und korrigieren können, die komplexe Multi-Vektor-Risiken darstellen können.

Um weitere Informationen zu den anderen Integrationen zu erhalten, die in enthalten sind Wiz Vulnerability Response Schritte zur Integration, Installation und Konfiguration finden Sie unter Verstehen von Wiz Vulnerability Response Integration.

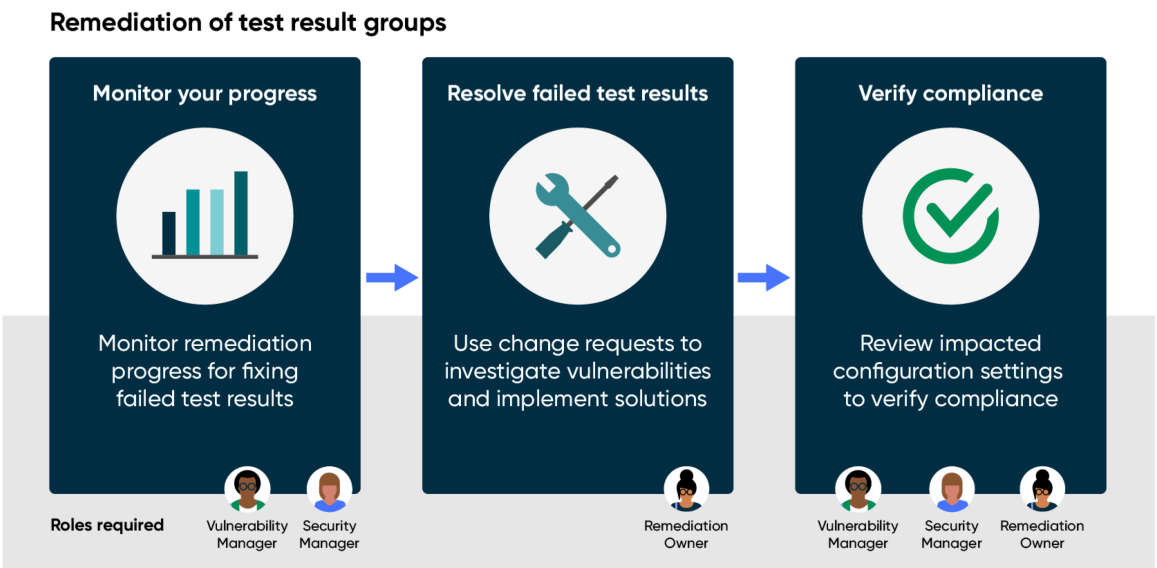
Konfigurations-Compliance – Fehlerkorrektur

Konfigurations-Compliance Die Korrektur ist in erster Linie ein manueller Prozess, der durch geplante Aufgaben (Integrationen), Korrekturaufgaben, Workflows und Change-Anforderungen erweitert wird.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe



Separate SCA-Plugins von Drittanbietern erfassen und transformieren Daten in Konfigurations-Compliance. Bevor Sie verwenden können Konfigurations-Compliance Um Konfigurationselemente zu korrigieren, müssen Sie eine Scannerintegration von Drittanbietern installieren und mindestens einen Netzwerkscan durchführen.

Verwenden Sie Change-Anforderungen, um einzelne Testfehler aus Korrekturaufgaben zu beheben.

Die status von Korrekturaufgaben gehen automatisch über, wenn zugehörige Change-Anforderungen ihre Lebenszyklen mit durchlaufen Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben. Benutzer mit der Rolle itil können Change-Anforderungen direkt aus Korrekturaufgaben erstellen und verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erstellen Sie manuell einen Konfigurations-Compliance Korrekturaufgabe

Erstellen Sie manuell einen Konfigurations-Compliance Korrekturaufgabe aus der Testergebnisliste

Change-Anforderung in Konfigurations-Compliance erstellen

Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu

Entfernen Sie Zuweisungen aus Korrekturaufgaben für Sie oder Ihre Gruppen

Automatisches Schließen von Testergebnissen

Schließen Sie eine Korrekturaufgabe

Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement in Konfigurations-Compliance

Erstellen Sie manuell einen Konfigurations-Compliance Korrekturaufgabe

Sie können eine Korrekturaufgabe manuell aus erstellen **Korrekturaufgaben** Modul und führen Sie die Korrektur durch.

Wichtig:
Sie können Korrekturaufgaben in erstellen:

- Arbeitsbereich des Schwachstellenmanagers Als Anwender mit der Rolle sn_vulc.admin.
- Arbeitsbereich für IT-Korrekturen Als Anwender mit der Rolle „sn_vulc.Remediation_owner“.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Durch die Verwendung von Regeln für Korrekturaufgaben wird automatisch ausgefüllt **Testergebnisse** Registerkarte. Die manuelle Erstellung ist für eine Korrekturaufgabe nützlich, die keine Regel benötigt oder wiederholt werden soll.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

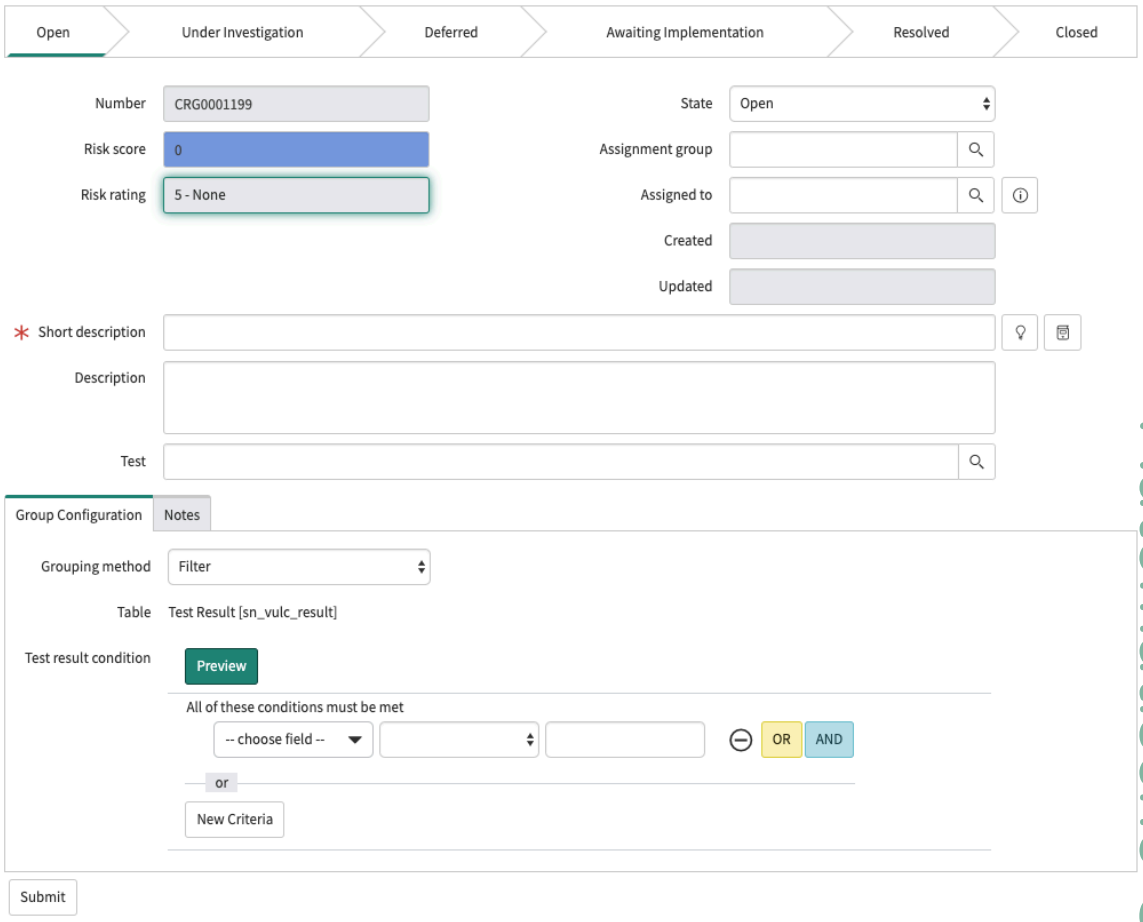
Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben**an.
2. Klicken Sie im Navigationsbereich auf **Meine Offenen Aufgaben** Oder **Alle Offenen Aufgaben** Zum Anzeigen der Liste.
3. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Korrekturaufgabe“



4. Füllen Sie die Felder im Formular „Korrekturaufgabe“ entsprechend aus.

Formular „Korrekturaufgabe“

Feld	Beschreibung
Anzahl	Automatisch zugewiesene ID im System.
Risikopunktzahl	Wird automatisch vom Risikopunktzahlrechner ausgefüllt. Dies ist eine Rollup-Risikopunktzahl. Diese Risikopunktzahl wird gewichtet, wobei 85 % der Punktzahl aus der maximalen Risikopunktzahl für alle nicht „geschlossenen“ Testergebnisse (offen, wird untersucht, wartet auf Implementierung, zurückgestellt, gelöst) verwendet werden. und 15 % der Punktzahl aus der Anzahl der Testergebnisse, die nicht „Geschlossen“ sind.
Risikobewertung	Wird automatisch vom Risikopunktzahlrechner ausgefüllt. Basierend auf einer Reihe von Risikopunktzahlen auf einer numerischen Skala von 1-5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen als 1 – Kritisch bis 5 – keine bewertet. Dieses Feld ersetzt das Feld Priorität in vorherigen Versionen.

Automatische Übersetzung

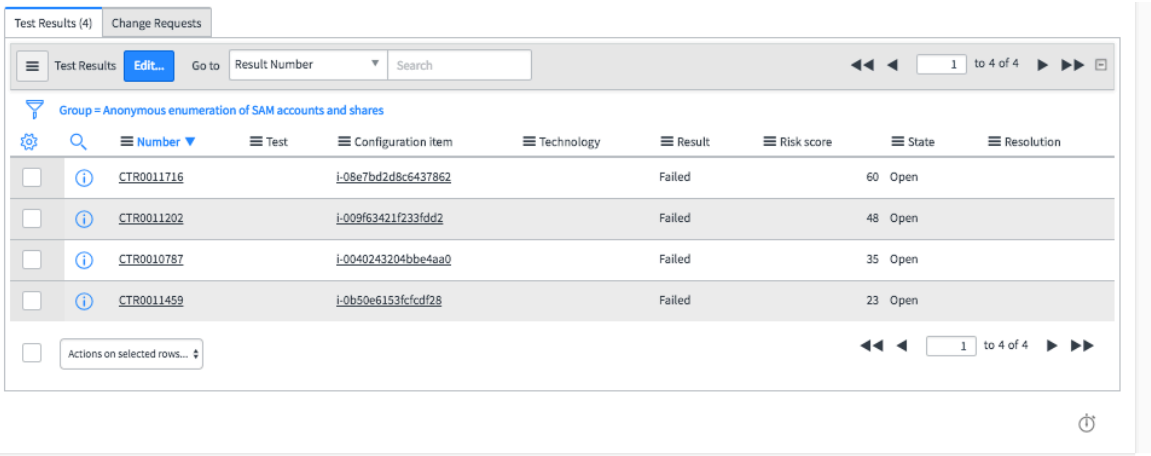
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Anfänglich **Öffnen** , Ist der Korrekturstatus der Korrekturaufgabe. Weitere Informationen finden Sie unter Konfigurations-Compliance status.
Zuweisungsgruppe	Weisen Sie die Korrekturaufgabe einer Korrekturgruppe zu.
Zugewiesen an	Weisen Sie Personal zu, um die Korrekturaufgabe zu korrigieren.
Erstellt	Datum, an dem Sie diese Korrekturaufgabe erstellt haben.
Aktualisiert	Datum, an dem Sie diese Korrekturaufgabe aktualisiert haben.
Kurzbeschreibung	Name der Korrekturaufgabe.
Beschreibung	Beschreibung dieser Korrekturaufgabe.
Test	Wählen Sie einen Konfigurationstest für diese Korrekturaufgabe aus.
Zugehörige Registerkarten	
Gruppenkonfiguration	Zu verwendende Gruppierungsmethoden: ◦ Manuell (Standard): ◦ Filter- oder Gruppenregel: Tabelle: Vorausgewählt als Testergebnis [sn_vulc_result] Testergebnisbedingung: Wählen Sie die zu verwendenden Filter aus. **Hinweis:** Der Link „Datensätze stimmen mit Bedingung überein“ oberhalb der Filterbedingungen zeigt die von Ihnen ausgewählten Testergebnisdatensätze in einem neuen Fenster an. Klicken Sie Auf **Vorschau** Um anzuzeigen, wie viele Ergebnisse Ihre Filterkriterien zurückgeben, bevor Sie die neue Gruppe speichern. Die zugehörige Liste „Testergebnisse“ muss manuell erstellt werden, indem Sie auf klicken **Bearbeiten** Schaltfläche in **Testergebnisse** Zugehörige Registerkarte.
Notizen	Arbeitsnotizen im Zusammenhang mit dieser Korrekturaufgabe.

5. Klicken Sie mit der rechten Maustaste in den Header zu **Speichern** Oder klicken Sie auf **Übermitteln** Um zu speichern und zur Liste der Korrekturaufgaben zurückzukehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigt an **Testergebnisse** Und **Change-Anforderung** Zugehörige Listen.



Erstellen Sie manuell einen Konfigurations-Compliance Korrekturaufgabe aus der Testergebnisliste

Sie können eine Korrekturaufgabe manuell aus erstellen **Testergebnis** Listet die resultierende Korrekturaufgabe auf, und führt sie aus.

Vorbereitungen

Erforderliche Rolle: sn_vulc.admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Methode erfordert die Auswahl von Testergebnissen, die einbezogen werden sollen, und die Erstellung der Gruppe aus dem **Aktionen für ausgewählte Zeilen...** Menü. Diese Methode eignet sich für Ergebnisse, die nicht leicht gefiltert werden können, oder Situationen, in denen Sie Testergebnisse zur Korrektur angeben möchten.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

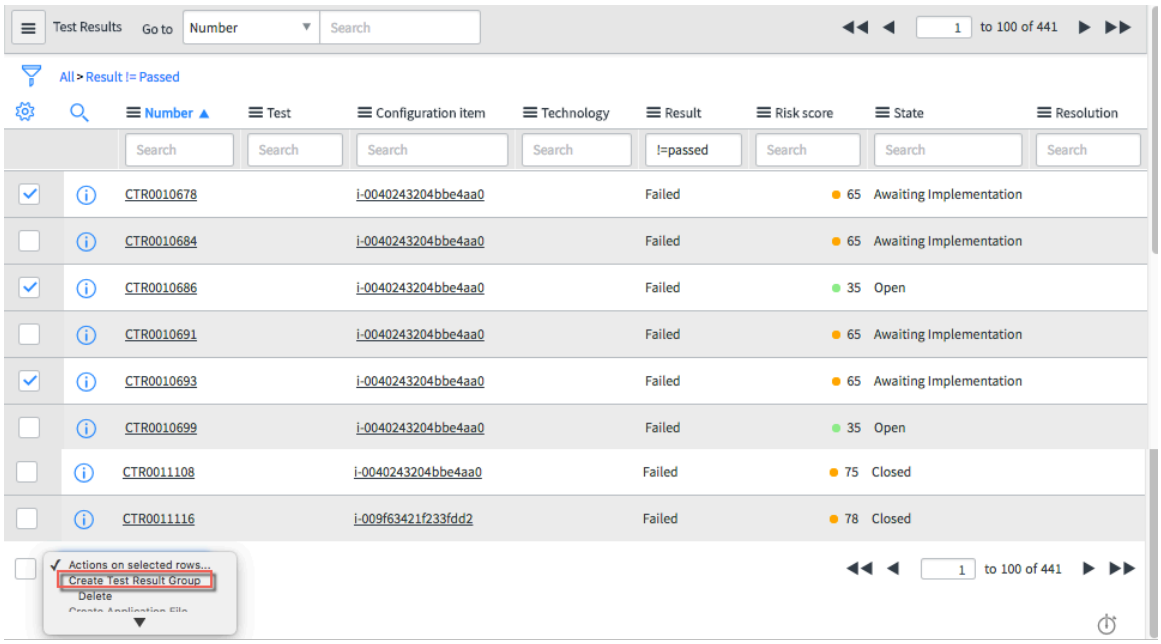
Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Testergebnisse**an.
2. Wählen Sie im Navigationsbereich ein Testergebnismodul aus, um eine Liste zu öffnen.
3. Wählen Sie die Testergebnisse aus, die in die Korrekturaufgabe aufgenommen werden sollen, indem Sie das Kontrollkästchen neben jedem aktivieren.
4. Öffnen Sie **Aktionen für ausgewählte Zeilen...** Menü unten in der Liste.

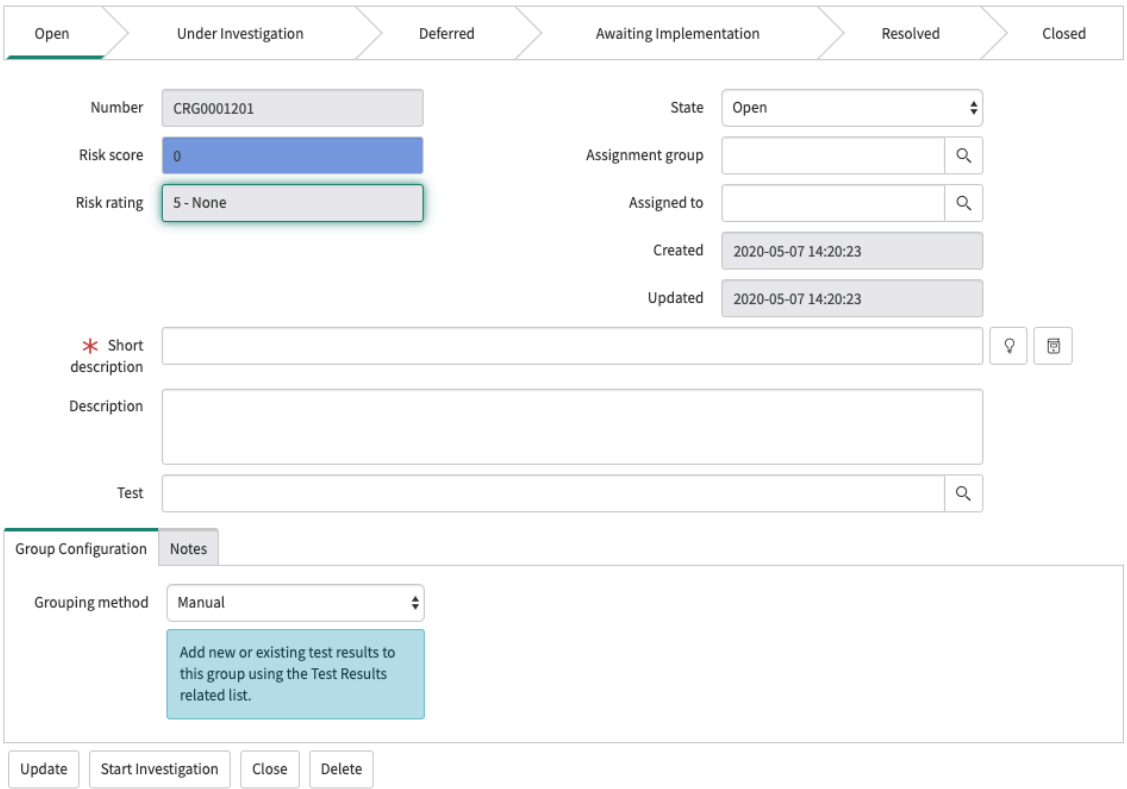
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie Aus **Erstellen Sie Eine Korrekturaufgabe** .
Die Korrekturaufgabe wird erstellt und geöffnet.

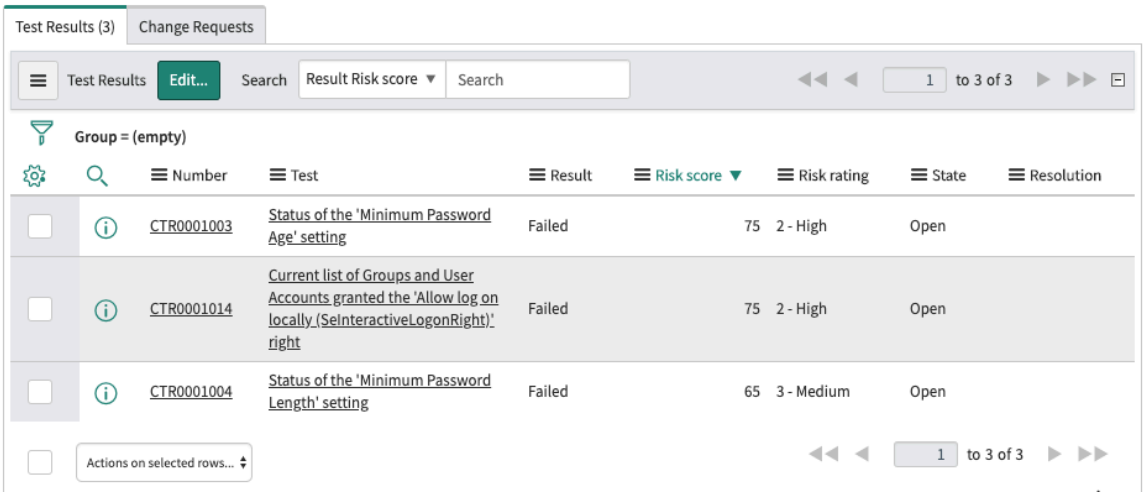
Formular „Korrekturaufgabe“



Die Testergebnisse, die Sie für die Korrekturaufgabe ausgewählt haben, werden in der zugehörigen Liste Testergebnisse zusammen mit allen zugehörigen Change-Anforderungen angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Anzahl	Automatisch zugewiesene ID im System.
Punktzahl	Wird automatisch vom Rollup-Rechner für Risikopunktzahl ausgefüllt. Dies ist eine Rollup-Risikopunktzahl. Diese Risikopunktzahl wird gewichtet, wobei 85 % der Punktzahl aus der maximalen Risikopunktzahl für alle nicht „geschlossenen“ Testergebnisse (offen, wird untersucht, wartet auf Implementierung, zurückgestellt, gelöst) verwendet werden. und 15 % der Punktzahl aus der Anzahl der Testergebnisse, die nicht „Geschlossen“ sind.
Bewertung	Wird automatisch vom Rollup-Rechner für Risikopunktzahl ausgefüllt. Basierend auf einer Reihe von Risikopunktzahlen auf einer numerischen Skala von 1-5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen als 1 – Kritisch bis 5 – keine bewertet. Dieses Feld ersetzt das Feld Priorität in vorherigen Versionen.
Historische Risikopunktzahl	Wird automatisch vom Rollup-Rechner für Risikopunktzahl ausgefüllt. Die inhärente Risikopunktzahl für alle bestandenen Tests führt zu einer Korrekturaufgabe. Dieses Feld zeigt das Ausmaß des Risikos an, das von einer Testgruppe korrigiert wurde, und wird erst angezeigt, nachdem sich eine Testgruppe im Status „Geschlossen“ befindet und die Risikopunktzahl null ist.
Status	Anfänglich **Öffnen** , Ist der Korrekturstatus der Korrekturaufgabe. Weitere Informationen finden Sie unter Konfigurations-Compliance status.
Zuweisungsgruppe	Weisen Sie die Korrekturaufgabe einer Korrekturgruppe zu.
Zugewiesen an	Weisen Sie Personal zu, um die Korrekturaufgabe zu korrigieren.
Erstellt	Datum, an dem Sie diese Korrekturaufgabe erstellt haben.
Aktualisiert	Datum, an dem Sie diese Korrekturaufgabe aktualisiert haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Kurzbeschreibung	Name der Korrekturaufgabe.
Beschreibung	Textbeschreibung dieser Korrekturaufgabe.
	Wählen Sie einen Konfigurationstest für diese Korrekturaufgabe aus.
Zugehörige Registerkarten	
Gruppenkonfiguration	Zu verwendende Gruppierungsmethoden: ○ Manuell (Standard) ○ Filter Tabelle: Vorausgewählt als Testergebnis Testergebnisbedingung: Wählen Sie die zu verwendenden Filter aus. **Hinweis:** Der Link „Datensätze stimmen mit Bedingung überein“ oberhalb der Filterbedingungen zeigt die von Ihnen ausgewählten Testergebnisdatensätze in einem neuen Fenster an. Klicken Sie Auf **Vorschau** Um anzuzeigen, wie viele Ergebnisse Ihre Filterkriterien zurückgeben, bevor Sie die neue Korrekturaufgabe speichern.
Notizen	Arbeitsnotizen im Zusammenhang mit dieser Korrekturaufgabe.
Zugehörige Listen	
Testergebnisse	Testergebnisse, die in dieser Korrekturaufgabe enthalten sind.
Change-Anforderungen	Change-Anforderungen, die dieser Korrekturaufgabe zugeordnet sind.

7. Klicken Sie mit der rechten Maustaste auf den Header zu **Speichern** Oder klicken Sie auf **Übermitteln** Um zu speichern und zur Liste der Korrekturaufgaben zurückzukehren.

Change-Anforderung in Konfigurations-Compliance erstellen

Sie können eine Change-Anforderung aus einer Korrekturaufgabe in erstellen Konfigurations-Compliance Anwendung.

Vorbereitungen
Erforderliche Rolle: Anwender mit der Rolle itil

Warum und wann dieser Vorgang ausgeführt wird
Erstellen Sie als IT- oder Korrekturspezialist eine Change-Anforderung (CHG) direkt aus einer Korrekturaufgabe für alle darin enthaltenen Testergebnisse. Erstellen Sie eine Change-Anforderung mit vorab ausgefüllten Informationen, um Ihre Untersuchung auf Schwachstellen zu beschleunigen, die manuelles Eingreifen erfordern.

Sie können Change-Anforderungen direkt aus Korrekturaufgaben erstellen, genehmigen, implementieren, überprüfen und schließen, die Ihnen zugewiesen sind. Sie können drei Arten von Change-Anforderungen mit vorab ausgefüllten Informationen aus einer Korrekturaufgabe erstellen:

Standard

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein zuvor autorisierter Change, der als risikoarm und relativ gängig gilt und anhand eines festgelegten Verfahrens oder einer festgelegten Arbeitsanweisung implementiert wird.

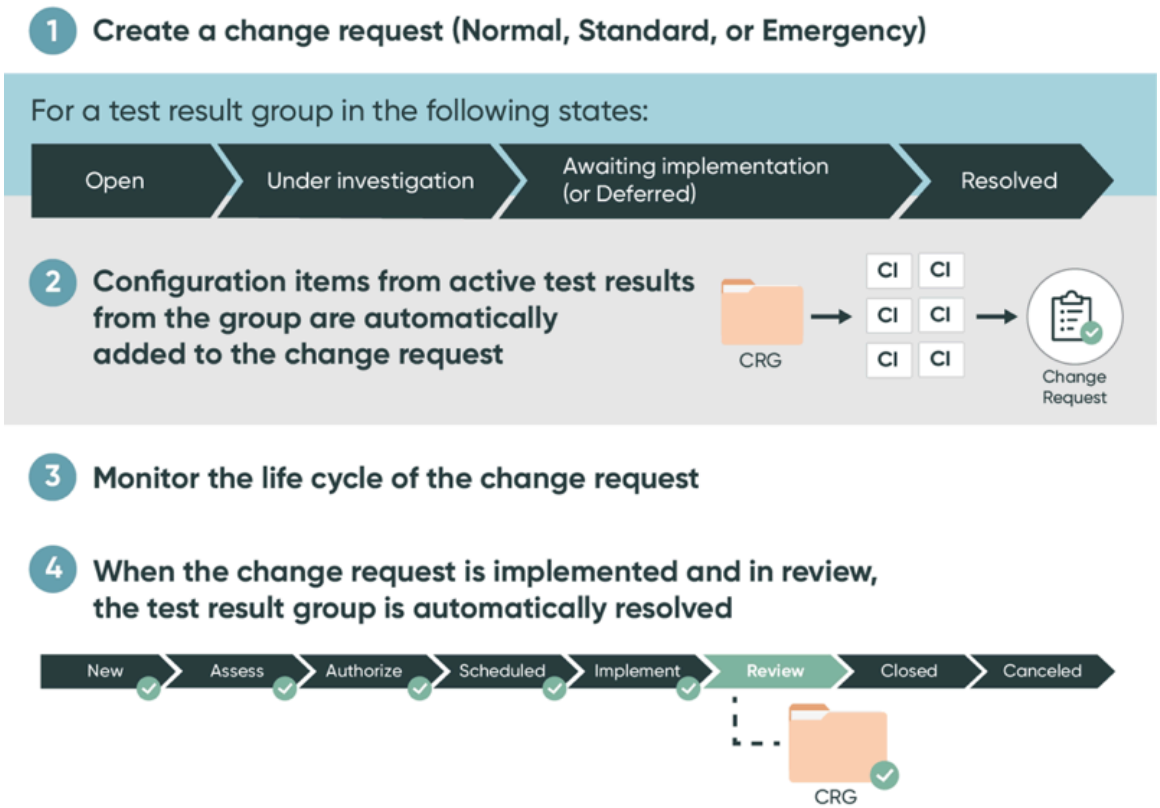
Normal

Normale Change-Anforderungen folgen einem verbindlichen Prozess, der zwei Genehmigungsstufen erfordert, bevor sie implementiert, überprüft und geschlossen werden.

Notfall

Ein Change zur Lösung eines schwerwiegenden Incident.

Die folgende Abbildung zeigt den grundlegenden Flow zum Erstellen einer Change-Anforderung aus einer Korrekturaufgabe. Die detaillierten Schritte für diesen Flow folgen dem Bild.



Ab Version 19,0 von Vulnerability Response, Sie können Change-Anforderungen für Korrekturaufgaben im IT-Korrekturarbeitsbereich erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Change-Anforderung in Arbeitsbereich für IT-Korrekturen.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben** > **Meine offenen Aufgaben**an.
   Die Liste der Korrekturaufgaben, die Ihren Gruppen zugewiesen sind, wird angezeigt.
2. Klicken Sie in der Spalte Nummer auf die Korrekturaufgabe, für die Sie eine Change-Anforderung erstellen möchten.
   Sie können Change-Anforderungen aus Korrekturaufgaben in einem anderen status als erstellen **Geschlossen** Oder **Wird überprüft** .

   Der Datensatz der Korrekturaufgabe wird angezeigt.
3. Klicken Sie oben rechts im Datensatz auf **Erstellen Sie Einen Change** .
   Das Formular „Change-Anforderung“ wird angezeigt.
4. Füllen Sie die Felder aus.
   a. Aus der Liste von **Gilt für** Feld auswählen, um fortzufahren.
5. Für **Fügen Sie der CR CIs hinzu** Kontrollkästchen auswählen, um fortzufahren.
6. Aus der Liste für **Change-Typ** Feld auswählen, um fortzufahren.

   Die Funktion liest automatisch die Arten von Change-Anforderungen, die Sie in Ihrem Katalog in ITSM Change-Management eingerichtet haben. Wenn Sie beispielsweise den Namen für Ihre Standard-Change-Anforderungen in ITSM von ändern Standard Bis Vorab genehmigt , Ihr neuer Name wird automatisch in der Liste „Change-Typ“ im Formular „Change-Anforderung erstellen“ angezeigt.
7. Die Felder im Abschnitt „Change-Anforderungsvorschau“ des Formulars sind vorab mit Informationen aus der Korrekturaufgabe gefüllt.
   Bearbeiten Sie diese Felder bei Bedarf.
8. Klicken Sie Auf **Erstellen Sie Einen Change** .
   Die Change-Anforderung wird angezeigt. In der zugehörigen Liste Betroffene CIs werden die CIs aus den Testergebnissen angezeigt, die Ihren Kriterien entsprechen. Wenn die Change-Anforderung eine Genehmigung erfordert, wird die **Genehmigung Anfordern** Schaltfläche wird angezeigt.

   Nachdem die Change-Anforderung erstellt wurde, wird die Testergebnisgruppe zu verschoben **Warten Auf Implementierung** status. Nachdem die Change-Anforderung für diese Korrekturaufgabe gelöst wurde und keine weiteren offenen Change-Anforderungen mit dieser Korrekturaufgabe verknüpft sind, wird die Korrekturaufgabe ebenfalls in verschoben **Gelöst** status.

   Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

   Hinweis:
   Sie können Change-Anforderungen und Korrekturaufgaben weiterhin manuell durch die status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn jedoch die Statussynchronisierung aktiviert ist. Wenn das System registriert, dass sich der Status einer Change-Anforderung geändert hat, oder Sie eine Change-Anforderung hinzufügen oder sie aus einer Korrekturaufgabe entfernen, kann die Statussynchronisierung Ihre manuellen Eingriffe möglicherweise überschreiben. status von Change-Anforderungen verschieben die Korrekturaufgabe jedoch nicht automatisch aus dem Geschlossen Oder Zurückgestellt status.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu

Ordnen Sie eine Korrekturaufgabe in zu Konfigurations-Compliance Anwendung auf eine vorhandene Change-Anforderung.

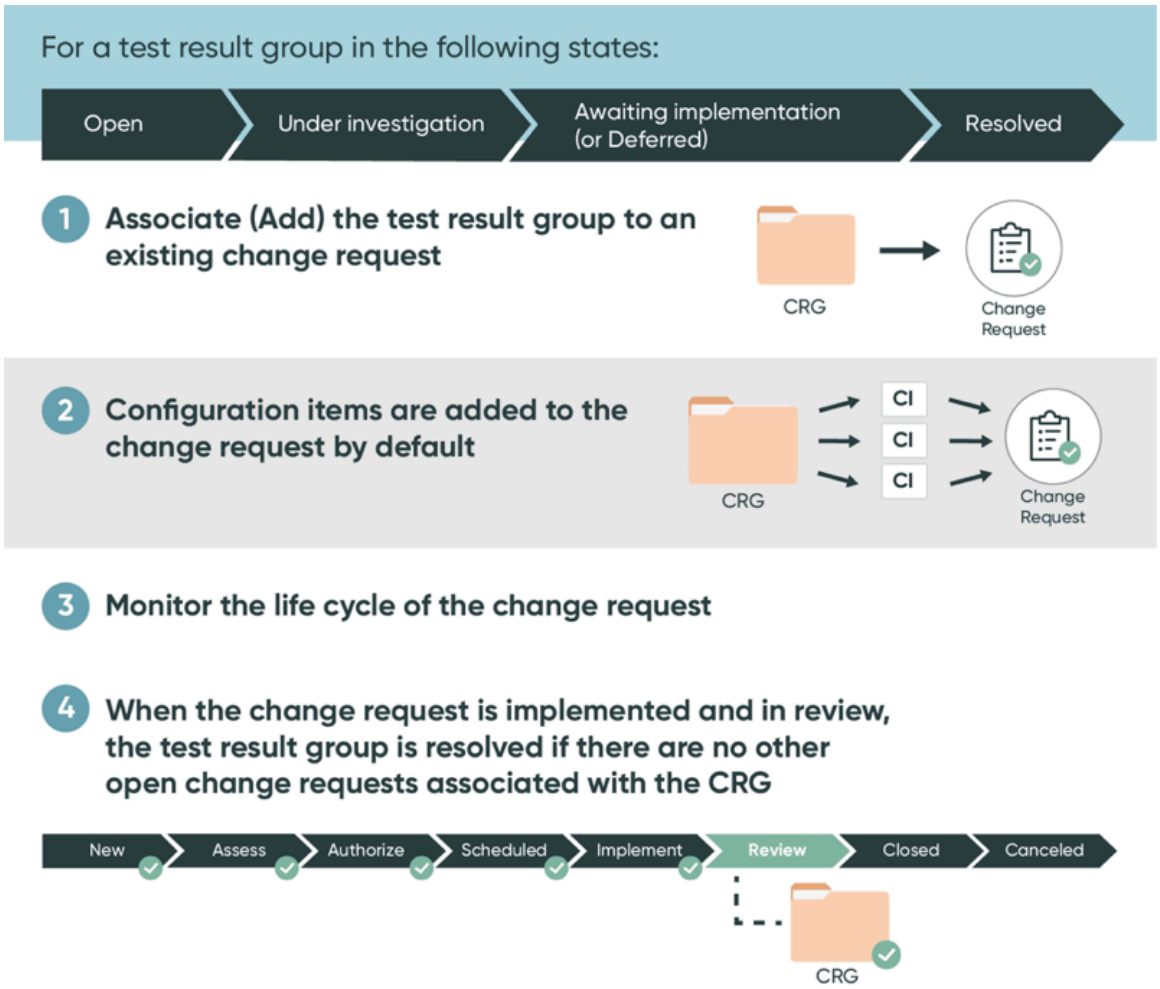
Vorbereitungen
Erforderliche Rolle: Ein Anwender mit der Rolle itil

Warum und wann dieser Vorgang ausgeführt wird
Vermeiden Sie als IT- oder Korrekturspezialist die Erstellung doppelter Change-Anforderungen (CHG), wenn Sie an der Lösung Ihrer Korrekturaufgaben arbeiten, indem Sie eine Korrekturaufgabe (RT) einer Change-Anforderung zuordnen, die bereits in Ihrer Instanz verfügbar ist.

Sie können Korrekturaufgaben, die Ihnen oder Ihrer Zuweisungsgruppe zugewiesen sind, vorhandenen Change-Anforderungen direkt aus den Korrekturaufgaben-Datensätzen zuordnen. Die folgende Abbildung zeigt den grundlegenden Flow zum Zuordnen einer vorhandenen Change-Anforderung zu einer Korrekturaufgabe. Die detaillierten Schritte für diesen Flow folgen dem Bild.

Hinweis:
Sie können eine vorhandene Change-Anforderung einer Korrekturaufgabe in einem anderen Status als zuordnen **Abgebrochen** (**Öffnen** , **Wird Untersucht** , **Warten Auf Implementierung** , **Geschlossen** , Und **Zurückgestellt**). Change-Anforderungen, einschließlich der in den letzten 90 Tagen geschlossenen, können über das Formular zugeordnet werden. Wenn Sie eine Change-Anforderung einer vorhandenen Korrekturaufgabe zuordnen, werden der Change-Anforderung nur die aktiven Testergebnisse und ihre Konfigurationselemente hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben** > **Meine offenen Aufgaben**an.
   Die Liste der Korrekturaufgaben, die Ihren Gruppen zugewiesen sind, wird angezeigt.
2. Klicken Sie in der Spalte Nummer auf die Korrekturaufgabe, für die Sie eine Change-Anforderung erstellen möchten.

   Der Datensatz der Korrekturaufgabe wird angezeigt.
3. Klicken Sie oben rechts im Datensatz auf **Erstellen Sie Einen Change** .
   Das Formular „Change-Anforderung“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Scrollen Sie zur zugehörigen Liste Change-Anforderungen, und wählen Sie sie aus.
   Alle Change-Anforderungen, die der Korrekturaufgabe zugeordnet sind, werden zusammen mit angezeigt **Hinzufügen** Schaltfläche.
5. Klicken Sie auf **Hinzufügen**.
   Das Dialogfeld vorhandene Change-Anforderung zu Korrekturaufgabe hinzufügen wird angezeigt.
6. Klicken Sie auf das Suchsymbol, und wählen Sie ein Element aus der Liste aus.
   Sie können die angezeigte Liste filtern, um Ihre Suche einzugrenzen.
7. Klicken Sie auf **Absenden**.
   Das TRG wird zusammen mit einer Meldung angezeigt, die angibt, dass die Change-Anforderung erfolgreich der Korrekturaufgabe zugeordnet wurde. In der zugehörigen Liste „Change-Anforderungen“ wird die neue Change-Anforderung angezeigt. Die CIs aus der Korrekturaufgabe werden standardmäßig der Change-Anforderung hinzugefügt und in der zugehörigen Liste „Betroffene CIs“ angezeigt. Sie können der Change-Anforderung auch CIs aus dieser zugehörigen Liste hinzufügen. Eine Meldung gibt die Anzahl der Testergebnisse an, die in die neue Korrekturaufgabe verschoben wurden, und die neue RT wird angezeigt.

   Hinweis:
   Bei weniger als 200 Testergebnissen wird der Aufteilungsvorgang synchron ausgeführt, und die Testergebnisse werden in der neuen Korrekturaufgabe angezeigt.

   Bei mehr als 200 Testergebnissen wird der Aufteilungsvorgang asynchron im Hintergrund ausgeführt, und es kann einige Sekunden dauern, bis die Testergebnisse in der neuen Korrekturaufgabe angezeigt werden. Die folgende Meldung wird ebenfalls angezeigt: n Testergebnisse werden in Kürze von TRGxxxxxx in die neue Korrekturaufgabe GRCxxxxx verschoben.

Sie können der Korrekturaufgabe alle Change-Anforderungen zuordnen, mit den folgenden Ausnahmen:

- Change-Anforderungen in **Abgebrochen** status.
- Change-Anforderungen in **Geschlossen** status älter als 90 Tage.
- Change-Anforderungen, die der RT bereits zugeordnet sind. Das System erlaubt Ihnen nicht, eine Change-Anforderung zuzuordnen, die bereits der RT zugeordnet ist.

Nachdem die Change-Anforderung für diese Korrekturaufgabe gelöst wurde und keine weiteren offenen Change-Anforderungen mit dieser Korrekturaufgabe verknüpft sind, wird die Korrekturaufgabe ebenfalls in verschoben **Gelöst** status.

Hinweis:
Sie können Change-Anforderungen und Korrekturaufgaben weiterhin manuell durch die status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn jedoch die Statussynchronisierung aktiviert ist. Wenn das System registriert, dass sich der Status einer Change-Anforderung geändert hat, oder Sie eine Change-Anforderung hinzufügen oder sie aus einer Korrekturaufgabe entfernen, kann die Statussynchronisierung Ihre manuellen Eingriffe möglicherweise überschreiben. status von Change-Anforderungen verschieben die Korrekturaufgabe jedoch nicht automatisch aus dem Geschlossen Oder Zurückgestellt status.

Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

Teilen Sie eine Korrekturaufgabe auf

Aus einer vorhandenen Korrekturaufgabe in Konfigurations-Compliance Anwendung: Identifizieren Sie eine Teilmenge der Testergebnisse, die Sie in eine neue Korrekturaufgabe verschieben möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Als Administrator und Korrekturbesitzer können Sie eine Korrekturaufgabe aus dem aufteilen Vulnerability Manager-Arbeitsbereich Und IT-Korrekturarbeitsbereich Entsprechend.

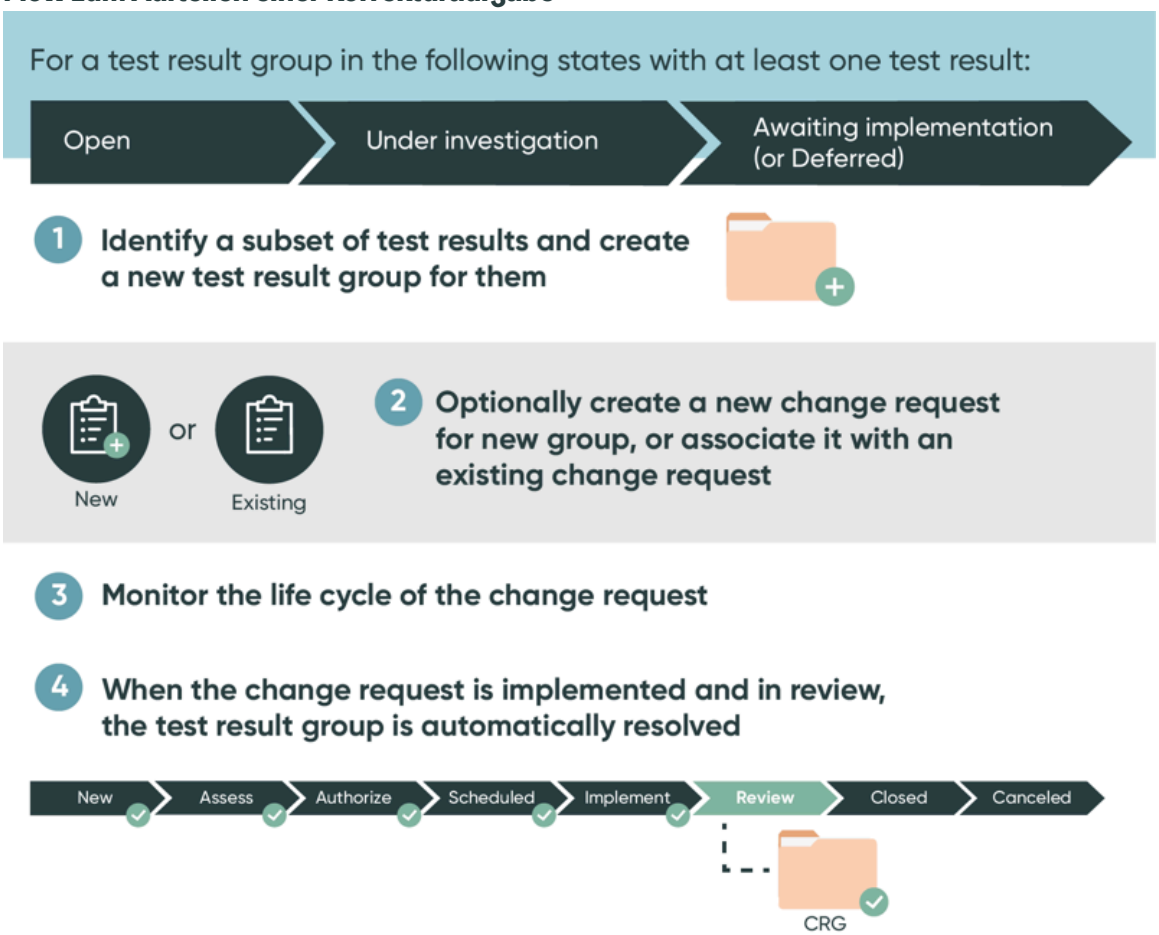
Vorbereitungen
Erforderliche Rolle: Ein Anwender mit der Rolle itil

Warum und wann dieser Vorgang ausgeführt wird
Als IT- oder Korrekturspezialist können Sie vorhandene Korrekturaufgaben in aufteilen **Öffnen** , **Wird Untersucht** , Oder **Warten Auf Implementierung** status mit mehr als einem Testergebnis. Indem Sie eine neue Korrekturaufgabe mit Testergebnissen erstellen, die bestimmten Kriterien entsprechen, können Sie mit einer bestimmten Gruppe von Testergebnissen arbeiten, ohne die ursprüngliche Korrekturaufgabe zu beeinträchtigen.

Wenn Sie die Bedingungen für die Testergebnisse angeben, die Sie mit dem Bedingungsgenerator in eine neue Korrekturaufgabe verschieben möchten, werden nur die aktiven Testergebnisse, die Ihren Kriterien entsprechen, in die neue Aufgabe verschoben. Sie müssen keine Change-Anforderungen (CHGs) erstellen, wenn Sie eine Korrekturaufgabe aufteilen. Sie haben die Möglichkeit, eine Korrekturaufgabe gleichzeitig aufzuteilen, wenn Sie eine Change-Anforderung erstellen, oder Sie können eine Korrekturaufgabe aufteilen, ohne eine Change-Anforderung zu erstellen.

Die folgende Abbildung zeigt den grundlegenden Flow zum Aufteilen einer Korrekturaufgabe. Die detaillierten Schritte für diesen Flow folgen dem Bild.

Flow zum Aufteilen einer Korrekturaufgabe



Anwendungsfälle zum Aufteilen von Testergebnissen aus vorhandenen Korrekturaufgaben in neue Aufgaben können die folgenden Beispiele umfassen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie eine Change-Anforderung oder Change-Anforderungen für eine geteilte Aufgabe erstellen möchten.
- Wenn Sie eine geteilte Aufgabe einem anderen Anwender in Ihrer Zuweisungsgruppe neu zuweisen.
- Wenn Sie eine Zurückstellung oder Ausnahme für eine geteilte Aufgabe anfordern, da Sie wissen, dass einige Testergebnisse zu bestimmten Konfigurationselementen (Configuration Items, CI) in einem bestimmten Zeitrahmen nicht behoben werden können.

[store-future: BEGIN review]Ab Version 19,0 von Vulnerability Response, Sie können Korrekturaufgaben im IT-Korrekturarbeitsbereich aufteilen.[End]

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Tests** > **Korrekturaufgaben** > **Meine offenen Aufgaben**an.
   Die Liste der Korrekturaufgaben, die Ihren Gruppen zugewiesen sind, wird angezeigt.
2. Klicken Sie in der Spalte Nummer auf die Korrekturaufgabe, die Sie aufteilen möchten.

   Der Datensatz der Korrekturaufgabe wird angezeigt.
3. Führen Sie die folgenden Schritte aus, um eine Teilmenge von Testergebnissen für eine neue Aufgabe zu erstellen, die bestimmten Kriterien entspricht.

   Klicken Sie oben rechts im Datensatz auf **Aufgabe Aufteilen** .

   Sie können diese Methode zum Erstellen einer neuen Korrekturaufgabe bevorzugen, wenn Sie aus einer großen Gruppe mit mehreren Testergebnissen arbeiten.

   Das Formular „Korrekturaufgabe aufteilen“ wird angezeigt.
4. Geben Sie bei angezeigtem Bedingungsgenerator die Bedingungen für die Testergebnisse an, die Sie in eine neue Korrekturaufgabe verschieben möchten.

   Beispielsweise möchten Sie nur Testergebnisse herausfiltern, die den folgenden Bedingungen entsprechen:

   - In **Öffnen** status.
   - Risikopunktzahlen größer als 75.
   - Ergebnis ist **Fehlgeschlagen** .

   Wenn Testergebnisse mit Ihrem Filter übereinstimmen, nachdem Sie die Bedingungen eingegeben haben, wird eine Meldung mit der Anzahl der übereinstimmenden Testergebnisse angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine Meldung angezeigt wird, dass keine Testergebnisse mit Ihrem Filter übereinstimmen oder dass alle Ihre Testergebnisse Ihren Kriterien entsprechen, passen Sie die Bedingungen so an, dass mindestens ein Testergebnis Ihren Filterkriterien entspricht.

5. Klicken Sie Auf **Vorschau der Elemente anzeigen** Zum Anzeigen der übereinstimmenden Testergebnisse.
   In einem neuen Fenster, Korrekturaufgaben, werden die Elemente angezeigt.
6. Um eine Vorschau der Testergebnisse anzuzeigen, die Ihren Filterkriterien entsprechen, führen Sie die folgenden Schritte aus, bevor Sie auf klicken **Aufgabe Aufteilen** Um die neue Gruppe zu erstellen. Diese Details umfassen die Zuweisungsgruppe und die Zuweisungsgruppe, der das Testergebnis zugewiesen ist. Das Anzeigen dieser Informationen in der Vorschau kann dazu beitragen, dass die neue Aufgabe ordnungsgemäß zugewiesen wird.

   a. Klicken Sie in der Vorschau auf ein Element in der Ergebnisspalte, wenn die Liste „Nachbesserungen“ angezeigt wird.
      Der Testergebnisdatensatz wird angezeigt.

   b. Verifizieren Sie **Zuweisungsgruppe** Und **Zugewiesen an** Felder sind korrekt.

   c. Klicken Sie auf **Aktualisieren**.

7. Wenn Sie bereit sind, die neue Korrekturaufgabe zu erstellen, klicken Sie auf **Aufgabe Aufteilen** .
   Eine Meldung gibt die Anzahl der Testergebnisse an, die in die neue Korrekturaufgabe verschoben werden, und die neue Korrekturaufgabe wird angezeigt. Um die neue Aufgabe zu identifizieren, sollten Sie den Text möglicherweise in bearbeiten **Kurzbeschreibung** Feld und bearbeiten Sie die Felder Zuweisungsgruppe oder Zugewiesen an erneut, falls erforderlich.

   Hinweis:
   Bei weniger als 200 Testergebnissen wird der Aufteilungsvorgang synchron ausgeführt, und die Testergebnisse werden in der neuen Aufgabe angezeigt.

   Bei mehr als 200 Testergebnissen wird der Aufteilungsvorgang asynchron im Hintergrund ausgeführt, und es kann einige Sekunden dauern, bis die Testergebnisse in der neuen Aufgabe angezeigt werden. Die folgende Meldung wird ebenfalls angezeigt: n Testergebnisse werden in Kürze von TRGxxxxxx in die neue Korrekturaufgabe GRCxxxxx verschoben.

8. Alternativ können Sie eine neue Korrekturaufgabe erstellen, indem Sie Testergebnisse direkt aus der zugehörigen Liste Testergebnisse in einer Korrekturaufgabe auswählen.

   Sie können diese Methode bevorzugen, wenn Sie nur wenige Testergebnisse in einer Korrekturaufgabe haben oder genau wissen, welche Tests Sie in eine neue Korrekturaufgabe verschieben möchten.

   a. Wenn der Datensatz der Korrekturaufgabe angezeigt wird, scrollen Sie zur zugehörigen Liste Testergebnisse.

   b. Aktivieren Sie in der Spalte ganz links die Kontrollkästchen für die Testergebnisse, für die Sie eine neue Korrekturaufgabe erstellen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Klicken Sie in der Liste Aktionen für ausgewählte Zeilen unten links im Datensatz auf **Aufgabe Aufteilen** .

d. Im angezeigten Formular „Korrekturaufgabe aufteilen“ können Sie den Text im bearbeiten, um die neue Gruppe zu identifizieren **Kurzbeschreibung** Feld.

e. Klicken Sie Auf **Aufgabe Aufteilen** .
Eine Meldung gibt die Anzahl der Testergebnisse an, die in die neue Aufgabe verschoben wurden, und die neue Korrekturaufgabe wird angezeigt.

Nachdem die Change-Anforderung für diese Korrekturaufgabe gelöst wurde und keine weiteren offenen Change-Anforderungen mit dieser Korrekturaufgabe verknüpft sind, wird die Korrekturaufgabe ebenfalls in verschoben **Gelöst** status.

Hinweis:
Sie können Change-Anforderungen und Korrekturaufgaben weiterhin manuell durch die status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn jedoch die Statussynchronisierung aktiviert ist. Wenn das System registriert, dass sich der Status einer Change-Anforderung geändert hat, oder Sie eine Change-Anforderung hinzufügen oder sie aus einer Korrekturaufgabe entfernen, kann die Statussynchronisierung Ihre manuellen Eingriffe möglicherweise überschreiben. status von Change-Anforderungen verschieben die Korrekturaufgabe jedoch nicht automatisch aus dem Geschlossen Oder Zurückgestellt status.

Weitere Informationen finden Sie unter Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben.

Nächste Maßnahme
Sie können Change-Anforderungen für Ihre neuen Korrekturaufgaben erstellen oder zuordnen. Weitere Informationen finden Sie unter Ordnen Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe zu und Change-Anforderung in Konfigurations-Compliance erstellen.

Entfernen Sie Zuweisungen aus Korrekturaufgaben für Sie oder Ihre Gruppen

Weisen Sie die Testergebnisdatensätze in neu zu Konfigurations-Compliance Anwendung, wenn die Datensätze Ihnen oder Ihrer Gruppe falsch zugewiesen wurden.

Vorbereitungen
Erforderliche Rolle: sn_vulc.Remediation_owner

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie feststellen, dass Korrekturaufgaben (RTS) und die zugehörigen Testergebnisse nicht in Ihrem Korrekturbereich liegen oder wenn Sie der Meinung sind, dass Datensätze Ihnen oder Ihren Gruppen falsch zugewiesen wurden, können Sie sich selbst oder Ihre Gruppen aus den Feldern Zugewiesen an und Zuweisungsgruppe in RT-Datensätzen entfernen.

Die **Zuweisung Aufheben** Die Schaltfläche wird in Korrekturaufgabendatensätzen in einem anderen Status als dem status „Geschlossen“ oder „gelöst“ angezeigt.

Prozedur

1. Navigieren Sie zu einem Ihnen zugewiesenen Korrekturaufgabendatensatz, der sich in einem anderen Status als „Geschlossen“ oder „gelöst“ befindet.
2. Zum Löschen von **Zugewiesen an** Und **Zuweisungsgruppe** Wählen Sie oben im Datensatz Felder aus **Zuweisung Aufheben** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. In **Zuweisung Aufheben** Dialogfeld, geben Sie Arbeitsnotizen an, und wählen Sie aus **Übermitteln** .
   - Die von Ihnen angegebenen Arbeitsnotizen werden im Abschnitt „Notizen“ angezeigt.
   - Auf der **Genehmigung Der Statusänderung** Registerkarte zeigt der Datensatz für die Genehmigung von Statusänderungen (CA#) den Status in Überprüfung an, was Ihnen hilft, den Genehmigungs-Workflow nachzuverfolgen.
   - Auf der **Angeforderte Genehmigungen** Registerkarte wird Ihre Anforderung zum Entfernen von Ihnen oder Ihrer Zuweisungsgruppe als Status angefordert angezeigt.
4. **Wahlweise:** Alternativ wählen Sie aus **Zuweisung Aufheben** Im Menü „weitere Optionen“ (

), um die Zuweisungsfelder zu löschen.

Ergebnisse

Die Anforderung wird mit einem standardmäßigen Genehmigungs-Workflow auf einer Ebene genehmigt. Weitere Informationen finden Sie unter Genehmigen Sie eine Anforderung zum Aufheben der Zuweisung in Configuration Compliance .

- Wenn Ihre Anforderung genehmigt ist, gehen der Status-Change-Genehmigungsdatensatz und der Datensatz für angeforderte Genehmigung zu über **Genehmigt** . Sie und Ihre Gruppen werden aus entfernt **Zugewiesen an** Und **Zuweisungsgruppe** Felder. Nicht Zugewiesen Wird in angezeigt **Zuweisungstyp** Und die Korrekturaufgabe wird in der Liste des Moduls nicht zugewiesen für angezeigt Konfigurations-Compliance Anwendung.

  Benachrichtigungen, dass Datensätze nicht zugewiesen werden, werden automatisch an Schwachstellenmanager oder Analysten in der Benachrichtigungsgruppe „Zuweisung aufheben“ gesendet. Weitere Informationen zu den Benachrichtigungen und den Eigenschaften für diese Funktion finden Sie unter Entfernen von Zuweisungen aus Konfigurations-Compliance-Testergebnisgruppen .

- Wenn Ihre Anforderung abgelehnt wird, wechseln der Status „Genehmigungsdatensatz“ und der Datensatz „angeforderte Genehmigung“ in „abgelehnt“.

Hinweis:
Als Schwachstellenadministrator können Sie festlegen `sn_vulc.unassign_test_result_group.approval_required`Systemeigenschaft zu **Falsch** Zum Deaktivieren des Genehmigungsprozesses.

Nächste Maßnahme

Navigieren Sie zum Modul nicht zugewiesen für Konfigurations-Compliance Die Anwendung überwacht alle nicht zugewiesenen Datensätze auf Elemente, die in Ihren Bereich fallen könnten, und weist sie dann sich selbst neu zu.

Genehmigen Sie eine Anforderung zum Aufheben der Zuweisung in Konfigurations-Compliance

Genehmigen Sie Anforderungen zum Entfernen von Korrekturaufgaben aus einer Zuweisungsgruppe oder einem einzelnen Anwender in Konfigurations-Compliance Anwendung.

Vorbereitungen

Erforderliche Rolle: sn_vulc.unassign_Approver

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig wird eine Genehmigungskonfiguration bereitgestellt. Zum Aufheben der Zuweisung von Genehmigungen ist ein Genehmiger in der Genehmigungsgruppe „Genehmiger – Ebene 1“ erforderlich. Standardmäßig hebt die Zuweisung der Genehmigungsgruppe auf (Zuweisung des Genehmigers aufheben CC – Ebene 1) Wird erstellt, und Anwender, die Teil dieser Gruppe sind, können die Anforderung genehmigen. Standardmäßig enthält diese Gruppe die Rolle „Genehmiger aufheben“, „sn_vulc.unassign_Approver“. Sie können eine Gruppe ändern oder erstellen und die Genehmigungskonfiguration aktualisieren, indem Sie zu navigieren **Alle** > **Konfigurations-Compliance** > **Administration** > **Genehmigungsregeln** > **Change-Anforderung für Korrekturaufgabenfeld** > **Zuweisung der Korrekturaufgabe aufheben**an.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Meine Genehmigungen**an.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie ab, indem Sie die entsprechenden Kommentare hinzufügen.

Automatisches Schließen von Testergebnissen

Sie können Testergebnisse (TRs), die stillgelegten Konfigurationselementen (Configuration Items, CIs) zugeordnet sind, automatisch schließen.

Um die Option zum automatischen Schließen zu konfigurieren, navigieren Sie zur Systemeigenschaft **sn_vulc.auto_close_test_results_linked_to_retired_CIs** Und legen Sie sie auf „wahr“ fest. Informationen zum automatischen Schließen von TRs im Zusammenhang mit stillgelegten CIs finden Sie unter Schließen Sie Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch.

Informationen zum Arbeiten mit stillgelegten Konfigurationselementen finden Sie unter Arbeiten mit stillgelegten Konfigurationselementen in Konfigurations-Compliance.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Arbeiten mit stillgelegten Konfigurationselementen in Konfigurations-Compliance

Außer Betrieb genommene Konfigurationselemente (CIs) werden in den Status „stillgelegt“, „archiviert“ oder „gelöscht“ verschoben Configuration Management Database (CMDB). Konfigurations-Compliance Enthält Testergebnisse (TRs), die aus CIs bestehen. Wenn der Status eines CI auf „stillgelegt“ aktualisiert wird, werden die zugehörigen TRs mit dem Substatus „CI außer Betrieb genommen“ geschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Wenn die CMDB den Status der Lebenszyklusphase eines CI in „stillgelegt“ ändert, können Sie die zugehörigen TRs automatisch schließen. Weitere Informationen zum automatischen Schließen der zugehörigen TRs finden Sie unter Schließen Sie Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch.

Das stillgelegte CI wird schließlich archiviert oder endgültig aus dem gelöscht CMDB.

Auswirkung der Stilllegung der CIs:

- **Auswirkung auf erkannte Elemente:** Wenn das CI stillgelegt wird, wird das zugehörige DI als „CI außer Betrieb genommen“ markiert.
- **Auswirkung auf Testergebnisse:** Wenn der Status eines DI auf „CI außer Betrieb genommen“ aktualisiert wird, wird die zugehörige TR geschlossen, und der Abschnitt „Notizen“ wird automatisch aktualisiert.

Hinweis:
Der Status eines DI wird automatisch auf „CI außer Betrieb genommen“ aktualisiert, wenn der Lebenszyklusstatus eines CI aktualisiert wird. Andererseits wird der Status einer TR nur dann auf „Geschlossen“ aktualisiert, wenn **sn_vulc.auto_close_test_results_linked_to_retired_CIs** Eigenschaft ist auf „wahr“ festgelegt. Weitere Informationen zum automatischen Schließen der zugehörigen TRs finden Sie unter Schließen Sie Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch.

Die geplante Aufgabe *`Close Test Results for decommissioned CIs`*Wird täglich für die aktualisierte DIS ausgeführt. Wenn die Konfigurationsoption für das automatische Schließen für stillgelegte CIs aktiviert ist, identifiziert sie den DI, der ein stillgelegtes CI enthält, und schließt die zugehörige TR mit dem Substatus „CI außer Betrieb genommen“. Wenn alle TRs in einer Korrekturaufgabe geschlossen sind und ihr Substatus „CI außer Betrieb genommen“ lautet, wird die Korrekturaufgabe auch mit dem Substatus „Abgebrochen“ geschlossen.

Hinweis:
Wenn ein CI vom Status „stillgelegt“ in den ursprünglichen Status zurückversetzt wird, wird auch der Eintrag „erkannte Elemente“ aktualisiert. TRS werden automatisch geöffnet, wenn Daten erneut vom Scanner erfasst werden.

Schließen Sie Testergebnisse im Zusammenhang mit stillgelegten CIs automatisch

Wenn Configuration Management Database (CMDB)Ändert den Status der Lebenszyklusphase eines Konfigurationselements (Configuration Item, CI) in „stillgelegt“. Sie können die zugehörigen Testergebnisse (TRs) automatisch schließen.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Um die zugehörigen TRs automatisch zu schließen, müssen Sie aktivieren Systemeigenschaft **sn_vulc.auto_close_test_results_linked_to_retired_CIs** Dient zum automatischen Schließen von TRs, die stillgelegten CIs zugeordnet sind. Wenn diese Option aktiviert ist, werden neue und vorhandene TRs, die für dasselbe CI gemeldet wurden, automatisch im Status „Geschlossen“ erstellt oder aktualisiert. Diese basieren auf der Asset-ID in der Scanner-Nutzlast und dem Eintragsstatus „erkannte Elemente“. Weitere Informationen zu den Auswirkungen stillgelegter CIs finden Sie unter Arbeiten mit stillgelegten Konfigurationselementen in Konfigurations-Compliance.

Hinweis:
Der Status eines DI wird immer dann auf „CI außer Betrieb genommen“ aktualisiert, wenn der Lebenszyklusstatus eines CI aktualisiert wird. Andererseits wird der Status einer TR nur dann auf „Geschlossen“ aktualisiert, wenn **sn_vulc.auto_close_test_results_linked_to_retired_CIs** Systemeigenschaft ist aktiviert.

Prozedur

1. Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften** Und filtern nach `sn_vulc.auto_close_test_results_linked_to_retired_CIs`In der Spalte Name.
2. Wählen Sie die Eigenschaft aus.
3. Um Testergebnisse, die den stillgelegten CIs zugeordnet sind, automatisch zu schließen, legen Sie den Wert der Eigenschaft auf „wahr“ fest.

Veraltete Testergebnisse in werden automatisch geschlossen Konfigurations-Compliance

Sie können die Funktion „veraltete Testergebnisse automatisch schließen“ aktivieren, um ältere Testergebnisse automatisch zu schließen, die kürzlich von Ihren Drittpartei-Integrationen nicht gefunden wurden. Diese Testergebnisse werden nach verschoben **Geschlossen – Veraltet** Reduziert die Anzahl der aktiven Testergebnisse und Korrekturaufgaben in Ihrer Instanz und hilft Ihnen beim Abgleich von Assets in Ihrem Configuration Management Database (CMDB).

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Übersicht

Das Modul „veraltete Testergebnisse automatisch schließen“ hilft Ihnen, ältere, veraltete Testergebnisse, die kürzlich von Ihren Drittpartei-Integrationen nicht gefunden wurden, automatisch zu schließen. Testergebnisse werden nach verschoben **Geschlossen – Veraltet** Basierend auf den Bedingungen, die Sie im Bedingungsgenerator festgelegt haben.

Wichtige Begriffe

Testergebnis

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Testergebnisse sind importierte Ergebnisse aus Bibliotheken von Konfigurationstests, die Frameworks, Richtlinien und autoritativen Quellen zugeordnet sind, die definieren, wie eine Klasse von Technologie-Assets gesteuert werden soll. Die Konfigurations-Compliance Die Anwendung berechnet die Testergebnisse nicht, importiert sie jedoch mit Integrationen von Drittparteien.

Datum des letzten Scans des Assets

Bezieht sich auf den Wert der Datumsspalte des letzten Konfigurations-Compliance-Scans der Tabelle „erkanntes Element“, die sich auf das Testergebnis bezieht. Dieses Datum bezieht sich auf das aktuelle Datum und die Uhrzeit, zu der ein Asset zuletzt von einem Scanner einer Drittpartei gescannt wurde.

Datum des letzten Fehlschlags

Bezieht sich auf das Datum der zuletzt angezeigten Spalte in der Tabelle „Testergebnisse“, wenn **Ergebnis** Feldwert ist [fehlgeschlagen].

Veraltete Testergebnisse

Bezieht sich auf Testergebnisse in Ihrer Instanz, die veraltet sind und für einen erheblichen Zeitraum nicht von Integrationsscans von Drittparteien gefunden, aktualisiert oder erkannt wurden.

Zuletzt gefundene Testergebnisse

Diese Suchoption verwendet ein Datum und eine Uhrzeit, die vom Scanner des Drittanbieters bereitgestellt werden. Dieser Begriff bezieht sich auf das aktuellste oder späteste Datum (vor Tagen), an dem Testergebnisse vom Scanner erneut gefunden wurden. Dieser Parameter kann konfiguriert werden.

Anwendungsfall

Manchmal werden Assets (Konfigurationselemente) in Ihrer Umgebung außer Betrieb genommen oder von Drittanbieterscannern gelöscht. Wenn dies geschieht, werden die zugehörigen Konfigurationstestergebnisse der Assets in nicht aktualisiert Konfigurations-Compliance Anwendung durch importierte Erkennungen, und sie werden inaktiv (veraltet).

Um die Anzahl der aktiven Testergebnisse (TRs) und Korrekturaufgaben (RTS) in Ihrer Instanz zu reduzieren, aktivieren Sie die Funktion „veraltete Testergebnisse automatisch schließen“. Diese Funktion schließt automatisch veraltete Testergebnisse, die keinen unveränderten status haben oder kürzlich nicht von Ihren Integrationen importiert wurden.

Angenommen, ein bestimmtes Konfigurationselement (Configuration Item, CI) hat mehrere Asset-IDs, und eine dieser IDs wurde in den letzten 90 Tagen nicht für Erkennungen von einem Drittpartei-Scanner importiert. Wenn Sie den Bedingungsgenerator im Modul „veraltete Testergebnisse automatisch schließen“ festlegen, um Testergebnisse zu schließen, die in den letzten 90 Tagen oder mehr nicht gefunden oder aktualisiert wurden, schließt diese Funktion automatisch alle Testergebnisse, die dieser Filterung entsprechen.

Hinweis:
Diese Funktion schließt Testergebniserkennungen nur basierend auf den Filterbedingungen, die Sie im Bedingungsgenerator festgelegt haben und von Ihren Scannerintegrationen von Drittanbietern erkannt werden.

Das Feld Lösung

Zur Unterscheidung zwischen den Erkennungen, die von Drittanbieterscannern wie geschlossen werden Qualys Und Tenable.io Produkte und die Funktion „veraltete Testergebnisse automatisch schließen“ in Ihrer Instanz, ein neuer Wert für **Lösung** Feld [Closed-veraltet] wurde hinzugefügt. **Geschlossen – Veraltet** Gibt an, dass eine TR durch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die automatische Schließfunktion geschlossen wurde. **Geschlossen** Oder **Behoben – Geschlossen** Gibt an, dass eine TR von einem Scanner geschlossen wurde.

Rollup von TR-status zu TRGS mit der Funktion „Automatisches Schließen“

Statusfortschritt und -Vorrang für Testergebnisse sind: **Öffnen** > **Geschlossen** > **Behoben – Geschlossen** > **Geschlossen – Veraltet**an.

1. Ob TRs in einer TRG sind **Öffnen** , Der TRG-Status wird nicht geändert.
2. Wenn mindestens eine TR ist **Geschlossen: Behoben** Und der Rest ist es **Geschlossen: Veraltet** , Der TRG-Status wechselt zu **Geschlossen: Behoben** .
3. Wenn alle TRs in einer TRG sind **Geschlossen: Veraltet** , Der TRG-Status wechselt zu **Geschlossen: Abgebrochen** .

Unterstützte Integrationen

Weitere Informationen zu den Integrationen von Drittparteien, die diese Funktion unterstützen, finden Sie unter Qualys Vulnerability Integration verstehen Und Tenable.io Integrationen mit Vulnerability Response Und Konfigurations-Compliance Anwendungen.

Verwenden Sie veraltete Testergebnisse automatisch schließen in Konfigurations-Compliance

Aktivieren Sie das automatische Schließen veralteter Testergebnisse (TRs), um ältere Testergebnisse basierend auf von Ihnen festgelegten Filterbedingungen automatisch zu schließen.

Vorbereitungen

Weitere Informationen zu dieser Funktion, wichtigen Begriffen und allen Setups, die möglicherweise für Ihre Drittanbieterintegrationen erforderlich sind, die Testergebnisdaten importieren, finden Sie unter Veraltete Testergebnisse in werden automatisch geschlossen Konfigurations-Compliance.

Erforderliche Rolle: sn_vulc.admin

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Administration** > **Veraltete Testergebnisse automatisch schließen**an.
2. Füllen Sie die Felder aus

Feld	Wert
Name	Name für diesen Konfigurationsdatensatz.
Aktiv	Wenn diese Option ausgewählt ist, ist dieser Datensatz aktiv und schließt automatisch alle Testergebnisse, die seinen Filterkriterien entsprechen.
Veraltete TRs für zurückgestellte TRs ignorieren	Wenn ausgewählt, werden alle TRs, die dem zugeordnet sind **Wird überprüft** Oder **Zurückgestellt** status werden ignoriert und nicht geschlossen. Wenn Sie diese Option deaktivieren, werden alle TRs geschlossen, die Ihren Kriterien entsprechen.
Ausführungsreihenfolge	100 ist der Standardwert. Dieser Wert bestimmt die Reihenfolge der Ausführung in aufsteigender Reihenfolge für jeden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	Konfigurationsdatensatz, der zum Suchen und Markieren veralteter Testergebnisse verwendet wird.
Beschreibung	Eine Beschreibung für diesen Datensatz. Dieser Text kann Ihnen helfen, ihn leicht wiederzufinden, wenn Sie eine größere Anzahl von Datensätzen erstellen.
Bedingung	Die Filterbedingungen, die zum Suchen von TRs verwendet werden, die geschlossen werden sollen. Der Standardfilter ist **Erkanntes Element** > **Letzter Scan**an.

3. Klicken Sie auf **Absenden**.

   Die geplante Aufgabe, *`Auto-Close Stale Test Results`*, Wird täglich ausgeführt. Dieser Auftrag identifiziert die TRs basierend auf den von Ihnen angegebenen Bedingungen und überträgt diejenigen, die dem Status entsprechen: **Geschlossen** .

   Nachdem TRs als Status markiert wurden: **Geschlossen – Veraltet** Wenn der Scanner diese TRs erneut findet, werden die Testergebnisse erneut geöffnet, und der status wird zurück zu **Öffnen** .

   Wenn eine TR als Status markiert ist: **Geschlossen – Veraltet** , Und der Scanner stellt fest, dass es behoben wurde (Auflösung: **Behoben**) Wechselt die TR in den Status: **Geschlossen** Lösung: **Behoben** . TRS, die haben **Ergebnis** : **Bestanden** Als Status beibehalten: **Geschlossen** Lösung: **Behoben** . Status-Rollup auch zu Korrekturaufgaben, wie in der folgenden Liste beschrieben:

   a. Wenn TRs in einer Korrekturaufgabe vorhanden sind **Öffnen** , Der Status der Korrekturaufgabe wird nicht geändert.
   b. Wenn mindestens ein TR den Status hat: **Geschlossen** Lösung: **Behoben** Und der Rest ist es **Geschlossen – Veraltet** , Der Status der Korrekturaufgabe wechselt zu **Geschlossen** Lösung: **Behoben** .
   c. Wenn alle TRs in einer Korrekturaufgabe sind **Geschlossen** Lösung: **Behoben** , Der TRG-Status wechselt in Status: **Geschlossen** Lösung: **Abgebrochen** .

   Weitere Informationen zu Statusübergängen finden Sie unter Statusübergänge von Testergebnissen und Korrekturaufgaben in Konfigurations-Compliance Anwendung.

Schließen Sie eine Korrekturaufgabe

Wenn Sie feststellen, dass das Problem, das einer Korrekturaufgabe zugeordnet ist, sofort ohne weitere Analyse geschlossen werden kann, können Sie verwenden **Schließen** Funktion.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin
- sn_vulc.Remediation_owner

Hinweis:
Mit der Rolle sn_vulc.Remediation_owner können Sie Korrekturaufgaben, die Ihnen oder Ihren Zuweisungsgruppen zugewiesen sind, neu zuweisen oder schließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Ab v15.0 von Konfigurations-Compliance, **Schließen** Schaltfläche wurde für eine Korrekturaufgabe entfernt.

Wenn Sie eine Korrekturaufgabe lösen, werden die Lösungshinweise angezeigt Spiegelt sich in den Arbeitsnotizen aller Testergebnisse wider.

Prozedur

1. Öffnen Sie den Korrekturaufgaben-Datensatz.
2. Wählen Sie aus **Schließen** Schaltfläche.
3. Beschreiben Sie im Popup-Fenster, warum das Problem geschlossen wird.
4. Wählen Sie **Schließen**.

Zugehörige Informationen

Konfigurations-Compliance status

Fordert eine Ausnahme für eine Korrekturaufgabe an und genehmigt sie

Sie können anfordern, die Korrektur einer Korrekturaufgabe für einen bestimmten Zeitraum zu verschieben. Anwender, die Teil der Genehmigergruppe sind, können Ausnahmeanforderungen genehmigen.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Informationen zum anfordern oder Genehmigen von Ausnahmeanforderungen finden Sie unter:

- Fordern Sie eine Ausnahme für eine Korrekturaufgabe in an Konfigurations-Compliance
- Genehmigen Sie eine Ausnahmeanforderung in Konfigurations-Compliance

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

E-Mail-Benachrichtigungen werden in jeder Phase des Ausnahmemanagements gesendet, die den Status und andere Details einer Anforderung angeben. Wenn beispielsweise eine Ausnahme angefordert wird, erhält die anfordernde Person eine E-Mail, die bestätigt, dass die Anforderung ausgelöst wurde. Der Genehmiger erhält auch eine E-Mail, in der angegeben wird, dass eine Ausnahme angefordert wurde.

Ab v14.11 von Konfigurations-Compliance, Sie können die Zeitrahmen für die Genehmigung von Ausnahmen sowie E-Mail-Benachrichtigungen für den Genehmiger und die anfordernde Person nach einer festgelegten Anzahl von Tagen konfigurieren. Wenn eine Anforderung ausgelöst wird, ändert sich das Testergebnis in den Status „in Überprüfung“, und ein Statusänderungsdatensatz wird erstellt. Wenn der Genehmiger nicht innerhalb des konfigurierten Zeitrahmens antwortet, wird das Testergebnis auf den Status „Offen“ zurückgesetzt. Der vorherige Status wird in gespeichert **Backup_State** Feld. Weitere Informationen finden Sie unter Konfigurieren Sie Genehmigungsregeln für das Ausnahmemanagement.

Fordern Sie eine Ausnahme für eine Korrekturaufgabe in an Konfigurations-Compliance

Fordern Sie eine Ausnahme an, um die Korrektur einer Korrekturaufgabe für einen bestimmten Zeitraum aufzuschieben, wenn sie nicht sofort behoben werden kann.

Vorbereitungen

Erforderliche Rolle: sn_vulc.Remediation_owner

Warum und wann dieser Vorgang ausgeführt wird

Wichtig:

Sie können eine Ausnahme anfordern für:

- Korrekturaufgaben in Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen. Weitere Informationen finden Sie unter Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen.
- Mehrere Testergebnisse gleichzeitig von Arbeitsbereich des Schwachstellenmanagers. Weitere Informationen finden Sie unter Fordern Sie eine Massenausnahme im Vulnerability Manager-Arbeitsbereich an.

Hinweis:

Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben** > **Alle Aufgaben**an.
2. Wählen Sie die Korrekturaufgabe aus, für die Sie eine Ausnahme anfordern möchten.
   Die ausgewählte Aufgabe muss sich im Status Offen, wird untersucht oder wartet auf Implementierung befinden.
3. Klicken Sie im Formular „Korrekturaufgabe“ auf **Ausnahme Anfordern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Abhängig davon, ob Vulnerability Response Oder GRC: Richtlinien- und Compliance-Management Ist in ausgewählt **Konfigurations-Compliance** > **Ausnahmenverwaltung** Bildschirm ändert sich das Formular „Ausnahme anfordern“. Siehe Konfigurieren Sie das Ausnahmemanagement für Konfigurations-Compliance

4. Wenn Vulnerability Response Im Bildschirm „Ausnahmemanagement“ ausgewählt ist, gehen Sie dann wie folgt vor:

   a. Füllen Sie im Formular die Felder aus.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Bis	Datum, an dem die Ausnahmeanforderung abläuft. Dieses Datum muss innerhalb der in ausgewählten Dauer liegen **Alle** > **Konfigurations-Compliance** > **Administration** > **Ausnahmenverwaltung** Bildschirm. Wenn die Ausnahmeanforderung abläuft, kehrt die Korrekturaufgabe in den Status „Offen“ zurück. **Hinweis:** Ab Version 14,7 von Konfigurations-Compliance(CC) wenn eine zurückgestellte Korrekturaufgabe von einem Scanner erneut geöffnet wird, bevor das Ausnahmefenster abläuft, ändert sich der Status der Korrekturaufgabe von Offen in zurückgestellt. Diese Funktionalität ist standardmäßig deaktiviert. Um diese Funktionalität zu aktivieren, legen Sie den Wert der Systemeigenschaft fest `sn_vulc.auto_defer_test_result_in_active_exc` „wahr“. Außerdem wird das Datum „Zurückgestellt bis“ auch nach dem Ablaufdatum der Korrekturaufgabe beibehalten.
Grund	Grund für die Ausnahme. Die Auswahlmöglichkeiten lauten wie folgt: ▪ Risiko akzeptiert ▪ Warten auf Wartungsfenster ▪ Behebung nicht verfügbar ▪ Ausgleichende Steuerung vorhanden ▪ Sonstige Informationen zum Hinzufügen neuer Ursachenauswahlen finden Sie unter Definieren Sie Richtliniengrundzuordnungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zusätzliche Information	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer aktualisiert werden.

b. Senden Sie die Ausnahmeanforderung, indem Sie auf klicken **Genehmigung Anfordern** .

Ergebnisse
Der Status der Korrekturaufgabe ändert sich in „in Überprüfung“. Verwenden Sie **Genehmigung Der Statusänderung** Registerkarte zum Nachverfolgen des Status der Ausnahmeanforderung.

Fordern Sie eine Verlängerung für eine Korrekturaufgabe an

Fordern Sie eine Verlängerung für eine zurückgestellte Korrekturaufgabe an, bevor sie das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch eine Verlängerung über anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Vulnerability Manager-Arbeitsbereich an.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur
1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben**an.
2. Öffnen Sie eine zurückgestellte Korrekturaufgabe.
3. Wählen Sie Aus **Verlängerung Anfordern** .
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, an dem der Status Zurückstellen abläuft und die Korrekturaufgabe erneut aktiviert wird.
Grund	Geben Sie den Grund für die Zurückstellung des Problems ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Risiko akzeptiert ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.

Hinweis:

- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Die Schaltfläche „Verlängerung anfordern“ ist für Korrekturaufgaben nicht verfügbar, die als Teil einer Ausnahmeregel erstellt werden.
- Wenn eine zurückgestellte Korrekturaufgabe erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End.

Fordern Sie eine Verlängerung für eine Ausnahmeregel in an Konfigurations-Compliance

Fordern Sie eine Verlängerung für eine zurückgestellte Ausnahmeregel an, bevor sie das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen

Erforderliche Rolle: sn_vul.Exception_Approver

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch eine Verlängerung über anfordern Vulnerability Response Arbeitsbereiche. Weitere Informationen finden Sie unter Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Vulnerability Manager-Arbeitsbereich an.

Hinweis:

Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Ausnahmeregeln**an.
2. Wählen Sie eine genehmigte Ausnahmeregel aus.
3. Wählen Sie Aus **Verlängerung Anfordern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem die Ausnahmeregel erweitert werden muss.
Grund	Geben Sie den Grund für die Zurückstellung der Ausnahmeregel ein. Zur Auswahl stehen: ○ Risiko akzeptiert ○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

5. Wählen Sie **Genehmigung anfordern**.
   Bei Genehmigung der Anforderung werden die Felder Zurückgestellt bis, Grund und zusätzliche Informationen für die Ausnahmeregel und die zugehörigen Korrekturaufgaben aktualisiert. Eine E-Mail wird auch bei der Übermittlung der Anforderung und der nachfolgenden Aktion durch den Genehmiger ausgelöst.

Hinweis:
- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Wenn eine zurückgestellte Ausnahmeregel erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End.

Fordern Sie mit eine Ausnahme für Korrekturaufgaben an GRC: Richtlinien- und Compliance-Management

Fordern Sie Richtlinienausnahmen mit an GRC Fähigkeit zur Verwaltung von Richtlinienausnahmen in Richtlinien- und Compliance-Management Anwendung von innerhalb Konfigurations-Compliance.

Vorbereitungen

Bevor Sie die Integration von Richtlinienausnahmen verwenden können, um Richtlinienausnahmen anzufordern, müssen Sie herunterladen GRC: Richtlinien- und Compliance-Management Anwendung aus dem ServiceNow Store.

Erforderliche Rolle: sn_vulc.Remediation_owner

Sie können auch Ausnahmen in der klassischen Anwenderoberfläche anfordern.

Warum und wann dieser Vorgang ausgeführt wird

Wichtig:
Als Administrator und Korrekturbesitzer können Sie im eine Richtlinienausnahme für eine Korrekturaufgabe (RT) anfordern Vulnerability Manager-Arbeitsbereich Und IT-Korrekturarbeitsbereich Entsprechend.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehebungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Application Vulnerability Response** > **Angreifbare Anwendungselemente** (Oder **Korrekturaufgaben**)> **Alle** , Und öffnen Sie das Element oder die Gruppe, für das Sie eine Ausnahme anfordern möchten.
   Das ausgewählte Element oder die ausgewählte Gruppe muss sich im Status „Offen“, „wird untersucht“ oder „Warten auf Implementierung“ befinden.
2. Klicken Sie im ausgewählten Formular auf **Ausnahme Anfordern** .
3. Wenn GRC: Richtlinien- und Compliance-Management Im Bildschirm „Ausnahmemanagement“ ausgewählt ist, gehen Sie wie folgt vor.

   a. Füllen Sie im Formular die Felder aus.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Richtlinie	Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft und der Status des angreifbaren Elements oder der angreifbaren Gruppe von zurückgestellt in Offen geändert wird. **Hinweis:** Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf nicht überschreiten **Maximale Ausnahmedauer (Tage)** Die Sie für die Richtlinie in Richtlinie und Compliance festgelegt haben. Weitere Informationen finden Sie unter Erstellen Sie eine Richtlinie .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Grund	Grund für die Anforderung einer Ausnahme.
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer ausgefüllt werden.

b. Senden Sie die Ausnahmeanforderung, indem Sie auf klicken **Genehmigung Anfordern** .
Der Status der Korrekturaufgabe ändert sich in „in Überprüfung“, und eine Richtlinienausnahme wird erstellt. Verwenden Sie **Genehmigung Der Statusänderung** Registerkarte zum Nachverfolgen des Status der Ausnahmeanforderung.

c. Zeigen Sie die Richtlinienausnahme an, indem Sie auf die zugehörige Liste Richtlinienausnahmen klicken.

d. Klicken Sie auf die Nummer der Richtlinienausnahme.

e. In **Genehmiger** Wählen Sie den Namen des Genehmigers aus.

f. Klicken Sie auf die Registerkarte Quelle, und wählen Sie ein Kontrollziel aus **Kontrollziel** Feld.

g. Klicken Sie auf die Registerkarte Risikobewertung, und wählen Sie die Risikobewertung aus **Risikobewertung** Feld.

h. Speichern Sie das Formular.

i. Klicken Sie auf **Betroffene Steuerungen** Registerkarte.

j. Fügen Sie die Steuerungen hinzu, indem Sie auf klicken **Hinzufügen** .

k. Speichern Sie das Formular.

Hinweis:
Sie können eine Compliance-Überprüfung starten, indem Sie auf klicken **Compliance-Überprüfung anfordern** .

Das Genehmigungsformular wird an den Genehmiger gesendet.

Der Genehmiger kann die Anforderung entweder genehmigen, indem er auf klickt **Genehmigen** Oder fordern Sie eine zusätzliche Genehmigung an, indem Sie auf klicken **Zusätzliche Genehmigung Anfordern** .

Der Datensatzstatus ändert sich in zurückgestellt. Der angegebene Grund ist der, den Sie beim Auslösen der Ausnahmeanforderung ausgewählt haben. Die **Zurückstellung** Die Registerkarte enthält zusätzliche Notizen zum Datensatz.

Hinweis:
Wenn die Anforderung abgelehnt wird, wird der Datensatz in den vorherigen Status verschoben.

4. Klicken Sie auf **Absenden**.
Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Korrekturbesitzer und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigen Sie eine Ausnahmeanforderung in Konfigurations-Compliance

Genehmigen Sie Ausnahmeanforderungen für Korrekturaufgaben, die nicht sofort behoben werden können. Sie müssen diese Anforderungen auf Risiko bewerten und sie dann zur Zurückstellung genehmigen, bis sie behoben werden können.

Wichtig:
Als Administrator oder Analyst können Sie eine Ausnahmeanforderung aus dem Arbeitssapce für Schwachstellenmanager genehmigen oder ablehnen.

Vorbereitungen
Erforderliche Rolle: sn_vulc.Exception_Approver

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Meine Genehmigungen**an.
2. Wählen Sie eine Anforderung aus Ihrer Warteschlange aus.
3. Genehmigen Sie die Anforderung, oder lehnen Sie sie mit entsprechenden Kommentaren ab.

Hinweis:
Im Falle eines zweistufigen Genehmigungs-Workflows wird die Anforderung nach der Genehmigung der ersten Ebene zur weiteren Genehmigung an die zweite Ebene übermittelt. Wenn auf der zweiten Ebene keine Anwender vorhanden sind, wird die Anforderung nach der Genehmigung auf der ersten Ebene automatisch genehmigt.

Nachdem die Anforderung genehmigt wurde, wechselt die Korrekturaufgabe in den Status zurückgestellt. Im Falle einer Ablehnung wird die Korrekturaufgabe in ihren früheren Status zurückgesetzt.

Definieren Sie Richtliniengrundzuordnungen

Sie können die Ursachenauswahlen definieren, die jedem Anwender zur Verfügung stehen, der eine Ausnahme anfordert.

Vorbereitungen
Erforderliche Rolle: sn_vul.compliance.manager und sn_vulc.admin

Prozedur

1. Navigieren zu **Alle** > **Richtlinien und Compliance** > **Richtlinienausnahmen** > **Integrationsregistrierung**an.

Hinweis:
Sie können entweder einen Grund aus den Ursachenauswahlen auswählen, die in der Tabelle „Ursachenauswahlen“ verfügbar sind, oder einen neuen Grund hinzufügen.

2. Klicken Sie auf die Integrationsregistrierung Container Vulnerability Response – CVIT.
3. Führen Sie die folgenden Schritte aus, um eine vorhandene Ursachenauswahl hinzuzufügen:
   a. Klicken Sie in der Liste Ursachenauswahlen auf **Neu** .
   b. Klicken Sie auf das Lupensymbol, um einen Grund auszuwählen.
4. Führen Sie die folgenden Schritte aus, um der Tabelle „Ursachenauswahlen“ neue Ursachenauswahlen hinzuzufügen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der Liste der Ursachenauswahlen auf **Neu** .

b. Klicken Sie auf das Lupensymbol.

c. Klicken Sie auf **Neu**.

d. Füllen Sie im Formular die Felder aus.

Formular „Ursachenauswahlliste“

Feld	Beschreibung
Bezeichnung	Eindeutige Bezeichnung für diese Auswahl.
Wert	Eindeutiger Wert für diese Auswahl. Dieser Wert wird in der Tabelle „Zuordnungen des Grunds für Richtlinienausnahme“ für die jeweiligen Anwendungen zugeordnet. Um zu dieser Tabelle zu navigieren, geben Sie sn_sec_cmn_Policy_reason_Mapping.LIST im Filternavigator ein.
Reihenfolge	Reihenfolge für diese Auswahl. Gründe werden basierend auf dieser Nummer sortiert.
Standard	Option, die angibt, dass diese Ursachenauswahl immer verfügbar ist, wenn eine Richtlinienausnahme bei Bedarf angefordert wird. Wenn die Integrationsregistrierung keine anwendungsspezifischen Auswahlmöglichkeiten enthält, werden alle Ursachenauswahlen mit angegeben **Standard** Das ausgewählte Feld ist verfügbar.
Aktiv	Option zum Anzeigen der Auswahl in der Liste der Ursachenauswahlen.

5. Klicken Sie auf **Absenden**.

Berichterstellung und Analytics für Konfigurations-Compliance

Die folgenden Berichte werden zur Überwachung bereitgestellt.

Zeigen Sie Richtlinien, CIs, Tests und Testergebnisse im an Konfigurations-ComplianceÜbersichtsberichte.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Konfigurations-Compliance Berichterstellung

Die Konfigurations-Compliance Homepage bietet einen Überblick über Richtlinien, CIs, Tests und Testergebnisse für Führungskräfte, sodass Sicherheitspersonal Problembereiche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

schnell erkennen können. Konfigurations-Compliance Bedeutungsdiagramme können nach Bedarf hinzugefügt werden. Sie können auch zurückkehren Konfigurations-Compliance-Zugehörige Informationen mit der globalen Suchfunktion.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

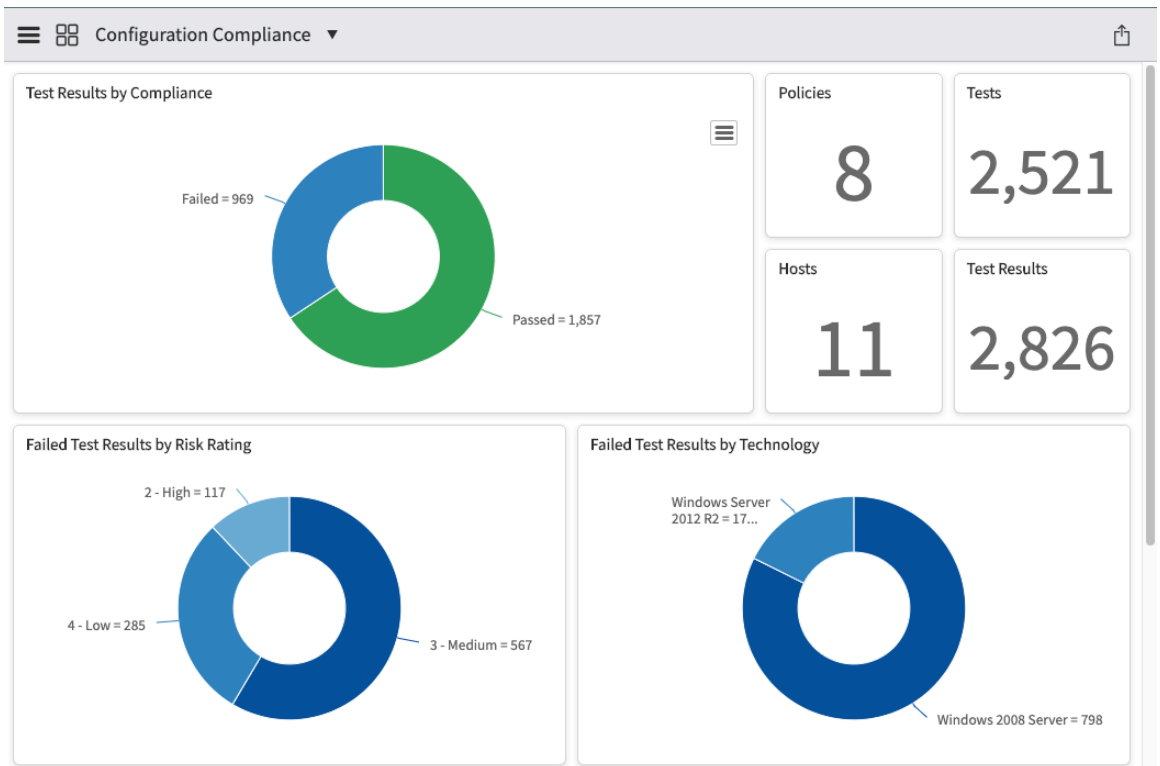
Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

In jedem Diagramm können Sie auf einen beliebigen Teil eines Diagramms (Balken, Kreis, Datenpunkt) verweisen, um allgemeine Daten anzuzeigen, die für diesen Teil des Diagramms spezifisch sind. Wenn Sie auf einen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Hinweis:

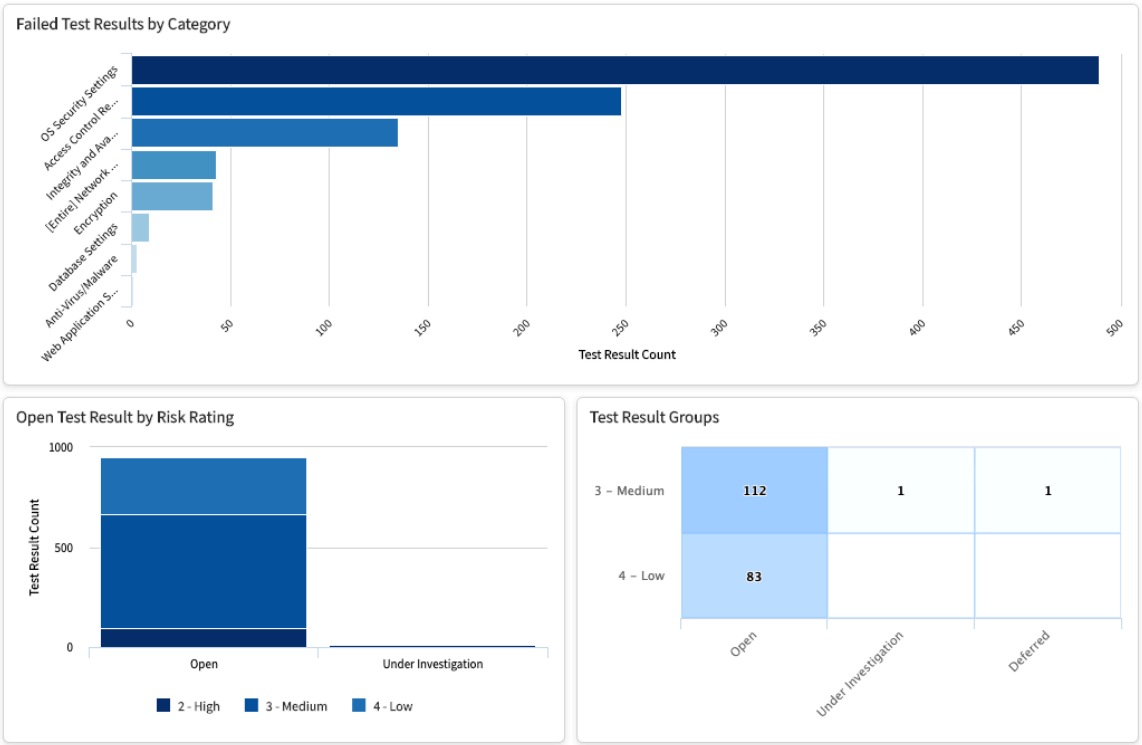
- Dashboards auf der Konfigurations-Compliance Homepage ist nur verfügbar, wenn die Anwendung Performance Analytics für Configuration Compliance aktiviert ist. Schritte zum Aktivieren dieser Anwendung finden Sie unter Performance Analytics für Konfigurations-Compliance aktivieren.
- Jeder mit der Rolle „sn_vulc.read“ kann das Dashboard anzeigen. Jeder mit der Rolle „sn_vulc.write“ oder „sn_vulc.admin“ kann ein Dashboard erstellen und bearbeiten. Nur sn_vulc.admin kann ein Dashboard löschen.

Berichte zur Schwachstellenübersicht



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance-Bericht



Berichte zur Schwachstellenübersicht

Name	Visuell	Beschreibung
Testergebnisse nach Compliance	Ring	Zeigt die Anzahl der offenen Tests an, die bestanden oder fehlgeschlagen sind.
Richtlinien	Anzahl	Anzahl der Richtlinien mit fehlgeschlagenen Testergebnissen.
Tests	Anzahl	Anzahl der Tests mit fehlgeschlagenen Testergebnissen.
Hosts	Anzahl	Anzahl der Hosts mit fehlgeschlagenen Testergebnissen.
Testergebnisse	Anzahl	Zeigt die Anzahl der Testergebnisse an.
Ergebnisse fehlgeschlagener Tests nach Risikobewertung	Ring	Zeigt die Anzahl der fehlgeschlagenen Tests nach Risikobewertung an.
Ergebnisse fehlgeschlagener Tests nach Technologie	Ring	Zeigt Modelle mit fehlgeschlagenen Tests an.
Ergebnisse fehlgeschlagener Tests nach Kategorie	Balkendiagramm	Zeigt Kategorien mit den am häufigsten fehlgeschlagenen Testergebnissen an.
Öffnen Sie das Testergebnis nach Risikobewertung	Balkendiagramm	Zeigt die Anzahl der offenen Testergebnisse nach Risikobewertung an.
Korrekturaufgaben	Diagramm	Zeigt Korrekturaufgaben nach Status und Risikobewertung an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance Dashboard

Dies Platform Analytics-Lösung Enthält vorverpackt Performance Analytics Und Reporting Inhalt zur Verwendung mit anderen ServiceNow AI Platform Produkte. Dies Platform Analytics-Lösung Bietet Einblick in nicht konforme Konfigurationen der Host-Ebene und der Cloud-Steuerungsebene.

Diese Platform Analytics-Lösung enthält vorgefertigte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen ServiceNow AI Platform Produkte. Diese Platform Analytics-Lösung bietet Einblick in nicht konforme Konfigurationen der Host-Ebene und der Cloud-Steuerungsebene.

Das Dashboard „Performance Analytics für Konfigurations-Compliance“ enthält mehrere Widgets, die Daten für verschiedene Dimensionen darstellen. Sie bietet einen umfassenden Überblick über Compliance-Trends, Konfigurationsprobleme, Nachbesserungstrends und Ausnahmemanagement.

Hinweis:
Die Performance Analytics Für Konfigurations-Compliance Plugin muss installiert sein, um anzuzeigen Konfigurations-Compliance[PA] Dashboard in Next Experience Framework. Wenn nicht installiert, können Sie das vorhandene Dashboard anzeigen, das mit dem Reporting-Framework erstellt wird.

Performance Analytics für Konfigurations-Compliance aktivieren

Aktivieren Sie das Inhaltspaket ServiceNow Store Anwendung für Platform Analytics-Lösung.

Vorbereitungen

Aktivieren Sie die vollständige Abonnementversion von Performance Analytics auf der Instanz, auf der Sie diese Platform Analytics-Lösung aktivieren. Sie können Performance Analytics in einer Instanz außerhalb der Produktion aktivieren, ohne ein Abonnement zu erwerben. Weitere Informationen finden Sie unter Performance Analytics-Abonnement aktivieren .

Sie benötigen einen Now Support Account und Berechtigung zum anfordern von Anwendungen für die betroffenen Instanzen. Die Now Support Account und die Instanz müssen Teil desselben Unternehmens sein. Weitere Informationen finden Sie unter Install a ServiceNow Product (ServiceNow-Produkte installieren) im ServiceNow Store.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Performance Analytics Für Konfigurations-Compliance Dashboard zum Generieren von Berichten zu Korrekturaufgaben, Compliance-Status, Korrekturaktionen und Ausnahmeanforderungen.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle Anwendungen** > **ServiceNow Store**an.
2. Suchen Sie nach Performance Analytics Für Konfigurations-Compliance Und überprüfen Sie, ob Sie über die gültigen Berechtigungen verfügen.
3. Suchen Sie nach Performance Analytics für Konfigurations-Compliance .
4. Installieren Sie die Anwendung.

   Wenn Sie diese Anwendung installieren, aktivieren Sie auch Konfigurations-Compliance Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzeigen von Performance Analytics Für Konfigurations-Compliance Dashboard

Sie können Ihre wichtigsten Konfigurationsprobleme verwalten und schnell beheben, indem Sie die Berichte im anzeigen Konfigurations-Compliance Performance Analytics(PA)-Dashboard.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Erforderliche ServiceNow AI Platform-Rollen

Die folgenden Rollen sind für erforderlich Konfigurations-Compliance Performance Analytics Dashboard:

- administrator: Ein Administrator kann installieren und aktivieren Performance Analytics Für Konfigurations-ComplianceUnd nehmen Sie Änderungen an den Systemeigenschaften vor.
- pa_admin: Ein Performance Analytics-Administrator kann Hintergrundaufträge, Indikatoren, Aufgliederungen, Widgets und Dashboards erstellen und überprüfen. Dieser Administrator kann die Datensammlung auch einrichten und starten.
- sn_vulc.read: Ein Anwender mit der Rolle „Lesen“ kann die Dashboard-Daten überprüfen.

Greifen Sie auf zu Konfigurations-Compliance Dashboard

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Konfigurations-Compliance** > **Übersicht**an.

Wichtig:

Ab Version 14,9 von Konfigurations-Compliance, Dieses Dashboard kann auch in der Next Experience-UI angezeigt werden. Um das Dashboard in der neuen Anwenderoberfläche anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** Und klicken Sie auf **Dashboards** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um andere Dashboards anzuzeigen, klicken Sie auf die Dropdown-Liste neben dem Dashboard-Namen. Weitere Informationen finden Sie unter Dashboards im Vulnerability Manager-Arbeitsbereich Und Dashboards im Arbeitsbereich „IT-Korrektur“ .

Hinweis:
Wenn Sie auf sind Tokyo, Sie können die Dashboards in der Next Experience-UI anzeigen, jedoch mit einem gewissen Funktionsverlust.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance [PA] Dashboard-Registerkarten

Registerkarte „Übersicht“

Die **Übersicht** Die Registerkarte bietet fünf Filter. Diese Filter sind die Asset-Kategorie, der Cloud-Ressourcentyp, der Cloud-Service Provider, der Cloud-Account und die Cloud-Region. die Sie anwenden können, um die Berichte für die angewendeten Filter zu visualisieren. Wenn Sie eine Kategorie auswählen und die Änderungen anwenden, werden alle Widgets aktualisiert, die die Kategorie unterstützen. Jedes Widget zeigt unten den angewendeten Filter und die Anzahl der angewendeten Filter auf das Filtersymbol des Widgets an. Klicken Sie in einem Widget auf den Bericht, um die zusätzlichen Informationen zu anzuzeigen **KPI-Details** Registerkarte. Auf der **KPI-Details** Registerkarte können Sie:

- Zeigen Sie die Datensätze an.
- Vergleichen Sie die Datensätze.
- Ändern Sie den Diagrammtyp.
- Wählen Sie den Datumsbereich aus.
- Zeigen Sie die Trends an, die auf der Dauer basieren.
- Wenden Sie die zusätzlichen Filter an, einschließlich der Filter, die auf nicht verfügbar sind **Übersicht** Registerkarte. Ein Beispiel ist das Host-Tag.

Das folgende Beispiel zeigt, wie Sie die Filter in anwenden können **Übersicht** Registerkarte und führen Sie die Aktionen in aus **KPI-Details** Registerkarte.

Registerkarte „Übersicht“ im Dashboard „Konfigurations-Compliance“

Registerkarte „Compliance“

Die **Compliance** Auf der Registerkarte wird der Compliance-Prozentsatz für die verschiedenen autoritativen Quellen angezeigt, z. B. Health Insurance Portability and Accountability Act (HIPAA) und Data Interchange Standards Association (DISA). Sie können diese Liste verfeinern, indem Sie die Spalten-Header-Filter verwenden und eine Kategorie auswählen.

Das folgende Beispiel zeigt, wie Sie die Daten in filtern können **Compliance** Registerkarte.

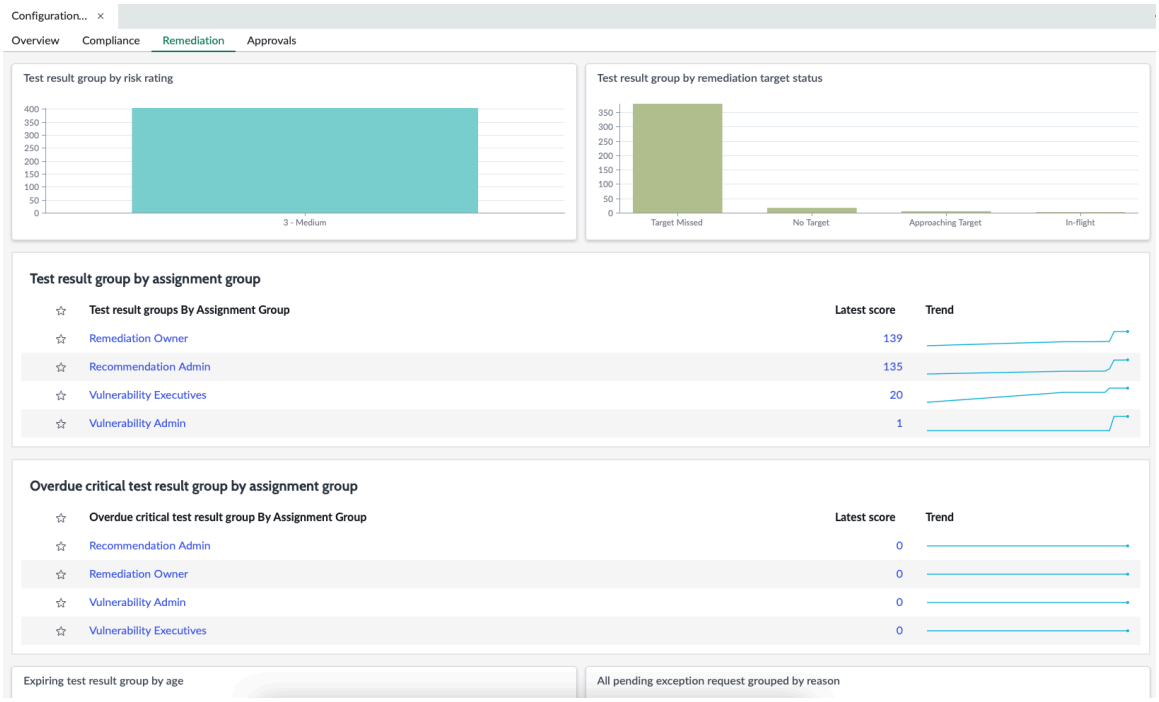
Registerkarte „Compliance“ im Dashboard „Konfigurations-Compliance“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Remediation“

Die **Korrektur** Auf der Registerkarte werden Informationen zum Fortschritt der Korrektur angezeigt. Sie können diese Registerkarte verwenden, um die Hygiene für Fehlkonfigurationskorrekturen anzuzeigen.

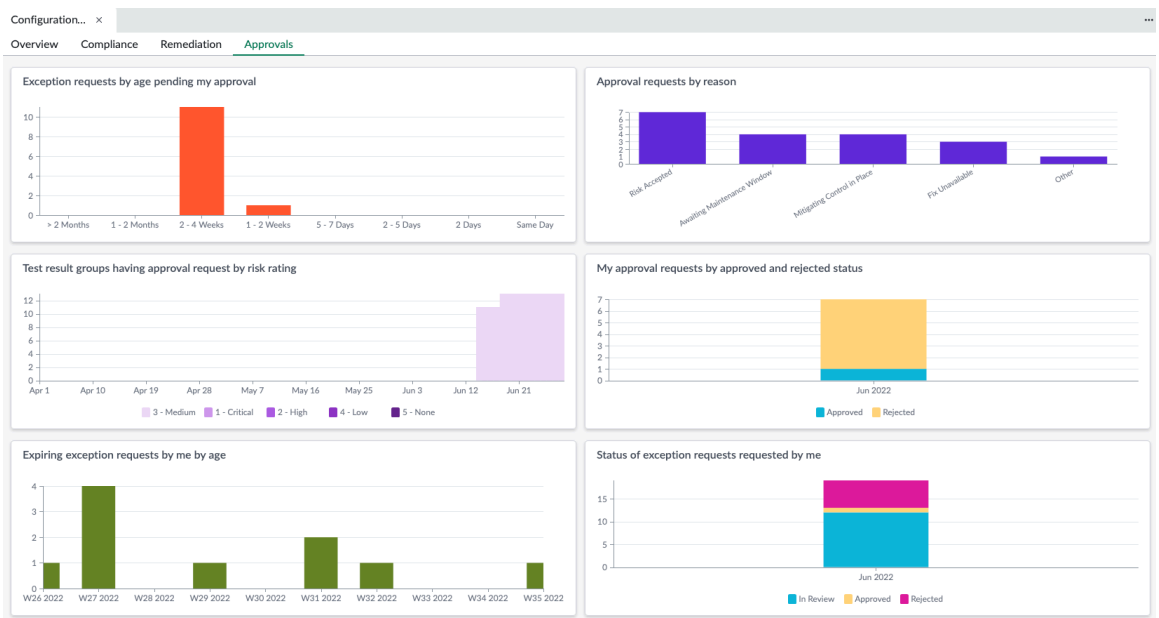
Das folgende Beispiel zeigt **Korrektur** Registerkarte.



Registerkarte Genehmigungen

Die Berichte in der **Genehmigungen** Auf der Registerkarte werden Informationen zu den Ausnahmeanforderungen und ihrem Genehmigungsstatus angezeigt.

Das folgende Beispiel zeigt **Genehmigungen** Registerkarte.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgliederungen

Die von den Indikatoren verwendeten Aufgliederungen lauten wie folgt:

- Grund für Zurückstellung
- Alter
- Zuweisungsgruppe
- Korrekturstatus
- Ergebnis
- Risikobewertung
- Asset-Kategorie
- Host-Tag
- Konfigurationstest
- Cloud-Service-Provider
- Cloud-Region
- Cloud-Account
- Cloud-Ressourcentyp

Hinweis:
Die Anpassung der Berechnung von Alter und Alter geschlossen für Testergebnisse kann zu einem starken Anstieg oder Rückgang der Performance Analytics (PA)-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung von Alter und Alter der geschlossenen Testergebnisse finden Sie unter KB1703270 KB-artikel.

Filter

In **Übersicht** Registerkarte können Sie die folgenden Filter auf die Widgets anwenden, um die gefilterten Daten zu visualisieren.

Name	Typ	Beschreibung
Asset-Kategorie	Auswahl	Art des Assets. Die vier Optionen sind: • Cloud • Behälter • Infra • OT
Cloud-Ressourcentyp	Auswahl	Typ der Ressource. Ein Beispiel ist eine virtuelle Maschine. Die Daten im Filter werden ausgefüllt, wenn Sie die Integration ausführen.

Automatische Übersetzung

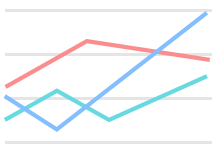
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
Cloud-Service-Provider	Auswahl	Service Provider für die Cloud. Die drei Optionen sind: • Amazon Web Services (AWS • Microsoft Azure • Google Cloud Platform (GCP)
Cloud-Account	Auswahl	Account-ID, die erstellt wird, wenn ein Account in einem Cloud-Service erstellt wird. Beispiel: AWS. Die Account-ID-Daten werden in den Filter eingegeben, wenn Sie die Integration ausführen.
Cloud-Region	Auswahl	Standort, an dem die Ressource gehostet wird.

Hinweis:
Sie können mehrere Optionen aus den Filtern auswählen und auswählen **Anwenden** . Jedes Widget zeigt die angewendeten Filter und die nicht angewendeten Filter an. Abhängig von den verfügbaren Daten wird der Bericht generiert. Das Widget zeigt auch die Anzahl des unterstützten Filters an.

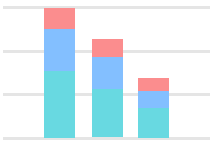
Datenvisualisierungen

Visualisierungen der Registerkarte „Übersicht“

Berichtname	Typ	Quelltabelle	Beschreibung
Compliance-Trend	Liniendiagramm 	Testergebnisse	Informationen zum Compliance-Trend: • Ressourcen: Gesamtzahl der Ressourcen, die im System verfügbar sind. • Fehlgeschlagen: Anzahl der Ressourcen mit mindestens einem fehlgeschlagenen Testergebnis. • Bestanden: Anzahl der Ressourcen mit allen Testergebnissen im Status „Bestanden“.
Fehlerbehungsaufgabe	Einzelne Punktzahl	Testergebnisse	Anzahl der Korrekturaufgaben, die

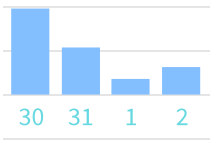
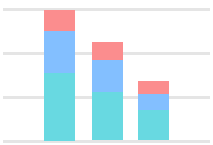
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen der Registerkarte „Übersicht“ (Fortsetzung)

Berichtname	Typ	Quelltabelle	Beschreibung
			im System vorhanden sind und sich in einem aktiven Status befinden.
Kritische Korrekturaufgaben kurz vor der Fälligkeit	Einzelne Punktzahl	Testergebnisse	Anzahl der Korrekturaufgaben, bei denen die Risikobewertung „Kritisch“ und der Korrekturstatus „Annäherung an Ziel“ lautet.
Testergebnisse nach Risikobewertung	Balkendiagramm 	Testergebnisse	Testergebnisse im Status „Fehlgeschlagen“, die gemäß der Risikobewertung gruppiert werden.
Testergebnisse nach Alter	Balkendiagramm	Testergebnisse	Testergebnisse im Status „Fehlgeschlagen“, die nach dem Zeitpunkt gruppiert werden, an dem die Testergebnisse erstellt wurden.

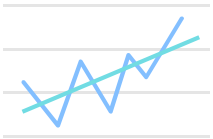
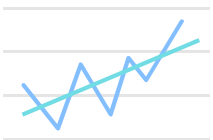
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen der Registerkarte „Übersicht“ (Fortsetzung)

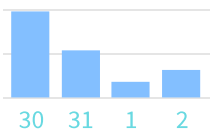
Berichtname	Typ	Quelltabelle	Beschreibung
			**Hinweis:** Die Anpassung der Berechnung von Alter und Alter geschlossen für Testergebnisse kann zu einem starken Anstieg oder Rückgang der Performance Analytics (PA)-Berichte (Performance Analytics) führen, die diese Metriken enthalten. Weitere Informationen zum Anpassen der Berechnung von Alter und Alter der geschlossenen Testergebnisse finden Sie unter KB1703270 KB-artikel.
Geschlossene Testergebnisse nach Einhaltung des Korrekturziels	Balkendiagramm 	Testergebnisse	Testergebnisse im Status „Bestanden“, was darauf hinweist, dass dieser Test geschlossen ist.
Überfällige kritische Testergebnisse nach Zuweisungsgruppe	Liste und Punktzahl	Testergebnisse	Anzahl der Testergebnisse, bei denen die Risikobewertung „Kritisch“ und der Korrekturstatus „Ziel verfehlt“ lautet. Der Bericht zeigt an, dass sich die Testergebnisse im Status „Offen“ befinden. Wenn die Testergebnisse das Korrekturzieldatum überschreiten, gelten sie als überfällig.
Überfällige Testergebnisse – Services	Liste, Punktzahl und Trend	PA-Dashboards-Datenbankansicht für Services	Anzahl der Testergebnisse für Services, bei denen der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen der Registerkarte „Übersicht“ (Fortsetzung)

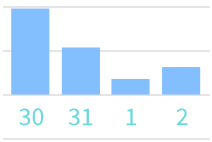
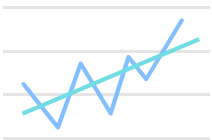
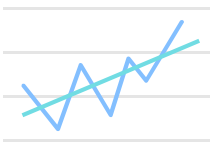
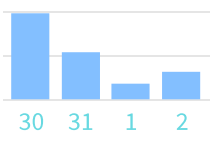
Berichtname	Typ	Quelltabelle	Beschreibung
			Korrekturstatus „Ziel verfehlt“ lautet. Dieser Bericht zeigt auch den Namen der Services oder Abteilungen mit den höchsten Testergebnissen an.
Überfällige Testergebnisse – Serviceverantwortliche	Liste, Punktzahl und Trend 	PA-Dashboards-Datenbankansicht für Services	Anzahl der Testergebnisse für Serviceverantwortliche, deren Korrekturstatus „Ziel verfehlt“ lautet. Dieser Bericht zeigt auch den Namen der Services oder Abteilungen mit den höchsten Testergebnissen an.

Visualisierungen der Registerkarte „Korrektur“

Titel	Typ	Quelltabelle	Beschreibung
Korrekturaufgabe nach Risikobewertung	Balkendiagramm 	Nachbesserungsaufgabe	Aufgliederung der Risikobewertungen aller Testergebnisgruppen, die sich im Status „aktiv“ befinden.
Korrekturaufgabe nach Status des Korrekturziels	Balkendiagramm	Nachbesserungsaufgabe	Aufgliederung der Korrekturziele aller Testergebnisgruppen, die das Ziel verfehlt haben, kein Ziel haben und sich dem Ziel nähern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

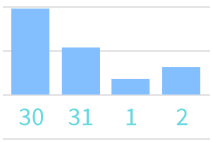
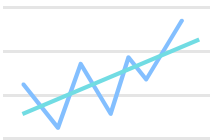
Visualisierungen der Registerkarte „Korrektur“ (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			
Korrekturaufgabe nach Zuweisungsgruppe	Liste, Punktzahl und Trend 	Nachbesserungsaufgabe	Aufgliederung der Korrekturaufgaben, die auf einer Zuweisungsgruppe basieren.
Überfällige kritische Korrekturaufgabe nach Zuweisungsgruppe	Liste, Punktzahl und Trend 	Nachbesserungsaufgabe	Aufgliederung der Korrekturaufgaben, die auf einer Zuweisungsgruppe basieren. Diese Korrekturaufgaben haben eine Risikobewertung als „Kritisch“, und ihr Korrekturziel wurde nicht erreicht.
Auslaufende Korrekturaufgaben nach Alter	Balkendiagramm 	Fehlerbehungsaufgabe	Korrekturaufgaben, die innerhalb einer bestimmten Dauer ablaufen. Es können maximal 10 Dauer-Buckets erstellt werden.
Alle ausstehenden Ausnahmeanforderungen gruppiert nach Grund	Balkendiagramm	Genehmigung der Statusänderung	Genehmigungsanforderungen für Statusänderung, die

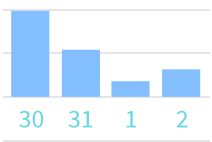
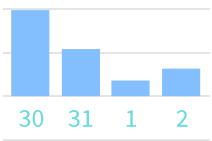
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen der Registerkarte „Korrektur“ (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			nach dem Grund für die Ausnahme gruppiert sind.
Kritische Ausnahmen bei Testergebnissen nach Zuweisungsgruppe	Liste, Punktzahl und Trend 	Testergebnisse	Testergebnisse, die sich in einem zurückgestellten und kritischen Status befinden und basierend auf der Zuweisungsgruppe gruppiert sind.

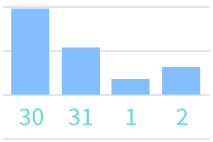
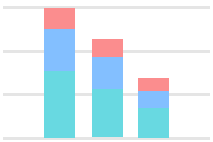
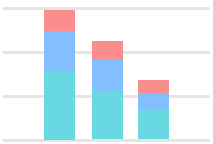
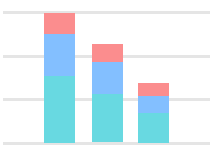
Visualisierungen der Registerkarte „Genehmigungen“

Berichte	Typ	Quelltabelle	Beschreibung
Ausnahmeanforderungen nach Alter, für die meine Genehmigung aussteht	Balkendiagramm 	Freigabe	Ausnahmeanforderungen, die von Ihnen erstellt wurden und deren Genehmigung aussteht. Die Anforderungen werden nach der Dauer der Anforderung gruppiert.
Genehmigungsanforderungen nach Grund	Balkendiagramm 	Genehmigung der Statusänderung	Geben Sie Genehmigungsanforderungen für Statusänderungen zum Erstellen einer Ausnahme an, und geben Sie den Grund für die Ausnahme an.
Korrekturaufgaben mit Genehmigungsanforderung nach Risikobewertung	Balkendiagramm	Nachbesserungsaufgabe	Korrekturaufgaben mit einer Genehmigungsanforderung, die auf der Relevanz basiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen der Registerkarte „Genehmigungen“ (Fortsetzung)

Berichte	Typ	Quelltabelle	Beschreibung
			
Meine Genehmigungsanforderungen nach Status „Genehmigt“ und „Abgelehnt“	Balkendiagramm 	Genehmigung der Statusänderung	Ausnahmeanforderungen, die nach den Status „genehmigt“ und „abgelehnt“ gruppiert sind.
Ablaufende Ausnahmeanforderungen von mir nach Alter	Balkendiagramm 	Genehmigung der Statusänderung	Ausnahmeanforderungen, die in den nächsten Wochen ablaufen. Die Ausnahmeanforderungen werden basierend auf Wochen gruppiert. Immer wenn eine Ausnahmeanforderung erstellt wird, wird ein Datum für die Gültigkeit der Ausnahmeanforderung ausgewählt. Die Berechnung des Alters der Anforderung basiert auf diesem Datum.
Status der von mir angeforderten Ausnahmeanforderungen	Balkendiagramm 	Genehmigung der Statusänderung	Ausnahmeanforderungen, die von Ihnen erstellt wurden und die gemäß den folgenden Status gruppiert sind: • Wird überprüft • Genehmigt • Abgelehnt

Framework für zusammengefasste Berichte für Konfigurations-Compliance

Mit dem Framework für zusammengefasste Berichte können Sie Berichte für die Daten erstellen, die komplexe und lang laufende On-the-fly-Abfragen umfassen, um die Leistung zu verbessern.

Das Framework für zusammengefasste Berichte verbessert die Leistung durch:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwendung weniger Ressourcen und schnelleres Rendern von Berichten,
- Aggregieren der Daten und Wiederverwendung von Zusammenfassungen und Aufgliederungen (Gruppieren nach) und
- Die Abfragen in der Datenbank werden reduziert

Wenn Sie mehr als eine Million Konfigurationstestergebnisse haben, verwenden Sie das Framework für zusammengefasste Berichte neben den Standardberichten.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- ServiceNow AI Platform Administrator (admin): Installiert und aktiviert Platform Analytics-Lösung und nimmt alle erforderlichen Änderungen an Systemeigenschaften vor.
- Performance Analytics Administrator (PA_admin): Überprüfen Sie die Zusammenfassungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.
- Administrator (sn_vul_cmn.admin): Zusammenfassungen erstellen.
- VR write(sn_vul_cmn.write): Bearbeiten Sie die Daten in den Zusammenfassungen und aggregierten Ergebnissen.
- VR-Lesen (sn_vul_cmn.read): Überprüfen Sie die Daten in den Zusammenfassungen und aggregierten Ergebnissen.
- Schwachstellenanalyst (sn_vul.Vulnerability_Analyst): Überprüfen Sie die zusammengefassten Ergebnisse.

Zugehörige Informationen

Konfigurieren Sie eine Zusammenfassung für Quelldaten

Führen Sie mehrere Zusammenfassungen gleichzeitig aus

Konfigurieren Sie die Anzahl der Zusammenfassungen, die gleichzeitig ausgeführt werden können

Erstellen Sie einen Bericht mithilfe einer Zusammenfassung

Konfigurations-Compliance Referenzinformationen

Bei der Aktivierung von werden verschiedene Arten von Komponenten installiert Konfigurations-Compliance Anwendung, einschließlich Tabellen, geplanten Aufgaben und Anwenderrollen.

Die folgenden Themen enthalten Referenzinformationen, Problembehandlung sowie Felddaten in den Formularen und Datensätzen in Konfigurations-Compliance.

- Mit Konfigurations-Compliance installierte Komponenten
- Testergebnis-Formularfelder
- Wird Aufgelöst Konfigurations-Compliance Importprobleme
- Ändern Sie das Startdatum der Qualys-PC-Ergebnisse

Mit Konfigurations-Compliance installierte Komponenten

Bei der Aktivierung des Konfigurations-Compliance-Plugins werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Anwenderrollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab v15.1.5 von Konfigurations-Compliance, Die am häufigsten verwendeten Systemeigenschaften sind jetzt innerhalb von zugänglich Konfigurations-Compliance Anwendung. Um diese Systemeigenschaften anzuzeigen, navigieren Sie zu **Alle**Konfigurations-Compliance**Eigenschaften**an.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Zeigen Sie gefilterte Listen für Komponenten an, die mit einer Anwendung installiert wurden

Filtern Sie die Tabelle „Anwendungsdateien“ so, dass nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert werden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, sollte installiert werden, damit ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Führen Sie die folgenden Schritte aus, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im Filternavigator ein **sys_metadata.list** Um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) aus, und wählen Sie, **Anwendung** > **ist** Gefolgt vom Namen Ihrer Anwendung. Beispiel: **Anwendung** > **ist** > **Vulnerability Response**an.
3. Wählen Sie im Bedingungsgenerator aus, um einen zweiten Filter hinzuzufügen **UND** , Und wählen Sie dann aus, **Klasse** > **ist ein** Und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle** , **Geplante Aufgabe** , Oder **Tabelle** .
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die von Ihnen ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
Konfigurations-Compliance-Administrator	Kann Anwendungseigenschaft, Konfiguration, Regeln	sn_vulc.write

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
[sn_vulc.admin]	aktualisieren und Integrationen von ändern Konfigurations-Compliance Anwendung. Ab v15.0 kann ein Administratoranwender Quelldatensätze wie Expliots, CVEs usw. nicht löschen	**Hinweis:** Erbt die Rollen, die für die Verwaltung der Datensätze der Configuration Compliance-Anwendung erforderlich sind.
gelesen [sn_vulc.read]	Lesen Sie Listen und Datensätze in Configuration Compliance. **Wichtig:** Ab v24.0 von Vulnerability Response, Die Rolle „sn_vulc.read“ hat die Berechtigung zum Zugriff auf Arbeitsbereich des Schwachstellenmanagers.	• sn_sec_cmn.calc_read • sn_vul.View_Manager_Workspace
Schreiben [sn_vulc.write]	Schreiben Sie Listen und Datensätze in Configuration Compliance.	• sn_vulc.read • sn_vulc.Remediation_owner
Schreibzuweisung [sn_vulc.write_assignment	Schreiben Sie in Zuweisungsfelder für Testergebnisse.	Enthalten in der Rolle sn_vulc.Remediation_owner.
Korrekturbesitzer sn_vulc.Remediation_owner	Zeigen Sie die Berechtigung für Testergebnisse an, die Ihnen oder Ihrer Gruppe zugewiesen sind, und aktualisieren Sie sie.	Enthalten in der Rolle itil. Enthält: • sn_sec_cmn.read • sn_vulc.write_assignment • sn_vul.View_rem_Workspace
CC.System sn_vulc.Import_admin	Führt alle geplanten Aufgaben in der Konfigurations-Compliance-Anwendung aus. **Hinweis:** Dieser Anwender ist der standardmäßige „Run as“-Anwender für jede geplante Aufgabe in der Konfigurations-Compliance.	• sn_vulc.write • import_admin • sn_vul_Tenable.read_Integration

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
VRCommon.System sn_vul_cmn.admin	Standard-Run-as-Anwender für alle geplanten Aufgaben in der allgemeinen Vulnerability Response-Anwendung.	• sn_vul_cmn.write • sn_sec_cmn.admin • report_admin
SecCommon.System sn_sec_cmn.admin	Standard-Run-as-Anwender für alle geplanten Aufgaben, die für die Funktion „Hintergrundaufträge“ in der allgemeinen Anwendung „Sicherheitssupport“ verwendet werden	• sn_sec_cmn.int_write • sn_sec_cmn.write • workflow_admin • sn_sec_cmn.calc_write • sn_sec_Core.read_dictionary • sn_sec_cmn.Manage_Approval_rules • sn_sec_int.admin • sn_sec_cmn.cap_email_write • sn_sec_cmn.Manage_classification_rules • sn_sec_cmn.Manage_background_Job
V14.7: sn_vulc.Edit_watch_topic	Bearbeiten Sie Überwachungsthemen für Konfigurations-Compliance.	sn_vulc.read_watch_topic
V14.7: sn_vulc.read_watch_topic	Lesen Sie die Überwachungsthemen für Konfigurations-Compliance.	cmdb_read
V14.7: sn_vulc.create_watch_topic	Erstellen Sie Überwachungsthemen für Konfigurations-Compliance.	sn_vulc.read_watch_topic
sn_vulc.auditor	Lesen für alle Konfigurations-Compliance-Module zulassen	sn_vulc.read sn_vulc.Advanced_read
sn_vulc.Advanced_read	Lesen für alle Konfigurations-Compliance-Administrationsmodule zulassen	sn_vulc.read_Auto_close_rules sn_vulc.read_Exception_Configuration sn_vulc.read_assignment_rules sn_vulc.read_Task_rules sn_vulc.read_Auto_Exception_rule sn_vulc.read_Notifications sn_vulc.read_Risk_Score_Configuration sn_vulc.read_Test_Critizality_Mapping sn_sec_cmn.read_Approval_rules

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
		sn_vulc.read_Auto_delete sn_vulc.read_Remediation_target_rules
sn_vulc.read_Test_Critizality_Mapping	Lesezugriff für Test-Relevanzzuordnung zulassen	
sn_vulc.read_Task_rules	Lesen für Regeln für Korrekturaufgaben zulassen	
sn_vulc.read_assignment_rules	Lesen für Zuweisungsregeln zulassen	
sn_vulc.read_Risk_Score_Configuration	Lesen für Konfiguration der Risikopunktzahl zulassen	
sn_vulc.read_Auto_close_rules	Lesen für Konfiguration des automatischen Schließens zulassen	
sn_vulc.false_positive_Approver	Ermöglicht das Genehmigen/ Ablehnen des Abschlusses von Korrekturaufgaben als falsch positiv	sn_vul.View_Manager_Workspace
sn_vulc.Exception_Approver	Hat Ausnahmeanforderungen genehmigt oder lehnt sie ab.	sn_vul.View_Manager_Workspace
sn_vulc.delete	Löscht Quelldatensätze.	

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
V15.0: Aktualisieren Sie die Testgruppe bei Konfigurationstests	Aktualisiert die Testgruppe bei Tests für Tenable und Microsoft Defender-Quelle. Dies ist ein einmaliger Auftrag.
V15.0: Füllen Sie vorhandene Testergebnisfelder aus	Aktualisiert Werte in neu hinzugefügten Spalten (z. B. Alter, geschlossenes Alter, aktiv usw.) in der Testergebnistabelle, gespeicherten Filtern und Modulen. Dies ist ein einmaliger Auftrag.
V15.0: Tabelle „angreifbare CIs“ ausfüllen – Löschen und für Testergebnisse neu ausfüllen	Füllt die Gesamtzahl der Datensätze in der Tabelle „angreifbare CIs“ aus. Dies ist ein einmaliger Auftrag.
Version 12,0 Berechnen Sie Korrekturmetriken für alle Testergebnisgruppen	Berechnet und aktualisiert Werte für Statusmetriken in Korrekturaufgaben-Datensätzen.
Version 12.0: Berechnen Sie Korrekturmetriken für alle Testergebnisse	Berechnet und aktualisiert Werte für Statusmetriken in Testergebnisdatensätzen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
Version 12.0: Statussynchronisierung Der Change-Anforderung	On-Demand-Auftrag, der die status aller vorhandenen Korrekturaufgaben (RTS) mit Change-Anforderungen (CHGs) synchronisiert. Während eine Change-Anforderung ihren Lebenszyklus durchläuft, verschiebt sie auch die status aller zugehörigen Korrekturaufgaben automatisch. Aktiviert die Statussynchronisierung in Zukunft.
Version 11.1: Überprüfen Sie Die Zurückstellung Der Testergebnisgruppen Ablauf	Sendet Benachrichtigungen, wenn Korrekturaufgaben abgelaufen sind (und wenn sie in einer Woche ablaufen).
Konfigurations-Compliance-CI-Anzahl	Füllt die Anzahl der eindeutigen Konfigurationselemente (CI) und den gleitenden Durchschnitt von 90 Tagen in der Tabelle „Anzahl der Konfigurationselemente“ [sn_vulc_cc_Configuration_item_count] aus.
Version 11.1: Korrekturziele bewerten und benachrichtigen	Legt Korrekturzieldaten für alle Testergebnisse fest oder aktualisiert sie. Bestimmt den Status von Korrekturzieldaten anhand von Regeln. Sendet Benachrichtigungen
V14.7: Fügen Sie Testergebnisgruppen in die einheitliche Korrekturaufgabe ein	Einmalige geplante Aufgabe zum Einfügen aller in der klassischen Anwenderoberfläche erstellten Korrekturaufgaben in die einheitliche Korrekturaufgabe (sn_vul_Remediation_Task).
Version 12.0: Füllen Sie CR-TRG m2m für CR und CR-übergeordnetes Element aus	Füllt Change-Anforderungen für Korrekturaufgaben aus.
Entfernt in v11.1: Zurückgestellte Testergebnisgruppen erneut öffnen **Hinweis:** Für Versionen vor 11.1 veraltet. Nicht verwenden.	Öffnet zurückgestellte Gruppen erneut, wenn das Fälligkeitsdatum abgelaufen ist.
Wenden Sie alle Zuweisungsregeln erneut an	Wendet alle Zuweisungsregeln erneut an.
Version 14.3: Anzahl der Neuzuweisungen für Zuweisungsregeln	Wird täglich ausgeführt und veröffentlicht die Gesamtzahl der Testergebnisse und Korrekturaufgaben, die von dieser Funktion für eine bestimmte Zuweisungsregel nicht zugewiesen werden.
Bewerten Sie den Status der Testergebnisgruppen neu	Bewertet den Status von Korrekturaufgaben für Einträge, bei denen eine Neubewertung erfolgt **Bewerten_Status** Ist „falsch“. Wird alle 15 Minuten ausgeführt.
Rollup der Testergebnis-Risikopunktzahl zur Testergebnisgruppe und -Konfiguration Testen	Wird stündlich ausgeführt und berechnet die Rollup-Punktzahlen für die geänderten Konfigurationstests und Korrekturaufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
	• Berechnet die Rollup-Risikopunktzahl für alle Tests in sn_vulc_Test_manifest und löscht den Manifestdatensatz nach Abschluss. • Berechnet die Rollup-Risikopunktzahl für alle Tests in sn_vulc_result_Group_manifest und löscht das Manifest nach Abschluss.
Version 12.0: Aktualisieren Sie Richtlinienkorrekturmetriken	Ab v15.0 von Konfigurations-Compliance, Diese geplante Aufgabe wurde in Korrekturmetriken aktualisieren umbenannt. • Berechnet und aktualisiert Werte für Statusmetriken in Richtliniendatensätzen. • Berechnet die Compliance von Testergebnissen in % eines CI für das erkannte Element.
Version 14.3: Anzahl der Zurückstellungen festlegen	Erfasst, wie oft ein Testergebnis oder eine Korrekturaufgabe zurückgestellt wird.
Aktualisieren Sie die Risikobewertung für Testergebnisse	Aktualisiert die Risikobewertung für Testergebnisse.
Aktualisieren Sie die Rollup-Risikopunktzahl für alle nicht geschlossenen Ergebnisgruppen und Konfigurationstests.	Aktualisiert die Rollup-Risikopunktzahl für alle nicht geschlossenen Ergebnisgruppen und Konfigurations-Compliance Tests.

Installierte Tabellen

Tabelle	Beschreibung
Zuweisungsregel [sn_vulc_Assignment_rule]	Enthält den Satz von Regeln, die ausgewertet wurden, um die Zuweisungsgruppe für Testergebnisse festzulegen.
Autoritative Quelle [sn_vulc_auth_src]	Importierte autorisierende Quellen speichern.
Rechner [sn_vulc_Calculator_Risk_Score]	Enthält den Rechner, der bestimmte Testergebnisfelder festlegt, wenn bestimmte Bedingungen erfüllt sind.
CC-Konfigurationselement: Anzahl [sn_vulc_cc_Configuration_item_count]	Enthält die Gesamtzahl der Konfigurationselemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Version 12.0: Zuordnung von Change-Anforderungen [sn_vulc_action_Associate_cr]	Bereitstellungstabelle, die zum Zuordnen von Change-Anforderungen zu Korrekturaufgaben verwendet wird.
Version 12.0: Erstellung einer Change-Anforderung [sn_vulc_action_create_cr]	Bereitstellungstabelle, die zum Erstellen von Change-Anforderungsformularen verwendet wird.
Version 12.0: Formular „Change-Anforderung“ [sn_vulc_cr_Form]	Basistabelle für das Change Request-Management.
Bezugsvermerk [sn_vulc_Zitat]	Enthält importierte Bezugsvermerke
Konfigurationstest [sn_vulc_Test]	Enthält importierte Konfigurationstestdaten.
Konfigurationstest-Manifest [sn_vulc_Test_Manifest]	Enthält die Konfigurationstests, für die die Rollup-Risikopunktzahl berechnet werden muss.
Version 12,2 fehlende Asset-Tabelle [sn_vul_missing_Asset]	Enthält temporäre Asset-Datensätze für importierte Konfigurations-Compliance-Bewertungsdaten mit nicht abgeglichenen Assets.
Konfigurationstest Technologie [sn_vulc_Test_Technology]	Enthält importierte Konfigurationstesttechnologien.
Regel für Korrekturaufgaben [sn_vulc_grouping_rule]	Enthält die Regeln, die die Kriterien definieren, mit denen Gruppen für eine Reihe von Testergebnissen automatisch erstellt werden.
Testgruppen [sn_vulc_Policy]	Enthält importierte Richtlinien.
Richtlinienkonfigurationstest [sn_vulc_Policy_Test]	Enthält importierte Testdaten für Richtlinienkonfiguration.
Korrekturzielregel [sn_vulc_ttr_rule]	Definiert den erwarteten Zeitrahmen für die Korrektur eines Testergebnisses.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Risikorechner [sn_vulc_Calculator_Group]	Enthält die Gruppierung von Konfigurations-Compliance Rechner. Die Reihenfolge der Rechnergruppe bestimmt, welche Gruppe zuerst ausgewertet wird, und in jeder Gruppe wird höchstens ein Rechner verwendet.
Rollup-Rechner für Risikopunktzahl [sn_vulc_Risk_Score_Rollup]	Enthält Rollup-Rechnerkonfigurationen.
Korrekturaufgaben aufteilen [sn_vulc_action_Split_trg]	Bereitstellungstabelle, die zum Aufteilen von Korrekturaufgaben verwendet wird.
Genehmigung der Zustandsänderung [sn_vulc_State_Change_Approval]	Enthält Prozessdaten zum Genehmigungsstatus.
Technologie [sn_vulc_Technology]	Enthält importierte Technologien.
Relevanz-Zuordnung testen [sn_vulc_Test_Critizality_Map]	Enthält Relevanzzuordnungsdaten.
Testergebnis [sn_vulc_result]	Enthält importierte Testergebnisse.
Korrekturaufgaben [sn_vulc_result_Group]	Enthält importierte Korrekturaufgaben.
Version 12.0: Change-Anforderungen für Korrekturaufgaben	Enthält Change-Anforderungen für Korrekturaufgaben.
Manifest der Korrekturaufgabe [sn_vulc_result_Group_manifest]	Enthält die Korrekturaufgaben, für die die Rollup-Risikopunktzahl berechnet werden muss.
Korrekturaufgaben [sn_vulc_m2m_result_result_Group]	Enthält Daten zur Korrekturaufgabe.
Testergebnisverlauf [sn_vulc_result_history]	Enthält den Verlauf der importierten Testergebnisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Testergebnis Korrekturstatus	Status des Testergebnisses für die am nächsten angewendete Korrekturzielregel.
V14.7: Testanzahlen des Überwachungsthemas [sn_vulc_wt_Test_count]	Cache-Tabelle für die Registerkarte eindeutige Konfigurationstests im Vulnerability Manager-Arbeitsbereich.

Anzeigen Konfigurations-Compliance Testgruppen

Sobald Sie die Ergebnisse eines Drittpartei-Scans in Ihre Instanz importiert haben, können Sie Ihre Test-Compliance auf Testgruppenebene anzeigen. Verwenden Sie diese Ansicht vor einem Audit dieser Testgruppe und aller zugehörigen Testdatensätze.

Vorbereitungen

Erforderliche Rolle: sn_vulc.read und sn_vulc.Remediation_owner zum Anzeigen

Warum und wann dieser Vorgang ausgeführt wird

Testgruppen sind importierte Datensätze, die Sie nicht in bearbeiten können Konfigurations-Compliance Anwendung.

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Testgruppen**an.
   Die Liste der Testergebnisse wird angezeigt. Ab v15.0 von Konfigurations-Compliance, **% Compliance Der Testergebnisse** Die Spalte zeigt den Prozentsatz der Testergebnisse an, die den Tests in einer Testgruppe entsprechen.

   % Compliance der Testergebnisse = (Anzahl der in einer Testgruppe geschlossenen Testergebnisse/ Gesamtzahl der geschlossenen Testergebnisse Von Testergebnissen, die einer Testgruppe zugeordnet sind) * 100

2. Klicken Sie auf **Kurzbeschreibung** Der Testgruppe, die Sie anzeigen möchten.

Konfigurations-Compliance Testgruppen-Formularfelder

Feld	Beschreibung
Quelle	Systemname des Drittanbieterscanners oder der in eingegebene Name ServiceNow Plugin für die API, mit der kommuniziert wird Konfigurations-Compliance.
Technologien	Liste der Technologien, die der Testgruppe in der Scanner-Anwendung der Drittpartei zugeordnet sind.
Quell-ID	Bezeichner, der dieser Testgruppe vom Drittparteiscanner zugewiesen ist.
Quelle erstellt	Datum und Uhrzeit, zu der die Testgruppe in der Scanner-Anwendung der Drittpartei definiert wurde.
Quelle aktualisiert	Datum und Uhrzeit der letzten Änderung der Testgruppe in der Scanner-Anwendung der dritten Richtlinie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Kurzbeschreibung	Zusammenfassungsbeschreibung oder Titel, die der Testgruppe in der Scanner-Anwendung der Drittpartei zugewiesen ist.
Beschreibung	Detaillierte Beschreibung der Testgruppe, wie in der Scanner-Anwendung der Drittpartei definiert.
Tests	Liste der Tests, die auf diese Testgruppe verweisen. Aus dem Scanner der Drittpartei importiert. Sie können bei Bedarf in der Liste zu detaillierten Informationen zu einem bestimmten Test navigieren.
Korrekturstatus (Version 12.0)	
Zurückgestellte sind ausgeschlossen	Diese Werte enthalten keine CIs aus zurückgestellten Testergebnissen. ○ **Verbleibende CIs** : Die Anzahl (Anzahl) der Konfigurationselemente (CIs) mit aktiven Testergebnissen (beliebiger Status außer **Geschlossen**) Für diese Richtlinie. ○ **% Der korrigierten CIs** : Prozentsatz der konformen CIs für diese Testgruppe. Diese Zahl schließt CIs mit zurückgestellten Testergebnissen aus. ○ **CIs insgesamt** : Die Gesamtzahl der CIs, die von dieser Testgruppe betroffen sind. Diese Anzahl schließt zurückgestellte Testergebnisse aus.
Beinhaltet Zurückgestellte	Die Werte stellen CIs aus allen aktiven Testergebnissen dar (beliebiger Status außer **Geschlossen**). ○ **Verbleibende CIs** : Die Anzahl der eindeutigen CIs, die einem oder mehreren nicht geschlossenen Testergebnissen zugeordnet sind, auf die diese Testgruppe angewendet wurde. ○ **% Der korrigierten CIs** : Der Prozentsatz der konformen CIs für diese Testgruppe. ○ **CIs insgesamt** : Gesamtzahl der CIs, die von dieser Testgruppe betroffen sind.

Um diese Werte ab Version 12.0 bei Bedarf zu aktualisieren, klicken Sie unter der Registerkarte „Korrekturstatus“ auf **Status Aktualisieren** Zugehöriger Link. Eine Nachricht wird angezeigt, die angibt, dass die Daten aktualisiert werden. Klicken Sie auf **Status anzeigen** Link zum Anzeigen des Fortschritts der Aktualisierung. Nach einigen Minuten werden alle Daten, die sich seit der letzten geplanten Aufgabe geändert oder aktualisiert haben, im Datensatz aktualisiert. Aktualisierte Feldwerte werden aktualisiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Deaktivieren Sie den Import von Testergebnissen für eine Testgruppe, indem Sie auswählen **Import deaktivieren** Schaltfläche.

   (Optional) Der Wert in **Ist Import deaktiviert** Spalte ändert sich in *Wahr* . Die Testergebnisse für die Testgruppe werden nicht aus der bevorstehenden Erfassung importiert.

   Hinweis:
   Die **Import deaktivieren** Die Schaltfläche ist für die Testergebnisse verfügbar, die von abgerufen wurden Qualys Nur Scanner.

   Ab v23.0 von Vulnerability Response:

   - Sie können den Import von Testergebnissen für aktivieren oder deaktivieren Qualys Testgruppe in Arbeitsbereich des Schwachstellenmanagers. Weitere Informationen finden Sie unter Aktivieren oder deaktivieren Sie den Import von Testergebnissen für einen Qualys Testgruppe.
   - Die **Als veraltet markieren** Schaltfläche wurde umbenannt in **Import deaktivieren** .
   - Die **Ist veraltet** Spalte wird umbenannt in **Ist Import deaktiviert** .

Anzeigen Konfigurations-Compliance Autorisierende Quellen

Verwenden Sie dieses Modul, um Zusammenfassungsinformationen zu jeder autorisierenden Quelle anzuzeigen und die Quellveröffentlichungen zu recherchieren, die zum Erstellen des Datensatzes verwendet wurden.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zum Aktualisieren
- sn_vulc.Remediation_owner zum Anzeigen

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Unterstützungsdaten** > **Autoritative Quellen**an.
2. Klicken Sie auf **Kurzbeschreibung** Der autoritativen Quelle, die Sie anzeigen möchten.

Konfigurations-Compliance Formularfelder für autorisierende Quellen

Feld	Beschreibung
Anzahl	ID-Nummer, die der autoritativen Quelle von Ihrer Instanz während des Importprozesses zugewiesen wurde.
Quelle	Systemname der Scanner-Anwendung der Drittpartei oder der im Scanner-Plugin eingegebene Name für die API, die mit kommuniziert Konfigurations-Compliance.
Quell-ID	Bezeichner, der der autorisierenden Quelle vom Drittparteiscanner zugewiesen ist.
Kurzbeschreibung	Name, der dieser autorisierenden Quelle im Scanner der Drittpartei zugewiesen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Herausgeber	Name der Organisation oder Veröffentlichung, die die ursprüngliche Informationsquelle für diese autorisierende Quelle war.
Bezugsvermerke	Liste der zitierten Informationen zu den Testergebnissen. Aus dem Scanner der Drittpartei importiert. Sie können diese Liste bei Bedarf zu detaillierten Informationen zu einem bestimmten Test navigieren.

3. **Wahlweise:** Fügen Sie ein hinzu **Herausgeber** .
4. Klicken Sie auf **Aktualisieren**.
5. Sie können diesen Datensatz löschen, indem Sie auf klicken **Löschen** .
   Entfernt den Datensatz aus Ihrer Instanz. Wenn sie noch in Ihrer Drittpartei-Integration verwendet wird, wird sie beim nächsten Import zurückgegeben

Anzeigen Konfigurations-Compliance Technologien

Verwenden Sie dieses Modul, um Zusammenfassungsinformationen zu den einzelnen autoritativen Quellen und Zitaten anzuzeigen (in Qualys auch als Framework bekannt). Sie können die Quellveröffentlichungen recherchieren, die zum Erstellen des Datensatzes verwendet wurden.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zum Aktualisieren
- sn_vulc.Remediation_owner zum Anzeigen

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Unterstützungsdaten** > **Technologien**an.
2. Klicken Sie auf **Kurzbeschreibung** Der autoritativen Quelle, die Sie anzeigen möchten.

Konfigurations-Compliance Formularfelder für autorisierende Quellen

Feld	Beschreibung
Anzahl	ID-Nummer, die der autoritativen Quelle von Ihrer Instanz während des Importprozesses zugewiesen wurde.
Quelle	Systemname des Drittpartei-Scanners oder der Name, der im Plugin des Drittpartei-Scanners für die API eingegeben wurde, die mit kommuniziert Konfigurations-Compliance.
Quell-ID	Bezeichner, der der autorisierenden Quelle vom Drittparteiscanner zugewiesen ist.

3. Sie können diesen Datensatz löschen, indem Sie auf klicken **Löschen** .
   Entfernt den Datensatz aus Ihrer Instanz. Wenn sie noch in Ihrer Drittpartei-Integration verwendet wird, wird sie beim nächsten Import zurückgegeben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzeigen Konfigurations-Compliance Tests

Verwenden Sie dieses Modul, um detaillierte Informationen zu diesen Tests zu recherchieren. Enthalten sind die Expertenquellenvermerke, die bei der Erstellung verwendet wurden, die Konfigurationsrichtlinien von Drittparteien, in denen sie verwendet werden, und die Ergebnisse des Scans.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zum Aktualisieren
- sn_vulc.Remediation_owner zum Anzeigen

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Steuerungen**an.
2. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Tests**
3. Öffnen Sie in der Liste die Steuerung (Compliance-Test), die Sie anzeigen möchten.

Um diese Werte ab Version 12.0 bei Bedarf zu aktualisieren, klicken Sie unter der Registerkarte „Korrekturstatus“ auf **Status Aktualisieren** Zugehöriger Link. Eine Nachricht wird angezeigt, die angibt, dass die Daten aktualisiert werden. Klicken Sie auf **Status anzeigen** Link zum Anzeigen des Fortschritts der Aktualisierung. Nach einigen Minuten werden alle Daten, die sich seit der letzten geplanten Aufgabe geändert oder aktualisiert haben, im Datensatz aktualisiert. Feldwerte wie **Risikopunktzahl** , **Risikobewertung** , **Korrekturzieldatum** , **Status** , Und die Felder auf der **Korrekturstatus** Registerkarte wird aktualisiert.

Konfigurations-Compliance Testformularfelder

Feld	Beschreibung
Anzahl	Nummer, die dem Steuerelement während des Importvorgangs zugewiesen ist.
Ergebnis	Status des Scans. Bestanden oder fehlgeschlagen. Wenn dieser Test zu mehreren Korrekturaufgaben gehört, wird sein Status nach einem bestimmt Rangfolge .
Quelle	Systemname der Drittanbieter-Integrationsanwendung oder der im Plugin eingegebene Name für die API, die für die Kommunikation mit verwendet wird Konfigurations-Compliance.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Relevanz	Schweregrad des Konfigurationsproblems oder der Probleme, die der Steuerung zugeordnet sind, wie in der Drittpartei-Integration definiert. Der Grad der Relevanz wird an die Granularität ähnlicher Schwachstellenindikatoren angepasst, die in verfügbar sind Vulnerability Response. Die möglichen Ebenen sind: **Kritisch** Das Konfigurationsproblem, das der Steuerung zugeordnet ist, verursacht eine Unterbrechung eines oder mehrerer geschäftskritischer CIs. **Hoch** Das Konfigurationsproblem, das der Steuerung zugeordnet ist, ist eine Bedrohung, verursacht jedoch nicht das Herunterfahren kritischer Netzwerkressourcen. **Mittel** Das Konfigurationsproblem, das der Steuerung zugeordnet ist, ist ein Risiko, aber keine unmittelbare Bedrohung. **Niedrig** Das Konfigurationsproblem, das der Steuerung zugeordnet ist, ist eine Bedrohung auf niedriger Ebene und kann zugunsten von CIs ignoriert werden, die einem höheren Risiko ausgesetzt sind. **Kleiner** Das Konfigurationsproblem, das der Steuerung zugeordnet ist, ist ein geringfügiges Risiko und kann bei Bedarf ignoriert werden.
Quell-ID	Bezeichner, der der Steuerung von der Drittparteiintegration zugewiesen ist.
Kategorie	Hauptklassifizierungskategorie, die dieser Art von Kontrolle durch den Drittparteilieferanten zugewiesen wird.
Risikopunktzahl	Dies ist eine Rollup-Risikopunktzahl. Diese Risikopunktzahl wird gewichtet, wobei 85 % der Punktzahl aus der maximalen Risikopunktzahl für alle nicht „geschlossenen“ Testergebnisse (offen, wird untersucht, wartet auf Implementierung, zurückgestellt, gelöst) verwendet werden. und 15 % der Punktzahl aus der Anzahl der Testergebnisse, die nicht „geschlossen“ sind.Wert, der von Risikopunktzahlrechnern berechnet wird, der auf

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	den Business Relevanz- und Testrelevanzwerten der Testergebnisse basiert.
Unterkategorie	Unterkategorie, die dieser Testklasse vom Drittparteilieferanten zugewiesen ist.
Risikobewertung	Basierend auf einer Reihe von Risikopunktzahlen auf einer numerischen Skala von 1-5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen als 1 – Kritisch bis 5 – keine bewertet. Dieses Feld ersetzt das Feld Priorität in vorherigen Versionen.
Technologien	Liste der von diesem Test abgedeckten Technologien.
Quelle erstellt	Datum, an dem der Test zuerst in der Drittpartei-Integration definiert wurde.
Quelle aktualisiert	Datum, an dem der Test zuletzt in der Drittpartei-Integration aktualisiert wurde.
Kurzbeschreibung	Zusammenfassungsbeschreibung oder Titel, die oder der dem Test in der Drittpartei-Integration eingegeben oder zugewiesen wurde.
Korrekturstatus (V 12.0)	
Zurückgestellte sind ausgeschlossen	Diese Werte enthalten keine zurückgestellten Testergebnisse. ○ **Öffnen Sie Testergebnisse** : Die Anzahl (Anzahl) der aktiven (beliebiger Status außer **Geschlossen**) Testergebnisse für diesen Konfigurationstest. ○ **% Der korrigierten Testergebnisse** : Der Prozentsatz der korrigierten Testergebnisse für diese Korrekturaufgabe. ○ **Gesamtzahl der Testergebnisse** : Die Gesamtzahl der Testergebnisse für diese Korrekturaufgabe.
Beinhaltet Zurückgestellte	Diese Werte enthalten zurückgestellte Testergebnisse. ○ **Öffnen Sie Testergebnisse** : Die Anzahl (Anzahl) aller aktiven (beliebiger Status außer **Geschlossen**) Testergebnisse für diese Korrekturaufgabe. ○ **% Der korrigierten Testergebnisse** : Der Prozentsatz der korrigierten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Testergebnisse für diese Korrekturaufgabe. ○ **Gesamtzahl der Testergebnisse** : Die Gesamtzahl der Testergebnisse für diese Korrekturaufgabe.
Beschreibung	Lange Beschreibung des Tests. Für die Qualys Vulnerability Integration ist dieses Feld standardmäßig auf den Inhalt von festgelegt Qualys Cloud Platform Titelseite.
Korrektur	Schritte Anweisungen, die beschreiben, wie die Nichteinhaltung behoben werden kann.
Zugehörige Registerkarten	
Bezugsvermerke	Liste der Zitate, die für jede autorisierende Quelle eingegeben wurden, die dem Test zugeordnet ist.
Testgruppen	Liste von Konfigurations-Compliance Testgruppen, die diesen Test verwenden.
Testergebnisse	Liste der CIs, die von dem Konfigurationsproblem oder den mit diesem Test verbundenen Problemen betroffen sind. Sie können auf einzelne Tests zugreifen, ServiceNow Konfigurationselemente oder ggf. die Liste der betroffenen Technologien.
GRC-Richtlinienanweisungen	Wenn GRC Richtlinien- und Compliance-Management Plugin ist installiert. Diese Registerkarte enthält die zugehörigen GRC Richtlinie. Sie können diese Liste bearbeiten, um Richtlinienanweisungen hinzuzufügen oder zu entfernen.

Anzeigen Konfigurations-Compliance Testergebnisse

Anzeigen Konfigurations-Compliance Testergebnisse für Audits und Korrekturen. Die Testergebnisse werden während der Integrationsimporte von Schwachstellen von Drittparteien automatisch erstellt.

Wichtig:
Sie können die Testergebnisse anzeigen, die während der Integrationsimporte von Drittanbietern für Schwachstellen im Vulnerability Manager-Arbeitsbereich erstellt wurden. Weitere Informationen finden Sie unter Listenseite in Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.zum Anzeigen lesen
- sn_vulc.Remediation_owner zum Anzeigen und Aktualisieren
- sn_vulc.delete zu löschen

Warum und wann dieser Vorgang ausgeführt wird

Konfigurations-Compliance Erstellt oder aktualisiert die Testergebnisse nicht, importiert sie jedoch als Teil einer Drittpartei-Integration. Sobald sie in angezeigt werden können Konfigurations-Compliance, Werden sie mit korrigiert **Testergebnisgruppen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Testergebnisse**an.
   Ab v15.0 von Konfigurations-Compliance, Die folgenden Spalten werden in der Liste Testergebnisse angezeigt.

Testergebnisliste

Spalte	Beschreibung
Aktiv	Gibt an, ob ein Testergebnis aktiv ist. Ein Testergebnis wird markiert: ○ Wahr: Wenn der Status nicht „Geschlossen“ ist. ○ Falsch: Wenn der Status „Geschlossen“ ist.
Alter	Zeitraum, für den ein Testergebnis seit dem letzten Öffnen aktiv ist. Dieses Feld ist für ein geschlossenes Testergebnis leer. Format: Tage HH:MM: SS Weitere Informationen zum Anpassen der Altersberechnung finden Sie unter KB1703270 artikel.
Alter der Schließung	Zeitraum, für den ein Testergebnis aktiv war, bevor es in „Geschlossen“ übergegangen ist. Wenn das Testergebnis in „Geschlossen“ übergeht, wird der Wert aus der Spalte „Alter“ im Feld „Geschlossen“ angezeigt. Dieses Feld ist für ein aktives Testergebnis leer. Format: Tage HH:MM: SS Weitere Informationen zum Anpassen der Berechnung des Alters geschlossen finden Sie unter KB1703270 artikel.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Geschlossen	Zeitstempel, zu dem ein Testergebnis geschlossen wird. FORMAT: JJJJ-MM-TT HH:MM: SS
Zuletzt geöffnet	Zeitstempel, zu dem ein Testergebnis geöffnet wird, d. h. wenn **Aktiv** Feldwert ändert sich in *Wahr* .

2. Öffnen Sie die Steuerung, die Sie anzeigen möchten.

Konfigurations-Compliance Testergebnis-Formularfelder

Feld	Beschreibung
Anzahl	Die Nummer, die dem Test während des Importvorgangs zugewiesen ist.
Quelle	Der Systemname der SCA-Anwendung der Drittpartei oder der im Anwendungs-Plugin eingegebene Name für die API, die für die Kommunikation mit verwendet wird Konfigurations-Compliance.
Quell-ID	Der Bezeichner, der der Steuerung von der SCA-Anwendung zugewiesen ist.
Ergebnis	Bestanden, Fehlgeschlagen, Fehler oder Unbekannt. Aus Qualys importiert.
Risikopunktzahl	Rechnerergebnis für diesen Test. Vor v15.0 von Konfigurations-Compliance, Die Risikopunktzahl eines bestandenen Testergebnisses wird auf „0“ festgelegt. Ab v15.0 von Konfigurations-Compliance, Die Risikopunktzahl des bestandenen Testergebnisses wird nicht in „0“ geändert, sodass Sie das geminderte Risiko schätzen können. Die Risikopunktzahl des bestandenen Testergebnisses wird nicht in die Berechnung der Risikopunktzahl einer Korrekturaufgabe einbezogen.
Risikobewertung	Basierend auf einer Reihe von Risikopunktzahlen auf einer numerischen Skala von 1-5, die das Gesamtrisiko basierend auf einem Bereich von Risikopunktzahlen als 1 – Kritisch bis 5 – keine bewertet. Dieses Feld ersetzt das Feld Priorität in vorherigen Versionen.
Status	Berechnet aus den Korrekturaufgaben, zu denen das Testergebnis gehört. Wenn das Testergebnis zu mehreren Gruppen gehört, wird ein Rangfolge Wird angewendet, um den Status zu bestimmen.
Lösung	Berechnet aus den Korrekturaufgaben, zu denen das Testergebnis gehört. Wenn das Testergebnis zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	mehreren Gruppen gehört, wird ein Rangfolge Wird angewendet, um die Lösung zu bestimmen.
Zuerst gesehen	Datum des ersten Imports in Konfigurations-Compliance. Ab v13.1.1, die **Zuerst gesehen** Feld zeigt das vom Scanner bereitgestellte Datum an. Andernfalls wird das Datum des ersten Imports in angezeigt Konfigurations-Compliance.
Zuletzt gesehen	Datum des letzten Imports in Konfigurations-Compliance. Ab v13.1.1, die **Zuletzt gesehen** Feld zeigt das vom Scanner bereitgestellte Datum an. Andernfalls wird das Datum des letzten Imports in angezeigt Konfigurations-Compliance.
Letzte Übergabe	Spätestes Datum, an dem das Testergebnis bestanden wurde.
Test	Name des Tests.
Konfigurationselement	Name des an den Test angehängten CI.
Technologie	Softwareversion, die auf dem CI ausgeführt wird.
Beschreibung	Beschreibung des Tests
Erwartete Werte	Erwartete Werte, die in Qualys konfiguriert und von importiert wurden Konfigurations-Compliance. Dieser Wert ist ein boolescher Ausdruck, der bei Auswertung als „wahr“ das Testergebnis ergibt **Bestanden** . Der Ausdruck kann eine Kombination aus logischen, Set- oder regulären Ausdrucksoperatoren sein.
Ist-Werte	Vom Test zurückgegebene Werte. Diese Werte werden in den booleschen Ausdruck „erwartete Werte“ eingefügt, um zu bestimmen, ob das Ergebnis erfolgreich sein oder fehlschlagen soll. Sie werden aus Qualys importiert. Ab Version 14,9 von Konfigurations-Compliance, Die Werte Erweiterter Nachweis und Fehlerursache werden der Spalte ist-Werte hinzugefügt.
Korrektur	Korrekturanweisungen.
Zugehörige Registerkarten	
Korrekturaufgaben	Korrekturaufgaben, die diesem Testergebnis zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Testergebnisverlauf	Zugehörige Liste von Testergebnissen, die den Verlauf der Ergebnisse von Bestanden/ Fehlgeschlagen für dasselbe CI/dieselbe Technologie/denselben Test anzeigen.

Zeigen Sie eine Korrekturaufgabe an

Sie können eine Korrekturaufgabe anzeigen oder alternativ erstellen und die Korrektur durchführen.

Wichtig:
Sie können die Korrekturaufgaben im Vulnerability Manager-Arbeitsbereich anzeigen. Weitere Informationen finden Sie unter Listenseite in Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle:

- sn_vulc.admin zum Aktualisieren oder Erstellen
- sn_vulc.Remediation_owner zum Anzeigen

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Konfigurations-Compliance** > **Korrekturaufgaben**an.
2. Klicken Sie in der Liste auf den Datensatz, den Sie anzeigen möchten.
3. Alternativ können Sie auf klicken **Neu** Um eine neue Korrekturaufgabe zu erstellen und die Felder auszufüllen.

Formularfelder für Konfigurations-Compliance-Korrekturaufgabe

Feld	Beschreibung
Anzahl	Die automatisch generierte Zahl für diesen Datensatz.
Status	Fortschrittsstatus der Korrekturaufgabe. ○ Öffnen ○ Wird untersucht ○ Warten auf Implementierung ○ Zurückgestellt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Gelöst ○ Geschlossen
Risikopunktzahl	Diese Punktzahl ist der Rollup-Wert der Risikopunktzahlen für alle aktiven Testergebnisse in einer Korrekturaufgabe. Diese Punktzahl ändert sich, wenn Testergebnisse in der Korrekturaufgabe korrigiert werden.
Zuweisungsgruppe	Gruppe, die zur Bearbeitung dieser Korrekturaufgabe ausgewählt wurde.
Risikobewertung	Das Ausmaß des Risikos, das ein fehlgeschlagenes Testergebnis für Ihr System darstellt. Sie basiert auf einer Reihe von Risikopunktzahlen auf einer numerischen Skala von 1-5, die Risiken als kritisch (1) bis keine (5) bewertet.
Zugewiesen an	Einzelperson aus der ausgewählten Zuweisungsgruppe, die an diesem Satz von Aufgaben arbeitet.
Korrekturziel	Datum, bis zu dem die Testergebnisse korrigiert werden sollen, seit der ersten Identifizierung.
Erstellt	Datum und Uhrzeit der Erstellung dieser Korrekturaufgabe.
Korrekturstatus	Status der Korrektur für die Gruppe. Sie wird durch das Testergebnis mit dem nächsten Fälligkeitsdatum bestimmt. Für offene gruppenstatus sind „in Bearbeitung“, „Annäherung an Ziel“ und „Ziel verfehlt“. Für geschlossene Gruppen umfassen die status kein Ziel, Ziel erfüllt und Ziel verfehlt. Wenn für berechnete Korrekturzieldaten die Korrekturaufgabe geschlossen ist, wird der Gesamtkorrekturstatus aller geschlossenen Testergebnisse in der Korrekturaufgabe angezeigt. Diese bestimmen, ob die Gruppe ihr Datum erreicht hat oder nicht. Der Korrekturstatus einer geschlossenen Korrekturaufgabe ist **Kein Ziel** Wenn keines der geschlossenen Ergebnisse ein Korrekturzieldatum hatte. Ist es **Ziel Verfehlt** Wenn eines der geschlossenen Ergebnisse das Zieldatum verfehlt hat. Ist es **Ziel Erfüllt** Wenn mindestens ein geschlossenes Ergebnis sein Ziel erreicht hat und keiner der anderen es verfehlt hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktualisiert	Datum und Uhrzeit der letzten Änderung dieses Datensatzes.
Kurzbeschreibung	Kurze Beschreibung dieser Korrekturaufgabe.
Beschreibung	Lange Beschreibung der Korrekturaufgabe, die die Liste der Software enthält, die dieser Korrekturaufgabe zugeordnet ist.
Test	Der Konfigurationstest, der dieser Korrekturaufgabe zugeordnet ist.
Korrekturstatus (Version 12.0)	
Zurückgestellte sind ausgeschlossen	Diese Werte enthalten keine zurückgestellten Testergebnisse. ○ **Öffnen Sie Testergebnisse** : Die Anzahl (Anzahl) der aktiven (beliebiger Status außer **Geschlossen**) Testergebnisse für diese Korrekturaufgabe. ○ **% Der korrigierten Testergebnisse** : Der Prozentsatz der korrigierten (geschlossenen) Testergebnisse für diese Korrekturaufgabe. ○ **Gesamtzahl der Testergebnisse** : Die Gesamtzahl der Testergebnisse für diese Korrekturaufgabe.
Beinhaltet Zurückgestellte	Die Werte stellen alle aktiven Testergebnisse dar (alle Status außer **Geschlossen**). ○ **Öffnen Sie Testergebnisse** : Die Anzahl (Anzahl) der aktiven (beliebiger Status außer **Geschlossen**) Testergebnisse für diese Korrekturaufgabe. ○ **% Der korrigierten Testergebnisse** : Der Prozentsatz der korrigierten (geschlossenen) Testergebnisse für diese Korrekturaufgabe. ○ **Gesamtzahl der Testergebnisse** : Die Gesamtzahl der Testergebnisse für diese Korrekturaufgabe.
Gruppenkonfiguration	Der Typ der Filterung, die zum Auswählen der Testergebnisse für die Korrekturaufgabe verwendet wird.
Gruppierungsmethode	Name der verwendeten Methode.
Gruppenregel	Name der verwendeten Gruppenregel.
Notizen	Systemnotizen, die dem Datensatz zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zugehörige Links	**Version 12.0: Statuslink aktualisieren** . Aktualisieren Sie die Werte im Testergebnisdatensatz bei Bedarf. Zeigen Sie alle Daten an, die seit der letzten geplanten Aufgabe geändert oder aktualisiert wurden.
Testergebnisse	Die Testergebnisse dieser Korrekturaufgabe.
Change-Anforderungen (V 12.0)	Die Liste der Change-Anforderungen, die dieser Korrekturaufgabe zugeordnet sind.
Genehmigungen der Statusänderung (V 12.0)	Status und status der Change-Anforderungsgenehmigungen, die dieser Korrekturaufgabe zugeordnet sind.

Statusübergänge von Testergebnissen und Korrekturaufgaben in Konfigurations-Compliance Anwendung

Die status von Konfigurationstestdatensätzen und den zugehörigen Korrekturaufgaben (RTS) sind betroffen, wenn Testergebnisdatensätze zurückgestellt, gelöst, erneut geöffnet und an andere Korrekturmaßnahmen (RES) übertragen werden.

Statusübergangsszenarien zwischen Testergebnissen und Korrekturaufgaben

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Die folgende Tabelle zeigt, wie status und substatus zwischen Konfigurationstestergebnissen und Korrekturaufgaben übergehen.

Wenn der Status einer Korrekturaufgabe von übergeht...	...An Bundesländer/ unterstatus	Die zugeordneten testergebnisstatus übergehen von...	...An Bundesländer/ unterstatus	Beschreibung
Öffnen	Wird untersucht	Öffnen	Wird untersucht	Statusübergang bidirektional.
Öffnen	Wird überprüft	Öffnen	Wird überprüft	Statusübergang bidirektional.
Öffnen	Zurückgestellt/mit einem beliebigen Grund für die Lösung ausgewählt	Öffnen	Zurückgestellt	Testergebnisse behalten denselben Grund für die Lösung wie die Korrekturaufgabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Status einer Korrekturaufgabe von übergeht...	...An Bundesländer/ unterstatus	Die zugeordneten testergebnisstatus übergehen von...	...An Bundesländer/ unterstatus	Beschreibung
Zurückgestellt/mit beliebigem Grund für die Lösung	Öffnen	Testergebnisse bleiben zurückgestellt		Testergebnisse behalten die gleiche Lösung wie die Korrekturaufgabe bei.
Öffnen	Gelöst/Behoben	Öffnen	Gelöst	Status-/substatus-Übergang bidirektional.
Öffnen	„Gelöst“ und „gelöst“ zu „Geschlossen/ behoben“	Öffnen	Gelöst	Wenn eine Korrekturaufgabe in „Geschlossen/ behoben“ übergeht, kann sie wieder in „Offen“ übergehen. Wenn die Aufgabe in „Offen“ übergeht, werden die zugehörigen Testergebnisse von „gelöst“ zurück zu „Offen“ übergehen.
Öffnen	Gelöst	Offen	Gelöst	Status-/substatus-Übergang bidirektional.
Öffnen	Gelöst/Abgebrochen	Öffnen	Gelöst	Status-/substatus-Übergang bidirektional.
Öffnen	Gelöst und gelöst zu Geschlossen	Öffnen	Gelöst	Wenn eine Korrekturaufgabe automatisch in „Geschlossen“ übergeht, können die zugehörigen Testergebnisse wieder in „Offen“ übergehen.
Öffnen	Gelöst und gelöst zu „Geschlossen“/ Ergebnis ungültig	Öffnen	Gelöst und gelöst zu „Geschlossen“/ Ergebnis ungültig	Wenn eine Korrekturaufgabe in „gelöst“ übergeht, kann sie wieder in „Offen“ übergehen. Wenn eine Korrekturaufgabe in „Geschlossen“/

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn der Status einer Korrekturaufgabe von übergeht...	...An Bundesländer/ unterstatus	Die zugeordneten testergebnisstatus übergehen von...	...An Bundesländer/ unterstatus	Beschreibung
				„Ergebnis ungültig“ übergeht, können sie und die zugehörigen Testergebnisse nicht erneut geöffnet werden.
Öffnen	Geschlossen/ Behoben	Testergebnisse bleiben offen		

Hinweis:

- Ab v14.12 von Konfigurations-Compliance, **Ergebnis ungültig** Option wird in entfernt **Lösung** Feld im Dialogfeld „Schließen“.
- Ab v14.12 von Konfigurations-Compliance, **Statusgenehmigung Der Korrekturaufgabe** Der Workflow ist veraltet und wird im Flow Designer durch den Flow „Korrekturaufgabe – Statusgenehmigung“ ersetzt.

Statussynchronisierung zwischen Change-Anforderungen und Korrekturaufgaben

Es gibt eine synchronisierte Beziehung zwischen den Statusfeldern von Korrekturaufgaben und den Statusfeldern von Change-Anforderungen (CHGs) in Konfigurations-Compliance Anwendung.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Während eine Change-Anforderung ihren Lebenszyklus durchläuft, verschiebt sie auch den Status aller zugehörigen Korrekturaufgaben automatisch. Die Statussynchronisierung wird durch eine Systemeigenschaft aktiviert (sn_vulc.cr_State_Sync) Standardmäßig in Ihrer Instanz, wenn Sie herunterladen Konfigurations-Compliance Anwendung aus dem ServiceNow Store Ab v12.0.

Wenn die Statussynchronisierung aktiviert ist, ändert das Feld CHG-Status das Feld Status der Korrekturaufgabe in den folgenden Fällen automatisch:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

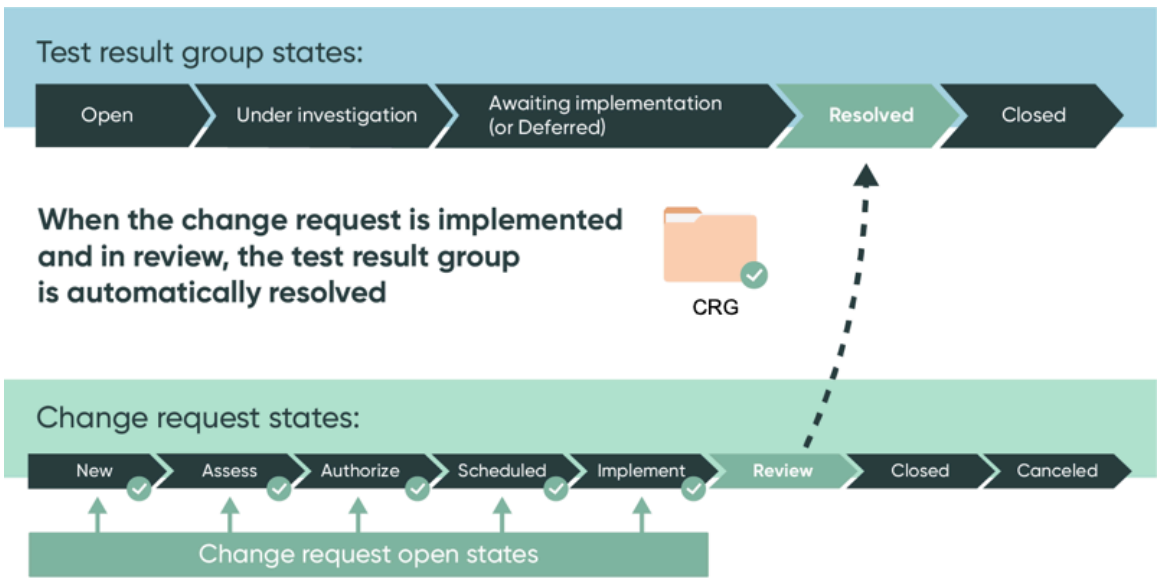
- Wenn eine neue Change-Anforderung für eine Korrekturaufgabe erstellt wird, wenn sie sich nicht in befindet **Warten Auf Implementierung** , Der Status der Korrekturaufgabe wird in verschoben **Warten Auf Implementierung** .
- Wenn eine vorhandene Change-Anforderung einer Korrekturaufgabe zugeordnet ist, wenn sie sich nicht in befindet **Warten Auf Implementierung** , Der Status der Korrekturaufgabe wird in verschoben **Warten Auf Implementierung** .
- Nachdem die Aufgaben für eine Change-Anforderung abgeschlossen sind (Implementiert), und das CHG wird in verschoben **Überprüfen** status, in den die Korrekturaufgabe verschoben wird **Gelöst** .

Weitere Informationen und Beispiele für die Statussynchronisierung finden Sie in den folgenden Abschnitten.

Hinweis:
Sie können Change-Anforderungen und Korrekturaufgaben weiterhin manuell durch die status ihrer Lebenszyklen in ihren jeweiligen Datensätzen verschieben, wenn jedoch die Statussynchronisierung aktiviert ist. Wenn das System registriert, dass sich der Status einer Change-Anforderung geändert hat, oder Sie eine Change-Anforderung hinzufügen oder sie aus einer Korrekturaufgabe entfernen, kann die Statussynchronisierung Ihre manuellen Eingriffe möglicherweise überschreiben. Change-anforderungsstatus verschieben die Korrekturaufgabe jedoch nicht automatisch aus dem **Geschlossen** .

Statussynchronisierung weiterleiten

Die folgende Abbildung zeigt, wie CHG-status die status der Korrekturaufgabe in einem Vorwärtslebenszyklus automatisch verschieben, also von **Öffnen** Bis **Gelöst** .



Sie können neue Change-Anforderungen für jede Korrekturaufgabe in einem anderen Status als erstellen **Gelöst** Oder **Geschlossen** . Bei der Statussynchronisierung wird der TRG automatisch bidirektional durch verschoben **Öffnen** , **Wird Untersucht** , **Warten Auf Implementierung** , Und **Gelöst** status. Diese Bewegung basiert auf bestimmten Werten des Statusfelds in der Change-Anforderung. Die Statussynchronisierung zwischen der Change-Anforderung und der Korrekturaufgabe wird automatisch aufgerufen, sofern das Kontrollkästchen nicht aktiviert ist (**Fügen Sie der CR CIs hinzu**) Wird in einem Formular angezeigt, und Sie deaktivieren das Kontrollkästchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Korrekturaufgabe wird nicht zu verschoben **Gelöst** Wenn sich ein CHG im status „Offen“ befindet. Alle CHG in status vor **Überprüfen** In seinem Lebenszyklus, z. B. **Neu** , **Bewerten** , **Autorisieren** , **Geplant** Oder **Implementieren** , Wie in der vorherigen Abbildung gezeigt, gelten als offene status für das CHG. Offene status verschieben das Statusfeld in der Korrekturaufgabe nicht, da Untersuchungen oder Aufgaben im CHG nicht abgeschlossen sind. Die Statussynchronisierung wird aufgerufen, wenn ein CHG für die Korrekturaufgabe erstellt oder zugeordnet wird oder wenn sich der Status einer vorhandenen Beziehung im CHG ändert. Die abgeschlossenen CHG-status sind **Überprüfen** Und erfolgreich **Geschlossen** . Wenn ein CHG erfolgreich geschlossen wird, lauten seine geschlossenen Codes: **Erfolgreich** , Oder **Erfolgreich mit Problemen** , In welchem Fall die Korrekturaufgabe zu verschoben wird **Gelöst** .

Statussynchronisierung rückwärts

Da ein CHG während seines Lebenszyklus verarbeitet wird, kann es irgendwann abgebrochen werden. In diesem Fall, wenn CHG lautet **Abgebrochen** , Oder **Geschlossen** (Mit dem Abschlusscode **Nicht Erfolgreich**), wird die Korrekturaufgabe automatisch zurück zu verschoben **Wird Untersucht** . Die Korrekturaufgabe wird zurück zu verschoben **Wird Untersucht** , Da kein aktiver Plan zur Behebung der Schwachstelle vorhanden ist.

Wenn sich eine Korrekturaufgabe in befindet **Gelöst** status, und Sie erstellen eine neue CHG oder ordnen sie einer vorhandenen CHG in einem der anfänglichen offenen status zu , die Korrekturaufgabe wird automatisch zurück zu **Warten Auf Implementierung** . Die Korrekturaufgabe wird in diesen Status zurückversetzt, da dem CHG jetzt weitere Arbeit zugewiesen ist.

Korrekturaufgaben mit mehr als einem CHG

Wenn eine Korrekturaufgabe in ist **Warten Auf Implementierung** Hat mehr als ein CHG zugeordnet. Die Statussynchronisierung basiert auf dem Status des CHG im frühesten Status seines Lebenszyklus. Angenommen, einer Korrekturaufgabe sind vier CHG zugeordnet, CHG1, CHG2, CHG3 und CHG4, wie in der folgenden Tabelle dargestellt.

CHG-Nummer	CHG-Status
1	**Implementieren**
2	**Abgebrochen**
3	Geschlossen (Abschlusscode von **Nicht Erfolgreich**)
4	Geschlossen (Abschlusscode **Nicht Erfolgreich**)

Die Statussynchronisierung zwischen CHG und Korrekturaufgabe basiert in diesem Fall auf CHG1, das sich im frühesten Status der vier CHG befindet, (**Implementieren**). In diesem Fall verbleibt die Korrekturaufgabe in **Warten Auf Implementierung** .

In einem anderen Beispiel, wenn sich eine Korrekturaufgabe in befindet **Gelöst** status und hat ein vorhandenes CHG, das implementiert wurde und sich in befindet **Überprüfen** status und ein neues CHG wird erstellt, aus dem die Korrekturaufgabe zurückverschoben wird **Gelöst** Bis **Warten Auf Implementierung** . Die Statussynchronisierung basiert auf dem CHG in der **Neu** status: Das CHG im frühesten Status.

CHG-Nummer	CHG-Status
1	Prüfung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CHG-Nummer	CHG-Status
2	Neu

Wenn Korrekturaufgaben mehr als ein CHG haben, wird der Status der Korrekturaufgabe in den folgenden Fällen automatisch übergegangen:

- Wenn ein CHG vorwärts zu verschoben wird **Überprüfen** , Wenn sich alle anderen CHGs, die der Korrekturaufgabe zugeordnet sind, in befinden **Überprüfen** Oder **Geschlossen** status (mit erfolgreichem Abschlusscode),in die die Korrekturaufgabe automatisch übergeht **Gelöst** . Alle anderen zugehörigen CHGs, die abgebrochen oder nicht erfolgreich geschlossen wurden, werden ignoriert.
- Wenn ein CHG zu verschoben wird **Abgebrochen** Oder **Geschlossen** (Abschlusscode von **Nicht Erfolgreich**), wenn sich alle anderen CHGs, die der Korrekturaufgabe zugeordnet sind, im gleichen Status befinden, wird die Korrekturaufgabe automatisch zurück zu **Wird Untersucht** .

Weitere Informationen zu den status der Korrekturaufgabe und zu den Aktionen in den einzelnen Status finden Sie unter Konfigurations-Compliance status.

Domain Separation und Konfigurations-Compliance

Die Domänentrennung wird in Konfigurations-Compliance unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Support-Stufe: Standard

- Enthält alle Aspekte von **Standard** Level-Support.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

So funktioniert Domain Separation in Konfigurations-Compliance

Mit der Domänentrennung können Sie standardisieren (Konfigurations-Compliance) Verfahren für den gesamten Kundenstamm, den Sie bedienen, mit niedrigeren Betriebskosten und einer höheren Servicequalität.

Separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. stellen sicher, dass Kundendaten getrennt werden und niemals anderen Clients zugänglich gemacht werden.

Unterstützung der Domänentrennung in Konfigurations-Compliance Nach Versionsveröffentlichungen

Release	Supportstufe	Notizen
Orlando	Standard	
Paris	Standard	
Quebec	Standard	
Rom	Standard	
San Diego	Standard	
Tokio	Standard	
Utah	Standard	
Vancouver	Standard	

Domänentrennung für Konfigurations-Compliance Die Anwendung deckt die folgenden Produktfunktionen ab:

- Erfasst die Testergebnisse von Drittanbieterscannern (Qualys) In der richtigen Domäne.

  Die Daten werden in derselben Domäne erfasst wie der Integrationsanwender, dessen Anmeldeinformationen für die Integration verwendet werden.
- Scannt bestimmte Hosts von erneut Konfigurations-Compliance In der Domäne, von der sie angefordert wurde.
- Verwendet den CMDB-CI-Suchprozess, um sicherzustellen, dass die CI-Informationen aus den Scannern mit den CIs in der CMDB der Domäne des Integrationsanwenders übereinstimmen.
- Berechnet Risikopunktzahlen auf Testergebnisebene gemäß dem Risikopunktzahlrechner, der in derselben Domäne wie der Integrationsanwender definiert ist.
- Regel(n) für Korrekturaufgaben kann/können definiert, zugewiesen und in derselben Domäne wie die Domäne des Integrationsanwenders verbleiben.
- Korrekturaufgaben, die mit den Regeln für Dokumentkorrekturaufgaben erstellt wurden, bleiben in derselben Domäne wie die Regeln für Korrekturaufgaben erstellt werden.
- Der Zurückstellungsworkflow durchläuft den Genehmigungsprozess in derselben Domäne, für die die Zurückstellung angefordert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Berichte und Dashboards zeigen die testergebnisstatus an, z. B. Alter der Testergebnisse, offene Testergebnisse nach CI, Testergebnisse nach Auswirkung in der Domäne, zu der sie gehören.
- Wissen von Drittanbieterscannern (Qualys) Können in der globalen Domäne erfasst werden, und Daten können für mehrere Clients freigegeben werden.

Hinweis:
In allen obigen Fällen gelten die übergreifenden Prinzipien der Sichtbarkeit in getrennten Domänen-Trennung in der NOW Platform.

Anwendungsfälle

Die Konfigurations-Compliance Die Anwendung verwaltet den Lebenszyklus eines Testergebnisses von Ende bis Ende Die folgenden Anwendungsfälle sind auf Domänentrennung ausgerichtet:

- **Erfassen** Testergebnisse von Qualys
  - Erfasst Daten aus mehreren Instanzen
  - Deduplizieren Sie die Testergebnisse
  - Mit CMDB-CI abgleichen
- **Ergänzung** Von Testergebnissen mit Risikopunktzahlen
  - Asset-Ergänzung (CMDB)
  - Risikopunktzahl
- **Gruppe** Testen Sie die Ergebnisse, und weisen Sie die Korrekturaufgabe zu
  - Gruppieren Sie die Testergebnisse automatisch
  - Weisen Sie die Korrekturaufgabe automatisch zu
- **Beheben**
  - Korrekturaufgabe, die als Korrekturaufgabe zugewiesen ist
  - Umfassender Korrekturlebenszyklus
  - Zurückstellungs-Workflow
- **Messen** Die Sicherheitslage der Organisation und das Compliance-Management-Programm
  - Ergebnistrend nach Compliance, Kategorie, Relevanz und Technologie
  - Status und Verteilung auf Richtlinien, Tests, Hosts, Testergebnisse und Risikopunktzahl

Setup

Domänentrennung für wird eingerichtet Konfigurations-Compliance Erfordert keine zusätzlichen Schritte. Alle Konfigurations-Compliance Tabellen beziehen die Domänenspalte, nachdem die Instanz domänengetrennt ist. Sie können die Importdaten der Testergebnisintegration an bestimmte Domänen weiterleiten. Weitere Informationen finden Sie unter Erstellen Sie domänengetrennte Importe für eine Integration. Weitere Informationen zu zusätzlichen Vorsichtsmaßnahmen und Einstellungen finden Sie unter Zusätzliche Einstellungen für Domänentrennung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänengetrennte Daten

Daten können domänengetrennt werden, was bedeutet:

- Testergebnisse, die von Drittanbieterscannern erfasst wurden, bleiben in derselben Domäne wie die Domäne des Integrationsanwenders und sind von keiner anderen Domäne aus zugänglich.
- Testergebnisse oder Hosts in einer Domäne können nicht von anderen Domänen aus angezeigt werden.
- Der Risikobewertungsalgorithmus und die Gruppenregeln für Testergebnisse können von niemandem außerhalb der Domäne angezeigt werden.
- In einer Domäne erstellte Zurückstellungs-Workflows sind in einer anderen Domäne nicht sichtbar.
- Alle E-Mail-Benachrichtigungen befinden sich in der Domäne, zu der sie gehören.

Wie Compliance-Analysten ihre eigenen Anwendungsdaten verwalten

- Analysten erstellen eigene Anwendungsinstallation, Verwaltung von Anwendungen mit mehreren Quellen und CI-Suchregeln.
- Analysten können bestimmte Integrationen ausschließlich für die Verwendung innerhalb der Domäne konfigurieren.
- Analysten können eigene Zurückstellungs- und Change-Management-Workflows erstellen.
- Analysten können eigene Regeln für Korrekturaufgaben und Risikobewertungslogik erstellen, um Ergebnisse genau zu priorisieren, Korrekturaufgaben automatisch zuzuweisen und der richtigen Zuweisungsgruppe zuzuweisen.
- Domänenanwender erstellen eine manuelle Korrekturaufgabe und schließen sie dann.

Geschäftslogik und Prozesse, die vom Instanzbesitzer domänengetrennt werden können

- Konfigurations-Compliance Anwender und Gruppen
- Konfigurations-Compliance Integrationen (ab Madrid-Release)
- Vollständige Setup-Konfiguration (Anwender- und Gruppenverwaltung, Anwendungsinstallation, Verwaltung von Anwendungen mit mehreren Quellen, CI-Suchregeln, Regeln für Korrekturaufgaben, Risikorechner usw.)
- Schließen Sie den Korrekturlebenszyklus ab, einschließlich Zurückstellung

Zugehörige Informationen

Domänentrennung für Service Provider

Konfigurations-Compliance Relevanzzuordnungen

Konfigurations-Compliance Die Relevanzzuordnung transformiert Relevanzfelder aus der Quelle in Felder in Konfigurations-Compliance.

Die Konfigurations-Compliance Das Basissystem wird mit einem Standard geliefert Qualys Cloud Platform Auf Standard ServiceNow Zuordnung. Das Erstellen oder Bearbeiten einer Relevanzzuordnung ist nur für anwenderdefinierte oder nicht standardmäßige Zuordnungen von Drittparteien in Ihrer Umgebung vorgesehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance status

Mit Konfigurations-Compliance, Sie können ein Statusmodell anzeigen, um zu einem bestimmten Zeitpunkt den Status der Korrekturaufgabe zu erfahren. Die status der Korrekturaufgabe steuern die testergebnisstatus nach Priorität.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

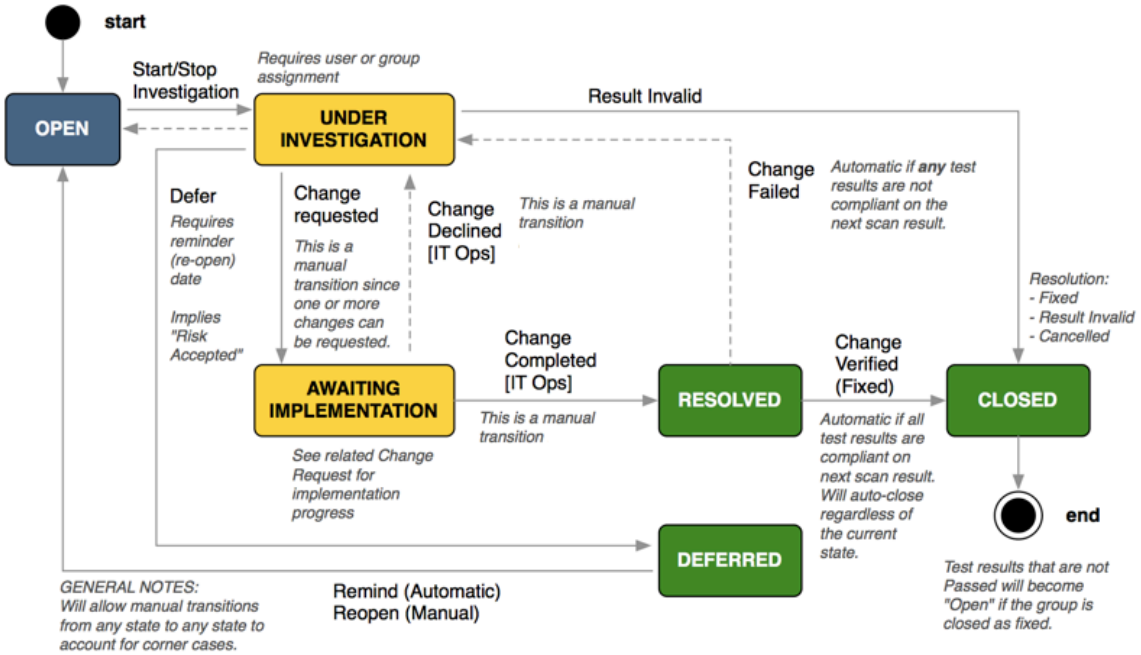
Status Der Korrekturaufgabe

Korrekturaufgaben (RTS) haben viele mögliche status. Der automatische Übergang ist ab dem Status gelöst basierend auf den nächsten Scan-Ergebnissen verfügbar. Wenn alle Testergebnisse beim nächsten Scan bestanden werden, wird die Korrekturaufgabe geschlossen. Andernfalls wechselt er in den Status „wird untersucht“. Das System überprüft diesen Status „Geschlossen“, wertet den Status der Korrekturaufgabe jedoch erneut aus, wenn ein Testergebnis zur Korrekturaufgabe hinzugefügt oder aus dieser gelöscht wird. Die Arbeitsnotizen werden aktualisiert, um den Übergang widerzuspiegeln.

Die folgende Abbildung zeigt, wie der Status einer Korrekturaufgabe vom Status Offen in den Status Geschlossen übergeht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status-Flow der Konfigurations-Compliance (Vor v15.0)



Hinweis:

- Jedes Formular für Korrekturaufgaben enthält **Folgen** Und **Aktualisieren** Schaltflächen, die Standard für sind ServiceNow Aufgaben.
- Ab v15.0 von Konfigurations-Compliance, Folgendes wurde entfernt:
  - **Schließen** Schaltfläche
  - Die **Lösung** Feld im modalen Dialogfeld „Lösen“.

In der folgenden Tabelle sind aufgeführt Konfigurations-Compliance status.

Konfigurations-Compliance-status

Status	Beschreibung
Öffnen	Status bei Erstellung.
Wird untersucht	Ausgelöst durch **Untersuchung Starten** Schaltfläche. In diesem Status können Sie: **Erstellen Sie eine Change-Anforderung** Weitere Informationen finden Sie unter Change-Anforderung in Konfigurations-Compliance erstellen. **Ausnahme anfordern** Geben Sie einen Grund an, und wählen Sie ein Datum für die erneute Öffnung aus. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe. **Als falsch positiv markieren** Geben Sie einen Grund und Hinweise an. Markiert die Korrekturaufgabe als falsch positiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance-status (Fortsetzung)

Status	Beschreibung
Wird überprüft	Wird ausgelöst, wenn die Korrekturaufgabe für die nächste Aktion bewertet wird. Wird normalerweise verwendet, um Untersuchungsergebnisse zu validieren oder vorgeschlagene Changes/Ausnahmen vor der Implementierung zu genehmigen. Von diesem Status aus können Sie basierend auf Ihrer Genehmigung oder Ablehnungen zu einem der folgenden wechseln: **Warten auf Implementierung** Übergang zu „Warten auf Implementierung“, falls genehmigt **Wird untersucht** Wechseln Sie zurück zu „wird untersucht“, wenn eine weitere Analyse erforderlich ist. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe.
Zurückgestellt	Ausgelöst durch **Zurückstellen** Schaltfläche. In diesem Status können Sie: **Erneut öffnen** Übergang zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Gruppe. Aufschubinformationen werden unter angezeigt **Zurückstellen/ Schließen** Zugehörige Registerkarte. Am Zurückstellungsdatum wird die Gruppe zur Korrektur erneut geöffnet.
Warten auf Implementierung	Ausgelöst durch **Warten Auf Implementierung** Schaltfläche. In diesem Status können Sie: **Security Incident** Weitere Informationen finden Sie unter Erstellen Sie einen Security Incident . **Erstellen Sie eine Change-Anforderung** Weitere Informationen finden Sie unter Change-Anforderung in Konfigurations-Compliance erstellen. **Lösen** In **Lösungshinweise** Fügen Sie den Grund hinzu, warum Sie die Korrekturaufgabe lösen. Der Status wird gelöst. Notizen werden unter angezeigt **Lösung** Zugehörige Registerkarte. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe.
Gelöst	Ausgelöst von **Lösen** Schaltfläche. In diesem Status können Sie: **Security Incident** Weitere Informationen finden Sie unter Erstellen Sie einen Security Incident . **Erneut öffnen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurations-Compliance-status (Fortsetzung)

Status	Beschreibung
	Übergang zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Korrekturaufgabe. Notizen werden unter angezeigt **Notizen** Zugehörige Registerkarte. Lösungsinformationen werden unter angezeigt **Lösung** Zugehörige Registerkarte. Die Notizen spiegeln sich in wider **Arbeitsnotizen** Aller Testergebnisse, die der Korrekturaufgabe zugeordnet sind.
Geschlossen	Ausgelöst von **Schließen** Schaltfläche oder **Als falsch positiv markieren** Schaltfläche. Ab v14.12 von Konfigurations-Compliance, Sie können eine Korrekturaufgabe schließen, indem Sie sie als falsch positiv markieren. In diesem Status können Sie: **Erneut öffnen** Übergang zurück in den Status „Offen“. **Löschen** Bestätigen Sie den Löschvorgang. Entfernt die Gruppe. Abschlussinformationen werden unter angezeigt **Zurückstellen/ Schließen** Zugehörige Registerkarte. Die Notizen spiegeln sich in wider **Arbeitsnotizen** Aller Testergebnisse, die der Korrekturaufgabe zugeordnet sind.

- Wenn die Korrekturaufgabe als „Geschlossen“ oder „behoben“ markiert ist und das hinzugefügte Testergebnis nicht selbst „Geschlossen“ oder „behoben“ ist, ändert sich der Testergebnisstatus nicht, und der Status der Korrekturaufgabe wird in „Offen“ geändert.
- Wenn Sie eine neue Korrekturaufgabe erstellen oder eine Korrekturaufgabe aufteilen, wird der **Grund** , Und **Bis** Felder werden für neue und alte Korrekturaufgaben neu ausgewertet. Wenn der Status aller Testergebnisse zurückgestellt ist, wird der Wert in angezeigt **Grund** Und **Bis** Felder werden für die Korrekturaufgabe zusammengefasst.
  - Wenn alle Testergebnisse in einer Korrekturaufgabe zurückgestellt werden und dieselben aufweisen **Grund** , Dann wird der Korrekturaufgabe dieselbe zugewiesen **Grund** . Andernfalls wird **Grund** Feld wird in geändert **Keine** .
  - Das Datum in **Bis** Das Feld wird mit dem nächsten bis-Datum aller Korrekturaufgaben aktualisiert, zu denen die Testergebnisse gehören.

Hinweis:
Diese Auswertung wird von durchgeführt `Rollup test result values to test result RT1nd configuration test`Geplante Aufgabe, die alle eine Stunde ausgeführt wird.

- Wenn **Zuletzt Gesehen** Ist größer als **Lösungsdatum** Für ein gelöstes Testergebnis wird das Testergebnis erneut geöffnet. Wenn in einer gelösten Korrekturaufgabe mindestens ein Testergebnis während der Erfassung erneut geöffnet wird, wird die Korrekturaufgabe in den Status wird untersucht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Testergebnisstatus

Der Status einer Korrekturaufgabe ändert auch den Status der zugehörigen Testergebnisse. Dieser Mechanismus hat zwei Fälle:

Testergebnisse, die nur zu einer Korrekturaufgabe gehören

Ergebnisse stimmen mit dem Status der Korrekturaufgabe überein Mit drei Ausnahmen:

- Wenn die Korrekturaufgabe ist Ändert seinen Status in „Geschlossen“ und seine Lösung (Substatus) in „behoben“. Das Element ignoriert diese Änderung und kehrt dann in den Status „Offen“ zurück.
- Wenn die Korrekturaufgabe ist Ändert seinen Status in „Geschlossen“ und seine Lösung (Substatus) in „Abgebrochen“. Das Element ignoriert diese Änderung und kehrt dann in den Status „Offen“ zurück.
- Wenn der Status der Testergebnisquelle behoben ist (durch einen Scan oder Import aktualisiert), dann wenn die Korrekturaufgabe Ändert seinen Status, das Testergebnis ändert seinen Status in Geschlossen (behoben), unabhängig davon, welcher Status die Korrekturaufgabe ist Ist in .

Testergebnisse, die zu mehreren Korrekturaufgaben gehören

Testergebnisse stimmen nicht automatisch mit dem Status der Korrekturaufgabe überein. Stattdessen sucht es unter allen zugeordneten Gruppen, um den Status mit der höchsten anzuwendenden Priorität zu finden. Dies ist der Status der Priorität:

Geschlossen > **Geschlossen (Substatus: Falsch positiv)** > **Zurückgestellt** > **Gelöst** > **Wird überprüft** > **Warten auf Implementierung** > **Wird untersucht** > **Öffnen** > **Geschlossen (Substatus: Abgebrochen)** > **Geschlossen (Substatus: Behoben)**

Hinweis:
Geschlossen (Substatus: Behoben) Und **Geschlossen (Substatus: Abgebrochen)** Sind zwei Sonderfälle.

Hinweis:
Ab v15.0 von Konfigurations-Compliance, **Ergebnis Ungültig** Substatus wurde veraltet.

Beispiele für Status der Korrekturaufgabe

Zum Beispiel:

Status Der Korrekturaufgaben	Testergebnisstatus
RT1: **Öffnen** > **Wird untersucht** RT2: **Öffnen**	**Wird untersucht** Wenn RT1 untersucht wird und RT2 Offen ist, ändert sich das Testergebnis in wird untersucht, da RT1 nach der Suche zwischen RT1 und RT2 den Status mit der höchsten Priorität hat.
RT1: **Wird Untersucht** RT2: **Öffnen** > **Wird untersucht**	**Wird untersucht** Wenn RT2 untersucht wird und RT1 untersucht wird, bleibt das Testergebnis als wird untersucht, da sie nach der Suche zwischen RT1 und RT2 den Status mit derselben Priorität haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status Der Korrekturaufgaben	Testergebnisstatus
RT1: **Wird Untersucht** RT2: **Wird untersucht** > **Warten auf Implementierung**	**Warten auf Implementierung** Wenn RT2 auf Implementierung wartet und RT1 untersucht wird, ändert sich das Testergebnis in Implementierung warten, da RT2 nach der Suche zwischen RT1 und RT2 den Status mit der höchsten Priorität hat.
RT1: **Wird untersucht** > **Zurückgestellt** RT2: **Warten auf Implementierung**	**Zurückgestellt** Wenn RT1 zurückgestellt ist und RT2 auf Implementierung wartet, ändert sich das Testergebnis in zurückgestellt, da Element 1 nach der Suche herausgefunden hat, dass RT1 zwischen RT1 und RT2 den Status mit der höchsten Priorität hat
RT1: **Zurückgestellt** RT2: **Warten auf Implementierung** > **Geschlossen (Ergebnis Ungültig)**	**Geschlossen (Ergebnis Ungültig)** > **Zurückgestellt** Wenn RT2 geschlossen ist und die Lösung (Substatus) Ergebnis ungültig ist und RT1 zurückgestellt ist, ändert sich das Testergebnis in Geschlossen (Ergebnis ungültig), da RT2 nach der Suche zwischen RT1 und RT2 den Status mit der höchsten Priorität hat.
RT1: **Zurückgestellt** RT2: **Geschlossen (Ergebnis Ungültig)** > **Öffnen (über erneut öffnen)**	**Zurückgestellt** Wenn RT2 erneut geöffnet wird und sich der Status in Offen ändert und RT1 zurückgestellt ist, ändert sich das Testergebnis in zurückgestellt, da RT1 nach der Suche zwischen RT1 und RT2 den Status mit der höchsten Priorität hat.
RT1: **Zurückgestellt** RT2: **Warten auf Implementierung** > **Geschlossen (Falsch Positiv)**	**Geschlossen (Falsch Positiv)** Wenn RT2 geschlossen ist und die Lösung (Substatus) falsch positiv ist und RT1 zurückgestellt ist, ändert sich das Testergebnis in Geschlossen (falsch positiv), da RT2 nach der Suche zwischen RT1 und RT2 den Status mit der höchsten Priorität hat.

Testergebnisstatus – Sonderfälle

Status Der Korrekturaufgabe	Testergebnisstatus
RT1: **Wird untersucht** RT2: **Warten auf Implementierung** > **Geschlossen (behoben oder Abgebrochen)**	**Wird untersucht** Wenn RT2 geschlossen ist (Substatus „behoben“ oder Substatus „Abgebrochen“) und RT1 untersucht wird, ändert sich das Testergebnis von „Warten auf

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Testergebnisstatus – Sonderfälle (Fortsetzung)

Status Der Korrekturaufgabe	Testergebnisstatus
	Implementierung“ (zuvor höchste Priorität) in „wird untersucht“ (derzeit höchste Priorität).
RT1: Beliebiger Status RT2: Beliebiger Status	Wenn der Status der Testergebnisquelle behoben ist (durch einen Scan oder Import aktualisiert), dann wenn die Korrekturaufgabe Ändert seinen Status, das Testergebnis ändert seinen Status in „Geschlossen (behoben)“, unabhängig davon, welcher status die anderen zugehörigen Korrekturaufgaben aufweist Befinden sich in. Die Testergebnissuche nach Korrekturaufgabe status tritt nicht auf.

Status-Rollup- und Rollup-Szenarien

Status-Rollup- und Rollup-Szenarien synchronisieren automatisch den Status von Korrekturaufgaben (RTS) und Konfigurationstestergebnis (CTR), wodurch Echtzeitaktualisierungen für beide sichergestellt werden. Diese dynamische Interaktion reduziert die manuelle Nachverfolgung, verbessert die Genauigkeit und bietet Anwendern eine aktuelle Ansicht des Fortschritts, wodurch die Konfigurations-Compliance effizienter wird und Anwender schnell fundierte Entscheidungen treffen können.

Rollup-Verhalten

Wenn sich der Status des Konfigurationstestergebnisses (Configuration Testergebnis, CTR) ändert, können sich diese Änderungen bis zur Ebene der Korrekturaufgabe (RT) ausbreiten.

Die folgende Tabelle fasst wichtige Rollup-Szenarien zusammen, in denen Änderungen des Status des Konfigurationstestergebnisses (Configuration Test result, CTR) den Status der zugehörigen Korrekturaufgabe (RT) beeinflussen können, basierend auf Abschlussbedingungen, Neuzuweisungen und Zurückstellungen.

Rollup-Szenarien

CTR-Status	RT-Status
Öffnen > Geschlossen – Behoben	Öffnen > Geschlossen – Behoben
Öffnen > Geschlossen-Veraltet	Öffnen > Geschlossen – Abgebrochen

Rolldown-Verhalten

Wenn sich der Status einer Korrekturaufgabe ändert, wird der Status häufig an die zugehörigen CTRs weitergegeben, es sei denn, dies wird durch manuelle Updates oder Ausnahmen überschrieben.

Die folgende Tabelle fasst wichtige Rollup-Szenarien zusammen, in denen Änderungen des Status der Korrekturaufgabe (RT) den Status des zugehörigen Konfigurationstestergebnisses (Configuration Test result, CTR) beeinflussen können, basierend auf Rangfolgeregeln und speziellen Bedingungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollup-Szenarien

RT-Status	CTR-Status
Öffnen Sie > Wird Untersucht	Öffnen Sie > Wird Untersucht
Öffnen Sie > In Überprüfung	Öffnen Sie > In Überprüfung
Öffnen Sie > Zurückgestellt	Öffnen Sie > Zurückgestellt
Zurückgestellt > Offen	Bleibt Zurückgestellt
Öffnen Sie > Gelöst – Behoben	Öffnen Sie > Gelöst – Behoben
Öffnen Sie > Gelöst-Behoben > Geschlossen-Behoben	Öffnen Sie > Gelöst-Behoben > Geschlossen-Behoben
Öffnen > Gelöstes Ergebnis Ungültig	Öffnen > Gelöstes Ergebnis Ungültig
Öffnen > Gelöst – Abgebrochen	Öffnen > Gelöst – Abgebrochen
„Offen“ > „Gelöst – Abgebrochen“ > „Geschlossen“	„Offen“ > „Gelöst – Abgebrochen“ > „Geschlossen“
Öffnen > Gelöstes Ergebnis Ungültig > Geschlossenes Ergebnis Ungültig	Öffnen > Gelöstes Ergebnis Ungültig > Geschlossenes Ergebnis Ungültig
Öffnen > Geschlossen – Behoben	Öffnen > Geschlossen – Behoben

Wird Aufgelöst Konfigurations-Compliance Importprobleme

Lösen Sie Probleme mit dem Import der Drittpartei-Integration.

Problemlösung importieren

Problem	Lösung
Testergebnisse fehlen	Überprüfen Sie `Start Time` Auf der **Qualys-PC-Ergebnisse** Integration. Möglicherweise ist sie nicht weit genug zurückgesetzt. Weitere Informationen finden Sie unter Ändern Sie das Startdatum der Qualys-PC-Ergebnisse.
Die Integration schlägt fehl	Überprüfen Sie **Ausführung Der Schwachstellenintegration** Status. Einzelne Integrationsprozesseinträge enthalten die importierte XML, die auf unerwartete Informationen überprüft werden kann. Navigieren zu **Qualys Schwachstellenintegration** > **Primäre Integrationen** > **QualysPC-Ergebnisse** > **Ausführungen der Schwachstellen-Integration** Zugehörige Registerkarte. Wählen Sie die neueste Ausführung aus. Überprüfen Sie den Status und die Notizen der Einträge in der zugehörigen Liste **Integrationsprozess Für Schwachstellen** Für Anomalien. an.

Ändern Sie das Startdatum der Qualys-PC-Ergebnisse

Wenn Daten für das Startdatum im Qualys PC-Ergebnisimport fehlen, können sie geändert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_vul_qualys.admin

Prozedur

1. Navigieren zu **Alle** > **Qualys Schwachstellenintegration** > **Administration** > **Primäre Integrationen**an.
2. Klicken Sie Auf **Qualys-PC-Ergebnisse** Integration.
3. Klicken Sie Auf **Integrationsdetails** .
4. Legen Sie fest **Startzeit** Feld mit einem Wert in der Vergangenheit, sodass alle gescannten und erkannten Testergebnisse seit diesem Zeitpunkt erkannt werden.

   Hinweis:
   Wenn das Datum leer gelassen wird, werden bei der ersten Ausführung keine Daten zurückgegeben. Legen Sie den Wert auf maximal einen Monat in der Vergangenheit fest. Diese Einstellung verhindert, dass große Datenmengen die Qualys-API-Quotenbeschränkungen überschreiten und Ausführungszeitüberschreitungen auslösen.

5. Klicken Sie auf **Absenden** oder **Aktualisieren**.
6. **Wahlweise:** Klicken Sie Auf **Jetzt Ausführen** Zur sofortigen Ausführung.

CI-Suchregeln für Microsoft Defender for Cloud Integration Für Security Operations Und Palo Alto Prisma Cloud

Sie können die Suchregeln für Konfigurationselemente (Configuration Item, CI) für verwenden Microsoft Defender for Cloud Integration Und Palo Alto Prisma Cloud Integrationen, um eine richtige Übereinstimmung mit häufig verwendeten Ressourcentypen in zu finden Configuration Management Database (CMDB).

Übersicht

Das Modul „CI-Suchregeln“ enthält die Regeln, mit denen Sie die Felder definieren können, die die übereinstimmenden Daten in enthalten Configuration Management Database (CMDB). Sie können diese Regeln verwenden, um die Anwendungen und Anwendungs-Releases zu identifizieren. Alle Microsoft Defender for Cloud Integration Und Palo Alto Prisma Cloud Assets werden anhand der Kombination aus Objekt-ID, Cloud-Account und logischem Rechenzentrum im eindeutig identifiziert ServiceNow Plattform . ServiceNow Discovery füllt die Ressourcen-ID in aus `Object_ID` Spalte von CMDB In verschiedenen Formaten für die verschiedenen Ressourcentypen. Die folgende Tabelle zeigt die Objekt-ID-Formate häufig verwendeter Ressourcentypen, die der Discovery-Service zum Ausfüllen in verwendet `Object_ID` Spalte des CI. Jeder Scanner, der ein Asset eines bestimmten Ressourcentyps suchen möchte, muss mit dem richtigen Objekt-ID-Format suchen. Sie Kann das richtige Objekt-ID-Format abrufen, indem Sie die Objekt-ID-Spalte des entsprechenden betrachten CMDB CI-Klasse und versuchen Sie dann, die Objekt-ID anhand der vom Scanner empfangenen Werte zu erstellen.

Objekt-ID-Format für verschiedene Ressourcentypen

Ressourcentyp	Format
AWS::EC2::Instance	Objekt-ID
AWS::ElasticLoadBalancing::LoadBalancer	Name des Lastenausgleichsmoduls
AWS::S3::Bucket	arn:aws:s3:::<Bucket Name>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die CI-Übereinstimmung für ein Testergebnis wurde möglicherweise nicht genau in gefunden Configuration Management Database (CMDB) Es sei denn, das gleiche Format von ist `Object_ID` Wird in der Suchregel verwendet. Meistens finden die OOB-CI-Suchregeln eine Übereinstimmung für die am häufigsten verwendeten Ressourcentypen für Microsoft Defender for Cloud Integration Und Palo Alto Prisma Cloud.Wenn die folgenden CI-Suchregeln die CIs in nicht finden CMDB Für Ihre Testergebnisse können Sie eine CI-Suchregel für einen Ressourcentyp erstellen. Weitere Informationen zum Erstellen einer CI-Suchregel finden Sie unter Erstellen Sie eine CI-Suchregel .

CI-Suchregeln

Die folgenden CI-Suchregeln gelten spezifisch für Microsoft Defender for Cloud Integration Und Palo Alto Prisma Cloud.

S3-Bucket

Diese Suchregel versucht, das CI in zu finden CMDB Durch den Wert, der durch Verkettung von erhalten wurde `arn:aws:s3:::` Und Ressourcenname. Der erhaltene Wert wird in gesucht `Object_ID` Spalte von `cmdb_ci_Cloud_object_Storage` Tabelle. Diese Suchregel gilt nur, wenn der Ressourcentyp lautet `AWS::S3::Bucket` .

Name

Diese Suchregel versucht, das CI in zu finden CMDB Nach Name. Der Name, der in gesucht wird `Object_ID` Spalte der CI-Klasse, entspricht einem Ressourcentyp in `sn_CAPI_resource_type` Tabelle.

Hinweis:
Für die Palo Alto Prisma Cloud-Anwendung wird diese CI-Suchregel nur für ausgeführt `AWS::RDS::DBInstance` , `AWS::ElasticLoadBalancing::LoadBalancer` , Und `AWS::CloudTrail::Trail` Ressourcentypen. Sie können die Ressourcentypen hinzufügen, für die Sie diese CI-Suchregel ausführen möchten.

Ressourcen-ID

Diese Suchregel versucht, das CI in zu finden CMDB Anhand der Ressourcen-ID. Die Ressourcen-ID, die in gesucht wird `Object_ID` Spalte der CI-Klasse, entspricht einem Ressourcentyp in `sn_CAPI_resource_type` Tabelle.

Hinweis:
Sie können die Priorität für eine CI-Suchregel in festlegen **Reihenfolge** Feld. Die CI-Suchregel mit dem niedrigsten Reihenfolgewert wird zuerst ausgeführt.

Vulnerability Response Arbeitsbereiche

Vulnerability Response-Arbeitsbereiche bieten eine konsolidierte Ansicht der Funktionen Dies ermöglicht es Ihnen, mehrere Aufgaben innerhalb desselben Bereichs auszuführen, indem Sie die Produktivität steigern und Zeit sparen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vulnerability Response Arbeitsbereiche

Arbeitsbereich des Schwachstellenmanagers	Arbeitsbereich für IT-Korrekturen	Arbeitsbereich der Schwachstellenbewertung
Erfahren Sie mehr über den Vulnerability Manager-Arbeitsbereich	Erfahren Sie mehr über den Arbeitsbereich „IT-Korrektur“	Erfahren Sie mehr über den Arbeitsbereich „Schwachstellenbewertung“

Bevor Sie beginnen

Bevor Sie die Arbeitsbereiche verwenden können:

- Sie müssen einige Konfigurationsaufgaben ausführen. Weitere Informationen finden Sie unter Konfigurieren Sie Vulnerability Response Arbeitsbereiche.
- Überprüfen Sie wichtige Informationen zu Aktualisierungen von Korrekturaufgaben, Regeln für Korrekturaufgaben sowie wichtige Begriffe und Konzepte zu den Arbeitsbereichen in Vulnerability Response Arbeitsbereiche und Updates für Korrekturaufgaben und Korrekturaufgabe Regeln.

Problembehandlung und Hilfe

- Security Operations in der ServiceNow-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Vulnerability Response Übersicht über Arbeitsbereiche

Unterstützt Schwachstellenmanager und IT-Korrekturarbeitsbereiche Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance.

Die Arbeitsbereiche „Schwachstellenmanager“, „IT-Korrektur“ und „Schwachstellenbewertung“

Arbeitsbereich des Schwachstellenmanagers

Als Schwachstellenmanager schützen Sie die Assets Ihres Unternehmens vor Malware und böswilligen Angriffen. Von einem einzelnen Arbeitsbereich in Ihrem aus ServiceNow AI Platform®, Mit Vulnerability Response Die Anwendung identifiziert zusammen mit aktuellen Schwachstellendaten, die aus Schwachstellenbibliotheken und Scannerdatenanwendungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

von Drittanbietern in Ihre Instanz importiert werden, kritische Schwachstellen und Fehlkonfigurationen, priorisiert sie und sendet Listen von Korrekturaufgaben an DIE IT, damit ihre Spezialisten reagieren können.

Arbeitsbereich für IT-Korrekturen

Verwenden Sie als IT-Spezialist Listen oder Korrekturaufgaben (RT), die von Schwachstellenmanagern gesendet werden, um kritische Schwachstellen zu überwachen und zu beheben, die Ihnen oder Ihren Gruppen zugewiesen sind. Gruppen angreifbarer Elemente mit Patches, Lösungen, Schwachstellen-Rescans, Change-Anforderungen, Ausnahmen beheben und andere Tools zur Korrektur angreifbarer Elemente und zum Testen von Ergebnissen alle von einem Ort aus.

Arbeitsbereich der Schwachstellenbewertung

Führen Sie als Schwachstellen-Ereignismanager eine Risikobewertung durch, und verwalten Sie kritische Schwachstellenereignisse proaktiv, insbesondere während kritischer Schwachstellenereignisse wie einem Zero-Day-Ereignis.

Schlüsselfunktionen

Die Vulnerability Response Arbeitsbereiche enthalten die folgenden Funktionen und Erweiterungen.

- Verwenden Sie die Massenbearbeitungsfunktion in Arbeitsbereich des Schwachstellenmanagers Dient zum gleichzeitigen Aktualisieren mehrerer Datensätze. Weitere Informationen finden Sie unter Massenbearbeitung in verwenden Arbeitsbereich des Schwachstellenmanagers.
- Zeigen Sie die Dashboards Vulnerability Management (PA), Schwachstellengenehmigungen, CISO, Container Vulnerability Management-Übersicht, Anwendungs-Schwachstellenmanagement-Dashboard, Unified Vulnerability Response und Health in der Next Experience-UI auf der Dashboards-Seite des Vulnerability Manager-Arbeitsbereichs an. Weitere Informationen finden Sie unter Seite „Dashboards“ in Arbeitsbereich des Schwachstellenmanagers.
- Zeigen Sie das Dashboard „Schwachstellenkorrektur“ in der Next Experience-UI auf der Seite „Dashboards“ des IT-Korrekturarbeitsbereichs an. Weitere Informationen finden Sie unter Seite „Dashboards“ in Arbeitsbereich für IT-Korrekturen.
- Erstellen Sie die Korrekturaufgaben (VUL, AVUL, CVUL oder CRG) manuell in Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen. Weitere Informationen finden Sie unter Erstellen Sie eine Korrekturaufgabe manuell in Arbeitsbereich des Schwachstellenmanagers und Erstellen Sie eine Korrekturaufgabe manuell in Arbeitsbereich für IT-Korrekturen.
- Teilen Sie die Korrekturaufgaben (VUL, AVUL, CVUL und CRG) in auf Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen. Weitere Informationen finden Sie unter Fordern Sie Ausnahmen für Korrekturaufgaben und -Datensätze in an Arbeitsbereich des Schwachstellenmanagers Und Teilen Sie eine Korrekturaufgabe in auf Arbeitsbereich für IT-Korrekturen Entsprechend.
- Fordern Sie die Richtlinienausnahmen für angreifbare Elemente (Vits, AVITs und CVITs) und Korrekturaufgaben (VUL, AVUL, CVUL und CRG) in den Schwachstellenmanager- und IT-Korrekturarbeitsbereichen an. Weitere Informationen finden Sie unter Fordern Sie Ausnahmen für Korrekturaufgaben und -Datensätze in an Arbeitsbereich des Schwachstellenmanagers Und Fordern Sie eine Ausnahme mit an GRC: Richtlinien- und Compliance-Management In Arbeitsbereich für IT-Korrekturen Entsprechend.
- Erstellen und verfolgen Sie kritische Schwachstellenereignisse über das Vulnerability Crisis Management (VCM). Weitere Informationen finden Sie unter Arbeitsbereich für Schwachstellenbewertung kennenlernen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fügen Sie der Bibliothek für Ausgleichssteuerungen in Ausgleichssteuerungen Ausgleichssteuerungen hinzu Arbeitsbereich des Schwachstellenmanagers. Weitere Informationen finden Sie unter Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu.
- Fordern Sie im IT-Korrekturarbeitsbereich eine Risikominderung für ein angreifbares Host-Element und eine Korrekturaufgabe an. Weitere Informationen finden Sie unter Fordern Sie eine Risikominderung für ein angreifbares Element oder eine Korrekturaufgabe an.
- Erstellen Sie ein Agile-Problem und ein Jira-Problem für angreifbare Anwendungs- und Container-Elemente aus dem Arbeitsbereich des Schwachstellenmanagers. Weitere Informationen finden Sie unter Erstellen Sie agiles Problem manuell mithilfe der Formularaktion und Erstellen Sie agiles Problem manuell mithilfe der Listenaktion.

Weitere Informationen zur Versionskompatibilität mit den Familien-Releases finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema artikel in der HI Knowledge Base.

Patch-Orchestration mit Vulnerability Response Arbeitsbereiche

Mit Patch Orchestration mit können Sie Patches und Patch-Bereitstellungen für kritische Schwachstellen für große Gruppen Ihrer Assets verwalten Vulnerability Response.

Patch-Orchestration in den Arbeitsbereichen

Patch-Orchestration mit Vulnerability Response Die Anwendung verwendet geplante Importe aus Integrationen von Drittanbieterlösungen, Patch-Lieferanten und Schwachstellen-Scannern.

Patch-Orchestration mit Vulnerability Response Die Anwendung wird sowohl in der klassischen Umgebung als auch in unterstützt Vulnerability Response Arbeitsbereiche. Korrelierte Daten werden zusammengefasst und sowohl in den Arbeitsbereichen als auch in der klassischen Umgebung angezeigt. Eine Übersicht über die Funktionen, Anforderungen und Informationen zur Patch-Orchestration in der klassischen Umgebung finden Sie unter Patch-Orchestration mit Vulnerability Response.

- Weitere Informationen zu den unterstützten Integrationen mit Patch-Lieferanten finden Sie unter Verständnis der Integration der HCL BigFix-Patch-Orchestration mit Vulnerability Response Und Verstehen von Vulnerability Response Patch-Orchestration-Integration mit Microsoft SCCM.
- Informationen zum Planen von Patches-Formulardatensätzen in Arbeitsbereichen finden Sie unter Planen Sie Patches mit Microsoft SCCM-Integration mit Vulnerability Response Und Planen Sie Patches mit Vulnerability Response Patch-Orchestration-Integration HCL BigFix.

Verfügbare Versionen von Anwendungen und Abhängigkeiten, die für die Patch-Orchestration-Integration erforderlich sind

Dient zum Anzeigen von Patch Orchestration-Daten und verfügbaren Updates (Patches) in den Arbeitsbereichen in Vulnerability Response, Die folgenden Anwendungen sind erforderlich. Alle aufgeführten Anwendungen sind in verfügbar ServiceNow® Store. Einige Anwendungen erfordern separate Abonnements. Weitere Informationen finden Sie unter Patch-Orchestration mit Vulnerability Response.

Erforderliche Rollen

Zusätzlich zu den Rollen sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin, die für erforderlich sind Vulnerability Response Arbeitsbereiche benötigen Anwender Rollen, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für die Patch-Orchestration-Integrationen spezifisch sind, die Sie verwenden, um Daten anzuzeigen und Patches zu planen. Weitere Informationen zu diesen Rollen finden Sie in den folgenden unterstützten Integrationen.

Siehe Verständnis der Integration der HCL BigFix-Patch-Orchestration mit Vulnerability Response und Verstehen von Vulnerability Response Patch-Orchestration-Integration mit Microsoft SCCM.

Daten in patchen Vulnerability Response Arbeitsbereiche

In IT-Korrekturarbeitsbereich , Sie können Patch-Daten in den Arbeitsbereichen anzeigen:

- Klicken Sie in der Startseite-Ansicht auf Bewertungslisten, um Datensätze für bevorzugte Lösungen für VIS, angreifbare CIs und bevorzugte Patches für VIS anzuzeigen.
- Zeigen Sie in der Listenansicht alle Patch-Update-Datensätze (VPUs) und die Ihnen zugewiesenen angreifbaren Elemente an, die Patches aus den verfügbaren Links enthalten.

Sie können Patches aus den folgenden Datensätzen planen:

- Patch-Update (VPU)
- Korrekturaufgabe (RT)
- Erkanntes Element (SDI)

In Arbeitsbereich des Schwachstellenmanagers, Sie können Patches anzeigen:

- In der Startansicht der Überwachungsthemen auf der Registerkarte angreifbare Elemente können Sie bevorzugte und potenzielle Patches, geplante Patches und andere Informationen anzeigen.
- In der Listenansicht von Korrekturmaßnahmen-Datensätzen können Sie Patch-Daten in VIT-Datensätzen auf der Registerkarte angreifbare Elemente anzeigen.

Vulnerability Response Arbeitsbereiche und Updates für Korrekturaufgaben und Korrekturaufgabe Regeln

Korrekturaufgaben bündeln Datensätze (Vits, AVITs, CVITs oder CTRs) in der Vulnerability Response Arbeitsbereiche.

Schlüsselbegriffe für Vulnerability Response Arbeitsbereiche

Vulnerability Response-Arbeitsbereiche oder -Arbeitsbereiche

Vulnerability Response Unterstützt Vulnerability Response Arbeitsbereiche. Sie können entweder den klassischen verwenden Core-UI Experience oder die Arbeitsbereiche.

Klassische (veraltete) UI

Bezieht sich auf Core-UI Experience. Sie führen weiterhin einige Aktionen aus und zeigen einige Listen in der klassischen Umgebung an.

Arbeitsbereich des Schwachstellenmanagers

In diesem Arbeitsbereich überwachen Manager gezielte Schwachstellen und wählen die VIS und Testergebnisse aus, die ihnen am wichtigsten sind, um SIE IHM zuzuweisen.

Arbeitsbereich für IT-Korrekturen

In diesem Arbeitsbereich können sich IT-Teams auf die wichtigsten Schwachstellen konzentrieren, die ihnen von der Sicherheit zugewiesen sind. IT-zentrierte Informationen, die betroffene, eindeutige Konfigurationselemente (Configuration Items, CIs), Lösungen und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturfortschritt enthalten, sind für Korrekturverantwortliche in diesem Arbeitsbereich leicht verfügbar.

Arbeitsbereich der Schwachstellenbewertung

In diesem Arbeitsbereich können Schwachstellenanalysten während der Zero-Day-Schwachstellenanalyse Schwachstellenbewertungen durchführen. Nachdem eine Zero-Day-Schwachstelle identifiziert wurde, können sie die potenziellen Auswirkungen und das mit der Schwachstelle verbundene Risiko bewerten. Die Analysten können die betroffenen System-, Anwendungen- oder Netzwerkkomponenten analysieren, um den Schweregrad und mögliche Angriffsvektoren innerhalb der Organisation zu verstehen.

Überwachungsthema

Überwachungsthemen definieren ein Segment der angreifbaren Elemente, die Schwachstellenmanager und Analysten im Vulnerability Manager-Arbeitsbereich überwachen möchten. Überwachungsthemen zeigen einen fokussierten Übersichtssatz von Berichten, die sich auf ein Segment von VIS beziehen Und Testergebnisse Mit Trends, CI- und Schwachstellenbezogenen Statistiken. Die Dashboards zu diesen Themen können zur Überwachung von Trends verwendet werden. Die Dashboards können Managern auch helfen:

- Zeigen Sie den Korrekturfortschritt für kritische Elemente an
- Bestimmen Sie das Vorhandensein von Schwachstellen in kritischen Systemen
- Sehen Sie, wann ein neuer Exploit herauskommt
- Schnelle Reaktion zur Behebung eines bestimmten Satzes von Schwachstellen

Korrekturmaßnahme (RE)

Korrekturmaßnahmen werden von Schwachstellenmanagern erstellt, wenn sie bestimmen, dass es an der Zeit ist, dass DIE IT die in einem Überwachungsthema aufgeführten Schwachstellen beheben muss. Schwachstellenmanager und Analysten können wählen, wie sie Korrekturaufgaben erstellen möchten, z. B. nach Zuweisungsgruppe und Schwachstelle. Korrekturaufgaben sind in der Korrekturmaßnahme enthalten.

Korrekturaufgabe (VUL)

IT-Teams verwenden Korrekturaufgaben, um die ihnen von der Sicherheit zugewiesenen Schwachstellen zu beheben. Korrekturaufgaben sind Listen der Aktionen, die zum Beheben von Schwachstellen erforderlich sind. Korrekturaufgaben werden automatisch erstellt, wenn Sicherheitsmanager Korrekturmaßnahmen erstellen.

Entwicklung der Arbeitsbereiche

In vorherigen Versionen von Vulnerability Response, Sie hatten zwei Optionen, um als Sicherheits- und Schwachstellenanalyst eine Reihe von Datensätzen (Vits, AVITs, CVITs oder CTRs) zu überwachen:

- Das Übersichts-Dashboard, das alle VIS zusammenfasst
- Korrekturaufgaben

Angreifbare Elemente wurden sortiert Korrekturaufgaben Automatisch gemäß Ihren vordefinierten Regeln für Korrekturaufgaben. Korrekturaufgaben Wurden entwickelt, um IT-Teams bei der Korrektur von verwaltbaren Blöcken angreifbarer Elemente zu unterstützen.

Diese Automatisierung ermöglichte es, eine sehr große Anzahl von Datensätzen automatisch zur Massenzuweisung und -Korrektur zu gruppieren. Schwachstellenanalysten und Manager haben jedoch festgestellt, dass die Überwachung des gesamten Datensatzes von Korrekturaufgaben herausfordert. Zusätzlich zu Leistungsproblemen mit großen Gruppen wird funktionale erstellt Korrekturaufgabe Regeln, die nur die Schwachstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

herausgefiltert haben, die Sie als besonders kritisch eingestuft haben, können schwierig sein.

Die Vulnerability Response Arbeitsbereiche:

- Helfen Sie Sicherheitsmanagern, aktive VIS und herauszufiltern und zu überwachen Testergebnisse Im Laufe der Zeit und fördern die Korrektur der Schwachstellen, die sie bestimmen, sind die wichtigsten.
- Stellen Sie IT-Teams an einem Ort IT-zentrierte Informationen bereit, mit denen sie die ihnen von der Sicherheit zugewiesenen Schwachstellen beheben können.

Aktualisiert Korrekturaufgaben in den Arbeitsbereichen

Im Vulnerability Manager-Arbeitsbereich verwenden Schwachstellenanalysten und Manager *Überwachungsthemen* Und *Korrekturmaßnahmen* Als zwei neue Methoden für die Überwachung und Zuweisung von VIS zur Korrektur.

Schwachstellengruppen werden umbenannt, *Korrekturaufgaben* . Diese Änderung gilt für Bezeichnungen in Listen, Datensätzen und Regeln sowohl in der Legacy-UI als auch in den Arbeitsbereichen. Korrekturaufgaben sind so eingerichtet, dass IT-Teams im IT-Korrekturarbeitsbereich mit ihnen arbeiten können. Die folgende Liste zeigt, wie Sie als Schwachstellenmanager oder Schwachstellenanalyst Schwachstellen überwachen können Und Testergebnisse, Filtern Sie sie, und weisen Sie sie zu:

1. Im Vulnerability Manager-Arbeitsbereich überwachen Manager importierte Schwachstellen und Fehlkonfigurationen zu Überwachungsthemen. Manager und Analysten verwenden Überwachungsthemen, um eine dynamische Reihe gefilterter Datensätze im Zeitverlauf zu überwachen, die ihrer Meinung nach die kritischsten sind.
2. Mit Überwachungsthemen können Sicherheitsmanager bestimmen, wann und welche Arten von VIS in Remediation Efficiency (RES) an IT-Teams übergeben werden sollen. Diese RES sind statische Listen der VIS, die die Sicherheit VON IT-Teams beheben möchte.

   Von Korrekturmaßnahmen haben Manager vier Optionen, um Datensätze in Korrekturaufgaben (VULs, AVULs, CVULs oder CRGs) zu bündeln. Korrekturaufgaben werden IT-Teams basierend auf den Zuweisungsgruppen, die ursprünglich den Datensätzen zugeordnet sind, automatisch zugewiesen.
3. IT-Teams arbeiten im IT-Korrekturarbeitsbereich an Korrekturaufgaben, ohne alle Datensätze sortieren zu müssen.

   Eine Korrekturaufgabe durchläuft dieselben status wie die Korrekturaufgabe in früheren Versionen von Vulnerability Response. Wenn alle Datensätze in einer Korrekturaufgabe geschlossen sind, wird die Korrekturaufgabe geschlossen und auf festgelegt **Inaktiv** .

   Der Korrekturfortschritt wird bei Datenvisualisierungen in den Überwachungsthemen und auf der Homepage der IT-Korrektur aktualisiert.

Aktualisiert die Regeln für Korrekturaufgaben in den Arbeitsbereichen

Schwachstellen-Gruppenregeln werden aufgerufen *Regeln Für Korrekturaufgaben* . Diese Änderung gilt für die Bezeichnungen in Listen, Datensätzen und Regeln sowohl in der Legacy-UI als auch in den Arbeitsbereichen.

Tabellennamen, z. B. [sn_vul_m2m_vul_Group_item], werden nicht geändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie Schwachstellen-Gruppenregeln in einer früheren Version von erstellt haben Vulnerability Response, Sind sie für Sie weiterhin verfügbar, die als Regeln für Korrekturaufgaben gekennzeichnet sind.

In den Arbeitsbereichen werden jedoch keine Regeln für Korrekturaufgaben mehr als primäre Methode zum Organisieren einer großen Menge von Datensätzen in Korrekturaufgaben verwendet. Möglicherweise möchten Sie Ihre Regeln für Korrekturaufgaben inaktiv lassen, wenn Sie sich an die Arbeitsbereiche gewöhnen.

Sie sollten stattdessen schrittweise mit der Verwendung von beginnen Vulnerability Response Arbeitsbereiche.

1. Wenn Sie ein Upgrade von einer vorherigen Version von durchführen Vulnerability Response Ihre vorhandenen Regeln für Korrekturaufgaben werden beibehalten. Sie stehen Ihnen weiterhin in den Arbeitsbereichen zur Verfügung. Die standardmäßige Gruppenregel Schwachstelle ist standardmäßig inaktiv.
2. Konfigurieren Sie Zuweisungsregeln und ggf. Risikoregeln, und führen Sie dann einen Import durch.
3. Als Schwachstellenmanager oder -Analyst können Sie Segmente auswählen, die überwacht werden sollen, aus den Überwachungsthemen im Vulnerability Manager-Arbeitsbereich. Sie können Überwachungsthemen als eigenständige Funktionen verwenden. Wählen Sie eine Teilmenge von Datensätzen aus, und verwenden Sie das Dashboard dafür, um Trends zu überwachen. Mit ihnen können Sie entscheiden, wo und wann Korrekturmaßnahmen konzentriert werden sollen.
4. Als Schwachstellenmanager oder Analyst erstellen Sie Korrekturmaßnahmen aus Überwachungsthemen, wenn Sie entscheiden, dass es an der Zeit ist, eine Teilmenge von Datensätzen zu korrigieren. Eine Korrekturaufgabe wird ebenfalls automatisch erstellt, um SIE bei der Erstellung einer Korrekturmaßnahme an DIE IT zu übergeben.
5. Im Laufe der Zeit entdecken Sie als Schwachstellenmanager oder Analyst möglicherweise einige Routinemuster, die Sie automatisch mit Regeln für Korrekturaufgaben verarbeiten können.

Um Ihre Regeln für Korrekturaufgaben anzuzeigen, navigieren Sie zu entsprechenden **Regeln Für Korrekturaufgaben** Module in Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance Von **Alle** Menü.

Weitere Informationen zu Zuweisungsregeln, Regeln für Korrekturaufgaben, Korrekturmaßnahmen und angreifbaren Elementen in Vulnerability Response Arbeitsbereiche

- Datensätze der Korrekturaufgabe werden in Listen und Datensätzen sowohl in der klassischen Umgebung als auch in den Arbeitsbereichen angezeigt.
- Eine Korrekturaufgabe durchläuft dieselben status wie eine Schwachstellengruppe. Wenn alle Datensätze in einer Korrekturaufgabe geschlossen sind, wechselt die Korrekturaufgabe in den Status „Inaktiv“.
- Um Ihren Teams bei der Korrektur zu helfen, kann ein angreifbares Element nur in einer Korrekturmaßnahme sein. Sobald es sich in einer Korrekturmaßnahme befindet, wird ein angreifbares Element keinem anderen von Ihnen erstellten Korrekturmaßnahmen hinzugefügt.
- Wenn Sie eine Korrekturmaßnahme löschen, wird die Korrekturmaßnahme inaktiv, und alle aktiven VIS sind für neue Korrekturmaßnahmen verfügbar.
- Ein Datensatz (VIT, AVIT, CVIT oder CTR) kann sich in mehreren Korrekturaufgaben befinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Korrekturaufgaben werden IT-Teams basierend auf der Zuweisungsgruppe, die einem angreifbaren Element in einer Korrekturmaßnahme zugeordnet ist, automatisch zugewiesen. Wenn Sie bei Bedarf eine Korrekturaufgabe erstellen, wählen Sie die Zuweisungsgruppe aus.
- Wenn Sie ein Upgrade von einer vorherigen Version von durchführen Vulnerability Response, Ihre Zuweisungsregeln wurden in der Legacy-UI beibehalten.
- Wenn Sie ein Upgrade von einer vorherigen Version von durchführen Vulnerability Response, Ihre aktuellen Anwender und Gruppen werden geerbt und können in den Arbeitsbereichen für Sie zugänglich sein.

Weitere Informationen zu den Lebenszyklen von Korrekturmaßnahmen finden Sie unter Lebenszyklen von Korrekturmaßnahmen, Korrekturaufgaben und Datensätzen in den Vulnerability Response-Arbeitsbereichen.

Konfiguration und Setup für Vulnerability Response Arbeitsbereiche

Weitere Informationen zu Zuweisungsregeln und Regeln für Korrekturaufgaben finden Sie unter Konfigurieren Sie Vulnerability Response Arbeitsbereiche Und Vulnerability Response Übersicht über Zuweisungsregeln.

Wenn Sie ein neuer Kunde sind und ihn noch nicht hinzugefügt haben, müssen Sie Anwender und Gruppen so einrichten, dass angreifbare Elemente und Korrekturaufgaben den gewünschten Korrekturgruppen zugewiesen werden. Vulnerability Response-Zuweisungsregeln Werden verwendet, um Gruppen Arbeit zuzuweisen.

Konfigurieren Sie Vulnerability Response Arbeitsbereiche

Bevor Sie die Arbeitsbereiche verwenden können, bestätigen Sie, dass Sie die folgenden Setup-Aufgaben abgeschlossen haben.

Vorbereitungen
Erforderliche Rolle: administrator zum Zuweisen von Rollen zu Anwendern und Gruppen und von Anwendern zu Gruppen.

sn_vul.Vulnerability_admin zum Bearbeiten, Erstellen von Regeln und Konfigurieren von Vulnerability Response Anwendung.

Bestätigen Sie, dass Sie die folgenden Setup-Aufgaben abgeschlossen haben. Weitere Informationen zur Ausführung dieser Aufgaben finden Sie in den Schritten nach der Liste.

Aufgabe	Beschreibung
☐	Wenn nicht bereits zugewiesen, weisen Sie Anwendern und Gruppen die richtigen Rollen zu, damit sie Zugriff auf die Arbeitsbereiche haben. Erforderliche Rolle: admin. Weitere Informationen finden Sie in den folgenden Schritten.
☐	Richten Sie Zuweisungsregeln ein, damit angreifbare Elemente zur Korrektur den richtigen Gruppen zugewiesen werden. Erforderliche Rolle: sn_vul.Vulnerability_admin.

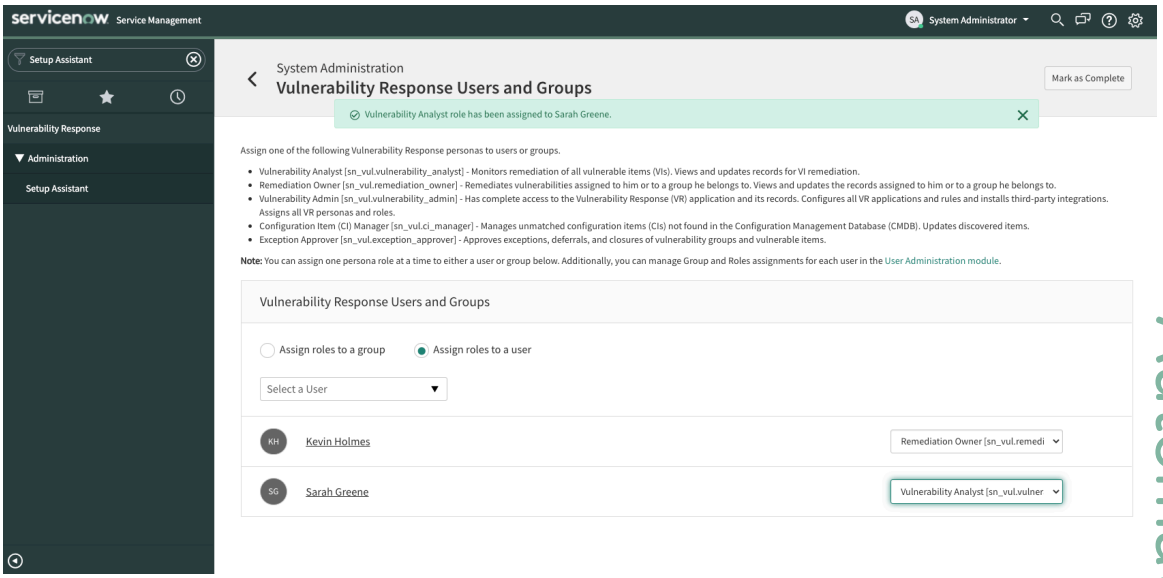
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Sie erstellen und bearbeiten Zuweisungsregeln in der klassischen Umgebung.
☐	(Optional): Bearbeiten oder erstellen Sie Ihre Regeln für Korrekturaufgaben. Erforderliche Rolle: sn_vul.Vulnerability_admin. **Hinweis:** Funktionell funktionieren die Regeln für Korrekturaufgaben genau wie die Regeln für Korrekturaufgaben in früheren Versionen von Vulnerability Response. Im Gegensatz zu den Schwachstellen-Gruppen, die automatisch aus Ihren Regeln für Korrekturaufgaben erstellt wurden, werden Korrekturaufgaben jedoch erstellt, wenn Sie Korrekturmaßnahmen erstellen. Sie haben die folgenden Optionen, um die angreifbaren Elemente in einer Korrekturmaßnahme in Korrekturaufgaben zu bündeln: • Nach Zuweisungsgruppe • Nach Zuweisungsgruppe und Konfigurationselement • Nach Zuweisungsgruppe und Schwachstelle • Keine: Verwenden Sie diese Option, wenn Sie einer Korrekturaufgabe VIS manuell hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie eine Korrekturaufgabe bei Bedarf aus der Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers. Weitere Informationen dazu, wie VIS automatisch gruppiert werden und wie die Gruppenregeln in der klassischen Umgebung erneut angewendet werden, finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.
☐	Bearbeiten Sie Korrekturzielregeln. Erforderliche Rolle: sn_vul.Vulnerability_admin. Fügen Sie Korrekturzielregeln in der klassischen Umgebung hinzu. Weitere Informationen zu Korrekturzielregeln finden Sie unter Erstellen oder bearbeiten Vulnerability Response Korrekturzielregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Nachdem Sie installiert und aktiviert haben Vulnerability Response Navigieren Sie in der klassischen Umgebung als Anwender mit der Administratorrolle zu **Alle** > **Vulnerability Response** > **Administration** > **Setup-Assistent**an.



2. Weisen Sie im Setup-Assistenten Anwender den folgenden Gruppen zu.

> **Hinweis:**
> 1000 ist der Grenzwert für die Anzahl der Anwendergruppen, denen ein Anwender in den Vulnerability Response-Arbeitsbereichen zugewiesen werden kann.

Die folgenden Gruppen werden mit bereitgestellt Vulnerability Response Anwendung und werden in den Arbeitsbereichen verwendet. Sie können ihnen im Setup-Assistenten Anwender zuweisen:

- Korrekturbesitzer: Diese Gruppe ist für IT-Korrekturbesitzer im IT-Korrekturarbeitsbereich bestimmt. Anwender mit dieser Rolle beheben Schwachstellen, die ihnen in Korrekturaufgaben zugewiesen sind.

  > **Hinweis:**
  >
  > Wenn Ihre Korrekturbesitzer Change-Anforderungen erstellen und anzeigen sollen Und zeigen Sie Daten von angreifbaren Konfigurationselementen (CI) im Arbeitsbereich „IT-Korrektur“ und in der klassischen Umgebung an , Weisen Sie ihnen die Rolle itil zu. Möglicherweise ziehen Sie es vor, die itil-Rolle einzelnen Anwendern anstatt allen Mitgliedern in einer Gruppe zuzuweisen. Die Rolle cmdb_read ist auch eine Option für Anwender, CI-Daten in den Arbeitsbereichen anzuzeigen.

- Ab v16.1 können Sie E-Mail-Erinnerungen an Ihre IT-Korrekturbesitzer einrichten. Informationen zum Einrichten von E-Mail-Benachrichtigungen für Arbeitsbereiche finden Sie unter Richten Sie E-Mail-Benachrichtigungen in ein Vulnerability Response Arbeitsbereiche.
- Schwachstellenadministrator: Diese Gruppe ist für Schwachstellenmanager vorgesehen. Diese Rolle konfiguriert Vulnerability Response Anwendung im Setup-Assistenten. Diese Rolle hat auch die Berechtigung, Ausnahmen und falsch positive Anforderungen zu verarbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schwachstellenanalyst: Diese Gruppe ist für Sicherheitsmanager, Schwachstellenmanager und Analysten im Schwachstellenmanager-Arbeitsbereich vorgesehen. Diese Rolle überwacht Schwachstellen, erstellt Überwachungsthemen und Korrekturmaßnahmen und überwacht den Korrekturfortschritt.
- Falsch positiver Genehmiger: Anwender in dieser Gruppe verarbeiten falsch positive Anforderungen für angreifbare Elemente oder Korrekturaufgaben. Eine falsch positive Anforderung erfordert einen einstufigen Genehmigungsprozess. Sie können die Zuweisung von Anwendern zu dieser Gruppe außerhalb des Setup-Assistenten in verwalten **Anwenderverwaltung** .
- Ausnahmegenehmiger: Eine Ausnahmeanforderung für ein angreifbares Element oder eine Korrekturaufgabe wird mit einem standardmäßigen Genehmigungs-Workflow auf zwei Ebenen genehmigt. Die Ausnahmeanforderung erfordert zwei Ebenen von Genehmigern. Fügen Sie beiden Genehmigungsgruppen Anwender hinzu: Ausnahmegenehmiger – Ebene 1 und Ausnahmegenehmiger-Ebene – 2. Nachdem die Anforderung vom Genehmiger der Ebene 1 genehmigt wurde, wird sie an den Genehmiger der zweiten Ebene gesendet. Sie verwalten die Zuweisung von Anwendern zu dieser Gruppe außerhalb des Setup-Assistenten in **Anwenderverwaltung** .

Hinweis:
Fügen Sie den Genehmigungsgruppen Anwender hinzu, bevor Sie falsch positive Anforderungen und Ausnahmeanforderungen übermitteln. Wenn Sie Anforderungen erstellen, bevor Sie Anwendern mit Genehmigungsberechtigung zuweisen, sind die Anforderungen möglicherweise nicht für sie sichtbar.

Alternativ können Sie auf klicken **Anwenderverwaltung** Link zum Verwalten und Zuweisen der folgenden granularen Rollen an Ihre Anwender und vorhandenen Gruppen. Mit diesen Rollen können Anwender bestimmte Aktionen innerhalb von ausführen Vulnerability Response Anwendung und die Arbeitsbereiche.

- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vul.remediation_owner
- Zum Erstellen und Anzeigen von Change-Anforderungen Weisen Sie ihnen im IT-Korrekturarbeitsbereich und in der klassischen Umgebung die Rolle itil zu.

Siehe Vulnerability Response Personas und granulare Rollen Und Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent Weitere Informationen zum Zuweisen von Persona-Rollen zu Anwendern und Anwendern zu Gruppen.

3. Korrekturaufgaben werden automatisch an IT-Korrekturzuweisungsgruppen zur Verarbeitung übergeben, wenn sie erstellt werden.
   - Nach Zuweisungsgruppe
   - Nach Zuweisungsgruppe und Konfigurationselement
   - Nach Zuweisungsgruppe und Schwachstelle
   - Keine: Verwenden Sie diese Option, wenn Sie einer Korrekturaufgabe VIS manuell hinzufügen möchten.

Hinweis:
Für die Version 18,0 von Vulnerability Response, **Keine** Option ist nicht verfügbar.

Wenn Sie ein Upgrade von einer vorherigen Version von durchführen Vulnerability Response, Ihre Zuweisungsgruppen werden beibehalten. Sie sollten diese Gruppen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

jedoch möglicherweise so bearbeiten, dass angreifbare Elemente bestimmten Zuweisungsgruppen zugeordnet werden, bis Sie sich daran gewöhnt haben, wie Überwachungsthemen und Korrekturmaßnahmen funktionieren. Sie können beispielsweise Zuweisungsgruppen nach Produkt oder Region erstellen, aber Sie können alle Kriterien verwenden, die am besten zu Ihrer Organisation passen.

Sie können auch Zuweisungsregeln verwenden, um Gruppen Korrekturaufgaben zuzuweisen. Möglicherweise möchten Sie nur Regeln mit hoher Priorität für die folgenden Elemente ausführen:

- Elemente, die eine besondere Behandlung erfordern
- Elemente, bei denen das Risiko kritisch ist oder ein VI die Behandlung durch regulatorische Compliance erfordert

Die folgenden Zuweisungsregeln, die mit der Anwendung bereitgestellt werden, sind standardmäßig aktiv:

- Stillgelegte CI-Zuweisungsregel
- An CI-Supportgruppe zuweisen
- Zuweisungsregel Für Arbeitsstationen
- Datenbank-Zuweisungsregel
- Zuweisungsregel Für Webanwendung
- Windows Server-Zuweisungsregel
- Zuweisungsregel für nicht-Windows-Server
- Zuweisungsregel „Alle Erfassen“

Weitere Informationen zu Zuweisungsregeln finden Sie unter Vulnerability Response Übersicht über Zuweisungsregeln. Sie erstellen und bearbeiten Zuweisungsregeln in der klassischen Umgebung.

4. **Wahlweise:** Bearbeiten oder erstellen Sie Ihre Regeln für Korrekturaufgaben.

(Optional) In den Arbeitsbereichen werden Korrekturaufgaben erstellt, wenn Sie Korrekturmaßnahmen erstellen. Sie haben die folgenden Optionen, um die angreifbaren Elemente in einer Korrekturmaßnahme in Korrekturaufgaben zu bündeln:

- Nach Zuweisungsgruppe
- Nach Zuweisungsgruppe und Konfigurationselement
- Nach Zuweisungsgruppe und Schwachstelle
- Keine: Verwenden Sie diese Option, wenn Sie einer Korrekturaufgabe VIS manuell hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie eine Korrekturaufgabe bei Bedarf aus der Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers.

Hinweis:
In t He Version 18,0 von Vulnerability Response, **Keine** Option ist nicht verfügbar.

Weitere Informationen dazu, wie VIS automatisch gruppiert werden und wie die Gruppenregeln in der klassischen Umgebung erneut angewendet werden, finden Sie unter Vulnerability Response Übersicht über Korrekturaufgaben und Regeln für Korrekturaufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

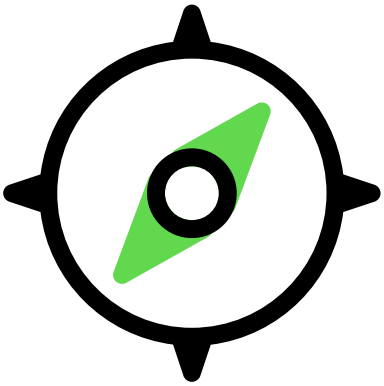
Arbeitsbereich des Schwachstellenmanagers

Die Arbeitsbereich des Schwachstellenmanagers Ermöglicht Schwachstellenmanagern und Analysten, die Schwachstellen und Fehlkonfigurationen zu überwachen, die ihnen am meisten wichtig sind, und strategisch zu entscheiden, welche Schwachstellen sie an IT-Teams senden, um sie zu beheben.

V18.0 – Demo zum Vulnerability Manager-Arbeitsbereich

Erste Schritte

Untersuchen

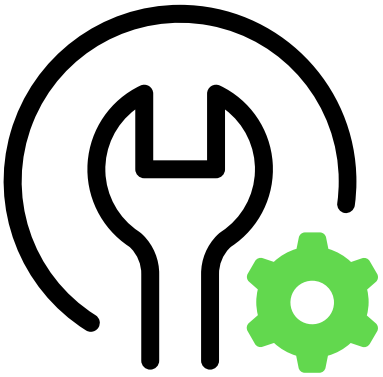


Erfahren Sie mehr über die Funktionen in Arbeitsbereich des Schwachstellenmanagers

Überwachen und verwalten

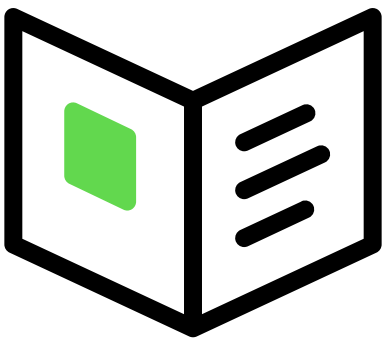
Erfahren Sie, wie angreifbare Elemente (Vits, AVITs und CVITs) und Testergebnisse im überwacht und verwaltet werden Arbeitsbereich des Schwachstellenmanagers

Beheben



Erfahren Sie, wie Sie angreifbare Elemente (Vits, AVITs und CVITs) und Testergebnisse im beheben können Arbeitsbereich des Schwachstellenmanagers

Referenz



Erfahren Sie mehr über die zusätzlichen Informationen, die zur Verwendung von erforderlich sind Arbeitsbereich des Schwachstellenmanagers

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- Security Operations in der ServiceNow-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Arbeitsbereich des Schwachstellenmanagers erkunden

Als Schwachstellenmanager und -Analyst erhalten Sie einen Einheitliche Ansicht aller Schwachstellentypen in Arbeitsbereich des Schwachstellenmanagers. Sie können Host-, Anwendungs- und Container-Schwachstellen und Konfigurationsprobleme anzeigen, Überwachungsthemen für diese Schwachstellen und Fehlkonfigurationen erstellen, Korrekturmaßnahmen und Korrekturaufgaben erstellen.

Hinweis:
Ab v19.0 von Vulnerability Response, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie v19.0 und höher
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Sie können anzeigen Arbeitsbereich des Schwachstellenmanagers Indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.

Die Arbeitsbereich des Schwachstellenmanagers Besteht aus den folgenden Seiten:

Homepage

Besteht aus vordefinierten Filtern, die zur Visualisierung der Zusammenfassung der Host-Schwachstellen, Anwendungsschwachstellen, Container-Schwachstellen und Konfigurationstestergebnisse verwendet werden.

Weitere Informationen zur Homepage finden Sie unter Homepage in Arbeitsbereich des Schwachstellenmanagers.

Hinweis:
Ab v21.0 von Vulnerability Response, Die Überwachungsthemen werden auf der Seite „Überwachungsthemen“ angezeigt.

Seite „Überwachungsthemen“

Besteht aus einer Liste von Überwachungsthemen, die in vier Module kategorisiert sind – Host-Schwachstellen, Anwendungsschwachstellen, Container-Schwachstellen und Konfigurationstestergebnisse.

Weitere Informationen zu Überwachungsthemen finden Sie unter Seite „Überwachungsthemen“ in Arbeitsbereich des Schwachstellenmanagers.

Seite „Dashboards“

Besteht aus den Dashboards Vulnerability Management, Vulnerability Management (PA), Vulnerability Approvals, CISO, Container Vulnerability Management Overview, Application Vulnerability Management, Unified Vulnerability Response und Health.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Seite „Dashboards“ in Arbeitsbereich des Schwachstellenmanagers.

Hinweis:
Die Seite „Dashboards“ wird ab Version 19,0 von angezeigt Vulnerability Response.

Listen-Seite

Besteht aus den standardmäßigen und anwenderdefinierten Listenseiten für Korrekturmaßnahmen, Korrekturaufgaben, angreifbare Host-Elemente, angreifbare Anwendungselemente, angreifbare Container-Elemente, Konfigurationstestergebnisse, Ausnahmen, Genehmigungen und Bibliotheken.

Weitere Informationen finden Sie unter Listenseite in Arbeitsbereich des Schwachstellenmanagers.

Homepage in Arbeitsbereich des Schwachstellenmanagers

Die Homepage in Arbeitsbereich des Schwachstellenmanagers Bietet eine Zusammenfassung der aktiven Datensätze, indem Visualisierungen der Risikobewertung, des Korrekturfortschritts, Zuweisungen an Zuweisungsgruppen, Datensätze in Korrekturaufgaben und Schwachstellen aus Cloud-Ressourcen angezeigt werden.

Auf der Homepage können Sie die Visualisierungen für die vorgefilterten angreifbaren Host-Elemente, angreifbaren Container-Elemente, angreifbaren Anwendungselemente und Konfigurationstestergebnisse anzeigen. Sie können auch Visualisierungen für eine Reihe gewünschter Datensätze anzeigen, indem Sie Filter erstellen und anwenden. Weitere Informationen zum Erstellen, Aktualisieren, Anwenden und Löschen von Filtern finden Sie unter Filter für die Zusammenfassung aktiver Datensätze erstellen und anwenden (Vits, AVITs, CVITs und CTRs).

Tipp:

Wenn *sn_vul_cmn_ws.navigate_to_workspace*Systemeigenschaft ist auf festgelegt Wahr Vom -Administrator bei Auswahl der vordefinierten Filterlinks in den Modulen angreifbare Elemente, angreifbare Anwendungselemente, angreifbare Container-Elemente und Testergebnisse aus dem **Alle** Menü, werden diese Links im geöffnet Arbeitsbereich des Schwachstellenmanagers Startseite von mit automatischer Auswahl des entsprechenden gespeicherten Filters.

Beispiel: Wenn Sie auswählen **Hohes Risiko** Indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Angreifbare Elemente**, Dieser Link wird zur Homepage von weitergeleitet Arbeitsbereich des Schwachstellenmanagers Mit automatischer Auswahl von **Hohes Risiko** Filter auf der Registerkarte Host-Schwachstellen.

Auf der Homepage können Sie Folgendes ausführen:

- Führen Sie einen Drilldown zu den Daten durch, und zeigen Sie die Liste der Datensätze an, indem Sie auf die Visualisierungen klicken.
- Navigieren Sie zur Liste der aktiven Datensätze in der klassischen Anwenderoberfläche, indem Sie auswählen **Zeigen Sie die klassische Liste an** Link.
- Öffnen Sie die Liste der aktiven Datensätze in Arbeitsbereich des Schwachstellenmanagers Durch Auswahl der Anzahl der aktiven Datensätze neben **Anzeigen nach** Dropdown-Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktualisieren Sie die Visualisierungen, indem Sie auswählen **Aktualisieren Sie Den Ausgewählten Gespeicherten Filter** Symbol.
- Zeigen Sie die neuesten Informationen an, indem Sie auswählen **Aktualisieren** Option im Menü „drei Punkte“ in einem Widget.

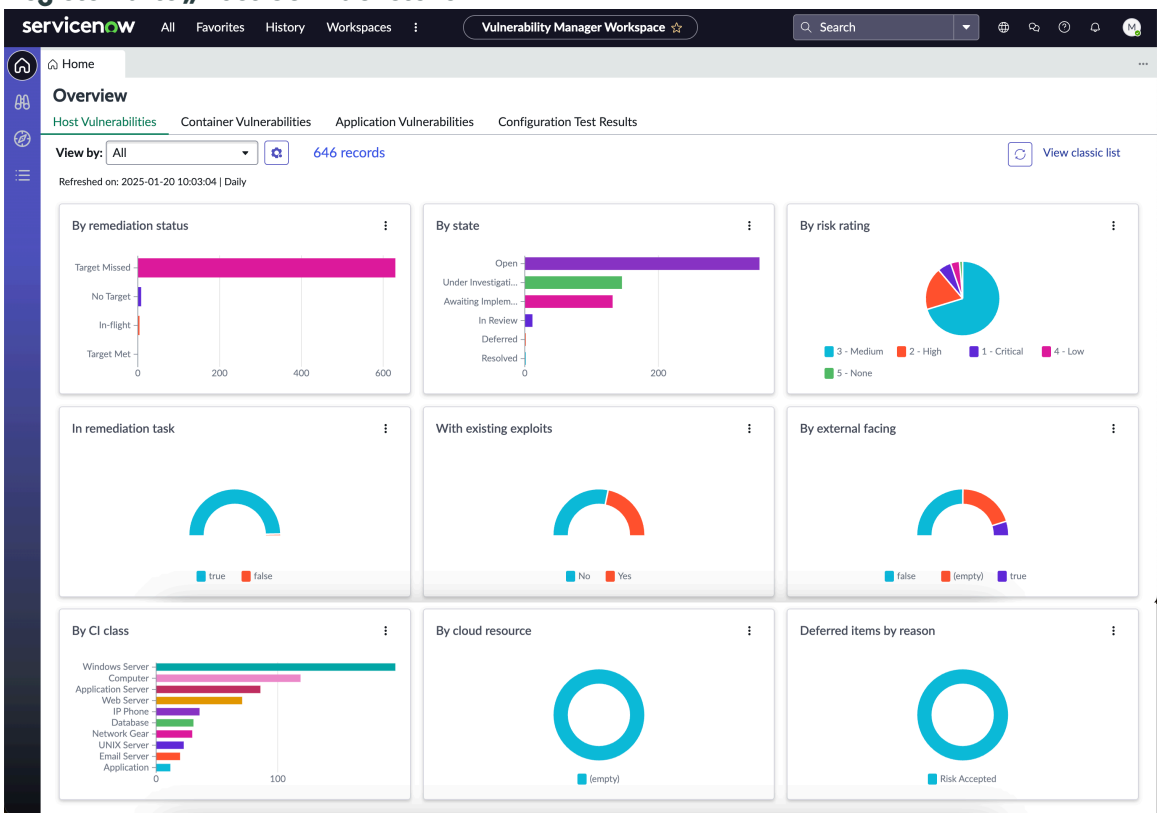
Host-Schwachstellen

Die **Host-Schwachstellen** Die Registerkarte enthält Visualisierungen, die eine allgemeine Zusammenfassung der aktiven Host-Schwachstellen bieten.

Erforderliche Rollen:

- sn_vul.Vulnerability_Analyst und sn_vul.Vulnerability_admin, um die Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- Granulare Rolle sn_vul.read_all zum Anzeigen der Visualisierungen durch Anwenden von Filtern.

Registerkarte „Host-Schwachstellen“



Die folgende Tabelle beschreibt die Visualisierungen auf der Registerkarte Host-Schwachstellen auf der Homepage. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze abzurufen.

Visualisierungen auf der Registerkarte Host-Schwachstellen auf der Homepage

Visualisierung	Typ	Beschreibung
Nach Zuweisungsgruppe und Korrekturstatus	Verteilungsleiste	Aktive Datensätze, die verschiedenen Zuweisungsgruppen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen auf der Registerkarte Host-Schwachstellen auf der Homepage (Fortsetzung)

Visualisierung	Typ	Beschreibung
		zugewiesen sind, die nach Korrekturstatus gruppiert sind.
nach Status	Balkendiagramm	Aktive Datensätze kategorisiert nach verschiedenen status (Offen, wird untersucht, wartet auf Implementierung, wird überprüft, gelöst, und zurückgestellt).
Nach Risikobewertung	Kreisdiagramm	Aktive Datensätze kategorisiert nach Risikobewertung (1 – Kritisch, 2 – hoch, 3 – Mittel, 4 – Niedrig und 5 – keine)
In Korrekturaufgabe	Halbring	Aktive Datensätze, die nicht Teil der Korrekturaufgabe sind und sind.
Mit vorhandenen Exploits	Halbring	Aktive Datensätze mit und ohne bekannte Exploits.
Nach externer Ausrichtung	Halbring	Aktive Datensätze, kategorisiert nach dem Asset-Risiko im Internet.
Nach CI-Klasse	Balkendiagramm	Aktive Datensätze, kategorisiert nach CI-Klassen.
Nach Cloud-Ressource	Ringdiagramm	Aktive Datensätze, kategorisiert nach verschiedenen Cloud-Ressourcen.
Zurückgestellte Elemente nach Grund	Ringdiagramm	Aktive zurückgestellte Datensätze gruppiert nach Grund.

Container-Schwachstellen

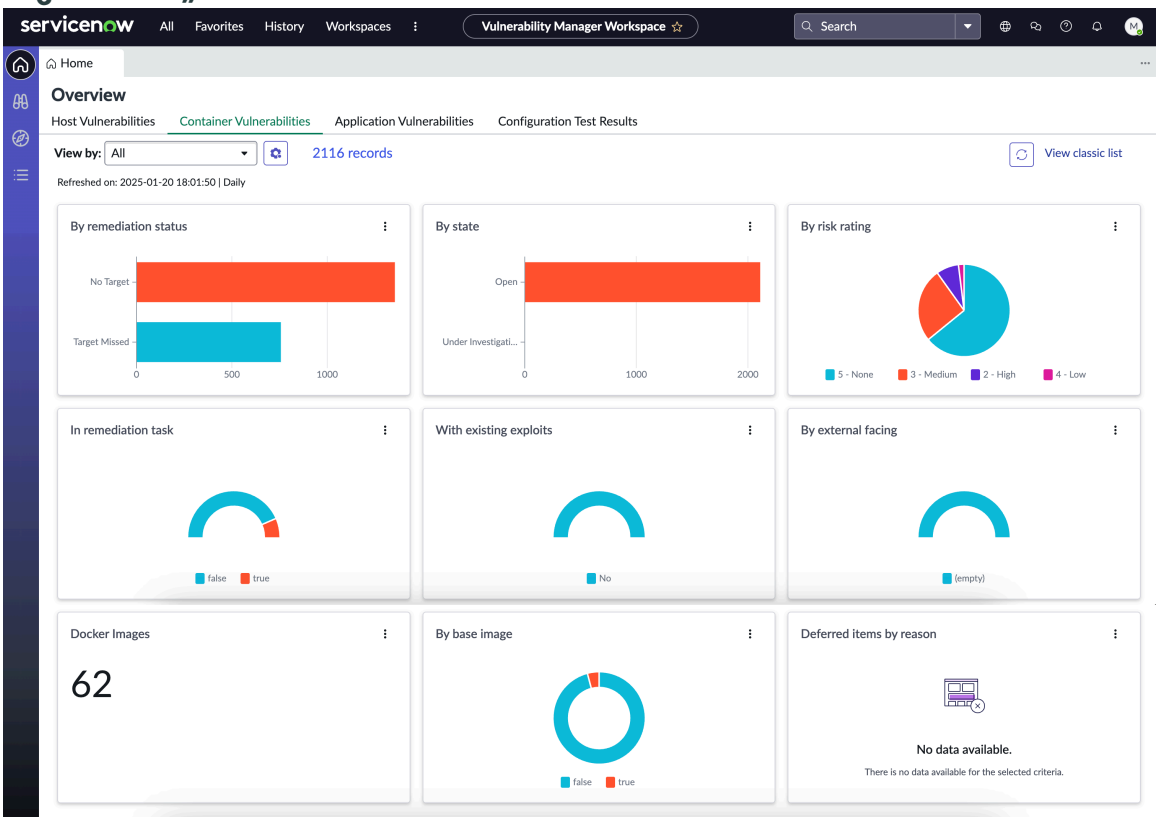
Die **Container-Schwachstellen** Die Registerkarte enthält Visualisierungen, die eine allgemeine Zusammenfassung der aktiven angreifbaren Container-Elemente bereitstellen.

Erforderliche Rollen:

- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin, um die Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- Granulare Rolle sn_vul_Container.read_all zum Anzeigen der Visualisierungen durch Anwenden von Filtern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Container-Schwachstellen“



Die folgende Tabelle beschreibt die Visualisierungen auf der Registerkarte Host-Schwachstellen auf der Homepage. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze abzurufen.

Visualisierungen auf der Registerkarte Container-Schwachstellen auf der Homepage

Visualisierung	Typ	Beschreibung
Nach Zuweisungsgruppe und Korrekturstatus	Verteilungsleiste	Aktive Datensätze, die verschiedenen Zuweisungsgruppen zugewiesen sind, die nach Korrekturstatus gruppiert sind.
nach Status	Balkendiagramm	Aktive Datensätze kategorisiert nach verschiedenen status (Offen, wird untersucht, wartet auf Implementierung, wird überprüft, gelöst, und zurückgestellt).
Nach Risikobewertung	Kreisdiagramm	Aktive Datensätze kategorisiert nach Risikobewertung (1 – Kritisch, 2 – hoch, 3 – Mittel, 4 – Niedrig und 5 – keine)
In Korrekturaufgabe	Halbring	Aktive Datensätze, die nicht Teil der Korrekturaufgabe sind und sind.
Mit vorhandenen Exploits	Halbring	Aktive Datensätze mit und ohne bekannte Exploits.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen auf der Registerkarte Container-Schwachstellen auf der Homepage (Fortsetzung)

Visualisierung	Typ	Beschreibung
Nach externer Ausrichtung	Halbring	Aktive Datensätze, kategorisiert nach dem Asset-Risiko im Internet.
Docker-Images	Anzahl	Anzahl der eindeutigen Docker-Images.
Nach Basis-Image	Ringdiagramm	Aktive Datensätze, kategorisiert nach dem Typ des Bilds.
Zurückgestellte Elemente nach Grund	Ringdiagramm	Aktive zurückgestellte Datensätze gruppiert nach Grund.

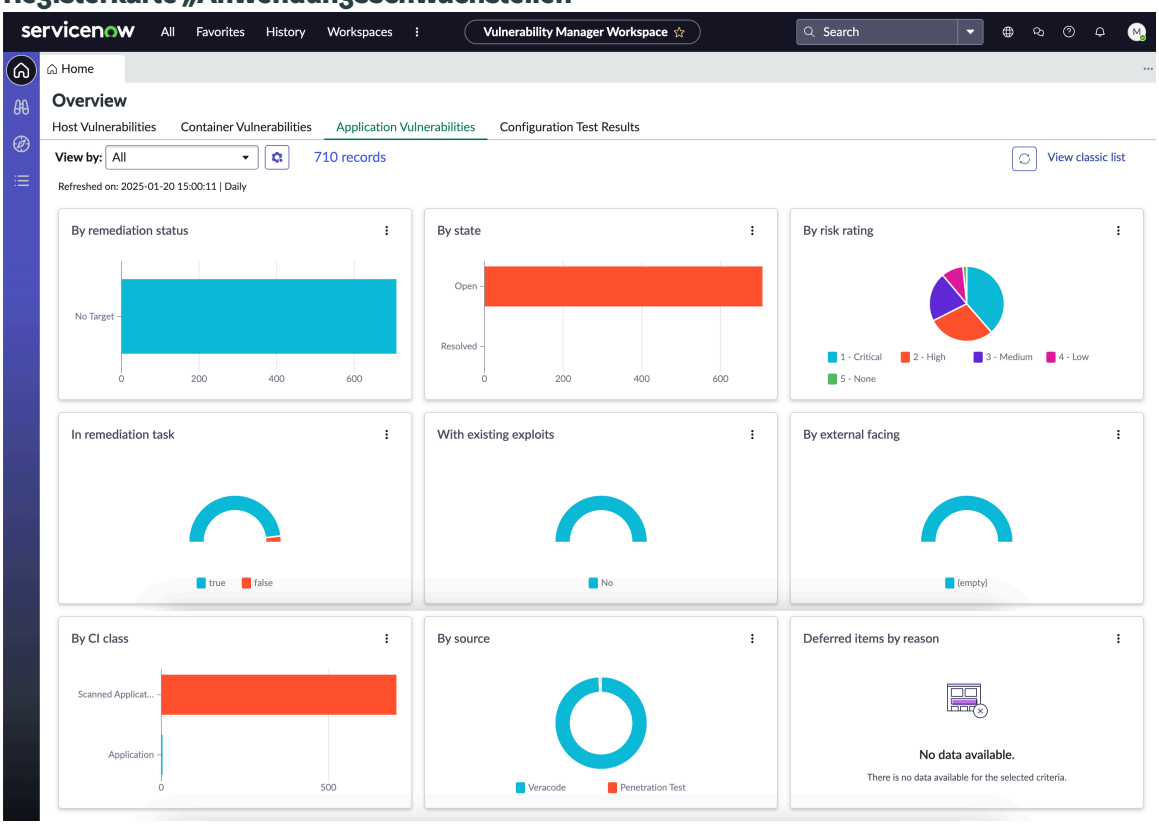
Anwendungsschwachstellen

Die **Anwendungsschwachstellen** Die Registerkarte enthält Visualisierungen, die eine allgemeine Zusammenfassung der Anwendungsschwachstellen bieten.

Erforderliche Rollen:

- sn_vul.App_sec_Manager, um die Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- Granulare Rolle sn_vul.App_read_all zum Anzeigen der Visualisierungen durch Anwenden von Filtern.

Registerkarte „Anwendungsschwachstellen“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Tabelle beschreibt die Visualisierungen auf der Registerkarte Host-Schwachstellen auf der Homepage. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze abzurufen.

Visualisierungen auf der Registerkarte Anwendungsschwachstellen auf der Homepage

Visualisierung	Typ	Beschreibung
Nach Zuweisungsgruppe und Korrekturstatus	Verteilungsleiste	Aktive Datensätze, die verschiedenen Zuweisungsgruppen zugewiesen sind, die nach Korrekturstatus gruppiert sind.
nach Status	Balkendiagramm	Aktive Datensätze kategorisiert nach verschiedenen status (Offen, wird untersucht, wartet auf Implementierung, wird überprüft, gelöst, und zurückgestellt).
Nach Risikobewertung	Kreisdiagramm	Aktive Datensätze kategorisiert nach Risikobewertung (1 – Kritisch, 2 – hoch, 3 – Mittel, 4 – Niedrig und 5 – keine)
In Korrekturaufgabe	Halbring	Aktive Datensätze, die nicht Teil der Korrekturaufgabe sind und sind.
Mit vorhandenen Exploits	Halbring	Aktive Datensätze mit und ohne bekannte Exploits.
Nach externer Ausrichtung	Halbring	Aktive Datensätze, kategorisiert nach dem Asset-Risiko im Internet.
Nach CI-Klasse	Balkendiagramm	Aktive Datensätze, kategorisiert nach CI-Klassen.
Nach Cloud-Ressource	Ringdiagramm	Aktive Datensätze, kategorisiert nach verschiedenen Cloud-Ressourcen.
Zurückgestellte Elemente nach Grund	Ringdiagramm	Aktive zurückgestellte Datensätze gruppiert nach Grund.

Konfigurationstestergebnisse

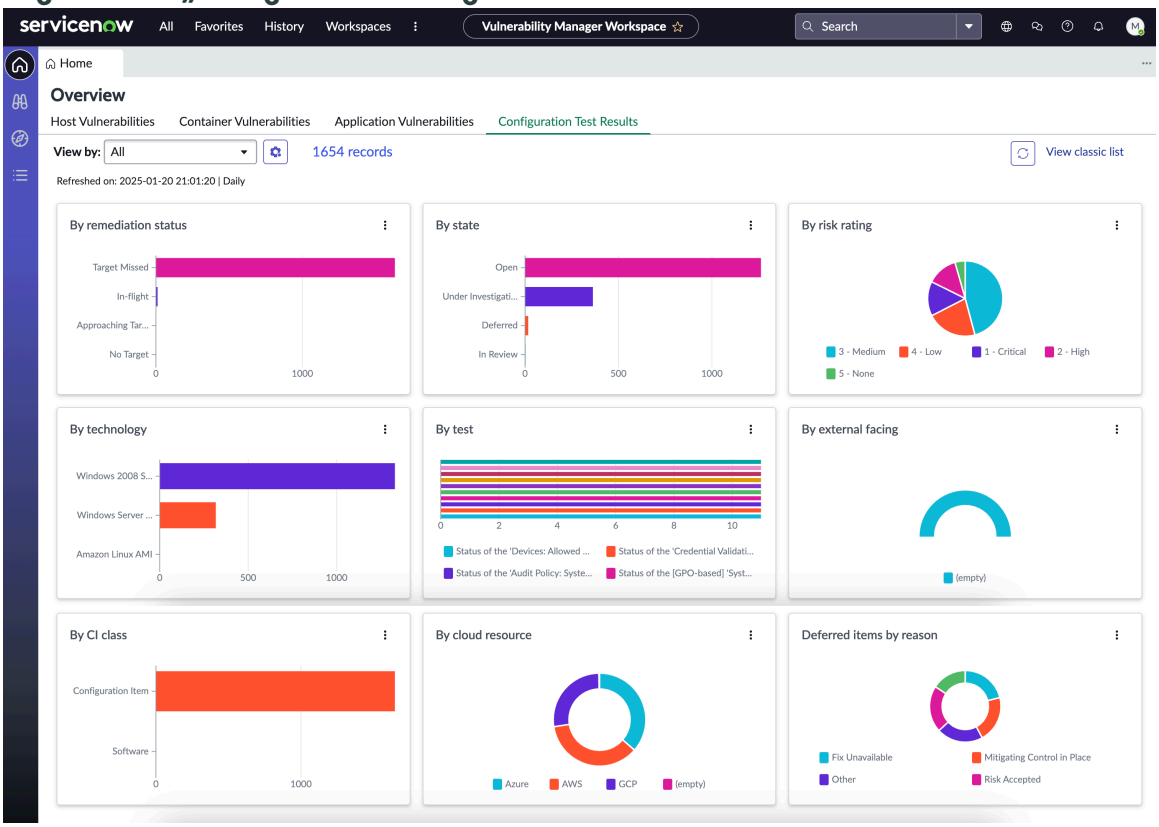
Die **Konfigurationstestergebnisse** Die Registerkarte enthält Visualisierungen, die eine allgemeine Zusammenfassung der aktiven Fehlkonfigurationen der Assets in Ihrer Organisation bieten.

Erforderliche Rollen:

- sn_vulc.admin, um die Visualisierungen durch Anwenden von Filtern anzuzeigen und Filter zu erstellen.
- sn_vulc.read granulare Rolle, um die Visualisierungen durch Anwenden von Filtern anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Konfigurationstestergebnisse“



Die folgende Tabelle beschreibt die Visualisierungen auf der Registerkarte Konfigurationstestergebnisse auf der Homepage. Wählen Sie diese Visualisierungen aus, um die Liste der entsprechenden Datensätze abzurufen.

Visualisierungen auf der Registerkarte Konfigurationstestergebnisse auf der Homepage

Visualisierung		Beschreibung
Nach Zuweisungsgruppe und Korrekturstatus	Verteilungsleiste	Aktive Datensätze, die verschiedenen Zuweisungsgruppen zugewiesen sind, die nach Korrekturstatus gruppiert sind.
nach Status	Balkendiagramm	Aktive Datensätze kategorisiert nach verschiedenen status (Offen, wird untersucht, wartet auf Implementierung, wird überprüft, gelöst, und zurückgestellt).
Nach Risikobewertung	Kreisdiagramm	Aktive Datensätze kategorisiert nach Risikobewertung (1 – Kritisch, 2 – hoch, 3 – Mittel, 4 – Niedrig und 5 – keine)
Durch Technologie	Balkendiagramm	Aktive Datensätze, kategorisiert nach Technologie.
Durch Test	Balkendiagramm	Aktive Datensätze, kategorisiert nach Tests.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visualisierungen auf der Registerkarte Konfigurationstestergebnisse auf der Homepage (Fortsetzung)

Visualisierung		Beschreibung
Nach externer Ausrichtung	Halbring	Aktive Datensätze, kategorisiert nach dem Asset-Risiko im Internet.
Nach CI-Klasse	Balkendiagramm	Aktive Datensätze, kategorisiert nach CI-Klassen.
Nach Cloud-Ressource	Ringdiagramm	Aktive Datensätze, kategorisiert nach verschiedenen Cloud-Ressourcen.
Zurückgestellte Elemente nach Grund	Ringdiagramm	Aktive zurückgestellte Datensätze gruppiert nach Grund.

Seite „Überwachungsthemen“ in Arbeitsbereich des Schwachstellenmanagers

Seite „Überwachungsthemen“ in Arbeitsbereich des Schwachstellenmanagers Ermöglicht Ihnen das Erstellen und Bearbeiten eines Überwachungsthemas. A *Überwachungsthema* Ist ein Satz von Datenvisualisierungen, mit denen Sie einen gefilterten Satz von Datensätzen (Vits, AVITs, CVITs und CTRs) im Laufe der Zeit in einem Dashboard überwachen können, die für Ihre Organisation von besonderem Interesse oder bestimmter Priorität sein könnten.

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Die in den Datenvisualisierungen in den Überwachungsthemen angezeigten Daten werden dynamisch aktualisiert, wenn sich Schwachstellendaten beim Import ändern. Verwenden Sie die Dashboards, um Trends, Umfang und Typen von Schwachstellen und Ihre Konfigurationselemente für das ausgewählte Überwachungsthema zu überwachen. Mit diesen Informationen können Sie bestimmen, wie sich die Schwachstellen in den einzelnen Überwachungsthemen auf Ihre Umgebung auswirken. Die Seite „Überwachungsthemen“ besteht aus vier Modulen – Host-Schwachstellen, Container-Schwachstellen, Anwendungsschwachstellen, Konfigurationstestergebnisse und Inaktiv. Weitere Informationen zu den Registerkarten „zugehörige Elemente“ und ihren Visualisierungen in einem Überwachungsthema finden Sie unter Liste der zugehörigen Elemente und Visualisierungen in einem Überwachungsthema.

Die folgenden Überwachungsthemen werden mit dem Basissystem im Modul Host-Schwachstellen auf der Seite „Überwachungsthemen“ bereitgestellt:

- Schwachstellen in externen Assets
- Schwachstellen mit verfügbaren Exploits
- Schwachstellen auf Windows-Servern
- Schwachstellen auf LINUX-Servern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Kritische Überfällige Schwachstellen
- Kritische Schwachstellen, die nicht in Korrekturaufgaben enthalten sind

Hinweis:
Wenn eine Datenvisualisierung zeigt, dass keine Datensätze für diese Kategorie vorhanden sind, Sie aber eine Liste von Datensätzen anzeigen können, wenn Sie auf das Diagrammsymbol klicken, überprüfen Sie die Spalte mit dem Namen des Überwachungsthemas in der angezeigten Liste. Überprüfen Sie, ob der Wert für alle Datensätze, die in der Spalte des Überwachungsthemas aufgeführt sind, z. B. mit Internetverbindung Falsch . Dieser Wert in diesem Beispiel gibt an, dass für dieses Überwachungsthema keine Datensätze mit Internetverbindung vorhanden sind.

Um die Korrektur zu starten oder wenn ein kritischer Bedarf für die Datensätze in einem Überwachungsthema besteht, können Sie einen erstellen *Korrekturmaßnahme* Aus einem Überwachungsthema. Weitere Informationen finden Sie unter Erstellen Sie eine Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers.

Zugehörige Informationen

Liste der zugehörigen Elemente und Visualisierungen in einem Überwachungsthema

Verwenden Überwachungsthemen in Arbeitsbereich des Schwachstellenmanagers

Erstellen Sie ein Überwachungsthema in Arbeitsbereich des Schwachstellenmanagers

Bearbeiten oder löschen Sie ein Überwachungsthema in Arbeitsbereich des Schwachstellenmanagers

Deaktivieren oder aktivieren Sie ein Überwachungsthema

Liste der zugehörigen Elemente und Visualisierungen in einem Überwachungsthema

Auf der Seite „Überwachungsthemen“ von Arbeitsbereich des Schwachstellenmanagers, Sie können Überwachungsthemen erstellen, die in vier Module kategorisiert sind: Host-Schwachstellen, Container-Schwachstellen, Anwendungsschwachstellen und Konfigurationstestergebnisse. Die Registerkarten „zugehörige Elemente“ in einem Überwachungsthema unterscheiden sich für jedes Modul.

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Der Navigationsbereich auf der Seite „Überwachungsthemen“ enthält die folgenden Module:

- Host-Schwachstellen: Zeigt die Überwachungsthemen an, die die angreifbaren Host-Elemente enthalten.
- Container-Schwachstellen: Zeigt die Überwachungsthemen an, die die angreifbaren Container-Elemente enthalten.
- Anwendungsschwachstellen: Zeigt die Überwachungsthemen an, die die angreifbaren Anwendungselemente enthalten.
- Konfigurationstestergebnisse: Zeigt die Überwachungsthemen an, die die Konfigurationselemente enthalten.
- Inaktiv: Zeigt die inaktiven Überwachungsthemen aus allen vier Modulen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Tabelle zeigt die Registerkarten für zugehörige Elemente, die für verschiedene Überwachungsthemenmodule verfügbar sind:

Überwachungsthema und zugehörige Elemente

Überwachungsthema	Registerkarten „zugehörige Elemente“
Host-Schwachstellen	Übersicht, betroffene CIs, eindeutige Schwachstellen und angreifbare Elemente
Container-Schwachstellen	Übersicht, betroffene CIs, eindeutige Schwachstellen und angreifbare Elemente
Anwendungsschwachstellen	Übersicht und angreifbare Elemente
Konfigurationstestergebnisse	Übersicht, betroffene CIs, eindeutige Konfigurationstests und Konfigurationstestergebnisse

Die folgende Tabelle enthält eine Beschreibung der Registerkarten „zugehörige Elemente“ und der Visualisierungen in einem Überwachungsthema.

Registerkarten für zugehörige Elemente und Visualisierung in einem Überwachungsthema

Registerkarte „zugehörige Elemente“ und Visualisierung	Beschreibung
Übersicht	
Aktive angreifbare Elemente im Zeitverlauf	Anzahl der aktiven angreifbaren Elemente (VIS) im Zeitverlauf. Sie können die Trends aus diesen Daten für die letzten 30 Tage überwachen. Sie Kann die Daten auch mithilfe von filtern Asset-Kategorie Filter.
VIs in Korrekturmaßnahmen	Anzahl der aktiven VIS von der Gesamtzahl der VIS, die sich bereits in den aktiven Korrekturmaßnahmen befinden.
Aktive Korrekturmaßnahmen	Liste der aktiven Korrekturmaßnahmen.
Betroffen CIs	
Eindeutige CIs	Anzahl der Konfigurationselemente (CIs) (Assets) betroffen von diesen Schwachstellen.
VIs pro CI-Klasse	Anzahl der angreifbaren Elemente (VIS) für jedes Configuration Management Database (CMDB) CI-Klasse. **Hinweis:** Dieses Widget wird nur für die Überwachungsthemen im Modul „Host-, Anwendungs- und Container-Schwachstellen“ angezeigt.
Konfigurationsprobleme pro CI-Klasse	Anzahl der CIs für jeden Configuration Management Database (CMDB) CI-Klasse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarten für zugehörige Elemente und Visualisierung in einem Überwachungsthema (Fortsetzung)

Registerkarte „zugehörige Elemente“ und Visualisierung	Beschreibung
	Hinweis: Dieses Widget wird nur für die Überwachungsthemen im Modul „Konfigurationsprobleme“ angezeigt.
VIs mit Internetzugriff	Anzahl der aktiven VIS von der Gesamtzahl der VIS für Ihre Assets, die mit dem Internet verbunden sind. **Hinweis:** Dieses Widget wird nur für die Überwachungsthemen im Modul „Host-, Anwendungs- und Container-Schwachstellen“ angezeigt.
Konfigurationsprobleme mit Internetzugriff	Anzahl der aktiven CIs von der Gesamtzahl der CIs für Ihre Assets, die mit dem Internet verbunden sind. **Hinweis:** Dieses Widget wird nur für die Überwachungsthemen im Modul „Konfigurationsprobleme“ angezeigt.
Eindeutige Schwachstellen	
VIs mit vorhandenen Exploits	Aktive VIS mit bekannten Exploits.
Eindeutige Schwachstellen	Anzahl der einzelnen, eindeutigen Schwachstellen, die Ihren Assets zugeordnet sind. Die eindeutigen Schwachstellen können basierend auf dem Problemtyp gefiltert werden.
VIs mit PCI-Schwachstellen	Anzahl der einzelnen, eindeutigen Assets, die aktive VIS mit Schwachstellen der Zahlungskartenbranche (Payment Card Industry, PCI) aufweisen.
Artikel mit Schwachstellen	
Angreifbare Host-Elemente	Liste aller angreifbaren Host-Elemente. Sie können diese Liste so filtern, dass nur die Datensätze angezeigt werden, die Sie anzeigen möchten. **Hinweis:** Diese Liste wird nur für die Überwachungsthemen im Modul „Host-Schwachstellen“ angezeigt.
Angreifbare Anwendungselemente	Liste aller angreifbaren Anwendungselemente. Sie können diese Liste so filtern, dass nur die Datensätze angezeigt werden, die Sie anzeigen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarten für zugehörige Elemente und Visualisierung in einem Überwachungsthema (Fortsetzung)

Registerkarte „zugehörige Elemente“ und Visualisierung	Beschreibung
	Hinweis: Diese Liste wird nur für die Überwachungsthemen im Modul „Anwendungsschwachstellen“ angezeigt.
Angreifbare Container-Elemente	Liste aller angreifbaren Container-Elemente. Sie können diese Liste filtern, um sie anzuzeigen, sodass nur die Datensätze angezeigt werden, die Sie anzeigen möchten. **Hinweis:** Diese Liste wird nur für die Überwachungsthemen im Modul „Container-Schwachstellen“ angezeigt.
Übersicht Registerkarte in einem Überwachungsthema im Modul Konfigurationstestergebnisse	
Aktive Konfigurationstestergebnisse im Zeitverlauf	Anzahl der aktiven Konfigurationstestergebnisse im Zeitverlauf. Sie können die Trends aus diesen Daten für die letzten 30 Tage überwachen.
Konfigurationstestergebnisse bei Korrekturmaßnahmen	Anzahl der aktiven Konfigurationstestergebnisse aus der Gesamtzahl der Datensätze, die sich bereits in den aktiven Korrekturmaßnahmen befinden.
Aktive Korrekturmaßnahmen	Liste der aktiven Korrekturmaßnahmen.
Eindeutige Konfigurationstests Registerkarte in einem Überwachungsthema im Modul Konfigurationstestergebnisse	
Konfigurationstestergebnisse über Testrelevanz	Konfigurationstestergebnisse, die auf der Relevanz der Probleme basieren.
Unterschiedliche Konfigurationstests	Anzahl eindeutiger Konfigurationstests.
Konfigurationstestergebnisse Registerkarte in einem Überwachungsthema im Modul Konfigurationstestergebnisse	Liste der Konfigurationstestergebnisse.

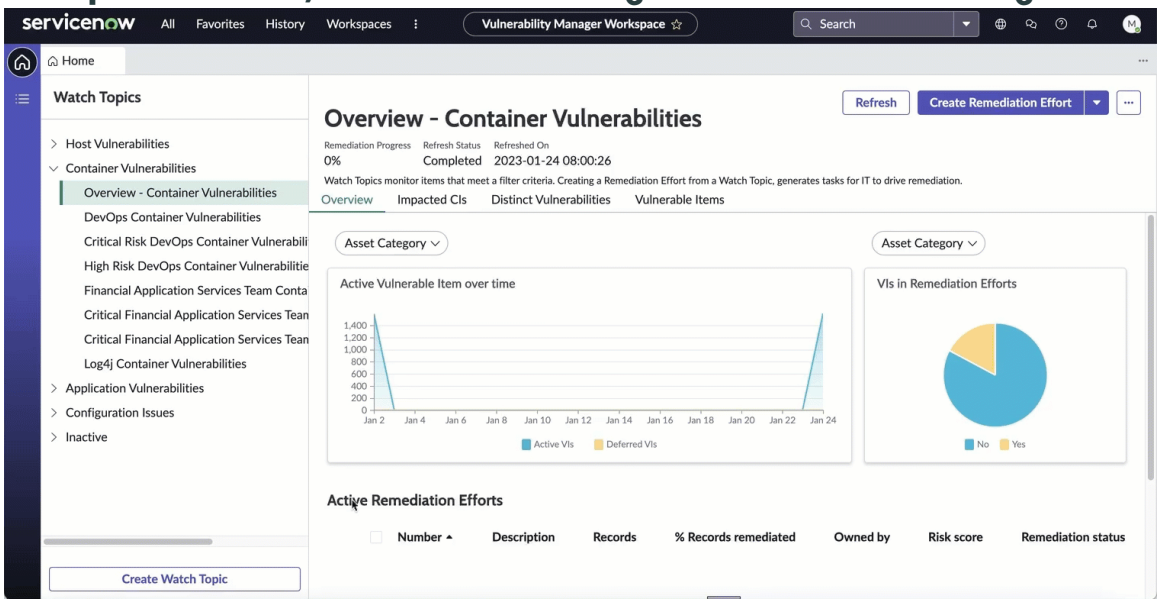
Sie können die neuesten Details zu einem Überwachungsthema abrufen, indem Sie auswählen **Aktualisieren** Schaltfläche. Der aktuelle Aktualisierungsstatus und der Zeitstempel werden unter dem Namen des Überwachungsthemas angezeigt. Wenn Sie ein Überwachungsthema aktualisieren, werden alle Details des Überwachungsthemas aktualisiert, einschließlich der Diagramme und Korrekturmaßnahmen. Ein Überwachungsthema wird automatisch aktualisiert, wenn es erstellt oder aktualisiert wird.

Hinweis:
Da Sie ein inaktives Überwachungsthema nicht aktualisieren können, ist **Aktualisieren** Die Schaltfläche ist für ein inaktives Überwachungsthema inaktiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie in einem der Widgets auf eine Datendarstellung, um zusätzliche Informationen zu den Datensätzen anzuzeigen.

Example: Version 18,0 Datenvisualisierungen in einem Überwachungsthema



Korrekturmaßnahmen in Arbeitsbereich des Schwachstellenmanagers

Eine Korrekturmaßnahme ist eine Reihe von Datensätzen, die einem Überwachungsthema zugeordnet sind. Die in einer Korrekturmaßnahme aufgeführten Datensätze sind statisch. Sie werden nicht durch neue Importdaten oder Änderungen aktualisiert, die Sie zur Überwachung von Themen vornehmen.

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Mit **Aktiv** Unter ausgewählt **Korrekturmaßnahmen** Liste Klicken Sie auf der Listenseite auf einen Link zur Korrekturmaßnahme, um ihn zu öffnen. Um die Korrekturmaßnahmen in angreifbare Host-Elemente (Vits), angreifbare Anwendungselemente (AVITs), angreifbare Container-Elemente (CVITs) und Konfigurationstestergebnisse (CTRs) zu kategorisieren, wählen Sie im das drei-Punkte-Menü aus **Datensatztyp** Spalte und wählen Sie dann aus **Nach Datensatztyp gruppieren** .

Die zugehörigen Listenelemente im Datensatz der Korrekturmaßnahme ermöglichen es Ihnen, den Gesamtfortschritt und den Status der Korrekturmaßnahme in den zugehörigen Datensätzen anzuzeigen.

- Auf der **Übersicht** Registerkarte die mit dieser Korrekturmaßnahme verknüpften Datensätze überwachen, die im Laufe der Zeit geschlossen wurden. Klicken Sie rechts neben dem Datensatz auf das Filtersymbol im Diagramm, um die auf die Datenvisualisierung angewendeten Filter anzuzeigen.
- Auf der **Details** Registerkarte Details zur Korrekturmaßnahme anzeigen, einschließlich des zugehörigen Überwachungsthemas und Status (aktiv oder inaktiv). Sie können eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturmaßnahme auf dieser Seite deaktivieren. Wenn Sie die Korrekturmaßnahme deaktivieren, bevor alle Datensätze geschlossen wurden, werden alle aktiven Datensätze verfügbar, um sie neuen Korrekturmaßnahmen hinzuzufügen.

- Auf der **Korrekturaufgaben** Registerkarte die Korrekturaufgaben anzeigen, die dieser Korrekturmaßnahme zugeordnet sind. Zeigen Sie den Prozentsatz der Datensätze an, die dieser Aufgabe zugeordnet sind und korrigiert werden.
- Auf der **Angreifbare Elemente** Registerkarte die Datensätze anzeigen, die dieser Korrekturmaßnahme zugeordnet sind. Wenn alle Datensätze in einer Korrekturaufgabe abgeschlossen und geschlossen sind, wechselt die Korrekturmaßnahme in „Inaktiv“. Wenn eine Korrekturmaßnahme inaktiv ist, können nicht alle geschlossenen Datensätze, die der Korrekturmaßnahme zugeordnet sind, zu neuen Korrekturmaßnahmen hinzugefügt werden.

Hinweis:
Die **Angreifbare Elemente** Die Registerkarte wird für die Korrekturmaßnahmen angezeigt, die Überwachungsthemen in den Modulen Host-Schwachstellen, Anwendungsschwachstellen und Container-Schwachstellen zugeordnet sind.

- Auf der **Konfigurationstestergebnisse** Registerkarte die Konfigurationstestergebnisse anzeigen, die der Korrekturmaßnahme zugeordnet sind. Wenn alle Datensätze in einer Korrekturaufgabe abgeschlossen und geschlossen sind, wechselt die Korrekturmaßnahme in „Inaktiv“. Wenn eine Korrekturmaßnahme inaktiv ist, können nicht alle geschlossenen Datensätze, die der Korrekturmaßnahme zugeordnet sind, zu neuen Korrekturmaßnahmen hinzugefügt werden.

Hinweis:
Die **Konfigurationstestergebnisse** Die Registerkarte wird für die Korrekturmaßnahmen angezeigt, die den Überwachungsthemen im Modul Konfigurationstestergebnisse zugeordnet sind.

Weitere Details und UI-Aktionen, die Sie aus einer Korrekturmaßnahme ausführen können, finden Sie unter Verwenden Sie Datensätze für Korrekturmaßnahmen.

Zugehörige Informationen

Lebenszyklen von Korrekturmaßnahmen, Korrekturaufgaben und Datensätzen in den Vulnerability Response-Arbeitsbereichen

Erstellen Sie eine Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers

Erstellen Sie eine Korrekturaufgabe bei Bedarf aus der Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers

Erstellen Sie eine wiederkehrende Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers

Übertragen Sie Datensätze an Korrekturmaßnahmen in der Arbeitsbereich des Schwachstellenmanagers

Lebenszyklen von Korrekturmaßnahmen, Korrekturaufgaben und Datensätzen in den Vulnerability Response-Arbeitsbereichen

Die status von Datensätzen und die zugehörigen Korrekturaufgaben (RTS) sind betroffen, wenn Datensätze zurückgestellt, gelöst, erneut geöffnet und an andere Korrekturmaßnahmen (RES) übertragen werden.

Erforderliche Rollen:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Korrekturmaßnahmen werden erstellt

Wie sich die status und Lebenszyklen von Korrekturmaßnahmen, Korrekturaufgaben und Datensätzen auswirken, hängt davon ab, wie eine Korrekturmaßnahme erstellt wird, wann sie erstellt wird und ob sie deaktiviert ist.

In der Liste oben rechts in einem Überwachungsthema können Sie eine Korrekturmaßnahme erstellen, indem Sie auf klicken **Erstellen Sie eine Korrekturmaßnahme** Oder **Erstellen Sie wiederkehrende Maßnahme** . Sie können eine wiederkehrende Korrekturmaßnahme pro Überwachungsthema erstellen. Wenn Sie eine wiederkehrende Korrekturmaßnahme erstellen, werden nachfolgende Korrekturmaßnahmen für das zugehörige Überwachungsthema automatisch basierend auf den von Ihnen festgelegten Kriterien erstellt. In beiden Fällen:

- Um die Korrektur zu erleichtern, werden den Korrekturmaßnahmen nur aktive Datensätze hinzugefügt.
- Alle Datensätze in neuen Korrekturmaßnahmen werden in neuen Korrekturaufgaben platziert. Datensätze können in mehreren Korrekturaufgaben vorhanden sein, einer Korrekturmaßnahme kann jedoch nur ein Datensatz zugeordnet werden.

Hinweis:
Eine Korrekturmaßnahme wird automatisch deaktiviert, wenn keine aktiven Datensätze vorhanden sind.

Datensätze werden übertragen oder Datensatzübertragung

Sie können Datensätze von einer Korrekturmaßnahme zu einer anderen übertragen, wenn Sie eine Korrekturmaßnahme erstellen, indem Sie auswählen **Übertragen Sie übereinstimmende Datensätze aus anderen aktiven Korrekturmaßnahmen** Kontrollkästchen. Weitere Informationen zum Übertragen der Datensätze finden Sie unter Übertragen Sie Datensätze an Korrekturmaßnahmen in der Arbeitsbereich des Schwachstellenmanagers. Wenn Datensätze von einer Korrekturmaßnahme übertragen oder in wiederkehrende Korrekturmaßnahmen übertragen werden:

Zu einer neuen Korrekturmaßnahme im selben Überwachungsthema

- Alle Korrekturaufgaben aus der alten Korrekturmaßnahme werden in die neue Korrekturmaßnahme verschoben.
- Neue Korrekturaufgaben werden basierend auf den ausgewählten Gruppierungskriterien für die Datensätze erstellt, die zuvor nicht Teil einer Korrekturaufgabe waren.
- Die alte Korrekturmaßnahme ist deaktiviert.

Zu einer neuen Korrekturmaßnahme in einem anderen Überwachungsthema

Alle Datensätze aus der alten Korrekturmaßnahme werden in die neue Korrekturmaßnahme verschoben, und Korrekturaufgaben werden basierend auf den ausgewählten Gruppierungskriterien erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn alle Datensätze in den Korrekturaufgaben übertragen werden, die der alten Korrekturmaßnahme zugeordnet sind, werden diese Korrekturaufgaben als abgebrochen geschlossen.
- Wenn nur eine Teilmenge von Datensätzen übertragen wird, werden die Korrekturaufgaben, die der alten Korrekturmaßnahme zugeordnet sind, aufgeteilt und bleiben aktiv.

Die geschlossenen Korrekturaufgaben, die der alten Korrekturmaßnahme zugeordnet sind, sind nicht betroffen.

Hinweis:
Sie können keine Datensätze aus wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Sie können jedoch Datensätze aus vorhandenen, nicht wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Siehe Übertragen Sie Datensätze an Korrekturmaßnahmen in der Arbeitsbereich des Schwachstellenmanagers Weitere Informationen zum Übertragen von Datensätzen.

Seite „Dashboards“ in Arbeitsbereich des Schwachstellenmanagers

Auf der Seite „Dashboards“ von Arbeitsbereich des Schwachstellenmanagers, Sie können die Dashboards in anzeigen Next Experience UI und verwenden Sie diese Dashboards, um die Schwachstellen nachzuverfolgen und zu analysieren.

Erforderliche Rollen:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Greifen Sie in auf die Dashboards zu Arbeitsbereich des Schwachstellenmanagers Indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** Und wählen Sie aus **Dashboards** Symbol. Das Standard-Dashboard wird basierend auf Ihrer Rolle angezeigt.

Die folgende Tabelle zeigt das Standard-Dashboard, das für eine bestimmte Rolle angezeigt wird.

Standard-Dashboard

Standard-Dashboard	Rolle
Einheitliches Dashboard	sn_vul_cmn_Vulnerability_admin oder sn_vul_cmn_Vulnerability_Analyst
Schwachstellen-PA-Dashboard	sn_vul_Vulnerability_admin oder sn_vul_Vulnerability_Analyst
Bewerbungsübersicht	sn_vul_App_sec_Manager
Containerübersicht	sn_vul_Container_Vulnerability_admin oder sn_vul_Container_Analyst

Sie können die folgenden Dashboards für die Aufgaben anzeigen, die Sie ausführen möchten, indem Sie sie aus der Dropdown-Liste auf der Dashboards-Seite auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboards in Arbeitsbereich des Schwachstellenmanagers

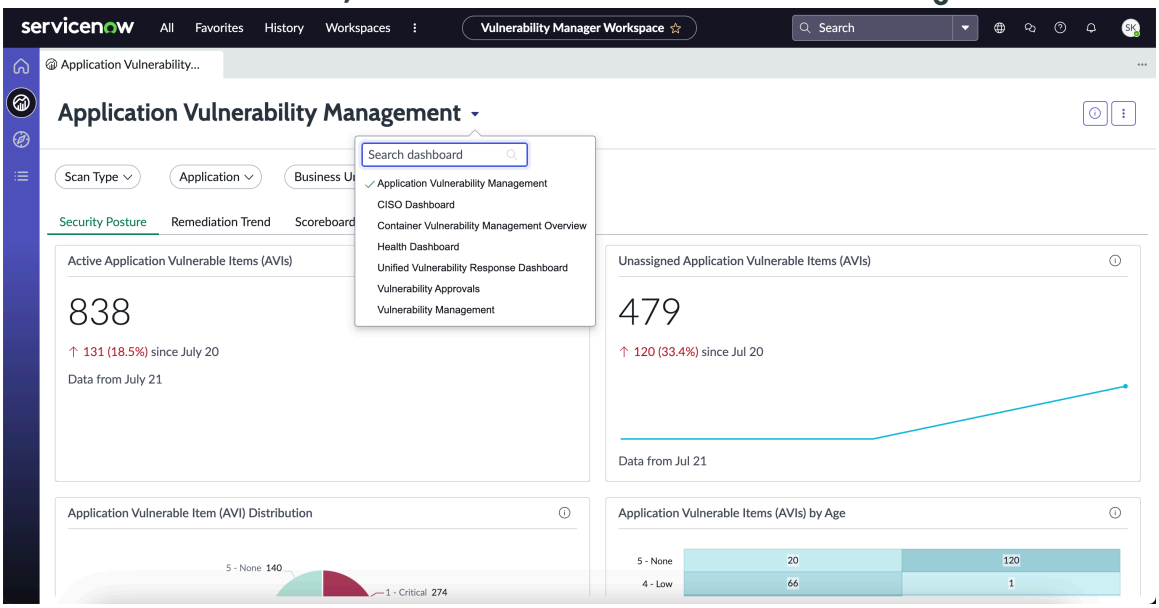
Dashboard	Beschreibung
Schwachstellenmanagement (PA)	Verfolgen Sie das Volumen, die Leistung und den Fortschritt der Host-Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur. Weitere Informationen finden Sie unter Vulnerability Management(PA) Dashboard.
Schwachstellengenehmigungen	Zeigen Sie die Anzahl der genehmigten, abgelehnten und ausstehenden Genehmigungsanforderungen an. Weitere Informationen finden Sie unter Wird standardmäßig verwendet Vulnerability Response Dashboards.
CISO-Dashboard	Zeigt die allgemeine Sicherheitslage Ihrer Organisation an, einschließlich der Sicherheitslücke und Incidents. Weitere Informationen finden Sie unter Vulnerability Management CISO Dashboard.
Container-Schwachstellenmanagement – Übersicht	Verfolgen Sie das Volumen, die Leistung und den Fortschritt der Container-Schwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur. Weitere Informationen finden Sie unter Container Vulnerability Response-Dashboard.
Dashboard Für Anwendungsschwachstellenmanagement	Verfolgen Sie das Volumen, die Leistung und den Fortschritt der Anwendungsschwachstellen von der ersten Analyse und Erkennung bis zur Eindämmung oder Korrektur. Weitere Informationen finden Sie unter Application Vulnerability Management (PA)-Dashboard
Einheitliches Vulnerability Response-Dashboard	Bietet Transparenz über mehrere Schwachstellen-Scanner und Sicherheitstools, um einen umfassenden Überblick über die Schwachstellen und Risiken einer Organisation zu erhalten. Weitere Informationen finden Sie unter Analytics- und Reporting-Lösungen für das Unified Vulnerability Response-Dashboard.
Vulnerability Response-Integritäts-Dashboard	Zeigt die Gesamtintegritätspunktzahl der Vulnerability Response-Anwendung an. Weitere Informationen finden Sie unter Dashboard „Integrität von SecOps Vulnerability Response“.

Die folgende Abbildung zeigt die Dashboards-Seite in Arbeitsbereich des Schwachstellenmanagers.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboards der Version 19,0 in Arbeitsbereich des Schwachstellenmanagers



Sie können auch ein anwenderdefiniertes Dashboard erstellen, indem Sie das Symbol „weitere Optionen“ auswählen ⋮ Und dann auswählen **Erstellen Sie ein neues Dashboard** .

Listenseite in Arbeitsbereich des Schwachstellenmanagers

Die Listenseite in Arbeitsbereich des Schwachstellenmanagers Ermöglicht Schwachstellen- und Sicherheitsmanagern und Analysten, den Korrekturfortschritt in Datensätzen anzuzeigen, Detailinformationen in Datensätzen anzuzeigen und den Status ihrer Genehmigungsanforderungen und Ausnahmen anzuzeigen.

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Diese Listen und Links bieten Ihnen einfachen Zugriff auf Datensätze und Aufgaben. Es enthält zwei Registerkarten:

- **Listen** Registerkarte: Zeigt die Standardlisten für Korrekturmaßnahmen, Korrekturaufgaben, angreifbare Elemente, Konfigurationstestergebnisse, Lösungen an Ausnahmen und Bibliotheken.
- **Meine Listen** Registerkarte: Zeigt alle Listen an, die Sie auf der Registerkarte Listen umbenannt haben, und alle von Ihnen erstellten Listen.

  Sie können auch eine eigene Liste erstellen, um den Korrekturfortschritt zu überwachen. Weitere Informationen finden Sie unter Erstellen Sie eine anwenderdefinierte Liste von Datensätzen.

Registerkarte „Listen“

Die folgende Tabelle zeigt die Listen, die auf der Registerkarte Listen der Listenseite verfügbar sind:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tipp:

Wenn *sn_vul_cmn_ws.navigate_to_workspace*Systemeigenschaft ist auf festgelegt Wahr Von einem Administrator bei Auswahl der vordefinierten Filterlinks in den Modulen Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response und Configuration Compliance aus dem **Alle** Menü, werden diese Links auf der Listenseite von geöffnet Arbeitsbereich des Schwachstellenmanagers Basierend auf Ihrer Rolle.

Beispiel: Wenn Sie auswählen **Meinen Gruppen zugewiesen** Indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**, Dieser Link wird zu weitergeleitet Arbeitsbereich des Schwachstellenmanagers. Die **Meinen Gruppen zugewiesen** Liste in **Korrekturaufgaben** Das Modul wird auf der Listenseite des Schwachstellenmanager-Arbeitsbereichs geöffnet, wenn Sie die Rolle „Schwachstellenadministrator“ oder „Analyst“ innehaben. Um die Host-Korrekturaufgaben anzuzeigen, gruppieren Sie die Aufgaben nach Datensatztyp.

Mit können Sie die Datensatzanzahl in den Listen ausblenden *glide.ui.list.seismic.omit.count*Systemeigenschaft. Weitere Informationen zum Deaktivieren/Aktivieren der Datensatzanzahl in einer Liste finden Sie unter KBB0010402 KB-artikel.

Listen

Listenelement	Beschreibung	Module	Erforderliche Rollen
Korrekturmaßnahmen (RES)	Liste der aktiven RES und aller Ihren Zuweisungsgruppen zugewiesenen RES. Gruppieren Sie die Korrekturmaßnahmen nach **Datensatztyp** Um sie nach angreifbaren Host-Elementen, angreifbaren Anwendungselementen, angreifbaren Containerelementen und Konfigurationstestergebnissen zu kategorisieren.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance	• sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits) • sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs) • sn_vul_Container.Vulnerability_Anal oder sn_vul_Container.Vulnerability_admi für angreifbare Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)
Korrekturaufgaben	Enthält die folgenden Listen: • Aktiv: Liste aller aktiven Host-, Anwendungs-, Container- und Testergebnis-Korrekturaufgaben.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance	• sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	• Alle: Liste der aktiven und inaktiven Host-, Anwendungs-, Container- und Testergebnis-Korrekturaufgaben. • Mir zugewiesen: Liste der Korrekturaufgaben, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Korrekturaufgaben, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind. Gruppieren Sie die Korrekturaufgaben nach **Datensatztyp** Um sie nach angreifbaren Host-Elementen, angreifbaren Anwendungselementen, angreifbaren Containerelementen und Konfigurationstestergebnissen zu kategorisieren.		• sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs) • sn_vul_Container.Vulnerability_Anal oder sn_vul_Container.Vulnerability_admi für angreifbare Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	Hinweis: Die Liste „Korrekturaufgaben“ enthält Aufgaben, die während der Erstellung der Korrekturmaßnahme in generiert wurden Arbeitsbereich des Schwachstellenmanagers, Sowie die manuell und durch Regeln für Korrekturaufgaben und andere Prozesse in der klassischen Anwenderoberfläche erstellten. Die Spalte „Korrekturmaßnahme“ ist für alle Korrekturaufgaben leer, die nicht im Rahmen der Korrekturmaßnahme erstellt wurden.		
Angreifbare Host-Elemente	Enthält die folgenden Listen • Aktiv: Liste aller aktiven angreifbaren Host-Elemente. • Alle: Liste der aktiven und inaktiven angreifbaren Host-Elemente. • Mir zugewiesen: Liste der angreifbaren Host-Elemente, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Liste der angreifbaren Host-Elemente, die Ihren	Vulnerability Response	sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	Zuweisungsgruppen zur Korrektur zugewiesen sind.		
Angreifbare Anwendungselemente	Enthält die folgenden Listen: • Aktiv: Liste aller aktiven angreifbaren Anwendungselemente. • Alle: Liste der aktiven und inaktiven angreifbaren Anwendungselemente. • Mir zugewiesen: Liste der angreifbaren Anwendungselemente, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Liste der angreifbaren Anwendungselemente, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind. Sie können ein neues angreifbares Anwendungselement erstellen, indem Sie auswählen **Neu** Schaltfläche.	Application Vulnerability Response	sn_vul.App_sec_Manager
Angreifbare Container-Elemente	Enthält die folgenden Listen: • Aktiv: Liste aller aktiven angreifbaren Container-Elemente. • Alle: Liste der aktiven und inaktiven angreifbaren	Container Vulnerability Response	sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	Container-Elemente. • Mir zugewiesen: Liste der angreifbaren Container-Elemente, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Liste der angreifbaren Container-Elemente, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind.		
Konfigurationstestergebnisse	Enthält die folgenden Listen: • Aktiv: Liste aller aktiven Testergebnisse. • Alle: Liste der aktiven und inaktiven Testergebnisse. • Mir zugewiesen: Liste der Testergebnisse, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Liste der Testergebnisse, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind.	Konfigurations-Compliance	sn_vulc.admin
Lösungen	Enthält die folgenden Listen: • Alle: Zeigt alle verfügbaren Lösungen an, mit denen Sie	Vulnerability Response	sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	die angreifbaren Host-Elemente korrigieren können. • Höchste Ersetzung: Zeigt alle Lösungen an, die zum Ausfüllen bevorzugter Lösungen verwendet werden. • Mit angreifbaren Elementen: Zeigt die Lösungen an, die als bevorzugte Lösung für angreifbare Elemente verwendet werden.		
Ausnahmen	Zeigt die genehmigungsstatus für alle Ausnahmen und falsch positiven Anforderungen an, die Ihren Zuweisungsgruppen zugeordnet sind. • Alle: Liste der Ausnahmeanforderungen, der falsch positiven Anforderungen und der Aufhebung der Zuweisung von Genehmigungen im Zusammenhang mit Vits, AVITs und CVITs und ihren Korrekturaufgaben (VUL, AVUL und CVUL). • Alle (Konfigurations-Compliance): Liste der Ausnahmen, falsch positiv und Zuweisung von Genehmigungsanforderungen im Zusammenhang mit Testergebnissen	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance	• sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits) • sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs) • sn_vul_Container.Vulnerability_Anal oder sn_vul_Container.Vulnerability_admi für angreifbare Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	und Korrekturaufgaben aufheben (CTR#). Gruppieren Sie die Ausnahmen nach **Datensatztyp** Um sie nach angreifbaren Host-Elementen, angreifbaren Anwendungselementen, angreifbaren Containerelementen und Konfigurationstestergebnissen zu kategorisieren.		
Genehmigungen	Mir zugewiesen: Zeigt die Genehmigungsanforderungen an, die Ihnen zur Verarbeitung zugewiesen sind. Informationen zur Verarbeitung Ihrer Genehmigungen im Arbeitsbereich finden Sie unter Genehmigen oder lehnen Sie Anforderungen in ab Arbeitsbereich des Schwachstellenmanagers.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance	• sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits) • sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs) • sn_vul_Container.Vulnerability_Anal oder sn_vul_Container.Vulnerability_admi für angreifbare Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)
Bibliotheken	Besteht aus den folgenden Listen: • CVEs (NVD): Liste aller Common Vulnerability and Exposures (CVEs) von Vulnerability Response, Application Vulnerability Response, Und Container Vulnerability Response.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance	• sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits) • sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs) • sn_vul_Container.Vulnerability_Anal oder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	• TPEs: Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste zugehöriger Referenzen, angreifbarer Elemente, Exploits und CVEs. • CWEs: Liste aller allgemeinen Schwachstellen-Aufzählungen (Common Schwachstellen Enumerations, CWEs) von Vulnerability Response, Application Vulnerability Response, Und Container Vulnerability Response. • App-Schwachstellen: Liste aller Einträge für Schwachstellen in Drittpartei-Anwendungen. • Testgruppen: Liste aller Konfigurations-Compliance Testgruppen. Sie können den Prozentsatz der CI-Compliance und der Compliance der Testergebnisse für eine Testgruppe in der Datensatzansicht anzeigen. • Tests: Liste aller Tests aus Konfigurations-Compliance. Sie können den Prozentsatz der		sn_vul_Container.Vulnerability_admi für angreifbare Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	Compliance der Testergebnisse für einen Test in der Datensatzansicht anzeigen. • Ausgleichssteuerungen: Liste aller Ausgleichssteuerungen, die für Risikoreduzierungsanforderungen verwendet werden können. Sie können eine Ausgleichssteuerung hinzufügen, indem Sie auf klicken **Neu** . Weitere Informationen zum Hinzufügen einer Ausgleichssteuerung finden Sie unter Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu.		
CMDB	Enthält die folgenden Listen • **Erkannte Elemente** : Liste aller erkannten Elemente. • **Erkannte Container-Images** : Liste der Container-Images. Diese Container-Images enthalten Informationen zur Image-ID, zum Docker-Image und zum Image-Repository zusammen mit den Ebeneninformationen. • **Tabelle „erkannte Anwendungen“** Der Ansicht „Vulnerability	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance	• sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits) • sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs) • sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs) • sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	Manager-Arbeitsbereich“ hinzugefügt. Ermöglicht die erneute Anwendung auf ausgewählte oder gefilterte erkannte Elemente oder Anwendungen im Arbeitsbereich.		
Anforderungen für Penetrationstestbewertung	Enthält die folgenden Listen: • **Aktiv** : Liste der aktiven Penetrationstestbewertungsanforderungen. • **Alle** : Liste der aktiven und inaktiven Penetrationstestbewertungsanforderungen • **Mir zugewiesen** : Liste der von Ihnen gestellten Penetrationstestbewertungsanforderungen. • **Meiner Gruppe zugewiesen** : Liste der Penetrationstestbewertungsanforderungen, die von den Anwendern in Ihren Zuweisungsgruppen gestellt wurden. Informationen zum Erstellen einer Penetrationstest-Bewertungsanforderung finden Sie unter Neue Anforderung für Penetrationstestbewertung erstellen.	Application Vulnerability Response	sn_vul.App_sec_Manager
Penetrationstest-Ergebnisse	Enthält die folgenden Listen:	Application Vulnerability Response	sn_vul.App_sec_Manager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	• Aktiv: Liste aller aktiven Penetrationstestergebnisse. • Alle: Liste der aktiven und inaktiven Penetrationstestergebnisse. • Mir zugewiesen: Liste der Penetrationstestergebnisse, die Ihnen zur Korrektur zugewiesen sind. • Meiner Gruppe zugewiesen: Liste der Penetrationstestergebnisse, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind. Informationen zum Erstellen von Penetrationstestergebnissen finden Sie unter Erstellen Sie Penetrationstestergebnisse basierend auf einem Bewertungsfragebogen.		
Patches	Alle: Liste aller verfügbaren Patches, die zur Korrektur angreifbarer Host-Elemente verwendet werden können.	Vulnerability Response	sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin
Unterstützungsdaten	Enthält die folgenden Listen: • **Autorisierende Quellen** : Liste der maßgeblichen Quellen, die Zusammenfassungsinformationen bereitstellen, die für die Recherche der Quellveröffentlichungen nützlich sind.	Konfigurations-Compliance	sn_vulc.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Module	Erforderliche Rollen
	• **Technologien** : Liste der Technologien, die Zusammenfassungsinformationen zu jeder autoritativen Quelle und Bezugsvermerk bereitstellen (auch in Qualys als Framework bekannt).		

Zugehörige Informationen

Verwenden Sie die Listenansicht in Arbeitsbereich des Schwachstellenmanagers

Massenbearbeitung in Arbeitsbereich des Schwachstellenmanagers

In Arbeitsbereich des Schwachstellenmanagers, Mit der Massenbearbeitungsfunktion können Sie mehrere angreifbare Elemente (Vits, AVITs oder CVITs) oder Konfigurationstestergebnisse (TRs) gleichzeitig aktualisieren und so den Verwaltungs- und Korrekturprozess optimieren.

Mit der Massenbearbeitung können Sie mehrere Schwachstellen auswählen und konsistente Änderungen anwenden, z. B. das Zuweisen von Korrekturbesitzern, das Aktualisieren des Status, das Hinzufügen von Arbeitsnotizen, das anfordern von Ausnahmen und das anfordern von falsch positiven Werten. Dies spart Zeit und Aufwand, da angreifbare Elemente nicht einzeln bearbeitet werden müssen, was ein effizientes und konsistentes Management von Schwachstellen fördert.

Die Massenbearbeitungsfunktion ist verfügbar für:

- Angreifbare Host-Elemente (Vits) ab v21.0 von Vulnerability Response.
- Angreifbare Anwendungselemente (AVITs) und angreifbare Container-Elemente (CVITs) ab v22.0 von Vulnerability Response.
- Testergebnisse (TRs) ab v23.0 von Vulnerability Response.

Erforderliche Rollen:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Sie können die folgenden Aufgaben mit der Massenbearbeitungsfunktion in ausführen Arbeitsbereich des Schwachstellenmanagers:

- Weisen Sie einer Zuweisungsgruppe Datensätze in Massenarbeit zu
- Fordern Sie eine Massenausnahme im Vulnerability Manager-Arbeitsbereich an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Entfernen Sie Zuweisungen für angreifbare Host-Elemente in Massen
- Massenbearbeitung für falsch positive Werte im Vulnerability Manager-Arbeitsbereich
- Schließen Sie Datensätze in einem Massenvorgang in Arbeitsbereich des Schwachstellenmanagers

Erläuterungen zu Ausgleichssteuerungen Zur Risikominderung

Ausgleichssteuerungen sind die Maßnahmen, die ergriffen werden, um das Risiko von Schwachstellen zu reduzieren, die nicht sofort gepatcht werden können. Sie können verwendet werden, um die Wahrscheinlichkeit oder die Auswirkungen eines erfolgreichen Exploits zu mindern.

Hinweis:
Die Funktion „Ausgleichssteuerungen“ ist nur für Host-Schwachstellen verfügbar.

Das Anwenden von Ausgleichssteuerungen kann dazu beitragen, das Risiko einer Schwachstelle zu reduzieren.

Die folgende Tabelle zeigt die Anwendungsfälle für Ausgleichssteuerungen:

Anwendungsfälle für Ausgleichssteuerungen

Anwendungsfall	Ausgleichssteuerung
Eine Schwachstelle in einem Webserver, die es Angreifern ermöglicht, beliebigen Code auszuführen.	Implementieren Sie eine Web Application Firewall (WAF), um schädliche Anforderungen an den Webserver zu blockieren.
Eine Schwachstelle in einem Betriebssystem, die es Angreifern ermöglicht, Berechtigungen an den Stamm zu eskalieren.	Implementieren Sie eine Anwendungssteuerung, um die Ausführung von Anwendungen auf dem Hostsystem einzuschränken.
Eine Schwachstelle in einem Datenbankserver, die Angreifern den Zugriff auf vertrauliche Daten ermöglicht.	Implementieren Sie die Netzwerksegmentierung, um den Datenbankserver von anderen Hosts und kritischen Systemen zu isolieren.

Weitere Informationen zu den Auswirkungen von Ausgleichssteuerungen auf die Risikopunktzahl eines angreifbaren Elements und die Korrekturaufgabe finden Sie unter Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum.

Zugehörige Informationen

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikoreduzierungsanforderungen zu

Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

Analytics- und Reporting-Lösungen für das Unified Vulnerability Response-Dashboard

Das einheitliche Vulnerability Response-Dashboard ist ein zentralisiertes aggregiertes Dashboard, das Transparenz aus mehreren Schwachstellen-Scannern und Sicherheitstools bietet, um einen umfassenden Überblick über die Schwachstellen und Risiken einer Organisation zu erhalten.

Erforderliche Rollen

Die folgenden Rollen und Aufgaben sind dieser Lösung zugeordnet. Sie sind zum Anzeigen und Freigeben der Berichte erforderlich:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul.App_sec_Manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_Container.Vulnerability_admin
- sn_vul_Container.Vulnerability_Analyst
- sn_vul.App_Developer
- sn_vulc.Vulnerability_Analyst

Einheitliches Vulnerability Response-Dashboard

Das Dashboard „Unified Vulnerability Response“ bietet einen umfassenden Überblick über die Schwachstellen und Risiken einer Organisation. Die Schwachstellen im Zusammenhang mit Infrastruktur, Cloud, Anwendungen und Containern können in einem zentralen Dashboard angezeigt werden, um die Transparenz und die Korrektur zu verbessern.

Sehen Sie sich dieses vierminütige Video an, um mehr über das einheitliche Vulnerability Response-Dashboard zu erfahren.

https://player.vimeo.com/video/1046083623?h=74c3349c9c&badge=0&autopause=0&player_id=0&app_id=58479

Erforderliche ServiceNow AI Platform-Rollen

Die folgenden Rollen sind dieser Lösung zugeordnet. Sie sind zum Anzeigen, Bearbeiten und Freigeben der Berichte erforderlich:

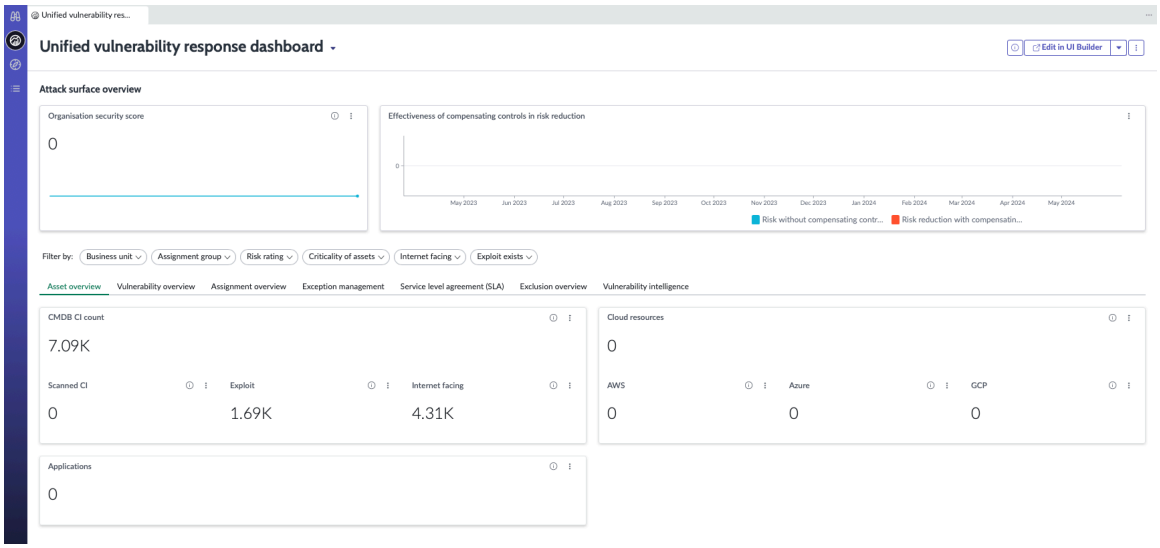
- sn_vul.App_sec_Manager
- sn_vul.vulnerability_admin
- sn_vul.vulnerability_analyst
- sn_vulc.admin
- sn_vul_Container.Vulnerability_admin
- sn_vul_Container.Vulnerability_Analyst
- sn_vul.App_Developer
- sn_vulc.Vulnerability_Analyst

Greifen Sie auf zu Einheitliches Vulnerability Response-Dashboard

Um das Dashboard zu öffnen, navigieren Sie zu einer der folgenden Optionen:

- **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers** Und wählen Sie aus **Dashboards** Symbol. Abhängig von Ihrer Rolle wird das Standard-Dashboard angezeigt. Um das einheitliche Vulnerability Response-Dashboard anzuzeigen, wählen Sie die Dropdown-Liste neben dem Dashboard-Namen aus.
- **Arbeitsbereiche** > **Platform Analytics-Arbeitsbereich** > **Dashboards** > **Einheitliches Vulnerability Response-Dashboard**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

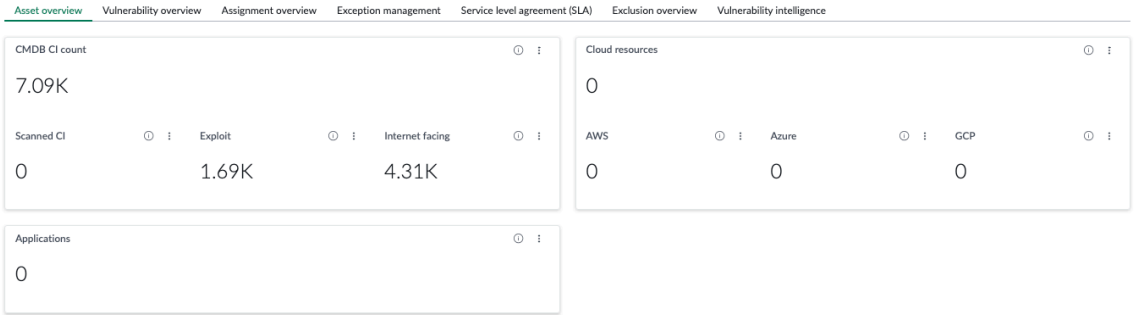
Anwender	Dashboard-Verwendung
• Schwachstellenmanager • Schwachstellenanalysten	• Bietet Echtzeittransparenz der Risiken in Infrastruktur, Anwendungen, Konfigurationen und Containern. Ermöglicht Schwachstellenmanagern und Schwachstellenanalysten, Schwachstellen zeitnah zu priorisieren und zu beheben. • Bietet eine Angriffsoberfläche – Übersicht über kritische Assets, die verwendet werden kann, um den Korrekturfortschritt und die Korrekturmaßnahmen nachzuverfolgen. • Bietet einen Überblick über Risiken in Geschäftsbereichen (Bus). Sie können Filter verwenden, um Bus auszuwählen und den Fortschritt zu vergleichen, um Ressourcen nach Bedarf neu zuzuweisen. Dem BU-Leiter muss Zugriff auf Rollenebene gewährt werden. • Bietet Einblick in die potenziellen Auswirkungen nach Bus. Sie können den Filter Common Vulnerability and Exposure (CVE) verwenden, um Risiken im gesamten Unternehmen zu identifizieren. • Bietet Einblick in die EPSS-Punktzahlen, die durch angreifbare Einträge erreicht werden, die im CISA-KEV-Katalog für angreifbare Anwendungs-, Host- und Container-Elemente vorhanden sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarten des Unified Vulnerability Response-Dashboards

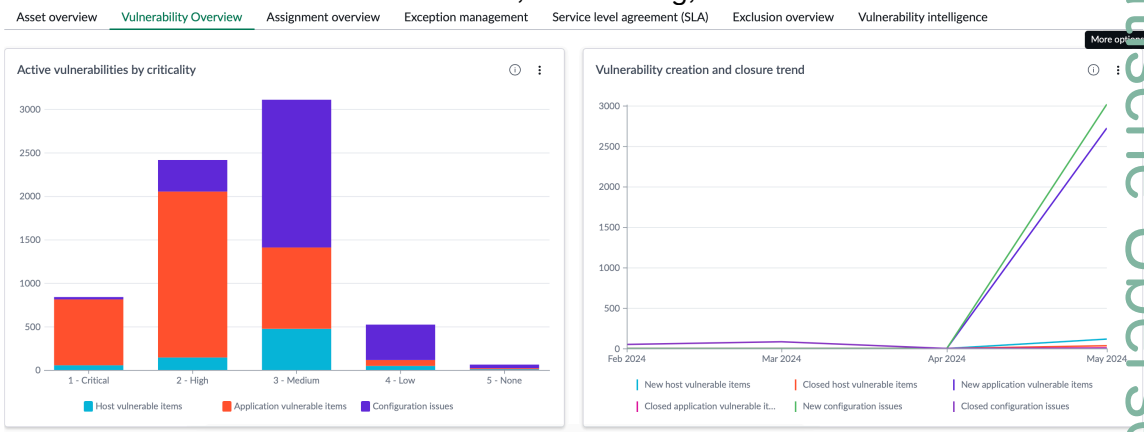
In diesem Dashboard können Sie die Schwachstellen oder Probleme anzeigen, die in Hosts, Cloud, Konfigurationen, Anwendungen und Containern vorhanden sind. Sie können die Schwachstellen basierend auf dem Geschäftsbereich, der Zuweisungsgruppe, der Risikobewertung, der Relevanz und dem Vorhandensein eines Exploits für die Schwachstellen anzeigen.

Die **Asset-Übersicht**Die Registerkarte stellt den Gesamtstatus von Konfigurationselementen (Configuration Items, CIs) im System



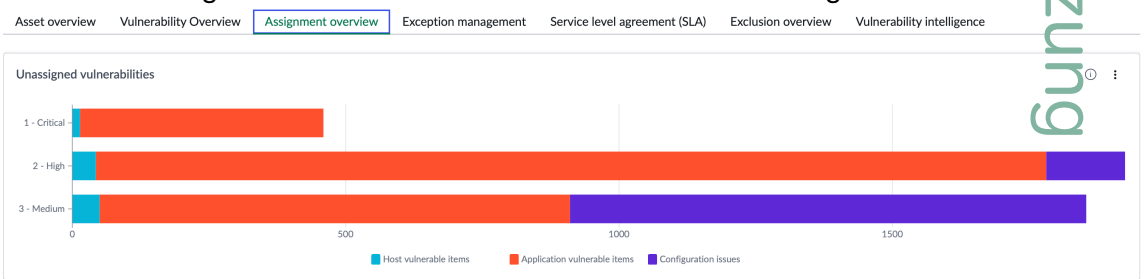
bereit.

Die **Schwachstellenübersicht**Die Registerkarte bietet einen Status für die Arten von Schwachstellen wie Host, Anwendung,



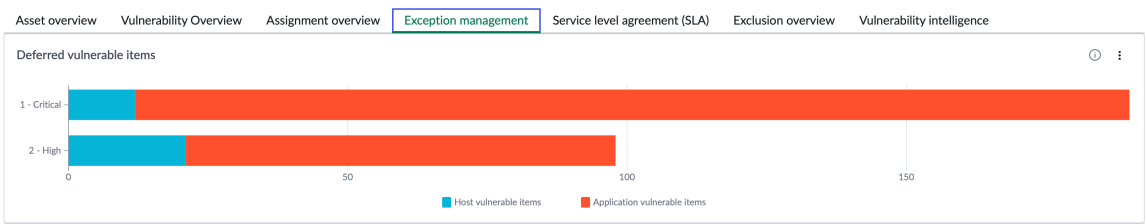
Container.

Die **Zuweisungsübersicht**Die Registerkarte bietet einen Status für die Zuweisung der



Schwachstellen.

Die **Ausnahmeverwaltung**Die Registerkarte stellt einen Status der zurückgestellten Schwachstellen



bereit.

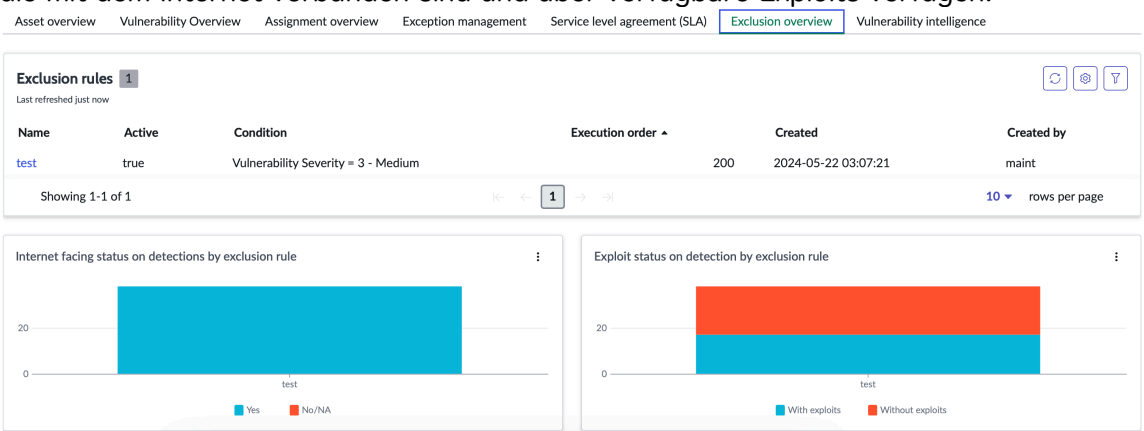
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

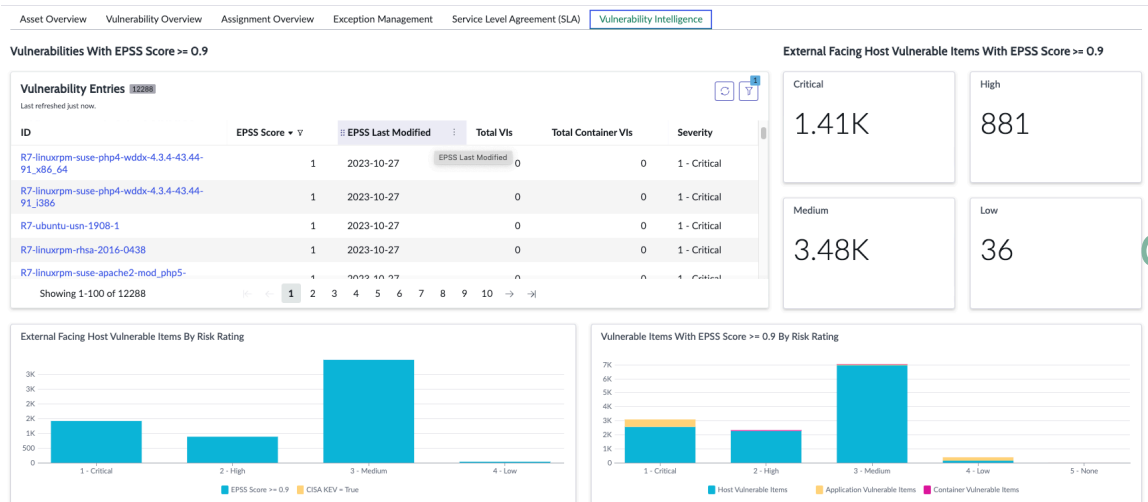
Die **Servicelevel-Vereinbarung (SLA)**Die Registerkarte bietet einen Status der Servicelevel-Vereinbarung, die von verschiedenen Zuweisungsgruppen erreicht

wurde.

Die **Ausschlussübersicht**Die Registerkarte enthält einen Status der von Ihnen erstellten Ausschlussregeln sowie diejenigen, die sich auf Erkennungen auswirken, die mit dem Internet verbunden sind und über verfügbare Exploits verfügen.



Die **Vulnerability Intelligence**Die Registerkarte bietet einen Status der EPSS-Punktzahlen, die durch Schwachstellen mit der CISA-KEV-Kennzeichnung „wahr“ und der EPSS-Punktzahl >= 0,9 für angreifbare Anwendungs-, Host- und Container-Elemente erreicht



werden.

Filter

Sie können die Widgets nach folgenden Kriterien filtern:

- Geschäftsbereich
- Zuweisungsgruppe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Risikobewertung
- Relevanz von Assets
- Mit Internetzugriff
- Exploit vorhanden

Wenn ein Filter ausgewählt ist, werden die Daten in allen Widgets aktualisiert. Wenn ein Filter jedoch nicht für ein Widget gilt, wird neben dem Filternamen ein Kreuzsymbol angezeigt.

Hinweis:
In sind nur Filter für Geschäftsbereich und Zuweisungsgruppe verfügbar Tokyo. Alle Filter sind in verfügbar Utah Ab.

Indikatoren

Gescannte Assets

Formelindikator für Assets, die in den letzten 60 Tagen gescannt wurden. Enthält gescannte erkannte Element-Assets, gescannte Anwendungsrelease-Assets und gescannte erkannte Container-Image-Assets als beitragende Indikatoren.

Assets – Exploit vorhanden

Formelindikator für Assets, bei denen Exploit in den Schwachstellen vorhanden ist. Enthält Host-Assets – Exploit vorhanden, Anwendungs-Assets – Exploit vorhanden, Container-Assets – Exploit ist als beitragende Indikatoren vorhanden.

Infra-Asset – mit Internetzugriff

Indikator zum Abrufen der Anzahl der Assets mit Internetzugriff.

Erkannte Elemente basierend auf Cloud-Ressourcentyp

Indikator zum Abrufen der Anzahl der Assets mit einer Asset-Kategorie wie „Cloud“.

Basis-Images

Indikator zum Abrufen der Anzahl der Basis-Images.

CISA-KEVs-Asset-Typ

Formelindikator, der die Anzahl der angreifbaren Container- und Host-Elemente angibt, bei denen für die Schwachstelle die Kennzeichnung „CISA KEV“ (BOD 22-01) auf „wahr“ festgelegt ist. Enthält „CISA vorhanden CVR“ und „CISA vorhanden“ als beitragende Indikatoren.

CISA vorhanden – angreifbare Elemente – nicht zugewiesen

Formelindikator, der die Anzahl der angreifbaren Container- und Host-Elemente angibt, bei denen für die Schwachstelle die Kennzeichnung CISA KEV (BOD 22-01) auf „wahr“ festgelegt ist und die Zuweisung der angreifbaren Elemente aufgehoben ist. Enthält nicht zugewiesene angreifbare Container-Elemente, nicht zugewiesenes angreifbares Host-Element als beitragende Indikatoren.

CISA vorhanden – Angreifbare Elemente – Ziel verfehlt

Formelindikator, der die Anzahl der angreifbaren Container- und Host-Elemente angibt, bei denen für die Schwachstelle die Kennzeichnung CISA KEV (BOD 22-01) auf „wahr“ festgelegt ist und die angreifbaren Elemente das Ziel verfehlt haben. Enthält „CISA vorhanden – angreifbare Elemente“, „CISA vorhanden – CVR“ als beitragende Indikatoren.

Aktive Host-VITs

Anzahl der aktiven angreifbaren Host-Elemente (Vits).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktive Anwendungs-VITs

Anzahl der aktiven angreifbaren Anwendungselemente (AVITs).

Aktive Container-VITs

Anzahl der aktiven angreifbaren Container-Elemente (CVITs).

Neue VITs

Anzahl der Vits, die an einem Tag geöffnet wurden.

Neue AVITs

Anzahl der AVITs, die an einem Tag geöffnet wurden.

Neue CVITs

Anzahl der CVITs, die an einem Tag geöffnet wurden.

Neue Testergebnisse

Anzahl der Testergebnisse (TRs), die an einem Tag erstellt wurden.

Geschlossene AVITs

Anzahl der an einem Tag geschlossenen Vits.

Geschlossene VITs

Anzahl der an einem Tag geschlossenen AVITs.

Geschlossene CVITs

Anzahl der an einem Tag geschlossenen CVITs.

Geschlossene Testergebnisse

Anzahl der an einem Tag geschlossenen TRs.

Offene Konfigurationsprobleme – Testergebnisse

Anzahl aller offenen Testergebnisse, die sich im Status „Fehlgeschlagen“ befinden.

Risikopunktzahl der Organisation

Risikopunktzahl einer Organisation aus der Tabelle „Risikopunktzahl der Rollup-Anwendung“.

Nicht zugewiesene angreifbare Anwendungselemente

AVITs ohne Zuweisungsgruppe oder Zugewiesen an.

Nicht zugewiesene angreifbare Host-Elemente

Vits ohne Zuweisungsgruppe oder „Zugewiesen an“.

Nicht zugewiesene angreifbare Container-Elemente

CVITs ohne Zuweisungsgruppe oder Zugewiesen an.

Nicht zugewiesene Konfigurationsprobleme

TRS ohne Zuweisungsgruppe oder Zugewiesen an.

Zurückgestellte VITs

Vits im Status „zurückgestellt“.

Zurückgestellte AVITs

AVITs im Status „zurückgestellt“.

Zurückgestellte CVITs

CVITs im Status „zurückgestellt“.

Host-SLA – Geschlossen

Durchschnittliches Alter der geschlossenen Vits.

Anwendungs-SLA – Geschlossen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durchschnittliches Alter der geschlossenen AVITs.

Container-SLA – Geschlossen

Durchschnittliches Alter geschlossener CVITs.

Testergebnis-SLA – Bestanden

Durchschnittliches geschlossenes Alter der bestandenen TRs.

Host-SLA – Geschlossen (Kritisch und Hoch)

Durchschnittliches Alter der geschlossenen Vits „Kritisch“ und „hoch“.

Anwendungs-SLA – Geschlossen (Kritisch und Hoch)

Durchschnittliches geschlossenes Alter kritischer und hoher AVITs.

Container-SLA – Geschlossen (Kritisch und Hoch)

Durchschnittliches Alter der geschlossenen kritischen und hohen CVITs.

Testergebnis-SLA – Bestanden (Kritisch und Hoch)

Durchschnittliches geschlossenes Alter der bestandenen kritischen und hohen TRs.

Aggregierte MTTR

Durchschnittliches Alter der geschlossenen Vits, AVITs, CVITs und TRs.

SLA verfehlt

Durchschnittliches Alter der geschlossenen und verpassten Vits, AVITs, CVITs und TRs.

Schwachstellen mit EPSS-Punktzahlen >= 0,9

Anzahl der Schwachstelleneinträge mit EPSS-Punktzahlen größer oder gleich 0,9.

Aufgliederungen

- VIT-Typ (einheitlich)
- Mit Internetzugriff (einheitlich)
- Risikobewertung (einheitlich)
- Exploit vorhanden (einheitlich)
- Erkanntes Element – Cloud-Ressourcentyp (einheitlich)
- CISA vorhanden (einheitlich)
- CMDB-Klasse (einheitlich)
- Geschäftsbereich (einheitlich)
- Business-Relevanz (einheitlich)
- Grund für Zurückstellung (einheitlich)
- Zuweisungsgruppe (einheitlich)
- Korrekturstatus (einheitlich)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenvisualisierungen

Registerkarte „Asset-Übersicht“

Titel	Typ	Beschreibung
Angriffsoberfläche – Übersicht	Einzelwert	Zahl, die die zusammengefasste Punktzahl der Sicherheit einer Organisation darstellt.
CMDB-CI-Anzahl	Einzelwert	Anzahl der CIs in der Organisation, die in registriert und nachverfolgt werden Configuration Management Database (CMDB). Stellt eine Aufgliederung der folgenden CIs bereit: • Gescannte CIs: Anzahl der gescannten CIs • Exploit: Anzahl der verfügbaren Exploits • Mit Internetzugriff: Anzahl der CIs mit Internetzugriff
Cloud-Ressource	Einzelwert	Anzahl der CIs mit Asset-Kategorie wie Cloud. Bietet eine Aufgliederung der folgenden Cloud-Assets: • AWS • Azure • GCP
Docker-Bild	Einzelwert	Anzahl der Docker-Images einschließlich der Anzahl der Basis-Images.

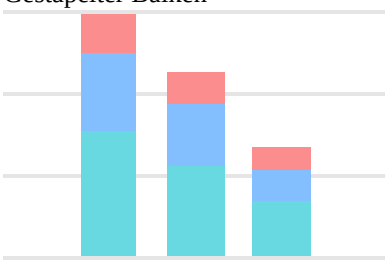
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Asset-Übersicht“ (Fortsetzung)

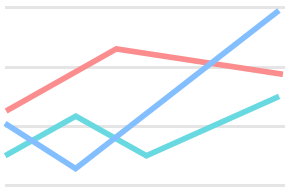
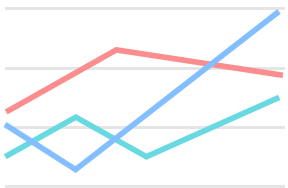
Titel	Typ	Beschreibung
Anwendungen	Einzelwert	Anzahl der Anwendungen in der Organisation.

Registerkarte „Schwachstellenübersicht“

Titel	Typ	Beschreibung
CISA-KEVs	Kreisdiagramm	Anzahl der Schwachstellen, die mit verknüpft sind CISA Kennzeichnung für Katalog und CISA als „wahr“. Bietet eine Aufgliederung basierend auf den folgenden Elementen: • CISA-Schwachstelle: Typen von Schwachstellen mit CISA-Kennzeichnung als „wahr“ • Host-CIs: Mit Internetzugriff: CIs mit Internetzugriff • Nicht zugewiesene Vits: Nicht zugewiesene Vits mit CISA-Kennzeichnung als „wahr“ • Vits – Ziel verfehlt: Vits, die das Ziel verfehlt haben, mit CISA-Kennzeichnung als „wahr“
Aktive Schwachstellen nach Relevanz	Gestapelter Balken 	Anzahl der aktiven Vits, AVITs und CVITs basierend auf Relevanz.

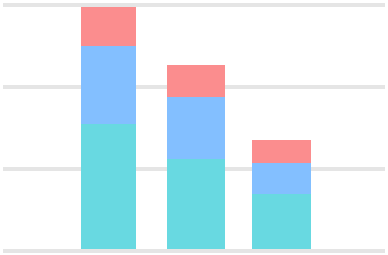
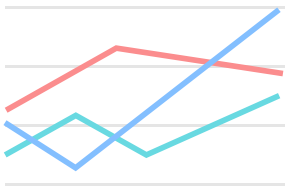
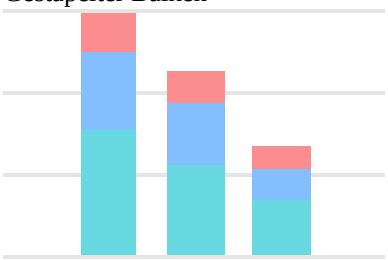
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Schwachstellenübersicht“ (Fortsetzung)

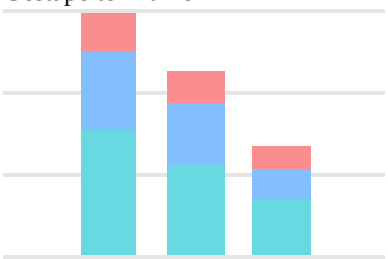
Titel	Typ	Beschreibung
Trend bei der Erstellung und Schließung von Schwachstellen	Mehrzeilig 	Anzahl der neuen und geschlossenen Schwachstellen für alle Anwendungen. Stellt einen Trend für die letzten drei Monate bereit.
Falsche Konfiguration nach Cloud-Plattform	Mehrzeilig 	Anzahl der Konfigurationsprobleme basierend auf der Risikobewertung für jedes Cloud-Asset.
Cloud-Compliance	Tabelle	Liste der Ressourcen mit der Asset-Kategorie „Cloud“ zusammen mit den folgenden Details: • Ressourcenname • Klasse • Schwachstellenprobleme: Anzahl der in der Ressource vorhandenen Probleme, die basierend auf der Risikobewertung aggregiert werden. • Konfigurationsprobleme: Anzahl der Ressourcen mit Konfigurationsproblemen zusammen mit der Risikobewertung. • Cloud-Account: Cloud-Account-ID. • Cloud-Region: Standort der Cloud-Ressourcen. • Cloud-Provider: Name des Cloud-Providers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Zuweisungsübersicht“

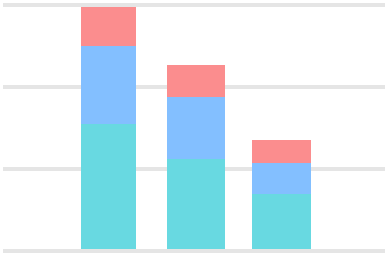
Titel	Typ	Beschreibung
Nicht zugewiesene VITs	Gestapelter Balken 	Anzahl der Schwachstellen, die keiner Gruppe oder Person zugewiesen sind, zusammen mit der Risikobewertung.
MTTR nach Zuweisungsgruppe – Top 10	Mehrzeilig 	Durchschnittliche Zeit, die eine Zuweisungsgruppe benötigt, um Sicherheitsschwachstellen oder -Probleme zu identifizieren und zu beheben. Es werden die Top 10 Zuweisungsgruppen angezeigt, die die höchste durchschnittliche Zeit für die Korrektur aufweisen.
Top-10-Zuweisungsgruppen ohne SLA (als „kritisch“ und „hoch“ eingestufte Schwachstelle)	Gestapelter Balken 	Top-10-Zuweisungsgruppen, die das Zieldatum der Korrektur kritischer und hoher Schwachstellen nicht eingehalten haben.

Registerkarte „Ausnahmeverwaltung“

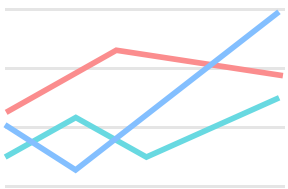
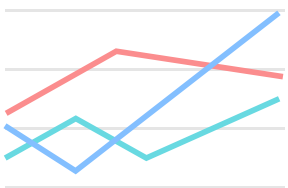
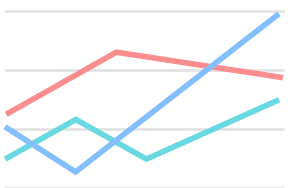
Titel	Typ	Beschreibung
Zurückgestellte VITs	Gestapelter Balken 	Anzahl der Schwachstellen im Status „zurückgestellt“ basierend auf der Risikobewertung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Ausnahmeverwaltung“ (Fortsetzung)

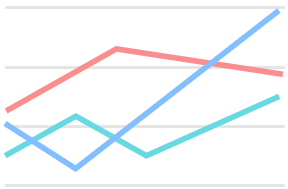
Titel	Typ	Beschreibung
Als „kritisch“ und „hoch“ eingestufte zurückgestellte VITs nach Zuweisungsgruppe	Gestapelter Balken 	Anzahl der Schwachstellen mit kritischen und hohen Risikobewertungen im Status „zurückgestellt“, die basierend auf den Zuweisungsgruppen kategorisiert wird.

Registerkarte „Servicelevel-Vereinbarung (SLA)“

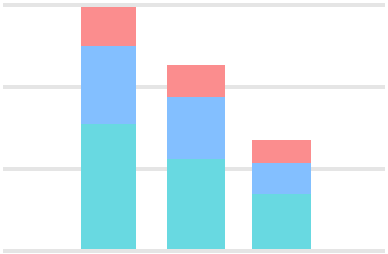
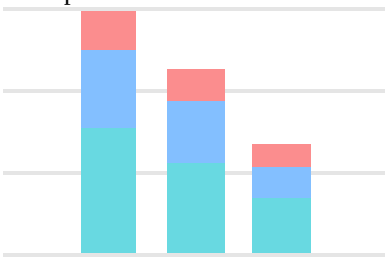
Titel	Typ	Beschreibung
Host-Schwachstelle: SLA-Erreichung nach Zuweisungsgruppe	Mehrzeilig 	Zeit, die eine Zuweisungsgruppe benötigt, um Host-Schwachstellen zu beheben. Stellt einen Trend für die letzten 10 Monate bereit.
Compliance-Probleme: SLA-Erreichung nach Zuweisungsgruppe	Mehrzeilig 	Zeit, die eine Zuweisungsgruppe benötigt, um Compliance-Probleme zu beheben. Stellt einen Trend für die letzten 10 Monate bereit.
Anwendungsschwachstelle: SLA-Erreichung nach Zuweisungsgruppe	Mehrzeilig 	Zeit, die eine Zuweisungsgruppe benötigt, um Anwendungsschwachstellen zu beheben. Stellt einen Trend für die letzten 10 Monate bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Servicelevel-Vereinbarung (SLA)“ (Fortsetzung)

Titel	Typ	Beschreibung
Container-Schwachstelle: SLA-Erreichung nach Zuweisungsgruppe	Mehrzeilig 	Zeit, die eine Zuweisungsgruppe benötigt, um Container-Schwachstellen zu beheben. Stellt einen Trend für die letzten 10 Monate bereit.

Registerkarte „Ausschlussübersicht“

Titel	Typ	Beschreibung
Ausschlussregeln	Tabelle	Liste aller von Ihnen erstellten Ausschlussregeln.
Ausschlussregeln im Vergleich zu Internetzugriff	Gestapelter Balken 	Ausschlussregeln, die sich auf Erkennungen auswirken, die zu Assets mit Internetzugriff gehören.
Ausschlussregeln vs/s Exploit vorhanden	Gestapelter Balken 	Ausschlussregeln, die sich auf Erkennungen auswirken, die für vorhandene Exploits angreifbar sind.

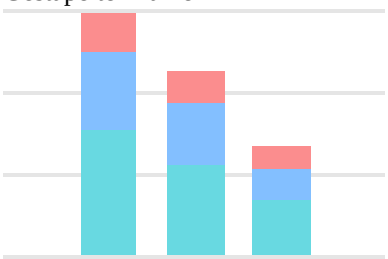
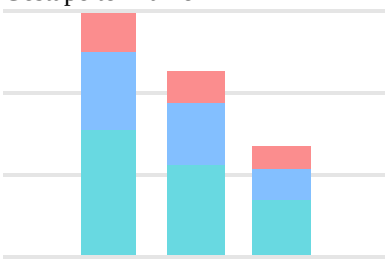
Registerkarte „Vulnerability Intelligence“

Titel	Typ	Beschreibung
Schwachstellen mit EPSS-Punktzahl>= 0,9	Tabelle	Vollständige Listenansicht aller angreifbaren Einträge (CVEs oder TPEs) mit einer EPSS-Punktzahl größer oder gleich 0,9 zusammen mit den folgenden Details. • ID: CVE-ID der Schwachstelle • EPSS-Punktzahl • EPSS – Zuletzt geändert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Vulnerability Intelligence“ (Fortsetzung)

Titel	Typ	Beschreibung
		• CISA-KEV-BOD 22-01: Gibt an, ob der Eintrag im CISA-KEV-BOD (Binding Operational Directive 22-01) vorhanden ist • Gesamtanzahl der VIS: Gesamtanzahl der VIS, die für diesen Schwachstelleneintrag vorhanden sind. • Container-VIS insgesamt: Gesamtanzahl der Container-VIS, die für diesen Schwachstelleneintrag vorhanden sind. • Schweregrad
Nach außen gerichtete angreifbare Host-Elemente mit einer EPSS-Punktzahl >= 0,9	Einzelwert 	Zahl, die die aggregierte Anzahl der externen angreifbaren Host-Elemente mit einer EPSS-Punktzahl größer oder gleich 0,9 angibt. Stellt einzelne Punktzahlen bereit, sortiert nach Schweregrad der Risikobewertung.
Nach außen gerichtete angreifbare Host-Elemente nach Risikobewertung	Gestapelter Balken 	Anzahl der nach außen gerichteten angreifbaren Host-Elemente nach Risikobewertung. Die Stapelbalken werden nach EPSS-Punktzahl >=0,9 und CISA KEV =wahr kategorisiert.
Angreifbare Elemente mit EPSS-Punktzahl >= 0,9 nach Risikobewertung	Gestapelter Balken 	Anzahl der Schwachstellen mit einer EPSS-Punktzahl größer oder gleich 0,9, sortiert nach Risikobewertung. Bietet eine Aufgliederung nach angreifbaren Host-Elementen, angreifbaren Anwendungselementen und angreifbaren Container-Elementen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgaben für die Datensammlung

Datensammlungsaufträge sammeln automatisch Punkte für automatisierte Indikatoren und Aufgliederungen. Die folgenden geplanten Aufgaben werden ausgeführt, um Punktzahlen für neue Daten automatisch zu erfassen.

Warnung:
Standardmäßig sind die folgenden Datensammlungsaufträge im Basissystem deaktiviert:

- Einheitliches Dashboard – Tägliche Datensammlung
- Einheitliches Dashboard – Wöchentliche Datensammlung
- Vereinheitlichtes Dashboard – Verlaufsdatensammlung

Lesen Sie vor dem Aktivieren der Aufträge nach KB .

Geplante Aufgabe	Häufigkeit	Beschreibung
Vereinheitlichtes Dashboard – Verlaufsdatensammlung	Einmal	Sammelt Punktzahlen und Snapshots für vorhandene Datensätze.
Einheitliches Dashboard – Wöchentliche Datensammlung	Wöchentlich	Erfasst wöchentlich Daten.
Einheitliches Dashboard – Tägliche Datensammlung	Täglich	Erfasst täglich Daten.
Rollup von Risikopunktzahlen an Organisation	Täglich	Sammelt die zusammengefasste Risikopunktzahl für eine Organisation.
Füllen Sie die tägliche Anzahl der Cloud-Compliance aus	Täglich	Sammelt Daten für Cloud-Compliance.
Täglicher EPSS-Auftrag	Täglich	Erfasst EPSS-Daten von First.org.

Eine neue Tabelle „Rollup-Anwendungsrisikopunktzahl“ [sn_vul_cmn_rollup_App_Risk_Score] wird im Bereich „Allgemeine Schwachstellen“ erstellt. Diese Tabelle wird täglich mit den folgenden Rollup-Rechnern über die geplanten Aufgaben ausgefüllt.

Name des Rollup-Rechners	Beschreibung
Rollup für Risikopunktzahl der Organisation	Fasst die Risikopunktzahlen für alle angreifbaren Elemente und Konfigurationsprobleme in einer Organisation zusammen. Sie stellt eine Gesamtrisikopunktzahl für eine Organisation bereit.
Rollup für angreifbare Elemente	Fasst die Risikopunktzahlen für alle angreifbaren Elemente in einer Organisation zusammen, um zur Gesamtrisikopunktzahl einer Organisation beizutragen.
Rollup für angreifbare Anwendungselemente	Fasst die Risikopunktzahlen für alle angreifbaren Anwendungselemente in einer Organisation zusammen, um zur Gesamtrisikopunktzahl einer Organisation beizutragen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name des Rollup-Rechners	Beschreibung
Rollup für angreifbare Container-Elemente	Fasst die Risikopunktzahlen für alle angreifbaren Container-Elemente in einer Organisation zusammen, um zur Gesamtrisikopunktzahl einer Organisation beizutragen.
Testergebnis-Rollup	Führt einen Rollup der Risikopunktzahlen für alle Testergebnisse in einer Organisation durch, um zur Gesamtrisikopunktzahl einer Organisation beizutragen.
Rollup von EPSS-Punktzahlen von NVDs zu TPEs	Rollup von EPSS-Punktzahlen von NVDs zu TPEs, um zur Gesamtrisikopunktzahl einer Organisation beizutragen.

Zeigen Sie ein Workflow-Beispiel in an Arbeitsbereich des Schwachstellenmanagers

Zeigen Sie ein Beispiel für einen End-to-End-Workflow in an Arbeitsbereich des Schwachstellenmanagers. Sehen Sie, wie ein Schwachstellenmanager oder Analyst den Arbeitsbereich zur Überwachung kritischer Elemente verwenden kann Datensätze Und erstellen Sie Korrekturaufgaben, um SIE an DIE IT zu übergeben.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

Klicken Sie auf das folgende Video, um die Schritte des Workflows anzuzeigen.
Arbeitsbereich des Schwachstellenmanagers Demo

Das vorherige Video enthält die folgenden Aufgaben:

a. Klicken Sie auf ein Überwachungsthema im **Überwachungsthemen** Seite des Arbeitsbereichs zum Anzeigen von Daten in einem Dashboard.

b. Erstellen Sie ein Überwachungsthema mithilfe von Filterbedingungen, und zeigen Sie eine Vorschau der übereinstimmenden Datensätze an. Weitere Informationen zum Erstellen eines Überwachungsthemas finden Sie unter Erstellen Sie ein Überwachungsthema in Arbeitsbereich des Schwachstellenmanagers.

c. Zeigen Sie Daten zu Datensätzen und ihren zugehörigen Konfigurationselementen auf der an **Betroffene CIs** Registerkarte in einem Überwachungsthema. Weitere Informationen zu den Visualisierungen finden Sie unter Liste der zugehörigen Elemente und Visualisierungen in einem Überwachungsthema.

d. Zeigen Sie Daten zu Schwachstellen in an **Eindeutige Schwachstellen** Registerkarte in einem Überwachungsthema.

e. Zeigen Sie die Datensätze an, die dem Überwachungsthema im zugeordnet sind **Angreifbare Elemente** Oder **Konfigurationstestergebnisse** Registerkarte in einem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachungsthema. Scrollen Sie nach rechts, um in der Spalte Korrekturmaßnahme anzuzeigen, welche Datensätze sich bereits in einer Korrekturmaßnahme befinden.

f. Wählen Sie Aus **Erstellen Sie eine Korrekturmaßnahme** In einem Überwachungsthema, wenn Sie bereit sind, Aufgaben für bestimmte Arten von Datensätzen zu erstellen und sie IHM zur Korrektur zuzuweisen. Weitere Informationen zum Erstellen einer Korrekturmaßnahme finden Sie unter Erstellen Sie eine Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers.

g. Wählen Sie aus **Liste** Anzeigen, um Listen Ihrer Korrekturmaßnahmen, Korrekturaufgaben, Datensätze, Ausnahmen und Genehmigungen anzuzeigen. Weitere Informationen zur Seite „Listen“ finden Sie unter Listenseite in Arbeitsbereich des Schwachstellenmanagers.

h. Wählen Sie aus **Aktiv** Liste der Korrekturmaßnahmen in der Listenansicht, um einen Korrekturmaßnahmendatensatz zu öffnen, um Status und Informationen zum Datensatz anzuzeigen. Weitere Informationen finden Sie unter Listenseite in Arbeitsbereich des Schwachstellenmanagers.

i. Wählen Sie aus **Korrekturaufgabe** Registerkarte im Datensatz der Korrekturmaßnahme, um die Korrekturaufgaben anzuzeigen, die dem Korrekturdatensatz zugeordnet sind. Weitere Informationen finden Sie unter Listenseite in Arbeitsbereich des Schwachstellenmanagers.

j. Wählen Sie aus **Angreifbare Elemente** Registerkarte, **Angreifbare Anwendungselemente** Registerkarte, **Angreifbare Container-Elemente** Registerkarte oder **Konfigurationstestergebnisse** Registerkarte im entsprechenden Korrekturmaßnahmendatensatz, um eine Liste der Datensätze anzuzeigen, die einer Korrekturmaßnahme zugeordnet sind. Weitere Informationen finden Sie unter Listenseite in Arbeitsbereich des Schwachstellenmanagers.

k. Wenn Sie aus der Korrekturmaßnahme für eine Teilmenge von Datensätzen bei Bedarf eine neue Korrekturaufgabe erstellen möchten, wählen Sie die Datensätze aus, die Sie verschieben möchten, und klicken Sie auf **Erstellen Sie eine Korrekturaufgabe** . Weitere Informationen finden Sie unter Erstellen Sie eine Korrekturaufgabe bei Bedarf aus der Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers

Überwachung und Verwaltung angreifbarer Elemente und Testergebnisse in Arbeitsbereich des Schwachstellenmanagers

Die Arbeitsbereich des Schwachstellenmanagers Mit können Sie angreifbare Elemente (Vits, AVITs und CVITs) und Testergebnisse (TRs) mithilfe von Überwachungsthemen überwachen und ihren Korrekturfortschritt nachverfolgen und verwalten, indem Sie Korrekturmaßnahmen erstellen.

Öffnen Sie Suchergebnisse in Arbeitsbereich des Schwachstellenmanagers

Öffnen Sie Suchergebnisse in Arbeitsbereich des Schwachstellenmanagers Anstelle der klassischen UI durch Ändern des Anwendungsbereichs.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst, sn_vul.Vulnerability_admin oder sn_vul.read_all für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager oder sn_vul.App_read_all für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst, sn_vul_Container.Vulnerability_admin oder sn_vul_Container.read_all für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin oder sn_vulc.read für Konfigurationstestergebnisse (TRs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Beispiel: Wenn Sie nach einem angreifbaren Host-Element mit seiner Nummer in suchen **Suchen** Feld, indem der Anwendungsbereich auf festgelegt wird Arbeitsbereich des Schwachstellenmanagers, Wird die VIT in ihrer Datensatzansicht in geöffnet Arbeitsbereich des Schwachstellenmanagers.

Prozedur

1. Wählen Sie in der einheitlichen Navigationsleiste das Globe-Symbol aus .
2. Wählen Sie Aus **Anwendungsbereich** .
3. Legen Sie den Bereich auf fest **Vulnerability Manager-Arbeitsbereich** .

Nächste Maßnahme

Wenn Sie in nach Datensätzen wie Vits, Korrekturaufgaben, Status-Change-Genehmigungen usw. suchen **Suchen** Feld in der einheitlichen Navigationsleiste werden die Datensätze in geöffnet Arbeitsbereich des Schwachstellenmanagers.

Wenn der Bereich nicht global ist, wird das Globe-Symbol mit einem roten Ring angezeigt . Wählen Sie sie erneut aus, um den Umfang zu ändern.

Filter für die Zusammenfassung aktiver Datensätze erstellen und anwenden (Vits, AVITs, CVITs und CTRs)

Als Schwachstellenmanager und -Analyst können Sie die gewünschten Datensätze filtern, um ihre Zusammenfassung auf der Homepage von zu visualisieren Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Homepage**an.
2. Wählen Sie das Zahnradsymbol , Und wählen Sie dann aus **Filter erstellen** Auf den Registerkarten Host-Schwachstellen, Container-Schwachstellen, Anwendungsschwachstellen oder Konfigurationstestergebnisse.
3. Füllen Sie die Felder im Popup-Fenster Filter erstellen aus.

Erstellen Popup-Fenster „Filter“

Feld	Beschreibung
Filtername	Name für den Filter.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bedingungen	Bedingung, um nur die Datensätze anzuzeigen, für die Sie Visualisierungen anzeigen möchten.
Täglich aktualisieren	Aktualisieren Sie die Visualisierungsinformationen jeden Tag.

4. Wählen Sie **Speichern**.
5. Zeigen Sie die Visualisierungen für die gefilterten Datensätze an, indem Sie den neuen Filter im auswählen **Anzeigen nach** Feld.
   Weitere Informationen zu den Widgets finden Sie unter Homepage in Arbeitsbereich des Schwachstellenmanagers.
6. So aktualisieren oder löschen Sie einen Filter:

   a. Wählen Sie das Zahnradsymbol Und wählen Sie dann aus **Filter bearbeiten** .

   b. Wählen Sie im Popup-Fenster gespeicherte Filter den Filter aus, den Sie aktualisieren oder löschen möchten.

   c. Aktualisieren oder löschen Sie den Filter.

Aktion	Schritte
Löschen Sie den Filter.	Wählen Sie **Löschen**.
Ändern Sie den Filternamen	Bearbeiten Sie den Filternamen, und wählen Sie aus **Aktualisieren** .
Ändern Sie die Filterbedingungen	Bearbeiten Sie die Bedingung, um Informationen nur für bestimmte Datensätze anzuzeigen, und wählen Sie sie aus **Aktualisieren** .
Täglich aktualisieren	Legen Sie fest, ob die Visualisierungsinformationen jeden Tag aktualisiert werden sollen, und wählen Sie aus **Aktualisieren** .

Zugehörige Informationen

Homepage in Arbeitsbereich des Schwachstellenmanagers

Verwenden Überwachungsthemen in Arbeitsbereich des Schwachstellenmanagers

Überwachungsthemen in verwenden Arbeitsbereich des Schwachstellenmanagers Dient zum Anzeigen von Schwachstellen und Fehlkonfigurationen, die aus Ihren importierten Daten aus den von Ihnen festgelegten Kriterien gefiltert werden. Verwenden Sie diese Informationen, um zu bestimmen, wie sich die Schwachstellen und Fehlkonfigurationen in den einzelnen Überwachungsthemen auf Ihre Umgebung auswirken können.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Auf der Seite „Überwachungsthemen“ können Sie die folgenden Aufgaben ausführen:

- Überwachen Sie die Anzahl der Korrekturmaßnahmen und -Datensätze (Vits, AVITs, CVITs und TRs), um den Fortschritt Ihrer Schwachstellenbeseitigung zu sehen.
- Bearbeiten oder löschen Sie Ihre vorhandenen Überwachungsthemen, und erstellen Sie Überwachungsthemen.
- Erstellen Sie Korrekturmaßnahmen, und übergeben Sie die Korrekturaufgaben automatisch nur für die Schwachstellen, die Sie beheben möchten, an Ihre IT-Teams.

Hinweis:
Ab v19.0 von Vulnerability Response, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie v19.0 und höher
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Prozedur

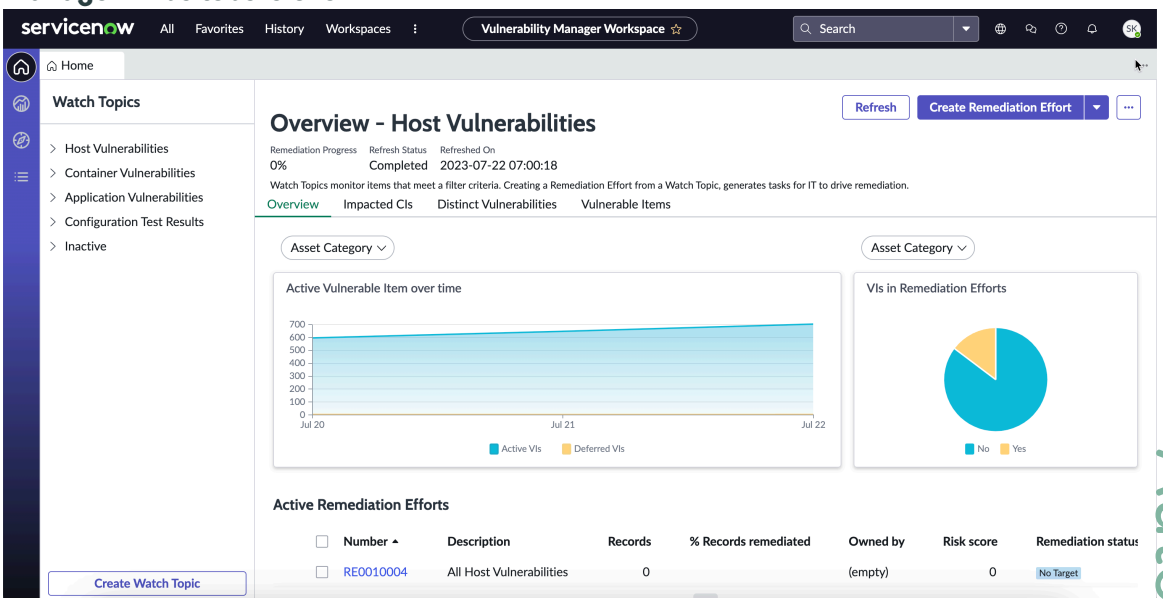
1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Wählen Sie das Symbol „Überwachungsthemen“ aus.
3. Wählen Sie auf der Seite „Überwachungsthemen“ auf den Registerkarten Host-Schwachstellen, Container-Schwachstellen, Anwendungsschwachstellen oder Konfigurationstestergebnisse ein Überwachungsthema aus.

   Wenn Sie ein Überwachungsthema auswählen, wird die **Übersicht** Die Registerkarte wird standardmäßig angezeigt.

   Weitere Informationen zu den Überwachungsthemen finden Sie unter Seite „Überwachungsthemen“ in Arbeitsbereich des Schwachstellenmanagers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Version 19,0 Registerkarte „Übersicht“ in Homepage des Schwachstellen-Manager-Arbeitsbereichs



Die Dashboards sind dynamisch, und neue Schwachstellendaten werden beim Import aktualisiert.

4. Wählen Sie ein aus **Registerkarte „zugehörige Elemente“** Um weitere Daten anzuzeigen.

   Weitere Informationen zur Liste der zugehörigen Elemente und zu Visualisierungen in einem Überwachungsthema finden Sie unter Liste der zugehörigen Elemente und Visualisierungen in einem Überwachungsthema.

5. Führen Sie die UI-Aktionen auf der Seite „Überwachungsthemen“ aus.

6. **Wahlweise:** Wählen Sie einen Datensatz aus, um weitere Details anzuzeigen.

Erstellen Sie ein Überwachungsthema in Arbeitsbereich des Schwachstellenmanagers

Schwachstellenmanager und Analysten können Überwachungsthemen mithilfe einer Reihe von Bedingungen erstellen, um Teilmengen von Datensätzen (Vits, AVITs, CVITs oder CTRs) herauszufiltern, die sie überwachen möchten.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Auf der Registerkarte Übersicht von Überwachungsthemen zeigt ein nächtlich aktualisierter Trendbericht zusammen mit anderen Berichten den aktuellen Status der Datensätze für dieses Überwachungsthema an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v19.0 von Vulnerability Response, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie v19.0 und höher
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers** > **Überwachungsthemen**an.
2. **Wahlweise:** Alternativ klicken Sie rechts neben der Schaltfläche Korrekturmaßnahme erstellen auf die drei Punkte ..., Gefolgt von „Bearbeiten“, um ein vorhandenes Überwachungsthema zu ändern.

   Hinweis:
   Möglicherweise bemerken Sie eine Verzögerung, bevor aktuelle Daten für ein Überwachungsthema angezeigt werden, nachdem Sie die Filterung geändert haben.

3. Wählen Sie unten links auf der Seite die Option aus **Überwachungsthema Erstellen** .
4. Füllen Sie die Felder im angezeigten Modal aus.
   Weitere Informationen zu den modalen Feldern „Überwachungsthema erstellen“ finden Sie unter Formularfelder für Überwachungsthema erstellen.
5. Definieren Sie Bedingungen für die ausgewählte Datensatzkategorie.

   Hinweis:
   Wenn Sie in Ihrem Überwachungsthema keine Bedingungen festlegen, werden keine Daten in das Dashboard abgerufen.

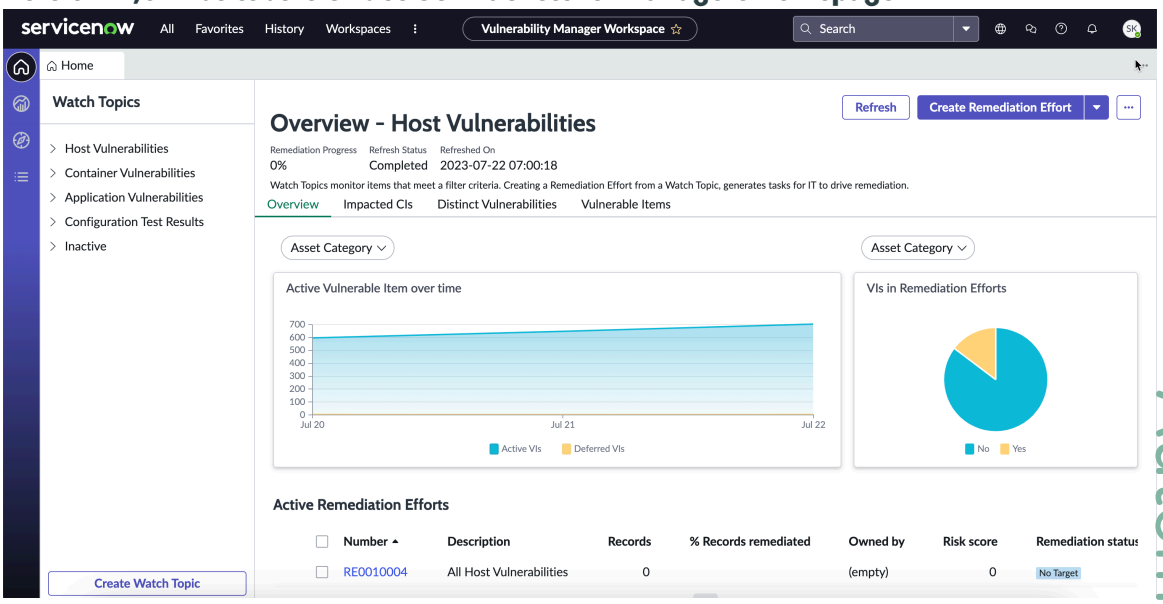
6. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihr neues Überwachungsthema wird auf der Startseite-Zielseite angezeigt. T Die Überwachungsthemen werden im Navigationsbereich nach Datensatztyp kategorisiert.

Version 19,0 Arbeitsbereich des Schwachstellenmanagers Homepage



Nächste Maßnahme

Erstellen Sie eine Korrekturmaßnahme.

Bearbeiten oder löschen Sie ein Überwachungsthema in Arbeitsbereich des Schwachstellenmanagers

Sie können ein vorhandenes Überwachungsthema in bearbeiten oder löschen Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein vorhandenes Überwachungsthema bearbeiten:

- Die Daten im Dashboard werden aktualisiert, um Ihre Änderungen widerzuspiegeln.
- Die Datensätze, die sich derzeit in den vorhandenen Korrekturmaßnahmen befinden, bleiben unverändert.
- Die Datensätze, die sich derzeit nicht in Korrekturmaßnahmen befinden, werden basierend auf den Kriterien angezeigt, die Sie im Bedingungsgenerator eingeben.

Wenn Sie ein Überwachungsthema löschen, bevor alle zugehörigen Datensätze behoben wurden, sind die Datensätze, die mit diesem Überwachungsthema angezeigt werden, nicht betroffen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Überwachungsthemen**an.
2. Öffnen Sie das Überwachungsthema, das Sie bearbeiten möchten.
3. Klicken Sie auf die drei Punkte Und klicken Sie auf **Bearbeiten** .

   Hinweis:
   Sie können kein inaktives Überwachungsthema bearbeiten.

4. Ändern Sie im modalen Dialogfeld „Überwachungsthema bearbeiten“ die Felder.
5. Klicken Sie auf **Absenden**.

   Hinweis:
   Möglicherweise bemerken Sie eine Verzögerung, bevor aktuelle Daten für ein Überwachungsthema angezeigt werden, nachdem Sie die Filterung geändert haben.

   Sie können auch vorhandene wiederkehrende Korrekturmaßnahmen bearbeiten. Wenn für ein Überwachungsthema eine wiederkehrende Korrekturmaßnahme vorhanden ist, **Bearbeiten Sie den wiederkehrenden Aufwand** Ist über das Menü verfügbar. Wählen Sie diese Option aus, um den wiederkehrenden Aufwand zu bearbeiten.

   Alle Änderungen, die Sie im Datensatz der Korrekturmaßnahme vornehmen und speichern, wirken sich nicht auf die anderen Korrekturmaßnahmen aus, die Sie bereits aus dem Überwachungsthema erstellt haben.

6. **Wahlweise:** Um ein Überwachungsthema zu löschen, wählen Sie das Menü mit drei Punkten aus Wählen Sie im Überwachungsthema aus, und wählen Sie aus **Löschen** .

Deaktivieren oder aktivieren Sie ein Überwachungsthema

Sie können ein Überwachungsthema im Vulnerability Manager-Arbeitsbereich deaktivieren oder aktivieren.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

- Alle inaktiven Überwachungsthemen werden in angezeigt **Inaktiv** Modul im Navigationsbereich.
- Sie können keine Korrekturmaßnahme oder wiederkehrende Korrekturmaßnahme für ein inaktives Überwachungsthema erstellen.
- Sie können ein inaktives Überwachungsthema nicht aktualisieren.
- Die Details eines inaktiven Überwachungsthemas und der zugehörigen Korrekturmaßnahmen werden nicht aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Überwachungsthemen**an.
2. Öffnen Sie das Überwachungsthema, das Sie deaktivieren möchten.
3. Klicken Sie auf die drei Punkte, und klicken Sie auf **Deaktivieren** .
   Das Überwachungsthema wird im Modul „Inaktiv“ angezeigt.
4. Um ein Überwachungsthema zu aktivieren, wählen Sie im Modul „Inaktiv“ ein Überwachungsthema aus, wählen Sie das Menü „drei Punkte“ aus, und wählen Sie aus **Aktivieren** .
   Das aktivierte Überwachungsthema wird zum entsprechenden Modul im Navigationsbereich verschoben.

Verwenden Sie Datensätze für Korrekturmaßnahmen

Wenn Schwachstellenmanager und Analysten Korrekturmaßnahmen (RES) erstellen, werden Korrekturaufgaben (VUL, AVUL, CVUL und CRG) automatisch IT-Teams zur Korrektur zugewiesen.

Vorbereitungen

Sie müssen eine Korrekturmaßnahme erstellen, bevor Sie sie verwenden können, um den Korrekturfortschritt für Korrekturaufgaben zu überwachen.

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Wenn nicht ausgewählt, klicken Sie oben links auf das Listensymbol.

   Die Listenansicht mit aktiven Datensätzen für Korrekturmaßnahmen wird angezeigt.
2. Wählen Sie in der Spalte Datensatztyp das Menü mit drei Punkten aus, und wählen Sie aus **Nach Datensatztyp gruppieren** .
   Die Korrekturmaßnahmen werden in angreifbare Host-Elemente, angreifbare Anwendungselemente, angreifbare Container-Elemente und Konfigurationstestergebnisse kategorisiert.
3. Klicken Sie auf der Zielseite der Listenansicht, wenn in den gefilterten Listen aktive Korrekturmaßnahmen ausgewählt sind, auf einen Datensatz, um ihn zu öffnen.
   Der Datensatz wird angezeigt. Sie können die Korrekturaufgaben und anzeigen Datensätze Die der ausgewählten Korrekturmaßnahme zugeordnet sind.
4. In der folgenden Tabelle finden Sie die Aktionen, die Sie für den Datensatz der Korrekturmaßnahme ausführen können.

   Nachdem Sie einen Datensatz erstellt haben, kann es einige Minuten dauern, bis die Korrekturaufgaben und eine große Anzahl von Datensätzen angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UI-Aktion	Beschreibung
Fügen Sie ein Tag hinzu	Klicken Sie rechts neben dem Header auf das kleine Tag-Symbol. Möglicherweise möchten Sie Text hinzufügen, der Ihnen bei der Identifizierung dieses Datensatzes hilft. Sie können beispielsweise ein Tag hinzufügen, dass dieser Datensatz PCI- oder andere kritische Daten enthält.
Fügen Sie dem Datensatz eine Arbeitsnotiz hinzu	Klicken Sie ganz rechts auf dem Bildschirm auf **Aktivität** Symbol (Blitzsymbol) und geben Sie eine Arbeitsnotiz ein. Klicken Sie auf das Symbol, um den Bereich umzuschalten.
Datensatz aktualisieren	Auf der **Details** Klicken Sie für alle bearbeitbaren Felder auf ein Feld, um es auszuwählen, nehmen Sie Ihre Änderungen vor, und klicken Sie auf **Speichern** Zum Aktualisieren des Datensatzes.
Wenn angezeigt, klicken Sie auf das Filtersymbol, um die Daten auf der angezeigten Seite zu verfeinern	Mit einer der Korrekturaufgaben, angreifbare Elemente, o r Konfigurationstestergebnisse Ausgewählte Registerkarten ganz rechts klicken Sie auf das Filtersymbol, um die Filter anzuzeigen, die für die Registerkarte gelten. Klicken Sie im angezeigten Bereich auf **Erweiterte Ansicht** Zum Hinzufügen oder Ändern von Filterbedingungen für die Elemente auf der Seite. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern. Zum Beispiel auf der **Angreifbare Elemente** Auf der Registerkarte können Sie das Feld Alter hinzufügen und einen Bereich eingeben, um nur Datensätze aus einem bestimmten Zeitraum anzuzeigen. Datensätze, die den von Ihnen festgelegten Bedingungen entsprechen, werden in der Liste angezeigt.
Verfeinern Sie Filter für Elemente in einer Spalte	Wählen Sie eine Spalte aus, und klicken Sie auf das Menü „drei vertikale Punkte“, erweitern Sie sie, und geben Sie Bedingungen ein, um die Daten in der Spalte zu verfeinern und zu gruppieren.
Filtern Sie Elemente aus einer Zeile in einer Spalte heraus, oder gleichen Sie Elemente ab	Angenommen, Sie möchten nur Datensätze anzeigen, die eine bestimmte Schwachstelle aufweisen. Wählen Sie in der Liste der Datensätze die Zeile des Datensatzes aus **Zusammenfassung** Spalte. Klicken Sie auf das angezeigte vertikale Punktmenü, und wählen Sie eines aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UI-Aktion	Beschreibung
	○ **Übereinstimmungen anzeigen** – Alle anderen Datensätze mit dieser Schwachstelle anzeigen. ○ **Herausfiltern** – Zeigt alle Datensätze an, die diese Schwachstelle nicht aufweisen.

5. Auf den Registerkarten Korrekturaufgaben, angreifbare Elemente und Konfigurationstestergebnisse können Sie Detailinformationen zu einzelnen Korrekturaufgaben (VUL, AVUL, CVUL oder CRG), angreifbaren Elementen (VIT, AVIT, oder CVIT) Und Testergebnis (CTR) Datensätze.

Nächste Maßnahme

Informationen zum Erstellen einer Korrekturaufgabe bei Bedarf aus einer Korrekturmaßnahme finden Sie unter Erstellen Sie eine Korrekturaufgabe bei Bedarf aus der Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers. Sie können auch Erstellen Sie eine anwenderdefinierte Liste von Datensätzen Damit Sie den Korrekturfortschritt überwachen können.

Erstellen Sie eine Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers

Ein Korrekturmaßnahmendatensatz ist eine statische Liste von Datensätzen, die Sie aus einem Überwachungsthema in erstellen Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Sie verwenden Korrekturmaßnahmen, um die Aufgaben zu übergeben, die IT-Teams zur Behebung von Schwachstellen und Fehlkonfigurationen verwenden.

- Sie können vorhandene Korrekturmaßnahmen bearbeiten.
- Erstellen Sie Korrekturmaßnahmen, die automatisch zu den von Ihnen festgelegten Daten und Uhrzeiten erstellt werden.
- Übertragen Sie Datensätze aus vorhandenen Korrekturmaßnahmen in eine neue Korrekturmaßnahme.

Ab Version 18.0, da Sie keine Korrekturmaßnahme für ein inaktives Überwachungsthema erstellen können, die **Erstellen Sie Eine Korrekturmaßnahme** Schaltfläche ist inaktiv.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers** > **Überwachungsthemen**an.
2. Wählen Sie auf der Seite „Überwachungsthemen“ ein Überwachungsthema aus, für das Sie eine Korrekturmaßnahme erstellen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Um die Datensätze anzuzeigen, die dem ausgewählten Überwachungsthema zugeordnet sind, klicken Sie unter der Datensatzüberschrift auf **Angreifbare Elemente** , **Angreifbare Anwendungselemente** , **Angreifbare Container-Elemente** Oder **Konfigurationstestergebnisse** Registerkarte in ihren jeweiligen Überwachungsthemen.

   Die Datensätze werden angezeigt.

   Beispielsweise können Sie im Header auf der Registerkarte angreifbare Elemente die Gesamtzahl der Datensätze dieses Überwachungsthemas anzeigen.

   Die folgenden Spalten und Daten werden angezeigt:

Spalten auf der Registerkarte angreifbare Elemente

Spalte	Beschreibung
Anzahl	Die Datensatznummer.
Zusammenfassung	Beschreibung der Schwachstelle.
Konfigurationselement	Das Asset, das der Schwachstelle zugeordnet ist.
Risikobewertung	Quantifizierte Risikopunktzahl, die Datensätze in „Kritisch“, „hoch“, „Mittel“, „Niedrig“ und „keine“ trennt.
Status	Status des Datensatzes.
Korrekturstatus	Status der Korrektur für einen Datensatz.
Zuweisungsgruppe	Zuweisungsgruppen, die für die Korrektur verantwortlich sind. Die Zuweisung von Datensätzen zu Gruppen basiert auf den von Ihnen erstellten Zuweisungsregeln.
Korrekturmaßnahme	Wenn er einer Korrekturmaßnahme zugewiesen ist, listet jeder Datensatz die ihm zugewiesene Korrekturmaßnahme auf. Nachdem er einer Korrekturmaßnahme hinzugefügt wurde, wird keinem anderen von Ihnen erstellten Korrekturmaßnahmen ein Datensatz hinzugefügt.
Zuweisungsgruppe	Zuweisungsgruppen, die für die Korrektur verantwortlich sind. Die Zuweisung von Datensätzen zu Gruppen basiert auf den von Ihnen erstellten Zuweisungsregeln.
Korrekturmaßnahme	Wenn er einer Korrekturmaßnahme zugewiesen ist, listet jeder Datensatz die ihm zugewiesene Korrekturmaßnahme auf. Nachdem er einer Korrekturmaßnahme hinzugefügt wurde, wird keinem anderen von Ihnen erstellten Korrekturmaßnahmen ein Datensatz hinzugefügt.
In Korrekturaufgabe	Wenn Wahr , Dieser Wert gibt an, dass sich ein Datensatz bereits in einer Korrekturaufgabe befindet. Datensätze können sich in mehreren Korrekturaufgaben befinden, ein Datensatz kann jedoch nur einer Korrekturmaßnahme hinzugefügt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Exploit vorhanden	Gibt an, ob ein bekannter Exploit für einen Datensatz vorhanden ist.
Zuletzt geöffnet	Datum, an dem der Datensatz zuletzt in geöffnet wurde ServiceNow AI Platform. Wenn der Datensatz geschlossen und dann erneut geöffnet wurde, ist dies das letzte Mal, dass der Datensatz erneut geöffnet wurde.

4. Um eine Korrekturmaßnahme zu erstellen, klicken Sie auf **Erstellen Sie Eine Korrekturmaßnahme** .

   Wenn Sie Korrekturmaßnahmen erstellen, werden Datensätze, die sich bereits in vorhandenen Korrekturmaßnahmen befinden, keinen neuen Korrekturmaßnahmen hinzugefügt, die Sie aus diesem Überwachungsthema erstellen.

   Wenn Datensätze aktualisiert oder neue Datensätze in Überwachungsthemen erstellt werden, können Sie Korrekturmaßnahmen erstellen.

5. Alternativ können Sie auch Erstellen Sie eine wiederkehrende Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers.

   Die **Bearbeiten** Die Schaltfläche ist im Menü für vorhandene Korrekturmaßnahmen verfügbar. Sie haben die Möglichkeit, die Felder und Bedingungen über ein angezeigtes modales Element zu ändern. Alle Änderungen, die Sie im Datensatz der Korrekturmaßnahme vornehmen und speichern, wirken sich nicht auf die anderen Korrekturmaßnahmen aus, die Sie bereits aus dem Überwachungsthema erstellt haben.

6. Füllen Sie die Felder in Schritt 1 des Modals „Korrekturmaßnahme erstellen“ aus.

   Geben Sie im Feld Kurzbeschreibung Text ein, der die wiederkehrende Korrekturmaßnahme beschreibt und Ihnen hilft, sie aus der Aufwandsliste zu finden und nachzuverfolgen.

   Geben Sie im Feld Beschreibung mehr Text zum Kontext der Maßnahme ein, damit Sie sie leicht aus der Liste der Korrekturmaßnahmen finden können.

7. Wählen Sie in Schritt 2, Aufgabengenerierung, eine Methode aus der Liste aus, um die Datensätze in den Korrekturaufgaben zu bündeln, die Sie aus dieser Korrekturmaßnahme generieren, nachdem sie erstellt wurde.

8. Um die doppelten angreifbaren Host-Elemente automatisch zu aktualisieren, müssen Sie auswählen **Doppelte angreifbare Elemente für die erstellten Korrekturaufgaben automatisch aktualisieren** Kontrollkästchen.

   Hinweis:
   Dieses Kontrollkästchen ist nur für Host-Schwachstellen verfügbar.

9. Überprüfen Sie in Schritt 3 „Übertragen“, wie viele Datensätze Sie der Korrekturmaßnahme hinzufügen möchten, und sehen Sie, wie viele Datensätze für die Übertragung von anderen aktiven Korrekturmaßnahmen verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

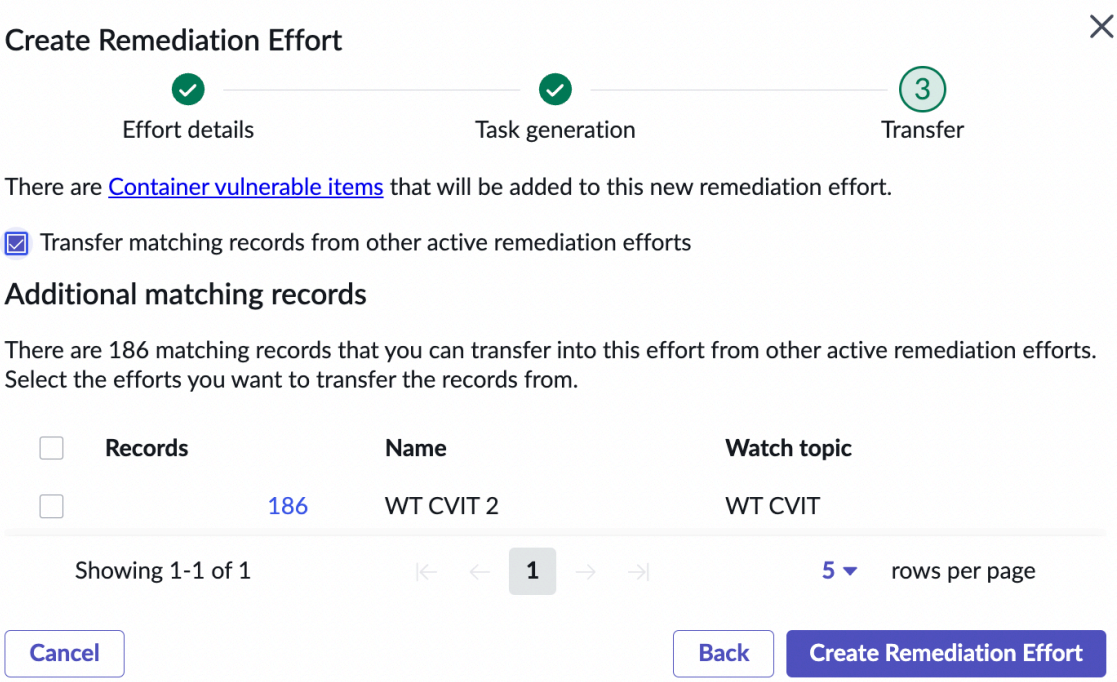
Wenn keine neuen aktiven Datensätze zum Hinzufügen vorhanden sind, wird der folgende Text angezeigt:

Es sind keine aktiven Datensätze verfügbar, die Sie dieser neuen Korrekturmaßnahme hinzufügen können.

Alle zusätzlichen Datensätze, die für die Übertragung an diese Maßnahme verfügbar sind, sind unter aufgeführt Zusätzliche übereinstimmende Datensätze .

Wählen Sie aus **Übertragen Sie übereinstimmende Datensätze aus anderen aktiven Korrekturmaßnahmen** Aktivieren Sie das Kontrollkästchen, und aktivieren Sie dann die Kontrollkästchen für die Datensätze, die Sie von anderen aktiven Korrekturmaßnahmen übertragen möchten.

Version 18,0 Erstellen Sie Eine Korrekturmaßnahme



Nachdem Sie auf geklickt haben **Erstellen Sie Eine Korrekturmaßnahme** , In wenigen Minuten wird die neue Korrekturmaßnahme angezeigt. Je nach Anzahl der Datensätze kann es einige Zeit dauern, den neuen Datensatz auszufüllen. Eine Nachricht gibt an, ob der Datensatz noch ausgefüllt wird.

Die neue Korrekturmaßnahme wird mit allen Datensätzen erstellt, die aus dem zu ihrer Erstellung verwendeten Überwachungsthema verfügbar sind, zusätzlich zu allen Datensätzen, die Sie für die Übertragung aus vorhandenen Maßnahmen ausgewählt haben.

Wenn Sie Datensätze auswählen, die von einer vorhandenen Maßnahme übertragen werden sollen, und die vorhandene Maßnahme alle ihre Datensätze in Ihre neue Maßnahme überträgt, wird die Korrekturmaßnahme, aus der Sie die Datensätze verschoben haben, geschlossen. Weitere Informationen dazu, wie sich die Korrekturaufgaben, die den Korrekturmaßnahmen zugeordnet sind, von der Datensatzübertragung auswirken, finden Sie unter Lebenszyklen von Korrekturmaßnahmen, Korrekturaufgaben und Datensätzen in den Vulnerability Response-Arbeitsbereichen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn keine Datensätze aus dem Überwachungsthema verfügbar sind oder keine Datensätze für die Übertragung ausgewählt sind, wird die verwendet **Erstellen Sie Eine Korrekturmaßnahme** Schaltfläche ist deaktiviert.

Die *Populate Efforts*Die geplante Aufgabe wird alle 10 Minuten ausgeführt, um die Daten in den Widgets basierend auf der ausgewählten Bedingung auszufüllen.

Klicken Sie auf die Registerkarte Korrekturfortschritt, um den Korrekturfortschritt anzuzeigen. Klicken Sie auf ein beliebiges Element, um Details anzuzeigen, einschließlich Datensatztyp, Risikopunktzahl, Risikobewertung, Prozentsatz der korrigierten Datensätze, Datensätze im Status „zurückgestellt“ und „nicht zurückgestellt“ sowie die Gesamtzahl der Datensätze, die im Überwachungsthema verwendeten Bedingungen und den Korrekturstatus. Die Korrekturstatusinformationen wie Korrekturziel und Korrekturstatus werden aus der Tabelle „angreifbare Elemente“ zusammengefasst. Die höchste Datensatz-Risikopunktzahl wird aus der Tabelle „Schwachstellenrechner“ zusammengefasst, während die Risikopunktzahl aus dem Rollup ausgeführt wird **Rechner für Schwachstellen-Rollup** > **Rollup von Korrekturmaßnahme** an.

Auf der Registerkarte Korrekturaufgaben werden die Aufgaben für alle Arten von Problemen angezeigt. Die Felder werden ausgefüllt, wenn die folgenden geplanten Aufgaben ausgeführt werden. Sie werden alle 15 Minuten automatisch ausgeführt:

- Rollup der Werte angreifbarer Anwendungselemente für Schwachstelle und Gruppe.
- Rollup der Werte angreifbarer Container-Elemente zu Schwachstelle und Gruppe.
- Rollup von Testergebniswerten zum Testergebnisgruppen- und Konfigurationstest.
- Rollup der Werte angreifbarer Elemente zu Schwachstelle und Gruppe.

In der Listenansicht können Sie Korrekturmaßnahmen, Korrekturaufgaben, angreifbare Elemente, Konfigurationstestergebnisse usw. anzeigen. Sie können eine Korrekturaufgabe oder ein angreifbares Element öffnen und die Seite „Details“ anzeigen. Klicken Sie auf die Ellipsen weitere Aktionen, und klicken Sie auf **Untersuchung Starten** Dient zum Lösen einer Korrekturaufgabe.

10. **Wahlweise:** Sie können auch vorhandene wiederkehrende Korrekturmaßnahmen bearbeiten.

    (Optional) Wenn für ein Überwachungsthema eine wiederkehrende Korrekturmaßnahme vorhanden ist, **Bearbeiten Sie den wiederkehrenden Aufwand** Ist über das Menü oben rechts in einem Überwachungsthema verfügbar. Wählen Sie diese Option aus, um den wiederkehrenden Aufwand zu bearbeiten.

    Alle Änderungen, die Sie im Datensatz der Korrekturmaßnahme vornehmen und speichern, wirken sich nicht auf die anderen Korrekturmaßnahmen aus, die Sie bereits aus dem Überwachungsthema erstellt haben.

Erstellen Sie eine Korrekturaufgabe bei Bedarf aus der Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers

Erstellen Sie bei Bedarf eine Korrekturaufgabe aus einer Korrekturmaßnahme. Wenn Sie bei Bedarf eine Korrekturaufgabe erstellen, wählen Sie die Datensätze aus, die Sie manuell hinzufügen möchten.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Für Version 18,0 von Vulnerability Response, Sie können keine Korrekturaufgabe aus der Datensatzansicht einer Korrekturmaßnahme erstellen.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Klicken Sie oben links im Arbeitsbereich mit der angezeigten Homepage auf **Liste** Ansichtssymbol, um die Zielseite der Liste anzuzeigen.
3. Klicken Sie unter Korrekturmaßnahmen auf eine der beiden Optionen **Aktiv** Oder **Alle** .
4. Klicken Sie in der angezeigten Liste auf einen Datensatz, um ihn zu öffnen.
   Die Registerkarte „Übersicht“ des Datensatzes wird angezeigt.
5. Klicken Sie auf **Angreifbare Elemente** Registerkarte.
   Die Liste der Datensätze wird angezeigt.
6. Um eine neue Korrekturaufgabe zu erstellen, wählen Sie in der Spalte Nummer die Datensätze aus, die Sie hinzufügen möchten.
7. Klicken Sie Auf **Erstellen Sie eine Korrekturaufgabe** .
8. Füllen Sie die Felder im angezeigten Modal aus.
9. Klicken Sie auf **Erstellen**.
10. Die neue Korrekturaufgabe wird mit den von Ihnen ausgewählten aktiven Datensätzen angezeigt.

Erstellen Sie eine wiederkehrende Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers

Sie können wiederkehrende Korrekturmaßnahmen erstellen und planen, die automatisch zu den von Ihnen festgelegten Daten und Uhrzeiten generiert werden.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Sie können wiederkehrende Korrekturmaßnahmen automatisch nach einem Zeitplan erstellen, mit dem Sie Schwachstellen nachverfolgen können, die möglicherweise auftreten und sofortige und laufende Maßnahmen erfordern.

Ab Version 18.0, da Sie keine wiederkehrenden Korrekturmaßnahmen für ein inaktives Überwachungsthema erstellen können, die **Erstellen Sie Wiederkehrende Maßnahme** Option ist inaktiv. Wenn Sie ein Überwachungsthema deaktivieren, für das bereits eine wiederkehrende Maßnahme geplant ist, wird erst dann eine neue Korrekturmaßnahme erstellt, wenn das Überwachungsthema aktiviert ist. Auch die **Aufwandswiederholung** Und **Nächstes Wiederholungsdatum** Details werden oben rechts ausgeblendet. Nachdem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie das Überwachungsthema aktiviert haben, wird im bevorstehenden Zeitplan eine Korrekturmaßnahme erstellt.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers** > **Überwachungsthemen**an.
2. Wählen Sie auf der Seite „Überwachungsthemen“ ein Überwachungsthema aus, für das Sie eine wiederkehrende Korrekturmaßnahme erstellen möchten.

   Sie können eine wiederkehrende Korrekturmaßnahme pro Überwachungsthema erstellen.

   Hinweis:
   Sie können keine Datensätze aus wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Sie können jedoch Datensätze aus vorhandenen, nicht wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Siehe Übertragen Sie Datensätze an Korrekturmaßnahmen in der Arbeitsbereich des Schwachstellenmanagers Weitere Informationen zum Übertragen von Datensätzen.

3. Wählen Sie in einem Überwachungsthema oben rechts in der Liste Korrekturmaßnahme erstellen die Option aus **Erstellen Sie Wiederkehrende Maßnahme** .

   Das Modal „Wiederkehrenden Aufwand erstellen“ wird angezeigt.

4. Füllen Sie in Schritt 1 „Aufwandsdetails“ die erforderlichen Felder aus.

   Geben Sie im Feld Kurzbeschreibung den Text ein, der die wiederkehrende Korrekturmaßnahme beschreibt, mit der Sie sie finden und aus der Aufwandsliste nachverfolgen können.

   Geben Sie im Feld Beschreibung mehr Text zum Kontext der Maßnahme ein, damit Sie sie leicht aus der Liste der Korrekturmaßnahmen finden können. Beispiel: `Schwachstellen in externen Assets` .

5. Klicken Sie auf **Next (Weiter)**.
   Details zur Aufgabengenerierung werden angezeigt.
6. Wählen Sie in Schritt 2, Aufgabengenerierung, eine Methode aus der Liste aus, um die angreifbaren Elemente in den Korrekturaufgaben zu bündeln, die Sie aus dieser Korrekturmaßnahme generieren, nachdem sie erstellt wurde.
   - Nach Zuweisungsgruppe
   - Nach Zuweisungsgruppe und Konfigurationselement
   - Nach Zuweisungsgruppe und Schwachstelle
   - Keine (es werden keine Korrekturaufgaben erstellt). Verwenden Sie diese Methode, wenn Sie einer Korrekturaufgabe für diese Maßnahme Datensätze manuell hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie eine Korrekturaufgabe bei Bedarf aus der Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers.
7. Um die doppelten angreifbaren Host-Elemente automatisch zu aktualisieren, müssen Sie auswählen **Doppelte angreifbare Elemente für die erstellten Korrekturaufgaben automatisch aktualisieren** Option.

   Hinweis:
   Dieses Kontrollkästchen ist nur für Host-Schwachstellen verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie Auf **Als Nächstes** Um fortzufahren.
9. Wählen Sie in Schritt 3 „Wiederholung“ die Häufigkeit aus.

   a. Definieren Sie den Wiederholungszeitplan.

   Verwenden Sie die Listen, um Monat/Tag/Stunde/Minute auszuwählen, für die die Korrekturmaßnahme erstellt werden soll. Die Zeitzone für die Planung ist standardmäßig Ihre Zeitzone.

   Hinweis:
   Wenn Sie viele Schwachstellen haben, ziehen Sie es möglicherweise vor, die Erstellung auf Ruhezeiten festzulegen.

   Wenn der Auftrag am letzten Tag des Monats erstellt werden soll, erstellt die geplante Aufgabe die wiederkehrende Korrekturmaßnahme am letzten Tag des Monats. Eine Meldung wird angezeigt, wenn der Monat keine 31 Tage hat.

   b. **Wahlweise:** Wählen Sie Aus **Schwachstellen übertragen** Aktive Schwachstellen in dieser Korrekturmaßnahme, um sie in jede nachfolgende erstellte Korrekturmaßnahme zu übertragen.

10. Klicken Sie Auf **Wiederholung planen** .
    Es wird eine Nachricht angezeigt, dass der Datensatz für die wiederkehrende Korrektur erstellt wurde. Die neue Korrekturmaßnahme wird nicht sofort angezeigt. Sie wird bei der Planung erstellt. Sie wird in Ihren Listen angezeigt, nachdem sie von der geplanten Aufgabe erstellt wurde.

    Das Datum, an dem die Korrekturmaßnahme erstellt wird, wird im entsprechenden Überwachungsthema angezeigt. Weitere Informationen dazu, wie sich die Korrekturaufgaben, die den Korrekturmaßnahmen zugeordnet sind, von der Übertragung von Datensätzen auswirken, finden Sie unter Lebenszyklen von Korrekturmaßnahmen, Korrekturaufgaben und Datensätzen in den Vulnerability Response-Arbeitsbereichen.

Übertragen Sie Datensätze an Korrekturmaßnahmen in der Arbeitsbereich des Schwachstellenmanagers

Sie können Datensätze aus vorhandenen Korrekturmaßnahmen in neue Korrekturmaßnahmen in übertragen Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Wenn Sie mit einer Zero-Day-Bedrohung oder einer sehr kritischen Schwachstelle konfrontiert sind, die Sie schnell beheben möchten, sollten Sie alle aktiven Datensätze, die Sie bereits für diese Schwachstelle haben, in einer Korrekturmaßnahme konsolidieren. Jeder Datensatz kann jedoch nur in einer Aktion sein, und Datensätze können sich zwischen Überwachungsthemen überschneiden. Um sie alle zu erfassen, müssen Sie diese Datensätze aus mehreren vorhandenen Maßnahmen in eine Korrekturmaßnahme übertragen.

Angenommen, Sie haben eine Korrekturmaßnahme mit einer Schwachstelle mit hoher Priorität erstellt. Da diese Schwachstelle weit verbreitet ist und sich potenziell auf die anderen Bereiche in Ihrer Umgebung auswirkt, haben Sie möglicherweise Datensätze, die dieser Schwachstelle zugeordnet sind, bereits in vorhandenen Korrekturmaßnahmen. Um diese Datensätze so zu kombinieren, dass sie alle in einer Korrekturmaßnahme sind, können Sie alle Datensätze aus vorhandenen Korrekturmaßnahmen in eine neue Korrekturmaßnahme übertragen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können keine Datensätze aus wiederkehrenden Korrekturmaßnahmen in neue Korrekturmaßnahmen übertragen. Weitere Informationen finden Sie unter Erstellen Sie eine wiederkehrende Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers.

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Wählen Sie das Symbol „Überwachungsthemen“ aus.
3. Wählen Sie auf der Seite „Überwachungsthemen“ ein Überwachungsthema aus, für das Sie eine wiederkehrende Korrekturmaßnahme erstellen möchten.
4. Klicken Sie Auf **Erstellen Sie Eine Korrekturmaßnahme** .
   Das Modal „Korrekturmaßnahme erstellen“ wird angezeigt.
5. Füllen Sie im ersten Schritt „Aufwandsdetails“ die erforderlichen Felder aus.

   Geben Sie im Feld Kurzbeschreibung Text ein, der die wiederkehrende Korrekturmaßnahme beschreibt, mit der Sie sie finden und aus der Aufwandsliste nachverfolgen können.

   Geben Sie im Feld Beschreibung mehr Text zum Kontext der Maßnahme ein, damit Sie sie leicht aus der Liste der Korrekturmaßnahmen finden können. Beispiel: `Aktive log4j-Schwachstellen` .

   a. Geben Sie im Feld Name einen Namen für Ihre neue Korrekturmaßnahme ein.
   Standardmäßig wird der Name des Überwachungsthemas angezeigt.

   b. Geben Sie im Feld Beschreibung Text ein, der Ihnen hilft, diese Korrekturmaßnahme einfach aus der Liste der Korrekturmaßnahmen zu finden.

6. Klicken Sie auf **Next (Weiter)**.
   Details zur Aufgabengenerierung werden angezeigt.
7. Wählen Sie in Schritt 2, Aufgabengenerierung, eine Methode aus der Liste aus, um die Datensätze in den Korrekturaufgaben zu bündeln, die Sie aus dieser Korrekturmaßnahme generieren, nachdem sie erstellt wurde.
   - Nach Zuweisungsgruppe
   - Nach Zuweisungsgruppe und Konfigurationselement
   - Nach Zuweisungsgruppe und Schwachstelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

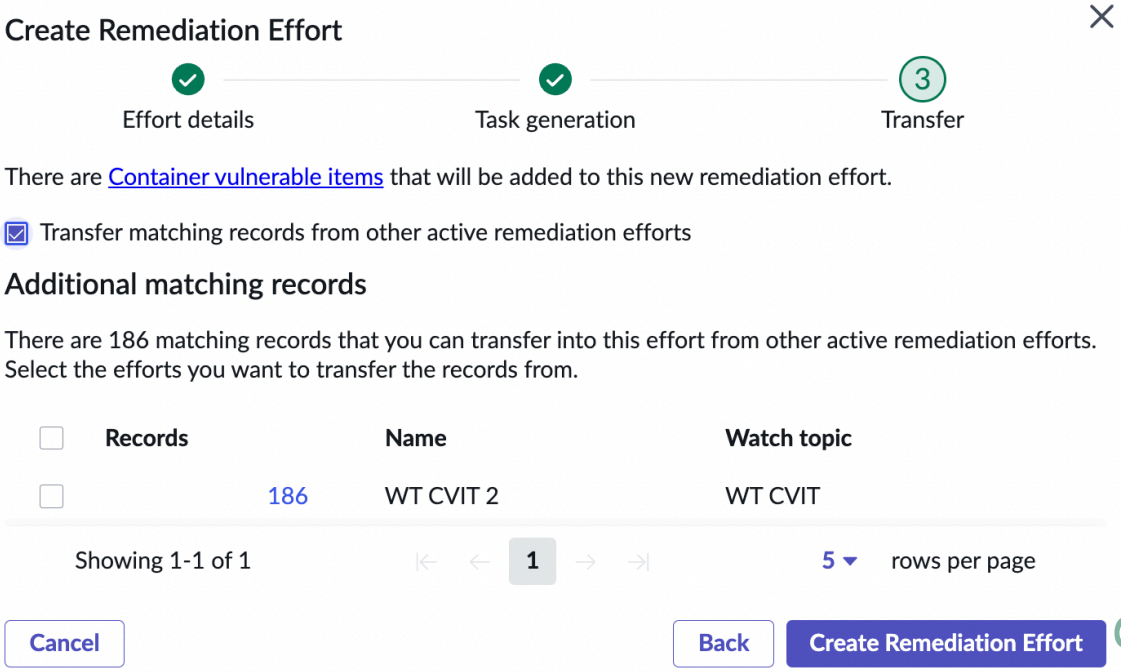
- Keine (es werden keine Korrekturaufgaben erstellt). Verwenden Sie diese Methode, wenn Sie einer Korrekturaufgabe für diese Maßnahme Datensätze manuell hinzufügen möchten. Weitere Informationen finden Sie unter Erstellen Sie eine Korrekturaufgabe bei Bedarf aus der Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers.

8. Um die doppelten angreifbaren Elemente automatisch zu aktualisieren, müssen Sie auswählen **Doppelte angreifbare Elemente für die erstellten Korrekturaufgaben automatisch aktualisieren** Option.
9. Klicken Sie auf **Next (Weiter)**.
10. Überprüfen Sie in Schritt 3 „Übertragen“, wie viele Datensätze der Korrekturmaßnahme hinzugefügt werden, und sehen Sie, wie viele Datensätze für die Übertragung von anderen aktiven Korrekturmaßnahmen verfügbar sind.
11. Um Datensätze aus anderen Maßnahmen zu übertragen, aktivieren Sie in der Liste die Kontrollkästchen für die gewünschten Datensätze.

    Wählen Sie aus **Übertragen Sie übereinstimmende Datensätze aus anderen aktiven Korrekturmaßnahmen** Aktivieren Sie das Kontrollkästchen, und aktivieren Sie dann die Kontrollkästchen für die Datensätze, die Sie von anderen aktiven Korrekturmaßnahmen übertragen möchten.

Automatische Übersetzung

Version 18,0 Erstellen Sie Eine Korrekturmaßnahme



12. Klicken Sie Auf **Erstellen Sie Eine Korrekturmaßnahme** .

    Nach einigen Minuten wird die neue Korrekturmaßnahme angezeigt. Je nach Anzahl der Datensätze kann dies einige Zeit dauern. Eine Nachricht gibt an, dass der Datensatz ausgefüllt wird.

    Die neue Korrekturmaßnahme wird mit allen Datensätzen erstellt, die aus dem zu ihrer Erstellung verwendeten Überwachungsthema verfügbar sind, zusätzlich zu allen Datensätzen, die Sie für die Übertragung aus vorhandenen Maßnahmen ausgewählt haben.

    Wenn Sie Datensätze auswählen, die von einer vorhandenen Maßnahme übertragen werden sollen, und die vorhandene Maßnahme alle ihre Datensätze in Ihre neue

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Maßnahme überträgt, wird die Korrekturmaßnahme, aus der Sie die Datensätze verschoben haben, geschlossen.

Hinweis:
Wenn weder Datensätze aus dem Überwachungsthema verfügbar sind noch Datensätze für die Übertragung ausgewählt sind, wird der **Erstellen Sie Eine Korrekturmaßnahme** Schaltfläche ist deaktiviert.

Weitere Informationen dazu, wie sich die Korrekturaufgaben, die den Korrekturmaßnahmen zugeordnet sind, von der Übertragung von Datensätzen auswirken, finden Sie unter Datensätze werden übertragen oder Datensatzübertragung .

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

Fügen Sie als Schwachstellenmanager oder -Analyst der Bibliothek „Ausgleichssteuerungen“ in eine Liste von Ausgleichssteuerungen hinzu Arbeitsbereich des Schwachstellenmanagers, Die für die Risikominderung von angreifbaren Host-Elementen und Korrekturaufgaben angewendet werden kann.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Einige häufig verwendete Ausgleichssteuerungen werden mit dem Basissystem geliefert. Sie können diese Ausgleichssteuerungen anzeigen, indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Listen** > **Bibliotheken** > **Ausgleichssteuerungen**an. Sie können diese Ausgleichssteuerungen entsprechend Ihren Anforderungen aktivieren oder deaktivieren.

Hinweis:
Die Funktion „Ausgleichssteuerungen“ ist nur für Host-Schwachstellen verfügbar.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Wählen Sie auf der Listenseite unter Bibliotheken die Option aus **Ausgleichssteuerungen** .
3. Klicken Sie auf **Neu**.
4. Füllen Sie die Felder im Formular Ausgleichssteuerungen erstellen aus.

Formularfelder für Ausgleichssteuerungen erstellen

Feld	Beschreibung
Name	Name der Ausgleichssteuerung, die als Option in angezeigt wird **Ausgleichssteuerungen** Dropdown-Liste des modalen Elements „Ausnahme anfordern“.
Beschreibung	Kurze Informationen, die Details zur Ausgleichssteuerung enthalten.
Aktiv	Status der Ausgleichssteuerung. Nur aktive Steuerungen werden in angezeigt **Ausgleichssteuerungen** Dropdown-Liste des modalen Elements „Ausnahme anfordern“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie **Speichern**.
6. Wählen Sie in der Liste Ausgleichssteuerungen unter Bibliotheken die gewünschte Ausgleichssteuerung aus, und wählen Sie aus **Bearbeiten** , Aktivieren oder deaktivieren Sie eine Ausgleichssteuerung, und klicken Sie auf **Speichern** Zum Ändern der Ausgleichssteuerungen.
   Alle aktiven Ausgleichssteuerungen werden als Option in angezeigt **Ausgleichssteuerungen** Dropdown-Liste des modalen Elements „Ausnahme anfordern“ für Risikoreduzierungsanforderungen.

Nächste Maßnahme

Ab v21.0 von Vulnerability Response, Sie können Ausgleichssteuerungen CVEs oder TPEs zuordnen, nachdem Sie der Bibliothek Ausgleichssteuerungen hinzugefügt haben. Weitere Informationen zum Zuordnen von Ausgleichssteuerungen finden Sie unter Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikoreduzierungsanforderungen zu.

Zugehörige Informationen

Erläuterungen zu Ausgleichssteuerungen Zur Risikominderung

Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikoreduzierungsanforderungen zu

Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum

Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikoreduzierungsanforderungen zu

Als Schwachstellenmanager oder -Analyst können Sie relevante Ausgleichssteuerungen einem Common Vulnerability Entry (CVE) oder einem Drittpartei-Eintrag (TPE) in zuordnen Arbeitsbereich des Schwachstellenmanagers, Die verwendet werden kann, um das von einer Schwachstelle ausgehende Risiko zu reduzieren.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird

- Wenn Sie einem CVE oder TPE keine Ausgleichssteuerungen zuordnen, werden alle aktiven Steuerungen im angezeigt Wählen Sie Ausgleichssteuerungen Aus Feld des Formulars „Ausnahme anfordern“.
- Wenn Sie einem CVE eine Ausgleichssteuerung zuordnen, wird diese Ausgleichssteuerung automatisch dem TPE zugeordnet, das dem CVE zugeordnet ist.

Hinweis:
Die Funktion „Ausgleichssteuerungen“ ist nur für Host-Schwachstellen verfügbar.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Öffnen Sie auf der Seite „Listen“ unter Bibliotheken eine der folgenden Elemente, denen Sie die Steuerungen zuordnen möchten:
   - **CVE** Aus der CVEs-Liste.
   - **TPE** Aus der TPEs-Liste.
3. Wählen Sie Aus **Ordnen Sie Steuerungen zu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die **Ordnen Sie Steuerungen zu** Die Schaltfläche wird nur angezeigt, wenn die Risikominderung für ein CVE oder TPE aktiviert ist. Mit anderen Worten: Sie können Ausgleichssteuerungen nur zuordnen, wenn die Risikominderung für ein CVE oder TPE aktiviert ist. Wenn **Ordnen Sie Steuerungen zu** Schaltfläche ist nicht sichtbar, wählen Sie aus **Aktivieren Sie die Risikominderung** .

4. Wählen Sie im Modal „Steuerungen zuordnen“ die Ausgleichssteuerungen aus, die zur Risikominderung auf Schwachstellen angewendet werden können, die mit CVE oder TPE verknüpft sind.
5. Wählen Sie **Absenden**.
   - Die zugehörigen Ausgleichssteuerungen werden auf der Registerkarte „anwendbare Ausgleichssteuerungen“ in der Datensatzansicht von CVE und TPE angezeigt.
   - Während ein Korrekturbesitzer eine Risikominderung anfordert, werden diese zugehörigen Ausgleichssteuerungen in angezeigt Wählen Sie Ausgleichssteuerungen Aus Feld im modalen Element „Ausnahme anfordern“.

Zugehörige Informationen

Erläuterungen zu Ausgleichssteuerungen Zur Risikominderung

Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum

Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

Als Schwachstellenmanager und -Analyst können Sie die Risikoreduzierungsanforderungen für die Host-Schwachstellen deaktivieren oder aktivieren, die einem Common Vulnerability Entry (CVE) oder zugeordnet sind Drittparteieintrag (TPE) in Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Risikominderung für CVE und TPE ist standardmäßig aktiviert.

Hinweis:
Die Funktion „Ausgleichssteuerungen“ ist nur für Host-Schwachstellen verfügbar.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.
   Öffnen Sie auf der Seite Listen unter Bibliotheken eine der folgenden Optionen, für die Sie die Risikoreduzierungsanforderungen deaktivieren möchten:
   - **CVE** Aus der CVEs-Liste.
   - **TPEs** Aus der TPEs-Liste.
2. Wählen Sie Aus **Deaktivieren Sie die Risikominderung** .
   Der Korrekturbesitzer kann keine Risikominderung für die angreifbaren Host-Elemente anfordern, die sich auf dieses CVE oder TPE beziehen. Mit anderen Worten: Anforderung zur Risikominderung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontrollkästchen wird nicht angezeigt, wenn **Grund** Ist als ausgewählt Ausgleichende Kontrolle vorhanden Im modalen Dialogfeld „Ausnahme anfordern“.

3. Um die Risikoreduzierungsanforderungen für angreifbare Host-Elemente zu aktivieren, wählen Sie aus **Aktivieren Sie die Risikominderung** .

Zugehörige Informationen

Erläuterungen zu Ausgleichssteuerungen Zur Risikominderung

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikoreduzierungsanforderungen zu

Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum

Scannen Sie Datensätze und Korrekturaufgaben in erneut Arbeitsbereich des Schwachstellenmanagers

Um sicherzustellen, dass Ihre Korrekturaufgaben und -Datensätze zwischen den geplanten Scanzyklen gelöst wurden, initiieren Sie erneutes Scannen über ServiceNow AI Platform Bei Bedarf.

Erforderliche Rolle: sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin.

Durch erneutes Scannen können Sie verifizieren, ob Ihre Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben haben.

Die Rapid7 Und Qualys Scanner sind standardmäßig in deaktiviert Vulnerability Response Anwendung. Wenn Sie versuchen, einen erneuten Scan von den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, wird der **Erneut Scannen** Schaltfläche ist nicht verfügbar.

So aktivieren Sie diese Scanner als Anwender mit der Rolle sn_vul.Vulnerability_admin:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**an.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um ihn zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

   Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle in den Datensätzen für angreifbare Elemente und Korrekturaufgaben angezeigt **Erneut Scannen** Ist als UI-Aktion verfügbar.

Erneutes Scannen wird für Datensätze und Korrekturaufgaben mit den folgenden Integrationen in unterstützt Arbeitsbereich des Schwachstellenmanagers. Weitere Informationen finden Sie in den folgenden Themen:

- Erneut Scannen Rapid7 Angreifbare Elemente aus dem Vulnerability Response Arbeitsbereiche
- Erneut Scannen Qualys Angreifbare Elemente aus dem Vulnerability Response Arbeitsbereiche
- Erneut Scannen Tenable.io Und Tenable.sc Angreifbare Elemente aus dem Vulnerability Response Arbeitsbereiche

Um erneutes Scannen in zu initiieren Arbeitsbereich des Schwachstellenmanagers Aus Datensätzen für angreifbare Elemente und Korrekturaufgaben benötigen die Datensätze einen unterstützten Scanner als Quelle.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Möglicherweise möchten Sie eine gefilterte Liste erstellen, die Datensätze nach ihrer Quelle anzeigt. Siehe Erstellen Sie eine anwenderdefinierte Liste von Datensätzen Ein Beispiel für das Erstellen einer Liste.

Bewerten Sie die Korrektureigenschaften der Datensätze in neu Arbeitsbereich des Schwachstellenmanagers

Bewerten Sie die Zuweisungen, das Korrekturzieldatum, die Korrekturaufgaben, Ausnahmen und die Risikopunktzahl für eine Reihe von Datensätzen (Vits, AVITs, CVITs oder TRs) in der Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Vor Version 23,0 von Vulnerability Response mussten die Regeln auf alle Datensätze angewendet werden, um die neuesten Zuweisungen, Korrekturzieldaten, Risikopunktzahlen und Korrekturaufgaben zu erhalten. Dies war ein zeitaufwändiger Prozess. Ab Version 23.0 können Sie diese Eigenschaften für bestimmte Datensätze selektiv auswerten und aktualisieren, wodurch die Verarbeitungszeit reduziert wird. Darüber hinaus können Sie den Korrekturprozess basierend auf diesen aktualisierten Eigenschaften verfeinern. Ab v24.0.6 von Vulnerability Response können Sie die Ausnahmeregeln für ausgewählte Datensätze in auswerten Arbeitsbereich des Schwachstellenmanagers.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Öffnen Sie auf der Listenseite die Liste aktiv oder alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Anwendungselemente
   - Angreifbare Container-Elemente
   - Konfigurationstestergebnisse
3. **Wahlweise:** Aktivieren Sie das Kontrollkästchen der gewünschten Datensätze, um nur die ausgewählten Datensätze zu aktualisieren, indem Sie die Option ausgewählte Elemente im Modal auswählen.
4. Wählen Sie aus **Neu bewerten** Schaltfläche.
5. Wählen Sie im Modal „Korrektureigenschaften neu bewerten und aktualisieren“ die Eigenschaften aus, die Sie für die ausgewählten Datensätze aktualisieren möchten.

   Hinweis:
   Wenn Sie eine Eigenschaft auswählen, werden ihre abhängigen Eigenschaften automatisch ausgewählt.

6. Wählen Sie **Übernehmen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Die Eigenschaften werden für die ausgewählten Datensätze aktualisiert. Sie können überprüfen **Arbeitsnotizen** Der Datensätze für die vorherigen und neuesten Werte der aktualisierten Korrektureigenschaften.

Direkte Zurückstellung angreifbarer Elemente (Vits) nach Ausnahmeregeln ohne Erstellung von Korrekturaufgaben

Ausnahmeregeln werden direkt auf die angreifbaren Elemente (VIT) angewendet, wodurch der Prozess zum Erstellen einer Korrekturaufgabe entfällt. Automatisch – die Spalte „Ausnahmeregel“ wird der Formularansicht hinzugefügt, wodurch die aktuelle Ausnahmeregel ausgefüllt wird, die auf das angreifbare Element (VIT) angewendet wird.

Genehmigung der Ausnahmeregel/erneute Anwendung:

Eine Ausnahmeregel wird für ein bestimmtes angreifbares Element (VIT) erstellt, das sich in befindet **Offen, wird untersucht, wartet auf Implementierung** status anfänglich. Sobald die Regel genehmigt wurde, wird sie von einer täglichen, nächtlichen geplanten Aufgabe verarbeitet, die die Ausnahmeregel erneut anwendet.

Wenn die geplante Aufgabe ausgeführt wird und die VIT aufgrund einer falschen Zuordnung von VIT zur Ausnahmeregel zurückgestellt (verschoben) wird, wird die VIT durch die geplante Aufgabe erneut geöffnet, um eine neue Ausnahmeregel erneut anzuwenden.

Eine neue Regel mit einer späteren Ausführungsreihenfolge kann auch aktiviert werden, um die vorherige zu ersetzen.

Hinweis:
Das Datum „Zurückgestellt bis“ ist standardmäßig auf 12 Monate festgelegt, und Sie können ihn nach Bedarf über die Seite „Konfigurationseinstellungen für Ausnahmemanagement“ bearbeiten. Wenn Sie versuchen, ein Zurückstellungsdatum nach dem Standarddatum auszuwählen, löst das System einen Fehler aus.

Verarbeitung von abgebrochenen oder gelöschten Ausnahmeregeln:

Wenn die alte Ausnahmeregel abgebrochen oder gelöscht wird, wird ein Hintergrundauftrag ausgelöst, um:

- Öffnen Sie alle zugeordneten Vits.
- Verschieben Sie die Ausnahmeregel in den Entwurfsstatus, wenn die Regel abgebrochen wird.
- Wenden Sie eine neue Ausnahmeregel auf die Vits an. (Wenn eine anwendbare Ausnahmeregel vorhanden ist, wird ihr die VIT zugeordnet, und der VIT-Status wird zurückgestellt).

Neue VIT-Erstellung (Einfügung):

Wenn eine neue VIT erstellt wird (z. B. eine Erfassung), wird ihr automatisch die Ausnahmeregel zugewiesen. Die neue VIT wird auch mit derselben Begründung und demselben bis-Datum zurückgestellt, wobei der gleiche Prozess wie beim Abbrechen einer Ausnahmeregel ausgeführt wird.

Im VM Manager Workspace ist ein klickbarer Link verfügbar, um direkt auf die Ausnahmeregel zuzugreifen, sodass der Anwender sehen kann, welche Ausnahmeregel sich auf eine bestimmte VIT auswirkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die Listenansicht in Arbeitsbereich des Schwachstellenmanagers

Die Listenansicht in Arbeitsbereich des Schwachstellenmanagers Ermöglicht Schwachstellen- und Sicherheitsmanagern und Analysten, den Korrekturfortschritt in Datensätzen anzuzeigen, Detailinformationen in Vulnerability Response-Datensätzen anzuzeigen und den Status ihrer Genehmigungsanforderungen und Ausnahmen anzuzeigen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Klicken Sie oben links im Arbeitsbereich mit der angezeigten Homepage auf **Liste** Symbol.
3. **Wahlweise:** Klicken Sie Auf **Meine Listen** Um eine Liste zu erstellen.
   Weitere Informationen zum Erstellen einer Liste finden Sie unter Erstellen Sie eine anwenderdefinierte Liste von Datensätzen.
4. In der folgenden Tabelle finden Sie die Aktionen, die Sie auf der Listenseite ausführen können.

UI-Aktion	Beschreibung
Öffnen Sie eine Korrekturmaßnahme	Mit **Aktiv** Unter ausgewählt **Korrekturmaßnahmen** Liste klicken Sie auf einen Link zur Korrekturmaßnahme, um ihn zu öffnen. Eine Korrekturmaßnahme ist eine Reihe von Datensätzen, die einem Überwachungsthema zugeordnet sind. Die in einer Korrekturmaßnahme aufgeführten Datensätze sind statisch. Sie werden nicht durch neue Importdaten oder Änderungen aktualisiert, die Sie zur Überwachung von Themen vornehmen. Die zugehörigen Listenelemente im Datensatz der Korrekturmaßnahme ermöglichen es Ihnen, den Gesamtfortschritt und den Status der Korrekturmaßnahme in den zugehörigen Datensätzen anzuzeigen. Weitere Details und UI-Aktionen, die Sie aus einer Korrekturmaßnahme ausführen können, finden Sie unter Verwenden Sie Datensätze für Korrekturmaßnahmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UI-Aktion	Beschreibung
Links neben der Spalte Nummer mit einer angezeigten Liste bewegen Sie den Mauszeiger über eine Zeile, und klicken Sie auf das Symbol für kleine Informationen **(i)** Für einen Datensatz.	Details zu den Datensätzen werden im rechten Seitenbereich der Seite angezeigt. Details: ○ Zuweisungsgruppe ○ Schwachstelle ○ Zugewiesen an ○ Kurzbeschreibung ○ Beschreibung Sie können die Felder bearbeiten. Wenn das Kontrollkästchen aktiv angezeigt wird, können Sie den Datensatz aktivieren oder deaktivieren. Klicken Sie auf **Aktualisieren** Um Ihre Änderungen zu speichern.
Liste aktualisieren	Mit dem Aktualisierungssymbol oben rechts auf der Seite laden Sie die aktuelle Seite neu.
Breiten zurücksetzen	Klicken Sie auf das Zahnradsymbol, um die Spaltenbreiten in Ihren Listen anzupassen. Eine Kopie der ursprünglichen Liste wird unter gespeichert **Ihre Listen** .
Kopieren Sie die URL für die angezeigte Seite	Kopieren Sie die URL zur Verwendung an anderer Stelle.
Exportieren Sie die Seite	Geben Sie im Modal die Datei- und Bereitstellungstypen ein, und klicken Sie auf **Exportieren** .
Filter für die Daten auf der Seite verfeinern.	Wählen Sie eine Spalte aus, und erweitern Sie das Menü mit drei vertikalen Punkten, um Optionen anzuzeigen, die die Daten in der Spalte weiter filtern. Sie könnten beispielsweise die Spalte Zuweisungsgruppe aus der Liste der aktiven Korrekturaufgaben nach einer bestimmten Zuweisungsgruppe filtern.
Filtern Sie Elemente aus einer Zeile in einer Spalte heraus, oder gleichen Sie Elemente ab	Wählen Sie eine Zelle in einer Spalte aus, und verfeinern Sie die angezeigten Daten, indem Sie eine auswählen: ○ Übereinstimmung anzeigen: Zeigen Sie nur Elemente an, die der ausgewählten Zelle in der Spalte entsprechen. ○ Herausfiltern: Filtert die Elemente aus der Spalte heraus, die der ausgewählten Zelle in der Spalte entsprechen.

5. Erstellen Sie ein angreifbares Anwendungselement aus dem **Aktiv** Oder **Alle** Liste unter *`Application Vulnerable items`*Indem Sie auf klicken **Neu** Schaltfläche oben rechts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine anwenderdefinierte Liste von Datensätzen

Sie können eine anwenderdefinierte Liste in erstellen Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Wählen Sie aus **Liste** Symbol und klicken Sie auf **Meine Listen** .
3. Wählen Sie Aus **Neue Liste** .
4. Klicken Sie im Modal „neue Liste“ auf **Von vorhandenem starten** Und suchen Sie in der Listenauswahlliste nach einer vorhandenen Liste, die als Vorlage verwendet werden soll.
5. Bearbeiten Sie den Listennamen.
6. Fügen Sie Filter hinzu.
   Sie können beispielsweise eine Liste aktiver Datensätze für einen bestimmten Scanner erstellen, den Sie auf erneute Scans überwachen möchten. Sie können die Filter verwenden: „Aktiv“ ist „wahr“ , Und Quelle enthält (Name Ihres Scanners) .
7. Bearbeiten Sie die Spalten, die in Ihrer Liste angezeigt werden sollen.
8. Klicken Sie auf **Erstellen**.
   Ihre neue Liste wird angezeigt.
9. Alternativ können Sie auf klicken **Erstellen Sie Ihre eigenen** , Geben Sie einen Namen gefolgt von ein **Wählen Sie Quelle Aus** .
10. Beginnen Sie mit der Eingabe in das Feld, und wählen Sie aus den Quellen aus, die für Ihre neue Liste angezeigt werden.
11. Klicken Sie auf **Erstellen**.
    Ihre neue Liste wird angezeigt.

    Hinweis:
    Wenn Sie das Listenmodul verlassen, wird die Liste angezeigt, die beim Beenden angezeigt wird, wenn Sie zurückkehren.

12. Klicken Sie auf das Zahnradsymbol oben rechts auf der Seite, um eine Liste mit der angezeigten Liste zu löschen.

Erstellen Sie eine Korrekturaufgabe manuell in Arbeitsbereich des Schwachstellenmanagers

Ab v25.0.4 von Vulnerability Response, Sie können Korrekturaufgaben manuell aus den Listen angreifbarer Host-Elemente, angreifbare Anwendungselemente, angreifbare Container-Elemente und Konfigurationstestergebnisse auf der Listenseite von erstellen Arbeitsbereich des Schwachstellenmanagers. Sie können Korrekturaufgaben auch aus den Drilldown-Listen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erstellen, die angezeigt werden, wenn Sie auf die Visualisierungen auf der Homepage klicken.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.write_all, sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_write_all oder sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.write_all, sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.write oder sn_vulc.admin für Konfigurationstestergebnisse (TRs)

Warum und wann dieser Vorgang ausgeführt wird

Manuelle Erstellung von Korrekturaufgaben (RTS) in Arbeitsbereich des Schwachstellenmanagers Bietet granulare Kontrolle über das Management von Korrekturaufgaben, indem Sie Datensätze (Vits, CVITs, AVITs oder TRs) dynamisch in Echtzeit in Korrekturaufgaben gruppieren können.

Sie können eine Korrekturaufgabe manuell erstellen, wenn Sie:

- Gruppieren Sie angreifbare Elemente nach etwas anderem als den Regelkriterien für Korrekturaufgaben. Sie können beispielsweise Korrekturaufgaben für einen bestimmten Manager oder für aktive, neue Exploits wie Ransomware erstellen, die verschiedene Schwachstellen enthält.
- Gruppieren Sie nicht gruppierte Datensätze.
- Regeln für Korrekturaufgaben sind inaktiv.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste**an.
2. Öffnen Sie auf der Listenseite die **Aktiv** Oder **Alle** Listen Sie in einer der folgenden Listen auf:
   - Angreifbare Host-Elemente
   - Angreifbare Anwendungselemente
   - Angreifbare Container-Elemente
   - Konfigurationstestergebnisse
3. **Wahlweise:** Aktivieren Sie das Kontrollkästchen der Datensätze, die Sie aktualisieren möchten, und wählen Sie dann aus Ausgewählte Elemente Option im Feld Datensatzauswahl im Modal „Korrekturaufgabe erstellen“.
4. Wählen Sie Aus **Erstellen Sie Eine Korrekturaufgabe** .
5. Geben Sie im Modal „Korrekturaufgabe erstellen“ die folgenden Details ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modales Element „Korrekturaufgabe erstellen“

Feld	Beschreibung
Datensatzauswahl	○ **Ausgewählte Elemente** : Aktualisiert nur die ausgewählten Datensätze. ○ **Alle Elemente** : Aktualisiert alle Datensätze in der Liste.
Kurzbeschreibung	Kurze Notiz zu den Korrekturaufgaben.
Gruppierungskriterien	Die Auswahlmöglichkeiten lauten wie folgt: ○ **Zuweisungsgruppe** : Datensätze mit derselben Zuweisungsgruppe werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Konfigurationselement** : Datensätze mit derselben Zuweisungsgruppe und demselben Konfigurationselement werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Schwachstelle** : Datensätze mit derselben Zuweisungsgruppe und Schwachstelle werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Risikobewertung** : Datensätze mit derselben Zuweisungsgruppe und Risikobewertung werden in einer Korrekturaufgabe gruppiert.
Datensätze in anderen Korrekturaufgaben werden verwaltet.	Die Auswahlmöglichkeiten lauten wie folgt: ○ **Überspringen Sie Datensätze für neue Korrekturaufgaben** : Für die Datensätze, die Teil anderer Korrekturaufgaben sind, wird keine Aktion ausgeführt. ○ **Wechseln Sie zu neuen Korrekturaufgaben** : Datensätze, die Teil anderer Korrekturaufgaben sind, werden an neue Korrekturaufgaben übertragen. ○ **Behalten Sie sowohl aktuelle als auch neue Korrekturaufgaben bei** : Datensätze, die Teil anderer Korrekturaufgaben sind, werden sowohl in alten als auch in neuen Korrekturaufgaben aufbewahrt.

6. Wählen Sie Aus **Erstellen Sie eine Korrekturaufgabe** .

Ergebnisse

Korrekturaufgaben werden basierend auf den Gruppierungskriterien erstellt. Eine E-Mail-Benachrichtigung wird an die Korrekturbesitzer in der Zuweisungsgruppe gesendet, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sie darüber informiert, dass eine Korrekturaufgabe erstellt und ihrer Gruppe zugewiesen wurde. Beispiele dafür, wie Korrekturaufgaben basierend auf den Gruppierungskriterien erstellt werden, finden Sie unter Beispiele für die Erstellung von Korrekturaufgaben in Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen.

Aktivieren oder deaktivieren Sie den Import von Testergebnissen für einen Qualys Testgruppe

Ab v23.0 von Vulnerability Response, Steuern Sie den Import der Testergebnisse für die Tests in Qualys Testgruppe mit verwenden **Import aktivieren/deaktivieren** Schaltfläche, die in der Datensatzansicht der Testgruppe verfügbar ist.

Vorbereitungen
Erforderliche Rolle: sn_vulc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Listen**an.
2. Öffnen Sie in den Bibliotheken unter der Liste Testgruppen eine Qualys Testgruppe in der Datensatzansicht.
3. Deaktivieren Sie den Import der Testergebnisse, die einem zugeordnet sind Qualys Testen Sie die Gruppe, indem Sie auswählen **Import deaktivieren** Schaltfläche.
   Bei der bevorstehenden Datenerfassung werden die Testergebnisse für nicht importiert Qualys Testgruppe. Der Wert in **Ist Import deaktiviert** Feld ändert sich in *Wahr* .
4. **Wahlweise:** Aktivieren Sie den Import der Testergebnisse, indem Sie auswählen **Aktivieren Sie den Import** Schaltfläche.

Ändern Sie den Schweregrad für ein CVE oder TPE

Als Schwachstellenmanager oder -Analyst können Sie den Schweregrad von Common Vulnerability Entry (CVE) oder TPE (Drittpartei-Eintrag) im Arbeitsbereich des Schwachstellenmanagers ändern.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager, sn_vul.App_Developer für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Listen** > **Bibliotheken**an.
2. Öffnen Sie den entsprechenden Eintrag:
   - **CVEs (NVD)** : Zum Ändern des Schweregrads eines CVE.
   - **TPEs** : Zum Ändern des Schweregrads eines TPE.
3. Wählen Sie Aus **Ändern Sie den Schweregrad** Von **Weitere Aktionen**Symbol ...
4. Wählen Sie den neuen Schweregrad aus der Dropdown-Liste aus.
5. Geben Sie eine Begründung für Ihr Update an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie **Absenden**.

Hinweis:

- Sie können den ursprünglichen Quellschweregrad mithilfe von wiederherstellen **Schweregrad Zurücksetzen** Option von **Weitere Aktionen** Menü. Diese Option wird erst angezeigt, nachdem Sie den Schweregrad geändert haben.
- Die **Schweregrad geändert** Das Feld wird nur angezeigt, wenn Sie den Quellschweregrad ändern. Wenn Sie es auf den ursprünglichen Wert zurücksetzen, wird das Feld entfernt.
- Das System verwendet **Schweregrad geändert** Für Risikoberechnungen ab der nächsten geplanten Aufgabe. Wenn der Schweregrad zurückgesetzt wird, wird stattdessen der ursprüngliche Quellschweregrad angewendet.

Genehmigen oder lehnen Sie Anforderungen in ab Arbeitsbereich des Schwachstellenmanagers

Genehmigen oder lehnen Sie Anforderungen ab, die von Korrekturbesitzern übermittelt werden.

Vorbereitungen

Erforderliche Rollen:

Genehmigerrollen, die für verschiedene Genehmigungsanforderungen erforderlich sind

Genehmigungstyp	Genehmigungsebenen erforderlich	Genehmigerrollen	Zusätzliche Information
Falsch positive Genehmigungen	Eins	• Granulare Rolle sn_vul.false_positive_Approver für angreifbare Elemente (Vits). • Rolle „sn_vul.App_false_positive_Approver“ für angreifbare Anwendungselemente (AVITs) • Rolle „sn_vul_Container.false_positive_Approver“ für angreifbare Container-Elemente (CVITs) • sn_vulc.false_positive_Approver für Konfigurationstestergebnisse Oder Genehmiger müssen sich in der Anwendergruppe „falsch positive	-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigerrollen, die für verschiedene Genehmigungsanforderungen erforderlich sind (Fortsetzung)

Genehmigungstyp	Genehmigungsebenen erforderlich	Genehmigerrollen	Zusätzliche Information
		Genehmiger“ befinden.	
Ausnahmegenehmigungen (Zurückstellungen)	Zwei	• In der Gruppe „Genehmiger – Ebene 1“ ist ein Genehmiger erforderlich • In der Gruppe „Genehmiger – Ebene 2“ ist ein Genehmiger erforderlich	Eine Ausnahmeanforderung für einen Datensatz oder eine Korrekturaufgabe wird mit einem standardmäßigen Genehmigungs-Workflow auf zwei Ebenen genehmigt. Die Ausnahmeanforderung erfordert zwei Ebenen von Genehmigern. Nachdem die Anforderung vom Genehmiger der Ebene 1 genehmigt wurde, wird sie an den Genehmiger der zweiten Ebene gesendet und ist dann in der Warteschlange des Genehmigers 2 sichtbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigerrollen, die für verschiedene Genehmigungsanforderungen erforderlich sind (Fortsetzung)

Genehmigungstyp	Genehmigungsebenen erforderlich	Genehmigerrollen	Zusätzliche Information
Heben Sie die Zuweisung von Genehmigungen auf	In der Gruppe „Genehmiger – Ebene 1“ ist ein Genehmiger erforderlich	• sn_vul.unassign_Appr für AVITs und Vits • sn_vul_Container.una für CVITs • sn_vulc.unassign_App für Konfigurationsproble (CIs)	**Hinweis:** Standardmäßig wird eine Genehmigungskonfiguration bereitgestellt, und eine Genehmigungsgruppe zum Aufheben der Zuweisung wird erstellt. Anwender (Genehmiger-Zuweisung aufheben – Ebene 1) dieser Gruppe können die Anforderung genehmigen. Diese Gruppe enthält standardmäßig die Rolle „Genehmiger aufheben“, sn_vul.unassign_Approver. Sie können eine neue Gruppe ändern oder erstellen und die Genehmigungskonfiguration aktualisieren. Um Genehmigungsregeln zu konfigurieren, navigieren Sie zum jeweiligen Modul „Genehmigungsregeln“, wählen Sie eine der folgenden Genehmigungsregeln aus, und navigieren Sie zur Genehmigungskonfiguration in **Genehmigungskonfigurationen** Registerkarte: • *Vulnerable item field change request* Für ein angreifbares Element. • *Vulnerability field change*

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc., in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigerrollen, die für verschiedene Genehmigungsanforderungen erforderlich sind (Fortsetzung)

Genehmigungstyp	Genehmigungsebenen erforderlich	Genehmigerrollen	Zusätzliche Information
Genehmigungen zur Risikominderung	Zwei	• In der Gruppe „Genehmiger – Ebene 1“ ist ein Genehmiger erforderlich • In der Gruppe „Genehmiger – Ebene 2“ ist ein Genehmiger erforderlich	Der Genehmigungs-Flow für die Risikominderung ist mit den Ausnahmegenehmigungen (Zurückstellungen) identisch.

Siehe Vulnerability Response Personas und granulare Rollen Und Weisen Sie zu Vulnerability Response Persona-Rollen mit Setup-Assistent Weitere Informationen zum Zuweisen von Persona-Rollen zu Anwendern und Anwendern zu Gruppen.

Hinweis:
Fügen Sie den Genehmigungsgruppen Anwender hinzu, bevor Sie Genehmigungsanforderungen übermitteln. Wenn Sie Anforderungen erstellen, bevor Sie den Genehmigungsgruppen Anwender hinzufügen, sind die Anforderungen möglicherweise nicht für die Anwender sichtbar, die über die Genehmigungsberechtigung verfügen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.
   Wenn ein Genehmiger keinen Zugriff auf den Arbeitsbereich hat, können Genehmigungen unter verarbeitet werden **Vulnerability Response** > **Meine Genehmigungen** In der klassischen Umgebung.
2. Wählen Sie das Symbol Listenansicht ( ).
   Die Listenseite wird angezeigt.
3. Wählen Sie in der Liste gefilterte Genehmigungen die Option aus **Mir zugewiesen** .
4. Suchen Sie nach einer Anforderung, die Sie verarbeiten möchten, und wählen Sie dann den Link in der Spalte Status aus.
   Der Datensatz „Change-Genehmigung des Schwachstellenstatus“ (VCA#) wird angezeigt.
5. Wählen Sie eine der folgenden Optionen aus, um die Anforderung zu genehmigen oder abzulehnen.

Richten Sie E-Mail-Benachrichtigungen in ein Vulnerability Response Arbeitsbereiche

Identifizieren Sie Anwender für automatische E-Mail-Erinnerungen, die an Anwender in der Anwendergruppe „Korrekturbesitzer“ gesendet werden.

Vorbereitungen
Erforderliche Rolle: Administrator

Diese Funktion generiert automatisch einen E-Mail-Digest für Anwender in der Anwendergruppe „Korrekturbesitzer“. Fügen Sie alle Anwender hinzu, die Sie E-Mail-Benachrichtigungen erhalten möchten, wie in beschrieben Verwenden Sie den E-Mail-Digest in den Vulnerability Response-Arbeitsbereichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie, ob Anwender eine aktive E-Mail-Adresse in ihren Anwenderdatensatz eingegeben haben und ob Sie sie der Anwendergruppe „Korrekturbesitzer“ hinzugefügt haben.

Wenn Sie die Zustellhäufigkeit, den Tag oder die Uhrzeit der E-Mails ändern oder die Funktion deaktivieren möchten, gehen Sie wie folgt vor.

Prozedur

1. Navigieren zu **Alle** > **Geplante Aufgaben**an.
2. Suchen Sie nach **Generieren Sie den Korrektur-Digest** Und klicken Sie darauf, um den Datensatz zu öffnen.

   Möglicherweise möchten Sie die Felder in ihren Standardeinstellungen belassen, bis Sie verifiziert haben, dass Benachrichtigungen gesendet werden. Standardmäßig werden E-Mails wöchentlich am Montagmorgen um 9:00 UHR in der Zeitzone der Instanz gesendet, die den Auftrag ausführt.
3. Ändern Sie die Felder im Formular.
   Weitere Informationen zu den Formularfeldern finden Sie unter Generieren Sie Formularfelder für Korrektur-Digest.
4. Klicken Sie auf **Aktualisieren**.

Nächste Maßnahme

Wenn Sie überprüft haben, dass alle zuvor aufgeführten Informationen korrekt sind und Sie Anwender in der Anwendergruppe „Korrekturbesitzer“ haben, die E-Mails jedoch nicht wie erwartet gesendet werden, überprüfen Sie, ob Kanäle aktiviert sind, um E-Mail-Benachrichtigungen zu erhalten. Weitere Informationen finden Sie unter Create notification channels .

Korrektur angreifbarer Elemente und Testergebnisse in Arbeitsbereich für Sicherheits- und Gesundheitsschutzmanagement

In Arbeitsbereich des Schwachstellenmanagers, Sie können angreifbare Elemente und Testergebnisse in einem Überwachungsthema nachbessern, indem Sie eine Bedingung definieren, und Sie können ihren Korrekturfortschritt nachverfolgen, indem Sie Korrekturmaßnahmen erstellen.

Massenbearbeitung in verwenden Arbeitsbereich des Schwachstellenmanagers

In Arbeitsbereich des Schwachstellenmanagers, Sie können den Status der Datensätze aktualisieren, Ausnahmen und falsch positive Ergebnisse anfordern und einer Zuweisungsgruppe mehrere angreifbare Elemente (Vits, AVITs oder CVITs) gleichzeitig mit der Massenbearbeitungsfunktion zuweisen.

Die Massenbearbeitungsfunktion ist verfügbar für:

- Angreifbare Host-Elemente (Vits) ab v21.0 von Vulnerability Response.
- Angreifbare Anwendungselemente (AVITs) und angreifbare Container-Elemente (CVITs) ab v22.0 von Vulnerability Response.
- Testergebnisse ab v23.0 von Vulnerability Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktualisieren Sie den Status von Datensätzen im Massenvorgang Arbeitsbereich des Schwachstellenmanagers

Aktualisieren Sie den Status mehrerer Datensätze (Vits, AVITs oder CVITs) gleichzeitig entsprechend ihrem Korrekturfortschritt mithilfe der Massenbearbeitungsfunktion in Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste**an.
2. Öffnen Sie auf der Listenseite die Liste aktiv oder alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Container-Elemente
   - Angreifbare Anwendungselemente
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie verwenden möchten **Nur Ausgewählte Elemente** Option in **Datensatzauswahl** Feld.
   - Wenden Sie Filter an, wenn Sie verwenden möchten **Alle angreifbaren Elemente, die dem Filter entsprechen** Option in **Datensatzauswahl** Feld.
4. Wählen Sie aus **Massenbearbeitung** Schaltfläche.
5. Füllen Sie im modalen Dialogfeld „Massenbearbeitung“ die folgenden Felder aus, um den Status der Datensätze zu aktualisieren.

Modale Felder für Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nur ausgewählte Elemente: Wählen Sie diese Option aus, wenn Sie die mit dem Kontrollkästchen ausgewählten Datensätze aktualisieren möchten. ○ Alle angreifbaren Elemente, die dem Filter entsprechen: Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ Korrekturaufgabe: Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren möchten, und wählen Sie dann die gewünschte Korrekturaufgabe in aus **Korrekturaufgabe** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Schwachstelleneintrag: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die für einen allgemeinen angreifbaren Eintrag (CVE) spezifisch sind, und wählen Sie dann das CVE im aus **Schwachstelleneintrag** Feld. **Hinweis:** Datensätze mit ungültigem CI oder außer Betrieb genommenem CI werden nicht aktualisiert.
Status	Ändern Sie für **Status** Im Datensatz. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nicht aktualisieren ○ Öffnen ○ Wird untersucht ○ Warten auf Implementierung ○ Zurückgestellt Weitere Informationen finden Sie unter Fordern Sie eine Massenausnahme im Vulnerability Manager-Arbeitsbereich an. ○ Geschlossen Weitere Informationen finden Sie unter Massenbearbeitung für falsch positive Werte im Vulnerability Manager-Arbeitsbereich ○ Gelöst **Hinweis:** Nur die Datensätze, für die der Statusübergang gültig ist, werden aktualisiert.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Wählen Sie Aus **Bearbeiten** .

Ein asynchroner Massenbearbeitungsauftrag aktualisiert die ausgewählten Datensätze.

Massenbearbeitung angreifbarer Host-Elemente mit Patches und Lösungen

Empfehlen Sie einen Patch oder eine Lösung für mehrere angreifbare Host-Elemente, die gleichzeitig die Massenbearbeitungsfunktion in verwenden Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle: sn_vul.Vulnerability_Analyst, sn_vul.Vulnerability_admin und jede Rolle mit der granularen Rolle „sn_vul.Bulk_Edit“.

Warum und wann dieser Vorgang ausgeführt wird

Im Modal „Massenbearbeitung“ können Sie beim Hinzufügen einer bevorzugten Lösung und eines bevorzugten Patches auch die Zuweisung mehrerer angreifbarer Host-Elemente (Vits) aufheben oder gleichzeitig einer Zuweisungsgruppe zuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.

   Hinweis:
   Die ausgewählten Datensätze müssen sich im Status Offen, wird untersucht oder wartet auf Implementierung befinden.

2. Öffnen Sie auf der Listenseite unter angreifbare Host-Elemente die Liste aktiv oder alle.
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie verwenden möchten **Nur Ausgewählte Elemente** Option in **Datensatzauswahl** Feld.
   - Wenden Sie Filter an, wenn Sie verwenden möchten **Alle angreifbaren Elemente, die dem Filter entsprechen** Option in **Datensatzauswahl** Feld.
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie verwenden möchten **Nur Ausgewählte Elemente** Option in Datensatzauswahlfeld des Modals „Massenbearbeitung“.
   - Wenden Sie Filter an, wenn Sie verwenden möchten **Alle angreifbaren Elemente, die dem Filter entsprechen** Option in Datensatzauswahlfeld des Modals „Massenbearbeitung“.
4. Wählen Sie aus **Massenbearbeitung** Schaltfläche.
5. Füllen Sie im modalen Dialogfeld „Massenbearbeitung“ die Felder aus, um einen Patch oder eine Lösung für mehrere angreifbare Host-Elemente zu empfehlen.

Modale Felder für Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nur ausgewählte Elemente: Wählen Sie diese Option aus, wenn Sie die mit dem Kontrollkästchen ausgewählten Datensätze aktualisieren möchten. ○ Alle angreifbaren Elemente, die dem Filter entsprechen: Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ Korrekturaufgabe: Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren möchten, und wählen Sie dann die gewünschte Korrekturaufgabe in aus **Korrekturaufgabe** Feld. ○ Schwachstelleneintrag: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die für einen allgemeinen angreifbaren Eintrag (CVE) spezifisch sind, und wählen Sie dann das CVE im aus **Schwachstelleneintrag** Feld. **Hinweis:** ○ Datensätze mit ungültigem CI oder außer Betrieb genommenem CI werden nicht aktualisiert. ○ Nur die Datensätze (Vits) in Offen, wird untersucht oder wartet auf Implementierung status werden aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Ändern Sie für **Status** Der angreifbaren Host-Elemente. Sie können bevorzugte Lösungen und Patches nur hinzufügen, wenn Sie die folgenden status auswählen. ○ Nicht aktualisieren ○ Öffnen ○ Wird untersucht ○ Warten auf Implementierung
Bevorzugte Lösung	Lösung, die auf die Korrektur aller angreifbaren Elemente ausgerichtet ist, die für die Massenbearbeitung ausgewählt wurden. Wählen Sie den Change für aus **Bevorzugte Lösung** Feld im angreifbaren Element. Auswahlmöglichkeiten stammen aus einer Suchliste verfügbarer bevorzugter Lösungen für die ausgewählten Vits. **Hinweis:** ○ Der Satz der verfügbaren bevorzugten Lösungen ist ein Schnittpunkt aller potenziellen Lösungen der Schwachstellen in allen ausgewählten Vits. ○ Bei Auswahl von **Datensatzauswahl** > **Schwachstelleneintrag** Für eine Massenbearbeitung werden alle Vits für die Schwachstelle auf die ausgewählte bevorzugte Lösung festgelegt. **Hinweis:** Dieser Vorgang legt nicht fest **Bevorzugte Lösung** Auf der Ebene des Schwachstelleneintrags. Wird festgelegt **Bevorzugte Lösung** Auf der Ebene des Schwachstelleneintrags würde festlegen **Bevorzugte Lösung** Für alle neuen Vits in Zukunft. Die Massenbearbeitung ändert nur den aktuellen Satz von Vits. ○ Eindeutige Schwachstellen für die Auswahlkriterien sind auf 500 beschränkt. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, Vits mit verschiedenen Kriterien zum Festlegen von auszuwählen **Bevorzugte Lösung** . ○ Die Gesamtzahl der Lösungen, die in der Suchliste angezeigt werden können, ist auf 170 begrenzt. Wenn mehr als 170 Lösungen vorhanden sind, wird eine Warnmeldung angezeigt. Der aktualisierte Wert wird in der Listenansicht der angreifbaren Elemente angezeigt.
Bevorzugter Patch	Patch, der darauf ausgerichtet ist, alle für die Massenbearbeitung ausgewählten angreifbaren Elemente zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ◦ Sie müssen Patch Orchestration installieren, um die Liste der bevorzugten Patches anzuzeigen. ◦ Der Satz der verfügbaren bevorzugten Patches ist eine Kreuzung aller potenziellen Patches in allen ausgewählten Vits. ◦ Eindeutige Schwachstellen für die Auswahlkriterien sind auf 500 beschränkt. Wenn mehr als 500 verschiedene Schwachstellen vorhanden sind, wird eine Warnmeldung angezeigt, in der Sie aufgefordert werden, Vits mit verschiedenen Kriterien zum Festlegen von auszuwählen **Bevorzugter Patch** . ◦ Die Gesamtzahl der Patches, die in der Suchliste angezeigt werden können, ist auf 170 begrenzt. Wenn mehr als 170 Patches vorhanden sind, wird eine Warnmeldung angezeigt.
Zuweisung aufheben	Die Zuweisung aller ausgewählten Elemente für die Zuweisungsgruppe und den Korrekturbesitzer wird aufgehoben. **Hinweis:** ◦ Dieses Feld wird angezeigt, wenn Sie Status als nicht aktualisieren auswählen. ◦ Wenn Sie die Zuweisung von Datensätzen aufheben, wird eine Korrekturaufgabe erstellt, die zur Genehmigung gesendet wird. Weitere Informationen finden Sie unter Entfernen Sie Zuweisungen für angreifbare Host-Elemente in Massen
Zuweisungsgruppe	Zuweisungsgruppe für die Datensätze. Alle aktiven Zuweisungsgruppen werden in diesem Feld angezeigt. **Hinweis:** Dieses Feld ist deaktiviert, wenn Sie das Kontrollkästchen Zuweisung aufheben aktivieren.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Wählen Sie **Bearbeiten**.

Ergebnisse

Ein asynchroner Massenbearbeitungsauftrag aktualisiert die ausgewählten angreifbaren Host-Elemente (Vits). Die bevorzugte Lösung und der bevorzugte Patch werden den relevanten angreifbaren Host-Elementen (Vits) hinzugefügt. Öffnen Sie ein angreifbares Host-Element, und zeigen Sie die bevorzugte Lösung und den bevorzugten Patch im Abschnitt „Korrektur“ der Registerkarte „Details“ an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weisen Sie einer Zuweisungsgruppe Datensätze in Massenarbeit zu

Weisen Sie mehrere Datensätze (Vits, AVITs, CVITs oder TRs) gleichzeitig einer Zuweisungsgruppe zu, indem Sie die Massenbearbeitungsfunktion in verwenden Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste**an.
2. Öffnen Sie auf der Listenseite die Liste aktiv oder alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Container-Elemente
   - Angreifbare Anwendungselemente
   - Konfigurationstestergebnisse
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie verwenden möchten **Nur Ausgewählte Elemente** Option in Datensatzauswahl Feld.
   - Wenden Sie Filter an, wenn Sie verwenden möchten **Alle Datensätze, die dem Filter entsprechen** Option in Datensatzauswahl Feld.
4. Wählen Sie aus **Massenbearbeitung** Schaltfläche.
5. Füllen Sie im Formular die Felder aus, um die Datensätze einer Zuweisungsgruppe zuzuweisen.

Modale Felder für Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ *Nur Ausgewählte Elemente* : Wählen Sie diese Option aus, wenn Sie die mit dem Kontrollkästchen ausgewählten Datensätze aktualisieren möchten. ○ *Alle Datensätze Die dem Filter entsprechen* : Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ *Korrekturaufgabe* : Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren möchten, und wählen Sie dann die gewünschte Korrekturaufgabe in aus **Korrekturaufgabe** Feld. ○ *Schwachstelleneintrag* : Wählen Sie diese Option aus, wenn Sie die für einen spezifischen Datensätze aktualisieren möchten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Schwachstelle y Und wählen Sie dann ein CVE oder TPE im aus **Schwachstelleneintrag** Feld. **Hinweis:** Dieses Feld wird für angreifbare Host-Elemente, angreifbare Anwendungselemente und angreifbare Container-Elemente angezeigt. ○ *Konfigurationstest* : Wählen Sie diese Option aus, wenn Sie die Testergebnisse aktualisieren möchten, die für einen Test spezifisch sind, und wählen Sie dann einen Test in aus **Konfigurationstest** Feld. **Hinweis:** Diese Option wird nur für Konfigurationstestergebnisse angezeigt. **Hinweis:** ○ Datensätze mit ungültigem CI oder außer Betrieb genommenem CI werden nicht aktualisiert. ○ Nur die Datensätze im Status „Offen“, „wird untersucht“, „Warten auf Implementierung“ oder „Zurückgestellt“ werden aktualisiert.
Zuweisungsgruppe	Zuweisungsgruppe für die Datensätze. Alle aktiven Zuweisungsgruppen werden in diesem Feld angezeigt. **Hinweis:** Dieses Feld ist deaktiviert, wenn Sie das Kontrollkästchen Zuweisung aufheben aktivieren Für Vits .
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Klicken Sie Auf **Bearbeiten** .

Ergebnisse
Öffnen Sie einen Datensatz, für den Sie die Zuweisungsgruppe aktualisiert haben, und navigieren Sie zur Registerkarte Übersicht. Die Anwendergruppe, der der Datensatz zugewiesen ist, wird in angezeigt **Zuweisungsgruppe** Feld.

Entfernen Sie Zuweisungen für angreifbare Host-Elemente in Massen

Entfernen Sie sich selbst oder Ihre Gruppen aus dem **Zugewiesen an** Und **Zuweisungsgruppe** Felder für angreifbare Host-Elemente (Vits) oder Korrekturaufgaben (VUL), wenn Sie feststellen, dass die Datensätze nicht in Ihrem Korrekturbereich liegen oder wenn Sie der Meinung sind, dass Datensätze Ihnen oder Ihren Gruppen falsch zugewiesen wurden.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_Analyst und sn_vul.Vulnerability_admin

Warum und wann dieser Vorgang ausgeführt wird
Die##Funktion „Zuweisung aufheben“ gilt für Datensätze in einem anderen Status als „Geschlossen“ oder „gelöst“. Wenn Sie Zuweisungen für angreifbare Host-Elemente mithilfe der Massenbearbeitungsfunktion entfernen, werden nur relevante Datensätze aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Öffnen Sie auf der Listenseite unter angreifbare Host-Elemente die Liste aktiv oder alle.
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie verwenden möchten **Nur Ausgewählte Elemente** Option in Datensatzauswahl Feld.
   - Wenden Sie Filter an, wenn Sie verwenden möchten **Alle angreifbaren Elemente, die dem Filter entsprechen** Option in Datensatzauswahl Feld.
4. Wählen Sie aus **Massenbearbeitung** Schaltfläche.
5. Füllen Sie im Formular die Felder aus, um Zuweisungen in Massenarbeit zu entfernen.

Modale Felder für Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nur ausgewählte Elemente: Wählen Sie diese Option aus, wenn Sie die mit dem Kontrollkästchen ausgewählten Datensätze aktualisieren möchten. ○ Alle angreifbaren Elemente, die dem Filter entsprechen: Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ Korrekturaufgabe: Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren möchten, und wählen Sie dann die gewünschte Korrekturaufgabe in aus **Korrekturaufgabe** Feld. ○ Schwachstelleneintrag: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die für einen allgemeinen angreifbaren Eintrag (CVE) spezifisch sind, und wählen Sie dann das CVE im aus **Schwachstelleneintrag** Feld. **Hinweis:** ○ Datensätze mit ungültigem CI oder außer Betrieb genommenem CI werden nicht aktualisiert. ○ Nur die Datensätze im Status „Offen“, „wird untersucht“, „Warten auf Implementierung“ oder „Zurückgestellt“ werden aktualisiert.
Status	Wählen Sie den Status nicht aktualisieren aus.
Zuweisung aufheben	Alle ausgewählten angreifbaren Elemente werden der Zuweisungsgruppe und dem Korrekturbesitzer nicht zugewiesen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ○ Dieses Feld wird angezeigt, wenn Sie Status als nicht aktualisieren auswählen. ○ Wenn Sie die Zuweisung von Datensätzen aufheben, wird eine Korrekturaufgabe erstellt, die zur Genehmigung gesendet wird.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Klicken Sie Auf **Bearbeiten** .
   Eine Korrekturaufgabe wird mit den ausgewählten angreifbaren Host-Elementen (Vits) erstellt.

   Ihre Anforderung wird zur Genehmigung übermittelt, und der Genehmiger erhält eine E-Mail-Benachrichtigung über Ihre Anforderung.

   Der Status der angreifbaren Host-Elemente (Vits) und der Korrekturaufgabe (VUL) wechselt zu „in Überprüfung“. Wenn eine Korrekturaufgabe mit dieser Funktion aktualisiert wird, wird **Zugewiesen an** Und **Zuweisungsgruppe** Felder in allen zugehörigen Vits werden auch nach Genehmigung Ihrer Anforderung gelöscht.

Ergebnisse
Navigieren Sie im Vulnerability Manager-Arbeitsbereich auf der Listenseite zu **Ausnahmeanforderungen** > **Alle** Öffnen Sie den entsprechenden Datensatz für die Genehmigung von Statusänderungen (VCA#), und überprüfen Sie den Status Ihrer Anforderung in der Spalte Genehmigungsstatus:

Genehmigungsstatus	Ergebnis
Genehmigt	Die **Zugewiesen an** Und **Zuweisungsgruppe** Felder aller angreifbaren Host-Elemente werden gelöscht.
Abgelehnt	Die **Zugewiesen an** Und **Zuweisungsgruppe** Felder aller angreifbaren Host-Elemente werden nicht aktualisiert.

In **Aktivitätenstrom** Eines Datensatzes oder einer Korrekturaufgabe können Sie den gesamten Workflow Ihrer Anforderung anzeigen.

Fordern Sie eine Massenausnahme im Vulnerability Manager-Arbeitsbereich an

Fordern Sie eine Ausnahme für mehrere Datensätze (Vits, AVITs, CVITs oder TRs) gleichzeitig an, indem Sie die Massenbearbeitungsfunktion verwenden, anstatt jeden Datensatz manuell auszuwählen.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie eine Ausnahme für einen oder mehrere Datensätze über das Modal „Massenbearbeitung“ anfordern, wird eine Korrekturaufgabe mit den ausgewählten Datensätzen erstellt.

Hinweis:
Die AVITs (Application Angreifbare Elemente) aus den Scannern mit **Verwalten Sie Ausnahmen in ServiceNow** Parameter, der auf „falsch“ festgelegt ist, wurden nicht aktualisiert.

- Wenn Sie AVITs aus verschiedenen Scannern auswählen, einige mit **Verwalten Sie Ausnahmen in ServiceNow** Parameter auf „wahr“ und „andere“ auf „falsch“ festgelegt, die AVITs, die mit ihm mit den Scannern verknüpft sind **Verwalten Sie Ausnahmen in ServiceNow** Parameter, der auf „falsch“ festgelegt ist, wurden nicht aktualisiert.
- Wenn Sie AVITs nur aus den Scannern mit auswählen **Verwalten Sie Ausnahmen in ServiceNow** Parameter auf „falsch“ festgelegt, die *Zurückstellen* Option wird nicht in angezeigt **Status** Feld im Modal „Massenbearbeitung“.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers**an.
2. Öffnen Sie auf der Listenseite die Aktiv Oder alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Container-Elemente
   - Angreifbare Anwendungselemente
   - Konfigurationstestergebnisse
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie verwenden möchten *Nur Ausgewählte Elemente* Option in Datensatzauswahl Feld.
   - Wenden Sie Filter an, wenn Sie verwenden möchten *Alle Datensätze, die dem Filter entsprechen* Option in Datensatzauswahl Feld.
4. Wählen Sie aus **Massenbearbeitung** Schaltfläche.
5. Füllen Sie im Formular die folgenden Felder aus, um eine Ausnahme für mehrere Datensätze (Vits, AVITs, CVITs oder TRs) gleichzeitig anzufordern.

Modale Felder für Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ *Nur Ausgewählte Elemente* : Wählen Sie diese Option aus, wenn Sie die mit dem Kontrollkästchen ausgewählten Datensätze aktualisieren möchten. ○ *Alle Datensätze, die dem Filter entsprechen* : Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ *Korrekturaufgabe* : Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren möchten, und wählen Sie dann die gewünschte Korrekturaufgabe in aus **Korrekturaufgabe** Feld. ○ *Schwachstelleneintrag* : Wählen Sie diese Option aus, wenn Sie die für eine Schwachstelle spezifischen Datensätze aktualisieren möchten Und wählen Sie dann ein CVE oder TPE im aus **Schwachstelleneintrag** Feld. **Hinweis:** Dieses Feld wird für angreifbare Host-Elemente, angreifbare Anwendungselemente und angreifbare Container-Elemente angezeigt. ○ *Konfigurationstest* : Wählen Sie diese Option aus, wenn Sie die Testergebnisse aktualisieren möchten, die für einen Test spezifisch sind, und wählen Sie dann einen Test in aus **Konfigurationstest** Feld. **Hinweis:** Diese Option wird nur für Konfigurationstestergebnisse angezeigt. **Hinweis:** ○ Datensätze mit ungültigem CI oder außer Betrieb genommenem CI werden nicht aktualisiert. ○ Nur die Datensätze im Status „Offen“, „wird untersucht“ oder „Warten auf Implementierung“ werden aktualisiert.
Status	Wählen Sie aus *Zurückgestellt* status, um eine Ausnahme für die ausgewählten Datensätze anzufordern. **Hinweis:** ○ Wenn Sie diese Option auswählen, werden die Felder Grund, Kurzbeschreibung, bis und zusätzliche Informationen angezeigt. ○ Wenn Sie Datensätze zurückstellen, wird eine Korrekturaufgabe erstellt, und diese Aufgabe wird zur Genehmigung gesendet.
Grund	Grund für die Zurückstellung von Datensätzen: ○ Warten auf Wartungsfenster ○ Behebung nicht verfügbar ○ Risiko akzeptiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Ausgleichende Steuerung vorhanden ○ Sonstige **Hinweis:** Die **Grund** Das Feld wird angezeigt, wenn Sie Status als zurückgestellt auswählen.
Kurzbeschreibung	Kurze Notiz, die die Gründe für die Zurückstellungsanforderung beschreibt. Diese Informationen spiegeln sich in wider **Beschreibung** Feld der Korrekturaufgabe, die für eine Zurückstellungsanforderung erstellt wird. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie den Status als zurückgestellt und als falsch positiv geschlossen auswählen.
Bis	Datum, bis zu dem der Datensatz zurückgestellt bleibt. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie Status als zurückgestellt auswählen.
Zusätzliche Information	Alle anderen erforderlichen Informationen. Diese Informationen spiegeln sich im Feld zusätzliche Informationen auf der Registerkarte Übersicht der Korrekturaufgabe wider, die für Zurückstellungs- und geschlossene falsch positive Anforderungen erstellt wird. Wenn Ihre Zurückstellungsanforderung genehmigt wird, werden diese zusätzlichen Informationen als Zurückstellungshinweise für VIT und Korrekturaufgabe angezeigt. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie den Status als zurückgestellt und als falsch positiv geschlossen auswählen.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Klicken Sie Auf **Bearbeiten** .
7. Beantworten Sie im Modal „Fragebogen ausfüllen“ die Fragen, und klicken Sie auf **Übermitteln** .

   Eine Korrekturaufgabe wird erstellt, die die von Ihnen ausgewählten Datensätze enthält. Ihre Anforderung wird zur Genehmigung übermittelt, und der Status der Datensätze ändert sich in#„in Überprüfung“.

   Hinweis:
   Die **Nehmen Sie An Dem Fragebogen Teil** Modal wird nur angezeigt, wenn der Fragebogen für Ausnahmeanforderungen im Formular „Ausnahmemanagement“ aktiviert ist. Weitere Informationen zum Konfigurieren eines Fragebogens für Ausnahmeanforderungen finden Sie unter Konfigurieren Sie das Ausnahmemanagement für Vulnerability Response, Konfigurieren Sie das Ausnahmemanagement für Application Vulnerability Response, Und Konfigurieren Sie das Ausnahmemanagement für Container Vulnerability Response, Und Konfigurations-Compliance Ausnahmemanagement – Übersicht.

   Der Genehmiger erhält eine E-Mail-Benachrichtigung über Ihre Anforderung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Navigieren Sie im Vulnerability Manager-Arbeitsbereich auf der Listenseite zu **Ausnahmen** > **Alle**Öffnen Sie den entsprechenden Datensatz für die Genehmigung von Statusänderungen (VCA#), und überprüfen Sie den Status Ihrer Anforderung in der Spalte Genehmigungsstatus:

Genehmigungsstatus	Ergebnis
Genehmigt	Der Status der Korrekturaufgabe wechselt in zurückgestellt, und der angegebene Grund ist Substatus. Status und Grund werden in die Datensätze zusammengefasst.
Abgelehnt	Der Status der Korrekturaufgabe und ihrer Datensätze ändert sich nicht.

In **Aktivitätenstrom** Eines Datensatzes oder einer Korrekturaufgabe können Sie den gesamten Workflow Ihrer Anforderung anzeigen.

Massenbearbeitung für falsch positive Werte im Vulnerability Manager-Arbeitsbereich

Markieren Sie einen oder mehrere Datensätze (Vits, AVITs, CVITs oder TRs) gleichzeitig mit der Massenbearbeitungsfunktion im Vulnerability Manager-Arbeitsbereich als falsch positiv, anstatt jedes Element manuell auszuwählen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie eine falsch positive Anforderung für einen oder mehrere Datensätze über das Modal „Massenbearbeitung“ stellen, wird eine Korrekturaufgabe mit den ausgewählten Datensätzen erstellt.

Hinweis:

Wenn Sie eine falsch positive Anforderung für die AVITs (Application Angreifbare Elemente) mit der Massenbearbeitungsfunktion stellen, werden die AVITs aus den Scannern mit erstellt **Verwalten Sie falsch positive mit ServiceNow** Parameter, der auf „falsch“ festgelegt ist, wurden nicht aktualisiert.

- Wenn Sie AVITs aus verschiedenen Scannern auswählen, einige mit **Verwalten Sie falsch positive mit ServiceNow** Parameter auf „wahr“ und „andere“ auf „falsch“ festgelegt, die AVITs, die mit den Scannern verknüpft sind, mit verknüpft sind **Verwalten Sie falsch positive mit ServiceNow** Parameter, der auf „falsch“ festgelegt ist, wurden nicht aktualisiert.
- Wenn Sie AVITs nur aus den Scannern mit auswählen **Verwalten Sie falsch positive mit ServiceNow** Parameter auf „falsch“ festgelegt, die *Falsch positiv* Option wird nicht in angezeigt **Grund** Feld im Modal „Massenbearbeitung“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste**an.

   Hinweis:
   Die ausgewählten Datensätze müssen sich im Status Offen, wird untersucht oder wartet auf Implementierung befinden.

2. Öffnen Sie auf der Listenseite die Liste aktiv oder alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Container-Elemente
   - Angreifbare Anwendungselemente
   - Konfigurationstestergebnisse
3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie verwenden möchten *Nur Ausgewählte Elemente* Option in **Datensatzauswahl** Feld.
   - Wenden Sie Filter an, wenn Sie verwenden möchten *Alle Datensätze, die dem Filter entsprechen* Option in **Datensatzauswahl** Feld.
4. Wählen Sie aus **Massenbearbeitung** Schaltfläche.
5. Füllen Sie die Felder im Formular aus, um falsch positive Werte für mehrere Datensätze anzufordern.

Modale Felder für Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ *Nur Ausgewählte Elemente* : Wählen Sie diese Option aus, wenn Sie die mit dem Kontrollkästchen ausgewählten Datensätze aktualisieren möchten. ○ *Alle Datensätze, die dem Filter entsprechen* : Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ *Korrekturaufgabe* : Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren möchten, und wählen Sie dann die gewünschte Korrekturaufgabe in aus **Korrekturaufgabe** Feld. ○ *Schwachstelleneintrag* : Wählen Sie diese Option aus, wenn Sie die für eine Schwachstelle spezifischen Datensätze aktualisieren möchten Und wählen Sie dann ein CVE oder TPE im aus **Schwachstelleneintrag** Feld. **Hinweis:** Dieses Feld wird für angreifbare Host-Elemente, angreifbare Anwendungselemente und angreifbare Container-Elemente angezeigt. ○ *Konfigurationstest* : Wählen Sie diese Option aus, wenn Sie die Testergebnisse aktualisieren möchten, die für einen Test spezifisch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	sind, und wählen Sie dann einen Test in aus **Konfigurationstest** Feld. **Hinweis:** Diese Option wird nur für Konfigurationstestergebnisse angezeigt. **Hinweis:** ○ Datensätze mit ungültigem CI oder außer Betrieb genommenem CI werden nicht aktualisiert. ○ Nur die Datensätze im Status „Offen“, „wird untersucht“ oder „Warten auf Implementierung“ werden aktualisiert.
Status	Wählen Sie aus **Geschlossen** status.
Grund	Wählen Sie den Grund als falsch positiv aus. **Hinweis:** ○ Wenn Sie diese Option auswählen, werden die Felder Kurzbeschreibung und zusätzliche Informationen angezeigt. ○ Eine Korrekturaufgabe wird erstellt, wenn Sie die Datensätze als falsch-positiv markieren, und diese Aufgabe wird zur Genehmigung gesendet. **Hinweis:** Die **Grund** Das Feld wird angezeigt, wenn Sie den Status als zurückgestellt oder Geschlossen auswählen.
Kurzbeschreibung	Kurze Notiz, die die Gründe für die geschlossene falsch positive Anforderung beschreibt. Diese Informationen spiegeln sich in wider **Beschreibung** Feld der Korrekturaufgabe, das für eine geschlossene falsch positive Anforderung erstellt wird. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie den Status als zurückgestellt oder als falsch positiv geschlossen auswählen.
Zusätzliche Information	Alle anderen erforderlichen Informationen. Diese Informationen spiegeln sich im Feld zusätzliche Informationen auf der Registerkarte Übersicht der Korrekturaufgabe wider, die für die Anforderung „Geschlossen – falsch positiv“ erstellt wird. Wenn Ihre falsch positive Anforderung genehmigt wird, werden diese zusätzlichen Informationen als Notizen für VIT und Korrekturaufgabe angezeigt. **Hinweis:** Dieses Feld wird angezeigt, wenn Sie den Status als zurückgestellt oder als falsch positiv geschlossen auswählen.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Klicken Sie Auf **Bearbeiten** .
7. Beantworten Sie im Modal „Fragebogen ausfüllen“ die Fragen, und wählen Sie aus **Übermitteln** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit den ausgewählten Datensätzen wird eine Korrekturaufgabe erstellt. Ihre Anforderung wird zur Genehmigung übermittelt, und der Status der Korrekturaufgabe ändert sich in#„in Überprüfung“.

Hinweis:
Die **Nehmen Sie An Dem Fragebogen Teil** Modal wird nur angezeigt, wenn der Fragebogen für falsch positive Anforderungen im Formular „Ausnahmemanagement“ aktiviert ist. Weitere Informationen zum Konfigurieren eines Fragebogens für falsch positive Anforderungen finden Sie unter Konfigurieren Sie das Ausnahmemanagement für Vulnerability Response, Konfigurieren Sie das Ausnahmemanagement für Application Vulnerability Response, Und Konfigurieren Sie das Ausnahmemanagement für Container Vulnerability Response.

Der Genehmiger erhält eine E-Mail-Benachrichtigung über Ihre Anforderung.

Ergebnisse

Navigieren Sie im Vulnerability Manager-Arbeitsbereich auf der Listenseite zu **Ausnahmen** > **Alle**Öffnen Sie den entsprechenden Datensatz für die Genehmigung von Statusänderungen (VCA#), und überprüfen Sie den Status Ihrer Anforderung in der Spalte Genehmigungsstatus:

Genehmigungsstatus	Ergebnis
Genehmigt	Der Status der Korrekturaufgabe wechselt zu „Geschlossen“ mit dem Grund „falsch positiv“. Status und Grund werden in die Datensätze zusammengefasst.
Abgelehnt	Der Status der Korrekturaufgabe und ihrer Datensätze ändert sich nicht.

In **Aktivitätenstrom** Eines Datensatzes oder einer Korrekturaufgabe können Sie den gesamten Workflow Ihrer Anforderung anzeigen.

Schließen Sie Datensätze in einem Massenvorgang in Arbeitsbereich des Schwachstellenmanagers

Schließen Sie mehrere Datensätze (Vits, AVITs oder CVITs) gleichzeitig mit der Massenbearbeitungsfunktion in Arbeitsbereich des Schwachstellenmanagers.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich des Schwachstellenmanagers** > **Liste**an.
2. Öffnen Sie auf der Listenseite die Liste aktiv oder alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Container-Elemente
   - Angreifbare Anwendungselemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Führen Sie einen der folgenden Schritte aus:
   - Aktivieren Sie das Kontrollkästchen neben jedem Element, wenn Sie die Option nur ausgewählte Elemente in verwenden möchten **Datensatzauswahl** Feld.
   - Wenden Sie Filter an, wenn Sie die Option alle angreifbaren Elemente, die dem Filter entsprechen, in verwenden möchten **Datensatzauswahl** Feld.
4. Wählen Sie aus **Massenbearbeitung** Schaltfläche.
5. Füllen Sie die Felder im Formular aus, um die ausgewählten Datensätze zu schließen.

Modale Felder für Massenbearbeitung

Feld	Beschreibung
Datensatzauswahl	Zu aktualisierende Datensätze. Die Auswahlmöglichkeiten lauten wie folgt: ○ Nur ausgewählte Elemente: Wählen Sie diese Option aus, wenn Sie die mit dem Kontrollkästchen ausgewählten Datensätze aktualisieren möchten. ○ Alle angreifbaren Elemente, die dem Filter entsprechen: Wählen Sie diese Option aus, wenn Sie die gefilterten Datensätze aktualisieren möchten. ○ Korrekturaufgabe: Wählen Sie diese Option aus, wenn Sie die Datensätze in einer Korrekturaufgabe aktualisieren möchten, und wählen Sie dann die gewünschte Korrekturaufgabe in aus **Korrekturaufgabe** Feld. ○ Schwachstelleneintrag: Wählen Sie diese Option aus, wenn Sie die Datensätze aktualisieren möchten, die für einen allgemeinen angreifbaren Eintrag (CVE) spezifisch sind, und wählen Sie dann das CVE im aus **Schwachstelleneintrag** Feld. **Hinweis:** ○ Datensätze mit ungültigem CI oder außer Betrieb genommenem CI werden nicht aktualisiert. ○ Nur die Datensätze im Status „Offen“, „wird untersucht“ oder „Warten auf Implementierung“ werden aktualisiert.
Status	Wählen Sie den Status als Geschlossen aus.
Grund	Grund für das Schließen von Datensätzen: ○ Falsch positiv **Hinweis:** Wenn Sie diese Option auswählen, um die Datensätze als falsch positiv zu markieren, werden die Felder Grund, Kurzbeschreibung und zusätzliche Informationen angezeigt. Weitere Informationen zur Massenbearbeitung von falsch positiven Werten finden Sie unter Massenbearbeitung für falsch positive Werte im Vulnerability Manager-Arbeitsbereich. ○ Abgebrochen ○ Repariert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Die Gründe „Abgebrochen“ und „behoben“ gelten nicht für CVITs.
Arbeitsnotizen	Text, den Sie eingeben, um die Änderungen zu beschreiben.

6. Klicken Sie Auf **Bearbeiten** .

Ein asynchroner Massenbearbeitungsauftrag aktualisiert die relevanten Datensätze.

Fordern Sie Ausnahmen für Korrekturaufgaben und -Datensätze in an Arbeitsbereich des Schwachstellenmanagers

Von Arbeitsbereich des Schwachstellenmanagers, Schwachstellenmanager und Analysten können Ausnahmen und falsch positive Ergebnisse für eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) und einen Datensatz (VIT, CVIT, AVIT oder CTR) anfordern. Sie können auch eine Korrekturaufgabe aufteilen und Change-Anforderungen erstellen.

Erforderliche Rolle:

- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin für angreifbare Host-Elemente (Vits)
- sn_vul.App_sec_Manager für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin für angreifbare Container-Elemente (CVITs)
- sn_vulc.admin für Konfigurationstestergebnisse (CTRs)

Hinweis:
Ab v19.0 von Vulnerability Response, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie v19.0 und höher
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

In Arbeitsbereich des Schwachstellenmanagers, Sie können für die Datensätze und Korrekturaufgaben Folgendes ausführen:

- Teilen Sie eine Korrekturaufgabe auf (VUL, AVUL, CVUL und CRG).
- Fordern Sie eine Ausnahme für einen Datensatz (VIT, AVIT oder CVIT) oder eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) an.
- Fordern Sie eine Richtlinienausnahme für Datensätze (VIT, AVIT oder CVIT) oder Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) an.
- Risikominderung für ein angreifbares Host-Element (VIT) und eine Korrekturaufgabe (VUL) anfordern
- Erstellen Sie eine Change-Anforderung für eine Korrekturaufgabe (VUL, CVUL oder CRG).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fordern Sie ein falsch positives Ergebnis für den Datensatz (VIT, AVIT oder CVIT) oder die Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) an.

Hinweis:
Sie können falsch positive Anforderungen für eine Reihe von Testergebnissen aus einer Korrekturaufgabe (CRG) stellen.

Sie initiieren diese UI-Aktionen aus Datensätzen in Arbeitsbereich des Schwachstellenmanagers, So wie Korrekturbesitzer diese Aufgaben in ausführen Arbeitsbereich für IT-Korrekturen.

Weitere Informationen finden Sie in den folgenden Themen:

- Fordern Sie ein falsch positives Ergebnis für ein angreifbares Element oder eine Korrekturaufgabe an
- Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen
- Fordern Sie eine Risikominderung für ein angreifbares Element oder eine Korrekturaufgabe an
- Teilen Sie eine Korrekturaufgabe in auf Arbeitsbereich für IT-Korrekturen
- Erstellen Sie eine Change-Anforderung in Arbeitsbereich für IT-Korrekturen
- Fordern Sie eine Ausnahme mit an GRC: Richtlinien- und Compliance-Management In Arbeitsbereich für IT-Korrekturen
- Fordern Sie ein falsch positives Ergebnis für eine Reihe von Testergebnissen an

Zugehörige Informationen

Ausnahmemanagement – Übersicht

Konfigurations-Compliance Ausnahmemanagement – Übersicht

Fordern Sie eine Massenausnahme im Vulnerability Manager-Arbeitsbereich an

Massenbearbeitung für falsch positive Werte im Vulnerability Manager-Arbeitsbereich

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element im Vulnerability Manager-Arbeitsbereich an

Fordern Sie eine Verlängerung für ein zurückgestelltes angreifbares Element an, bevor es das Fälligkeitsdatum „zurückgestellt bis“ erreicht. Als Korrekturbesitzer müssen Sie nicht mehr bis zum zurückgestellten Fälligkeitsdatum warten, um diese Anforderung zu stellen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Vulnerability_admin oder sn_vul.admin (veraltet)

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch eine Erweiterung in der klassischen Umgebung anfordern.

Verwenden Sie das gleiche Verfahren, um eine Erweiterung für ein angreifbares Anwendungselement, ein angreifbares Container-Element, eine Testergebnisgruppe und eine Korrekturaufgabe anzufordern.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Schwachstellen-Manager-Arbeitsbereiche**an.
2. Wählen Sie Listen Aus.
3. Wählen Sie unter angreifbare Host-Elemente die Option aus **Alle** .
4. Filtern Sie die Liste, indem Sie in der Spalte Status die Option Zurückgestellt auswählen.
5. Wählen Sie ein zurückgestelltes angreifbares Element aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Schaltfläche „Verlängerung anfordern“ ist nur sichtbar, wenn der Status des angreifbaren Elements „Zurückgestellt“ lautet.

6. Wählen Sie aus **Verlängerung Anfordern** Schaltfläche.
7. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Verlängern bis	Wählen Sie das Datum aus, bis zu dem das zurückgestellte angreifbare Element zur Korrektur verlängert werden muss.
Grund	Geben Sie den Grund für die Zurückstellung des Problems ein. Zur Auswahl stehen: ○ Warten auf Wartungsfenster ○ Korrektur nicht verfügbar ○ Risiko akzeptiert ○ Mindernde Kontrolle vorhanden ○ Sonstige
Zusätzliche Information	Geben Sie andere relevante Informationen ein.

8. Wählen Sie Aus **Verlängerung Anfordern** .
Bei der Übermittlung der Anforderung und der nachfolgenden Aktion durch den Genehmiger wird eine E-Mail ausgelöst.

Hinweis:
- Die Anforderung durchläuft zwei Genehmigungsebenen.
- Wenn ein zurückgestelltes angreifbares Element erneut erweitert wird, erhöht sich die Anzahl der Zurückstellungen im Back-End.

9. Nachdem die Anforderung genehmigt wurde, werden „bis“, „Grund“ und „Zurückstellungshinweise“ aktualisiert.

Arbeitsbereich des Schwachstellenmanagers Referenzinformationen

Die folgenden Themen enthalten Links, Referenzinformationen sowie Felddaten in den Formularen und Datensätzen, die in gefunden werden Arbeitsbereich des Schwachstellenmanagers.

Formularfelder für Überwachungsthema erstellen

In der folgenden Tabelle werden die Felder im Formular „Überwachungsthema erstellen“ in beschrieben Arbeitsbereich des Schwachstellenmanagers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name für Ihr Überwachungsthema, z. B. Kritische VIS .
Eigentum von	Der Name des Anwenders, der das Überwachungsthema besitzt.
Anzeigereihenfolge	Geben Sie einen Wert zwischen 100 und 1000 ein. 100 ist der Standardwert. Niedrigere Werte, die mit 100 beginnen, werden in aufsteigender Reihenfolge in Listen angezeigt.
Besitzergruppe	Der Name der Gruppe, die das Überwachungsthema besitzt.
Aktiv	Aktivieren oder deaktivieren Sie das Überwachungsthema. Standard ist ausgewählt (aktiv).
Beobachtungsliste	Fügen Sie Namen der Anwender hinzu, die Benachrichtigungen erhalten und das Überwachungsthema anzeigen können.
Beschreibung	Text, der Ihr Überwachungsthema beschreibt. Dieser Text wird im Feld Beschreibung angezeigt, wenn Sie aus diesem Überwachungsthema eine Korrekturmaßnahme erstellen.
Kategorie	Typ des Datensatzes, für den das Überwachungsthema erstellt wird.

Zugehörige Informationen

Erstellen Sie ein Überwachungsthema in Arbeitsbereich des Schwachstellenmanagers

Formularfelder für GRC-Anforderungsausnahme

Die folgende Tabelle zeigt die Feldbeschreibungen für das GRC-Anforderungsausnahmeformular.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Richtlinie	Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft, und der Status des angreifbaren Elements oder der angreifbaren Gruppe von zurückgestellt in Offen ändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Ausnahme anfordern“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf nicht überschreiten **Maximale Ausnahmedauer (Tage)** Die Sie für die Richtlinie in Richtlinie und Compliance festgelegt haben. Weitere Informationen finden Sie unter Erstellen Sie eine Richtlinie .
Grund	Grund für die Anforderung einer Ausnahme.
Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird. Dieses Feld muss vom Korrekturbesitzer ausgefüllt werden.

Generieren Sie Formularfelder für Korrektur-Digest

Die folgende Tabelle zeigt die Felder im Formular „Nachbesserungs-Digest generieren“.

Generieren Sie Korrekturdigest-Felder

Feld	Beschreibung
Aktives Kontrollkästchen	Dieses Kontrollkästchen ist standardmäßig aktiviert. Wenn Sie keine E-Mail-Benachrichtigungen senden möchten, deaktivieren Sie dieses Feld.
Ausführen	Wöchentlich ist der Standard. Wählen Sie eine Option aus der Liste aus.
Tag	„Monday“ ist der Standard. Wählen Sie eine Option aus der Liste aus.
Zeit	Legen Sie eine Zeit für die Zustellung der E-Mails fest. Wählen Sie eine Zeitzone aus, wenn Sie eine andere Zeitzone als die von der Instanz verwenden möchten, die den Auftrag ausführt.

Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum

Als Korrekturbesitzer können Sie eine Risikominderung für ein angreifbares Host-Element oder eine Korrekturaufgabe anfordern. Und der Schwachstellenmanager oder -Analyst kann diese Anforderungen zur Risikominderung genehmigen.

Weitere Informationen zum anfordern der Risikominderung und zur Genehmigung der Risikominderung finden Sie unter Fordern Sie eine Risikominderung für ein angreifbares Element oder eine Korrekturaufgabe an Und Genehmigen oder lehnen Sie Anforderungen in ab Arbeitsbereich des Schwachstellenmanagers Entsprechend.

Wenn eine Anforderung zur Risikominderung genehmigt wird, wird die Risikopunktzahl gemäß reduziert **Gewünschter Wert** (Risikobewertung) im Datensatz „Genehmigung von Statusänderungen“ (VCA#). Die höchste Risikopunktzahl der gewünschten Risikobewertung wird dem Datensatz zugewiesen, wenn Ihre Anforderung zur Risikominderung genehmigt wird. Das folgende Beispiel zeigt, wie die Risikopunktzahl und die ursprüngliche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risikopunktzahl aktualisiert werden, wenn Ausgleichssteuerungen angewendet werden. Die standardmäßigen höchsten Risikopunktzahlen der Risikobewertungen werden im folgenden Beispiel verwendet.

Auswirkung der Ausgleichssteuerungen auf die Risikopunktzahl und die ursprüngliche Risikopunktzahl

Szenario	Risikobewertung	Risikopunktzahl	Ursprüngliche Risikopunktzahl (berechnete Risikopunktzahl)
Daten vor v20.0	2 – Hoch	80	Das Feld ist vor v20.0 nicht verfügbar.
Nach dem Upgrade auf v20.0	2 – Hoch	80	Null
Die berechnete Risikopunktzahl ändert sich während der Erfassung in 90	1 – Kritisch	90.0	Null
Wenn Sie Ausgleichssteuerungen anwenden	3 – Mittel	69	90.0
Die berechnete Risikopunktzahl ändert sich während der Erfassung in 70	3 – Mittel	69	70
Die berechnete Risikopunktzahl ändert sich während der Erfassung in 50	3 – Mittel	50	50
Die berechnete Risikopunktzahl ändert sich während der Erfassung in 80	3 – Mittel	50	80
Wenn Ausgleichssteuerungen am ablaufen **Bis-Datum für die Risikominderung**	2 – Hoch	80	Null

Auswirkung von Ausgleichssteuerungen auf eine Korrekturaufgabe

Wenn Ihre Anforderung zur Risikominderung für eine Korrekturaufgabe genehmigt wird, wirken sich Ausgleichssteuerungen auf ihre angreifbaren Elemente wie folgt aus:

- Die Ausgleichssteuerungen, die auf die Korrekturaufgabe angewendet werden, werden auf ihre angreifbaren Elemente angewendet (andere als diejenigen im Status „Geschlossen“), deren Risikopunktzahl größer ist als die Risikopunktzahl, die dem entspricht **Gewünschter Wert** Im Status Change-Genehmigung einer Korrekturaufgabe. Und die Risikopunktzahl dieser angreifbaren Elemente wird gemäß reduziert **Gewünschter Wert** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die **Bis-Datum für die Risikominderung** Bleibt für die angreifbaren Elemente unverändert, auf die bereits eine Ausgleichssteuerung angewendet wird. Es wird nicht mit aktualisiert **Bis-Datum für die Risikominderung** Der Korrekturaufgabe.
- Die **Bis-Datum für die Risikominderung** Wird nur dann auf die angreifbaren Elemente zurückgesetzt, wenn zuvor keine Ausgleichssteuerung auf ein angreifbares Element angewendet wurde. Wenn Sie die Ausgleichssteuerungen erneut auf die Korrekturaufgabe anwenden, wird der **Bis-Datum für die Risikominderung** Wird nicht als vorhandenes auf die angreifbaren Elemente zurückgesetzt **Bis-Datum für die Risikominderung** Der angreifbaren Elemente wird Priorität zugewiesen.
- Wenn einer Korrekturaufgabe, für die bereits Ausgleichssteuerungen angewendet werden, ein neues angreifbares Element hinzugefügt wird, wird das Risiko nicht auf das angreifbare Element zurückgesetzt.

Auswirkung einer Ausgleichssteuerung auf ein angreifbares Element

Wenn Ihre Anforderung zur Risikominderung für ein angreifbares Element genehmigt wird:

- Die neue Risikopunktzahl wird in angezeigt **Risikopunktzahl** Feld und die alte Risikopunktzahl (berechnete Risikopunktzahl) wird in verschoben **Ursprüngliche Risikopunktzahl** Feld. Dieser Change wird bis zu dem in angegebenen Datum beibehalten **Bis-Datum für die Risikominderung** Feld.
- Wenn für ein angreifbares Element bereits Ausgleichssteuerungen angewendet wurden, gehen Sie während der Erfassung wie folgt vor:
  - Wenn die berechnete Risikopunktzahl größer als die Risikopunktzahl ist, bleibt die Risikopunktzahl unverändert, und die ursprüngliche Risikopunktzahl wird mit der berechneten Risikopunktzahl aktualisiert.
  - Wenn die berechnete Risikopunktzahl kleiner als die Risikopunktzahl ist, werden sowohl die Risikopunktzahl als auch die ursprüngliche Risikopunktzahl mit der berechneten Risikopunktzahl aktualisiert.
- Wenn ein Konfigurationselement (Configuration Item, CI) für ein angreifbares Element geändert wird, auf das bereits eine Ausgleichssteuerung angewendet wird:
  - Das CI wird für ein angreifbares Element standardmäßig als aktualisiert *sn_sec_cmn.update_on_ci_change*Systemeigenschaft ist auf „wahr“ festgelegt.

    Die Ausgleichssteuerung gilt weiterhin für das angreifbare Element.
  - Das angreifbare Element wird geschlossen, und wenn wird ein neues angreifbares Element erstellt *sn_sec_cmn.update_on_ci_change*Systemeigenschaft ist auf „falsch“ festgelegt.

    Die Ausgleichssteuerung, die auf das alte angreifbare Element angewendet wird, wird auf das neue angreifbare Element und die angewendet **Bis-Datum für die Risikominderung** , **Ursprüngliche Risikopunktzahl** Und **Risikopunktzahl** Bleiben Sie gleich.
- Wenn ein angreifbares Element vom Scanner erneut geöffnet wird und bereits eine Ausgleichssteuerung darauf angewendet wird, wird dieselbe Ausgleichssteuerung angewendet, nachdem es erneut geöffnet wurde.

Zugehörige Informationen

Erläuterungen zu Ausgleichssteuerungen Zur Risikominderung

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ordnen Sie Ausgleichssteuerungen CVEs oder TPEs für Risikoreduzierungsanforderungen zu

Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

#unique_159_Connect_42_li-risk-reduction-vmws

Beispiele für die Erstellung von Korrekturaufgaben in Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen

Wenn Sie Korrekturaufgaben manuell in erstellen Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen, Datensätze werden basierend auf den von Ihnen ausgewählten Gruppierungskriterien in eine Korrekturaufgabe gruppiert.

Betrachten Sie das folgende Beispiel, in dem 10 Datensätze für die Erstellung von Korrekturaufgaben ausgewählt werden. Nachdem Sie die Details zur Datensatzauswahl und eine kurze Beschreibung angegeben haben, wählen Sie aus **Gruppierungskriterien** Entsprechend Ihren Anforderungen und wählen Sie dann aus, wie Sie die Datensätze verwalten möchten, die bereits Teil vorhandener Korrekturaufgaben sind.

Example: Erstellung von Korrekturaufgaben basierend auf den Gruppierungskriterien

Angreifbare Elemente, die für die Erstellung der Korrekturaufgabe ausgewählt wurden

ID des angreifbaren Elements	Vorhandene Korrekturaufgab	Zuweisungsgrup	Konfigurationsel	Schwachstelle	Risikobewertung
VIT10001	VUL10021, VUL10022	Korrekturmanager	APSVR-NY-1672	CVE-2018-9020	4
VIT10002	-	Vulnerability Response	DEV-IBM-NY-682	CVE-2018-9020	2
VIT10003	VUL10021	LDAP-Administratoren	DEV-IBM-NY-682	CVE-2012-5357	1
VIT10004	-	Korrekturmanager	CRMBK-SD-4210	CVE-2013-1710	4
VIT10005	VUL10022	Vulnerability Response	DEV-IBM-NY-682	CVE-2018-9020	2
VIT10006	-	Korrekturmanager	CRMBK-SD-4210	CVE-2013-1710	2
VIT10007	-	LDAP-Administratoren	DEV-SAP-SD-9388	CVE-2013-3906	1
VIT10008	-	LDAP-Administratoren	DEV-IBM-NY-682	CVE-2013-3906	1
VIT10009	-	Korrekturmanager	CRMBK-SD-4210	CVE-2013-1710	2
VIT10010	-	LDAP-Administratoren	DEV-SAP-SD-9388	CVE-2013-3906	4

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Liste zeigt, wie die Datensätze basierend auf den beim Erstellen der Korrekturaufgabe ausgewählten Gruppierungskriterien in Korrekturaufgaben gruppiert werden.

Szenario 1: Gruppierungskriterien ist als „Zuweisungsgruppe“ ausgewählt, und das Verwalten von Datensätzen in anderen Korrekturaufgaben ist als „Datensätze für die neuen Korrekturaufgaben überspringen“ ausgewählt.

Die Datensätze mit derselben Zuweisungsgruppe werden in einer Korrekturaufgabe gruppiert. Die Datensätze, die bereits Teil vorhandener Korrekturaufgaben sind, werden den neuen Korrekturaufgaben nicht hinzugefügt. Hier werden drei Korrekturaufgaben erstellt, die jeweils die Datensätze enthalten, die dem zugewiesen sind **Korrekturmanager** , **LDAP-Administratoren** , Und **Vulnerability Response** Zuweisungsgruppen.

In Szenario 1 erstellte Korrekturaufgabe

Korrekturaufgaben erstellt	Datensätze in der Korrekturaufgabe
Korrekturaufgabe 1: VUL10001	Diese Korrekturaufgabe enthält die Datensätze, die dem zugewiesen sind **Korrekturmanager** Zuweisungsgruppe: • VIT10004 • VIT10006 • VIT10009 Der VIT10001-Datensatz wird nicht in die VUL10001-Korrekturaufgabe verschoben.
Korrekturaufgabe 2: VUL10002	Diese Korrekturaufgabe enthält den VIT10002-Datensatz, der dem zugewiesen ist **Vulnerability Response** Zuweisungsgruppe. Der VIT10005-Datensatz wird nicht in die VUL10002-Aufgabe verschoben.
Korrekturaufgabe 3 – VUL10003	Diese Korrekturaufgabe enthält die Datensätze, die dem zugewiesen sind **LDAP-Administratoren** Zuweisungsgruppe: • VIT10007 • VIT10008 • VIT10010 Der VIT10003-Datensatz wird nicht in die VUL10003-Korrekturaufgabe verschoben.

Szenario 2: Gruppierungskriterien sind als „Zuweisungsgruppe und Konfigurationselement“ ausgewählt, und das Verwalten von Datensätzen in anderen Korrekturaufgaben ist als „Datensätze an die neuen Korrekturaufgaben übertragen“ ausgewählt.

Die Datensätze mit demselben Konfigurationselement, die derselben Zuweisungsgruppe zugewiesen sind, werden in einer Korrekturaufgabe gruppiert. Die Datensätze VIT10001,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VIT10003 und VIT10005 werden aus ihren alten Korrekturaufgaben entfernt und in die neuen Korrekturaufgaben verschoben. Hier werden fünf Korrekturaufgaben erstellt.

In Szenario 2 erstellte Korrekturaufgaben

Korrekturaufgaben erstellt	Datensätze, die Teil der Korrekturaufgabe sind
Korrekturaufgabe 1 – VUL10004	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **Korrekturbesitzer** Zuweisungsgruppe und mit **APSVR-NY-1672** Konfigurationselement. • VIT10001 • [store-future: BEGIN review][End] Der VIT10001-Datensatz wird aus den Korrekturaufgaben VUL10021 und VUL10022 entfernt.
Korrekturaufgabe 2: VUL10005	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **Vulnerability Response** Zuweisungsgruppe und mit **DEV-IBM-NY-682** Konfigurationselement. • VIT10002 • VIT10005 Der VIT10005-Datensatz wird aus der Korrekturaufgabe VUL10022 entfernt.
Korrekturaufgabe 3 – VUL10006	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **LDAP-Administratoren** Zuweisungsgruppe und mit **DEV-IBM-NY-682** Konfigurationselement. • VIT10003 • VIT10008 Der VIT10003-Datensatz wird aus der VUL10021-Korrekturaufgabe entfernt.
Korrekturaufgabe 4 – VUL10007	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **Korrekturmanager** Zuweisungsgruppe und mit **CRMBK-SD-4210** Konfigurationselement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In Szenario 2 erstellte Korrekturaufgaben (Fortsetzung)

Korrekturaufgaben erstellt	Datensätze, die Teil der Korrekturaufgabe sind
	• VIT10004 • VIT10006 • VIT10009
Korrekturaufgabe 5 – VUL10008	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **LDAP-Administratoren** Zuweisungsgruppe und mit **DEV-SAP-SD-9388** Konfigurationselement. • VIT10007 • VIT10010

Szenario 3: Gruppierungskriterien ist als „Zuweisungsgruppe und Schwachstelle“ ausgewählt, und das Verwalten von Datensätzen in anderen Korrekturaufgaben ist als „Datensätze in aktuellen und neuen Korrekturaufgaben beibehalten“ ausgewählt.

Die Datensätze mit derselben Schwachstelle, die derselben Zuweisungsgruppe zugewiesen sind, werden in einer Korrekturaufgabe gruppiert. Die Datensätze VIT10001, VIT10003 und VIT10005 werden ihren jeweiligen neuen Korrekturaufgaben hinzugefügt, ohne aus ihren alten Korrekturaufgaben entfernt zu werden.hier werden fünf Korrekturaufgaben erstellt.

In Szenario 3 erstellte Korrekturaufgaben

Korrekturaufgaben erstellt	Datensätze, die Teil der Korrekturaufgabe sind
Korrekturaufgabe 1 – VUL10009	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **Korrekturbesitzer** Zuweisungsgruppe und mit **CVE-2018-9020** Schwachstelle. • VIT10001 • [store-future: BEGIN review][End] Der VIT10001-Datensatz bleibt Teil der Korrekturaufgaben VUL10021 und VUL10022.
Korrekturaufgabe 2 – VUL10010	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **Vulnerability Response** Zuweisungsgruppe und mit **CVE-2018-9020** Schwachstelle. • VIT10002 • VIT10005

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In Szenario 3 erstellte Korrekturaufgaben (Fortsetzung)

Korrekturaufgaben erstellt	Datensätze, die Teil der Korrekturaufgabe sind
	Der VIT10005-Datensatz bleibt auch Teil der VUL10022-Korrekturaufgabe.
Korrekturaufgabe 3 – VUL10011	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **LDAP-Administratoren** Zuweisungsgruppe und mit **CVE-2012-5357** Schwachstelle. • VIT10003 • [store-future: BEGIN review][End] Der VIT10003-Datensatz ist weiterhin Teil der VUL10021-Korrekturaufgabe.
Korrekturaufgabe 4 – VUL10012	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **Korrekturmanager** Zuweisungsgruppe und mit **CVE-2013-1710** Schwachstelle. • VIT10004 • VIT10006 • VIT10009
Korrekturaufgabe 5 – VUL10013	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **LDAP-Administratoren** Zuweisungsgruppe und mit **CVE-2013-3906** Schwachstelle. • VIT10007 • VIT10008 • VIT10010

Szenario 4: Gruppierungskriterien als „Zuweisungsgruppe und Risikobewertung“ und „Verwalten von Datensätzen in anderen Korrekturaufgaben“ ist als „Datensätze in aktuellen und neuen Korrekturaufgaben aufbewahren“ ausgewählt.

Die Datensätze mit derselben Risikobewertung, die derselben Zuweisungsgruppe zugewiesen sind, werden in einer Korrekturaufgabe gruppiert. Die Datensätze VIT10001, VIT10003 und VIT10005 werden ihren jeweiligen neuen Korrekturaufgaben hinzugefügt, ohne aus ihren alten Korrekturaufgaben entfernt zu werden. Hier werden fünf Korrekturaufgaben erstellt.

Korrekturaufgabe, die in Szenario 4 erstellt wurde

Korrekturaufgaben erstellt	Datensätze, die Teil der Korrekturaufgabe sind
Korrekturaufgabe 1 – VUL10014	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrekturaufgabe, die in Szenario 4 erstellt wurde (Fortsetzung)

Korrekturaufgaben erstellt	Datensätze, die Teil der Korrekturaufgabe sind
	Korrekturbesitzer Zuweisungsgruppe und mit **4** Risikobewertung. • VIT10001 • VIT10004 Der VIT10001-Datensatz ist weiterhin Teil der Korrekturaufgaben VUL10021und VUL10022.
Korrekturaufgabe 2 – VUL10015	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **Vulnerability Response** Zuweisungsgruppe und mit **2** Risikobewertung. • VIT10002 • VIT10005 Der VIT10005-Datensatz ist weiterhin Teil der VUL10022-Korrekturaufgabe.
Korrekturaufgabe 3 – VUL10016	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **LDAP-Administratoren** Zuweisungsgruppe und mit **1** Risikobewertung. • VIT10003 • VIT10007 • VIT10008 Der VIT10003-Datensatz ist weiterhin Teil der VUL10021-Korrekturaufgabe.
Korrekturaufgabe 4 – VUL10017	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **Korrekturmanager** Zuweisungsgruppe und mit **2** Risikobewertung. • VIT10006 • VIT10009
Korrekturaufgabe 5 – VUL10018	Diese Korrekturaufgabe enthält die Datensätze, die zugewiesen sind **LDAP-Administratoren** Zuweisungsgruppe und mit **4** Risikobewertung. • VIT10010 • [store-future: BEGIN review][End]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erstellen Sie eine Korrekturaufgabe manuell in Arbeitsbereich des Schwachstellenmanagers

Erstellen Sie eine Korrekturaufgabe manuell in Arbeitsbereich für IT-Korrekturen

Die Ausnahmen für ausgewählte Datensätze in werden neu bewertet Arbeitsbereich des Schwachstellenmanagers

In Arbeitsbereich des Schwachstellenmanagers, Wenn Sie die Ausnahmeregeln für eine Reihe von Datensätzen im Modal „Korrektureigenschaften neu bewerten und aktualisieren“ auswerten, werden ihr Zurückstellungsstatus und das bis-Datum der Zurückstellung gemäß den neuesten Ausnahmeregeln aktualisiert.

Szenarien

Wenn Sie die Ausnahmen für einen ausgewählten Satz von Datensätzen im modalen Element „Korrektureigenschaften neu bewerten und aktualisieren“ auswerten, können Sie auf die folgenden Szenarien stoßen Arbeitsbereich des Schwachstellenmanagers:

Szenario 1: Wenn die ausgewählten Datensätze bereits manuell zurückgestellt wurden und sie der Bedingung einer Ausnahmeregel entsprechen, bleiben diese Datensätze ohne Änderungen im Status zurückgestellt.

Szenario 2: Wenn die ausgewählten Datensätze mit der Bedingung in den Ausnahmeregeln übereinstimmen und sich diese Datensätze in einem Status ohne Zurückstellung befinden (z. B. „Offen“, „in Überprüfung“, „wird untersucht“), werden diese Datensätze bis zu dem in der Ausnahmeregel definierten Datum zurückgestellt.

Szenario 3: Wenn sich die ausgewählten Datensätze bereits im Status zurückgestellt befinden (die mithilfe der Ausnahmeregel A zurückgestellt werden), verbleiben sie in den folgenden Szenarien im Status zurückgestellt:

- Die Ausnahmeregel läuft ab, und die Datensätze entsprechen nicht der Bedingung
- Die Ausnahmeregel läuft ab, und die Datensätze entsprechen der Bedingung
- Die Ausnahmeregel A läuft ab, und Datensätze entsprechen der Bedingung einer anderen Ausnahmeregel B.

Szenario 4: Berücksichtigen Sie, dass die Datensätze mithilfe einer Ausnahmeregel zurückgestellt werden. Wenn Sie die Ausnahmeregelbedingung so ändern, dass der Status zurückgestellt der Datensätze nicht mehr gültig ist, und dann die Ausnahmeregeln für diese Datensätze neu bewerten:

- Die Datensätze werden in den Status Offen versetzt
- Die Felder bis-Datum, Zurückstellungsdatum, Anzahl der Zurückstellungen und andere Felder werden aktualisiert.

Example: Berücksichtigen Sie, dass Sie die Ausnahmen für die folgenden angreifbaren Host-Elemente (Vits) bewerten.

Berücksichtigen Sie die Ausnahmeregel mit den folgenden Details:

Ausnahmeregeldetails

Feld	Beschreibung	Wert
Name	Name der Ausnahmeregel.	Kritische Vits werden zurückgestellt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausnahmeregeldetails (Fortsetzung)

Feld	Beschreibung	Wert
Gültig ab	Datum, ab dem diese Regel aktiv ist, um die VIS aufzuschieben.	20-08-2024
Gültig bis	Datum, ab dem die Korrekturaufgabe keine neuen VIS mehr akzeptiert.	30-11-2024
Grund	Grund für die Erstellung dieser Ausnahmeregel.	Risiko akzeptiert
Zuweisungsgruppe	Gruppe, der die Korrekturaufgabe zugewiesen ist, die für die Nachverfolgung der zurückgestellten VIS erstellt wurde.	Korrekturgruppe 1
Zusätzliche Information	Zusätzliche Informationen, die die anfordernde Person dem Genehmiger bereitstellen möchte. Diese Informationen werden im Beschreibungsfeld der Korrekturaufgabe ausgefüllt.	Diese Regel wurde erstellt, um die kritischen Vits automatisch zurückzustellen.
Bedingung	Filterbedingung für die VIS, die bei der Verarbeitung der VIS definiert werden kann.	Risikobewertung = 5 – Kritisch
Für vorhandene Daten ausführen	Option, mit der Sie diese Regel bei der ersten Ausführung dieser Regel für vorhandene Daten ausführen können.	Ja
Status	Status der Ausnahmeregel.	Genehmigt
Ausführungsreihenfolge	Eindeutige Reihenfolge für jede Ausnahmeregel.	100
Zurückgestellt bis	Datum, bis zu dem die VULs und VIS zurückgestellt werden. An diesem Datum wird die erstellte ÄNDERUNG geschlossen, alle VIS werden aus der Gruppe entfernt, und Gruppenregeln werden erneut angewendet.	2024-12-23 16:10:29

Die folgende Tabelle zeigt, wie sich der Status ändert, wenn die Ausnahmeregeln für mehrere Vits gleichzeitig neu ausgewertet werden:

Datensätze, für die Ausnahmen neu ausgewertet werden

VIT-Nummer	Status	Risikobewertung	Status wurde nach der Neubewertung der Ausnahmen -1 aktualisiert	Bis-Datum: 1
VIT120067	Öffnen	2 - Niedrig	Öffnen	-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensätze, für die Ausnahmen neu ausgewertet werden (Fortsetzung)

VIT-Nummer	Status	Risikobewertung	Status wurde nach der Neubewertung der Ausnahmen -1 aktualisiert	Bis-Datum: 1
VIT120068	Wird überprüft	3 – Mittel	Wird überprüft	-
VIT120069	Wird untersucht	5: Kritisch	Zurückgestellt	2024-12-23 16:10:29
VIT120070	Zurückgestellt	5: Kritisch	Zurückgestellt	2024-12-23 16:10:29
VIT120071	Zurückgestellt	2 - Niedrig	Zurückgestellt	2024-10-02 16:10:29 (manuell zurückgestellt)
VIT120072	Geschlossen	5: Kritisch	Geschlossen	-

Wenn die Bedingung in der vorherigen Ausnahmeregel in geändert wird `Risikobewertung = 2 – Niedrig` Und **Zurückgestellt bis** Wird geändert in `2024-12-31 14:10:23` Die Datensätze werden wie folgt aktualisiert:

Datensätze, für die Ausnahmen neu ausgewertet werden

VIT-Nummer	Status wurde nach der Neubewertung der Ausnahmen -1 aktualisiert	Risikobewertung	Status nach Neubewertung der Ausnahmen aktualisiert – 2	Bis-Datum: 2
VIT120067	Öffnen	2 - Niedrig	Zurückgestellt	2024-12-31 14:10:23
VIT120068	Wird überprüft	3 – Mittel	Wird überprüft	-
VIT120069	Zurückgestellt	5: Kritisch	Zurückgestellt	2024-12-23 16:10:29
VIT120070	Zurückgestellt	5: Kritisch	Zurückgestellt	2024-12-23 16:10:29
VIT120071	Zurückgestellt	2 - Niedrig	Zurückgestellt (keine Statusänderung)	2024-10-02 16:10:29 (keine Änderung des bis-Datums)
VIT120072	Geschlossen	5: Kritisch	Geschlossen	-

Zugehörige Informationen

Bewerten Sie die Korrektureigenschaften der Datensätze in neu Arbeitsbereich des Schwachstellenmanagers

Übersicht über Ausnahmeregeln

Konfigurations-Compliance Ausnahmemanagement – Übersicht

[store-future: BEGIN review]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Umleitung zu Arbeitsbereich des Schwachstellenmanagers Aus dem Menü alle

Wenn ein Administrator den festlegt *sn_vul_cmn_ws.navigate_to_workspace*Systemeigenschaft zu `Wahr` , Sie werden zu weitergeleitet Arbeitsbereich des Schwachstellenmanagers Bei Auswahl der vordefinierten Filter-Links in Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance Module aus dem **Alle** Menü.

Umleitung zur Homepage von Arbeitsbereich des Schwachstellenmanagers

Als Benutzer mit der Rolle sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin, wenn Sie die folgenden vordefinierten Filterlinks im Modul „angreifbare Elemente“ auswählen, indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Angreifbare Elemente**, Diese Links werden in geöffnet Arbeitsbereich des Schwachstellenmanagers Startseite von mit automatischer Auswahl des entsprechenden gespeicherten Filters auf der Registerkarte Host-Schwachstellen:

- Kritisches Risiko
- Ziel verfehlt
- Mehrere Zurückstellungen
- Älter als 90 Tage
- Nicht zugewiesen
- Nicht gruppiert
- Hohes Risiko
- Innerhalb der letzten 90 Tage
- Außer Betrieb genommen
- Ziel rückt näher
- Nutzbar

Als Benutzer mit der Rolle sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin, wenn Sie die folgenden vordefinierten Filterlinks im Modul „angreifbare Container-Elemente“ auswählen, indem Sie zu navigieren **Alle** > **Container Vulnerability Response** > **Angreifbare Container-Elemente**, Diese Links werden in geöffnet Arbeitsbereich des Schwachstellenmanagers Startseite von mit automatischer Auswahl des entsprechenden gespeicherten Filters auf der Registerkarte „Container-Schwachstellen“:

- Nicht zugewiesen
- Kritisches und hohes Risiko
- Nutzbar
- Ziel rückt näher
- Ziel verfehlt
- Mehrfache Zurückstellung
- Alle

Als Benutzer mit der Rolle sn_vul.App_sec_Manager, wenn Sie die folgenden vordefinierten Filterlinks im Modul „angreifbare Anwendungselemente“ auswählen, indem Sie zu navigieren **Alle** > **Application Vulnerability Response** > **Angreifbare Elemente**, Diese Links werden in geöffnet Arbeitsbereich des Schwachstellenmanagers Startseite von mit automatischer Auswahl des entsprechenden gespeicherten Filters auf der Registerkarte Anwendungsschwachstellen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktiv
- Datum der Korrekturzusage vergangen
- Mehrfache Zurückstellung
- Nicht zugewiesen
- Alle

Wenn Sie als Anwender mit der Rolle sn_vulc.admin die folgenden vordefinierten Filterlinks im Modul „Testergebnisse“ auswählen, indem Sie zu navigieren **Alle** > **Konfigurations-Compliance** > **Testergebnisse**, Diese Links werden in geöffnet Arbeitsbereich des Schwachstellenmanagers Startseite von mit automatischer Auswahl des entsprechenden gespeicherten Filters auf der Registerkarte Konfigurationstestergebnisse:

- Nicht selektierte Testergebnisse
- Offene Testergebnisse
- Ziel rückt näher
- Ziel verfehlt
- Mehrfache Zurückstellung
- Nicht zugewiesen
- Alle

Umleitung zur Listenseite von Arbeitsbereich des Schwachstellenmanagers

Als Benutzer mit der Rolle sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin, wenn Sie im Modul Vulnerability Response die folgenden vordefinierten Filterlinks auswählen, indem Sie zu navigieren **Alle** > **Vulnerability Response**, Diese Links werden auf der Listenseite von geöffnet Arbeitsbereich des Schwachstellenmanagers:

- Korrekturaufgaben: Aktiv, mir zugewiesen, meinen Gruppen zugewiesen und alle
- Angreifbare Elemente: Mir zugewiesen und meinen Gruppen zugewiesen
- Bibliotheken: NVD, CWE, Drittpartei und angreifbare Software
- Lösungen: Alle, höchste Ersatzlösung und mit angreifbaren Elementen
- Meine Genehmigungen

Als Benutzer mit der Rolle sn_vul_Container.Vulnerability_Analyst oder sn_vul_Container.Vulnerability_admin, wenn Sie die folgenden vordefinierten Filterlinks im Container Vulnerability Response-Modul auswählen, indem Sie zu navigieren **Alle** > **Container Vulnerability Response**, Diese Links werden auf der Listenseite von geöffnet Arbeitsbereich des Schwachstellenmanagers:

- Container-Korrekturaufgaben: Aktiv, mir zugewiesen, meinen Gruppen zugewiesen und alle
- Angreifbare Container-Elemente: Mir zugewiesen und meinen Gruppen zugewiesen
- Bibliotheken: NVD, CWE und Drittpartei
- Meine Genehmigungen

Wenn Sie als Anwender mit der Rolle sn_vul.App_sec_Manager die folgenden vordefinierten Filterlinks im Modul „Application Vulnerability Response“ auswählen, indem Sie zu navigieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle > **Application Vulnerability Response**, Diese Links werden auf der Listenseite von geöffnet Arbeitsbereich des Schwachstellenmanagers:

- Korrekturaufgaben: Aktiv, mir zugewiesen, meinen Gruppen zugewiesen und alle
- Angreifbare Elemente: Mir zugewiesen und meinen Gruppen zugewiesen
- Meine Genehmigungen
- Bibliotheken: NVD, CWE und Drittpartei
- Penetrationstest – Anforderungen bewerten: Aktiv, alle mir zugewiesen und meinen Gruppen zugewiesen
- Penetrationstestergebnisse: Aktiv, Validierung ausstehend, mir zugewiesen, meiner Gruppe zugewiesen und alle

Als Anwender mit der Rolle sn_vul.App_sec_Manager, wenn Sie die folgenden vordefinierten Filterlinks im Modul Konfigurations-Compliance auswählen, indem Sie zu navigieren **Alle** > **Konfigurations-Compliance**, Diese Links werden auf der Listenseite von geöffnet Arbeitsbereich des Schwachstellenmanagers:

- Korrekturaufgaben: Meine offenen Aufgaben, alle offenen Aufgaben, mehrere Zurückstellungen und alle Aufgaben
- Tests
- Testgruppen
- Unterstützungsdaten: Autorisierende Quellen und Technologien

[End]

Arbeitsbereich für IT-Korrekturen

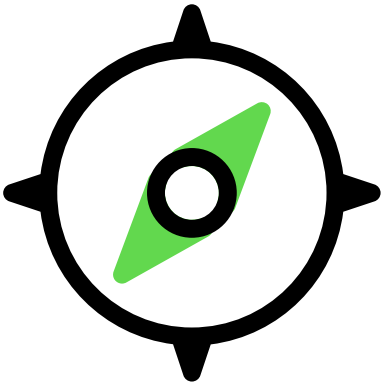
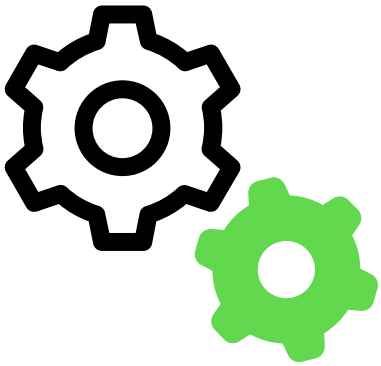
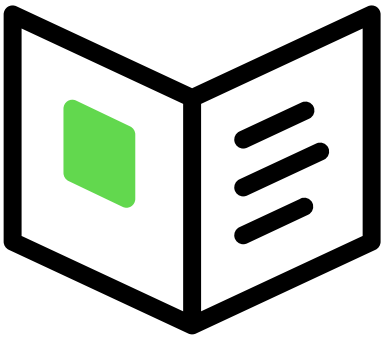
IT-Teams können Zeit sparen, um IT-bezogene Schwachstellen zu beheben, indem sie einfach Change-Anforderungen erstellen, angreifbare Elemente erneut scannen und Ausnahmeanforderungen von übermitteln Arbeitsbereich für IT-Korrekturen.

V18.0 – Demo zum Arbeitsbereich für IT-Korrektur

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Beheben	Referenz
		
Erfahren Sie mehr über Arbeitsbereich für IT-Korrekturen	Erfahren Sie, wie Sie Schwachstellen und Fehlkonfigurationen von beheben können Arbeitsbereich für IT-Korrekturen	Rufen Sie zusätzliche Informationen ab, die Sie zum Konfigurieren und Verwalten verwenden Arbeitsbereich für IT-Korrekturen

Problembehandlung und Hilfe

- Security Operations in der ServiceNow-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Arbeitsbereich für IT-Korrekturen erkunden

Die Arbeitsbereich für IT-Korrekturen Ist für IT-Korrekturbesitzer und IT-Gruppen vorgesehen. Es besteht aus Start- und Listenansichten sowie Datenvisualisierungen, auf die Sie klicken können, um die Ihnen zugewiesenen Korrekturaufgaben und die Anzahl der Ihnen zugewiesenen Datensätze anzuzeigen.

Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v19.0 von Vulnerability Response, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie v19.0 und höher
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Die Arbeitsbereich für IT-Korrekturen Besteht aus den folgenden Seiten, Listen und Formularen:

Zielseite (Homepage)

Die Homepage besteht aus der Karte „zugewiesene Korrekturaufgaben“, der Karte „bevorzugte Lösungen auf VIS“, der Karte „Betroffene CIs“, der Liste „bevorzugte Patches auf der VIS-Karte“ und der Liste „Korrekturaufgaben“. Weitere Informationen zur Homepage finden Sie unter Homepage in Arbeitsbereich für IT-Korrekturen.

Seite „Dashboards“

Die Dashboards-Seite besteht aus dem Dashboard „Schwachstellenbeseitigung“. Weitere Informationen zur Seite „Dashboards“ finden Sie unter Seite „Dashboards“ in Arbeitsbereich für IT-Korrekturen.

Listen-Seite

Diese Ansicht besteht aus standardmäßigen und anwenderdefinierten Listen von Korrekturaufgaben, angreifbaren Host-Elementen, angreifbaren Anwendungselementen, angreifbaren Container-Elementen, Ihnen zugewiesenen Konfigurationstestergebnissen und Lösungen, Ausnahmeanforderungen usw. Weitere Informationen zur Listenseite finden Sie unter Listenseite in Arbeitsbereich für IT-Korrekturen. Weitere Informationen dazu, was Sie auf dieser Seite tun können, finden Sie unter Erstellen Sie eine Liste in Arbeitsbereich für IT-Korrekturen.

Zeigen Sie ein Workflow-Beispiel in an Arbeitsbereich für IT-Korrekturen

Zeigen Sie ein Beispiel für einen End-to-End-Workflow in an Arbeitsbereich für IT-Korrekturen. Sehen Sie, wie IT-Spezialisten den Arbeitsbereich verwenden können, um kritische angreifbare Elemente (Vits, AVITs und CVITs) und Testergebnisse (TRs) zu überwachen und die ihnen zugewiesenen Schwachstellen zu beheben.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Prozedur

Klicken Sie auf das folgende Bild, um die Schritte des Workflows anzuzeigen.
IT-Korrekturarbeitsbereich-Demo

Das Bild enthält die folgenden Aufgaben:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie auf der Homepage (Zielseite IT-Korrekturbesitzer) die Ihnen zugewiesenen Korrekturaufgaben an. Wechseln Sie zwischen der Arbeit, die Ihnen zugewiesen ist, und Ihrer Gruppe. Sehen Sie sich die Host-Korrekturaufgaben an, die Lösungen enthalten. Weitere Informationen zur Homepage finden Sie unter Homepage in Arbeitsbereich für IT-Korrekturen.
- Wählen Sie aus **Liste** Anzeigen, um die Listen Ihrer zugewiesenen Arbeit anzuzeigen.
- In der Listenansicht mit **Meiner Gruppe zugewiesen** Liste, die in der Liste „Korrekturaufgaben“ ausgewählt ist, identifizieren Sie die Arbeit, und weisen Sie sie sich selbst zu. Weitere Informationen zur Listenseite finden Sie unter Listenseite in Arbeitsbereich für IT-Korrekturen.
- Gruppieren Sie die Korrekturaufgaben nach Datensatztyp: Wählen Sie das drei-Punkte-Menü im aus **Datensatztyp** Spalte und wählen Sie dann aus **Nach Datensatztyp gruppieren** .
- Bei einer offenen Korrekturaufgabe (VUL, AVUL, CVUL und CRG):
  - Wählen Sie aus **Übersicht** Registerkarte zum Anzeigen der Datensätze (Vits, AVITs, CVITs und TRs) und der betroffenen Konfigurationselemente (CIs), die dem Datensatz zugeordnet sind.
  - Wählen Sie aus **Lösungen** Registerkarte, um bevorzugte und potenzielle Lösungen für eine Host-Korrekturaufgabe anzuzeigen.
  - Wählen Sie aus **Details** Registerkarte, um bearbeitbare Felder wie Status, Zuweisungsgruppe, Zugewiesen an und Kurzbeschreibung zu ändern und die für eine Korrekturaufgabe ausgeführten Aktionen anzuzeigen.
  - Wählen Sie aus **Genehmigung Der Statusänderung** Registerkarte, um die Datensätze für die Genehmigung von Statusänderungen (CA#) anzuzeigen, mit denen Sie den Genehmigungs-Workflow nachverfolgen können.
  - Wählen Sie aus **Change-Anforderungen** Registerkarte , um den Genehmigungsstatus der Change-Anforderungen anzuzeigen und eine neue Change-Anforderung zu erstellen, indem Sie auswählen **Neu** Schaltfläche.
  - Wählen Sie die UI-Aktionen aus: **Als falsch positiv markieren** , **Erstellen Sie Einen Change** , **Aufgabe Aufteilen** , **Status aktualisieren Ausnahme Anfordern** , **Löschen** Und so weiter. Befolgen Sie die Anweisungen in den Dialogfeldern, um Sie bei der Korrektur zu unterstützen.

Homepage in Arbeitsbereich für IT-Korrekturen

Die Homepage in Arbeitsbereich für IT-Korrekturen Stellt eine konsolidierte Liste von Host-, Anwendungs-, Container- und Testergebnis-Korrekturaufgaben bereit, die Ihnen und Ihren Zuweisungsgruppen zugewiesen sind.

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Die Homepage besteht aus den folgenden Karten und einer Liste der Korrekturaufgaben, die Ihnen und Ihren Zuweisungsgruppen zugewiesen sind. Datensätze, die Ihnen zugewiesen sind, haben Lösungen.

Karte „zugewiesene Korrekturaufgaben“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzahl der Ihnen zugewiesenen aktiven Korrekturaufgaben. Wählen Sie die Kachel aus, um die Liste der Korrekturaufgaben anzuzeigen.

Bevorzugte Lösungen auf der VIS-Karte

Anzahl der bevorzugten Lösungen, die zur Korrektur der angreifbaren Host-Elemente verfügbar sind. Die Liste Lösungen wird angezeigt, wenn die Anwendung Schwachstellenlösungsmanagement installiert ist. Diese Karte zeigt Ihnen Lösungsdaten, potenzielle und bevorzugte Lösungen von Drittanbietern zu Ihren angreifbaren Elementen.

Karte „Betroffene CIs“

Die Anzahl der Konfigurationselemente mit VIS, die Ihnen oder Ihren Gruppen zugewiesen sind. Weitere Informationen finden Sie unter Zeigen Sie Konfigurationselemente mit Schwachstellen in an Arbeitsbereich für IT-Korrekturen.

Bevorzugte Patches auf der VIS-Karte

Anzahl der bevorzugten verfügbaren Patches, die zur Korrektur der angreifbaren Host-Elemente verwendet werden können.

Liste der Korrekturaufgaben

Die Liste der Korrekturaufgaben, die Ihnen und Ihren Zuweisungsgruppen zugewiesen sind. Sie können die Datensätze filtern, indem Sie auswählen **Mir zugewiesen** Und **Meinen Gruppen zugewiesen** Optionen.

Sie können auf eine Korrekturaufgabe klicken, um die Details anzuzeigen und eine Untersuchung zu starten. In der Listenansicht können Sie Korrekturaufgaben, angreifbare Elemente, Konfigurationstestergebnisse usw. anzeigen. Sie können eine Korrekturaufgabe öffnen und auf klicken **Mir zuweisen** Um die Aufgabe sich selbst zuzuweisen und die Untersuchung zu starten.

Hinweis:
Wenn Sie sich die Aufgabe in der Korrekturaufgabe nicht selbst zuweisen, können Sie keine UI-Aktionen auf Datensatzebene anzeigen.

Klicken Sie auf die Ellipsen weitere Aktionen, und klicken Sie auf **Untersuchung Starten** Dient zum Lösen einer Korrekturaufgabe.

Weitere Informationen dazu, was Sie auf der Homepage tun können, finden Sie unter Verwenden Sie Korrekturaufgaben-Datensätze in Arbeitsbereich für IT-Korrekturen.

Seite „Dashboards“ in Arbeitsbereich für IT-Korrekturen

Die Seite „Dashboards“ in Arbeitsbereich für IT-Korrekturen Stellt das Dashboard „Schwachstellenkorrektur“ in bereit Next Experience UI, die verwendet werden kann, um sich auf die Korrekturaufgaben und angreifbaren Elemente zu konzentrieren.

Als Korrekturbesitzer (sn_vul.Remediation_owner) können Sie auf zugreifen **Schwachstellenkorrektur** Dashboard, indem Sie zu navigieren **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen** Und wählen Sie das Dashboards-Symbol. Weitere Informationen zum Dashboard „Schwachstellenkorrektur“ finden Sie unter Wird standardmäßig verwendet Vulnerability Response Dashboards.

Sie können ein anwenderdefiniertes Dashboard erstellen, indem Sie das Symbol „weitere Optionen“ auswählen ⋮ Und auswählen **Erstellen Sie neu** .

Listenseite in Arbeitsbereich für IT-Korrekturen

Die Listenansicht in Arbeitsbereich für IT-Korrekturen Ermöglicht es Korrekturbesitzern, die ihnen zugewiesenen Datensätze (Vits, AVITs, CVITs und TRs) und ihre Zuweisungsgruppen anzuzeigen und diese Schwachstellen und Fehlkonfigurationen zu beheben. Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können auch die Liste der bevorzugten Lösungen anzeigen, die für die Korrektur der angreifbaren Host-Elemente (Vits) empfohlen werden. Zusammen mit diesen Listen können Sie die Liste der von Ihnen gestellten Ausnahmeanforderungen und Penetrationstestbewertungsanforderungen, Penetrationstestergebnisse, die Ihren Penetrationstestbewertungsanforderungen zugeordnet sind, unterstützte Bibliotheken und andere unterstützte Daten anzeigen.

Erforderliche Rollen:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Die Listen und Links auf der Listenseite bieten einfachen Zugriff auf Datensätze und Aufgaben. Es enthält zwei Registerkarten:

- **Listen** Registerkarte: Zeigt die Standardlisten für Korrekturmaßnahmen, Korrekturaufgaben, angreifbare Elemente (Vits, AVITs oder CVITs) an, Lösungen, Ausnahmen und Konfigurationstestergebnisse usw. Weitere Informationen finden Sie in der folgenden Tabelle.
- **Meine Listen** Registerkarte: Zeigt eine Liste an, die Sie auf der Registerkarte Liste umbenannt haben, und eine Liste, die Sie erstellen.

  Sie können auch eine eigene Liste von Datensätzen erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Liste in Arbeitsbereich für IT-Korrekturen.

Tipp:

Wenn *sn_vul_cmn_ws.navigate_to_workspace*Systemeigenschaft ist auf festgelegt `Wahr` Vom -Administrator bei Auswahl der vordefinierten Filterlinks im Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Testergebnismodul in Konfigurations-Compliance Unter **Alle** Menü, werden diese Links auf der Listenseite in geöffnet Arbeitsbereich für IT-Korrekturen.

Beispiel: Wenn Sie auswählen **Meinen Gruppen zugewiesen** Indem Sie zu navigieren **Alle** > **Vulnerability Response** > **Korrekturaufgaben** > **Meinen Gruppen zugewiesen**, Dieser Link wird zu weitergeleitet Arbeitsbereich für IT-Korrekturen. Die Liste „meiner Gruppe zugewiesen“ im Modul „Korrekturaufgaben“ wird auf der Listenseite des IT-Korrekturarbeitsbereichs geöffnet, wenn Sie über die Rolle „Korrekturbesitzer“ verfügen. Um die Host-Korrekturaufgaben anzuzeigen, gruppieren Sie die Aufgaben nach **Datensatztyp** .

Mit können Sie die Datensatzanzahl in einer Liste ausblenden *glide.ui.list.seismic.omit.count*Systemeigenschaft. Weitere Informationen zum Deaktivieren/Aktivieren der Anzeige der Datensatzanzahl in einer Liste finden Sie unter KBB0010402 KB-artikel.

Registerkarte „Listen“

Die folgenden Listen werden angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle Erforderlich
Korrekturaufgaben	Zeigen Sie die Liste der Korrekturaufgaben an, und navigieren Sie zur gewünschten Aufgabe, um mit der Bearbeitung zu beginnen. Die folgenden Listen sind verfügbar: • **Ihnen zugewiesen** : Listet alle Ihnen zugewiesenen Host-, Anwendungs-, Container- und Testergebnis-Korrekturaufgaben auf. • **Meiner Gruppe zugewiesen** : Listet alle Host-, Anwendungs-, Container- und Testergebnis-Korrekturaufgaben auf, die den Zuweisungsgruppen zugewiesen sind, denen Sie angehören. Gruppieren Sie die Aufgaben nach dem Datensatztyp, um sie in Korrekturaufgaben für Host-, Anwendungs-, Container- und Konfigurationstestergebnisse zu kategorisieren. Korrekturaufgaben, die von den Regeln für Korrekturaufgaben in der klassischen Anwenderoberfläche erstellt werden, haben eine leere Korrekturmaßnahme.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance	• sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits) • sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs) • sn_vul_Container.Remediation_owne für angreifbare Container-Elemente (CVITs) • sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle Erforderlich
Betroffene Assets	Zeigen Sie die Liste der betroffenen Assets an. Die folgenden Listen sind verfügbar: • **Ihnen zugewiesen** : Liste der betroffenen Konfigurationselemente, die Ihnen zugewiesen sind • **Meiner Gruppe zugewiesen** : Liste der betroffenen Konfigurationselemente, die Ihren Zuweisungsgruppen zugewiesen sind.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance	• sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits) • sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs) • sn_vul_Container.Remediation_owne für angreifbare Container-Elemente (CVITs) • sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)
Angreifbare Host-Elemente	Zeigen Sie die Liste der angreifbaren Host-Elemente an, und navigieren Sie zum gewünschten Element, um mit der Bearbeitung zu beginnen. Diese Listen sind verfügbar: • **Mir zugewiesen** : Liste der angreifbaren Host-Elemente, die Ihnen zur Korrektur zugewiesen sind. • **Meiner Gruppe zugewiesen** : Liste der angreifbaren Host-Elemente, die den Zuweisungsgruppen zugewiesen sind, denen Sie angehören.	Vulnerability Response	sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
Angreifbare Anwendungselemente	Zeigen Sie die Liste der angreifbaren Host-Elemente an, und navigieren Sie zum gewünschten Element, um mit der Bearbeitung	Application Vulnerability Response	sn_vul.App_Security_Champion

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle Erforderlich
	zu beginnen. Die folgenden Listen sind verfügbar: • **Mir zugewiesen** : Liste der angreifbaren Anwendungselemente, die Ihnen zur Korrektur zugewiesen sind. • **Meiner Gruppe zugewiesen** : Liste der angreifbaren Anwendungselemente, die den Zuweisungsgruppen zugewiesen sind, denen Sie angehören.		
Angreifbare Container-Elemente	Zeigen Sie die Liste der angreifbaren Container-Elemente an, und navigieren Sie zum gewünschten Element, um mit der Bearbeitung zu beginnen. Diese Listenansicht enthält: • **Mir zugewiesen** : Liste der angreifbaren Container-Elemente, die Ihnen zur Korrektur zugewiesen sind. • **Meiner Gruppe zugewiesen** : Liste der angreifbaren Container-Elemente, die den Zuweisungsgruppen zugewiesen sind, denen Sie angehören.	Container Vulnerability Response	sn_vul_Container.Remediation_owner Zeigen Sie die Liste der Bewertungen an, die für die Überprüfung nach Incident erforderlich sind.
Konfigurationstestergebnisse	Zeigen Sie die Liste der Testergebnisse an, und navigieren Sie zum	Konfigurations-Compliance	sn_vulc.Remediation_owner

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle Erforderlich
	gewünschten Datensatz, um mit der Bearbeitung zu beginnen. Diese Listenansicht enthält: • **Mir zugewiesen** : Liste der Konfigurationstestergebnisse, die Ihnen zur Korrektur zugewiesen sind. • **Meiner Gruppe zugewiesen** : Liste der Konfigurationstestergebnisse, die den Zuweisungsgruppen zugewiesen sind, denen Sie angehören.		
Lösungen	Listet die Lösungen aus der Anwendung „Lösungsmanagement“ auf. Die Liste Lösungen wird angezeigt, wenn die Anwendung Schwachstellenlösungsmanagement installiert ist. • **Alle** : Zeigt alle verfügbaren Lösungen an, die Sie zum Beheben der angreifbaren Host-Elemente verwenden. • **Höchster Ersatz** : Zeigt alle Lösungen an, die für ausgefüllte bevorzugte Lösungen verwendet werden. • **Mit angreifbaren Elementen** : Zeigt die Lösungen an, die als bevorzugte	Vulnerability Response	sn_vul.remediation_owner

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle Erforderlich
	Lösung für angreifbare Elemente verwendet werden.		
Ausnahmeanforderungen	• **Meine Anforderungen** : Liste aller Ausnahmen, falsch positive und nicht zugewiesene Genehmigungsanforderungen für angreifbare Host-, Anwendungs- und Container-Elemente und deren Korrekturaufgaben. • **Meine Anforderungen (Konfigurations-Compliance)** : Liste aller von Ihnen für die Testergebnisse und deren Korrekturaufgaben gestellten Ausnahmeanforderungen, falsch positiv und Zuweisung aufheben.	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance	• sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits) • sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs) • sn_vul_Container.Remediation_owne für angreifbare Container-Elemente (CVITs) • sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)
Bibliotheken	Enthält die folgenden Listen: • **NVDs** : Eine umfassende Bibliothek von Schwachstellen-Intelligence, die vom National Institute of Standards and Technology (NIST) verwaltet wird. Liste der von NVD gefundenen Schwachstellen	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance	• sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits) • sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs) • sn_vul_Container.Remediation_owne für angreifbare Container-Elemente (CVITs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle Erforderlich
	und enthält Sicherheitsprüflisten, sicherheitsbezogene Softwarefehler, Fehlkonfigurationen, Produktnamen und Auswirkungsmetriken einschließlich Exploits. • **CWEs** : Liste der in der Community entwickelten Softwareschwächungstypen. Jeder CWE-Datensatz enthält auch einen zugehörigen wissensartikel, der die Schwachstelle beschreibt. • **App-Schwachstellen** : Liste aller Einträge für Schwachstellen in Drittpartei-Anwendungen. • **TPEs** : Liste der importierten Schwachstellen von Drittparteien in Ihrer Instanz. Enthält eine Liste zugehöriger Referenzen, angreifbarer Elemente, Exploits und CVEs. • **Tests** : Tests, die aus den Drittparteiintegrationen importiert wurden, denen die Testergebnisse entsprechen müssen. • **Testgruppen** : Liste der Testgruppen/ Richtlinien, die aus den		• sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle Erforderlich
	Drittparteiintegrationen importiert wurden. Eine Testgruppe enthält eine Reihe von Tests.		
CMDB	• **Erkannte Elemente** : Liste aller erkannten Elemente. • **Erkannte Container-Images** :	Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance	• sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits) • sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs) • sn_vul_Container.Remediation_owne für angreifbare Container-Elemente (CVITs) • sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)
Anforderungen für Penetrationstestbewertung	Penetrationstest-Bewertungsanforderungen, die von Ihnen an das Sicherheitsteam übermittelt wurden, um eine Sicherheitsbewertung einer Geschäftsanwendung durchzuführen. Diese Liste enthält: • **Mir zugewiesen** : Liste der von Ihnen gestellten Penetrationstestbewertungsanforderungen. • **Meinen Gruppen zugewiesen** : Liste der Penetrationstestbewertungsanforderungen, die von den Anwendern	Application Vulnerability Response	sn_vul.App_Security_Champion

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle Erforderlich
	in Ihren Zuweisungsgruppen gestellt wurden.		
Penetrationstest-Ergebnisse	Liste der Schwachstellen, die während der vom Sicherheitsteam durchgeführten Pen-Testbewertung identifiziert wurden: • **Mir zugewiesen** : Liste der Penetrationstestergebnisse, die Ihnen zur Korrektur zugewiesen sind. • **Meinen Gruppen zugewiesen** : Liste der Penetrationstestergebnisse, die Ihren Zuweisungsgruppen zur Korrektur zugewiesen sind.	Application Vulnerability Response	sn_vul.App_Security_Champion
Unterstützungsdaten	Diese Listenansicht enthält: • **Autorisierende Quellen** : Liste der autorisierenden Quellen, die Zusammenfassungsinformationen bereitstellen, die für die Recherche der Quellveröffentlichungen nützlich sind, die zum Erstellen des Datensatzes verwendet wurden. • **Technologien** : Liste der Technologien, die Zusammenfassungsinformationen zu jeder autoritativen Quelle und Bezugsvermerk	Konfigurations-Compliance	sn_vulc.Remediation_owner

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Anwendungen erforderlich	Rolle Erforderlich
	bereitstellen (auch in Qualys als Framework bekannt).		

Zugehörige Informationen

Verwenden Sie die Listenansicht in Arbeitsbereich des Schwachstellenmanagers

Arbeitsbereich für IT-Korrekturen verwenden

Die Arbeitsbereich für IT-Korrekturen Bietet eine konsolidierte Liste von Host-Schwachstellen, Anwendungsschwachstellen, Container-Schwachstellen und Fehlkonfigurationen, die Ihnen und Ihrer Gruppe zugewiesen sind. Sie können diesen Arbeitsbereich verwenden, um Ausnahmen für Schwachstellen und Fehlkonfigurationen zu beheben und anzufordern.

Öffnen Sie Suchergebnisse in Arbeitsbereich für IT-Korrekturen

Legen Sie den Anwendungsbereich auf fest Arbeitsbereich für IT-Korrekturen Um Ihre Suchergebnisse in zu öffnen Arbeitsbereich für IT-Korrekturen Anstelle der klassischen UI durch Ändern des Anwendungsbereichs.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Beispiel: Wenn Sie nach einem angreifbaren Host-Element mit seiner Nummer in suchen **Suchen** Feld, indem der Anwendungsbereich auf festgelegt wird Arbeitsbereich für IT-Korrekturen, Wird die VIT in ihrer Datensatzansicht in geöffnet Arbeitsbereich für IT-Korrekturen.

Prozedur

1. Wählen Sie in der einheitlichen Navigationsleiste das Globus-Symbol aus .
2. Wählen Sie Aus **Anwendungsbereich** , Und legen Sie dann den Bereich auf fest **IT-Korrekturarbeitsbereich** .

Ergebnisse

Wenn Sie in nach Datensätzen wie Vits, Korrekturaufgaben, Status-Change-Genehmigungen usw. suchen **Suchen** Feld in der einheitlichen Navigationsleiste werden die Datensätze in geöffnet Arbeitsbereich für IT-Korrekturen.

Wenn der Umfang nicht global ist, wird das Globus-Symbol mit einem roten Ring angezeigt . Wählen Sie sie erneut aus, um den Umfang zu ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie den E-Mail-Digest in den Vulnerability Response-Arbeitsbereichen

Verwenden Sie E-Mail-Benachrichtigungen, um Ihren Korrekturfortschritt anzuzeigen und Sie daran zu erinnern, wenn sich Aufgaben nähern oder SLA-vergangen sind.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Kommen Sie als Korrekturbesitzer in Ihren Arbeitsbereich, und sehen Sie Ihre E-Mail-Benachrichtigung als Zusammenfassung Ihrer Arbeit. Sehen Sie, was Sie erreicht haben, was bevorsteht und was überfällig ist. Verwenden Sie die Benachrichtigung, um Ihre kritischen Korrekturaktionen zu organisieren und zu priorisieren. Klicken Sie auf einen Link in der E-Mail, um Sie direkt zu Ihrem Arbeitsbereich zu gelangen. Benachrichtigungen können IT-Spezialisten helfen, den Status ihrer Arbeit auf einen Blick zu sehen. Als Schwachstellenmanager helfen Sie Ihren IT-Spezialisten, direkt über ihren E-Mail-Service zur Plattform zu gelangen, um Korrekturaufgaben zu erledigen.

Siehe Richten Sie E-Mail-Benachrichtigungen in ein Vulnerability Response Arbeitsbereiche Weitere Informationen zum Konfigurieren dieser Funktion.

Die E-Mail zeigt standardmäßig die von Ihnen geschlossenen Aufgaben, die Gesamtzahl der Ihnen und Ihren Gruppen zugewiesenen aktiven Aufgaben, neu zugewiesen, geschlossene Vits und andere Informationen an.

Prozedur

1. Navigieren Sie zu Ihrer E-Mail, suchen Sie nach einer Benachrichtigung, und klicken Sie, um sie zu öffnen. Die Benachrichtigung wird mit Informationen zu Ihrem Arbeitsstatus angezeigt.
2. Klicken Sie Auf **Wechseln Sie zum Arbeitsbereich** Um zu Ihrem Arbeitsbereich zu navigieren.

Erstellen Sie eine Liste in Arbeitsbereich für IT-Korrekturen

Mit der Listenansicht in Arbeitsbereich für IT-Korrekturen, Sie können Korrekturaufgaben und Datensätze anzeigen, die Ihnen und Ihren Gruppen zugewiesen sind. Sie können auch Ihre Ausnahmen und falsch positiven Anforderungen für Korrekturaufgaben (VUL, AVUL, CVUL und CRG), angreifbare Elemente (VIT, AVIT und CVIT) und Testergebnisse (TRs) und Lösungen anzeigen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**an.
2. Wählen Sie das Listensymbol ( ) aus.
   Die Listenansicht wird angezeigt.
   - Klicken Sie auf eine gefilterte Liste, um die Gesamtzahl der aktiven Korrekturaufgaben oder Datensätze anzuzeigen, die Ihnen oder Ihrer Gruppe zugewiesen sind. Siehe Verwenden Sie Korrekturaufgaben-Datensätze in Arbeitsbereich für IT-Korrekturen Um weitere Informationen darüber zu erhalten, was Sie aus diesen Datensätzen tun können.
   - Zeigen Sie die Gesamtzahl der Ihnen oder Ihren Gruppen zugewiesenen VIS an, die Lösungen haben. Klicken Sie auf **Bevorzugte Lösungen für VIS** Karte zum Anzeigen der Liste.
   - Zeigen Sie die Ihnen und Ihren Gruppen zugewiesenen angreifbaren CIs an, die Schwachstellen aufweisen, auf der an **Angreifbare CIs** Registerkarte oder in den Ihnen zugewiesenen angreifbaren CIs und Ihrer Gruppenliste in der Listenansicht.
3. Wählen Sie die Registerkarte **Meine Listen** aus.
4. Wählen Sie **Neue Liste hinzufügen**.
5. Erstellen Sie die Liste entweder basierend auf einer vorhandenen Liste oder Ihrem eigenen Setup.
6. **Wahlweise:** Erstellen Sie eine gefilterte Liste.
   a. In **Wählen Sie Spalten aus** Feld festlegen, welche Spalten in der Liste angezeigt werden, indem alle Felder gelöscht werden, die nicht angezeigt werden sollen.
   b. Geben Sie Bedingungen zum Filtern der Liste an.
      (Optional) Um mehr als eine Bedingung hinzuzufügen, wählen Sie aus **Neuer Bedingungssatz** .
      Wenn Sie beispielsweise eine Liste aktiver angreifbarer Elemente für einen Scanner erstellen möchten, den Sie überwachen möchten, können Sie die Bedingungen eingeben **[Aktiv][ist][wahr]** Und **[Quelle][enthält][Scanner-Name]** .
   c. Wählen Sie **Erstellen** aus.
      Ihre neue Liste wird angezeigt.

      Hinweis:
      Wenn Sie das Listenmodul verlassen, wird die Liste angezeigt, die beim Beenden angezeigt wird, wenn Sie zurückkehren. Um die von Ihnen erstellten anwenderdefinierten Listen zu löschen und die Liste rechts im Bereich anzuzeigen, wählen Sie das Zahnradsymbol und dann aus **Löschen** .
7. In der folgenden Tabelle finden Sie, was Sie in der Listenansicht tun können.

Verwenden Sie Datensätze in Arbeitsbereich für IT-Korrekturen

Verwenden Sie Datensätze, um Ihren Korrekturfortschritt und die Auswirkungen angreifbarer Elemente auf Ihre Assets anzuzeigen.

Vorbereitungen

Erforderliche Rolle:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Prozedur

1. In Ihrem ServiceNow AI Platform Instanz, navigieren Sie zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**an.
   Die Startseite-Zielseite wird angezeigt.
2. Navigieren Sie zu einem Datensatz für angreifbare Elemente, und öffnen Sie ihn entweder auf der Startseite oder in der Listenansicht.

   Die Registerkarte „Details“ enthält Informationen im Formularheader oben, die sich auf die Art der Schwachstelle beziehen, z. B. CVE-2013-5014 unter LINUX-DAL-4331 erkannt . Unter dem Formularheader werden Werte für Status, Risikobewertung, Korrekturzieldatum angezeigt.
3. In der folgenden Tabelle finden Sie die UI-Aktionen, die Sie für den Korrekturaufgaben-Datensatz ausführen können.

Erstellen Sie eine Korrekturaufgabe manuell in Arbeitsbereich für IT-Korrekturen

Ab v25.0.4 von Vulnerability Response, Sie können Korrekturaufgaben manuell aus den Listen angreifbare Host-Elemente, angreifbare Anwendungselemente, angreifbare Container-Elemente und Konfigurationstestergebnisse auf der Listenseite von erstellen Arbeitsbereich für IT-Korrekturen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.write_assigned oder sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_write_assigned oder sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Writer_assigned oder sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen** > **Liste**an.
2. Öffnen Sie auf der Listenseite die Liste aktiv oder alle in einer der folgenden Listen:
   - Angreifbare Host-Elemente
   - Angreifbare Anwendungselemente
   - Angreifbare Container-Elemente
   - Konfigurationstestergebnisse
3. Aktivieren Sie das Kontrollkästchen der Datensätze, die Sie aktualisieren möchten, und wählen Sie dann aus Ausgewählte Elemente Option im Feld Datensatzauswahl im Modal „Korrekturaufgabe erstellen“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie Aus **Erstellen Sie Eine Korrekturaufgabe** .
5. Geben Sie im Modal „Korrekturaufgabe erstellen“ die folgenden Details ein.

Modales Element „Korrekturaufgabe erstellen“

Feld	Beschreibung
Datensatzauswahl	**Ausgewählte Elemente** : Aktualisiert nur die ausgewählten Datensätze.
Kurzbeschreibung	Kurze Notiz zu den Korrekturaufgaben.
Gruppierungskriterien	Die Auswahlmöglichkeiten lauten wie folgt: ○ **Zuweisungsgruppe** : Datensätze mit derselben Zuweisungsgruppe werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Konfigurationselement** : Datensätze mit derselben Zuweisungsgruppe und demselben Konfigurationselement werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Schwachstelle** : Datensätze mit derselben Zuweisungsgruppe und Schwachstelle werden in einer Korrekturaufgabe gruppiert. ○ **Zuweisungsgruppe und Risikobewertung** : Datensätze mit derselben Zuweisungsgruppe und Risikobewertung werden in einer Korrekturaufgabe gruppiert.
Datensätze in anderen Korrekturaufgaben werden verwaltet.	Die Auswahlmöglichkeiten lauten wie folgt: ○ **Überspringen Sie Datensätze für neue Korrekturaufgaben** : Für die Datensätze, die Teil anderer Korrekturaufgaben sind, wird keine Aktion ausgeführt. ○ **Wechseln Sie zu neuen Korrekturaufgaben** : Datensätze, die Teil anderer Korrekturaufgaben sind, werden an neue Korrekturaufgaben übertragen. ○ **Behalten Sie sowohl aktuelle als auch neue Korrekturaufgaben bei** : Datensätze, die Teil anderer Korrekturaufgaben sind, werden sowohl in alten als auch in neuen Korrekturaufgaben aufbewahrt.

6. Wählen Sie Aus **Erstellen Sie eine Korrekturaufgabe** .

Ergebnisse

Korrekturaufgaben werden basierend auf den Gruppierungskriterien erstellt. Eine E-Mail-Benachrichtigung wird an die Korrekturbesitzer in der Zuweisungsgruppe gesendet, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sie darüber informiert, dass eine Korrekturaufgabe erstellt und ihrer Gruppe zugewiesen wurde. Beispiele dafür, wie Korrekturaufgaben basierend auf den Gruppierungskriterien und Datensatzverwaltungskriterien erstellt werden, finden Sie unter Beispiele für die Erstellung von Korrekturaufgaben in Arbeitsbereich des Schwachstellenmanagers Und Arbeitsbereich für IT-Korrekturen.

Verwenden Sie Korrekturaufgaben-Datensätze in Arbeitsbereich für IT-Korrekturen

Korrekturaufgaben werden automatisch aus Korrekturmaßnahmen erstellt und zugewiesen. IT-Teams und Korrekturbesitzer können Korrekturaufgaben in anzeigen Arbeitsbereich für IT-Korrekturen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Wenn Schwachstellenmanager und Analysten Korrekturmaßnahmen erstellen, um die Korrektur voranzutreiben, werden Korrekturaufgaben automatisch erstellt und IT-Teams basierend auf der Gruppe zugewiesen, die den Datensätzen zugeordnet ist In einer Korrekturmaßnahme.

Zeigen Sie die Ihnen und Ihren Gruppen zugewiesenen angreifbaren CIs an, die Schwachstellen aufweisen, auf der an **Angreifbare CIs** Registerkarte oder in den Ihnen zugewiesenen angreifbaren CIs und Ihrer Gruppenliste in der Listenansicht.

Prozedur

1. In Ihrem ServiceNow AI Platform Instanz, navigieren Sie zu **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**an.
   Die Startseite-Zielseite wird angezeigt.
2. Klicken Sie im Abschnitt Korrekturaufgaben auf eine Korrekturaufgabe, um sie zu öffnen.
3. **Wahlweise:** Alternativ können Sie auf der Homepage oben links auf das Listensymbol klicken, um alle Korrekturaufgaben (VULs, AVULs, CVULs und CRGs) und Datensätze (Vits, AVITs, CVITs und TRs) anzuzeigen. Ihnen und Ihren Gruppen zugewiesen.
   Weitere Informationen zur Verwendung der Listenansicht finden Sie unter Erstellen Sie eine Liste in Arbeitsbereich für IT-Korrekturen.
4. Klicken Sie entweder auf der Homepage oder in der Listenansicht auf eine Korrekturaufgabe, um sie zu öffnen.

   In **Details** Registerkarte können Sie einige der Informationen im Datensatz aktualisieren, z. B. Zuweisungsgruppe, Status, Kurzbeschreibung usw. Klicken Sie auf **Speichern**, um Ihre Änderungen anzuwenden.
5. In der folgenden Tabelle finden Sie die UI-Aktionen, die Sie über den Korrekturaufgabendatensatz ausführen können.

   Auf der Registerkarte „Lösungen“ in einer Host-Korrekturaufgabe werden Informationen zu bevorzugten und potenziellen Lösungen angezeigt, die am besten mit der Schwachstelle übereinstimmen, die der Korrekturaufgabe zugeordnet ist. Lösungen sind Patches, die Ihre IT-Teams anwenden, um Schwachstellen zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Anwendung „Schwachstellenlösungsmanagement“ installiert ist, *Bevorzugte Lösungen* Sind die am häufigsten ersetzenden Lösungen, die auf angreifbare Elemente angewendet werden. Die Liste der Lösungen basiert auf den angreifbaren Elementen in der Host-Korrekturaufgabe.

Potenzielle Lösungen sind die Liste aller Lösungen, die für Vits in einer Host-Korrekturaufgabe verfügbar sind.

Sie können die CIs (Assets), die von dieser Schwachstelle betroffen sind, in der Korrekturaufgabe anzeigen, indem Sie zu navigieren **Übersicht** > **Betroffene CIs**an.

Weisen Sie sich im eine Korrekturaufgabe oder einen Korrekturdatensatz zu Arbeitsbereich für IT-Korrekturen

Weisen Sie sich selbst auf der Listenseite in eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) oder einen Datensatz (VIT, AVIT, CVIT oder TR) zu Arbeitsbereich für IT-Korrekturen Arbeitsbereich.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen** > **Liste** > **Korrekturaufgaben** > **Meiner Gruppe zugewiesen**an.
2. Öffnen Sie eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) aus der Liste „Korrekturaufgaben“.
3. Klicken Sie in den UI-Aktionsschaltflächen auf der rechten Seite auf **Mir zuweisen** .

   Die **Mir zuweisen** Die Schaltfläche ist nur verfügbar, wenn der Datensatz Ihnen nicht bereits zugewiesen ist.

   Die Korrekturaufgabe wird in der Liste mir zugewiesen unter Korrekturaufgaben angezeigt.
4. Sie können sich auch einen Datensatz (VIT, AVIT, CVIT oder TR) zuweisen, indem Sie dieselben Schritte aus einem offenen Datensatz ausführen.
   Die **Mir zuweisen** Die Schaltfläche ist nur verfügbar, wenn der Datensatz Ihnen nicht bereits zugewiesen ist.

Zeigen Sie Konfigurationselemente mit Schwachstellen in an Arbeitsbereich für IT-Korrekturen

Die folgenden Erweiterungen wurden Korrekturaufgaben mit Version 16,1 von hinzugefügt Vulnerability Response Anwendung.

Vorbereitungen
Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Die Rolle itil oder cmdb_read ist auch erforderlich, wenn Sie CI-Daten in den Arbeitsbereichen anzeigen möchten.

Warum und wann dieser Vorgang ausgeführt wird
Sehen Sie sich die Ihnen zugewiesenen Konfigurationselemente (Configuration Items, CI) an, die Schwachstellen aufweisen. Klicken Sie Auf **Betroffene CIs** Bewertungsliste. Klicken Sie oben links auf die Liste Filter, um zwischen umzuschalten **Mir zugewiesen** Und **Meinen Gruppen zugewiesen** . Klicken Sie in der Listenansicht auf die Links.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**an.
   Die Startseite-Zielseite wird angezeigt.
2. Alternativ können Sie diese Listen über die Links in der Listenansicht anzeigen oder zu ihren Modulen navigieren, z. B. **Alle** > **Vulnerability Response** > **Korrekturaufgaben**an.
3. Wählen Sie eine, um fortzufahren.
   Je nachdem, was im Filterumschalter ausgewählt ist, zeigen Sie die Listen der folgenden Datensätze an, die Ihnen oder Ihnen und Ihren Gruppen zugewiesen sind.
4. Klicken Sie auf **Betroffene CIs** Bewertungsliste.

   Die Liste der CI-Datensätze wird angezeigt.
5. Klicken Sie auf ein Konfigurationselement, um den zugehörigen Datensatz zu öffnen.
   Der Datensatz wird angezeigt.

   Mit den zugehörigen Listen können Sie Details und verschiedene zugehörige Datensätze anzeigen. Zu den neuen verfügbaren Daten für diesen Datensatz mit diesem Release gehören:
   - Eine Zeitlinie, die die letzte Aktivität für diesen Datensatz anzeigt.
   - Alle Change-Anforderungen, die diesem CI zugeordnet sind.
   - Navigieren Sie einfach zu Bewertungslisten, und zeigen Sie die Korrekturaufgaben, angreifbaren Elemente und bevorzugten Lösungen an, die diesem CI zugeordnet sind.
   - Sie können zu den Bewertungslisten navigieren und die bevorzugten Patches anzeigen, die diesem CI zugeordnet sind. Bevorzugte Patches sind die Patches, die den angreifbaren Elementen zugeordnet sind. Auf der Registerkarte Patches in der zugehörigen Liste werden die installierten und fehlenden Patches für die CIs angezeigt.
   - Informationen zum CI, einschließlich Klasse, Standort, Internetverbindung, Umgebung und Wartungszeitplan.

Erstellen Sie eine Change-Anforderung in Arbeitsbereich für IT-Korrekturen

Erstellen Sie aus einer Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) eine Change-Anforderung. Alternativ können Sie einer vorhandenen Change-Anforderung eine Korrekturaufgabe hinzufügen.

Vorbereitungen
Erforderliche Rolle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Hinweis:
Die Rolle „itli“ ist erforderlich, wenn Sie Change-Anforderungen über übermitteln möchten Arbeitsbereich für IT-Korrekturen.

Warum und wann dieser Vorgang ausgeführt wird

Es kann verschiedene Gründe geben, warum Sie eine Change-Anforderung für eine Korrekturaufgabe erstellen möchten. Normalerweise liegt dies daran, dass Ihre Untersuchung manuelle Eingriffe erfordert, um die Schwachstellen zu beheben.

Weitere Informationen zu den Change-Anforderungen und zum Erstellen von Change-Anforderungen in der klassischen Umgebung finden Sie unter Change-Management für Vulnerability Response.

Hinweis:
Ab v19.0 von Vulnerability Response, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie v19.0 und höher
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**an.
2. Wählen Sie das Listensymbol.
3. Suchen Sie auf der Listenseite in der Liste Korrekturaufgaben nach einer Korrekturaufgabe (VUL, AVUL, CVUL oder CRG), für die Sie eine Change-Anforderung erstellen möchten.
4. Erweitern Sie in den UI-Aktionsschaltflächen auf der rechten Seite die Liste, und wählen Sie eine aus:
   - Klicken Sie Auf **Erstellen Sie Einen Change**
   - **Zu vorhandenem Change hinzufügen**
5. Um eine neue Change-Anforderung zu erstellen, füllen Sie die Felder im angezeigten Modal aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Formularfelder für Change-Anforderungen erstellen.
6. Wählen Sie Aus **Erstellen Sie Eine Change-Anforderung** .
   Der Datensatz der Korrekturaufgabe wird angezeigt, und eine Meldung gibt an, dass die Change-Anforderung erfolgreich erstellt wurde.

   Klicken Sie in einem Datensatz auf den zugehörigen Link Change-Anforderungen, um alle dem Datensatz zugeordneten Change-Anforderungen anzuzeigen.
7. Alternativ führen Sie die folgenden Schritte aus, um diese Korrekturaufgabe einer vorhandenen Change-Anforderung hinzuzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf den Abwärtspfeil, um die Liste im zu erweitern **Erstellen Sie Einen Change** Schaltfläche.

b. Wählen Sie Aus **Zu vorhandenem Change hinzufügen** .

c. Klicken Sie im angezeigten Modal auf das Suchsymbol, um die Liste der vorhandenen Change-Anforderungen anzuzeigen.

d. Um der Liste Bedingungen hinzuzufügen, um die Liste der Change-Anforderungen zu fokussieren, klicken Sie oben rechts im Modal auf das Filtersymbol (Trichter).

e. Klicken Sie im neuen Bereich, der angezeigt wird, auf **Erweiterte Ansicht** .

f. Verwenden Sie den Bedingungsgenerator, um Ihre Bedingungen zu erstellen.

g. Wählen Sie **Aktualisieren**.

h. Klicken Sie in der Liste auf eine Change-Anforderung, um sie auszuwählen.
Ein aktualisiertes modales Element wird mit Ihrer Auswahl angezeigt.

i. **Wahlweise:** Aktivieren Sie im Modal das Kontrollkästchen CIs zu CR hinzufügen, um Konfigurationselemente aus allen aktiven angreifbaren Elementen zur Change-Anforderung hinzuzufügen.

j. Wählen Sie Aus **Fügen Sie einen Change hinzu** .
Der Korrekturdatensatz wird angezeigt, und eine Meldung gibt an, dass die Change-Anforderung erfolgreich erstellt und zur Genehmigung übermittelt wurde.

- Klicken Sie auf **Zeigen Sie den Change an** Link in der Nachricht zum Öffnen des Change Request-Datensatzes (CHG).
- Wählen Sie aus **Change-Anforderungen** Menülink für zugehöriges Element im Korrekturaufgaben-Datensatz, um alle dem Datensatz zugeordneten Change-Anforderungen anzuzeigen.

Alternativ navigieren Sie in der klassischen Umgebung zu **Selfservice** > **Meine Anforderungen**an. Wenn die Statussynchronisierung aktiviert ist, wird die Korrekturaufgabe automatisch zu verschoben, nachdem Sie den Change übermittelt und implementiert haben Gelöst . Weitere Informationen zu status und Statussynchronisierung in Change-Anforderungen finden Sie unter Erstellen Sie eine Change-Anforderung aus einer Korrekturaufgabe.

Teilen Sie eine Korrekturaufgabe in auf Arbeitsbereich für IT-Korrekturen

Identifizieren Sie in einer Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) eine Teilmenge von Datensätzen, und erstellen Sie eine neue Korrekturaufgabe für sie.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird
Sie können einzelne Datensätze auf der Registerkarte Übersicht einer Korrekturaufgabe auswählen und in eine neue Korrekturaufgabe verschieben.

Anwendungsfälle zum Aufteilen von Datensätzen (Vits, AVITs, CVITs oder CTRs) aus vorhandenen Korrekturaufgaben in neue Aufgaben können die folgenden Beispiele umfassen:

- Sie möchten eine Change-Anforderung oder Change-Anforderungen für eine geteilte Aufgabe erstellen.
- Sie möchten eine geteilte Aufgabe einem anderen Anwender in Ihrer Zuweisungsgruppe zuweisen.
- Sie fordern eine Zurückstellung oder Ausnahme für eine geteilte Aufgabe an, da Sie wissen, dass einige Schwachstellen bei bestimmten Konfigurationselementen (Configuration Items, CIs) bis zum Zieldatum nicht behoben werden können.

Weitere Informationen zu Change-Anforderungen und zum Aufteilen einer Korrekturaufgabe in der klassischen Umgebung und für Versionen von finden Sie Vulnerability Response Vor v15.0 finden Sie unter Teilen Sie eine Korrekturaufgabe auf.

Hinweis:
Ab v19.0 von Vulnerability Response, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie v19.0 und höher
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**an.
2. Öffnen Sie eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) auf der Homepage oder Listenseite.
3. Wählen Sie auf der Registerkarte Übersicht die Datensätze (Vits, AVITs, CVITs oder CTRs) aus, die Sie in eine neue Korrekturaufgabe verschieben möchten.
4. Klicken Sie Auf **Aufgabe Aufteilen** .
5. Im angezeigten Dialogfeld wird die Anzahl der Datensätze (Vits, AVITs, CVITs oder CTRs) angezeigt, die Sie aus der Liste ausgewählt haben.
6. Klicken Sie Auf **Aufgabe Aufteilen** Erneut.
   Eine Bestätigungsnachricht mit einem Link zur neuen Korrekturaufgabe wird angezeigt.

   Alternativ können Sie den Bedingungsgenerator verwenden, um Datensätze (Vits, AVITs, CVITs oder CTRs) zu filtern.
7. Suchen Sie eine Korrekturaufgabe, die Sie aufteilen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie in den UI-Aktionsschaltflächen auf der rechten Seite auf **Aufgabe Aufteilen** .
   Nach einigen Minuten wird der Bedingungsgenerator angezeigt.
9. Verwenden Sie im angezeigten Modal den Bedingungsgenerator, um die gewünschte Teilmenge der Datensätze (Vits, AVITs, CVITs oder CTRs) zu identifizieren Bis Fügen Sie einer neuen Korrekturaufgabe hinzu.
10. Klicken Sie Auf **Aufgabe Aufteilen** .
    Wenn eine Meldung angezeigt wird, dass keine Datensätze Ihren Bedingungen entsprechen, müssen Sie Ihre Kriterien anpassen und auf klicken **Aufgabe Aufteilen** Erneut. Bearbeiten Sie das Feld Kurzbeschreibung nach Bedarf. Dieses Feld kann Ihnen helfen, Ihre neue Korrekturaufgabe nach ihrer Erstellung zu finden.

    Wenn Datensätze Ihren Bedingungen entsprechen, wird die Anzahl der übereinstimmenden Datensätze in einer Nachricht angezeigt.
11. **Wahlweise:** Klicken Sie auf **Vorschau der Elemente anzeigen** Link zum Anzeigen der Datensätze, die Ihren Filterbedingungen entsprechen.
    Die neue Korrekturaufgabe wird als neue Registerkarte angezeigt.

Fordern Sie ein falsch positives Ergebnis für ein angreifbares Element oder eine Korrekturaufgabe an

Geben Sie eine falsch positive Anforderung für das Host Angreifbare Element (VIT), das Angreifbare Anwendungselement (AVIT), das Angreifbare Container-Element (CVIT) oder die Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) in an Arbeitsbereich für IT-Korrekturen. Ein falsch positives ist eine Bedingung, bei der ein Scanner fälschlicherweise meldet, dass eine Schwachstelle im System aufgrund von Situationen wie einer falschen Klassifizierung, einer falschen Logik oder einem Algorithmus im Scanner vorhanden ist.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Informationen zum anfordern eines falsch positiven Werts für eine Reihe von Testergebnissen finden Sie unter Fordern Sie ein falsch positives Ergebnis für eine Reihe von Testergebnissen an.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**an.
2. Wählen Sie Listensymbol ( ).
3. Wählen Sie die Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) oder das angreifbare Element (VIT, AVIT oder CVIT) aus.
4. Wählen Sie Aus **Als falsch positiv markieren** .
5. Geben Sie Informationen zur Anforderung ein.
6. Wählen Sie **Genehmigung anfordern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Geben Sie dem Genehmiger zusätzliche Informationen zu Ihrer Anforderung an, und wählen Sie aus **Übermitteln** .

> **Hinweis:**
> Das modale Element „Fragebogen ausfüllen“ wird nur angezeigt, wenn die **Aktivieren Sie den Fragebogen, um falsch positiv zu markieren** Das Kontrollkästchen ist im Formular „Konfiguration für Ausnahmemanagement“ aktiviert. Weitere Informationen finden Sie unter Konfigurieren Sie das Ausnahmemanagement für Vulnerability Response, Konfigurieren Sie das Ausnahmemanagement für Application Vulnerability Response, Konfigurieren Sie das Ausnahmemanagement für Container Vulnerability Response, Und Konfigurieren Sie das Ausnahmemanagement für Konfigurations-Compliance.

Ergebnisse

Der Status des angreifbaren Elements (VIT, AVIT oder CVIT) oder der Korrekturaufgabe (VUL, AVUL oder CVUL) wechselt zu „in Überprüfung“.

Ihre Anforderung wird zur Genehmigung übermittelt, und der Genehmiger erhält eine E-Mail-Benachrichtigung über Ihre Anforderung.

Sie erhalten eine E-Mail-Benachrichtigung, wenn Sie Ihre Anforderung genehmigen oder ablehnen.

Nächste Maßnahme

Navigieren Sie im IT-Korrekturarbeitsbereich auf der Listenseite zu **Ausnahmeanforderungen** > **Meine Anforderungen** Öffnen Sie den entsprechenden Datensatz für die Genehmigung von Statusänderungen (VCA#), und überprüfen Sie den Status Ihrer Anforderung in der Spalte Genehmigungsstatus:

Genehmigungsstatus	Datensatz (VIT, AVIT oder CVIT)	Korrekturaufgabe (VUL, AVUL, CVUL oder CRG)
Genehmigt	Der Status des Datensatzes wechselt zu „Geschlossen“ mit dem Grund „falsch positiv“.	Der Status der Korrekturaufgabe wechselt zu „Geschlossen“ mit dem Grund „falsch positiv“. Der Status wird entsprechend auf die Datensätze in der Korrekturaufgabe zurückgesetzt. Navigieren Sie zur Registerkarte Details einer Korrekturaufgabe, und legen Sie das Ablaufdatum für falsch positiv in fest **Bis** Feld, falls erforderlich. Die Korrekturaufgabe wird nach dem angegebenen Datum in den Status Offen zurückgesetzt, und der Status wird auf die Testergebnisse zurückgesetzt.
Abgelehnt	Der Status des Datensatzes ändert sich nicht.	Der Status der Korrekturaufgabe und ihrer Datensätze wird auf den vorherigen Status zurückgesetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In **Aktivitätenstrom** Eines Datensatzes oder einer Korrekturaufgabe können Sie den gesamten Workflow der falsch positiven Anforderung anzeigen.

Zugehörige Informationen

Falsch Positiv Übersicht

Fordern Sie ein falsch positives Ergebnis für eine Reihe von Testergebnissen an

Stellen Sie eine falsch positive Anforderung für eine Reihe von Testergebnissen innerhalb einer Korrekturaufgabe in der Arbeitsbereich für IT-Korrekturen.

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Bedingungen müssen erfüllt sein, damit Sie ein falsch positives Ergebnis für eine Reihe von Testergebnissen innerhalb einer Korrekturaufgabe anfordern können:

- Version 22,0 von Vulnerability Response Muss installiert sein.
- Mindestens ein ausgewähltes Testergebnis muss sich im Status „aktiv“ befinden
- Die Korrekturaufgabe muss mindestens zwei Testergebnisse aufweisen
- Mindestens ein Testergebnis ist nicht ausgewählt

Vorbereitungen

Erforderliche Rolle: sn_vulc.Remediation_owner

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**an.
2. Wählen Sie das Listensymbol ( ) aus.
3. Wählen Sie auf der Listenseite die aus Konfigurations-Compliance Korrekturaufgabe.
4. Wählen Sie in der zugehörigen Liste Übersicht auf der Registerkarte Testergebnisse die Testergebnisse aus, die Sie als falsch positiv markieren möchten.
5. Wählen Sie aus **Als falsch positiv markieren** Schaltfläche auf der Registerkarte Konfigurationstestergebnisse.
6. Geben Sie im angezeigten Dialogfeld Informationen zur Anforderung ein, und wählen Sie aus **Genehmigung Anfordern** .
7. Beantworten Sie im Modal „Fragebogen erstellen“ die Fragen, um dem Genehmiger zusätzliche Informationen zu Ihrer Anforderung bereitzustellen, und wählen Sie aus **Übermitteln** .

Hinweis:
Das modale Element „Fragebogen ausfüllen“ wird nur angezeigt, wenn die **Aktivieren Sie den Fragebogen, um falsch positiv zu markieren** Das Kontrollkästchen ist im Formular „Konfiguration für Ausnahmemanagement“ aktiviert. Weitere Informationen zur Konfiguration eines Fragebogens finden Sie unter Konfigurieren Sie das Ausnahmemanagement für Konfigurations-Compliance.

Ergebnisse

Die ausgewählten Testergebnisse werden in eine neue Korrekturaufgabe verschoben, und Ihre Anforderung wird zur Genehmigung übermittelt. Die Aufgabennummer wird in angezeigt **Aktivitätenstrom** Der alten Korrekturaufgabe. Der Genehmiger erhält eine E-Mail-Benachrichtigung über Ihre Anforderung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie erhalten eine E-Mail-Benachrichtigung über die Genehmigung oder Ablehnung Ihrer Anforderung. In **Aktivitätenstrom** Eines Testergebnisses oder einer Korrekturaufgabe können Sie den gesamten Workflow der falsch positiven Anforderung anzeigen.

Nächste Maßnahme

1. In Arbeitsbereich für IT-Korrekturen Navigieren Sie auf der Listenseite zu **Ausnahmeanforderungen** > **Meine Anforderungen**an.
2. Öffnen Sie den entsprechenden Datensatz für die Genehmigung von Statusänderungen (VCA#), und überprüfen Sie den Status Ihrer Anforderung in der Spalte Genehmigungsstatus:

Genehmigungsstatus	Ergebnis
Genehmigt	Der Status der neuen Korrekturaufgabe wechselt zu „Geschlossen“ mit dem Grund „falsch positiv“.
Abgelehnt	Der Status der neuen Korrekturaufgabe ändert sich in Offen.

3. Nachdem die Anforderung genehmigt wurde, navigieren Sie zur Registerkarte Details der neuen Korrekturaufgabe, und legen Sie das Ablaufdatum für falsch positiv in fest **Bis** Feld, falls erforderlich.

   Die Korrekturaufgabe kehrt nach dem angegebenen Datum in den Status Offen zurück, und der Status wird auf die Testergebnisse zurückgesetzt.

Fordern Sie eine Ausnahme in an Arbeitsbereich für IT-Korrekturen

Fordern Sie eine Ausnahme für das angreifbare Host-Element (VIT), das angreifbare Anwendungselement (AVIT), das angreifbare Container-Element (CVIT) und die Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) von an Arbeitsbereich für IT-Korrekturen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Einige Schwachstellen haben möglicherweise keinen Patch, eine Korrektur oder eine Lösung. Oder Sie können feststellen, dass eine Korrekturaufgabe bis zum Zieldatum nicht gelöst werden kann. Wenn Ihre Korrektur nicht mit einer veröffentlichten Schwachstellenmanagement- oder Sicherheitsrichtlinie, einem Standard oder einer Richtlinie für Schwachstellenmanagement oder -Sicherheit übereinstimmen kann, können Sie eine Ausnahme anfordern.

Sie können Ausnahmen für Korrekturaufgaben (VUL, AVUL, CVUL oder CRG) und angreifbare Elemente (VIT, AVIT oder CVIT) über anfordern Arbeitsbereich für IT-Korrekturen Die Ihnen zugewiesen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ab v19.0 von Vulnerability Response, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie v19.0 und höher
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Ab Version 18,0 , Sie können Ausnahmen für Schwachstellen-Anwendungselemente und Container-Schwachstellen-Elemente anfordern.

Weitere Informationen zum anfordern von Ausnahmen in der klassischen Umgebung finden Sie unter Fordern Sie eine Ausnahme für eine Korrekturaufgabe an.

Prozedur

1. Navigieren zu **Alle** > **Vulnerability Response** > **Arbeitsbereich für IT-Korrekturen**an.
2. Wählen Sie das Listensymbol.
3. Öffnen Sie in der Liste „Korrekturaufgaben“ eine Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) oder einen Datensatz (Vits, AVITs oder CVITs), für den Sie eine Ausnahme anfordern möchten.
4. Klicken Sie in den UI-Aktionsschaltflächen auf der rechten Seite auf **Ausnahme Anfordern** .
5. Geben Sie im angezeigten Dialogfeld das Enddatum für die Ausnahme ein, wählen Sie einen Grund aus der Liste aus, und fügen Sie weitere erforderliche Informationen hinzu.
6. Klicken Sie Auf **Ausnahme Anfordern** .
7. Auf der **Nehmen Sie An Dem Fragebogen Teil** Modal, beantworten Sie die Fragen, und klicken Sie auf **Übermitteln** .

Hinweis:
Die **Nehmen Sie An Dem Fragebogen Teil** Modal wird nur angezeigt, wenn **Aktivieren Sie den Fragebogen, um eine Ausnahme anzufordern** Das Kontrollkästchen ist in aktiviert **Ausnahmeverwaltungskonfiguration** Formular.

Eine Meldung zeigt an, dass Ihre Anforderung erfolgreich zur Genehmigung übermittelt wurde.

Eine Ausnahmeanforderung für eine Korrekturaufgabe wird mit einem standardmäßigen Genehmigungs-Workflow auf zwei Ebenen genehmigt. Nachdem die Anforderung vom Genehmiger der Ebene 1 genehmigt wurde, wird sie an den Genehmiger der Ebene 2 gesendet.

- Die Korrekturaufgabe oder der Korrekturdatensatz wechselt zu „in Überprüfung“, während die Ausnahmeanforderung geöffnet ist.
- Die Korrekturaufgabe oder der Korrekturdatensatz wechselt zu zurückgestellt, wenn die Anforderung genehmigt wird.
- Der Ausnahmeanforderungsdatensatz (VCA#) wird geschlossen, nachdem Ihre Ausnahmeanforderung genehmigt wurde.

Um den Status Ihrer Genehmigungsanforderungen anzuzeigen, klicken Sie unter Ausnahmeanforderungen auf der Listenseite auf **Meine Anforderungen** . Die Nummer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für die Anforderung (VCA#) wird angezeigt, wenn Sie den Datensatz oder die Korrekturaufgabe aus der Liste öffnen.

- Wenn die Anforderung abgelehnt wird, wird der Anforderungsdatensatz (VCA#) angezeigt **Abgelehnt** In der Spalte Genehmigungsstatus in Ihrer Listenansicht unter meine Anforderungen.
- Sie müssen eine neue Ausnahmeanforderung übermitteln, wenn Sie dieses Element trotzdem zurückstellen möchten.

Fordern Sie eine Ausnahme mit an GRC: Richtlinien- und Compliance-Management In Arbeitsbereich für IT-Korrekturen

Fordern Sie eine Richtlinienausnahme für das angreifbare Host-Element (VIT), das angreifbare Anwendungselement (AVIT), das angreifbare Container-Element (CVIT) oder die Korrekturaufgabe (VUL, AVUL, CVUL oder CRG) von an Arbeitsbereich für IT-Korrekturen.

Vorbereitungen

Erforderliche Rolle:

- sn_vul.Remediation_owner für angreifbare Host-Elemente (Vits)
- sn_vul.App_Security_Champion für angreifbare Anwendungselemente (AVITs)
- sn_vul_Container.Remediation_owner für angreifbare Container-Elemente (CVITs)
- sn_vulc.Remediation_owner für Konfigurationstestergebnisse (CTRs)

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Ab v19.0 von Vulnerability Response, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v19.0	Terminologie v19.0 und höher
Testergebnisgruppen	Korrekturaufgaben
Konfigurationsprobleme	Konfigurationstestergebnisse
Richtlinie	Testgruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**an.
2. Wählen Sie im Anwendungsnavigator das Listensymbol ( ).
3. Wählen Sie auf der Listenseite unter angreifbare Host-Elemente, angreifbare Anwendungselemente, angreifbare Container-Elemente oder Korrekturaufgaben (VUL, AVUL, CVUL oder CRG) den Datensatz aus, für den Sie eine Ausnahme anfordern möchten.
   Der von Ihnen ausgewählte Datensatz muss sich im Status „Offen“, „wird untersucht“ oder „Warten auf Implementierung“ befinden.
4. Wählen Sie aus **Ausnahme Anfordern** Schaltfläche.
5. Füllen Sie im Formular die Felder aus.
   Weitere Informationen zu den Formularfeldern finden Sie unter Formularfelder „Ausnahme anfordern“ für Richtlinienausnahmen.
6. Wählen Sie Aus **Ausnahme Anfordern** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Beantworten Sie im Modal „Fragebogen erstellen“ die Fragen, um zusätzliche Informationen zu Ihrer Anforderung bereitzustellen, und wählen Sie aus **Übermitteln** .

> **Hinweis:**
> Das Modal „Fragebogen ausfüllen“ wird nur angezeigt, wenn die Fragebogendetails der jeweiligen Integrationsregistrierung hinzugefügt werden.

Es wird eine Nachricht angezeigt, dass Ihre Anforderung erfolgreich zur Genehmigung übermittelt wurde.

Weitere Informationen zur Integration von Richtlinienausnahmen und zur Übergabe zwischen dem Korrekturbesitzer und dem Compliance-Manager finden Sie unter Optionales Setup für Richtlinien- und Compliance-Management .

Fordern Sie eine Risikominderung für ein angreifbares Element oder eine Korrekturaufgabe an

Fordern Sie eine Risikominderung für ein angreifbares Host-Element oder eine Korrekturaufgabe in an Arbeitsbereich für IT-Korrekturen.

Vorbereitungen
Erforderliche Rolle: sn_vul.Remediation_owner

Warum und wann dieser Vorgang ausgeführt wird
Ab v21.0 von Vulnerability Response, Sie können die Risikominderung nur für die folgenden Elemente anfordern :

- A Korrekturaufgabe Nur Wenn alle seine angreifbaren Elemente zugeordnet sind Die Gleicher allgemeiner Schwachstelleneintrag (CVE) Unabhängig davon, ob die Risikominderung für CVEs aktiviert ist.
- Eine Drittpartei (TPE), für die die Risikominderung aktiviert ist.

> **Hinweis:**
> Die Funktion „Ausgleichssteuerungen“ ist nur für Host-Schwachstellen verfügbar.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für IT-Korrekturen**an.
2. Wählen Sie das Listensymbol ( ) aus.
3. Öffnen Sie auf der Listenseite ein angreifbares Host-Element oder eine Korrekturaufgabe.
4. Wählen Sie das Symbol „weitere Optionen“, und wählen Sie aus **Ausnahme Anfordern** .
5. Füllen Sie die Felder im Formular „Ausnahme anfordern“ aus.
   Eine Beschreibung der Feldwerte finden Sie unter Formular „Ausnahme anfordern“ Zur Risikominderung.
6. Wählen Sie Aus **Ausnahme Anfordern** .
7. Wenn das Modal „Fragebogen ausfüllen“ angezeigt wird, beantworten Sie die Fragen, um zusätzliche Informationen zu Ihrer Anforderung bereitzustellen, und wählen Sie aus **Übermitteln** .

> **Hinweis:**
> Das Modal „Fragebogen ausfüllen“ wird nur angezeigt, wenn der Fragebogen für das Ausnahmemanagement aktiviert ist. Weitere Informationen finden Sie unter Konfigurieren Sie das Ausnahmemanagement für Vulnerability Response.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Eine Nachricht wird angezeigt, dass Ihre Anforderung erfolgreich zur Genehmigung übermittelt wurde. Eine Benachrichtigung über Ihre Anforderung wird an den Genehmiger gesendet.

- Wenn Ihre Anforderung eine Zurückstellung und Risikominderung betrifft:
  - Zwei Status-Change-Genehmigungen (VCA#) werden für die Zurückstellung und die Risikominderung erstellt.
  - Der Status des Datensatzes ändert sich in „in Überprüfung“.
- Wenn Ihre Anforderung nur zur Risikominderung dient:
  - Eine Statusänderungsgenehmigung (VCA#) wird erstellt.
  - Der Status ändert sich nicht.

Bei Genehmigung oder Ablehnung Ihrer Anforderung erhalten Sie eine Benachrichtigung. Weitere Informationen zum Genehmigungsprozess finden Sie unter Genehmigen oder lehnen Sie Anforderungen in ab Arbeitsbereich des Schwachstellenmanagers.

Weitere Informationen dazu finden Sie unter **Bis-Datum für die Risikominderung**
Wird für eine Korrekturaufgabe und ein angreifbares Element aktualisiert, wenn eine Anforderung zur Risikominderung genehmigt wird, siehe Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum.

Zugehörige Informationen

Erläuterungen zu Ausgleichssteuerungen Zur Risikominderung

Deaktivieren oder aktivieren Sie die Risikominderung für ein CVE oder TPE

Fügen Sie der Bibliothek eine Ausgleichssteuerung hinzu

Auswirkung der Ausgleichssteuerungen auf Risikopunktzahl und Ablaufdatum

Scannen Sie angreifbare Elemente und Korrekturaufgaben in erneut Arbeitsbereich für IT-Korrekturen

Überprüfen Sie, ob Ihre angreifbaren Elemente zwischen den geplanten Scanzyklen behoben wurden. Initiieren Sie erneutes Scannen über Arbeitsbereich für IT-Korrekturen In Ihrem ServiceNow AI Platform Bei Bedarf.

Durch erneutes Scannen können Sie verifizieren, ob Ihre Korrekturaktivitäten, Patches und anderen Aktionen bestimmte Schwachstellen in Ihren Konfigurationselementen (Configuration Items, CIs) erfolgreich behoben haben.

Erneutes Scannen wird für die folgenden Integrationen in unterstützt Arbeitsbereich für IT-Korrekturen. Weitere Informationen finden Sie in den folgenden Themen:

- Erneut Scannen Qualys Angreifbare Elemente aus dem Vulnerability Response Arbeitsbereiche
- Erneut Scannen Rapid7 Angreifbare Elemente aus dem Vulnerability Response Arbeitsbereiche
- Erneut Scannen Tenable.io Und Tenable.sc Angreifbare Elemente aus dem Vulnerability Response Arbeitsbereiche

Erforderliche Rollen: sn_vul.Remediation_owner für Arbeitsbereich für IT-Korrekturen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erneut Scannen Qualys Angreifbare Elemente aus dem Vulnerability Response Arbeitsbereiche

Überprüfen Sie, ob Ihre angreifbaren Elemente zwischen den geplanten Scanzyklen behoben wurden. Initiieren Sie erneutes Scannen in Qualys Produkt bei Bedarf von Arbeitsbereich für IT-Korrekturen In Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen

Um einen erneuten Scan für zu initiieren Qualys Produkt aus der klassischen Umgebung, siehe Initiieren Sie einen erneuten Scan für Qualys Vulnerability Integration.

Die Qualys Scanner sind standardmäßig in deaktiviert Vulnerability Response Anwendung. Wenn Sie versuchen, einen erneuten Scan von den angreifbaren Elementen oder Korrekturaufgaben durchzuführen, die diese Anwendungen als Quelle haben, wird der **Erneut Scannen** Schaltfläche ist nicht verfügbar.

So aktivieren Sie diese Scanner als Anwender mit der Rolle sn_vul.Vulnerability_admin:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**an.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um es zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

   Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle in Datensätzen für angreifbare Elemente und Korrekturaufgaben angezeigt **Erneut Scannen** Ist als UI-Aktion verfügbar.

Weitere Informationen zum Einrichten von finden Sie Qualys Scanner, siehe Richten Sie Scannergeräte ein Und Erweitert Qualys Konfigurationen und Änderungen.

- Sie können bei Bedarf erneute Scans für angreifbare Elemente und Korrekturaufgaben initiieren, die über verfügen Qualys Produkt als Quelle von Arbeitsbereich für IT-Korrekturen In Ihrem ServiceNow AI Platform.
- Bei einem Korrekturaufgabendatensatz kann sich der Datensatz in einem anderen Status als befinden **Geschlossen** , Und alle zugeordneten VIS müssen aus dem stammen Qualys Produkt.
- Um erneutes Scannen im IT-Korrekturarbeitsbereich aus Datensätzen für angreifbare Elemente und Korrekturaufgaben zu initiieren, müssen Ihnen diese Datensätze zugewiesen werden.

Erforderliche Rollen:

- sn_vul.Remediation_owner für Arbeitsbereich für IT-Korrekturen.
- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin aus dem Vulnerability Manager-Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zu einem angreifbaren Element oder einer Korrekturaufgabe, die Ihnen zugewiesen wurde, und öffnen Sie sie.

   Hinweis:
   Wenn Sie eine Korrekturmaßnahme auswählen, um einen erneuten Scan zu initiieren, werden alle diesem Datensatz zugeordneten VIS gescannt.

2. Klicken Sie oben rechts im Datensatz auf **Erneut Scannen** .
3. Wählen Sie im Modal „erneut scannen“ ein Optionsprofil aus.
   Ein Optionsprofil ist erforderlich, wenn Sie eine initiieren Qualys Scannen Sie von Ihrem aus ServiceNow AI Platform®. Optionsprofile enthalten Qualys Scaneinstellungen.
4. Klicken Sie im Modal „erneut scannen“ auf **Erneutes Scannen anfordern** .
   Die Nachricht, Die Scan-Anforderung wird verarbeitet Wird angezeigt.
5. Klicken Sie auf **Status anzeigen** Link in der Nachricht, um den Fortschritt des Scans anzuzeigen.

   Der Scan-Datensatz (VSCAN#) wird angezeigt. Unter dem Datensatz-Header mit der Scan-Nummer werden in den zugehörigen Elementlisten die folgenden Informationen angezeigt:

   - In der Liste Details werden die Scan-Nummer des übergeordneten Scans, die Scannerquelle und der Status angezeigt. Zeigen Sie abgeschlossene und fehlgeschlagene Scans im Abschnitt „Scan-Zusammenfassung“ an.
   - In der Liste „Scans“ werden alle untergeordneten Scans und ihre status angezeigt. Wenn alle untergeordneten Scans abgeschlossen sind, wechselt der Status des übergeordneten Scans in „Abgeschlossen“.
   - Die Liste Quelle zeigt das für den Scan verwendete angreifbare Element, das zugehörige Konfigurationselement und die Schwachstelle, den Status des VI und seinen Korrekturstatus an.

   Ihr ServiceNow AI Platform® Die Instanz verfolgt den Status des erneuten Scans, bis er erfolgreich abgeschlossen ist, oder bis der festgelegte Nachverfolgungszeitraum abgelaufen ist, je nachdem, was zuerst geschieht.

   Durch die Zeitüberschreitung wird der Scan nicht beendet. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, an dem der ServiceNow AI Platform® Die Nachverfolgung des Status des erneuten Scans wurde beendet, nicht wenn der tatsächliche erneute Scan beendet wurde.

   Alle VIS, die in „Geschlossen/behoben“ übergegangen sind oder übergehen werden, werden mit dem nächsten geplanten Import von importiert Qualys Integrationen.

Erneut Scannen Rapid7 Angreifbare Elemente aus dem Vulnerability Response Arbeitsbereiche

Überprüfen Sie, ob Ihre angreifbaren Elemente zwischen den geplanten Scanzyklen behoben wurden. Initiieren Sie erneutes Scannen in Rapid7 Produkt bei Bedarf aus dem IT-Korrekturarbeitsbereich in Ihrem ServiceNow AI Platform Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Informationen zum Initiieren eines erneuten Scans für das Produkt aus der klassischen Umgebung finden Sie unter Initiieren Sie einen erneuten Scan für Rapid7 Schwachstellenintegration. Dieses Thema enthält auch Informationen zum Planen von Scans mit den Integrationsparametern in Rapid7 Integrationsinstanz.

Die Rapid7 Scanner sind standardmäßig in deaktiviert Vulnerability Response Anwendung. Wenn Sie versuchen, einen erneuten Scan über die angreifbaren Elemente oder Korrekturaufgaben durchzuführen, die haben Rapid7 Anwendung als Quelle, die **Erneut Scannen** Schaltfläche ist nicht verfügbar.

So aktivieren Sie diese Scanner als Anwender mit der Rolle sn_vul.Vulnerability_admin:

1. Navigieren zu **Alle** > **Vulnerability Response** > **Schwachstellenscan** > **Scanner**an.
2. Suchen Sie das Scannerprodukt, das Sie aktivieren möchten, und klicken Sie auf den Datensatz, um es zu öffnen.
3. Aktivieren Sie die Checkbox Aktiv.
4. Klicken Sie auf **Aktualisieren**.

   Das von Ihnen aktivierte Produkt wird nach dem nächsten Import im Feld Quelle in Datensätzen für angreifbare Elemente und Korrekturaufgaben angezeigt **Erneut Scannen** Ist als UI-Aktion verfügbar.

- Sie können bei Bedarf erneute Scans für angreifbare Elemente und Korrekturaufgaben initiieren, die über verfügen Rapid7 InsightVM Produkt als Quelle aus dem IT-Korrekturarbeitsbereich in Ihrem ServiceNow AI Platform.
- Bei einem Korrekturaufgabendatensatz kann sich der Datensatz in einem anderen Status als befinden **Geschlossen** , Und alle zugeordneten VIS müssen aus dem stammen Rapid7 Produkt.
- Um erneutes Scannen im IT-Korrekturarbeitsbereich aus Datensätzen für angreifbare Elemente und Korrekturaufgaben zu initiieren, müssen Ihnen diese Datensätze zugewiesen werden.

Erforderliche Rollen:

- sn_vul.Remediation_owner für den IT-Korrekturarbeitsbereich
- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin aus dem Vulnerability Manager-Arbeitsbereich

Prozedur

1. Navigieren Sie zu einem angreifbaren Element oder einer Korrekturaufgabe, die Ihnen zugewiesen wurde, und öffnen Sie sie.

   Hinweis:
   Wenn Sie eine Korrekturmaßnahme auswählen, um einen erneuten Scan zu initiieren, werden alle diesem Datensatz zugeordneten VIS gescannt.

2. Klicken Sie oben rechts im Datensatz auf **Erneut Scannen** .
3. Klicken Sie im Modal „erneut scannen bestätigen“ auf **Erneutes Scannen anfordern** .
   Die Nachricht, Die Scan-Anforderung wird verarbeitet Wird angezeigt.
4. Klicken Sie auf **Status anzeigen** Link in der Nachricht, um den Fortschritt des Scans anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Scan-Datensatz (VSCAN#) wird angezeigt. Unter dem Datensatz-Header mit der Scan-Nummer werden in den zugehörigen Elementlisten die folgenden Informationen angezeigt:

- In der Liste Details werden die Scan-Nummer des übergeordneten Scans, die Scannerquelle und der Status angezeigt. Zeigen Sie abgeschlossene und fehlgeschlagene Scans im Abschnitt „Scan-Zusammenfassung“ an.
- In der Liste „Scans“ werden alle untergeordneten Scans und ihre status angezeigt. Wenn alle untergeordneten Scans abgeschlossen sind, wechselt der Status des übergeordneten Scans in „Abgeschlossen“.
- Die Liste Quelle zeigt das für den Scan verwendete angreifbare Element, das zugehörige Konfigurationselement und die Schwachstelle, den Status des VI und seinen Korrekturstatus an.

Ihr ServiceNow AI Platform® Die Instanz verfolgt den Status des erneuten Scans, bis er erfolgreich abgeschlossen ist, oder bis der festgelegte Nachverfolgungszeitraum abgelaufen ist, je nachdem, was zuerst geschieht.

Durch die Zeitüberschreitung wird der Scan nicht beendet. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, an dem der ServiceNow AI Platform® Die Nachverfolgung des Status des erneuten Scans wurde beendet, nicht wenn der tatsächliche erneute Scan beendet wurde.

Alle VIS, die in „Geschlossen/behoben“ übergegangen sind oder übergehen werden, werden mit dem nächsten geplanten Import von importiert Rapid7 Integrationen.

Erneut Scannen Tenable.io Und Tenable.sc Angreifbare Elemente aus dem Vulnerability Response Arbeitsbereiche

Überprüfen Sie, ob Ihre angreifbaren Elemente zwischen den geplanten Scanzyklen behoben wurden. Initiieren Sie erneutes Scannen in Tenable.io Und Tenable.sc Produkte bei Bedarf aus dem Arbeitsbereich „IT-Korrektur“ in Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen

Um einen erneuten Scan für zu initiieren Tenable.io Und Tenable.sc Produkte aus der klassischen Umgebung von Vulnerability Response, Siehe Initiieren Sie einen erneuten Scan für Tenable.sc Integration Und Initiieren Sie einen erneuten Scan für Tenable.io Integration.

Um erneutes Scannen von durchzuführen ServiceNow AI Platform, Sie benötigen Ihre Tenable-Anmeldeinformationen. Weitere Informationen zum Einrichten von finden Sie Tenable.io Und Tenable.sc Scanner und Importieren Ihrer Anmeldeinformationen aus Tenable, siehe Konfigurieren Sie die Tenable-Schwachstellenintegration mit dem Setup-Assistenten.

- Sie können bei Bedarf erneute Scans für angreifbare Elemente und Korrekturaufgaben initiieren, die über verfügen Tenable.io Oder Tenable.sc Produkt als Quelle aus dem IT-Korrekturarbeitsbereich in Ihrem ServiceNow AI Platform.
- Bei einem Korrekturaufgabendatensatz kann sich der Datensatz in einem anderen Status als befinden **Geschlossen** , Und alle zugeordneten VIS müssen aus dem stammen Tenable.io Oder Tenable.sc Produkt.
- Um erneutes Scannen in zu initiieren Arbeitsbereich für IT-Korrekturen Aus Datensätzen für angreifbare Elemente und Korrekturaufgaben müssen Ihnen diese Datensätze zugewiesen werden.

Erforderliche Rollen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_vul.Remediation_owner für Arbeitsbereich für IT-Korrekturen
- sn_vul.Vulnerability_Analyst oder sn_vul.Vulnerability_admin aus dem Vulnerability Manager-Arbeitsbereich

Prozedur

1. Navigieren Sie zu einem angreifbaren Element oder einer Korrekturaufgabe, die Ihnen zugewiesen wurde, und öffnen Sie sie.

   Hinweis:
   Wenn Sie eine Korrekturmaßnahme auswählen, um einen erneuten Scan zu initiieren, werden alle diesem Datensatz zugeordneten VIS gescannt.

2. Klicken Sie oben rechts in einem Datensatz auf **Erneut Scannen** .
   Sie werden aufgefordert, die Instanz oder Instanzen für den erneuten Scan und die Scanner-Anmeldeinformationen auszuwählen, die Sie für den Zugriff auf den Scanner verwenden möchten. Die angezeigten Anmeldeinformationen sind die, die von importiert wurden Tenable.io Und Tenable.sc Integrationen Von Anmeldeinformationen Scannen.
3. Klicken Sie im Modal auf das Suchsymbol.

   Verwenden Sie im angezeigten Modal „Scan-Anmeldeinformationen auswählen“ die Filter in den Spaltenüberschriften, um den Namen, die Instanz und oder die Instanzen und die Anmeldeinformationstypen auszuwählen, die Sie verwenden möchten.

   Weitere Informationen finden Sie in der folgenden Tabelle.

4. Klicken Sie im aktualisierten Modal „erneut scannen“ auf **Erneutes Scannen anfordern** .
   Die Nachricht, Die Scan-Anforderung wird verarbeitet Wird angezeigt.
5. Klicken Sie auf **Status anzeigen** Link in der Nachricht, um den Fortschritt des Scans anzuzeigen.

   Der Scan-Datensatz (VSCAN#) wird angezeigt. Unter dem Datensatz-Header mit der Scan-Nummer werden in den zugehörigen Elementlisten die folgenden Informationen angezeigt:
   - In der Liste Details werden die Scan-Nummer des übergeordneten Scans, die Scannerquelle und der Status angezeigt. Zeigen Sie abgeschlossene und fehlgeschlagene Scans im Abschnitt „Scan-Zusammenfassung“ an.
   - In der Liste „Scans“ werden alle untergeordneten Scans und ihre status angezeigt. Wenn alle untergeordneten Scans abgeschlossen sind, wechselt der Status des übergeordneten Scans in „Abgeschlossen“.
   - Die Liste Quelle zeigt das für den Scan verwendete angreifbare Element, das zugehörige Konfigurationselement und die Schwachstelle, den Status des VI und seinen Korrekturstatus an.

   Ihr ServiceNow AI Platform® Die Instanz verfolgt den Status des erneuten Scans, bis er erfolgreich abgeschlossen ist, oder bis der festgelegte Nachverfolgungszeitraum abgelaufen ist, je nachdem, was zuerst geschieht.

   Durch die Zeitüberschreitung wird der Scan nicht beendet. Die Zeitüberschreitung bezieht sich auf den Zeitpunkt, an dem der ServiceNow AI Platform® Die Nachverfolgung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

des Status des erneuten Scans wurde beendet, nicht wenn der tatsächliche erneute Scan beendet wurde.

Alle VIS, die in „Geschlossen/behoben“ übergegangen sind oder übergehen werden, werden mit dem nächsten geplanten Import von importiert Tenable.io Oder Tenable.sc Integrationen.

Arbeitsbereich für IT-Korrekturen Referenzinformationen

Die folgenden Themen enthalten Links, Referenzinformationen sowie Felddaten in den Formularen und Datensätzen, die in gefunden werden Arbeitsbereich für IT-Korrekturen.

[store-future: BEGIN review]

Umleitung zu Arbeitsbereich für IT-Korrekturen Aus dem Menü alle

Wenn ein Administrator den festlegt *sn_vul_cmn_ws.navigate_to_workspace*Systemeigenschaft zu `Wahr` , Sie werden zu weitergeleitet Arbeitsbereich für IT-Korrekturen Bei Auswahl der vordefinierten Filter-Links in Vulnerability Response, Application Vulnerability Response, Container Vulnerability Response, Und Konfigurations-Compliance Module aus dem **Alle** Menü.

Umleitung zur Listenseite von Arbeitsbereich für IT-Korrekturen

Wenn Sie als Anwender mit der Rolle sn_vul.Remediation_owner die folgenden vordefinierten Filterlinks im Vulnerability Response-Modul auswählen, indem Sie zu navigieren **Alle** > **Vulnerability Response**, Diese Links werden auf der Listenseite von geöffnet Arbeitsbereich für IT-Korrekturen:

- Korrekturaufgaben: Mir zugewiesen und meinen Gruppen zugewiesen
- Angreifbare Elemente: Mir zugewiesen und meinen Gruppen zugewiesen
- Bibliotheken: NVD, CWE und Drittpartei
- Lösungen: Alle, höchste Ersatzlösung und mit angreifbaren Elementen
- Meine Genehmigungen

Als Anwender mit der Rolle sn_vul_Container.Remediation_owner, wenn Sie die folgenden vordefinierten Filterlinks im Container Vulnerability Response-Modul auswählen, indem Sie zu navigieren **Alle** > **Container Vulnerability Response**, Diese Links werden auf der Listenseite von geöffnet Arbeitsbereich für IT-Korrekturen:

- Container-Korrekturaufgaben: Aktiv, mir zugewiesen, meinen Gruppen zugewiesen und alle
- Angreifbare Container-Elemente: Mir zugewiesen und meinen Gruppen zugewiesen
- Meine Genehmigungen
- Bibliotheken: NVD, CWE und Drittpartei

Wenn Sie als Anwender mit der Rolle sn_vul.App_Security_Champion die folgenden vordefinierten Filterlinks im Modul „Application Vulnerability Response“ auswählen, indem Sie zu navigieren **Alle** > **Application Vulnerability Response**, Diese Links werden auf der Listenseite von geöffnet Arbeitsbereich für IT-Korrekturen:

- Korrekturaufgaben: Aktiv, mir zugewiesen, meinen Gruppen zugewiesen und alle
- Angreifbare Elemente: Mir zugewiesen und meinen Gruppen zugewiesen
- Meine Genehmigungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bibliotheken: NVD, CWE und Drittpartei
- Penetrationstest-Bewertungsanforderungen: Aktiv, alle mir zugewiesen und meinen Gruppen zugewiesen
- Penetrationstestergebnisse: Aktiv, Validierung ausstehend, mir zugewiesen, meiner Gruppe zugewiesen und alle

Als Anwender mit der Rolle „sn_vulc.Remediation_owner“, wenn Sie die folgenden vordefinierten Filterlinks im Modul „Konfigurations-Compliance“ auswählen, indem Sie zu navigieren **Alle** > **Konfigurations-Compliance**, Diese Links werden auf der Listenseite von geöffnet Arbeitsbereich für IT-Korrekturen:

- Korrekturaufgaben: Meine offenen Aufgaben, alle offenen Aufgaben, mehrere Zurückstellungen und alle Aufgaben
- Tests
- Testgruppen
- Unterstützungsdaten: Autorisierende Quellen und Technologien

[End]

Formularfelder für Change-Anforderungen erstellen

Die folgende Tabelle zeigt die Felder und ihre Beschreibung im Formular „Change-Anforderung erstellen“.

Feld	Beschreibung
Änderungstyp	Normal: Standard ist „Normal“. Standard: Zwei zusätzliche Felder werden angezeigt: Standard-Change-Kategorie: Wählen Sie eine Kategorie aus der Liste aus Standard-Change-Vorlage: Wählen Sie eine Vorlage aus der Auswahlliste aus, die für diese Change-Anforderung verwendet werden soll Notfall: Kritische Priorität
CIs zu Change-Anforderung hinzufügen	Standard ist aktiviert. Wenn diese Option aktiviert ist, fügt die Change-Anforderung alle Konfigurationselemente (Configuration Items, CI) hinzu, die zu aktiven angreifbaren Elementen in dieser Korrekturmaßnahme gehören.
Priorität	„Hoch“ ist der Standard. Wählen Sie eine Priorität aus der Liste aus.
Zuweisungsgruppe	Die Zuweisungsgruppe wird standardmäßig aus dem Überwachungsthema übernommen. Klicken Sie auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	das Suchsymbol, und wählen Sie im Modal eine andere Zuweisungsgruppe aus.
Geplantes Enddatum	Klicken Sie auf das Kalendersymbol, um ein geplantes Enddatum auszuwählen.
Zugewiesen an	Der aktuelle Anwender ist standardmäßig der Korrekturaufgabe zugewiesen. Klicken Sie auf das Suchsymbol, und wählen Sie im Modal einen anderen Anwender aus.
Kurzbeschreibung	Die Kurzbeschreibung stammt aus der Korrekturaufgabe. Klicken Sie auf den Text, um ihn zu bearbeiten.
Beschreibung	Die Beschreibung stammt aus der Korrekturaufgabe. Klicken Sie auf den Text, um ihn zu bearbeiten.
Begründung	Die Begründung aus der Korrekturaufgabe. Klicken Sie auf den Text, um ihn zu bearbeiten.
Implementierungsplan	Vorab mit Informationen zur bevorzugten Lösung ausgefüllt, falls verfügbar. Zeigen Sie die Lösung an, oder geben Sie einen Begründungsplan ein.

Zugehörige Informationen

Erstellen Sie eine Change-Anforderung in Arbeitsbereich für IT-Korrekturen

Formularfelder „Ausnahme anfordern“ für Richtlinienausnahmen

Die folgende Tabelle zeigt die Felder, die Sie im Formular „Ausnahme anfordern“ für Richtlinienausnahmen ausfüllen müssen.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Richtlinie	Schwachstellenmanagement-Richtlinie, für die Sie eine Ausnahme anfordern.
Kontrollziel	Kontrollziele, die der von Ihnen ausgewählten Richtlinie zugeordnet sind. Wenn keine Richtlinie ausgewählt ist, werden alle Kontrollziele aufgelistet.
Gültig ab	Datum, an dem die Ausnahme beginnt. Der Standardwert ist das aktuelle Datum. Dieses Datum darf nicht in der Vergangenheit liegen.
Gültig bis	Datum, an dem die Richtlinienausnahme abläuft, und der Status des angreifbaren Elements oder der angreifbaren Gruppe von zurückgestellt in Offen ändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Ausnahme anfordern“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: Die Anzahl der Tage, für die die Richtlinienausnahme gültig ist, darf den Wert in nicht überschreiten **Maximale Ausnahmedauer (Tage)** Feld, das Sie für die Richtlinie festgelegt haben. Weitere Informationen finden Sie unter Erstellen Sie eine Richtlinie .
Grund	Grund für die Anforderung einer Ausnahme.
Begründung	Details im Zusammenhang mit dem Grund, aus dem diese Ausnahme angefordert wird. Dieses Feld muss vom Korrekturbesitzer ausgefüllt werden.

Zugehörige Informationen

Fordern Sie eine Ausnahme mit an GRC: Richtlinien- und Compliance-Management In Arbeitsbereich für IT-Korrekturen

Formular „Ausnahme anfordern“ Zur Risikominderung

Die folgende Tabelle zeigt die Felder, die Sie im Formular „Ausnahme anfordern“ für Risikoreduzierungsanforderungen ausfüllen müssen.

Formular „Ausnahme anfordern“

Feld	Beschreibung
Grund	Grund für Ihre Ausnahmeanforderung. Wählen Sie Aus *Ausgleichende Kontrolle vorhanden* Für Anforderung zur Risikominderung. Informationen zum Hinzufügen neuer Ursachenauswahlen finden Sie unter Definieren Sie die Zuordnung des Richtliniengrunds.
Zurückstellungsanforderung	Verschieben Sie den Datensatz. Dieses Feld ist standardmäßig ausgewählt. **Hinweis:** Dieses Feld wird nur angezeigt, wenn *Ausgleichende Kontrolle vorhanden* Option ist in ausgewählt **Grund** Feld.
Risikominderungsanforderung	Ermöglicht Ihnen, die Reduzierung der Risikopunktzahl anzufordern. **Hinweis:** Dieses Kontrollkästchen wird nur angezeigt, wenn *Ausgleichende Kontrolle vorhanden* Option ist in ausgewählt **Grund** Feld.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Ausnahme anfordern“ (Fortsetzung)

Feld	Beschreibung
Aktuelle Risikobewertung	Aktueller Schweregrad des Risikos. **Hinweis:** Dieses Feld wird nur angezeigt, wenn **Anforderung zur Risikominderung** Das Kontrollkästchen ist aktiviert.
Gewünschte Risikobewertung	Neue Risikobewertung, die Sie dem Datensatz zuweisen möchten. Die höchste Risikopunktzahl in diesem Risikobewertungsbereich wird auf den Datensatz angewendet, wenn Ihre Anforderung genehmigt wird. **Hinweis:** Dieses Feld wird nur angezeigt, wenn **Anforderung zur Risikominderung** Das Kontrollkästchen ist aktiviert.
Wählen Sie Ausgleichssteuerungen Aus	Grund für Ihre Anforderung zur Reduzierung der Risikobewertung.
Bis	Datum, an dem die Zurückstellungs- oder Risikoreduzierungsanforderung abläuft. Wenn die Ausnahmeanforderung abläuft: • Der Datensatz wird in den Status Offen zurückgesetzt. • Die Ausgleichssteuerungen laufen ab. • Die berechnete Punktzahl wird anstelle einer reduzierten Punktzahl verwendet.
Hinweise zur Begründung	Details, die sich auf den Grund beziehen, warum diese Anforderung gestellt wird.

Zugehörige Informationen

Fordern Sie eine Risikominderung für ein angreifbares Element oder eine Korrekturaufgabe an

Arbeitsbereich für Schwachstellenbewertung kennenlernen

Der Vulnerability Assessment-Arbeitsbereich ist für den Vulnerability Event Manager konzipiert, um Risikobewertungen durchzuführen und kritische Schwachstellenereignisse proaktiv zu verwalten, insbesondere während kritischer Schwachstellenereignisse wie einem Zero-Day-Ereignis.

Nachdem eine kritische Schwachstelle identifiziert wurde, können Schwachstellen-Ereignismanager die potenziellen Auswirkungen und das mit der Schwachstelle verbundene Risiko bewerten. Die Analysten können die betroffenen Systeme, Anwendungen oder Netzwerkkomponenten analysieren, um den Schweregrad und mögliche Angriffsvektoren innerhalb der Organisation zu verstehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Arbeitsbereich für Schwachstellenbewertung enthält:

Seite „Risikobewertung“

Bietet detaillierten Einblick in die Assets, die Schwachstellen und angreifbarer Software ausgesetzt sind. Die Funktionalität „Risikobewertung“ bietet:

- Einblick in betroffene Assets für Schwachstellen und betroffene Software
- Fähigkeit, eigenständige Bewertungen für ein einzelnes CVE oder angreifbare Software durchzuführen
- Transparenz für betroffene Assets für CISA-CVEs mit bekannten ausgenutzten Schwachstellen
- Sichtbarkeit des Risikos durch zusätzliche Discovery-Modelle und -Assets.
- Möglichkeit, angreifbare Elemente zu erstellen

Seite „Schwachstellenbewertung“

Seite „Schwachstellenbewertung“, auf der Sie Schwachstellenkrisen-Ereignisse von der Bewertung bis zur Lösung mithilfe des Schwachstellenkrisen-Management-Workflows verarbeiten können. Mit dem Workflow können Sie relevante Schwachstellenereignisse nachverfolgen, Risiken analysieren, die mit ihnen verbunden sind, eine Risikobewertung für mehrere Bestände durchführen (z. B. Softwareinstallationsbestand) und sie als Krise für eine erhöhte Antwortinteraktion deklarieren. Sie können dann den Schwachstellenbewertungsdatensatz einem schwerwiegenden Security Incident zuordnen und dem Security Incident Response-Team ermöglichen, auf die Krise zu reagieren.

- Erstellen und ändern Sie Schwachstellenbewertungen für kritische Schwachstellenereignisse
- Zeichnen Sie Schlüsselattribute der Schwachstelle auf, um das Risiko zu berechnen
- Führen Sie eine Schwachstellenbewertung durch, um das Gefahrenniveau und die Priorität zu bestimmen
- Deklarieren Sie die Schwachstellenbewertung als kritisches Ereignis
- Ordnen Sie die Schwachstellenbewertung einem schwerwiegenden Security Incident zu, indem Sie die Schwachstellenbewertung mit einem schwerwiegenden Security Incident verknüpfen, vorschlagen oder heraufstufen.

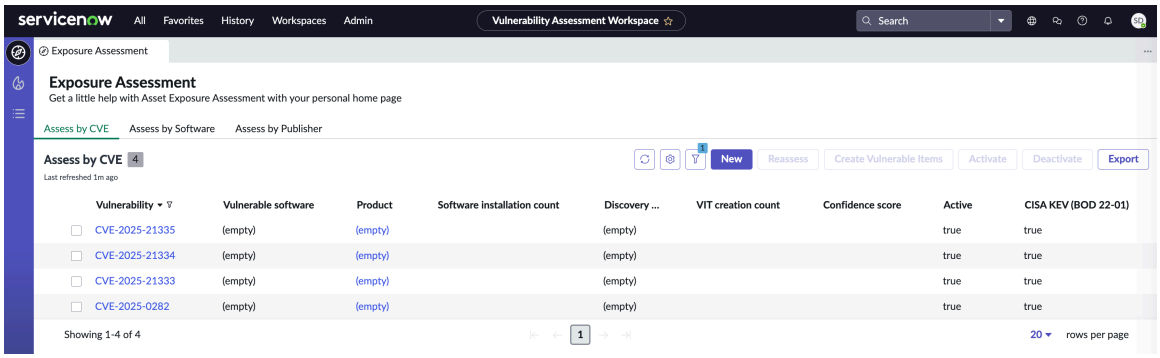
Listen-Seite

Die Listenseite besteht aus einer Bibliothek, die Folgendes enthält:

- CVEs
- TPEs
- CWEs

Die folgende Abbildung zeigt die Homepage des Arbeitsbereichs für Schwachstellenbewertung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erkunden Sie die Risikobewertung

Die Risikobewertung verwendet das CPE-Framework (Common Platform Enumeration), das Teil des CVEs-Systems (Common Vulnerabilities and Exposures) ist, um das Schwachstellenrisiko Ihrer Assets für Schwachstellensoftware zu bewerten. Diese Bewertung wird mit einem Software-Discovery-Modell durchgeführt.

Durch die Verwendung eines übereinstimmenden Algorithmus werden die relevanten CPEs dem Software-Discovery-Modell zugeordnet und zugeordnet, wodurch potenzielle Risiken identifiziert werden können.

Sie können die Risikobewertung durch CVE oder Software verwenden, um das Risiko potenzieller Schwachstellen für die folgenden Szenarien zu identifizieren:

- Schwachstellen, die von herkömmlichen Scannern möglicherweise nicht identifiziert werden
- Zero-Day-Schwachstellen vor dem Scanner liefern die Signatur für die Schwachstellenerkennung

Die Risikobewertung bietet eine Frühwarnung, um diese Schwachstellen zu beheben und die Reife des Schwachstellenmanagementprogramms zu verbessern.

Voraussetzungen für die Risikobewertung

Verfügbare Versionen

Anwendung	Version
Plugin „Schwachstellen-Krisenmanagement“	1.0
Vulnerability Response	20,0
Vulnerability Response Mit NVD	1.3
Vulnerability Response integration with CISA	1.2
Vulnerability Response-Integration mit NVD **Hinweis:** Weitere Informationen finden Sie unter Verstehen der NVD-Integrationen.	1.3
Software Asset Management	Software Asset Management Foundation-Plugin Oder Software Asset Management Professional Plugin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfälle

Beispiele dafür, wie die Organisation von Schwachstellenanalysten den Arbeitsbereich „Bewertung des Schwachstellenrisikos“ verwenden würde, finden Sie in diesen Anwendungsfällen.

Bewertungstyp	Verwenden
Nach CVE bewerten	Bewerten Sie Schwachstellen nach CVE, um ein vollständiges Verständnis der Auswirkungen und Risiken der betroffenen Systeme mit zu erhalten Software Asset Management(SAM) und Discovery Daten. Führen Sie Korrekturaktionen durch, indem Sie manuelle Vits erstellen und sie den Korrekturbesitzern zuweisen. Die Bewertung durch CVEs ist von Vorteil, da Scanner möglicherweise nicht alle betroffenen Systeme erkennen Discovery Identifiziert normalerweise den Großteil der Software auf der Angriffsoberfläche.
Nach Software bewerten	Bewerten Sie die Auswirkungen von Software, wenn CVE nicht verfügbar ist, um die Anzahl der CIs zu identifizieren, in denen die Software installiert ist. Durch die Bewertung nach Software können Sie proaktiv auf Zero-Day-Schwachstellen oder kritische Schwachstellen reagieren, indem Sie eine manuelle VIT erstellen und sie dem Korrekturbesitzer zuweisen, bevor sie offiziell veröffentlicht werden oder bevor Scanner sie identifizieren.
Nach Herausgeber bewerten	Bewerten Sie Schwachstellen durch einen Softwareanbieter, um die Auswirkungen und das Risiko betroffener Systeme für die vom Lieferanten innerhalb eines Zeitraums veröffentlichten CVEs zu verstehen. Die Bewertung durch den Herausgeber hilft Ihnen, das Lieferantenrisiko und kritische Schwachstellen zu bewerten und ermöglicht so eine proaktive Korrektur.

Kompatibilitäts- und Systemanforderungen

Die Vulnerability Response Anwendung ist auf verfügbar ServiceNow Store. Die ITSM Software Asset Management Anwendung (com.snc.Asset_Management) ist für das Modul „Risikobewertung“ erforderlich. Diese Anwendung verwaltet alle Ihre Assets und Softwarelizenzen und die SAM Foundation Version dieser Anwendung ist Teil von Vulnerability Response Anwendung, die Sie aus herunterladen ServiceNow Store.

Wichtig:
Die Anwendung „Risikobewertung“ funktioniert mit den folgenden Plugins:

- Software Asset Management Foundation-Plugin (com.snc.sams)
- Software Asset Management Professional (Com.snc.PA.samp)
- Software Asset Management-Plugin (Com.snc.Software_Asset_Management)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zum Überprüfen von SAM Foundation Die Anwendung ist auf Ihrer Instanz installiert. Navigieren Sie zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** Und suchen Sie nach com.snc.Asset_Management. Wenn die Anwendung nicht installiert ist, wählen Sie aus **Installieren** . Als Schwachstelle Die Anwendung „Risikobewertung“ erfordert Zugriff auf die Asset-Daten in Ihrem ServiceNow AI Platform® Instanz müssen die Asset-Management-Anwendungen über Daten verfügen, auf die verwiesen werden soll. Die Tabelle „Software-Discovery-Modelle“ (cmdb_sam_SW_Discovery_model) und die Softwareinstallationen (cmdb_sam_SW_install) erfordern Daten.

Übereinstimmende Algorithmusfelder für Software-Discovery-Modelle

Die Software Asset Management Professional Mit der Anwendung können Sie ein Software-Discovery-Modell bearbeiten, um erkannte Software, die nicht vollständig normalisiert wurde (teilweise normalisiert, Herausgeber normalisiert oder Übereinstimmung nicht gefunden), im Formular „Software-Discovery-Modelle“ manuell zu normalisieren, damit sie abgeglichen werden kann. Ab Version 20,0 von Vulnerability Response Unterstützt ein normalisiertes Discovery-Modell, das aus stammt Software Asset Management Professional. Die folgenden Felder werden für den Übereinstimmungsalgorithmus für Software-Discovery-Modelle verwendet.

CPE (Softwaremodell)	SAM-Grundlagen	SAM Professional
Lieferant	Primärer Schlüssel	Primärer Schlüssel
Produkt	Anzeigename	Anzeigename
Version	Erkannter Herausgeber	Erkannter Herausgeber
Edition	Erkanntes Produkt	Erkanntes Produkt
	Erkannte Version	Erkannte Version
		Normalisierter Herausgeber
		Normalisiertes Produkt
		Normalisierte Version

Hinweis:
Die SAM Professional-Anwendung ist nicht Teil des Core Vulnerability Response Produkt aus dem ServiceNow Store Und erfordert ein separates Abonnement.

Systemeigenschaft

Legen Sie die Systemeigenschaft fest, um die von CISA ausgenutzten Schwachstellen automatisch für die Risikobewertung zu verarbeiten *sn_vul_analyst.enable_exposure_for_cisa*Bis *true*. Der Standardwert ist *false*.

Geplante Aufgaben

Im Folgenden finden Sie die geplanten Aufgaben.

Name der geplanten Aufgabe	Beschreibung
Überprüfen Sie das potenzielle Schwachstellenrisiko	Verarbeitet die Delta-CVEs, Software und Installationen, um das Risiko zu ermitteln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name der geplanten Aufgabe	Beschreibung
	Hinweis: Diese geplante Aufgabe wird alle 12 Stunden ausgeführt. Sie wird länger ausgeführt als die anderen geplanten Aufgaben.
Fügen Sie das ausgenutzte CISA-CVE in die Risikokonfiguration ein	Bei Bedarf. Fügt die CISA-CVEs in die Tabelle „Risikokonfigurationstabelle“ ein, um das Risiko zu berechnen.
Risikobewertung für konfigurierte CVEs ausführen	Bei Bedarf. Berechnet das Risiko für alle CVE-Datensätze in der Tabelle „Risikokonfiguration“.
Führen Sie das Softwarerisiko aus	Bei Bedarf. Berechnet das Risiko für alle Softwaredatensätze in der Tabelle „Risikokonfiguration“.

Wichtige Begriffe

- **Konfidenzpunktzahl:** Eine Konfidenzpunktzahl ist eine Messung der Zuverlässigkeit bei der Bereitstellung einer Empfehlung für ein Feld. Je höher die Punktzahl, desto zuverlässiger ist die Empfehlung. Beispielberechnungen finden Sie unter Beispiel zur Berechnung der Konfidenzpunktzahl.
- **Anzahl der Softwareinstallationen:** Anzahl der von der Schwachstelle betroffenen Software-Assets.
- **Softwaremodell:** Softwaremodell, das dem Produkt zugeordnet ist. Führen Sie einen Drilldown zum Softwaremodell durch, um das Softwaremodellergebnis anzuzeigen. Weitere Informationen finden Sie unter Software Asset Management Foundation plugin discovery models and software installations .

Die **Anzahl der Softwareinstallationen** Das Feld gibt die Gesamtzahl der Softwareinstallationen unabhängig von ihrem aktiven oder inaktiven Status im Discovery-Modell an. Beginnend mit v22.0 von Vulnerability Response, Eine neue Systemeigenschaft, *sn_vul.filter_inactive_sw_installs*, Wurde eingeführt, um zu bestimmen, ob inaktive Softwareinstallationen für die Risikobewertung herausgefiltert werden sollen [store-future: BEGIN review]Oder Schwachstellen-Krisenmanagement (VCM) [End]. Standardmäßig ist die Eigenschaft im Basissystem aktiviert. Wenn der Filter aktiviert ist, werden nur aktive Installationen angezeigt.

Die **Discovery-Modell** Das Feld zeigt insbesondere die Anzahl der aktiven Softwareinstallationen an, da die inaktiven basierend auf dem standardmäßigen Filter „Active=true“ in der Tabelle „Software Discovery-Modell“ herausgefiltert werden. Die Anzahl in diesem Feld muss mit der gefilterten Anzahl übereinstimmen, die in angezeigt wird **Anzahl der Softwareinstallationen** Feld. Die Anzahl in **Softwareinstallation** Das Feld bleibt auch dann bestehen, wenn Sie die Systemeigenschaft aktualisieren. Um die aktualisierte Anzahl zu erhalten, müssen Sie die geplanten Aufgaben ausführen *Run exposure assessment for configured CVEs*Und *Run software exposure that updates the count*.

Risikobewertung nach CVE

Die Risikobewertung verwendet Common Vulnerabilities and Exposures (CVEs), um das Risiko Ihrer Assets mithilfe des Software-Discovery-Modells zu bewerten. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Risikobewertung von CVE verwenden, um das Risiko potenzieller Schwachstellen zu identifizieren.

Informationen zur Bewertung des Risikos nach CVE finden Sie unter:

- Fügen Sie CVEs hinzu, um das Risiko zu bewerten
- Erstellen Sie VIS für CVEs für die Risikobewertung
- Aktivieren oder deaktivieren Sie CVEs für die Risikobewertung
- Exportieren Sie betroffene CIs für die Risikobewertung
- Beispiel zur Berechnung der Konfidenzpunktzahl

Fügen Sie CVEs hinzu, um das Risiko zu bewerten

Fügen Sie der Risikokonfigurationsliste von CVEs in der Gefahrenbewertung Common Vulnerabilities and Exposures (CVEs) hinzu, um die Auswirkungen einer neuen Schwachstelle oder Zero-Day-Schwachstelle zu bewerten.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**an.
2. Wählen Sie **Hinzufügen**.
3. Wählen Sie im Dialogfeld CVE hinzufügen die CVEs aus, die Sie der Liste hinzufügen möchten, und wählen Sie aus **Hinzufügen** Option.
   CVEs, die sich bereits in der Liste befinden, werden nicht erneut hinzugefügt. Der Rest wird der Liste der CVEs hinzugefügt.

   Hinweis:
   Wählen Sie das Filtersymbol aus, um zu navigieren **Erweiterte Ansicht** Und geben Sie die CVEs an, die Sie anzeigen möchten.

4. So bewerten Sie die Auswirkungen der CVEs, die sich bereits in der Liste befinden:

   a. Aktivieren Sie das Kontrollkästchen der CVEs, die Sie neu bewerten möchten.

   b. Wählen Sie aus **Neu Bewerten** Schaltfläche.
   Die aktualisierten Details werden in den entsprechenden Spalten angezeigt.

Erstellen Sie VIS für CVEs für die Risikobewertung

Erstellen Sie angreifbare Elemente (VIS) auf der Seite „Risikobewertung“. Manager von Schwachstellenereignissen analysieren dann diese Liste von VIS und empfehlen Lösungen und Patches, mit denen das IT-Team diese Schwachstellen beheben kann.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Warum und wann dieser Vorgang ausgeführt wird
Nachdem das Risiko bewertet wurde, wird die Liste für die potenzielle Bewertung im Risikobewertungsdatensatz mit der Anzahl der Konfigurationselemente (Configuration Items, CIs) angezeigt. Sie können die Datensätze auswählen und in der Listenaktion

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auswählen **Erstellen Sie angreifbare Elemente** Dient zum Erstellen angreifbarer Elemente (VIS) für die CIs, in denen die angreifbare Software vorhanden ist, und für Common Vulnerabilities and Exposures (CVEs). VIS werden im Hintergrund erstellt. Dieser Prozess kann einige Zeit dauern. Nachdem die Elemente erstellt wurden, können Sie zur VI-Tabelle navigieren, um die erstellten Datensätze anzuzeigen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**an.
2. Wählen Sie die erforderlichen CVEs aus, und wählen Sie aus **Erstellen Sie Angreifbare Elemente** Option.
3. Wählen Sie im Dialogfeld Angreifbare Elemente erstellen die aus **Erstellen Sie angreifbare Elemente** Option.
4. Wählen Sie aus **Status anzeigen** Link zum Anzeigen des Status des Hintergrundauftrags, der zum Erstellen der VIS verwendet wird.

Aktivieren oder deaktivieren Sie CVEs für die Risikobewertung

Für die Delta-Verarbeitung eines CVE können Sie es aktivieren und somit der aktiven Liste der CVEs hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Hinweis:
Ab Version 4.0.1 der Bewertung des Schwachstellenrisikos wird der Risikobewertungsdatensatz für dieses CVE automatisch als inaktiv markiert, wenn ein allgemeiner Schwachstelleneintrag (Common Vulnerability Entry, CVE) in den letzten 30 Tagen nicht aktualisiert wurde oder angreifbare Elemente (Vits) erstellt wurden. Sie können diese Datensätze jedoch manuell aktivieren oder deaktivieren. Zusätzlich die geplante Aufgabe `Check potential vulnerability exposure`Wird kontinuierlich ausgeführt, um nach solchen CVEs zu suchen, um sie als inaktiv zu kennzeichnen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**an.
2. Wählen Sie die erforderlichen aktiven CVEs aus, und wählen Sie aus **Deaktivieren** Option.
   Die CVEs sind deaktiviert.

   Hinweis:
   Um Software zu aktivieren, führen Sie denselben Prozess aus, und wählen Sie aus **Aktivieren** Option.

3. Aktualisieren Sie die Seite, um den aktualisierten Status (falsch) in der Spalte aktiv anzuzeigen.

Exportieren Sie betroffene CIs für die Risikobewertung

Sie können die Liste der betroffenen Assets für ein neues CVE nachverfolgen, indem Sie die Konfigurationselemente (Configuration Items, CIs), die sich auf einen Risikobewertungsdatensatz beziehen, in ein Excel-Blatt exportieren. Dieses Blatt kann verwendet werden, um die Asset-Details und Besitzer freizugeben, um Incidents mit den bekannten betroffenen Assets für die Zero-Day-Schwachstellen zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach CVE bewerten**an.
2. Wählen Sie das Discovery-Modell für den Datensatz aus, dessen CIs Sie exportieren möchten. Die Registerkarte Softwareinstallationen enthält die aktiven CIs im Zusammenhang mit dem Softwaredatensatz. Diese CIs werden in gespeichert **Installiert auf** Spalte.
3. Wählen Sie aus **Exportieren** Option.
4. Wählen Sie im Dialogfeld „Exportieren“ den Dateityp und den Bereitstellungstyp aus, um die zugehörigen CIs zu exportieren.
5. Wählen Sie aus **Exportieren** Option.

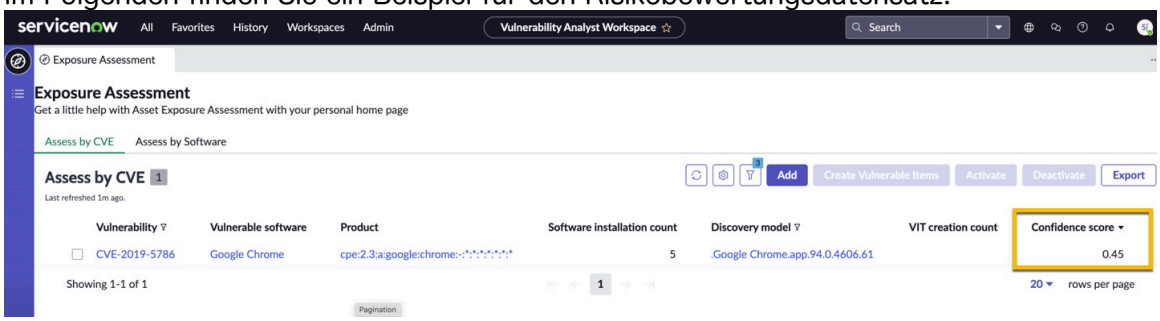
Beispiel zur Berechnung der Konfidenzpunktzahl

Beispiel für die Berechnung der Konfidenz für eine Zero-Day-Schwachstelle basierend auf ihren CVE-Informationen (Common Vulnerabilities and Exposures).

Im Folgenden finden Sie ein Beispiel für die Berechnung der Konfidenzpunktzahl anhand der CPE-Informationen (Common Platform Enumeration) von **CVE-2019-5786** .

Hinweis:
Um die CPEs anzuzeigen, können Sie die Spalte Schwachstelle nach Schwachstelle gruppieren. Details zum Anzeigen der Details zu angreifbarer Software finden Sie unter Zeigen Sie Details zu angreifbarer Software an.

Im Folgenden finden Sie ein Beispiel für den Risikobewertungsdatensatz:



Im Folgenden finden Sie ein Beispiel für ein Discovery-Modell:

So berechnen Sie die Konfidenzpunktzahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Konfidenzpunktzahlbereich liegt zwischen 0 und 1. Basierend auf den CPE-Informationen wird die Konfidenzpunktzahl mit der folgenden Formel berechnet:

```
((BASE SCORE) + (publisher score) +(product score) + (version score) + (edition score) +
 (display name score)) / 100
```

=

```
((25) + (10) + (10)) / 100
```

=

```
45 / 100
```

=

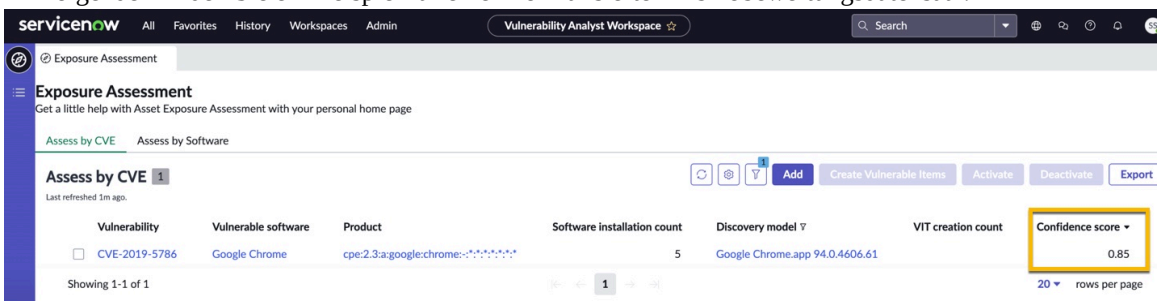
```
.45
```

Hinweis:
Informationen zu den Werten, die zur Berechnung der Konfidenzpunktzahl verwendet werden, finden Sie unter Referenztabellen der Konfidenzpunktzahl für die Risikobewertung.

Berechnung der Konfidenzpunktzahl, wenn das Softwaremodell mit dem normalisierten Discovery-Modell abgeglichen wird

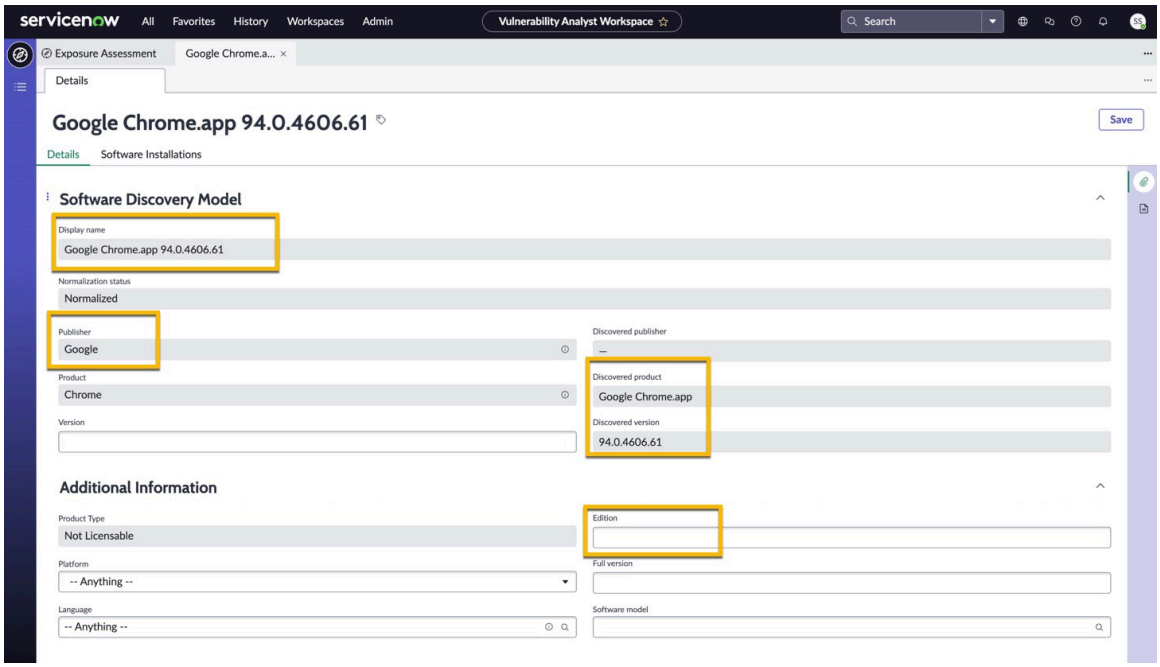
Wenn Sie das normalisierte Discovery-Modell verwenden, bieten die zusätzlichen Informationen, die für das Software-Discovery-Modell verfügbar sind, eine verbesserte Konfidenzpunktzahl. Im Folgenden finden Sie die Beispielberechnung:

Im Folgenden finden Sie ein Beispiel für einen normalisierten Risikobewertungsdatensatz.



Im Folgenden finden Sie ein Beispiel für ein normalisiertes Discovery-Modell.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.




```
((BASE SCORE) + (publisher score) + (product score) + (version score) + (edition score) + (display name score)) / 100
```

=

```
((25) + (20) + (15) + (15) + (0) + (10)) / 100
```

=

```
85 / 100
```

=

```
.85
```

Hinweis:
Informationen zu den Werten, die zur Berechnung der Konfidenzpunktzahl verwendet werden, finden Sie unter Referenztabellen der Konfidenzpunktzahl für die Risikobewertung.

Zeigen Sie Details zu angreifbarer Software an

Zeigen Sie die Details der angreifbaren Software an, in diesem Fall Google Chrome. Es wird mit dem Discovery-Modell und der Common Platform Enumeration (CPE) abgeglichen. Diese CPE-Version wirkt sich auf alle Google Chrome-Versionen aus.

Vorbereitungen

Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Prozedur

1. Navigieren Sie zu **Alle** Und geben Sie ein *sn_vul_software.LIST*.
2. Suchen Sie in der Liste der angreifbaren Software nach **cpe:2,3:a:google:Chrome:-:*:*:*:*:*:*:*:*** Um die Informationen anzuzeigen.

Referenztabellen der Konfidenzpunktzahl für die Risikobewertung

Referenzwerte, die zur Berechnung der Konfidenzpunktzahl verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenztabellen

Referenztabelle zur Berechnung der Konfidenzpunktzahl

Segment der angreifbaren Software	Discovery-Modellsegment	Punktzahl	Discovery-Modell – Segment mit genauer Übereinstimmung	Punktzahl für genaue Übereinstimmung
Herausgeber	Anzeigename	15	Herausgeber	5
Modell	Anzeigename	15	Modell	5
Version	Anzeigename	10	Version	5
Edition	Anzeigename	3	Normalisierte Edition	2
Anzeigename	Anzeigename	10	Anzeigename	5

Zusammenfassungstabelle der Konfidenzbewertung

Punktzahl	Wert
Summe aller Punktzahlen	75
Basispunktzahl **Hinweis:** Mindestpunktzahl für alle übereinstimmenden Discovery-Modelle.	25
Gesamtpunktzahl	100

Risikobewertung nach Software

Risikobewertung für Zero-Day-Schwachstellen, wenn Common Vulnerabilities and Exposures (CVEs) für das Asset oder das Konfigurationselement nicht verfügbar ist. Es verwendet die Softwareinformationen, um das Risiko mithilfe des Software-Discovery-Modells zu bewerten.

Informationen zur Bewertung des Risikos durch Software finden Sie unter:

- Fügen Sie Software für die Risikobewertung hinzu
- Erstellen Sie VIS für Software für die Risikobewertung
- Aktivieren oder deaktivieren Sie Software für die Risikobewertung
- Exportieren Sie betroffene CIs für Software im Arbeitsbereich „Schwachstellenbewertung“

Fügen Sie Software für die Risikobewertung hinzu

Fügen Sie dem Modul „Risikobewertung“ eine neue Software hinzu, um die Auswirkungen einer neuen Schwachstelle oder Zero-Day-Schwachstelle zu bewerten.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten** > **Hinzufügen**an.
2. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Herausgeber	Herausgeber der Software.
Produkt	Produktname der Software.
Version	Version des Softwareprodukts.
Edition	Edition der Software.

Hinweis:
Wenn Sie versuchen, das Risiko für Software hinzuzufügen, die in der Tabelle mit dem Status „falsch“ vorhanden ist, wird kein doppelter Datensatz erstellt. Der Status der vorhandenen Software wird auf „wahr“ aktualisiert.

3. Wählen Sie aus **Hinzufügen** Option.
4. So bewerten Sie die Auswirkungen der Software, die sich bereits in der Liste befindet:
   a. Aktivieren Sie das Kontrollkästchen der Software, die Sie neu bewerten möchten.
   b. Wählen Sie aus **Neu Bewerten** Schaltfläche.
   Die aktualisierten Details werden in den entsprechenden Spalten angezeigt.

Erstellen Sie VIS für Software für die Risikobewertung

Erstellen Sie angreifbare Elemente (VIS) auf der Seite „Risikobewertung“. Manager von Schwachstellenereignissen analysieren dann diese Liste von VIS und empfehlen Lösungen und Patches, mit denen das IT-Team diese Schwachstellen beheben kann.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten**an.
2. Wählen Sie die Datensätze aus, für die Sie VIS erstellen möchten.
3. Wählen Sie aus **Erstellen Sie Angreifbare Elemente** Option.
4. Wählen Sie im Dialogfeld Angreifbare Elemente erstellen aus:
   - Vorhandene Schwachstelle
   - Neue Schwachstelle
5. Wählen Sie aus **Erstellen Sie Angreifbare Elemente** Option.

Aktivieren oder deaktivieren Sie Software für die Risikobewertung

Um die weitere Delta-Verarbeitung von Software zu stoppen, können Sie sie deaktivieren und somit aus der aktiven Liste der Software entfernen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten**an.
2. Zum Deaktivieren wählen Sie die erforderliche aktive Software aus, und wählen Sie aus **Deaktivieren** Option.
   Die Software ist deaktiviert.

   Hinweis:
   Um Software zu aktivieren, führen Sie denselben Prozess aus, und wählen Sie aus **Aktivieren** Option.

3. Aktualisieren Sie die Seite, um den aktualisierten Status (falsch) in der Spalte aktiv anzuzeigen.

Exportieren Sie betroffene CIs für Software im Arbeitsbereich „Schwachstellenbewertung“

Sie können die Liste der betroffenen Assets für neue Software nachverfolgen, indem Sie die Konfigurationselemente (Configuration Items, CIs), die sich auf einen Risikobewertungsdatensatz beziehen, in ein Excel-Blatt exportieren. Dieses Blatt kann verwendet werden, um die Asset-Details und Besitzer freizugeben, um Incidents mit den bekannten betroffenen Assets für die Zero-Day-Schwachstellen zu erstellen.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Software bewerten**an.
2. Wählen Sie das Discovery-Modell für den Datensatz aus, dessen CIs Sie exportieren möchten.
   Die Registerkarte Softwareinstallationen enthält die aktiven CIs im Zusammenhang mit dem Softwaredatensatz. Diese CIs werden in gespeichert **Installiert auf** Spalte.
3. Wählen Sie aus **Exportieren** Option.
4. Wählen Sie im Dialogfeld „Exportieren“ die Option aus **Dateityp** Und **Liefertyp** Zum Exportieren der zugehörigen CIs.
5. Wählen Sie aus **Exportieren** Option.

Risikobewertung durch Herausgebersoftware

Bewerten Sie das Risiko für Zero-Day-Schwachstellen, wenn Common Vulnerabilities and Exposures (CVEs) für das Asset oder das Konfigurationselement nicht verfügbar ist. Es verwendet die Softwareinformationen, um das Risiko mithilfe des Software-Discovery-Modells zu bewerten.

Informationen zur Bewertung des Risikos durch Software finden Sie unter:

- Fügen Sie Software von einem Herausgeber für die Risikobewertung hinzu
- Erstellen Sie VIS für Software von einem Herausgeber für die Risikobewertung
- Aktivieren oder deaktivieren Sie Software durch einen Herausgeber für die Risikobewertung
- Exportieren Sie betroffene CIs für Software von einem Herausgeber im Arbeitsbereich „Schwachstellenbewertung“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie Software von einem Herausgeber für die Risikobewertung hinzu

Fügen Sie dem Modul „Risikobewertung“ Software eines Herausgebers hinzu, um die Auswirkungen einer neuen Schwachstelle oder Zero-Day-Schwachstelle zu bewerten.

Vorbereitungen

Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Herausgeber bewerten** > **„Neu“**an.
2. In Neue Bewertung Wählen Sie den Herausgeber aus, für den Sie die Bewertung durchführen möchten.
3. Wählen Sie im ein Datum aus **CVE veröffentlicht von** Feld.
   Wenn einer der Common Vulnerability Entries (CVEs), die der Software zugeordnet sind, nach dem ausgewählten Datum geändert wird, wird diese Software für die Risikobewertung berücksichtigt.
4. Wählen Sie den Schweregrad des CVE in aus **CVE-Schweregrad** Abschnitt.
5. Wählen Sie Aus **Bewertung starten** .
   Sobald der Auftrag abgeschlossen ist, werden die ausgewählten Datensätze erstellt.

Erstellen Sie VIS für Software von einem Herausgeber für die Risikobewertung

Erstellen Sie angreifbare Elemente (VIS) auf der Seite „Risikobewertung“, um die Liste der VIS zu analysieren und Lösungen und Patches zu empfehlen, die dem IT-Team helfen können, die Schwachstellen zu beheben.

Vorbereitungen

Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Herausgeber bewerten**an.
2. Wählen Sie die Datensätze aus, für die Sie VIS erstellen möchten.
3. Wählen Sie aus **Erstellen Sie Angreifbare Elemente** Option.
4. Wählen Sie im Dialogfeld Angreifbare Elemente erstellen aus:
   - Vorhandene Schwachstelle
   - Neue Schwachstelle
5. Wählen Sie aus **Erstellen Sie Angreifbare Elemente** Option.

Aktivieren oder deaktivieren Sie Software durch einen Herausgeber für die Risikobewertung

Aktivieren oder deaktivieren Sie Software durch einen Herausgeber, um die Delta-Verarbeitung der Software zu stoppen und sie aus der aktiven Liste der Software zu entfernen.

Vorbereitungen

Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Herausgeber bewerten**an.
2. Zum Deaktivieren wählen Sie die erforderliche aktive Software von einem Herausgeber aus, und wählen Sie aus **Deaktivieren** Option unter **Neu Bewerten** Schaltfläche.
   Der Herausgeber ist deaktiviert.

   Hinweis:
   Um die Software durch einen Herausgeber zu aktivieren, führen Sie denselben Prozess aus, und wählen Sie aus **Aktivieren** Option.

3. Aktualisieren Sie die Seite, um den aktualisierten Status (falsch) in der Spalte aktiv anzuzeigen.

Exportieren Sie betroffene CIs für Software von einem Herausgeber im Arbeitsbereich „Schwachstellenbewertung“

Sie können die Liste der betroffenen Assets für neue Software nachverfolgen, indem Sie die Konfigurationselemente (Configuration Items, CIs), die sich auf einen Risikobewertungsdatensatz beziehen, in ein Excel-Blatt exportieren. Dieses Blatt kann verwendet werden, um die Asset-Details und Besitzer freizugeben, um Incidents mit den bekannten betroffenen Assets für die Zero-Day-Schwachstellen zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertung des Gefahrenpotenzials** > **Nach Herausgeber bewerten**an.
2. Wählen Sie das Discovery-Modell für den Datensatz aus, dessen CIs Sie exportieren möchten.
   Die Registerkarte Softwareinstallationen enthält die aktiven CIs im Zusammenhang mit dem Softwaredatensatz. Diese CIs werden in gespeichert **Installiert auf** Spalte.
3. Wählen Sie aus **Exportieren** Option.
4. Wählen Sie im Dialogfeld „Exportieren“ die Option aus **Dateityp** Und **Liefertyp** Zum Exportieren der zugehörigen CIs.
5. Wählen Sie aus **Exportieren** Option.

Schwachstellenbewertung erkunden

Der Vulnerability Assessment-Arbeitsbereich ist für den Vulnerability Event Manager konzipiert, um ein Schwachstellenereignis zu erstellen und Schwachstellenbewertungen durchzuführen, insbesondere während der Zero-Day-Schwachstellenanalyse.

Sie können den Arbeitsbereich für die Schwachstellenbewertung verwenden, um kritische Schwachstellen zu verwalten, z. B.:

- Zero-Day-Schwachstellen mit Schweregrad „Kritisch“ oder „hoch“
- Neue bedrohungsinformationen für eine Schwachstelle identifiziert
- Schnelle Ausnutzung einer Schwachstelle mit dem Schweregrad „Kritisch“ oder „hoch“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsbereich für Schwachstellenbewertung und Schwachstellenkrisenmanagement

Identifizieren und erstellen Sie als Schwachstellen-Ereignismanager einen Schwachstellen-Ereignisdatensatz für Schwachstellen von Interesse. Sobald Sie das angreifbare Ereignis erstellt haben, können Sie eine Risikobewertung durchführen, die Risikoattribute manuell aktualisieren und die Risikopunktzahl automatisch berechnen. Mit dem Arbeitsbereich „Schwachstellenbewertung“ können Sie die folgenden Aktionen ausführen, um Schwachstellenkrisenereignis von Beginn bis zur Lösung zu verarbeiten.

- Erstellen Sie einen Schwachstellenbewertungsdatensatz
- Ändern Sie den Schwachstellenbewertungsdatensatz
- Führen Sie eine Schwachstellenbewertung durch
- Überprüfen Sie die Bewertungsdetails
- Weisen Sie dem Schwachstellenbewertungsdatensatz eine Priorität und ein Gefahrenpotenzial zu
- Fügen Sie dem Bewertungsdatensatz betroffene CIs hinzu
- Erstellen Sie angreifbare Elemente für das betroffene CI oder die betroffene Softwarekomponente
- Verknüpfen Sie den Schwachstellenbewertungsdatensatz mit einem schwerwiegenden Security Incident in Management schwerwiegender Sicherheits-Incidents

Voraussetzungen für die Schwachstellenbewertung

Verfügbare Versionen

Anwendung	Version
Plugin „Schwachstellen-Krisenmanagement“	1.0
Vulnerability Response	20,0
Vulnerability Response Mit NVD **Hinweis:** Weitere Informationen finden Sie unter Verstehen der NVD-Integrationen.	1.4.2
Vulnerability Response integration with CISA	1.2
Datenmodell für SBOM	1.1.2
Software Bill of Materials Zentral	2.0.2
Software Asset Management	Software Asset Management Foundation-Plugin Oder Software Asset Management Professional Plugin
Management schwerwiegender Sicherheits-Incidents	2.2.5

Geplante Aufgaben

Im Folgenden sind die geplanten Aufgaben aufgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name der geplanten Aufgabe	Beschreibung
Schwachstellenbewertung	Aktualisiert die Tabelle „Betroffene Konfigurationselemente“ und die Quelle des CI, wenn angreifbare Elemente (Vits oder AVITs) nach der Bewertung erstellt werden. **Hinweis:** Diese planmäßige Aufgabe wird täglich ausgeführt. Sie wird länger ausgeführt als die anderen geplanten Aufgaben.

Zugehörige Informationen

Schwachstellen-Krisenmanagement

Erstellen Sie einen Schwachstellenbewertungsdatensatz

Erstellen Sie Bewertungsdatensätze für Schwachstellen von Interesse. Nachdem Sie die Bewertung erstellt haben, können Sie die erste Risikobewertung initiieren, den Datensatz manuell aktualisieren und die Risikopunktzahl automatisch berechnen.

Vorbereitungen

Sie müssen Teil der Zuweisungsgruppe des Basissystems „Vulnerability Assessment Event Manager“ sein, um die mit der Schwachstellenbewertung verknüpften Aufgaben ausführen zu können.

Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager, sn_vul_Analyst.Emergency_response

Warum und wann dieser Vorgang ausgeführt wird

Sie können einen Schwachstellenbewertungsdatensatz für Schwachstellen von Interesse erstellen, indem Sie den Ereignisdatensatz entweder einem primären CVE oder einem betroffenen Produkt zuordnen.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**an.
2. Wählen Sie aus **Schwachstellenbewertung** Symbol.
3. Wählen Sie **Neu**.
4. Geben Sie einen entsprechenden Titel in ein **Titel** Feld.
5. **Wahlweise:** Wählen Sie ein primäres CVE aus, das dem neuen Bewertungsdatensatz zugeordnet werden soll **Primäres CVE** Feld.

   Hinweis:
   Alle vorläufigen Details im Bewertungsdatensatz werden basierend auf dem Produkt, das Sie auswählen oder erstellen, oder dem primären CVE, das Sie dem Datensatz zuordnen, ausgefüllt.

6. Wählen Sie **Absenden**.
   Der Schwachstellenbewertungsdatensatz mit dem von Ihnen eingegebenen Titel wird erstellt und auf einer neuen Registerkarte „Schwachstellenbewertung“ angezeigt. Standardmäßig wird der Schwachstellenbewertungsdatensatz in angezeigt **Details** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Standardmäßig werden die Details des primären zugeordneten/zugeordneten CVE angezeigt.

- Wenn während der Erstellung des Datensatzes des Schwachstellenbewertungsereignisses kein primäres CVE ausgewählt ist, wird ein Standarddatensatz erstellt.
- Wenn dem primären CVE CVE CVEs zugeordnet sind, werden die zugehörigen CVEs in ausgefüllt **Schwachstelleneinträge** Registerkarte. Sie können weitere zugeordnete CVEs aus hinzufügen **Schwachstelleneinträge** Registerkarte.

7. Navigieren Sie zu **Betroffene Produkte** Registerkarte.

a. Wählen Sie **Neu**.

b. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Herausgeber	Herausgeber der Software. Das ist ein Pflichtfeld.
Produkt	Produktname der Software. Das ist ein Pflichtfeld.
Version	Version des Softwareprodukts.
Edition	Edition der Software.

Hinweis:
Wenn Sie versuchen, eine Schwachstelle für Software hinzuzufügen, die in der Tabelle mit dem Status „falsch“ vorhanden ist, wird kein doppelter Datensatz erstellt. Der Status der vorhandenen Software wird auf „wahr“ aktualisiert.

c. Wählen Sie **OK**.

8. Wählen Sie **Speichern**.

Aktualisieren Sie den Datensatz für die automatische Entleerung der Schwachstellenbewertung

Aktualisieren Sie den Datensatz für die automatische Entleerung der Schwachstellenbewertung.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Warum und wann dieser Vorgang ausgeführt wird
Im Basissystem ist der Aufbewahrungszeitraum für Schwachstellenbewertungsdatensätze auf 6 Monate festgelegt. Wenn ein Schwachstellenbewertungsdatensatz den Status Geschlossen hat, werden die Schwachstellenbewertungsdatensätze nur bis zum definierten Aufbewahrungszeitraum gespeichert, und die zugehörigen Datensätze dieser Bewertung werden nach 6 Monaten aus allen zugehörigen Tabellen entfernt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Automatisch entleeren**an.
2. Öffnen Sie den Datensatz mit Tabelle, sn_vul_Analyst_Vulnerability_assessment .
3. Wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren der automatischen Entleerungsoption für den Schwachstellenbewertungsdatensatz.
4. Klicken Sie auf **Aktualisieren**.

Ändern Sie den Schwachstellenbewertungsdatensatz

Aktualisieren Sie den Schwachstellenbewertungsdatensatz nach der Erstellung. Basierend auf den Werten des Felds können Sie die Risikopunktzahl berechnen .

Vorbereitungen

Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Warum und wann dieser Vorgang ausgeführt wird

Nachdem das primäre CVE der Schwachstellenbewertung hinzugefügt wurde, wird der Datensatz in den Status „Bewertung ausstehend“ verschoben. Sie können weitere zugehörige CVEs in hinzufügen **Schwachstelleneinträge** Oder fügen Sie die von dieser Schwachstelle betroffenen Produkte aus der hinzu **Betroffene Produkte** Registerkarte. Sie können weitere Änderungen an vornehmen **Risikobewertung** Felder und **Risikopunktzahl** Für wird der Bewertungsdatensatz automatisch entsprechend aktualisiert.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereich der Schwachstellenbewertung** > **Schwachstellenbewertung**an.
2. Auf der **Details** Registerkarte aktualisieren Sie die Felder.

Feld	Beschreibung
Titel	Titel, der das Schwachstellenereignis beschreibt Datensatz.
Primäres CVE	Primäres CVE, das Sie dem Ereignisdatensatz zugeordnet haben.
Status	Aktueller Status des Ereignisdatensatzes.
Priorität	Priorität des Ereignisdatensatzes auf einer Skala von 1 bis 5.
Warnungsquelle	Quelle des potenziellen Schwachstellenereignisses.
Risikopunktzahl	Automatisch berechnete Risikopunktzahl. Standardmäßig nicht bearbeitbar.
Gefahrenniveau	Das Gefahrenniveau des Schwachstellenereignisses auf einer Skala von 1 bis 5.
Zuweisungsgruppe	Die Zuweisungsgruppe, der der Ereignisdatensatz zugewiesen ist.
Zugewiesen an	Der Anwender, dem der Ereignisdatensatz zugewiesen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Detaillierte Beschreibung des Ereignisdatensatzes.

3. Navigieren Sie zu **Schwachstelleneinträge** Registerkarte zum Hinzufügen zugeordneter oder zugehöriger CVEs.
   a. Wählen Sie **Neu**.
   b. Suchen Sie im nach dem Datensatz **Schwachstelleneintrag** Feld.
   c. Wählen Sie den Schwachstellendatensatz aus, den Sie dem Bewertungsdatensatz zuordnen möchten.
   d. **Wahlweise:** Wählen Sie Aus **Durchsuchen** Zum Durchsuchen und Anhängen einer Datei.
   e. Wählen Sie **Speichern**.
   Die von Ihnen ausgewählten Schwachstellendatensätze werden dem Bewertungsdatensatz hinzugefügt und in angezeigt **Schwachstelleneinträge** Registerkarte.
4. **Wahlweise:** Fügen Sie betroffene Produkte hinzu.
5. Fügen Sie dem Bewertungsdatensatz einen zugehörigen Link hinzu.
6. Ändern Sie **Risikoattribute** Für das primäre CVE, das dem Ereignisdatensatz der Schwachstellenbewertung zugeordnet ist.

Feld	Beschreibung
Speicherbeschädigung	Gibt an, ob dieser Ereignisdatensatz den Arbeitsspeicher beschädigen kann.
Ausführbarer Remotecode	Gibt an, ob die Remotecodeausführung möglich ist.
Lokale Berechtigungsausweitung	Gibt an, ob eine lokale Schwachstelle für die Berechtigungseskalation vorhanden ist.
Nicht autorisierter Zugriff	Gibt an, ob eine Schwachstelle für nicht autorisierten Zugriff vorhanden ist.
DDoS	Gibt an, ob das potenzielle Ereignis verteilte Denial of Service beinhalten könnte.
Angriffskomplexität	Gibt die Komplexität des Anhangs an. Optionen sind Niedrig, Mittel oder hoch.
Angriffsvektor	Gibt den potenziellen Pfad oder die potenzielle Methode des Angriffs an. Optionen sind – Netzwerk, angrenzendes Netzwerk, Lokal, physisch, keine.
Erforderliche Berechtigungen	Gibt die Ebene der Berechtigungen an, die ein Angreifer zum Ausnutzen der Schwachstelle benötigt. Optionen sind „keine“, „Niedrig“ oder „hoch“.
Anwenderinteraktion	Gibt an, ob eine Anwenderinteraktion erforderlich ist, um die Schwachstelle auszunutzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Auswirkung auf die Vertraulichkeit	Gibt das Maß für die potenziellen Auswirkungen auf die Vertraulichkeit der Schwachstelle an. Optionen sind „keine“, „Niedrig“ oder „hoch“
Umfangsänderung	Gibt an, ob der Umfang geändert wurde, wenn sich die Bewertung geändert hat.
Auswirkung auf die Verfügbarkeit	Gibt die potenziellen Auswirkungen auf die Verfügbarkeit einer erfolgreich ausgenutzten Schwachstelle bei Missbrauch an. Verfügbarkeit bezieht sich auf die Zugänglichkeit von Informationsressourcen. Optionen sind „keine“, „Niedrig“ oder „hoch“
Auswirkung auf die Integrität	Gibt die potenziellen Auswirkungen einer erfolgreich ausgenutzten Schwachstelle auf die Integrität an. Integrität bezieht sich auf die Vertrauenswürdigkeit und garantierte Richtigkeit von Informationen. Optionen sind „keine“, „Niedrig“ oder „hoch“
Korrekturstufe	Gibt den Status oder die Verfügbarkeit der Korrektur für die Schwachstelle an. Optionen sind „Offizielle Korrektur“, „temporäre Korrektur“, „Workaround“, „nicht verfügbar“, „nicht definiert“.
Reife des Exploit-Codes	Gibt die Wahrscheinlichkeit der Ausnutzung der Schwachstelle basierend auf dem vorhandenen Status der Exploit-Techniken und der Codeverfügbarkeit an. Optionen sind „nicht erprobt“, „Proof-of-Concept“, „funktional“, „hoch“ und „nicht definiert“.
Berichtskonfidenz	Gibt an, wie zuversichtlich Sie sind, dass die Schwachstelle vorhanden ist.

7. Geben Sie relevante Kommentare in ein **Verfassen** Feld.
   - Geben Sie Ihre Arbeitsnotizen in ein **Arbeitsnotizen (privat)** Feld.
   - Geben Sie Ihre Kommentare (für alle sichtbar) in ein **Kommentare** Feld.
8. **Speichern** Der Bewertungsdatensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basierend auf den Aktualisierungen, die Sie an vorgenommen haben **Risikoattribut** Felder für das primäre CVE oder das betroffene Produkt, das dem Bewertungsdatensatz zugeordnet ist, die **Risikopunktzahl** Feld wird automatisch aktualisiert.

Hinweis:
Um die Regeln oder Kriterien des Basissystem-Risikopunktzahlrechners zu ändern, navigieren Sie zu **Alle** > **Rechner für Schwachstellenbewertung** > **Risikorechner für Schwachstellenbewertung** > **Schwachstellenbewertung – Risikoregel**an. Sie können Kriterien hinzufügen und die Gewichtung auf Feldebene nach Bedarf an vorhandene Kriterien ändern.

Nächste Maßnahme
Führen Sie eine erste Bewertung des Ereignisdatensatzes durch.

Löschen Sie zugeordnete CVEs oder betroffene Produkte aus dem Schwachstellenbewertungsdatensatz

Löschen Sie einen Schwachstellen-Ereignisdatensatz, wenn er nicht mehr benötigt wird.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Warum und wann dieser Vorgang ausgeführt wird
Sie können CVEs oder betroffene Produkte löschen, die dem Schwachstellenbewertungsdatensatz zugeordnet sind. Sie können Schwachstelleneinträge/ zugehörige CVEs oder betroffene Produkte nur löschen, wenn sie sich in befinden **Neu** Oder **Bewertung ausstehend** status.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Schwachstellenbewertung**an.
2. Wählen Sie den Schwachstellenbewertungsdatensatz aus.
3. Wählen Sie aus **Schwachstelleneinträge** Registerkarte oder **Betroffene Produkte** Registerkarte.
4. Wählen Sie das zugehörige CVE oder den Datensatz des betroffenen Produkts aus.
5. Wählen Sie **Löschen**.

Hinweis:
Die **Löschen** Die Schaltfläche wird nur für einen Bewertungsdatensatz angezeigt, wenn er sich in befindet **Neu** Oder **Bewertung Ausstehend** status.

Fügen Sie dem Bewertungsdatensatz einen zugehörigen Link hinzu

Fügen Sie zusätzliche Links und Informationen im Zusammenhang mit dem Bewertungsdatensatz hinzu.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**an.
2. Wählen Sie den Bewertungsdatensatzeintrag aus.
3. Wählen Sie aus **Zugehörige Links** Registerkarte.
4. Geben Sie eine relevante Beschreibung in ein **Beschreibung** Feld.
5. Geben Sie die URL in ein **Link** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie **OK**.
   Der zugehörige Link wird hinzugefügt und auf der Registerkarte zugehörige Links aufgeführt.

Führen Sie eine Bewertung durch

Nachdem Sie den Schwachstellenbewertungsdatensatz erstellt und die Risikoattributfelder aktualisiert haben, führen Sie eine Bewertung des Ereignisdatensatzes aus.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Warum und wann dieser Vorgang ausgeführt wird
Führen Sie eine erste Bewertung durch, nachdem ein Ereignis für eine Schwachstelle von Interesse erstellt und festgestellt wurde, dass ein Risiko für Systeme und Daten darstellt. Der Zweck dieser Aktivität besteht darin, die Bedrohung weiter zu analysieren, indem die Risikobewertung mit einer detaillierten Risikobewertung aktualisiert wird.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Schwachstellenbewertung**an.
2. Wählen Sie den relevanten Datensatz aus der Liste der Ereignisdatensätze der Schwachstellenbewertung aus.
3. Wählen Sie Aus **Bewerten** Zum Ausführen der Schwachstellenbewertung.
   Die Vulnerability Response: Verarbeiten Sie das Schwachstellenbewertungsereignis Hintergrundauftrag wird initiiert, und eine relevante Benachrichtigung wird angezeigt.
4. Wählen Sie Aus **Status Anzeigen** In der Benachrichtigung, um den Status des laufenden Auftrags anzuzeigen.
5. Wählen Sie **Speichern**.

   Die **Bewertungen** Auf der Registerkarte werden Bewertungsdetails angezeigt. Wenn die Bewertung verarbeitet wird, werden die Vits oder AVITs, die den angreifbaren Einträgen oder CVEs zugeordnet sind, in angezeigt **Angreifbare Elemente** Oder **Angreifbare Anwendungselemente** Registerkarte.

Ergebnisse

- Angreifbare Elemente oder TPEs, die sich auf die zugeordneten CVEs beziehen, werden während der Bewertung abgerufen. Die CIs im Zusammenhang mit den angreifbaren Elementen werden auch identifiziert und in der Tabelle „Betroffene Konfigurationselemente“ angezeigt.
- Wenn die zugeordneten CIs in der Tabelle „Betroffene CI“ nicht vorhanden sind, werden die identifizierten CIs der Tabelle und der hinzugefügt **Hat angreifbares Element** Feldwert ist auf festgelegt **Wahr** , Und **Quelle** Der Wert des Felds ist auf Scanner festgelegt.
- Wenn das CI bereits in der Tabelle „Betroffene CI“ vorhanden ist, wird nur der verwendet **Hat angreifbares Element** Feldwert ist auf festgelegt **Wahr** Und **Quelle** Der Feldwert für das CI bleibt derselbe wie bei der Erstellung des Bewertungsdatensatzes.
- Wenn angreifbare Elemente nach der Bewertung erstellt werden Schwachstellenbewertung Die geplante Aufgabe wird ausgeführt, um die Tabelle „Betroffene CIs“ und die Quelle des CI zu aktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Weisen Sie dem Schwachstellenbewertungsdatensatz eine Priorität und ein Gefahrenpotenzial zu
- Fügen Sie dem Bewertungsdatensatz betroffene CIs hinzu
- Erstellen Sie angreifbare Elemente für das betroffene CI oder die betroffene Softwarekomponente
- Fügen Sie dem Bewertungsdatensatz einen zugehörigen Link hinzu

Zugehörige Informationen

Registerkarte „Bewertung“

Registerkarte „Übersicht“

Registerkarte „Bewertung“

Überprüfen Sie die Bewertungsergebnisse auf der Registerkarte „Bewertung“. Nachdem Sie eine Bewertung des Schwachstellenereignisses durchgeführt haben, wird der Datensatz mit den Daten von korreliert Software Bill of Materials Und Software Asset Management Und werden mit Visualisierungen angezeigt.

Auf der Registerkarte „Bewertung“ werden Daten (falls verfügbar) basierend auf dem Bewertungsdatensatz ausgefüllt, den Sie erstellen, und die Details werden mit Bewertungen aus korreliert Software Asset Management Und Software Bill of Materials Komponentendaten in der CMDB.

Funktionsweise der Bewertung

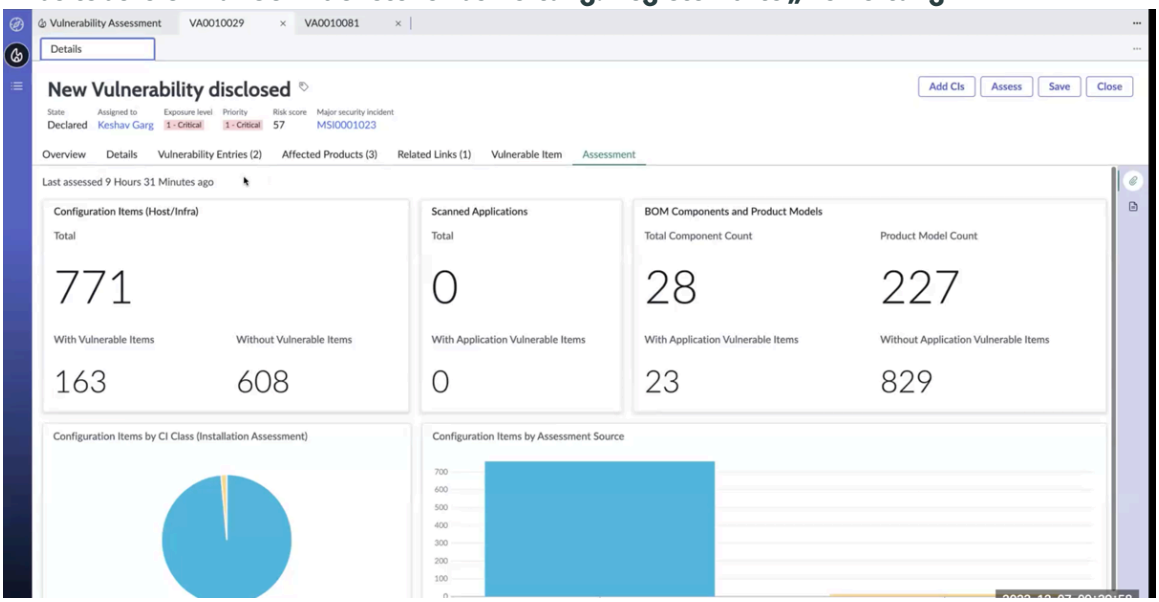
Bei Auswahl von **Bewerten** Schaltfläche, eine Bewertung für alle zugehörigen CVEs und betroffenen Produkte, die beide verwenden Software Asset Management Und SBOM Daten werden initiiert. Ein Hintergrundauftrag wird ausgelöst, und wenn die Bewertung verarbeitet wird, werden die Vits oder AVITs, die den angreifbaren Einträgen oder CVEs zugeordnet sind, in angezeigt **Angreifbare Elemente** Und **Angreifbare Anwendungselemente** Registerkarten.

- Alle angreifbaren Elemente oder TPEs im Zusammenhang mit dem CVE werden identifiziert.
- Die Konfigurationselemente (Configuration Items, CIs), die sich auf die angreifbaren Elemente beziehen, werden ebenfalls identifiziert und in der Tabelle „Betroffene Konfigurationselemente“ angezeigt.
- Wenn die CIs in der Tabelle „Betroffene CI“ nicht vorhanden sind, werden die identifizierten CIs der Tabelle und der hinzugefügt **Hat angreifbares Element** Kennzeichnung wird auf „wahr“ gesetzt, und die **Quelle** Der Wert des Felds ist auf Scanner festgelegt.
- Wenn das CI bereits in der Tabelle „Betroffene Konfigurationselemente“ vorhanden ist, nur der **Hat angreifbares Element** Die Kennzeichnung ist auf „wahr“ und festgelegt **Quelle** Bleibt unverändert ab dem Zeitpunkt, zu dem der Bewertungsdatensatz erstellt wurde.
- Wenn angreifbare Elemente nach der Bewertung erstellt werden Schwachstellenbewertung Die geplante Aufgabe wird ausgeführt, um die Tabelle „Betroffene CIs“ und die Quelle des CI zu aktualisieren.
- Im Bewertungsarbeitsbereich können Sie Zeitstempel anzeigen, um die letzte Bewertung der Ereignisse anzuzeigen. Die **Bewertung** Die Registerkarte ist nur sichtbar, wenn die neuen Bewertungen erstellt werden. Wenn die Bewertung den Status „in Bearbeitung“ aufweist, wird der letzte Bewertungsstatus angezeigt, während die Bewertung in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bearbeitung ist. Um den aktualisierten Bewertungsstatus anzuzeigen, müssen Sie die Seite aktualisieren. Sobald die Bewertung abgeschlossen ist, kann der Anwender alle zugehörigen Registerkarten für diese Bewertung anzeigen.

Arbeitsbereich Für Schwachstellenbewertung: Registerkarte „Bewertung“



Die Bewertungsdetails werden für die folgenden Widgets angezeigt.

- Konfigurationselemente (Host/Infra)
- Gescannte Anwendungen
- Stücklistenkomponenten und Produktmodelle
- Konfigurationselemente nach CI-Klasse (Installationsbewertung)
- Konfigurationselemente nach Bewertungsquelle: Zeigt die Liste „Betroffene Konfigurationselemente“ an.

Datenvisualisierungen

Name	Typ	Beschreibung
Konfigurationselemente (Host/Infra)	Einzelne Punktzahl	Zeigt die Anzahl der CIs mit und ohne VIS an. Das Widget „Konfigurationselemente“ zeigt die Gesamtanzahl der CIs an, die dem Bewertungsdatensatz zugeordnet sind. Das Widget zeigt außerdem die Konfigurationselemente mit angreifbaren Elementen und ohne angreifbare Elemente an.
Gescannte Anwendungen	Anzahl	Gesamtanzahl der mit AVITs gescannten Anwendungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
		Hinweis: Sie können die Anzahl der gescannten Anwendungen für primäre und sekundäre CVEs anzeigen.
Stücklistenkomponenten und Produktmodelle	Einzelne Punktzahl	Gesamtanzahl der Komponenten, Anzahl der Produktmodelle, mit Anzahl der angreifbaren Anwendungselemente, ohne Anzahl der angreifbaren Anwendungselemente.
Konfigurationselemente nach Bewertungsquelle	Gestapelter Balken	Betroffene Konfigurationselemente, gestapelt von der Bewertungsquelle.
Konfigurationselemente nach CI-Klasse (Installationsbewertung)	Kreisdiagramm	Konfigurationselemente gestapelt nach CI-Klasse.

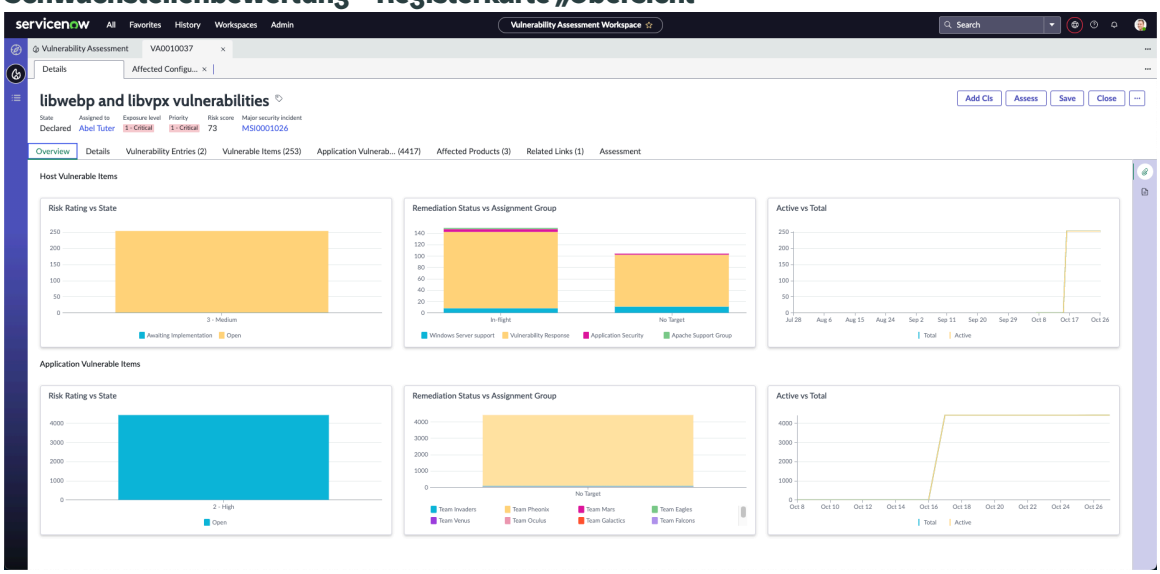
Registerkarte „Übersicht“

Übersicht über die Bewertungsdetails, die auf der Registerkarte Übersicht angezeigt werden. Nachdem Sie die erste Bewertung durchgeführt haben, wird der Datensatz mit den Daten aus korreliert Software Bill of Materials Und Software Asset Management Und werden mit Visualisierungen angezeigt.

Registerkarte „Übersicht“

Die Registerkarte Übersicht füllt Daten (falls verfügbar) basierend auf dem Bewertungsdatensatz aus, den Sie erstellen, und korreliert die Details mit Bewertungen aus Software Asset Management Und Software Bill of Materials Daten in der CMDB. Die zugehörigen Listen namens

Schwachstellenbewertung – Registerkarte „Übersicht“



Die Bewertungsdetails werden für die folgenden Widgets angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Angreifbare Host-Elemente (Host/Infrastruktur)
  - Risikobewertung vs. Status
  - Korrekturstatus vs. Zuweisungsgruppe
  - Aktiv vs. Gesamt
- Angreifbare Anwendungselemente
  - Risikobewertung vs. Status
  - Korrekturstatus vs. Zuweisungsgruppe
  - Aktiv vs. Gesamt

Datenvisualisierungen

Angreifbare Host-Elemente

Name	Typ	Beschreibung
Risikobewertung vs. Status	Gestapelter Balken	Status der angreifbaren Elemente, gestapelt nach ihrer Risikobewertung.
Korrekturstatus vs. Zuweisungsgruppe	Gestapelter Balken	Korrekturstatus des angreifbaren Elements, gestapelt nach seiner Zuweisungsgruppe.
Aktiv vs. Gesamt	Liste und Zeile	Gesamtzahl der angreifbaren Elemente, die diesem Eintrag zugeordnet sind, im Vergleich zu aktiven angreifbaren Elementen.

Angreifbare Anwendungselemente

Name	Typ	Beschreibung
Risikobewertung vs. Status	Gestapelter Balken	Status der angreifbaren Anwendungselemente, gestapelt nach ihrer Risikobewertung.
Korrekturstatus vs. Zuweisungsgruppe	Gestapelter Balken	Korrekturstatus des angreifbaren Anwendungselements, gestapelt nach seiner Zuweisungsgruppe.
Aktiv vs. Gesamt	Liste und Zeile	Gesamtzahl der angreifbaren Anwendungselemente, die diesem Eintrag zugeordnet sind, im Vergleich zu aktiven angreifbaren Elementen.

Weisen Sie dem Schwachstellenbewertungsdatensatz eine Priorität und ein Gefahrenpotenzial zu

Weisen Sie dem Schwachstellenbewertungsdatensatz manuell Priorität und Gefahrenniveau zu.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Schwachstellenbewertung**an.
2. Wählen Sie einen Schwachstellenbewertungsdatensatz aus.
3. Navigieren Sie zu **Risikoattribute** In **Details** Registerkarte.
4. Wählen Sie ein aus **Priorität** Aus der Liste der Optionen.
5. Wählen Sie eine aus **Gefahrenniveau** Aus der Liste der Optionen.
6. Wählen Sie **Speichern**.

Fügen Sie dem Bewertungsdatensatz betroffene CIs hinzu

Fügen Sie manuell die CIs in Ihrer Organisation hinzu, die Ihrer Meinung nach dem Schwachstellenbewertungsdatensatz zugeordnet werden sollten, aber nach nicht in den betroffenen CIs angezeigt werden Anfänglich Bewertung.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager

Warum und wann dieser Vorgang ausgeführt wird
Fügen Sie CIs hinzu, von denen Sie wissen, dass sie möglicherweise betroffen waren, die jedoch nach Abschluss der Bewertung nicht angezeigt werden. Sie können CIs nur hinzufügen, wenn sich der Bewertungsdatensatz in befindet **Deklariert** Oder **Bewertung ausstehend** status.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**an.
2. Wählen Sie den erforderlichen Bewertungsdatensatz aus der Liste aus.
3. Wählen Sie Aus **Fügen Sie CIs hinzu** .
4. Wählen Sie die Konfigurationselemente im Dialogfeld Konfigurationselemente aus.
5. Wählen Sie Aus **Fügen Sie CIs hinzu** .
   Die Vulnerability Response: Fügen Sie Konfigurationselemente zu Ereignis hinzu Hintergrundauftrag wird initiiert, und eine relevante Benachrichtigung wird angezeigt.
6. Wählen Sie Aus **Status Anzeigen** In der Benachrichtigung, um den Status des laufenden Auftrags anzuzeigen.

Ergebnisse
Datensätze werden der Tabelle „Betroffene Konfigurationselemente“ mit hinzugefügt **Quelle** Als `Manuell` .

Nächste Maßnahme
Navigieren Sie zu **Bewertung** Und aktualisieren Sie **Konfigurationselemente (Host/Infra)** Widget zum Anzeigen der von Ihnen hinzugefügten CIs.

Erstellen Sie angreifbare Elemente für das betroffene CI oder die betroffene Softwarekomponente

Erstellen Sie angreifbare Elemente (VIS) oder angreifbare Anwendungselemente (AVITs) im Arbeitsbereich für Schwachstellenbewertung. Schwachstellenanalysten analysieren die Liste der VIS und empfehlen Lösungen und Patches, die dem IT-Team helfen, diese Schwachstellen zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Schwachstellenereignismanager sollte in der Lage sein, ein, mehrere oder alle Suchergebnisse für das Risiko auszuwählen, um Schwachstellenelemente zu erstellen.

- Angreifbares Anwendungselement für SBOM-Bewertungsergebnisse, denen keine AVITs zugeordnet sind
- Angreifbare Elemente für Konfigurationselemente, denen keine Vits zugeordnet sind
- Ordnen Sie das primäre CVE den Schwachstellen-Elementen zu.

Erstellen Sie VIS für Konfigurationselemente, denen angreifbare Elemente zugeordnet sind

Erstellen Sie Vits für angreifbare Elemente für Konfigurationselemente, die durch die Schwachstellenbewertung identifiziert wurden, denen jedoch keine Vits zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertungen**an.
2. Wählen Sie den Bewertungsdatensatz aus, für den Sie die VIT erstellen müssen.
3. Wählen Sie aus **Bewertung** Registerkarte.
4. Wählen Sie Aus **Ohne Konfigurationselemente** Anzahl aus **Konfigurationselemente (Host-Infra)** Widget.
5. Wählen Sie die Konfigurationselemente aus, für die Sie Vits aus erstellen möchten **Betroffene Konfigurationselemente** Liste.
6. Wählen Sie Aus **Erstellen Sie Ein Angreifbares Element** .
   Die Vulnerability Response – Manuelle Vits-Bewertung erstellen Hintergrundauftrag wird initiiert, und eine relevante Benachrichtigung wird angezeigt.
7. Wählen Sie Aus **Status Anzeigen** In der Benachrichtigung, um den Status des laufenden Auftrags anzuzeigen.
   Angreifbare Elemente für die von Ihnen ausgewählten betroffenen Konfigurationselemente werden erstellt.

   Die **Konfigurationselemente (Host-Infra)** Widget zeigt jetzt dasselbe CI in an **Mit Angreifbaren Elementen** Anzahl.

Erstellen Sie angreifbare Anwendungselemente (AVITs) für betroffene Produktmodelle oder Komponenten ohne zugehörige angreifbare Anwendungselemente

Erstellen Sie angreifbare Anwendungselemente (AVITs) für betroffene Produkte oder Komponentenelemente, die durch die Schwachstellenbewertung identifiziert wurden, denen jedoch keine AVITs zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung** > **Bewertungen**an.
2. Wählen Sie den Bewertungsdatensatz aus, für den Sie die VIT erstellen müssen.
3. Wählen Sie aus **Bewertung** Registerkarte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie Aus **Ohne Angreifbare Anwendungselemente** Anzahl aus **Stücklistenkomponenten und Produktmodelle** Widget.
5. Wählen Sie die betroffenen Produktmodelle aus, für die Sie AVITs aus erstellen möchten **Betroffene Produktmodelle** Liste.
6. Wählen Sie Aus **Erstellen Sie Ein Angreifbares Anwendungselement** .
   Die Vulnerability Response – Manuelle Vits-Bewertung erstellen Hintergrundauftrag wird initiiert, und eine relevante Benachrichtigung wird angezeigt.
7. Wählen Sie Aus **Status Anzeigen** In der Benachrichtigung, um den Status des laufenden Auftrags anzuzeigen.
   Angreifbare Anwendungselemente für die von Ihnen ausgewählten betroffenen Produktmodellelemente werden erstellt. Für das primäre CVE, das dem Datensatz zugeordnet ist.

   Die **Stücklistenkomponenten und Produktmodelle** Widget zeigt jetzt dasselbe Produktmodell oder dieselbe Komponente in an **Mit Angreifbaren Anwendungselementen** Anzahl.

Verknüpfen Sie den Schwachstellenbewertungsdatensatz mit einem schwerwiegenden Security Incident in Management schwerwiegender Sicherheits-Incidents

Sie können den Bewertungsdatensatz zu einem verknüpfen, vorschlagen oder heraufstufen Major Security Incident Vorausgesetzt, Sie haben Zugriff auf Management schwerwiegender Sicherheits-Incidents Anwendung.

Vorbereitungen
Erforderliche Rolle: sn_vul_Analyst.vul_event_Manager, sn_si.Analyst, sn_msi.Workspace_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können den Bewertungsdatensatz verschieben, der einem vorhandenen schwerwiegenden Security Incident zugeordnet werden soll, aus dem Bewertungsdatensatz ein neues MSI erstellen oder den Schwachstellenbewertungsdatensatz zu einem schwerwiegenden Security Incident heraufstufen. Nutzen Sie Management schwerwiegender Sicherheits-Incidents Funktionen wie die -Integrationen mit Microsoft Teams Und Microsoft SharePoint.

Sie können auch den Link zu schwerwiegenden Security Incidents im Vulnerability Manager-Arbeitsbereich für angreifbare Elemente anzeigen. Die MSIM Der Link wird der Bewertung der angreifbaren Elemente zugeordnet, die in den angreifbaren Elementen und in den anderen Arbeitsbereichen von angezeigt wird Vulnerability Response.

Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich der Schwachstellenbewertung**an.
2. Wählen Sie den Bewertungsdatensatz aus, den Sie mit einem schwerwiegenden Security Incident verknüpfen möchten.
3. Wählen Sie aus **Weitere Aktionen** Symbol, auf der **Details** Registerkarte.
4. Wählen Sie eine der folgenden Antworten aus.

Option	Bezeichnung
Mit schwerwiegendem Security Incident verknüpfen	Wählen Sie den vorhandenen MSI-Datensatz aus der Liste der schwerwiegenden Security Incidents aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Der Schwachstellenbewertungsdatensatz ist mit dem vorhandenen schwerwiegenden Security Incident verknüpft.
Als schwerwiegenden Security Incident vorschlagen	Geben Sie die folgenden Details ein, und wählen Sie aus **Vorschlagen** . ○ Erkennungsdatum ○ Begründung ○ Potenzieller Impact
Als schwerwiegendem Security Incident heraufstufen	Geben Sie die folgenden Details ein, und wählen Sie aus **Heraufstufen** . ○ Erkennungsdatum ○ Geschätztes Lösungsdatum ○ Begründung ○ Potenzieller Impact

5. Wählen Sie **Speichern**.

Nächste Maßnahme

Wählen Sie den MSI-Datensatz aus, um den Datensatz in zu öffnen Management schwerwiegender Sicherheits-Incidents Anzeigen.

Zugehörige Informationen

Verknüpfen mit Major Security Incident

Als vorschlagen Major Security Incident

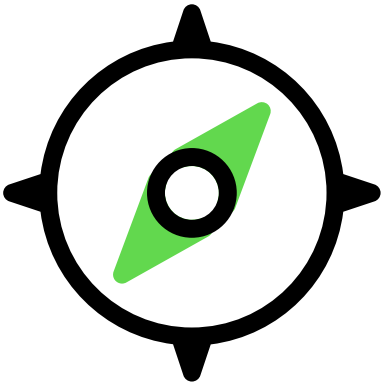
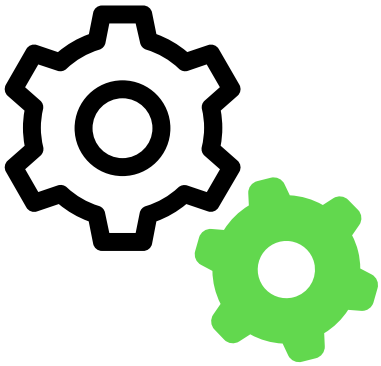
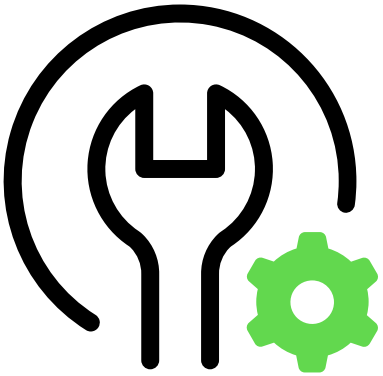
Zu heraufstufen Major Security Incident

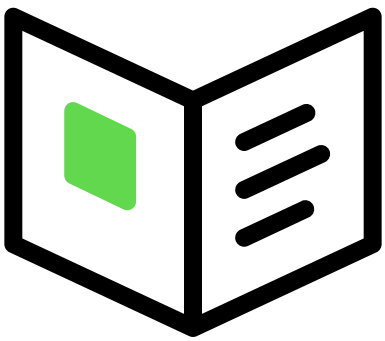
Software-Stückliste

Zeigen Sie eine Liste der Open Source- und Drittanbietersoftwarekomponenten an, die Sie in Ihrer Anwendungsentwicklung verwenden. Erhalten Sie Einblicke in Softwarelizenzen, Versionsinformationen und die bekannten Schwachstellen in Ihren -Komponenten in Software Bill of Materials(SBOM) Dateien, die Sie in Ihre Instanz hochladen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Konfigurieren	Verwenden
		
Erfahren Sie mehr über SBOM Konzepte und Funktionen.	Konfigurieren SBOM Anwendungen.	Erfahren Sie, wie Sie importieren SBOM Komponenten und zeigen Sie Daten im Arbeitsbereich an.

Referenz

Rufen Sie Details zu ab SBOM Formulare, Felder, Tabellen und Eigenschaften.

Problembehandlung und Hilfe

- Security Operations-Community
- CycloneDX – Software Bill of Materials (SBOM) .
- SPDX .
- Durchsuchen Sie das Known Error-Portal nach Known Error-Artikeln .
- Kontakt Kundenservice und Support an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Software Bill of Materials erkunden

Identifizieren Sie die Komponenten, die in den Anwendungen Ihrer Organisation verwendet werden, aus Software Bill of Materials(SBOM) Dateien, die Sie in Ihre Instanz hochladen. Machen Sie sich mit allen Risiken im Zusammenhang mit der Verwendung von Open Source-Software vertraut, um Ihr potenzielles Risiko zu ermitteln, die Lizenz-Compliance anzuzeigen und Schwachstellen zu beheben.

Software Bill of Materials – Übersicht

Drittanbieter- und Open Source-Komponenten bieten Ihnen viele Vorteile für die schnelle Erstellung und Veröffentlichung Ihrer Softwareprojekte. In einigen Fällen bestehen jedoch Risiken im Zusammenhang mit der Verwendung öffentlich zugänglicher Komponenten, z. B.:

- Fehlende Transparenz in der Komponentenintegrität
- Schwachstellen in der Open Source-Software
- Package Intelligence für Open Source-Software
- Nicht konforme Softwarelizenzen

Sie können Ihre Software-Stücklistendateien über eine API oder manuell hochladen. Zeigen Sie die Dateien an, die Sie als Entitäten importieren, d. h. Bestände der in Ihrer Software verwendeten Komponentenbibliotheken von Drittanbietern, einschließlich aller transitiven Abhängigkeiten und verfügbaren Lizenzierungsinformationen.

Weitere Informationen darüber, was in den Softwarebeständen in CycloneDX- und SPDX-SBOMs enthalten ist, finden Sie unter CycloneDX – Software Bill of Materials (SBOM) Und SPDX .

Software Bill of Materials – Anwender

Anwender

Anwender	Beschreibung
Schwachstellenmanager und Analysten	Zeigen Sie hochgeladene Software-Stücklistendateien in Datensätzen, Datenvisualisierungen sowie erweiterte Schwachstellen-Intelligence in an Software Bill of Materials(SBOM) Arbeitsbereich. Schwachstellenmanager und Analysten verwenden diese Informationen, um die Compliance Ihrer Softwarelizenzen und das potenzielle Risiko bei der Verwendung von Open Source-Software zu bestimmen.
Anwender, die Folgendes umfassen können, aber nicht beschränkt sind: • Technologie- oder Softwareanwälte • IT-Manager • Auditoren • Software-Asset-Manager und -Teams	Zeigen Sie hochgeladene proprietäre und Open Source-Softwarelizenzen für Komponenten von hochgeladenen an SBOM Dateien. Erstellen Sie eine Datenbank mit proprietären und Open Source-Softwarelizenzen für die Komponenten. Überprüfen und klassifizieren Sie Lizenzen mit fehlenden Informationen gemäß Ihren internen oder regulatorischen Richtlinien. Ordnen Sie Ihre Komponenten Lizenzen zu, bestimmen Sie Ihre allgemeine Lizenz-Compliance, und sehen Sie sich Ihr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender (Fortsetzung)

Anwender	Beschreibung
	potenzielles Risiko durch gesperrte, eingeschränkte oder fehlende Lizenzen an.

Software Bill of Materials – Workflow

Mit den SBOM-Anwendungen können Sie Dateien hochladen und Details für Entitäten, Komponentenbestände, Schwachstellen und Softwarelizenzinformationen im Arbeitsbereich „Software Bill of Materials“ (SBOM) anzeigen.

- Hochladen SBOM Dateien mit einer API oder manuell.
- Überprüfen Sie die Komponenten in SBOM Datei, die Sie in hochgeladen haben SBOM Arbeitsbereich.
- Überprüfen Sie die Komponentenlizenzinformationen aus dem hochgeladenen SBOM Dateien und klassifizieren Sie sie, damit Sie Ihr Risiko durch eingeschränkte oder gesperrte Lizenzen identifizieren können.
- Bewerten Sie Ihr Risikorisiko, und erstellen Sie angreifbare Elemente für Komponenten mit zugehörigen Schwachstellen.
- Zeigen Sie Berichte und Dashboards sowie Ihre allgemeine Lizenz-Compliance für hochgeladen an SBOM Komponenten auf der Homepage in SBOM Arbeitsbereich.

Software Bill of Materials – Vorteile

Mit drei Anwendungen für Softwarestücklisten können Sie einen genauen Bestand Ihrer Softwarekomponenten und zugehörigen Risiken anzeigen:

- Datenmodell für SBOM
- SBOM Zentral
- SBOM Antwort

Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema .

SBOM – Vorteile

Leistung	Anwendung	Unterstützte Versionen
Diese Anwendung stellt die zum Speichern verwendeten Tabellen bereit SBOM Daten. Diese Anwendung ist erforderlich. Sie enthält die Tabellen, ACLs und Rollen, die gelesen werden müssen SBOM Daten.	Datenmodell für SBOM	V4.0, v3.0, v2.0
Diese Anwendung ist erforderlich. Sie enthält die zum Hochladen erforderliche API SBOM Dokumente und die Geschäftslogik, die zum Analysieren und Importieren der Daten aus diesen Dokumenten in Ihre Instanz erforderlich ist. Sie können einen Bestand Ihrer Softwarekomponenten in anzeigen SBOM Arbeitsbereich, aber Sie können die	SBOM Zentral	V6.0, v5.0, v4.0 Ab Version 4,0 SBOM Core-Unterstützung:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SBOM – Vorteile (Fortsetzung)

Leistung	Anwendung	Unterstützte Versionen
Datenvisualisierungen auf der Zielseite nicht anzeigen . Laden Sie Ihre Software-Stücklistendateien in CycloneDX- und SPDX-Standards hoch, analysieren und verarbeiten Sie sie. Die unterstützten Dateiformate und Versionen für diese Produkte finden Sie in der Spalte unterstützte Versionen. Zeigen Sie Stücklistenentitäten und einen Bestand Ihrer Softwarekomponenten an. Eine Stücklistenentität ist die Komponente auf Stammebene in einer SBOM-Datei. Zum Beispiel für einen CycloneDX SBOM, Die in den Metadaten aufgeführte Komponente wird als Stücklistenentität betrachtet.		• XML- und JSON-Versionen 1,0 bis 1,6 von CycloneDX. • JSON-Versionen 2,2 bis 2,3 von SPDX.
• SBOM Antwort ist erforderlich, wenn Sie Zugriff auf die Funktionen und Daten haben möchten Visualisierungen auf der Zielseite In SBOM Arbeitsbereich. • SBOM Antwort erfordert Vulnerability Response Anwendung. • Zeigen Sie Ihren Komponentenbestand an, und bewerten Sie Ihr Risikorisiko im SBOM Arbeitsbereich. Richten Sie Regeln ein, um angreifbare Anwendungselemente (AVITs) automatisch zu erstellen und mit zu korrigieren Application Vulnerability Response Workflow. • Zeigen Sie Komponentenlizenzinformationen an, die mit hochgeladen werden SBOM Dateien in Lizenzverwaltungsmodul . Klassifizieren Sie die Komponenten, die Sie in hochladen, und lösen Sie sie auf (Abgleichen) Application Vulnerability Response Dateien zu Lizenzen, damit Sie den Status Ihrer allgemeinen Lizenz-Compliance anzeigen können. • Ab Version 4,0 von Application Vulnerability Response Antwort: Sie können Komponenten anzeigen, die als veraltet oder als „nicht konform“ verworfen wurden, in der PACE-Schnittstelle (Policy as Code Engine), die in verfügbar ist SBOM Arbeitsbereich.	SBOM Antwort	V6.0, v5.0, v4.0

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SBOM – Vorteile (Fortsetzung)

Leistung	Anwendung	Unterstützte Versionen
• Die Integrationen OSV.deV und Deps.deV sind bei der Installation enthalten SBOM Antwort. ◦ OSV.deV ist eine Open Source-API, die Schwachstelleninformationen für eine bestimmte Version eines Pakets oder einer Bibliothek bereitstellt. ◦ Deps.deV ist eine Open Source-API, die eine Versionsliste für ein bestimmtes Paket oder eine bestimmte Bibliothek bereitstellt und Komponenten identifiziert, die sich in befinden **Veraltet** Und **Verworfen** status. Weitere Informationen finden Sie unter Konfigurieren der Integrationen Deps.deV, OSV.deV und PACE für Software Bill of Materials. Siehe Integrating PaCE with other applications Weitere Informationen zu PACE- und PACE-Richtlinien.		
Generieren und hochladen Software Bill of Materials(SBOM) Dateien für Software während ihrer kontinuierlichen Integrations- und Bereitstellungsentwicklungszyklen.	SBOM Antwort	• Datenmodell für SBOM: V1.4 und höher. • SBOM Core: V3.0 und höher. • SBOM Antwort: V4.0 und höher.

Vulnerability Response Anwendungen Und CSDM Tabellen

Die Vulnerability Response, Application Vulnerability Response, Integrationen von Schwachstellen von Drittparteien und Software Bill of Materials Anwendungen verwalten (Daten mittragen zu) CSDM Tabellen. Diese Anwendungen verwenden auch Daten aus CSDM Tabellen, die andere Anwendungen generieren. Mehrere ServiceNow Produkte profitieren daher von diesen und fügen ihnen einen Mehrwert hinzu Security Operations Anwendungen. Weitere Informationen finden Sie unter Vulnerability Response Anwendungen Und CSDM Tabellen.

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Software Bill of Materials finden Sie unter:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Unterstützte Anwendungen für erkunden Software Bill of Materials
- Software Bill of Materials konfigurieren
- Hochladen und Anzeigen von SBOM Dateien in SBOM Arbeitsbereich
- Berichte und Dashboards in anzeigen Software Bill of Materials Arbeitsbereich

Unterstützte Anwendungen für erkunden Software Bill of Materials

Schwachstellen-Intelligence von Drittanbietern und andere Integrationen mit Software Bill of Materials Anwendungen können die Daten Ihrer hochgeladenen Dateien verbessern.

Vorteile unterstützter Anwendungen

Schwachstellen-Intelligence von Drittanbietern und andere Integrationen mit Software Bill of Materials Mit Anwendungen können Sie die Anzahl der Komponenten anzeigen, die als veraltet und verworfen gelten, sowie Informationen darüber, ob Sie Schwachstellen im Zusammenhang mit Komponenten beheben können.

Die ServiceNow® Anwendungen und Drittanbieterintegrationen, die in der folgenden Tabelle aufgeführt sind, werden von unterstützt SBOM Anwendungen. Diese Anwendungen bieten Ihnen angereicherte Schwachstellendaten, Schwachstelleninformationen und andere wichtige Informationen, mit denen Sie die Schwachstellen anzeigen und priorisieren können, die mit SBOM-Dateien verknüpft sind. Alle diese Anwendungen und Integrationen sind über verfügbar ServiceNow® Store.

Unterstützte Anwendungen und Integrationen von Drittparteien

Leistung	Anwendung	Unterstützte Versionen	Anwender
Vulnerability Response Ist erforderlich, wenn Sie installieren SBOM Antwortanwendung. Installieren Sie Vulnerability Response Anwendung vor der Installation von SBOM Response. Application Vulnerability Response-Funktionen werden mit installiert Vulnerability Response. Diese Funktionen ermöglichen den Zugriff auf den Vulnerability Manager-Arbeitsbereich im Vulnerability Response Anwendung und Schwachstellen-Workflow, mit dem Sie angreifbare Anwendungselemente	Vulnerability Response	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema .	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Anwendungen und Integrationen von Drittparteien (Fortsetzung)

Leistung	Anwendung	Unterstützte Versionen	Anwender
(AVIT) beheben können			
Zeigen Sie erweiterte NVD-Schwachstellen- und -Schweregraddaten an. Zeigen Sie importierte Daten aus den NVD- und CWE-Integrationen an, um Schwachstellendaten anzureichern, die Sie in Ihren SBOM-Daten finden könnten. Weitere Informationen finden Sie unter Importieren von Daten mit den NVD- und CWE-Integrationen und Verwalten von Drittparteibibliotheken.	Vulnerability Response-Integration mit NVD und SBOM Response	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema .	
Importieren Sie Softwarerechnungen von Materialdateien mit Veracode Vulnerability Integration. Die Veracode Vulnerability Integration Enthält die folgenden Erweiterungen von Veracode SBOM-Dateien: • Wenn Sie installiert haben SBOM Antwort haben Sie die Möglichkeit, von gefundene Schwachstellen einzubeziehen SBOM Für SBOM Dateien, die Sie hochladen. • SBOM Ist dem Quellfeld für Datensätze in der Tabelle „Stückliste“ [sn_sbom_doc] für zugeordnet SBOM SBOM Dateien, die Sie hochladen.	Veracode Vulnerability Integration und SBOM Response	Ab Version 4,3 von Veracode Vulnerability Integration. Wenn Sie haben Veracode Vulnerability Integration Bereits installiert, können Sie auch importierte hochladen Veracode SBOM Daten in den Formaten CycloneDX (JSON und XML) und SPDX (XML) ab Version v3.0 von SBOM Kern. Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema .	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Anwendungen und Integrationen von Drittparteien (Fortsetzung)

Leistung	Anwendung	Unterstützte Versionen	Anwender
Weitere Informationen finden Sie unter Veracode Vulnerability Integration.			
Hochladen SBOM Dateien in ServiceNow AI Platform Aus Ihren GitHub-Repositorys. Bestimmen Sie, ob SBOM Dateien, die in Ihren CI/CD-Pipelines (kontinuierliche Integration und kontinuierliche Bereitstellung/ -Bereitstellung) generiert wurden, wurden erfolgreich in der Warteschlange in Ihrer eingefügt ServiceNow AI Platform Instanz. Schützen Sie Ihre Umgebungen während der Softwareentwicklungszyklen vor potenziell schädlichen Komponenten mit GitHub-Aktionen, die Sie aus Ihrer GitHub-Umgebung initiieren.	Rufen Sie alle erforderlichen GitHub-Aktionen für ab SBOM Laden Sie in den GitHub Marketplace hoch.	Ab Version 4,0 von SBOM Kern.	

Software Bill of Materials konfigurieren

Laden Sie die erforderlichen Anwendungen für herunter, und aktivieren Sie sie Software Bill of Materials(SBOM) Anwendung vor dem Hochladen SBOM Dateien.

Konfiguration – Übersicht

1. Laden Sie die erforderlichen herunter SBOM Anwendungen und alle zusätzlichen unterstützten Anwendungen und Integrationen aus dem ServiceNow Store in Ihre ServiceNow-Instanz. Siehe Software Bill of Materials erkunden Und Laden Sie eine Anwendung aus dem herunter ServiceNow Store Zum ersten Mal Weitere Informationen zu unterstützten Anwendungen.

   Die Anwendung Vulnerability Response ist für erforderlich SBOM Antwort. Installieren Sie die Anwendung Vulnerability Response vor der Installation SBOM Antwort.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Suchen Sie die heruntergeladenen SBOM-Anwendungen, und wählen Sie Installieren, um sie zusammen mit ihren Abhängigkeiten in der folgenden Reihenfolge zu aktivieren. Weitere Informationen finden Sie unter Installieren Sie die unterstützten Anwendungen für Software Bill of Materials.

   - Vulnerability Response und ihre Abhängigkeiten
   - Vulnerability Response-Integration mit NVD
   - Datenmodell für SBOM
   - SBOM Zentral
   - SBOM Antwort, die die OSV.de-V- und Deps.de-V-Integrationen und den Zugriff auf die Fähigkeiten der Policy as Code Engine (PACE) im SBOM-Arbeitsbereich umfasst.

3. Konfigurieren Sie die Integrationen Deps.deV und OSV.deV. Diese Integrationen sind in enthalten SBOM Antwortanwendung und werden automatisch installiert und aktiviert. Sie müssen die OSV.de-V-Integration – umfassende On-Demand-Integration über den zugehörigen Integrationsdatensatz initiieren. Siehe Konfigurieren der Integrationen Deps.deV, OSV.deV und PACE für Software Bill of Materials Und Software Bill of Materials erkunden Weitere Informationen finden Sie unter .

   Die Deps.de-V-Integration enthält Informationen zu Komponenten, die sich in befinden **Veraltet** Und **Verworfen** status für eine bestimmte Version eines Pakets oder einer Bibliothek, das Sie in hochladen SBOM Dateien.

   OSV.deV ruft Schwachstellendaten aus einer Open Source-Datenbank für eine Version eines Pakets oder einer Bibliothek ab, die Sie in hochladen SBOM Dateien.

4. Informationen zur Konfiguration zusätzlicher unterstützter Anwendungen und Integrationen, die Sie installiert haben, finden Sie in der Produktdokumentation. Siehe Vulnerability Response-Integrationen und Integration von Application Vulnerability Response mit anderen Anwendungen.

Installieren Sie die unterstützten Anwendungen für Software Bill of Materials

Laden Sie die erforderlichen Anwendungen für herunter, und aktivieren Sie sie Software Bill of Materials(SBOM) Anwendung vor dem Hochladen von Dateien.

Vorbereitungen

Erforderliche Rollen: administrator für Download, Installation und Aktivierung aller Anwendungen und Rollenzuweisungen in Ihrer Instanz.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Laden Sie die erforderlichen herunter SBOM Anwendungen aus dem ServiceNow Store In Ihren ServiceNow Instanz.

   Mit diesen Anwendungen können Sie hochladen und importieren SBOM Dateien in Ihrer Instanz. Sie können Stücklistenentitäts- und Komponentendaten in anzeigen SBOM Arbeitsbereich, falls vorhanden SBOM Core installiert.

   Sie können Stücklistenentität, Komponentendaten und Datenvisualisierungen in anzeigen SBOM Arbeitsbereich, falls vorhanden SBOM Antwort installiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Datenmodell für SBOM
- SBOM Zentral

Weitere Informationen zum Herunterladen und Aktivieren von Anwendungen finden Sie unter:

- Install a ServiceNow Store application
- Install an update to a ServiceNow Store application

2. **Wahlweise:** Wenn Sie Ihren anzeigen möchten SBOM Daten in SBOM-Arbeitsbereich, zeigen Sie importierte Schwachstellen-Intelligence von Drittanbietern an, bewerten Sie Ihr Risikorisiko, und beheben Sie Schwachstellen mit Application Vulnerability Response Und Vulnerability Response Workflows: Laden Sie die folgenden Anwendungen herunter:
   - Vulnerability Response Und ihre Abhängigkeiten
   - Vulnerability Response-Integration mit NVD
   - SBOM Antwort

   Um weitere Informationen zu diesen und anderen unterstützten Elementen zu erhalten SBOM Anwendungen, siehe Software Bill of Materials erkunden.

3. Nachdem Sie die Anwendungen heruntergeladen haben, navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
4. Suchen Sie nach SBOM Anwendungen, die Sie heruntergeladen und ausgewählt haben **Installieren** Um sie zusammen mit ihren Abhängigkeiten zu aktivieren.

   Eine Nachricht wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde. Aktivieren Sie die Anwendungen in der folgenden Reihenfolge:
   - Vulnerability Response Und ihre Abhängigkeiten
   - Vulnerability Response-Integration mit NVD
   - Datenmodell für SBOM
   - SBOM Zentral
   - SBOM Antwort, die die OSV.de-V- und Deps.de-V-Integrationen enthält und die PACE-Schnittstelle (Policy as Code Engine) in unterstützt SBOM Arbeitsbereich.

   Siehe Konfigurieren der Integrationen Deps.deV, OSV.deV und PACE für Software Bill of Materials Weitere Informationen zum Konfigurieren dieser Integrationsanwendungen nach der Installation SBOM Antwort.

5. **Wahlweise:** Aktivieren Sie Integrationen, indem Sie zu navigieren **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle** Und auswählen **Installieren** .

   (Optional) Weitere Informationen zu diesen Integrationen und den von ihnen bereitgestellten Fähigkeiten finden Sie unter Software Bill of Materials erkunden.
   - Vulnerability Response-Integration mit Veracode. Weitere Informationen finden Sie unter Installieren Sie ServiceNow Vulnerability Response-Integration mit Veracode.
   - Vulnerability Response-Integration mit NVD, die erforderlich ist, wenn Sie die erweiterten Daten für Schwachstellen anzeigen möchten, die hochgeladenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten zugeordnet sind. Weitere Informationen finden Sie unter Verstehen der NVD-Integrationen.

- CWE – umfassende 2000-Integration. Siehe Konfigurieren und führen Sie die geplante Aufgabe zum Aktualisieren von CWE-Datensätzen aus Weitere Informationen zum Aktivieren dieser geplanten Aufgabe.

Eine Nachricht wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde.

6. Weisen Sie Anwendern die folgenden Rollen zu.
   - sn_sbom_dm.App_create
   - sn_sbom_dm.App_read
   - sn_sbom_dm.App_write
   - sn_sbom_Core.sbom_ingest
   - sn_sbom_Core.admin
   - sn_sbom_Resp.sbom_Analyst
   - sn_sbom_Resp.Manage_avi_rule
   - sn_sbom_response.managelicense
   - sn_sbom_response.licenseresolver
7. **Wahlweise:** Weisen Sie der App-SEC-Manager-Gruppe Anwender zu, wenn Sie angreifbare Anwendungselemente für Schwachstellen in Ihrem importieren erstellen SBOM Daten.

   (Optional) Anwender, die der App-SEC-Manager-Gruppe zugewiesen sind, priorisieren und verwalten angreifbare Anwendungselemente. Anwender in dieser Gruppe erben viele der Rollen, die zum Lesen und Bearbeiten von Datensätzen und zum Konfigurieren der von unterstützten Anwendungen erforderlich sind Application Vulnerability Response Anwendung und ihre Korrektur-Workflows.
8. **Wahlweise:** Deaktivieren Sie AVITs erneut öffnen, wenn erkannt (*sn_sbom_resp.reopen_avits_if_detected*) Systemeigenschaft, wenn nicht gewünscht **Geschlossen** AVITs, um zurück zum zu wechseln **Öffnen** status automatisch.

   (Optional) A **Geschlossen** Angreifbares Anwendungselement (AVIT) für eine Komponente mit einer zugehörigen Schwachstelle wird erneut geöffnet (auf festgelegt **Öffnen**) Automatisch und im SBOM-Arbeitsbereich sichtbar, wenn die folgenden Bedingungen vorhanden sind:

   - Der AVIT mit der zugehörigen Schwachstelle wird von den Schwachstellen-Scans einer Drittpartei-Integration erneut erkannt, oder die Komponente mit der Schwachstelle ist Teil eines nachfolgenden SBOM-Uploads.
   - Sie haben AVITs erneut öffnen, wenn erkannt (*sn_sbom_resp.reopen_avits_if_detected*) Systemeigenschaft. Diese Systemeigenschaft ist standardmäßig aktiviert.
   - Der Substatus von **Geschlossen** AVIT ist keine der folgenden: **Minderungssteuerung vorhanden** , **Nicht Betroffen** , Oder **Falsch Positiv** . AVITs mit diesen Substatus werden von der Systemeigenschaft nicht erneut geöffnet.

Nächste Maßnahme

Laden Sie Ihr hoch SBOM Dateien. Siehe Hochladen Software Bill of Materials Dateien manuell und Wird Hochgeladen Software Bill of Materials Dateien, die eine REST-API verwenden, um weitere Informationen zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren der Integrationen Deps.deV, OSV.deV und PACE für Software Bill of Materials

Sie können einige der Parameter für die Integrationen Deps.deV und OSV.deV bearbeiten. Es gibt auch zwei Codeauslöserversionen dieser Integrationen, die ausschließlich für interne Workflows verwendet werden. Sie sollten diese Integrationen nicht bei Bedarf initiieren. Darüber hinaus können Sie eine geplante Aufgabe aktivieren, um Richtlinien mit der Richtlinie als Code-Engine (PACE) zu erstellen.

Codeauslöserintegrationen für interne Workflows

Ab v3.2 von SBOM Antwort, Leistungsverbesserungen beinhalteten die Hinzufügung von zwei OSV.deV und Deps.deV Codeauslöser Integrationen:

- OSV-Integration (Codeauslöser bei Bedarf)
- Deps.de-V-Integration (Codeauslöser bei Bedarf)

Diese Integrationen werden automatisch von internen Workflows initiiert und dienen nur zur internen Verwendung. Obwohl Sie sie finden können, dürfen Sie diese Integrationen nicht bei Bedarf mit initiieren **Jetzt Ausführen** Schaltfläche aus ihren Integrationsdatensätzen.

Konfigurieren des Ausführungszeitplans für die Deps.de-V-Integration

Die Deps.de-V-Integration Ist mit installiert SBOM Antwort. Die Integration ist standardmäßig aktiviert (Kontrollkästchen „aktiv“ im Integrationsdatensatz ausgewählt) und wird wöchentlich ausgeführt. Beachten Sie, dass dies nicht die On-Demand-Deps.de-V-Code-Auslöserintegration ist. Sie können den Zeitplan bearbeiten und die geplante Aufgabe bei Bedarf aus dem zugehörigen Integrationsdatensatz initiieren. .

Um den Zeitplan zu ändern, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen** > **Deps.dev-Integration**an. Die Rolle sn_vul.App_configure_Integrations ist erforderlich, um den Zeitplan dieser Integration zu bearbeiten.

Diese Deps.de-V-Integration wird verwendet, um Komponenten zu identifizieren, die sich in befinden **Veraltet** Und **Verworfen** status. Die Version einer veralteten Komponente liegt mehr als zwei Hauptversionen hinter der neuesten Version und zwei Jahre hinter der neuesten Version. Eine verworfene Komponente wurde seit mehr als zwei Jahren nicht aktualisiert. Die Schwellenwerte für zwei Jahre und zwei Versionen können mit Systemeigenschaften bearbeitet werden. Um diese Parameter zu bearbeiten, navigieren Sie zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften** Und suchen Sie die folgenden Datensätze:

- sn_sbom_Resp.pkg_abandoned_threshold
- sn_sbom_Resp.pkg_stale_threshold
- sn_sbom_Resp.pkg_stale_Version_threshold

Die Schwellenwerte für „verworfen“ und „veraltet“ liegen in Monaten. Der Schwellenwert für Version ist numerisch.

Sie können importierte Daten auf der Homepage des Arbeitsbereichs und im Modul „Stücklistenwarteschlange“ anzeigen. Importierte Daten werden in der Tabelle „Paketgruppen“ [sn_sbom_pkg_Group] gespeichert.

Konfigurieren und Initiieren der OSV.de-V-Integration – umfassend

Die OSV.de-V-Integration – umfassend Integration wird mit installiert SBOM Antwort. Die Integration ist standardmäßig aktiviert (Kontrollkästchen „aktiv“ im Integrationsdatensatz ausgewählt). Beachten Sie, dass

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dies nicht die On-Demand-OSV.de-V-Code-Auslöserintegration ist. Sie müssen diese Integration bei Bedarf aus dem zugehörigen Integrationsdatensatz initiieren.

Um diese Integration zu konfigurieren und zu initiieren, navigieren Sie zu **Alle** > **Vulnerability Response** > **Administration** > **Integrationen** > **OSV.de-V-Integration: Umfassend**an. Die Rolle „sn_vul.App_configure_Integrations“ ist erforderlich.

Sie können importierte Daten auf der Homepage des Arbeitsbereichs auf der Registerkarte Schwachstelle in Datensätzen aus der Entitätsliste und im Modul Bibliotheken anzeigen. Importierte Daten werden in den Tabellen „angreifbare Anwendungseinträge“ [sn_vul_App_vul_entry] und „nationale Schwachstellendatenbankeinträge“ [sn_vul_nvd_entry] gespeichert.

Hinweis:
Sie können OSV.dev's konfigurieren *batchSize*Integrationsparameter auf der Registerkarte „Integrationsparameter“ auf der **Open Source-Schwachstellen-Instanz** Befindet sich in **Alle** > **Vulnerability Response** > **Administration** > **Integrationen** > **Schwachstellen-Integrationen** > **Open Source-Schwachstellen-Instanz**an. Der Standardwert ist 75 PURLs pro API-Aufruf.

Möglicherweise möchten Sie diesen Wert in seiner Standardeinstellung belassen. Das Ändern des Werts kann sich auf die Leistung auswirken.

PACE wird aktiviert

Ab Version 4,0 von SBOM Antwort: Sie können Komponenten anzeigen, die als veraltet oder als „nicht konform“ verworfen wurden, in der PACE-Schnittstelle (Policy as Code Engine), die in verfügbar ist SBOM Arbeitsbereich.

- Bestimmen Sie, ob Komponenten mit veraltet oder verworfen wurden *Run PaCE policies for SBOM Response*Geplante Aufgabe. Diese geplante Aufgabe ist standardmäßig deaktiviert.
- Zeigen Sie Komponenten an, die als veraltet oder als nicht konform verworfen wurden, in der PACE-Schnittstelle, die verfügbar und in angezeigt wird SBOM Arbeitsbereich.

Siehe Integrating PaCE with other applications Weitere Informationen zu PACE- und PACE-Richtlinien.

Hochladen und Anzeigen von SBOM Dateien in SBOM Arbeitsbereich

Die SBOM Mit Anwendungen können Sie Dateien hochladen und Details für Entitäten, Komponentenbestände, Lizenzinformationen und andere Details im Arbeitsbereich „Software-Stückliste“ anzeigen.

Übersicht über Wird hochgeladen SBOM Dateien

Sie können Ihre Software-Stücklistendateien über eine API oder manuell hochladen. Zeigen Sie die Dateien an, die Sie als Entitäten importieren. Dabei handelt es sich um Bestände der in Ihrer Software verwendeten Komponentenbibliotheken von Drittanbietern, einschließlich aller transitiven Abhängigkeiten.

- Wird Hochgeladen Software Bill of Materials Dateien, die eine REST-API verwenden.

  Die Upload-API wird zum Hochladen und Erfassen von verwendet SBOM Datei (CycloneDX/SPDX) in Ihrer Instanz.

- Hochladen Software Bill of Materials Dateien manuell.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Laden Sie Software-Stücklistendateien manuell hoch. Die Methode, mit der Sie Ihre Dateien hochladen, hängt davon ab, ob Sie über verfügen SBOM Kern oder SBOM Antwortanwendungen installiert.

- Wird Hochgeladen Software Bill of Materials Für DevOps SBOM Dateien.

  Generieren und hochladen SBOM Dateien für Software während ihrer kontinuierlichen Integrations- und Bereitstellungsentwicklungszyklen.

- Klassifizieren und lösen Sie Komponentenlizenzen im Lizenzverwaltungsmodul auf.

  Überprüfen Klassifizieren , Und Lösen (Zuweisen) Lizenzinformationen für die Komponenten, die Sie in hochladen SBOM Dateien gemäß Ihren internen oder regulatorischen Richtlinien. Sie können Ihre Komponenten mit Lizenzen abgleichen und Ihre allgemeine Lizenz-Compliance bestimmen, um Ihr potenzielles Risiko durch gesperrte, eingeschränkte oder fehlende Lizenzen zu sehen.

- Berichte und Dashboards in anzeigen Software Bill of Materials Arbeitsbereich

  Schwachstellenanalysten und -Manager können hochgeladene Software-Stücklistendateien und wichtige Daten in Datensätzen, Datenvisualisierungen sowie erweiterte Schwachstelleninformationen und Lizenzinformationen anzeigen Software Bill of Materials(SBOM) Arbeitsbereich.

Hinweis:
Sie müssen installieren SBOM Antwort, wenn Sie die Datenvisualisierungen auf der Zielseite (Homepage) des Arbeitsbereichs anzeigen möchten.

Wird Hochgeladen Software Bill of Materials Dateien, die eine REST-API verwenden

Überprüfen Sie die folgenden Informationen vor dem Hochladen Software Bill of Materials Dateien, die eine API verwenden.

Mit der REST-API

Zum Hochladen einer SBOM-Datei mit einer API ist die Rolle sn_sbom_Core.sbom_ingest erforderlich.

API hochladen.

Diese API wird zum Hochladen und Erfassen einer SBOM-Datei (CycloneDX/SPDX) in Ihre Instanz verwendet.

Version 4,0 von SBOM Core-Unterstützung:

- XML und JSON in CycloneDx (Versionen 1.0–1.6).
- JSON in SPDX (Versionen 2,2–2,3)

- **Hinweis:**
  Dateien mit mehr als 32 MB werden möglicherweise nicht ordnungsgemäß geladen.

HTTP-Methode: (POST)

API-URL: `<host_name>/api/sbom/Core/Upload`

Hinweis:
`<host_name>` Ist Ihr ServiceNow Instanzname.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle folgenden Anforderungsparameter sind optional. Der Anforderungstext ist der SBOM-Dateiinhalt. Wenn Sie DevOps als Teil Ihres Entwicklungsprozesses verwenden, muss der Wert von „requestedBy“ „devops“ sein. Siehe Wird Hochgeladen Software Bill of Materials Für DevOps SBOM Dateien Für allgemeinere Informationen zu DevOps. Wenn der Wert für „requestedby“ „devops“ (Bereitstellungsvorgänge) ist, sind diese Parameter obligatorisch:

- BuildId
- LebenszyklusPhase

Wenn „requestedBy“ auf „devops“ festgelegt ist, werden außerdem Daten für fetchVulenrabilityInfo und fetchPackageInfo enthalten.

- BuildId: Zeichenfolge, die Sie senden
- LifecycleStage: Zwei Werte, Production oder Pre_Production
- FetchVulenrabilityInfo – t/f
- FetchPackageInfo-t/f

Anforderungsparameter	Mögliche Werte	Beschreibung
productModelId	Sys-ID	SYS-ID des Produktmodells, das der angegebenen Stammanwendung zugeordnet werden soll SBOM.
BusinessApplicationId	Sys-ID	SYS-ID der Geschäftsanwendung, die der angegebenen Stammanwendung zugeordnet werden soll SBOM.
BusinessApplicationName (veraltet)	Name der Geschäftsanwendung	Name der Geschäftsanwendung, die der angegebenen Stammanwendung zugeordnet werden soll SBOM.
SbomSource	Ein Produkt wie Veracode, Zum Beispiel	Die Quelle für Ihren SBOM Datei.
requestedBy	Ein Tool oder Name einer Methode, Jenkins. Wenn Sie „devops“ verwenden, sind „buildId“ und „lifecycleStage“ obligatorisch.	Upload angefordert von
BuildId	Eine Zeichenfolge, die von der anfordernden Person gesendet wird.	Build-ID von SBOM Erstellen.
LebenszyklusPhase	Production oder Pre_Production	Lebenszyklusphase der Entität.
Ruft VulenrabilityInfo ab	t/W	Bei „wahr“ wird die Integration von Vulnerability Intelligence ausgelöst.
Ruft Paketinformationen ab	t/W	Bei „wahr“ wird die Package Intelligence-Integration ausgelöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Upload-API-Antwort: Enthält „Status“ erfolgreich/fehlgeschlagen, „message“ (Zeichenfolge), „bomRecordId“ (dies ist die SYS-ID der SBOM, die über die Upload-API für einen erfolgreichen SBOM-Upload zurückgegeben wird).

```
{

"result": {

"status": "success",

"message": "Queued for processing.",

"bomRecordId": "f207059b4393c290629aa597cbb8f247"

}

}
```

Status-API

Diese API ruft den Status und die Zusammenfassung einer SBOM ab, die sich in der Warteschlange für die Erfassung befindet.

- API-URL: `/api/sbom/Core/upload/Status`
- HTTP-Methode (GET)

Anforderungsparameter	Mögliche Werte	Beschreibung
BomRecordId	Sys-ID	SBOM-Datensatz-ID, die über die Upload-API für einen erfolgreichen SBOM-Upload zurückgegeben wird.

Beispiel für Standard-Antwort der Status-API.

```
{
  "result": {
    "bomRecordId": "0407c0fea3e70a505df340f5251e617e",
    "uploadStatus": "processed",
    "additionalInfoStatus": "not_requested",
    "uploadSummary": {
      "components": {
        "added": 0,
        "removed": 0,
        "total": 70
      }
    }
  }
}
```

Beispiel für Status-API-Antwort mit zusätzlichen Parametern. Wenn Sie fetchVulenrabilityInfo für diese SBOM angefordert haben, erhalten Sie die Schwachstellenaufgliederung als Teil der Antwort.

```
{
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"result": {
 "bomRecordId": "93af349b4393c290629aa597cbb8f258",
 "uploadStatus": "processed",
 "additionalInfoStatus": "complete",
 "uploadSummary": {
  "components": {
   "added": 0,
   "removed": 0,
   "total": 3
  },
  "vulnerabilityInfo": {
   "critical": 0,
   "high": 0,
   "medium": 0,
   "low": 0,
   "none": 0
  }
 },
 "buildId": "1"
}
}
```


Wenn Sie „fetchPackageInfo“ für diese SBOM angefordert haben, erhalten Sie als Teil der Antwort die Anzahl veralteter und verworfener Elemente.

Nach einem SBOM Wird erfolgreich verarbeitet, wobei Sie die hochgeladenen Datensätze anzeigen, hängt von den von Ihnen verwendeten Anwendungen ab.

- Wenn Sie verwenden SBOM Antwort: Der Stücklistenentitätsdatensatz wird auf angezeigt SBOM Erfassungsstatusliste im Modul „Stücklistenwarteschlange“ in SBOM Arbeitsbereich.
- Wenn Sie SBOM Core verwenden, navigieren Sie zu **SBOM-Core** > **Stücklisten-Erfassungsstatus**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterungen zu unterstützt SBOM Standards und allgemeine Nutzungsinformationen

Version 4,0 von SBOM Core-Unterstützung:

- XML und JSON in CycloneDx (Versionen 1.0–1.6).
- JSON in SPDX (Versionen 2,2–2,3)

- **Hinweis:**
  Dateien mit mehr als 32 MB werden möglicherweise nicht ordnungsgemäß geladen.

Ab v4.0 von SBOM Core, die folgenden Verbesserungen wurden vorgenommen, um CycloneDx-Standards für die Versionen 1,0 bis 1,6 zu unterstützen:

- Importieren Sie zusätzliche Informationen in CycloneDX SBOM-Dateien mit der Eigenschaft (sn_sbom_Core.Collect_properties). Diese Eigenschaft ist standardmäßig deaktiviert. Aktivieren Sie die Eigenschaft, um Informationen zu importieren, die im Allgemeinen nicht unterstützt werden. Alle aus diesen Eigenschaften importierten Informationen werden für Folgendes in die Tabelle „SBOM-Komponenteneigenschaft“ [sn_sbom_comp_property] hochgeladen:
  - SBOM-Dateien hochgeladen
  - Metadaten
  - Einzelne Schwachstellen
  - Komponenten
- Zeigen Sie importierte Komponentendaten für deklarierte und abgeschlossene Lizenzen für SBOM-Dateien in Versionen 1,4 und höher von CycloneDX in zwei neuen Lizenzfeldern an:
  - **Deklariert**
  - **Abgeschlossen**
- Die Unterstützung der SBOM-Analyse wird für die folgenden CycloneDX-Komponententypen erweitert:
  - Version 1,5: Plattform, Daten, Gerätetreiber, Modell für maschinelles Lernen
  - Version 1,6: Kryptografisch

Version 3,0 von SBOM Core-Unterstützung:

- XML und JSON in CycloneDx (bis einschließlich Version 1,4).
- JSON in SPDX (bis zu und einschließlich v2.3).

Wenn der aufrufende Anwender erfolgreich authentifiziert wurde und über die Rolle sn_sbom_Core.sbom_ingest in Ihrem verfügt ServiceNow-Instanz können Sie von außerhalb Ihrer -Instanz auf die API zugreifen, um hochzuladen SBOM Daten.

Nachdem Daten hochgeladen wurden, werden sie analysiert. Bevor Daten analysiert werden, werden die folgenden Anforderungen verifiziert:

- Eingehende Daten werden auf gültige JSON- oder XML-Dateien überprüft.
- Das Stücklistenformat wird unterstützt. Beginnend mit v2.1 von SBOM Die Formate Core, CycloneDX (JSON und XML) und SPDX (XML) werden unterstützt.
- Die Mindestanzahl von Feldern ist verfügbar, damit Daten analysiert werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem diese Prüfungen verifiziert wurden, wird ein Eintrag in die Tabelle „Stückliste“ [sn_sbom_doc] mit „eingehend“ vorgenommen SBOM Daten als Anhang.

Die *Process BOM file*Die Business-Regel wird automatisch durch das Einfügen von Datensätzen und die Datenanalyse ausgelöst.

Hinweis:
Diese Business-Regel wird während der Installation von aktiviert SBOM Standardmäßig Core.

Alle Komponenten, die in aufgeführt sind SBOM Haben eine definiert Typ .

- Komponenten, für die SBOM Dateien, die hochgeladen wurden, werden als Stücklistenentitäten betrachtet.
- Komponenten aufgeführt als Type=Library Werden als Komponenten von Drittparteien betrachtet.

Zugehörige Informationen

Zeigen Sie den Upload-Status für an Software Bill of Materials Dateien

Berichte und Dashboards in anzeigen Software Bill of Materials Arbeitsbereich

Hochladen Software Bill of Materials Dateien manuell

Hochladen Software Bill of Materials(SBOM) Dateien manuell.

Vorbereitungen
Ab Version 4,0 unterstützt SBOM Core:

- XML und JSON in den Versionen 1,0 bis 1,6 von CycloneDX.
- JSON in den Versionen 2,2 bis 2,3 von SPDX.

Erforderliche Rolle: sn_sbom_Core.sbom_ingest

Prozedur

1. Dateien manuell hochladen.

   Die Methode, mit der Sie Ihre Dateien hochladen, hängt davon ab, ob Sie über verfügen SBOM Kern oder SBOM Antwortanwendungen installiert.

2. **Wahlweise:** Hochladen SBOM Dateien, die von importiert wurden Veracode Vulnerability Integration.

   Hinweis:
   Sie können hochladen Veracode Dateien in den Formaten CycloneDX (JSON und XML) und SPDX (XML) nur, wenn Sie installiert und aktiviert haben Veracode Integration mit Application Vulnerability Response. Siehe Veracode Vulnerability Integration Weitere Informationen finden Sie unter .

Ergebnisse
Nach einem SBOM Wird erfolgreich verarbeitet, wobei Sie den Upload-Status anzeigen, abhängig von den von Ihnen verwendeten Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie verwenden SBOM Antwort: Der Stücklistenentitätsdatensatz wird auf angezeigt SBOM Erfassungsstatusliste im Modul „Stücklistenwarteschlange“ in SBOM Arbeitsbereich.
- Wenn Sie verwenden SBOM Core, navigieren Sie zu **SBOM-Core** > **Stücklisten-Erfassungsstatus**an.

Zugehörige Informationen

Wird Hochgeladen Software Bill of Materials Dateien, die eine REST-API verwenden

Wird Hochgeladen Software Bill of Materials Für DevOps SBOM Dateien

Generieren und hochladen Software Bill of Materials SBOM Dateien für Software während ihrer kontinuierlichen Integrations- und Bereitstellungsentwicklungszyklen.

DevOps und SBOM Dateien

SBOM Dateien können in mehreren Phasen während des gesamten Entwicklungszyklus der kontinuierlichen Integration und kontinuierlichen Bereitstellung (CI/CD) von Software generiert werden. Die meisten Softwareentwicklungsvorgänge (DevOps) in Organisationen verwenden eine Art von CI/CD-Prozess, um kostspielige Fehler zu identifizieren und zu verhindern, die nach dem Release auftreten könnten. In der gesamten CI/CD-Pipeline kann DevOps SBOM-Dateien generieren und proaktiv auf Schwachstellen und gefährdete Komponenten überprüfen. Diese Prüfungen können Unternehmen dabei helfen, die Softwarequalität zu verbessern und kostspielige Wartung später zu vermeiden. Wird Generiert SBOM Dateien sind für die erfolgreiche Implementierung und Automatisierung genauer Build-Bewertungen während der CI-/CD-Entwicklung von entscheidender Bedeutung.

Das Hochladen von SBOM-Dateien aus Entwicklungs-Pipelines wird ab den folgenden Versionen von unterstützt SBOM Anwendungen.

Unterstützte Versionen

Anwendung	Unterstützte Versionen
Datenmodell für SBOM	V3.0, v2.0
SBOM Zentral	V5.0, v4.0, v3.0
SBOM Antwort	V5.0, v4.0, v3.2, 3,1

Anwendungsfälle

Wird Generiert SBOM Dateien und das Senden über die SBOM-Upload-API als Teil der DevOps-Build-Pipeline können Anzahlen für Folgendes bereitstellen, um zu bestimmen, ob die Pipeline erfolgreich sein oder fehlschlagen soll:

- Komponenten hinzugefügt
- Komponenten entfernt
- Informationen zu Schwachstellen
- Paketinformationen (verworfene/veraltete Komponenten)

DevOps-Richtlinien und -Regeln für den Erfolg oder Fehler einer Pipeline können durch die Anzahlen der Schwachstellen und die Schwellenwerte für die Anzahl veralteter und verworfener Komponenten definiert werden, die von empfangen werden SBOM Status-API.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für eine fehlgeschlagene Pipeline können DevOps-Anwender in auf Informationen zum fehlgeschlagenen Build zugreifen ServiceNow® Instanz, um die Ursache und den Ursprung der Schwachstellen besser zu verstehen.

Siehe Wird Hochgeladen Software Bill of Materials Dateien, die eine REST-API verwenden Weitere Informationen zu (POST) und (GET) Parametern und URLs für die APIs „Upload“ und „Status“.

Domain Separation

Alle Tabellen in den SBOM-Anwendungen sind domänengetrennt.

Klassifizieren von Lizenzen und Auflösen von Komponentenlizenzen in Software Bill of Materials Arbeitsbereich

Klassifizieren Sie Lizenzen, und lösen Sie sie mit Komponenten ab (stimmen Sie sie ab), oder erstellen Sie Lizenzen im Lizenzverwaltungsmodul in SBOM Arbeitsbereich. Durch die Klassifizierung und den Abgleich von Lizenzen mit Ihren Komponenten können Sie Ihre Lizenz-Compliance für die proprietären, Open Source- und vom Lieferanten bereitgestellten Softwarekomponenten bestimmen, die Sie in hochladen SBOM Dateien.

Lizenzdaten und Software von Drittanbietern

Wenn Unternehmen mehr ihrer eigenen Softwareanwendungen erstellen, verwenden sie Open Source-Komponenten und vom Lieferanten bereitgestellte Software. Die Verwendung von Drittanbieter- und Open Source-Komponenten bietet viele Vorteile für die schnelle Erstellung und Veröffentlichung Ihrer Softwareprojekte. Die Verwendung dieser Komponenten birgt jedoch Lizenzierungsrisiken:

- Open Source- und vom Lieferanten bereitgestellte Softwarekomponenten haben manchmal Abhängigkeiten von anderen Komponenten, und jede Komponente kann eigene Lizenzierungsanforderungen haben.
- Wenn Sie die Bedingungen Ihrer Lizenzen für die Komponenten und Software in Ihren Anwendungen nicht einhalten, können Sie versehentlich Code versenden, der gegen Ihre internen Richtlinien und gesetzlichen Lizenzierungsanforderungen verstößt.

Das Lizenzverwaltungsmodul

Mit dem Lizenzverwaltungsmodul im SBOM-Arbeitsbereich können Sie die folgenden Aufgaben ausführen.

- Klassifizieren Sie Lizenzen, die dies für die Komponenten erfordern, die Sie mit hochladen SBOM Dateien.
- Lösen Sie jede Lizenz auf, die Sie für eine bestimmte Komponente klassifizieren.
- Sehen Sie sich in einer Datenvisualisierung auf der Homepage an, welcher Prozentsatz der von Ihnen verwendeten Komponenten nicht konform ist. Sie können diese Informationen verwenden, um Ihre allgemeine Sicherheitslage und das potenzielle Risiko zu bestimmen.

Wenn SBOM Dateien, die Sie hochladen, enthalten Lizenzinformationen. Die Lizenzdatenbank wächst automatisch, wenn bei jedem SBOM-Upload eindeutige Lizenzen beobachtet werden. Mit jedem SBOM-Upload können Sie eine Datenbank hochgeladener Lizenzen erstellen und sie dann bei Bedarf mit dem Lizenzverwaltungsmodul in klassifizieren SBOM Arbeitsbereich. Sie erstellen einen Bestand von Lizenzen, um sie Komponenten zuzuweisen, nachdem Sie sie in eine der folgenden Kategorien klassifiziert haben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zulässig
- Beschränkt
- Gesperrt
- Nicht klassifiziert

Juristische Mitarbeiter, Lizenzmanager, Compliance- und regulatorische Manager führen Aufgaben im Lizenzverwaltungsmodul aus.

Hochgeladene Lizenzdaten werden angezeigt

Sie haben die folgenden Optionen, um Lizenzinformationen anzuzeigen, die Sie mit Ihren Komponenten im SBOM-Arbeitsbereich hochgeladen haben.

- Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich** > **Komponenten**an.

  Auf der Seite „Komponenten“ zeigt die Karte Lizenzklassifizierung von Komponenten eine Visualisierung Ihrer allgemeinen Lizenz-Compliance mit den folgenden Kategorien an.

Kategorie	Beschreibung
Gesperrt	Lizenzierte Nutzung ist nicht zulässig.
Klassifizierung erforderlich	Die Lizenz ist noch nicht klassifiziert und erfordert eine Überprüfung.
Zulässig	Die lizenzierte Nutzung ist ohne Einschränkung zulässig.
Beschränkt	Die lizenzierte Nutzung ist in bestimmten Anwendungsfällen nicht zulässig.

  Dieser Snapshot verwendet die Klassifizierungen und gelösten Lizenzinformationen, die Sie im Lizenzverwaltungsmodul eingeben, um Ihre allgemeine Lizenz-Compliance zu berechnen.

  Wenn Sie einen Komponentendatensatz aus dieser Liste auswählen, können Sie die Lizenzinformationen der Komponente zusammen mit anderen Informationen im Feld Status anzeigen.

- Alternativ navigieren Sie zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich** > **Lizenzverwaltung** > **Lizenzklassifizierung**an.

  Auf dieser Seite wird die Gesamtzahl der eindeutigen Lizenzen nachverfolgt, die aus den von Ihnen hochgeladenen SBOM-Dateien erkannt wurden. Sie werden auch in Karten oben auf der Seite in den folgenden Kategorien gefiltert.

  - Nicht klassifiziert: Lizenz erfordert Überprüfung und Klassifizierung.
  - Gesperrt: Die Lizenznutzung ist nicht zulässig.
  - Eingeschränkt: Lizenz ist in bestimmten Anwendungsfällen nicht zulässig.
  - Zulässig: Die Lizenznutzung ist ohne Einschränkung zulässig.
  - Alle Lizenzen: Gesamtanzahl der Lizenzen.

  Alle Komponenten in Ihrer Organisation verwenden eine der auf dieser Seite aufgeführten Lizenzen. Wenn eine neue Lizenz aus einem SBOM-Upload erkannt wird, wird ein Datensatz erstellt, in der Tabelle „SBOM-Lizenz“ [sn_sbom_license] gespeichert und dieser Liste hinzugefügt. Die Klassifizierung ist standardmäßig, **Klassifizierung**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderlich . Lizenzdatensätze in diesem Status müssen überprüft und klassifiziert werden, bevor Sie sie mit Komponenten auflösen (abgleichen) können, damit Ihre allgemeine Lizenz-Compliance genau berechnet wird.

Informationen zum Klassifizieren von Lizenzen finden Sie unter Klassifizieren Sie importierte Lizenzen in Software Bill of Materials Arbeitsbereich.

Rollen

Neue Lizenzen müssen von einem Anwender mit der Rolle „sn_sbom_response.managelicense“ klassifiziert werden. Dieser Anwender zeigt hochgeladene Lizenzinformationen an und bestimmt, welche Lizenzen zulässig und welche gesperrt sind. Anwender mit dieser Rolle können das Modul zur Komponentenlizenzauflösung nur anzeigen, wenn sie über die Rolle sn_sbom_response.licenseresolver verfügen.

Nach der Klassifizierung müssen Lizenzen von einem Anwender mit der Rolle „sn_sbom_response.licenseresolver“ gelöst werden, damit Ihre allgemeine Lizenz-Compliance ermittelt werden kann. Dieser Anwender löst Lizenzen in Komponenten auf. Anwender mit dieser Rolle können das Lizenzklassifizierungsmodul nur anzeigen, wenn sie über die Rolle sn_sbom_response.managelicense verfügen.

Die Klassifizierung neuer Lizenzinformationen ist ein laufender Prozess. Möglicherweise möchten Sie die auf der nicht klassifizierten Karte angezeigte Gesamtzahl niedrig lassen. Als Lizenzmanager sollten Sie alle paar Tage und nach dem Hochladen von SBOM-Dateien nach Lizenzen suchen, die klassifiziert werden müssen.

Als Lizenz-Resolver sollten Sie möglicherweise alle paar Tage nach aktualisierten klassifizierten Lizenzen suchen.

Klassifizieren Sie importierte Lizenzen in Software Bill of Materials Arbeitsbereich

Klassifizieren Sie die Komponentenlizenzen, die Sie mit hochladen SBOM Dateien mit der Lizenzklassifizierungsfunktion.

Vorbereitungen

Die Klassifizierung neuer Lizenzinformationen ist ein laufender Prozess. Möglicherweise möchten Sie die auf der nicht klassifizierten Karte angezeigte Gesamtzahl niedrig lassen. Als Lizenzmanager sollten Sie alle paar Tage und nach dem Hochladen von SBOM-Dateien nach Lizenzen suchen, die klassifiziert werden müssen.

Erforderliche Rolle: sn_sbom_response.managelicense

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich** > **Lizenzverwaltung** > **Lizenzklassifizierung**an.

   Hinweis:
   Sofern Sie nicht auch über die Rolle sn_sbom_response.licenseresolver verfügen, ist nur die Registerkarte Lizenzklassifizierung sichtbar.

2. **Wahlweise:** Wählen Sie eine Karte aus, um Lizenzen nach ihren Klassifizierungen zu filtern.
3. Wählen Sie eine aus, um Lizenzen zu klassifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Nachdem Sie Lizenzen klassifiziert haben, sind Sie bereit für Lösen Sie klassifizierte Lizenzen in Komponenten auf .

Lösen Sie Lizenzen für Komponenten in auf Software Bill of Materials Arbeitsbereich

Lösen (weisen) Sie klassifizierte Lizenzen bestimmten Komponenten mit der Funktion Komponentenlizenzlösung zu. Weisen Sie Komponenten mit fehlenden Informationen oder falschen Lizenzinformationen Lizenzen zu, oder erstellen Sie neue Lizenzen, damit Ihre allgemeine Lizenz-Compliance berechnet werden kann.

Vorbereitungen

Erforderliche Rolle: sn_sbom_response.licenseresolver

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich** > **Lizenzverwaltung** > **Komponentenlizenzlösung**an.

   Hinweis:
   Sofern Sie nicht auch über die Rolle sn_sbom_response.managelicense verfügen, ist nur die Registerkarte Komponentenlizenzlösung sichtbar.

   Auf dieser Seite wird die Gesamtzahl der eindeutigen Lizenzen und eine Übersicht der Lizenzsummen nachverfolgt, die in den von Ihnen hochgeladenen SBOM-Dateien erkannt wurden. Lizenzen, die auf dieser Seite angezeigt werden, fallen in zwei allgemeine Kategorien, da sie sich auf Komponenten beziehen.

   - Alle Instanzen der Komponente stimmen einer Lizenz zu.
   - Es besteht eine Meinungsverschiedenheit über eine einzelne Lizenz, und es gibt mehr als eine Lizenz für eine Komponente.

   Im zweiten Fall müssen Sie diese Lizenzen abgleichen, damit eine einzelne Lizenz zu einer einzelnen Komponente aufgelöst wird. Die Lizenz-Compliance wird basierend auf einer gelösten Lizenz pro Komponente berechnet.

   Die Lizenzen auf dieser Seite werden in die folgenden Kategorien gefiltert, damit Sie sie lösen können.

Wert	Beschreibung
Komponenten mit nicht aufgelösten Lizenzen	Der Komponente ist keine Lizenz zugewiesen und erfordert eine Lösung. (Leer) Wird in der Spalte „aufgelöste Lizenz“ für diese Komponenten angezeigt. Sowohl fehlende als auch mehrere Lizenzen werden als Teil dieser Kategorie aufgeführt.
Komponenten mit fehlenden Lizenzen.	Komponenten mit fehlenden Lizenzinformationen, die eine Lösung erfordern.
Komponenten mit mehreren Lizenzen	Komponenten, die für mehrere Entitäten sichtbar sind, die unterschiedliche Lizenzen haben und eine Lösung erfordern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert	Beschreibung
Alle Komponenten	Gesamtliste der Komponenten, die in Ihrer Organisation nachverfolgt werden. Sie können Lizenzen aus dieser gefilterten Liste ändern.

2. Wählen Sie eine Karte aus.
3. Wählen Sie eine aus, um eine Lizenz aufzulösen.

4. Navigieren Sie zur Homepage im SBOM-Arbeitsbereich, um zu sehen, welcher Prozentsatz der von Ihnen verwendeten Komponenten nicht konform ist, in der Visualisierung der Lizenzklassifizierung von Komponenten.
   Die Daten für diese Visualisierung werden täglich durch die geplante Aufgabe „Lizenzaufgliederung“ der Stücklistenkomponenten aktualisiert. Dieser Auftrag ist Teil der geplanten Aufgabe „SBOM-Berichte – Datensammler“, die täglich ausgeführt wird.

Berichte und Dashboards in anzeigen Software Bill of Materials Arbeitsbereich

Schwachstellenanalysten zeigen hochgeladene Software-Stücklistendateien in Datensätzen, Datenvisualisierungen sowie erweiterte Schwachstelleninformationen in an Software Bill of Materials(SBOM) Arbeitsbereich.

SBOM Zentral

Sie können Stücklistenentitäten und eine Liste der Komponenten anzeigen, die Sie auf der Startseite (Zielseite) und im Komponentenmodul in hochgeladen haben SBOM Arbeitsbereich.

SBOM Antwort

Die SBOM Die Antwortanwendung bietet Ihnen Datenvisualisierungen mit detaillierten Informationen zu Stücklistenentitäten, Entitäten mit Schwachstellen und aktiven angreifbaren Anwendungselementen auf der Startseite (Zielseite) in SBOM Arbeitsbereich. Der Arbeitsbereich mit SBOM Antwort enthält die folgenden Module:

- Homepage – Datenvisualisierungen und erweiterte Schwachstellendetails.
- Komponenten: Versions- und Korrekturinformationen für Komponenten und Lizenzklassifizierung von Komponenten .
- Erstellungsregeln FÜR AVIT (angreifbares Anwendungselement): Bedingungen, unter denen angreifbare Anwendungselemente (AVITs) erstellt werden.
- Stücklistenwarteschlange: Status und Verlauf des Dateiupload.
- Liste: AVIT-Datensätze für Ihre angreifbaren Komponenten und Bibliotheken (NVD, CWE und Anwendungsschwachstellen).

Die folgenden Themen enthalten weitere Informationen darüber, wie Sie Details zu Ihren Komponenten in finden Software Bill of Materials Arbeitsbereich.

- Überprüfen Sie die Homepage in Software Bill of Materials Arbeitsbereich
- Überprüfen des Moduls „Komponenten“ in Software Bill of Materials Arbeitsbereich
- Zeigen Sie den Upload-Status für an Software Bill of Materials Dateien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überprüfen von Software Bill of Materials Entität für Schwachstellen
- Klassifizieren von Lizenzen und Auflösen von Komponentenlizenzen in Software Bill of Materials Arbeitsbereich

Überprüfen Sie die Homepage in Software Bill of Materials Arbeitsbereich

Hochgeladene Daten werden zu den Visualisierungen auf der Zielseite (Homepage) in zusammengefasst Software Bill of Materials(SBOM) Arbeitsbereich. Die Daten werden geändert, nachdem Sie Dateien hochgeladen haben, damit Schwachstellenanalysten Trends sehen und aktuelle Informationen zu Ihren Komponenten überprüfen können.

Vorbereitungen

Erforderliche Rollen: sn_sbom_resp.sbom_Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich**an.
   Standardmäßig wird die Zielseite (Startseite) angezeigt.

   Was Sie im Modul sehen können, hängt von den von Ihnen installierten Anwendungen ab.

   Importierte Daten werden nicht berechnet und durch Live-Abfragen ausgefüllt. Punktzahlen auf den Seiten „Startseite“ und „Komponenten“ werden einmal täglich mit Leistungsverbesserungen für die Berichterstellung aktualisiert. Diese Erweiterung bietet möglicherweise schnellere Ladezeiten für die Bewertungslisten in den Modulen „Startseite“ und „Komponenten“ in SBOM Arbeitsbereich.

   Diese Erweiterungen haben keine Auswirkungen darauf, wie oder wo Daten gespeichert werden.

Installierte Anwendung	Beschreibung
Wenn Sie installiert haben SBOM Kern	Alle Stücklistenentitäten. Die Liste enthält den Namen, den Klassifizierer (Anwendung, Container, Bibliothek usw.) und die Komponentenanzahl für jede Entität. Eine Stücklistenentität bezieht sich auf die Komponente auf Stammebene in einem SBOM Datei, für die ein SBOM Dokument wurde generiert und hochgeladen. Navigieren Sie im Arbeitsbereich zur Homepage Zum Anzeigen der Liste der Stücklistenentitäten.
Wenn Sie installiert haben SBOM Antwort	Die folgenden Datenvisualisierungen werden angezeigt. ○ Alle Stücklistenentitäten: Eine Aufgliederung der Stücklistenentitäten nach Typ: Anwendung, Container, Bibliothek und andere. Eine Stücklistenentität bezieht sich auf die Komponente auf Stammebene in einem SBOM Datei, für die ein SBOM Dokument wurde generiert und hochgeladen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Anwendung	Beschreibung
	○ Stücklistenentitäten mit Schwachstellen: Entitäten, denen eine Schwachstelle einer Komponente zugeordnet ist, von der sie abhängig sind. Wenn eine Entitätsabhängigkeit eine hat **Kritisch** Schwachstelle: Der Schweregrad der Entität wird als kritisch betrachtet. ○ Aktive Avis: Der Trend für die Anzahl der täglich erstellten angreifbaren Anwendungselemente (AVI). Die Datenvisualisierungen zeigen Daten für die letzten 30 Tage an. Der 30-Tage-Bereich kann nicht bearbeitet werden. Diese Daten sind verfügbar, nachdem Sie die Erstellungsregeln für angreifbare Anwendungselemente überprüft und eingerichtet haben. Weitere Informationen finden Sie unter Erstellen von Regeln für angreifbare Anwendungselemente in Software Bill of Materials Arbeitsbereich.

2. Wählen Sie eine Datenvisualisierungskarte aus, um die Liste der Datensätze anzuzeigen.
3. Wählen Sie aus **Startseite** Registerkarte, um zur Zielseite zurückzukehren.
4. Alternativ wählen Sie aus Ein Datensatz unter **Stücklistenentitäten** Liste.

   Der Entitätsname und die Version werden oben im Datensatz angezeigt, z. B. SNC-SECOPS-SIR2.0 .

   Hinweis:
   Mit dem Lizenzverwaltungsmodul wird die Entität-Lizenz-Beziehung in dieser Liste nicht angezeigt. Um die Entitäten anzuzeigen, in denen eine Komponente verwendet wird, navigieren Sie zum Komponentenmodul, und öffnen Sie einen Komponentendatensatz. Im Komponentendatensatz können Sie den Status „nicht gelöst“ oder „nicht klassifiziert“ anzeigen.

5. Wählen Sie die Registerkarten im Entitätsdatensatz aus, um die Daten zu überprüfen.

   a. Wenn nicht ausgewählt, wählen Sie aus **Übersicht** Registerkarte.

   Überprüfen Sie die Daten. Wenn in diesem Datensatz kein Feld ausgefüllt ist, wurden die Daten nicht in eingeschlossen SBOM Dateien, die Sie hochgeladen haben.

Name	Beschreibung
Name	Entitätsname.
Klassifizierer	Entitätstyp, z. B. eine Anwendung, Komponente oder Bibliothek.
Version	Versionsnummer der Entität.
Lieferant	Das Produkt, das die Entität bereitgestellt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Produktmodell	Wenn kein Produktmodell vorhanden ist oder Sie keines zum Zeitpunkt Ihres einbeziehen SBOM Laden Sie über die API hoch, eine wird erstellt. Der Name der Entität wird beispielsweise für den Produktmodelldatensatz verwendet SNC-SECOPS-SIR2.0 .

b. Wählen Sie aus **Abhängig von** Registerkarte.

Alle Abhängigkeiten dieser Entität sowie Klassifizierer werden aufgelistet, z. B. Bibliothek . Die Versionsnummer, Lizenzen , Und andere Informationen werden angezeigt.

Wenn Sie einen Link in dieser Liste auswählen, wird ein Datensatz geöffnet. Die Registerkarte wird unter den Registerkarten Startseite und Entitätsdatensatz angezeigt. Der von Ihnen geöffnete Datensatz enthält möglicherweise die folgenden zugehörigen Listen, die Sie überprüfen können: Übersicht, Hashes, Stücklistenentitäten, Schwachstellen und angreifbare Anwendungselemente (AVITs).

In der zugehörigen Liste Stücklistenentitäten werden alle Entitäten angezeigt, in denen dieses angezeigte Element verwendet wird.

c. Wählen Sie aus **Schwachstellen** Registerkarte, um die Schwachstellen anzuzeigen, die einer Abhängigkeit dieser Entität zugeordnet sind.

Weitere Informationen zu den für eine Entität angezeigten Schwachstellen finden Sie unter Zeigen Sie den Upload-Status für an Software Bill of Materials Dateien.

d. Wählen Sie aus **Avis** Registerkarte, um zu sehen, ob angreifbare Anwendungselemente für diese Entität vorhanden sind.

6. Wahlweise: Nachdem Sie Datensätze überprüft haben, können Sie einen oder mehrere Stücklistenentitätsdatensätze löschen, wenn Sie feststellen, dass Sie sie nicht mehr benötigen.

Hinweis:
Durch das Löschen von Stücklistenentitätsdatensätzen werden sie und ihre Komponentenbeziehungen dauerhaft entfernt. Alle angreifbaren Anwendungselemente (AVIT), die den Stücklistenentitäten zugeordnet sind, gehen zu über **Geschlossen** . Wenn Sie später entscheiden, dass die von Ihnen gelöschten Datensätze und Komponentenbeziehungen wieder in der Liste der Stücklistenentitäten enthalten und im Arbeitsbereich verfügbar sind, müssen Sie diese Stücklistenentitäten erneut hochladen.

a. Wenn nicht auf der Homepage, wählen Sie aus **Startseite** Registerkarte, um zu ihr zurückzukehren.

b. Wählen Sie die Datensätze unter aus **Stücklistenentitäten** Liste, die Sie löschen möchten.

c. Wählen Sie **Löschen**.

Überprüfen des Moduls „Komponenten“ in Software Bill of Materials Arbeitsbereich

Das Modul Komponenten in der Software Bill of Materials(SBOM) Arbeitsbereich zeigt aktuelle Informationen zu Kombinationen angreifbarer, veralteter, verworfener und risikoreicher Komponenten an, die Sie importieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul „Komponenten“ anzeigen

Erforderliche Rolle: sn_sbom_resp.sbom_Analyst

Navigieren zu **Arbeitsbereiche** > **SBOM-Arbeitsbereich** > **Komponenten**an.

Was Sie im Modul sehen können, hängt von den von Ihnen installierten Anwendungen ab.

Importierte Daten werden nicht berechnet und durch Live-Abfragen ausgefüllt. Punktzahlen auf den Seiten „Startseite“ und „Komponenten“ werden einmal täglich mit Leistungsverbesserungen für die Berichterstellung aktualisiert. Diese Erweiterung bietet möglicherweise schnellere Ladezeiten für die Bewertungslisten in den Modulen „Startseite“ und „Komponenten“ in SBOM Arbeitsbereich.

Diese Erweiterungen haben keine Auswirkungen darauf, wie oder wo Daten gespeichert werden.

Installierte Anwendung	Beschreibung
Wenn Sie installiert haben SBOM Kern	Ein Bestand aller hochgeladenen Komponenten, der die folgenden Informationen enthält: • Name • Beschreibung • Version • Anzahl der Stücklistenentitäten
Wenn Sie installiert haben SBOM Antwort	Wählen Sie ein Diagramm oder eine Zahl im Diagramm aus, um eine Liste der zugehörigen Datensätze anzuzeigen. **Alle Komponenten** Die Liste von **Veraltet** Und **Verworfen** Komponenten sowie Komponenten mit mindestens einer Schwachstelle in Ihrer Gesamtzahl der Komponenten. Diese Anzahlen können Ihnen helfen, Komponenten zu identifizieren, die Ihre Aufmerksamkeit erfordern. Diese Teilmengen von Komponenten stimmen möglicherweise nicht mit Ihrer Gesamtanzahl der Komponenten überein, da alle Ihre Komponenten möglicherweise nicht in diese Kategorien passen. • Die Version einer veralteten Komponente liegt mehr als zwei Hauptversionen hinter der neuesten Version und zwei Jahre hinter der neuesten Version.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Anwendung	Beschreibung
	• Eine verworfene Komponente wurde seit mehr als zwei Jahren nicht aktualisiert. • Angreifbare Komponenten sind Komponenten mit Schwachstellen mit einem Schweregrad von **Hoch** Oder größer. **Kombinationen mit hohem Risiko** Komponenten mit hohem Risiko erfordern möglicherweise sofortige Aufmerksamkeit. Die Deps.de-V-Integration, die bei der Installation von installiert wird SBOM Antwortanwendung, stellt die Paketintelligenz für Komponenten in bereit **Veraltet** Und **Verworfen** status. Importierte Kombinationen mit hohem Risiko bestehen aus veralteten und verworfenen Komponenten mit mindestens einer schwerwiegenden Komponente (**Kritisch** Oder **Hoch**) Schwachstelle, die Sie durch Updates, Ersatz oder eine andere Art von Reparatur beheben können. Die **Vollständig reparierbar** Status bedeutet, dass eine Komponente über eine verfügbare Version verfügt, die sie beheben kann. Der Prozentsatz der Gesamtzahl der Komponenten mit hohem Risiko, die korrigierbare Versionen haben, wird notiert. **Fixierbarkeit angreifbarer Komponenten** Gesamtsummen und Aufgliederungen der Komponenten mit **Kritisch** , **Hoch** , **Mittel** , Und **Niedrig** Schwachstellen und ob einige oder alle ihrer Schwachstellen behoben werden können. Wenn eine Komponente mehr als eine Schwachstelle aufweist, hat die kritischste Schwachstelle Vorrang. Der Korrekturstatus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Anwendung	Beschreibung
	• Abgeschlossen: Es gibt Korrekturversionen für alle Schwachstellen, die der aktuellen Version der Komponente zugeordnet sind. • Teilweise: Es gibt eine Korrekturversion für mindestens eine, aber nicht alle der aktuellen Version der Komponente zugeordneten Schwachstellen. **Lizenzklassifizierung von Komponenten** Gesamtsummen und Aufgliederungen von Komponenten nach ihren Lizenzklassifizierungen. In der Komponentenliste unter den Visualisierungen können Sie Name, Beschreibung, Version und Entitätsanzahlen anzeigen. Im rechten Bereich können Sie einen Versionsverlauf anzeigen. Die aktuelle Version wird im Versionsverlauf hervorgehoben. Die allgemeinen Schwachstellen und das Risiko (**CVE**) Und **Behebbarkeit** Spalten werden ebenfalls angezeigt.

Bewerten Sie Ihr Risiko mit Vulnerability Intelligence

Siehe Überprüfen von Software Bill of Materials Entität für Schwachstellen Weitere Informationen zum Überprüfen von Schwachstellen-Intelligence-Daten im Arbeitsbereich.

Bewerten Sie Ihr Risiko mit Lizenz-Compliance

Siehe Klassifizieren von Lizenzen und Auflösen von Komponentenlizenzen in Software Bill of Materials Arbeitsbereich Weitere Informationen zum Lizenzieren von Daten, die Sie importieren, mit Ihren Komponenten und zum Anzeigen Ihrer allgemeinen Lizenz-Compliance im Arbeitsbereich.

Erstellen von Regeln für angreifbare Anwendungselemente in Software Bill of Materials Arbeitsbereich

Bevor Sie angreifbare Anwendungselemente (AVITs) in der Software-Stückliste (SBOM) Arbeitsbereich müssen Sie die Bedingungen einrichten, unter denen AVITs erstellt werden.

AVITs in SBOM Arbeitsbereich

Wenn Sie installiert und aktiviert haben SBOM Antwortanwendung, für die AVITs erstellt werden SBOM Dateien, wenn eine der importierten Daten den Bedingungen Ihrer vorhandenen AVIT-Erstellungsregeln entspricht.

Die SBOM Antwort und Vulnerability Response Anwendungen sind erforderlich, um Regeln für die automatische Erstellung angreifbarer Anwendungselemente (AVITs) und deren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrektur mit einzurichten Application Vulnerability Response Workflow. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Als Anwender mit der Rolle „sn_sbom_resp.manage_avi_rule“ müssen Sie AVIT-Erstellungsregeln in hinzufügen SBOM Arbeitsbereich, bevor Sie AVITs für die in erfassten Schwachstellen erstellen können SBOM Daten. Mit AVITs können Sie die Integrität der Drittanbieterkomponenten in Ihren Anwendungen bewerten. Ein AVIT wird in Ihrer Instanz erstellt, wenn eine Anwendung mit einer Komponente abgeglichen wird, der eine Schwachstelle zugeordnet ist.

In SBOM Arbeitsbereich können Sie nur SBOM-AVITs anzeigen. Sie können jedoch anzeigen SBOM AVITs zusammen mit anderen Arten von angreifbaren Elementen im Vulnerability Manager-Arbeitsbereich in Vulnerability Response. Sie können alle AVITs anzeigen, die im SBOM-Arbeitsbereich im Listenmodul erstellt wurden. Das Listenmodul enthält auch alle NVD- und CWE-Einträge und Anwendungsschwachstellen.

Sie können AVITs auch basierend auf Empfehlungen aus bekannten Schwachstellenlisten wie der National Vulnerability Database (NVD) zuweisen. Eine geplante Aufgabe wird ausgelöst, und wenn die Bedingungen Ihrer Erstellungsregeln mit den erfassten Daten übereinstimmen, werden AVITs erstellt.

Sie können AVITs nachverfolgen und korrigieren, indem Sie anwenderdefinierte Regeln einrichten.

Siehe Erstellen Sie eine Regel für angreifbare Anwendungselemente in Software Bill of Materials Arbeitsbereich Informationen zum Erstellen einer Regel.

SBOM AVITs in Arbeitsbereich des Schwachstellenmanagers In Vulnerability Response

Sie können beliebig anzeigen SBOM AVITs, die in erstellt werden SBOM Arbeitsbereich in Arbeitsbereich des Schwachstellenmanagers Wenn Sie Zugriff darauf haben.

Hinweis:
Nur zum Anzeigen SBOM AVITs aus der Liste angreifbare Anwendungselemente in Arbeitsbereich des Schwachstellenmanagers Legen Sie die Bedingung anstelle aller AVITs fest **[Quelle] [ist] [SBOM] UND [Scan-Typ] [ist] [SBOM-SCA]** In der Tabelle „angreifbare Anwendungselemente“ [sn_vul_App_vulnerable_item]. Um die Tabelle anzuzeigen, navigieren Sie in Ihrer Instanz zu **Alle** Und geben Sie ein **sn_vul_App_vulnerable_item.list** Im Filternavigator.

Weitere Informationen zum Vulnerability Manager-Arbeitsbereich, zum Anzeigen von Überwachungsthemen, Anwendungskorrekturmaßnahmen und Anwendungskorrekturaufgabenregeln für AVITs, die über konfiguriert werden Vulnerability Response Anwendung in Arbeitsbereich des Schwachstellenmanagers, Siehe Verwenden Überwachungsthemen in Arbeitsbereich des Schwachstellenmanagers.

Korrekturaufgaben (AVULs) werden aus AVITs erstellt und basierend auf Ihren Zuweisungsregeln automatisch Gruppen zur Korrektur zugewiesen. Weitere Informationen zum Erstellen dieser Regeln finden Sie in den folgenden Themen:

- Erstellen oder bearbeiten Vulnerability Response Zuweisungsregeln
- Erstellen oder bearbeiten Vulnerability Response Regeln für Korrekturaufgaben und Erstellen Sie eine Korrekturmaßnahme in Arbeitsbereich des Schwachstellenmanagers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angreifbare Anwendungselemente in SBOM-Antwort werden erneut geöffnet

A **Geschlossen** Ein angreifbares Anwendungselement (AVIT) für eine Komponente mit einer zugehörigen Schwachstelle wird automatisch erneut geöffnet und in sichtbar SBOM Arbeitsbereich, wenn die folgenden Bedingungen vorhanden sind:

- Der AVIT mit der zugehörigen Schwachstelle wird von den Schwachstellen-Scans einer Drittpartei-Integration erneut erkannt, oder die Komponente mit der Schwachstelle ist Teil einer nachfolgenden SBOM Hochladen.
- Sie haben AVITs erneut öffnen, wenn erkannt (*sn_sbom_resp.reopen_avits_if_detected*) Systemeigenschaft. Diese Systemeigenschaft ist standardmäßig aktiviert.
- Der Substatus von **Geschlossen** AVIT ist keine der folgenden: **Minderungssteuerung vorhanden** , **Nicht Betroffen** , Oder **Falsch Positiv** . AVITs mit diesen Substatus werden von der Systemeigenschaft nicht erneut geöffnet.

Deaktivieren Sie diese Systemeigenschaft nur, wenn Sie dies nicht möchten **Geschlossen** AVITs zum automatischen erneuten Öffnen.

Zeigen Sie den Upload-Status für an Software Bill of Materials Dateien

Überprüfen Sie den Upload-Status für die Software-Stückliste (SBOM) Dateien, die Sie im Modul „Stücklistenwarteschlange“ in hochladen Software Bill of Materials(SBOM) Arbeitsbereich. Verfolgen Sie die Dateien, die Sie erfolgreich hochladen, Ihren Upload-Verlauf und Fehler nach.

Vorbereitungen

Erforderliche Rolle: sn_sbom_resp.sbom_Analyst

Prozedur

1. Zeigen Sie Ihren Upload-Status an.

   Die Methode, mit der Sie Ihren Upload-Status anzeigen, hängt von den von Ihnen installierten Anwendungen ab.

Option	Beschreibung
SBOM Zentral	**a.** Navigieren zu **Alle** > **SBOM-Core** > **Stücklisten-Erfassungsstatus**an. **b.** Überprüfen Sie in der Liste Stückliste die Spalten wie **Status** , **Stücklistengenerierungszeit** , Und **Erstellt** Spalten für Details.
SBOM Antwort	**a.** Navigieren zu **Alle** > **SBOM-Arbeitsbereich** > **Stücklisten-Warteschlange**an. **b.** Wählen Sie eine Visualisierungskarte aus, um die folgenden Details für die Kategorien Ihrer hochgeladenen Dateien zu überprüfen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	▪ Stücklistenaktualisierungen in den letzten 30 Tagen: Gesamtzahl der Stücklistenentitäten, die in den letzten 30 Tagen erfolgreich hochgeladen und analysiert wurden. ▪ Upload-Quelle: Gesamtzahl der erfolgreich hochgeladenen SBOM Dateien und eine Aufgliederung der zum Erfassen verwendeten Methoden (API oder manuell). ▪ Upload-Fehler nach Kategorie: Top-fünf-Kategorien von Upload-Fehlern. Wenn in dieser Visualisierung keine Daten angezeigt werden, sind alle Ihre SBOM Dateien erfolgreich hochgeladen.

Die Statusinformationen in der Tabelle „Stückliste“ [sn_sbom_doc_list] und im Modul „Stücklistenwarteschlange“ enthalten beide Stücklistenformate, Erfassungsstatus und Stücklistengenerierungszeit. Die Spalte Status für die Stücklistenerfassung enthält die folgenden status:

- In Warteschlange – SBOM Daten wurden hochgeladen.
- Verarbeitung: Die Komponentendaten werden als Teil des Imports verarbeitet.
- Verarbeitet: Die Datenerfassung wurde erfolgreich abgeschlossen.
- Fehler: Während der Verarbeitung ist ein Fehler aufgetreten.

Zusätzlich zum Status Ihrer hochgeladenen Dateien können Sie Listen von Komponenten anzeigen, die Sie erfasst haben, indem Sie einen Stücklistenentitätsdatensatz auswählen.

2. **Wahlweise:** Greifen Sie auf weitere Informationen zu Fehlern und Upload-Status zu, indem Sie das Zahnradsymbol wählen Und Hinzufügen von Feldern wie **Fehlerkategorie** Und **Fehlerdetail** .

Überprüfen von Software Bill of Materials Entität für Schwachstellen

Bestimmen Sie, ob den Komponenten in einem hochgeladenen Schwachstellen zugeordnet sind Software Bill of Materials(SBOM) Datei.

Die folgenden Anwendungen müssen installiert und aktiviert werden, bevor Sie die Schwachstellen und erweiterten Schwachstellendaten anzeigen können:

- SBOM Antwort
- Vulnerability Response-Integration mit NVD- und CWE-Aufträgen
- Vulnerability Response

Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Erforderliche Rolle: sn_sbom_resp.sbom_Analyst

1. Navigieren zu **Alle** > **SBOM-Arbeitsbereich** > **Komponenten**an.
2. Sie können Informationen zu Schwachstellen entweder über eine Visualisierung oder einen Komponentendatensatz anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Methode	Aktionen
Stücklistenentitäten mit Visualisierung von Schwachstellen	Wählen Sie aus **Stücklistenentitäten mit Schwachstellen** Visualisierungsdiagramm. ○ Wenn dieser Komponente Schwachstellen zugeordnet sind, werden die Summen in den Spalten CVE und CWE in der Liste angezeigt. Eine Komponente kann mehr als eine Schwachstelle aufweisen. Falls verfügbar, können Sie die Spalte Korrekturfähigkeit in dieser Liste auf Einträge überprüfen. ○ Wenn dieser Komponente keine Schwachstellen zugeordnet sind, werden diese Spalten angezeigt 0 Oder keine Werte für die Komponente. Wenn die Spalten CVE, CWE und Fixibilty nicht angezeigt werden, können Sie sie der Seite hinzufügen, indem Sie das Zahnradsymbol wählen Oben rechts auf der Seite und **Bearbeiten Sie Spalten** . Wählen Sie sie aus der Liste der verfügbaren Spalten aus, und wählen Sie aus **OK** .
Komponentendatensatz	**a.** Wählen Sie einen Datensatz aus der Liste unter den Visualisierungen aus. **b.** Wählen Sie aus **Schwachstellen** Registerkarte im Datensatz. **i.** Wenn keine Daten angezeigt werden, sind dem Datensatz keine gemeldeten Schwachstellen zugeordnet. **ii.** Informationen zur Anzeige von Daten finden Sie unter Überprüfen des Moduls „Komponenten“ in Software Bill of Materials Arbeitsbereich Und befolgen Sie die Schritte im Korrektur-Workflow für Application Vulnerability Response Um die Schwachstelle zu beheben. Weitere Informationen finden Sie unter Wird Korrigiert Application Vulnerability Response Schwachstellen.

Bewerten Sie Ihr Risiko mit Vulnerability Intelligence

Zeigen Sie mit erweiterte Schwachstellendaten an SBOM Antwort auf Komponentendatensätze. Die SBOM Geplante Aufgaben der Antwortanwendung, Vulnerability Response, Integration der National Vulnerability Database (NVD) und Common

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weakness Enumeration (CWE), die in beschrieben werden Unterstützte Anwendungen Muss installiert und aktiviert sein.

1. Wählen Sie aus **Alle Komponenten** Visualisierung, um die Liste der zugehörigen Datensätze anzuzeigen.
2. Wählen Sie einen Link in aus **Name** Spalte zum Öffnen eines Datensatzes.

   Die Status, **Veraltet** , **Verworfen** , Und **Angreifbar** Werden unter dem Komponentennamen angezeigt. Eine Komponente kann eine beliebige Kombination dieser status aufweisen. Wenn kein Status angezeigt wird, ist die Komponente nicht veraltet, verworfen oder angreifbar.

   Überprüfen Sie die aktuelle Version und die neueste veröffentlichte Version. Im rechten Bereich können Sie einen Versionsverlauf anzeigen. Die aktuelle Version wird im Versionsverlauf hervorgehoben, und ihr Speicherort in der Liste bietet Ihnen möglicherweise Einblicke in die Gründe für eine Komponente **Veraltet** , **Verworfen** , Und **Angreifbar** . Beispielsweise verwenden Sie möglicherweise eine ältere Version einer Komponente.
3. Wählen Sie aus **Übersicht** , **Hashes** , **Stücklistenentitäten** , **Schwachstellen** , Und **Avis** Zugehörige Registerkarten im Datensatz.
   - Übersicht: Eine Zusammenfassung der Komponentendetails.
   - Stücklistenentitäten: Eine Liste der Entitäten, die dieser Komponente zugeordnet sind.
   - Hashes: Wenn importiert, werden Hashes angezeigt.
   - Schwachstellen: Informationen zu bekannten Schwachstellen, die dieser Komponente zugeordnet sind. Wenn diese Liste leer ist, sind keine Schwachstellen bekannt.

     Wenn die Liste ausgefüllt ist, wählen Sie die Registerkarte aus, um Schwachstellen-IDs, Zusammenfassungen und andere Schwachstellen-Informationen für Common Vulnerabilities and Exposures (CVE) und Common Sschwäche Enumeration (CWE) anzuzeigen, die diesem Datensatz zugeordnet sind. CVEs werden nach Schweregrad aufgeschlüsselt, CWEs werden danach aufgeschlüsselt, wie wahrscheinlich die Komponente ausgenutzt werden kann. Sie können die erweiterten Schwachstellendatensätze in anzeigen Vulnerability Response Oder Application Vulnerability Response Anwendungen, indem Sie den Link Schwachstellen-ID auswählen.
   - Avis (AVITs): Angreifbare Anwendungselemente, die dieser Komponente zugeordnet sind, wenn Sie AVIT-Erstellungsregeln erstellt haben, die die Komponente mit einer bekannten Schwachstelle abgleichen. Die Anwendung Application Vulnerability Response (AVR) verknüpft eine Schwachstelle mit einer Anwendung, um einen AVI-Datensatz zu erstellen. Weitere Informationen finden Sie unter Erstellen von Regeln für angreifbare Anwendungselemente in Software Bill of Materials Arbeitsbereich.

Mit installierte Komponenten Software Bill of Materials Anwendungen

Bei der Aktivierung von werden verschiedene Arten von Komponenten installiert Software Bill of Materials Anwendungen, einschließlich Tabellen, Anwenderrollen und geplante Aufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_sbom_response.managelicense	Diese Rolle wird mit installiert SBOM Antwortanwendung. Mit dieser Rolle können Sie Lizenzen für Komponenten auflösen.	Keine
sn_sbom_response.licenseresolver	Diese Rolle wird mit installiert SBOM Antwortanwendung. Mit dieser Rolle können Sie hochgeladene Lizenzinformationen anzeigen und bestimmen, welche Lizenzen zulässig und welche gesperrt sind.	Keine
SBOM Schreiben [sn_sbom_dm.App_write], SBOM[sn_sbom_dm.App_create] erstellen, SBOM Lesen [sbom_dm.App_read]	Diese Rollen werden mit dem Datenmodell für installiert SBOM Anwendung. Sie ermöglichen es Ihnen, Datensätze in zu lesen, zu erstellen und zu bearbeiten SBOM Tabellen.	Keine
SBOM Kerne erfassen [sn_sbom_Core.sbom_ingest] und SBOM Core-Administrator [sn_sbom_Core.admin]	Diese Rollen werden mit installiert SBOM Kernanwendung. Mit der Rolle sn_sbom_Core.sbom_ingest können Sie SBOMs manuell und über die REST API hochladen. Mit der Rolle sn_sbom_Core.admin können Sie SBOMs erstellen, lesen, bearbeiten und hochladen. Mit dieser Rolle erhalten Sie auch Zugriff auf SBOM Kernmodule in Ihrer Instanz. Er erbt die Rollen vom Datenmodell für SBOM Anwendung.	• sn_sbom_dm.App_write • sn_sbom_dm.App_create • sn_ sbom_dm.App_read

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
SBOM-Analyst [sn_sbom_Resp.sbom_Analyst]	Diese Rolle wird mit installiert SBOM Antwortanwendung. Er erbt die Rolle sn_sbom_Core.admin und ermöglicht Ihnen den Zugriff auf SBOM Arbeitsbereich.	• sn_sbom_Core.admin • sn_sbom_dm.App_write • sn_sbom_dm.App_create • sn_ sbom_dm.App_read • sn_sbom_Resp.Manage_avi_rule • Tabelle „sn_sbom_config_rule“

Mit installierte Tabellen SBOM Anwendungen

Die in der folgenden Tabelle aufgeführten Tabellen werden mit dem Datenmodell für installiert SBOM Anwendung.

Datenmodell für SBOM Tabellen

Tabelle	Beschreibung
SBOM Dokument [sn_sbom_doc]	Enthält die Stücklistenentitäten, die Sie hochgeladen haben.
SBOM Komponente [sn_sbom_component]	Enthält importiert SBOM Komponenten, Klassifizierer und Versionen, die in der übergeordneten Komponente enthalten sind.
SBOM Komponentenbeziehung [sn_sbom_comp_Relationship]	Enthält Komponenten und ihre Abhängigkeiten.
SBOM m2m-stücklistenkomponente [sn_sbom_m2m_bom_comp]	Enthält die Zuordnungen der Stücklistenkomponente.
SBOM-Lizenz [sn_sbom_license]	Enthält die Open Source-Lizenz-IDs, die für Komponenten verwendet werden.
SBOM Lieferant [sn_sbom_Supplier]	Enthält die Organisation, die die Komponente bereitgestellt hat, bei der es sich um einen Hersteller, einen Händler oder einen Umpacker handeln kann.
SBOM Komponenten-ID [sn_sbom_comp_ID]	Enthält die Komponentenbezeichner.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenmodell für SBOM Tabellen (Fortsetzung)

Tabelle	Beschreibung
SBOM Komponenteneigenschaften [sn_sbom_comp_property]	Enthält die Name-Wert-Eigenschaften der Komponente.
SBOM Hash [sn_sbom_hash]	Enthält Komponenten-Hashing-Algorithmen.
SBOM Kontakt [sn_sbom_contact]	Enthält Kontaktinformationen für den Lieferanten.
SBOM Externe Referenzen [sn_sbom_comp_external_ref]	Enthält Komponenten, Komponententypen und externe URLs, die Systeme, Sites und Informationen dokumentieren, die möglicherweise relevant sind, aber nicht im enthalten sind SBOM.
SBOM Paketgruppe [sn_sbom_pkg_Group]	Enthält die Paketgruppeninformationen für jede Komponente. Mehrere Versionen von Bibliotheken können anwendungsübergreifend verwendet werden. Versionen derselben Komponenten werden gruppiert und dieser Tabelle hinzugefügt, um zu vermeiden, dass dieselben Daten mehrmals abgerufen werden.

Die in der folgenden Tabelle aufgeführten Tabellen werden mit installiert SBOM Antwortanwendung

SBOM Antworttabellen

Tabelle	Beschreibung
SBOM Konfiguration der Erstellungsregel [sn_sbom_config_rule]	Enthält AVIT-Erstellungsregeln, die in verwendet werden SBOM Arbeitsbereich.
SBOM Schwachstellen der m2m-Komponente [sn_sbom_m2m_comp_vuln]	Enthält die Komponenten und zugehörigen Schwachstellen.
Informationen zur Korrektur von Schwachstellen für Komponente [sn_sbom_comp_vuln_fix_info]	Enthält die Korrekturversionen für jede Drittpartei-Schwachstelle, die einer Version der Komponente zugeordnet ist.
Einblicke in Komponentenberichte [sn_sbom_comp_Report_Insight]	Enthält Einblicke zu veralteten, verworfenen und Korrekturdaten für Komponenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SBOM Antworttabellen (Fortsetzung)

Tabelle	Beschreibung
Deps-Integrationsimporte [sn_sbom_deps_Integration_Import]	Enthält importierte Versionslisteninformationen für ein bestimmtes Paket oder eine bestimmte Bibliothek.
OSV-Integrationsimporte [sn_sbom_osv_Integration_Import]	Enthält Schwachstellen-Intelligence-Informationen für eine bestimmte Version eines Pakets oder einer Bibliothek.
Komponentenversionslisten [sn_sbom_St_Version_list]	Enthält Versionsinformationen und Veröffentlichungsdaten für Komponenten.

Geplante Aufgaben

Auftrag	Beschreibung
Berechnen Sie Komponentenreparatur und Schwachstelle	Berechnet Informationen darüber, wie Komponenten mit Schwachstellen behoben werden können und wie wahrscheinlich es ist, dass Sie Komponenten beheben können.
OSV-Integration – neue Komponenten	Ruft alle öffentlich bekannten Schwachstellen ab, die Paketen (Bibliotheken) zugeordnet sind, die nach der letzten Integrationsausführung importiert wurden.
OSV-Integration umfassend	Ruft alle öffentlich bekannten Schwachstellen ab, die allen Paketen zugeordnet sind, die importiert wurden.
Deps.dev-Integration	Ruft alle öffentlich bekannten Versionen für Pakete ab, die mit zum Identifizieren von Komponenten in verwendet werden **Veraltet** Und **Verworfen** status.
Aktualisieren Sie „vuln_based_Critizality“ für stücklistenkomponenten	Aktualisiert die Relevanz für Komponenten mit Schwachstellen.

Erstellen Sie eine Regel für angreifbare Anwendungselemente in Software Bill of Materials Arbeitsbereich

Richten Sie die Bedingungen ein, unter denen angreifbare Anwendungselemente (AVITs) automatisch im Modul „AVI-Erstellungsregeln“ in erstellt werden Software Bill of Materials(SBOM) Arbeitsbereich.

Vorbereitungen

Die SBOM Antwortanwendung ist erforderlich, wenn Sie angreifbare Anwendungselemente erstellen möchten. Weitere Informationen finden Sie unter Software Bill of Materials erkunden.

Erforderliche Rolle: sn_sbom_resp.manage_avi_rule.

Prozedur

1. Navigieren zu **SBOM-Arbeitsbereich** > **AVI-Erstellungsregeln**an.
2. Wählen Sie **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die Felder aus.

Feld	Beschreibung
Name	Name der Regel.
Aktiv	Gibt an, ob die Erstellungsregel aktiviert ist.
Ausführungsreihenfolge	Reihenfolge, in der die Regeln ausgewertet werden. Die Regel mit dem niedrigsten numerischen Wert wird zuerst ausgeführt. Sie können beispielsweise Regeln mit höherer Priorität für Elemente erstellen, die eine besondere Behandlung erfordern oder bei denen das Risiko kritisch ist, damit sie zuerst ausgeführt werden. Erstellen Sie als Nächstes allgemeine Regeln für Elemente, die keine spezielle Behandlung erfordern. Erstellen Sie abschließend eine Standardregel, um alle Komponenten mit Schwachstellen zu erfassen.
Beschreibung	Beschreibung der Regel, damit Sie sie von anderen Regeln unterscheiden können.
Bedingungen	Erstellen Sie die Bedingungen, unter denen angreifbare Anwendungselemente (Avis) erstellt werden. Sie können beispielsweise auswählen **[Schwachstelle > Schweregrad][ist][1-Kritisch]** Dient zum Erstellen von AVITs für Komponenten mit Schwachstellen, die ein hohes Risiko darstellen und sich ernsthaft auf Sie auswirken könnten. Beachten Sie, dass Sie weitere Bedingungen hinzufügen können.

4. Wählen Sie **Speichern**.
Ihre Erstellungsregel wird nach dem nächsten Upload automatisch ausgeführt und erstellt Avis für Komponenten, die Ihren Bedingungen entsprechen. Sie können die Regel auch bei Bedarf über das AVI-Erstellungsregeln-Modul ausführen, indem Sie auswählen **Jetzt Ausführen** .

Ergebnisse

Nachdem sie erstellt wurden, können Sie überprüfen, ob speziell für eine AVIT erstellt wurde SBOM Daten durch Überprüfen der Werte in **Quelle** Und **Scan-Typ** Felder in einem AVI-Datensatz.

Feld	Wert
Quelle	SBOM
Überprüfungstyp	SBOM-SCA

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

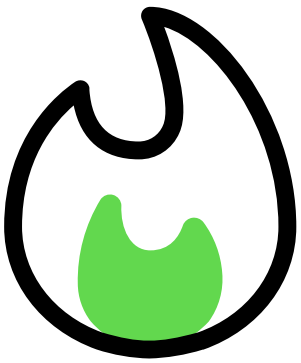
Enterprise Security Case Management-Anwendungen

Enterprise Security Case Management-Anwendungen umfassen Security Incident Response, Eine Lösung für Sicherheits-Orchestration und Automatisierungsantwort (SOAR), mit der Sie schnell auf sich entwickelnde Bedrohungen reagieren und gleichzeitig Sicherheitsvorgänge in Unternehmen optimieren und orchestrieren können. Es beseitigt Fehler und Reibungen, die bei manuellen Übergaben über Systeme, Teams und Verantwortlichkeiten hinweg inhärent sind.

Erste Schritte

Folgendes Security Incident Response Anwendungen sind mit separaten Abonnements von verfügbar ServiceNow® Store. Siehe Security Operations Und ServiceNow Store Weitere Informationen dazu, wie Sie Apps suchen, Berechtigungen abrufen und auf Ihre Instanz herunterladen.

Security Incident Response



Erfahren Sie mehr über die Anwendung Security Incident Response

Management schwerwiegender Sicherheits-Incidents

Erfahren Sie mehr über die Anwendung Management schwerwiegender Security Incidents

Threat Intelligence

Erfahren Sie mehr über die Anwendung Threat Intelligence

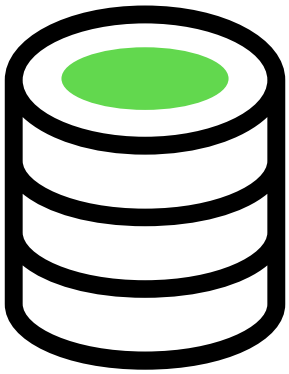
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence-Sicherheitszentrum

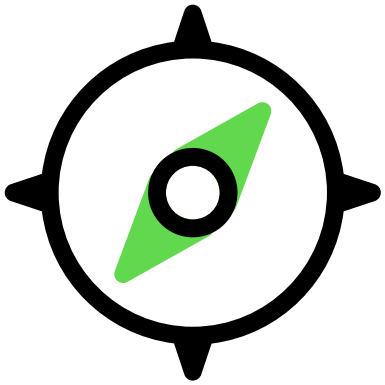
Erfahren Sie mehr über die Anwendung Threat Intelligence Security Center

Reaktion auf Incident zur Vermeidung von Datenverlust



Erfahren Sie mehr über die Anwendung zur Vermeidung von Datenverlust

Gemeinsam genutzte Funktionen von Security Incident Response-Anwendungen



Erfahren Sie mehr über die Funktionen, die von den Security Incident Response-Anwendungen gemeinsam genutzt werden

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Security Incident Response

Die ServiceNow® Security Incident Response Die Anwendung verfolgt den Fortschritt von Security Incidents von der Erkennung und ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur abschließenden Überprüfung nach Incident, Erstellung und Abschluss von Knowledge Base-artikeln.

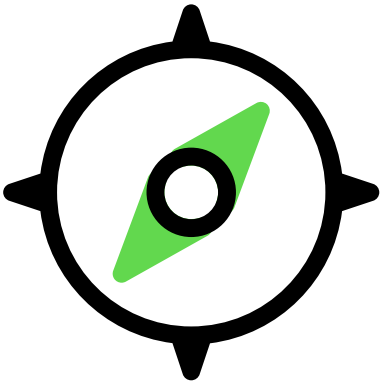
Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

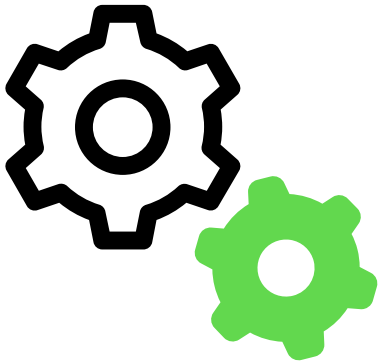
Security Incident Response

Untersuchen



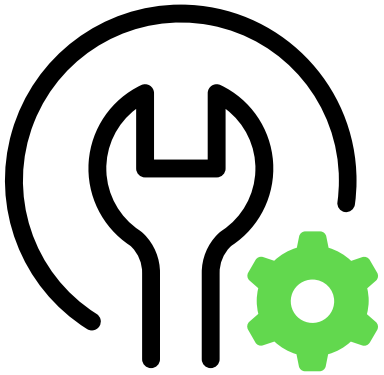
Erfahren Sie mehr über die Funktionen von Security Incident Response

Einrichten und konfigurieren



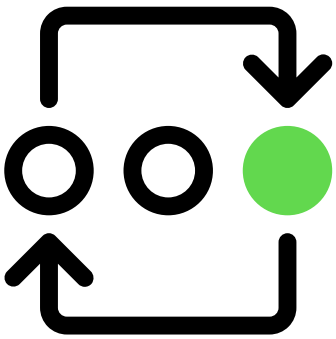
Installieren und richten Sie Ihre Security Incident Response-Anwendung ein

Verwalten



Verwalten und passen Sie Ihre Security Incidents an

Integrieren

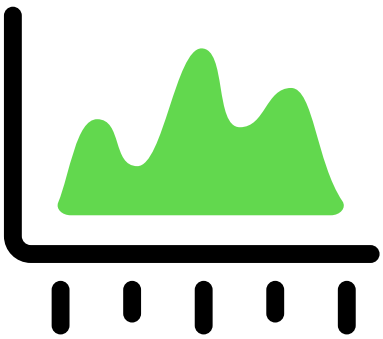


Erweitern Sie die Security Incident Response durch Integration mit anderen Anwendungen

Verwenden Sie den Security Incident Response-Arbeitsbereich

Erfahren Sie, wie Sie die Arbeitsbereiche „Security Incident Response“ und „IT-Korrektur“ verwenden

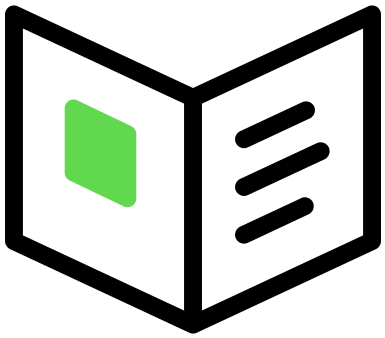
Analytics und Reporting



Überwachen Sie den Korrekturfortschritt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Rufen Sie zusätzliche Informationen zur Antwort auf Security Incidents ab

Security Operations-Apps im Store anfordern

Wenn Sie neu sind Security Operations Kunde am London Patch 6 oder höher besuchen Sie ServiceNow Store Website zum Anzeigen aller verfügbaren Apps und zum Senden von Anforderungen an den Store.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Security Incident Response verstehen

Mit Security Incident Response(SIR) verwalten Sie den Lebenszyklus Ihrer Security Incidents von der ersten Analyse bis zur Eindämmung, Beseitigung und Wiederherstellung. Mit Security Incident Response können Sie ein umfassendes Verständnis der von Ihren Analysten durchgeführten Incident-Antwortverfahren erhalten und Trends und Engpässe bei diesen Verfahren mit analytisch gesteuerten Dashboards und Berichten verstehen.

Eine Einführung in die Security Incident Response, die zeigt, wie Sie die Anwendung verwenden.

Sehen Sie sich dieses neunminütige Video an, um mehr über den SIR-Prozess mit zu erfahren Security Incident Response Dient zum Abwehr von Angriffen und zum Anzeigen von Sicherheitsaktivitäten in Security Incident Response Explorer.

Integrierte Integrationen mit Cybersicherheitslösungen von Drittanbietern und von Partnern entwickelten Integrationen aus dem ServiceNow Store Aktivieren Sie die Sicherheitsautomatisierung und -Orchestration für eine effiziente und genaue Reaktion auf Incidents.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um Ihre Untersuchungen zu schützen und Security Incidents privat zu halten, Security Incident Response Bietet die Möglichkeit, den Zugriff auf das System auf bestimmte sicherheitsbezogene Rollen und ACLs zu beschränken. Administratoren, die nicht sicherheitsbezogen sind, können Zugriff verweigert werden, es sei denn, Sie lassen ihnen ausdrücklich den Eintritt zu.

Hinweis:
IT-Systemadministratoren [admin] können die Identität von ServiceNow-Anwendern annehmen. Wenn ein Administrator jedoch die Identität eines Anwenders mit einer Anwendungsadministratorrolle für Security Incident Response annimmt, kann er nicht auf Funktionen zugreifen, die von dieser Rolle gewährt werden, einschließlich Security Incidents und Profilinformationen. Der Zugriff auf Module und Anwendungen in der Navigationsleiste ist ebenfalls eingeschränkt. Außerdem kann der Administrator das Passwort eines Anwenders mit einer Anwendungsadministratorrolle für Security Incident Response nicht ändern.

Security Incident Response-Informations-Flow

Security Incident Response verwendet den folgenden Informationsfluss, von der Integration über die Untersuchung bis zur Lösung und Überprüfung.

Hinweis:
Dies ist eine interaktive Infografik. Sie können also versuchen, auf eines der Symbole oder Schritte im Bild zu klicken, um mehr über diesen Prozess oder diese Aufgabe zu erfahren.

1. Klicken Sie auf dieses Bild, um mehr über SIR-Integrationen zu erfahren
2. Klicken Sie auf dieses Bild, um mehr über die Erstellung von Security Incidents zu erfahren
3. Klicken Sie auf dieses Bild, um mehr über Threat Intelligence zu erfahren
4. Klicken Sie auf dieses Bild, um mehr über SIR Workspace zu erfahren
5. Klicken Sie auf dieses Bild, um mehr über die MITRE-Angriffsfunktionen zu erfahren
6. Klicken Sie auf dieses Bild, um mehr über Aktivitäten zur Überprüfung nach Incident zu erfahren

Discovery

Security Incidents können auf folgende Arten protokolliert oder erstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aus dem Security Incident-Formular
- Aus Ereignissen, die intern ausgelöst oder von externen Überwachungs- oder Schwachstellennachverfolgungssystemen über Warnungsregeln oder manuell erstellt werden
- Aus externen Überwachungs- oder Nachverfolgungssystemen
- Aus dem Servicekatalog

Analyse

Abhängig von der ausgewählten Ansicht, die Sie verwenden (Standard, nicht-IT-Sicherheit, Security ITIL usw.), kann das Formular „Security Incident“ eine beliebige Kombination von Schwachstellen, Incidents, Changes, Problemen, Aufgaben für das betroffene CI und die betroffenen CI-Gruppen anzeigen. Das System kann Malware, Viren und andere Schwachstellen identifizieren, indem es auf die Datenbank des National Institute of Standards and Technology (NIST) oder andere Erkennungssoftware von Drittanbietern verweist. Wenn Security Incidents gelöst werden, können Sie jeden Incident verwenden, um einen Sicherheits-Knowledge Base-artikel zur späteren Referenz zu erstellen.

Führen Sie eine weitere Analyse mithilfe einer Business-Service-Zuordnung durch, um andere betroffene Systeme oder Business-Services zu finden, die infiziert werden können.

Eindämmung, Beseitigung und Wiederherstellung

Während Sie Schwachstellen überwachen und analysieren, können Sie Aufgaben erstellen und anderen Abteilungen zuweisen. Sie können eine Business-Service-Zuordnung verwenden, um Aufgaben, Probleme oder Changes für alle betroffenen Systeme, Dokumente, Aktivitäten, SMS-Nachrichten, Bridge-Aufrufe zu erstellen, und so weiter.

Prüfung

Nachdem der Incident gelöst wurde, können vor dem Abschluss weitere Schritte ausgeführt werden. Sie können eine Überprüfung nach Incident durchführen. Das Erstellen von Knowledge Base-Artikeln kann bei zukünftigen ähnlichen Incidents helfen. Für signifikante Incidents ist möglicherweise eine Überprüfung der Lösung nach dem Incident erforderlich. Diese Überprüfung kann verschiedene Formen annehmen. Zum Beispiel:

- Führen Sie eine Besprechung durch, um den Incident zu besprechen und Antworten zu sammeln.
- Schreiben Sie eine Liste von Fragen zur Lösungsüberprüfung, die für jede Kategorie oder Priorität des Incident konzipiert sind, und verteilen Sie sie an die Teams, die an einem Incident gearbeitet haben.
- Incident-Manager können den Bericht selbst schreiben und Informationen sammeln.

Ein Bericht zur Überprüfung der Incident-Lösung kann automatisch generiert werden, der Folgendes enthält:

1. Eine Zusammenfassung dessen, was getan wurde
2. Die Zeitlinie
3. Der Typ des aufgetretenen Security Incidents
4. Alle zugehörigen Incidents, Changes, Probleme, Aufgaben, CI-Gruppen
5. Die Details der Lösung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Darüber hinaus ist ein automatisiertes Umfragesystem zur Überprüfung der Lösung von Security Incidents verfügbar. Es sammelt die Namen aller Anwender, die einem Security Incident zugewiesen sind, und sendet eine anwenderdefinierte Umfrage, um Daten zur Behandlung des Incident zu sammeln. Diese Daten können dann in einem generierten Security Incident-Überprüfungsbericht verfügbar gemacht werden, den Sie in einen endgültigen Entwurf bearbeiten können. Ähnliche Daten können einem Knowledge Base-artikel hinzugefügt werden, um gelernte Lektionen und die Schritte zur Lösung ähnlicher Probleme in der Zukunft zu enthalten.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Security Incident Response-Terminologie

Die folgenden Begriffe werden in verwendet Security Incident Response.

Benennung	Definition
Aktiv	Jeder Security Incident, der sich nicht im Status „Geschlossen“ oder „Abgebrochen“ befindet.
Administratorsperre	Die Fähigkeit zum Einschränken Security Incident Response Zugriff auf Mitarbeiter mit sicherheitsbezogenen Rollen und ACLs.
Eingehende Sicherheitsanforderungen	Anforderungen, die für Sicherheitsanforderungen mit geringer Auswirkung übermittelt werden, z. B. die Anforderung eines neuen elektronischen Abzeichens.
Verwalten Sie Aktivitäten nach dem Incident	Eine Überprüfung der Ursprünge und der Behandlung eines Security Incidents. Das endgültige Produkt ist ein Bericht nach dem Incident, der alle durchgeführten Aktionen und die Gründe für ihre Ausführung dokumentiert.
Antwortaufgaben	Aufgaben, die einem Security Incident zugewiesen sind, um Aktionen als Reaktion auf die Bedrohung nachzuverfolgen.
Verstehen von Security Incident-Rechnern	Rechner, die zum Aktualisieren von Datensatzwerten verwendet werden, wenn vorkonfigurierte Bedingungen erfüllt sind.
Security Incident-Verzeichnisse	Diagrammtyp, der Security Incident-Daten hierarchisch in Form geschachtelter Rechtecke anzeigt.
Bedrohungssuche	Eine aus dem Security Incident-Katalog übermittelte Anforderung zum Scannen von Dateien, URLs und IP-Adressen auf Malware.
Schwachstellen-Scan	Eine vom Formular „Security Incident“ initiierte Anforderung zum Scannen betroffener Ressourcen (Server, Computer und andere Konfigurationselemente) auf Schwachstellen.

Domain Separation und Security Incident Response

Die Domänentrennung wird in Security Incident Response unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support-Stufe: Standard

- Enthält alle Aspekte von **Standard** Level-Support.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Übersicht

In Security Incident Response Anwendungs- und Domänentrennung ermöglicht Service Providern (SPS) die Standardisierung von SOC-Verfahren (Security Operations Center) und Security Incident Response (SIR) im gesamten Kundenstamm, für den sie arbeiten, mit geringeren Betriebskosten und einer höheren Servicequalität. Separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. stellen sicher, dass Kundendaten getrennt werden und niemals anderen Clients zugänglich gemacht werden.

Unterstützung der Domänentrennung in Security Incident Response nach Versionsveröffentlichungen

Release	Supportstufe	Notizen
Genf, Helsinki	Kein Support	Initiierung der Domänentrennung auf Datenebene
Istanbul	Nur Daten	
Jakarta	Ebene 2 (Daten, Anfordernde Person, Erfüller)	**Neue Funktionen** : Unterstützung von Drittanbieterintegrationen mit Domänentrennung der Ebene 2 unter einer einzigen Integrationsinstanz, einschließlich Threat Intelligence-Integrationen
Kingston	Ebene 2 (Daten, Anfordernde Person, Erfüller)	**Neue Funktionen** : Die Integration der Sichtungssuche für SIR ist mit mehreren Instanzen aktiviert, aber alle Instanzen befinden sich weiterhin in einer einzigen Domäne. Beispiel: Wenn zwei Instanzen einer Splunk-Integration konfiguriert sind (SplunkCLOUD und SplunkCORP), werden beide noch für Incident-Antwortaktivitäten in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützung der Domänentrennung in Security Incident Response nach Versionsveröffentlichungen (Fortsetzung)

Release	Supportstufe	Notizen
		einer einzigen Domäne genutzt, in der die Implementierung ursprünglich konfiguriert wurde.
London	Ebene 2 (Daten, Anfordernde Person, Erfüller)	**Neue Funktionen** : Alle Integrationen befinden sich über mehrere Domänen hinweg
Madrid	Ebene 2 (Daten, Anfordernde Person, Erfüller)	Alle Integrationen können sich jetzt über mehrere Domänen hinweg befinden. Im obigen Beispiel kann SplunkCloud domain1 und SplunkCORP domain2 sein.
New York	Ebene 2 (Daten, Anfordernde Person, Erfüller)	Alle Integrationen befinden sich über mehrere Domänen hinweg.
Orlando	Standard	Alle Integrationen befinden sich über mehrere Domänen hinweg.
Paris	Standard	Alle Integrationen befinden sich über mehrere Domänen hinweg.

Domänentrennung für Security Incident Response Die Anwendung deckt die folgenden Produktfunktionen ab:

- Sicherheitswarnungen werden an die entsprechende Domäne des Anwenders weitergeleitet, dessen ID/Anmeldeinformationen/Umfang den Incident generiert und als Security Incident registriert ist.
- Warnungen generieren „erkennbare Elemente“, die statusbehaftete Eigenschaften oder messbare Ereignisse darstellen: Sicherheits-Workflows in der Domäne des Security Incidents werden verwendet, um die Antwort zu orchestrieren.
- Integrationen werden in der Domäne des Security Incidents für die Antwortautomatisierung konfiguriert.
- Fähigkeiten werden in der Domäne des Security Incidents für die Antwortautomatisierung konfiguriert. Diese Fähigkeiten (ab Kingston-Release) umfassen:
  - Bedrohungssuche
  - Erkennbares Element ergänzen
  - Bereichern Sie das Konfigurationselement
  - Laufenden Prozess abrufen
  - Netzwerkstatistiken abrufen
  - Sperranforderung
  - Host isolieren
  - Sichtungssuche
  - E-Mails suchen und löschen
  - In Beobachtungsliste veröffentlichen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ergebnisse aus der Antwortautomatisierung (z. B. Bedrohungssuche oder Sichtungssuche) werden in der Domäne des Security Incidents gespeichert.
- Andere Security Incidents werden basierend auf einem gemeinsam genutzten Satz erkennbarer Elemente in derselben Domäne des Security Incidents referenziert.
- Andere Anwender werden in der Domäne des Security Incident mit Querverweisen versehen.
- Konfigurationselemente werden in derselben Domäne wie der Security Incident querreferenziert.
- Manuelle Antwortaufgaben werden der Domäne des Security Incidents hinzugefügt.
- In der Domäne des Security Incident wird auf Knowledge Base-Artikel und Ausführungsbücher verwiesen.
- Security Incident Response-Metriken, die für Incidents in der Domäne relevant sind, werden in Dashboards sowie im Reporting angezeigt.

Hinweis:
In den vorherigen Fällen gelten die übergreifenden Prinzipien der Sichtbarkeit in getrennten Domänen in der NOW Platform. Wie immer kann ein Incident in der übergeordneten Domäne auf Artefakte in der untergeordneten Domäne verweisen, aber nicht umgekehrt.

Funktionsweise der Domänentrennung in Security Incident Response

Die Security Incident Response Die Anwendung verwaltet den Lebenszyklus eines Security Incidents von Ende bis Ende Die folgenden Anwendungsfälle sind auf Domänentrennung ausgerichtet:

- **Erfassung von Ereignissen und Warnungen** So erstellen Sie Security Incidents für den Analysten im SOC des Kunden oder im MSP, um zu reagieren:
  - E-Mail-Parser (plattformbasiert, von Anwendern gemeldetes Phishing, anwenderdefiniert)
  - Deduplizierungsereignisse/Warnungen vor der Incident-Erstellung
  - Automatische Extraktion von erkennbaren Elementen
  - Anwendungen im SIEM-Store einer Drittpartei
- **Ergänzung** Von Artefakten, die an den Incidents beteiligt sind (IP, URLs, Domänen, Datei-Hashes):
  - Asset-Ergänzung (CMDB)
  - Anwender (Plattform)
  - Automatisierung: Ergänzung erkennbarer Elemente (z. B. WHOIS)
- **Untersuchen** Die Incidents mit Hilfe der Artefakte und ihre Reputation oder Zuordnung zu bekannten Bedrohungen
  - Orchestrieren: Playbooks und Knowledge Base-Artikel
  - Automatisierung: Bedrohungssuche (z. B. Virustotal), Sichtungssuche (z. B. Splunk), laufende Prozesse abrufen (z. B. Carbon Black)
- **Beseitigen** Die bedrohungsbezogenen Artefakte, die an dem Incident beteiligt sind, basierend auf der durchgeführten Untersuchung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Orchestrieren: Playbooks und Knowledge Base-Artikel
- Automatisierung: E-Mail-Suche und -Löschung (z. B. Microsoft Exchange), IP blockieren (z. B. Palo Alto Firewall)

- **Messen** Die Vorgänge „Effizienz“ oder „Reaktion auf Incidents“
  - Performance Analytics-Dashboards: Produktivitäts- und Incident-Trends
  - Rekonstruktion von Incident-Untersuchungsschritten aus Arbeitsnotizen
  - Überprüfung nach Incident

Domänentrennung – Einrichtung

Domänentrennung für wird eingerichtet Security Incident Response Erfordert keine zusätzlichen Schritte. Alle Security Incident Response Tabellen beziehen die Domänenspalte, nachdem die Instanz domänengetrennt ist.

Domänengetrennte Daten

Daten können domänengetrennt sein, was bedeutet:

- Security Incidents in einer Domäne können nicht in anderen Domänen angezeigt werden.
- Aus dem Security Incident extrahierte erkennbare Elemente werden in derselben Domäne platziert und können nicht in anderen Domänen angezeigt werden.
- Bis zum Kingston-Release sind konfigurierte Drittanbieterintegrationen in der globalen Domäne vorhanden und für alle anderen Domänen in der Instanz zugänglich.
- Im Madrid-Release können Integrationen von Drittparteien pro Domäne konfiguriert und aktiviert werden. Dies bedeutet, dass die in einer Domäne aktivierte und konfigurierte Integration nicht in einer anderen Domäne genutzt werden kann.
- Automatisierungen, die für die erkennbaren Elemente mithilfe von Drittanbieterintegrationen ausgeführt werden (für Bedrohungsuntersuchung, Eindämmung oder Beseitigung), platzieren ihre Ergebnisse in der Domäne des Security Incidents, und die Ergebnisse können nicht aus einer anderen Domäne angezeigt werden.
- Orchestration-Workflows, die in einer Domäne erstellt wurden, sind in einer anderen Domäne nicht sichtbar.
- Fähigkeiten (wie in der Liste der Preeding-Funktionen beschrieben), die aufgerufen werden, bleiben domänenübergreifend generisch, wobei die aufgerufene Fähigkeit domänenspezifisch implementiert wird. Beispielsweise kann eine Sichtungssuche auf einer IP eine Splunk-Implementierung in einer Domäne und eine QRadar-Implementierung in einer anderen Domäne aufrufen.

Konfiguration

Alle Aspekte der Produktkonfiguration sind in einer domänengetrennten Umgebung enthalten. Das Setup kann auf einzelne Domänen zugeschnitten werden.

Hinweis:
Die Geschäftslogik und die Prozesse in #2-5 unten können innerhalb der Mandantendomäne verwaltet werden.

Die folgenden Aufgaben müssen konfiguriert werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Systemverwaltung
   - Weisen Sie Anwendern und Anwendergruppen Rollen zu: Mit Security Incident Response installierte Anwenderrollen
   - Installieren Sie ein oder mehrere Drittanbieter-Integrations-Plugins, mit denen Sie arbeiten können Security Incident Response: Security Incident Response-Integrationen
2. Security Incident Response -Administration
   - Rollen hinzufügen oder überprüfen: Mit Security Incident Response installierte Komponenten
   - Gruppen und Anwender konfigurieren: Erstellen Sie eine Security Incident-Gruppe
   - Incident-Eskalationen einrichten: Eskalieren Sie einen Security Incident
   - Richten Sie Security Incident-Risikopunktzahlrechner ein: Verstehen von Security Incident-Rechnern
   - Richten Sie Servicelevel-Vereinbarungen ein: Erstellen Sie einen Security Incident Response SLA
   - Richten Sie Security Incident-Prozessdefinitionen ein: Beschreibung der Prozessdefinition für Security Incident Response
   - Richten Sie Prozesse für die Überprüfung nach Incidents ein: Verwalten Sie Aktivitäten nach dem Incident
3. E-Mail-Einstellungen für Security Incidents
   - Posteingang für E-Mail-Analyse festlegen: Security Operations E-Mail-Analyse
   - Richten Sie E-Mail-Parser für die Warnungserfassung ein: Erstellen Sie E-Mail-Parser in Security Operations
   - Richten Sie E-Mail-Übereinstimmungsregeln für von Anwendern gemeldetes Phishing ein: Erstellen Sie Regeln, um von Anwendern gemeldete Phishing-Angriffe zu validieren
   - Aktionen für eingehende E-Mails einrichten: Aktionen für eingehende E-Mails
4. Playbook-Einstellungen für Security Incidents
   - Runbook-Dokumente überprüfen und einrichten: Erstellen Sie ein Security Incident Response-Runbook
   - Richten Sie Security Incident-Workflows ein: Security Operations Allgemeine Funktionalität
5. Fähigkeitskonfigurationen
   - Anforderung blockieren: Integration von Security Operations: Fähigkeit zum Blockieren von Anforderungen
   - E-Mail suchen und löschen: Integration von Security Operations: Funktion „E-Mail suchen und löschen“
   - Konfigurationselement anreichern: Security Operations-Integration: Bereichern Sie die CI-Fähigkeit
   - Erkennbares Element anreichern: Integration von Security Operations: Bereichern Sie die Fähigkeit erkennbarer Elemente
   - Netzwerkstatistiken abrufen: Integration von Security Operations: Fähigkeit zum Abrufen von Netzwerkstatistiken
   - Laufende Prozesse abrufen: Integration von Security Operations: Fähigkeit zum Abrufen laufender Prozesse
   - Host isolieren: Integration von Security Operations: Fähigkeit zum Isolieren des Hosts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In Beobachtungsliste veröffentlichen: Integration von Security Operations: Funktion „in Beobachtungsliste veröffentlichen“
- Sichtungssuche: Integration von Security Operations: Sichtungssuchfunktion
- Bedrohungssuche: Integration von Security Operations: Fähigkeit zur Bedrohungssuche

Wie Mandantendomänen ihre eigenen Anwendungsdaten verwalten

- Mandantendomänenbesitzer erstellen eigene E-Mail-Analyseregeln für die Erfassung von Security Incidents.
- Mandantendomänenbesitzer können bestimmte Integrationen ausschließlich für die Verwendung innerhalb der Domäne konfigurieren.
- Mandantendomänenbesitzer können eigene Workflows für die Reaktion auf Incidents erstellen.
- Mandantendomänenbesitzer können eigene Incident-Kategorien, Knowledge Base-Artikel und Runbooks für Incident-Antworten erstellen, die mit Incident-Response-Workflows verknüpft werden.
- Mandantendomänenanwender erstellen und schließen ihre eigenen Security Incidents.

Geschäftslogik und Prozesse, die nach Instanzbesitzern domänengetrennt werden können

- Security Incident Response Anwender und Gruppen
- Security Incident Response Integrationen (ab Madrid-Release)
- E-Mail-Analyseregeln für die Incident-Erstellung
- Geschäftsregeln zum Konsolidieren mehrerer Ereignisse oder Warnungen zu einem Security Incident
- Workflows für die Orchestration der Reaktion auf Incidents
- Security Incident-Risikopunktzahlrechner
- Eskalationspfad für Security Incidents
- Security Incident-SLAs
- Security Incident-Prozessdefinitionen
- Prozesse zur Überprüfung von Security Incidents nach Incidents

Zugehörige Informationen

Domänentrennung für Service Provider

Setup von Security Incident Response

Setup für Security Incident Response Umfasst einige obligatorische Schritte und mehrere optionale Schritte, je nach Ihren spezifischen Anforderungen. Nachdem Sie heruntergeladen haben Security Incident Response Von ServiceNow Store Und installiert, können Sie den Setup-Assistenten ausführen, um die Standardkonfiguration für durchzuführen Security Incident Response Und Drittpartei-Integrationen.

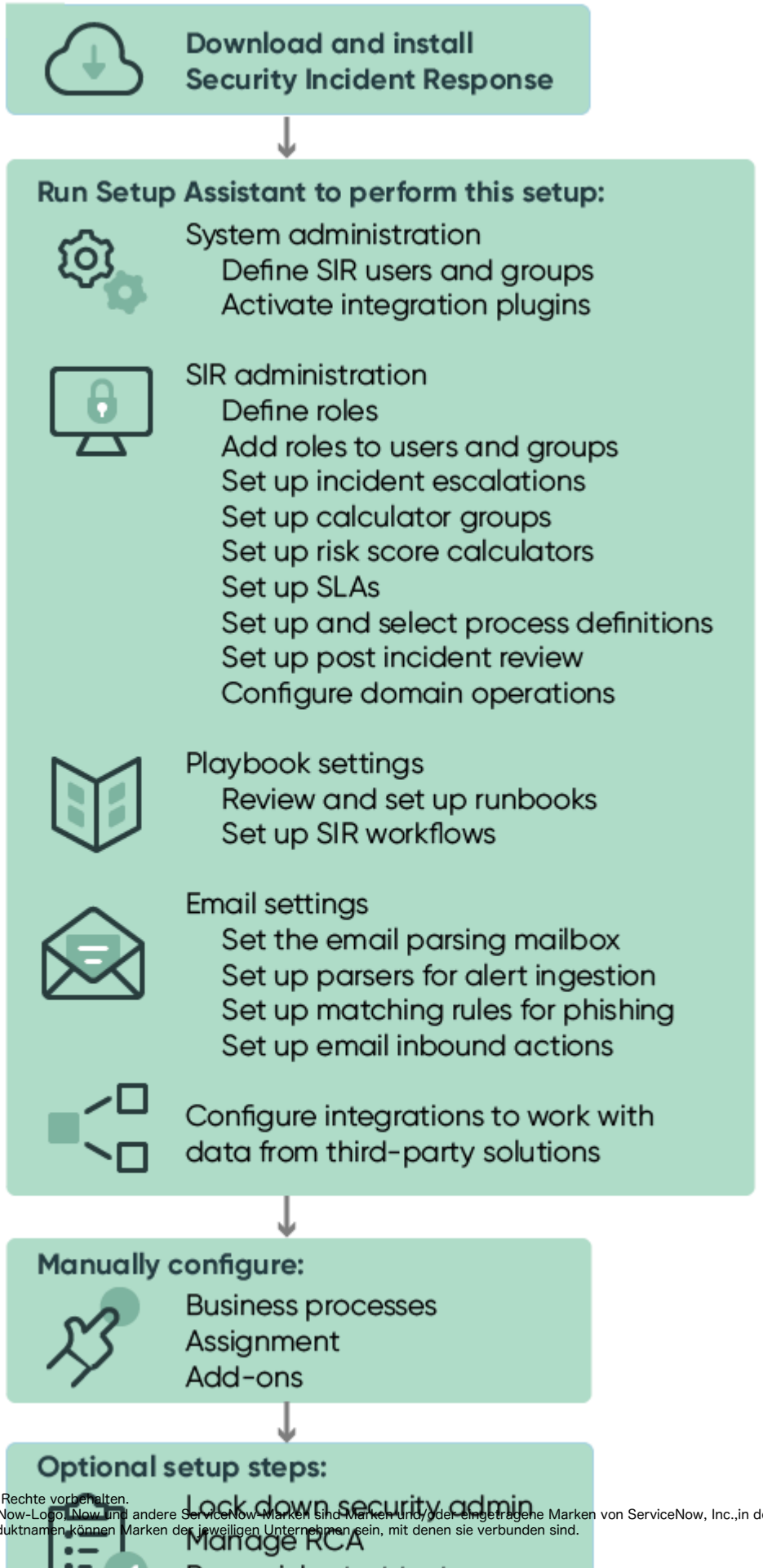
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Security Incident Response Setup-Prozess

Das folgende Diagramm zeigt den Setup-Prozess. Es ist in zwei Unterprozesse unterteilt, wobei heruntergeladen und konfiguriert wird Security Incident Response Anwendung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der erste Setup-Schritt ist bis Laden Sie herunter Security Incident Response Anwendung aus dem ServiceNow Storean. Wenn der Download abgeschlossen ist, werden mehrere abhängige Anwendungen geladen, einschließlich des Setup-Assistenten, und sie können konfiguriert werden Security Incident Response.

Setup-Assistent

Die Security Incident Response Der Setup-Assistent ist eine assistentenähnliche Anwendung, die Sie Schritt für Schritt durch das Setup Ihrer Basis führt Security Incident Response Instanz.

Die Setup-Schritte sind ziemlich selbsterklärend. Wenn Sie jedoch zusätzliche Erklärungen benötigen, finden Sie zusätzliche Hilfe in Referenz des Setup-Assistenten . Nachdem Sie das Setup mit dem Setup-Assistenten abgeschlossen haben, können Sie durchführen Andere optionale Setup-Verfahren , Nach Bedarf. Diese Verfahren enthalten Optionen für:

- Einrichten des Anforderungslebenszyklus
- Kataloge und Anforderungen werden erstellt
- Benachrichtigungen werden konfiguriert
- Manuelle und automatische Zuweisung einrichten
- Aktivieren der Knowledge Base, verwalteter Dokumente und Aufgabenaktivitäten

Ein neuer und verbesserter Security Incident Response-Arbeitsbereich ist verfügbar. Weitere Informationen finden Sie unter Arbeitsbereich für Security Incident Response.

Security Incident Response installieren und konfigurieren

Bevor Sie ausführen Security Incident Response In Ihrer Instanz müssen Sie es aus herunterladen ServiceNow Store Und schließen Sie die Konfigurationsschritte ab.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

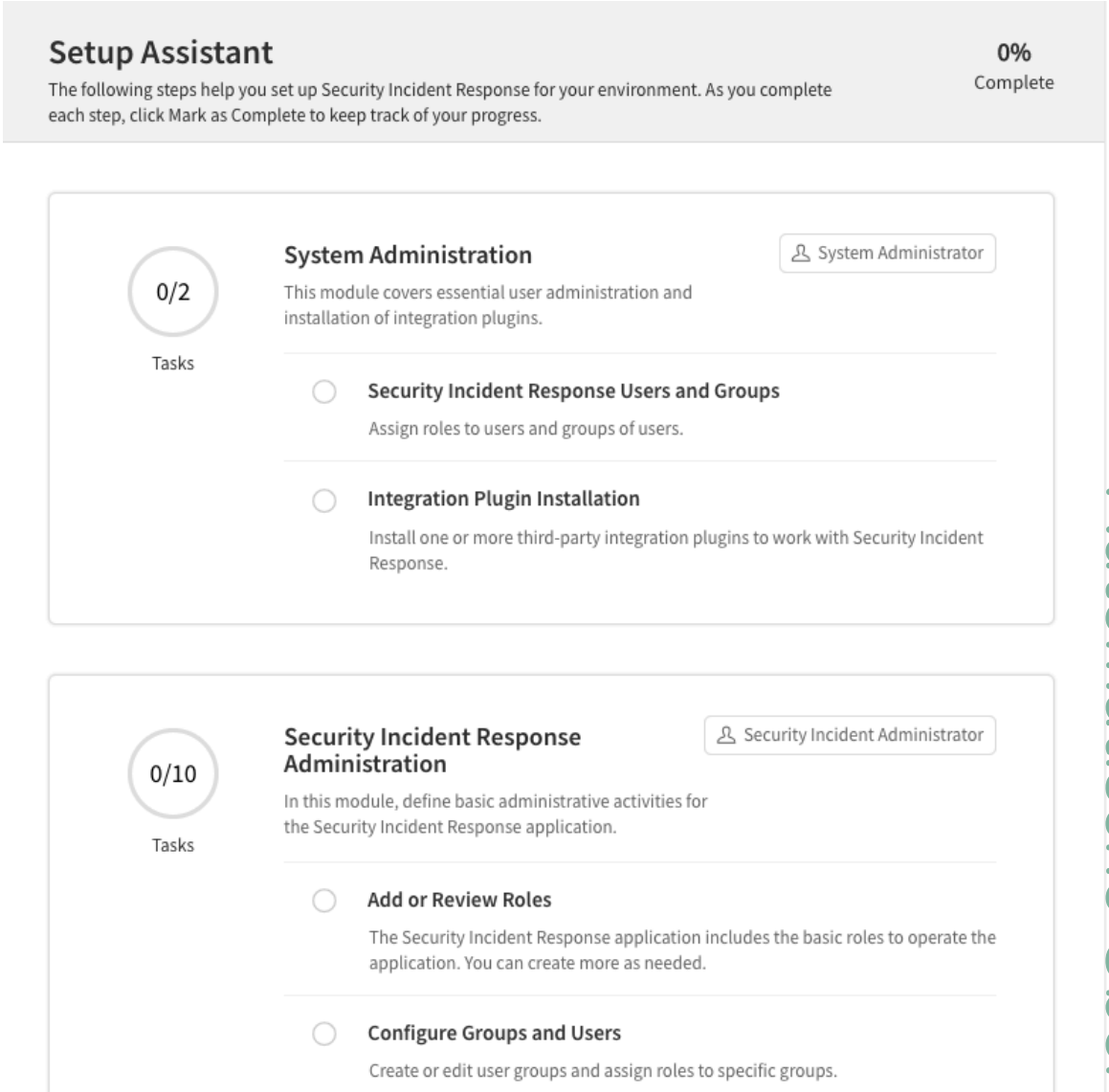
Wichtig:

- Installieren von Security Incident Response Version 13.4.5 oder höher aus ServiceNow Store Installiert automatisch Arbeitsbereich für Security Incident Response(sn_si_aw) Version 1.5.1 oder höher standardmäßig. Weitere Informationen zu den abhängigen Anwendungen finden Sie unter SIR-Arbeitsbereich Plugins und Rollen Abschnitt.
- Beachten Sie, dass die Version 1.5.1 und höher des Security Incident Response Workspace nur durch eine Installation/Aktualisierung von Security Incident Response installiert/aktualisiert werden kann und nicht unabhängig installiert werden kann.
- Die neuesten Funktionen in Security Incident Response Sind ausschließlich in verfügbar Arbeitsbereich für Security Incident Response. Installieren oder aktualisieren Sie auf den neuesten Security Incident Response Oder Arbeitsbereich für Security Incident Response Version für den Zugriff auf und die Nutzung von Funktionen wie Schichtübergabe, Risikobewertungsrechner usw.

Prozedur

1. Befolgen Sie die Anweisungen für Lädt eine Anwendung aus dem herunter ServiceNow Storean.
2. Nachdem Sie heruntergeladen haben Security Incident Response Navigieren Sie zu Anwendung und allen zugehörigen Abhängigkeitsanwendungen **Security Incident** > **Setup Des Analysten-Arbeitsbereichs** > **Setup-Assistent**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Befolgen Sie die Anweisungen in den Formularen, um zu konfigurieren Security Incident Response Basissystem.
   Weitere Informationen zu einigen der komplizierteren Setup-Aufgaben finden Sie unter Referenz des Setup-Assistenten, Nach Bedarf.

Laden Sie den Sicherheitsanalysten-Arbeitsbereich herunter, und installieren Sie ihn

Bevor Sie ausführen Security Incident Response Neue UI in Ihrer Instanz müssen Sie sie aus herunterladen ServiceNow® Store Und installieren Sie es.

Vorbereitungen

Um eine reibungslose Installation sicherzustellen, stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz. Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich:

- Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist die Rolle Security Incident Response Administrator [sn_si.admin] zu.
- Der Security Incident Response-Administrator [sn_si.admin] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

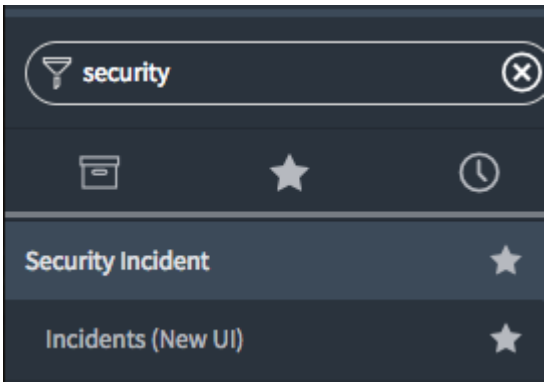
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Administrator

Prozedur

1. Befolgen Sie die Anweisungen für Lädt eine Anwendung aus dem herunter ServiceNow Store Und installieren Sie **UI für Security Incident Response** Anwendung.
2. Nach Abschluss der Installation können Sie den Sicherheitsanalysten-Arbeitsbereich öffnen, indem Sie zu navigieren **Security Incident** > **Incidents (neue UI)**



Mit Security Incident Response installierte Komponenten

Beim Herunterladen und Aktivieren von werden verschiedene Arten von Komponenten installiert Security Incident Response Anwendung, einschließlich Anwenderrollen, Tabellen, Eigenschaften und geplanten Aufgaben.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Installierte Eigenschaften

Benutzer mit der Rolle „Systemadministrator“ [admin] können die Eigenschaften anzeigen. Benutzer mit der Rolle „Sicherheitsadministrator“ [sn_si.admin] können sie ändern.

Eigenschaft	Monatlich
Die Standardkategorieknoten, die auf der Registerkarte „Beziehungsdiagramm“ im Arbeitsbereich angezeigt werden. Die Standardwerte stellen die Tabellennamen dar, die den zugehörigen Datensätzen entsprechen. sn_si_aw.defaultCategories	• **Typ**: Zeichenfolge • **Standardwert** : sn_ti_m2m_Task_observables,sn_si_m2m_Task_affected_user,
Standardmäßige Startzeit für alle Mitarbeiter, wenn kein Zeitplan festgelegt ist, formatiert als 08:00 sn_si.default.start.time	• **Typ**: Zeichenfolge • **Standardwert**: 08:00 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Monatlich
Standardmäßige Endzeit für alle Mitarbeiter, wenn kein Zeitplan festgelegt ist, im Format 17:00 sn_si.default.end.time	• **Typ**: Zeichenfolge • **Standardwert** : 17:00 Uhr • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Erkennbare Elemente vom Typ Ziel zusammen mit anderen erkennbaren Elementen vom Typ Kontext in die Security Incident-Anwender- und -CI-Beziehungen einschließen sn_si.Link_dest_ip	Bestimmt, ob ein erkennbares Security Incident-Element mit dem Kontexttyp angezeigt wird **Konfigurationselemente** Oder **Betroffene Anwender** Standardmäßig werden erkennbare Elemente mit einem Zielkontexttyp ausges die erkennbaren Elemente einzubeziehen, wählen Sie Ja.
Lassen Sie Anpassungen zu, wenn Sie ein Problem oder eine Change-Anforderung aus einem Security Incident erstellen sn_si.Popup	Wenn ein Problem oder Change erstellt wird, öffnet diese Eigen Popup-Fenster, um die Anforderung zu ändern. Wenn diese Eigenschaften auf festgelegt sind **Falsch**, Das Prob die Change-Anforderung hat die gleiche Priorität, Kurzbeschrei und Beschreibung wie der Security Incident, ohne dass Sie dies hinzufügen oder bearbeiten können. • **Typ**: true | false • **Standardwert**: true • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Ordnen Sie Sichtungssuchergebnisse CIs in der CMDB zu. sn_si.Associate_ci_with_Sighting_search	Bei „wahr“ enthalten Sichtungssuchergebnisse zugehörige Konfigurationsele in Ihrer CMDB befinden. • **Typ**: true | false • **Standardwert**: true • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Die Risikopunktzahl im Bereich wird grün hervorgehoben und im Format 0-49 formatiert sn_si.risk.score.green	In der Liste Security Incidents werden Security Incidents mit einer Risikopun 0 und 49 mit einem grünen Punkt markiert.
Risikopunktzahl im Bereich wird orange hervorgehoben und im Format 50-79 formatiert sn_si.risk.score.orange	In der Liste Security Incidents werden Security Incidents mit einer Risikopun 50 und 79 mit einem orangefarbenen Punkt markiert.
Die Risikopunktzahl im Bereich wird rot hervorgehoben und im Format 80-100 formatiert sn_si.risk.score.red	In der Liste Security Incidents werden Security Incidents mit einer Risikopun 80 und 100 mit einem roten Punkt markiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Monatlich
Dieser Parameter aktiviert oder deaktiviert Sichtungssuchkonfigurationen, die diese Funktion implementiert haben. sn_si.enable_Sighting_search	Bei „wahr“ können Sichtungssuchen für aktivierte Integrationen durchgeführt • **Typ**: true | false • **Standardwert**: true • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Die Anzahl der Zeilen mit Rohdaten, die gespeichert werden, wenn eine Sichtungssuche durchgeführt wird. Bereich 0-100 sn_si.Sighting_search_RAW_Data_rows	Diese Eigenschaft ist standardmäßig auf 50 Zeilen mit Rohdaten festgelegt. D der Ergebniszeilen wird ab Beginn des Suchzeitrahmens und die Hälfte ab En Suchzeitrahmens gemeldet. Wenn Sie also 50 Zeilen auswählen, stammen 25 Suchzeitrahmens und 25 vom Ende des Suchzeitrahmens.
Incident-Status automatisch auf „Eindämmen“ erhöhen, wenn eine Antwortaufgabe auf „In Arbeit“ gesetzt wird sn_si.Rollup_Task_State	Erwägen Sie bei der Verwendung von Flows oder Workflows, diese Eigensch festzulegen **Falsch** . Auf diese Weise können Sie den Incident-Status aus Flo Workflows steuern. Außerdem können potenzielle Konflikte beim Übergang Incident-Status in einen anderen vermieden werden. • **Typ**: true | false • **Standardwert**: true • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Zuweisungseigenschaften für Security Incident Response	
Standortgewichtung sn_si.location.weight	Eine Bewertung, die bei der Berechnung der Kriterien für die automatische Z eines Sicherheitsanalysten verwendet wird. Wenn beispielsweise der Standort Aufgabe berücksichtigt wird, wird der Wert der Standortgewichtung zur Bew Sicherheitsanalysten hinzugefügt. • **Typ**: Ganzzahl • **Standardwert**: 10 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Gewichtung der Kompetenzen sn_si.Skills.weight	Eine Bewertung, die bei der Berechnung der Kriterien für die automatische Z eines Sicherheitsanalysten verwendet wird. Wenn beispielsweise Kompetenze Aufgabe berücksichtigt werden, wird der Wert der Kompetenzgewichtung zu Sicherheitsanalysten hinzugefügt. • **Typ**: Ganzzahl • **Standardwert**: 10 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Legen Sie die maximale Anzahl von Sicherheitsanalysten fest, die durch automatische Zuweisung gleichzeitig verarbeitet werden sollen sn_si.max.agents.processed	Das System hat einen absoluten Grenzwert von 300 Sicherheitsanalysten. We als 300 angeben, wird der Wert auf diese Ebene festgelegt. Das System kann für eine Versandgruppe automatisch senden, die mehr Sicherheitsanalysten er konfigurierte Wert. • **Typ**: Ganzzahl • **Standardwert**: 100 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Monatlich
Gewichtung Zeitzone sn_si.timezone.weight	Eine Bewertung, die bei der Berechnung der Kriterien für die automatische Z eines Sicherheitsanalysten verwendet wird. Wenn beispielsweise die Zeitzone des Sicherheitsanalysten für eine Aufgabe berücksichtigt wird, wird der Wert Zeitzonengewichtung der Bewertung des Sicherheitsanalysten hinzugefügt. • **Typ**: Ganzzahl • **Standardwert**: 10 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Zwischen Ende einer Aufgabe und dem Reistestart der nächsten hinzuzufügende Dauer (in Minuten). sn_si.work.spacing	Ein Beispiel für einen gültigen Zeitwert ist 10. • **Typ**: Ganzzahl • **Standardwert**: 0 • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Angegebene Journalfelder mit `Code` Tags, die Inhalt als HTML rendern. sn_si.Journal_field.html_enabled	• **Typ**: Zeichenfolge • **Standardwert** : Work_Notes, Kommentare • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Berechnen Sie die betroffenen Services im Hintergrund. sn_si.refresh_Impact.event	Die zugehörige Liste „Betroffene Services/Betroffene CIs“ wird durch Ereign Wenn diese Option aktiviert ist, wird die Aktualisierung im Hintergrund ausg Incident werden Sicherheits-Tags hinzugefügt. Legen Sie den Wert auf fest **Wahr** Um den Vorgang im Hintergr auszuführen. • **Typ**: true | false • **Standardwert**: false • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**
Ruft den kritischen Service aus vorberechneten Daten ab. sn_si.critical_service.calculator.use_cache	Ermöglicht dem Rechner für kritische Services die Verwendung berechneter Daten von Konfigurationselementen. Legen Sie den Wert auf fest **Wahr** Um nach vorab berechneten suchen • **Typ**: true | false • **Standardwert**: false • **Standort**: **Security Incident** > **Administration** > **Eigenschaften**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
Security Incident-Administrator [sn_si.admin]	Vollständige Kontrolle über alle Security Incident Response Daten. Verwaltet auch Gebiete und Kompetenzen nach Bedarf. **Hinweis:** Im Basissystem hat der Administrator auch Zugriff auf sn_si.admin. Security Incident Response Kann vom Administrator beschränkt werden, solange mindestens einem anderen Anwender die Rolle „Sicherheitsadministrator“ zugewiesen ist.	• assessment_admin • catalog_admin • decision_table_admin • decision_table_reader • Filter_admin • flow_designer • pd_author • pd_content_author • pd_Operator • skill_admin • skill_model_admin • sn_si.analyst • sn_si.ingestion_profile_admin • sn_si.Knowledge_admin • sn_si.manager • sn_sec_cmn.admin • sn_si.restriction_Access_Manager • sn_si.special_Access_read_Manage • sn_si.special_Access_write_Manage • sn_ti.böswillig_attachment_Access • sn_ti.erkennbares Element.admin • Tags_admin • template_admin • territory_admin • Treemap_admin • user_admin
Profiladministrator [sn_si.ingestion_profile_admin]	Konfigurieren Sie die Plugins, erstellen, bearbeiten, löschen und verwalten Sie Profile für die Anwendung Splunk, Splunk es und Azure Sentinel Integration for Security Operations.	N/V

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Hinweis: Anwender mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt. Die Rolle sn_si.ingestion_profile_admin kann Anwendern vom sn_si.admin zugewiesen werden.	
Security Incident-Analyst [sn_si.Analyst]	Verwalten Sie Security Incidents. Zugrunde liegende Rolle für grundlegenden Sicherheitszugriff. Benutzer mit dieser Rolle können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Changes und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren.	• pd_Operator • snc_platform_rest_api_access • sn_msi.promoter • sn_msi.proposer • sn_si.basic • sn_ti.böswillig_attachment_Access
Security Incident – Standard [sn_si.Basic]	Zugrunde liegende Rolle für grundlegenden Sicherheitszugriff. Benutzer mit dieser Rolle können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Changes und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren.	• canvas_user • document_management_user • email_composer • flow_operator • inventory_user • pa_viewer • service_fullfiller • skill_user • sn_sec_cmn.write • sn_si.read • sn_ti.observable.read • sn_ti.erkennbares Element.Schreibe • sn_ti.read • task_activity_writer • task_editor • Treemap_user

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
Chief Information Security Officer (CISO) [sn_si.ciso]	Zeigen Sie das CISO-Dashboard an, und bearbeiten Sie es. Auch, wenn Vulnerability Response Plugin ist aktiviert. Benutzer mit dieser Rolle können dem Dashboard Baumaps zur Definition der Schwachstellenbedeutung hinzufügen. Sie können dasselbe auch mit tun Security Incident Response Plugin.	• pa_viewer • sn_si.basic • sn_si.read
Security Incident Extern [sn_si.extern]	Zeigen Sie alle Security Incidents an, die zu ihrer bestimmten Gruppe gehören. **Hinweis:** Die folgenden beiden Regeln gelten durchgehend ServiceNow Unabhängig vom bereichsbezogenen Administrator oder der bereichsbezogenen App. • Wenn Sie einer Gruppe einen Anwender hinzufügen, weisen Sie dieser Gruppe auch Rollen zu. Wenn Sie einen Anwender aus einer Gruppe entfernen, werden auch die geerbten Rollen entfernt. • Jede Rolle kann von einer Rolle mit höherer Priorität zugewiesen werden.	Service_Fulfiller
Security Incident-Integrationsanwender [sn_si.integration_user]	Externe Tools können neue Security Incident-Datensätze bereitstellen und Security Incident-Datensätze aktualisieren.	import_transformer
Security Incident-Wissensadministrator [sn_si.Knowledge_admin]	Verwalten, aktualisieren und löschen Sie die Informationen in der Security Incident Knowledge Base.	• knowledge_admin • sn_si.read
Security Incident-Manager [sn_si.Manager]	Gleicher Zugriff wie Sicherheitsanalysten.	• pd_author • pd_Operator • sn_si.basic
Security Incident Gelesen [sn_si.read]	Lesen Sie Security Incidents.	• canvas_user • sn_sec_cmn.read • sn_templated_snip.template_snippe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
		• sn_ti.erkennbares Element.Lesen • workspace_user
Zugriffsmanager für Sicherheitsbeschränkung [sn_si.restriction_Access_Manager]	Ermöglicht Anwendern oder Gruppen das Erzwingen von Einschränkungen für Security Incidents. Dies gilt nur für Feldänderungen.	N/V
Security Incident – Spezialzugriff sn_si.special_Access	Bietet Anwendern außerhalb der Security Operations-Organisation Zugriff auf bestimmte Security Incidents.	N/V
Aktivierer für speziellen Sicherheitszugriff [sn_si.special_Access_Enabler]	Stellt einem Anwender außerhalb der Security Operations-Organisation eine spezielle Zugriffsrolle für bestimmte Security Incidents bereit.	N/V
Security Incident – spezieller Lesemanager für Zugriff [sn_si.special_Access_read_Manager]	Verwalten Sie die Rolle „Special Access“ [sn_si.special_Access] für Security Incidents. Verwenden Sie diese Rolle, um zu ändern **Lesezugriff** Feld im Security Incident-Formular. Diese Rolle kann von sn_si.admin zugewiesen werden.	sn_si.special_Access_Enabler
Manager für Security Incident-Spezialzugriffsschreiber [sn_si.special_Access_write_Manager]	Verwalten Sie die Rolle „Special Access“ [sn_si.special_Access] für Security Incidents. Verwenden Sie diese Rolle, um zu ändern **Privilegierter Zugriff** Feld im Security Incident-Formular. Diese Rolle kann von sn_si.admin zugewiesen werden.	sn_si.special_Access_Enabler

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
Suchen Sie Erkennbare Security Incident-Elemente	Führt eine Suche nach erkennbaren Elementen in einem anwenderdefinierten Zeitplan durch.

Installierte Tabellen

Tabelle	Beschreibung
Nachrichtenfeed-Konfiguration [sn_si_Feed_Configuration]	Konfigurationsdatensätze, die zum Definieren des Inhalts verwendet werden, der im Security Incident-Nachrichtenfeed angezeigt wird.
Zuweisungsregel für die Überprüfung nach Incidents [sn_si_pir_condition]	Automatisiert die Auswahl der Teilnehmer einer Umfrage zur Überprüfung nach Incident, wenn ein Security Incident geschlossen wird.
Security Incident	Speichert einen Security Incident, die Antworten auf den Incident, alle verknüpften Aufgaben, Changes,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_si_Incident]	Probleme und Incidents im Zusammenhang mit diesem Security Incident.
Security Incident-Angriffsvektoren [sn_si_Attack_Vector]	Angriffsvektoroptionen.
Audit-Protokoll für Security Incidents [sn_si_Audit_log]	Speichert Auditprotokolle zur Ergänzung von Security Incidents.
Security Incident-Rechner [sn_si_Calculator]	Ein Rechner zum Festlegen bestimmter Security Incident-Felder, wenn bestimmte Bedingungen erfüllt sind.
Security Incident-Rechnergruppe [sn_si_Calculator_Group]	Eine Gruppierung von Security Incident-Rechnern. Die Reihenfolge der Rechnergruppe bestimmt, welche Gruppe zuerst ausgewertet wird, und in jeder Gruppe wird höchstens ein Rechner verwendet.
Security Incident-Anreicherung – Firewall [sn_si_Anreicherung_Firewall]	Erweitert sich aus der Basistabelle (sn_sec_cmn_Enrichment_Data_Base) und enthält alle Ergänzungsdatensätze, die für die Palo Alto Networks-Firewall spezifisch sind.
Malware-Ergebnisse Zur Anreicherung Von Security Incidents [sn_si_Anreicherung_Malware]	Erweitert sich aus der Basistabelle (sn_sec_cmn_Enrichment_Data_Base) und enthält alle für Malware spezifischen Ergänzungsdatensätze.
Security Incident-Anreicherung – Netzwerkstatistiken [sn_si_Enrichment_Network_statistics]	Erweitert sich aus der Basistabelle (sn_sec_cmn_Enrichment_Data_Base) und enthält alle Ergänzungsdatensätze, die für Netzwerkstatistiken spezifisch sind.
Security Incident-Anreicherung – Laufende Prozesse [sn_si_Enrichment_running _processes]	Erweitert sich aus der Basistabelle (sn_sec_cmn_Enrichment_Data_Base) und enthält alle Ergänzungsdatensätze, die für laufende Prozesse spezifisch sind.
Security Incident-Anreicherung – Laufende Services [sn_si_Anreicherung_Running_Service]	Erweitert sich aus der Basistabelle (sn_sec_cmn_Enrichment_Data_Base) und enthält alle Ergänzungsdatensätze, die für laufende Services spezifisch sind.
E-Mail-Suche für Security Incidents [sn_si_m2m_Incident_email_search]	Ordnet E-Mail-Suchdatensätze Security Incidents zu.
Security Incident-Import [sn_si_Incident_Import]	Importtabelle für Security Incidents. Wird verwendet, um Security Incidents aus externen Systemen zu erstellen.
Prozessdefinition für Security Incidents [sn_si_Process_Definition]	Speichert die Konfiguration für Security Incident-Prozess-Flows.
Prozessdefinitionsauswahl für Security Incidents	Speichert die Prozessdefinition für Security Incidents, die für Security Incidents verwendet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_si_Process_Definition_Selector]	
Mit Security Incident verbundener Kundenservicefall [sn_si_m2m_Incident_customerservice_Case]	Ordnet Kundenservicefälle und Security Incidents zu
Mit Security Incident verbundene Ergänzungsdaten [sn_si_m2m_Incident_Anreicherung]	Ordnet Security Incidents und zugehörige Ergänzungsdatensätze zu.
Security Incident Response Aufgabe [sn_si_Task]	Verwaltet Teilaufgaben im Zusammenhang mit der Behandlung eines Security Incidents. Diese Aufgaben können Sicherheitspersonal oder Personen in anderen Abteilungen zugewiesen werden, um die abteilungsübergreifende Kommunikation und die Aufgabennachverfolgung zu verwalten.
Security Incident Response Aufgabenvorlage [sn_si_Task_template]	Wird zum Erstellen von verwendet Security Incident Response Aufgabe. Diese Vorlagen werden häufig in Katalogeinträgen verwendet, um automatisch eine Reihe geeigneter Teilaufgaben für einen bestimmten Typ von Security Incidents zu erstellen.
Security Incident Runbook-Dokument [sn_si_runbook_document]	Ordnet Bedingungen oder Filter für Security Incidents einem wissensartikel zu. Wird verwendet, um Runbook-Verfahren für die Korrektur von Security Incidents anzugeben.
Vorlage für Security Incidents [sn_si_Incident_template]	Wird verwendet, um einen Security Incident zu erstellen. Diese Vorlagen werden häufig in Katalogeinträgen verwendet, um einen vorgefertigten Security Incident zu erstellen.
Sicherheitsanfrage [sn_si_Request]	Eine sicherheitsbezogene Anforderung an das Sicherheitsteam.
Anforderung für Sicherheitsprüfung [sn_si_Scan_Request]	Eine Anforderung für eine Bedrohungssuche.
Schweregradrechner sn_si_severity_Calculator	Definiert den Schweregrad, die Auswirkung, das Risiko und die Relevanzwerte für einen Security Incident.
Von Aufgabe betroffener Anwender [sn_si_m2m_Task_affected_user]	Eine viele-zu-viele-Tabelle, die Security Incidents betroffenen Anwendern zugeordnet.
Vorlagen-Workflow-Aktivität – Ergebnisauswertung [sn_si_wf_activity_result_Evaluator]	Ordnet eine Fähigkeit einem Auswertungsskript zu. Ein neuer Subflow kann einem Vorlagen-Workflow hinzugefügt werden, um ein Ergebnis einer Antwortaufgabe festzulegen, anstatt es manuell von einem Analysten festzulegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere zusätzliche Security Incident Response Setup-Aufgaben

Wenn Sie ein Administrator in der globalen Domäne sind, konfigurieren Sie wie Security Incident Response Verarbeitet tägliche Vorgänge.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Hinweis:

Diese Optionen sind Standard für viele Servicemanagement-Anwendungen und verwenden daher Servicemanagement-Terminologie. Beispielsweise wird „Anforderung“ für die Hauptaufgabe (also den Security Incident) und „Aufgabe“ für Teilaufgaben oder Antwortaufgaben verwendet.

Wenn Sie ein Administrator in einer Domäne unterhalb der globalen Domäne sind, können Sie den Bildschirm „Konfigurationen“ anzeigen, die Einstellungen jedoch nicht ändern.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Konfiguration**an.
   Die Optionen zum Konfigurieren der Anwendungen sind unter diesen Registerkarten organisiert:
   - Die Registerkarte **Geschäftsprozess** enthält Optionen für das Einrichten des Anforderungslebenszyklus, das Erstellen von Katalogen und Anforderungen und das Konfigurieren von Benachrichtigungen.
   - Die Registerkarte **Zuweisung** enthält Optionen für die Einrichtung der manuellen und automatischen Zuweisung.
   - Die Registerkarte **Add-Ons** enthält Optionen zum Aktivieren der Wissensdatenbank, verwalteter Dokumente und von Aufgabenaktivitäten.
2. Füllen Sie die Felder im aus **Geschäftsprozess** Registerkarte.

Konfigurationsbildschirm – Registerkarte „Geschäftsprozess“

Feld	Beschreibung
Lebenszyklus	
Zum Schließen oder Abbrechen einer Anforderung oder Aufgabe sind Arbeitsnotizen erforderlich.	Aktivieren Sie diese Option, damit der Anwender Arbeitsnotizen eingeben muss, bevor ein Security Incident oder eine Antwortaufgabe geschlossen oder abgebrochen werden kann.
Arbeitsnotizen zur Aufgabe in die Anforderung kopieren	Aktivieren Sie diese Option, um die Arbeitsnotizen der Antwortaufgabe mit den Arbeitsnotizen zum Security Incident zu synchronisieren. Wenn Arbeitsnotizen in der Aufgabe hinzugefügt werden, werden dieselben Arbeitsnotizen im übergeordneten Security Incident angezeigt.
Katalog- und Anforderungserstellung	
Anforderungen per eingehender E-Mail erstellen und aktualisieren	Aktivieren Sie diese Option, um Security Incidents aus eingehenden E-Mails zu erstellen oder zu aktualisieren.
Anforderungen werden erstellt mit	Wählen Sie Aus **Katalog- oder reguläres Formular** Um den Katalog zu aktivieren und die automatische Veröffentlichung von Security Incident-Vorlagen im Katalog zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wählen Sie Aus **Nur reguläres Formular** Zum Deaktivieren des Katalogs und zum Deaktivieren der automatischen Veröffentlichung von Security Incident-Vorlagen im Katalog.
Mit Vorlagen wird ein eigenes Katalogelement erstellt.	Aktivieren Sie diese Option, um die automatische Veröffentlichung von Katalogelementen für die Anwendung zu aktivieren.
Benachrichtigungen	
Senden Sie bei einer Anforderung oder Aufgabe, wenn sich das ausgewählte Feld ändert, eine Benachrichtigung an die Empfänger	Sie können Benachrichtigungen konfigurieren, die an bestimmte Empfänger gesendet werden, wenn sich ausgewählte Felder in Security Incidents und Antwortaufgaben ändern. **a.** Von **Tabelle** , Wählen Sie aus **Anforderung (Security Incident** Oder **Aufgabe (Antwortaufgabe)** . **b.** Wählen Sie unter **Feld** das Feld zum Generieren von Benachrichtigungen aus. Wenn eine Änderung am ausgewählten Feld vorgenommen wird, wird eine Benachrichtigung an die identifizierten Empfänger gesendet. **c.** Von **Empfänger** , Wählen Sie einen oder mehrere Empfänger aus. **d.** Wenn **ein bestimmter Benutzer** oder **eine bestimmte Gruppe** ausgewählt ist, werden Sie aufgefordert, einen Benutzer oder eine Gruppe auszuwählen. **e.** Um weitere Benachrichtigungen mit anderen Feldern oder Empfängern zu definieren, wiederholen Sie die vorherigen Schritte für den nächsten Satz von Benachrichtigungseinstellungen. **f.** Klicken Sie auf , um eine Benachrichtigung zu entfernen Symbol rechts neben der Benachrichtigung.

3. Klicken Sie auf die Registerkarte **Zuweisung**, und füllen Sie die Felder aus.

Konfigurationsbildschirm – Registerkarte „Zuweisung“

Feld	Beschreibung
Zuweisungsmethode für Anforderungen	Wählen Sie die Methode für die Zuweisung von Security Incidents aus: ○ **Automatische Zuweisung wird verwendet** : Security Incidents werden automatisch zugewiesen. ○ **Mithilfe eines Workflows** : Security Incidents werden vom ausgewählten Workflow zugewiesen. ○ **Manuell** : Security Incidents werden manuell zugewiesen.
Diesen Workflow zur Zuweisung von Anforderungen verwenden	Wählen Sie den Workflow für das Versenden von Security Incidents aus. Dieses Feld wird angezeigt, wenn **Mithilfe eines Workflows** Ist aus ausgewählt **Zuweisungsmethode für Anforderungen** Liste.
Zuweisungsmethode für Aufgaben	Wählen Sie die Methode für die Zuweisung von Antwortaufgaben aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Automatische Zuweisung wird verwendet** : Antwortaufgaben werden automatisch zugewiesen. ○ **Mithilfe eines Workflows** : Antwortaufgaben werden vom ausgewählten Workflow zugewiesen. ○ **Manuell** : Antwortaufgaben werden manuell zugewiesen.
Verwenden Sie diesen Workflow, um Aufgaben zuzuweisen	Wählen Sie den Workflow für die Zuweisung von Antwortaufgaben aus. Dieses Feld wird angezeigt, wenn **Mithilfe eines Workflows** Ist aus ausgewählt **Zuweisungsmethode für Aufgaben** Liste.
Anforderungen oder Aufgaben basierend auf Abdeckungsgebieten von Zuweisungsgruppen zuweisen	Aktivieren Sie diese Option, um die Zuweisung von Security Incidents und Antwortaufgaben auf Gruppen zu beschränken, die den Standort der Aufgabe abdecken.
Zeitplanung	
Bei der automatischen Auswahl von Service Desk-Mitarbeitern wird die Zeitzone für Aufgaben berücksichtigt	Aktivieren Sie diese Option, um die Zeitzone des Mitarbeiters zu berücksichtigen, wenn Sie eine Aufgabe zuweisen. Dieses Feld wird angezeigt, wenn die automatische Zuweisung für Security Incidents oder Antwortaufgaben ausgewählt ist.
Zusätzliche Faktoren	
Bei der automatischen Auswahl von Service Desk-Mitarbeitern wird der Standort von Service Desk-Mitarbeitern berücksichtigt	Aktivieren Sie diese Option, um Service Desk-Mitarbeitern, die näher am Aufgabenstandort sind, beim Zuweisen von Aufgaben Vorrang zu geben. Dieses Feld wird angezeigt, wenn die automatische Zuweisung für Security Incidents oder Antwortaufgaben ausgewählt ist.
Bei der automatischen Auswahl von Mitarbeitern für Aufgaben werden bestimmte Kompetenzen vorausgesetzt.	Wählen Sie den Grad aus, in dem die Kompetenzen von Service Desk-Mitarbeitern bei der Bestimmung der automatischen Zuweisung mit einer Aufgabe abgeglichen werden müssen. ○ Wählen Sie Aus **Alle** Damit muss ein zugewiesener Service Desk-Mitarbeiter über alle Kompetenzen verfügen, um die Aufgabe auszuführen. Ein Service Desk-Mitarbeiter, dem nur eine Kompetenz fehlt, wird eliminiert. ○ Wählen Sie Aus **Einige** Wenn Sie Service Desk-Mitarbeiter möchten, die über die meisten erforderlichen Kompetenzen verfügen, um die Aufgabe auszuführen. ○ Wählen Sie Aus **Keine** Wenn Sie Service Desk-Mitarbeiter automatisch zuweisen möchten, ohne Kompetenzen zu berücksichtigen. Dieses Feld wird angezeigt, wenn die automatische Zuweisung für Security Incidents oder Antwortaufgaben ausgewählt ist.
Bei der automatischen Auswahl wird versucht, allen Aufgaben in einer Anforderung denselben Service Desk-Mitarbeiter zuzuweisen	Aktivieren Sie diese Option, um alle Antwortaufgaben für einen Security Incident automatisch demselben Service Desk-Mitarbeiter zuzuweisen.

4. Klicken Sie auf die Registerkarte **Add-ons**, und füllen Sie die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsbildschirm – Registerkarte „Add-ons“

Feld	Beschreibung
Dokumentation	
Eigene Knowledge Base aktivieren	Aktivieren Sie diese Option, um die Knowledge Base für zu aktivieren Security Incident Response.
Verwaltete Dokumente aktivieren	Aktivieren Sie diese Option, um eine zugehörige Liste zu den verwalteten Dokumenten hinzuzufügen.
Aufgabenaktivitäten aktivieren	Aktivieren Sie diese Option, um Aufgabeninteraktionen und -Kommunikation wie Telefonanrufe und E-Mail-Nachrichten zu protokollieren.

5. Klicken Sie auf **Speichern**.

Sperren Sie die Sicherheitsverwaltung

Um Untersuchungen zu schützen und Security Incidents privat zu halten, können Sie einschränken Security Incident Response Zugriff auf sicherheitsspezifische Rollen und ACLs. Administratoren, die nicht sicherheitsbezogen sind, können Zugriff verweigert werden, es sei denn, Sie lassen ihnen ausdrücklich den Eintritt zu.

Vorbereitungen

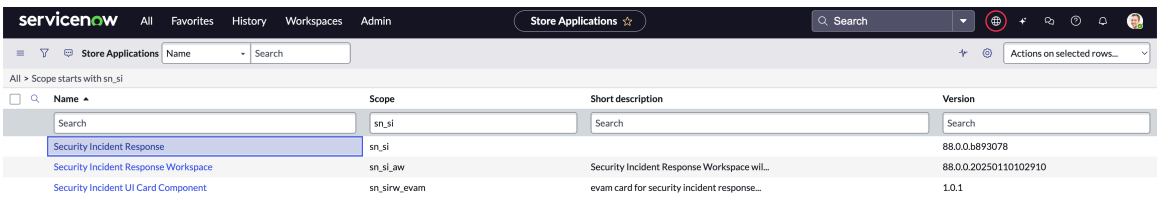
Wenn Security Incident Response Die Anwendung ist aktiviert, und dem Systemadministrator wird standardmäßig die Rolle sn_si.admin gewährt. Der Systemadministrator ist der einzige Administrator, der Sicherheitsgruppen und -Anwender einrichten kann.

Für Zugriff auf ist eine Sicherheitsrolle erforderlich Security Incident Response Funktionen und Datensätze.

Erforderliche Rolle: sn_si.admin

Prozedur

1. Nach Security Incident Response Plugin wurde aktiviert. Ein Anwender mit der Administratorrolle weist mindestens einem Anwender die Rolle „Bereichsbezogener Administrator“ (sn_si.admin) zu.
2. Der Anwender mit der Administratorrolle ändert sich in den Bereich Security Incident.
3. Navigieren zu **Alle** > **sys_Store_App.list**an.
4. Typ **sn_si** In **Umfang** Feld.



5. Klicken Sie Auf **Security Incident Response** .
6. Scrollen Sie nach unten zu **Zugehörige Links** Und klicken Sie auf **Entfernen Sie aus der Rolle des Administrators** .
7. Melden Sie sich ab, und melden Sie sich erneut an.
   Der Administratoranwender kann nicht auf zugreifen Security Incident Response Anwendung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Anwendungsverwaltung

Verwalten Sie Eingeschränkten Anruferzugriff

Mit der RCA-Funktion (Restricted Caller Access) kann ein Administrator den bereichsübergreifenden Zugriff auf eine Anwendung oder Anwendungsressource definieren und Zugriffsanforderungen zulassen oder verweigern. Diese Funktion ist in aktiviert Security Incident Response Standardmäßig können Sicherheitsanalysten vertrauliche sicherheitsbezogene Informationen schützen.

Ein Feld namens **Anruferzugriff** Wurde allen Tabellen und Skripteinbindungen in hinzugefügt Security Incident Response, Und das Feld ist standardmäßig auf festgelegt **Anrufernachverfolgung** . Diese Einstellung bedeutet, dass Anwendungsbereiche Zugriff auf haben Security Incident Response Tabellen und Skripteinbindungen. Für jeden Datensatz wird jedoch ein Nachverfolgungsdatensatz erstellt und in der Tabelle „eingeschränkte Anruferzugriffsberechtigung“ [sys_Restricted_caller_Access] gespeichert.

Hinweis:
Gehen Sie beim Ändern von Datensätzen von vorsichtig vor **Anrufernachverfolgung** Bis **Anrufer Eingeschränkt** . Auf Datensätze mit diesem Status kann erst zugegriffen werden, wenn ein Administrator den Zugriff manuell zulässt. Der Administrator muss zu navigieren **Systemanwendungen** > **Anwendung – Eingeschränkter Aufruferzugriff**, Suchen Sie die Tabelle oder Skripteinbindung, für die Zugriff angefordert wurde, und ändern Sie den **Status** Feld von **Angefordert** Bis **Zulässig** .

Zugehörige Informationen

Einstellungen für eingeschränkte Anruferzugriffsberechtigungen

Legen Sie den Anwendungsbereich, die Anwendungsressource und den Ereigniszugriff fest

Schnellstarttests für Security Incident Response ausführen

Validieren Sie dies Security Incident Response Funktioniert weiterhin, nachdem Sie Konfigurationsänderungen vorgenommen haben, z. B. das Anwenden eines Upgrades oder die Entwicklung einer Anwendung. Kopieren Sie diese Schnellstarttests und passen Sie sie an, um sie bei der Verwendung Ihrer instanzspezifischen Daten zu übergeben.

Security Incident Response-Schnellstarttests erfordern die Aktivierung des Plugins „Security Incident Response“ (com.snc.security_incident) und das Laden der Demodaten.

Security Incident Response-Tests

Test	Beschreibung	Release-Version
SIR: Sicherheitsincident erstellen	Ermittelt, ob ein Benutzer einen Sicherheitsincident erfolgreich aus dem Sicherheitsincident-Formular erstellen kann.	Madrid
SIR: Sicherheitsincident über den Sicherheitsincident-Katalog erstellen	Ermittelt, ob ein Benutzer einen Sicherheitsincident erfolgreich aus dem Katalog erstellen kann.	Madrid
SIR: Lebenszyklus des Sicherheitsincident	Validiert die Antwortaufgaben des Richtlinienverletzungs-Workflows.	Madrid
SIR: OOTB-Konfigurationstest für PIR-Bewertungen	Mit diesem Test können Sie PIR-Bewertungen und	Tokyo

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response-Tests (Fortsetzung)

Test	Beschreibung	Release-Version
	Basissystemkonfigurationen validieren.	
SIR: Bedingte Konfigurationstests für PIR-Bewertungen	Verifiziert, dass Security Incidents, die der obligatorischen bedingten Regel entsprechen, erst geschlossen werden, wenn die Bewertung nach dem Incident abgeschlossen ist. Verifiziert, dass Security Incidents, die der optionalen bedingten Regel entsprechen, geschlossen werden können, wenn die Bewertung nach dem Incident abgeschlossen ist. Verifiziert, dass für Security Incidents, die keiner Regel entsprechen, keine Bewertungen generiert werden.	Tokyo
SIR: PIR-Laufzeit-Experience	Überprüft, ob PIR-Berichte gemäß dem neuen Design konfiguriert und an Sicherheits-Incidents angehängt werden.	Tokyo
SIR: PIR-Designzeit-Experience	Überprüft, ob der Sicherheit-Incident je nach Administratorkonfiguration der Berichtsvorlage zugeordnet wird.	Tokyo
SIR: Security Incident mit einem vorhandenen schwerwiegenden Security Incident verknüpfen	Verknüpfen Sie einen Security Incident mit einem vorhandenen schwerwiegenden Security Incident, und validieren Sie die Daten, die aus dem Security Incident per Rollup zum schwerwiegenden Security Incident zusammengefasst werden.	Tokyo
SIR: Security Incident als schwerwiegenden Security Incident hochstufen	Stufen Sie einen Security Incident zu einem schwerwiegenden Security Incident hoch, und validieren Sie die Daten, die aus dem Security Incident per Rollup zum schwerwiegenden Security Incident zusammengefasst werden.	Tokyo
SIR: Security Incident als schwerwiegenden Security Incident vorschlagen	Schlagen Sie einen Security Incident als einen schwerwiegenden Security Incident	Tokyo

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response-Tests (Fortsetzung)

Test	Beschreibung	Release-Version
	vor, und validieren Sie die Daten, die aus dem Security Incident per Rollup zum schwerwiegenden Security Incident zusammengefasst werden.	
SIR: Lebenszyklus des Sicherheitsincident	Validieren Sie einen Security Incident-Lebenszyklus mit dem Workflow für Antwortaufgaben für Richtlinienverstöße.	Yokohama
SIR: Sicherheitsfall erstellen	Erstellen Sie einen Sicherheitsfall aus dem Security Incident-Formular.	Yokohama
Verifiziert, dass nur zulässige Mitglieder auf den Security Incident zugreifen können, wenn „Beschränkung erzwingen“ aktiviert ist	Verifiziert, dass nur die zulässigen Mitglieder auf den Security Incident zugreifen können, wenn „Beschränkung erzwingen“ aktiviert ist.	Yokohama
Stellen Sie sicher, dass Security Incident, der mit „Einschränkung erzwingen“ aktiviert ist, für keinen Anwender sichtbar ist	Stellen Sie sicher, dass Security Incident, der mit „Einschränkung erzwingen“ aktiviert ist, für keinen Anwender sichtbar ist.	Yokohama
Lesezugriff validieren	Validieren Sie den Anzeigezugriff.	Yokohama
Schreibzugriff validieren	Validieren Sie den Bearbeitungszugriff.	Yokohama
SIR-Arbeitsbereich: Lesezugriff	Stellen Sie sicher, dass der Lesezugriff-Anwender den Security Incident anzeigen kann, ohne über Sicherheitsrollen selbst im Arbeitsbereich zu verfügen.	Yokohama
SIR-Arbeitsbereich: Schreibzugriff	Stellen Sie sicher, dass der Schreibzugriff-Anwender den Security Incident aktualisieren kann, ohne über Sicherheitsrollen zu verfügen.	Yokohama
SIR-Arbeitsbereich: Neuen Security Incident erstellen	Erstellen Sie einen neuen Security Incident aus dem Arbeitsbereich.	Yokohama
SIR-Arbeitsbereich: Antwortaufgabe erstellen	Erstellen Sie eine neue Antwortaufgabe aus einem vorhandenen Security Incident.	Yokohama
Now Assist für Sicherheit: Zusammenfassung aktiver Security Incidents	Fassen Sie einen aktiven Security Incident zusammen, und validieren Sie die angezeigten Abschnitte.	Zurich
Now Assist für Sicherheit: Security Incident	Geben Sie die generierte Zusammenfassung für Arbeitsnotizen frei.	Zurich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response-Tests (Fortsetzung)

Test	Beschreibung	Release-Version
Summary_share zu Arbeitsnotizen		
Now Assist für Sicherheit: Zusammenfassung geschlossener Security Incidents	Fassen Sie einen geschlossenen Security Incident zusammen, und validieren Sie die angezeigten Abschnitte.	Zurich

Zugehörige Informationen

Schnellstarttests

Referenz des Setup-Assistenten

Der Setup-Assistent führt Sie durch die Schritte, die Sie zum Einrichten von ausführen müssen Security Incident Response Basissystem. Dieser Abschnitt enthält zusätzliche Informationen zu den komplizierten Schritten, für die Sie möglicherweise weitere Erklärungen benötigen.

Erstellen Sie einen Security Incident Response Prozessdefinition

Sie können eine Prozessdefinition erstellen, um zu definieren, wie Security Incidents von einem Status in den nächsten übergehen. Prozessdefinitionen geben Service Desks und Endanwender Hilfe, das Problem während seines gesamten Lebenszyklus nachzuverfolgen.

Vorbereitungen

Erforderliche Rolle: sn.si_admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Prozessdefinition**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

Prozessdefinitionen werden erstellt

Feld	Beschreibung
Name	Name des Datensatzes, der den in der Skripteinbindungsdatei codierten Prozess beschreibt. Der Name wird als Auswahl in angezeigt **Prozessdefinitionsauswahl** Liste.
Skripteinbindung	Der Name (einschließlich `sn_si` . Präfix) der Skripteinbindung, die die Definition des Prozesses enthält. Das Skript muss sich im Security Incident befinden (`sn_si`) Anwendungsbereich. Weitere Informationen finden Sie unter Erstellen Sie eine anwenderdefinierte Security Incident Response Skripteinbindung der Prozessdefinition. Wenn dieses Feld keinen gültigen Skripteinbindungsnamen enthält, wird die standardmäßige Definition ProcessDefinition_NIST_Stateful verwendet.
Beschreibung	Hilfreiche Informationen zur Skripteinbindung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Reihenfolge	Bestimmt die Position in der Prozessdefinitionsliste.
Aktiv	Wenn diese Option aktiviert ist, kann diese Prozessdefinition über ausgewählt werden **Prozessdefinitionsauswahl** Seite.

4. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Auswahl Des Prozesses Für Die Reaktion Auf Security Incidents

Beschreibung der Prozessdefinition für Security Incident Response

Beschreibung der Prozessdefinition für Security Incident Response

Security Incident Response Prozessdefinition Ersetzt Status-Flows und stellt Endanwendern und Service Desks den Status eines Problems zur Verfügung. Eine Prozessdefinition hilft, das Problem über seinen Lebenszyklus nachzuverfolgen. Security Incident Response Ist eine Service Management-Anwendung (SM), die über einen eigenen Satz von status verfügt. Ungültige status werden als Teil von gemeldet Prozessauswahl.

Definition Des Security Incident Response-Prozesses

Die Standardprozessdefinition (NIST Stateful) definiert die folgenden Incident-status:

Hinweis:
Verfügbare status variieren je nach aktuellem Status des Incident.

status der Security Incident-Prozessdefinition

Status	Beschreibung
Entwurf	Der Anforderungsinitiator fügt Informationen zum Security Incident hinzu, kann aber noch nicht bearbeitet werden.
Analyse	Der Incident wurde zugewiesen, und das Problem wird analysiert.
Begrenzen	Das Problem wurde identifiziert, und das Sicherheitspersonal arbeitet daran, es einzudämmen und die Schadenskontrolle durchzuführen. Diese Aktionen können umfassen, dass Server offline geschaltet werden, Geräte vom Internet getrennt werden und ob Sicherungen vorhanden sind.
Beseitigen	Das Problem wurde eingedämmt, und das Sicherheitspersonal ergreift Schritte, um das Problem zu beheben.
Wiederherstellen	Das Problem wurde gelöst, und die Betriebsbereitschaft der betroffenen Systeme wird überprüft.
Prüfung	Der Security Incident ist abgeschlossen, und alle Systeme funktionieren wieder normal. Eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

status der Security Incident-Prozessdefinition (Fortsetzung)

Status	Beschreibung
	Überprüfung nach dem Incident ist jedoch weiterhin erforderlich.
Geschlossen	Der Incident ist abgeschlossen, aber bevor ein Security Incident geschlossen werden kann, müssen Sie die Informationen in eingeben **Abschlussinformationen** Registerkarte.

Definitionen des Prozesses für Security Incident-Aufgaben

Die folgenden Prozessdefinitionen werden für Security Incident-Aufgaben verwendet.

definitionsstatus des Aufgabenprozesses

Status	Beschreibung
Bereit	Die Aufgabe kann bearbeitet werden, nachdem sie einem Service Desk-Mitarbeiter zugewiesen wurde.
Zugewiesen	Die Aufgabe ist einem Service Desk-Mitarbeiter zugewiesen.
In Bearbeitung	Der zugewiesene Service Desk-Mitarbeiter arbeitet an der Aufgabe.
Abschließen	Die Aufgabe ist abgeschlossen.
Abgebrochen	Die Aufgabe wurde abgebrochen.

NIST unterstützt die folgenden beiden Modelle:

- **NIST Stateful**

  Mit dieser Prozessdefinition können Analysten sequenziell von einem Status in einen anderen wechseln, ohne einen Schritt zu überspringen. Beispiel: Wenn der Analyst mit beginnt **Entwurf** status, dann ist die sequenzielle Reihenfolge dieser Prozessdefinition **Entwurf** > **Analyse** > **Enthalten** > **Beseitigen** > **Wiederherstellen** . Daher ist die NIST Stateful-Prozessdefinition unidirektional und ermöglicht es Analysten nur, nur in die vorwärtsstatus zu gelangen.

  Hier ist ein weiteres Beispiel: Wenn der Analyst mit dem Analysestatus beginnt, ist die sequenzielle Reihenfolge dieser Prozessdefinition **Analyse** > **Enthalten** > **Beseitigen** > **Wiederherstellen** .

- **NIST Open**

  Mit dieser Prozessdefinition können Analysten von einem Status in einen anderen wechseln, entweder vorwärts oder rückwärts. Beispiel: Wenn der Analyst mit beginnt **Analyse** status, dann kann die Reihenfolge der Prozessdefinition entweder sein **Analyse** > **Enthalten** > **Beseitigen** > **Wiederherstellen** Oder **Analyse** > **Entwurf** . Daher ist die Prozessdefinition „NIST Offen“ bidirektional und ermöglicht es Analysten, je nach Anforderungen in den Vorwärts- oder rückwärtsstatus zu wechseln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswahl Des Prozesses Für Die Reaktion Auf Security Incidents

Security Incident Response Prozessauswahl listet Prozesse mit ungültigen status für Security Incidents und Antwortaufgaben auf.

Ein Administrator kann den Incident oder die Aufgabe manuell oder mithilfe eines Skripts in gültige status korrigieren. Eine leere zugehörige Liste (keine Incidents, keine Aufgaben) gibt an, dass sich jede aktive Aufgabe in einem gültigen Status befindet. Verfügbare status variieren je nach aktuellem Status des Incident. Weitere Informationen finden Sie unter Korrektur ungültiger Status von Security Incidents oder Aufgaben mit Prozessdefinitionen.

Wählen Sie ein aus Security Incident Response Prozessdefinition

Sie können die Prozessdefinition auswählen, die für die entsprechenden status für Security Incidents und Antwortaufgaben Ihres Unternehmens verwendet werden soll.

Vorbereitungen

Erforderliche Rolle: admin und sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Security Incident Response** > **Administration** > **Prozessauswahl**an.
2. Klicken Sie auf das Suchsymbol, um die verfügbaren Prozessdefinitionen aufzulisten.

3. Wählen Sie eine Prozessdefinition aus.
4. Klicken Sie auf **Aktualisieren**.

Erstellen Sie eine anwenderdefinierte Security Incident Response Skripteinbindung der Prozessdefinition

Erstellen Sie ein anwenderdefiniertes Prozessdefinitionsskript für die entsprechenden status für Security Incidents und Antwortaufgaben Ihres Unternehmens.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Das Hauptskript „sn_si.ProcessDefinition“ steuert Prozessdefinitionen. **Prozessdefinition** Bestimmt, welche Definition verwendet wird (mit **Prozessauswahl**). Ruft die entsprechende Skripteinbindungsdatei auf, um die anfänglichen status und Übergänge für Security Incidents und Antwortaufgaben zu bestimmen.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Skripteinbindungen**an.
2. Klicken Sie auf **Neu**.

Automatische Übersetzung

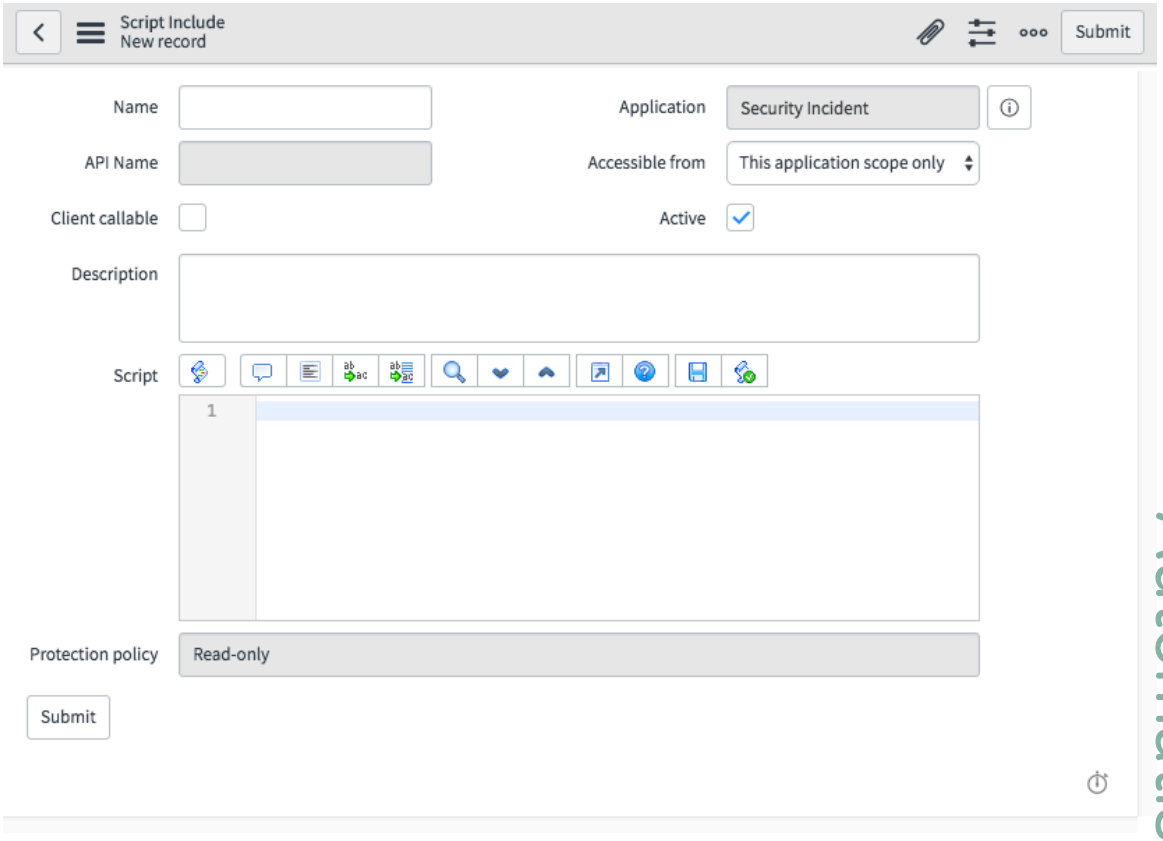
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie die Felder entsprechend aus.

Prozessdefinitionen werden erstellt

Feld	Beschreibung
Name	Name dieser Skripteinbindung.
API-Name	Erstellt basierend auf dem Namen der Skripteinbindung.
Vom Client aufrufbar	Macht die Skripteinbindung für Client-Skripts, Listen- und Berichtsfilter, Referenzqualifizierer oder verfügbar , Wenn angegeben , Als Teil der URL.
Anwendung	Security Incident
Zugänglich von	Wählen Sie Aus **Nur dieser Anwendungsbereich** .
Aktiv	Wenn diese Option aktiviert ist, kann diese Skripteinbindung aus der ausgewählt werden **Prozessdefinition** Seite.
Beschreibung	Hilfreiche Informationen zur Skripteinbindung.
Skript	Definiert das serverseitige Skript, das ausgeführt werden soll, wenn es von anderen Skripts aufgerufen wird. Das Skript muss eine einzelne JavaScript-Klasse oder eine globale Funktion definieren. Der Klassen- oder Funktionsname muss mit dem Wert im Feld Name übereinstimmen. Informationen zu Skriptinhalten finden Sie unter Skripteinbindung der Prozessdefinition.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Skripteinbindung der Prozessdefinition

Skripteinbindung der Prozessdefinition

Die Skripteinbindung „Prozessdefinition“ bietet Methoden zum Definieren einer Prozessdefinition.

Implementieren Sie die hier beschriebenen Konstanten, Attribute, Arrays und Methodenaufrufe, um eine Skripteinbindung für Prozessdefinitionen anzupassen.

Verwendungszweck

Verwenden Sie diese Skripteinbindung, um eine Prozessdefinition zu erstellen.

Skripteinbindungstext

Der Textkörper der Skripteinbindung besteht aus drei Abschnitten:

- Konstanten: Definitionen des Anfangsstatus
- Security Incident und Antwortaufgabe: Prozessdefinitions-Arrays
- Methodenaufrufe: Informationen werden abgerufen

Konstanten

Konstanten werden verwendet, um die anfangsstatus von Security Incidents und Antwortaufgaben zu definieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Verwendung von Konstanten ist optional, wird jedoch aus Gründen der Lesbarkeit empfohlen. Zum Beispiel:

```
INITIAL_INCIDENT_STATE: 10,
INITIAL_TASK_STATE: 1,
```

Welche später von den folgenden Methoden verwendet werden:

```
getInitialIncidentState: function() {
return this.INITIAL_INCIDENT_STATE;
},
getInitialTaskState: function() {
return this.INITIAL_TASK_STATE;
},
```

Der nächste Satz von Konstanten definiert die status für Security Incidents und Antwortaufgaben.

Jedes Array enthält auch die Definition, welche status verfügbar sind, wenn sich der Incident oder die Aufgabe in einem bestimmten Status befindet.

Zum Beispiel:

```
TASK_STATES: [{state:1, label:"Draft", choice:[1, 10]},
 {state:10, label:"Ready", choice:[10, 16]},
 {state:16, label:"Assigned", choice:[16, 18]},
 {state:18, label:"Work in Progress", choice:[18, 3]},
 {state:3, label:"Close Complete", choice:[]},
 {state:7, label:"Cancelled", choice:[]},
 ],
```

Das Beispiel ist ein Array von Objekten. Jedes Objekt definiert einen Status und mögliche übergangsstatus.

Die Reihenfolge des Statusobjekts bestimmt die gewünschte Reihenfolge für den Flow.

Wenn sich die Aufgabe im Status „Entwurf“ (Wert 1) befindet, sind folgende status möglich: 1 (Entwurf, was keine Änderung ist) und 10 (bereit, der nächste Schritt im Prozess).

Es gibt keine Beschränkung für die Anzahl der Übergänge aus einem Status. Die Status „Abgeschlossen“ und „Abgebrochen“ sind endgültige status und weisen daher keine möglichen Statusübergänge auf.

Die Reihenfolge der Attribute im Objekt ist nicht wichtig. Wenn die Definition klarer wird, setzen Sie die Bezeichnung zuerst.

Attribute

Erforderliche Attribute in einem Statusdefinitionsobjekt sind:

- status: Numerischer Wert des Status
- Bezeichnung: Visuell lesbarer Text, der dem Status zugeordnet ist
- Auswahl: Ein Array von Statuswerten, in die der Status übergehen kann (bestimmt den Inhalt der Dropdown-Liste „Status“)

Optionale Attribute sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Obligatorisch: Liste der Feld-IDs, die in diesem Status obligatorisch werden
- Schreibgeschützt: Liste der Feld-IDs, die in diesem Status schreibgeschützt werden
- Sichtbar: Liste der Feld-IDs, die in diesem Status sichtbar werden
- Nicht obligatorisch: Liste der Feld-IDs, die in diesem Status nicht obligatorisch werden
- Nicht sichtbar: Liste der Feld-IDs, die in diesem Status nicht mehr sichtbar wären

Hinweis:

Wenn optionale Attribute verwendet werden, liegt es in der Verantwortung des Autors sicherzustellen, dass Felder zwischen status sichtbar/unsichtbar, obligatorisch/nicht obligatorisch, sichtbar/ausgeblendet oder schreibgeschützt werden.

Wenn Sie beispielsweise ein Feld in einem Status ausblenden, wird es später nicht in einem anderen Status sichtbar, es sei denn, das Attribut „sichtbar“ wird verwendet.

Prozessfluss-Definitions-Arrays

Um die Informationen zu definieren, die im Prozess-Flow-Formatierer (der Balken oben in den Formularen „Security Incident“ und „Antwortaufgabe“) angezeigt werden, benötigt das System Informationen darüber, was für jeden Status angezeigt werden soll.

Zum Beispiel:

```
TASK_PF: [{label:"Draft", condition:"state=1^EQ", description:"<p>Security Incident Response Task is in draft</p>"},
{label:"Ready", condition:"state=10^EQ", description:"<p>Security Incident Response Task is ready to be assigned</p>"},
{label:"Assigned", condition:"state=16^EQ", description:"<p>Security Incident Response Task is assigned</p>"},
{label:"Work in Progress", condition:"state=18^EQ", description:"<p>Work has started on this Security Incident Response Task</p>"},
{label:"Closed", condition:"state=3^ORstate=4^ORstate=7^EQ", description:"<p>Security Incident Response Task is complete</p>"},
],
```

Das TASK_PF-Array ist eine Sammlung von Bezeichnungen, Bedingungen und Beschreibungen, die verwendet werden, um den in der Prozessformatierer-Leiste angezeigten Text (einschließlich Reihenfolge und Aktivität) zu bestimmen.

Im Beispiel ist der Text „bereit“ das zweite angezeigte Element. Wird hervorgehoben, wenn die Aufgabe die Bedingung „State=10^EQ“ erfüllt hat.

Wenn der Zeiger auf den Text zeigt, wird die Beschreibung „Security Incident Response-Aufgabe ist bereit für Zuweisung“ angezeigt.

Hinweis:

Status können zu einem einzelnen Formatierer-Status kombiniert werden.

Im Beispiel werden sowohl die status „Abgeschlossen“ als auch „Abgebrochen“ in der oberen Leiste als „Geschlossen“ angezeigt.

Methodenaufrufe

Die folgenden Methoden müssen in der Skripteinbindung vorhanden sein, da sie von sn_si.ProcessDefinition verwendet werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rückgabetyp	Methodenübersicht	Beschreibung
Zeichenfolge	GetInitialIncidentState: Function()	Gibt den numerischen Wert des anfänglichen Incident-Status zurück
Zeichenfolge	GetInitialTaskState: Function():	Geben Sie den numerischen Wert des anfänglichen Aufgabenstatus zurück
Array von Zeichenfolge	GetIncidentStates: Function():	Gibt das Array des Incident-Status zurück
Array von Zeichenfolge	GetTaskStates: Function():	Gibt das Array des Aufgabenstatus zurück
Array von Objekten	GetIncidentProcessFlows: Funktion():	Gibt das Array der Incident-Prozess-Flow-Definition zurück
Array von Objekten	GetTaskProcessFlows: Funktion():	Geben Sie das Array der Flow-Definition für den Aufgabenprozess zurück

Der nächste Satz von Methoden wird immer aufgerufen, wenn ein Incident oder eine Aufgabe aktualisiert wird, und ermöglicht das Ausführen von Aktionen für bestimmte Change-Übergänge.

Rückgabetyp	Methodenübersicht	Beschreibung
void	PerformIncidentStateChange: Funktion (aktuell, zurück)	In den Beispielen wird diese Methode verwendet, um SM-bezogene Werte festzulegen und sicherzustellen, dass ein Incident von „Entwurf“ entfernt wird, sobald ihm jemand zugewiesen wurde.
void	PerformTaskStateChange: Funktion (aktuell, zurück)	Im Beispiel wird diese Methode verwendet, um Zeitstempel (bei Zuweisung und Abschluss) zu aktualisieren und die Aufgabe von „bereit“ zu „zugewiesen“ zu ändern, sobald das Feld „assigned_to“ ausgefüllt ist.

Die gleichen Aktionen, die mit diesen beiden Methoden ausgeführt werden, können mit einer Business-Regel ausgeführt werden. Durch die Definition in der Skripteinbindung wird das Wechseln von Prozessdefinitionen erleichtert.

Korrektur ungültiger Status von Security Incidents oder Aufgaben mit Prozessdefinitionen

Ein Administrator kann den Security Incident oder die Aufgabe manuell oder mithilfe eines Skripts in einen gültigen status korrigieren. Verfügbare status variieren je nach aktuellem Status des Incident.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

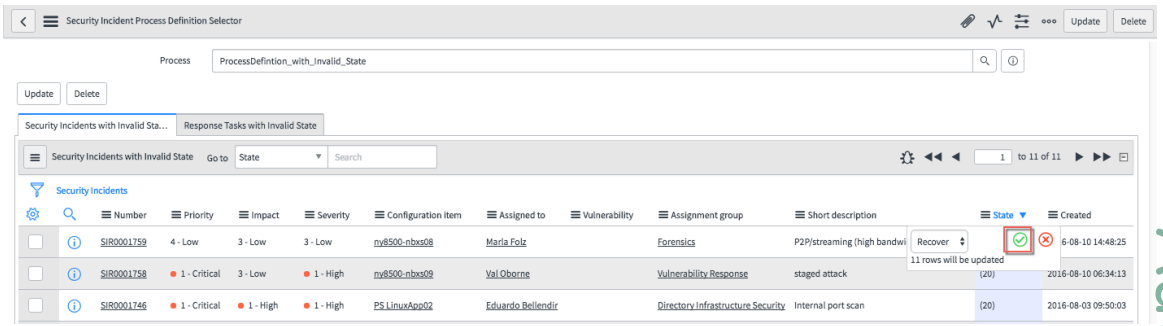
Nachdem Sie Prozessdefinitionen gewechselt haben, unterstützt die neue Definition möglicherweise einige der alten status nicht. Um den status von verwaisten Incidents oder Aufgaben zu korrigieren, können Sie Folgendes korrigieren Ändern Sie Ihre Prozessdefinition , Bearbeiten Sie Ihre Skripteinbindung , Oder öffnen Sie jeden Incident oder jede Aufgabe manuell, um den Status zu aktualisieren. Im Allgemeinen ist das Aktualisieren des Status (das in einem Massenvorgang durchgeführt werden kann) die einfachste Lösung.

Um status in einem Massenvorgang zu ändern, gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Prozessauswahl**an.
2. Heben Sie hervor **Status** Feld für die Incidents oder Aufgaben, die Sie ändern möchten.
3. Doppelt- Klicken Sie auf **Status** Wählen Sie im ersten Datensatz das neue aus **Status,** Und klicken Sie auf das grüne Häkchen ( ), um den Change abzuschließen.



4. Klicken Sie auf **Aktualisieren**.

Erstellen Sie eine Security Incident-Gruppe

Richten Sie eine Security Incident-Gruppe ein, und weisen Sie der Gruppe die entsprechenden Rollen und Anwender zu.

Vorbereitungen

Erforderliche Rollen:

- Wenn Sie über die Rolle user_admin verfügen, können Sie Security Incident-Zuweisungsgruppen erstellen.
- Wenn Sie die Rolle sn_si.admin innehaben, können Sie Security Incident-Zuweisungsgruppen erstellen und bearbeiten.

Warum und wann dieser Vorgang ausgeführt wird

Anwender in einer Gruppe erben die Rollen der Gruppe, daher müssen Sie nicht jedem Anwender Rollen separat zuweisen.
Es ist eine gute Praxis, in Ihrer Organisation so viele Gruppen wie erforderlich zu erstellen. Es empfiehlt sich auch, eine Gruppe für Administratoren zu erstellen und nur dieser Gruppe die Administratorrolle zuzuweisen.

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen** oder **Security Incident** > **Setup** > **Gruppen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Hinweis:

Weitere Informationen finden Sie unter Erstellen Sie eine Anwendergruppe .

4. Stellen Sie sicher, dass Sie auswählen **Security Incident** Typ für diese Gruppe.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wenn **Typ** Feld ist nicht sichtbar. Konfigurieren Sie das Formular, um es hinzuzufügen.

b. Klicken Sie auf das Schlosssymbol neben dem Feld **Typ**.

c. Klicken Sie auf das Referenzsuchsymbol ( )

d. Suchen Sie nach , und wählen Sie aus **Security Incident** Typ.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. In **Rollen** Zugehörige Liste: Fügen Sie die Rollen hinzu, die jedes Mitglied dieser Gruppe erhält.
   Beispiel: Wenn Sie eine Gruppe für erstellen Security Incident Response Teammitglieder, fügen Sie sn_si.Analyst hinzu. Wenn Sie eine Gruppe für erstellen Security Incident Response Administratoren, fügen Sie sn_si.admin hinzu.
7. In **Gruppenmitglieder** Zugehörige Liste: Fügen Sie dieser Gruppe Anwender hinzu.
8. Klicken Sie auf **Aktualisieren**.

Erstellen Sie eine Security Incident-Rechnergruppe

Security Incident-Rechnergruppen werden zum Gruppieren von Rechnern verwendet.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **Security Incident-Rechnergruppen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name des Security Incident-Rechners.
Anwendung	Die Anwendung, die diesen Datensatz enthält.
Reihenfolge	Die Reihenfolge, in der der Security Incident-Rechner ausgeführt wird. Ein Rechner mit einer Auftragseingabe von 100 wird vor einem Rechner mit einer Auftragseingabe von 200 ausgeführt.
Beschreibung	Eine Beschreibung dieser Rechnergruppe.
Erstellt von	Geben Sie den Namen des Anwenders ein, der erstellt hat

4. Klicken Sie auf **Absenden**.

Erstellen Sie einen Security Incident-Rechner

Mit Security Incident-Rechnern können Sie den Schweregrad eines Security Incidents basierend auf vordefinierten Formeln berechnen. Sie können nach Bedarf eigene Security Incident-Rechner definieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **Security Incident-Rechnergruppen**an.
2. Klicken Sie auf den Namen der Gruppe, für die Sie einen Rechner erstellen möchten, oder Sie können es Erstellen Sie eine Rechnergruppe .
3. Klicken Sie auf **Neu**.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name des Security Incident-Rechners.
Rechnergruppe	Name der Gruppe, zu der dieser Rechner gehört. **Hinweis:** Das Erstellen oder Ändern der Rechnergruppe ist verfügbar, nachdem Sie eine eingegeben haben **Name** Und **Tabelle** .
Tabelle	Wählen Sie die Tabelle aus, die für diesen Rechner verwendet werden soll. Wenn Sie Rechner zu anderen Tabellen als „Schwachstelle“ [sn_vul_Vulnerability] und „Angreifbares Element“ [sn_vul_vulnerable_item] hinzufügen, müssen Sie diesen Tabellen Business-Regeln und UI-Aktionen hinzufügen. So zeigen Sie Beispiele an: ○ Navigieren zu **Systemdefinition** > **Business-Regeln**, Und suchen Sie nach **Schweregrad Berechnen** Geschäftsregel in der Tabelle „Angreifbares Element“ [sn_vul_vulnerable_item]. ○ Navigieren zu **System-UI** > **UI-Aktionen**, Und suchen Sie nach **Schweregrad Berechnen** UI-Aktion für die Tabelle „Angreifbares Element“ [sn_vul_vulnerable_item]. Außerdem muss der Schwachstellen-Administratorrolle vollständige Lese-, Schreib- (oder Save_as_template)-Fähigkeiten in jeder von einem Rechner verwendeten Tabelle gewährt werden, um die auf die Vorlage anzuwendenden Werte ordnungsgemäß anzuzeigen.
Anwendung	Die bereichsbezogene Anwendung, zu der der Rechner gehört.
Reihenfolge	Die Reihenfolge, in der der Security Incident-Rechner ausgeführt wird. Ein Rechner mit einer Auftragseingabe von 100 wird vor einem Rechner mit einer Auftragseingabe von 200 ausgeführt.
Aktiv	Aktivieren oder deaktivieren Sie den Rechner.
Beschreibung	Eine Beschreibung dieses Rechners.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die **Bedingungen** Und **Anzuwendende Werte** Registerkarten werden angezeigt.
6. Füllen Sie die Felder im aus **Bedingungen** Registerkarte entsprechend.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Filtergruppe verwenden	Aktivieren Sie dieses Kontrollkästchen, um eine vordefinierte Filtergruppe oder zu verwenden Erstellen Sie eine neue Filtergruppe Zum Definieren der Rechnerkriterien.
Filtergruppe	Wählen Sie die Filtergruppe aus, die zum Definieren eines Rechners verwendet werden soll. Dieses Feld wird nur angezeigt, wenn Sie ausgewählt haben **Verwenden Sie Filtergruppen** Kontrollkästchen.
Erweiterte Bedingung verwenden	Aktivieren Sie dieses Kontrollkästchen, um anzugeben, dass eine Skriptbedingung verwendet wird, um zu bestimmen, wann dieser Rechner angewendet wird. Wenn Sie das Kontrollkästchen aktivieren, eine **Erweiterte Bedingung** Das Feld „Skripting“ wird angezeigt. Wenn Sie ausgewählt haben **Verwenden Sie die Filtergruppe** Kontrollkästchen, dieses Feld ist ausgeblendet. **Hinweis:** Bevor Sie erweiterte Bedingungen definieren und Skripts schreiben, um zu bestimmen, wann die Security Incident-Rechner angewendet werden, kehren Sie zur Liste Security Incident-Rechner zurück. Erkunden Sie die mit dem Basissystem gelieferten Rechnerdatensätze.
Bedingung	Definiert grundlegende Filterbedingungen zur Bestimmung, ob der Rechner verwendet wird. Wenn Sie eine der Optionen ausgewählt haben **Verwenden Sie die Filtergruppe** Oder **Erweiterte Bedingungen verwenden** Kontrollkästchen, dieses Feld ist ausgeblendet.

7. Klicken Sie auf **Anzuwendende Werte** Registerkarte und füllen Sie die Felder im Formular entsprechend aus.
   Sie können ein Skript zum Definieren der Werte erstellen, die auf die Berechnung angewendet werden sollen, oder eine Vorlage basierend auf Feldern in der ausgewählten Tabelle definieren.

Feld	Beschreibung
Skriptwerte verwenden	Aktivieren Sie dieses Kontrollkästchen, um Feldwerte mit einem Skript zu definieren.
Skriptwerte	Definiert, auf welche Werte die Berechnungen angewendet werden sollen. Dieses Feld wird nur angezeigt, wenn Sie ausgewählt haben **Verwenden Sie Skriptwerte** Kontrollkästchen.
Vorlage	Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**. Wählen Sie die Felder und Werte aus, die Sie für den Rechner verwenden möchten.

8. Wenn Sie alle Einträge abgeschlossen haben, klicken Sie auf **Übermitteln** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verstehen von Security Incident-Rechnern

Security Incident-Rechner werden verwendet, um Datensatzwerte zu aktualisieren, wenn vordefinierte Bedingungen erfüllt sind. Die Rechner werden basierend auf den Kriterien gruppiert, die verwendet werden, um zu bestimmen, wie die Datensätze aktualisiert werden.

Die Security Incident Response Das Basissystem enthält die folgenden Security Incident-Rechnergruppen und -Rechner. In jeder Gruppe wird der erste Rechner ausgeführt, der den Bedingungen entspricht.

Security Incident-Rechner im Basissystem

Gruppenname Des Security Incident-Rechners	In der Gruppe enthaltene Rechner	Beschreibung
Geschäftsauswirkung	Aus Schweregradrechnern zusammenfassen	Dieser Rechner delegiert an den Sicherheitsrelevanzrechner, der die Relevanz durch Gewichtung der Werte anderer Felder bestimmt.
Schweregrad	Geschäft betroffen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines einfachen Bedingungsgenerators.
	Wichtiger Service betroffen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe einer erweiterten Bedingung. Wenn das Konfigurationselement im Security Incident einem äußerst kritischen Business-Service zugeordnet ist, wird die **Risikopunktzahl** , **Geschäftsauswirkung** , Und **Priorität** Felder werden wie vom Rechner definiert erhöht.
	Kritische Serviceänderungen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe einer erweiterten Bedingung. Wenn der Security Incident die Bedingungen erfüllt, wird ein Skript ausgeführt, um zu definieren, auf welche Ebenen die Felder hochgestuft werden. Wenn das Konfigurationselement im Security Incident einem kritischsten oder etwas kritischen Business-Service zugeordnet ist, der **Risikopunktzahl** , **Geschäftsauswirkung** , Und **Priorität** Felder werden wie vom Rechner definiert erhöht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident-Rechner im Basissystem (Fortsetzung)

Gruppenname Des Security Incident-Rechners	In der Gruppe enthaltene Rechner	Beschreibung
	Mehrere Angriffsvektoren	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines einfachen Bedingungsgenerators. Wenn das Konfigurationselement im Security Incident Web-, E-Mail- und Identitätswechsel-Angriffsvektoren zugeordnet ist, wird die verwendet **Risikopunktzahl** , **Geschäftsauswirkung** , Und **Priorität** Felder werden wie vom Rechner definiert erhöht.
	Priorität mit Kategorie und Services festlegen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines erweiterten Bedingungsgenerators. Die Priorität des Security Incidents ist auf festgelegt **1: Kritisch** Wenn die folgenden Bedingungen erfüllt sind: • Dem Security Incident sind betroffene Services zugeordnet, und einer davon ist kritisch. • Die Kategorie „Security Incident“ ist eine der folgenden Kategorien: ◦ Denial of Service ◦ Spear-Phishing ◦ Böswillige Code-Aktivität **Hinweis:** Dieser Rechner ist im Basissystem verfügbar, wenn Sie die Preisstufe Starter Security Operations haben.
	Priorität für erkennbare Elemente festlegen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines erweiterten Bedingungsgenerators. Die Priorität des Security Incidents ist auf festgelegt **1: Kritisch** Wenn die folgenden Bedingungen erfüllt sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident-Rechner im Basissystem (Fortsetzung)

Gruppenname Des Security Incident-Rechners	In der Gruppe enthaltene Rechner	Beschreibung

		• Dem Security Incident sind betroffene Services zugeordnet, und einer davon ist kritisch.
		• Die Kategorie „Security Incident“ ist eine der folgenden Kategorien:
		  ○ Denial of Service
		  ○ Spear-Phishing
		  ○ Böswillige Code-Aktivität
		• Eines der zugeordneten erkennbaren Elemente oder Indikatoren hat eine Sichtungsanzahl, die zwei Sichtungen mit aktiven Indikatoren überschreitet (d. h. die erkennbaren Elemente oder Indikatoren werden aus mehreren Quellen als schlecht bestätigt).
		Hinweis: Dieser Rechner ist im Basissystem verfügbar, wenn Sie die Preisstufe „Advanced Security Operations“ haben und das Plugin „Threat Feeds“ aktivieren.

Anwenderrelevanz	Anwenderrelevanz abrufen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines einfachen Bedingungsgenerators. Dieser Schweregradrechner bewirkt, dass sich die Geschäftsrelevanz des Anwenders in ändert **1: Kritisch** Wenn **Abteilung** Feld wird in geändert **Finanzen** .
	Anwendergruppenrelevanz abrufen	Dieser Schweregradrechner definiert seine Auswahlkriterien mithilfe eines erweiterten Bedingungsgenerators. Dieser Schweregradrechner bietet ein Beispiel für einen Rechner, der für Daten in einer zugehörigen Liste ausgeführt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schweregradrechner

Wenn Sie einen Security Incident erstellen, wird die **Risikopunktzahl** , **Geschäftsauswirkung** , Und **Priorität** Felder enthalten Standardwerte. Wenn Sie den Incident speichern, validiert eine Geschäftsregel die Informationen im Security Incident automatisch anhand der in jedem Ihrer aktiven Schweregradrechner definierten Bedingungen. Sie werden jeweils ein Sicherheitsrechner in der von definierten Reihenfolge validiert **Reihenfolge** Feld in jedem Rechner. Wenn die Informationen im Security Incident den in einem der Rechner definierten Bedingungen entsprechen, werden die Feldwerte für den Schweregrad entsprechend den im Rechner festgelegten Regeln aktualisiert.

Angenommen, Sie erstellen einen Security Incident für ein betroffenes CI, und das CI ist sehr kritisch. Wenn der Security Incident gespeichert wird, werden die CI-Informationen mit den in den Schweregradrechnern definierten Bedingungen verglichen. Wenn der Security Incident anhand von validiert wird **Kritischer Service betroffen** Schweregradrechner, die Schweregradfelder werden automatisch aktualisiert, und oben im Security Incident wird eine Meldung ähnlich der folgenden angezeigt.

Severity Calculation applied: Critical service changes; Risk: High; impact: 1 - High; Priority: 1 - Critical; Severity: 1 - High

Sie können diese Schweregradrechner unverändert verwenden oder bearbeiten, um die Anforderungen Ihres Unternehmens besser zu erfüllen. Wenn Sie beispielsweise Web- und E-Mail-Bedrohungen identifizieren möchten, die für den Geschäftsbereich Finanzen spezifisch sind, können Sie die Bedingungen von ändern **Mehrere Angriffsvektoren** Rechner:

- [Angriffsvektor] [enthält] [Web]
- [Angriffsvektor] [enthält] [E-Mail]
- [Geschäftsbereich] [enthält] [Finanzen]

Sie können die Schweregradwerte in einem vorhandenen Security Incident auch jederzeit aktualisieren, indem Sie den Datensatz öffnen und auf klicken **Schweregrad Berechnen** Zugehöriger Link.

Security Incident-Risikopunktzahlrechner

Die **Legen Sie die Priorität mit Kategorie und Services fest** Und **Legen Sie die Priorität mit erkennbaren Elementen fest** Rechner werden verwendet, um eine Risikopunktzahl für einen Security Incident zu berechnen.

Anwenderrelevanzrechner

Die beiden Rechner in **Anwenderrelevanz** Gruppe (**Anwenderrelevanz abrufen** Und **Anwendergruppenrelevanz abrufen**) Geben Sie Beispiele dafür an, wie Sie die Relevanz basierend auf Kriterien fördern können, die in einem Anwenderdatensatz definiert sind, oder basierend auf der Gruppe, zu der ein Anwender gehört.

Sie können nach Bedarf bearbeitet werden, oder es können neue Anwender-Relevanzrechner erstellt werden.

Die **Anwenderrelevanz abrufen** Der Rechner bewirkt, dass sich die Geschäftsrelevanz des Anwenders in ändert **1: Kritisch** Wenn **Abteilung** Feld wird in geändert **Finanzen** .

Die **Anwendergruppenrelevanz abrufen** Der Rechner bewirkt, dass sich die Geschäftsrelevanz des Anwenders in ändert **1: Kritisch** Wenn der Anwender zu hinzugefügt wird **Datenbank** Gruppe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Anwendergruppenrelevanz abrufen Ist ein Beispiel für einen Rechner, der für Daten in einer zugehörigen Liste ausgeführt wird. Wenn Sie weitere Gruppen hinzufügen möchten, um eine Relevanzänderung zu initiieren, fügen Sie in der ersten Zeile des Skripts eine kommagetrennte Liste von Gruppen-sys_IDs hinzu. Beispiel: `VAR CRITICAL_GROUPS = [group1_sys_ID, group2_sys_ID, group3_sys_ID]` .

Berechnungen der Risikopunktzahl für Security Incidents

Die Risikopunktzahl wird als arithmetisches Mittel berechnet, das das Risiko basierend auf der Priorität eines Security Incidents, der Art des Security Incidents (Denial of Service, Spear Phishing oder böswillige Code-Aktivität) und der Anzahl der Quellen darstellt, die für einen Indikator eine fehlgeschlagene Reputationspunktzahl ausgelöst haben.

Die Risikopunktzahl hilft bei der Priorisierung der Security Incident-Arbeit für die Analysten.

Wichtig:
Informationen zur Verwendung des neuen Rechners für Risikopunktzahl finden Sie unter Definieren Sie die neuen Regeln für den Rechner der Risikopunktzahl.

Die **Legen Sie die Priorität mit Kategorie und Services fest** Und **Legen Sie die Priorität mit erkennbaren Elementen fest** Security Incident-Rechner Werden verwendet, um eine Risikopunktzahl für einen Security Incident zu berechnen. Darüber hinaus lösen die folgenden Business-Regeln die automatische Berechnung von Risikopunktzahlen aus:

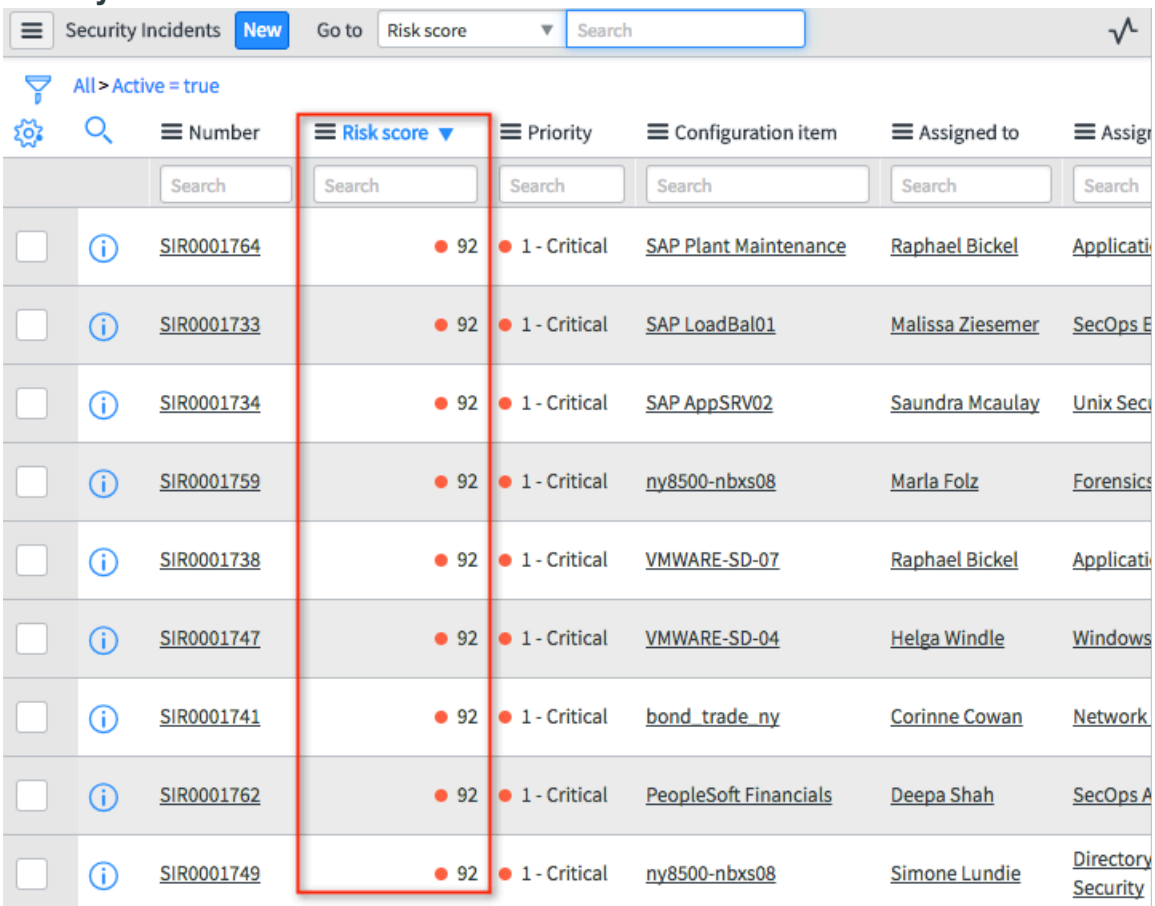
- Schweregrad berechnen
- Aktualisieren Sie die Risikopunktzahl
- SI-Risikopunktzahl aktualisieren

Hinweis:
Der im Basissystem verfügbare Risikorechner hängt von Ihrer Security Operations-Preisstufe ab.

Wenn Sie sich eine Liste von Security Incidents im Basissystem ansehen, beachten Sie die **Risikopunktzahl** Spalte.

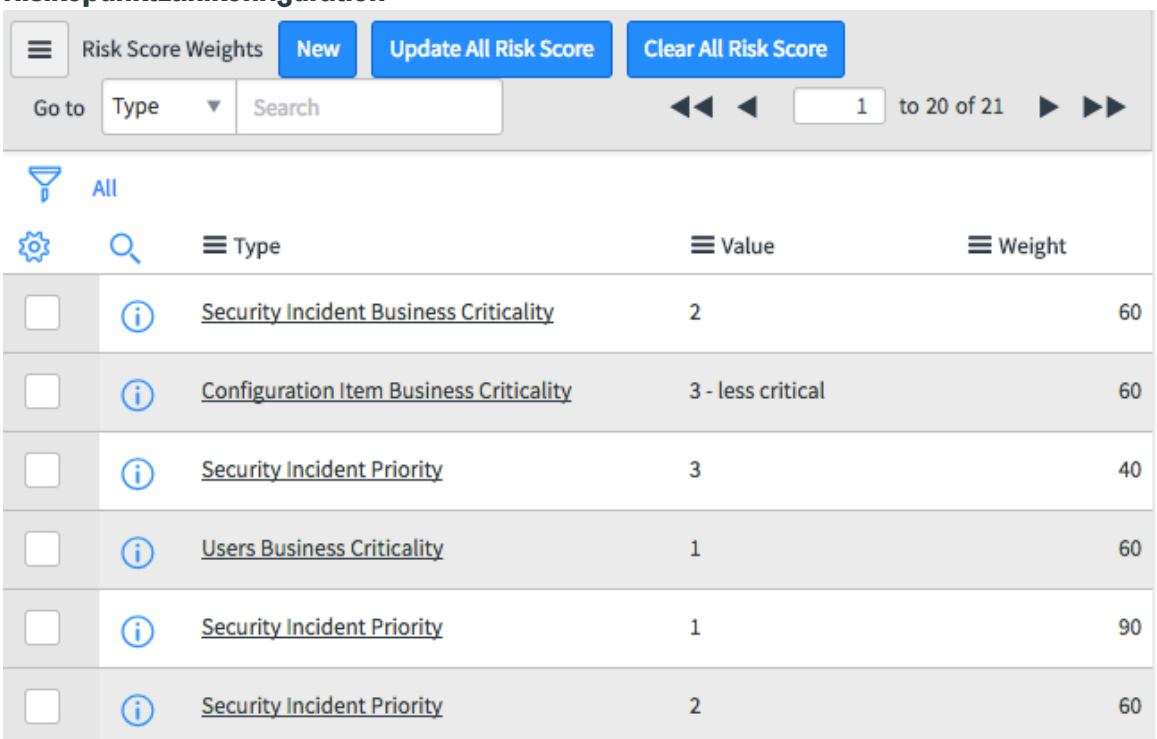
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incidents



Die Risikopunktzahl wird anhand der in definierten Gewichtungen berechnet **Konfiguration der Risikopunktzahl** .

Risikopunktzahlkonfiguration



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Wenn ein Security Incident einen hat **Geschäftsauswirkung** Auf festlegen **2 – Hoch** Und ein **Priorität** Auf festlegen **3 – Mittel** , Die jeweiligen Gewichtungen in der Tabelle mit Risikopunktzahlgewichtungen werden gesucht und so berechnet:

Security Incident – Geschäftsauswirkung Mit einem Wert von 2 = eine Gewichtung von 60.

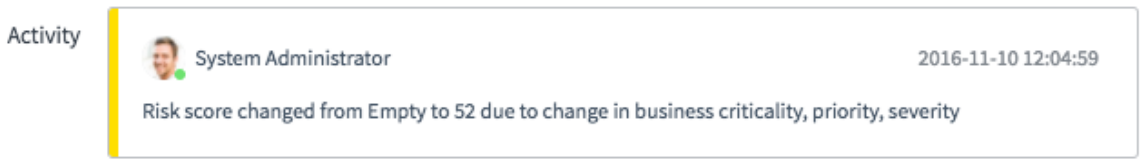
Security Incident-Priorität Mit einem Wert von 3 = eine Gewichtung von 40.

(60 + 40)/2 = eine Risikopunktzahl von 50.

Die Position des Security Incidents in der Security Incident-Liste wird dann basierend auf der aktualisierten Risikopunktzahl neu angeordnet.

Wenn im obigen Beispiel die **Geschäftsauswirkung** Oder **Priorität** Der Security Incidents werden geändert, die Risikopunktzahl wird neu berechnet, und die Änderungen werden in den Arbeitsnotizen berücksichtigt.

Arbeitsnotizen



Die Arbeitsnotizen werden aktualisiert, wenn die folgenden Felder geändert werden (wodurch die Risikopunktzahl aktualisiert wird):

- **Geschäftsauswirkung** Im Formular „Security Incident“
- **Priorität** Im Formular „Security Incident“
- **Schweregrad** Im Formular „Security Incident“ (standardmäßig ausgeblendet)
- **Geschäftsauswirkung** Auf der **Betroffene Anwender** Zugehörige Liste
- **Geschäftsauswirkung** Auf der **Betroffene Services** Zugehörige Liste
- **Geschäftsauswirkung** Auf Schwachstellen in **Angreifbare Elemente** Zugehörige Liste

Darüber hinaus werden die Arbeitsnotizen in den folgenden Situationen aktualisiert:

- Wenn eine Zuordnung zwischen betroffenen Anwendern und einem Security Incident erstellt oder geändert wird
- Wenn eine Zuordnung zwischen betroffenen Services und einem Security Incident erstellt oder geändert wird
- Wenn eine Zuordnung zwischen angreifbaren Elementen und einem Security Incident erstellt oder geändert wird

Arbeitsnotizen werden auch immer aktualisiert **Aktualisieren Sie Alle Risikopunktzahlen** Und **Löschen Sie Alle Risikopunktzahlen** Auf der Gewichtungen Der Risikopunktzahl Formular angeklickt.

Verwalten Sie Risikopunktzahlgewichtungen

Die Gewichtungen der Risikopunktzahl, die zur Berechnung der Risikopunktzahlen in Security Incidents verwendet werden, können einzeln entfernt oder aktualisiert werden. Sie können auch für alle Security Incidents entfernt oder aktualisiert werden. Die Möglichkeit, sie aus Security Incidents zu entfernen, ist nützlich, wenn Gewichtungswerte geändert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Hinweis:
Benutzer mit der Rolle „sn_si.read“ können die Konfiguration der Risikopunktzahl in anzeigen Security Incident Response.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **Konfiguration der Risikopunktzahl**an.

   Hinweis:
   Benutzer mit der Rolle „sn_si.read“ können die Konfiguration der Risikopunktzahl anzeigen, indem sie zu navigieren **Security Incident** > **Warnungen und Ereignisse** > **Risikopunktzahlkonfiguration**an.

2. Klicken Sie auf, um eine neue Gewichtung der Risikopunktzahl hinzuzufügen **Neu** Und geben Sie Informationen in die Felder ein.

Feld	Beschreibung
Typ	Wählen Sie den Typ der Risikopunktzahl aus, die Sie definieren.
Wert	Geben Sie den Wert an, der dem ausgewählten Typ zugeordnet ist. Wenn für den Typ mehrere Werte verfügbar sind, möchten Sie möglicherweise mehrere Datensätze zur Gewichtung der Risikopunktzahl definieren. Beispiel: Security Incident-Priorität mit einem Wert von 1, Security Incident-Priorität mit einem Wert von 2 usw.
Gewichtung	Die Gewichtung, die dem ausgewählten Typ/Wert-Paar zugeordnet ist. Gültige Einträge liegen zwischen 0 und 100, wobei 0 die niedrigste Gewichtung und 100 die höchste ist.

3. Klicken Sie auf **Absenden**.
4. Führen Sie bei Bedarf einen dieser Schritte aus.
   - Um einen Datensatz zur Gewichtung einer Risikopunktzahl zu löschen, öffnen Sie ihn aus der Liste, und klicken Sie auf **Löschen** .
   - Klicken Sie auf, um alle Datensätze zur Gewichtung der Risikopunktzahl zu löschen **Löschen Sie Alle Risikopunktzahlen** .
   - Klicken Sie auf, um alle Datensätze zur Gewichtung der Risikopunktzahl zu aktualisieren **Aktualisieren Sie Alle Risikopunktzahlen** .

Erstellen Sie einen Security Incident Response SLA

Sie können eine Servicelevel-Vereinbarung (Service Level Agreement, SLA) für definieren Security Incident Response.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Setup** > **SLAs**an.
2. Klicken Sie auf **Neu**.
   Feldbeschreibungen und detaillierte Anweisungen finden Sie unter Create an SLA definition .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Reparieren Sie Security Incident-SLAs

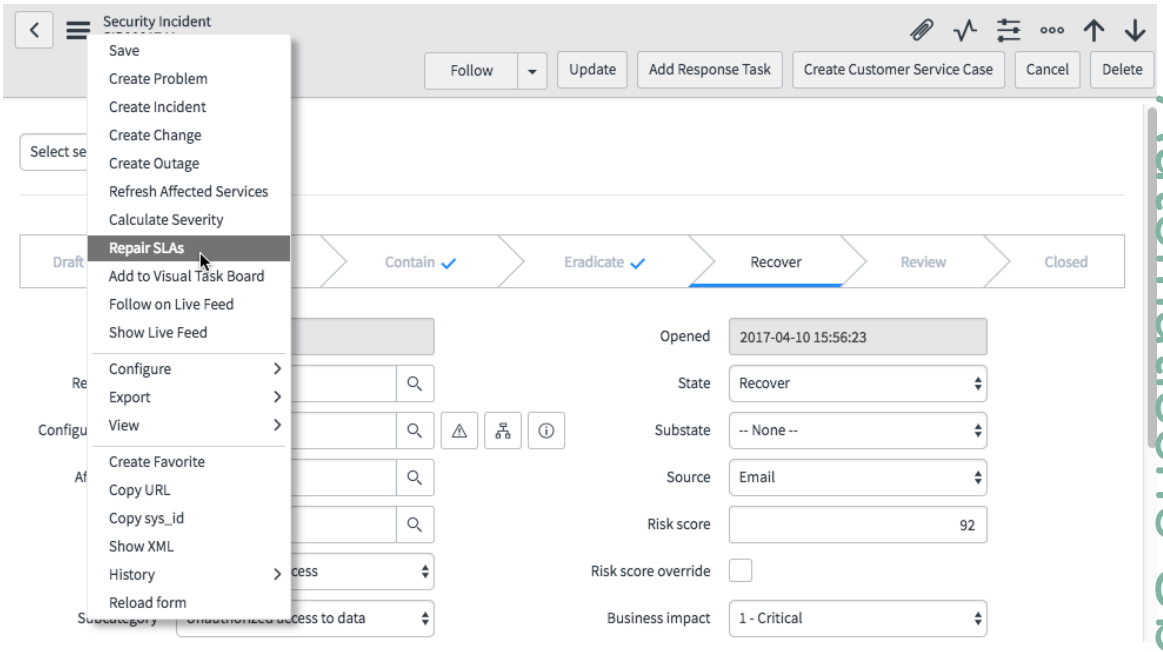
Sie können SLA-Datensätze reparieren, um sicherzustellen, dass SLA-Timing- und -Dauerinformationen korrekt sind.

Vorbereitungen

Erforderliche Rolle: sn_si.Basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie SLAs reparieren möchten.
2. Klicken Sie auf das Kontextmenü des Formularheaders, und wählen Sie aus **Reparieren Sie SLAs** :



3. Klicken Sie Auf **OK** Im Bestätigungsfeld Warnung.
   Weitere Informationen finden Sie unter Reparieren Sie SLAs .

Erstellen Sie ein Security Incident Response-Runbook

Ein Runbook ist eine Zuordnung zwischen einem veröffentlichten wissensartikel und einer bestimmten Aufgabe. Während Sie die Aufgabe ausführen, wird automatisch ein wissensartikel im Runbook geöffnet, der Informationen enthält, die für die Aufgabe relevant sind.

Vorbereitungen

Es müssen Wissensartikel in vorhanden sein Security Incident Response Runbook-Knowledge Base. Wenn Sie Erstellen Sie einen Security Incident-wissensartikel , Stellen Sie sicher, dass Sie auswählen **Security Incident Response Runbook** In **Knowledge Base** Feld. Nachdem Sie den artikel veröffentlicht haben, können Sie auf klicken **Erstellen Sie Runbook** Schaltfläche.

Erforderliche Rolle: sn.si.Knowledge_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Runbooks während der Erstellung von Security Incidents oder Antwortaufgaben verwenden oder die Knowledge Base-Artikel in einem Runbook Aufgaben im Playbook zuordnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Manuelles Runbook** > **Neues Runbook erstellen**an.
2. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Wissensartikel	Wählen Sie einen wissensartikel aus, der in das Runbook aufgenommen werden soll.
Aktiv	Aktivieren Sie das Kontrollkästchen, um das Runbook über verfügbar zu machen **Filternavigator** .
Filtergruppe verwenden	Aktivieren Sie dieses Kontrollkästchen, um eine vordefinierte Filtergruppe oder zu verwenden Erstellen Sie eine neue Filtergruppe Zum Definieren der Runbook-Kriterien.
Filtergruppe	Wählen Sie die Filtergruppe aus, die zum Definieren eines Runbooks verwendet werden soll. Dieses Feld wird nur angezeigt, wenn **Verwenden Sie Filtergruppen** Das Kontrollkästchen ist aktiviert.
Tabelle	Wählen Sie entweder Security Incident [sn_si_Incident] oder aus Security Incident Response Aufgabe [sn_si_Task]. Wenn Sie ausgewählt haben **Verwenden Sie die Filtergruppe** Kontrollkästchen und eine Filtergruppe ausgewählt. Dieses Feld wird standardmäßig auf die Tabelle gesetzt, die der ausgewählten Filtergruppe zugeordnet ist.
Bedingung	Legen Sie die Bedingungen fest, die dieses Runbook mit dem Incident oder der Aufgabe verbinden. Wenn Sie ausgewählt haben **Verwenden Sie die Filtergruppe** Aktivieren Sie das Kontrollkästchen, und wählen Sie eine Filtergruppe aus, die **Bedingung** Felder werden nicht angezeigt.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Registerkarte Wissensartikeldetails und eine Reihe von Schaltflächen werden angezeigt.
4. Klicken Sie auf , um die Details des Runbooks anzuzeigen **Knowledge Base-Details** Registerkarte.
5. Um den wissensartikel so anzuzeigen, wie er dem Anwender angezeigt wird, klicken Sie auf **Artikel Anzeigen** .
6. An Bearbeiten Sie die Details des wissensartikels , Klicken Sie auf **Bearbeiten Sie Den Artikel** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Regeln, um von Anwendern gemeldete Phishing-Angriffe zu validieren

Wenn Ihre Mitarbeiter E-Mails erhalten, die Phishing-Angriffe zu sein scheinen, können sie sie Ihnen unter Verwendung einer Phishing-E-Mail-Adresse melden. Die verdächtige E-Mail wird anhand von Regeln validiert, die von Ihrer Organisation definiert wurden.

Vorbereitungen
Bevor E-Mail-Übereinstimmungsregeln zur Identifizierung potenzieller Phishing-Angriffe verwendet werden können, definieren Sie eine E-Mail-Adresse, an die von Ihren Mitarbeitern weitergeleitete E-Mails zur Verarbeitung gesendet werden. Sie haben die folgenden Optionen zum Definieren dieser E-Mail-Adresse (vorausgesetzt, Ihre Unternehmens-E-Mail-Domäne ist acme.com):

- Definieren Sie eine E-Mail-Adresse wie **acme+phishing@service-now.com** . Die **+Phishing** Tag wird von SMTP unterstützt, um das Filtern zu ermöglichen, und Ihre Instanz kann E-Mails empfangen, die an sie gesendet werden.
- Definieren Sie eine E-Mail-Adresse, z. B. **phishing@acme.com** (Ihr Exchange-Postfach), das sie wiederum an weiterleitet **acme+phishing@service-now.com** (Ihr Instanz-Postfach, das durch eine E-Mail-Weiterleitungsregel definiert wurde).

Erforderliche Rolle: sn_sec_cmn.write

Warum und wann dieser Vorgang ausgeführt wird
Wenn ein Mitarbeiter auf eine verdächtige E-Mail-Adresse stößt, sollte er sie als Anhang an Ihre Phishing-E-Mail-Adresse weiterleiten. Wenn die angehängte E-Mail mit einer Regel übereinstimmt, die eine Bedrohung definiert, wird ein Security Incident erstellt.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Vom Anwender Gemeldetes Phishing**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder nach Bedarf aus.

Formular „E-Mail-Übereinstimmungsregeln“

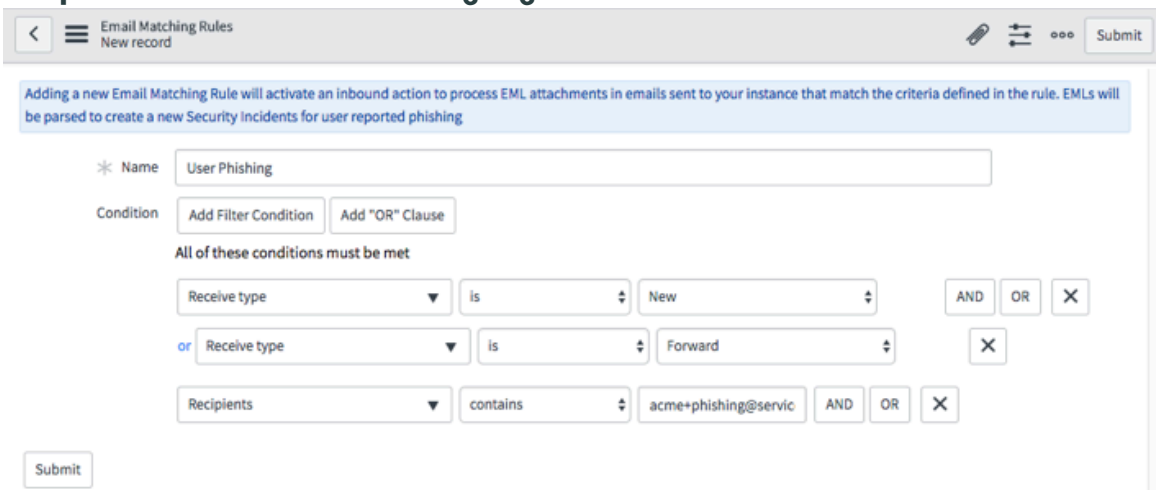
Feld	Beschreibung
Name	Name für diese E-Mail-Übereinstimmungsregel. Beispiel: Vom Anwender gemeldetes Phishing.
Bedingungen	Verwenden Sie den Bedingungsgenerator Dient zur Validierung, ob eine E-Mail, die an die Phishing-E-Mail-Adresse Ihres Unternehmens gesendet wird, ein Phishing-Angriff ist. Siehe folgendes Beispiel.

4. Klicken Sie auf **Absenden**.

Example:
Dieses Beispiel zeigt eine Übereinstimmungsregel für die Behandlung von vom Anwender gemeldetem Phishing.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für E-Mail-Übereinstimmungsregel



Konfigurieren Sie die Eigenschaften Sicherheitsanalyst-Arbeitsbereich

Konfigurieren Sie die Anwenderoberfläche des Incident-Datensatzes in Sicherheitsanalyst-Arbeitsbereich Um die Felder anzugeben, die angezeigt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Geben Sie die Felder an, die in Ihrem Incident-Datensatz angezeigt werden sollen, und geben Sie die Reihenfolge an, in der die Felder im Security Incident-Formular und im Antwortaufgabenformular angezeigt werden müssen. Sie können auch einen Grenzwert für die Anzahl der Felder festlegen, die angezeigt werden sollen.

Hinweis:

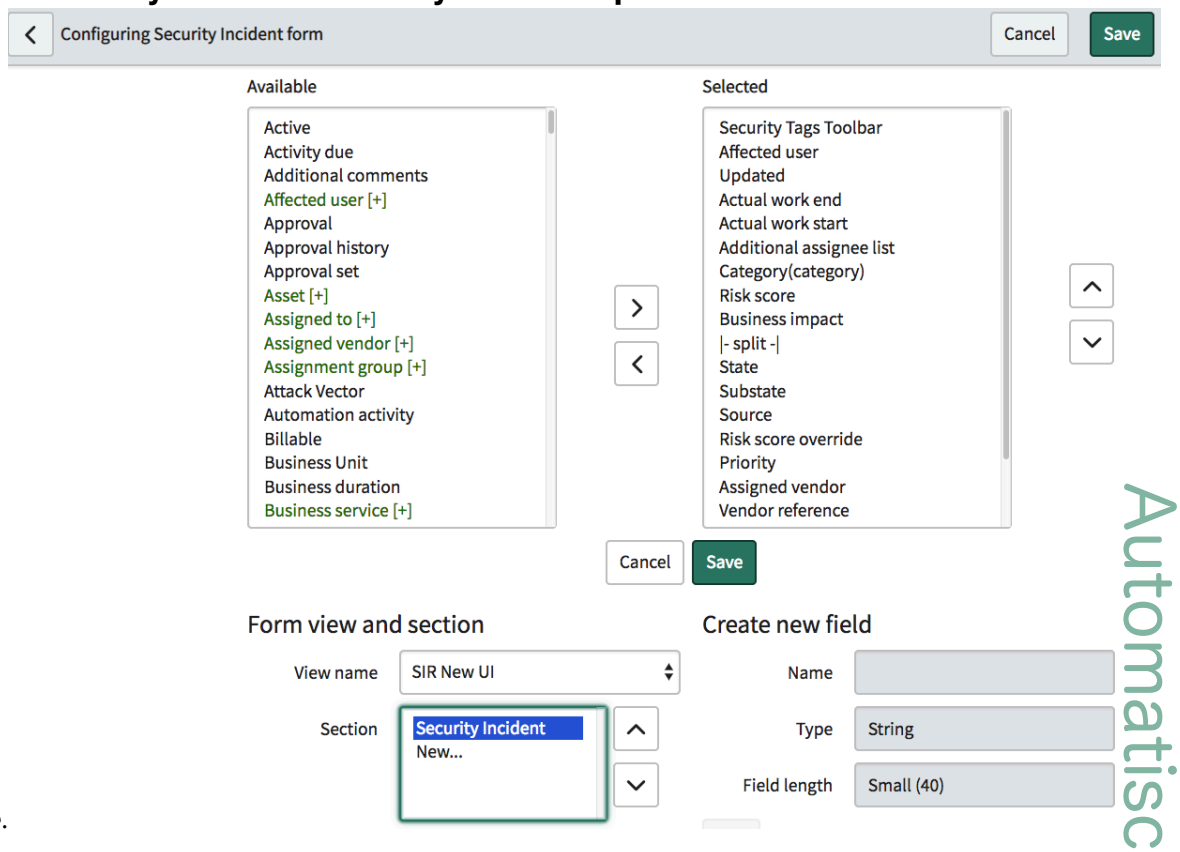
Sie können Regeln erstellen, um zu bestimmen, welche Ansicht für ein bestimmtes Formular verwendet werden soll. Das Basissystem enthält mehrere Ansichten, einschließlich der UI-Ansichten Standard und SIR New. Mehrere Ansichtsregeln sind ebenfalls im Lieferumfang des Basissystems enthalten, einschließlich der Regel „alle anderen Antwortaufgaben“. Diese Regel erzwingt die Standardansicht im Antwortaufgabenformular, wenn die in der Ansichtsregel angegebene Bedingung erfüllt ist. Die Sicherheitsanalyst-Arbeitsbereich Verwendet die SIR New-UI-Ansicht. Wenn die Formularfelder in angezeigt werden Sicherheitsanalyst-Arbeitsbereich Stimmen Sie nicht mit den Formularfeldern in der klassischen Umgebung überein, wahrscheinlich wird eine Ansichtsregel erzwungen. Zur Verwendung von **SIR – neue UI** Ansicht für das Formular müssen Sie die Ansichtsregel deaktivieren. Siehe Steuert, wann das System eine Ansicht anzeigt Für Details.

Prozedur

1. Navigieren Sie zu einer beliebigen Security Incident-Liste (z. B. **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**) an.
2. Klicken Sie zum Öffnen des Security Incident-Datensatzes auf einen Security Incident-Link.
3. Um zur Formularseite „Security Incident konfigurieren“ zu navigieren, klicken Sie auf Menüsymbol und wählen Sie aus **Konfigurieren** > **Formularlayout**an.
4. Von **Name der Ansicht** Liste, wählen Sie aus **SIR – neue UI** .
5. In **Abschnitt** Wählen Sie den entsprechenden Abschnitt aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dies kann sein **Security Incident** Oder **Security Incident Response-**



Aufgabe.

6. Wählen Sie die Felder und die Reihenfolge aus, in der sie im Incident-Banner in der neuen Anwenderoberfläche angezeigt werden sollen.
7. Klicken Sie auf **Speichern**.

Hinweis:

- Bestimmte Felder sind standardmäßig in den Bannern „Incident“ und „Antwortaufgabe“ ausgeblendet. Ändern Sie die Felder, die ausgeblendet oder angezeigt werden, indem Sie ändern `sn_app_secops_ui.form.excluded_fields.incident` Und `sn_App_secops_ui.Form.excluded_fields.response_Task` Eigenschaften wie in beschrieben Eigenschaften des Sicherheitsanalysten-Arbeitsbereichs.
- Geben Sie die Anzahl der Felder an, die in den Bannern für Incidents und Antwortaufgaben und in der ersten Zeile des Incident-Banners angezeigt werden können, indem Sie diese Eigenschaften festlegen:
  - sn_app_secops_ui.task_summary.single_summary.limit.incident
  - sn_App_secops_ui.Task_summary.Single_summary.limit.response_Task
  - sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line

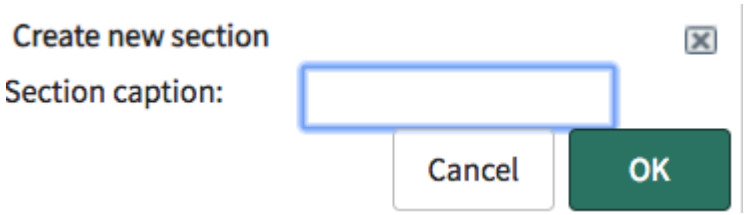
8. So konfigurieren Sie beispielsweise die Stile der gepunkteten Kreise, die neben einem Feldwert im Incident-Datensatz angezeigt werden: Navigieren Sie zu **System-UI** > **Feldstile** Und ändern oder erstellen Sie einen neuen Stildatensatz für die bestimmte Tabelle und den angegebenen Feldnamen.
   Die Eigenschaft „Hintergrundfarbe“ im Feld Stil des Stildatensatzes bestimmt die Farbe des gepunkteten Kreises.
9. Um das aktualisierte Incident-Banner anzuzeigen, klicken Sie auf **Security Incidents** > **Incidents (neue UI)** Zum Navigieren zum Incident-Datensatz in Sicherheitsanalyst-Arbeitsbereich Und aktualisieren Sie die Seite, um das aktualisierte Incident-Banner anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Um das Banner für Antwortaufgaben im Incident-Datensatz zu konfigurieren, navigieren Sie zu **Security Incidents** > **Antwortaufgaben** > **Alle Aufgaben anzeigen** Und wiederholen Sie die Schritte.
11. Wenn Sie eine neue Aufgabentabelle erstellen, die aus der Basistabelle „Security Incident Response Task“ erweitert wird, müssen Sie der Tabelle auch die UI-Ansicht SIR New hinzufügen.

    a. Von **Name Der Ansicht** Liste, wählen Sie aus **Neu** .



    b. Geben Sie Ein **SIR – neue UI** (Groß-/Kleinschreibung beachten) Klicken Sie im Fenster „neue Ansicht erstellen“ auf **OK** .

Ergebnisse

Die Security Incident- und Antwortaufgabenbanner werden in aktualisiert Sicherheitsanalyst-Arbeitsbereich(Verwalten Sie Sicherheitsbedrohungen mit Sicherheitsanalyst-Arbeitsbereich).

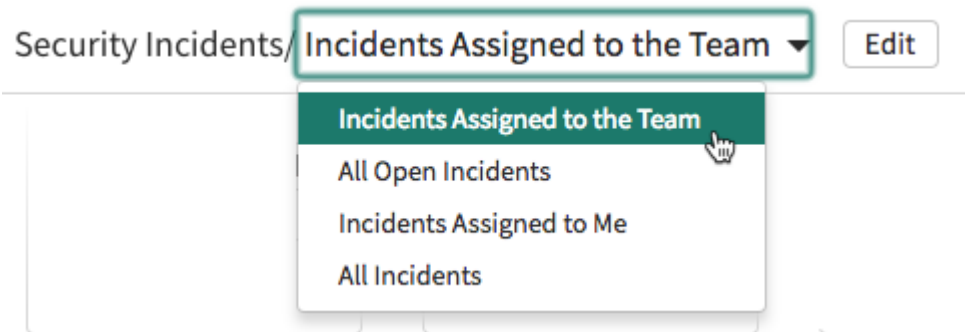
Richten Sie primäre und sekundäre Filter für ein Sicherheitsanalyst-Arbeitsbereich

Die Sicherheitsanalyst-Arbeitsbereich Das Basissystem enthält eine Reihe primärer Filter zum Eingrenzen der Liste der Security Incidents für die Analyse (für Ihnen zugewiesene Security Incidents, alle offenen Incidents usw.) und eine Reihe schneller (oder sekundärer) Filter zum weiteren Eingrenzen der Liste (nach neuen Incidents, offenen Incidents, nur kritischen Incidents usw.).

Vorbereitungen

Sie können die klassische Umgebung verwenden, um zusätzliche primäre und sekundäre Filter zu definieren.

Während Sie Filter definieren, die in verwendet werden sollen Sicherheitsanalyst-Arbeitsbereich, Sie können Tags zuweisen, um anzugeben, ob sie als primäre oder sekundäre Filter verwendet werden können. Primäre Filter werden oben in der Security Incident-Liste angezeigt.



Klicken Sie Auf **Bearbeiten** Neben der Option Schnellfilter zur Auswahl sekundärer (oder schneller) Filter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: admin oder sn_sec_cmn.write

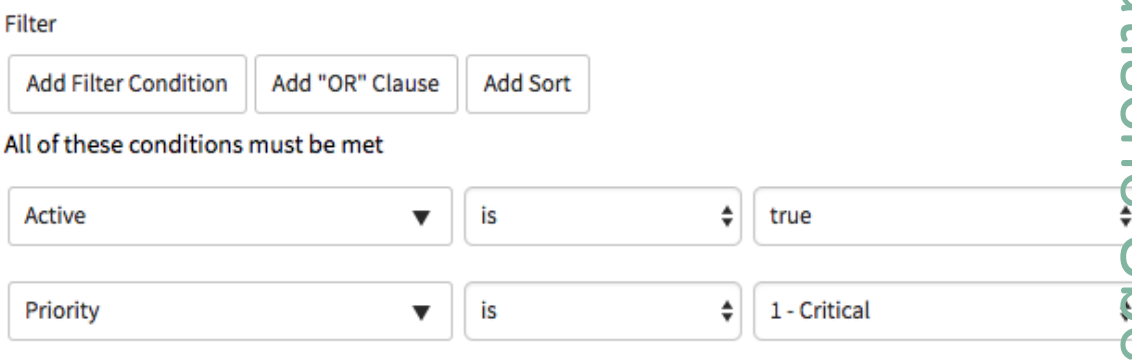
Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Filter**an.
2. Klicken Sie Auf **Neu** Und führen Sie die folgenden Schritte aus.

   a. Geben Sie ein **Titel** .

   b. Wählen Sie Aus **Security Incident [sn_si_Incident]** Von **Tabelle** Auswahlliste.

   c. Fügen Sie Ihre Filterbedingungen hinzu.
   Zum Beispiel die **Offene Incidents mit Priorität = Kritisch** Filter, verwendet diese Bedingungen.



   d. Klicken Sie auf **Absenden**.

3. Wenn **Tags** Spalte ist in der Filterliste nicht sichtbar. Klicken Sie auf das Zahnradsymbol, und personalisieren Sie die Ansicht, um sie hinzuzufügen.
4. Suchen Sie den von Ihnen erstellten Filter, und fügen Sie eines der folgenden Tags hinzu, um anzugeben, wie der Filter in angezeigt werden soll Sicherheitsanalyst-Arbeitsbereich.
   - **SN_SI_Primär** : Wenn dieses Tag ausgewählt ist, kann der Filter aus dem primären Filter-Slushbucket in ausgewählt werden Sicherheitsanalyst-Arbeitsbereich.
   - **SN_SI_PRIMARY_OOB** : Wenn dieses Tag ausgewählt ist, wird der Filter in angezeigt **Ausgewählt** Standardmäßig Seite des primären Filter-Slushbucket.
   - **SN_SI_Sekundär** : Wenn dieses Tag ausgewählt ist, kann der Filter aus dem sekundären (schnellen) Filter-Slushbucket ausgewählt werden.
   - **SN_SI_SECONDARY_OOB** : Wenn dieses Tag ausgewählt ist, wird der Filter in angezeigt **Ausgewählt** Standardmäßig Seite des primären Filter-Slushbucket.

Zugehörige Informationen

Erstellen und bearbeiten Sie Filter

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Sicherheitsanalysten-Arbeitsbereichs

Diese Systemeigenschaften werden verwendet, um den Arbeitsbereich für Sicherheitsanalysten zu konfigurieren.

Es gibt zwei Arten von Eigenschaften:

- Eigenschaften, die normalerweise nicht geändert werden, z. B. sys_IDs und Produktschlüssel.
- Eigenschaften, die nach Bedarf geändert werden, z. B. lange Abfrageintervalle und Anwenderoberflächenkonfigurationen.

Hinweis:
Die Eigenschaften des Sicherheitsanalysten-Arbeitsbereichs befinden sich an diesem Speicherort: **Security Incident** > **Setup Des Analysten-Arbeitsbereichs** > **Eigenschaften Des Analysten-Arbeitsbereichs**an.

Eigenschaften des Sicherheitsanalysten-Arbeitsbereichs

Eigenschaftsname	Beschreibung
Felder, die standardmäßig im Antwortaufgabenbanner ausgeblendet sind. sn_App_secops_ui.Form.excluded_fields.response_task	• **Typ**: Zeichenfolge • **Standardwert** : ○ Nummer ○ Kurzbeschreibung ○ Kommentare ○ work_notes ○ comments_and_work_notes ○ Work_Notes_list ○ Automation_activity
Felder, die standardmäßig im Incident-Banner ausgeblendet sind. sn_app_secops_ui.form.excluded_fields.incident	• **Typ**: Zeichenfolge • **Standardwert** : ○ Nummer ○ Kurzbeschreibung ○ Kommentare ○ work_notes ○ comments_and_work_notes ○ Work_Notes_list ○ Automation_activity ○ Security_Tags
Der Hintergrundfarbstil wird auf die hier aufgeführten Felder angewendet.	• **Typ**: Zeichenfolge • **Standardwert** :

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Sicherheitsanalysten-Arbeitsbereichs (Fortsetzung)

Eigenschaftsname	Beschreibung
sn_App_secops_ui.Form.color_coded_fields	○ Geschäftsrelevanz ○ impact ○ Priorität ○ risk_score ○ severity
Bei „wahr“ haben Tabellen, die aus der Tabelle „sn_si_Task-Basisantwortaufgabe“ erweitert wurden, auch Zugriff auf E-Mail-Vorlagen, die für die Tabelle „Basisantwortaufgabe“ erstellt wurden. sn_App_secops_ui.extend.Base.response_Task.email_Templates	• **Typ**: true | false • **Standardwert**: true
Legt die Breite jedes Zusammenfassungsfelds in jedem Antwortaufgabenbanner fest. sn_App_secops_ui.Task_summary.Single_summary.width.response_Task	• **Typ**: Ganzzahl • **Standardwert**: 10
Legt die Breite jedes Zusammenfassungsfelds in jedem Incident-Banner fest. sn_app_secops_ui.task_summary.single_summary.width.incident	• **Typ**: Ganzzahl • **Standardwert**: 15
Legt einen Grenzwert für die Anzahl der Zusammenfassungsfelder fest, die im Incident-Banner zulässig sind. sn_app_secops_ui.task_summary.single_summary.limit.incident	• **Typ**: Ganzzahl • **Standardwert**: 12
Legt einen Grenzwert für die Anzahl der Zusammenfassungsfelder fest, die im Antwortaufgabenbanner zulässig sind. sn_App_secops_ui.Task_summary.Single_summary.limit.response_Task	• **Typ**: Ganzzahl • **Standardwert**: 12
Legt einen Grenzwert für die Anzahl der Zusammenfassungsfelder fest, die in der ersten Zeile des Incident-Banners zulässig sind. sn_app_secops_ui.task_summary.single_summary.limit.incident.first_line	• **Typ**: Ganzzahl • **Standardwert**: 3

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Sicherheitsanalysten-Arbeitsbereichs (Fortsetzung)

Eigenschaftsname	Beschreibung
Kommagetrennte Liste von Feldern, die Anwenderfotos enthalten können. sn_app_secops_ui.form.user_fields	• **Typ**: Zeichenfolge • **Standardwert** : ○ Betroffene_Anwender ○ caller ○ sys_updated_by ○ sys_created_by ○ opened_by ○ closed_by ○ Übermittelt_von
Legt die Breite jedes Zusammenfassungsfelds in jeder Incident-PEEK-Ansicht fest. sn_app_secops_ui.task_summary.single_summary.width.incident_peek	• **Typ**: Ganzzahl • **Standardwert** : 13,5
Kommagetrennte Liste von Feldern, die die Zeit anzeigen. sn_App_secops_ui.Form.time_fields	• **Typ**: Zeichenfolge • **Standardwert** : ○ Geöffnet_um ○ sys_created_on ○ sys_updated_on
Steuert die Häufigkeit (in Millisekunden), mit der die Sichtungssuchergebnisse aktualisiert werden. sn_app_secops_ui.poller_interval.search_action	• **Typ**: Ganzzahl • **Standardwert** : 30000 **Minimum** : 15000
Steuert die Häufigkeit (in Millisekunden), mit der die Anzahl- oder Abfragedaten aktualisiert werden. sn_App_secops_ui.Poller_interval.related_list	• **Typ**: Ganzzahl • **Standardwert** : 30000 **Minimum** : 15000
Steuert die Häufigkeit (in Millisekunden), mit der die Ergebnisdaten aktualisiert werden (für das Playbook). sn_app_secops_ui.poller_interval.playbook_tasks	• **Typ**: Ganzzahl • **Standardwert** : 30000 **Minimum** : 15000

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Sicherheitsanalysten-Arbeitsbereichs (Fortsetzung)

Eigenschaftsname	Beschreibung
ID für die Security Operations-Integration – Host-Workflow isolieren. sn_App_secops_ui.Workflow.id.Isolate_Host	• **Typ**: Zeichenfolge • **Standardwert** : D72041f1ff203200c68c84648e94fa5e
ID für die Security Operations-Integration – Beobachtungslisten-Workflow. sn_App_secops_ui.Workflow.id.publish_to_Watchlist	• **Typ**: Zeichenfolge • **Standardwert** : 35800c0eff343200c68c84648e94fa85
ID für die Security Operations-Integration – Workflow für Blockanforderung. sn_App_secops_ui.Workflow.id.Block_Request	• **Typ**: Zeichenfolge • **Standardwert** : 11a6a5270b9032008f9108e3c5673a24
ID für die Anwenderrolle „sn_si_Analyst“. sn_App_secops_ui.roles.id.sn_si.write	• **Typ**: Zeichenfolge • **Standardwert** : 66878663ff123100158bffffffffffffff8d
ID für die Anwenderrolle „sn_si_read“. sn_app_secops_ui.roles.id.sn_si.read	• **Typ**: Zeichenfolge • **Standardwert** : Ae878663ff123100158bffffffffffff8e
ID für die Anwenderrolle sn_si_admin. sn_App_secops_ui.roles.id.sn_si.admin	• **Typ**: Zeichenfolge • **Standardwert** : 22878663ff123100158bffffffffffffff8d
ID für Microsoft Exchange – Führen Sie den Workflow „E-Mail-Suche und -Löschen“ aus sn_App_secops_ui.email.Phishing.Manual.Workflow	• **Typ**: Zeichenfolge • **Standardwert** : Ed9f289cc310220031fbdccdf3d3aeb4
ID für die anwenderdefinierte Aktion „zu Deny-Liste hinzufügen“ auf der Registerkarte „Durchsuchen“ in Sicherheitsanalyst-Arbeitsbereich. sn_app_secops_ui.explore.action.direct.id.deny_list	• **Typ**: Zeichenfolge • **Standardwert** : DENY_e9bd0ac50b632200263a089b37673a0b
ID für die anwenderdefinierte Aktion „Liste hinzufügen zu zulassen“ auf der Registerkarte „Durchsuchen“ in Sicherheitsanalyst-Arbeitsbereich	• **Typ**: Zeichenfolge • **Standardwert** : ALLOWLIST_e9bd0ac50b632200263a089b37673a0b

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Sicherheitsanalysten-Arbeitsbereichs (Fortsetzung)

Eigenschaftsname	Beschreibung
sn_App_secops_ui.Explore.action.direct.id.allow_list	
ID für die UI-Aktion „Bedrohungssuche ausführen“. sn_app_secops_ui.explore.action.id.run_threat_lookup	• **Typ**: Zeichenfolge • **Standardwert** : Da5ff4420b540300263a089b37673ae7
ID für die Integrationsfähigkeit „Bedrohungssuche“. sn_app_secops_ui.explore.capability.id.threat_lookup	• **Typ**: Zeichenfolge • **Standardwert** : 39344d4f0b273200263a089b37673ab1
ID für die anwenderdefinierte Aktion „Anreicherung erkennbarer Elemente“ auf der Registerkarte „Erkunden“ in Sicherheitsanalyst-Arbeitsbereich. sn_App_secops_ui.Explore.action.id.observable_Enrichment	• **Typ**: Zeichenfolge • **Standardwert** : OBS_ENRICHMENT_54e2f5d60b5003009f66e94685673
ID für die Integrationsfähigkeit „erkennbare Elemente anreichern“. sn_app_secops_ui.explore.capability.id.observable_enrichment	• **Typ**: Zeichenfolge • **Standardwert** : 9ad183640b1003009f66e94685673af4
ID für die UI-Aktion „in Beobachtungsliste veröffentlichen“. sn_App_secops_ui.Explore.action.id.publish_to_Watchlist	• **Typ**: Zeichenfolge • **Standardwert** : 8ee94002ff743200c68c84648e94faf9
ID für die UI-Aktion „Anforderung blockieren“. sn_App_secops_ui.Explore.action.id.Block_Request	• **Typ**: Zeichenfolge • **Standardwert** : 7158f6e40b2032008f9108e3c5673adf
ID für die UI-Aktion „Sichtungssuche ausführen“. sn_App_secops_ui.Explore.action.id.Sichtungen_Suche	• **Typ**: Zeichenfolge • **Standardwert** : 43f91a6f0b032200b97c67d985673a2c
ID für die UI-Aktion „untergeordneten Security Incident erstellen“. sn_App_secops_ui.Explore.action.id.create_Child_Incident	• **Typ**: Zeichenfolge • **Standardwert** : 5a688264536353009d5ddeeff7b1272

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Sicherheitsanalysten-Arbeitsbereichs (Fortsetzung)

Eigenschaftsname	Beschreibung
ID für die UI-Aktion „Sicherheitsanmerkung hinzufügen“. sn_App_secops_ui.Explore.action.id.add_Security_annotation	• **Typ**: Zeichenfolge • **Standardwert** : 1e3a3e723b5332005a9149a4d2efc4eb
ID für die anwenderdefinierte Aktion „CI-Anreicherung“ auf der Registerkarte „Erkunden“ in Sicherheitsanalyst-Arbeitsbereich. sn_App_secops_ui.Explore.action.id.ci_Anreicherung	• **Typ**: Zeichenfolge • **Standardwert** : CI_ENRICHMENT_54e2f5d60b5003009f66e94685673a1
ID für die UI-Aktion „Host isolieren“. sn_App_secops_ui.Explore.action.id.isolate_Host	• **Typ**: Zeichenfolge • **Standardwert** : D6244e0aff203200c68c84648e94fad3
ID für die UI-Aktion „mehrere erkennbare Elemente hinzufügen“. sn_App_secops_ui.Explore.action.id.multiple_observable	• **Typ**: Zeichenfolge • **Standardwert** :138de478d78322007a6de294de6103aa
Produktschlüssel für ag-Grid-Enterprise. sn_App_secops_ui.ag-Grid-license	• **Typ**: Zeichenfolge • **Standardwert** :ServiceNow_ServiceNow_5Devs2_August_2018_MTUzM

Zusätzliche Konfiguration des Sicherheitsanalysten-Arbeitsbereichs

Konfigurieren Sie Sicherheitsanalyst-Arbeitsbereich Und definieren Sie Filter, UI-Aktionen und zugehörige Listen.

- Zielseiten-Filterkonfiguration
- UI-Aktionen aktivieren
- Formular-UI-Aktionen
- Konfiguration der zugehörigen Liste
- UI-Aktionen der zugehörigen Liste
- Systemeigenschaften der Formularkonfiguration
- Aktivieren Sie Playbooks für die Analystenauswahl

Zielseiten-Filterkonfiguration

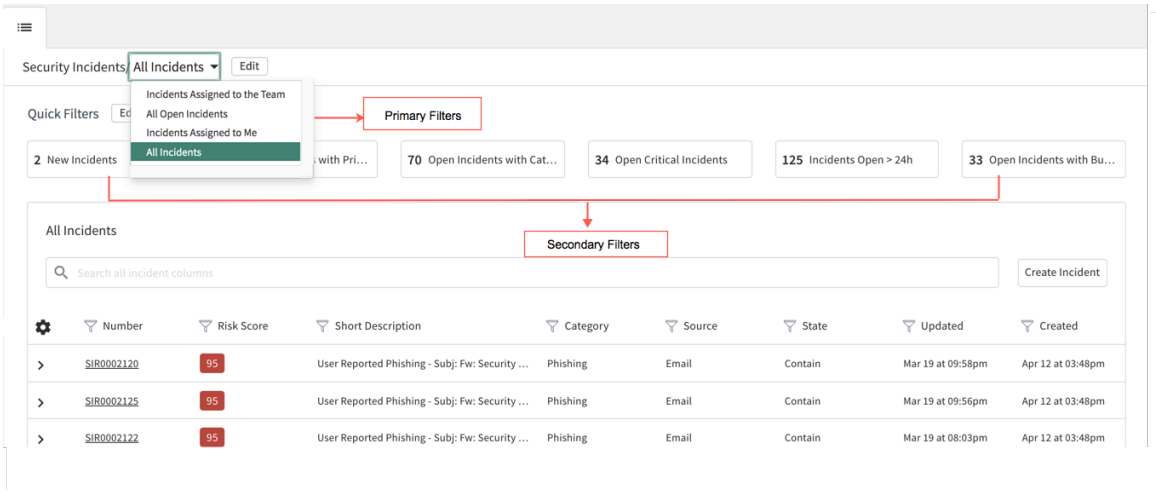
Sie können neue Filter hinzufügen oder vorhandene Filter ändern, die in angezeigt werden Sicherheitsanalyst-Arbeitsbereich.

Die Sicherheitsanalyst-Arbeitsbereich Verfügt über primäre und sekundäre Filter, mit denen Sie die Liste der Security Incidents filtern können, damit Sie schnell die Security Incidents

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

finden können, die Sie analysieren möchten. Weitere Informationen finden Sie unter Verwalten Sie Sicherheitsbedrohungen mit Sicherheitsanalyst-Arbeitsbereich.



Erstellen Sie einen neuen Filter

1. Navigieren zu **Security Incidents** > **Setup des Analysten-Arbeitsbereichs (neue UI)** > **Zielseiten-Filterkonfiguration**an.
2. Klicken Sie auf **Neu**.
3. Geben Sie einen Titel für den Filter ein, geben Sie die Filterbedingung an, und klicken Sie auf **Übermitteln** Um zur vorherigen Seite zurückzukehren.

   Der neu hinzugefügte Filter wird auf der Seite aufgeführt.
4. Fügen Sie ein Tag für diesen Filter hinzu, um anzugeben, ob es sich um einen primären oder sekundären Filter handelt. Die folgenden Tags sind verfügbar:
   - SN_SI_Primär
   - SN_SI_Sekundär

Bearbeiten Sie vorhandene Filter

Sie können auch Folgendes tun:

- Vorhandene Filter ändern: Klicken Sie auf den Titel eines vorhandenen Filters. Ändern Sie den Titel und die Filterbedingung, und klicken Sie auf **Aktualisieren** .
- Tags ändern: Wählen Sie einen Filter aus, und klicken Sie in der Zielseiten-Filterkonfiguration auf die Spalte Tag. Sie können das vorhandene Tag löschen oder ein neues Tag für den Filter hinzufügen.

UI-Aktionen aktivieren

Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in verfügbar sind Sicherheitsanalyst-Arbeitsbereich.

Hinweis:
Um die UI-Aktionen zu ändern, melden Sie sich als Anwender mit den folgenden Rollen an:

- ui_action_admin
- ui_page_admin
- web_service_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es gibt zwei Arten von UI-Aktionen, die für konfiguriert werden können Sicherheitsanalyst-Arbeitsbereich:

- Dialogbasierte UI-Aktion
- Serverseitige UI-Aktion

Dialogbasierte UI-Aktion

Dient zum Aktivieren dialogbasierter UI-Aktionen in Sicherheitsanalyst-Arbeitsbereich, Nehmen Sie die folgenden Änderungen an den UI-Seiten vor, die den jeweiligen Standard-UI-Aktionen zugeordnet sind.

1. **HTML-Abschnitt** : Ändern Sie den HTML-Abschnitt, um einzubeziehen `Reagieren` Eingabe-Tag. Die `Reagieren` Der Eingabe-Tag-Wert wird im Clientskript-Abschnitt verwendet, um zu identifizieren, ob die UI-Seite über gestartet wurde Sicherheitsanalyst-Arbeitsbereich. Ein Beispiel wird unten angezeigt:

   ```
   <input id="react" name="react" type="hidden"
   value="${JS,HTML:sysparm_react}" />
   ```

2. **Client-Skript** : Zusätzliche Logik muss in das Client-Skript geschrieben werden, wenn `Reagieren` Kennzeichnung ist „wahr“. Dies ist erforderlich, um zu verarbeiten **Übermitteln** Und **Abbrechen** Schaltflächenereignisse, die als Teil des Dialogfensters angezeigt werden.
   a. Der Ereignis-Handler „onCancel“ () muss das Ereignis „SIR_WORKBENCH_POPUP_CANCEL“ von senden Sicherheitsanalyst-Arbeitsbereich
   b. Der Ereignis-Handler „onSubmit“ () muss das Ereignis „SIR_WORKBENCH_POPUP_SUBMIT“ von senden Sicherheitsanalyst-Arbeitsbereich
3. Die Ausführung des Verarbeitungsskripts wird von übersprungen Sicherheitsanalyst-Arbeitsbereich Kontext als Aktion „onSubmit“ wurde geändert, um „falsch“ zurückzugeben, wenn `Reagieren` Tag-Eingabewert ist „wahr“. Die Logik des Verarbeitungsskripts muss entweder über ein vom Client aufrufbares Skript (aufgerufen über GlideAjax-API) oder EINEN REST-Ressourcenendpunkt verarbeitet werden.

Weitere Informationen finden Sie auf den folgenden Beispiel-UI-Seiten:

- Beispiel für UI-Aktion „zugehörige Liste“: In Beobachtungsliste veröffentlichen (UI-Seitenname: Publish_to_Watchlist)
- Beispiel für Formular-UI-Aktion: Problem erstellen (UI-Seitenname: Create_prb_Change_inc)

Serverseitige UI-Aktion

Um serverseitige UI-Aktionen zu aktivieren, müssen Sie wie folgt vorgehen:

Die Logik des Standard-UI-Aktionsskripts muss als Teil einer geskripteten REST-Ressource behandelt werden.

Weitere Informationen finden Sie in den folgenden Beispiel-Formular-UI-Aktionen:

- Ausfall erstellen
- Abbrechen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular-UI-Aktionen

Sie können die UI-Aktionen konfigurieren, die in angezeigt werden Sicherheitsanalyst-Arbeitsbereich.

Voraussetzungen:

Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in verfügbar sind Sicherheitsanalyst-Arbeitsbereich. Details siehe UI-Aktionen aktivieren.

Dient zum Konfigurieren einer Formular-UI-Aktion für Sicherheitsanalyst-Arbeitsbereich, Führen Sie die folgenden Schritte aus:

1. Navigieren zu **Security Incidents** > **Setup des Analysten-Arbeitsbereichs (neue UI)** > **Formular-UI-Aktionen**an.
2. Geben Sie die folgenden Details ein:

Feldname	Beschreibung
Aktion	Wählen Sie eine UI-Aktion aus der Auswahlliste aus.
Typ	Wählen Sie den Typ der Aktion aus. Dies kann sein: ○ Dialogbasierte Aktion: Dieser Aktionstyp wird verwendet, wenn Anwenderinteraktionen oder Eingaben erforderlich sind, um eine bestimmte Geschäftslogik auszuführen. ○ Serverseitige Aktion: Diese Aktion führt die erforderliche Geschäftslogik ohne zusätzliche Anwendereingaben aus. **Hinweis:** Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in verfügbar sind Sicherheitsanalyst-Arbeitsbereich. Details siehe UI-Aktionen aktivieren.
Anwendung	Hier wird der Name des Anwendungsbereichs (UI für Security Incident Response) angezeigt, in dem die UI-Aktion hinzugefügt wird.
Dialogbasierte Aktion Wenn Sie im Feld Typ die Option dialogbasierte Aktion auswählen, geben Sie die folgenden Details ein:	
UI-Seite	Wählen Sie die UI-Seite aus, die der Aktion zugeordnet ist.
Dialogdialogtitel	Geben Sie einen Titel für die Dialogfeldaktion ein.
Dialogfeldbreite und -Höhe	Geben Sie die Höhe und Breite des Dialogfelds in Pixel ein.
Skript	Für die ausgewählte UI-Seite können Sie hier zusätzliche Abfrageparameter angeben. Die mit dem Basissystem bereitgestellte Vorlage erstellt und gibt sie zurück `Sysparm_sys_ID` Nur Parameter. Sie können dies überschreiben, indem Sie hier verschiedene Parameter angeben.
Serverseitige Aktion	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

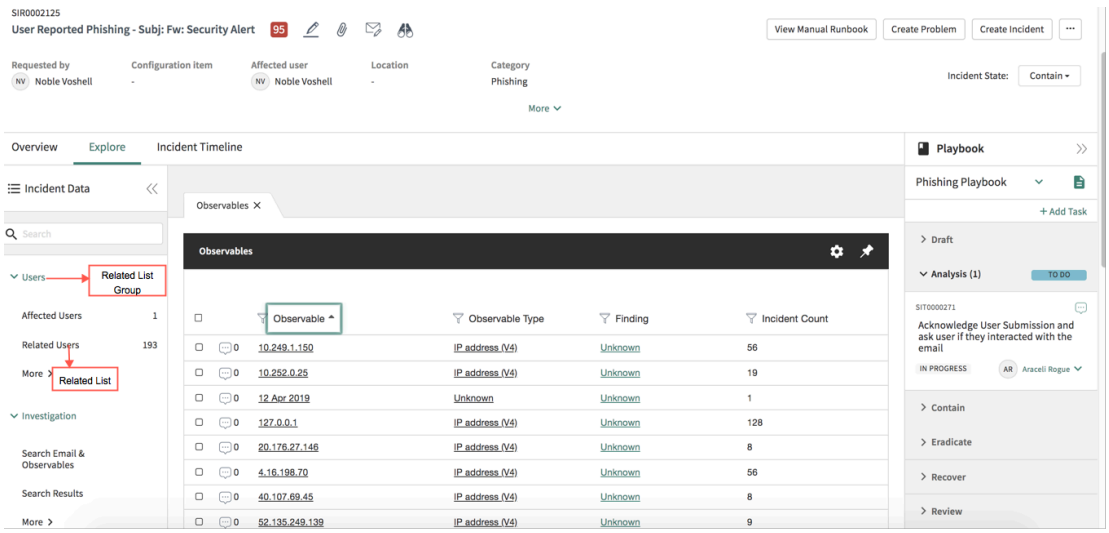
Feldname	Beschreibung
Wenn Sie im Feld Typ die Option serverseitige Aktion auswählen, geben Sie die folgenden Details ein:	
Geskriptete Rest-Ressource	Wählen Sie die geskriptete Rest-Ressource aus, die die Aktion definiert. **Hinweis:** Die **SIR-UI-ANALYST** ACL muss der Rest-Ressource hinzugefügt werden.

3. Klicken Sie auf **Absenden**.
4. Navigieren zu **Security Incidents** > **Incidents (neue UI)** Seite.
5. Klicken Sie auf eine Security Incident-Nummer, um den Security Incident-Datensatz anzuzeigen. Die neue UI-Aktion wird oben auf der Seite angezeigt.

Um eine vorhandene Formular-UI-Aktion zu ändern, klicken Sie auf den Aktionsnamen, um zur Seite „Formular-UI-Aktionen“ zu navigieren. Sie können den Aktionsnamen, den Typ und die übrigen Felder basierend auf dem ausgewählten Typ ändern.

Konfiguration der zugehörigen Liste

Sie können neue zugehörige Listen oder neue zugehörige Listengruppen hinzufügen und vorhandene Gruppen oder zugehörige Listen ändern, die in angezeigt werden Sicherheitsanalyst-Arbeitsbereich.



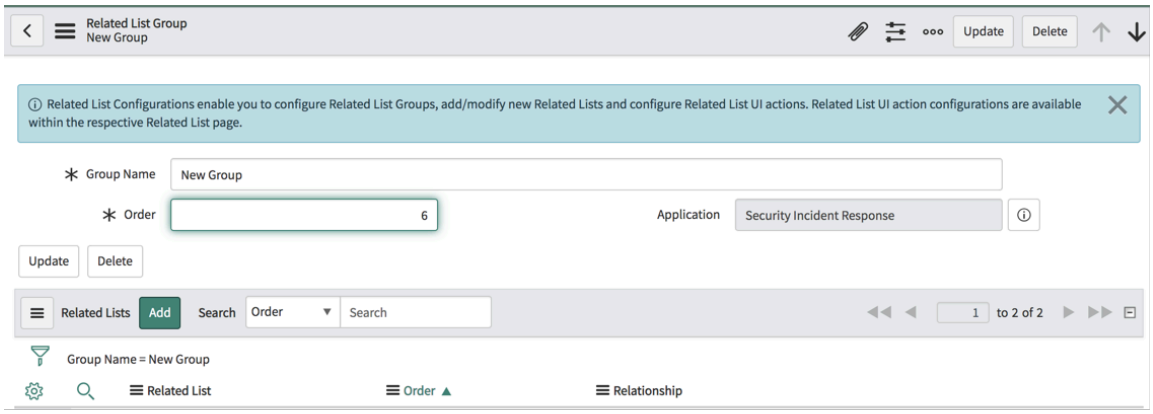
Fügen Sie eine zugehörige Listengruppe hinzu

Gehen Sie wie folgt vor, um eine zugehörige Listengruppe hinzuzufügen:

1. Navigieren zu **Security Incidents** > **Setup des Analysten-Arbeitsbereichs (neue UI)** > **Konfigurationen Der Zugehörigen Liste**an.
2. Klicken Sie Auf **Neu** Zum Hinzufügen einer neuen zugehörigen Listengruppe. Geben Sie den Gruppennamen und die Reihenfolge ein, in der er auf der Seite „Incidents“ (neue UI) angezeigt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Absenden**. Die neu hinzugefügte Gruppe wird auf der Seite „zugehörige Listengruppen“ angezeigt.



Fügen Sie eine zugehörige Liste hinzu

Um eine neue zugehörige Liste hinzuzufügen, gehen Sie wie folgt vor:

1. Klicken Sie auf den Link einer zugehörigen Listengruppe.
2. Klicken Sie im Abschnitt zugehörige Listen auf **Hinzufügen** Zum Hinzufügen einer neuen zugehörigen Liste.

   Wenn Sie nicht sehen **Hinzufügen** Schaltfläche, überprüfen Sie, ob Sie sich im gleichen Anwendungsbereich wie die zugehörige Listengruppe befinden.
3. Wählen Sie die zugehörige Liste aus, die in die Gruppe aufgenommen werden soll.

   Hinweis:
   Wenn keine bestimmte zugehörige Liste angezeigt wird, gehen Sie wie folgt vor:

   a. Navigieren zu **System-UI** > **Zugehörige Listen** Und suchen Sie nach zugehörigen Listen, die in vorhanden sind `sn_si_Incident` Tabelle.

   b. Klicken Sie auf `sn_si_Incident` Tabelle, die dem zugeordnet ist **SIR – neue UI** Anzeigen.

   c. Klicken Sie im Abschnitt zugehörige Listeneinträge auf **Neu** Um die zugehörige Liste zu hinzuzufügen **SIR – neue UI** Anzeigen.
4. Geben Sie die Reihenfolge an, in der sie angezeigt werden soll, und klicken Sie auf **Übermitteln** .

   Die zugehörige Liste, die Sie hinzugefügt haben, wird in angezeigt Sicherheitsanalyst-Arbeitsbereich.

Um eine vorhandene zugehörige Listengruppe zu ändern, klicken Sie auf den Gruppennamen, um zur Seite „zugehörige Listengruppe“ zu navigieren. Sie können den Gruppennamen und die Reihenfolge ändern und der Gruppe zugehörige Listen hinzufügen oder löschen.

UI-Aktionen der zugehörigen Liste

Sie können den zugehörigen Listen, die in angezeigt werden, neue UI-Aktionen hinzufügen Sicherheitsanalyst-Arbeitsbereich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen:

Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in verfügbar sind Sicherheitsanalyst-Arbeitsbereich. Details siehe UI-Aktionen aktivieren.

Um eine neue UI-Aktion für zugehörige Listen hinzuzufügen, gehen Sie wie folgt vor:

1. Navigieren zu **Security Incidents** > **Setup des Analysten-Arbeitsbereichs (neue UI)** > **Konfigurationen Der Zugehörigen Liste**an.
2. Klicken Sie auf den Gruppennamen. Die Konfigurationsseite der zugehörigen Listengruppe wird angezeigt.
3. Klicken Sie auf die zugehörige Liste, für die Sie eine UI-Aktion hinzufügen möchten.
4. Klicken Sie Auf **Hinzufügen** Im Abschnitt UI-Aktionen der zugehörigen Liste.
5. Geben Sie die folgenden Details ein:

Feldname	Beschreibung
Aktion	Wählen Sie eine UI-Aktion aus der Auswahlliste aus.
Typ	Wählen Sie den Typ der Aktion aus. Dies kann sein: ○ Dialogbasierte Aktion: Dieser Aktionstyp wird verwendet, wenn Anwenderinteraktionen oder Eingaben erforderlich sind, um eine bestimmte Geschäftslogik auszuführen. ○ Serverseitige Aktion: Diese Aktion führt die erforderliche Geschäftslogik ohne zusätzliche Anwendereingaben aus. **Hinweis:** Bevor Sie UI-Aktionen konfigurieren, müssen Sie bestimmte Schritte ausführen, um sie zu aktivieren, damit sie für die Konfiguration in verfügbar sind Sicherheitsanalyst-Arbeitsbereich. Details siehe UI-Aktionen aktivieren.
Anwendung	Hier wird der Name des Anwendungsbereichs (UI für Security Incident Response) angezeigt, in dem die UI-Aktion hinzugefügt wird.
Dialogbasierte Aktion Wenn Sie im Feld Typ die Option dialogbasierte Aktion auswählen, geben Sie die folgenden Details ein:	
UI-Seite	Wählen Sie die UI-Seite aus, die der Aktion zugeordnet ist.
Dialogdialogtitel	Geben Sie einen Titel für die Dialogfeldaktion ein.
Dialogfeldbreite und -Höhe	Geben Sie die Höhe und Breite des Dialogfelds in Pixel ein.
Skript	Für die ausgewählte UI-Seite können Sie hier zusätzliche Abfrageparameter angeben. Die mit dem Basissystem bereitgestellte Vorlage erstellt und gibt sie zurück `Sysparm_Incident_ID` , `Sysparm_Record_table` , Und `Sysparm_related_sys_IDs` Nur Parameter. Sie können sie überschreiben, indem Sie hier verschiedene Parameter angeben.
Serverseitige Aktion	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldname	Beschreibung
Wenn Sie im Feld Typ die Option serverseitige Aktion auswählen, geben Sie Folgendes an:	
Geskriptete Rest-Ressource	Wählen Sie die geskriptete Rest-Ressource aus, die die Aktion definiert. **Hinweis:** Die **SIR-UI-ANALYST** ACL muss der Rest-Ressource hinzugefügt werden.

6. Klicken Sie auf **Absenden**.
7. Navigieren zu **Security Incidents** > **Incidents (neue UI)** Seite.
8. Klicken Sie auf eine Security Incident-Nummer, um den Security Incident-Datensatz anzuzeigen. Starten Sie die entsprechende zugehörige Liste, um die neue UI-Aktion anzuzeigen.

Systemeigenschaften der Formularkonfiguration

Diese Systemeigenschaften definieren die Formularaktualisierungsintervalle für die Playbook-Aufgaben.

Um diese Eigenschaften zu konfigurieren, navigieren Sie zu **Setup des Analysten-Arbeitsbereichs (neue UI)** > **Eigenschaften Des Analysten-Arbeitsbereichs**an.

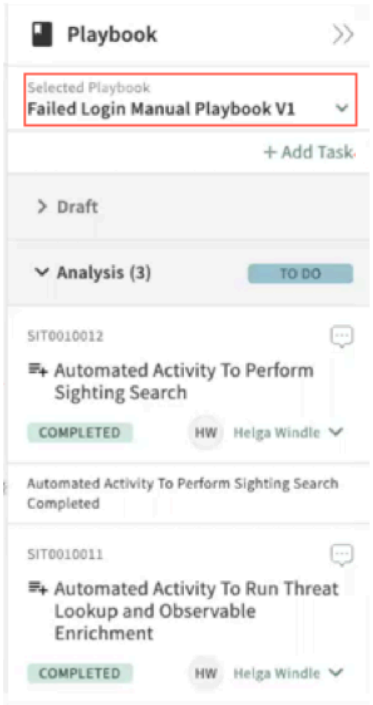
Eigenschaft	Standardwert	Beschreibung
sn_app_secops_ui.poller_interval.playbook_tasks	10000 ms	Die Intervallzeit, die von der Playbook-Komponente zum Aktualisieren ihrer Antwortaufgaben für jede konfigurierte Intervallzeit verwendet wird.
sn_app_secops_ui.poller_interval_count.playbook_tasks	9 Mal	Die Anzahl der Abrufe der Playbook-Komponente für Antwortaufgaben.
sn_App_secops_ui.Poller_interval.related_lists	30000 ms	Diese Intervallzeit wird von der Explore-Komponente verwendet, um die zugehörigen Listenanzahlen für jede konfigurierte Intervallzeit zu aktualisieren.

Aktivieren Sie Playbooks für die Analystenauswahl

Fügen Sie der Playbook-Auswahlliste neue Playbooks hinzu.

Sie können ein geeignetes Playbook auswählen, um Security Incidents in zu untersuchen Sicherheitsanalyst-Arbeitsbereich(Verwalten Sie Sicherheitsbedrohungen mit Sicherheitsanalyst-Arbeitsbereich). Die Playbook-Auswahloption unterstützt nur die Playbooks, die mit Flow Designer entworfen wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nachdem Sie ein Playbook mit Flow Designer erstellt haben, führen Sie die folgenden Schritte aus, um es in die Auswahlliste „ausgewähltes Playbook“ aufzunehmen:

1. Navigieren Sie zu *sys_Hub_Flow* Tabelle.
2. Suchen Sie nach dem neuen Playbook, das Sie mit Flow Designer erstellt haben.
3. Fügen Sie hinzu **Sir_Playbook** Tag für die Playbooks, die Sie in die Auswahlliste „ausgewähltes Playbook“ aufnehmen möchten.

Hinweis:
Wenn Sie alte Playbooks haben, die nicht von Workflows zu Flow Designer migriert wurden, werden sie nicht in der Liste angezeigt. Wenn jedoch ein mit Workflows erstellte Playbook einem Security Incident entweder durch eine Auslöserbedingung oder durch manuelle Auswahl (mit) zugewiesen wird **Orchestration Ausführen** Option in der klassischen Umgebung) wird dieses Playbook gestartet, wenn Sie den Security Incident in öffnen Sicherheitsanalyst-Arbeitsbereich.

Problembehandlung Bei Security Incident Response

Dieser Abschnitt behandelt wichtige Tipps zur Fehlerbehebung und häufig gestellte Fragen im Zusammenhang mit der Antwort auf Security Incidents.

Probleme mit Zugriffssteuerungsregeln

Zugriffssteuerungsregeln ermöglichen den Zugriff auf die angegebene Ressource, wenn alle folgenden drei Bedingungen erfüllt sind:

- Der Anwender hat eine der in angegebenen Rollen **Rolle** Liste, oder die Liste ist leer.
- Bedingungen in **Bedingung** Feld wird als „wahr“ ausgewertet, oder Bedingungen sind leer.
- Das Skript in **Skript** Feld (erweitert) wird als „wahr“ ausgewertet oder legt die Variable fest **Antwort** Auf „wahr“ oder ist leer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu Zugriffssteuerungsregeln finden Sie unter Explore Access Control Lists

Wichtig:
Wenn **Administrator-Überschreibungen** Die Option ist für eine Security Incident-Tabelle deaktiviert. Wenn der Administrator auf die Security Incident-Tabelle zugreifen kann, finden Sie unter KB1444673

Security Incident Response Platform Analytics-Lösungen

Platform Analytics-Lösungen enthalten vorkonfigurierte Dashboards. Die Dashboards enthalten wichtige Metriken für die Analyse von Security Incident Response Prozess, z. B. neue Security Incidents oder das durchschnittliche Alter offener Security Incidents.

Platform Analytics Datenvisualisierungen verwenden Performance Analytics *Indikator*Daten, die Ihnen Daten im Zeitverlauf anzeigen, damit Sie Ihre Geschäftsprozesse analysieren und Verbesserungsbereiche identifizieren können. Mit Platform Analytics-Lösungen können Sie mit einem minimalen Setup den Mehrwert von Performance Analytics für Ihre Anwendung nutzen. Sie können auch jederzeit eigene Objekte erstellen.

Die Security Incident Response Performance Analytics Lösung ist über verfügbar ServiceNow Store. Informationen zum Herunterladen und Installieren dieser Anwendung finden Sie unter Security Operations und ServiceNow Store .

Hinweis:
Um die Funktionalität zu bewerten, können Sie Performance Analytics-Lösungen und formularinterne Analysen für nicht lizenzierte Instanzen aktivieren Performance Analytics. Sie haben jedoch die folgenden Einschränkungen:

- Sie können keine neuen Indikatoren erstellen.
- Sie können keine Daten sammeln, die älter als 180 Tage sind.

Lizenzieren Sie Performance Analytics für vollständige Funktionalität. Weitere Informationen finden Sie unter Performance Analytics-Abonnement aktivieren .

Wichtig:
Standardmäßig das Datenerfassungslimit für `(Com.snc.PA.dc.max_Records)` Die Eigenschaft in Performance Analytics ist auf 5.000 Datensätze festgelegt. Sie können diesen Grenzwert jedoch gemäß Ihren Anforderungen erhöhen, z. B. 50.000 Datensätze. Das Erhöhen dieses Grenzwerts kann sich jedoch auf die Leistung während der Datenerfassung oder bei der Ausführung von Vorgängen in der Snapshot-Tabelle auswirken. Weitere Informationen zu den Performance Analytics-Eigenschaften finden Sie unter Performance Analytics properties .

Zugehörige Informationen

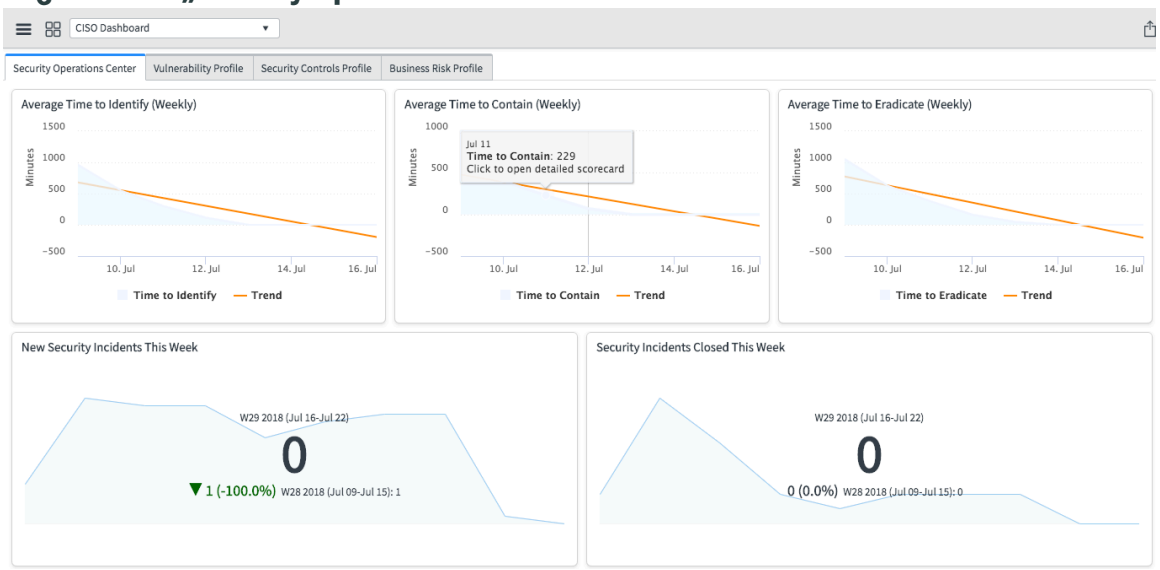
Performance Analytics-Abonnement aktivieren

CISO-Dashboard

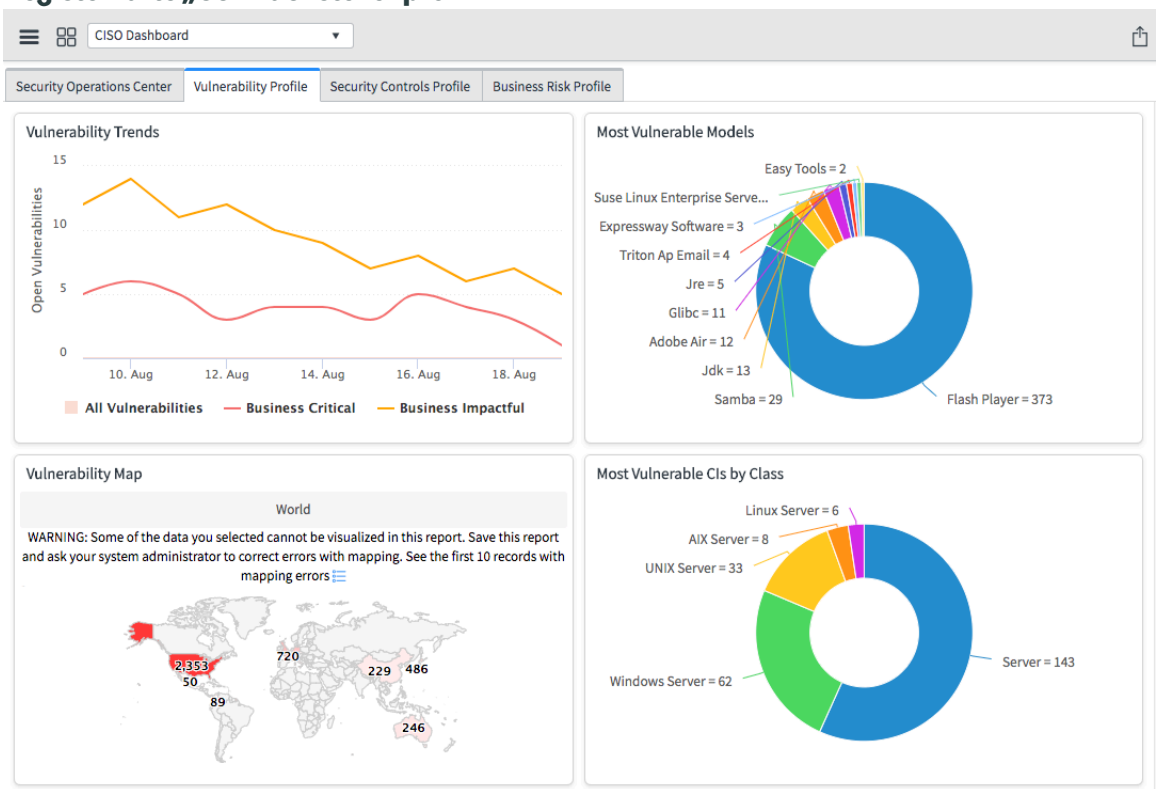
Dieses Dashboard zeigt die allgemeine Sicherheitslage Ihrer Organisation, einschließlich Sicherheitsschwachstellen und Incidents.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Security Operations Center“



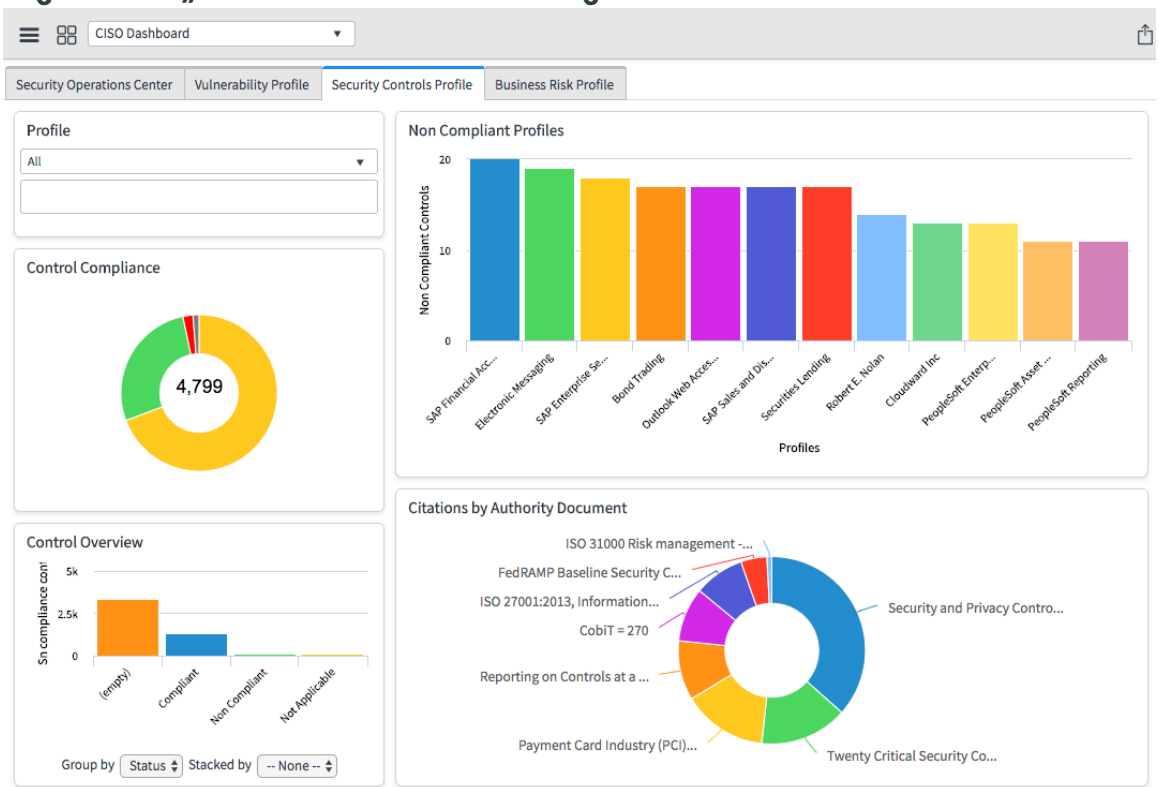
Registerkarte „Schwachstellenprofil“



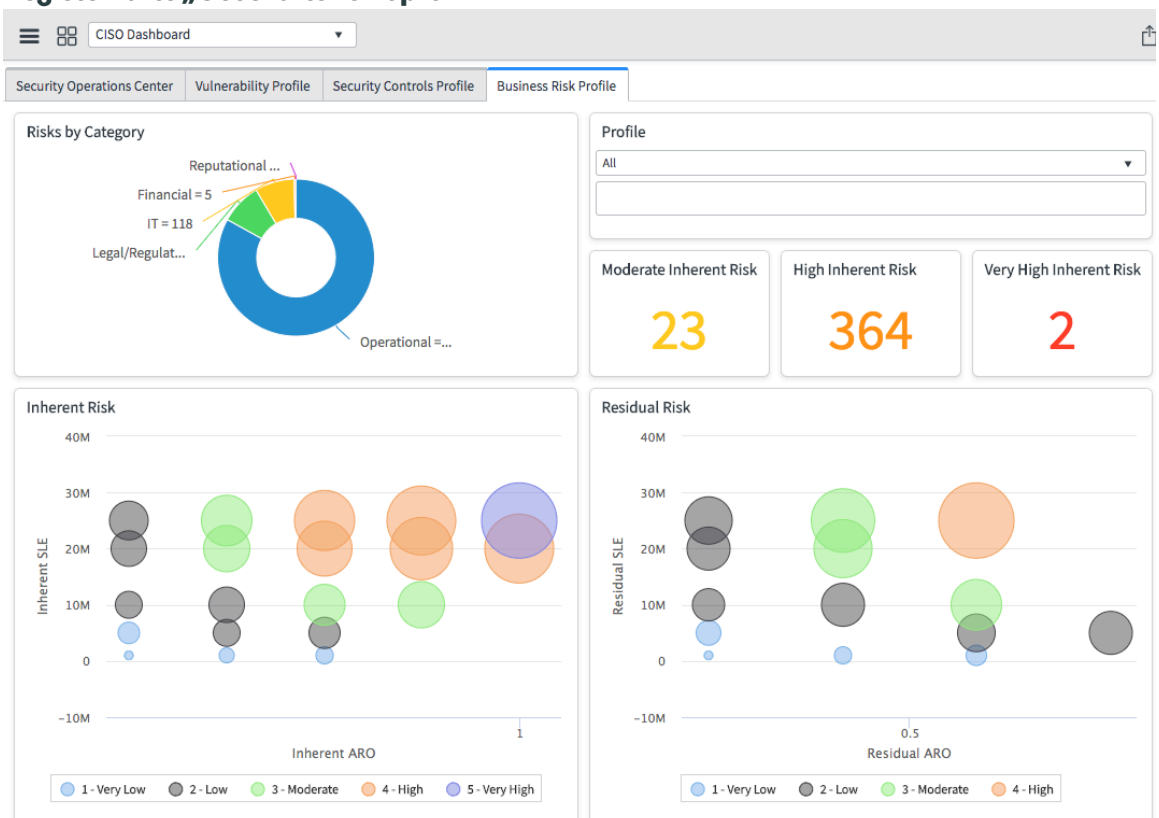
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Profil der Sicherheitssteuerungen“



Registerkarte „Geschäftsrisikoprofil“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Endanwender und Rollen

Endbenutzer und Ziel	Erforderliche Rolle
CISO: Benötigt klare Transparenz in Bezug auf die aktuelle Sicherheitslage der gesamten Organisation	sn_si.ciso

CISO-Dashboard-Indikatoren

Das CISO-Dashboard enthält die folgenden Leistungskennzahlen:

SI: Durchschnittliche Zeit bis zur Identifizierung

Ein 7-Tage-Durchschnitt der Zeit in Minuten, die zur Identifizierung eines Security Incidents benötigt wird, täglich berechnet.

Durchschnittliche Zeit bis zur Eindämmung

Ein 7-Tage-Durchschnitt der Zeit in Minuten, die zur Eindämmung eines Security Incidents benötigt wird, täglich berechnet.

Durchschnittliche Zeit bis Beseitigung

Ein 7-Tage-Durchschnitt der Zeit in Minuten, die zur Beseitigung eines Security Incidents benötigt wird, täglich berechnet. Sowohl die durchschnittliche Zeit bis zur Eindämmung als auch die durchschnittliche Zeit bis zur Beseitigung basieren auf dem Indikator SI – Durchschnittliche Dauer, aufgeschlüsselt nach Status des Security Incidents.

Neue Security Incidents diese Woche

Die wöchentliche Summe der Punktzahl des Indikators „tägliche Anzahl neuer Security Incidents“.

Geschlossene Security Incidents (wöchentlich)

Die laufende 7-Tage-Summe des Indikators „tägliche Anzahl geschlossener Security Incidents“.

Neue Security Incidents nach Priorität

Tägliche Aufgliederung des Indikators „Anzahl neuer Security Incidents“ nach Priorität.

Volumen neuer vs. Geschlossener Security Incidents (wöchentlich)

Die 7-Tage-laufende Summenzeitreihe des Indikators „Anzahl neuer Incidents“, dargestellt gegen die 7-Tage-laufende Summenzeitreihe des Indikators „Anzahl geschlossener Incidents“.

Heatmap Für Security Incidents

Eine globale Karte, die die Anzahl der offenen Security Incidents in jedem Land anzeigt.

Security Incident-Treemap

Eine interaktive Baumstruktur, in der Sie Folgendes anzeigen können:

- Security Incidents pro Business-Service, aufgeschlüsselt nach Geschäftsrelevanz
- Security Incidents, aufgeschlüsselt nach Kategorie oder Unterkategorie des Incident
- Security Incidents pro Zuweisungsgruppe oder pro Beauftragter
- „Opferstatistiken“ des Security Incidents pro betroffener Ressource oder betroffenem Anwender

Aufgliederungen

Die folgenden Aufgliederungen gelten für die Indikatoren im Dashboard:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Business-Relevanz
- Sicherheitsgruppe
- Alter des Security Incidents
- Kategorie von Security Incident
- Lösungscode für Security Incident
- Priorität von Security Incident
- Status des Security Incidents
- SI – Business-Service
- Schwachstelle

Datenvisualisierungen

Das Dashboard enthält die folgenden Visualisierungen:

Titel	Typ	Beschreibung
Security Incidents, die seit mehr als 30 Tagen offen sind, nach Zuweisungsgruppe und Status	Heatmap	Zeigt Modelle mit den am stärksten angreifbaren Elementen an.
Risiken nach Kategorie	Ring	Listet das Alter der erneut geöffneten angreifbaren Elemente auf.
Zitate nach Berechtigungsdokument	Ring	Anzahl der aktiven Schwachstellen
Security Incidents mit Beauftragtem, der nicht aktiv ist	Heatmap	Zeigt die Anzahl der offenen angreifbaren Elemente an, die Schwachstellen zugeordnet sind (CVE-Datensätze (Common Vulnerability Enumeration), von den meisten bis zu den geringsten.
Security Incidents, die seit mehr als 30 Tagen nach Zuweisungsgruppe und Status nicht aktualisiert wurden	Heatmap	Zeigt Herausgeber mit den am stärksten angreifbaren Elementen an.
Schwachstellenzuordnung	Zuordnung	Eine Weltkarte, die Schwachstellen nach Standort anzeigt
Modelle mit den meisten Schwachstellen	Ring	Die Anwendungen, die die meisten Schwachstellen enthalten
CIs mit den meisten Schwachstellen nach Klasse	Ring	CIs nach Servertyp
Services mit kritisch signifikanten Schwachstellen	Liste	
Nicht konforme Profile	Balken	Nicht konforme Steuerungen nach Profil
Kontrollübersicht	Balken	Anzahl der konformen und nicht konformen Steuerungen
Richtlinienausnahmen	Liste	Richtlinienausnahmen mit Priorität, Besitzer und Kurzbeschreibung
Risiken nach Kategorie	Ring	Die Anzahl der Risiken in jeder Risikokategorie

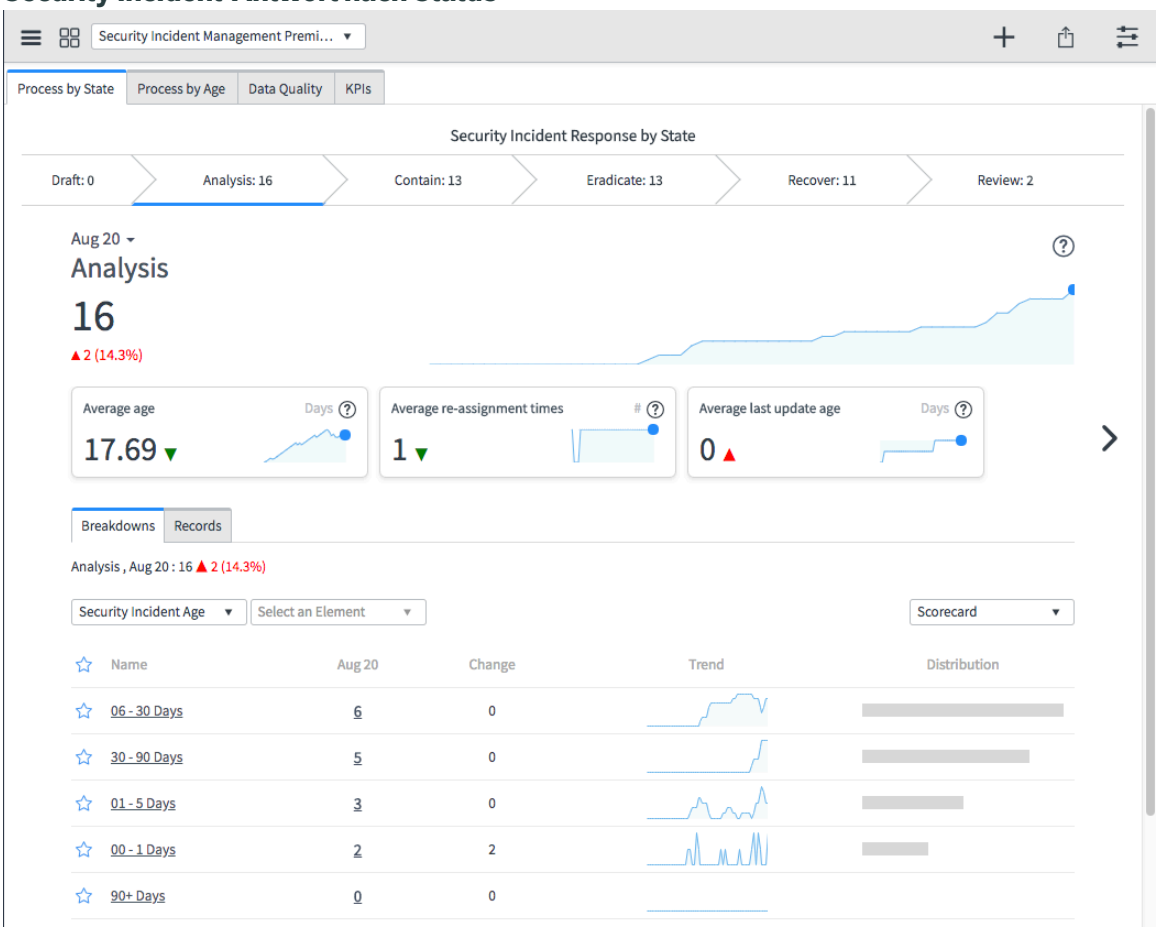
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
Inhärentes Risiko	Blase	Inhärente SLE vs. Inhärente ARO
Restrisiko	Blase	Rest-SLE vs. Rest-ARO
Mittlere, hohe und sehr hohe Risiken	Punktzahlen	Die Anzahl der mittleren, hohen und sehr hohen Risiken
Risiko nach Profil	Gestapelter Balken	Risikoanzahl, bei der Sie auswählen können, nach was gruppiert und nach was gestapelt werden soll

Security Incident Management Premium-Dashboard

Dieses Dashboard verwendet Advanced Platform Analytics Visualisierungen, die Sicherheitsmanagern helfen, das Volumen, die Leistung und den Fortschritt von Security Incidents nachzuverfolgen, von der ersten Analyse/Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung. Die lizenzierte Version von Performance Analytics Ist daher erforderlich.

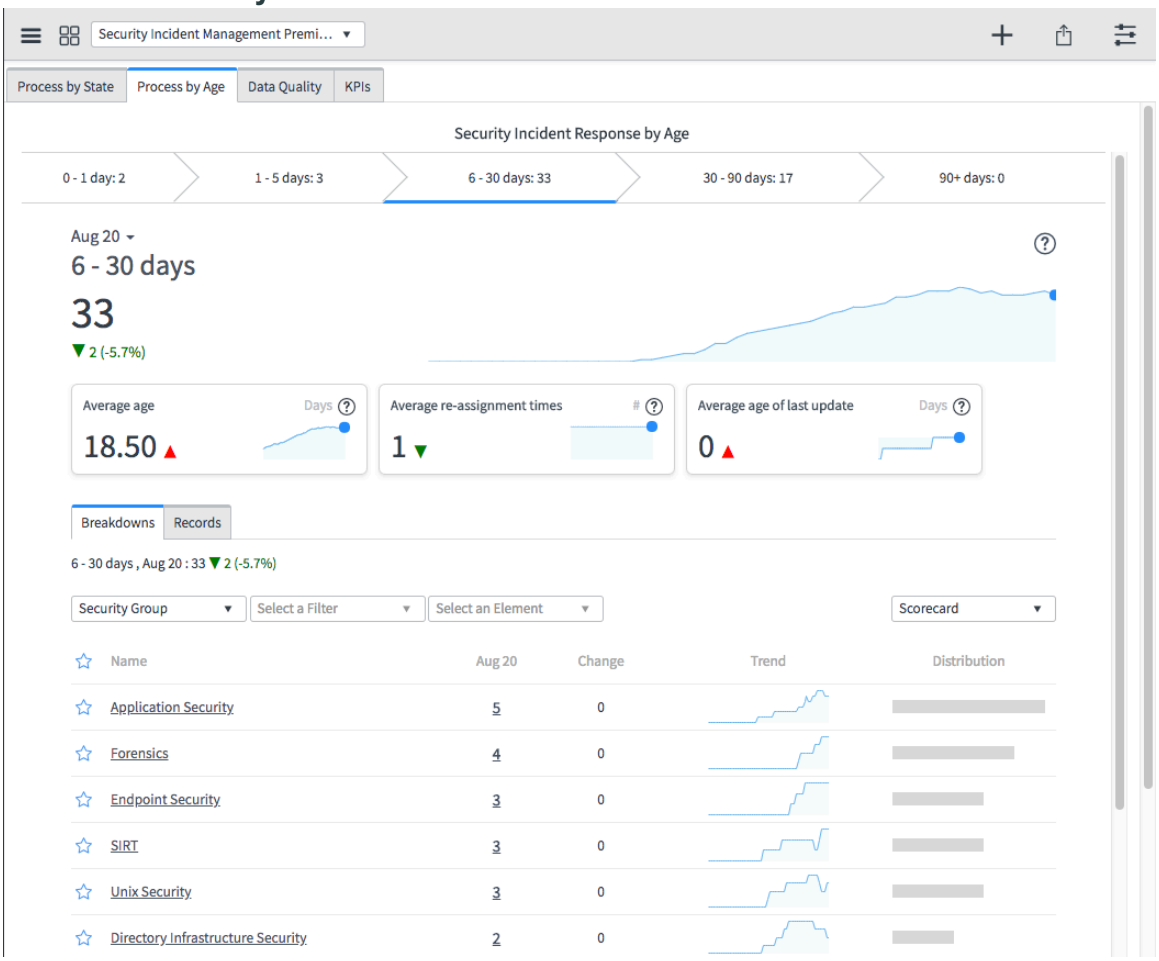
Security Incident-Antwort nach Status



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwort auf Security Incidents nach Alter



Endanwender und Rollen

Endbenutzer und Ziel	Erforderliche Rolle	Vorteile
Security Response Manager: Benötigt einen klaren Einblick in den Gesamtstatus und das Gesamtvolumen von Security Incidents, die Anwendungen und Services zugeordnet sind.	sn_si.manager	Kann die allgemeine Sicherheitslage mit der Möglichkeit überprüfen, die Mitglieder von Zuweisungsgruppen anzupassen.
Security Response-Administrator: Muss Problembereiche schnell erkennen und die vollständige Kontrolle über alle Security Incident Response-Daten haben und gleichzeitig Gebiete und Kompetenzen nach Bedarf verwalten.	sn_si.admin	Kann Risikoberechnungsparameter anpassen, um sicherzustellen, dass angreifbare Elemente, die für die Organisation am relevantesten sind, zuerst behandelt werden.
Security Response-Analysten: Muss schnell priorisieren, auf welche Schwachstellen basierend auf der Relevanz für die Organisation konzentriert werden sollen.	sn_si.analyst	Sicherheitsanalysten der Stufen 1 und 2 arbeiten an Security Incidents. Sie können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Changes und Ausfälle im

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Endbenutzer und Ziel	Erforderliche Rolle	Vorteile
		Zusammenhang mit ihren Incidents erstellen und aktualisieren.

Security Incident Management Premium-Indikatoren

Die Registerkarten „Prozess nach Status“ und „Prozess nach Alter“ enthalten Workbench-Widgets mit den folgenden Indikatoren:

Durchschnittliches Alter

Der Indikator für das durchschnittliche Alter offener Security Incidents verwendet die Formel [[summiertes Alter der offenen Security Incidents]] / [[Anzahl der offenen Security Incidents]] / 24 Um ein Ergebnis in Tagen zu geben.

Durchschnittliche Neuzuweisungszeiten

Der Indikator „Durchschnittliche Neuzuweisung offener Security Incidents“ verwendet die Formel Summierte Neuzuweisung der offenen Security Incidents/Anzahl der offenen Security Incidents .

Durchschnittliches Alter der letzten Aktualisierung

Das durchschnittliche Alter der letzten Aktualisierung offener Security Incidents verwendet die Formel Summiertes Alter der letzten Aktualisierung offener Security Incidents / Anzahl der offenen Security Incidents / 24 Um ein Ergebnis in Tagen zu geben.

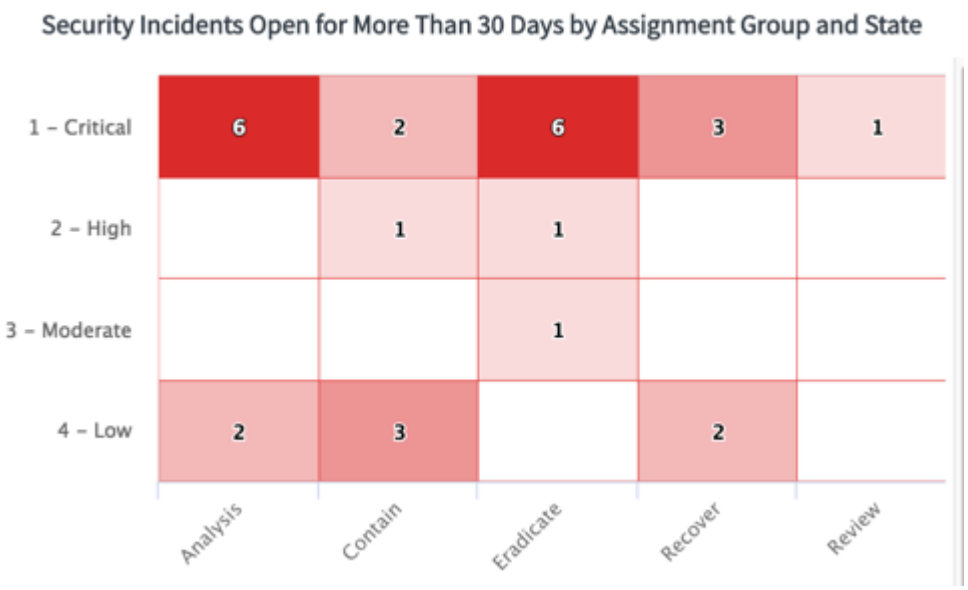
% in 5 Tagen nicht aktualisiert

Der Indikator für % der offenen Security Incidents, die in den letzten 5 Tagen nicht aktualisiert wurden, verwendet die Formel ([[Anzahl offener Security Incidents, die in den letzten 5 Tagen nicht aktualisiert wurden]] / [[Anzahl offener Security Incidents]]) * 100 .

Die Registerkarte „Datenqualität“ enthält interaktive Filter für die Kategorie des Security Incident und die Stufen von Risiko, Priorität und Schweregrad. Diese Filter werden gleichzeitig auf die folgenden Indikatoren angewendet:

Security Incidents, die seit mehr als 30 Tagen offen sind, nach Zuweisungsgruppe und Status

Die Anzahl der offenen Security Incidents, gefiltert nach einem Alter von 30 Tagen und aufgeschlüsselt nach Zuweisungsgruppe und Status.



Security Incidents mit Beauftragtem, der nicht aktiv ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anzahl der offenen Security Incidents ohne Beauftragten oder einen Beauftragten, der nicht aktiv ist.

Security Incidents, die seit mehr als 30 Tagen offen sind, nach Zuweisungsgruppe und Status

Der Indikator „Anzahl der offenen Security Incidents, die in den letzten 30 Tagen nicht aktualisiert wurden“, aufgeschlüsselt nach Zuweisungsgruppe und Status.

Die Registerkarte „KPI“ enthält die folgenden zusätzlichen Indikatoren:

- % der neuen kritischen Security Incidents
- Durchschnittliches Alter der offenen Security Incidents
- Durchschnittliche Abschlusszeit von Security Incidents
- % Der Security Incidents, die neu zugewiesen wurden
- % Der Security Incidents, die bei der ersten Zuweisung geschlossen wurden
- % Der durch Selfservice geschlossenen Security Incidents
- % Der nicht gelösten Security Incidents
- Durchschnittliche Abschlusszeit von Security Incident-Aufgaben

Aufgliederungen

Die folgenden Aufgliederungen gelten für die Indikatoren im Dashboard:

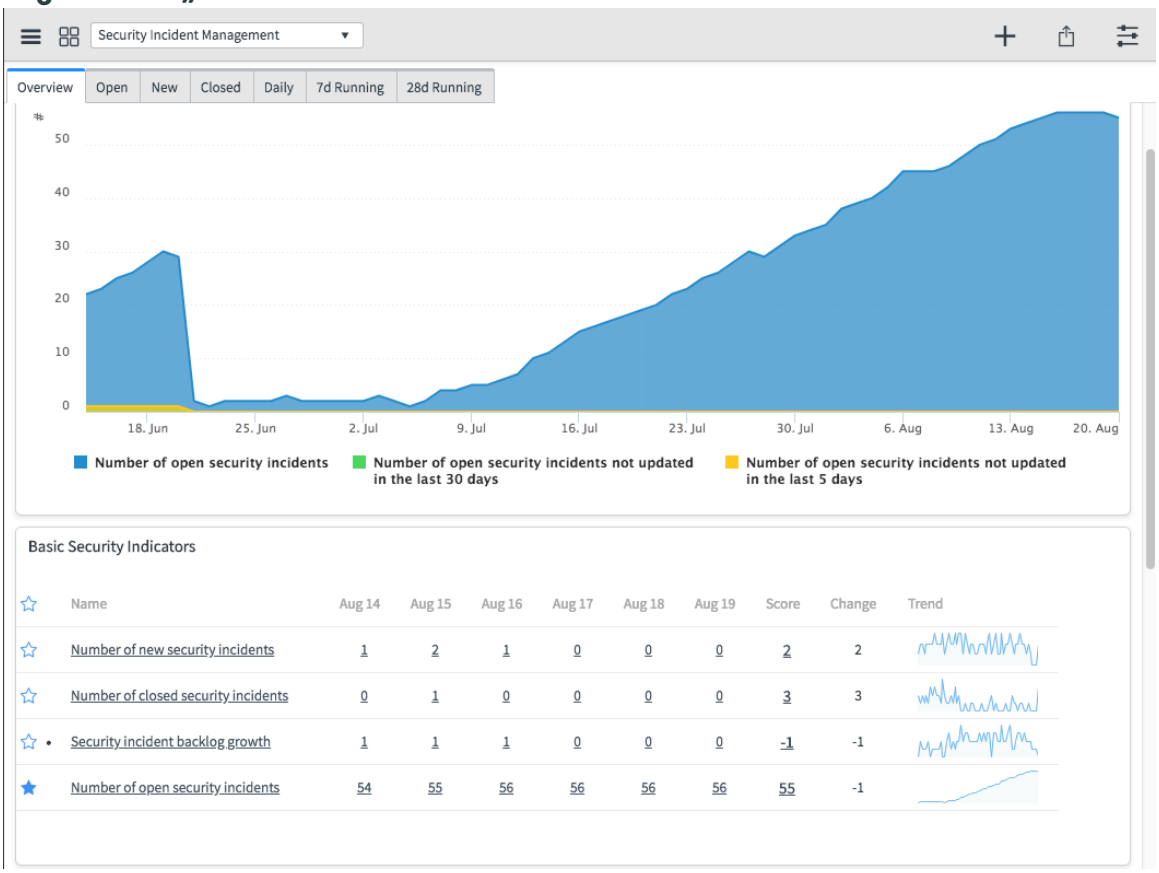
- Sicherheitsgruppe
- Alter des Security Incidents
- Kategorie von Security Incident
- Priorität von Security Incident
- Status des Security Incidents

Dashboard „Security Incident Management“

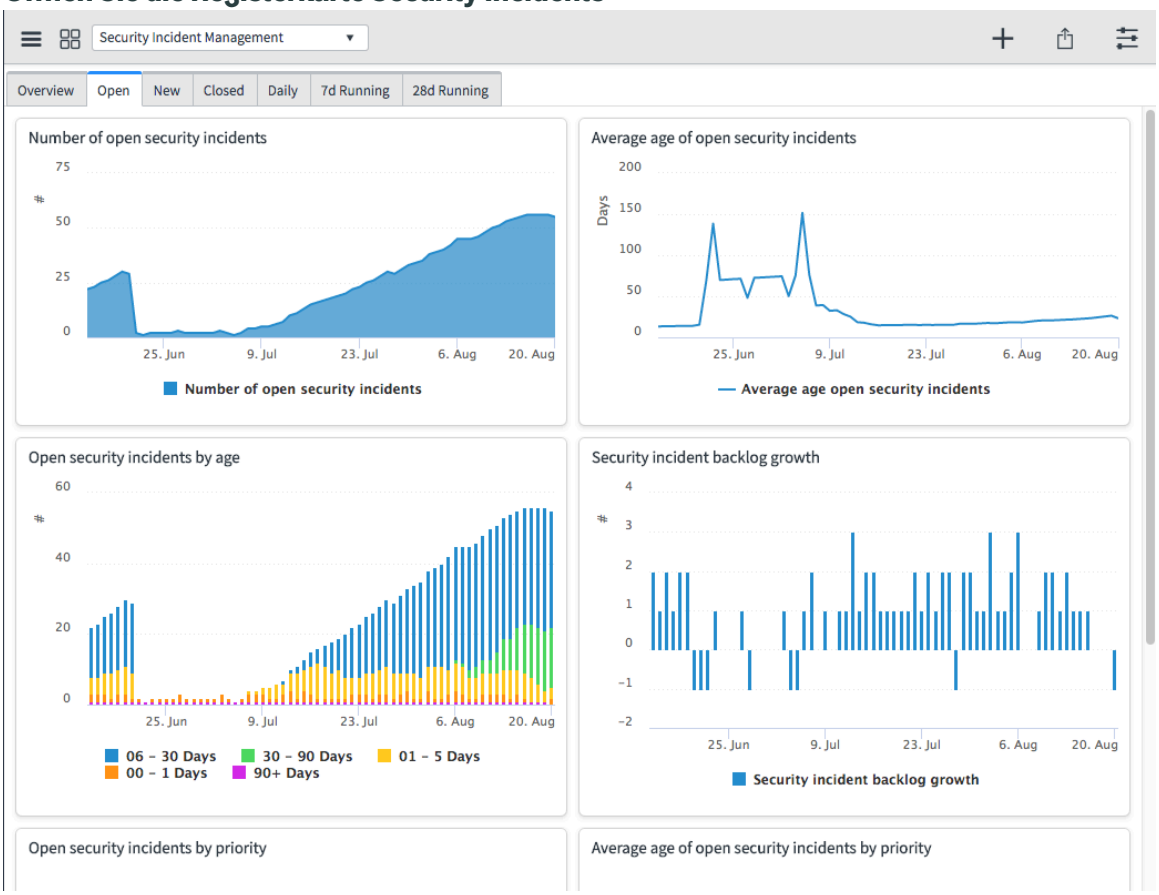
Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents problemlos nachverfolgen, von der ersten Analyse/Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Übersicht“



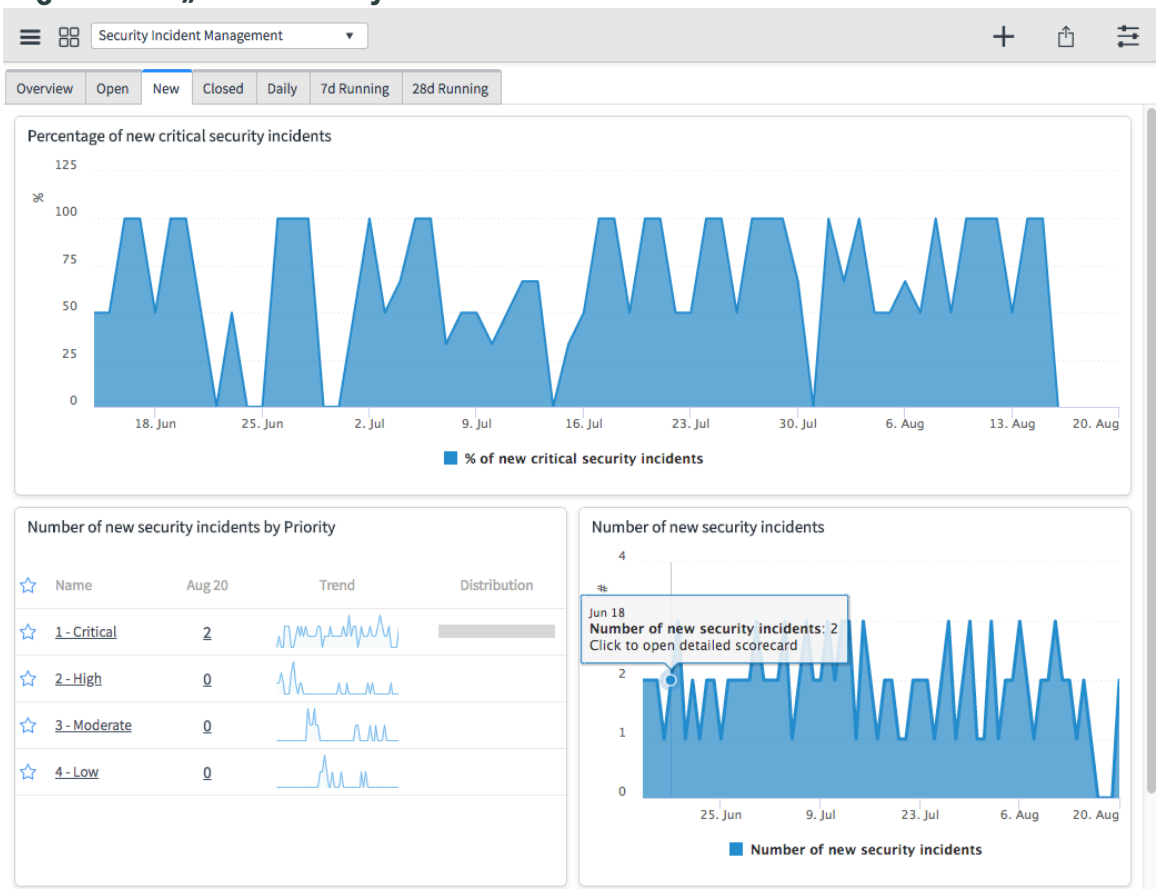
Öffnen Sie die Registerkarte Security Incidents



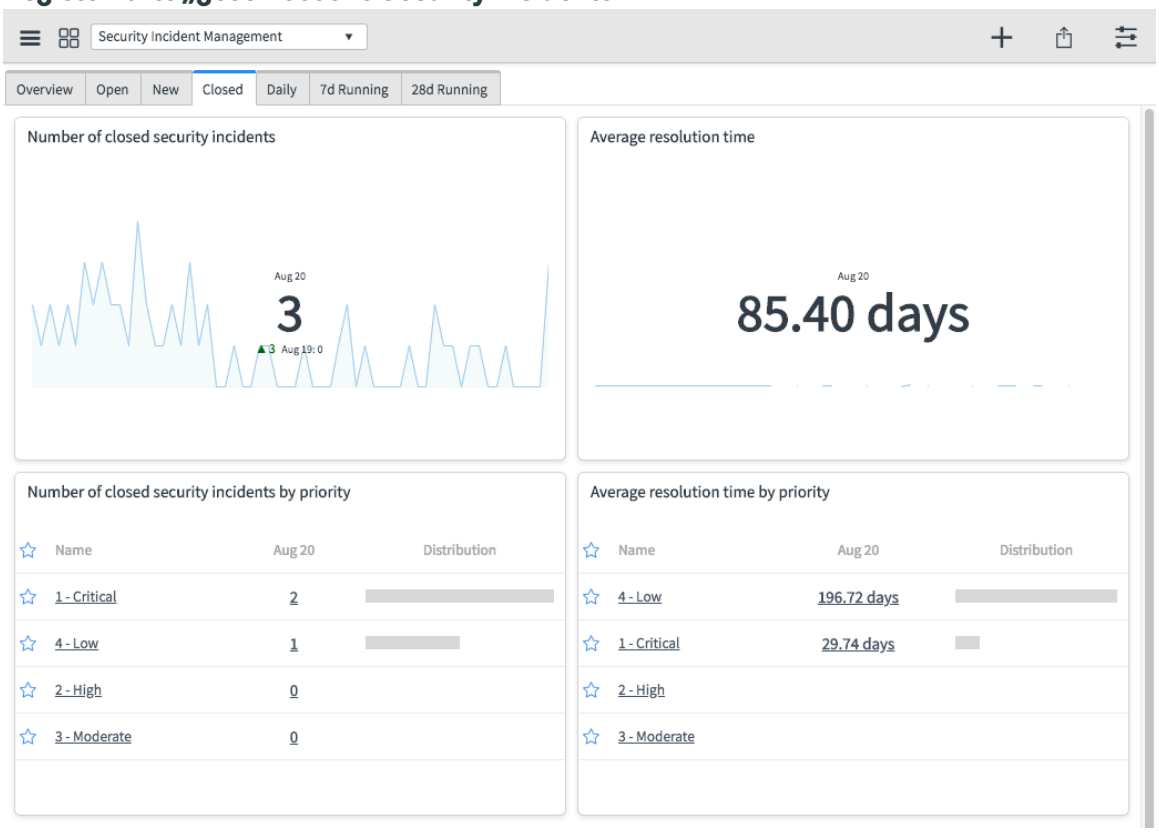
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „neuer Security Incident“



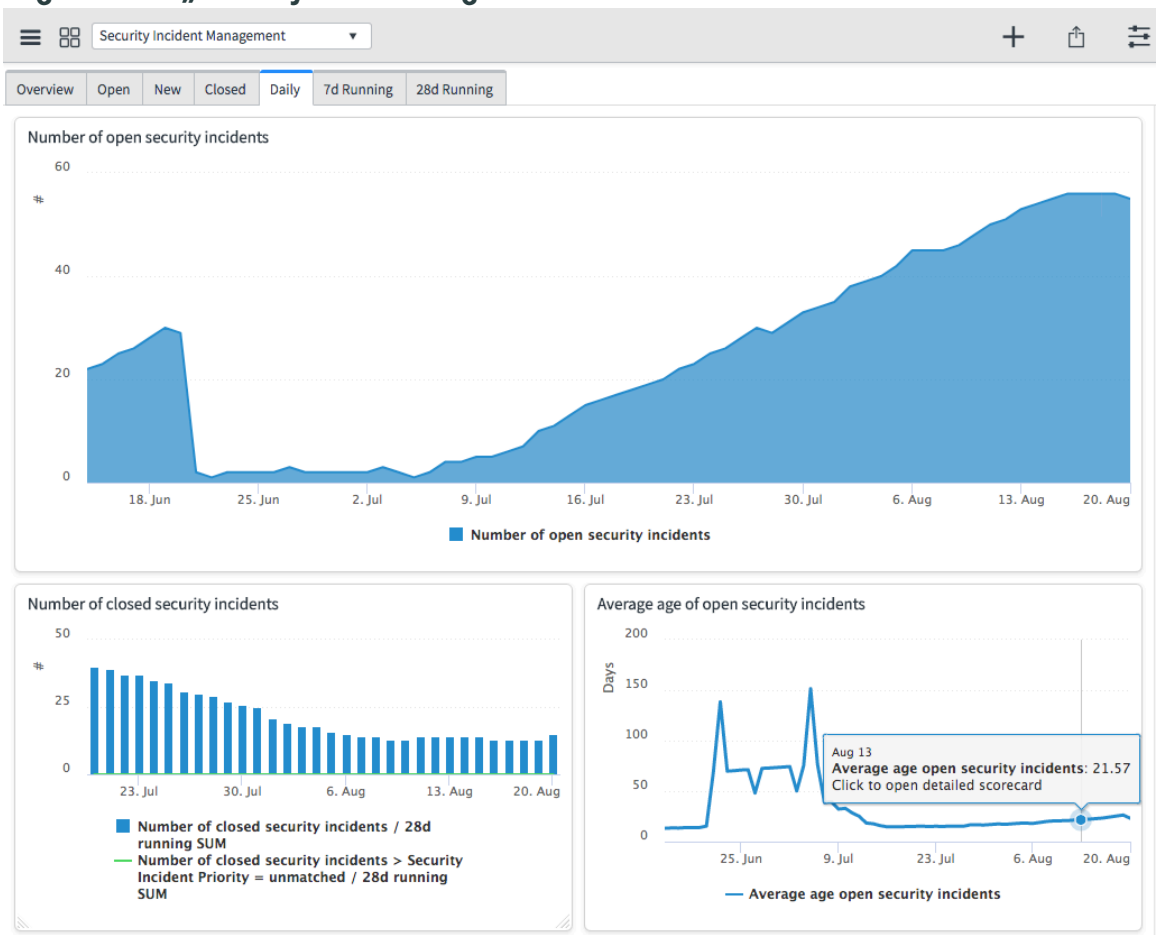
Registerkarte „geschlossene Security Incidents“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Security Incidents täglich“



Die **7 Tage wird ausgeführt** Und **28 Tage wird ausgeführt** Registerkarten entsprechen dem Format von **Täglich** Registerkarte.

Endanwender und Rollen

Endbenutzer und Ziel	Erforderliche Rolle	Vorteile
Security Response Manager: Benötigt einen klaren Einblick in den Gesamtstatus und das Gesamtvolumen von Security Incidents, die Anwendungen und Services zugeordnet sind.	sn_si.manager	Kann die allgemeine Sicherheitslage mit der Möglichkeit überprüfen, die Mitglieder von Zuweisungsgruppen anzupassen.
Security Response-Administrator: Muss Problembereiche schnell erkennen und die vollständige Kontrolle über alle Security Incident Response-Daten haben und gleichzeitig Gebiete und Kompetenzen nach Bedarf verwalten.	sn_si.admin	Kann Risikoberechnungsparameter anpassen, um sicherzustellen, dass angreifbare Elemente, die für die Organisation am relevantesten sind, zuerst behandelt werden.
Security Response-Analysten: Muss schnell priorisieren, auf welche Schwachstellen basierend auf der Relevanz für die	sn_si.analyst	Sicherheitsanalysten der Stufen 1 und 2 arbeiten an Security Incidents. Sie können Security Incidents, Anforderungen und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Endbenutzer und Ziel	Erforderliche Rolle	Vorteile
Organisation konzentriert werden sollen.		Aufgaben sowie Probleme, Changes und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren.

Indikatoren für Security Incident Management

Das Dashboard „Security Incident Management“ enthält die folgenden Leistungskennzahlen:

Neue Security Incidents

Ein Diagramm der Anzahl der neuen Security Incidents.

Offene Security Incidents

Ein Diagramm, in dem Sie die Anzahl der offenen Security Incidents, die Anzahl der offenen Security Incidents, die in den letzten 30 Tagen nicht aktualisiert wurden, und die Anzahl der offenen Security Incidents vergleichen können, die in den letzten 5 Tagen nicht aktualisiert wurden.

Indikatoren für einfache Sicherheit

Die Punktzahlen der letzten 6 Tage der Indikatoren für die Anzahl der neuen Security Incidents, die Anzahl der geschlossenen Security Incidents, das Wachstum des Security Incident-Backlogs und die Anzahl der offenen Security Incidents.

Neue Security Incidents nach Priorität

Die Anzahl der neuen Security Incidents, aufgeschlüsselt nach Priorität.

Aufgliederungen

Die folgenden Aufgliederungen gelten für die Indikatoren im Dashboard:

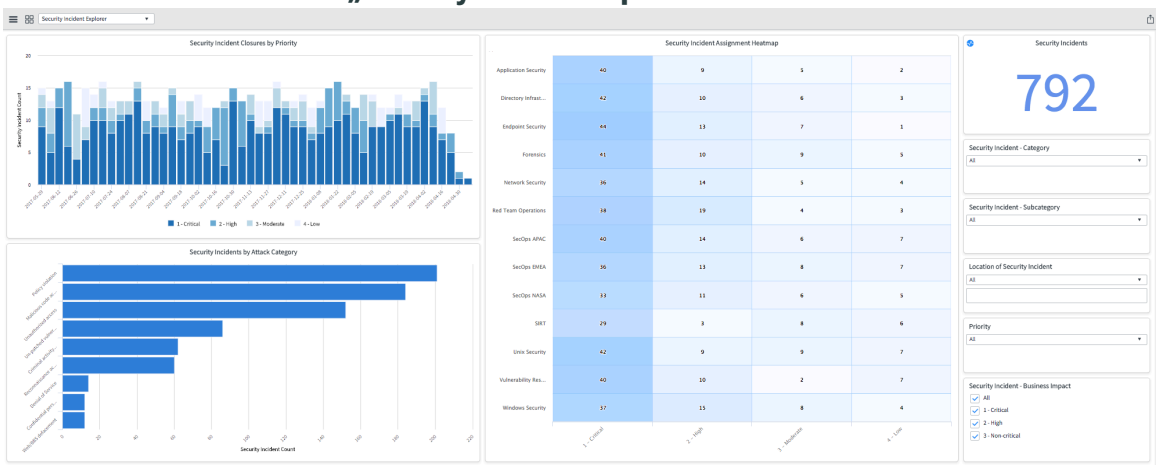
- Sicherheitsgruppe
- Alter des Security Incidents
- Kategorie von Security Incident
- Priorität von Security Incident
- Status des Security Incidents

Dashboard „Security Incident Explorer“

Mit diesem Dashboard können Sicherheitsmanager Security Incidents zusammengefasst und nach Kategorie, Unterkategorie, Standort, Priorität und Geschäftsauswirkungen gruppiert anzeigen. Mit diesen Ansichten erhalten Manager schnell Einblicke in die Häufigkeit, mit der Angriffe auftreten und welche Business-Services betroffen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Teilansicht des Dashboard „Security Incident Explorer“



Endanwender und Rollen

Endbenutzer und Ziel	Erforderliche Rolle	Vorteile
Security Response Manager: Benötigt einen klaren Einblick in den Gesamtstatus und das Gesamtvolumen von Security Incidents, die Anwendungen und Services zugeordnet sind.	sn_si.manager	Kann die allgemeine Sicherheitslage mit der Möglichkeit überprüfen, die Mitglieder von Zuweisungsgruppen anzupassen.
Security Response-Administrator: Muss Problembereiche schnell erkennen und die vollständige Kontrolle über alle Security Incident Response-Daten haben und gleichzeitig Gebiete und Kompetenzen nach Bedarf verwalten.	sn_si.admin	Kann Risikoberechnungsparameter anpassen, um sicherzustellen, dass angreifbare Elemente, die für die Organisation am relevantesten sind, zuerst behandelt werden.
Security Response Analyst:s müssen schnell priorisieren, auf welche Schwachstellen basierend auf der Relevanz für die Organisation konzentriert werden sollen.	sn_si.analyst	Sicherheitsanalysten der Stufen 1 und 2 arbeiten an Security Incidents. Sie können Security Incidents, Anforderungen und Aufgaben sowie Probleme, Changes und Ausfälle im Zusammenhang mit ihren Incidents erstellen und aktualisieren.

Indikatoren für Security Incident Explorer

Das Dashboard „Security Incident Explorer“ enthält die folgenden Leistungskennzahlen:

Security Incidents

Das Gesamtvolumen der offenen und ausstehenden Security Incidents.

Security Incident-Abschlüsse nach Priorität

Die Anzahl der geschlossenen Security Incidents, aufgeschlüsselt nach Priorität.

Security Incidents nach Angriffskategorie

Die Anzahl der offenen Security Incidents, aufgeschlüsselt nach Kategorie.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Heatmap Für Security Incident-Zuweisung

Eine zweistufige Aufgliederung der Anzahl der offenen Security Incidents nach Zuweisungsgruppe und Priorität.

Heatmap Für Security Incidents

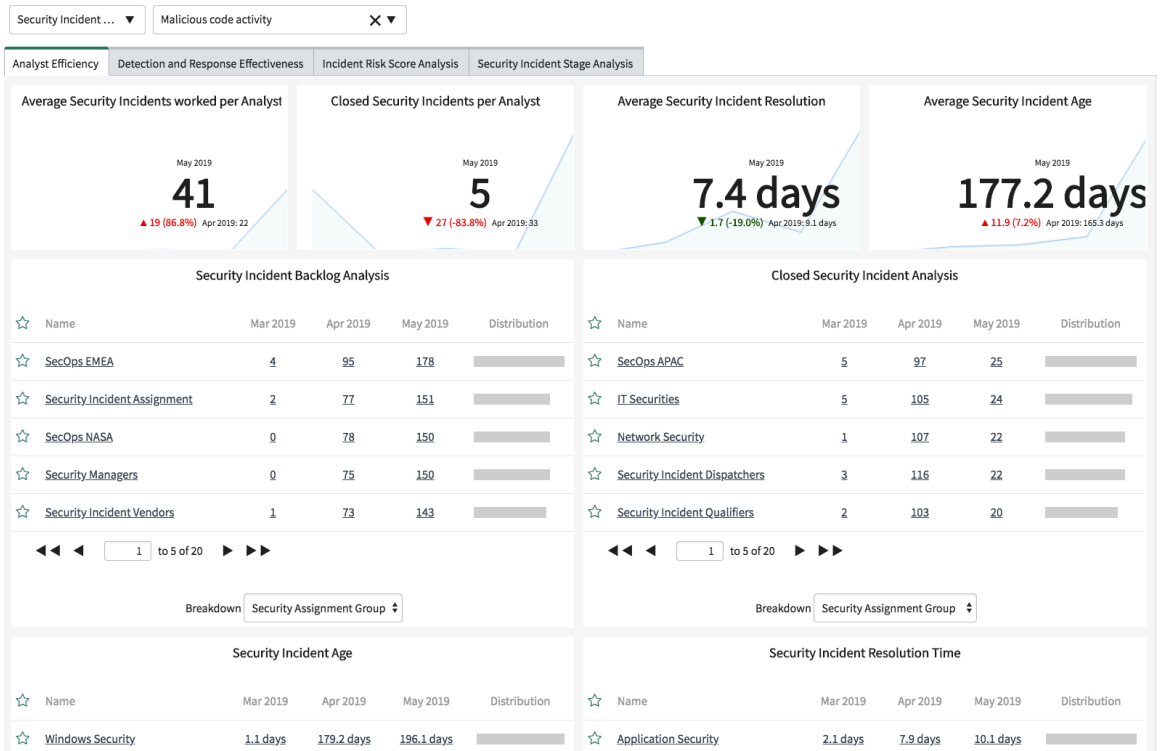
Eine globale Karte, die die Anzahl der offenen Security Incidents in jedem Land anzeigt.

Dashboard „Effizienz von Security Operations“

Manager des Security Operations Center (SOC) können allgemeine Effizienzmetriken anzeigen und die individuelle Leistung der SOC-Teammitglieder in der Organisation messen.

Der SOC-Manager kann das Performance Analytics-Dashboard verwenden, um die Effizienz zu verbessern und ein Bild davon zu entwickeln, wie SOC im Laufe der Zeit sowohl in allgemeinen als auch in bestimmten Bereichen abschneidet.

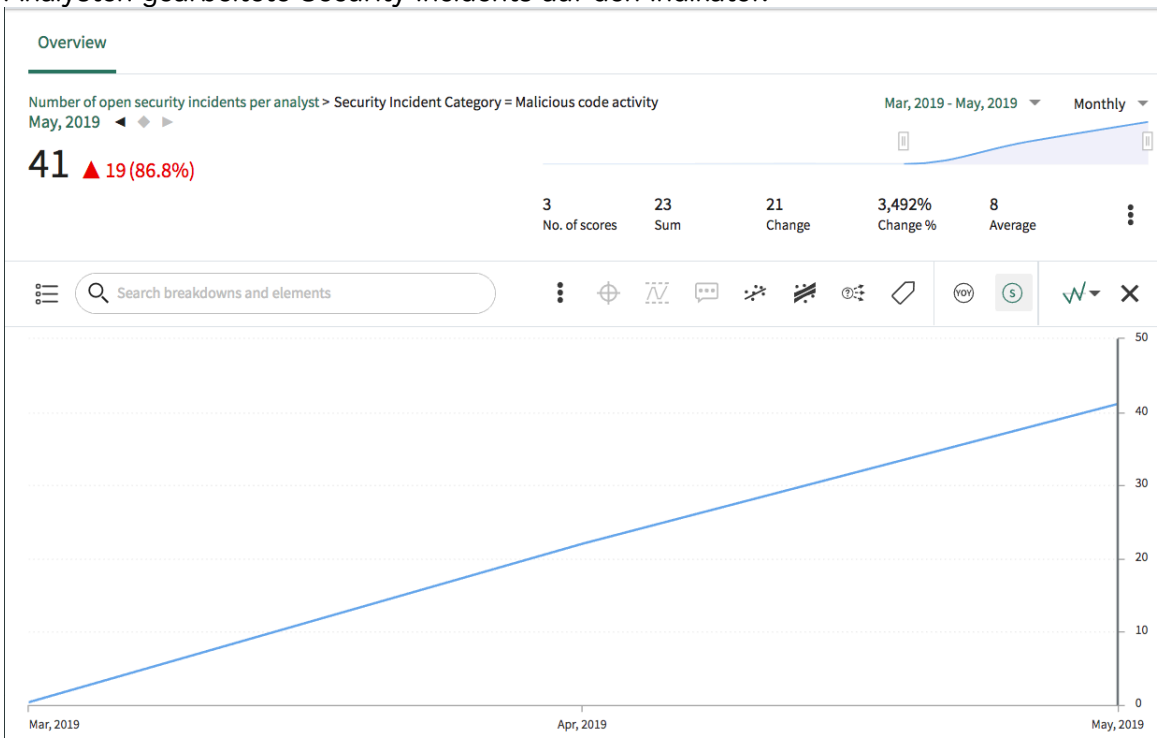
Registerkarte „Effizienz der Analysten“



Klicken Sie auf einen der Indikatoren, um weitere Details anzuzeigen.
Klicken Sie beispielsweise im Abschnitt Durchschnittliche pro

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Analysten gearbeitete Security Incidents auf den Indikator.



Das Diagramm zeigt, dass die Anzahl der offenen Security Incidents von 0 im März auf über 40 im Mai gestiegen ist. Beachten Sie die im Header angezeigten Daten:

- Trendindikator: Zeigt die Änderung der Anzahl der offenen Incidents im letzten Zeitraum an, für den die Daten erfasst wurden. Dieses Diagramm zeigt Daten für den Zeitraum März 2019 bis Mai 2019, und die Anzahl der offenen Incidents ist im Mai um 19 gestiegen. Die Effizienz der Analysten ist besser, wenn die Anzahl der offenen Incidents über einen bestimmten Zeitraum abgenommen hat.
- Anzahl der Punktzahlen: Der Zeitraum, für den die Daten erfasst wurden (März bis Mai 2019).
- Summe: Die Anzahl der neuen offenen Incidents für den Zeitraum zwischen März und Mai.
- Change: Die Anzahl der neuen offenen Incidents zwischen März und April.
- Durchschnitt: Die durchschnittliche Anzahl offener Incidents pro Analyst für den ausgewählten Zeitraum.

Registerkarte „Effizienz der Analysten“

Indikator	Beschreibung
Durchschnittliche pro Analyst bearbeitete Security Incidents	Durchschnittliche Anzahl offener Security Incidents pro Analyst für den angegebenen Zeitraum. Die verwendete Formel ist [[Anzahl der offenen Security Incidents / pro Monat – Durchschnitt +]]/[[Anzahl der Security Agents]]
Geschlossene Security Incidents pro Analyst	Die Gesamtzahl der Incidents, die von jedem Analyst in der ausgewählten Kategorie im angegebenen Zeitraum geschlossen wurden. Die verwendete Formel ist [Anzahl der geschlossenen Security Incidents > Kategorie der Security Incidents = <category_name> / pro Monat SUMME +]]/ [[Anzahl der Security Agents / pro Monat Durchschnitt +]]

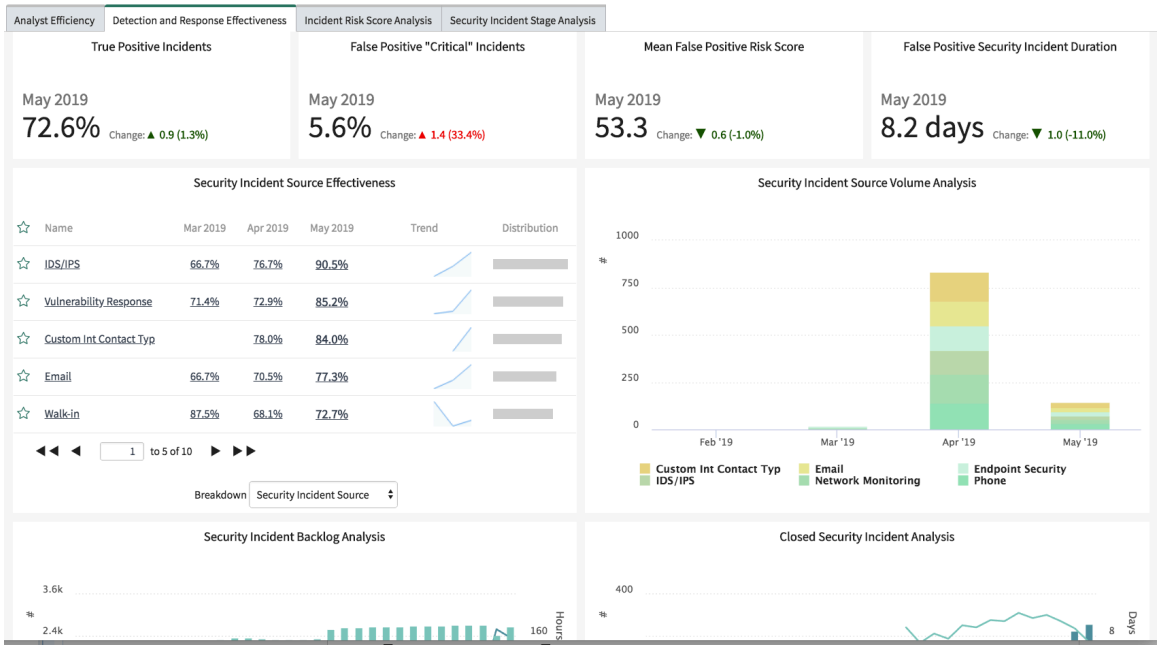
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Effizienz der Analysten“ (Fortsetzung)

Indikator	Beschreibung
Durchschnittliche Security Incident-Lösung	Die durchschnittliche Zeit, die jeder Analyst im angegebenen Zeitraum benötigt, um Security Incidents zu schließen. Die Formel, die zum Anzeigen des Ergebnisses in Tagen verwendet wird, ist ([[summierte Dauer der geschlossenen Security Incidents > Kategorie der Security Incidents = <category_name> / pro Monat Durchschnitt +]] / [[Anzahl der geschlossenen Security Incidents > Kategorie der Security Incidents = <category_name> / pro Monat Durchschnitt +]]) / 24
Durchschnittliches Alter von Security Incidents	Die durchschnittliche Anzahl der Tage, für die Security Incidents für jeden Analysten offen bleiben. Die Formel, die zum Anzeigen des Ergebnisses in Tagen verwendet wird, ist ([[summiertes Alter der offenen Security Incidents > Security Incident-Kategorie = <category_name> / pro Monat Durchschnitt +]]/ [[Anzahl der offenen Security Incidents > Security Incident-Kategorie = <category_name> / pro Monat Durchschnitt +]]) / 24
Analyse des Security Incident-Backlogs	Die Gesamtzahl der offenen Security Incidents im angegebenen Zeitraum. Wählen Sie eine Option aus der Aufgliederungsliste aus, um den Backlog für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Sie können auch die Anzahl der offenen Security Incidents zwischen zwei ausgewählten Monaten vergleichen.
Analyse geschlossener Security Incidents	Die Gesamtzahl der Security Incidents, die im angegebenen Zeitraum geschlossen wurden. Wählen Sie eine Option aus der Aufgliederungsliste aus, um die Anzahl für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Sie können auch die Anzahl der Security Incidents vergleichen, die zwischen zwei ausgewählten Monaten geschlossen wurden.
Alter des Security Incidents	Die durchschnittliche Anzahl von Tagen, die Security Incidents im angegebenen Zeitraum offen bleiben. Wählen Sie eine Option aus der Aufgliederungsliste aus, um das Alter von Security Incidents für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Die Formel, die zum Anzeigen des Ergebnisses in Tagen verwendet wird, ist ([[summiertes Alter der offenen Security Incidents > Security Incident-Kategorie = <category_name> > Sicherheitszuweisungsgruppe = <group_name> / nach Monat Durchschnitt +]]/ [[Anzahl der offenen Security Incidents > Security Incident-Kategorie = <category_name> > Sicherheitszuweisungsgruppe = <group_name> / nach Monat Durchschnitt +]]) / 24
Lösungszeit für Security Incidents	Die durchschnittliche Anzahl der Tage, die für die Lösung von Security Incidents während des angegebenen Zeitraums benötigt werden. Wählen Sie eine Option aus der Aufgliederungsliste aus, um die Lösungszeit für Security Incidents für jeden Analysten, jede Sicherheitsgruppe, jede Priorität usw. anzuzeigen. Die Formel, die zum Anzeigen des Ergebnisses in Tagen verwendet wird, ist ([[summierte Dauer der geschlossenen Security Incidents > Kategorie des Security Incidents = böswillige Codeaktivität > Sicherheit zugewiesen an = John Ashby / pro Monat Durchschnitt +]] / [[Anzahl der geschlossenen Security Incidents > Kategorie des Security Incidents = böswillige Codeaktivität > Sicherheit zugewiesen an = John Ashby / nach Monat Durchschnitt +]]) / 24

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erkennung und Effektivität der Reaktion“



Registerkarte „Erkennung und Effektivität der Reaktion“

Indikator	Beschreibung
Wirklich positive Incidents	Prozentsatz der wirklich positiven Security Incidents in der ausgewählten Kategorie für den angegebenen Zeitraum. Die verwendete Formel ist (1-([[Anzahl der falsch positiven Security Incidents > Kategorie der Security Incidents = böswillige Codeaktivität / pro Monat SUMME +]] / [[Anzahl der geschlossenen Security Incidents > Kategorie der Security Incidents = böswillige Codeaktivität / pro Monat SUMME +]]) * 100
Falsch positive kritische Incidents	Prozentsatz der falsch positiven kritischen Security Incidents in der ausgewählten Kategorie für den angegebenen Zeitraum. Die verwendete Formel ist ([[Anzahl der falsch positiven Security Incidents > Security Incident-Risikopunktzahl = Kritisches Risiko > Security Incident-Kategorie = böswillige Codeaktivität / pro Monat SUMME +]] / [[Anzahl der geschlossenen Security Incidents > Security Incident-Kategorie = böswillige Codeaktivität / pro Monat SUMME +]]) * 100 **Hinweis:** Alle Security Incidents, bei denen Geschlossener Code = Ungültige Schwachstelle oder falsch positiv Wird als falsch positiver Incident behandelt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erkennung und Effektivität der Reaktion“ (Fortsetzung)

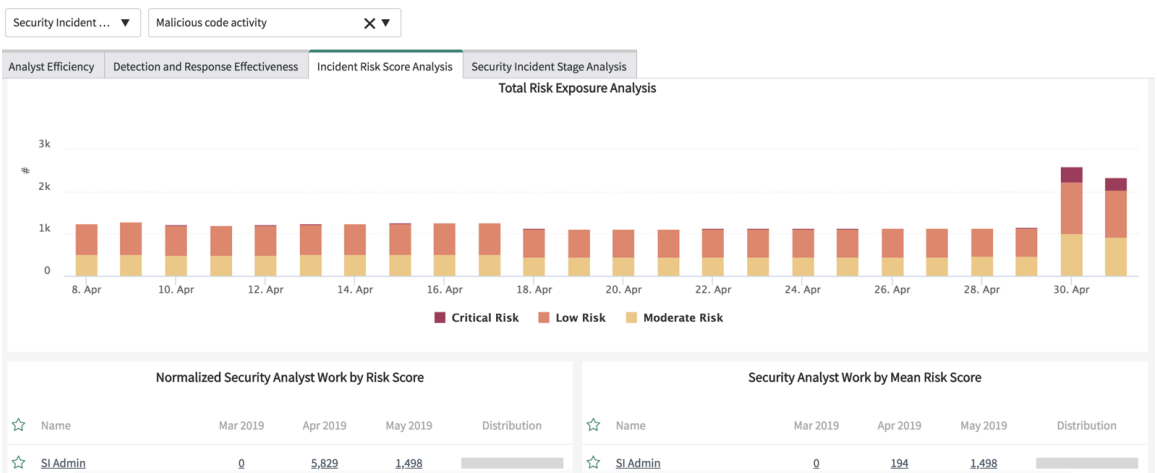
Indikator	Beschreibung
Mittlere falsch positive Risikopunktzahl	Durchschnittliche monatliche Risikopunktzahl der geschlossenen Security Incidents, die als falsch positive Incidents identifiziert wurden. Eine niedrigere Risikopunktzahl gibt an, dass die Sicherheitsanalysten weniger Zeit mit der Analyse falsch positiver Incidents verbracht haben. Die verwendete Formel ist ([[Anzahl der falsch positiven Security Incidents > Security Incident-Risikopunktzahl = Kritisches Risiko > Security Incident-Kategorie = böswillige Codeaktivität / pro Monat SUMME +]] / [[Anzahl der geschlossenen Security Incidents > Security Incident-Kategorie = böswillige Codeaktivität / pro Monat SUMME +]]) * 100
Dauer des falsch positiven Security Incidents	Durchschnittliche Anzahl der Tage, die die Sicherheitsanalysten für die Untersuchung falsch positiver Incidents aufgewendet haben. Die verwendete Formel ist ([[summierte Dauer falsch positiver Security Incidents]] / [[Anzahl falsch positiver Security Incidents]]) / 24
Effektivität der Security Incident-Quelle	Prozentsatz der wirklich positiven Security Incidents, die von einer bestimmten Quelle für den angegebenen Zeitraum identifiziert wurden. Die Quelle kann E-Mail, Netzwerkaktivität, Kundensupport usw. sein. Diese Daten helfen bei der Messung der Effektivität der Security Incident-Quelle. Die verwendete Formel ist (1-([[Anzahl der falsch positiven Security Incidents > Kategorie des Security Incidents = böswillige Codeaktivität > Quelle des Security Incidents = IDS/IPS / pro Monat SUMME +]]] / [[Anzahl der geschlossenen Security Incidents > Kategorie des Security Incidents = böswillige Codeaktivität > Quelle des Security Incidents = IDS/IPS / pro Monat SUMME +]]) * 100
Analyse des Quell-Volumes für Security Incidents	Anzahl der geschlossenen Security Incidents für den aktuellen Monat für jede Security Incident-Quelle. Sie können auch die Anzahl der Security Incidents für jeden Quelltyp zwischen zwei ausgewählten Monaten vergleichen.
Analyse des Security Incident-Backlogs	Die Gesamtzahl der offenen Security Incidents im angegebenen Zeitraum und die durchschnittliche Anzahl der Tage, für die die Incidents offen bleiben. Sie können auch die Anzahl der offenen Security Incidents zwischen zwei ausgewählten Monaten vergleichen. Die Formel, die zur Berechnung des durchschnittlichen Backlog-Zeitraums verwendet wird, lautet ([[summiertes Alter der offenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erkennung und Effektivität der Reaktion“ (Fortsetzung)

Indikator	Beschreibung
	Security Incidents > Security Incident-Kategorie = böswillige Codeaktivität]]/ [[Anzahl offener Security Incidents > Security Incident-Kategorie = böswillige Codeaktivität]]) / 24
Analyse geschlossener Security Incidents	Die Gesamtzahl der geschlossenen Security Incidents im angegebenen Zeitraum und die durchschnittliche Lösungszeit für diese Incidents. Die Formel, die zur Berechnung der durchschnittlichen Lösungszeit verwendet wird, beträgt ([[summierte Dauer der geschlossenen Security Incidents > Kategorie des Security Incidents = schädliche Codeaktivität]] / [[Anzahl der geschlossenen Security Incidents > Kategorie des Security Incidents = schädliche Codeaktivität]]) / 24

Registerkarte Analyse der Incident-Risikopunktzahl



Registerkarte Analyse der Incident-Risikopunktzahl

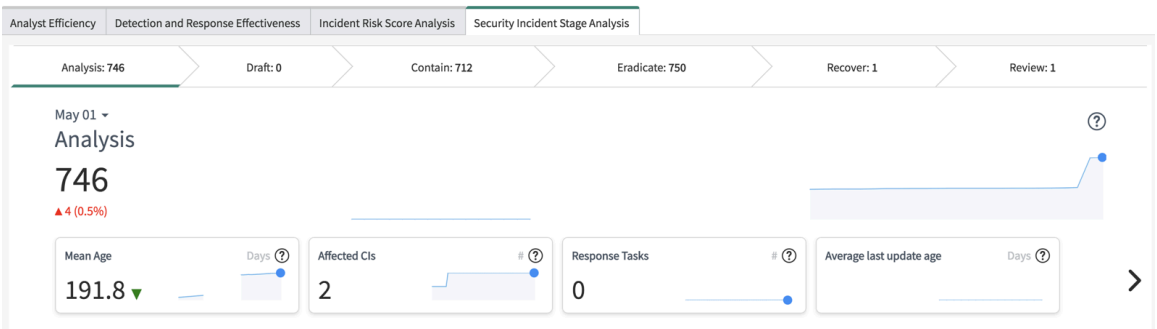
Indikator	Beschreibung
Analyse des Gesamtrisikorisikos	Gesamtzahl der offenen Incidents in jeder Risikokategorie (niedrig, Mittel und Kritisch) im angegebenen Zeitraum. Sie können auch die Anzahl der Incidents in den verschiedenen Risikokategorien zwischen zwei Monaten vergleichen.
Normalisierte Arbeit von Sicherheitsanalysten nach Risikopunktzahl	Die Gesamtrisikopunktzahl für jeden Sicherheitsanalysten für den angegebenen Zeitraum. Dies wird basierend auf der Anzahl der wirklich positiven Security Incidents berechnet, die der Sicherheitsanalyst geschlossen hat. Die verwendete Formel ist [[summierte Risikopunktzahl der geschlossenen Security Incidents > Kategorie des Security Incidents = böswillige

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte Analyse der Incident-Risikopunktzahl (Fortsetzung)

Indikator	Beschreibung
	Codeaktivität > Sicherheit zugewiesen = SI-Administrator / pro Monat SUMME +]] - [[summierte Risikopunktzahl der falsch positiven Security Incidents > Kategorie des Security Incidents = böswillige Codeaktivität > Sicherheit zugewiesen = SI-Administrator / pro Monat SUMME +]]]
Arbeit von Sicherheitsanalysten nach durchschnittlicher Risikopunktzahl	Die durchschnittliche Risikopunktzahl für jeden Sicherheitsanalysten für den angegebenen Zeitraum. Die verwendete Formel ist [[summierte Risikopunktzahl der geschlossenen Security Incidents > Kategorie des Security Incidents = böswillige Codeaktivität > Sicherheit zugewiesen = SI-Administrator / pro Monat Durchschnitt +]] - [[summierte Risikopunktzahl der falsch positiven Security Incidents > Kategorie des Security Incidents = böswillige Codeaktivität > Sicherheit zugewiesen an = SI-Administrator / pro Monat Durchschnitt +]]]

Registerkarte „Analyse der Security Incident-Phase“



Sie können die Anzahl der offenen Incidents an einem bestimmten Tag und den Status (Analyse, Entwurf, Eindämmung, Beseitigung, Wiederherstellung, oder überprüfen) dieser Incidents. In jeder Phase können Sie durchschnittliches Alter, betroffene CIs, Antwortaufgaben usw. anzeigen. Klicken Sie auf einen Link, um zusätzliche Details oder die Aufgliederung dieser Incidents anzuzeigen.

Arbeitsbereich für Security Incident Response

Die ServiceNow® Arbeitsbereich für Security Incident Response Ist eine neu konzipierte Schnittstelle, die Sicherheitsanalysten und SOC-Managern eine Anwender-Experience der nächsten Generation bietet. Sicherheitsanalysten können dies verwenden, um den Lebenszyklus von Security Incidents von der ersten Analyse bis zur Eindämmung, Beseitigung und Wiederherstellung zu verwalten.

Erste Schritte mit SIR-Arbeitsbereich

Wählen Sie eine Kachel aus, um mit den ersten Schritten zu beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsbereich Erkunden

Erfahren Sie mehr über SIR Workspace-Konzepte und -Funktionen

Administratoren, die den Arbeitsbereich verwenden

Konfigurieren Sie SIR-Arbeitsbereich und -Funktionen

Analysten, die den Arbeitsbereich verwenden

Erfahren Sie, wie Analysten SIR Workspace verwenden

SIR-Dashboards anzeigen

SIR Workspace-Dashboards anzeigen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Wichtig:

- Installieren von Security Incident Response Version 13.4.5 oder höher aus ServiceNow Store Installiert automatisch Arbeitsbereich für Security Incident Response(sn_si_aw) Version 1.5.1 oder höher standardmäßig. Weitere Informationen zu den abhängigen Anwendungen finden Sie unter SIR-Arbeitsbereich Plugins und Rollen Abschnitt.
- Beachten Sie, dass die Version 1.5.1 und höher des Security Incident Response Workspace nur durch eine Installation/Aktualisierung von Security Incident Response installiert/aktualisiert werden kann und nicht unabhängig installiert werden kann.

Weitere Ressourcen

Besuchen Sie Security Incident Response-forum auf der ServiceNow Community.

SIR-Arbeitsbereich erkunden

Erkunden Arbeitsbereich für Security Incident Response Um zu verstehen, wie Sicherheitsanalysten und -Manager ihre täglichen Vorgänge mit einer verbesserten Anwender-Experience ausführen, führen Sie eine vollständige Incident-Untersuchung durch, und erhalten Sie einen Überblick über die Security Incidents, Antwortaufgaben und SLAs, die dem Sicherheitsanalysten und -Team zugewiesen sind.

In diesem Abschnitt wird Folgendes beschrieben:

- SIR-Arbeitsbereich Plugins und erforderliche Rollen.
- Schlüssel SIR-Arbeitsbereich Funktionen.

SIR-Arbeitsbereich Plugins und Rollen

Im Folgenden sind die erforderlichen Anwendungen aufgeführt, mit denen gearbeitet werden soll Arbeitsbereich für Security Incident Response Plugin (sn_si_aw).

Anwendungen

Installieren von Security Incident Response In der Anwendungsversion 13.4.5 oder höher wird automatisch installiert Arbeitsbereich für Security Incident Response Und die folgenden Apps.

- Enterprise Security Case Management PAD-Commons [sn_escm_Pad_cmn]
- Allgemeiner Security Operations-Arbeitsbereich [sn_escm_WS_cmn]
- UI-Kartenkomponente für Security Incident [sn_sirw_evam]
- Security Operations-Spoke [sn_sec_Spoke]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

- Installieren von Security Incident Response Version 13.4.5 oder höher aus ServiceNow Store Installiert automatisch Arbeitsbereich für Security Incident Response(sn_si_aw) Version 1.5.1 oder höher standardmäßig. Weitere Informationen zu den abhängigen Anwendungen finden Sie unter SIR-Arbeitsbereich Plugins und Rollen Abschnitt.
- Beachten Sie, dass die Version 1.5.1 und höher des Security Incident Response Workspace nur durch eine Installation/Aktualisierung von Security Incident Response installiert/aktualisiert werden kann und nicht unabhängig installiert werden kann.

Enterprise Security Case Management PAD Commons Erfordert das Playbook-Experience-Plugin [Playbook_Experience].

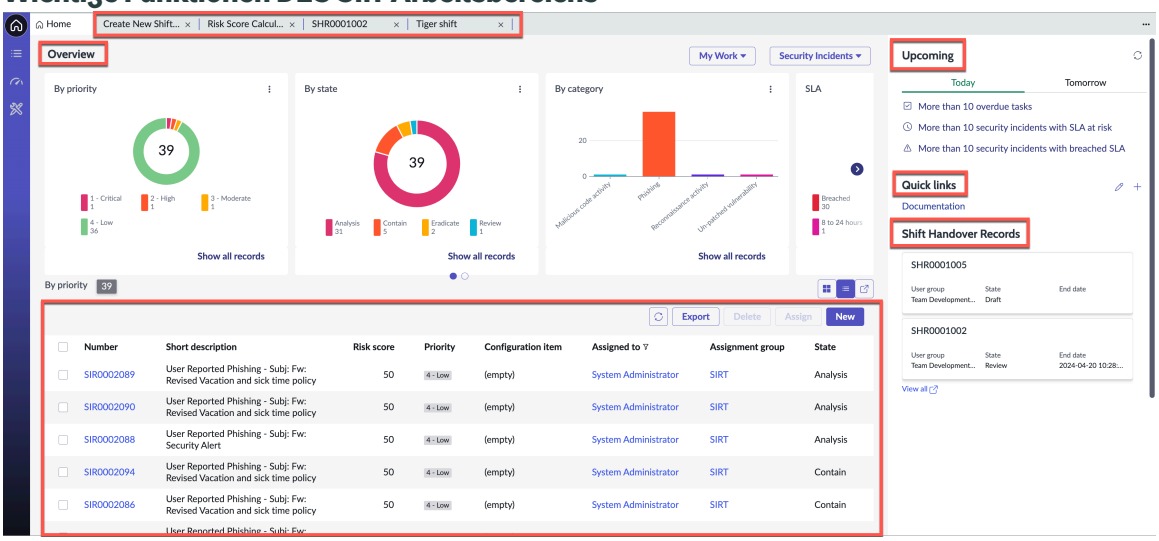
Für Informationen zu Security Incident Response Rollen, Tabellen, Eigenschaften und geplante Aufgaben, siehe Mit Security Incident Response installierte Komponenten

SIR-Arbeitsbereichsfunktionen

Die Arbeitsbereich für Security Incident Response Besteht aus den folgenden wichtigen Funktionen.

- Übersichtsbereich
- Abschnitt „Bevorstehend“
- Abschnitt „Quick-Links“
- Abschnitt „Schichtübergabedatensätze“
- Listenansicht
- Schnittstelle mit mehreren Registerkarten, die das Öffnen mehrerer Security Incidents unterstützt

Wichtige Funktionen DES SIR-Arbeitsbereichs



SIR-Arbeitsbereich Schnittstellenübersicht

Die SIR-Arbeitsbereich Die Übersichtsseite enthält die Details zu Security Incidents und Antwortaufgaben, die sich unter Sicherheitsanalysten und ihrem Team befinden.

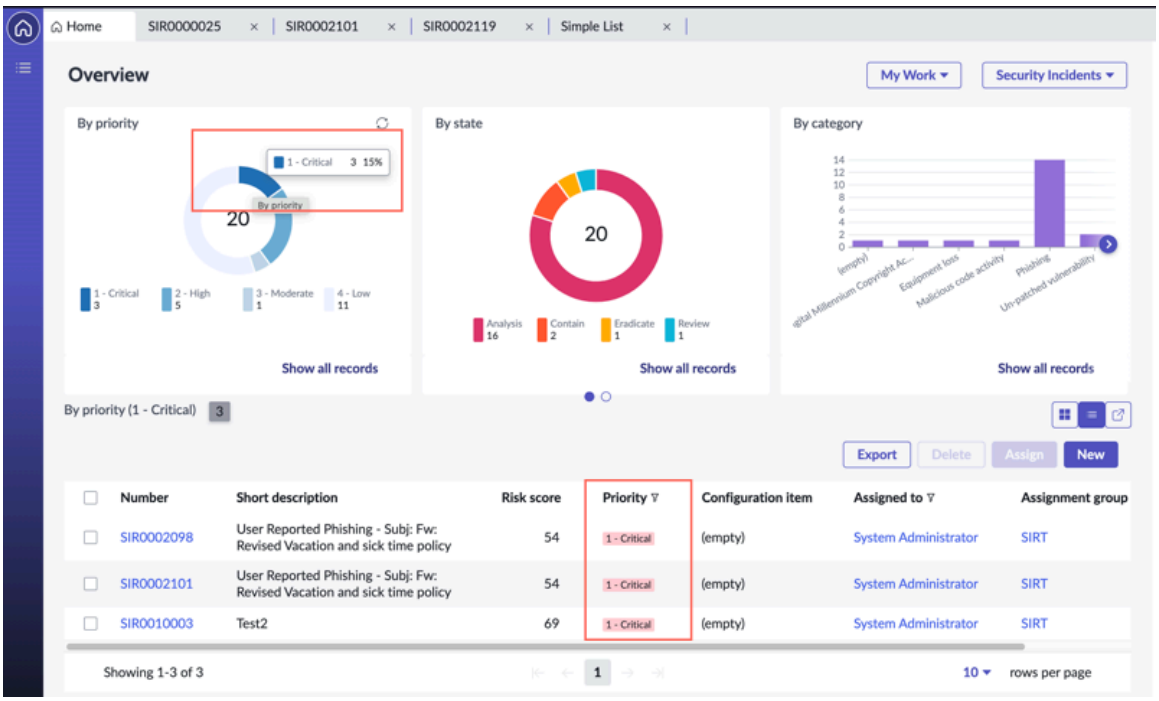
Unter jedem Filter sind verschiedene Widgets vorhanden, gruppiert nach Priorität, Kategorie, Status und SLA, die sich in den Warteschlangen der Sicherheitsanalysten und des Sicherheitsanalystenteams befinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Filter auf die Widgets angewendet werden, wird die untere Hälfte der Übersichtsseite mit den entsprechenden Security Incidents oder Antwortaufgaben als Karten oder Listenelemente gefüllt. Der Analyst kann nach Bedarf zwischen der Kartenansicht oder der Listenansicht wechseln.

Zum Beispiel auf der **Priorität** Widget wenn Sie alle kritischen Incidents oder Antwortaufgaben auswählen möchten, klicken Sie auf **Kritisch** Segment (Beispiel-Screenshot unten) des Widgets und die kritischen Incidents oder Antwortaufgaben werden in der Listen- oder Kartenansicht angezeigt.

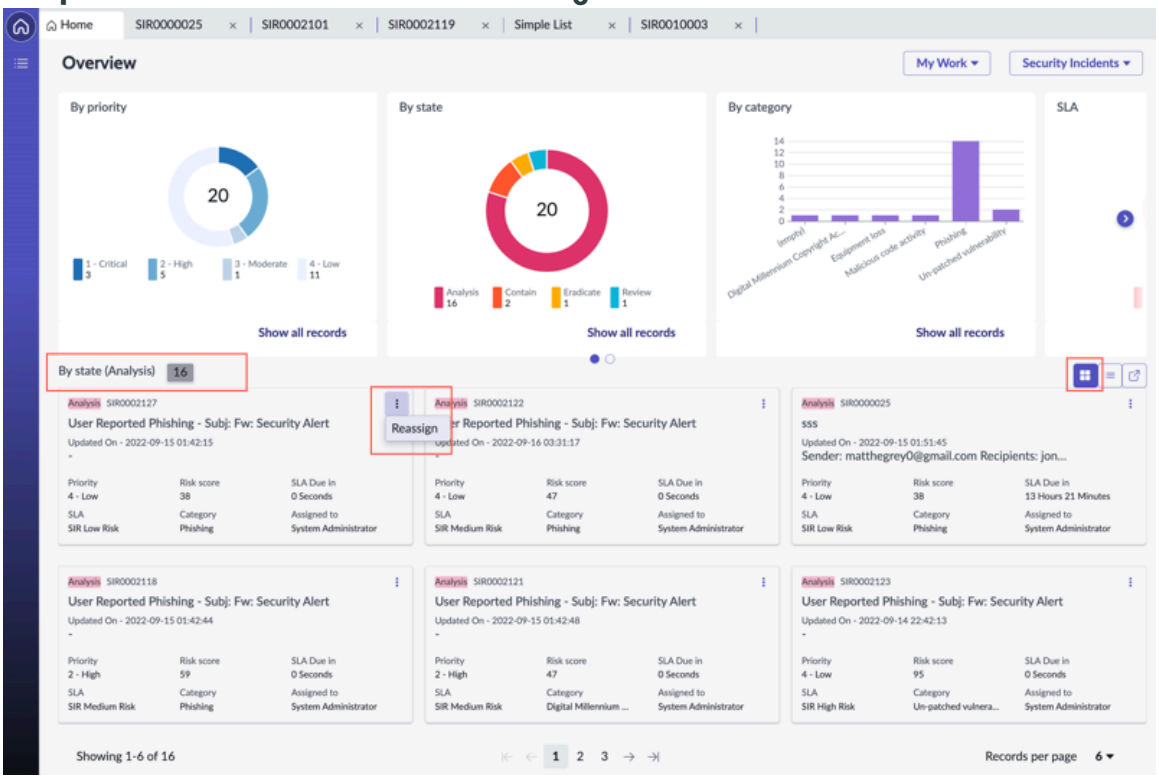
Übersichtsbereich



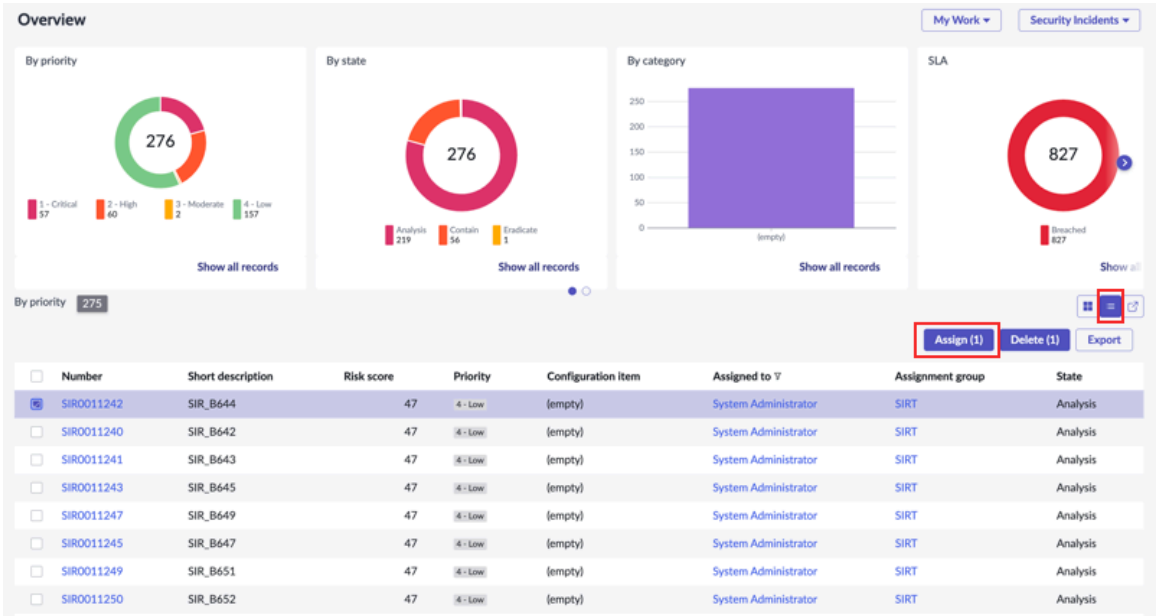
Sie können Security Incidents oder Antwortaufgaben direkt in dieser Ansicht zuweisen oder neu zuweisen, indem Sie auf das Ellipsensymbol klicken und auswählen **Zuweisen** (Option in Kartenansicht) oder direkt **Zuweisen** Schaltfläche (Option in Listenansicht), um einen Incident entsprechend zuzuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Kartenansicht und Neuzuweisung



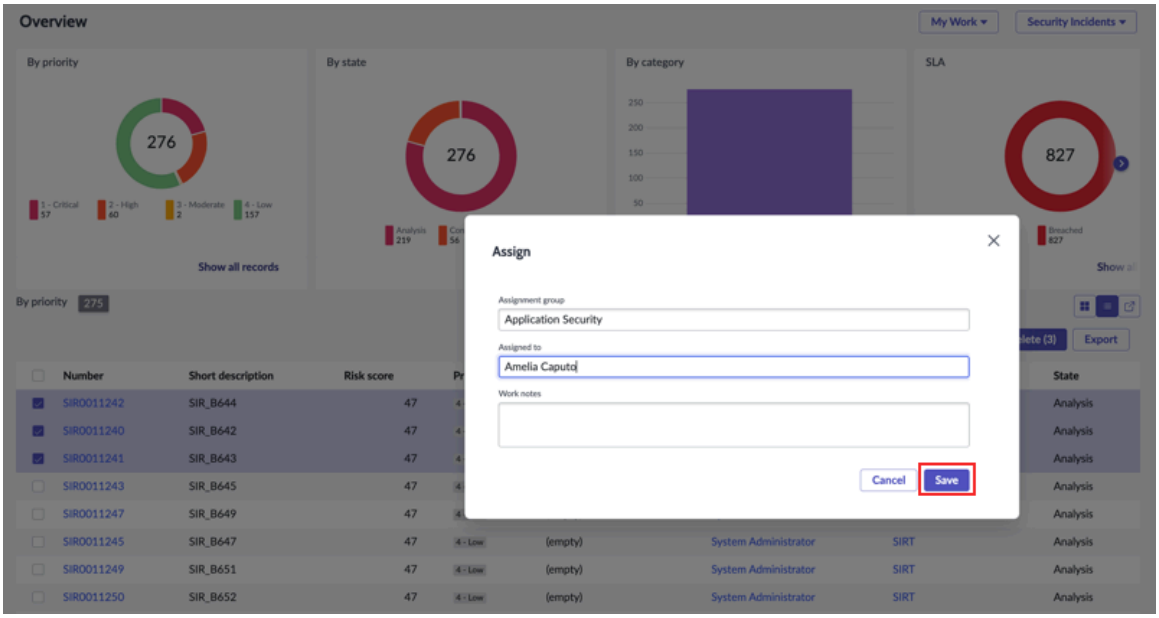
Incident zuweisen



Hier ist ein Beispiel für die Listenansicht. Der Anwender kann Incidents auch über die Listenansicht zuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incident zuweisen



Hinzufügen Oder ändern Sie die Details des Beauftragten, z. B. Zuweisungsgruppe und Zugewiesen an, und fügen Sie bei Bedarf Arbeitsnotizen hinzu.

Hinweis:

Sie können den Zuweisungsgruppen einen oder mehrere Security Incidents oder Antwortaufgaben zuweisen. Die ausgewählte Nummer wird auf angezeigt **Zuweisen** Schaltfläche.

Der Anwender kann Security Incidents aus dieser Ansicht löschen. Klicken Sie auf **Löschen** Schaltfläche zum Löschen des Security Incidents. Der Datensatz wird aus der Listenansicht gelöscht.

Der Anwender kann auch den Listeninhalt exportieren. Klicken Sie auf **Exportieren** Schaltfläche zum Exportieren der Liste im gewünschten Format.

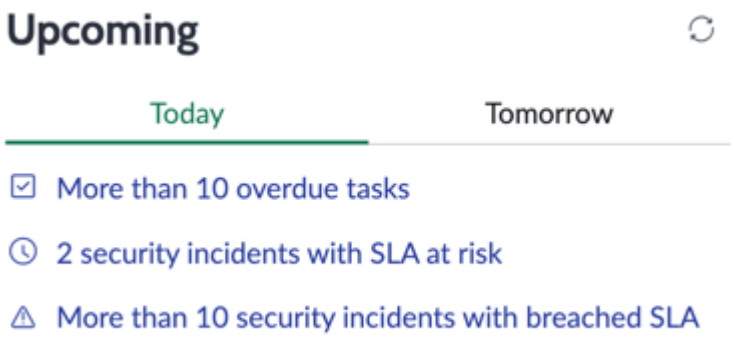
Abschnitt „Bevorstehend“

In diesem Abschnitt werden die bevorstehenden Aufgaben angezeigt, z. B. die Security Incidents und Antwortaufgaben, die am selben Tag und am nächsten Tag fällig sind.

Die angezeigte Liste „Security Incidents und Antwortaufgaben“ basiert auf dem Feld „Fälligkeitsdatum“ und der für diese Datensätze definierten SLA-Definition.

Wenn dieser Abschnitt mehr als einen Security Incident oder eine Antwortaufgabe enthält, werden alle diese Datensätze im Incident oder in den Datensätzen auf einer neuen Registerkarte geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zeigen Sie bevorstehende Aufgaben an

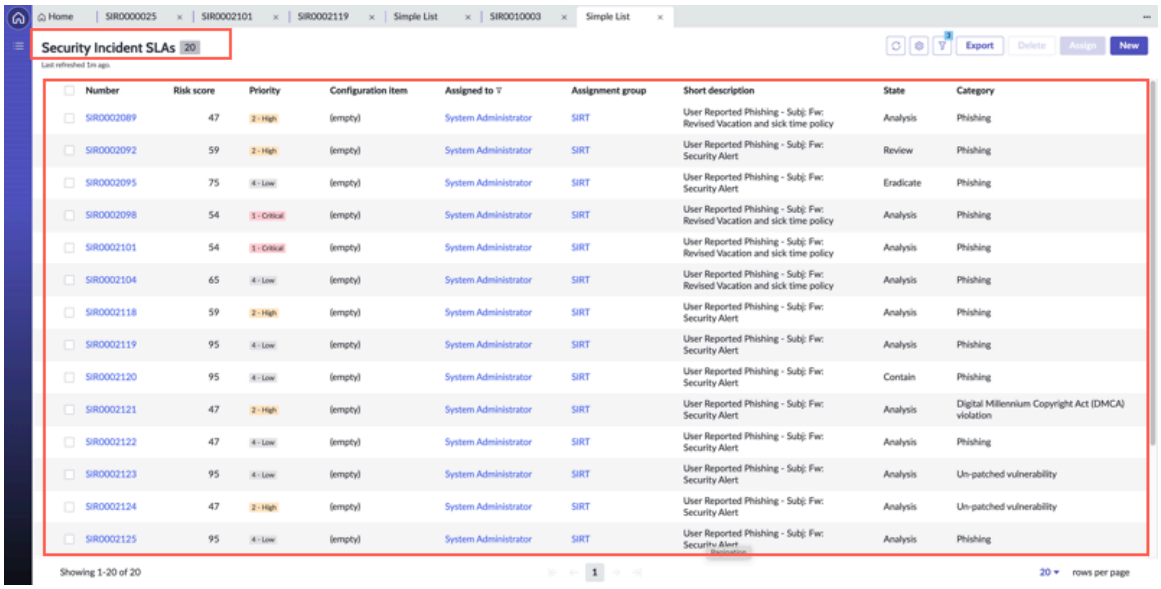
Der Sicherheitsanalyst kann die bevorstehenden Aufgaben im Zusammenhang mit Security Incidents und Antwortaufgaben anzeigen, die fällig, überfällig oder gegen das definierte SLA verstoßen haben.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Bevorstehend**an.
2. Klicken Sie Auf **Heute** Registerkarte zum Anzeigen der Aufgaben, die am selben Tag fällig sind.
3. Wählen Sie Aus **Morgen** Registerkarte zum Anzeigen der Aufgaben, die bis zum nächsten Tag überfällig sind.
   Im Abschnitt „bevorstehend“ werden die Security Incidents oder Antwortaufgaben aufgeführt, die basierend auf dem Fälligkeitsdatum überfällig sind und die gegen die SLA-Definition verstoßen haben.
4. Klicken Sie Auf **Aktualisieren** Symbol zum Aktualisieren der Liste der bevorstehenden Abschnitte.
   Wenn Sie beispielsweise auf den Link klicken, **Mehr als 10 Security Incidents mit SLA-Verstoß** Dann wird die Liste der Incidents mit SLA-Verstößen auf einer neuen Registerkarte im Arbeitsbereich angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Sie können in jeder Listenansicht Vorgänge „Neu“, „Zuweisen“, „Exportieren“ und „Löschen“ ausführen.

Abschnitt „Quick-Links“

Quick-Links funktionieren wie Lesezeichen-Links. Sie können externe URLs hinzufügen und schnell über den Arbeitsbereich darauf zugreifen.

Arbeiten mit Quick-Links

Fügen Sie Quick-Links zur einfachen Referenz hinzu.

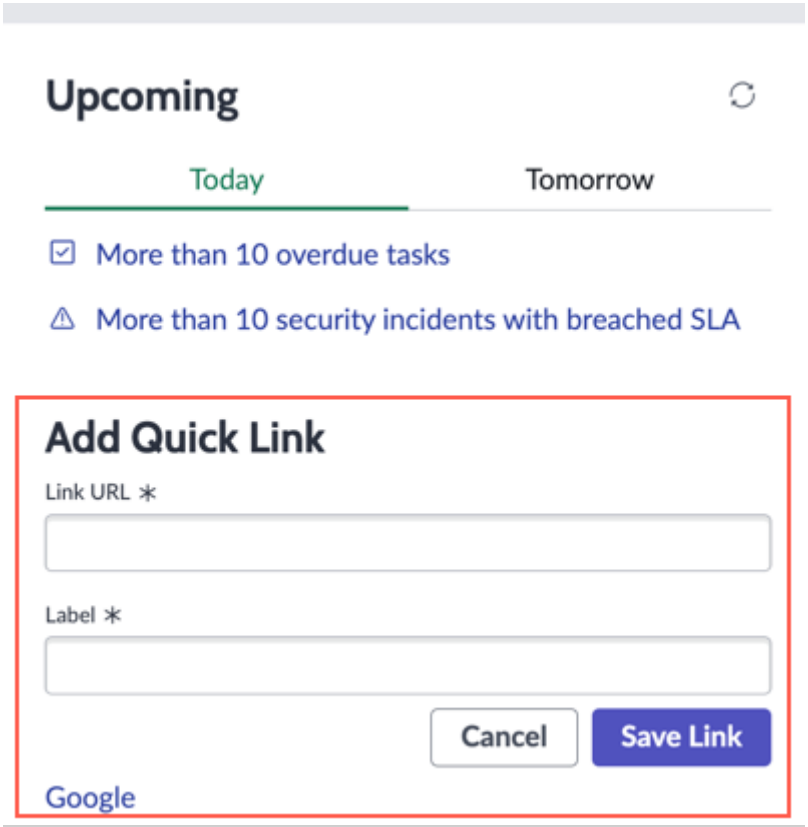
Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Sie können nützliche Quick-Links hinzufügen und ändern und diese Links, die bei der Lösung von Incidents helfen, mit Lesezeichen versehen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Quick-Links**an.
2. Klicken Sie Auf **Quick-Link Hinzufügen** Symbol zum Hinzufügen der Links.
3. Geben Sie den Link zur URL und Bezeichnung ein.
4. Klicken Sie Auf **Link Speichern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der neue Link wird unter dem Quick-Links-Abschnitt hinzugefügt.

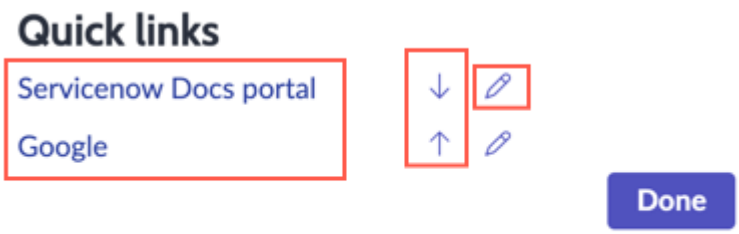
5. So ändern oder löschen Sie die Links:

a. Klicken Sie Auf **Link Bearbeiten** Symbol.

b. Ändern Sie den gewünschten Link oder Anzeigetext, der die Bezeichnung der URL ist.

c. Klicken Sie auf **Speichern**.

d. Klicken Sie auf **Erledigt**.



e. Verwenden Sie die nach-oben- und nach-unten-Pfeile, um die Position der Links zu verschieben.

f. Klicken Sie Auf **Löschen** Zum Löschen der Links während der Bearbeitung, die mit einem Lesezeichen versehen wurden.

Automatische Übersetzung

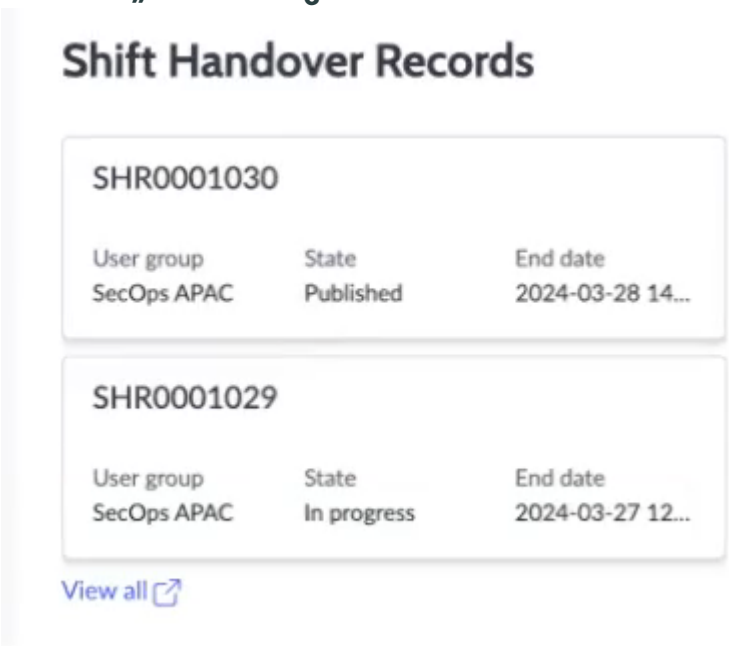
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt „Schichtübergabedatensätze“

Im Abschnitt wird die Liste der Schichtübergabedatensätze im Security Incident Response-Arbeitsbereich angezeigt.

Im Abschnitt „Schichtübergabedatensätze“ im Security Incident Response-Arbeitsbereich werden die letzten beiden Schichtübergabedatensätze basierend auf dem Enddatum, dem Status und den Anwendergruppenfeldern angezeigt, die für diese Datensätze definiert sind. Um alle Schichtübergabedatensätze anzuzeigen, wählen Sie aus **Alle anzeigen** .

Abschnitt „Schichtübergabedatensätze“



Listenansicht in SIR-Arbeitsbereich

Die Listenansicht besteht aus Security Incidents, Antwortaufgaben, Phishing-E-Mails und Bewertungen.

Die Listenansicht verfügt über vorab angewendete Filter wie „mir zugewiesen“, „dem Team zugewiesen“, „nicht zugewiesen“, „alle offen“, „alle“, „alle“, „alle“, und so weiter.

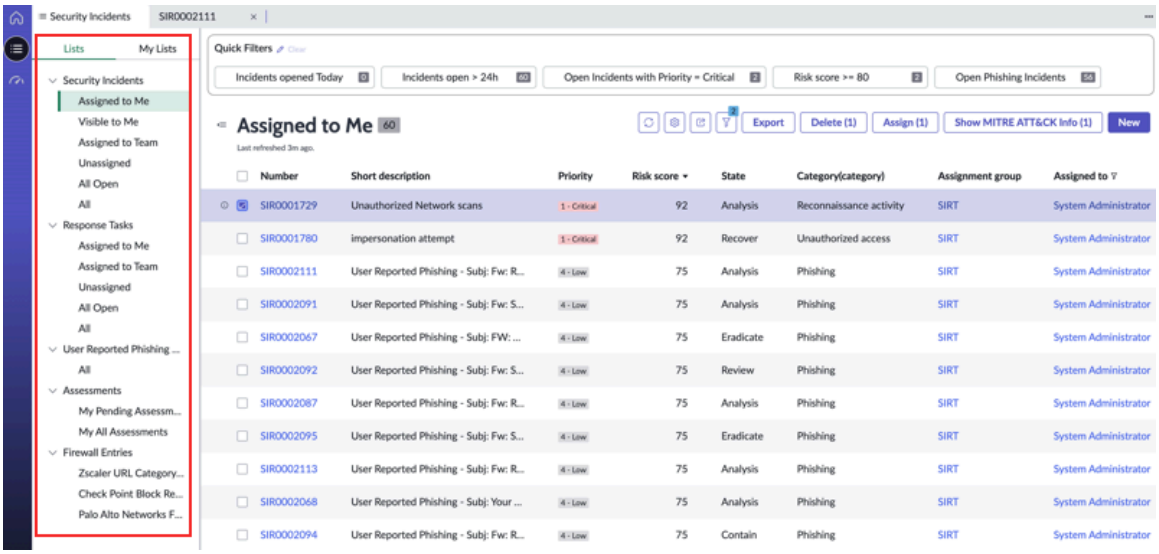
Mithilfe dieser Listenkategorien und gefilterten Listen können Analysten schnell die erforderlichen Security Incidents und Antwortaufgaben-Datensätze finden, an denen sie arbeiten müssen.

Um zur Listenansicht zu gelangen, müssen Sie auf das Listensymbol ( ). Wenn Sie in einer Listenansicht auf einen Datensatz klicken, wird der Datensatz in einer neuen Registerkarte geöffnet.

Listentypen

Im Folgenden finden Sie eine Beispielansicht der Listen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Listenbereich enthält die folgenden Abschnitte:

Listen

Listenelement	Beschreibung	Fähigkeit
Security Incidents	Zeigen Sie die Liste der Security Incidents an, und navigieren Sie zum gewünschten Incident, um mit der Bearbeitung zu beginnen. Die folgenden Listen sind verfügbar: • **Für mich sichtbar** : Security Incidents, die für den angemeldeten Anwender sichtbar sind. • **Mir zugewiesen** : Security Incidents, die dem Analysten zugewiesen sind. • **Dem Team zugewiesen** : Security Incidents, die allen Teams zugewiesen sind, denen die Analysten angehören. • **Nicht Zugewiesen** : Liste der nicht zugewiesenen Security Incidents. • **Alle Offen** : Liste aller offenen Security Incidents. • **Alle** : Liste aller Security Incidents.	• In der Listenansicht kann der Analyst die Liste der Spalten konfigurieren, indem er auf das Zahnradsymbol klickt, das über den Incident-Spalten verfügbar ist. • Der Analyst kann einen oder mehrere Security Incidents auswählen und diese Incidents anderen Anwendern zuweisen. • Der Analyst kann die Security Incidents löschen. • Der Analyst kann einen neuen Security Incident erstellen. • Der Analyst kann die Schnellfilter anwenden. Wenden Sie die Filter an, indem Sie auf klicken **Schnellfilter** Option anstelle der Verwendung von Erweitert **Filter** Option. Mit den Schnellfiltern können Sie schnell die Liste der Security Incidents filtern, die sofortige Aufmerksamkeit erfordern. Weitere Informationen finden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Fähigkeit
		Sie unter Arbeiten mit Schnellfiltern. • Die Analysten können die Liste der Incidents aktualisieren. • Der Analyst kann die Listenansicht in Excel-, CSV-, JSON- und PDF-Formate exportieren.
Schichtübergabedatensätze	Zeigen Sie die Liste der Schichtübergabedatensätze an. Die folgenden Listen sind verfügbar: • **Dem Team zugewiesen** : Schichtübergabedatensätze, die allen Teams/ Anwendergruppen zugewiesen sind, denen die Analysten angehören. • **Alle** : Liste aller Security Incidents.	Die Schichtübergabe unterstützt die folgenden drei Rollen: • Administrator: Schichtbesitzer-Rolle • Sicherheitsanalyst: Schichtanalyst-Rolle • Sicherheitsmanager: Schichtbesitzer-Rolle, hat jedoch keinen Zugriff auf die Anwendergruppe, der der Schichtübergabedatensatz zugewiesen ist. • Die Anwender mit der Rolle „Schichtbesitzer/ Analyst“, die Teil der Anwendergruppe in der aktiven Schicht sind, können Inhalte in den Schichtübergabedatensätzen im Entwurfsstatus hinzufügen oder ändern. • Anwender, die nicht über die Rolle „Schichtbesitzer/ Analyst“ verfügen oder nicht Teil der Anwendergruppe in der aktiven Schicht sind, können den Inhalt nur in den Schichtübergabedatensätzen anzeigen.
Antwortaufgaben	Zeigen Sie die Liste der Antwortaufgaben an, und navigieren Sie zur gewünschten Antwortaufgabe, um mit der	• In der Listenansicht kann der Analyst die Liste der Spalten konfigurieren, indem er auf das Zahnradsymbol klickt,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Fähigkeit
	Bearbeitung zu beginnen. Die Listenansicht enthält: • **Mir zugewiesen** : Antwortaufgaben, die dem Analysten zugewiesen sind. • **Dem Team zugewiesen** : Antwortaufgaben, die den Teams zugewiesen sind, denen die Analysten angehören. • **Nicht Zugewiesen** : Liste der nicht zugewiesenen Antwortaufgaben. • **Alle Offen** : Liste aller offenen Antwortaufgaben. • **Alle** : Liste aller Antwortaufgaben.	das über den Incident-Spalten verfügbar ist. • Der Analyst kann eine oder mehrere Antwortaufgaben auswählen und diese Aufgaben anderen Anwendern zuweisen. • Der Analyst kann eine neue Antwortaufgabe erstellen. • Der Analyst kann die Schnellfilter anwenden. Wenden Sie die Filter an, indem Sie auf klicken **Schnellfilter** Option anstelle der Verwendung von Erweitert **Filter** Option. Mit den Schnellfiltern können Sie schnell die Liste der Antwortaufgaben filtern, die sofortige Aufmerksamkeit erfordern. • Die Analysten können die Liste der Antwortaufgaben aktualisieren. • Der Analyst kann die Listenansicht in Excel-, CSV-, JSON- und PDF-Formate exportieren. Weitere Informationen finden Sie unter Exportieren Sie Security Incidents oder Antwortaufgaben.
Phishing-E-Mails	Zeigen Sie die Liste aller Phishing-E-Mails an. Die Listenansicht wird basierend auf der letzten Aktualisierung sortiert.	• Phishing-E-Mail Melden. Weitere Informationen finden Sie unter Phishing-E-Mail melden Wie eine Phishing-E-Mail gemeldet wird. • Löschen Sie Phishing-E-Mails. • Exportieren Sie die Listenansicht „Phishing-E-Mails“ im Excel-, CSV-, JSON- und PDF-Format.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listen (Fortsetzung)

Listenelement	Beschreibung	Fähigkeit
Bewertungen	Zeigen Sie die Liste der Bewertungen an, die für die Überprüfung nach Incident erforderlich sind. • **Meine ausstehenden Bewertungen** : Liste der ausstehenden Bewertungen. • **Meine Alle Bewertungen** : Liste aller Bewertungen.	Nehmen Sie Bewertungen vor.

Personalisieren Sie eine Liste

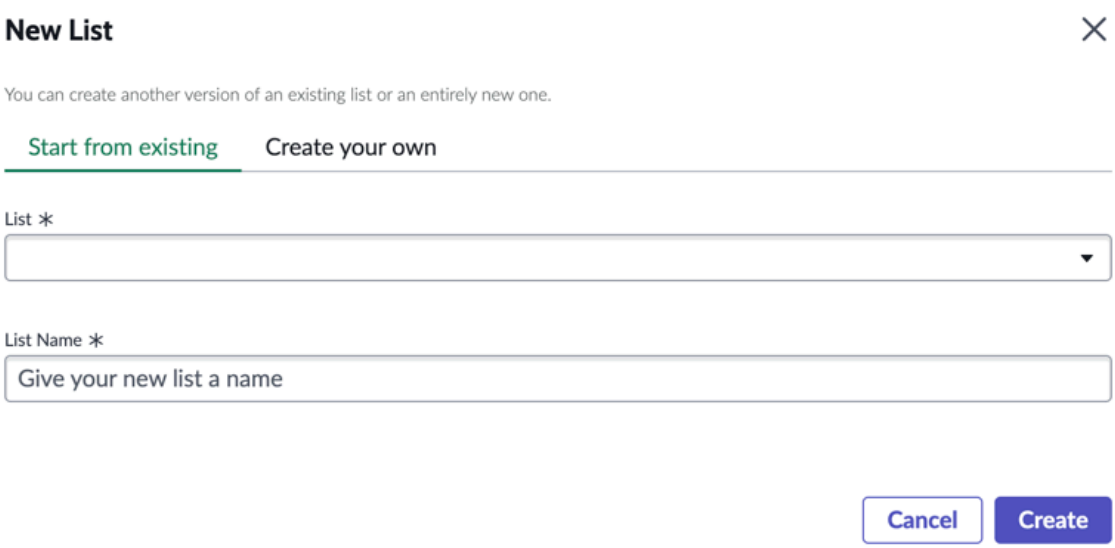
Sicherheitsanalysten oder Manager können die anwenderdefinierte Listenansicht für Security Incidents oder Antwortaufgaben oder Phishing-E-Mails basierend auf ihren individuellen Einstellungen personalisieren.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Klicken Sie Auf **Listenansicht** .
3. Klicken **Meine Listen**an.
4. Klicken Sie Auf **Fügen Sie eine neue Liste hinzu** , Verfügbar am unteren Rand von **Meine Listen** Anzeigen.



Sicherheitsanalysten können entweder eine andere Version einer vorhandenen Liste oder eine vollständig neue anwenderdefinierte Liste erstellen.

5. **So erstellen Sie aus einer vorhandenen Listenansicht:**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf **Von vorhandenem starten** Link.

b. Wählen Sie aus **Liste** Aus der Dropdown-Liste.

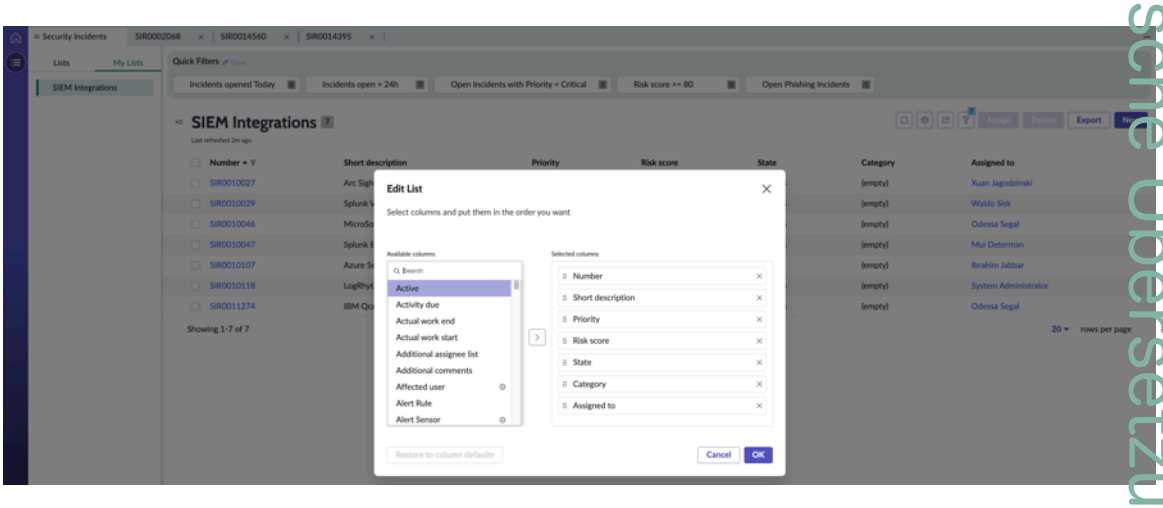
> **Hinweis:**
> Unabhängig davon, welche Liste Sie aus der Dropdown-Liste auswählen, der Listenname ist die Kopie Ihrer Hauptliste. Beispiel: Wenn Sie auswählen **Mir zugewiesen** Im Abschnitt „Security Incidents“ lautet der Listenname **Mir zugewiesen – Kopie** Des Abschnitts „Security Incidents“.

c. Wählen Sie die zu personalisierenden Spalten aus, und fügen Sie Filter hinzu.
Erstellen Sie einen Filter, indem Sie Bedingungen hinzufügen, die ein Feld, einen Operator und (einen) Wert/e enthalten.

d. Klicken Sie auf **Erstellen**.

> **Hinweis:**
> Um Ihre eigene Listenansicht anzupassen, können Sie anwenderdefinierte Spalten hinzufügen, Filter hinzufügen, Bedingungen festlegen und nach Bedarf nach der Reihenfolge sortieren.

e. Nachdem eine personalisierte Listenansicht erstellt wurde, klicken Sie auf das Zahnradsymbol, und passen Sie die Listenspalten an, indem Sie auswählen **Bearbeiten Sie Spalten** Option, um die Spalten zu bearbeiten und in der gewünschten Reihenfolge zu ordnen.



Sie haben auch die folgenden Möglichkeiten:

- **Umbenennen** Die personalisierte Listenansicht.
- **Löschen** Die personalisierte Listenansicht.
- Speichern Sie die personalisierte Listenansicht nach Bedarf mit **Speichern unter** Option.
- **Breite zurücksetzen** Der Listenansicht.

> **Hinweis:**
> Sie können diese Vorgänge auch direkt über die anderen bereitgestellten Schaltflächen „Listenaktionen“ ausführen, z. B. Zuweisen, Löschen und Exportieren der Listenansicht.

6. So erstellen Sie eine eigene Liste:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

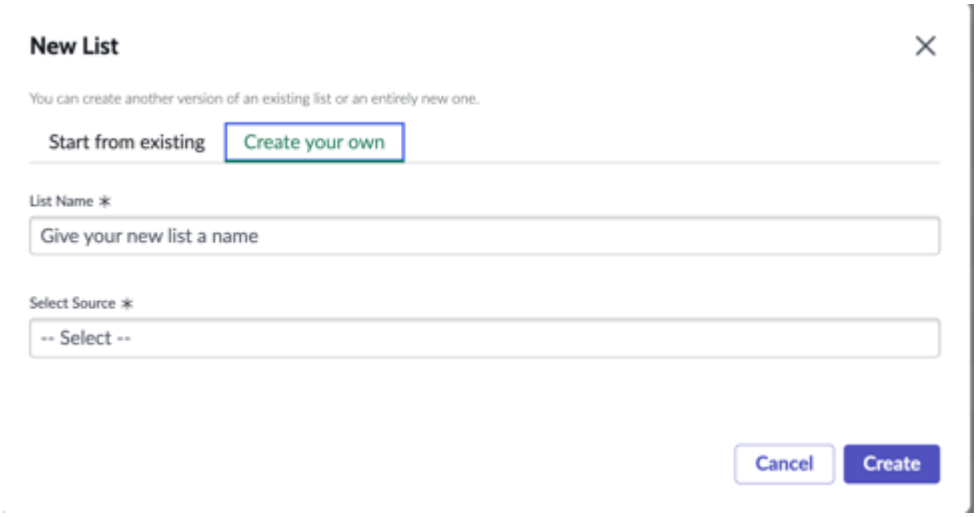
a. Klicken Sie auf **Erstellen Sie Ihre eigenen** Link.

b. Geben Sie ein an **Listenname** .

c. Wählen Sie aus **Quelle** Und **Spalten** .

d. Fügen Sie Filter hinzu.
Erstellen Sie einen Filter, indem Sie Bedingungen hinzufügen, und geben Sie die Reihenfolge an, in der die Liste angezeigt werden soll.

e. Klicken Sie auf **Erstellen**.



Eine neue Liste wird wie von Ihnen definiert und angepasst unter erstellt **Meine Listen** Abschnitt.

Hinweis:
Sie können **Neu Anordnen** Ihre personalisierte Ansicht, indem ihre Positionen verschoben werden.

Weisen Sie Security Incidents Zu

Weisen Sie Security Incidents zu.

Vorbereitungen
Erforderliche Rolle: sn_si.Basic

Prozedur

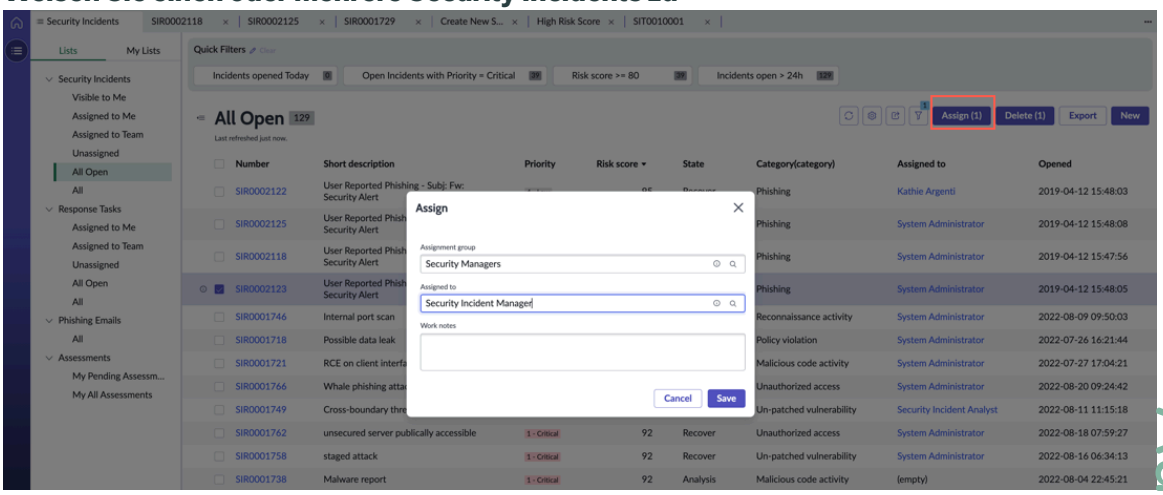
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Klicken Sie auf die Liste ( )-Symbol.
3. Klicken Sie auf **Listen**.
4. Wechseln Sie zum Beispiel zu **Security Incidents** > **Alle offen**an.
5. Wählen Sie mindestens einen Security Incident aus.
6. Klicken Sie auf **Zuweisen**.
7. Füllen Sie die Details wie Zuweisungsgruppe, Zugewiesen an aus, und fügen Sie bei Bedarf Arbeitsnotizen hinzu.
   Der Incident wird dann dem Anwender zugewiesen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf **Speichern**.

Weisen Sie einen oder mehrere Security Incidents zu



Mehrere Security Incidents schließen

Schließen Sie mehrere Security Incidents Gleichzeitig soll vermieden werden, dass zugehörige Incidents einzeln geschlossen werden müssen , Z. B. Incidents, die mit einer häufigen Ursache oder falsch positiv erstellt wurden Incidents.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Wählen Sie aus L Ist-Symbol ( ).
3. Wählen Sie Aus **Listen** .
4. Auswahlvorgang **Security Incidents** > **Alle offen**an.
5. Wählen Sie einen oder mehrere Security Incidents zum Schließen aus, und wählen Sie sie aus **Schließen** . Die Massenschließung der Security Incidents Fenster Wird angezeigt Links zu Zugriffslisten der Security Incidents, die geschlossen werden sollen.
   - Wenn mindestens ein ausgewählter Security Incident ausstehende Aktivitäten wie aktive Aufgaben, Playbooks, untergeordnete SIS, Bewertungen oder aktive Flows aufweist, die **Security Incidents mit aktiven Aufgaben, Playbooks, untergeordneten SIS, Bewertungen und aktiven Flows** Wird angezeigt.
   - Wenn für mindestens einen Security Incident, der zum Schließen ausgewählt wurde, keine ausstehenden Abschlussaktivitäten vorhanden sind, wird **Security Incidents sind bereit zum Schließen** Ist d IPlay ed .
6. **Wahlweise:** Überprüfen Sie die Security Incidents mit ausstehenden Aktivitäten .

Hinweis:
Wenn Sie ausstehende Aktivitäten nicht manuell schließen, werden sie automatisch geschlossen, wenn Sie mit dem Massenabschluss fortfahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Schließen Sie alle aktiven Aufgaben, Playbooks, untergeordneten SIS, Bewertungen und aktiven Flows.

b. Wählen Sie Aus **Bringen Sie mich zurück** Um zu zurückzukehren Schließen Sie das Security Incidents-Fenster in einem Massenvorgang .

7. Wählen Sie **Weiter**.
8. Wählen Sie die zutreffende aus **Abschlusscode** .
9. Geben Sie Ein **Notizen Schließen** .
10. Wählen Sie Aus **Massenschließung** .
    Die Abschlussaktivität für Incidents wird in ausgeführt Die Hintergrund.

Weisen Sie Antwortaufgaben Zu

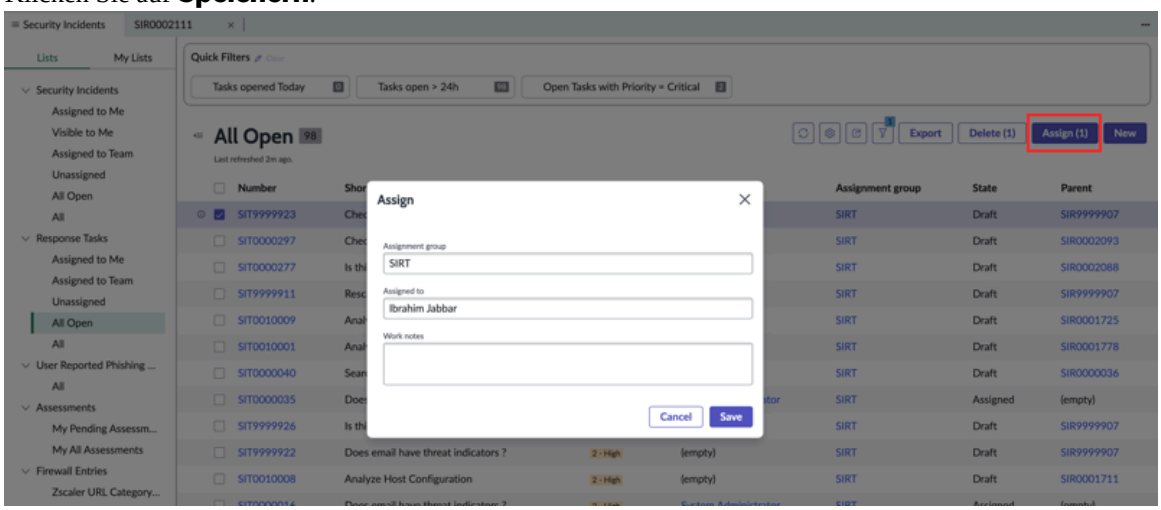
Weisen Sie Antwortaufgaben für ein Sicherheitsproblem zu.

Vorbereitungen

Erforderliche Rolle: sn_si.Basic

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Klicken Sie auf die Liste ( )-Symbol.
3. Klicken Sie auf **Listen**.
   Wechseln Sie zum Beispiel zu **Antwortaufgaben** > **Alle offen**an.
4. Wählen Sie eine oder mehrere Antwortaufgaben aus.
5. Klicken Sie auf **Zuweisen**.
6. Füllen Sie die Details wie Zuweisungsgruppe, Zugewiesen an aus, und fügen Sie bei Bedarf Arbeitsnotizen hinzu.
   Der Incident wird dann dem Anwender zugewiesen.
7. Klicken Sie auf **Speichern**.



Phishing-E-Mail melden

Melden Sie Phishing-E-Mails aus der Listenansicht.

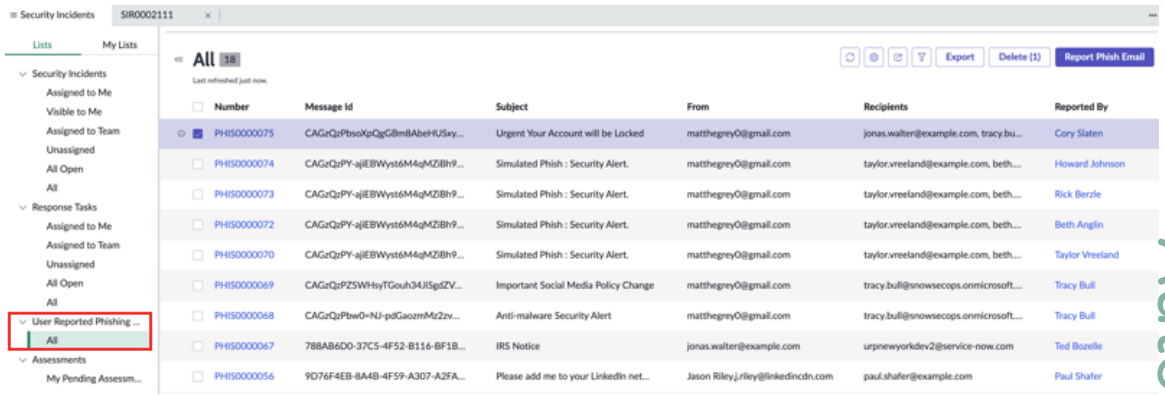
Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Klicken Sie auf die Liste ( )-Symbol.
3. Gehe zu **Vom Anwender gemeldete Phishing-E-Mails** > **Alle**an.
   Die Liste der vom Anwender gemeldeten Phishing-E-Mails wird angezeigt.



4. Klicken Sie Auf **Phishing-E-Mail Melden** Schaltfläche.
   Melden Sie eine Phishing-E-Mail, indem Sie sie hochladen.
5. Klicken Sie Auf **Datei Hinzufügen** Zum Hinzufügen von Anhängen.
6. Klicken Sie auf **Hochladen**.

Hinweis:
Melden Sie eine Phishing-E-Mail, indem Sie die Anhänge hochladen. Sie können nur eine Phishing-E-Mail gleichzeitig hochladen und müssen das EML-Format haben.

7. Klicken Sie auf **Absenden**.
   Die Phishing-E-Mail zum Protokollieren eines Security Incidents wird erstellt.

Arbeiten mit Schnellfiltern

Schnellfilter sind leicht zugängliche Filter, die in Security Incidents und Antwortaufgaben-Listen verfügbar sind.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Die SIR-Arbeitsbereich Bietet eine Schnellfilterfunktion, mit der Sie die Liste von Security Incidents oder Antwortaufgaben problemlos filtern können.

Sie können Schnellfilter verwenden, um neue Filter zu konfigurieren oder vorhandene Filter zu ändern, die für diese Listen angezeigt werden. Das Basissystem bietet die folgenden Schnellfilter für jeden Security Incident:

- **Heute geöffnete Incidents**
- **Incidents offen > 24 Stunden**
- **Offene Incidents mit Priorität = Kritisch**
- **Risiko >= 80**
- **Offene Phishing-Incidents**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

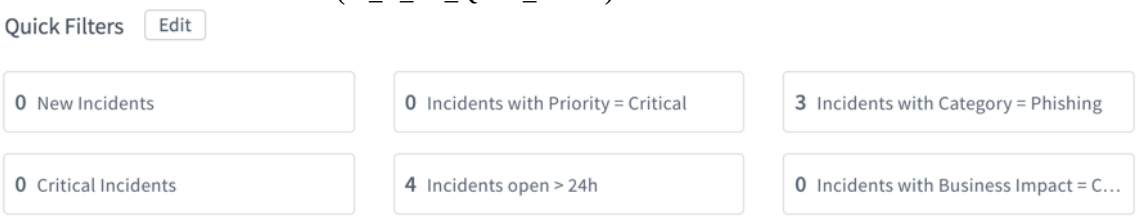
Das Basissystem bietet die folgenden Schnellfilter für jede Antwortaufgabe:

- **Aufgaben offen > 24 Stunden**
- **Offene Aufgaben mit Priorität = Kritisch**

Hinweis:
Ein Administrator kann die erforderliche Liste von Schnellfiltern entsprechend den Anforderungen der Organisation konfigurieren.

Prozedur

1. Navigieren zu **Systemdefinition** > **Tabellen**an.
2. Suchen Sie nach **Schnellfilter** (sn_si_aw_Quick_Filters).



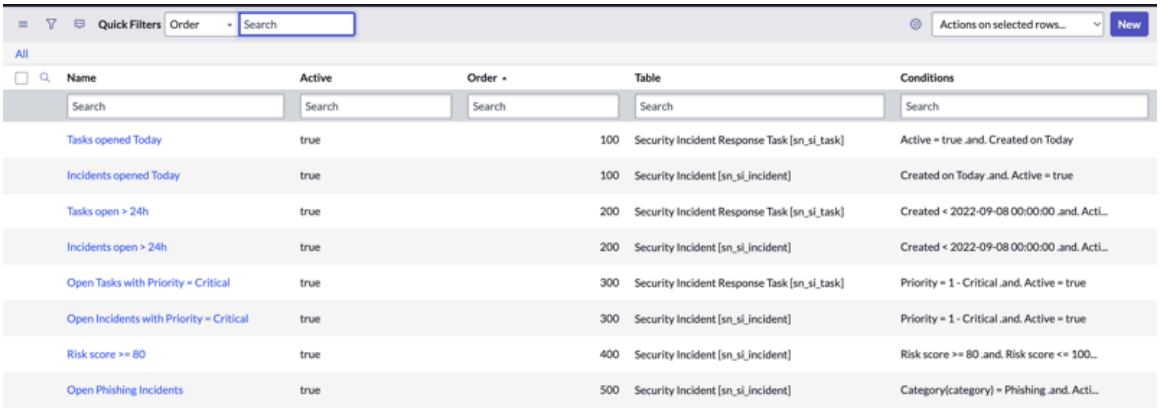
3. Gehe zu **Zugehörige Links** > **Liste anzeigen** Abschnitt.
   Die **Schnellfilter** Listenseite wird angezeigt. OOTB: Nachfolgend finden Sie die Liste der Schnellfilter, die mit der Anwendung geliefert werden.

Name	Tabelle	Wert
Heute geöffnete Aufgaben	Security Incident-Aufgabe [sn_si_Task]	True
Heute geöffnete Incidents	Security Incident [sn_si_incident]	True
Aufgaben offen > 24 Stunden	Security Incident Response-Aufgabe [sn_si_task]	True
Incidents offen > 24 Stunden	Security Incident [sn_si_incident]	True
Offene Aufgaben mit Priorität = Kritisch	Security Incident Response-Aufgabe [sn_si_Incident]	True
Offene Incidents mit Priorität = Kritisch	Security Incident [sn_si_incident]	True
Risikopunktzahl >= 80	Security Incident [sn_si_incident]	True
Offene Phishing-Incidents	Security Incident [sn_si_incident]	True

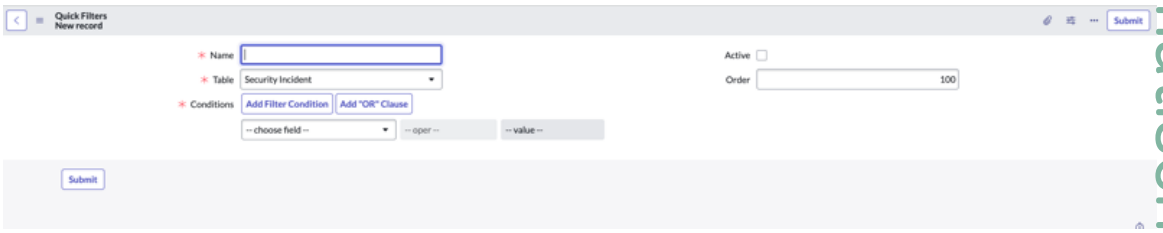
Hinweis:
Der Sicherheitsadministrator kann diese Schnellfilter konfigurieren. Je nach Geschäftsanforderung kann der Administrator den vorhandenen Wert in „falsch“ ändern und einen neuen Schnellfilter erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schnellfilter



4. Klicken Sie auf **Neu**, um einen neuen Filter zu erstellen.
5. Geben Sie einen Namen für den Filter ein, wählen Sie die Tabelle aus, und geben Sie die Filterbedingung an.
6. Klicken Sie Auf **Übermitteln** Um zur vorherigen Listenseite zurückzukehren.
   Der neu hinzugefügte Filter wird auf der Seite aufgeführt.

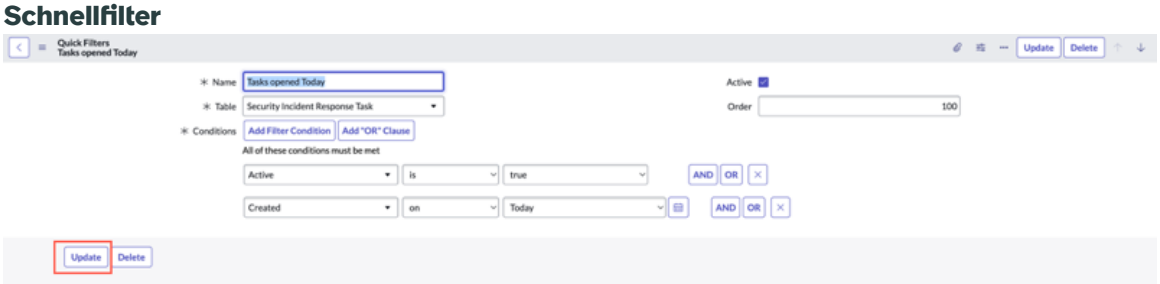


Hinweis:

- Der Schnellfilter gilt nur, wenn **Aktiv** Das Kontrollkästchen ist aktiviert.
- Innerhalb des Arbeitsbereichs kann jeder angemeldete Anwender die aktiven Schnellfilter personalisieren, die in der Anwendung verfügbar sind. Anwender können die neu erstellten Schnellfilter ein- oder ausblenden. Diese Funktion basiert auf ihrer Anwendereinstellung.
- Wenn ein Anwender die Einstellungen für Schnellfilter geändert hat und danach ein neuer Schnellfilter erstellt wird, gilt der Schnellfilter nicht für die Einstellung des Anwenders. Der Anwender muss die Einstellungen in der personalisierten Ansicht manuell ändern.

7. Wählen Sie einen vorhandenen Filterdatensatz aus, um die vorhandenen Schnellfilter zu ändern.
8. Ändern Sie den Namen und die Filterbedingung.
9. Klicken Sie auf **Aktualisieren**.

Schnellfilter



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie Schnellfilter hinzu, oder ändern Sie sie

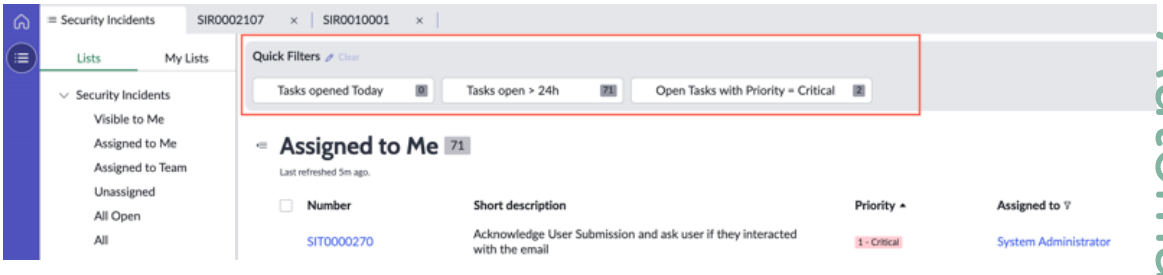
Fügen Sie in der Listenansicht Schnellfilter für Security Incidents oder Antwortaufgaben hinzu, oder ändern Sie sie.

Vorbereitungen

Erforderliche Rolle: sn_si.Basic

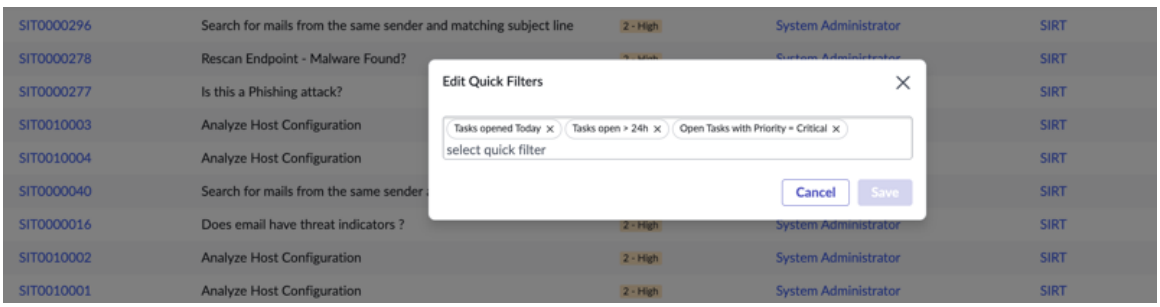
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Klicken Sie auf die Liste ( )-Symbol.
3. Wechseln Sie zum Beispiel zu **Listen** > **Security Incidents** > **Schnellfilter** Abschnitt.



4. Klicken Sie Auf **Bearbeiten** Symbol zum Vornehmen der Änderungen.

Hinweis:
Die von Ihnen vorgenommene Änderung wird beibehalten, und wenn der Anwender das nächste Mal zu dieser Seite zurückkehrt, wird die beibehaltene Einstellung angezeigt.



5. Klicken Sie auf **Speichern**.

Exportieren Sie Security Incidents oder Antwortaufgaben

Exportieren Sie die Security Incidents oder Antwortaufgaben aus der Listenansicht.

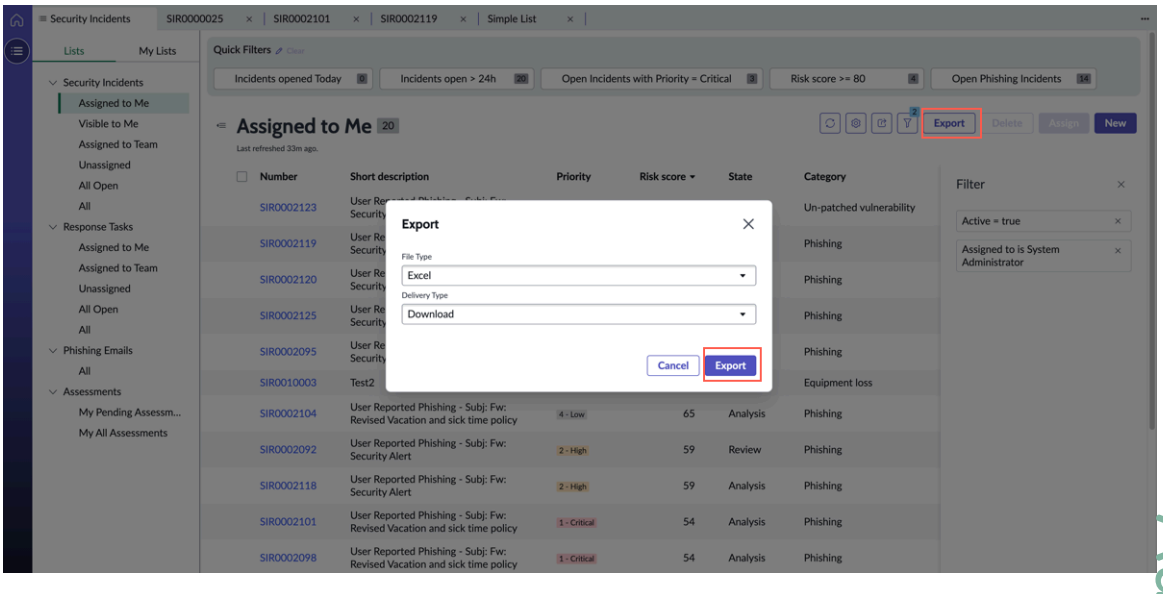
Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Klicken Sie auf die Liste Symbol.
3. Klicken Sie auf **Listen**.
4. Gehe zu **Security Incidents oder Antwortaufgaben** > **Alle offen**an.
5. Zeigen Sie die Liste an, und klicken Sie auf **Exportieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie aus **Dateityp** Und **Liefertyp** .
   Beispiel: **Excel** Und beide **Herunterladen** Oder **E-Mail** Die Liste.
7. Klicken Sie auf **Exportieren**.
   Die Datei wird gemäß der ausgewählten Option heruntergeladen oder per E-Mail gesendet.

Verwalten Sie Schichtübergabedatensätze

Verwenden Sie die Listenansicht Schichtübergabe-Datensätze, um Schichtübergabedatensätze zu erstellen, zu bearbeiten, zu kopieren oder zu löschen. Jeder Schichtübergabedatensatz ist einer Schichtübergabeberichtsvorlage zugeordnet.

Vorbereitungen

Erforderliche Rolle:

- sn_escm_sh.Shift_Analyst: Mindestanforderung für den Zugriff auf die Schichtübergabedatensätze.
- sn_escm_sh.Shift_owner: Erstellen, bearbeiten und löschen Sie Übergabeprotokolldatensätze in den Anwendergruppen, denen der Schichtbesitzer angehört. Diese Rolle erbt die Rolle sn_escm_sh.Shift_Analyst.
- sn_escm_sh.Shift_Analyst: Zeigen Sie alle Protokolldatensätze der Schichtübergabe an, können aber nur zu Datensätzen in Bearbeitung der Schichtübergabe beitragen, die der Gruppe des Schichtanalysten zugewiesen sind.
- sn_si.Analyst: Erbt die Rolle „sn_escm_sh.Shift_Analyst“.
- sn_si.admin: Erbt die Rolle sn_escm_sh.Shift_admin.
- sn_escm_sh.Shift_admin: Erbt die Rolle sn_escm_sh.Shift_owner

Wichtig:
Informationen zum Konfigurieren der Schichtübergabevorlage als Administrator finden Sie unter Konfigurieren Sie Schichtübergabevorlagen.

Warum und wann dieser Vorgang ausgeführt wird

Der Schichtbesitzer und das jeweilige Team oder die entsprechende Anwendergruppe erstellen die Protokolldatensätze der Schichtübergabe. Der Schichtbesitzer muss die Schichtübergabevorlage und die Anwendergruppe auswählen, die am

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schichtübergabebericht arbeiten. Nachdem der Schichtübergabebericht abgeschlossen ist, wird er für den nächsten aktiven Schichtbesitzer und das nächste Team freigegeben.

Schlüsselpunkte der Schichtübergabevorlage:

- Wenn ein anderer Analyst aus dem aktiven Schichtteam den Bericht bereits vor Ihnen aktualisiert hat und Änderungen verarbeitet werden, wird möglicherweise eine Fehlermeldung angezeigt, dass Inhaltsaktualisierungen ausstehen. Sie müssen 30 Sekunden warten und dann auswählen **Ändern Sie den Status in „Überprüfen“** Erneut. Sie können den konsolidierten Bericht im rechten Bereich anzeigen und mit aktualisierten Inhalten anderer Analysten aktualisieren.
- Wenn der Schichtbesitzer den Inhalt in einem Abschnitt im Status „Überprüfen“ geändert hat, wird derselbe Inhalt für den Analyst reflektiert, wenn der Datensatz in den Status „in Bearbeitung“ zurückversetzt wird.
- Der Schichtbesitzer muss aufmerksam sein, wenn er den Inhalt im Status „Überprüfen“ bearbeitet und Aktionen wie das Zusammenführen von zwei Zeilen, das Zusammenführen von zwei Abschnitten und das Entfernen eines Abschnitts durchführt, da dies sich auf den Schichtübergabebericht der anderen Analysten auswirkt.
- Nach der Veröffentlichung des Schichtübergabeberichts kann der Schichtbesitzer den Inhalt ändern, aber den Datensatzstatus kann er nicht ändern.
- Wenn jemand den Inhalt ändert und während dieser Zeit der Datensatzstatus von in Bearbeitung in Überprüfung geändert wird, werden die nicht gespeicherten Inhaltsänderungen verworfen.
- Der Schichtadministrator hat Schreibzugriff auf alle Schichtübergabeprotokolldatensätze unabhängig von Anwendergruppen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Wählen Sie die Security Incident-Liste aus Symbol.
3. Auf der **Listen** Wählen Sie die Registerkarte aus **Schichtübergabedatensätze** .
4. Wählen Sie Aus **Alle Datensätze** Zum Anzeigen der Liste aller Schichtübergabedatensätze.
5. Wählen Sie Aus **Dem Team zugewiesen** Dient zum Anzeigen der Liste der Schichtübergabedatensätze, die allen Teams/Anwendergruppen zugewiesen sind, denen die Analysten angehören.
6. Um einen neuen Schichtübergabedatensatz zu erstellen, wählen Sie aus **Neu** .
7. Füllen Sie die Felder im Formular aus.

Schichtübergabedatensätze

Feld	Beschreibung
Anzahl	Eindeutige Nummer, die automatisch für einen Schichtübergabedatensatz generiert wird.
Vorlage	Die zu verwendende Schichtübergabevorlage. Beispiel: Schichtvorlage.
Beschreibung	Beschreibung für den Schichtübergabedatensatz.
Anwendergruppe	Die Anwendergruppe/das Team, der der Schichtübergabedatensatz zugewiesen werden soll. Zum Beispiel Teamentwicklungscode-Überprüfer.

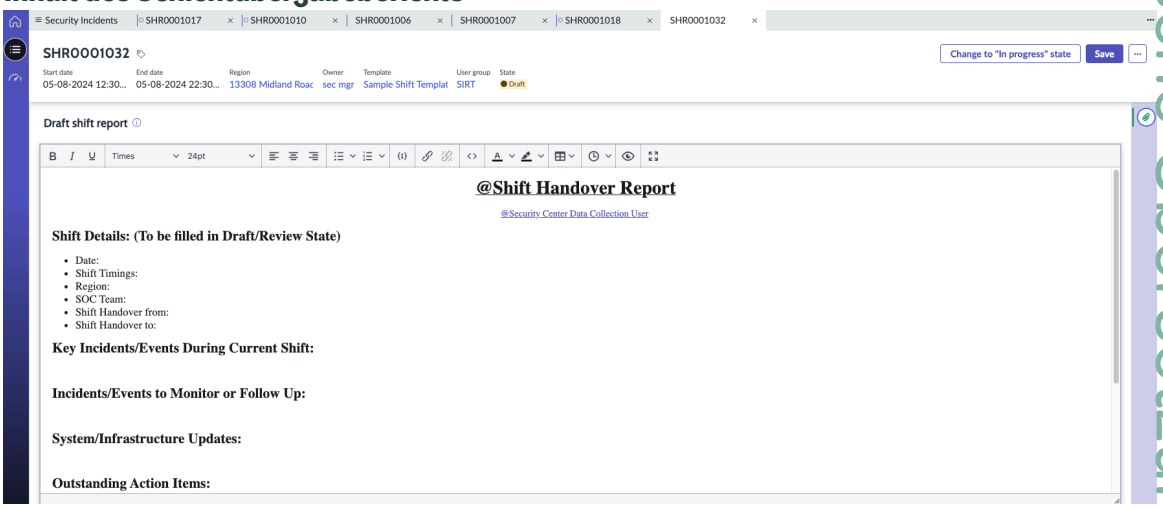
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Der aktuelle Status des Schichtübergabedatensatzes. Standardmäßig ist der Anfangsstatus Entwurf **Hinweis:** Der Status kann während der Erstellung eines Datensatzes nicht geändert werden.
Schichtname	Der Schichtname, der die Details zum Schichtstart und zum Schichtende enthält. Beispiel: US-Tagesschicht.

8. Wählen Sie **Erstellen** aus.
   Ein neuer Schichtübergabedatensatz wird basierend auf der Vorlage erstellt, die Sie ausgewählt und der Listenansicht hinzugefügt haben.
9. Öffnen Sie den neuen Schichtübergabedatensatz, um den Status und die Details der Security Incidents im Schichtübergabebericht zu aktualisieren.
   Standardmäßig befindet sich der Schichtübergabedatensatz im **Entwurf** status.

   Hinweis:
   Nur der Schichtbesitzer kann den Inhalt ändern.

   Inhalt des Schichtübergabeberichts

10. Verwenden Sie im Editor „Schichtentwurf“ die Abschnitte der Berichtsvorlage für die Schichtübergabe, um die Details der Security Incidents und Anwender zu aktualisieren.

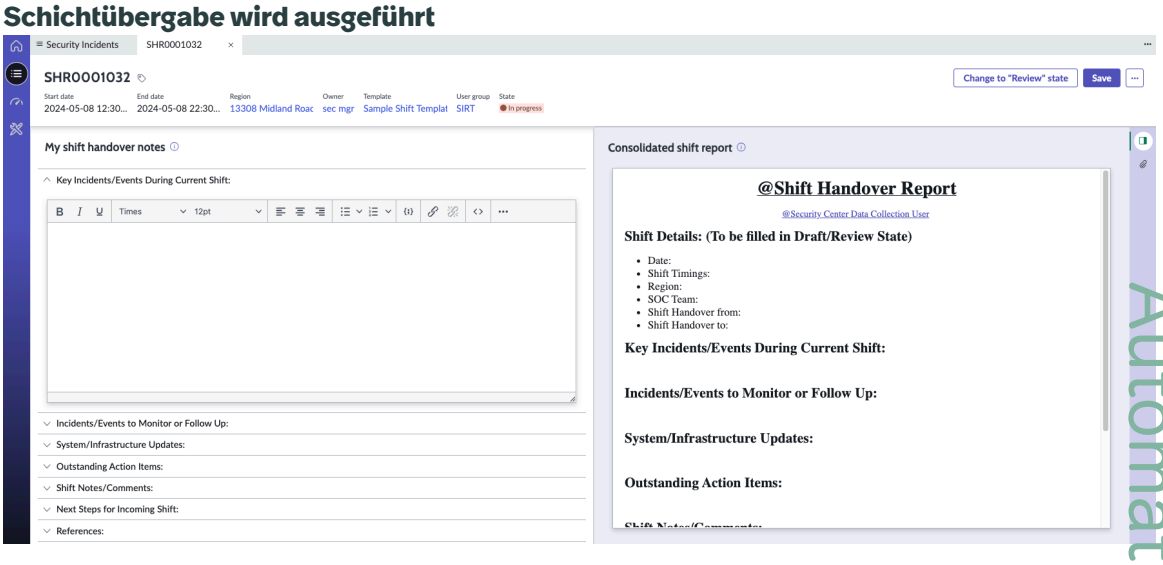
    Sie können Ihren Bericht mit allen Optionen im Editor formatieren, z. B. Schriftarten, Farben, Aufzählungszeichen, Links, und Anhänge.

    Hinweis:
    Der Schichtbesitzer und der Schichtanalyst können den Inhalt ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie aus, nachdem Sie die erforderlichen Änderungen am Schichtübergabebericht vorgenommen haben **Speichern** .

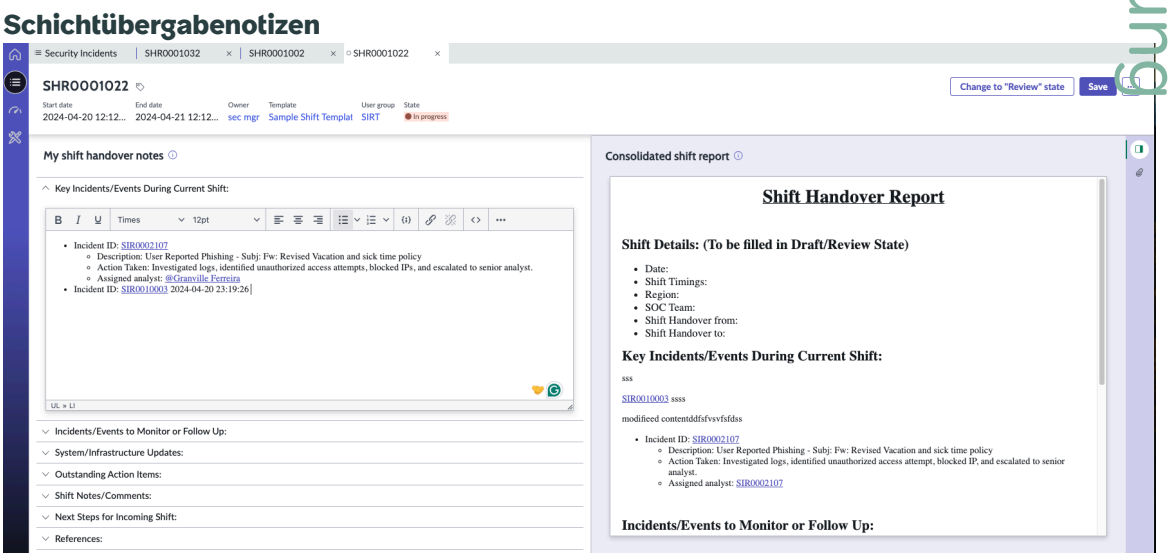
b. Wählen Sie Aus **Ändern Sie den Status in „in Bearbeitung“** Aktion zum Verschieben des Schichtübergabedatensatzes in den Status „in Bearbeitung“.



11. Aktualisieren Sie im Editor „meine Schichtübergabenotizen“ die erforderlichen Details für alle Abschnitte wie Security Incident und Anwenderdetails.

Hinweis:
Der Schichtbesitzer und der Schichtanalyst können den Inhalt ändern.

a. Um einen bestimmten Datensatz im Editor zu erwähnen, verwenden Sie **/** Und wählen Sie aus **Wählen Sie einen Datensatz aus** , Und wählen Sie dann einen Datensatz aus der Popup-Liste der Tabellen aus. Beispiel: Wenn Sie auswählen **Security Incidents** Datensatz, dann wird eine Liste der Security Incidents angezeigt. Wählen Sie einen Security Incident aus (**SIR0010025**) Aus der Liste und aktualisieren Sie die erforderlichen Schichtübergabedetails. Sie können auch die Felder erwähnen, die dem Security Incident zugeordnet sind, z. B. Kurzbeschreibung, Beobachtung ich st durch Verwenden **/** Nach der Security Incident-Nummer.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Um einen bestimmten Anwender im Editor zu erwähnen, verwenden Sie **/** Und wählen Sie aus **Wählen Sie einen Anwender aus** , Und wählen Sie dann einen Anwender aus der Popup-Liste aus.

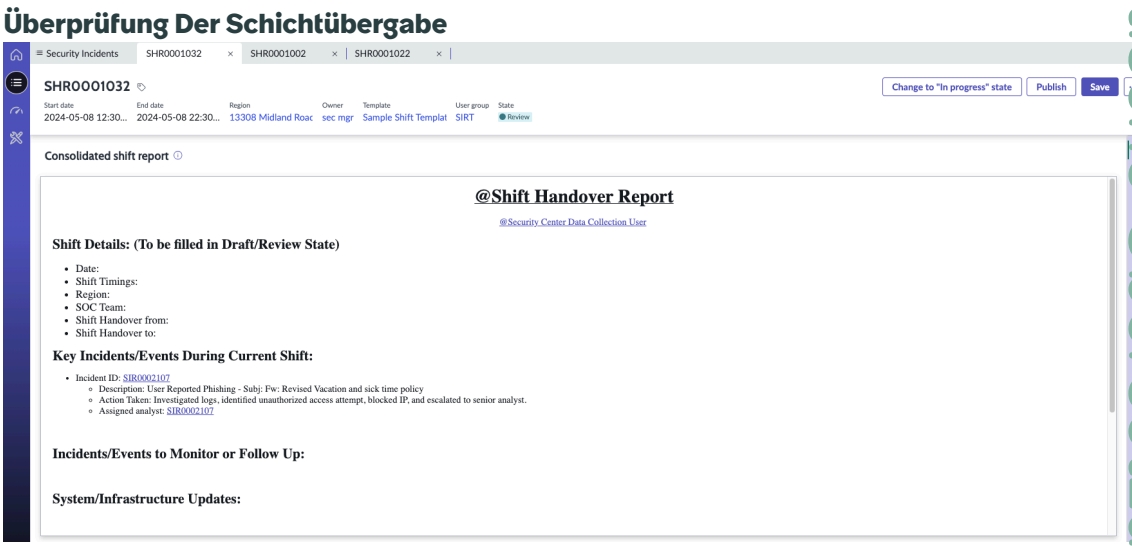
c. Um die Anzahl der Datensätze im Editor zu erwähnen, verwenden Sie **/** Und wählen Sie aus **Anzahl der Erwähnungen** , Und wählen Sie dann den Datensatz aus der Popup-Liste aus.

d. Sie können Ihren Bericht mit allen Optionen im Editor formatieren, z. B. Schriftarten, Farben, Aufzählungszeichen, Links, und Anhänge.

e. Wählen Sie aus, nachdem Sie die erforderlichen Änderungen an den Notizen zur Schichtübergabe vorgenommen haben **Speichern** .

f. Wählen Sie Aus **Ändern Sie den Status in „Überprüfen“** Aktion zum Verschieben des Schichtübergabedatensatzes in den Status „Überprüfen“.

Hinweis:
Wenn ein anderer Analyst aus dem aktiven Schichtteam den Bericht bereits vor Ihnen aktualisiert hat und Änderungen verarbeitet werden, wird möglicherweise eine Fehlermeldung angezeigt. Sie müssen einige Sekunden warten und dann auswählen **Ändern Sie den Status in „Überprüfen“** Erneut.



12. Überprüfen Sie im Bericht „konsolidierte Schicht“ den Bericht „Schichtübergabe“, und nehmen Sie die erforderlichen Änderungen vor.

Hinweis:
Nur der Schichtbesitzer kann den Inhalt ändern.

a. Wählen Sie aus, nachdem Sie die erforderlichen Änderungen an den Notizen zur Schichtübergabe vorgenommen haben **Speichern** .

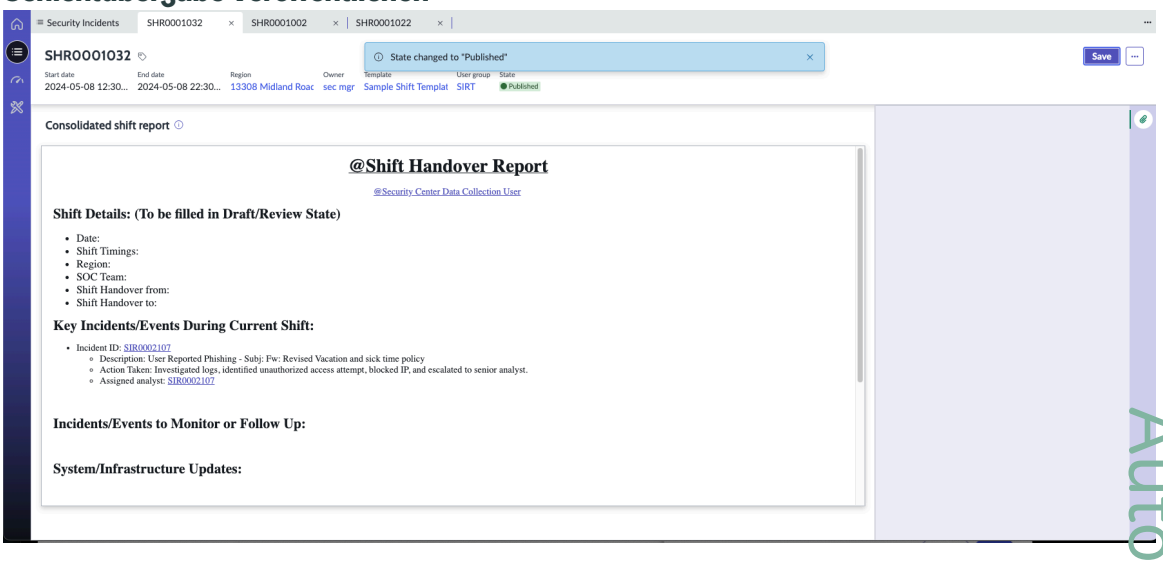
b. Wenn der Schichtübergabebericht weitere Updates von den Analysten erfordert, können Sie auswählen **Ändern Sie den Status in „in Bearbeitung“** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie Aus **Veröffentlichen** Aktion zum Veröffentlichen des Schichtübergabeberichts.

Schichtübergabe Veröffentlichen



13. Wählen Sie Aus **Speichern** Dient zum Speichern des Schichtübergabeberichts.
Nach dem Speichern wird im Vorschaubereich eine Vorschau des Schichtübergabeberichts mit Ihren neuesten Updates angezeigt.

> **Hinweis:**
> Sie können zwar sofort eine Vorschau der Aktualisierungen anzeigen, die Sie am Schichtübergabebericht vorgenommen haben, die anderen Analysten können jedoch einige Sekunden benötigen, um die Änderungen anzuzeigen.

14. Als Schichtbesitzer können Sie auch die folgenden Aktionen in der Listenansicht Schichtübergabe ausführen.

a. Um einen vorhandenen Schichtübergabedatensatz zu bearbeiten, wählen Sie den Datensatz und dann aus **Bearbeiten** Aktion.
Sie können nur die Startzeit, die Endzeit, die Beschreibung und die Region ändern.

b. Um eine Kopie eines Schichtübergabedatensatzes zu erstellen, wählen Sie den Datensatz aus, und wählen Sie aus **Kopie erstellen** Aktion.

c. Um einen vorhandenen Schichtübergabedatensatz zu löschen, wählen Sie den Datensatz und dann aus **Löschen** Aktion.

SIR-Arbeitsbereich konfigurieren

In diesem Abschnitt werden die Konfigurationen beschrieben, die für die Arbeit mit erforderlich sind Arbeitsbereich für Security Incident Response.

Richten Sie die Ansicht von SIR-Datensätzen ein

In diesem Abschnitt wird beschrieben, wie die zugehörigen Listen gruppiert und zur einfachen Navigation auf der Registerkarte „zugehörige SIR-Datensätze“ angezeigt werden.

Die Arbeitsbereichsanwender können die zugehörige Liste auch nach Namen durchsuchen. Weitere Informationen zum Konfigurieren zugehöriger Listen finden Sie unter SIR-Arbeitsbereich Zugehörige Datensätze.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie SI-Designzeituntersuchung

Verwenden Sie diesen Abschnitt, um die Seite „Security Incident Design Time Investigation“ zu konfigurieren, um mehrere Einstiegspunkte und die zugehörigen Datensätze innerhalb von hinzuzufügen Arbeitsbereich für Security Incident Response.

Erforderliche Rolle: sn_si.admin.

Im Folgenden werden die Schritte beschrieben, die bei der Konfiguration der Seite „Untersuchung“ auf der erforderlich sind Arbeitsbereich für Security Incident Response.

- Ansicht für zugehörige Informationstabellen wird erstellt
- Hinzufügen einer Einstiegspunktliste
- Zuordnungsansicht der Liste „Informationen der Einstiegspunktliste zuordnen“
- Konfigurieren Sie jede zugeordnete Liste in der Ansicht, um das Rendern von Laufzeitdaten zu verarbeiten

Zugehörige Informationen

Untersuchungs-Canvas Erkunden

Ansicht für zugehörige Informationstabellen wird erstellt

Der Bildschirm „Untersuchung“ nutzt die zugehörigen Listenansichten, die für Security Incidents erstellt wurden, um zugehörige Listen zu konfigurieren.

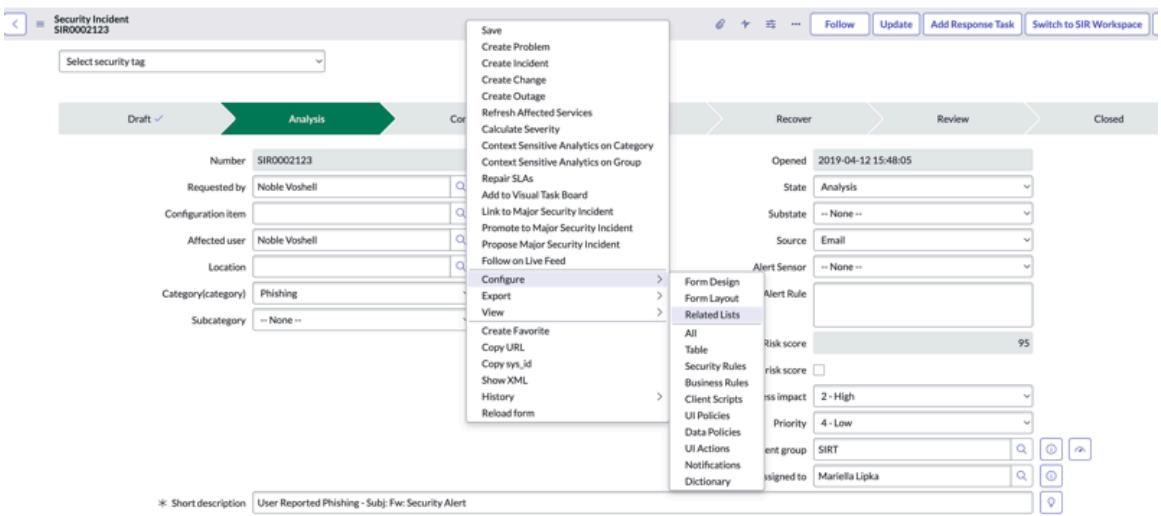
Vorbereitungen

Erforderliche Rolle: sn_si.admin

Im Folgenden finden Sie ein Verfahren zum Erstellen einer Ansicht und zum Hinzufügen zugehöriger Listen.

Prozedur

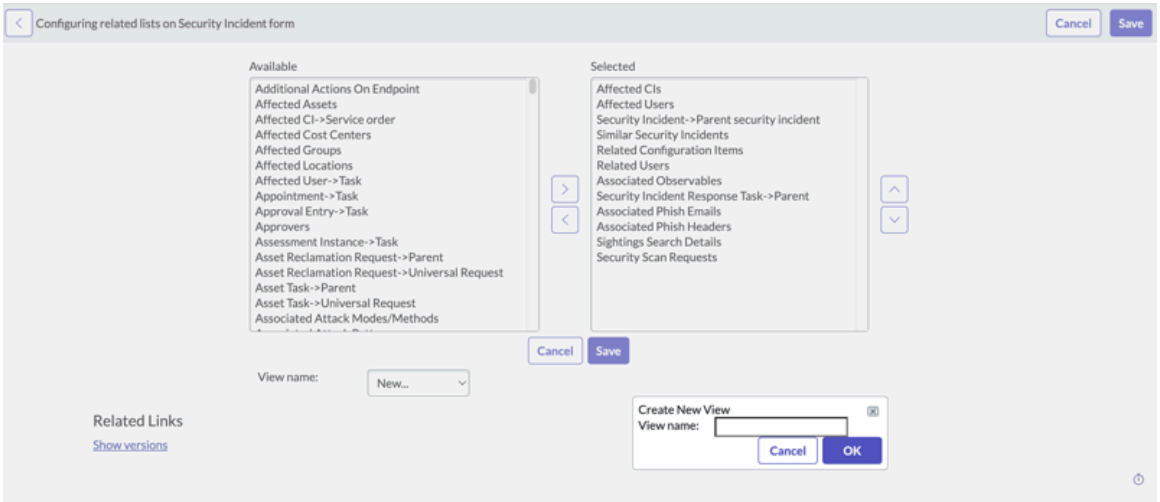
1. Navigieren Sie zu **Security Incident** Liste.
2. Öffnen Sie einen Security Incident in der klassischen Anwenderoberfläche.
3. Navigieren Sie im Kontextmenü des Formulars zu **Konfigurieren** > **Zugehörige Listen**an.
   Das Slush-Bucket-Fenster wird angezeigt.



4. Wechseln Sie zu **Name der Ansicht** Dropdown-Liste, und klicken Sie auf **Neu** Um eine neue Ansicht zu erstellen.
   Sie müssen der Ansicht einen Namen hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung



5. Fügen Sie die gewünschten zugehörigen Listen dem richtigen Bucket unter der neu erstellten Ansicht hinzu, und speichern Sie die Ansicht.
   Diese Ansicht wird zum Rendern der zugehörigen Informationen auf der Registerkarte „Untersuchung“ verwendet.

Hinzufügen einer Einstiegspunktliste

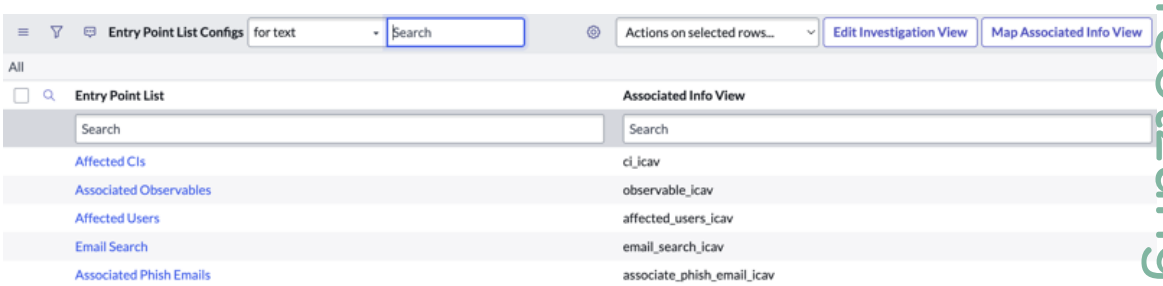
Konfigurieren Sie die neue Einstiegspunktliste, um sie der Seite „Untersuchung“ hinzuzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

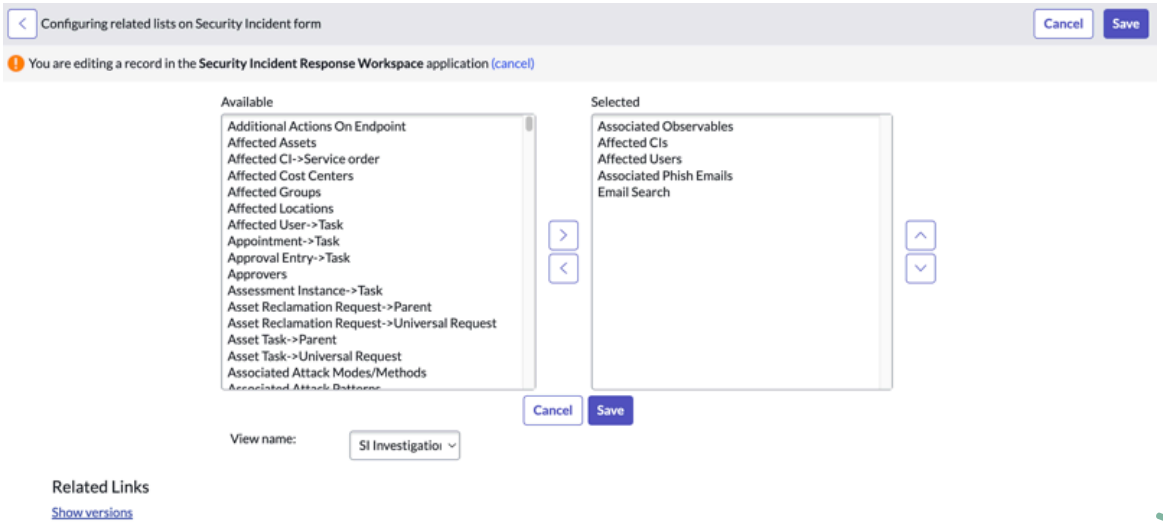
1. Navigieren zu **sn_si_aw_entry_Point_config.list**an.
   Die **Einstiegspunktlisten-Konfigurationen** Seite wird angezeigt.



2. Klicken Sie Auf **Bearbeiten Sie Die Untersuchungsansicht** Schaltfläche zum Hinzufügen einer Einstiegspunktliste zum Untersuchungsbildschirm.
   Die **Konfigurieren von zugehörigen Listen im Security Incident-Formular** Wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Fügen Sie die Einstiegspunktliste der Slush-Bucket-Ansicht hinzu, oder entfernen Sie sie.
4. Klicken Sie auf **Speichern**.

Hinweis:
Die Ansicht, die dem Untersuchungsbildschirm mit den Einstiegspunktlisten entspricht, wird aufgerufen **SI-Untersuchungsansicht** Und ist standardmäßig ausgewählt, wenn Sie zu navigieren **Bearbeiten Sie Die Untersuchungsansicht** Seite.

Die Reihenfolge, in der die Einstiegspunktlisten auf der Untersuchungs-Canvas angezeigt werden, wird durch die Reihenfolge in der ausgewählten Ansicht „Slush Bucket“ bestimmt.

Zuordnungsansicht der Liste „Informationen der Einstiegspunktliste zuordnen“

Ordnen Sie die zugeordnete Informationsansicht der neu hinzugefügten Einstiegspunktliste mit der Aktion zugeordnete Informationsansicht zuordnen zu.

Vorbereitungen

Hinweis:
Dieser Schritt ist erforderlich, damit die Einstiegspunktliste auf der Untersuchungsseite sichtbar ist. Auch wenn Sie nicht möchten, dass zugeordnete Informationslisten unter einem Einstiegspunkt angezeigt werden, müssen Sie dennoch eine Dummy-Ansicht erstellen und zuordnen.

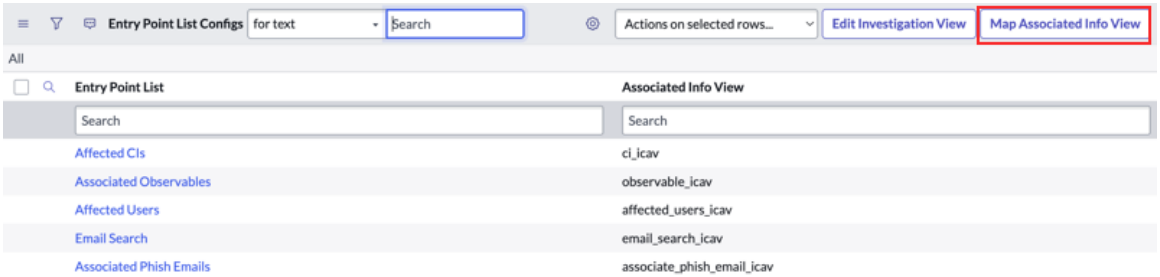
Erforderliche Rolle: Administrator

Automatische Übersetzung

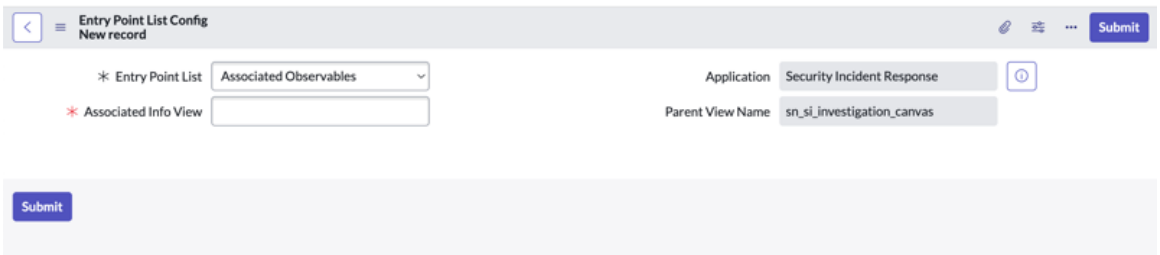
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie Auf **Zugeordnete Informationsansicht Zuordnen** Schaltfläche auf der **Einstiegspunktkonfigurationen** Seite.



2. Wählen Sie die neu hinzugefügte Einstiegspunktliste aus **Einstiegspunktliste** Dropdown-Liste.
3. Geben Sie den Ansichtsnamen ein, der die zugehörigen Listen mit Informationen enthält **Zugeordnete Informationsansicht** Feld.
   Informationen zum Erstellen einer Ansicht für die zugehörigen Listen mit Informationen finden Sie unter Ansicht für zugehörige Informationstabellen wird erstellt.



4. **Speichern** Sie das Formular.
5. Darüber hinaus können Sie bei Bedarf weitere zugeordnete Listen mit hinzufügen oder entfernen **Bearbeiten Sie Die Zugeordnete Informationsansicht** .
   Sie können das Listenlayout des Einstiegspunkts auch mit konfigurieren **Bearbeiten Sie Das Layout Der Einstiegspunkt-Liste** Aktion. Fügen Sie dem Slush-Bucket nach Bedarf Spalten hinzu, oder entfernen Sie sie daraus, und speichern Sie das Formular.

Konfigurieren Sie jede zugeordnete Liste in der Ansicht, um das Rendern von Laufzeitdaten zu verarbeiten

Konfigurieren Sie jede zugeordnete Liste in der Ansicht, um das Rendern von Laufzeitdaten zu verarbeiten.

Vorbereitungen

Hinweis:
Dieser Schritt ist für jede zugehörige Liste obligatorisch, die in der zugehörigen Informationsansicht konfiguriert ist. Andernfalls ist die zugehörige Liste auf der Seite „Untersuchung“ nicht verfügbar.

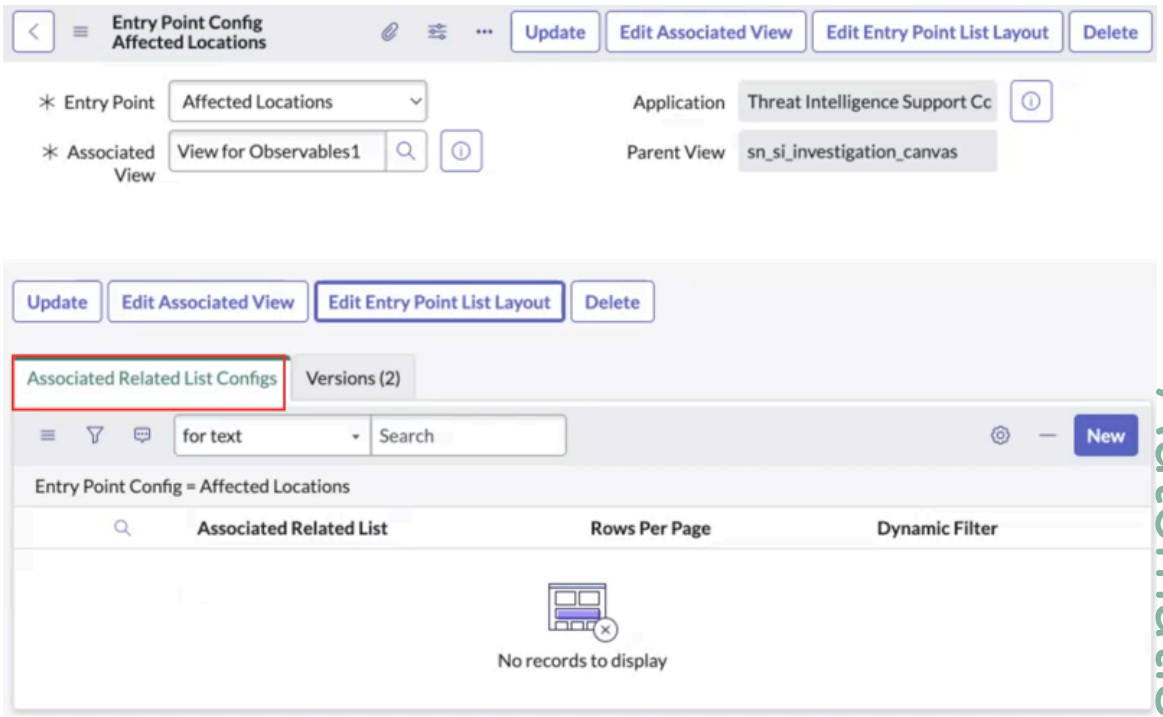
Jede der zugeordneten Listen hinzugefügt (während eine zugeordnete Informationsansicht einer Einstiegspunktliste zugeordnet wird) Zuordnungsansicht der Liste „Informationen der Einstiegspunktliste zuordnen“(Oder direkt aus der Ansicht) benötigt eine zusätzliche Konfiguration, um die Daten in Bezug auf die Auswahl des Laufzeitdatensatzes und die Filterauswahl zu filtern.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

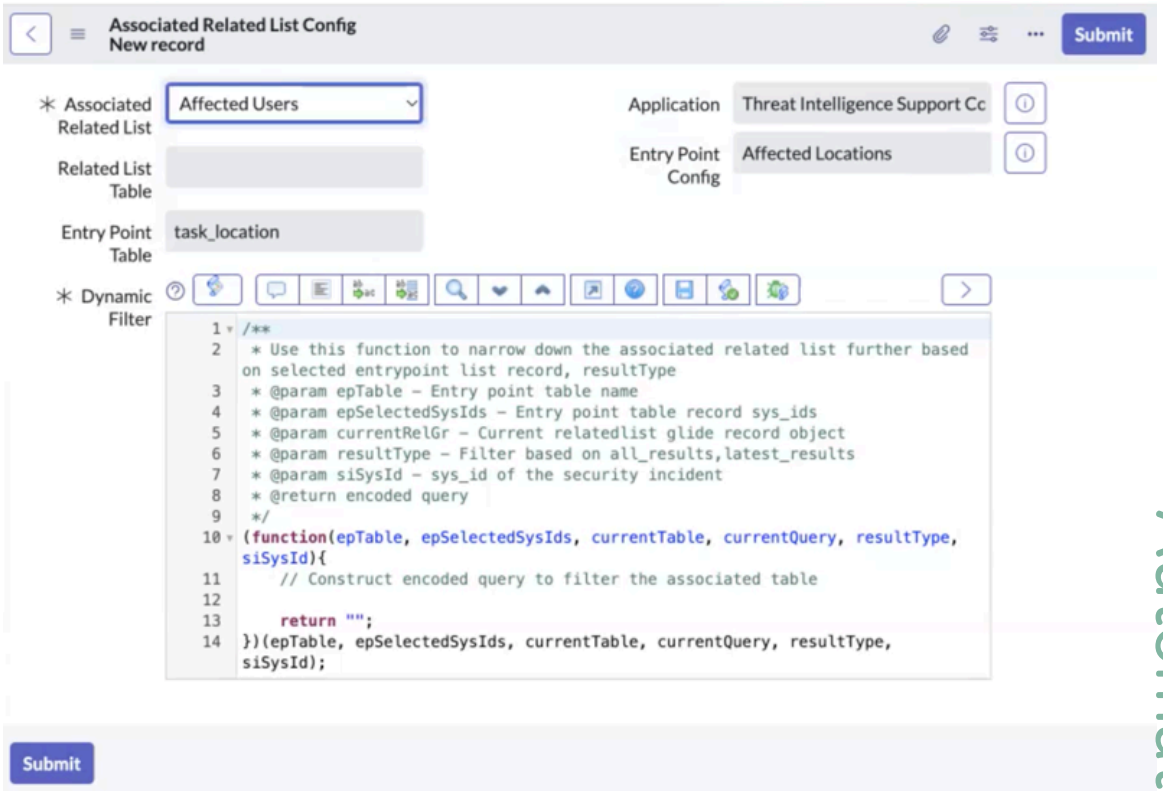
1. Klicken Sie Auf **Neu** Von **Zugeordnete Listenkonfigurationen** .



2. Wählen Sie Aus **Zugeordnete Liste** Feldwert.
3. Verwenden Sie **Dynamischer Filter** Spalte zum weiteren Filtern der zugeordneten Liste basierend auf den ausgewählten Einstiegspunktlistendatensätzen und dem Ergebnistyp (neueste Ergebnisse aus jeder Lieferantenimplementierung, alle Ergebnisse).
   Sehen Sie sich die vorhandenen Beispiele an, die im Lieferumfang des Produkts enthalten sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Außerdem können Sie das zugehörige Listenlayout mit konfigurieren **Bearbeiten Sie Das Layout Der Zugeordneten Liste** Aktion.
   Fügen Sie im Slush-Bucket-Fenster nach Bedarf Spalten hinzu oder entfernen Sie sie.

SIR-Arbeitsbereich Zugehörige Datensätze

Dieser Abschnitt besteht aus den zugehörigen Listenelementen, die in Abschnitte wie zugeordnete erkennbare Elemente und Konfigurationselemente gruppiert sind.

Die folgenden zugehörigen Listen Gruppen auf, die als Teil des Basissystems verfügbar sind. Sie können diese Gruppen ändern oder Gruppen in der Anwendung und ihren jeweiligen Aktionen erstellen.

Sie können diese Gruppen ändern oder neue Gruppen erstellen. Weitere Informationen finden Sie unter Konfigurieren Sie Die Zugehörige Liste „Security Incident“ Informationen zum Konfigurieren und Gruppieren der zugehörigen Liste für Security Incidents und Antwortaufgaben. Jede zugehörige Liste ist innerhalb von voll funktionsfähig SIR-Arbeitsbereich.

Zugehörige Liste	Gruppiertes Element
Geschäftsauswirkung	• Konfigurationselemente • Betroffene Anwender • Zugehörige Configuration Items • Zugehörige Anwender • Betroffene Services

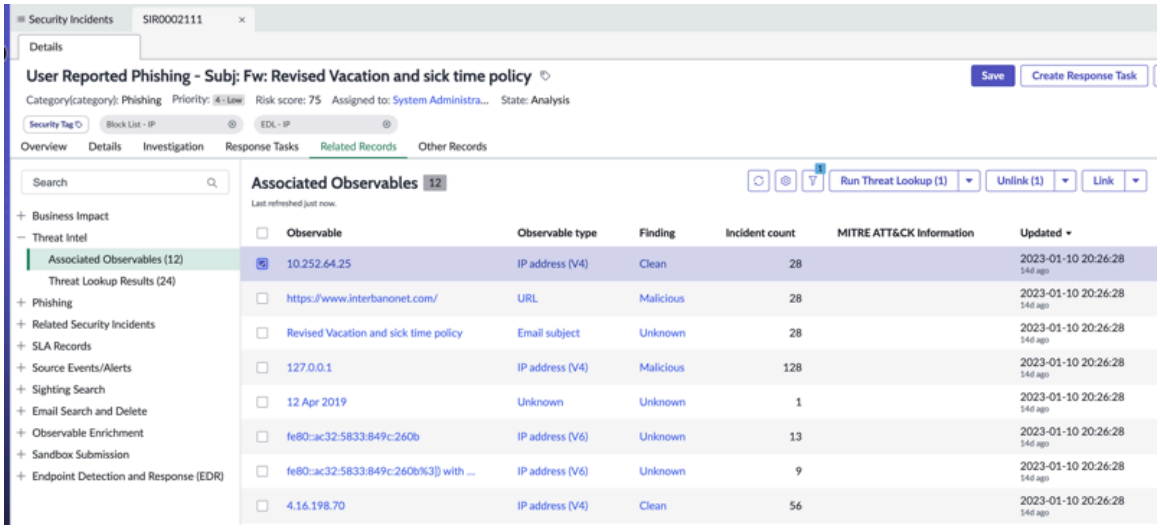
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Gruppiertes Element
Bedrohungsinformationen	• Zugehörige erkennbare Elemente • Bedrohungssuche – Ergebnisse
Phishing	• Zugeordnete Phishing-E-Mails • Zugehörige Phishing-Header
Zugehörige Security Incidents	• Übergeordneter Security Incident • Untergeordneter Security Incident • Ähnlicher Security Incident
SLA-Datensätze	Aufgaben-SLAs
Quell-Ereignisse/-warnungen	Quellereignisse oder Warnungen sind die zugehörige Liste „SIEM-Integration aktiviert“, z. B. Quell-E-Mail, LogRhythm-Drilldown-Protokolle, LogRhythm-Ereignisse, aggregierte IBM QRadar-Vergehen usw. **Hinweis:** Diese Liste hängt vollständig von der Integration ab, die Sie in Ihrer Instanz haben. Um die relevante zugehörige Liste der SIEM-Integration anzuzeigen, müssen Sie die neueste Version installieren.
Sichtungssuche	• Ergebnisse der Sichtungssuche • Details einer Sichtungssuche • Sighting
Ergänzung erkennbarer Elemente	• Erkennbare Elemente – Datenanreicherungs-Ergebnisse • Zugeordnete MISP-Ereignisse • MISP-Datenanreicherungs-Ergebnisse
Endpunkterkennung und -Antwort (EDR	• Hostdetails • Laufende Prozesse • Laufende Services • Angemeldete Anwender • Netzwerkstatistiken • Datei abrufen • Hosteinträge isolieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Gruppiertes Element
	• Zusätzliche Aktion für Endpunkt • Details zu Microsoft Defender für Endpunktbezogene Computer



Hinweis:
Im Allgemeinen können Sie neue Datensätze erstellen, vorhandene Datensätze oder neue Datensätze mit der zugehörigen Listengruppe verknüpfen oder deren Verknüpfung aufheben.

Zugehörige Informationen

Konfigurieren Sie Die Zugehörige Liste „Security Incident“

Konfigurieren Sie Die Zugehörige Liste „Security Incident“

Sie können neue zugehörige Listen oder neue zugehörige Listengruppen hinzufügen und vorhandene Gruppen oder zugehörige Listen ändern, die in angezeigt werden SIR-Arbeitsbereich.

Vorbereitungen

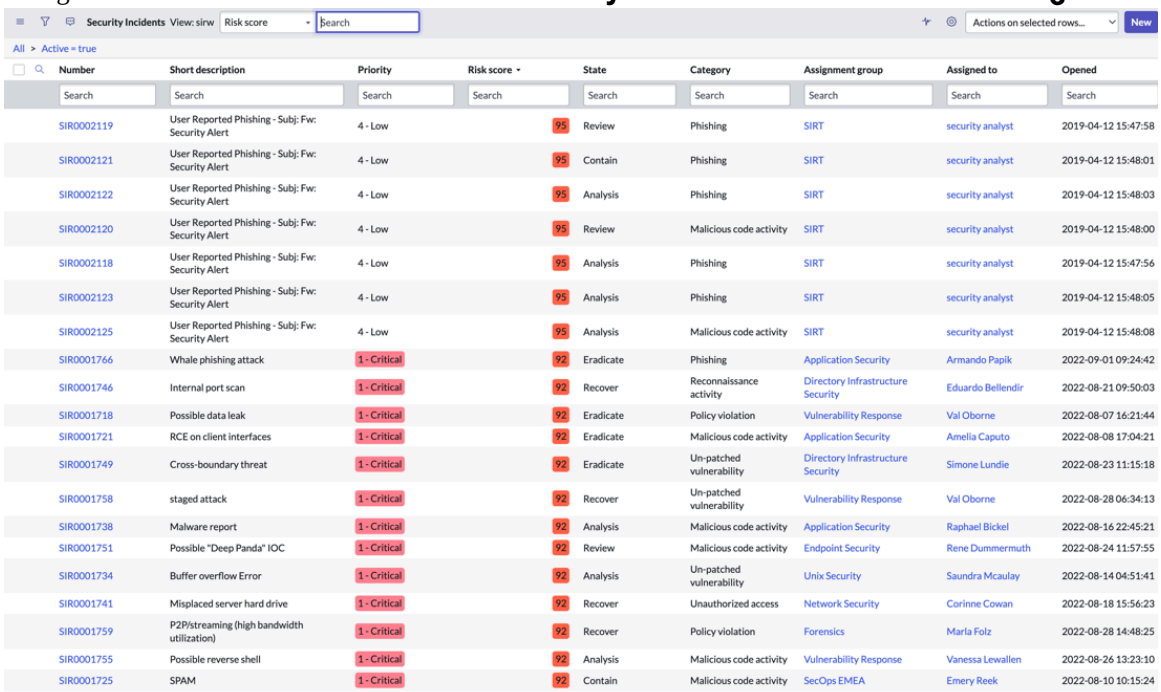
Die zugehörige Liste Security Incident wird gruppiert und als Gruppenbezogene Listenelemente auf der angezeigt **Zugehörige Datensätze** Registerkarte im Arbeitsbereich.

Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

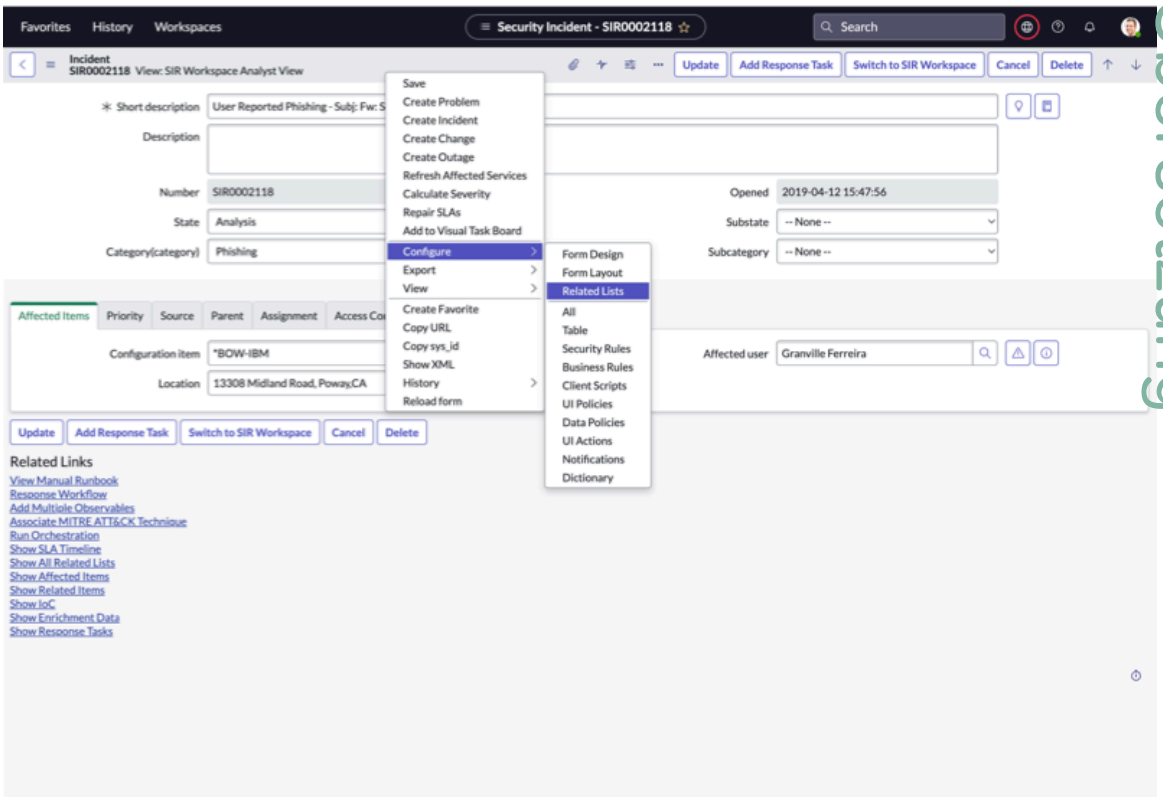
Prozedur

1. Navigieren Sie in der klassischen UI zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**an.



Number	Short description	Priority	Risk score	State	Category	Assignment group	Assigned to	Opened
SIR0002119	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Phishing	SIRT	security analyst	2019-04-12 15:47:58
SIR0002121	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Contain	Phishing	SIRT	security analyst	2019-04-12 15:48:01
SIR0002122	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:03
SIR0002120	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Review	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:00
SIR0002118	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:47:56
SIR0002123	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Phishing	SIRT	security analyst	2019-04-12 15:48:05
SIR0002125	User Reported Phishing - Subj: Fw: Security Alert	4 - Low	95	Analysis	Malicious code activity	SIRT	security analyst	2019-04-12 15:48:08
SIR0001766	Whale phishing attack	1 - Critical	92	Eradicate	Phishing	Application Security	Armando Papik	2022-09-01 09:24:42
SIR0001746	Internal port scan	1 - Critical	92	Recover	Reconnaissance activity	Directory Infrastructure Security	Eduardo Bellendir	2022-08-21 09:50:03
SIR0001718	Possible data leak	1 - Critical	92	Eradicate	Policy violation	Vulnerability Response	Val Oborne	2022-08-07 16:21:44
SIR0001721	RCE on client interfaces	1 - Critical	92	Eradicate	Malicious code activity	Application Security	Amelia Caputo	2022-08-08 17:04:21
SIR0001749	Cross-boundary threat	1 - Critical	92	Eradicate	Un-patched vulnerability	Directory Infrastructure Security	Simone Lundie	2022-08-23 11:15:18
SIR0001758	staged attack	1 - Critical	92	Recover	Un-patched vulnerability	Vulnerability Response	Val Oborne	2022-08-28 06:34:13
SIR0001738	Malware report	1 - Critical	92	Analysis	Malicious code activity	Application Security	Raphael Bickel	2022-08-16 22:45:21
SIR0001751	Possible "Deep Panda" IOC	1 - Critical	92	Review	Malicious code activity	Endpoint Security	Rene Dummermuth	2022-08-24 11:57:55
SIR0001734	Buffer overflow Error	1 - Critical	92	Analysis	Un-patched vulnerability	Unix Security	Saundra Mcaulay	2022-08-14 04:51:41
SIR0001741	Misplaced server hard drive	1 - Critical	92	Recover	Unauthorized access	Network Security	Corinne Cowan	2022-08-18 15:56:23
SIR0001759	P2P/streaming (high bandwidth utilization)	1 - Critical	92	Recover	Policy violation	Forensics	Marla Folz	2022-08-28 14:48:25
SIR0001755	Possible reverse shell	1 - Critical	92	Analysis	Malicious code activity	Vulnerability Response	Vanessa Lewallen	2022-08-26 13:23:10
SIR0001725	SPAM	1 - Critical	92	Contain	Malicious code activity	SecOps EMEA	Emery Reek	2022-08-10 10:15:24

2. Wählen Sie einen beliebigen Incident-Datensatz aus.
3. Klicken Sie mit der rechten Maustaste auf das Kontextmenü für Incidents.
4. Gehe zu **Konfigurieren** > **Zugehörige Liste**an.



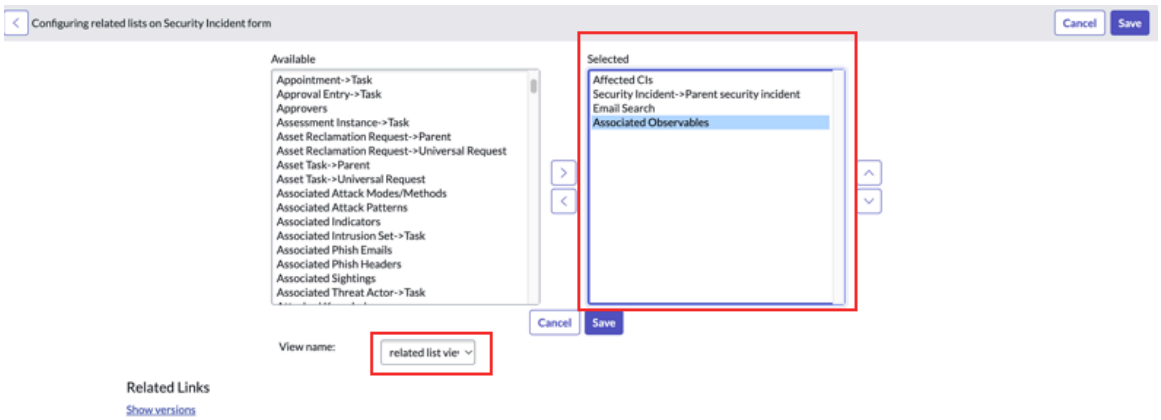
Die **Konfigurieren von zugehörigen Listen im Security Incident-Formular** Wird angezeigt.

5. Wechseln Sie zu **Name der Ansicht** Und wählen Sie aus **Neu** .

Automatische Übersetzung

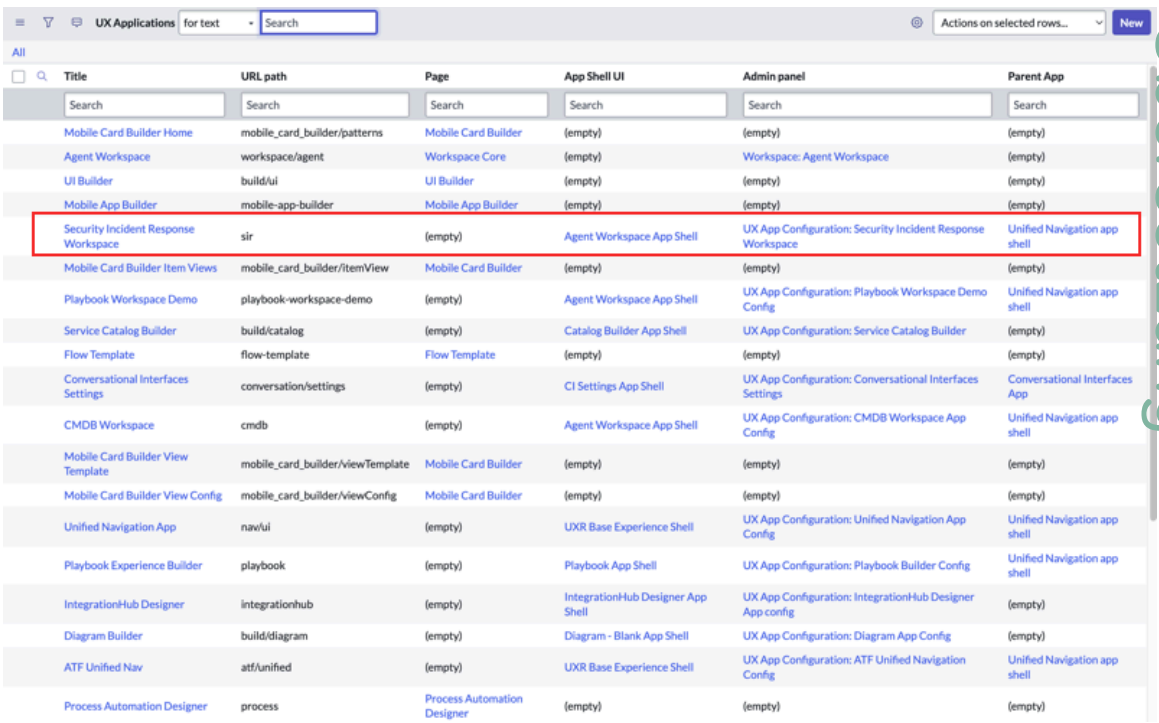
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Geben Sie einen Namen für die Ansicht ein.
7. Wählen Sie die neu erstellte Ansicht aus.
   Nachdem Sie die Ansicht ausgewählt haben, wählen Sie die erforderlichen zugehörigen Listenfelder aus dem Slush-Bucket aus.



Hinweis:
Wenn Sie etwas ändern möchten, wählen Sie die Ansicht aus, und entfernen oder fügen Sie die Elemente hinzu.

8. Klicken Sie auf **Speichern**.
9. Navigieren Sie in der linken Navigation zu **Alle** > **Now-Experience-Framework** > **Erfahrungen**an.
10. Wählen Sie Aus **Security Incident Response-Arbeitsbereich** .

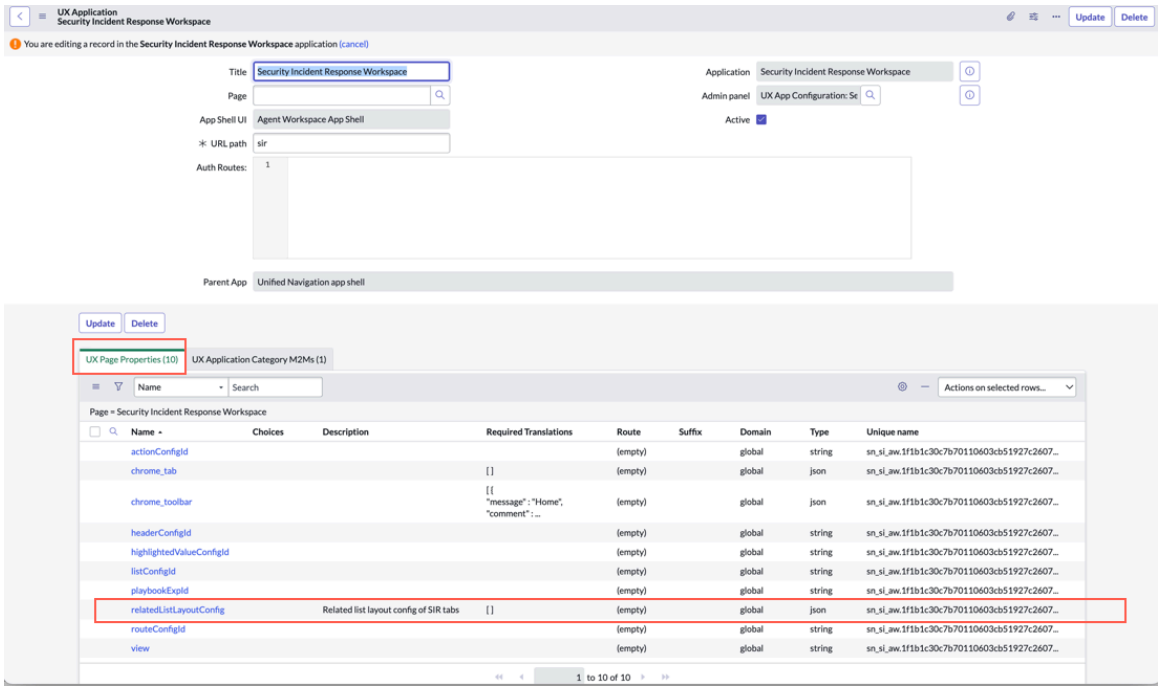


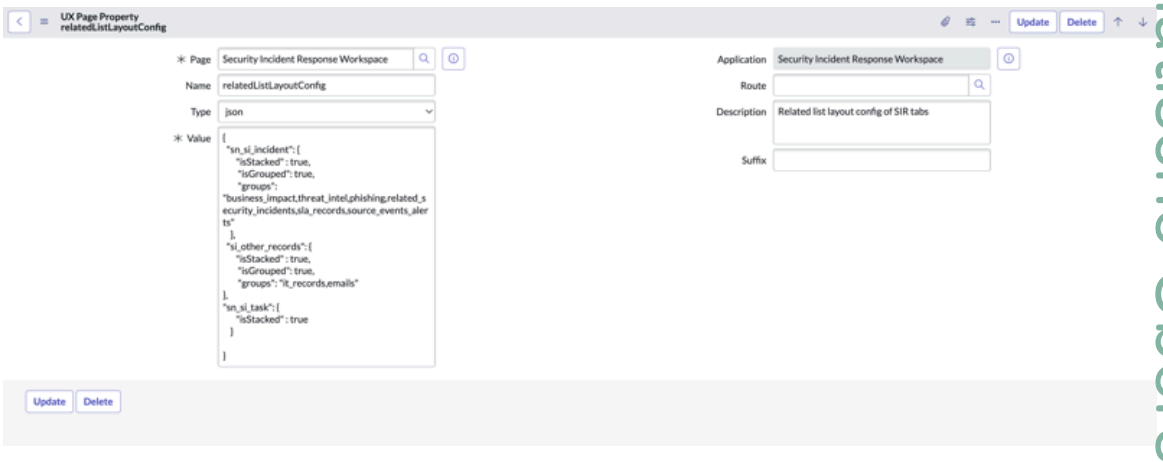
Die **UX-Anwendungssicherheit – Arbeitsbereich für die Reaktion auf Incidents** Seite wird angezeigt.

11. Wechseln Sie zu **UX-Seiteneigenschaften** Registerkarte und wählen Sie aus **RelatedListLayoutConfig** Option in der Listenansicht.

Automatische Übersetzung

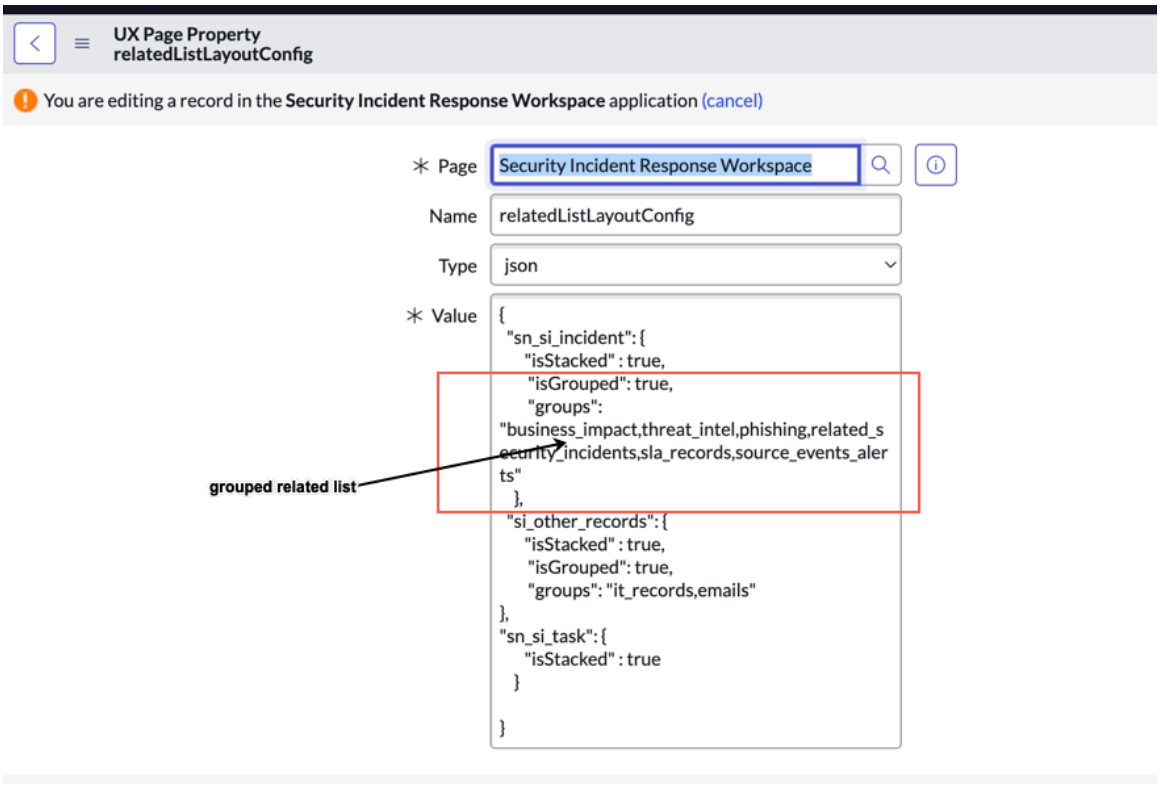
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.





12. Fügen Sie den neu erstellten Ansichtsnamen, getrennt durch ein Komma, einer bereits vorhandenen Werteliste in hinzu **Wert** Textfeld unter **sn_si_Incident.viewsUsedForGruppierung** Feld. Wenn Sie beispielsweise einen neuen Ansichtsnamen als erstellt haben, **Geschäftsauswirkung** Dann in **Wert** Textfeld, das Sie angeben müssen **Business_Impact** (Wird durch Unterstrich innerhalb des Ansichtsnamens getrennt und durch ein Komma nach einem vorhandenen Wert getrennt) im Feld sn_si_Incident:Groups.

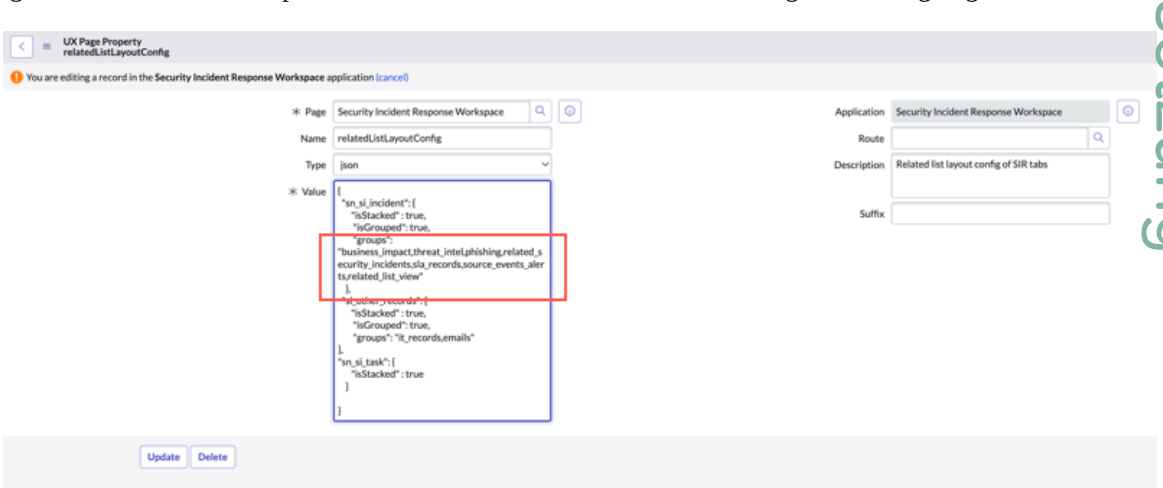
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Wenn Sie den neuen Ansichtsnamen unter hinzufügen **sn_si_Incident.viewsUsedForGruppierung** Feld, dann wird der Eintrag in erstellt **Zugehörige Datensätze** Registerkarte des Arbeitsbereichs.

Wenn Sie den Ansichtsnameneintrag in aktualisieren **si_Other_Records.ViewsUsedForGruppierung** Dann wird die zugehörige Listengruppe in hinzugefügt **Andere Datensätze** Registerkarte des Arbeitsbereichs.

Nachfolgend finden Sie eine Beispielansicht, die die neu erstellten Ansichten zeigt, die hinzugefügt wurden.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
AnforderungsRolesForGruppierung Enthält kommagetrennte sys_user_role-Datensatznamen. SIR-Arbeitsbereich-Anwender muss mindestens eine dieser Rollen haben, um die gruppierten zugehörigen Listen zu verwenden. Wenn ein Anwender über keine dieser Rollen verfügt, wird die Ansicht „zugehörige Listen“, die für die aktuelle Anwenderrolle konfiguriert ist, mit der Ansichtsregelkonfiguration vertikal ohne Gruppierung dargestellt. Diese Eigenschaft wird ignoriert, wenn **Ist gruppiert** Eigenschaft ist auf „falsch“ festgelegt. Wenn diese Eigenschaft leer ist, kann jeder Anwender auf die gruppierten zugehörigen Listen zugreifen.

13. Klicken Sie auf **Speichern**.
14. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
15. Wählen Sie einen bestimmten Security Incident aus.
16. Wechseln Sie zu **Zugehörige Datensätze** Registerkarte des Arbeitsbereichs.
    Die gruppierten zugehörigen Listen werden angezeigt.

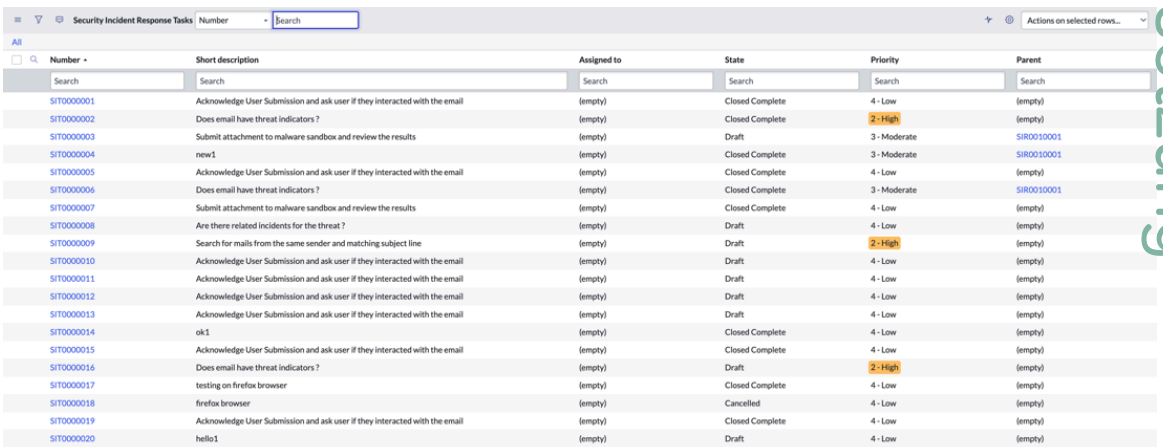
Konfigurieren Sie Die Zugehörige Liste Für Antwortaufgaben

Verwenden Sie diesen Abschnitt, um neue zugehörige Listen für Antwortaufgaben zu konfigurieren, die in der Anwendung Security Incident Response angezeigt werden.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Die zugehörige Liste „Antwortaufgaben“ ist nicht gruppiert, sondern wird als einzelne zugehörige Listenelemente angezeigt, da es nur wenige Standardlisten gibt. Zeigen Sie die zugehörigen Elemente für Antwortaufgaben in der an **Antwortaufgaben** Registerkarte des Security Incident-Datensatzes des Arbeitsbereichs.

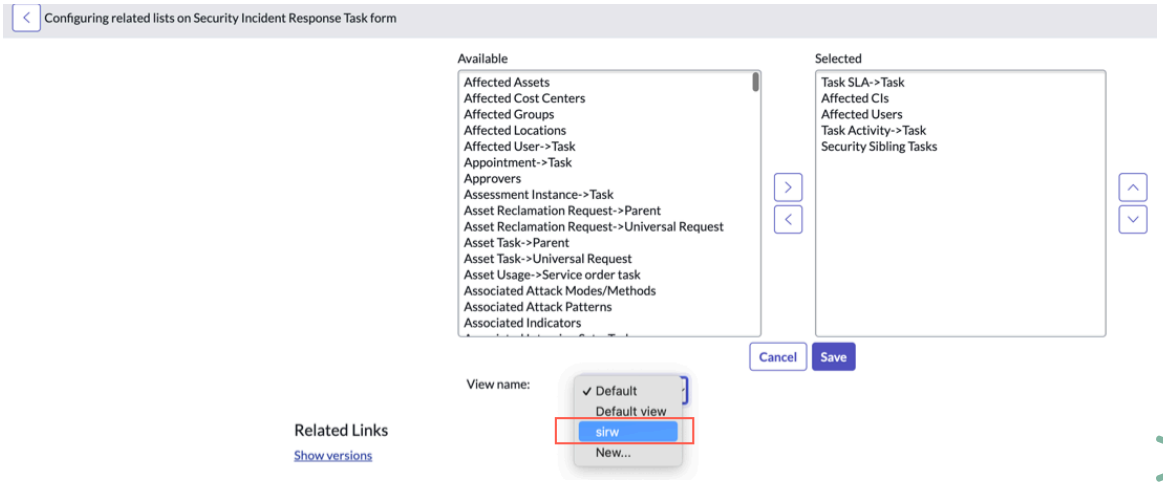
Prozedur
1. Navigieren zu **Alle** > **Security Incident** > **Antwortaufgaben** > **Alle Aufgaben anzeigen**an.



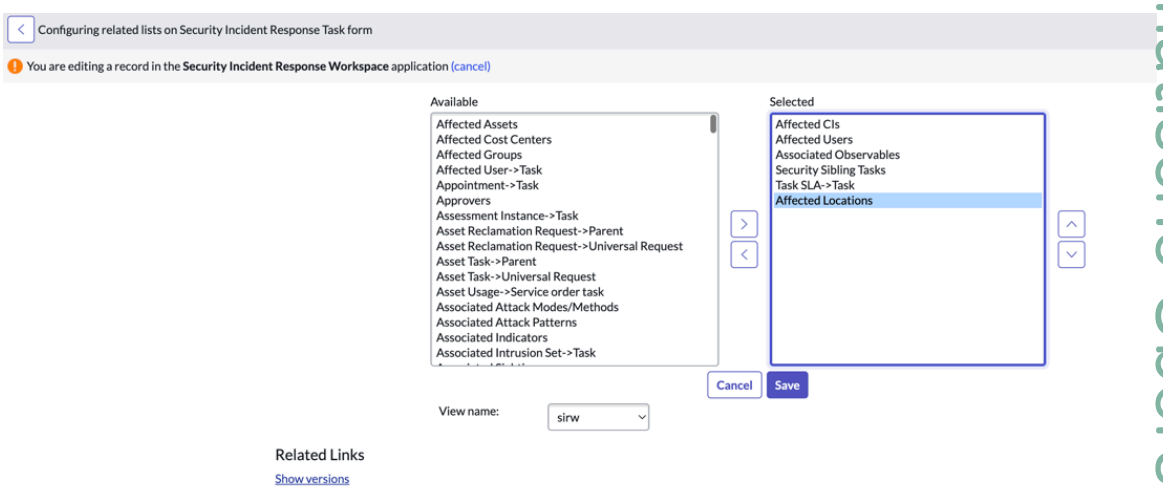
2. Wählen Sie einen beliebigen Antwortaufgabendatensatz aus.
3. Klicken Sie mit der rechten Maustaste auf das Kontextmenü der Security Incident Response-Aufgabe.
4. Navigieren zu **Konfigurieren** > **Zugehörige Liste**an.
   Die **Zugehörige Listen im Formular „Sicherheitsantwortaufgabe“ werden konfiguriert** Wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wechseln Sie zu **Name der Ansicht** Und wählen Sie aus **SIRW** Anzeigen.



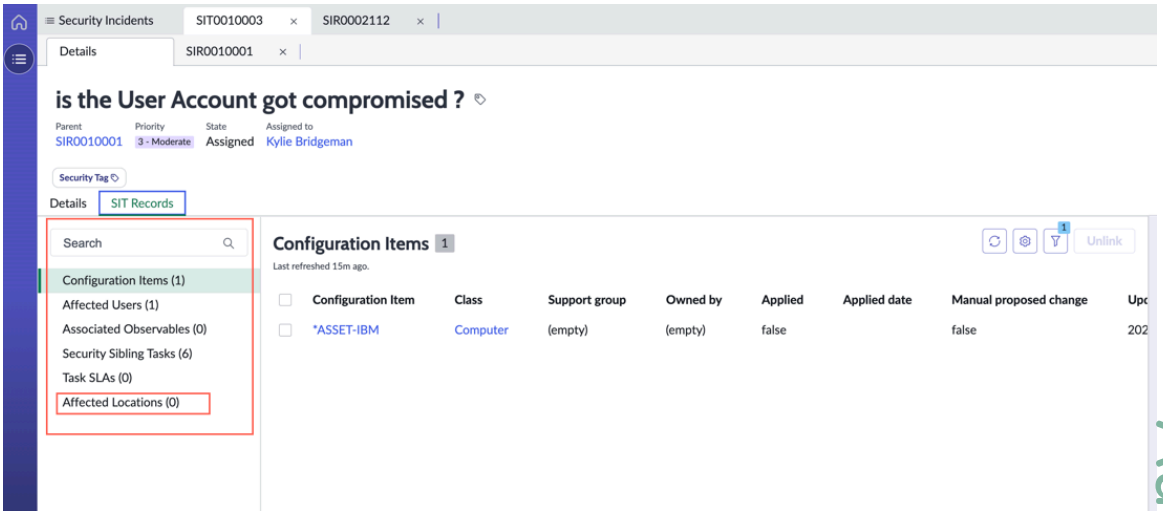
6. Wählen Sie die gewünschten zugehörigen Listenfelder aus dem Slush-Bucket aus.
   Beispiel: Betroffene Standorte.



7. Klicken Sie auf **Speichern**.
8. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Antwortaufgaben** > **SIT-Datensätze**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die konfigurierten zugehörigen Listen (z. B. betroffene Standorte wie ausgewählt) werden in der Liste der SIT-Datensätze aufgeführt.



Definieren Sie die neuen Regeln für den Rechner der Risikopunktzahl

Verwenden Sie den neuen Risikopunktzahlrechner, um die Risikopunktzahl von Security Incidents basierend auf den anwenderdefinierten Kriterien zu definieren und zu berechnen, die eine transparente Intelligence-Bewertung von Security Incidents bieten. Die Risikopunktzahl wird für die Security Incident-Datensätze automatisch berechnet.

Vorbereitungen

Erforderliche Rolle: sn_si.admin.

Aktivieren Sie den neuen Rechner für die Risikopunktzahl, indem Sie festlegen sn_si_aw.activate_New_Risk_Score_Calculator Systemeigenschaft auf „wahr“.

Warum und wann dieser Vorgang ausgeführt wird

Definieren Sie eine Risikopunktzahl für die Security Incident-Datensätze, die basierend auf den anwenderdefinierten Parametern generiert werden. Das Basissystem wird mit einer Risikobewertungsregel bereitgestellt, die angepasst und entsprechend aktiviert werden kann.

Hinweis:

- Standardmäßig ist die neue Regel für den Rechner der Risikopunktzahl inaktiv, und Sie müssen die Regel aktivieren, um die Risikopunktzahl der Security Incidents anzuzeigen.
- Informationen zur Berechnung der Risikopunktzahl für zusätzliche zugehörige Tabellen, die nicht im Basissystem verfügbar sind, finden Sie unter Risikopunktzahlrechner für zusätzliche zugehörige Tabellen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Administration**an.
2. Navigieren zu **Regel-Engine** > **Regel des Risikobewertungsrechners**an.
   Die Seite „Regel des Risikopunktzahlrechners“ wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Als Teil des Basissystems erhalten Sie eine vordefinierte Risikobewertungsregelvorlage zum Anzeigen, Bearbeiten oder Ändern der Risikopunktzahl. Sie können die vordefinierte Vorlage für die Risikopunktzahlregel jedoch nicht erstellen oder löschen.
- Die von Ihnen vorgenommenen Änderungen gelten für alle neuen Security Incidents oder Updates für die vorhandenen. Um historische Punktzahlen neu anzugeben, verwenden Sie **Berechnen Sie Die Punktzahl Neu** Aktion.

3. Wählen Sie aus **Rechner Für Risikopunktzahl** Regel.
4. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Name des Risikopunktzahlwerts. Beispiel: Rechner für Risikopunktzahl.
Gesamtgewichtung (gilt für den Kriteriengenerator)	Gewichtung dieses Felds innerhalb der Risikoregel. Dieses Feld kann nicht bearbeitet werden und zeigt die Gesamtgewichtung an, die vom System basierend auf der Gewichtung berechnet wird, die den aktivierten Kriterien entspricht. Die Gesamtgewichtung muss immer 100 % betragen.
Beschreibung	Beschreibung des Risikobewertungsdatensatzes. Beispielsweise berechnet die Risikopunktzahl basierend auf der gewichteten Summe vordefinierter Kriterienpunktzahlen.
Bewertungskriterien	Gibt die Bewertungskriterien für einen Security Incident an. Sie können das Risiko definieren **Bewertungskriterien** Mit den folgenden Optionen: ○ **Kriteriengenerator** : Verwenden Sie diese Option, um Kriterien hinzuzufügen, zu bearbeiten oder zu entfernen, zu aktivieren und zu deaktivieren, die zur Berechnung der Risikopunktzahl beitragen, und sicherzustellen, dass die zusammengefasste Gesamtgewichtung 100 % beträgt. ○ **Skript Verwenden (Erweitert)** : Die Skripting-Funktion ist eine erweiterte Funktion zum Erstellen eines anwenderdefinierten Skripts, das die Risikopunktzahl zurückgeben soll, bei der es sich um einen Ganzzahlwert zwischen 0 und 100 handelt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Zum Definieren von **Bewertungskriterien** Mit **Kriteriengenerator** , Führen Sie die folgenden Schritte aus:

Hinweis:
Sie können die vorhandenen Kriterien bearbeiten oder ändern oder neue Kriterien hinzufügen.

a. Um neue Kriterien hinzuzufügen, wählen Sie aus **+neue Kriterien** Aktion.

b. Wählen Sie aus **Tabelle** Für die Sie die Kriterien festlegen möchten.

Hinweis:

- Wenn die ausgewählte Tabelle ein Security Incident ist, wird die Bedingung auf den Security Incident-Datensatz angewendet, für den die Risikopunktzahl berechnet wird. Wenn die ausgewählte Tabelle kein Security Incident ist, wird die Bedingung nur angewendet, wenn sich die Datensätze auf den Security Incident beziehen, für den die Risikopunktzahl berechnet wird.
- Ein zusätzlicher Aggregattyp wird hinzugefügt, um die Punktzahlen basierend auf der Anzahl der Beziehungen zu definieren, die den Security Incidents zugeordnet sind.

c. Wählen Sie aus **Typ** Kriterien für die ausgewählte Tabelle.
Der Wert „Typ“ könnte entweder sein **Feld** Oder **Aggregieren** Basierend auf der von Ihnen ausgewählten Tabelle.

d. Wählen Sie aus **Feld** Kriterien für die ausgewählte Tabelle.
Wenn Sie den Wert Typ als ausgewählt haben **Feld** , Dann zeigen die Feldkriterien die Feldwerte an, die sich auf die Tabelle beziehen. Wenn Sie den Wert Typ als ausgewählt haben **Aggregieren** , Dann zeigen die Feldkriterien die Aggregatwerte an, die sich auf die Tabelle beziehen.

Hinweis:
Der Aggregattyp unterstützt nur den Zählwert.

Beispiel: Wenn Sie Tabellenkriterien als auswählen **Security Incident** , Dann werden nur die Typkriterien angezeigt **Feld** Option. Die Feldkriterien zeigen alle Feldwerte an, die sich auf die Tabelle beziehen, z. B. Schweregrad, aktiv usw., wenn Sie Tabellenkriterien als auswählen **Betroffene Anwender** , Dann zeigt die Typkriterien beide an **Feld** Und **Aggregieren** Option. Wenn Sie den Typ als Aggregat auswählen, zeigen die Feldkriterien die Aggregatwerte an, die sich auf die Tabelle beziehen **Anzahl** .

e. Geben Sie ein **Gewichtung** Der Kriterien zwischen 0 und 100.
Die Gesamtgewichtung aller Kriterien muss 100 % betragen.

f. Geben Sie den Namen und eine kurze Beschreibung der Kriterien ein.

g. Wählen Sie aus **Aktivieren Sie Bewertungskriterien** Kontrollkästchen zum Aktivieren der Bewertungskriterien.

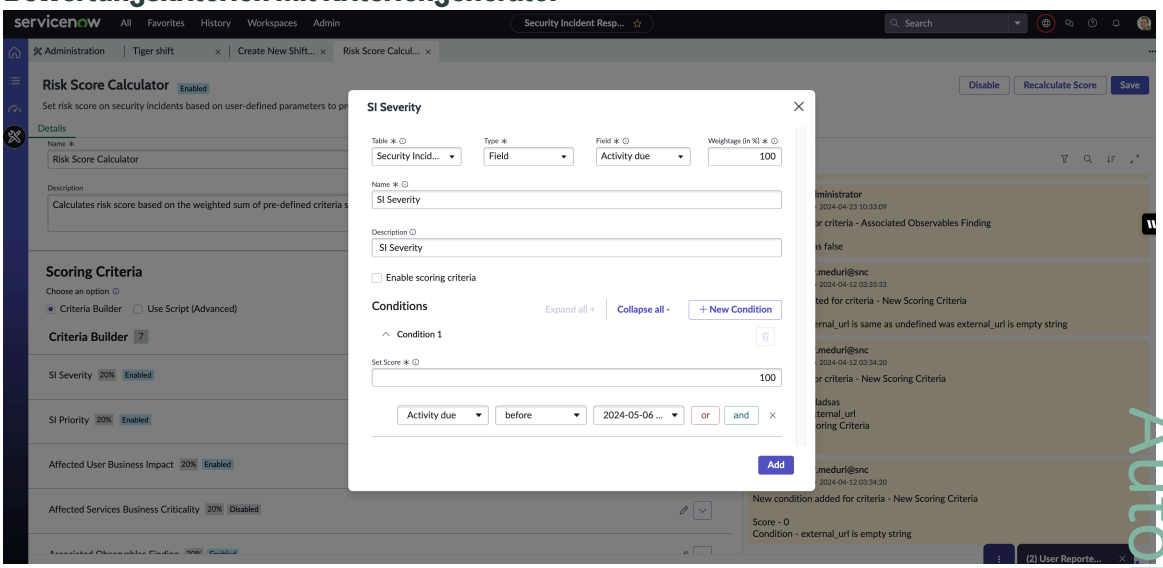
h. Definieren Sie **Bedingungen** Und legen Sie die Punktzahl für die Bedingungen fest.

i. Sie können auch neue Bedingungen mit hinzufügen **Neue Bedingung** Und löschen Sie vorhandene Bedingungen mit **Löschen Sie Kriterien** Symbol.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

j. Wählen Sie Aus **Hinzufügen** Um die konfigurierten Kriterien hinzuzufügen.

Bewertungskriterien mit Kriteriengenerator



6. Wählen Sie aus **Berechnen Sie Die Punktzahl Neu** Option zum Neuberechnen der Risikopunktzahl.

Beispiel: Wenn Änderungen an der Risikopunktzahlregel vorhanden sind. In diesem Fall müssen Sie die Bewertungsregel erneut auf die Security Incidents anwenden, deren Risikopunktzahl bereits in der Vergangenheit berechnet wurde. Verwenden Sie **Berechnen Sie Die Punktzahl Neu** Aktion zum Auslösen des Neuberechnungsauftrags.

7. Wählen Sie **Bestätigen** aus.

Hinweis:
Sobald Sie diese Aktion ausgelöst haben, wird der Prozess im Hintergrund ausgeführt und dauert einige Minuten. Sie können erst Änderungen vornehmen, wenn der Vorgang abgeschlossen ist.

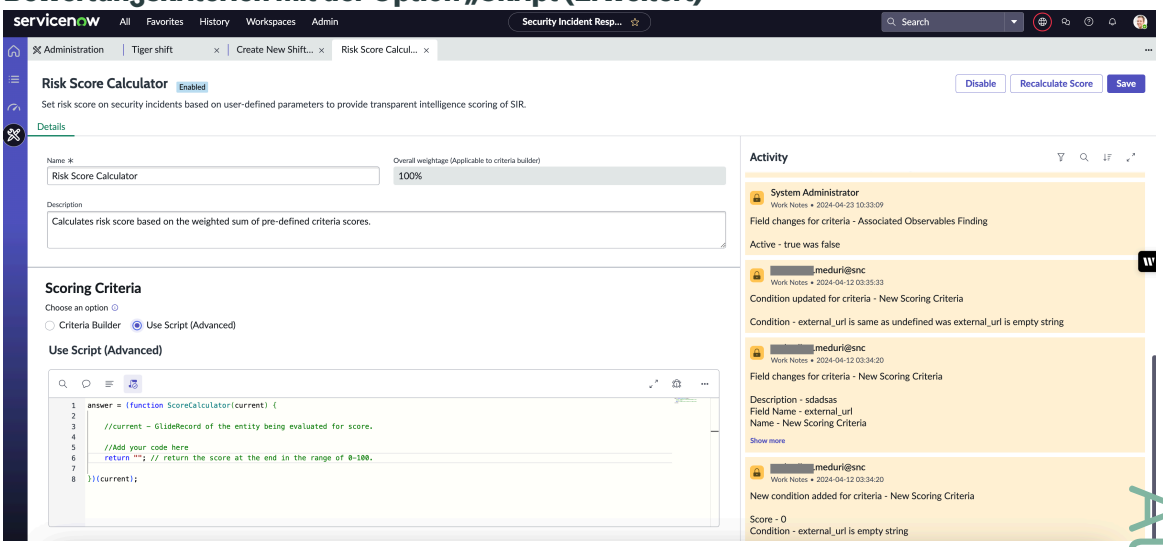
8. Zum Definieren von **Bewertungskriterien** Verwenden **Skript Verwenden (Erweitert)** Option führen Sie die folgenden Schritte aus:

a. Verwenden Sie dieses vordefinierte Skript, um ein anwenderdefiniertes Skript zu erstellen, das die Risikopunktzahl zurückgeben soll, bei der es sich um einen Ganzzahlwert zwischen 0 und 100 handelt. Das Feld „Erweitertes Skript“ wird automatisch mit einer Funktion ausgefüllt, die die Parameter übernimmt **Aktuell** Und diese Funktion sollte die Risikopunktzahl zurückgeben, bei der es sich um einen Ganzzahlwert im Bereich von 0 bis 100 handelt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewertungskriterien mit der Option „Skript (Erweitert)“



Hier ist der aktuelle Parameter das GlideRecord-Objekt der Entität (Security Incident), für die die Risikopunktzahl berechnet wird. Für die Security Incidents entspricht er dem GlideRecord für die Tabelle „sn_si_Incident“.

9. Um den Rechner für Risikopunktzahl zu deaktivieren, wählen Sie aus **Deaktivieren** .
10. Wählen Sie **Speichern**.

Risikopunktzahlrechner für zusätzliche zugehörige Tabellen

Der Risikopunktzahlrechner wird mit einer Risikobewertungsregel als Teil des Basissystems bereitgestellt, um die Risikopunktzahl von Security Incidents basierend auf anwenderdefinierten Kriterien zu berechnen. Sie können jedoch zusätzliche zugehörige Tabellen anpassen und einbeziehen, um die Risikopunktzahl zu berechnen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie einen beliebigen Security Incident-Datensatz aus.
3. Wählen Sie aus **Zusätzliche Aktionen** Option neben der Security Incident-Nummer.
4. Gehe zu **Konfigurieren** > **Zugehörige Listen**an.
5. Wechseln Sie zum Ansichtsnamen, und wählen Sie aus **Rechner Für Risikopunktzahl** .
   Nachdem Sie die Ansicht ausgewählt haben, wählen Sie die erforderliche zugehörige Liste aus, die Sie aus dem Slush-Bucket hinzufügen möchten. Zum Beispiel zugeordnete Sichtungen.
6. Wählen Sie **Speichern**.
   Sie haben die neuen zugehörigen Listen oder Tabellen, für die Sie die Risikopunktzahl berechnen möchten, erfolgreich hinzugefügt.

Wichtig:
Um die Risikopunktzahl für Security Incidents zu berechnen, die neue Kriterien mit den neu erstellten zugehörigen Listen aufweisen, müssen Sie Business-Regeln in der Basistabelle der zugehörigen Liste definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln**an.
   Sie können die folgenden beiden Business-Regeln als Referenz verwenden, um eigene Business-Regeln zu erstellen:
   - Fügen Sie Security Incidents (SIS) der Warteschlange des Punktzahlrechners hinzu
   - Beziehung zur Warteschlange des Punktzahlrechners hinzufügen (gilt für m2m-Tabellen)

Business-Regeln

Business Rules | Name | Search | Actions on selected rows... | New

All > Application = Security Incident Response Workspace

Name	Active	Table	Application	Order	Updated
Add Relation To Score Calculator Queue	true	Assets Affected [task_asset]	Security Incident Response Workspace	100	2024-04-01 11:05:40
Add Relation To Score Calculator Queue	true	Task Attack Pattern [sn_ti_stix2_m2m_task_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:05:35
Add Relation To Score Calculator Queue	true	Task Observable [sn_ti_m2m_task_observable]	Security Incident Response Workspace	100	2024-04-01 11:05:38
Add SI to Risk Score Processing Queue	true	Security Incident [sn_si_incident]	Security Incident Response Workspace	100	2024-04-16 10:55:55
Add SIs to Score Calculator Queue	true	Observable [sn_ti_observable]	Security Incident Response Workspace	100	2024-04-01 11:03:14
Add SIs to Score Calculator Queue	true	Threat Lookup Result [sn_ti_lookup_result]	Security Incident Response Workspace	100	2024-04-01 11:04:17
Add SIs to Score Calculator Queue	true	Sandbox Submission Results [sn_ti_sandbox_submission_results]	Security Incident Response Workspace	100	2024-04-01 11:03:48
Add SIs to Score Calculator Queue	true	Observable Enrichment Result [sn_ti_observable_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:39
Add SIs to Score Calculator Queue	true	Attack Pattern [sn_ti_stix2_attack_pattern]	Security Incident Response Workspace	100	2024-04-01 11:03:21
Add SIs to Score Calculator Queue	true	Configuration Item Enrichment [sn_sec_cmn_ci_enrichment_result]	Security Incident Response Workspace	100	2024-04-01 11:03:31
Add SIs to Score Calculator Queue	true	Email Search Result [sn_sec_cmn_email_search_result]	Security Incident Response Workspace	100	2024-04-22 05:56:53
Add SIs to Score Calculator Queue	true	Asset [alm_asset]	Security Incident Response Workspace	100	2024-04-01 11:03:03
Add SIs to Score Calculator Queue	true	Sightings Search Detail [sn_ti_sighting_search_detail]	Security Incident Response Workspace	100	2024-04-01 11:03:57
Check Duplicate Associated Related List	true	Associated List Config [sn_si_aw_entry_point_associated_rel_list_config]	Security Incident Response Workspace	100	2022-11-01 09:47:15
Check Duplicate Entry Point Config	true	Entry Point List Config [sn_si_aw_entry_point_config]	Security Incident Response Workspace	100	2022-11-01 08:47:45
Check unique name	true	Quick Filters [sn_si_aw_quick_filters]	Security Incident Response Workspace	100	2022-12-22 02:46:46

8. Damit beispielsweise die zugehörigen Kriterien für erkennbare Elemente funktionieren, haben wir zwei Business-Regeln definiert.

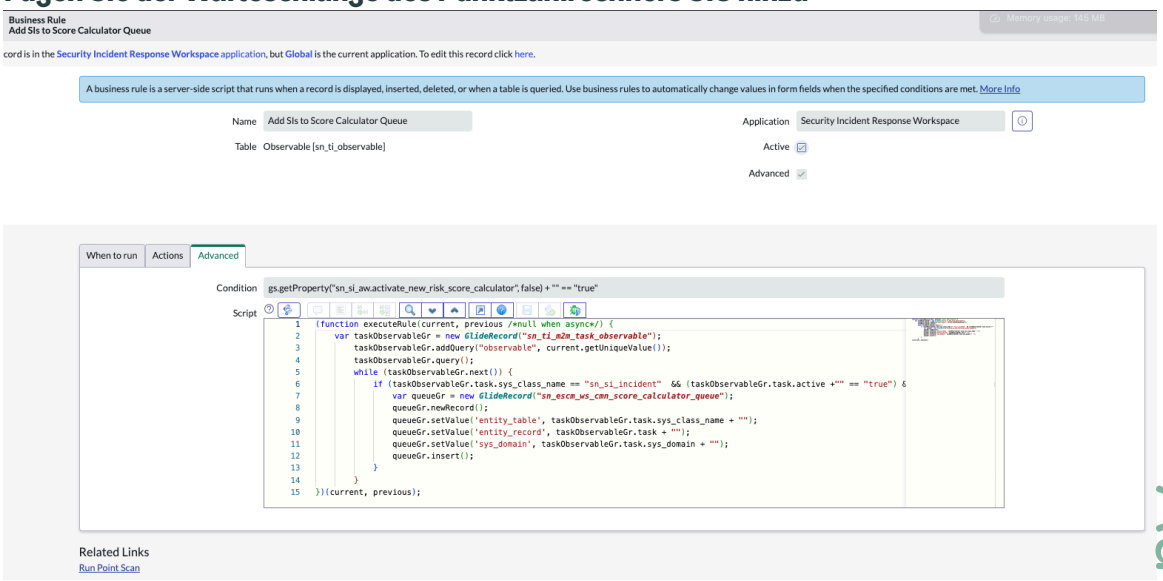
   Der erste ist der **Fügen Sie der Warteschlange des Punktzahlrechners SIS hinzu** Business-Regel.

   Beispielsweise wird ein neuer Security Incident erstellt und einem erkennbaren Element zugeordnet (Erkennbare Elemente[sn_ti_observable]) Tabelle. Nach der Bedrohungssuche wird festgestellt, dass das erkennbare Element schädlich ist. Sie müssen dann alle Security Incidents, die diesem schädlichen erkennbaren Element zugeordnet sind, der Warteschlange hinzufügen, um die Risikopunktzahl der Security Incidents neu zu berechnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

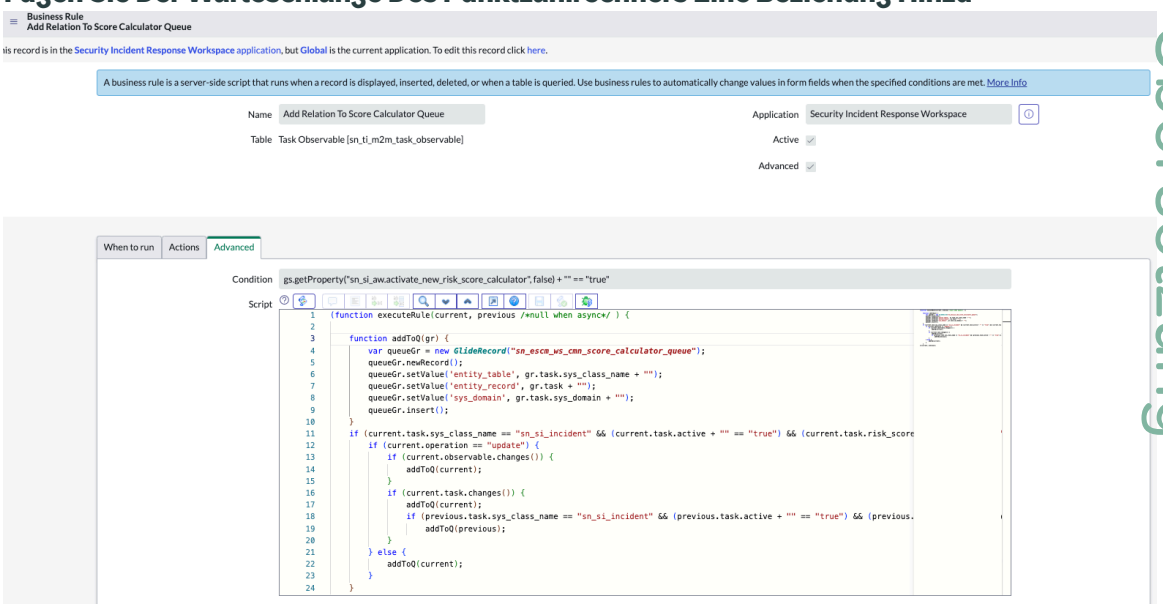
Fügen Sie der Warteschlange des Punktzahlrechners SIS hinzu



Die zweite ist die **Fügen Sie Der Warteschlange Des Punktzahlrechners Eine Beziehung Hinzu** Business-Regel.

Beispielsweise wird ein neuer Security Incident erstellt oder gelöscht und einem erkennbaren Element zugeordnet (Erkennbare Aufgaben[sn_ti_m2m_Task_observable]) Tabelle. Daher gibt es eine Änderung in der Zuordnung des Security Incidents. Sie müssen diesen Security Incident dann der Warteschlange hinzufügen, um die Risikopunktzahl des Security Incidents neu zu berechnen.

Fügen Sie Der Warteschlange Des Punktzahlrechners Eine Beziehung Hinzu



Konfigurieren Sie Die Schichtübergabe

Konfigurieren Sie die Einstellungen für die Schichtübergabe, um den Analysten der nächsten Schicht vollständige Schichtinformationen bereitzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Schichtübergabevorlagen

Der Administrator kann verschiedene Schichtübergabevorlagen für den Schichtbesitzer definieren und konfigurieren, um Schichtübergabedatensätze zu erstellen und sie an das nächste Schichtteam zu übergeben.

Vorbereitungen

Erforderliche Rolle:

- sn_escm_sh.Shift_admin
- sn_si.admin erbt die Rolle sn_escm_sh.Shift_admin

Warum und wann dieser Vorgang ausgeführt wird

Zum Konfigurieren einer Schichtübergabevorlage erstellt der Administrator entweder eine neue Schichtübergabevorlage oder öffnet eine vorhandene Vorlage im Basissystem mit dem Namen **Beispiel Für Schichtvorlage** Und ändert die Details und Abschnitte entsprechend Ihren Anforderungen.

Der Schichtbesitzer kann die konfigurierte Vorlage verwenden, um Protokolldatensätze für die Schichtübergabe zu erstellen. Dann wird der Schichtübergabebericht für den nächsten aktiven Schichtbesitzer und das nächste Team freigegeben.

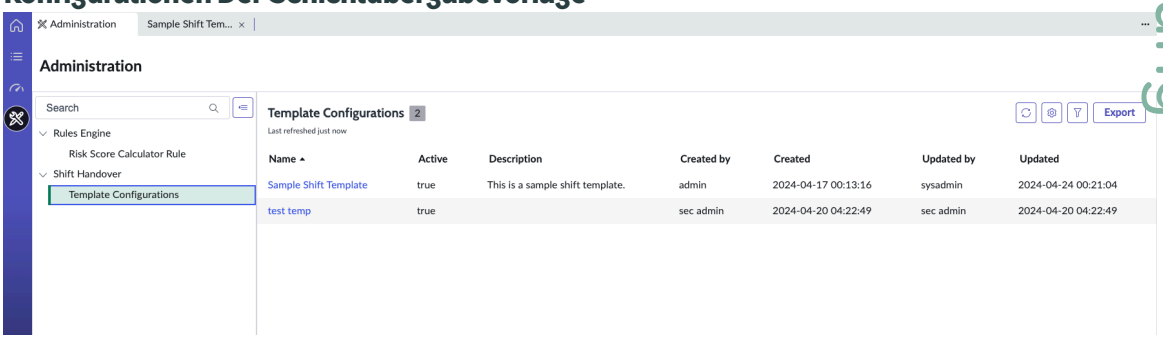
Hinweis:
Nur die aktiven Schichtübergabevorlagen sind für den Schichtbesitzer sichtbar, um Übergabeprotokolldatensätze zu erstellen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Administration**an.
2. Navigieren zu **Schichtübergabe** > **Vorlagenkonfigurationen**an.
   Die Seite Vorlagenkonfigurationen wird angezeigt.

   Hinweis:
   Als Teil des Basissystems erhalten Sie eine vordefinierte Vorlagenkonfiguration für die Schichtübergabe zum Anzeigen, Bearbeiten oder Ändern der Schichtübergabevorlage. Sie können die vordefinierte Vorlagenkonfiguration für die Schichtübergabe jedoch nicht erstellen oder löschen.

Konfigurationen Der Schichtübergabevorlage



3. Um eine neue Schichtübergabevorlage zu erstellen, wählen Sie aus **Neu** .
4. Füllen Sie die Felder im Formular „Details“ aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine neue Schichtübergabevorlage

Feld	Beschreibung
Name	Name der Schichtübergabevorlage. Beispiel: SIR-Vorlage.
Anwendung	Name der Anwendung, für die Sie die Schichtübergabevorlage erstellen. Beispiel: Security Incident Response-Arbeitsbereich.
Aktiv	Option, um anzugeben, ob die Schichtübergabevorlage aktiv ist. Aktivieren Sie diese Option, um die Schichtübergabevorlage zu aktivieren.
Beschreibung	Beschreibung der Schichtübergabevorlage.
Konfiguration der Datensatzerwähnung	Verwenden Sie dieses Feld, um die Datensatzerwähnungsdetails des Rich-Text-Editors (RTE) zu konfigurieren. Die Eingabe ist ein Array von JSON-Objekten mit den folgenden Feldern: ○ *`SourceTable`* : Name der Quelltabelle. ○ *`Bezeichnung`* : Name der anzuzeigenden Bezeichnung. ○ *`FilterCondition`* : Codierte Abfrage zum Filtern. Sie können mehrere Abfragen für dieselbe Tabelle hinzufügen, um die Werte dynamisch abzurufen. Dieser Wert wird aktualisiert, wenn der Schichtübergabedatensatz veröffentlicht wird oder basierend auf dem Startdatum oder/und Enddatum der Schicht. Beispiel: Anzahl der Security Incident-Datensätze nach Priorität, Anzahl der Security Incident-Datensätze nach Status. Sie können die Argumente {Start_date} und {end_date} in der Abfrage verwenden, um einen Datumsbereich anzugeben. Beispiel: „FilterCondition“: „Active=true^sys_created_on>=${Start_date}^sys_created_on<=${end_date}“ ○ *`Felder`* : Wählen Sie die Felder aus, um das Muster abzufragen. Beispielkonfiguration, die Sie kopieren und in das Konfigurationsfeld Datensatzerwähnung einfügen können. `[ { "sourceTable": "incident", "label": "Incidents active", "filterCondition": "active=true", "fields": [ "number" ] } { "sourceTable": "incident",`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung

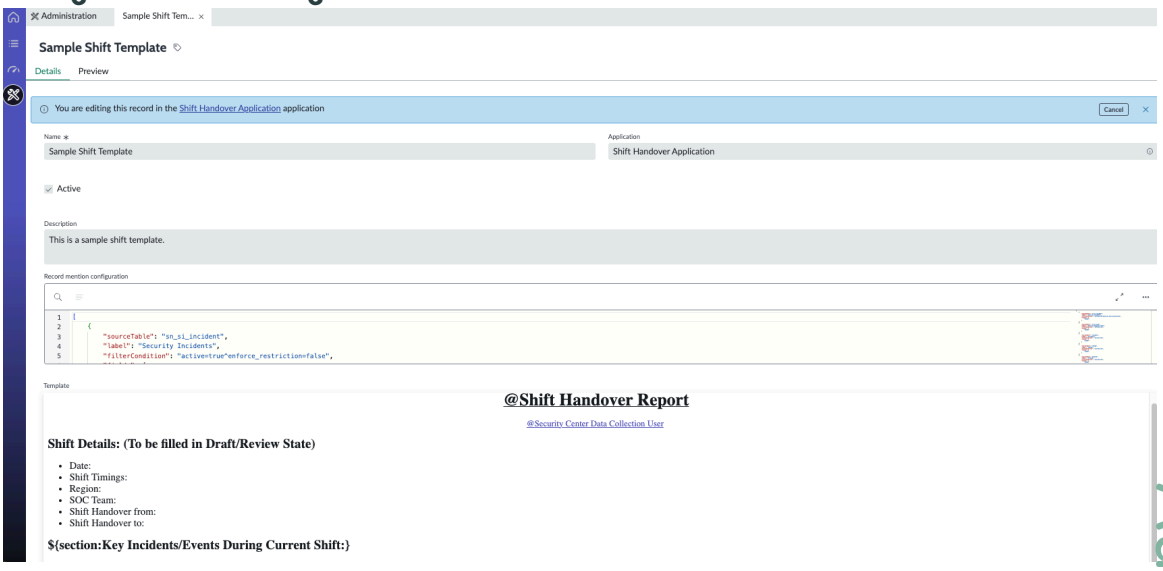
	<pre>"label": "Active incidents created after selected date",
	"filterCondition": "active=true^sys_created_on>=${start_date}",
	"fields": [
	"number"
	]
	}
	]</pre>
	Verwenden Sie zum Kopieren der Beispielkonfiguration **In Zwischenablage kopieren** Aktion im Bereich „kontextbezogene Unterstützung“. Anschließend können Sie basierend auf Ihren Anforderungen zusätzliche Änderungen vornehmen.

Vorlage	Erstellen Sie mithilfe von Abschnitten eine Schichtübergabevorlage. Stellen Sie sicher, dass mindestens ein Abschnitt vorhanden ist, in dem die Analysten basierend auf der Vorlage zu den Protokolldatensätzen der Schichtübergabe beitragen können.
	
	Die Vorlage kann statischen Text, Bilder usw. in den entsprechenden Abschnitten enthalten. Sie können Bilder direkt im Feld Vorlage kopieren und einfügen. Sie können Abschnitte in der Vorlage mit dem folgenden Code erstellen:
	<pre>${section:Section Label}</pre>
	Beispiel:
	<pre>${section:Key Incidents/Events During Current Shift}
	${section:Incidents/Events to Monitor or Follow Up}
	${section:System/Infrastructure Updates}
	${section:Next Steps for Incoming Shift}
	${section:References}</pre>
	Hinweis:
	Weitere Informationen finden Sie unter **Kontextbezogene Unterstützung** Im rechten Bereich.

5. Um eine vorhandene Schichtübergabevorlage zu verwenden und zu ändern, wählen Sie aus **Beispiel Für Schichtvorlage** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

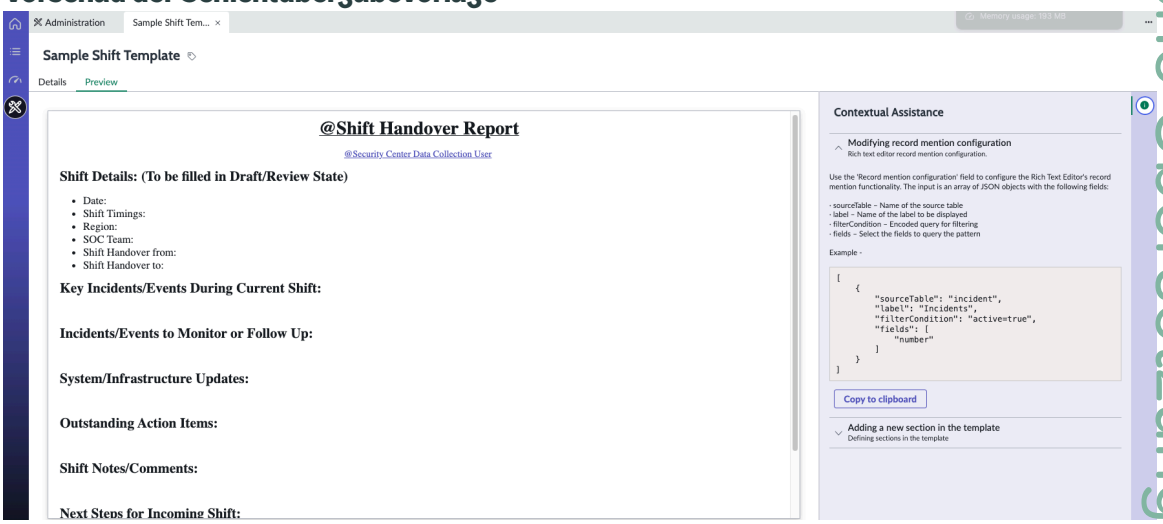
Vorlage für Schichtübergabe



6. Aktualisieren Sie die Vorlage für die Schichtübergabe entsprechend Ihren Anforderungen.
7. Wählen Sie Aus **Vorschau** Dient zum Anzeigen der Laufzeitvorschau der Schichtübergabevorlage.

   Der Bericht generiert eine Vorschau basierend auf der Konfiguration der Schichtübergabevorlage.

Vorschau der Schichtübergabevorlage



8. Wählen Sie Aus **Speichern** Zum Speichern der Schichtübergabevorlage.

Nächste Maßnahme

Informationen zum Verwalten von Schichtübergabedatensätzen in der Listenansicht und zum Ausführen von Aktionen wie Erstellen, Bearbeiten, Kopieren oder Löschen von Schichtübergabedatensätzen finden Sie unter Verwalten Sie Schichtübergabedatensätze.

Erstellen S Verschiebungen Bis Arbeitsbereich für Security Incident Response

Erstellen Sie Schichten Über Arbeitsbereich für Security Incident Response Bis Verwenden Beim Konfigurieren S Verschiebung H andover R Ekorde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

- sn_escm_sh.Shift_admin
- sn_si.admin erbt die Rolle sn_escm_sh.Shift_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Administration**an.
2. Navigieren zu **Schichtübergabe** > **Schichtkonfigurationen**an.
   Auf der Seite Schichtzeitkonfiguration werden alle vorhandenen Schichten angezeigt.
3. Wählen Sie **Neu**.
4. Geben Sie einen Namen ein In Die **Schicht** Feld .
5. Geben Sie An Start- und Endzeiten für die Schicht in Die **Startzeit** Und **Endzeit** Felder .

   Hinweis:
   Die Startzeit und die Endzeit sind in Die Aktuelle Anwender Konfiguriert Zeitzone .

6. Wählen Sie **Speichern**.

Security Incident Response c Onferenz c Alle Integration

Die Security Incident Response Mit der Integration von Telefonkonferenzen können Sie Telefonkonferenzen und Chats für Analysten, Manager und betroffene Anwender verwalten und initiieren.

Mit Security Incident Response Mit der Funktion „Telefonkonferenz“ können Sie mit Kunden und Peer-Mitarbeitern zusammenarbeiten, um Security Incidents während eines Anrufs zu lösen. Sie können auch über einen Gruppenchat zusammenarbeiten.

Sie können Telefonkonferenzen über Kommunikationskanäle von Drittparteien wie Microsoft Teams, Cisco Webex oder Zoom-Meetings initiieren. Um über Chat zusammenzuarbeiten, verwenden Sie den Sidebar-Chat der SIR-Anwendung.

Schlüsselfunktionen

Die Security Incident Response Call Collaboration bietet die folgenden wichtigen Funktionen:

- SIR-Manager/Analysten können eine Microsoft Teams-, Cisco Webex- oder Zoom-Telefonkonferenz direkt aus dem Security Incident initiieren.
- SIR-Manager/Analysten können einen Chat direkt über die SIR-Anwendung initiieren.
- Laden Sie zusätzliche Teilnehmer zum Anruf oder Chat ein.
- Zeigen Sie Anrufaufzeichnungen und Chat-Details an.
- Senden Sie Einladungen an Teilnehmer per E-Mail und Microsoft Teams-Chat.

Verwalten Sie Benutzer und Gruppen von Telefonkonferenzen

Der Administrator kann Einstellungen für Telefonkonferenzen konfigurieren, um eine vordefinierte Liste von Anwendern und Gruppen anzuzeigen, die einem Anruf hinzugefügt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response-Arbeitsbereiche** > **Administration**an.
2. Wählen Sie Aus **Telefonkonferenz** , Und dann **Anrufkonfiguration** .
3. Wählen Sie auf der Seite „Anrufkonfigurationen“ die Option aus **Konfiguration Der Telefonkonferenz** . Die Konfigurationsseite wird angezeigt, um eine vordefinierte Liste von Anwendern und Gruppen zu konfigurieren.
4. Füllen Sie die Felder im Formular „Details“ aus.

Feld	Beschreibung
Name	Name der Telefonkonferenzkonfiguration.
Anwender automatisch ausfüllen	Option zum automatischen Ausfüllen der konfigurierten Anwender für eine Telefonkonferenz. Wenn Sie diese Option auswählen, werden die konfigurierten Anwender und Gruppen zu einer Telefonkonferenz hinzugefügt. **Hinweis:** Sie können auch beim Initiieren eines Anrufs Anwender/Gruppen hinzufügen oder entfernen.
Betroffene Anwender anzeigen	Option zum Anzeigen der betroffenen Anwender zum Hinzufügen zu einem Anruf.
Zuweisungsgruppenanwender anzeigen	Option zum Anzeigen der Zuweisungsgruppenanwender zum Hinzufügen zu einem Anruf.
Standardgruppen	Option zum Hinzufügen von Standardgruppen zum Hinzufügen zu einem Anruf.
Standardanwender	Option zum Hinzufügen von Standardanwendern zum Hinzufügen zu einem Anruf.

5. Wählen Sie Aus **Speichern** Zum Speichern der Telefonkonferenzkonfiguration.

Integrieren Sie SIR in Kommunikationskanäle von Drittanbietern

Die SIR-Telefonkonferenz-Integration mit Kommunikationskanälen von Drittparteien wie Microsoft Teams, Zoom und Cisco Webex ermöglicht Ihnen die Verwaltung und Initiierung eines Anrufs direkt aus einem Security Incident.

Schlüsselfunktionen

- Starten und beenden Sie Telefonkonferenzen direkt aus einem Security Incident.
- Fügen Sie Teilnehmer an einer Telefonkonferenz hinzu oder entfernen Sie sie.
- Verfolgen und melden Sie Besprechungsdetails wie Besprechungsdauer und Teilnehmer zur weiteren Analyse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Überprüfen Sie, ob Sie die folgenden Integration Hub-Plugins in Ihrer ServiceNow-Instanz installiert haben.

- Notify-Plugin (com.snc.notify). Weitere Informationen finden Sie unterConfiguring Notify
- Notify-UI-Komponenten für konfigurierbare Arbeitsbereiche
- Für die Integration von Microsoft Teams als Kommunikationskanal:
  - Plugin „Microsoft Teams Communications-Spoke“ (sn_msteams_com_spk).
  - Plugin „Azure Active Directory-Anwenderzuordnung“ (sn_now_Azure).
- Für die Integration von Zoom als Kommunikationskanal:
  - Zoom-Spoke (sn_Zoom_Spoke)
  - Notify Zoom (sn_Notify_Zoom)
- Zur Integration von Cisco Webex als Kommunikationskanal:
  - Notify Cisco Webex Connector (sn_Notify_webex)
  - Cisco Webex Teams-Spoke (sn_cisco_Teams_spk)

Weitere Informationen finden Sie unter Request Integration Hub .

Konfiguration

Führen Sie die folgende Konfiguration für die Kommunikationskanäle durch, die Sie verwenden möchten:

- Informationen zum Konfigurieren der Cisco Webex-Integration für Telefonkonferenzen über den Kommunikationskanal Notify finden Sie unter Configure Notify Cisco Webex Connector .
- Informationen zum Konfigurieren der Zoom-Integration für Telefonkonferenzen über den Notify-Kommunikationskanal finden Sie unter Configure Notify Zoom connector in Notify .
- Informationen zum Konfigurieren der Microsoft Teams-Integration für Telefonkonferenzen mit der vorkonfigurierten App finden Sie unter Integrate Notify connector pre-published app with Microsoft Teams .
- Informationen zum Konfigurieren der Microsoft Teams-Integration für Telefonkonferenzen mit der selbst konfigurierten App finden Sie unter Integrating Notify connector self-configured app with Microsoft Teams .

Konfigurieren Sie Berichtsvorlagen in Security Incident Response

Sie können Berichtsvorlagen erstellen, die zum Generieren einer Incident-Zusammenfassung oder einer Kurzübersicht zur Analyse und Freigabe verwendet werden können.

Verwenden Security Incident Response Berichtsvorlagen-Funktion zum Erstellen von Berichtsvorlagen zum Generieren von Berichten, die eine Zusammenfassung auf Analystenebene oder auf Führungsebene eines Incident bereitstellen. Sie können den Bericht basierend auf Ihren Anforderungen mithilfe verschiedener Incident-Felder formatieren und konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Tabelle werden die Berichtsvorlagen erläutert, die im Basissystem bereitgestellt werden.

Berichtsvorlagen in Security Incident Response

Name	Beschreibung
Status-Reporting durch Analysten	Stellt für einen Analysten vollständige Informationen zu einem Security Incident bereit.
Kurzübersicht	Bietet eine Übersicht über den Status eines Security Incidents für das Management.

Hinweis:
Standardmäßig befinden sich diese Berichte im Entwurfsstatus und im schreibgeschützten Modus. Sie müssen diese Standardvorlagen wiederverwenden, um Berichtsvorlagen zu erstellen und zu veröffentlichen.

Erstellen Sie eine Berichtsvorlage in Security Incident Response

Erstellen Sie eine neue Berichtsvorlage für die Zusammenfassung von Analysten oder eine Zusammenfassung für einen Incident.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response-Arbeitsbereiche** > **Administration**an.
2. Wählen Sie Aus **Berichte** , Und dann **Berichtsvorlagen** .
   Die Seite „Berichtsvorlagen“ wird mit allen im Basissystem verfügbaren Vorlagen angezeigt.
3. Wählen Sie **Neu**.
   Zeigt an **Details** Seite der Vorlage.
4. Geben Sie den Namen und die Beschreibung der Vorlage ein.
5. Wählen Sie **Speichern**.
6. Wählen Sie Aus **Inhalt** Registerkarte.
   Zeigt die Inhaltsseite der Vorlage mit einem leeren Bericht an.
7. Wählen Sie Aus **Erweitern Sie** Und fügen Sie die gewünschten Felder in den Vorlagentext ein.
   - **Allgemeine SIR-Felder** : Die Liste der am häufigsten verwendeten Felder für einen Incident.
   - **Alle SIR-Felder** : Alle Felder im Zusammenhang mit einem Incident. Wenn Sie beispielsweise einen Incident-Bericht generieren und ein Feld mit der Bezeichnung Kurzbeschreibung hinzufügen möchten, können Sie dieses Feld aus den Feldern alle SIR auswählen. Das Feld Kurzbeschreibung wird der Berichtsvorlage als Variable hinzugefügt. Wenn Sie einen Bericht für den Analysten generieren, wird die Kurzbeschreibung des Incident im Bericht angezeigt.
   - **Zugehörige Datensätze** : Die zugehörigen Datensätze eines bestimmten Incident. Wenn Sie dem Bericht beispielsweise zugeordnete erkennbare Elemente hinzufügen möchten, können Sie sie Ihrer Berichtsvorlage hinzufügen. Diese zugehörigen Datensätze werden im Tabellenformat angezeigt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Skripts** : Um das Datum und die Uhrzeit des Berichts hinzuzufügen, können Sie Ihrer Berichtsvorlage das Skript „Aktuelles Datum/Uhrzeit“ hinzufügen. Dadurch werden Datum und Uhrzeit der Berichterstellung im Bericht hinzugefügt.
-

8. Wählen Sie Aus **Inhalt Speichern** Um den Inhalt Ihrer Berichtsvorlage zu speichern.
9. Wählen Sie Aus **Vorschau** Um eine Vorschau Ihres Berichtsformats anzuzeigen.

   Nachdem Sie Ihrer Berichtsvorlage alle erforderlichen Felder hinzugefügt haben, müssen Sie Ihre Berichtsvorlage veröffentlichen.
10. Wählen Sie Aus **Veröffentlichen** Um die Vorlage zu veröffentlichen.

    Es wird eine Bestätigungsnachricht angezeigt, ob Sie die Berichtsvorlage veröffentlichen möchten.
11. **Wahlweise:** Wählen Sie aus **Weitere Aktionen** Symbol und wählen Sie dann aus **Löschen** Zum Löschen der Berichtsvorlage.

Systemeigenschaften für Berichte

Die Systemeigenschaften für Security Incident Response Berichte werden unten erläutert.

Systemeigenschaften für Berichte

Eigenschaft	Beschreibung	Wert
sn_si.sn_si_Incident.load_all_Records	Lädt alle Datensätze für die Listen im Bericht, die aus einer Vorlage erstellt wurden. „true“ – lädt alle Datensätze; „false“ – lädt eine bestimmte Anzahl von Datensätzen, die durch die Eigenschaft „sn_si.sn_si_incident.reporting_list_records_count“ definiert ist.	Falsch
sn_si.sn_si_Incident.max_list_columns_shown	Beschränken Sie die Anzahl der Spalten, die beim Rendern von Listen in Berichts-pdfs hinzugefügt werden können. Dadurch werden die Spalten vom Anfang der Ansicht bis zum zulässigen Grenzwert verwendet.	5
sn_si.sn_si_Incident.Report_default_style_object	Verwenden Sie diese Eigenschaft, um die CSS von freien Formfeldern, dem linken Bereich und der Berichtslisten zu steuern.	(JSON-Objekt)
sn_si.sn_si_Incident.Reporting_list_Records_count	Lädt eine bestimmte Anzahl von Datensätzen im Berichtseditor.	200
sn_si_Reporting_email_template_sn_si_Incident	SYS_ID der E-Mail-Client-Vorlage für die SIR-Tabelle (sn_si_Incident), die im freigegebenen Bericht verwendet wird.	9ce97ae643461210416896ed3ab8f258

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaften für Berichte (Fortsetzung)

Eigenschaft	Beschreibung	Wert
sn_si.sn_si_Incident.ctx_menu_field_header	Feldheader	sn_si_Incident_Report_field_Header,sn_si_Incident_R
sn_si.sn_si_incident.defang_record_list_urls	Steuert, ob die URLs aus der Liste deaktiviert werden oder nicht.	Falsch
sn_si.sn_si_Incident.Reporting_dot_Walk_Tables	Liste der Tabellen, die für Dot-Walking in Berichten verfügbar sind.	(JSON-Objekt)

Duplizieren Sie eine Berichtsvorlage in Security Incident Response

Duplizieren Sie eine Berichtsvorlage, um eine vorhandene Vorlage zu bearbeiten oder wiederzuverwenden, um eine neue Vorlage zu erstellen.

Vorbereitungen

Hinweis:
Sie müssen eine Kopie der Vorlagen „Kurzzusammenfassung“ und „Statusberichte für Analysten“ erstellen, um sie wiederzuverwenden.

Um die Kurzzusammenfassung und die Statusberichte für Analysten wiederzuverwenden, müssen Sie eine Kopie dieser erstellen und dann

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response-Arbeitsbereiche** > **Administration**an.
2. Wählen Sie Aus **Berichte** , Und dann **Berichtsvorlagen** .
   Die Seite „Berichtsvorlagen“ wird mit allen im Basissystem verfügbaren Vorlagen angezeigt.
3. Wählen Sie die Vorlage aus.
4. Wählen Sie Aus **Duplikat** .

Ergebnisse

Der Inhalt der ausgewählten Vorlage wird dupliziert, und eine Kopie der ausgewählten Vorlage ist in der Liste der Vorlagen verfügbar. Die doppelte Vorlage befindet sich im Status Entwurf. Sie können den Inhalt anpassen und die Vorlage dann nach Bedarf umbenennen.

Nächste Maßnahme

Bearbeiten Sie eine Berichtsvorlage in Security Incident Response

Bearbeiten Sie eine Berichtsvorlage in Security Incident Response

Bearbeiten Sie eine Berichtsvorlage, um eine vorhandene Vorlage wiederzuverwenden, um eine neue Vorlage zu erstellen.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response-Arbeitsbereiche** > **Administration**an.
2. Wählen Sie Aus **Berichte** , Und dann **Berichtsvorlagen** .
   Die Seite „Berichtsvorlagen“ wird mit allen im Basissystem verfügbaren Vorlagen angezeigt.
3. Wählen Sie die Vorlage aus.
   Zeigt an **Details** Registerkarte der Vorlage im Bearbeitungsmodus.
4. Aktualisieren Sie den Namen und die Beschreibung der Vorlage.
5. Wählen Sie **Speichern**.
6. Wählen Sie Aus **Inhalt** Registerkarte.
   Zeigt die Inhaltsseite der Vorlage mit einem leeren Bericht an.
7. Wählen Sie Aus **Erweitern Sie** Und fügen Sie die gewünschten Felder ein/entfernen Sie sie.
   - **Allgemeine SIR-Felder** : Die Liste der am häufigsten verwendeten Felder für einen Incident.
   - **Alle SIR-Felder** : Alle Felder im Zusammenhang mit einem Incident. Wenn Sie beispielsweise einen Incident-Bericht generieren und ein Feld mit der Bezeichnung Kurzbeschreibung hinzufügen möchten, können Sie dieses Feld aus den Feldern alle SIR auswählen. Das Feld Kurzbeschreibung wird der Berichtsvorlage als Variable hinzugefügt. Wenn Sie einen Bericht für den Analysten generieren, wird die Kurzbeschreibung des Incident im Bericht angezeigt.
   - **Zugehörige Datensätze** : Die zugehörigen Datensätze eines bestimmten Incident. Wenn Sie dem Bericht beispielsweise zugeordnete erkennbare Elemente hinzufügen möchten, können Sie sie Ihrer Berichtsvorlage hinzufügen. Diese zugehörigen Datensätze werden im Tabellenformat angezeigt
   - **Skripts** : Um das Datum und die Uhrzeit des Berichts hinzuzufügen, können Sie Ihrer Berichtsvorlage das Skript „Aktuelles Datum/Uhrzeit“ hinzufügen. Dadurch werden Datum und Uhrzeit der Berichterstellung im Bericht hinzugefügt.
8. Wählen Sie Aus **Inhalt Speichern** Um den Inhalt Ihrer Berichtsvorlage zu speichern.
9. Wählen Sie Aus **Vorschau** Um eine Vorschau Ihres Berichtsformats anzuzeigen.

   Nachdem Sie Ihrer Berichtsvorlage alle erforderlichen Felder hinzugefügt haben, müssen Sie Ihre Berichtsvorlage veröffentlichen.
10. Wählen Sie Aus **Veröffentlichen** Um die Vorlage zu veröffentlichen.

    Es wird eine Bestätigungsnachricht angezeigt, ob Sie die Berichtsvorlage veröffentlichen möchten.

Bereitschaftsplanung in Security Incident Response

Verwenden Sie die Bereitschaftsplanung in Security Incident Response Zum Anzeigen und Verwalten von Schichten für Ihre Analysten.

Mit der Funktion „Bereitschaftsplanung“ können Sie Schichten anzeigen und verwalten sowie Abwesenheitsanträge genehmigen oder ablehnen. Sie können auch Benachrichtigungseinstellungen, Zustellkanäle, Eskalationsauslöserregeln und Richtlinien für Ihre Gruppe verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtige Funktionen für sn_si.Manager/Rota_Manager

- Zeigen Sie den Bereitschaftszeitplan an (einschließlich Lücken und Urlaubsanträge für Ihre Gruppe).
- Genehmigen oder lehnen Sie Auszeitanträge ab.
- Prüfen und beheben Sie Lücken und Konflikte.
- Stellen Sie Abdeckung (Vertretungen) bereit, bzw. ersetzen oder löschen Sie sie, und löschen Sie Urlaubsanträge.
- Erstellen Sie eine Schicht, und fügen Sie ihr Mitglieder hinzu, bzw. löschen Sie sie.
- Zeigen Sie Eskalations-, Gruppen- und Leistungsberichte an.

Wichtige Funktionen für sn_si.Analyst/oc_read

- Zeigen Sie Bereitschaftszeitpläne und die anderen Mitglieder Ihrer Schicht an.
- Übermitteln Sie Urlaubsanträge, und empfehlen Sie ein anderes Mitglied der Gruppe, das Ihre Schicht übernehmen kann.
- Geben Sie Ihre Verfügbarkeit und Ihre bevorzugten Kontaktmethoden an.
- Zeigen Sie die Mitglieder und Eskalationsdetails für eine Schicht an.

Dokumentation zur Bereitschaftsplanung

Detaillierte Informationen zum Konfigurieren und Verwenden von Funktionen zur Bereitschaftsplanung finden Sie unter IT Service Management On-Call Scheduling Dokumentation.

SIR-Arbeitsbereich verwenden

Sicherheitsanalysten und -Manager verwenden SIR-Arbeitsbereich Um tägliche Vorgänge mit einer verbesserten Anwender-Experience durchzuführen, führen Sie eine Incident-Untersuchung durch, und erhalten Sie einen Überblick.

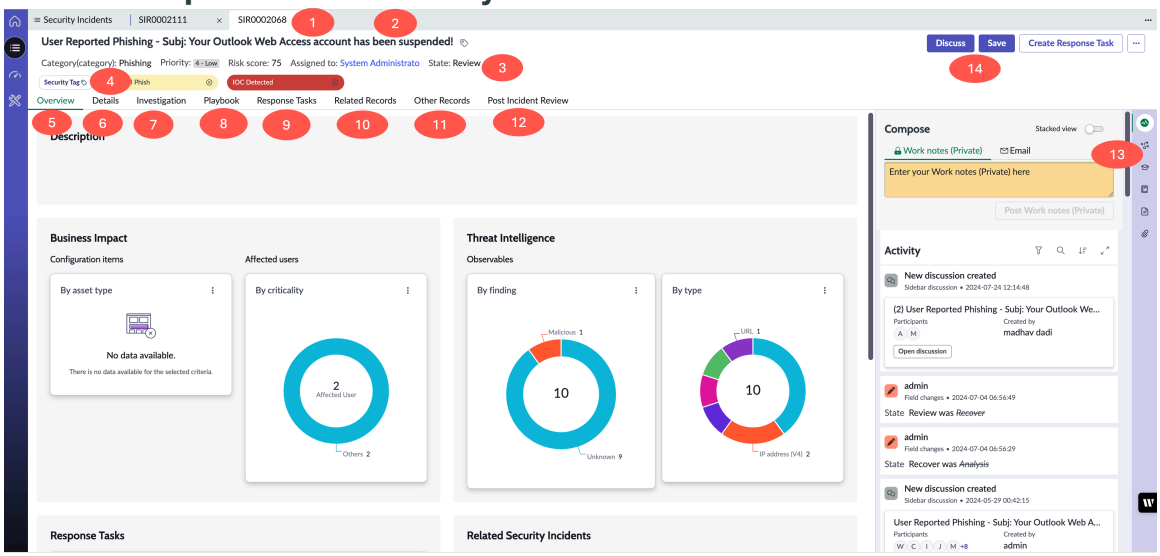
Arbeiten mit Security Incident-Datensätzen

Der Security Incident-Datensatz besteht aus folgenden Elementen.

Schlüsselkomponenten, die in einem Security Incident-Datensatz verfügbar sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselkomponenten eines Security Incidents



Anzahl	Name	Beschreibung
1	Security Incident-Nummer	Die Security Incident-Nummer ist für den Registerkartennamen verfügbar.
2	Kurzbeschreibung	Kurzbeschreibung des Security Incidents, die über dem Formularbanner angezeigt wird.
3	Formularbanner	Dies ist ein schreibgeschützter Abschnitt, der die Schlüsselfelder wie Kategorie, Priorität, Risikopunktzahl, Status und die Incident-Zuweisungsdetails enthält. **Hinweis:** Die regulären Plattform-Tags können auch hier angewendet werden.
4	Sicherheits-Tags	Zeigt die Sicherheits-Tags an, die einem Security Incident zugeordnet sind.
5	Übersicht	Bietet eine Snapshot-Übersicht über den Security Incident, z. B. Beschreibung, Geschäftsauswirkung mit Asset-Details nach Typ, Betroffene Anwender nach Relevanz, Threat Intelligence-Elemente, die aus erkennbaren Elementen nach Ergebnis und Typ bestehen, Antwortaufgaben, zugehörige Security Incidents, die aus untergeordneten Security Incidents und ähnlichen Security Incidents bestehen.
6	Details	Auf der Registerkarte „Details“ wird das Security Incident-Formular angezeigt.
7	Ermittlung	Auf der Registerkarte „Untersuchung“ wird die Experience für Incident-Untersuchungen angezeigt.
8	Playbook	Playbook wird über den Prozessautomatisierungs-Designer (PAD) ausgelöst. Wenn ein Prozess erstellt wird und die Auslöserbedingung so festgelegt ist, dass das Playbook für einen Security Incident ausgelöst wird. Dann wird ein Playbook angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzahl	Name	Beschreibung
9	Antwortaufgaben	Die Antwortaufgaben erfassen alle Antwortaufgaben, die einem Security Incident zugeordnet sind.
10	Zugehörige Datensätze	Die Registerkarte zugehörige Datensätze besteht aus allen zugehörigen Listen aus der klassischen Anwenderoberfläche in diesem Abschnitt. Die zugehörigen Listen sind in verschiedenen Abschnitten wie Geschäftsauswirkung, bedrohungsinformationen usw. gruppiert, um die Navigation zu erleichtern.
11	Andere Datensätze	Die Registerkarte „andere Datensätze“ besteht aus IT-Datensätzen wie Change-Anforderungen, Incidents und E-Mails, die in diesem Abschnitt gruppiert und angezeigt werden.
12	Registerkarte „Überprüfung nach Incident“	Wenn der Security Incident in den Status „Überprüfung“ übergeht, wird die Registerkarte Überprüfung nach Incident mit den Bewertungen und Berichten nach Incident auf der Registerkarte angezeigt.
13	Kontextmenü	Bietet einfachen Zugriff auf die Schnellaktionen und ist auf allen Registerkarten verfügbar, auf die Analysten bei Bedarf zugreifen können. Das Kontextmenü bietet eine einfache Navigation zu mehreren Ressourcen, z. B.: **1.** Aktivitätenstrom **2.** Playbook **3.** Analyst Assist **4.** Runbook **5.** Vorlagen **6.** Anhänge
14	Formular-UI-Aktionen	Die verschiedenen UI-Aktionen des Security Incident-Formulars werden oben rechts im Incident-Formular angezeigt. Die verfügbaren Formular-UI-Aktionen sind: • Diskutieren • Speichern • Antwortaufgabe erstellen • E-Mail erstellen • Playbook hinzufügen • Verknüpfte(n) Workflow(s) öffnen • Incident erstellen • Problem erstellen • Change-Anforderung erstellen • Ausfall erstellen • Schweregrad berechnen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzahl	Name	Beschreibung
		• Verknüpfen mit Major Security Incident • Vorschlagen als Major Security Incident • Heraufstufen zu Major Security Incident • Zusätzliche Aktion(en) für Endpunkt ausführen • MITRE ATT&CK-Technik zuordnen • Zu klassischer UI wechseln • Dem Sicherheitsfall hinzufügen • Löschen Weitere Informationen finden Sie unter Arbeiten mit Formular-UI-Aktionen.

Abschnitt „Security Incident-Übersicht“

Der Abschnitt „Übersicht“ im Arbeitsbereich enthält die wichtigsten Informationen, die dem Security Incident zugeordnet sind.

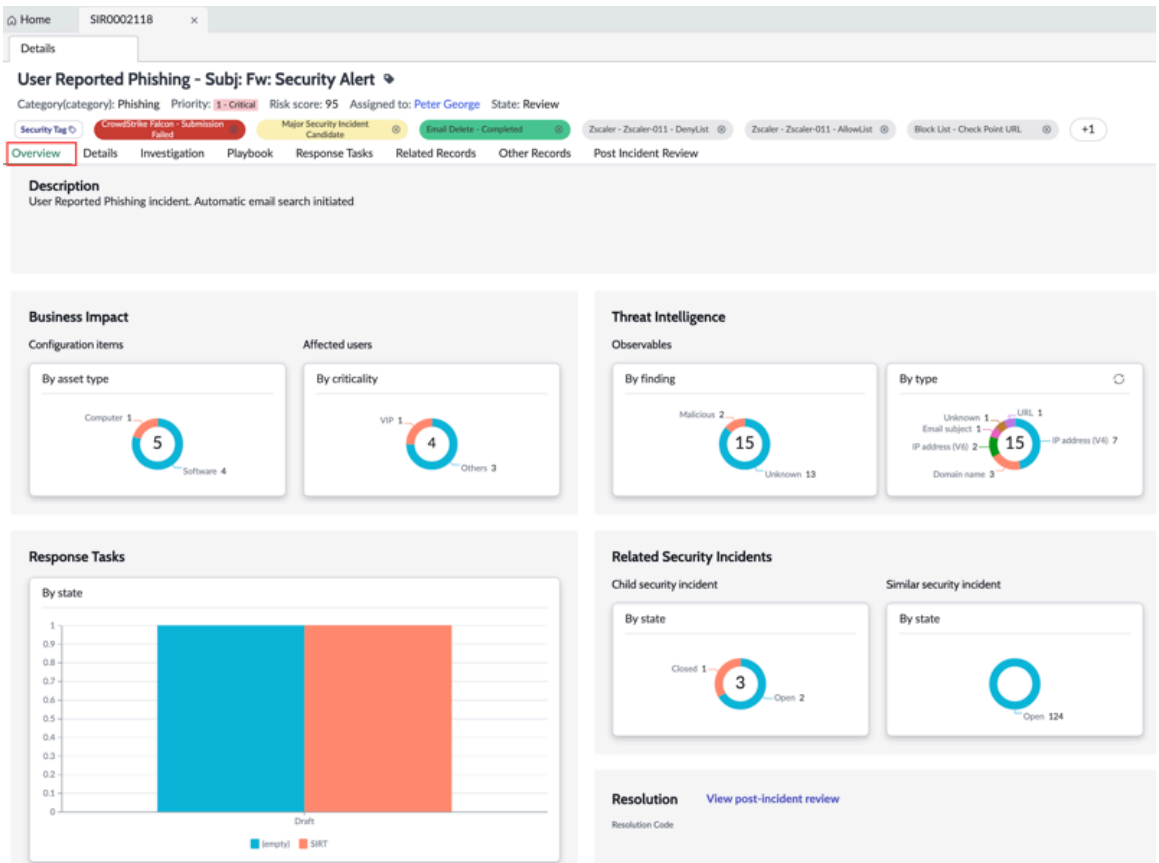
Die Ringdiagramme sind Drilldown aktiviert. Wenn ein Analyst eines der Diagrammelemente auswählt, navigiert er Sie zum entsprechenden Datensatz mit einer gefilterten Listenansicht von Elementen auf der entsprechenden Registerkarte. Beispiel: Wenn **Schädliche Erkennbare Elemente** Ist ausgewählt, gelangen Sie zu den erkennbaren Elementen mit einer gefilterten Listenansicht schädlicher erkennbarer Elemente auf der **Zugehörige Datensätze** Registerkarte.

Im Abschnitt Übersicht wird Folgendes angezeigt:

- Beschreibung des Security Incidents.
- Geschäftsauswirkungsdetails wie Konfigurationselemente nach Asset-Typ und betroffene Anwender nach Relevanz – ob VIP-Anwender oder andere Anwender.
- Threat Intelligence-Elemente wie erkennbare Elemente, indem ermittelt wird, ob die erkennbaren Elemente oder böswillig oder unbekannt sind, und nach Typ.
- Antwortaufgaben nach Status und Zuweisungsgruppe.
- Zugehörige Security Incidents mit untergeordneten Security Incidents nach Status – ob offen oder Geschlossen, und ähnlichen Security Incidents nach Status – ob offen oder Geschlossen.
- Der Abschnitt „Lösung“ wird angezeigt, wenn ein Incident in den Status „Überprüfen“ wechselt. Der Abschnitt „Lösung“ wird in angezeigt **Übersicht** Abschnitt mit der Möglichkeit, die Überprüfung nach dem Incident anzuzeigen.
- Lösung – Überprüfung nach Incident anzeigen: Wählen Sie den Link aus, um zu navigieren **Überprüfung nach Incident** Seite.
- Nachdem der Incident geschlossen wurde, werden im Abschnitt „Lösung“ der Lösungscode, die Lösungshinweise und der gelöst von (Anwender) zusammen mit den Details zur Überprüfung nach dem Incident angezeigt.
- Initialen aller Anwender, die derzeit auf denselben Incident zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersichtsbereich



Security Incident Abschnitt „Details“

In diesem Abschnitt werden die Formularfelder für Security Incidents angezeigt, die über die klassische UI für Security Incidents gerendert werden.

Die klassische UI hat eine Ansicht namens **SIRW** Ansicht erstellt. Diese Ansicht ist dem zugeordnet **Details** Registerkarte im neuen Arbeitsbereich. Alle erforderlichen Anpassungen müssen in dieser Ansicht implementiert werden.

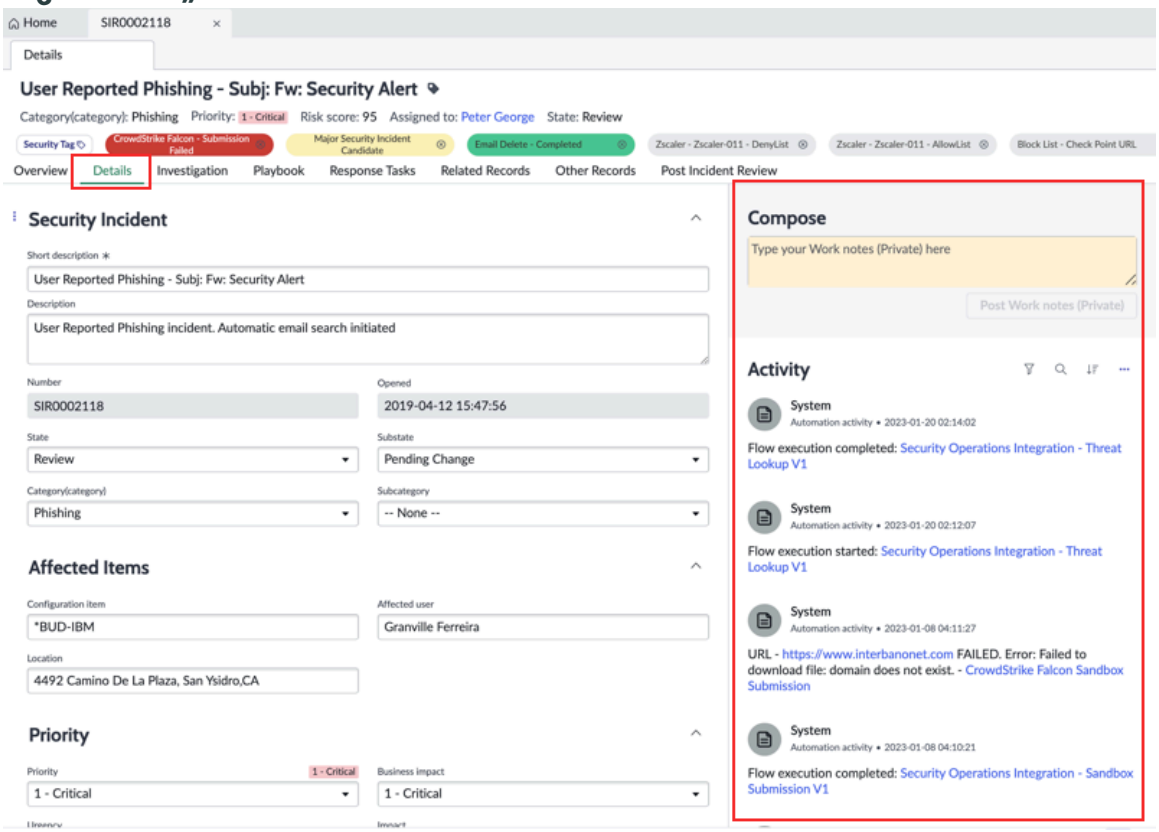
Die Formularfelder sind in die folgenden Abschnitte gruppiert und werden in der Formularansicht der Registerkarte „Details“ angezeigt. Klicken Sie auf einen der Abschnitte, oder wechseln Sie zum entsprechenden Abschnitt im Formular:

- Security Incident
- Priorität
- Quelle
- Übergeordnet
- Zuweisung
- Zugriffssteuerungen
- Betroffene Elemente
- Lösung

Die **Details** Registerkarte enthält **Aktivität** Stream-Abschnitt im Detailformular selbst für schnellen Zugriff auf die Sicherheitsanalysten, um Kommentare hinzuzufügen und zu veröffentlichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Details“ und Aktivitätenstrom

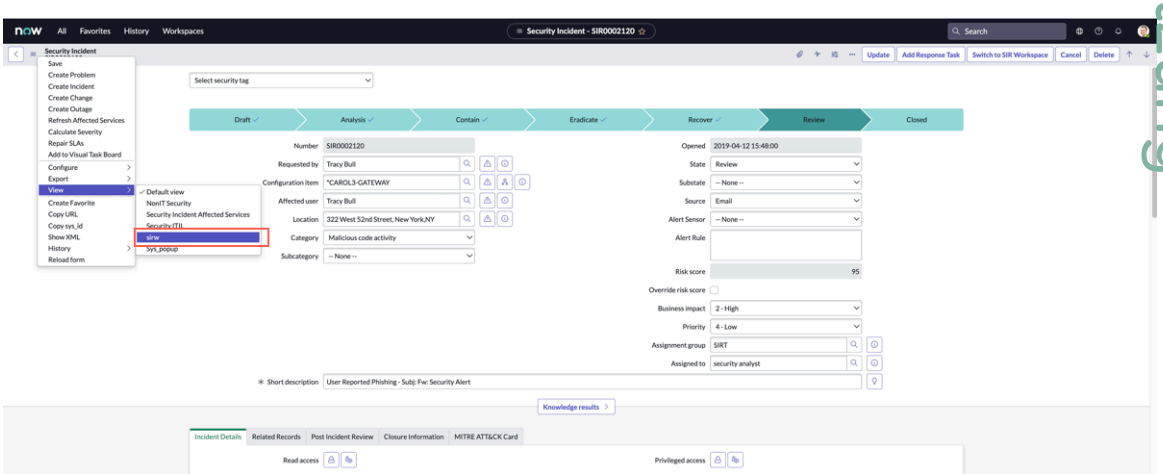


SIR Analyst Workspace-Ansicht anzeigen:

1. Navigieren zu **Alle** > **Security Incident** > **Zeigen Sie offene Incidents an**an.
2. Wählen Sie einen beliebigen Security Incident-Datensatz aus.
3. Klicken Sie auf das Kontextmenü, und wählen Sie aus **Ansicht** > **sirw**an.

Hinweis:

Sie können mit anpassen **SIRW** Arbeitsbereichsansicht im klassischen UI-Formular.

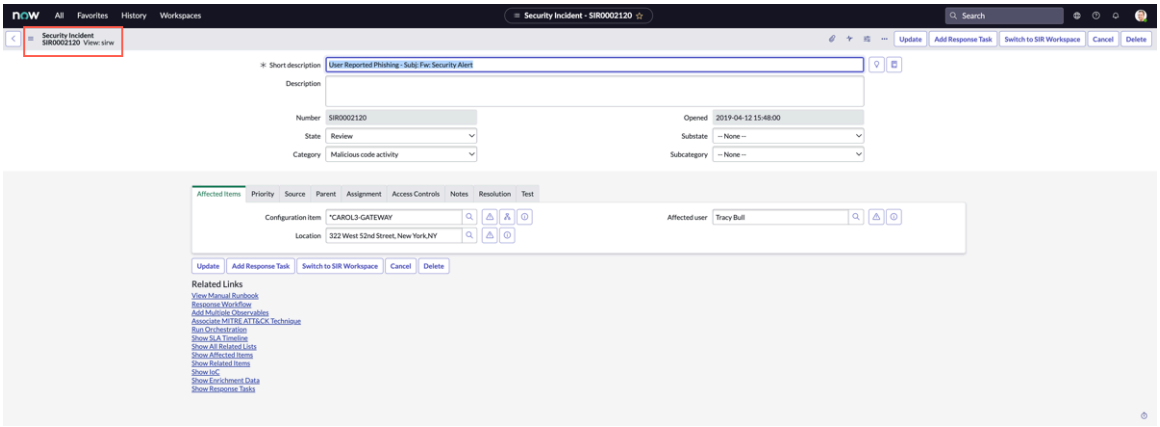


4. Die Ansicht des Security Incident-Arbeitsbereichs wird wie unten dargestellt gerendert.

Automatische Übersetzung

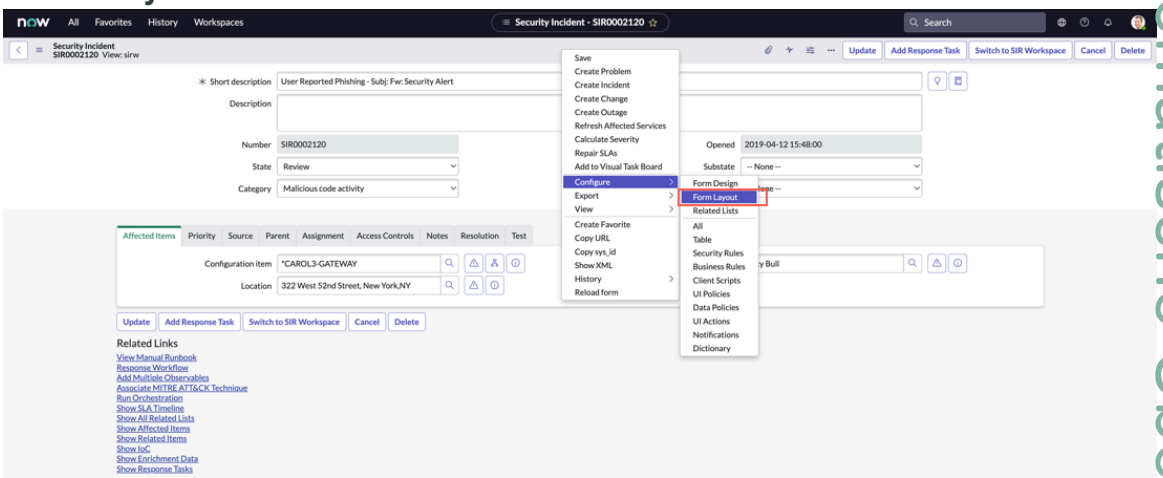
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SIR-Arbeitsbereichsansicht



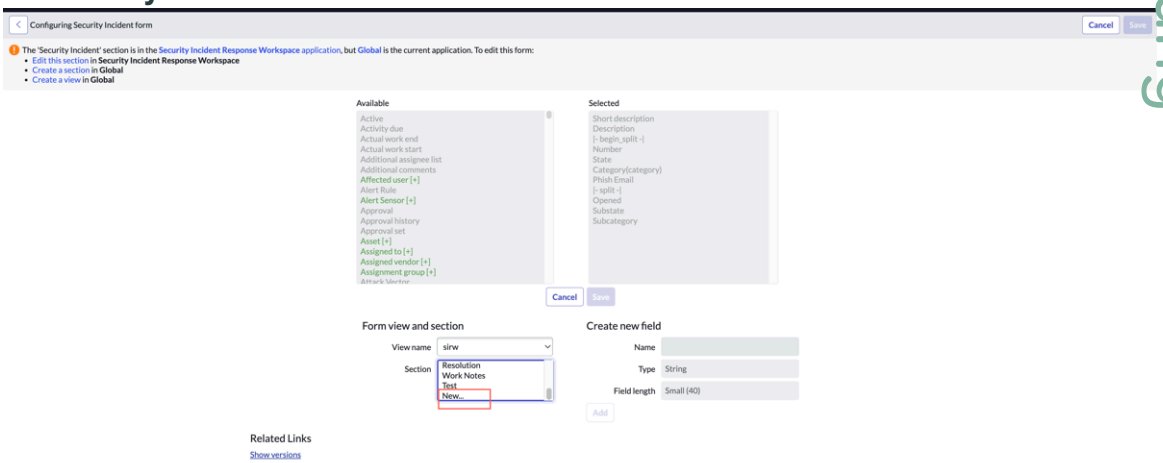
5. Klicken Sie im Security Incident-Datensatz mit der rechten Maustaste, und wechseln Sie zu **Konfigurieren** > **Formularlayout**an.

Formularlayout



6. Führen Sie einen Drilldown zu **Formularansicht und -Abschnitt** Und wählen Sie aus **Neu** Von **Abschnitt** Um einen neuen Abschnitt zu erstellen.

Formularlayout: Abschnittsansicht



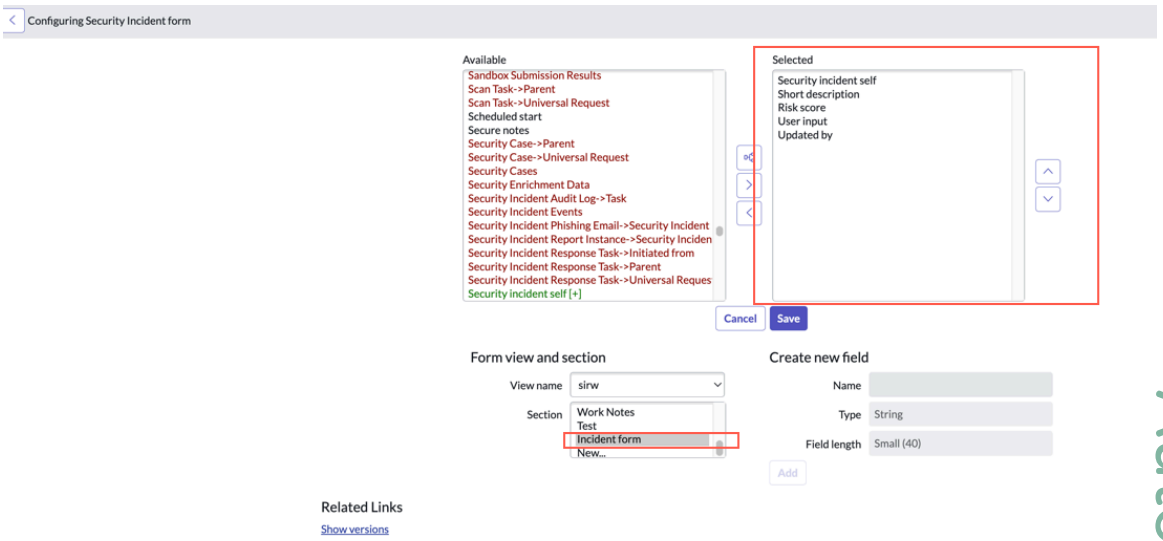
7. Geben Sie den neuen Abschnittsnamen an, und klicken Sie auf **OK** .

Automatische Übersetzung

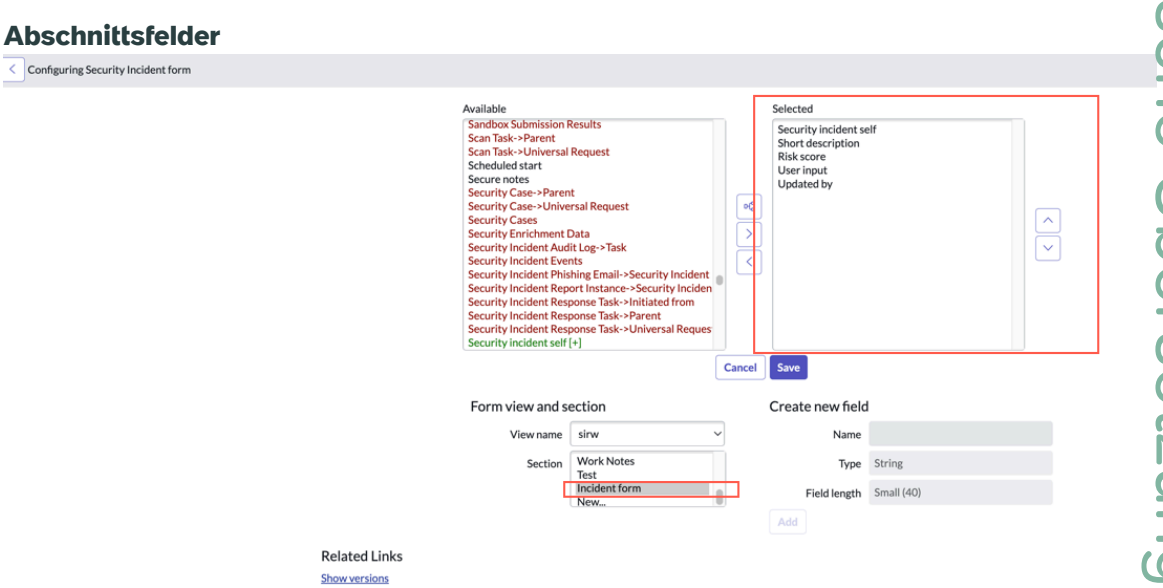
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Incident-Formular.

8. Der neue Abschnitt wird erstellt und dem hinzugefügt **Abschnitt** .



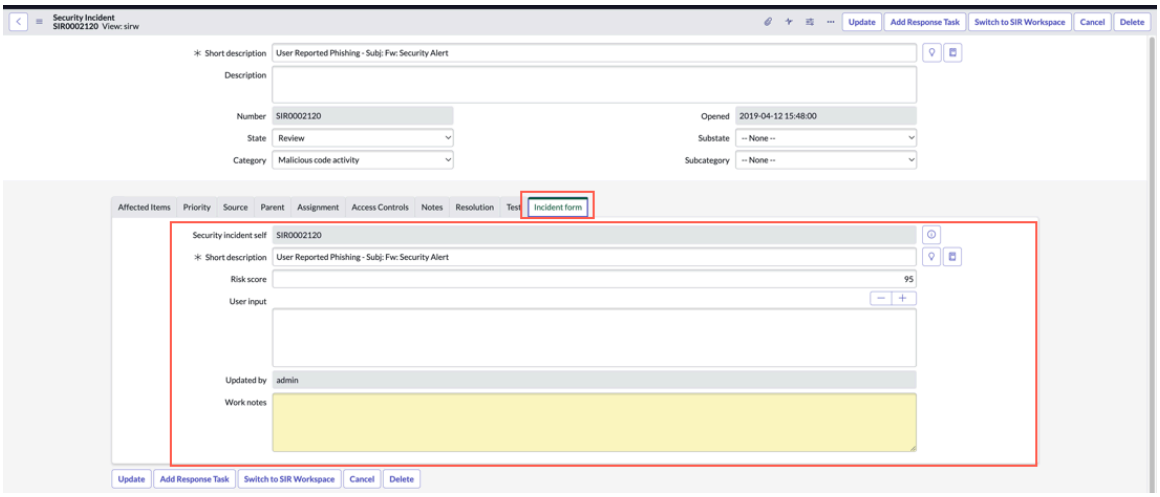
9. Wählen Sie Ihren neuen Abschnitt aus, fügen Sie dem Slush-Bucket die erforderlichen Abschnittsfelder hinzu, und klicken Sie auf **Speichern** .



10. Der neu hinzugefügte Abschnitt wird zusammen mit dem vorhandenen Abschnittslayout im Security Incident-Formular angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



11. Klicken Sie jetzt auf **Wechseln Sie zum SIR-Arbeitsbereich** Um zum Security Incident-Formular und zum anwenderdefinierten Abschnitt in zu wechseln **Details** Registerkarte des Arbeitsbereichs.

SIR-Arbeitsbereich Orchestration

Arbeitsbereich für Security Incident Response Orchestration-Aktivitäten helfen Sicherheitsanalysten, die Untersuchungs-Canvas anzuzeigen und verschiedene zutreffende Aktionen auszuführen.

SIR-Arbeitsbereich Untersuchungs-Canvas

Arbeitsbereich für Security Incident Response Ermöglicht es Sicherheitsanalysten, die Schlüsselinformationen anzuzeigen, die dem Security Incident während des Korrekturprozesses für Incidents zugeordnet sind. Die wichtigsten Informationen umfassen auch die zugehörigen Listen wie erkennbare Elemente, Ergebnisse der Bedrohungssuche, Sichtungssuche, Anreicherung erkennbarer Elemente usw.

In der klassischen Anwenderoberfläche sind die meisten Orchestration-Aktionen, die den sofort einsatzbereiten Integrationen zugeordnet sind, für die zugehörigen Listen verfügbar. Beispielsweise sind Bedrohungssuche ausführen, Anreicherung erkennbarer Elemente ausführen usw. für die zugehörige Liste zugeordneter erkennbarer Elemente vorhanden. Ebenso sind „Hostdetails abrufen“, „Netzwerkstatistiken abrufen“ usw. für die zugehörige Liste „Konfigurationselemente“ verfügbar.

Wenn ein Sicherheitsanalyst diese Aktionen ausführt, werden die Ergebnisse in einer anderen zugehörigen Liste ausgefüllt. Wenn ein Anwender beispielsweise Bedrohungssuche ausführen durchführt, sind die Ergebnisse in der Tabelle „Ergebnisse der Bedrohungssuche“ verfügbar. Manchmal sind Ergebnisse in mehreren verschiedenen Tabellen verfügbar. Während dieses Prozesses verfügen die Sicherheitsanalysten über eine unzusammenhängende und unorganisierte Anwender-Experience, um die Informationen von mehreren Orten miteinander zu verknüpfen.

In neu erstelltem neu SIR-Arbeitsbereich, **Untersuchung** Canvas (Registerkarte) stellt alle erforderlichen Informationen logisch gruppiert an einem Ort bereit, damit der Analyst die Untersuchung durchführen kann.

Untersuchungs-Canvas Erkunden

Das primäre Ziel des Untersuchungs-Canvas besteht darin, die erforderlichen Security Incident-Daten an einem gemeinsamen Ort zu präsentieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Innerhalb von SIR-Arbeitsbereich, Die Security Incident-Untersuchung dreht sich hauptsächlich um einige wichtige Einstiegspunkte.

Im Folgenden finden Sie einige wichtige Einstiegspunkte, die für die Sicherheitsanalysten im Basissystem bereitgestellt werden:

- Zugehörige erkennbare Elemente
- Konfigurationselemente
- Betroffene Anwender
- Zugeordnete Phishing-E-Mails
- E-Mail-Suche

Sie können die oben genannten Einstiegspunkte auch konfigurieren, indem Sie die Einstiegspunkte hinzufügen, ändern oder entfernen. Weitere Informationen finden Sie unter Konfigurieren Sie SI-Designzeituntersuchung.

Auf der **Untersuchung** Registerkarte fungiert die Einstiegspunkttabelle als übergeordnete Tabelle. Alle Tabellen, die die Ergebnisse einer Orchestration-Aktion enthalten, die für die übergeordnete Tabelle ausgeführt wird, werden als untergeordnete Tabelle innerhalb des Einstiegspunkts angezeigt.

Beispiel: Für **Zugeordnete Erkennbare Elemente** Einstiegspunkt, **Ordnen Sie Erkennbare Elemente Zu** Tabelle ist die übergeordnete Tabelle, und andere Tabellen wie Ergebnisse der Bedrohungssuche, Sandbox-Übermittlungsergebnisse usw. sind die untergeordnete Tabelle.

Der Sicherheitsanalyst kann alle Orchestration-Aktionen für die Tabelle der zugehörigen erkennbaren Elemente ausführen und alle zugehörigen Informationen auf derselben Seite anzeigen, ohne an mehreren Orten navigieren zu müssen.

Hinweis:
Wenn ein Anwender auf die interaktionsfähigen Diagramme im klickt **Übersicht** Seite, z. B. schädliche erkennbare Elemente, wird der Anwender zur gefilterten Ansicht schädlicher erkennbarer Elemente im Untersuchungs-Canvas navigiert. Alternativ kann der Anwender direkt mit der Untersuchung beginnen, indem er zum Untersuchungs-Canvas navigiert, der alle Daten enthält.

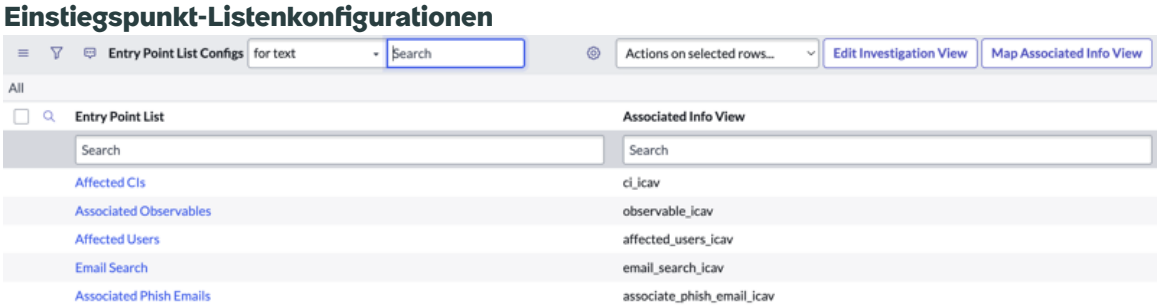
Die Liste der untergeordneten Tabellen unter einem Einstiegspunkt kann ebenfalls konfiguriert werden. Weitere Informationen finden Sie unter Konfigurieren Sie SI-Designzeituntersuchung.

Im Folgenden finden Sie ein detailliertes Beispiel für einen Einstiegspunkt (zugehöriges erkennbares Element), der im Basissystem konfiguriert und bereitgestellt wird:

1. Wählen Sie aus **Zugeordnete Erkennbare Elemente** Einstiegspunkt aus der Dropdown-Liste.

   Hier ist auch die übergeordnete Tabelle **Zugehöriges Erkennbares Element** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Wählen Sie ein oder mehrere erkennbare Elemente aus der übergeordneten Tabelle aus.
3. Führen Sie die gewünschte Fähigkeit aus.

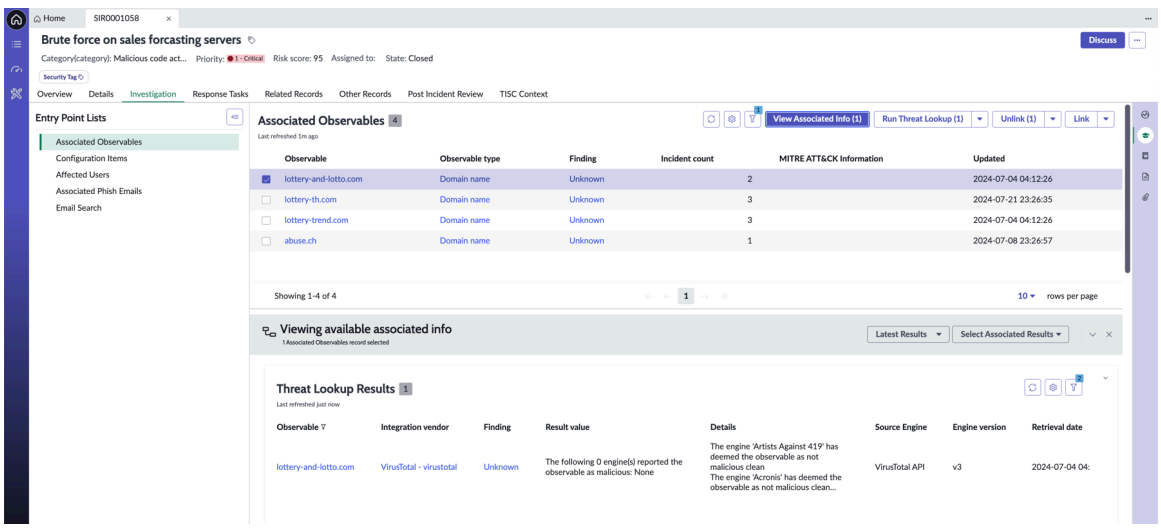
   Wählen Sie beispielsweise aus **Bedrohungssuche Ausführen** Zum Abrufen der Bedrohungssuchergebnisse für ein ausgewähltes erkennbares Element.

   Hinweis:
   Wenn eine entsprechende Aktion erkennbarer Elemente ausgeführt wird, wird der Prozess im Back-End ausgeführt, und die Ergebnisse werden unter der Liste erkennbarer Elemente angezeigt.

4. Klicken Sie Auf **Zeigen Sie Zugehörige Informationen An** Zum Anzeigen der Ergebnisse erkennbarer Elemente. Die Ergebnisse werden auf derselben Seite angezeigt.

   Hinweis:
   Sie können die Ergebnisse mithilfe von Filtern nach Ergebnissen anzeigen. Wählen Sie eine der beiden aus **Alle Ergebnisse** Oder **Neueste Ergebnisse** , Je nachdem, was die gewünschte Ansicht ist. Standardmäßig werden die neuesten Ergebnisse angezeigt. Wenn mehrere Implementierungen (von Integrationen) vorhanden sind, werden die neuesten Ergebnisse pro Implementierung angezeigt.

   Darüber hinaus können Sie die Ergebnisse filtern **Nach zugeordneten zugehörigen Listen** Welche sind die Ergebnisse der untergeordneten Tabelle. Standardmäßig werden alle konfigurierten zugehörigen Listen der untergeordneten Tabelle angezeigt. Weitere Informationen finden Sie unter Konfigurieren Sie SI-Designzeituntersuchung. Sie können jedoch nur die erforderlichen untergeordneten Tabellen auswählen.

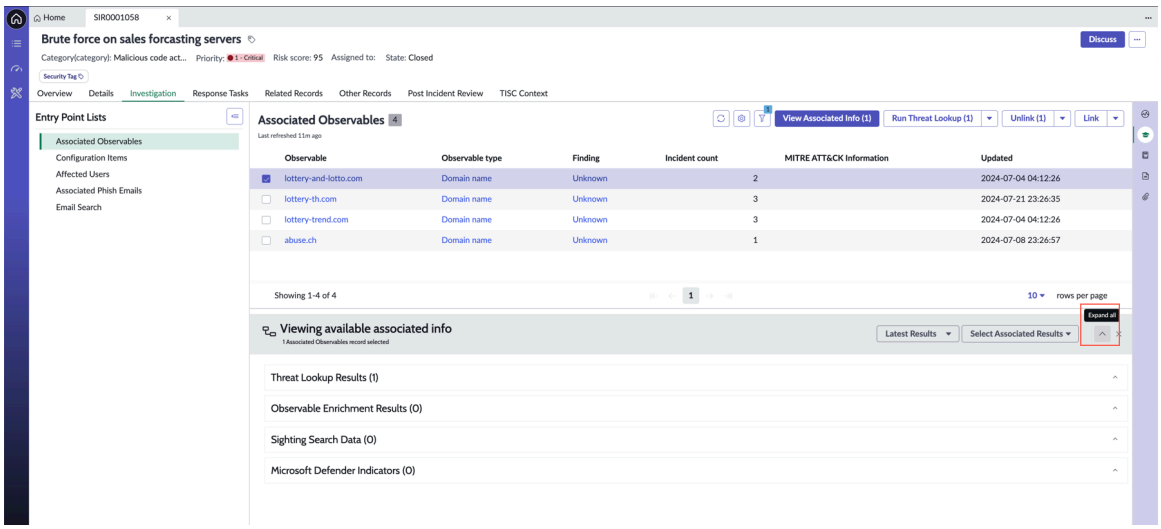


5. Durch Klicken **Zeigen Sie Zugehörige Informationen An** Sie können alle zugehörigen untergeordneten Tabellendaten an einem Ort anzeigen, Sie können jedoch die Ansicht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„zugehörige Listen“ schließen, indem Sie auswählen **Ansicht Schließen** Schaltfläche. Sobald Sie die Ansicht geschlossen haben, können Sie die übergeordnete Tabelle der erkennbaren Elemente nur wie zuvor anzeigen.

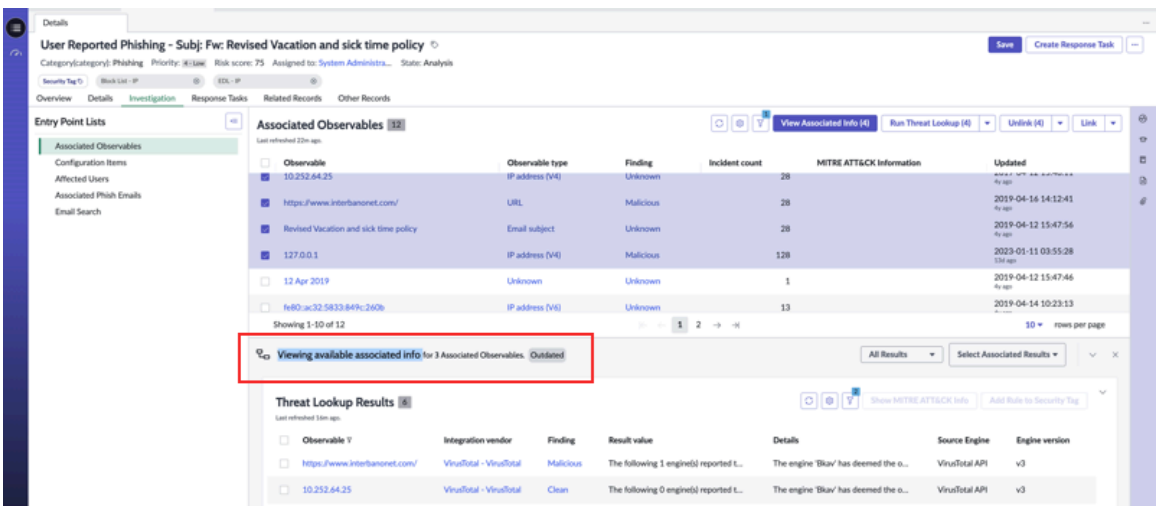
6. Klicken Sie Auf **Erweitern Sie alle** Symbol für Aufwärtsrichtung innerhalb von **Verfügbare zugehörige Informationen werden angezeigt** Ergebnistabelle zum erweitern aller untergeordneten Tabellendaten für zugehörige Listen.



7. Klicken Sie Auf **Reduzieren Sie alle** Symbol für Abwärtsrichtung, um alle untergeordneten Tabellendaten der zugehörigen Listen einzuklappen.

Hinweis:

Das Banner oben im Abschnitt „zugehörige Informationen“, das alle untergeordneten Tabellendaten enthält, zeigt an, wie viele zugehörige Informationen zu erkennbaren Elementen dem Anwender angezeigt werden. Beispiel: Zunächst, wenn Sie zwei erkennbare Elemente auswählen und auf klicken **Zeigen Sie Zugehörige Informationen An** , Das Banner zeigt an, **Anzeigen verfügbarer zugeordneter Informationen für 2 zugeordnete erkennbare Elemente.** . Wenn Sie beispielsweise ein anderes erkennbares Element auswählen, wird im Banner angegeben, dass die Informationen veraltet sind (Screenshot unten). Sie müssen auf klicken **Zeigen Sie Zugehörige Informationen An** Erneut, um die neuesten Daten abzurufen.



Zusätzlich zur obigen umfassenden Ansicht der zugehörigen Informationen erkennbarer Elemente können Sie weitere Informationen zu einem Datensatz in der übergeordneten Tabelle anzeigen, indem Sie auf das erkennbare Element klicken. Das Formular für den Datensatz der übergeordneten Tabelle wird in einer anderen Registerkarte mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einer detaillierteren Ansicht des ausgewählten Datensatzes geöffnet. Alle zugehörigen untergeordneten Tabellendaten dieses bestimmten ausgewählten Datensatzes werden auch unter angezeigt **Zugehörige Informationen** Abschnitt.

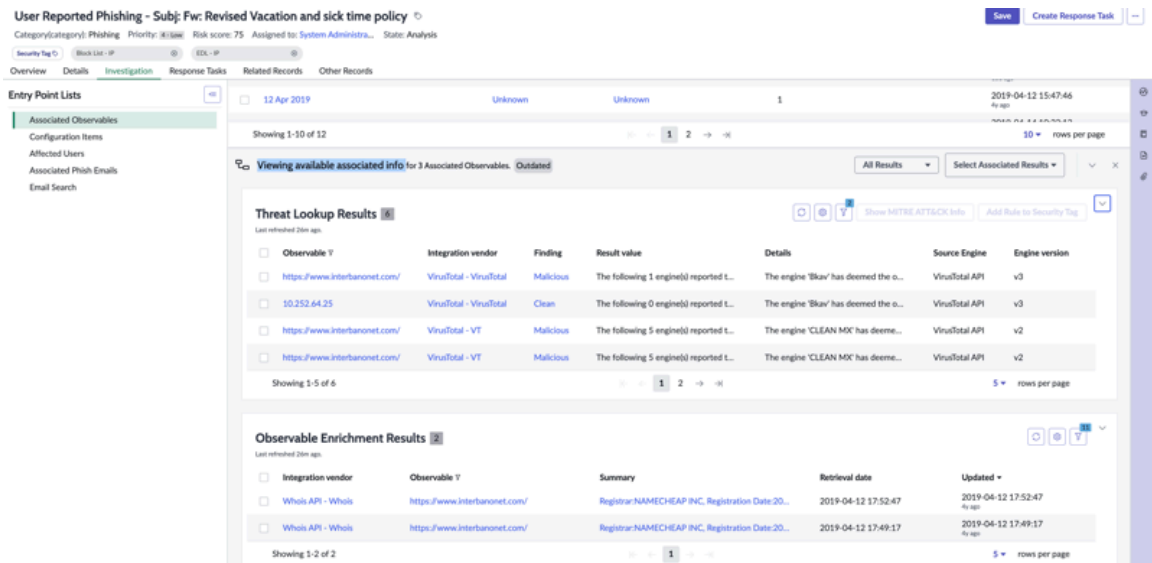
Im Abschnitt „zugehörige Informationen“ werden jedoch nur die neuesten Ergebnisse der untergeordneten Tabelle angezeigt, wie im Untersuchungs-Canvas im schreibgeschützten Modus. In dieser Ansicht sind keine Aktionen möglich. Die Formularseite der untergeordneten Tabelle kann in einer neuen Registerkarte geöffnet werden, auf der die voll funktionsfähige Seite mit allen Aktionen, falls vorhanden, gerendert wird.

Sie können mithilfe der Dropdown-Liste zwischen den verschiedenen Tabellen wechseln. Sie können auch jedes Formular im Abschnitt „zugehörige Informationen“ erweitern oder reduzieren.

Innerhalb von **Erkennbares Element** Formularseite (Formularseite des Datensatzes der übergeordneten Tabelle) Sie können bestimmte Aktionen wie verfügbar ausführen. Wenn Sie eine Aktion ausführen, können Sie im zugehörigen Infobanner auf „Aktualisieren“ klicken, um die Daten zu aktualisieren.

8. Klicken Sie Auf **Erweitern Sie alle** Um alle zugehörigen Listen der untergeordneten Tabelle zu erweitern. Standardmäßig werden alle untergeordneten Elemente erweitert.

Erweiterte Ansicht der erkennbaren Elemente



Zugehörige Informationen

Konfigurieren Sie SI-Designzeituntersuchung

Einheitliches Experience-Framework für Integrationen, die auf dem Fähigkeits-Framework basieren

In der klassischen UI wird die Experience bei der Ausführung von Orchestration-Aktivitäten wie der Ausführung der Bedrohungssuche, der Durchführung von Sichtungssuchen usw. getrennt. Jede Fähigkeit verfügt bei der Ausführung über eine eigene Erfahrung. Im neuen Arbeitsbereich gibt es eine einheitliche Experience für alle Fähigkeiten.

Die einheitliche Experience gilt nur für die Integrationen und Orchestration-Aktivitäten, die in das Fähigkeits-Framework fallen. Es kann Aktionen geben, die für die Integration spezifisch sind, z. B. Indikatoren in Microsoft Defender erstellen. Diese Aktionen verfügen über ihre eigene Erfahrung, wie im Anwendungsfall erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das neue Framework besteht aus modalen Bildschirmen mit drei Schritten, wie unten erläutert.

1. **Implementierungen** : Der erste Schritt umfasst die Auswahl einer oder mehrerer Implementierungen, die für die ausgewählte Fähigkeit vorhanden sind.

   Beispiel: Wenn der Analyst auf klickt **Bedrohungssuche Ausführen** , Der Analyst kann eine oder mehrere Implementierungen auswählen, die für vorhanden sind **Führen Sie die Funktion „Bedrohungssuche“ aus** .

   Jede Implementierung enthält die Details der Integrationsquelle. Siehe Tabelle unten. Für jede Implementierung werden auch zusätzliche Informationen angezeigt.

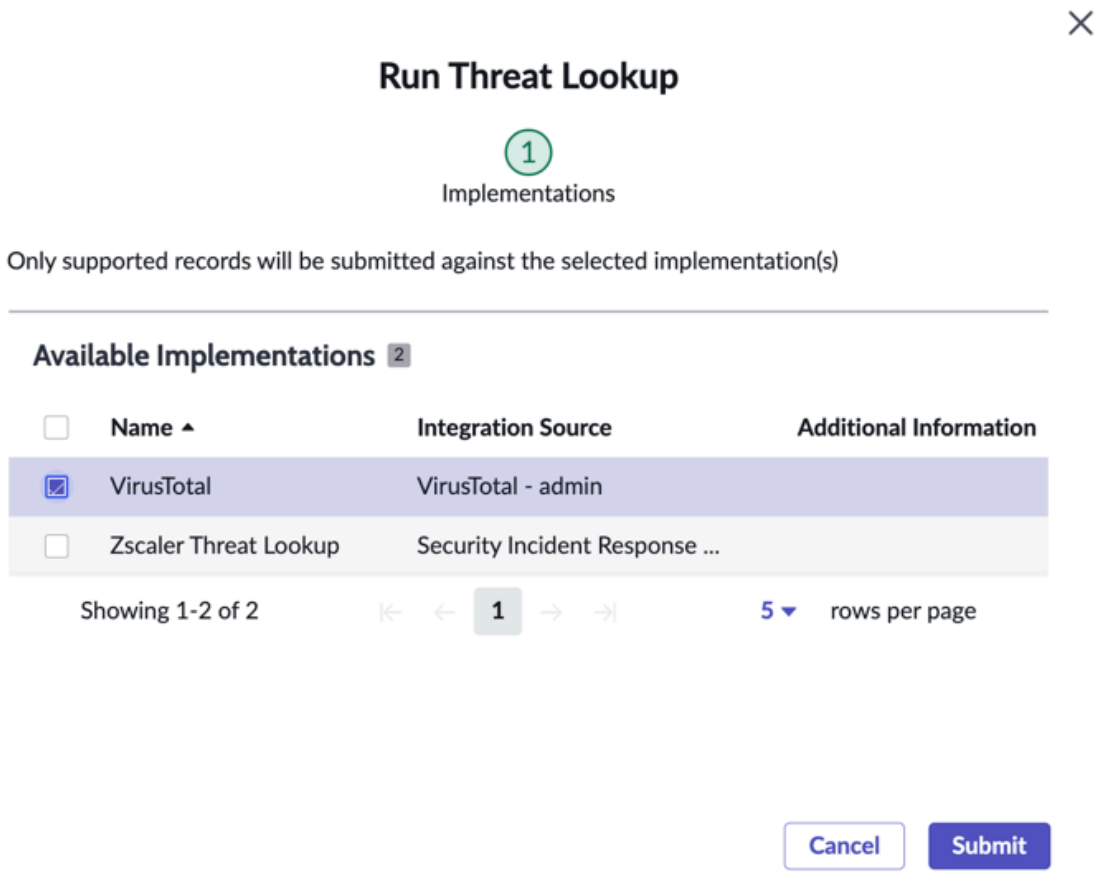
   Zusätzliche Informationen können z. B. Informationen zu Filtern, Typen der unterstützten erkennbaren Elemente usw. enthalten Die zusätzlichen Informationen können nach Bedarf konfiguriert werden. Weitere Informationen finden Sie unter technisches Konfigurationsverfahren für UX-Framework.

Modal Für Einheitliches Implementierungs-Framework

Implementierung	Beschreibung
Name	Name der Implementierung.
Integrationsquelle	Die Quelle der Implementierung, z. B. die verwendete Konfiguration.
Zusätzliche Informationen	Diese Spalte erfasst die statischen Informationen, die dem Sicherheitsanalysten mehr Kontext für die ausgewählten Implementierungen hinzufügen, um mit einer Aktion fortzufahren. Zum Beispiel Supportfähigkeit oder gefilterte Informationen. Wenn eine Implementierung auch nur einen bestimmten Typ erkennbarer Elemente wie Domäne oder URL unterstützt, können Sie diese zusätzlichen Informationen hier in dieser Spalte hinzufügen, um dem Anwender den Kontext bereitzustellen. **Hinweis:** Das UI-Framework ermöglicht grundsätzlich die Auswahl jeder Art von Implementierung und jeder Art von erkennbaren Elementen. Während der Übermittlung übernehmen die vorhandenen Basissystemintegrationen, die geliefert werden, die Filterung im Back-End und übermitteln nur den unterstützten Typ erkennbarer Elemente. Die restlichen Datensätze, die nicht mit der Supportfähigkeit übereinstimmen, werden ignoriert. Daher wird eine UI-Informationsnachricht angezeigt, während Sie die Fähigkeit auswählen: **Nur unterstützte Datensätze werden für die ausgewählten Implementierungen übermittelt.**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bildschirm 1: Implementierung(en)

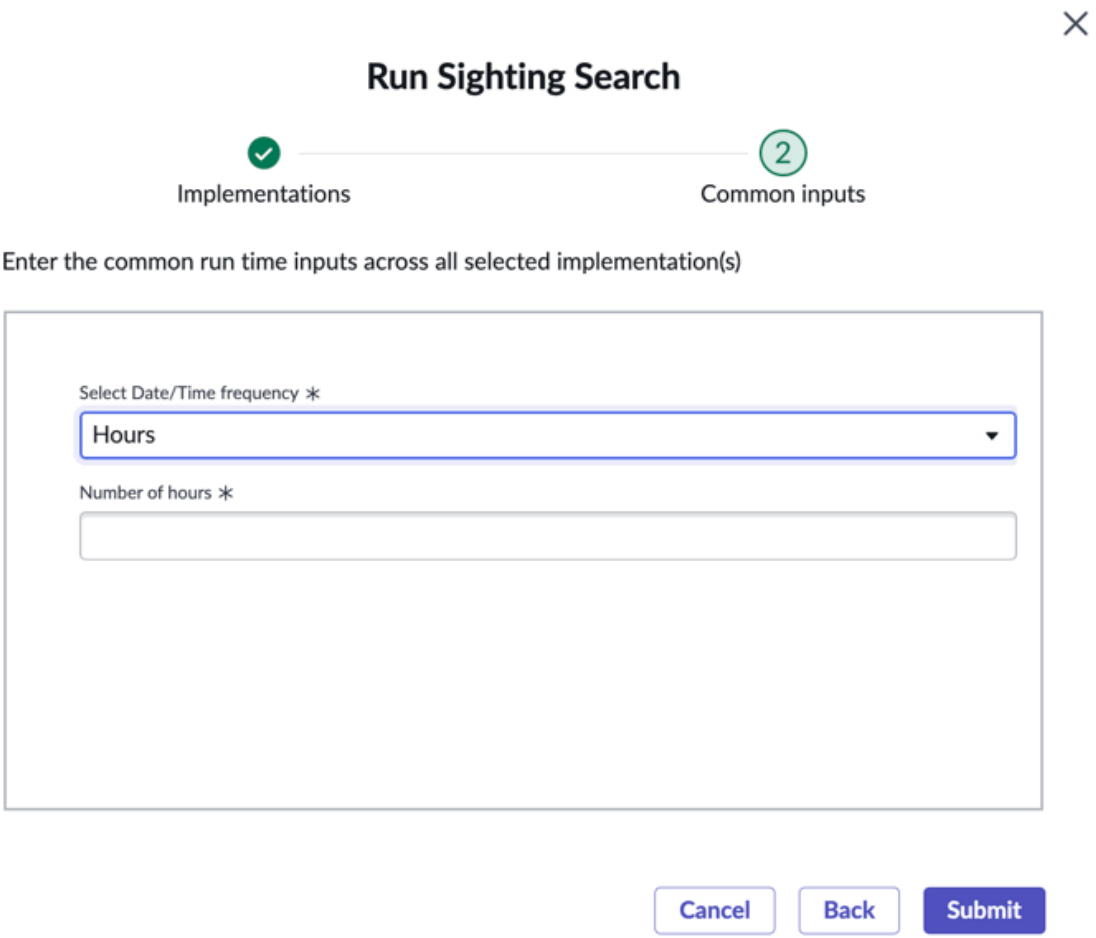


2. **Allgemeine Eingaben** : Fügen Sie allgemeine Eingaben für die ausgewählten Implementierungen oder für alle ausgewählten anwendbaren Implementierungen hinzu. Dies ist der Bildschirm 2 Ihrer Implementierung. Zum Beispiel nur ab jetzt **Sichtungssuche** Hat den Bildschirm „Allgemeine Eingaben“. Diese Implementierung ist eine Kombination aus Bildschirm 1 (Implementierungen) und Bildschirm 2 (allgemeine Eingaben).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bildschirm 1 + Bildschirm 2



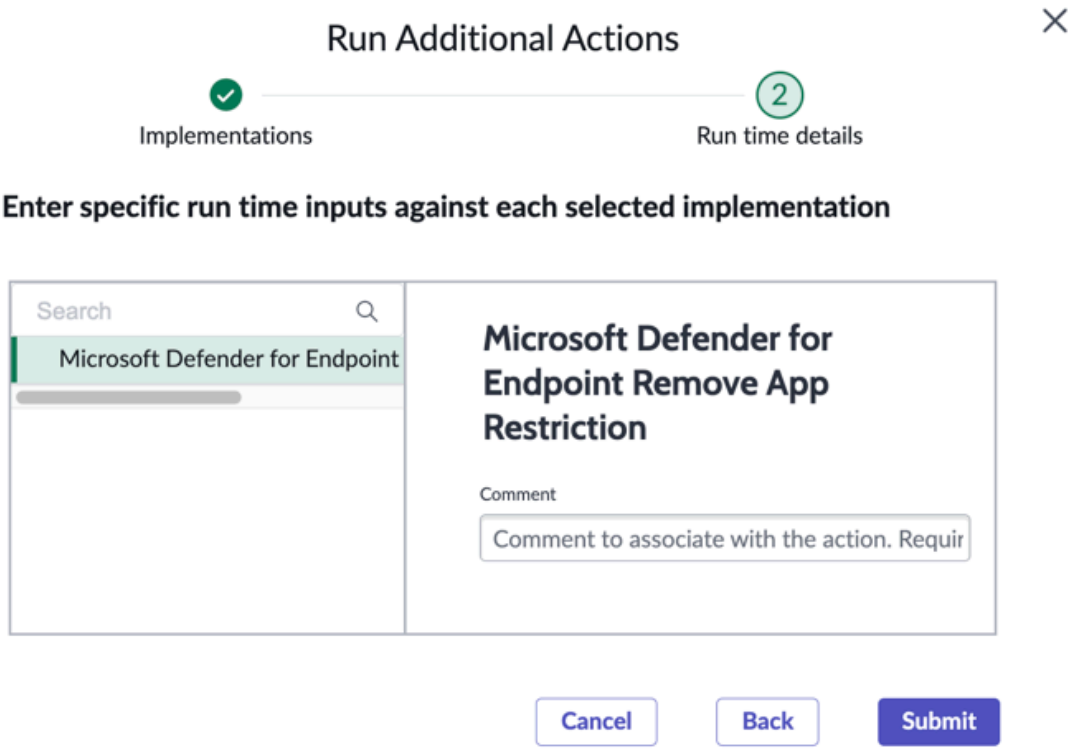
3. **Laufzeitdetails** : Fügen Sie bestimmte Laufzeiteingaben für die ausgewählten Implementierungen hinzu, die sich von den anderen Implementierungen unterscheiden. Dies ist der Bildschirm 3 Ihrer Implementierung. Diese Implementierung ist eine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kombination aus Bildschirm 1 (Implementierungen) und Bildschirm 3 (spezifische Laufzeiteingaben).

Bestimmte Eingaben



Hinweis:
Nicht alle drei Schritte sind immer erforderlich. Abhängig von der Fähigkeit und dem Typ der erforderlichen Eingaben sind der Schritt „Laufzeitdetails“ und der Schritt „Allgemeine Eingaben“ sichtbar.

Unified Experience-Funktionen und modale Bildschirme

In der folgenden Tabelle werden die Fähigkeiten und anwendbaren Bildschirme beschrieben.

Tabelle „Fähigkeiten und anwendbare Bildschirme“

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen Unterstützt
Bedrohungssuche durchführen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen Eingaben oder implementierungsspezifischen Eingaben, die für die Ausführung der Bedrohungssuche gelten. Daher wird dem Sicherheitsanalysten nur	• Viren insgesamt • Hybrid Analysis • Security Incident Response-Integration mit Zscaler • Phistank • Metadefender • Threatcrowd

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Fähigkeiten und anwendbare Bildschirme“ (Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen Unterstützt
	Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	• Wurde ich verpfändet? • Crowd Strike Falcon Intelligence
Anreicherung erkennbarer Elemente durchführen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar Es gibt keine allgemeinen Eingaben oder implementierungsspezifischen Eingaben, die für die Ausführung der Anreicherung erkennbarer Elemente gelten. Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	• MISP • Microsoft Defender-Endpunkt • Shodan • RiskIQ • WHOIS • WHOIS umkehren
Sichtungssuche Ausführen/ Websichtungssuche Ausführen/E-Mail-Sichtungssuche Ausführen	Bildschirm 1 – **Wählen Sie Implementierungen Aus** Und Bildschirm 2 – **Allgemeine Eingaben** Sind zutreffend. Die Sichtungssuche verwendet die Datums- und Uhrzeithäufigkeit als allgemeine Eingaben für mehrere Implementierungen von Splunk und anderen Integrationen. Dieser Bildschirm wird dem Sicherheitsanalysten angezeigt, um Datums- und Uhrzeitfrequenzen zu erfassen. Für Integrationen, die diese Eingaben nicht erfordern, z. B. FireEye HX, werden sie ignoriert.	• Splunk-Incident-Anreicherung • Carbon Black • Elastische Suche • FireEye HX • McAfee ESM • MSFT Defender für Endpunkt • Splunk-Sichtung • Qradar-Sichtungssuche • MISP

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Fähigkeiten und anwendbare Bildschirme“ (Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen Unterstützt
	Nachdem Sie eine oder mehrere Implementierungen ausgewählt und allgemeine Eingaben bereitgestellt haben, kann der Sicherheitsanalyst die Aktion übermitteln.	
An die Sandbox übermitteln	Bildschirm 1 – Implementierungen auswählen und Bildschirm 3 – Implementierungsspezifische Eingaben sind anwendbar. „An Sandbox senden“ verwendet verschiedene Eingaben für verschiedene Implementierungen. Für diese Fähigkeit sind derzeit keine allgemeinen Eingaben vorhanden. Wenn der Analyst beispielsweise CrowdStrike Falcon X Quick Scan, CrowdStrike Falcon X Windows 64, CrowdStrike Falcon X Linux und Zscaler auswählt, variieren die Eingaben. CrowdStrike Falcon X Quick Scan und Zscaler benötigen keine weiteren Laufzeiteingaben. CrowdStrike Falcon X Windows 64 verwendet optionale Laufzeiteingaben, die sich von CrowdStrike Falcon X Linux unterscheiden. Daher können diese in Bildschirm 3 speziell für einzelne ausgewählte Implementierungen bereitgestellt werden.	• CrowdStrike Falcon X Sandbox-Integration • Security Incident Response-Integration mit Zscaler
In Beobachtungsliste veröffentlichen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder implementierungsspezifischen Eingaben, die für gelten	Crowdstrike Falcon-Host

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Fähigkeiten und anwendbare Bildschirme“ (Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen Unterstützt
	In Beobachtungsliste veröffentlichen . Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	
Anforderung zulassen/blockieren	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder implementierungsspezifischen Eingaben, die für gelten **Anforderung Zulassen/ Blockieren** . Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	• Palo Alto-Netzwerk NGFW • Prüfpunkt NGFW • Security Incident Response-Integration mit Zscaler
Hostdetails abrufen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder implementierungsspezifischen Eingaben, die für das Abrufen von Hostdetails gelten. Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann	• FireEye HX • Microsoft Defender für Endpunkt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Fähigkeiten und anwendbare Bildschirme“ (Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen Unterstützt
	der Sicherheitsanalyst die Aktion übermitteln.	
Datei abrufen	Bildschirm 1 – Implementierungen auswählen und Bildschirm 2 – Allgemeine Eingaben sind anwendbar. „Datei abrufen“ nimmt den Dateinamen und den Pfad als allgemeine Eingaben an. Nachdem Sie eine oder mehrere Implementierungen ausgewählt und allgemeine Eingaben bereitgestellt haben, kann der Sicherheitsanalyst die Aktion übermitteln.	FireEye HX
Netzwerkstatistiken abrufen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder implementierungsspezifischen Eingaben, die für das Abrufen von Netzwerkstatistiken gelten. Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	• FireEye HX • Netstat
Laufende Prozesse abrufen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder implementierungsspezifischen Eingaben, die für das Abrufen laufender Prozesse gelten. Daher wird dem Sicherheitsanalysten nur Bildschirm 1 angezeigt,	• FireEye HX • Carbon Black • Systembefehl

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Fähigkeiten und anwendbare Bildschirme“ (Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen Unterstützt
	um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Sicherheitsanalyst die Aktion übermitteln.	
Laufende Services abrufen	Nur Bildschirm 1 – Implementierungen auswählen ist anwendbar. Es gibt keine allgemeinen oder implementierungsspezifischen Eingaben, die für das Abrufen laufender Services gelten. Daher wird dem Analyst nur Bildschirm 1 angezeigt, um eine oder mehrere Implementierungen auszuwählen. Nach Auswahl der Implementierungen kann der Analyst die Aktion übermitteln.	FireEye HX
Host Isolieren/Host Isolieren	Bildschirm 1 – Implementierungen auswählen und Bildschirm 3 – Implementierungsspezifische Eingaben sind anwendbar. Host isolieren/Host-Isolation aufheben verwendet verschiedene Eingaben für verschiedene Implementierungen. Für diese Fähigkeit sind derzeit keine allgemeinen Eingaben vorhanden. Wenn der Analyst beispielsweise FireEye HX und Microsoft Defender für Endpunkt auswählt, variieren die Eingaben. FireEye HX benötigt keine Laufzeiteingaben. Andererseits verwendet Microsoft Defender Eingaben wie Isolationstyp und Kommentare.	• FireEye HX • Microsoft Defender-Endpunkt • Carbon Black

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Fähigkeiten und anwendbare Bildschirme“ (Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen Unterstützt
	Daher können diese in Bildschirm 3 speziell für einzelne ausgewählte Implementierungen bereitgestellt werden.	
Zusätzliche Aktionen ausführen	Bildschirm 1 – Implementierungen auswählen und Bildschirm 3 – Implementierungsspezifische Eingaben sind anwendbar. Zusätzliche Aktionen ausführen Host verwendet verschiedene Eingaben für verschiedene Implementierungen. Für diese Fähigkeit sind derzeit keine allgemeinen Eingaben vorhanden. Wenn der Analyst beispielsweise FireEye HX Standard Investigative Details Script, FireEye HX Triage Acquisition und CrowdStrike Falcon Insight Reg. entladen auswählt, variieren die Eingaben. FireEye HX Standard Investigative Details Skript und FireEye HX Selektierung Akquisition nehmen Kommentare als Eingabe, die für beide unterschiedlich sein können. Für das Entladen der CrowdStrike Falcon Insight-Registrierung wird der Unterschlüssel als Eingabe verwendet. Daher können diese in Bildschirm 3 speziell für einzelne ausgewählte Implementierungen bereitgestellt werden.	• FireEye HX • Microsoft Defender für Endpunkt • Crowdstrike Falcon Insight

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Fähigkeiten und anwendbare Bildschirme“ (Fortsetzung)

Fähigkeit	UX-Frameworks-Bildschirme anwendbar	Integrationen Unterstützt
	Hinweis: Unterstützt derzeit nur eine einzelne Auswahl von Implementierungen. In zukünftigen Releases wird die Mehrfachauswahl der Implementierung unterstützt.	

Beispiele für einheitliche Experience

Dieses Beispiel zeigt die Funktionen des Unified Experience-Frameworks.

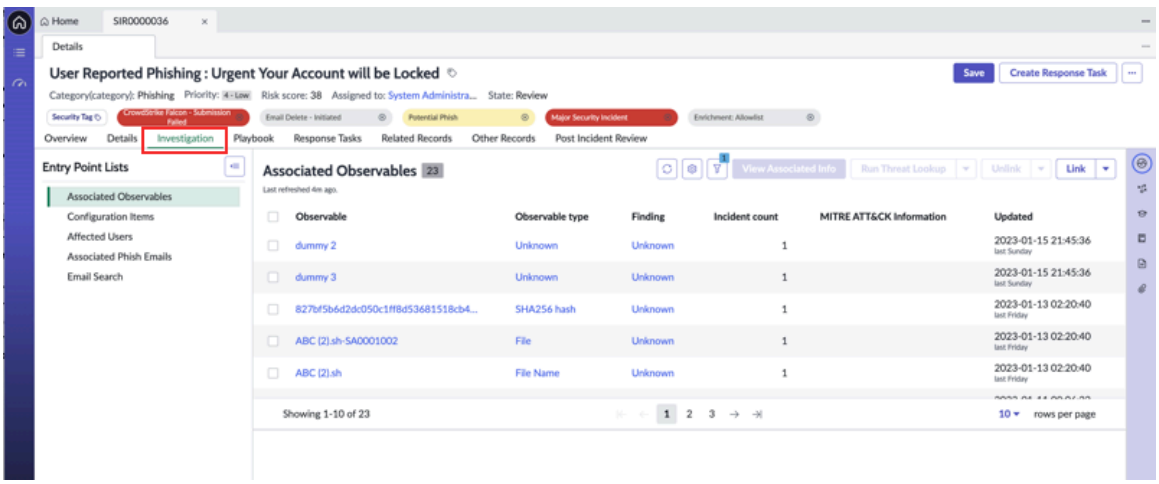
Beispiel 1: Implementierungen auswählen: Bedrohungssuche

Das folgende Beispiel zeigt die Implementierung(en).

Beispiel 1: Nur Bildschirm 1: Bedrohungssuche

Sie können ausführen **Bedrohungssuche Ausführen** Aktion für zugehörige Integrationsfähigkeiten mit **Untersuchung** Registerkarte von SIR-Arbeitsbereich.

1. Auf der **Untersuchung** Registerkarte navigieren Sie zu **Einstiegspunktlisten** Abschnitt, der auf der linken Seite angezeigt wird.
2. Wählen Sie einen beliebigen Einstiegspunkt aus, und führen Sie die Integrationsfähigkeitsaktion aus.



Hinweis:
Sie können auch zu navigieren **Zugehörige Datensätze** Registerkarte im Arbeitsbereich, um die Aktion „Integrationsfähigkeiten“ auszuführen.

Bedrohungssuche Ist eines der Beispiele, das detailliert beschrieben wird, wie die Integrationen durchgeführt werden.

Wählen Sie Implementierungen aus

Wählen Sie eine oder mehrere Implementierungen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

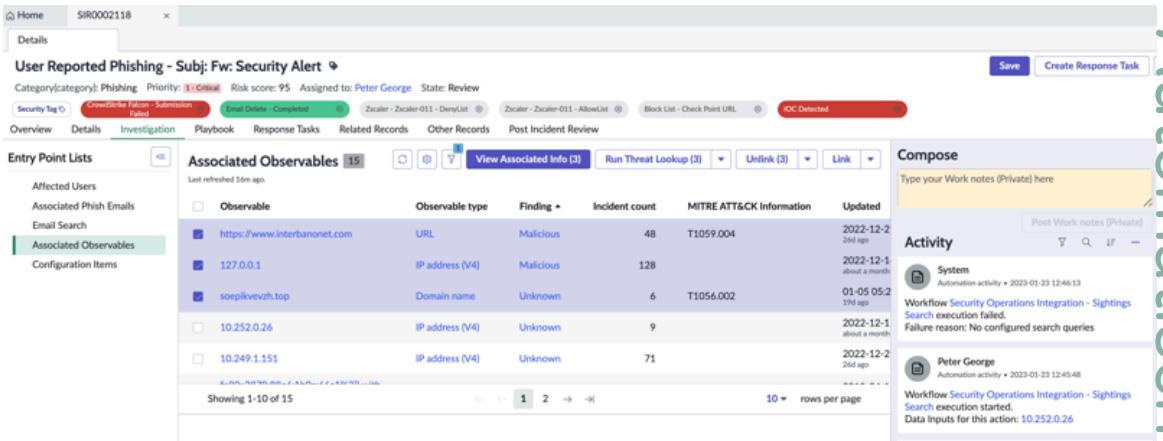
Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Die verfügbaren Implementierungen werden aufgelistet. Wählen Sie die Implementierung(en) aus. Nachdem Sie sie ausgewählt haben, werden nur die unterstützten Datensätze für jede ausgewählte(n) Implementierung(en) übermittelt.

Prozedur

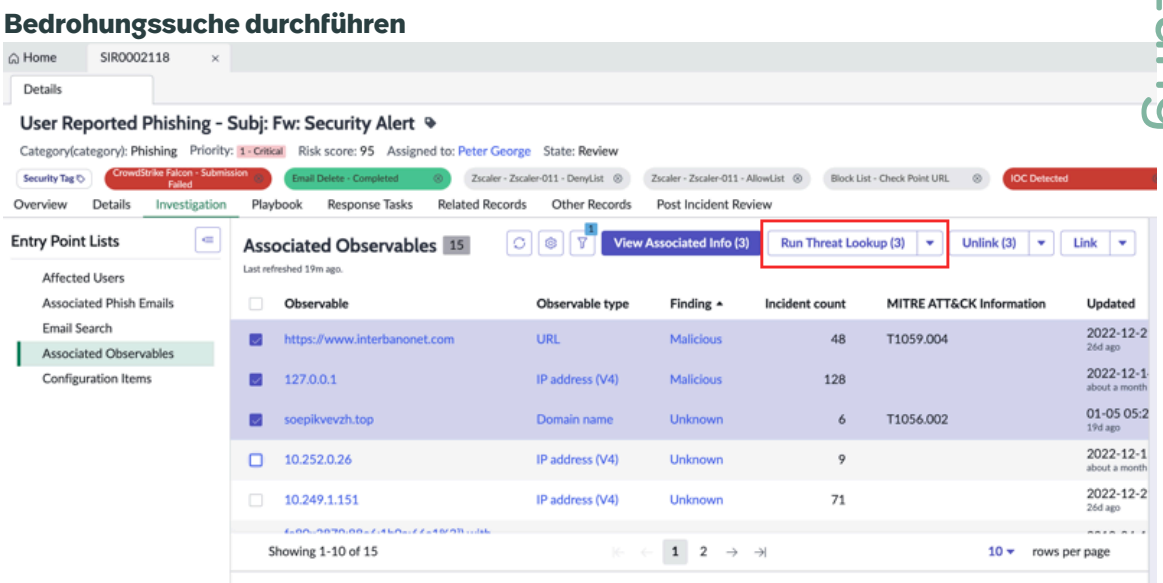
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen Security Incident.
3. Wechseln Sie zu **Untersuchung** Registerkarte des Arbeitsbereichs.
   Die Registerkarte Untersuchung mit den Einstiegspunktlisten wird angezeigt.



4. Wählen Sie das zugehörige erkennbare Element aus den Einstiegspunktlisten aus.
   Wählen Sie beispielsweise aus **Zugehörige erkennbare Elemente** Zugehörige Liste. Die entsprechenden Datensätze erkennbarer Elemente werden angezeigt.

Hinweis:

Sie können eine Implementierung auswählen, um eine Suche nach den ausgewählten erkennbaren Elementen durchzuführen, oder Sie können die Suche durchführen, indem Sie alle Implementierungen auswählen.



Automatische Übersetzung

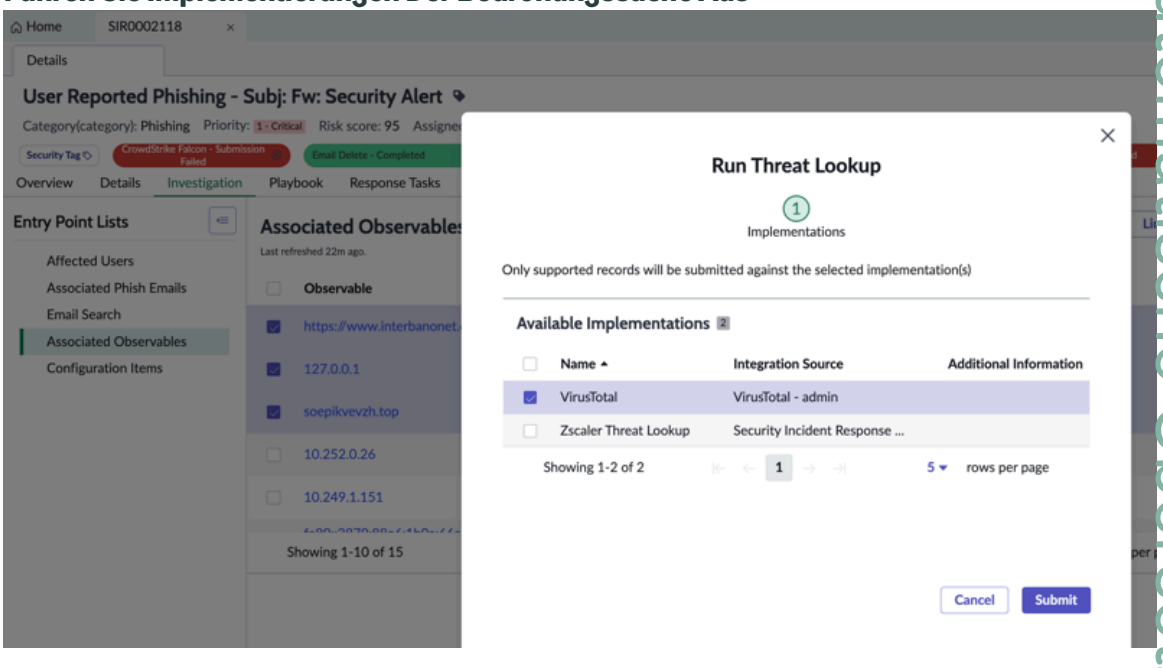
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Aktivieren Sie ein beliebiges Kontrollkästchen für erkennbare Elemente, für die Sie die Bedrohungssuche durchführen möchten.
6. Navigieren Sie zur Dropdown-Liste „Aktionen für zugehörige Listen“, die oben auf der Seite „zugehörige Listen“ angezeigt wird.
7. Wählen Sie Aus **Bedrohungssuche Ausführen** Zum Ausführen der Aktion „Threat intel-bezogene Integrationsfähigkeiten“.

Hinweis:
Die Funktion „Bedrohungssuchen ausführen“ führt Suchanfragen zu Threat Intelligence durch, um festzustellen, ob ein oder mehrere erkennbare Elemente bekannten Sicherheitsbedrohungen zugeordnet sind.

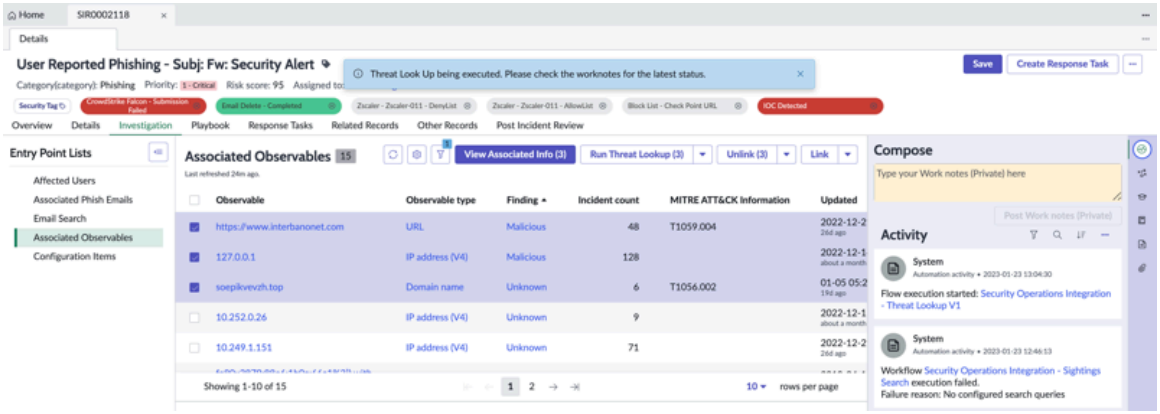
Die **Führen Sie Implementierungen Der Bedrohungssuche Aus** Der modale Bildschirm wird angezeigt.

Führen Sie Implementierungen Der Bedrohungssuche Aus



8. Wählen Sie eine oder mehrere Implementierungen aus der Liste aus.
9. Klicken Sie auf **Absenden**.
Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Nachricht angezeigt, dass die Suche ausgeführt wird. Sobald die Implementierung im Back-End verarbeitet wurde, werden die Ergebnisse im angezeigt **Ergebnisse Der Bedrohungssuche** Abschnitt „zugehörige Liste“. Außerdem wird die entsprechende Implementierungsaktivität in angezeigt **Aktivität** Abschnitt. Es werden zwei Aktivitäten angezeigt: Eine ist der Zeitpunkt, an dem die Implementierungsausführung gestartet wird, und die zweite, wenn die Ausführung abgeschlossen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Die **bedrohungsinformationen** Zugehörige Listen wie die zugehörigen Listen der zugehörigen erkennbaren Elemente werden in angezeigt **Ergebnisse Der Bedrohungssuche** Abschnitt, und **Sichtungssuche** Zugehörige Listen werden in angezeigt **Sichtungssuchergebnisse** Abschnitt unter den zugehörigen Datensätzen.

Beispiel 2: Allgemeine Eingaben: Sichtungssuche

Das folgende Beispiel zeigt die Aktion der Fähigkeit für allgemeine Eingaben.

Sie können ausführen **Sichtungssuche Ausführen** Aktion für zugehörige Integrationsfähigkeiten mit **Untersuchung** Registerkarte von SIR-Arbeitsbereich.

1. Auf der **Untersuchung** Registerkarte navigieren Sie zu **Einstiegspunktlisten** Abschnitt, der auf der linken Seite angezeigt wird.
2. Wählen Sie den entsprechenden Einstiegspunkt aus, und führen Sie die Aktion „Integrationsfähigkeit“ aus.

Hinweis:
Sie können auch zu navigieren **Zugehörige Datensätze** Registerkarte im Arbeitsbereich, um die Aktion „Integrationsfähigkeiten“ auszuführen.

Fügen Sie einer Implementierung allgemeine Eingaben hinzu

Fügen Sie allgemeine Laufzeiteingaben hinzu, die für alle ausgewählten Implementierungen gelten.

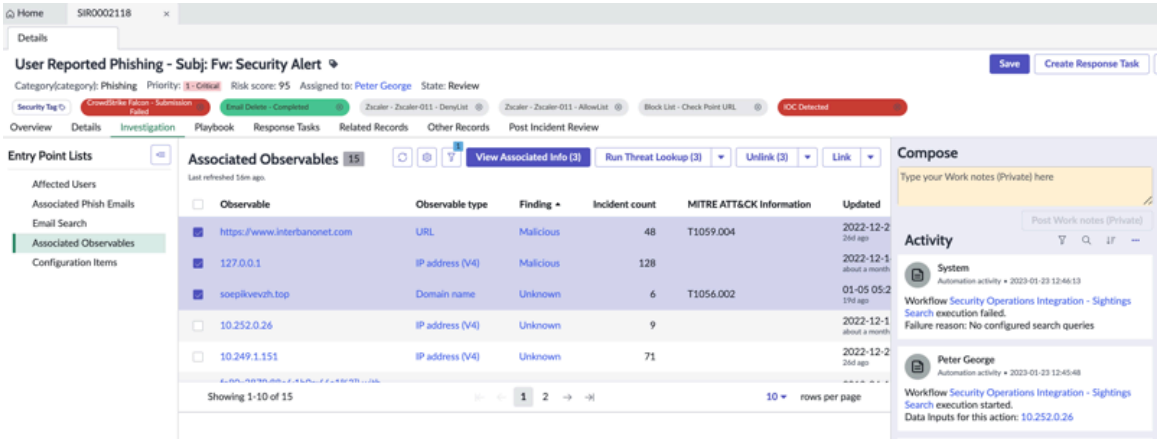
Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Die verfügbaren Implementierungen werden aufgelistet. Wählen Sie die Implementierung(en) aus. Nachdem Sie sie ausgewählt haben, werden nur die unterstützten Datensätze für jede ausgewählte(n) Implementierung(en) übermittelt.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen Security Incident.
3. Wechseln Sie zu **Untersuchung** Registerkarte des Arbeitsbereichs.
   Die Registerkarte Untersuchung mit den Einstiegspunktlisten wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

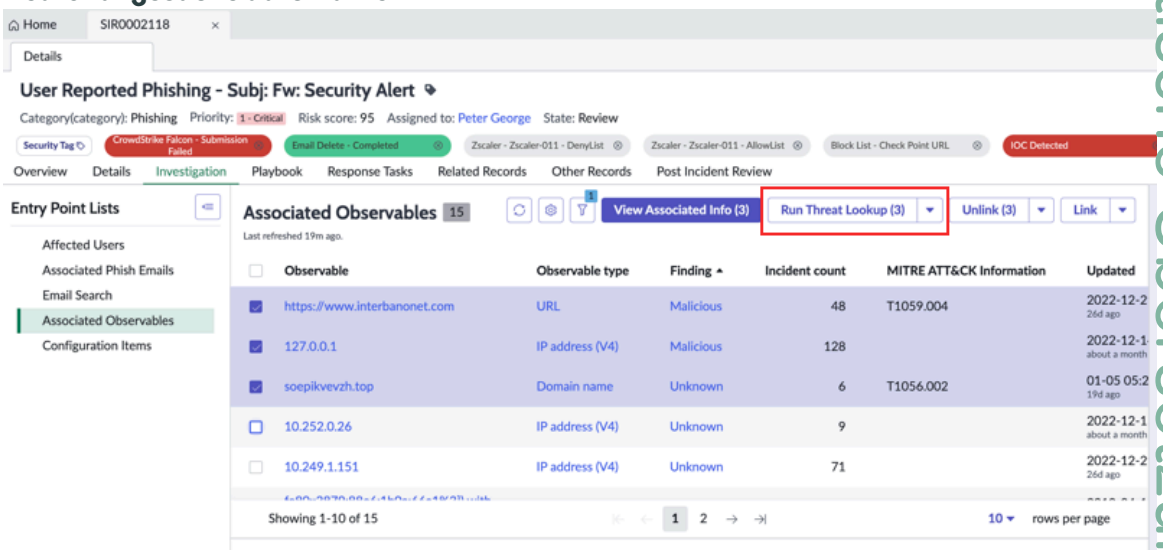


4. Wählen Sie das zugehörige erkennbare Element aus den Einstiegspunktlisten aus.
   Wählen Sie beispielsweise aus **Zugehörige erkennbare Elemente** Zugehörige Liste. Die entsprechenden Datensätze erkennbarer Elemente werden angezeigt.

Hinweis:

Sie können eine Implementierung auswählen, um eine Sichtungssuche für die ausgewählten erkennbaren Elemente durchzuführen, oder indem Sie mehrere Implementierungen auswählen.

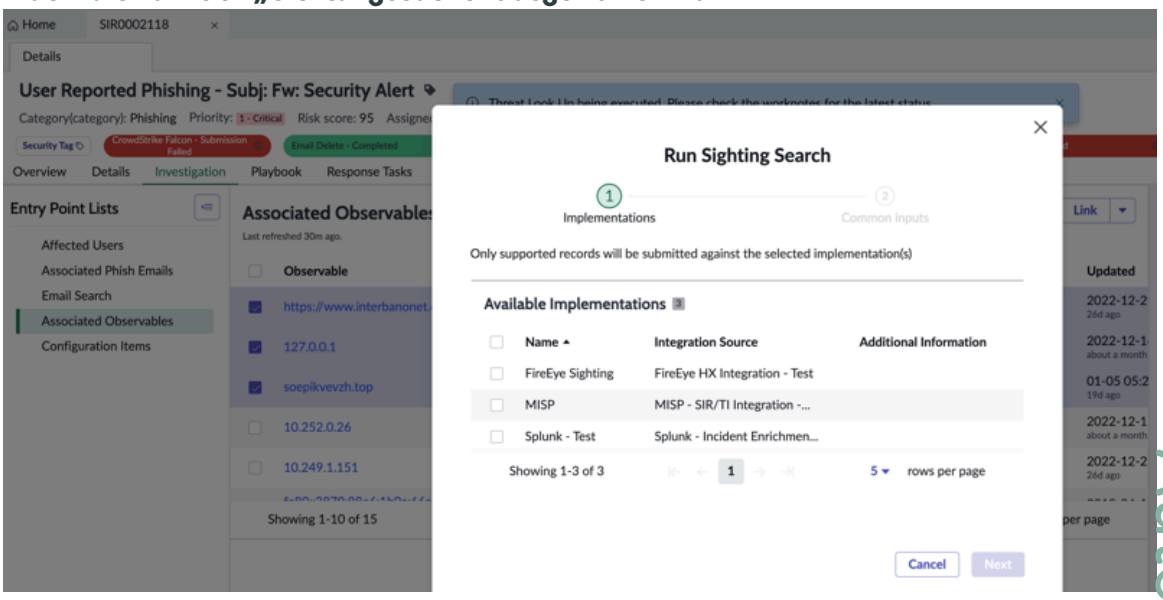
Bedrohungssuche durchführen



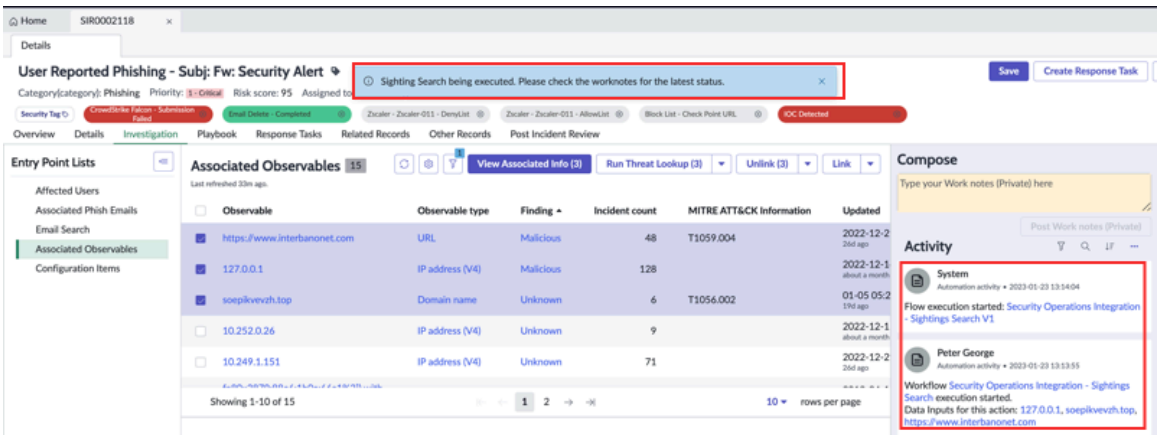
5. Aktivieren Sie ein beliebiges Kontrollkästchen für erkennbare Elemente, für die Sie die Bedrohungssuche durchführen möchten.
6. Wählen Sie Aus **Sichtungssuche Ausführen** Zum Durchführen der E-Mail-Suche.
   Das modale Dialogfeld Implementierungen der Sichtungssuche ausführen wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Beispiel, das zeigt, wie allgemeine Laufzeiteingaben hinzugefügt werden, indem die Funktion „Sichtungssuche“ ausgewählt wird



7. Wählen Sie eine oder mehrere Implementierungen aus der Liste aus.
8. Klicken Sie auf **Next (Weiter)**.
   Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Nachricht angezeigt, dass die Sichtungssuche angefordert wird. Sobald die Implementierung im Back-End verarbeitet wurde, werden die Ergebnisse im angezeigt **Sichtungssuche** Abschnitt „zugehörige Liste“. Außerdem wird die entsprechende Implementierungsaktivität im Abschnitt „Aktivität“ angezeigt. Es werden zwei Aktivitäten angezeigt: Eine ist der Zeitpunkt, an dem die Implementierungsausführung gestartet wird, und die zweite, wenn die Ausführung abgeschlossen ist.
9. Wählen Sie den allgemeinen Eingabewert für die Laufzeit aus.
10. Klicken Sie auf **Absenden**.



Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Nachricht angezeigt, dass die Sichtungssuche angefordert wird. Sobald die Implementierung im Back-End verarbeitet wurde, werden die Ergebnisse im angezeigt **Sichtungssuchergebnisse** Abschnitt „zugehörige Liste“. Außerdem wird der jeweilige Verarbeitungsstatus der Implementierungsaktivität in angezeigt **Aktivität** Abschnitt.

Beispiel 3: Fügen Sie einer Implementierung bestimmte Eingaben für Laufzeitdetails hinzu: Zusätzliche Aktionen ausführen

Fügen Sie einer Implementierung bestimmte Eingaben für Laufzeitdetails hinzu, und führen Sie zusätzliche Aktionen aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können ausführen **Führen Sie Zusätzliche Aktionen Aus** Aktion für zugehörige Integrationsfähigkeiten mit **Untersuchung** Registerkarte von SIR-Arbeitsbereich.

1. Auf der **Untersuchung** Registerkarte navigieren Sie zu **Einstiegspunktlisten** Abschnitt, der auf der linken Seite angezeigt wird.
2. Wählen Sie den entsprechenden Einstiegspunkt aus, und führen Sie die Aktion „Integrationsfähigkeit“ aus.

Hinweis:
Sie können auch zu navigieren **Zugehörige Datensätze** Registerkarte im Arbeitsbereich, um die Aktion „Integrationsfähigkeiten“ auszuführen.

Fügen Sie einer Implementierung bestimmte Eingaben hinzu

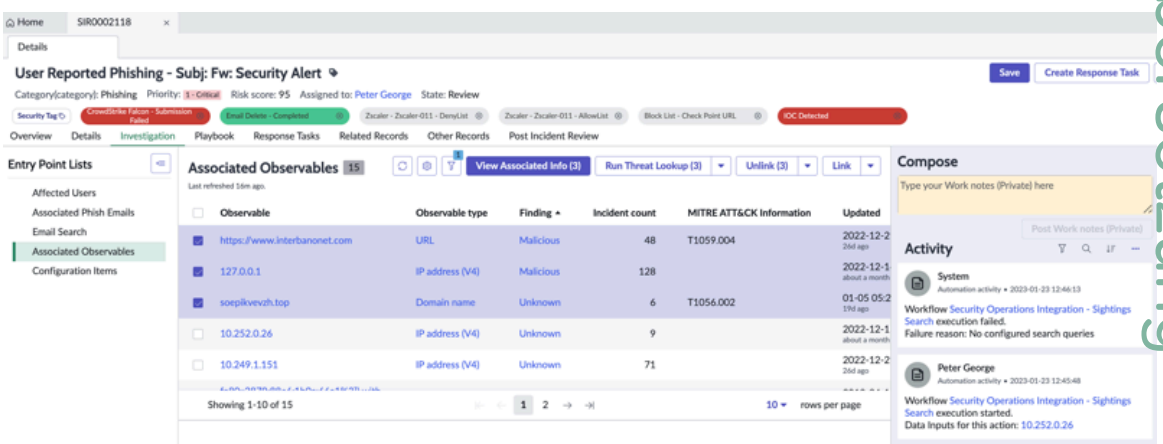
Fügen Sie je nach Bedarf bestimmte Laufzeiteingaben für jede der ausgewählten Implementierungen hinzu.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Die verfügbaren Implementierungen werden aufgelistet. Wählen Sie die Implementierung(en) aus. Nachdem Sie sie ausgewählt haben, werden nur die unterstützten Datensätze für jede ausgewählte(n) Implementierung(en) übermittelt.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen Security Incident.
3. Wechseln Sie zu **Untersuchung** Registerkarte des Arbeitsbereichs.
   Die Registerkarte Untersuchung mit den Einstiegspunktlisten wird angezeigt.

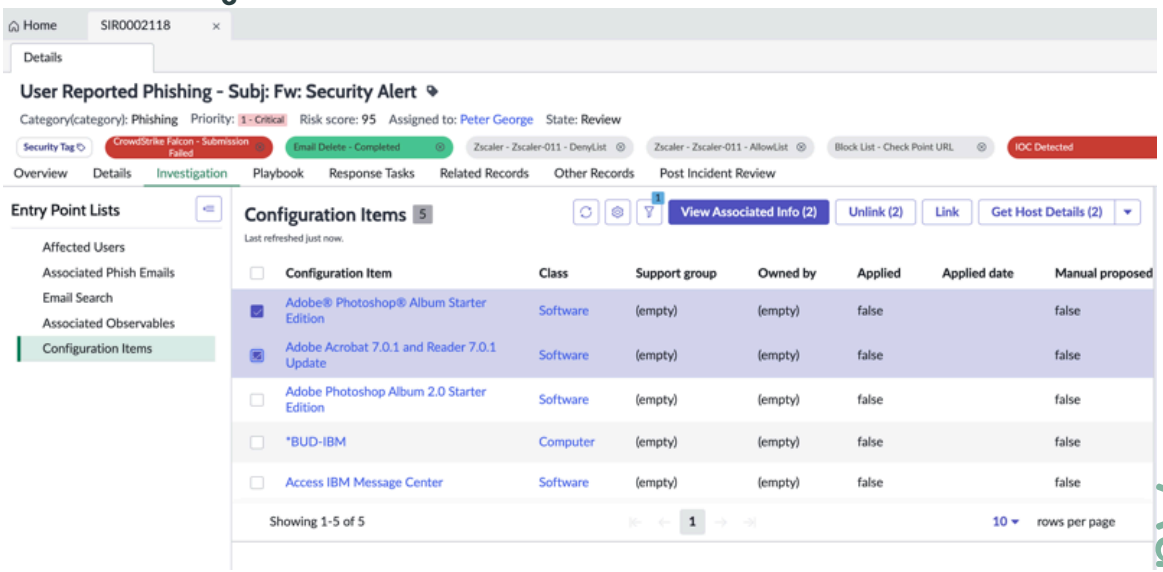


4. Wählen Sie das Konfigurationselement aus der Einstiegspunktliste aus.
   Wählen Sie beispielsweise aus **Konfigurationselement** Einstiegspunktliste. Die entsprechenden Konfigurationselementdatensätze werden angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

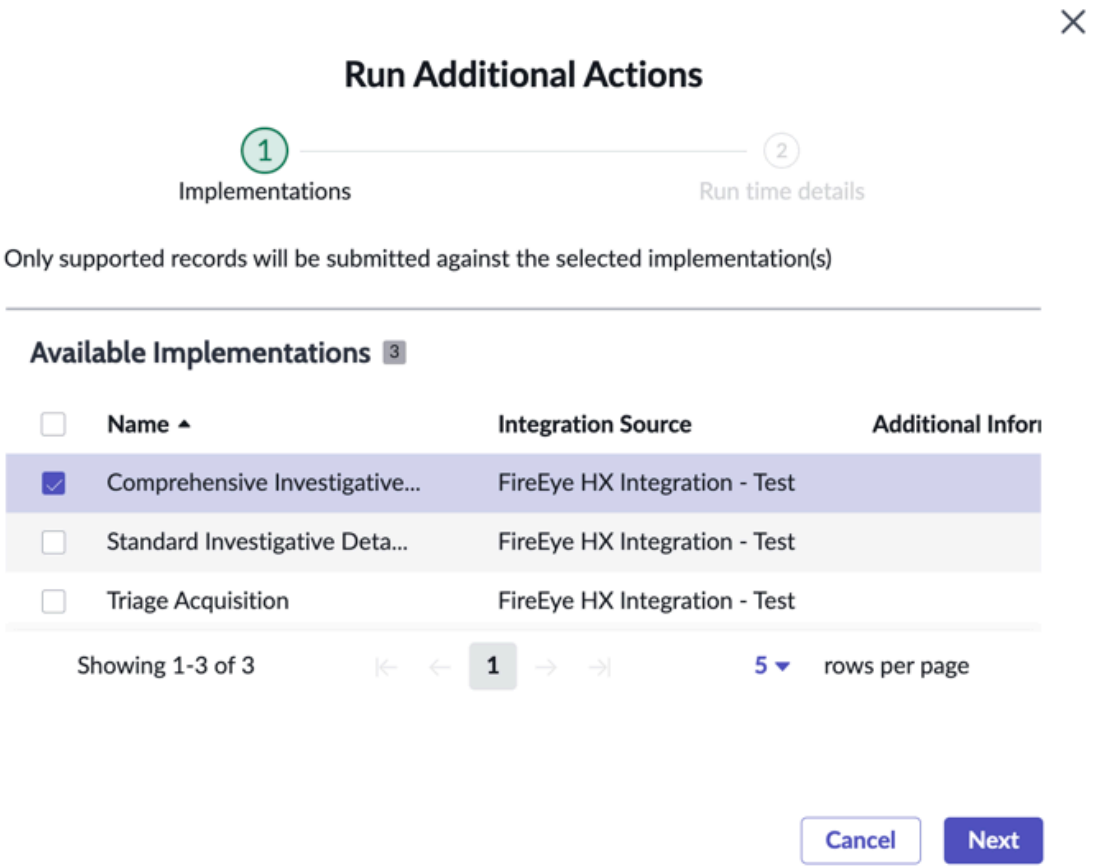
Wählen Sie Konfigurationselement Aus



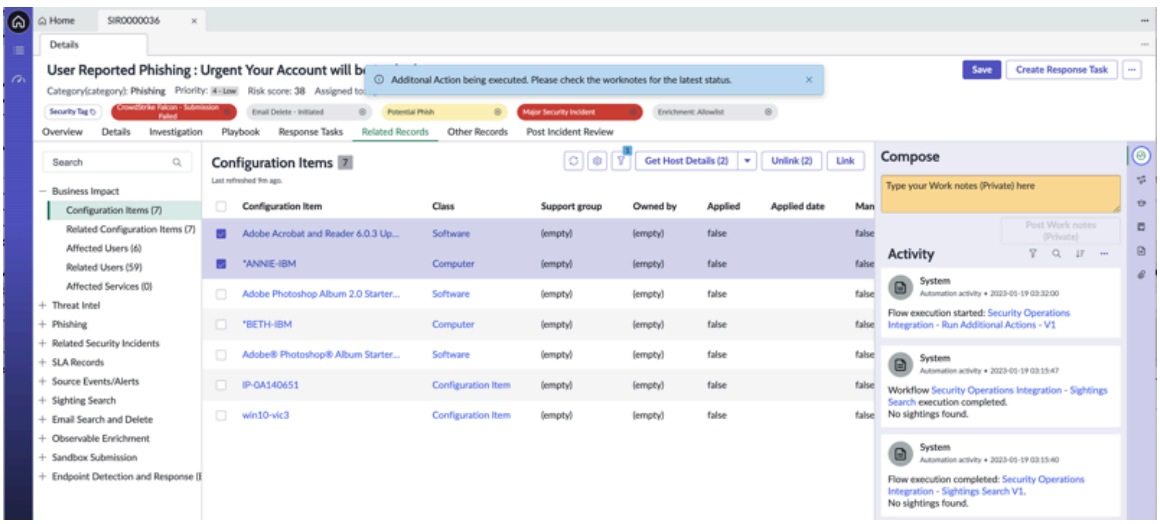
5. Wählen Sie beliebig aus **Konfigurationselement** .
6. Navigieren Sie zur Dropdown-Liste „zugehörige Listen“, die oben auf der Seite angezeigt wird.
   Für das Security Incident Configuration Item (CI) enthält die Dropdown-Listen die folgende Liste von Fähigkeitsaktionen. Die aufgeführten CI-Aktionen erfassen die Ergebnisse und speichern sie als Ergänzungsdaten für einen Security Incident:
   - Datei abrufen: Diese Fähigkeit führt die Aktion aus, um Dateien mit einem bestimmten Hash-Wert oder Dateinamen abzurufen.
   - Host isolieren: Diese Fähigkeit schränkt Systemverbindungen zu anderen Geräten ein.
   - Hostdetails abrufen: Diese Fähigkeit ruft die Hostdetails, Details der angemeldeten Anwender und andere Ergänzungsfunktionen ab.
   - Zusätzliche Aktionen ausführen: Diese Fähigkeit führt die zusätzlichen Aktionen über die Standardaktionen hinaus aus.
   - Netzwerkstatistiken abrufen: Diese Fähigkeit ruft die Netzwerkstatistiken für eine betroffene Ressource ab.
   - Laufenden Prozess abrufen: Diese Fähigkeit ruft eine Liste der laufenden Prozesse für ein Konfigurationselement (CI) von einem Host ab.
   - Angemeldete Anwender abrufen: Diese Fähigkeit sammelt die Daten angemeldeter Anwender und verknüpft sie mit dem Security Incident.
7. Wählen Sie Aus **Führen Sie Zusätzliche Aktionen Aus** Zum Ausführen der Aktion „Threat intel-bezogene Integrationsfähigkeiten“.
   Das Dialogfeld „zusätzliche Implementierungen ausführen“ wird angezeigt.
8. Wählen Sie eine oder mehrere Implementierungen aus der Liste aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Klicken Sie auf **Next (Weiter)**.
   Sie werden jetzt zum nächsten Schritt verschoben, um die Laufzeitdetails hinzuzufügen.
10. Geben Sie einen Kommentar ein, der der Aktion zugeordnet werden soll.
11. Klicken Sie auf **Absenden**.



Nachdem die ausgewählten Datensätze übermittelt wurden, wird eine Nachricht angezeigt, dass die Anforderung für zusätzliche Aktionen ausgeführt wird. Außerdem wird der jeweilige Fortschritt der Implementierungsaktion in angezeigt **Aktivität** Abschnitt.

12. Zeigen Sie die Ergebnisse im Abschnitt „zugehörige EDR-Liste“ an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

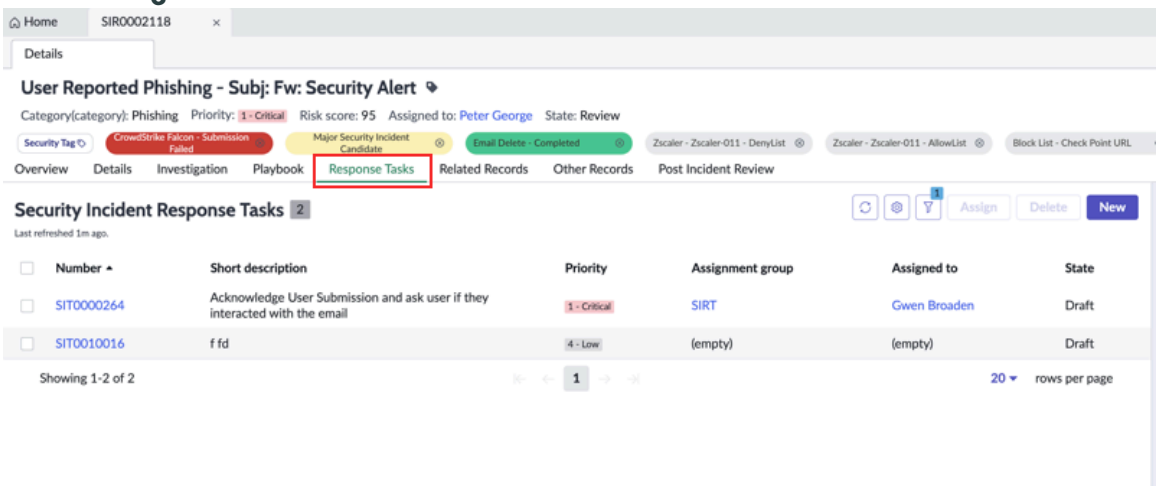
Security Incident Response-Aufgaben

Alle Antwortaufgaben, die einem Security Incident zugeordnet sind, werden im Abschnitt Antwortaufgaben angezeigt.

Der Analyst kann:

- Erstellen Sie eine neue Antwortaufgabe
- Weisen Sie sich selbst oder anderen Antwortaufgaben zu
- Löschen Sie Antwortaufgaben

Antwortaufgaben im Arbeitsbereich



Hinweis:
Um schnelle Änderungen an den Antwortaufgaben vorzunehmen. Wählen Sie die Antwortaufgabe aus, und eine Liste der Antwortaufgaben wird angezeigt. Wählen Sie den Datensatz aus, nehmen Sie Änderungen vor, und speichern Sie die Antwortaufgabe.

Erstellen Sie eine Antwortaufgabe

Erstellen Sie Antwortaufgaben, um separate Aktionen nachzuverfolgen, die zur Reaktion auf das Sicherheitsproblem ausgeführt werden sollen.

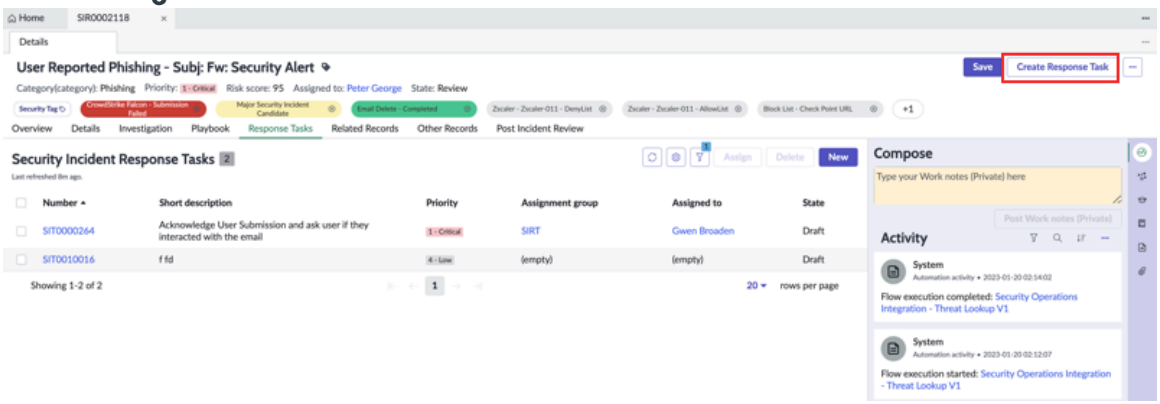
Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Klicken Sie auf **Erstellen Sie Eine Antwortaufgabe** Über die UI-Aktionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe erstellen



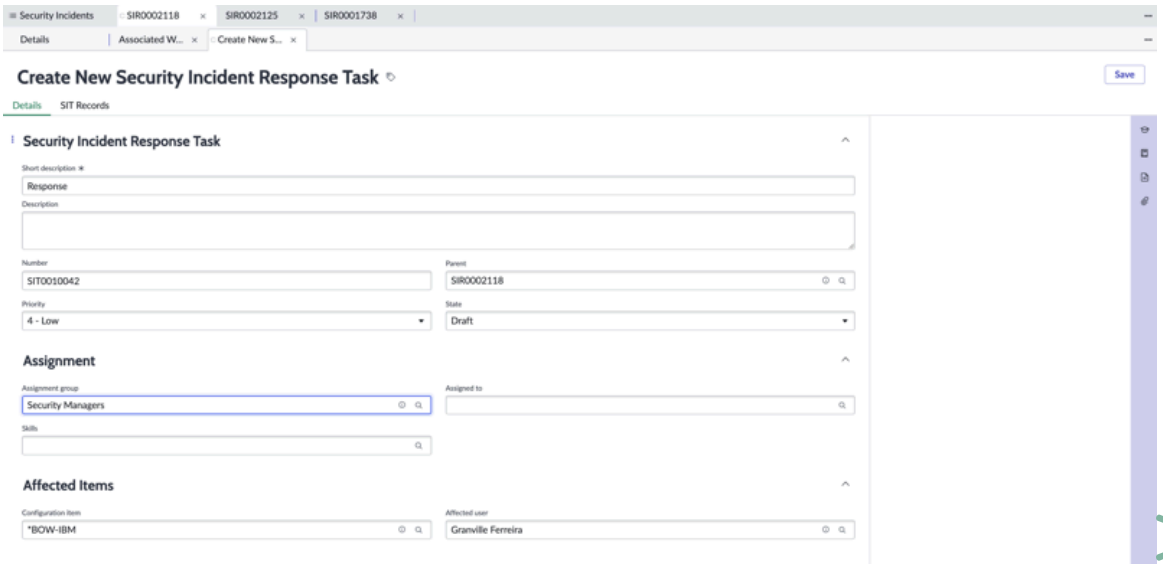
3. Füllen Sie die entsprechenden Felder im Formular aus.

Security Incident

Feld	Beschreibung
Kurzbeschreibung	Eine Beschreibung von Security Incident Response Aufgabe.
Beschreibung	Eine Beschreibung für die ausgewählte Aufgabe.
Anzahl	Eindeutige Nummer, die für einen Security Incident automatisch generiert wird.
Übergeordnet	Die Nummer des zugehörigen Security Incidents.
Priorität	Die Priorität, mit der bestimmt wird, wann diese Aufgabe ausgeführt wird.
Status	Der aktuelle Status der Sicherheitsantwortaufgabe. Standardmäßig ist der Anfangsstatus **Entwurf** .
Zuweisungsgruppe	Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird.
Zugewiesen an	Die Person, die der Ausführung der Aufgabe zugewiesen ist.
Kompetenzen	Die zur Ausführung dieser Aufgabe erforderliche Kompetenz. Suchen Sie in der Suche, und wählen Sie die erforderliche Kompetenz aus.
Betroffene Elemente	Die vom Sicherheitsproblem betroffenen Elemente.
Konfigurationselement	Das vom Sicherheitsproblem betroffene Konfigurationselement.
Betroffener Anwender	Die vom Sicherheitsproblem betroffene Person.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



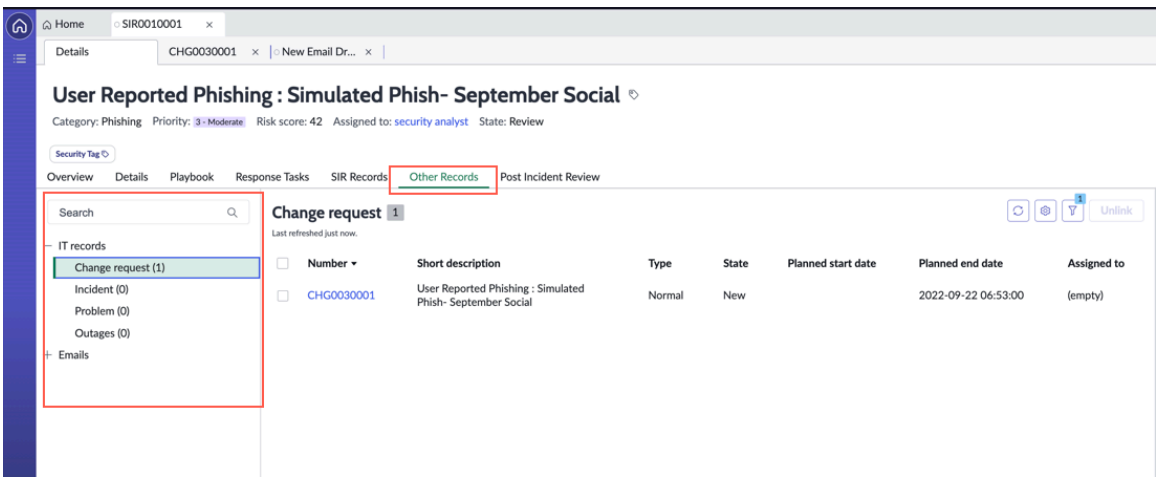
4. Klicken Sie auf **Speichern**.
   Die neue Antwortaufgabe (SIT) wird erstellt.

Security Incident Response – Andere Datensätze

In diesem Abschnitt werden die anderen Datensätze angezeigt, z. B. IT-bezogene Datensätze und E-Mail-Datensätze. Unter IT-Datensätzen werden Incident, Change-Anforderung, Problem und Ausfälle angezeigt.

Unter E-Mail werden Entwurf, gesendete E-Mails und empfangene E-Mails angezeigt.

Andere Datensätze



Incident erstellen

Erstellen Sie einen Incident in einem Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst.

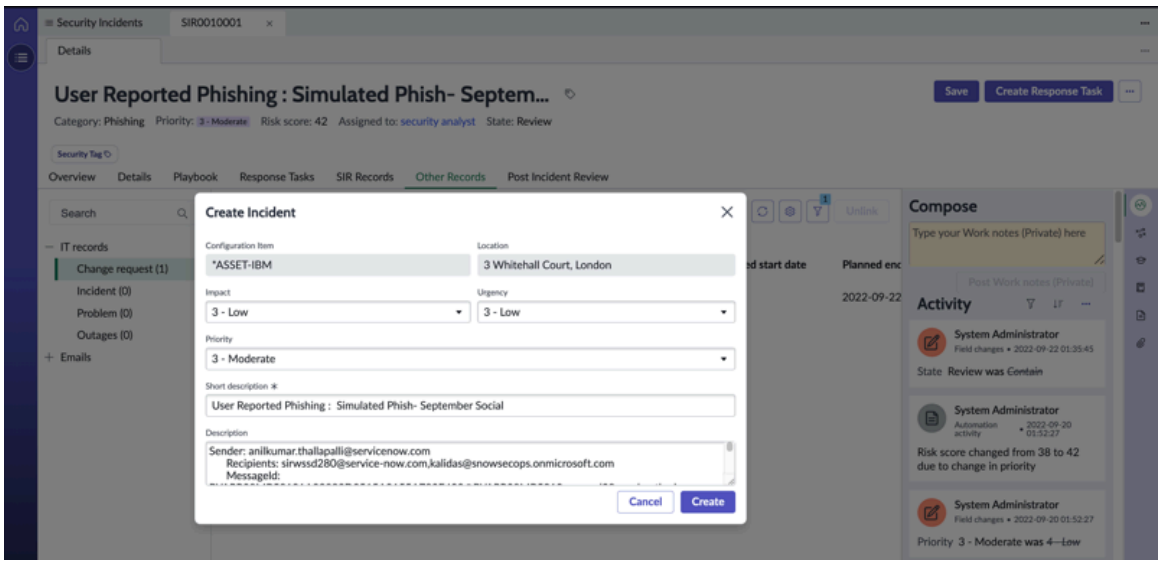
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen beliebigen Incident-Datensatz.

Automatische Übersetzung

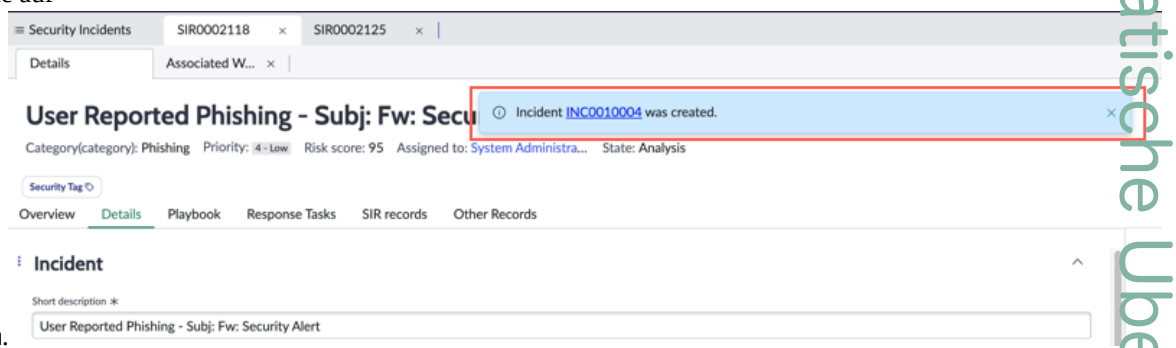
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Incident erstellen**.



4. Geben Sie die Details ein, z. B. Konfigurationselement, Auswirkung, Dringlichkeit, Standort, Priorität, und Kurzbeschreibung.

5. Klicken Sie auf **Erstellen**.



6. Ein Incident wird erstellt.

Verknüpfen Sie mehrere ITSM-Incidents

Link IT Service Management(ITSM) Incidents Bezieht sich auf einen Security Incident.

Vorbereitungen

Hinweis:
Sie können auch einen erstellen ITSM Incident, der mit einem Security Incident verknüpft werden soll. Weitere Informationen finden Sie unter Incident erstellen.

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Wählen Sie aus Liste Symbol (Symbol.
3. Öffnen Die Incident-Datensatz.
4. Wählen Sie aus **Andere Datensätze** Registerkarte.
5. Unter **IT-Datensätze** , Wählen Sie aus **Incident** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie zur klassischen UI wechseln, unter **Zugehörige Datensätze** Registerkarte, die **Incident** Feld wird entfernt.

6. Wählen Sie Aus **Link** .
7. S Auswählen Die ITSM Incidents, die Sie mit dem ausgewählten Security Incident verknüpfen möchten.
8. Wählen Sie Aus **Link** .

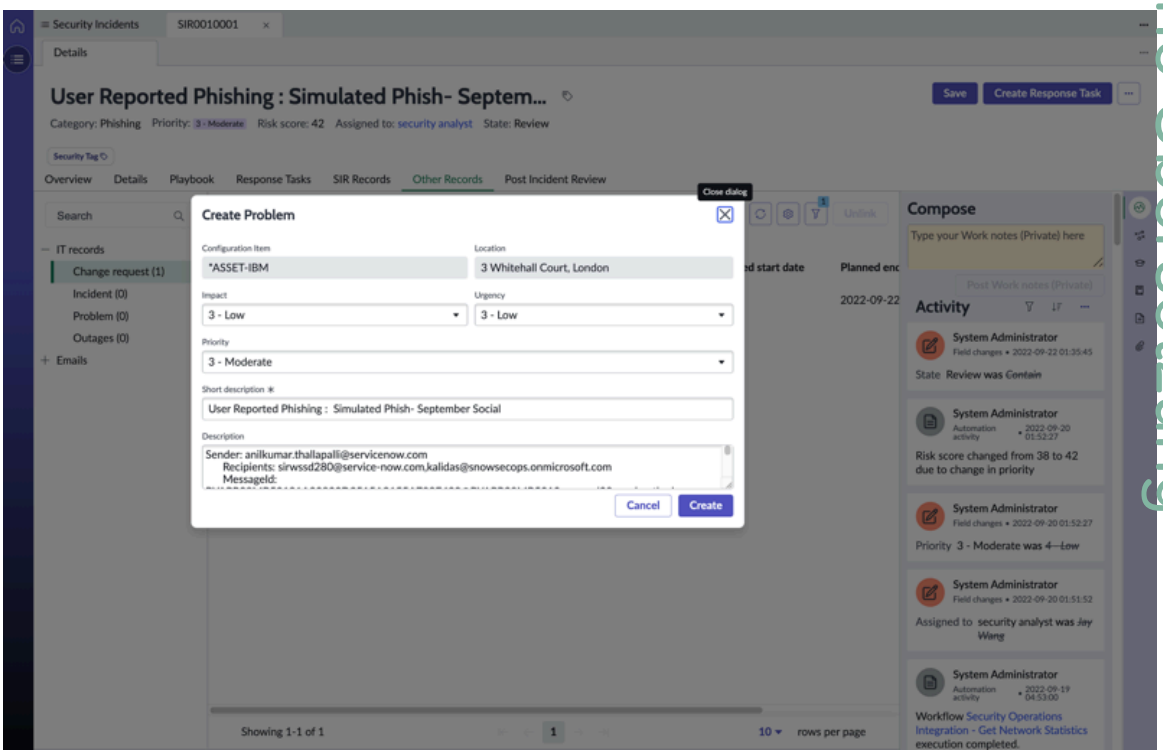
Ergebnisse
Ausgewählt ITSM Incidents werden aufgelistet In IT-Datensätze Abschnitt des ausgewählten Security Incidents Datensatz .

Problemaufgaben erstellen

Erstellen Sie eine Problemaufgabe.

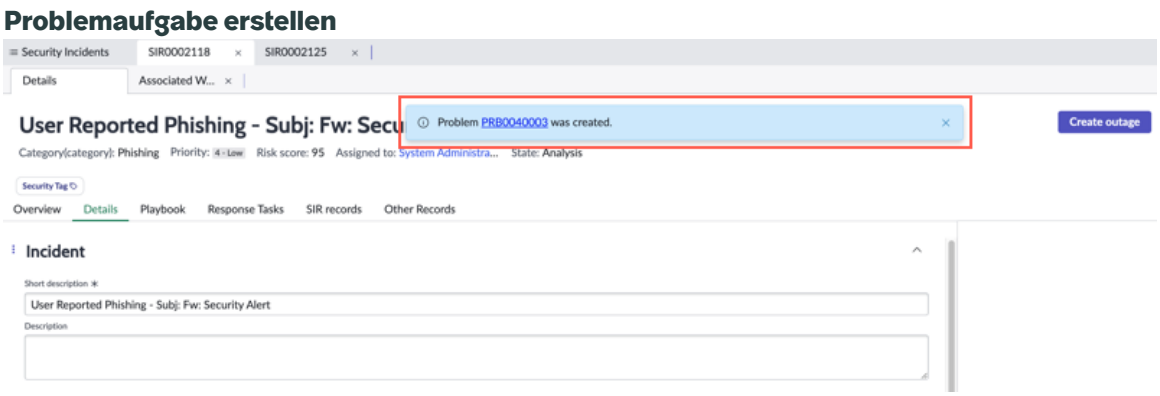
Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen beliebigen Incident-Datensatz.
3. Klicken Sie Auf **Problem Erstellen** .



4. Geben Sie die Details ein, z. B. Konfigurationselement, Standort, Auswirkung, Dringlichkeit, Priorität, und Kurzbeschreibung.
5. Klicken Sie auf **Erstellen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Eine Problemaufgabe wird erstellt.

Change-Anforderungen erstellen

Erstellen Sie eine Change-Anforderung.

Vorbereitungen

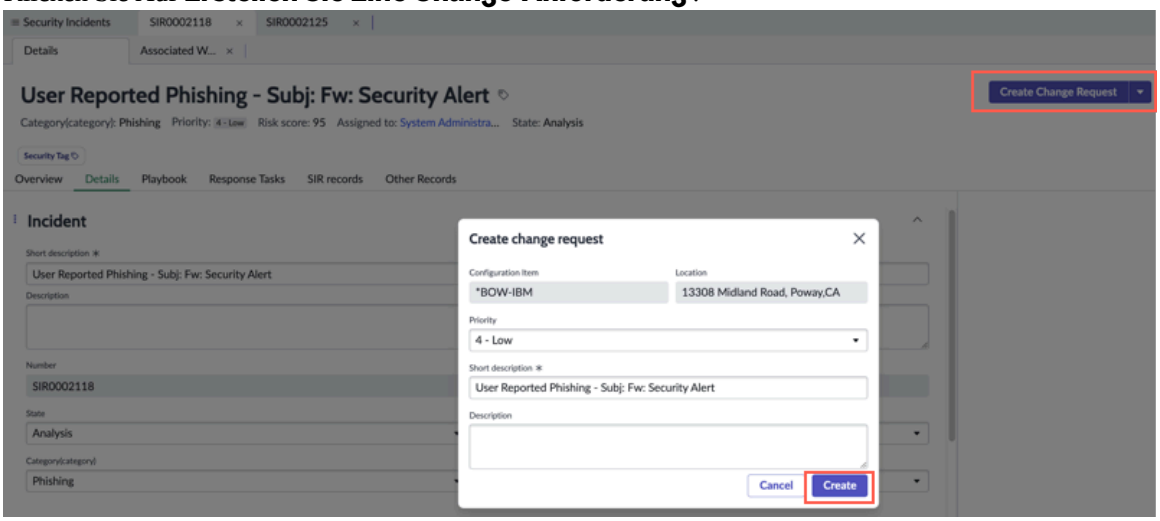
Erforderliche Rolle: sn_si.Analyst.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.

2. Öffnen Sie einen beliebigen Incident-Datensatz.

3. Klicken Sie Auf **Erstellen Sie Eine Change-Anforderung** .

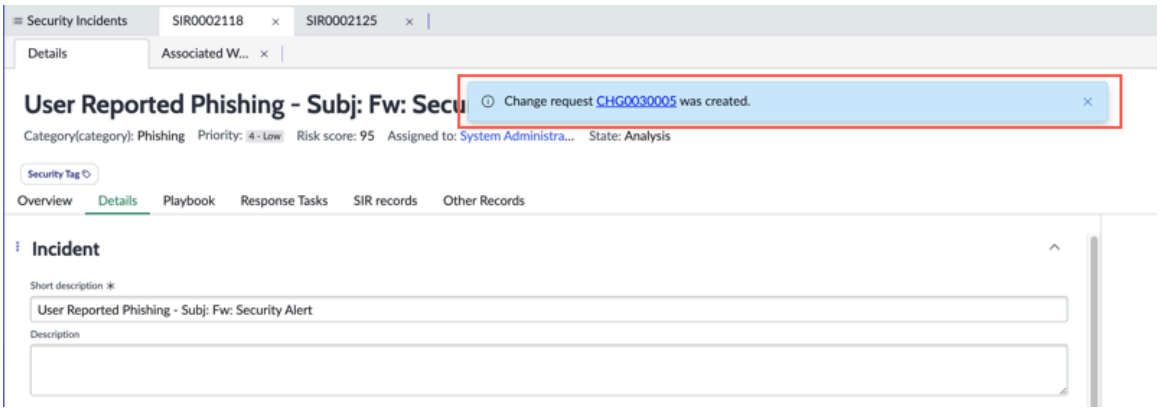


4. Geben Sie die Details ein, z. B. Konfigurationselement, Standort, Priorität und Kurzbeschreibung.

5. Klicken Sie auf **Erstellen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Eine Change-Anforderung wird erstellt.

Ausfall erstellen

Erstellen Sie einen Ausfall aus einem Incident, um die Ausfallzeit eines Konfigurationselements nachzuverfolgen.

Vorbereitungen

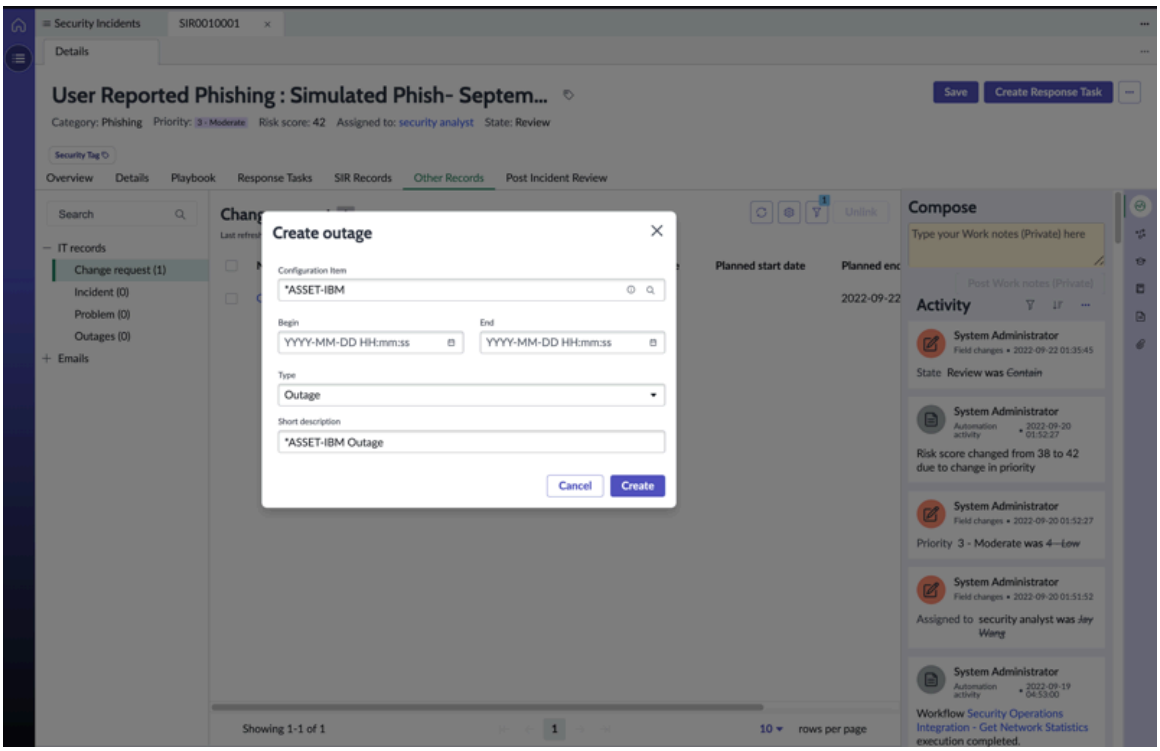
Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.

2. Öffnen Sie einen beliebigen Incident-Datensatz.

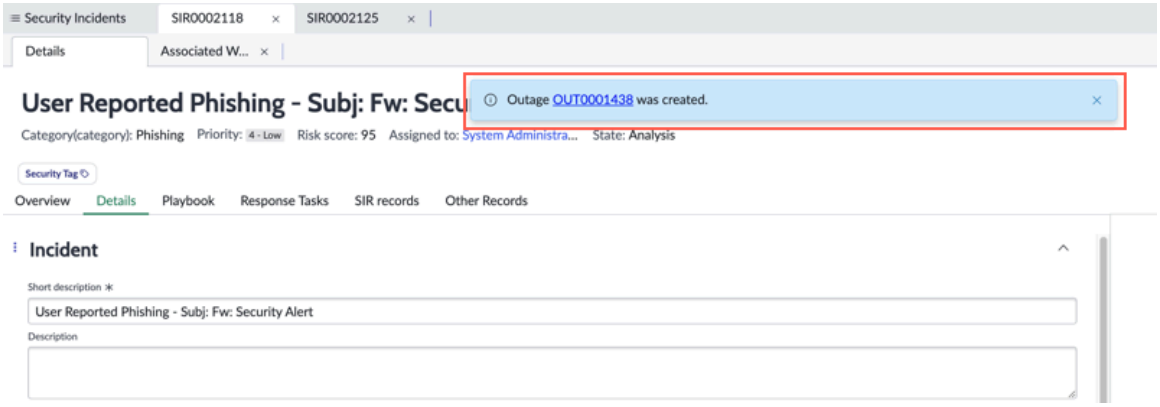
3. Klicken Sie Auf **Ausfall erstellen** .



4. Geben Sie die Details wie Konfigurationselement, Startdatum, Enddatum, Typ und Kurzbeschreibung ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Erstellen**.



Verfassen Sie E-Mails

Als Analyst können Sie E-Mails direkt aus Security Incidents verfassen.

Vorbereitungen

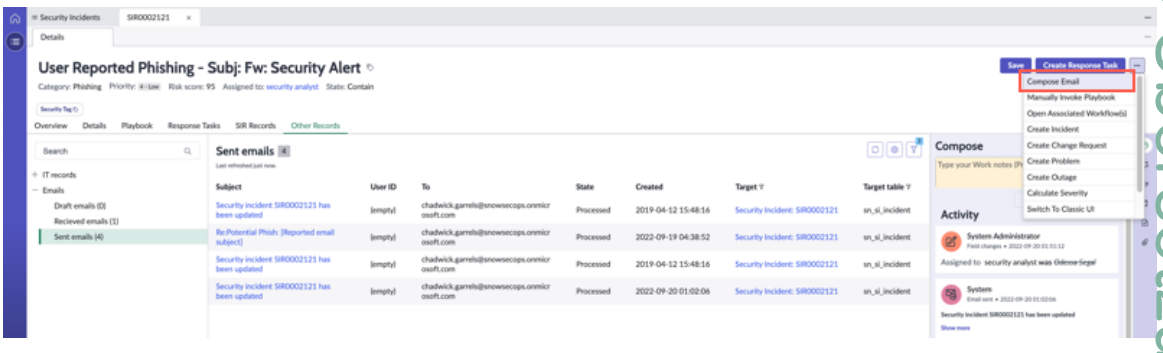
Erforderliche Rolle: sn_si.Analyst

Prozedur

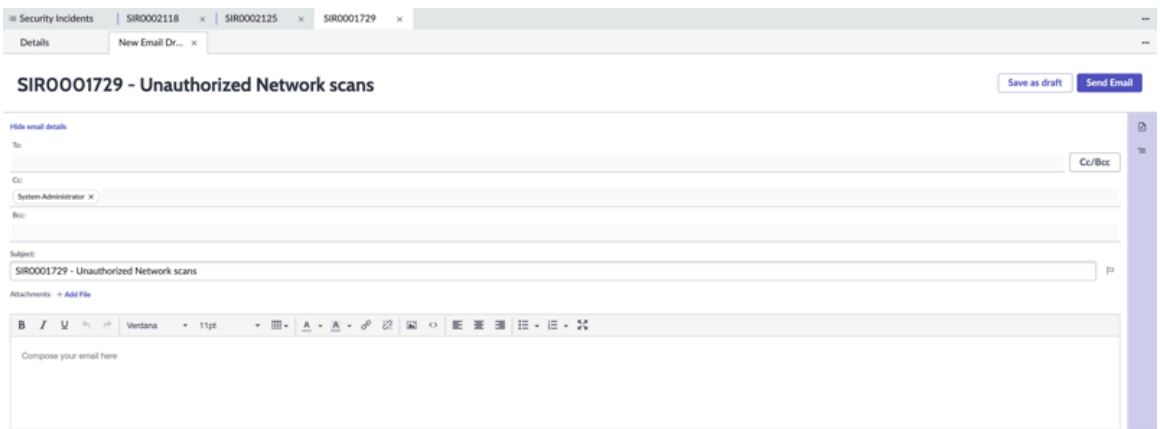
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.

2. Wählen Sie den Incident aus, für den Sie eine E-Mail verfassen möchten, und öffnen Sie ihn.

3. Klicken Sie auf den Überlauf, und wählen Sie aus **E-Mail Verfassen** .



4. Geben Sie ein **Bis** Und **CC** Feld.

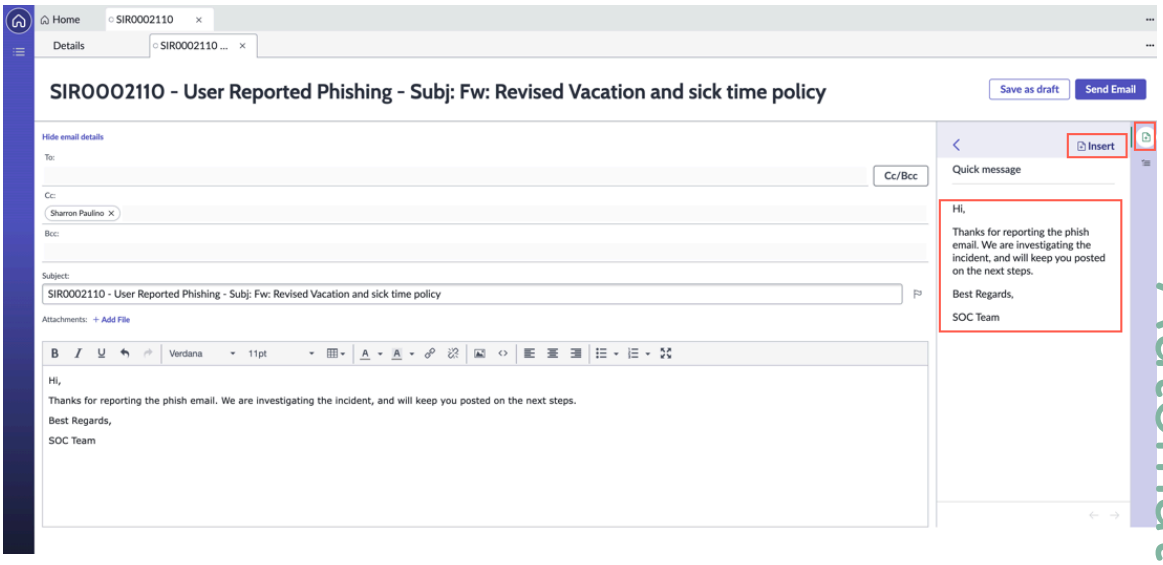


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Hinzufügen** Anhänge, falls vorhanden.

6. Klicken Sie im E-Mail-Formular auf **Schnellnachrichten** Zum Anzeigen der Schnellnachrichten, die auf der rechten Seite von angezeigt werden **Verfassen Sie E-Mails** Abschnitt.
   Die verfügbaren Schnellnachrichten werden angezeigt. Wählen Sie die Nachricht aus, und klicken Sie auf **Einfügen** . Die Nachrichten werden in den Text der E-Mail eingefügt.



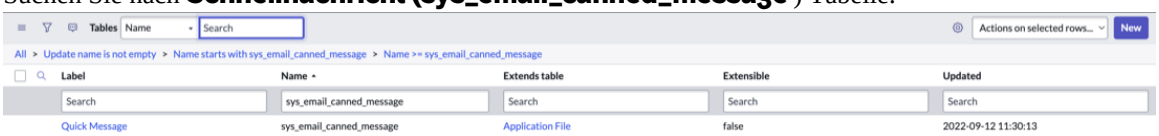
7. Verfassen Sie Ihre E-Mail, und klicken Sie auf **E-Mail Senden** .

> **Hinweis:**
> Sie können eine E-Mail als Entwurf speichern. Diese E-Mail-Entwürfe sind auf der Registerkarte „andere Datensätze“ verfügbar.

So konfigurieren Sie Schnellnachrichten:

a. Navigieren zu **Systemdefinitionen** > **Tabellen**an.

b. Suchen Sie nach **Schnellnachricht (sys_email_canned_message**) Tabelle.



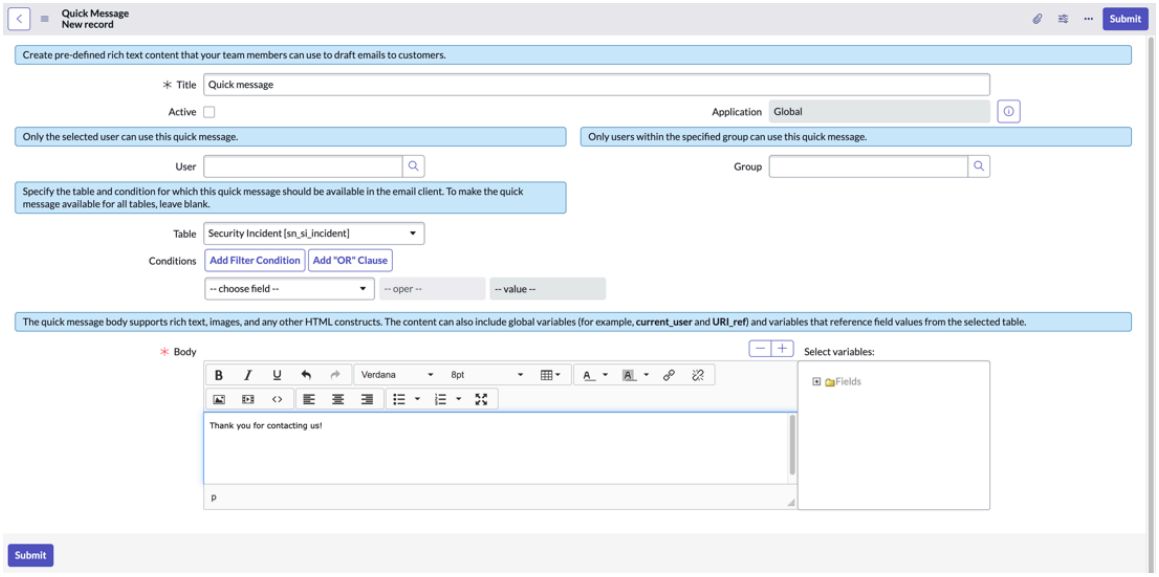
c. Gehe zu **Zugehörige Links** > **Liste anzeigen**an.

d. Erstellen **Neu** .

e. Geben Sie ein **Titel** , **Textkörper der Nachricht** , Wählen Sie aus **Tabelle: Security Incident (sn_si_Incident)** Und **Aktiv** Kontrollkästchen.

Automatische Übersetzung

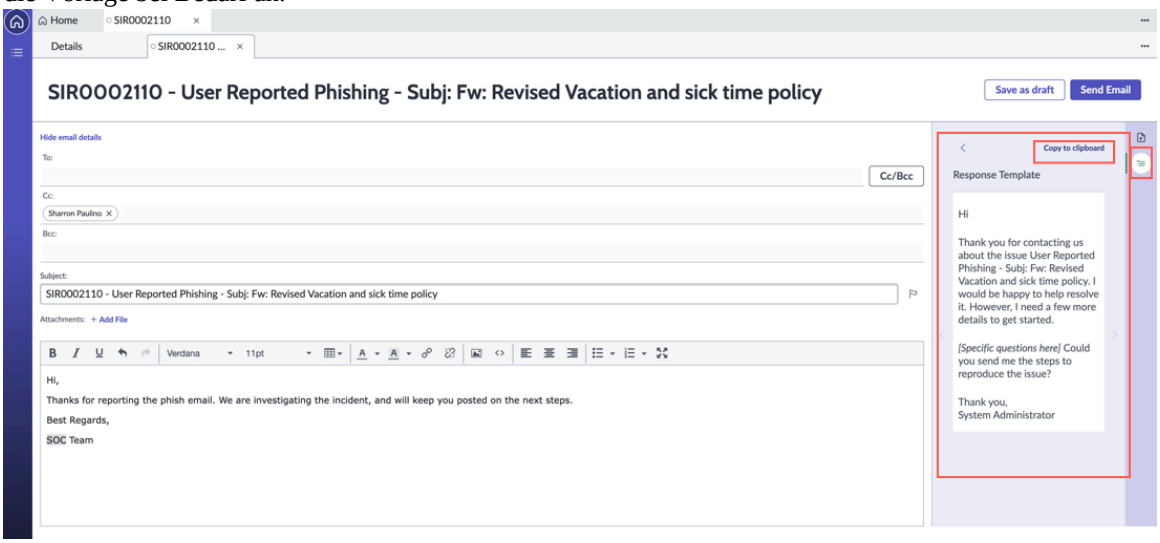
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



f. Klicken Sie auf **Absenden**.
Nachdem ein neuer Eintrag in der Tabelle erstellt wurde, wird die Schnellnachricht im Kontextmenü angezeigt.

8. Klicken Sie Auf **Vorlagen** Um bei Bedarf eine Vorlage hinzuzufügen.

9. Wählen Sie aus **Antwortvorlage** Und klicken Sie auf **In Zwischenablage kopieren** Und wenden Sie die Vorlage bei Bedarf an.

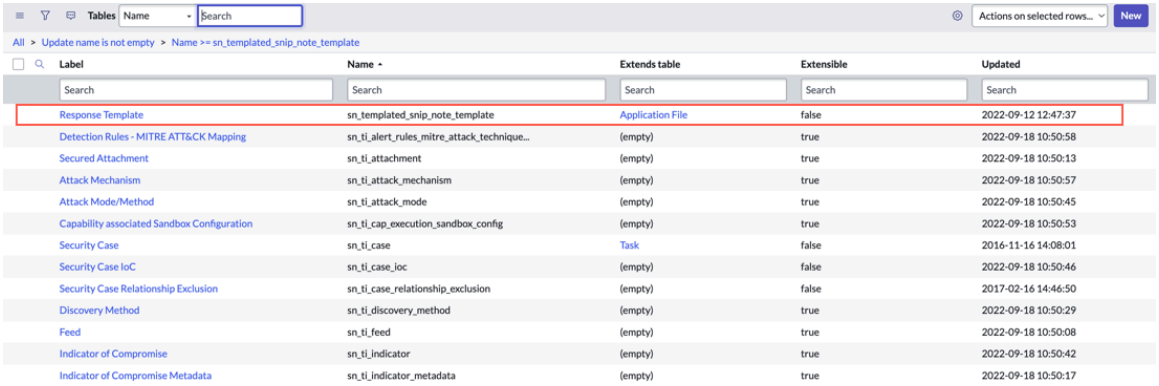


So konfigurieren Sie Antwortvorlagen:

a. Navigieren zu **Systemdefinitionen** > **Tabellen**an.

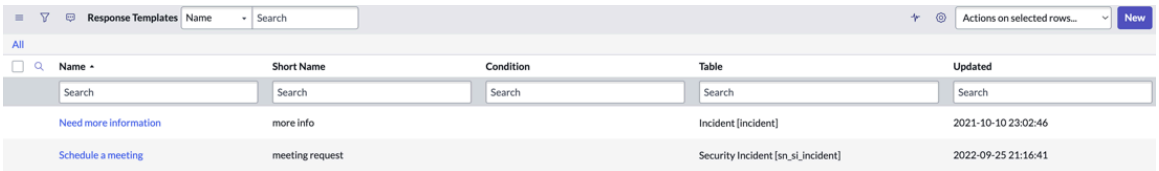
b. Suchen Sie nach **Antwortvorlage (sn_templates_snip_note_template)** Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

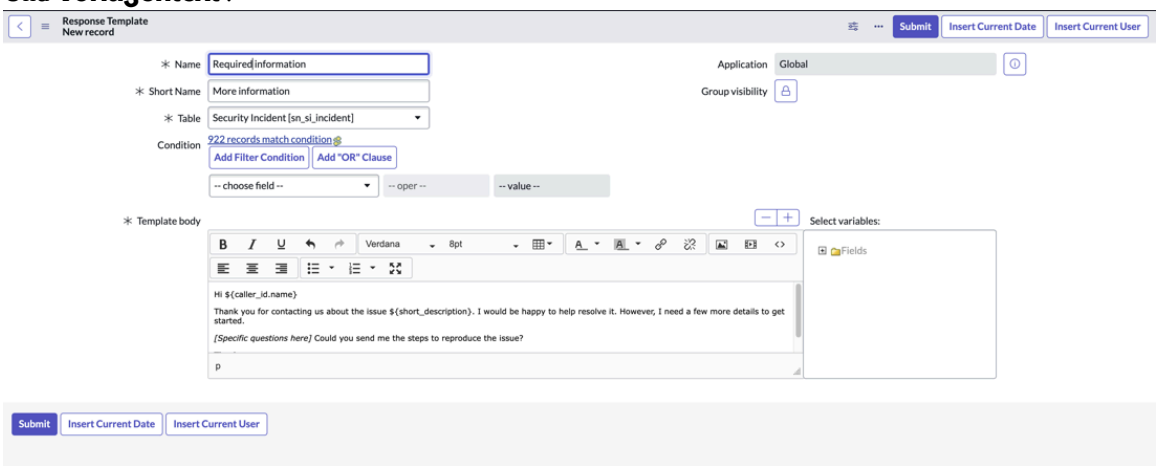


c. Gehe zu **Zugehörige Links** > **Liste anzeigen**an.

d. Erstellen **Neu** .



e. Geben Sie ein **Name** , **Kurzname** , Wählen Sie aus **Tabelle: Security Incident (sn_si_Incident)** Und **Vorlagentext** .



f. Klicken Sie auf **Absenden**.
Nachdem ein neuer Eintrag in der Tabelle erstellt wurde, wird die neue Vorlage im Kontextmenü angezeigt.

Security Incident Response – Überprüfung Nach Incident

Die Überprüfung nach Incident wird angezeigt, wenn ein Incident in den Status „Überprüfen“ verschoben wird.

Weitere Informationen zur Durchführung der Aktivitäten nach dem Incident finden Sie unter Prüfbericht nach Incident

Die Überprüfung nach Incident besteht aus den folgenden Abschnitten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Bewertungen
2. Berichte

Im Arbeitsbereich „Security Incident Response“ können Sie mithilfe dieser beiden neuen UI-Aktionen Bewertungen anfordern und vornehmen.

Name	Beschreibung
Bewertungen	Bewertung zeigt alle Bewertungen an, die dem Security Incident mit anderen Bewertungen verknüpft sind. Der Analyst kann Bewertungen vornehmen und Bewertungen anfordern. • **Nehmen Sie Bewertungen vor** : Klicken Sie auf **Nehmen Sie Bewertungen vor** Um die Bewertungen durchzuführen (falls zutreffend) und die Bewertung abzuschließen. Vor Abschluss der Bewertung lautet der Status des Security Incidents „bereit zur Bearbeitung“, und das Fälligkeitsdatum des Incident wird in Rot angezeigt. • Bewertungen anfordern: Klicken Sie auf **Bewertung anfordern** Für zusätzliche Bewertungen und können Sie die neuen Anwender hinzufügen, die Sie anfordern möchten. **Hinweis:** Anwender, die bereits angefordert haben, werden in diesem Abschnitt nicht angezeigt. Jede Bewertung für diesen Incident wurde basierend auf den Bedingungen konfiguriert, die für die Überprüfung nach Incident festgelegt wurden. Sie ist entweder obligatorisch oder optional.
Berichte	Ändern Sie die Laufzeitkonfigurationen, und generieren Sie den Bericht. Wählen Sie die Berichtsinstanz aus, ändern Sie die Filter, und speichern Sie den Bericht. Der Analysten kann eine Vorschau des PIR-Berichts anzeigen und herunterladen.

TISC-Integration in SIR Workspace

Der folgende Abschnitt enthält Informationen zur Integration des Threat Intelligence Security Center aus dem SIR-Arbeitsbereich-Kontext.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Senden Sie Daten aus SIR Workspace an TISC

Erfahren Sie, wie die Daten zusammenarbeiten und zwischen den Arbeitsbereichen Threat Intelligence Security Center (TISC) und Security Incident Response (SIR) geteilt werden, indem Sie die in den folgenden Abschnitten erläuterten Verfahren befolgen.

Systemeigenschaften zum Senden von Daten

Überprüfen Sie die Systemeigenschaften für TISC-Integrationen, die mit SIRW kombiniert werden sollen. Sie können diese Eigenschaften konfigurieren, um zu steuern, wie beide Anwendungen die Integrationen verwalten.

Wichtige Überlegungen

Die Systemeigenschaften für TISC-Integrationen bieten erweiterte Konfigurationsoptionen, wie die Anwendung erkennbare Elemente und Ergänzungen verarbeitet.

1. Um Systemeigenschaften von TISC-Integrationen in SIRW festzulegen, navigieren Sie zu **Systemeigenschaften** Für Threat Intelligence und greifen Sie auf die Tabelle [sys_properties] zu.
2. Die Systemeigenschaften steuern und behandeln das Verhalten jedes einzelnen Daten-Push-Vorgangs.
3. Wenn die Eigenschaft aktiviert ist, werden die Daten automatisch übertragen, wenn die Daten erkennbarer Elemente oder Ergänzungen im SIR-Arbeitsbereich generiert werden.
4. Wenn die Eigenschaft deaktiviert ist, werden die Daten manuell übertragen, sodass Anwender Daten mithilfe der UI-Aktionen aus dem SIR-Arbeitsbereich veröffentlichen können.

Die folgenden Listen zeigen die Systemeigenschaften für die TISC – SIR-Integration:

- Daten erkennbarer Elemente sowohl automatisch als auch manuell von SIR übertragen: Aktivieren Sie die Eigenschaft „sn_ti.allow_observable_and_Enrichment_Records_Push“, um die Daten entweder automatisch oder manuell zu übertragen. Wenn diese Eigenschaft deaktiviert ist, wird sowohl der automatische als auch der manuelle Modus für alle Daten-Push-Vorgänge von SIR deaktiviert.
- Ergebnisse der Bedrohungssuche veröffentlichen: Aktivieren Sie diese Systemeigenschaft sn_ti.automatic_push_threat_lookup_results, um Bedrohungssuchdaten automatisch an TISC zu übertragen. Wenn diese Option deaktiviert ist, können Sicherheitsanalysten die Bedrohungssuchdaten weiterhin manuell veröffentlichen.
- Sichtungssuchergebnisse an TISC verschieben: Aktivieren Sie diese Systemeigenschaft sn_ti.automatic_push_sighting_results_to_tisc, um Sichtungssuchdaten automatisch an TISC zu übertragen. Wenn diese Option deaktiviert ist, können Sicherheitsanalysten die Sichtungssuchdaten weiterhin manuell veröffentlichen.
- Erkennbare Elemente übertragen: Aktivieren Sie sn_ti.automatic_push_observable_to_tisc diese Systemeigenschaft, um Daten erkennbarer Elemente automatisch an TISC zu übertragen. Wenn diese Option deaktiviert ist, können Sicherheitsanalysten die Daten erkennbarer Elemente weiterhin manuell veröffentlichen.
- Ergänzungsergebnisse veröffentlichen: Aktivieren Sie diese Systemeigenschaft sn_ti.automatic_push_enichment_results, um Ergänzungsergebnisdaten automatisch an TISC zu übertragen. Wenn diese Option deaktiviert ist, können Sicherheitsanalysten die Ergänzungsergebnisdaten weiterhin manuell veröffentlichen.

Fügen Sie dem TISC-Fall einen Security Incident hinzu

Fügen Sie Security Incidents zu TISC-Falldatensätzen hinzu.

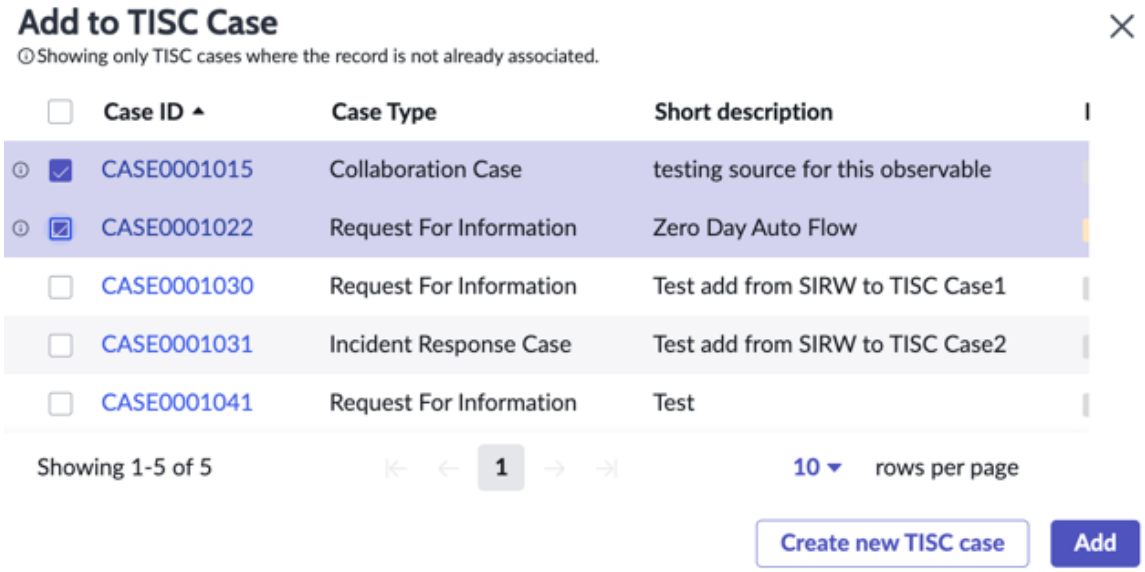
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst, sn_sec_tisc.case_write

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Alle**an.
2. Suchen und öffnen Sie jeden bestimmten Security Incident, den Sie untersuchen.
   Dies kann auch geschehen, indem Sie nach der Incident-ID suchen, im Abschnitt „Schnellfilter“ navigieren oder durch den Incident-Status filtern.
3. Klicken Sie auf **Weitere Aktionen** Symbol.
4. Klicken Sie Auf **Dem TISC-Fall hinzufügen** Aktion.
   Das Dialogfeld „zu TISC-Fall hinzufügen“ wird angezeigt, und es werden nur die TISC-Fälle angezeigt, denen der Incident noch nicht zugeordnet ist.
5. Wählen Sie den Fall(e) aus dem aus **Zu Fall hinzufügen** Dialogfeld.



Hinweis:
Erstellen Sie einen neuen TISC-Fall, wenn keine Falldatensätze vorhanden sind. Weitere Informationen zum Erstellen von Fällen finden Sie unter Erstellen von Fällen mit der Workbench für Bedrohungsanalysen.

6. Klicken Sie auf **Hinzufügen**.
7. Klicken Sie auf den Falldatensatz, um den Fall in TISC über die angezeigte Informationsnachricht oder über anzuzeigen **Aktivität** Stream.

Hinweis:
Um die verknüpften Security Incidents anzuzeigen, klicken Sie im Security Incident auf den entsprechenden Falldatensatz **Aktivität** Stream. Wenn Sie auf klicken, gelangen Sie zum Falldatensatz im TISC-Arbeitsbereich, und die Security Incidents werden unter hinzugefügt **Artefakte** Registerkarte des Fallmanagement-Moduls.

Fügen Sie dem TISC-Fall erkennbare Elemente hinzu

Fügen Sie TISC-Falldatensätze erkennbare Elemente hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst, sn_sec_tisc.case_write

Prozedur

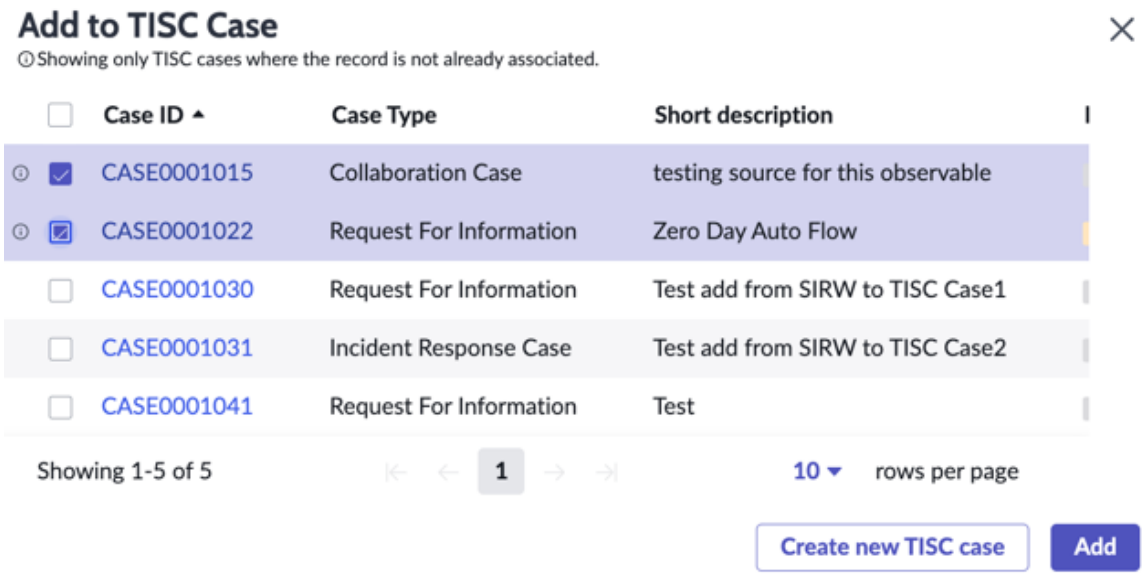
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Alle**an.
2. Suchen und öffnen Sie jeden bestimmten Security Incident, den Sie untersuchen.
   Dies kann auch geschehen, indem Sie nach der Incident-ID suchen, im Abschnitt „Schnellfilter“ navigieren oder durch den Incident-Status filtern.
3. Klicken Sie auf **Zugehörige Datensätze** Registerkarte im Arbeitsbereich.
   Sie können die Aktion zum Hinzufügen erkennbarer Elemente zu TISC-Fällen über verschiedene Registerkarten im Security Incident Response-Arbeitsbereich ausführen.

   Hinweis:
   Sie können zu folgendem Ort navigieren:
   - Detailseite für erkennbare Elemente auf der Registerkarte zugehörige Datensätze.
   - **Untersuchung** Und navigieren Sie zu **Einstiegspunktlisten** Abschnitt, der auf der linken Seite angezeigt wird, und wählen Sie aus **Zugeordnete Erkennbare Elemente** Dient zum Hinzufügen erkennbarer Elemente zum TISC-Fall.

4. Wählen Sie beispielsweise aus **Bedrohungsinformationen** > **Zugehörige erkennbare Elemente**an.
5. Wählen Sie ein oder mehrere erkennbare Elemente aus, um die ausgewählten erkennbaren Elemente zu Falldatensätzen hinzuzufügen.

   Hinweis:
   Sie können auch auf einen beliebigen Datensatz erkennbarer Elemente klicken. Dadurch wird die Detailseite für erkennbare Elemente auf einer anderen Registerkarte geöffnet. Sie können Falldatensätze von hier aus hinzufügen, indem Sie auf zu TISC-Fall hinzufügen klicken.

6. Klicken Sie auf **Fähigkeitsaktionen** Schaltfläche „Teilen“.
7. Wählen Sie Aus **Dem TISC-Fall hinzufügen** .
8. Wählen Sie den Fall(e) aus dem aus **Zu Fall hinzufügen** Dialogfeld.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Erstellen Sie einen neuen TISC-Fall, wenn keine Falldatensätze vorhanden sind. Weitere Informationen zum Erstellen von Fällen finden Sie unter Erstellen von Fällen mit der Workbench für Bedrohungsanalysen.

9. Klicken Sie auf **Hinzufügen**.
10. Klicken Sie auf den Falldatensatz, um den Fall in TISC über die angezeigte Informationsnachricht oder über anzuzeigen **Aktivität** Stream.

Hinweis:
Wenn das erkennbare Element kein entsprechendes TISC-erkennbares Element hat, wird das im SIR-Arbeitsbereich ausgewählte erkennbare Element automatisch an TISC gesendet und anschließend den ausgewählten TISC-Falldatensätzen hinzugefügt. Um die verknüpften erkennbaren Elemente anzuzeigen, klicken Sie in auf den entsprechenden Falldatensatz **Aktivität** Stream. Wenn Sie auf klicken, gelangen Sie zum Falldatensatz im TISC-Arbeitsbereich, und die erkennbaren Elemente werden unter hinzugefügt **Artefakte** Registerkarte des Fallmanagement-Moduls.

Ergebnisse
Sie haben die Daten erkennbarer Elemente erfolgreich an das Fallmanagement des Threat Intelligence Security Center gesendet.

Erkennbare Elemente an TISC senden

Mit dieser Funktion kann der Sicherheitsanalyst die Daten erkennbarer Elemente von SIR an TISC übertragen. Mit dem TISC-Kontext können Sie überprüfen, ob die erkennbaren Elemente in TISC vorhanden sind. Wenn nicht, kann der Sicherheitsanalysten die Daten jederzeit veröffentlichen.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Prozedur

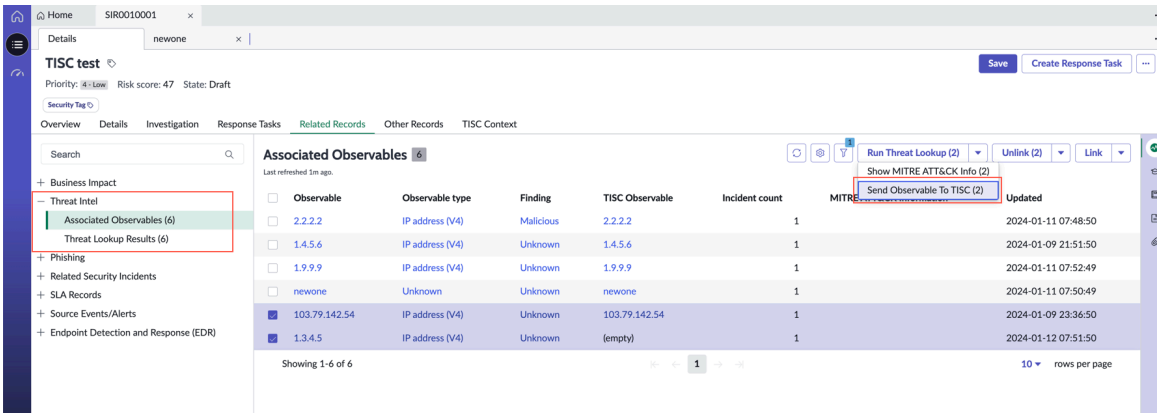
1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Alle**an.
2. Öffnen Sie einen Security Incident.
3. Wählen Sie aus **Zugehörige Datensätze** Registerkarte zum Ausführen der Aktion „TISC-Integrationsfähigkeit“.

Hinweis:

- Sie können auch zu navigieren **Untersuchung** Und navigieren Sie zu **Einstiegspunktlisten** Abschnitt, der auf der linken Seite angezeigt wird, und wählen Sie aus **Zugeordnete Erkennbare Elemente** Zum Durchführen des Push-Vorgangs.
- Auf der **Untersuchung** Wählen Sie die Registerkarte aus **Zeigen Sie Zugehörige Informationen An** Zum Anzeigen aller zugehörigen Bedrohungssuche-, Sichtungs- und Ergänzungsdaten für das ausgewählte erkennbare Element. Weitere Informationen finden Sie unter Untersuchungs-Canvas Erkunden.

4. Wählen Sie beispielsweise aus **Bedrohungsinformationen** > **Zugehörige erkennbare Elemente** Um den Push-Vorgang auszuführen und die Daten manuell in TISC zu verschieben.
5. Wählen Sie einen oder mehrere Datensätze erkennbarer Elemente aus, die ausgeführt werden sollen **Erkennbares Element an TISC senden** Vorgang zum Pushen der Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie Aus **Erkennbares Element an TISC senden** .

7. Geben Sie im Bildschirm „erkennbare Elemente an TISC senden“ Folgendes an:

Fügen Sie Informationen zu TISC-erkennbaren Elementen hinzu

Feld	Beschreibung
Vertrauen	Die Konfidenzpunktzahl für die erkennbaren Elemente.
TLP	Der TLP-Wert (Traffic Light Protocol) für die erkennbaren Elemente.
Notizen	Hinweise für die erkennbaren Elemente.
TISC-Tags	Tags für die zu sendenden erkennbaren Elemente. Sie können anwenderdefinierte Tags hinzufügen, die den erkennbaren Elementen hinzugefügt werden.

8. Wählen Sie **Senden**.

Hinweis:

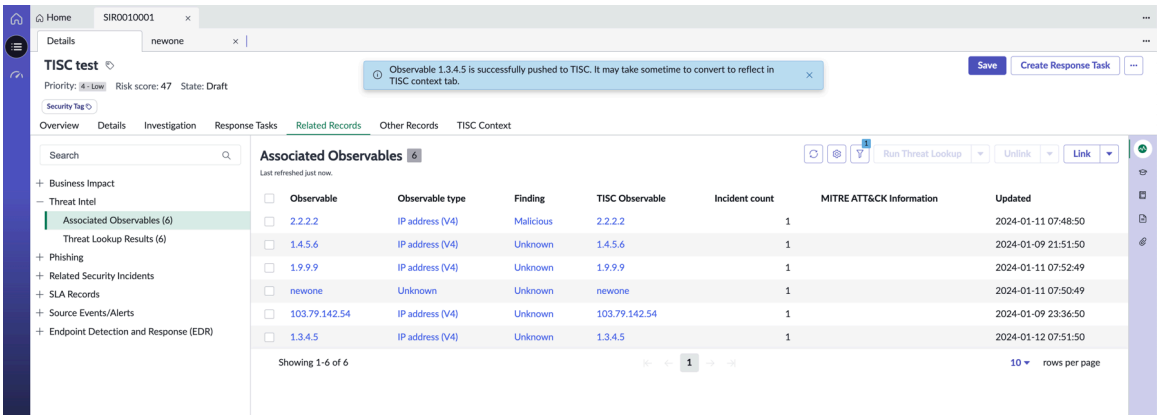
- Wenn das ausgewählte erkennbare Element nicht in TISC vorhanden ist, wird zuerst das erkennbare Element als Quelle des erkennbaren Elements erstellt, und sobald das erkennbare Quellelement einen TISC-Datensatz erstellt, wird der Datensatz des erkennbaren Elements automatisch dem neu erstellten erkennbaren Element zugeordnet.
- Sobald der Push-Vorgang für erkennbare Elemente ausgeführt wurde, wird eine Informationsmeldung angezeigt.

  Die folgenden erkennbaren Elemente wurden erfolgreich an TISC übertragen. Es kann einige Zeit dauern, bis es auf der Registerkarte „TISC-Kontext“ reflektiert wird. 0.0.0.0

- Wenn bereits ein erkennbares Element vorhanden ist, wird eine Fehlermeldung angezeigt.

  Die folgenden erkennbaren Elemente sind bereits in TISC vorhanden: 0.0.0.0

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Wählen Sie Aus **TISC-Kontext** .

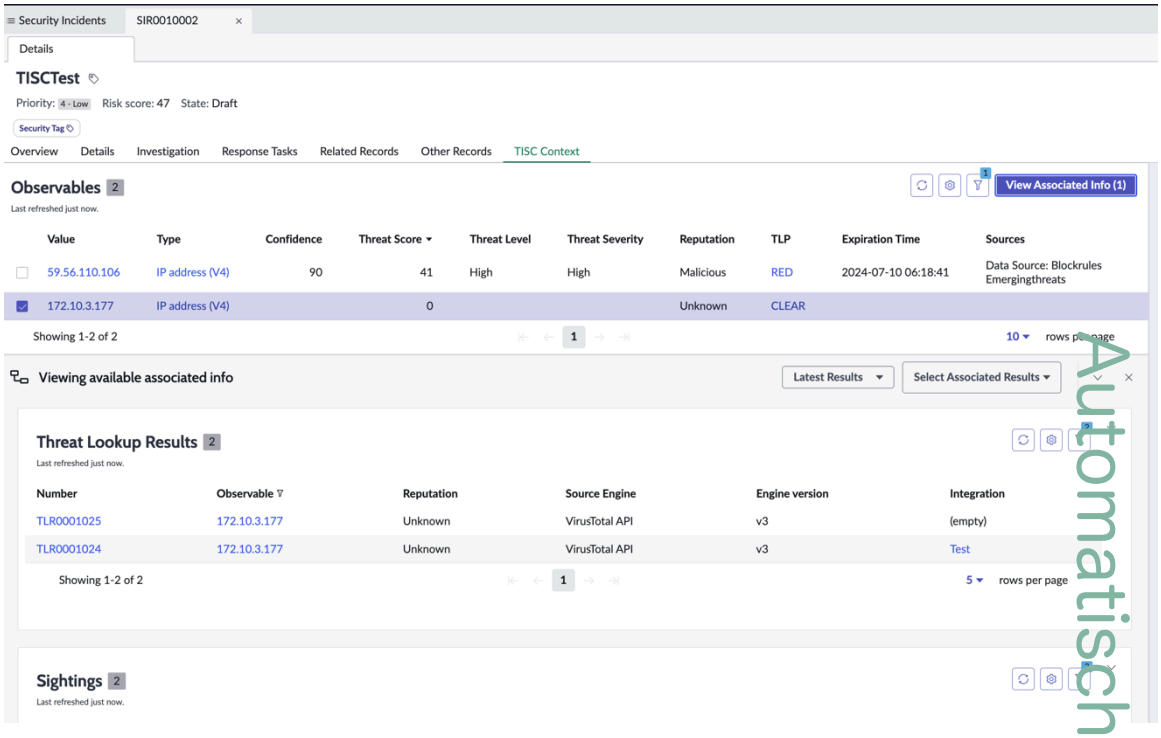
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

:

- Sie sehen jetzt das erkennbare Element, das von der SIR-Anwendung an TISC übertragen wird.



- **In einem manuellen Push-Vorgang** : Die Daten erkennbarer Elemente können nur übertragen werden, wenn sie mit den Security Incidents verknüpft sind. Sobald das erkennbare Element von SIR übertragen wurde, können diese Daten anhand von Quellen identifiziert werden, die Verweise auf Security Incidents enthalten, die mit dem erkennbaren Element verknüpft sind.
- **In einem automatischen Push-Vorgang** : Die erkennbaren Elemente oder Ergänzungsdaten werden automatisch übertragen, wenn sie einem Security Incident zugeordnet sind.

  Hinweis:
  Die **Erkennbares Element an TISC senden** Die Option wird ausgeblendet, sobald der automatisierte Flow aktiviert ist.

- **TISC-Kontext** Zeigt alle SIR-zugeordneten erkennbaren Elemente an, die auch in TISC vorhanden sind.
- Im TISC-Kontext können SIR-Analysten alle TISC-Anreicherungsdaten anzeigen, einschließlich Bedrohungssuchen, Sichtungssuche und Anreicherungsergebnisse erkennbarer Elemente.
- **Zeigen Sie Zugehörige Informationen An** Zeigt alle zugehörigen Ergänzungsdaten erkennbarer Elemente der ausgewählten erkennbaren Elemente an.

10. Zeigen Sie die Ergebnisse an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungssuche an TISC senden

Mit dieser Funktion kann der Sicherheitsanalyst die Bedrohungssuchdaten von SIR an TISC übertragen. Mit dem TISC-Kontext können Sie überprüfen, ob die Ergebnisse der Bedrohungssuche in TISC vorhanden sind. Andernfalls kann der Sicherheitsanalysten die Daten jederzeit veröffentlichen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

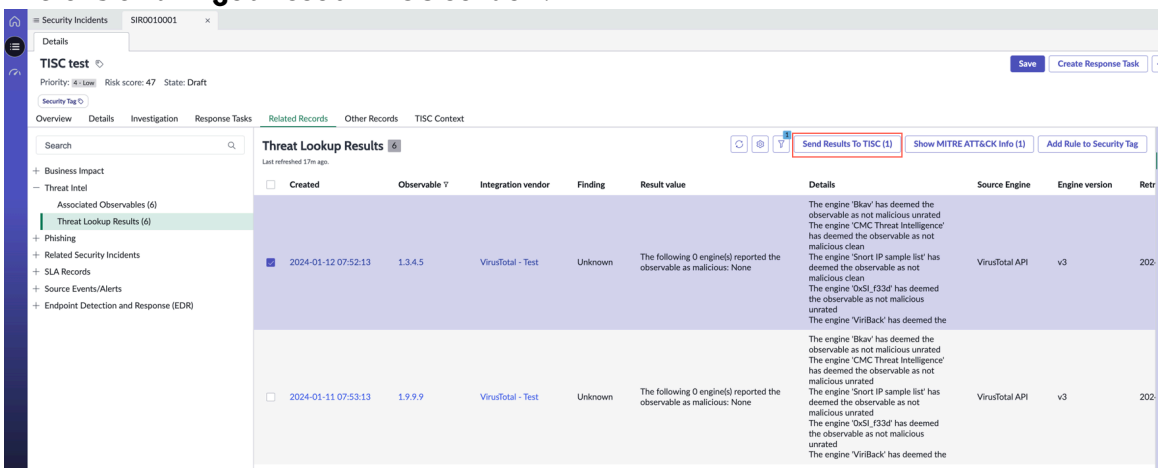
Prozedur

1. Navigieren Sie zu **Zugehörige Datensätze** Registerkarte im SIR-Arbeitsbereich, um die Aktion „TISC-Integrationsfähigkeit“ auszuführen.

   Hinweis:

   - Sie können auch zu navigieren **Untersuchung** Und navigieren Sie zu **Einstiegspunktlisten** Abschnitt, der auf der linken Seite angezeigt wird, und wählen Sie aus **Zugeordnete Erkennbare Elemente** Zum Durchführen des Push-Vorgangs.
   - Auf der **Untersuchung** Klicken Sie auf die Registerkarte **Zeigen Sie Zugehörige Informationen An** Zum Anzeigen aller zugehörigen Bedrohungssuche-, Sichtungs- und Ergänzungsdaten für das ausgewählte erkennbare Element. Weitere Informationen finden Sie unter Untersuchungs-Canvas Erkunden.

2. Auswahlvorgang **Bedrohungsinformationen** > **Bedrohungssuche – Ergebnisse** Um den Push-Vorgang auszuführen und die Daten manuell in TISC zu verschieben.
3. Wählen Sie einen oder mehrere Datensätze mit Bedrohungssuchergebnissen aus.
4. Klicken Sie Auf **Ergebnisse an TISC senden** .



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn das ausgewählte erkennbare Element für die Bedrohungssuche in TISC nicht vorhanden ist, wird das erkennbare Element im manuellen Modus zuerst als Quelle des erkennbaren Elements erstellt, und sobald das erkennbare Quellelement einen TISC-Datensatz erstellt, wird der Datensatz des erkennbaren Elements automatisch dem neu erstellten erkennbaren Element zugeordnet. Außerdem wird die ausgewählte Bedrohungssuche im manuellen Modus auch an das neu erstellte erkennbare Element „Bedrohungssuche“ übertragen.
- In einem automatischen Modus werden die erkennbaren Elemente nicht übertragen, wenn das erkennbare Element vorhanden ist. Dann werden die Bedrohungssuchen automatisch übertragen. Wenn die erkennbaren Elemente nicht vorhanden sind, werden die Bedrohungssuchen nicht übertragen.

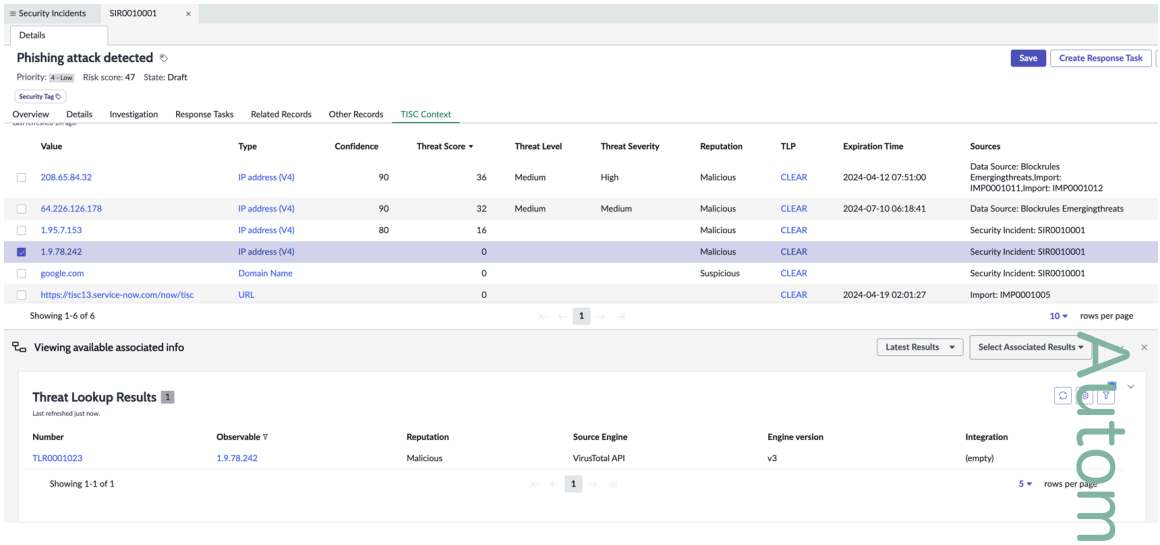
5. Eine Bestätigungsnachricht wird angezeigt, die angezeigt wird Das erkennbare Element (1,9.78.242) für den ausgewählten Bedrohungssuchdatensatz ist in TISC nicht vorhanden. Es dauert einige Zeit, um ein erkennbares Element zu erstellen und den Bedrohungssuchdatensatz für erkennbare Elemente automatisch in TISC zuzuordnen.
   Sobald dies verarbeitet und übertragen wurde, können Sie die Ergebnisse sehen.
6. Wählen Sie Aus **TISC-Kontext** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

:

- Sie sehen jetzt das erkennbare Element, das von der SIR-Anwendung an TISC übertragen wird.



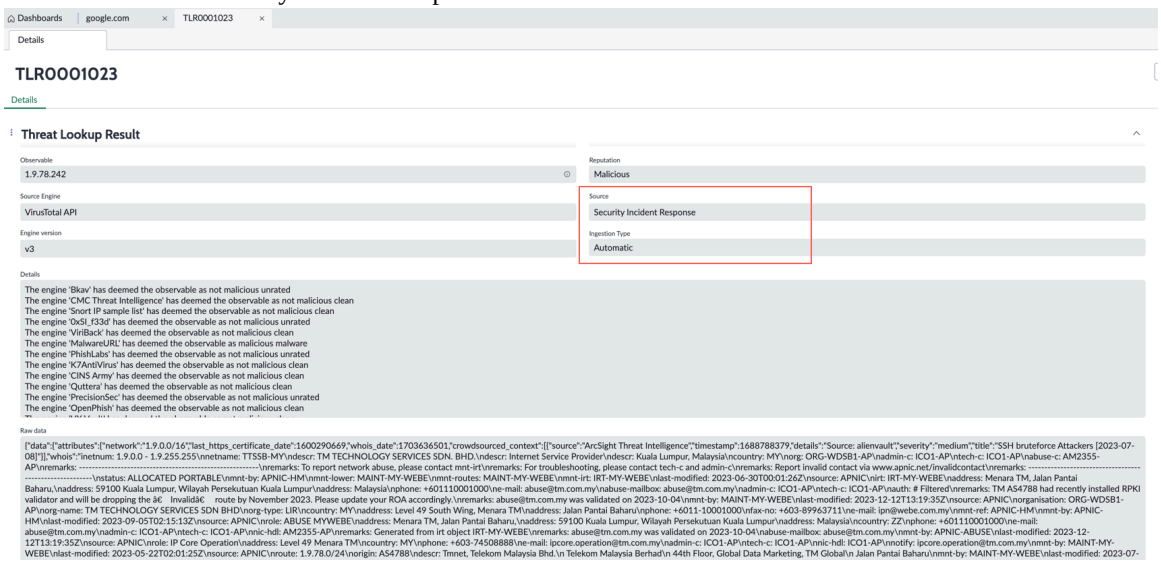
- **In einem manuellen Push-Vorgang** : Die Daten erkennbarer Elemente können nur übertragen werden, wenn sie mit den Security Incidents verknüpft sind. Sobald das erkennbare Element von SIR übertragen wurde, können diese Daten anhand von Quellen identifiziert werden, die Verweise auf Security Incidents enthalten, die mit dem erkennbaren Element verknüpft sind.
- **In einem automatischen Push-Vorgang** : Die erkennbaren Elemente oder Ergänzungsdaten werden automatisch übertragen, wenn sie einem Security Incident zugeordnet sind.
- **TISC-Kontext** Zeigt alle SIR-zugeordneten erkennbaren Elemente an, die auch in TISC vorhanden sind.
- Im TISC-Kontext können SIR-Analysten alle TISC-Anreicherungsdaten anzeigen, einschließlich Bedrohungssuchen, Sichtungssuche und Anreicherungsergebnisse erkennbarer Elemente.
- **Zeigen Sie Zugehörige Informationen An** Zeigt alle zugehörigen Ergänzungsdaten erkennbarer Elemente der ausgewählten erkennbaren Elemente an.

7. In der Listenansicht werden alle Ergebnisse der Bedrohungssuche angezeigt. Wählen Sie jedoch einen beliebigen Datensatz aus, und klicken Sie auf **Zeigen Sie Zugehörige Informationen An** Schaltfläche.
8. Zeigen Sie die Ergebnisse der Bedrohungssuche an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Klicken Sie auf einen beliebigen Datensatz mit Bedrohungssuchergebnissen, um den Datensatz in der Formularansicht anzuzeigen, die auch den Push oder anzeigt **Erfassungstyp** (Automatisch oder manuell) und **Quelle** Wird Security Incident Response sein.



Sichtungssuche an TISC senden

Mit dieser Funktion kann der Sicherheitsanalyst die Sichtungssuchdaten von SIR an TISC übertragen. Mit dem TISC-Kontext kann der Analyst überprüfen, ob die Sichtungssuchdaten in TISC vorhanden sind. Andernfalls kann der Sicherheitsanalyst die Daten jederzeit veröffentlichen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

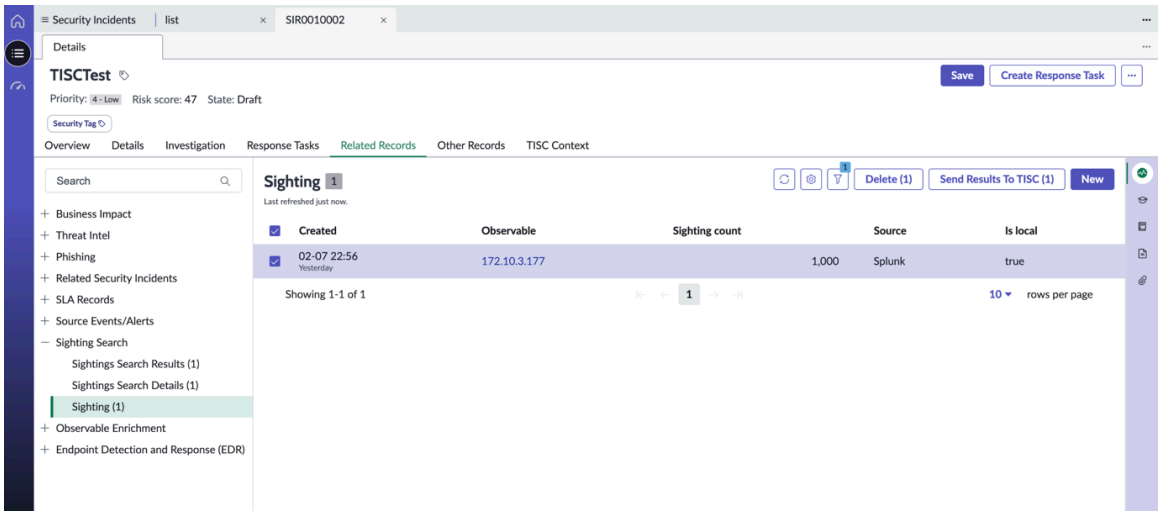
1. Navigieren Sie zu **Zugehörige Datensätze** Registerkarte im SIR-Arbeitsbereich, um die Aktion „TISC-Integrationsfähigkeit“ auszuführen.

   Hinweis:

   - Sie können auch zu navigieren **Untersuchung** Und navigieren Sie zu **Einstiegspunktlisten** Abschnitt, der auf der linken Seite angezeigt wird, und wählen Sie aus **Zugeordnete Erkennbare Elemente** Zum Durchführen des Push-Vorgangs.
   - Auf der **Untersuchung** Klicken Sie auf die Registerkarte **Zeigen Sie Zugehörige Informationen An** Zum Anzeigen aller zugehörigen Bedrohungssuche-, Sichtungs- und Ergänzungsdaten für das ausgewählte erkennbare Element. Weitere Informationen finden Sie unter Untersuchungs-Canvas Erkunden.

2. Auswahlvorgang **Sichtungssuche** > **Sichtungssuchergebnisse** Um den Push-Vorgang auszuführen und die Daten manuell in TISC zu verschieben.
3. Wählen Sie einen oder mehrere Datensätze mit Sichtungssuchergebnissen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

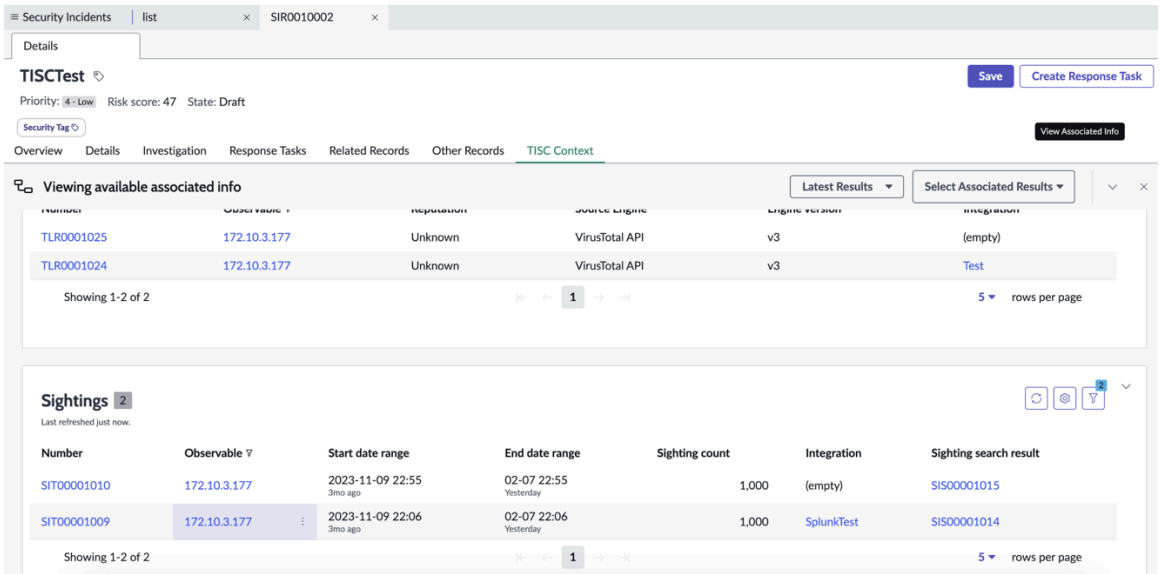


4. Klicken Sie Auf **Ergebnisse an TISC senden** .

Hinweis:

- Wenn das ausgewählte erkennbare Element für die Sichtungssuche in TISC nicht vorhanden ist, wird das erkennbare Element im manuellen Modus zuerst als Quelle für erkennbares Element erstellt, und sobald das erkennbare Quellelement einen TISC-Datensatz erstellt, wird der Datensatz des erkennbaren Elements automatisch dem neu erstellten erkennbaren Element zugeordnet. Außerdem wird die ausgewählte Sichtungssuche im manuellen Modus auch an das neu erstellte erkennbare Element „Bedrohungssuche“ übertragen.
- In einem automatischen Modus werden die erkennbaren Elemente nicht übertragen, wenn das erkennbare Element vorhanden ist. Dann werden die Bedrohungssuchen automatisch übertragen. Wenn die erkennbaren Elemente nicht vorhanden sind, werden die Bedrohungssuchen nicht übertragen.

5. Wählen Sie Aus **TISC-Kontext** .



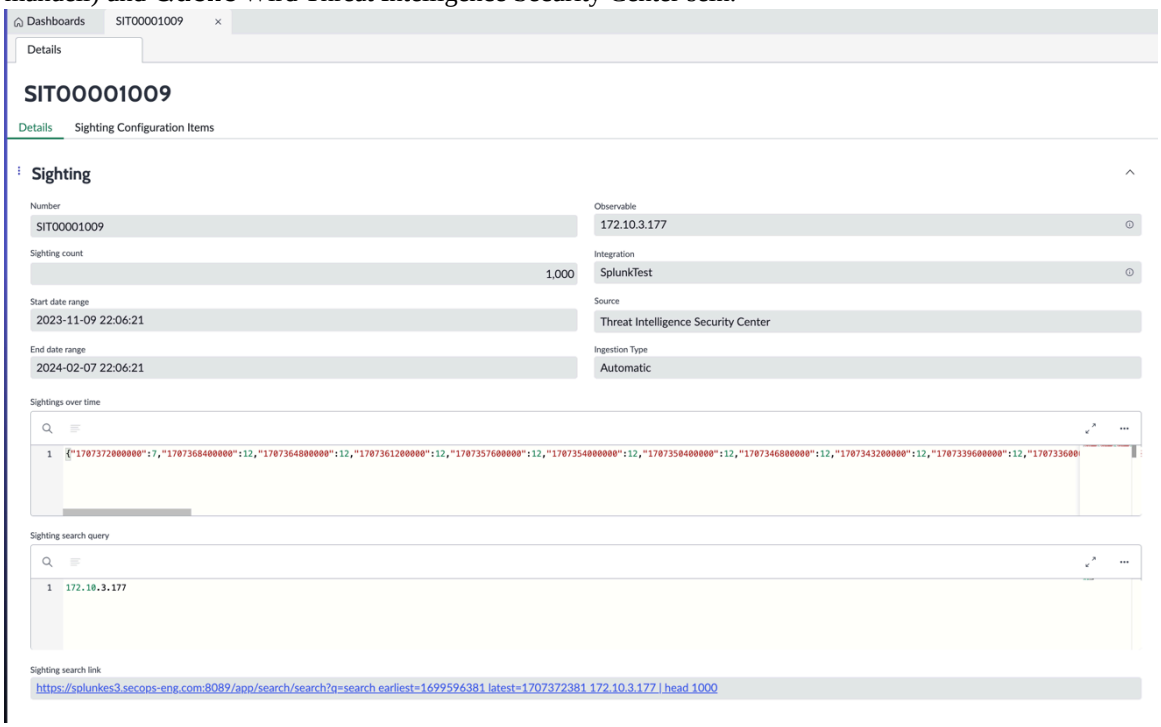
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

:

- Sie sehen jetzt das erkennbare Element, das von der SIR-Anwendung an TISC übertragen wird.
- **In einem manuellen Push-Vorgang** : Die Daten erkennbarer Elemente können nur übertragen werden, wenn sie mit den Security Incidents verknüpft sind. Sobald das erkennbare Element von SIR übertragen wurde, können diese Daten anhand von Quellen identifiziert werden, die Verweise auf Security Incidents enthalten, die mit dem erkennbaren Element verknüpft sind.
- **In einem automatischen Push-Vorgang** : Die erkennbaren Elemente oder Ergänzungsdaten werden automatisch übertragen, wenn sie einem Security Incident zugeordnet sind.
- **TISC-Kontext** Zeigt alle SIR-zugeordneten erkennbaren Elemente an, die auch in TISC vorhanden sind.
- Im TISC-Kontext können SIR-Analysten alle TISC-Anreicherungsdaten anzeigen, einschließlich Bedrohungssuchen, Sichtungssuche und Anreicherungsergebnisse erkennbarer Elemente.
- **Zeigen Sie Zugehörige Informationen An** Zeigt alle zugehörigen Ergänzungsdaten erkennbarer Elemente der ausgewählten erkennbaren Elemente an.

6. Sobald der Datensatz verarbeitet wurde, wählen Sie den Datensatz aus, und klicken Sie auf **Zeigen Sie die zugehörigen Informationen an** .
7. Zeigen Sie die Ergebnisse an.
8. Klicken Sie auf einen beliebigen Datensatz mit Sichtungssuchergebnissen, um den Datensatz in der Formularansicht anzuzeigen, die auch die Push-Option oder anzeigt **Erfassungstyp** (Automatisch oder manuell) und **Quelle** Wird Threat Intelligence Security Center sein.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergänzung erkennbarer Elemente an TISC senden

Mit dieser Funktion kann der Sicherheitsanalyst die Sichtungssuchdaten von SIR an TISC übertragen. Mit dem TISC-Kontext kann der Analyst überprüfen, ob die Sichtungssuchdaten in TISC vorhanden sind. Andernfalls kann der Sicherheitsanalyst die Daten jederzeit veröffentlichen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

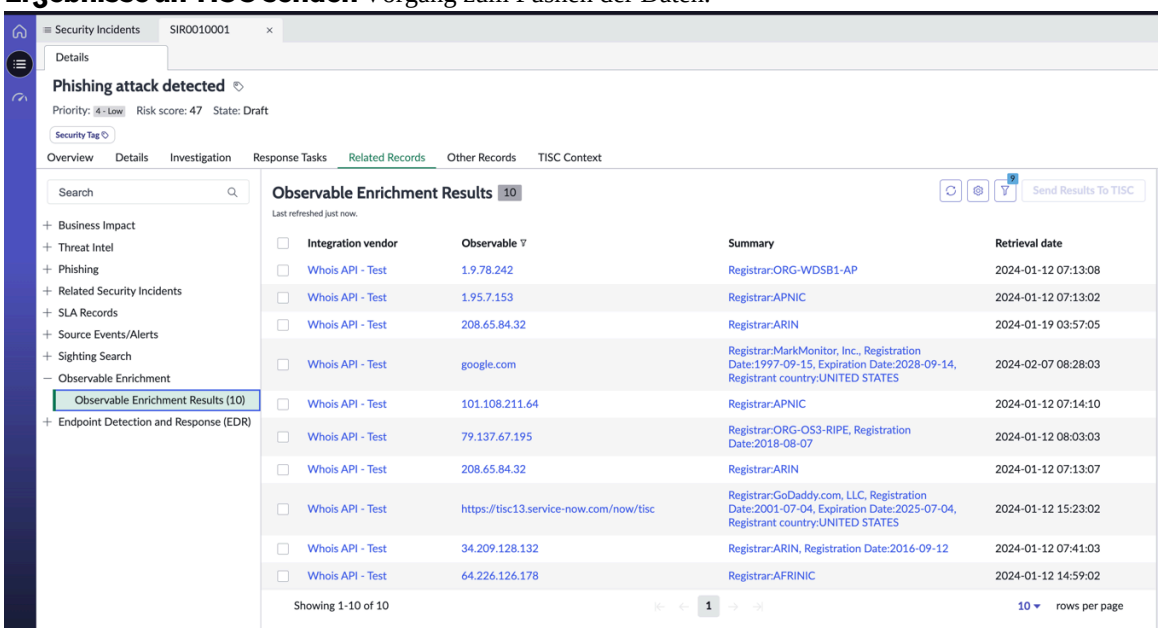
1. Navigieren Sie zu **Zugehörige Datensätze** Registerkarte im SIR-Arbeitsbereich, um die Aktion „TISC-Integrationsfähigkeit“ auszuführen.

   Hinweis:

   - Sie können auch zu navigieren **Untersuchung** Und navigieren Sie zu **Einstiegspunktlisten** Abschnitt, der auf der linken Seite angezeigt wird, und wählen Sie aus **Zugeordnete Erkennbare Elemente** Zum Durchführen des Push-Vorgangs.
   - Auf der **Untersuchung** Klicken Sie auf die Registerkarte **Zeigen Sie Zugehörige Informationen An** Zum Anzeigen aller zugehörigen Bedrohungssuche-, Sichtungs- und Ergänzungsdaten für das ausgewählte erkennbare Element. Weitere Informationen finden Sie unter Untersuchungs-Canvas Erkunden.

2. Auswahlvorgang **Ergänzung erkennbarer Elemente** > **Erkennbare Elemente – Datenanreicherungs-Ergebnisse** Um den Push-Vorgang auszuführen und die Daten manuell in TISC zu verschieben.

3. Wählen Sie einen oder mehrere Datensätze erkennbarer Elemente aus, die ausgeführt werden sollen **Ergebnisse an TISC senden** Vorgang zum Pushen der Daten.



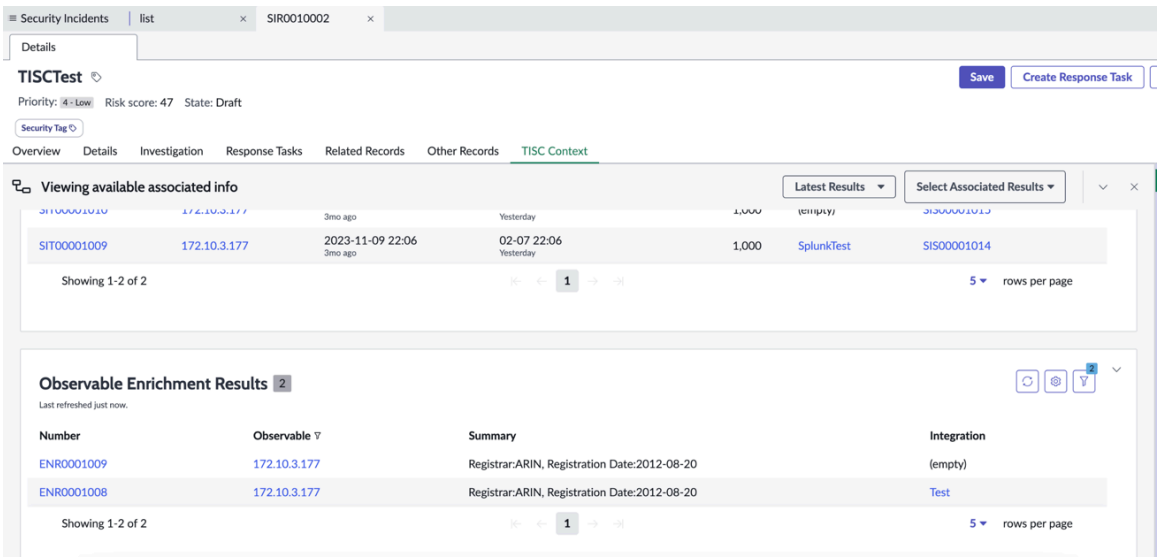
4. Klicken Sie Auf **Ergebnisse an TISC senden** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn das ausgewählte erkennbare Element nicht in TISC vorhanden ist, wird zuerst das erkennbare Element als Quelle des erkennbaren Elements erstellt, und sobald das erkennbare Quellelement einen TISC-Datensatz erstellt, wird der Datensatz des erkennbaren Elements automatisch dem neu erstellten erkennbaren Element zugeordnet.
- Sobald der Push-Vorgang für erkennbare Elemente ausgeführt wurde, wird eine Informationsnachricht angezeigt, die angezeigt wird Erkennbares Element 0.0.0.0 wurde erfolgreich an TISC übertragen. Es kann einige Zeit dauern, bis die Konvertierung in die Registerkarte „TISC-Kontext“ erfolgt .

5. Wählen Sie Aus **TISC-Kontext** .



Hinweis:

:

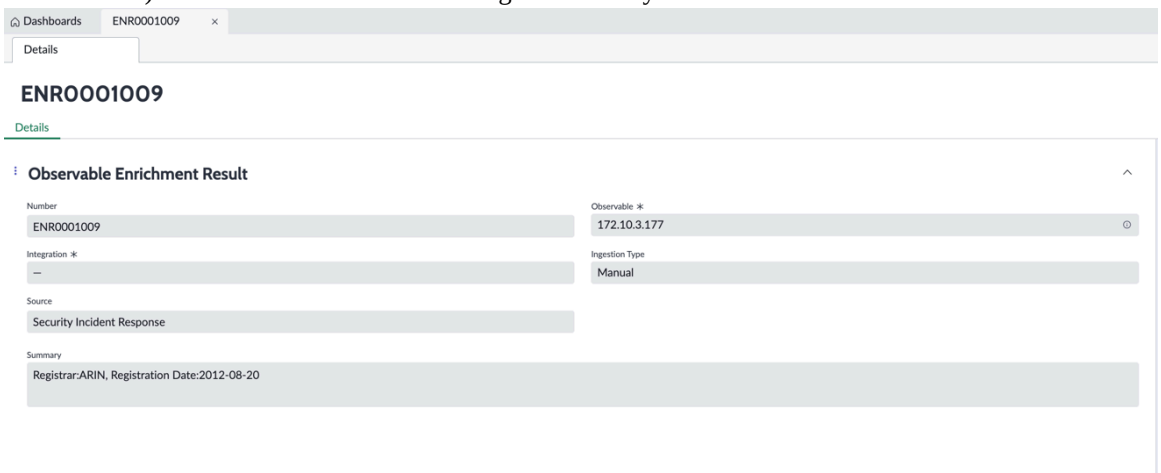
- Sie sehen jetzt das erkennbare Element, das von der SIR-Anwendung an TISC übertragen wird.
- **In einem manuellen Push-Vorgang** : Die Daten erkennbarer Elemente können nur übertragen werden, wenn sie mit den Security Incidents verknüpft sind. Sobald das erkennbare Element von SIR übertragen wurde, können diese Daten anhand von Quellen identifiziert werden, die Verweise auf Security Incidents enthalten, die mit dem erkennbaren Element verknüpft sind.
- **In einem automatischen Push-Vorgang** : Die erkennbaren Elemente oder Ergänzungsdaten werden automatisch übertragen, wenn sie einem Security Incident zugeordnet sind.
- **TISC-Kontext** Zeigt alle SIR-zugeordneten erkennbaren Elemente an, die auch in TISC vorhanden sind.
- Im TISC-Kontext können SIR-Analysten alle TISC-Anreicherungsdaten anzeigen, einschließlich Bedrohungssuchen, Sichtungssuche und Anreicherungsergebnisse erkennbarer Elemente.
- **Zeigen Sie Zugehörige Informationen An** Zeigt alle zugehörigen Ergänzungsdaten erkennbarer Elemente der ausgewählten erkennbaren Elemente an.

6. Zeigen Sie die Ergebnisse an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf einen beliebigen Datensatz mit Ergänzungsergebnissen erkennbarer Elemente, um den Datensatz in der Formularansicht anzuzeigen, die auch den Push oder anzeigt **Erfassungstyp** (Automatisch oder manuell) und **Quelle** Wird Threat Intelligence Security Center sein.



Arbeiten mit TISC-Kontext

Der TISC-Kontext erleichtert die Anzeige von Threat Intelligence-Daten wie erkennbaren Elementen im Security Incident Response-Arbeitsbereich.

Dies hilft Sicherheitsanalysten, Security Incidents effektiver im Arbeitsbereich zu erkennen, zu untersuchen und darauf zu reagieren.

Mit dem TISC-Kontext im Arbeitsbereich „Security Incident Response“ können Sicherheitsanalysten Security Incidents oder erkennbare Elemente direkt aus dem Arbeitsbereich zu TISC-Fällen hinzufügen, auch die Ergänzungsergebnisse anzeigen und erkennbare Elemente anzeigen, die zugehörige Bedrohungsakteure, Angriffsmuster, Kampagnen usw. sind.

In diesem Abschnitt können Sie Folgendes tun:

1. Ordnen Sie einem TISC-Fall erkennbare Elemente zu.
2. Zeigen Sie Informationen zu zugehörigen erkennbaren Elementen an.
3. Zeigen Sie Ergänzungsergebnisse erkennbarer Elemente an.

Ausführlichere Informationen und Verfahren finden Sie in den folgenden Abschnitten. Weitere Informationen zur Funktionsweise der Integration zwischen TISC- und SIR-Arbeitsbereichen finden Sie unter TISC-Integration mit SIR Workspace In Threat Intelligence-Sicherheitszentrum.

Fügen Sie dem TISC-Fall erkennbare Elemente hinzu

Verwenden Sie diesen Abschnitt, um einem TISC-Fall Security Incidents oder erkennbare Elemente hinzuzufügen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

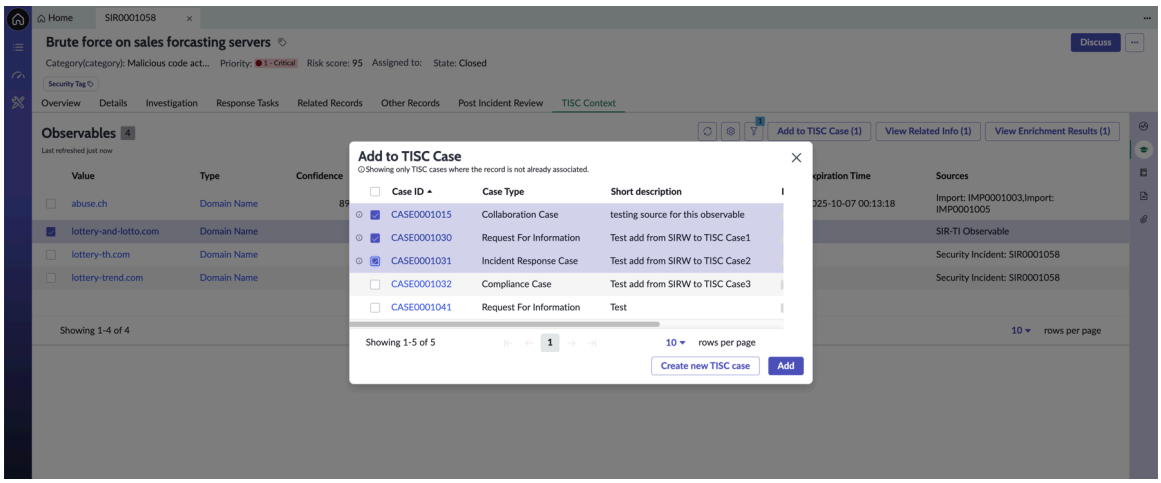
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Alle**an.
2. Suchen und öffnen Sie jeden bestimmten Security Incident, den Sie untersuchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dies kann auch geschehen, indem Sie nach der Incident-ID suchen, im Abschnitt „Schnellfilter“ filtern oder einen Incident-Status durchsuchen.

3. Wählen Sie Aus **TISC-Kontext** Registerkarte.
4. Klicken Sie Auf **Dem TISC-Fall hinzufügen** Schaltfläche.
   Das Dialogfeld „zu TISC-Fall hinzufügen“ wird angezeigt, und es werden nur die TISC-Fälle angezeigt, denen der Datensatz nicht bereits zugeordnet ist.
5. Wählen Sie die erkennbaren Elemente aus.
6. Wählen Sie Fall(e) aus, und klicken Sie auf **Hinzufügen** Um die Fälle den erkennbaren Elementen hinzuzufügen und dem Security Incident zuzuordnen.



Hinweis:
Sie können auch einen neuen Fall erstellen, indem Sie auf klicken **Erstellen Sie einen neuen TISC-Fall** , Falls Sie keine vorhandenen Fälle haben.

Die folgenden Bestätigungsnachrichten werden angezeigt:

- Die folgenden erkennbaren Elemente wurden erfolgreich als Artefakte hinzugefügt.
- Die folgenden erkennbaren Elemente werden an TISC gesendet und anschließend den ausgewählten TISC-Falldatensätzen hinzugefügt.

Hinweis:
Die Verarbeitung und Zuordnung der Aktivitäten erkennbarer Elemente wird im Aktivitätenstrom veröffentlicht, sobald die Zuordnung abgeschlossen ist.

7. Zeigen Sie die zugehörigen Falldatensätze an, indem Sie sich beim Arbeitsbereich des Threat Intelligence-Sicherheitszentrums für weitere Schritte anmelden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter TISC-Integration mit SIR Workspace.

Hinweis:

Im Arbeitsbereich „Security Incident Response“ können Sie auch erkennbare Elemente Falldatensätzen aus zuordnen **Untersuchung** Und **Zugehörige Datensätze** Registerkarten.

Hinweis:

Um erkennbare Elemente von zuzuordnen **Untersuchung** , Befolgen Sie das folgende Verfahren und , um von zuzuordnen **Zugehörige Datensätze** Hier erläutert Fügen Sie dem TISC-Fall erkennbare Elemente hinzu.Sie können auch zu navigieren **Untersuchung** Und navigieren Sie zu **Einstiegspunktlisten** Abschnitt, der auf der linken Seite angezeigt wird, und wählen Sie aus **Zugeordnete Erkennbare Elemente** Dient zum Hinzufügen erkennbarer Elemente zum TISC-Fall.

Zeigen Sie zugehörige Informationen aus TISC an

Verwenden Sie diesen Abschnitt, um die zugehörigen Informationen wie zugehörige Bedrohungsakteure, Angriffsmuster, Kampagnen und Fälle aus TISC im SIR-Arbeitsbereich anzuzeigen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Alle**an.
2. Suchen und öffnen Sie jeden bestimmten Security Incident, den Sie untersuchen.
   Dies kann auch geschehen, indem Sie nach der Incident-ID suchen, im Abschnitt „Schnellfilter“ navigieren oder durch den Incident-Status filtern.
3. Sobald der Incident geöffnet ist, navigieren Sie zu **TISC-Kontext** Registerkarte.
   Zugehörige Informationen Anzeigen:

   Innerhalb der Incident-Details können Sie zugehörige Informationen in mehreren Abschnitten anzeigen.

   a. Wählen Sie mindestens ein erkennbares Element aus.

   b. Klicken Sie auf **Zeigen Sie Zugehörige Informationen An** Schaltfläche.
   In diesem Abschnitt werden die zugehörigen Informationen angezeigt, die sich auf die ausgewählten erkennbaren Elemente beziehen.

Name	Beschreibung
Bedrohungsakteure	Zeigt Informationen aus TISC für Bedrohungsakteure im Zusammenhang mit den ausgewählten erkennbaren Elementen an.
Angriffsmuster	Zeigt Informationen aus TISC für Angriffsmuster im Zusammenhang mit den ausgewählten erkennbaren Elementen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Kampagnen	Zeigt Informationen aus TISC für Kampagnen an, die sich auf die ausgewählten erkennbaren Elemente beziehen.
Fälle	Zeigt Informationen aus TISC für TISC-Fälle an, die sich auf die ausgewählten erkennbaren Elemente beziehen.

Datenanreicherungs-Ergebnisse anzeigen

Verwenden Sie diesen Abschnitt, um die Ergänzungsergebnisse erkennbarer Elemente wie Ergebnisse der Bedrohungssuche, Sichtungen und Anreicherungsergebnisse erkennbarer Elemente aus TISC im SIR-Arbeitsbereich anzuzeigen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Alle**an.
2. Suchen und öffnen Sie jeden bestimmten Security Incident, den Sie untersuchen.
   Dies kann auch geschehen, indem Sie nach der Incident-ID suchen, im Abschnitt „Schnellfilter“ navigieren oder durch den Incident-Status filtern.
3. Sobald der Incident geöffnet ist, navigieren Sie zu **TISC-Kontext** Registerkarte.
   Anreicherungsergebnisse Anzeigen:

   Innerhalb der Incident-Details können Sie zugehörige Informationen in mehreren Abschnitten anzeigen.

   a. Wählen Sie mindestens ein erkennbares Element aus.

   b. Klicken Sie auf **Anreicherungsergebnisse Anzeigen** Schaltfläche.
   In diesem Abschnitt werden die Details angezeigt, die sich auf die ausgewählten erkennbaren Elemente beziehen.

Name	Beschreibung
Bedrohungssuche – Ergebnisse	Listet alle zugehörigen Bedrohungssuchergebnisse für ausgewählte erkennbare TISC-Elemente auf.
Sichtungen	Listet alle zugehörigen Sichtungen für ausgewählte erkennbare TISC-Elemente auf.
Erkennbare Elemente – Datenanreicherungs-Ergebnisse	Listet alle zugehörigen Ergänzungsergebnisse erkennbarer Elemente für ausgewählte TISC-erkennbare Elemente auf.

Berichte in Security Incident Response

Alle Berichte, die einem Security Incident zugeordnet sind, sind im Abschnitt „Berichte“ zur Analyse und Freigabe verfügbar.

Der Analyst kann:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bericht erstellen
- Bearbeiten Sie einen Bericht
- Berichte löschen

Bericht erstellen

Analysten können einen Bericht in erstellen Security Incident Response Um den Status eines Incident einzubeziehen und per E-Mail freizugeben.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen Security Incident.
3. Wählen Sie **Reports** (Berichte) aus.

   Die **Bericht** Seite zeigt eine Liste aller Berichte an, die für den ausgewählten Incident erstellt wurden.
4. Wählen Sie **Neu**.
   Die **Wählen Sie Vorlage Aus** Die Seite wird mit einer Liste aller veröffentlichten Vorlagen angezeigt. Die Liste der Vorlagen ist nur verfügbar, wenn der Administrator Berichtsvorlagen veröffentlicht hat. Weitere Informationen finden Sie unter Erstellen Sie eine Berichtsvorlage in Security Incident Response.
5. Wählen Sie eine Berichtsvorlage aus.
   Der Bericht wird im Bearbeitungsmodus mit den in der Vorlage konfigurierten Incident-Daten geöffnet.
6. Wählen Sie Aus **Erweitern Sie** Und fügen Sie die gewünschten Felder ein/entfernen Sie sie.
   - **Allgemeine SIR-Felder** : Die Liste der am häufigsten verwendeten Felder für einen Incident.
   - **Alle SIR-Felder** : Alle Felder im Zusammenhang mit einem Incident. Wenn Sie beispielsweise einen Incident-Bericht generieren und ein Feld mit der Bezeichnung Kurzbeschreibung hinzufügen möchten, können Sie dieses Feld aus der auswählen **Alle SIR-Felder** . Wenn Sie ein Feld hinzufügen, wird die Kurzbeschreibung des Incident im Bericht angezeigt.
   - **Zugehörige Datensätze** : Die zugehörigen Datensätze eines bestimmten Incident. Wenn Sie dem Bericht beispielsweise zugeordnete erkennbare Elemente hinzufügen möchten, können Sie sie Ihrem Bericht hinzufügen. Diese zugehörigen Datensätze werden im Tabellenformat angezeigt
   - **Skripts** : Um das Datum und die Uhrzeit des Berichts hinzuzufügen, können Sie Ihrem Bericht das aktuelle Datum/Uhrzeit-Skript hinzufügen. Dadurch werden Datum und Uhrzeit der Berichterstellung im Bericht hinzugefügt.
7. Wählen Sie Aus **Vorschau** Zum Anzeigen einer Vorschau des Berichts.
8. Wählen Sie Aus **Inhalt Speichern** Um die Änderungen zu speichern.
9. **Wahlweise:** Wählen Sie das Symbol „Berichtsdetails bearbeiten“, um den Berichtsnamen und die Beschreibung zu aktualisieren.
10. Wählen Sie Aus **Veröffentlichen** Um den Bericht zu veröffentlichen.
11. Wählen Sie das Symbol Bericht in E-Mail freigeben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Geben Sie die E-Mails des Empfängers in ein **Bis** Und **Cc/Bcc** Felder.

b. Aktualisieren Sie die E-Mail **Betreff und E-Mail-Text** .

c. Wählen Sie Aus **Senden** Um den Bericht per E-Mail freizugeben.

Bearbeiten Sie einen Bericht

Analysten können einen unveröffentlichten Bericht in ändern Security Incident Response Und teilen Sie es per E-Mail.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen Security Incident.
3. Wählen Sie **Reports** (Berichte) aus.

   Die **Bericht** Seite zeigt eine Liste aller Berichte an, die für den ausgewählten Incident erstellt wurden.
4. Öffnen Sie den zu aktualisierenden Bericht.
   Der Bericht wird im Bearbeitungsmodus mit den in der Vorlage konfigurierten Incident-Daten geöffnet.
5. Bearbeiten Sie den Bericht nach Bedarf.
6. Wählen Sie Aus **Vorschau** Zum Anzeigen einer Vorschau des Berichts.
7. Wählen Sie Aus **Inhalt Speichern** Um die Änderungen zu speichern.
8. **Wahlweise:** Wählen Sie das Symbol „Berichtsdetails bearbeiten“, um den Berichtsnamen und die Beschreibung zu aktualisieren.
9. Wählen Sie Aus **Veröffentlichen** Um den Bericht zu veröffentlichen.
10. Wählen Sie das Symbol Bericht in E-Mail freigeben .
    a. Geben Sie die E-Mails des Empfängers in ein **Bis** Und **Cc/Bcc** Felder.
    b. Aktualisieren Sie die E-Mail **Betreff und E-Mail-Text** .
    c. Wählen Sie Aus **Senden** Um den Bericht per E-Mail freizugeben.

Berichte löschen

Sie können einen Bericht in löschen Security Incident Response Die sich im Status „veröffentlicht“ oder „Entwurf“ befindet.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen Security Incident.
3. Wählen Sie **Reports** (Berichte) aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die **Bericht** Seite zeigt eine Liste aller Berichte an, die für den ausgewählten Incident erstellt wurden.

4. Öffnen Sie den zu löschenden Bericht.
5. Wählen Sie **Löschen**.
   Eine Bestätigungsnachricht wird angezeigt.
6. Wählen Sie Aus **Löschen** Um den Bericht zu löschen.

Arbeiten Sie mithilfe einer Telefonkonferenz oder eines Chats in zusammen Security Incident Response

Sie können mit Analysten und betroffenen Anwendern zusammenarbeiten, um einen Incident in zu lösen oder zu besprechen Security Incident Response Anwendung.

Zugehörige Informationen

Starten Sie eine Telefonkonferenz in Security Incident Response

Starten Sie einen Sidebar-Chat in Security Incident Response

Starten Sie eine Telefonkonferenz in Security Incident Response

Mithilfe einer Telefonkonferenz können Sicherheitsanalysten in Echtzeit mit anderen Analysten und betroffenen Anwendern zusammenarbeiten. Diese Aufrufe erleichtern den Austausch von Informationen, um Incidents zu lösen.

Vorbereitungen

Stellen Sie sicher, dass Sie die folgenden Apps und Plugins installiert und aktiviert haben:

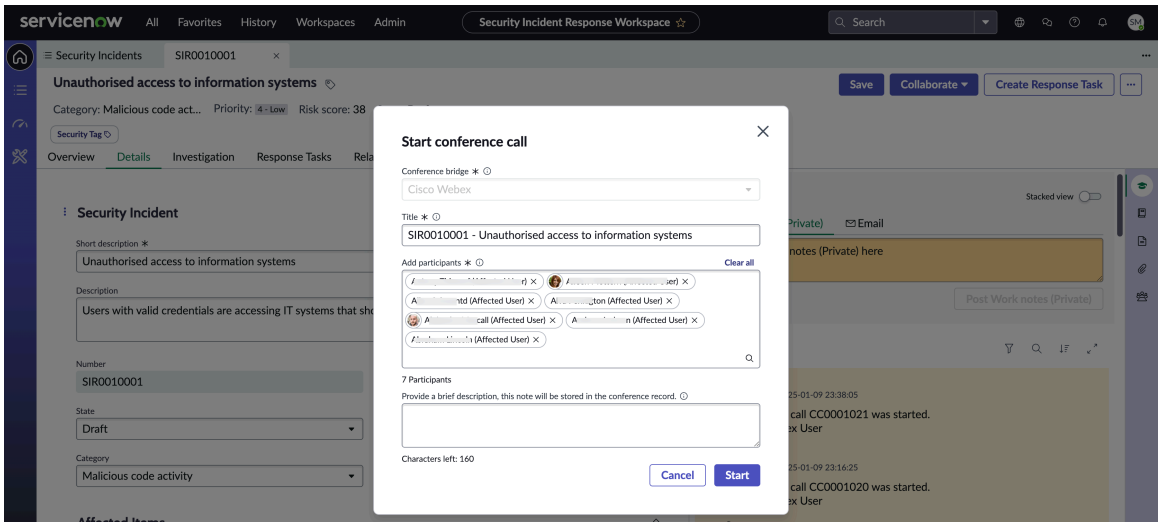
- Notify-Plugin (com.snc.notify).
- Notify-UI-Komponenten für die App „konfigurierbare Arbeitsbereiche“.
- Plugin „visuelles Taskboard“ (com.devsnc.snb_vtb)

Erforderliche Rolle: sn_si.Analyst oder sn_si.Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen Security Incident, für den Sie eine Telefonkonferenz initiieren möchten.
3. Wählen Sie Aus **Zusammenarbeiten** , Und wählen Sie dann aus **Starten Sie einen Anruf** , Oder Sie können das Telefonkonferenzsymbol auswählen Und wählen Sie dann das +-Symbol.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Popup-Fenster „Telefonkonferenz starten“ wird angezeigt.

4. Wählen Sie eine Konferenzbrücke in aus **Konferenzbrücke** Feld.
5. Geben Sie einen Titel für die Telefonkonferenz in an **Titel** .

   Hinweis:
   Standardmäßig wird der Titel des Incident als Titel des Anrufs ausgefüllt. Sie können den Standardtitel ändern.

6. Fügen Sie Anrufteilnehmer in hinzu, oder entfernen Sie sie **Fügen Sie Teilnehmer hinzu** .

   Hinweis:
   Basierend auf der Konfiguration in den Einstellungen für Telefonkonferenzen wird eine vorab ausgefüllte Liste von Teilnehmern zu hinzugefügt **Fügen Sie Teilnehmer hinzu** Oder ein **Empfehlungen** Liste der Teilnehmer ist verfügbar. Weitere Informationen finden Sie unter Verwalten Sie Benutzer und Gruppen von Telefonkonferenzen.

7. Geben Sie eine kurze Beschreibung für den Beginn der Telefonkonferenz an.
8. Wählen Sie **Start**.

   Die Telefonkonferenz beginnt in der ausgewählten Konferenzbrücke. Alle Teilnehmer erhalten Benachrichtigungen per E-Mail und über die Konferenzbrücke. Die Teilnehmer können den Link oder die Benachrichtigung verwenden, um an dem Anruf teilzunehmen.

9. Öffnen Sie den zugehörigen Incident in Security Incident Response Anwendung zum Anzeigen der Telefonkonferenzdetails.
10. **Wahlweise:** Wählen Sie Aus **Kopieren Sie die Einladung** Zum Hinzufügen von Teilnehmern in einem aktiven Anruf.
11. Wählen Sie **Anruf beenden** aus.
    Wenn der endgültige Teilnehmer die Telefonkonferenz verlässt, wird die Telefonkonferenz beendet
12. **Wahlweise:** Um eine Telefonkonferenz neu zu starten, navigieren Sie zu **Abgeschlossen** Abschnitt und wählen Sie aus **Erneut Initiieren** Option der erforderlichen Telefonkonferenz.

Fügen Sie der aktiven Telefonkonferenz Teilnehmer hinzu

Sie können einer aktiven Telefonkonferenz Teilnehmer hinzufügen, wenn Sie sie vor Beginn der Telefonkonferenz nicht hinzugefügt haben.

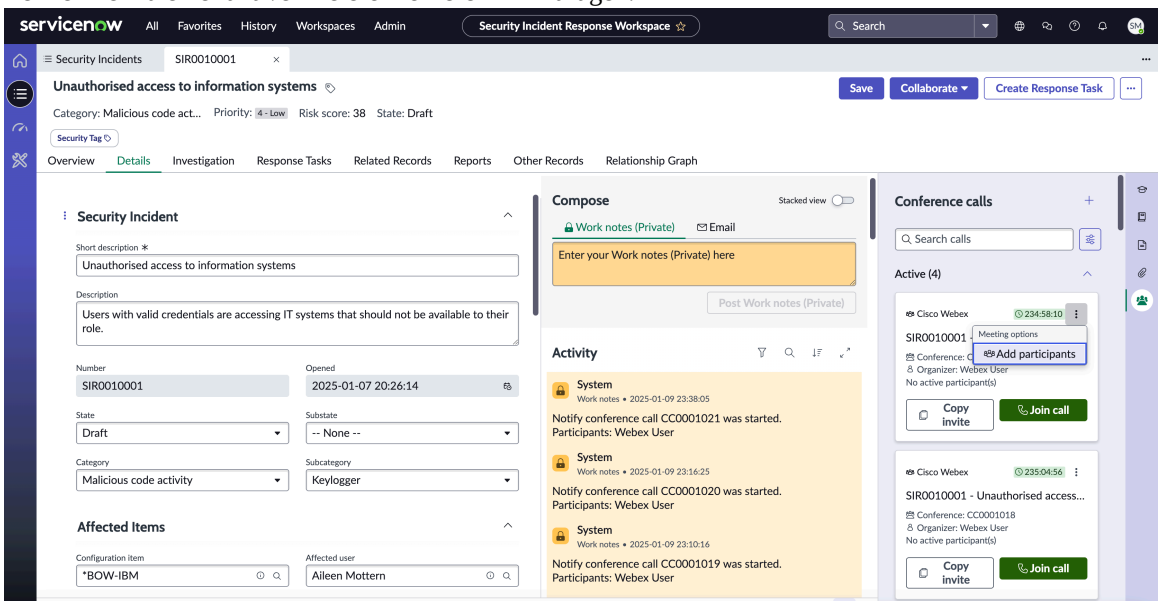
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst,sn_si.Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie den Security Incident, für den Sie eine Telefonkonferenz initiieren möchten.
3. Wählen Sie das Symbol Telefonkonferenz, um die Details der Telefonkonferenzen anzuzeigen.
4. Teilnehmer zu einer aktiven Telefonkonferenz hinzufügen:



   - Wählen Sie das Symbol für Besprechungsoptionen ⋮ Für die aktive Telefonkonferenz und wählen Sie aus **Fügen Sie Teilnehmer hinzu** .
   - Wählen Sie Aus **Kopieren Sie die Einladung** Auf der **Telefonkonferenzen** Und teilen Sie die Einladung für die erforderlichen Teilnehmer.

Starten Sie einen Sidebar-Chat in Security Incident Response

Mithilfe der Sidebar können Sicherheitsanalysten basierend auf einem aufgabenbasierten oder interaktionsbasierten Datensatz des Arbeitsbereichs in Echtzeit mit anderen zusammenarbeiten. Diese Sidebar-Diskussionen erleichtern den Austausch von Informationen und Wissen, um Probleme schneller und mit Ergebnissen höherer Qualität zu lösen.

Vorbereitungen
Erforderliche Rolle: sn_si.read

Überprüfen Sie, ob Sie das Plugin „Omni-Experience Standard-Funktionssatz“ aktiviert haben. Weitere Informationen finden Sie unter Installing Sidebar .

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Wählen Sie die Listenansicht aus Symbol.
3. Öffnen Sie einen Security Incident, für den Sie eine Sidebar-Diskussion initiieren möchten.
4. Wählen Sie Aus **Zusammenarbeiten** , Und wählen Sie dann aus **Starten Sie Den Chat** .

Automatische Übersetzung

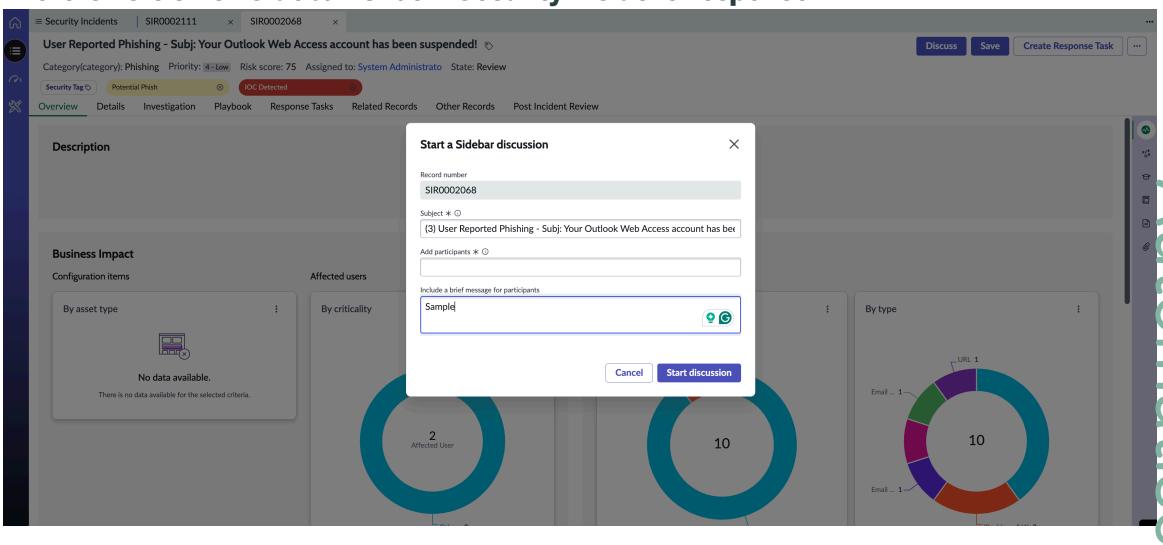
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Dialogfeld Sidebar-Diskussion starten wird angezeigt.

Hinweis:
Die Integration der Sidebar mit Microsoft Teams ermöglicht Sidebar-Anwendern und Microsoft Teams-Anwendern die Kommunikation über ihre jeweiligen Plattformen. Weitere Informationen finden Sie unter Sidebar and Microsoft Teams .

5. Füllen Sie die Felder im Dialogfeld Sidebar-Diskussion starten aus.

Initiieren Sie einen Sidebar-Chat in Security Incident Response



6. Wählen Sie **Start discussion (Diskussion starten)**.

7. Sie können zusätzliche Konfigurationen wie Schnellaktionen durchführen.
Um die Aktionsnutzung einzuschränken, können Sie verwenden **Auf Gruppe anwenden** Feld auf der Schnellaktionsseite. Weitere Informationen finden Sie unter Creating a quick action .

Incident-Details mit einem Beziehungsdiagramm anzeigen

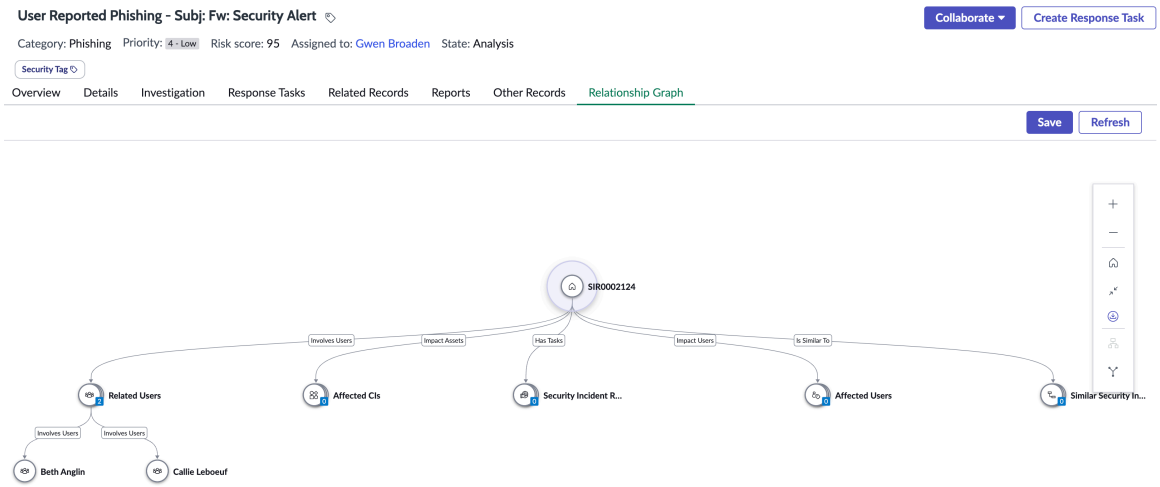
Beziehungsdiagramme in Security Incident Response Arbeitsbereich zeigt die Verbindungen zwischen einem Security Incident und seinen zugehörigen Elementen visuell an, damit Sie den vollständigen Kontext eines Security Incidents analysieren können.

Elemente im Zusammenhang mit einem Security Incident können zugehörige erkennbare Elemente, Konfigurationselemente (Configuration Items, CIs), ähnliche Security Incidents (SIRS), Antwortaufgaben und andere zugehörige Listen enthalten.

Das folgende Beziehungsdiagramm zeigt Details für einen Security Incident an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie ein Beziehungsdiagramm für einen Security Incident öffnen, sind die verfügbaren Konfigurationen standardmäßig sichtbar. Sie können wie folgt mit dem Diagramm interagieren:

- Vergrößern Sie ein beliebiges Objekt, das in den Bildschirm passt, und ziehen Sie die Knoten.
- Fügen Sie Unterknoten für jeden Knoten hinzu, falls verfügbar, und zeigen Sie Details der Unterknoten an.
- Blenden Sie Knoten oder Unterknoten im Diagramm aus.
- Zeigen Sie Details eines Unterknotens an.

Passen Sie ein Beziehungsdiagramm an

Visualisieren und analysieren Sie Security Incidents und die zugehörigen Daten in einem Beziehungsdiagramm.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response-Arbeitsbereiche** > **Administration**an.
2. Wählen Sie Aus **Beziehungsdiagramm** , Und dann **Beziehungsdiagrammkonfigurationen** .
3. Wählen Sie **Neu**.
4. Füllen Sie im Formular die Felder aus.

Beziehungsdiagrammkonfigurationen

Feld	Beschreibung
Zugehöriger Tabellenname	Die Tabelle, aus der Sie die erkennbaren Daten für Security Incidents abrufen möchten, z. B. die Tabelle „erkennbares Element zuordnen“ [sn_ti_observable] oder die Tabelle „Security Incident“ [sn_si_Incident].
Knotenbezeichnung	Die Knotenbezeichnung für das erkennbare Element, das im Beziehungsdiagramm angezeigt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der automatisch angegebene Wert hängt von der ausgewählten zugehörigen Tabelle ab.
Aktiv	Option zum Aktivieren der Konfiguration.
Datenknotenbezeichnung	Die primäre und sekundäre Bezeichnung, die auf dem Knoten für die ausgewählte zugehörige Liste angezeigt werden sollen.
Standardmäßig sichtbar	Option zum Anzeigen der Datenknotenbezeichnung.
Beziehungsbezeichnung	Die Beziehung zwischen einem Knoten und einem Linkknoten, die im Beziehungsdiagramm angezeigt werden soll.

5. Wählen Sie **Speichern**.

Erstellen Sie ein Beziehungsdiagramm für einen Incident

Erstellen Sie ein Knotenbeziehungsdiagramm in Security Incident Response Damit Sie einen Security Incident besser analysieren können, indem Sie ihn mit schädlichen erkennbaren Elementen, Konfigurationselementen (Configuration Items, CIs), ähnlichen Security Incidents (SIRS), Antwortaufgaben und anderen zugehörigen Informationen korrelieren.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Informationen zum Erstellen eines anwenderdefinierten Beziehungsdiagramms anstelle eines vordefinierten Diagramms finden Sie unter Passen Sie ein Beziehungsdiagramm an.

Hinweis:
Änderungen am Beziehungsdiagramm werden nicht automatisch gespeichert.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen Security Incident.
3. Wählen Sie aus **Beziehungsdiagramm** Registerkarte.
4. Wählen Sie im Beziehungsdiagramm den übergeordneten Knoten aus, halten Sie ihn gedrückt (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie dann aus **Knoten Hinzufügen** .
5. Wählen Sie einen oder mehrere Kategorieknoten aus, die im Beziehungsdiagramm angezeigt werden sollen, z. B. zugehörige Anwender, betroffene CIs, ähnliche Security Incidents (SIRS) oder betroffene Anwender.

   Hinweis:
   Sie können mehrere Kategorieknoten auswählen.

6. Wählen Sie einen Kategorieknoten aus, halten Sie ihn gedrückt (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie ihn aus **Knoten Verknüpfen** Zum Hinzufügen von Daten, die dem Kategorieknoten zugeordnet sind.

   Hinweis:
   Sie können Filter anwenden, um die Anzahl der Elemente in der Liste zu reduzieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Liste aller zugehörigen Datensätze für den ausgewählten Kategorieknoten wird angezeigt. Beispiel: Wenn Sie auswählen **Betroffene Anwender** In der Knotenkategorie wird eine Liste aller von diesem Incident betroffenen Anwender angezeigt.

7. Wählen Sie die gewünschten Datensätze aus der Liste aus, und wählen Sie aus **Hinzufügen** .
8. Wählen Sie **Hinzufügen**.
9. **Wahlweise:** Löschen Sie bei Bedarf Changes, indem Sie auswählen **Aktualisieren** .
10. Wählen Sie **Speichern**.

Hinweis:
Änderungen an Filtern werden auch gespeichert, wenn Sie das Beziehungsdiagramm speichern.

11. **Wahlweise:** Zeigen Sie die Details eines Unterknotens an.
    a. Wählen Sie einen Unterknoten aus.
    b. Wählen Sie Aus **Details Anzeigen** .
12. **Wahlweise:** Laden Sie die Karte auf Ihr System herunter.
    a. Wenn nur ein Teil der Karte auf dem Bildschirm sichtbar ist und Sie möchten, dass der gesamte Bildschirm in die PDF-Datei aufgenommen wird, wählen Sie das Symbol an Bildschirm anpassen ( ).

Hinweis:
Nur der Teil der Karte, der auf dem Bildschirm angezeigt wird, ist in der PDF-Datei enthalten.

    b. Wählen Sie das Symbol „Karte exportieren“ ( ).

Example: Video, das zeigt, wie ein Beziehungsdiagramm bearbeitet wird, um Kategorieknoten und Unterknoten hinzuzufügen

https://player.vimeo.com/video/1095955062?h=593c16e2b6&badge=0&autopause=0&player_id=0&app_id=58479

Security Incident-Playbook

Rufen Sie den Security Incident-Playbook-Flow automatisch oder manuell auf.

Ein Playbook ist nur sichtbar, wenn mindestens ein Playbook einem Security Incident zugeordnet ist. Die Playbook-Komponente funktioniert nur für die vom Prozessautomatisierungs-Designer (PAD) erstellten Prozesse und nicht für die vom Flow Designer erstellten Flows. Für die vorhandenen Flow Designer-fähigen Flows funktioniert es weiterhin, und die Aktivitäten werden weiterhin als Antwortaufgaben gerendert.

Es gibt zwei Möglichkeiten, dem Security Incident ein Playbook zuzuordnen:

- Playbook automatisch aufrufen
- Fügen Sie Playbook manuell hinzu

Playbook automatisch aufrufen

Damit ein Playbook automatisch aufgerufen wird, muss ein Prozess mit definiert werden **Prozessautomatisierungs-Designer (PAD)** , Und wenn die Auslöserbedingung erfüllt ist, wird automatisch die Playbook-Registerkarte gerendert und die Playbook-Aktivitäten angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie Playbook manuell hinzu

Damit ein Playbook manuell aufgerufen werden soll, navigieren Sie zur Dropdown-Liste der Formular-UI-Aktion, und wählen Sie aus **Fügen Sie Playbook Hinzu** . Weitere Informationen finden Sie unter . Playbook hinzufügen

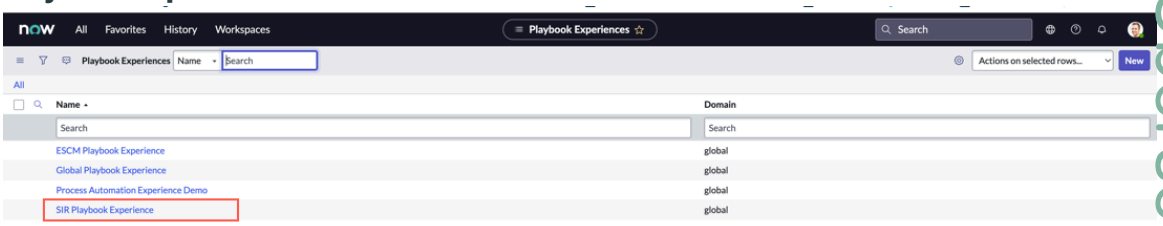
Hinweis:
Wenn bereits ein Playbook verfügbar ist, werden die neu hinzugefügten Playbooks parallel zu den vorhandenen Playbooks ausgeführt.

- Innerhalb des Playbooks kann der Analyst die Playbook-Karten nach Status filtern.
- Der Analyst kann ein Playbook abbrechen, indem er es über das Ellipsensymbol auswählt.
- Innerhalb jeder Aktivität kann der Analyst die in den Aktivitätskarten definierten Aktionen ausführen, z. B. Überspringen, als abgeschlossen markieren, Abbrechen oder Orchestration-Aktionen wie an Sandbox senden, E-Mails durchsuchen usw.
- Jede dieser Aktionen ist in der Aktivitätsdefinition definiert, und die vollständige sichtbare Karte kann zum Zeitpunkt der Erstellung der Aktivitätsdefinition selbst angepasst werden.

Hinweis:
Alle zukünftigen Aktivitätsdefinitionen und die nächsten auszuführenden Schritte werden mit einem Sperrsymbol angezeigt und befinden sich für den Anwender im schreibgeschützten Modus. Der Playbook-Anzeigemodus wird durch eine Konfiguration gesteuert, wie unten erläutert.

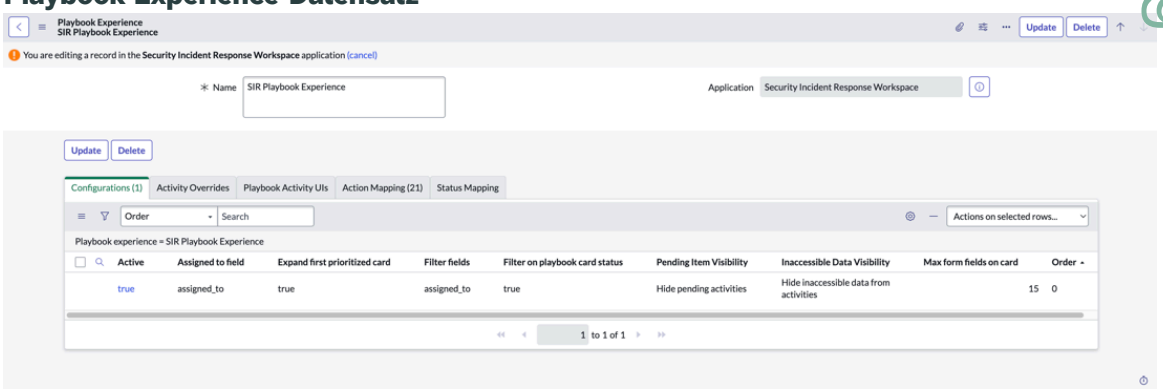
1. Navigieren zu **Alle** > **Playbook-Experiences**an.
2. Wählen Sie auf der Seite „Playbook-Experiences“ eine aus **SIR-Playbook-Experience** .

Playbook-Experience



Die **Playbook-Experience SIR-Playbook-Experience** Seite wird angezeigt.

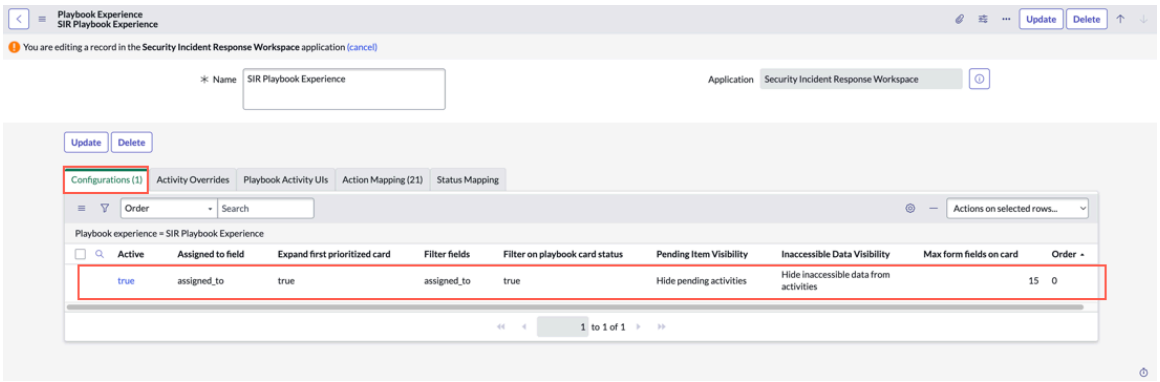
Playbook-Experience-Datensatz



3. Klicken Sie auf **Konfiguration** Datensatz.

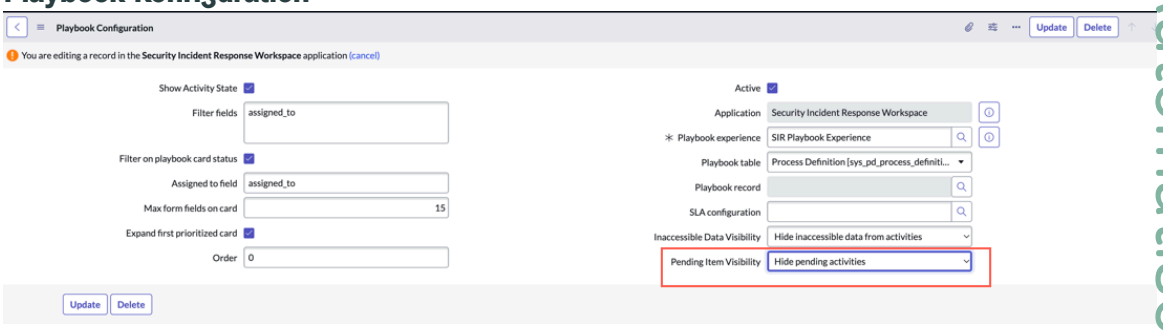
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



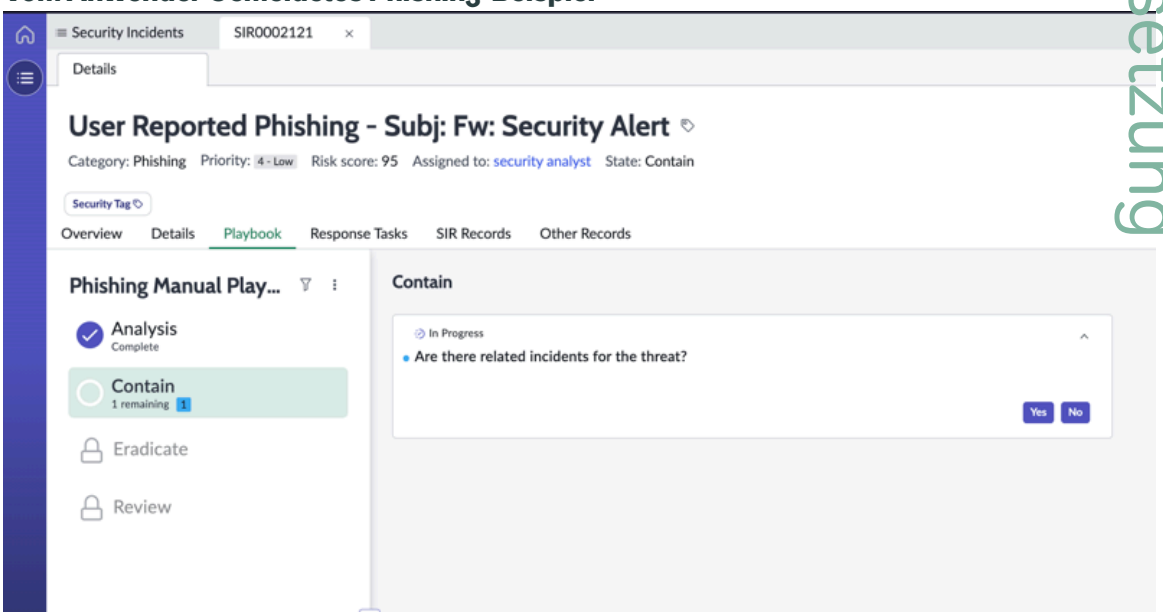
4. Klicken Sie auf der Registerkarte Konfiguration auf die SIR Playbook Experience-Konfiguration.

Playbook-Konfiguration



5. Navigieren Sie zu **Sichtbarkeit Ausstehender Elemente** Wählen Sie die gewünschte Option aus, und speichern Sie den Datensatz. Wählen Sie eine der folgenden Optionen aus:
   - **Ausstehende Aktivitäten ausblenden** : Wählen Sie diese Option aus, um die ausstehenden Aktivitäten auszublenden, die Sie im Playbook-Abschnitt des Arbeitsbereichs anzeigen möchten.

Vom Anwender Gemeldetes Phishing-Beispiel

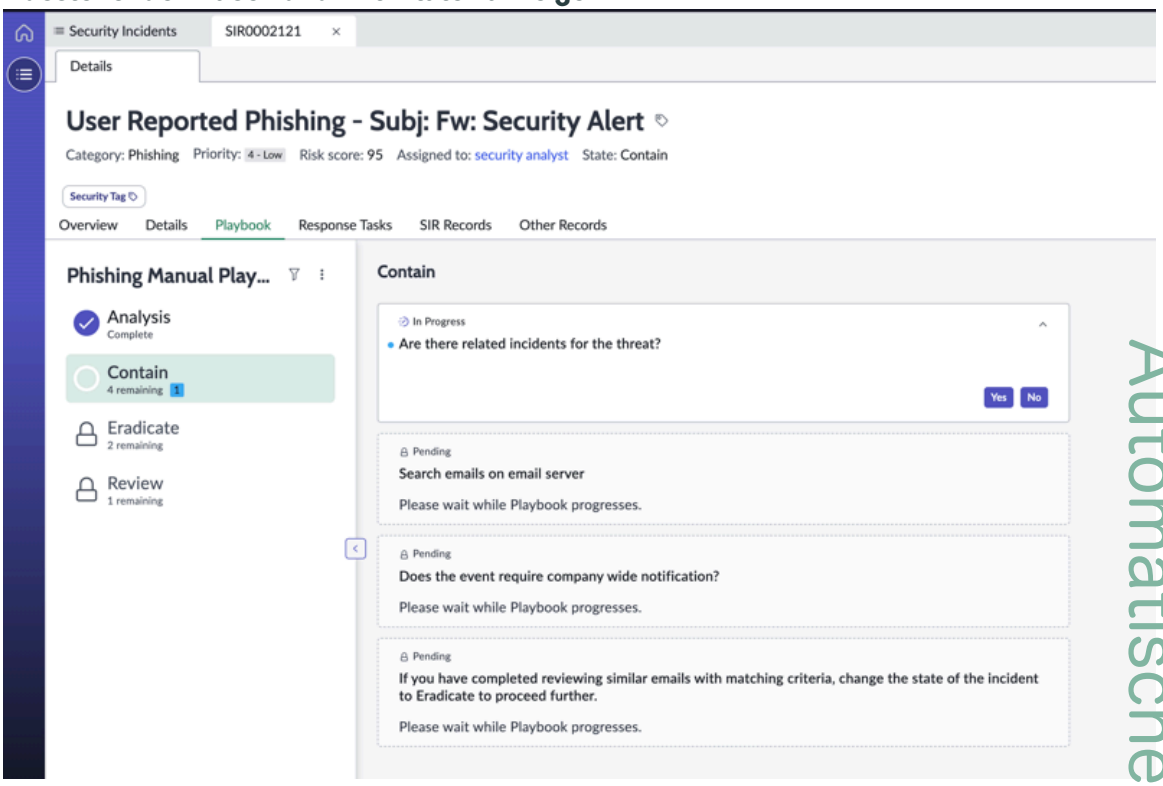


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

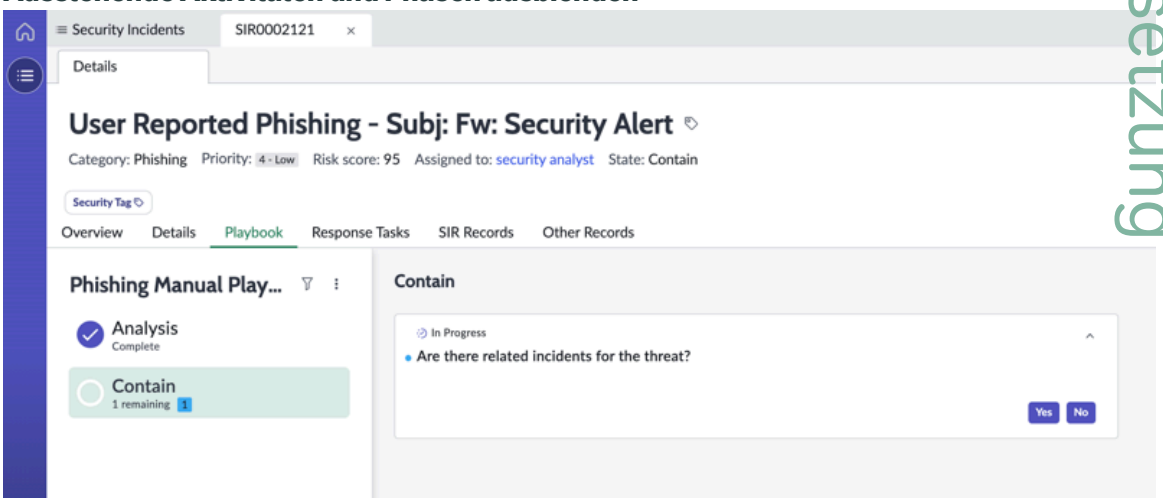
- **Ausstehende Phasen und Aktivitäten anzeigen** : Wählen Sie diese Option aus, um ausstehende Phasen und Aktivitäten anzuzeigen, die Sie im Playbook-Abschnitt des Arbeitsbereichs anzeigen möchten.

Ausstehende Phasen und Aktivitäten anzeigen



- **Ausstehende Aktivitäten und Phasen ausblenden** : Wählen Sie diese Option aus, um ausstehende Aktivitäten und Phasen auszublenden, die Sie im Playbook-Abschnitt des Arbeitsbereichs anzeigen möchten.

Ausstehende Aktivitäten und Phasen ausblenden

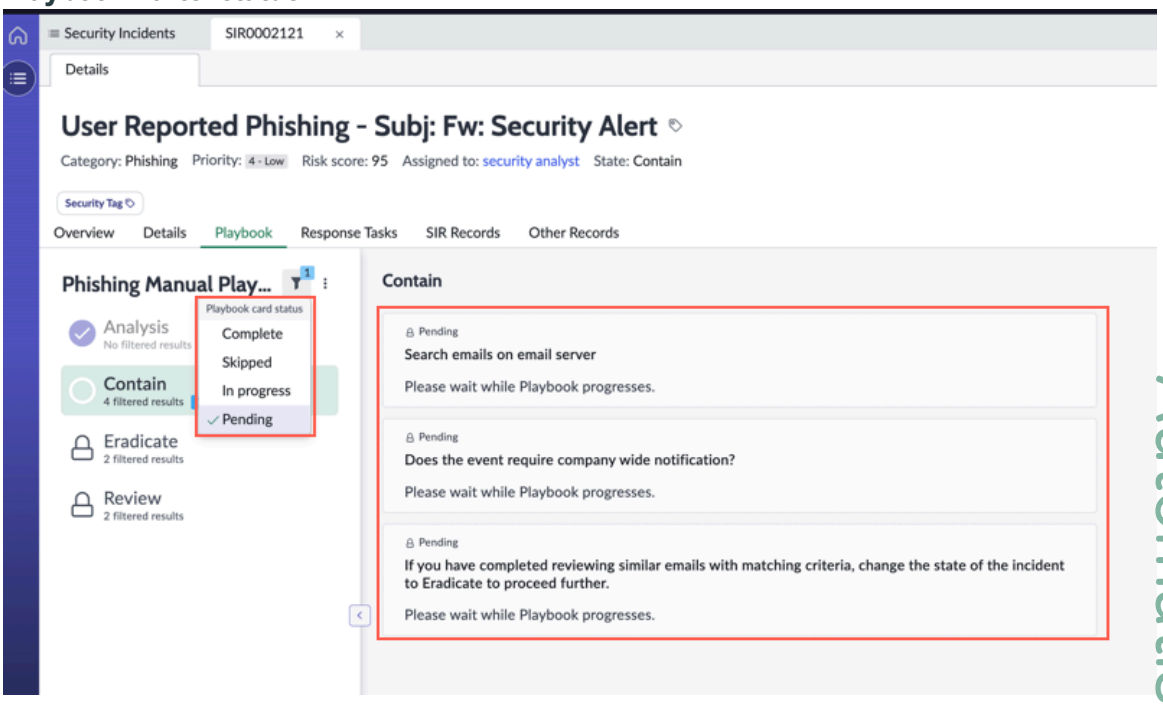


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Verwenden Sie im Abschnitt Playbook die Filteroption, um die Aktivitäten nach Playbook-Kartenstatus (Aktivitätsdefinition) zu filtern.

Playbook-Kartenstatus



Playbook hinzufügen

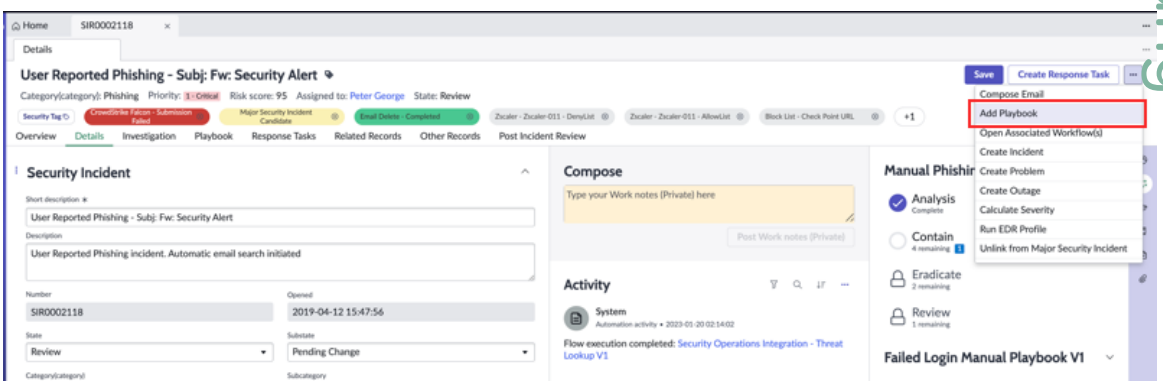
Verwenden Sie diesen Abschnitt, um Playbook manuell hinzuzufügen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

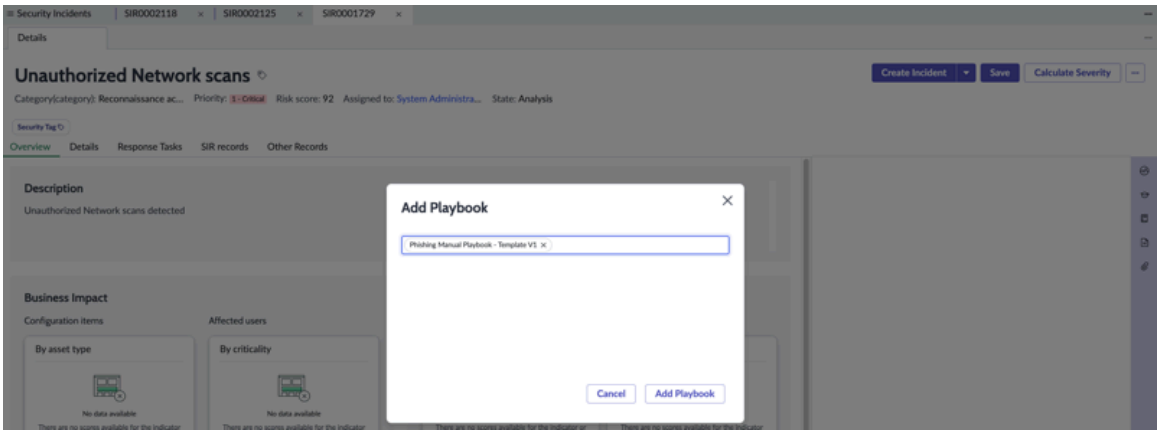
1. Navigieren zu **Alle** > **Security Incident** > **Security Analyst Workspace**an.
2. Öffnen Sie einen Incident-Datensatz.
3. Klicken Sie Auf **Fügen Sie Playbook Hinzu** .



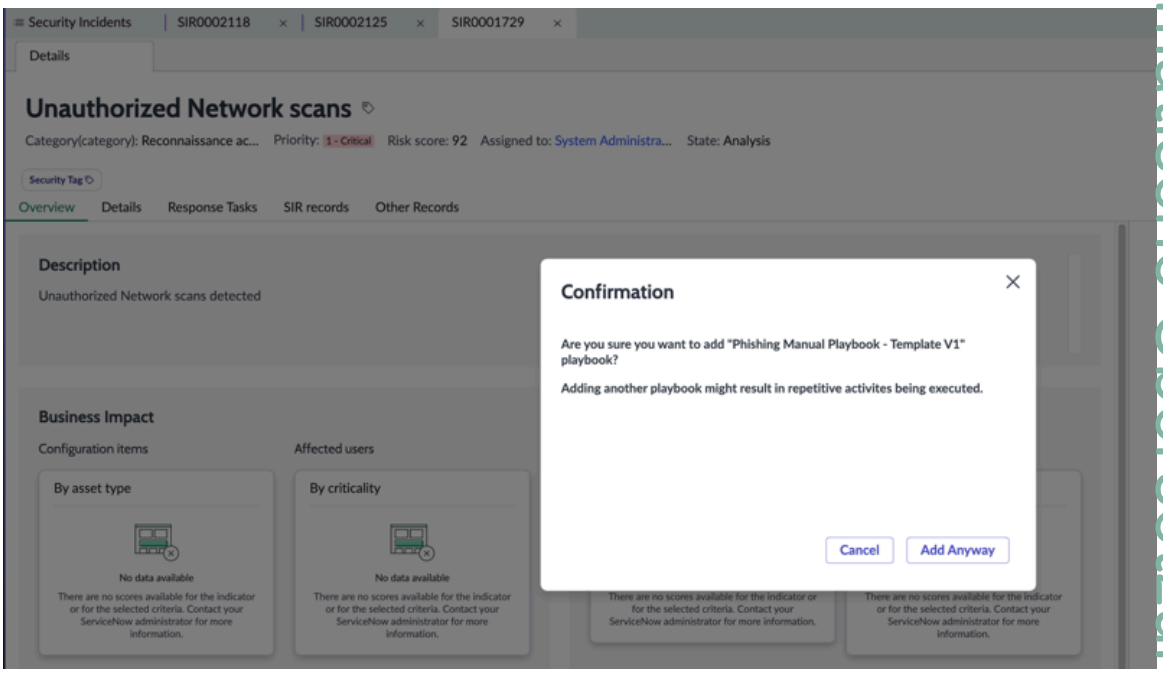
Die **Fügen Sie Playbook Hinzu** Dialogfeld wird angezeigt.

Automatische Übersetzung

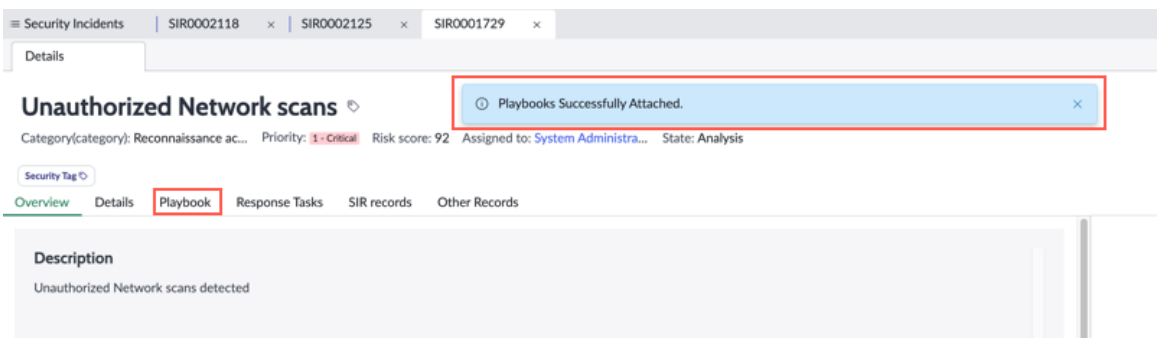
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Playbook-Vorlage aus.
5. Klicken Sie Auf **Fügen Sie Playbook Hinzu** .
   Ein Dialogfeld mit Bestätigungsnachricht wird angezeigt, in dem Sie bestätigen können.
6. Klicken Sie Auf **Trotzdem Hinzufügen** .



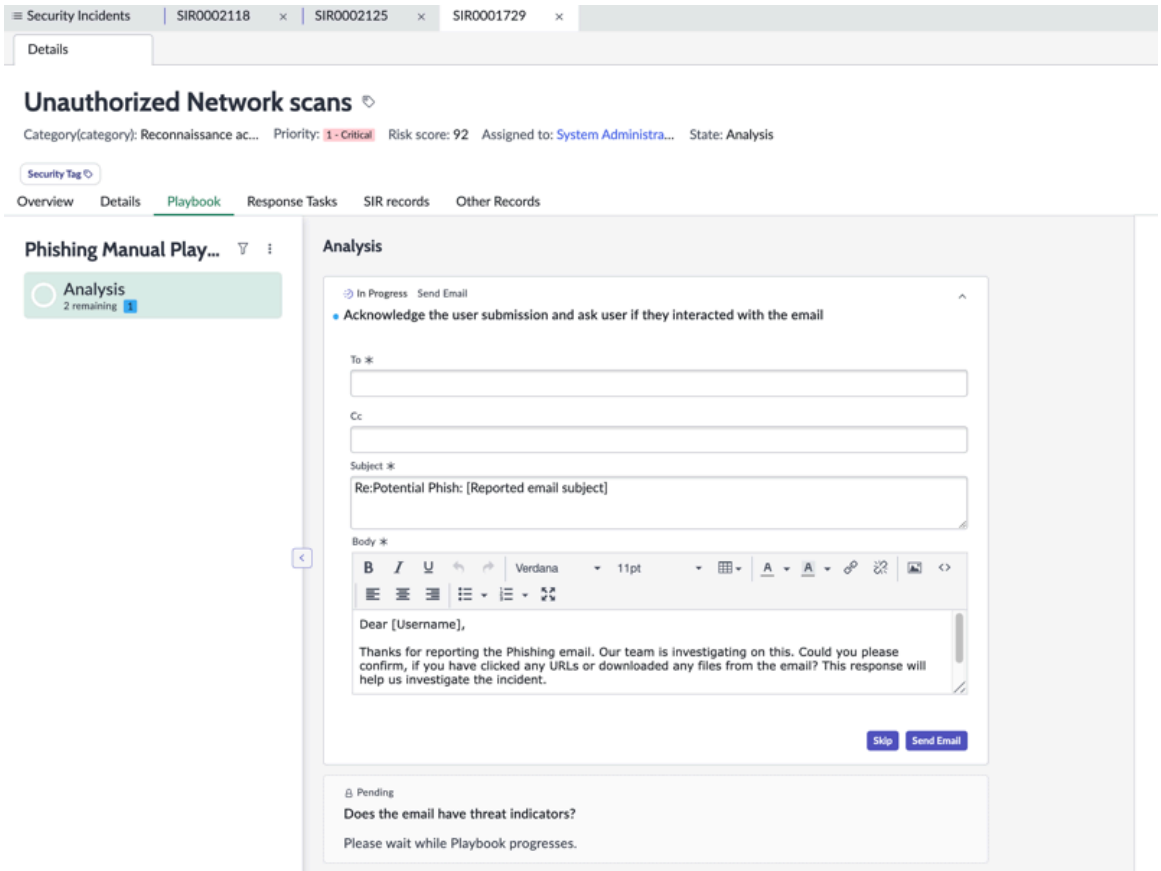
7. Die **Playbook** Wird neben hinzugefügt **Details** Registerkarte.



8. Klicken Sie auf **Playbook** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Führen Sie die aufgeführten Aktivitäten aus, um zur nächsten Ebene zu wechseln.

> **Hinweis:**
> Wenn ein Security Incident einem Playbook zugeordnet ist, kann der Anwender bis zum Schließen oder Abbrechen des zugehörigen Playbooks dasselbe Playbook nicht erneut demselben Security Incident zuordnen.

Voraussetzungen für die Playbooks

Sie benötigen die folgenden Rollen und Plugins, um die Playbooks zu erstellen.

Erforderliche Rolle: admin.

- Aktivieren Sie das Plugin Process Automation Designer (PAD) [com.Glide.Pad.license].
- Aktivieren Sie die folgenden Plugins für eine Playbook-Experience:
  - com.playbook_experience
  - Now_Playbook_exp
  - com.glide.playbook_experience.config
- Aktivieren Sie die Security Operations-Spoke, um auf Flows zuzugreifen [com.snc.secops.spoke].
- Enterprise Security Case Management PAD Commons.

Stellen Sie sicher, dass Sie die Plattformdokumentation in gelesen haben Exploring playbooks Und Prozessautomatisierungs-Designer Bevor Sie mit diesem Leitfaden beginnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorhandene Playbooks in werden neu erstellt Workflow-Studio

Sie können vorhandene Flows in nicht direkt in Playbooks konvertieren Workflow-Studio. Jeder Flow Designer-Schritt, der eine Antwortaufgabe erstellt, um den Analysten zu leiten, muss in separate Aktionen oder Subflows aufgeschlüsselt werden.

Sie dürfen vorhandene Flows in nicht direkt in Playbooks konvertieren Workflow-Studio. Jeder Flow Designer-Schritt, der eine Antwortaufgabe erstellt, um den Analysten zu leiten, muss in separate Aktionen oder Subflows aufgeschlüsselt werden. Mithilfe dieser granularen Subflows oder Aktionen müssen Sie Aktivitätsdefinitionen erstellen. Nachdem Sie diese Aktivitätsdefinitionen erstellt haben, werden sie als Aktivitäten innerhalb der Phase in der Prozessdefinition hinzugefügt. Sie können Aktivitätsdefinitionen in mehreren Playbooks wiederverwenden.

Sie können jede Aktivität anpassen, um die erforderlichen Aktionen darin zu rendern und wie die Karte beim Erstellen der Aktivitätsdefinition aussehen soll. Die Aktivität kann E-Mail-Clients, Tabellen, Aktionen, KB-Artikel, URLs anzeigen. und so weiter. Sie können definieren, wie die Aktivitätsdefinition und die zugrunde liegende Aktion oder Subflows erstellt werden.

Weitere Informationen finden Sie in den folgenden Abschnitten.

- Aktivitätsdefinitionen
- Process Automation Designer

Aktivitätsdefinitionen

Die ServiceNow AI Platform Stellt einige Aktivitätsdefinitionen im Basissystem bereit. Darüber hinaus sind für die Playbooks, auf denen SIR Workspace-Basissystem basiert, einige Aktivitätsdefinitionen im Basissystem in der Commons-Anwendung „Enterprise Security Case Management“ definiert.

Erforderliche Rolle: sn_si.admin.

Hier ist die Liste der Aktivitätsdefinitionen, die Teil des Basissystems sind:

Aktivitätsdefinition	Tabelle	Beschreibung	Anwendung
Warten-auf-Bedingung ohne Experience	Global[global]	Warten auf Bedingung ohne Experience	Enterprise Security Case Management PAD Commons
An CSF X Sandbox übermitteln	Security Incident [sn_si_incident]	An die Sandbox übermitteln	Enterprise Security Case Management PAD Commons
E-Mail senden	Security Incident [sn_si_incident]	E-Mail-Aktivität für SIR-Playbooks senden.	Enterprise Security Case Management PAD Commons
E-Mail durchsuchen	Security Incident [sn_si_incident]	E-Mails auf dem E-Mail-Server durchsuchen	Enterprise Security Case Management PAD Commons
Aufgabenstatus aktualisieren	Security Incident [sn_si_incident]	Aktualisieren Sie den Aufgabenstatus	Enterprise Security Case Management PAD Commons
E-Mail löschen	Security Incident [sn_si_incident]	E-Mails löschen	Enterprise Security Case Management PAD Commons

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivitätsdefinition	Tabelle	Beschreibung	Anwendung
Ja/Nein-Ergebnis	Aufgabe [task]	Erwartetes Ergebnis	Enterprise Security Case Management PAD Commons

Beispiel für Aktivitätsdefinition: E-Mail senden

Im Folgenden finden Sie ein Beispiel für die Aktivitätsdefinition „E-Mail senden“.

Standard

Die grundlegenden Details erfassen den Namen (Bezeichnung), die Anwendung, die Beschreibung, die Tabelle und alle Anwendungen, über die sie aufgerufen werden kann.

Fügen Sie den Automatisierungsplan und die Aktivitätenerfahrung hinzu, und übermitteln Sie ihn. Bearbeiten Sie das Dokument nach dem Senden, um weitere Details für jede Registerkarte hinzuzufügen.

Automatisierungsplan

Der Automatisierungsplan ordnet die Back-End-Aktion oder Subflows zu, die mit dem Flow Designer erstellt wurden. In diesem Beispiel wird Folgendes verwendet: **E-Mail senden: ESCM-Aktivität** subflow.

Dieser Subflow ermöglicht das Senden einer E-Mail. Es verfügt über die Kernlogik zum Senden einer E-Mail. Alle Eingabefelder und Ausgabefelder sind definiert.

Alle Eingabefelder werden im Abschnitt „Automatisierungsplan“ angezeigt. Jedes Eingabefeld kann so aktiviert werden, dass es nur für den Administrator sichtbar ist, im Standard-Modal, im Standard-Modal und im Konfigurationsbereich:

- **Nur Administratortransparenz** : Wenn auf „admin“ festgelegt, kann es nur der Administrator anzeigen.
- **In Standardmodell einschließen** : Wenn diese Option für die Anzeige im Standardmodal festgelegt ist, wird sie nur im Eigenschaftenmodal angezeigt.
- **In Standardmodell und Konfigurationsbereich einschließen** : Wenn diese Option für die Anzeige im Standardmodal und im Konfigurationsbereich festgelegt ist, wird sie im PAD-Konfigurationsbereich sowie im Eigenschaftenmodal angezeigt. Weitere Informationen finden Sie unter Aktivitätsdefinitionen

Sie können die Eingabefelder zum Zeitpunkt der Aktivitätsdefinition selbst definieren, sofern Sie diese Werte zum Zeitpunkt der Konfiguration nicht ändern müssen. Dies hilft dem Geschäftsprozessbesitzer, beim Konfigurieren einer Aktivität in einem Prozess Zeit zu sparen.

Aktivitäts-Experience

Die Registerkarte „Aktivitäts-Experience“ definiert, wie die Aktivitätenkarte zur Laufzeit gerendert wird. Das Basissystem bietet die folgenden Experience-Typen:

- Freigabe
- Katalogelement
- Datensatz erstellen
- Anweisend

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wissen
- Liste
- Benachrichtigung
- Datensatz

Je nach Typ der von Ihnen ausgewählten Experience werden die weiteren Felder ausgefüllt. Weitere Informationen finden Sie unter ServiceNow AI Platform Dokumentation.

In diesem Beispiel **Datensatz** Typ ist ausgewählt.

Hinweis:
Wenn Sie beispielsweise eine Tabelle rendern möchten, können Sie Liste als Experience-Typ auswählen.

Zugeordneter Datensatz

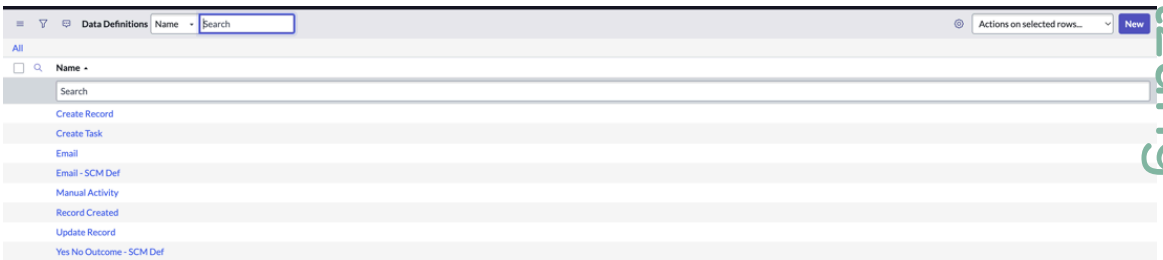
Verwenden Sie diesen Datensatz, um die zugehörigen Daten zu speichern, die sich auf die aktuelle Aktivität beziehen. Dadurch würden die Laufzeitdaten sowie der Status der Experience erfasst.

- Zugeordnete Tabelle: Flow-Daten
- Zugeordneter Datensatz: VL
- Experience-Statustabelle: Flow-Daten
- Experience-Statusdatensatz: VL

In diesem Beispiel wird die Flow-Datentabelle verwendet, um die Laufzeitdaten zu erfassen. Die Laufzeitdaten können je nach Anwendungsfall variieren. In diesem Beispiel sind die Laufzeitdaten Felder wie „an“, „cc“, „Betreff“ und „Textkörper“. Für jeden Anwendungsfall muss eine Flow-Datendefinition erstellt werden, um den Typ der Laufzeitdaten zu definieren.

1. Navigieren Sie zum linken Bereich, und geben Sie ein **sys_Flow_Data_Definition.list** . Zeigt die Liste der Definitionen an, die für die Flow-Datentabelle erstellt wurden.

Verbundener Datensatz

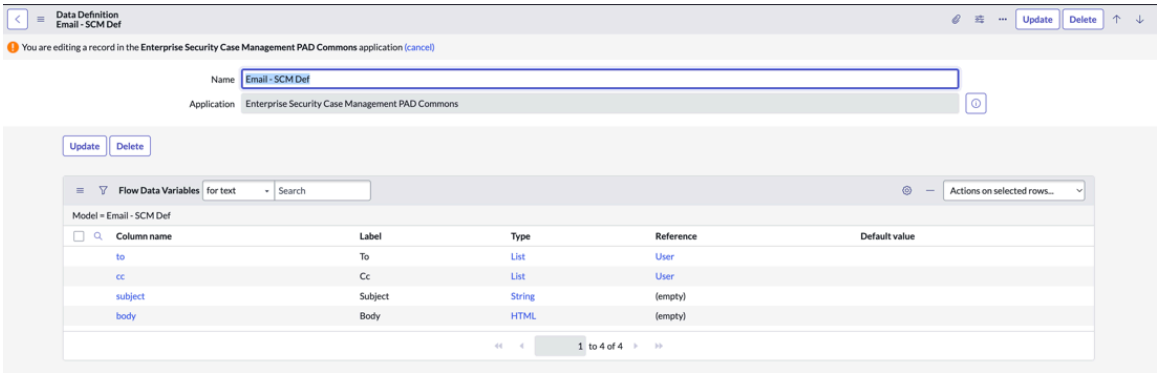


2. Öffnen **E-Mail: SCM-Definition** Zum Anzeigen der Definition im Zusammenhang mit diesem Beispiel.

Automatische Übersetzung

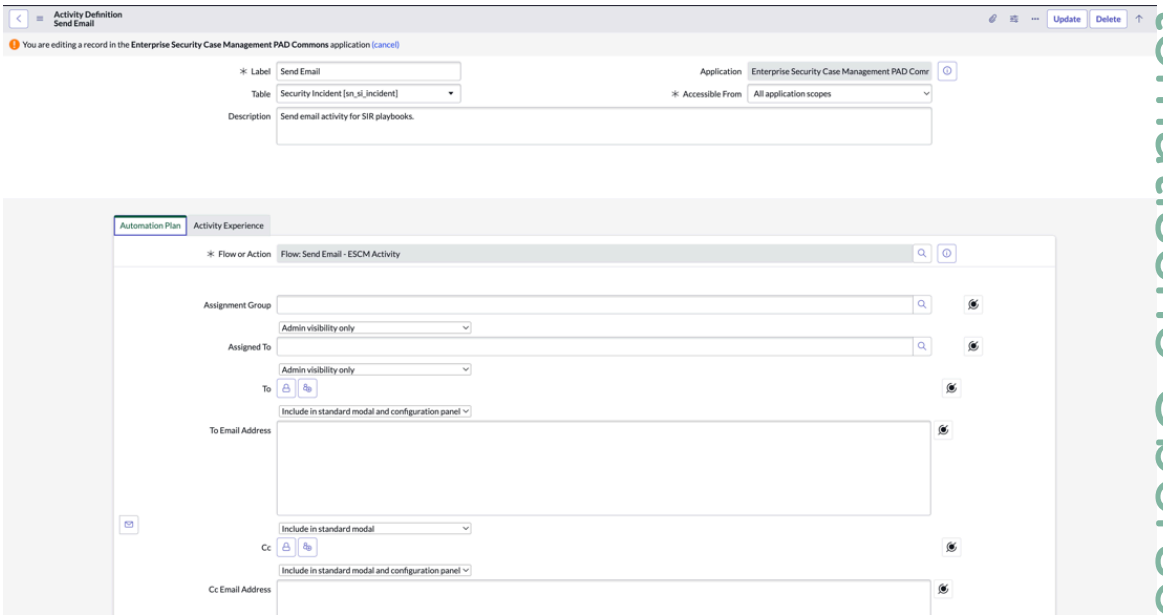
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail: SCM-Definition



Diese Flow-Datendefinition muss vom Subflow oder der Aktion verwendet werden, die dieser Aktivitätsdefinition zugeordnet ist (siehe Automatisierungsplan), um die Laufzeitdaten zu erfassen.

Aktivitätsdefinitionen

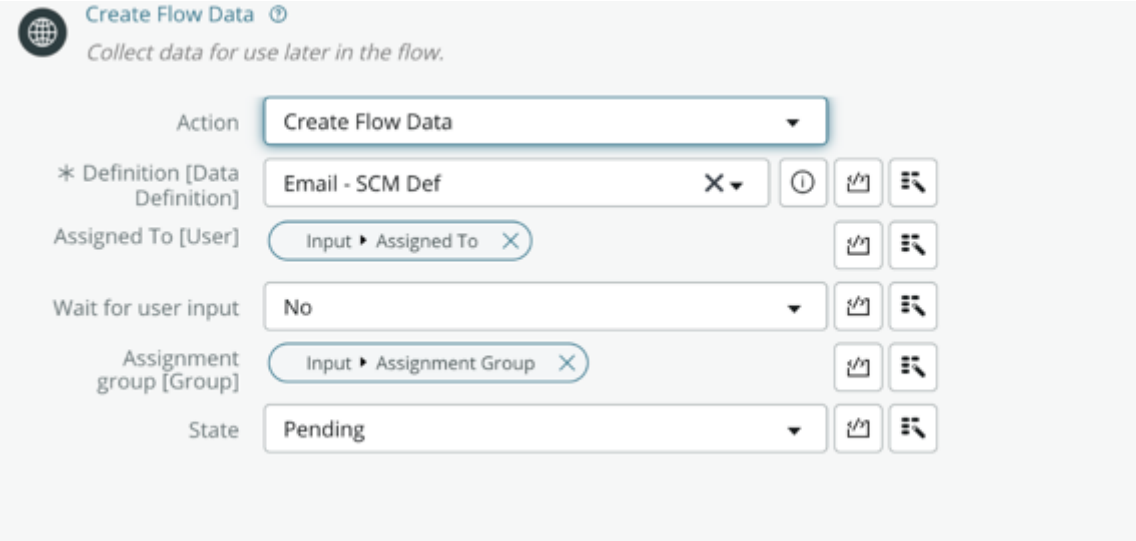


3. Öffnen Sie in diesem Beispiel den Subflow: **E-Mail senden: ESCM-Aktivität** . Unter **Erstellen Sie Flow-Daten** Schritt: Die von Ihnen erstellte Flow-Datendefinition wird dem zugeordnet **Definition** Feld. Dieser Flow-Datensatz wird im gesamten Subflow verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Beispiel wird der Aktivitätskartenstatus (Experience-Status) in der Flow-Datentabelle erfasst.

E-Mail senden: ESCM-Aktivität



Hinweis:

Wenn Sie die Laufzeitdaten in einem anderen Tabellendatensatz als der Flow-Datentabelle erfassen möchten, beispielsweise in einer Antwortaufgabe. Sie können die zugeordnete Tabelle als Antwortaufgabentabelle auswählen. Der zugeordnete Datensatz muss auf den vom Subflow erstellten Antwortaufgabendatensatz festgelegt werden.

Ebenso erfasst die Experience-Statustabelle den Status der Aktivitätskarte. Im Basissystem wird das Statusfeld der Flow-Datentabelle dem Aktivitätskartenstatus zugeordnet. Wenn also die Flow-Datentabelle zum Erfassen des Experience-Status verwendet wird, wird der Aktivitätskartenstatus automatisch aktualisiert. Sie können auch eine andere Tabelle als die Flow-Datentabelle verwenden, um den Experience-Status zu erfassen.

Wenn Sie beispielsweise den Antwortaufgabenstatus dem Aktivitätskartenstatus zuordnen möchten, ist dies möglich. Dazu:

1. Navigieren zu **Alle** > **Playbook-Experiences**an.

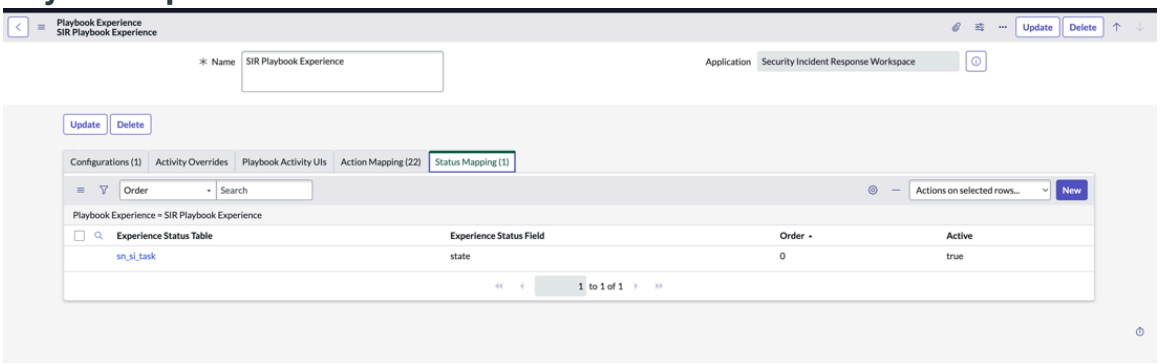
Playbook-Experiences

2. Öffnen **SIR-Playbook-Experience** .
3. Öffnen **Statuszuordnung** Zugehörige Liste.

Automatische Übersetzung

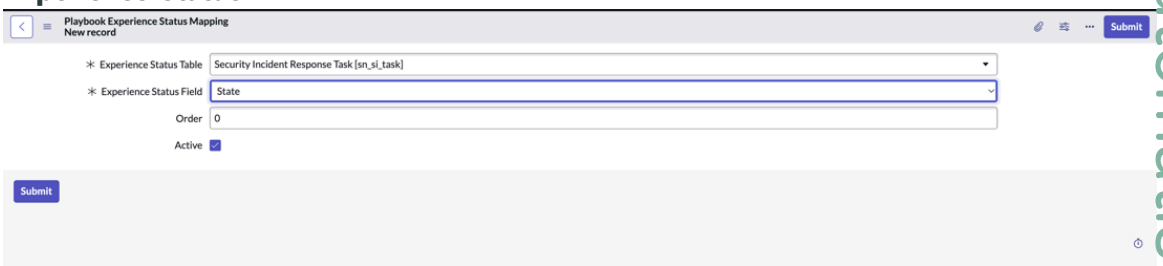
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook-Experience



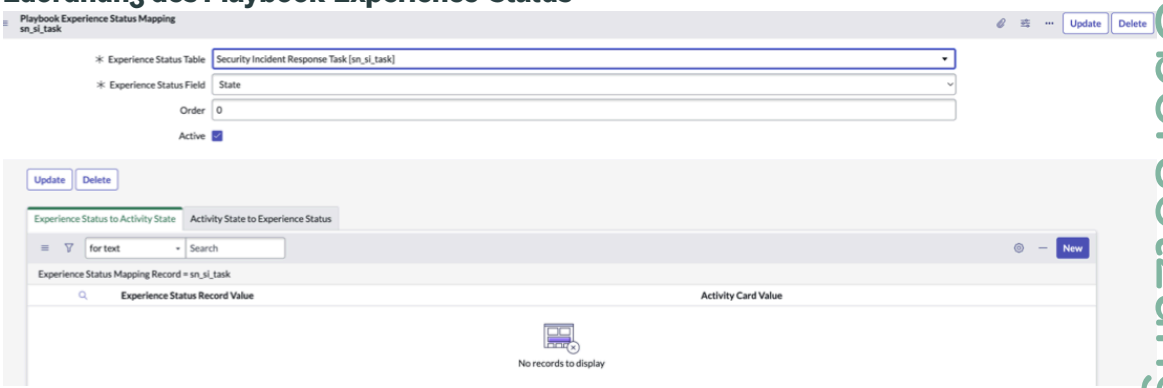
4. Geben Sie ein **Antwortaufgabe** Für Experience-Statustabellenfeld.
5. Geben Sie ein **Status** Für Experience-Statusfeld.

Experience-Status



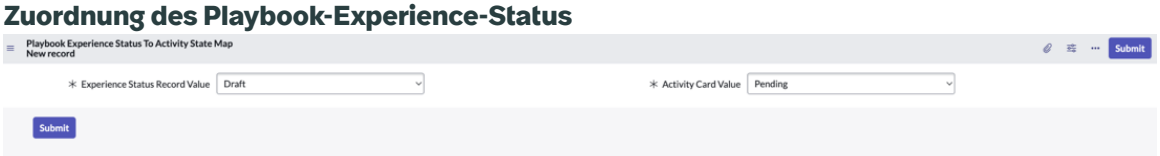
6. Klicken Sie auf **Absenden**. Der Datensatz wird erstellt.

Zuordnung des Playbook-Experience-Status



7. Ordnen Sie unter Experience-Status zu Aktivitätsstatus die status der Antwortaufgabe dem Aktivitätskartenstatus zu.
8. Auf der linken Seite werden die status der Antwortaufgabe angezeigt, auf der rechten Seite der Status der Aktivitätskarte.

Zuordnung des Playbook-Experience-Status



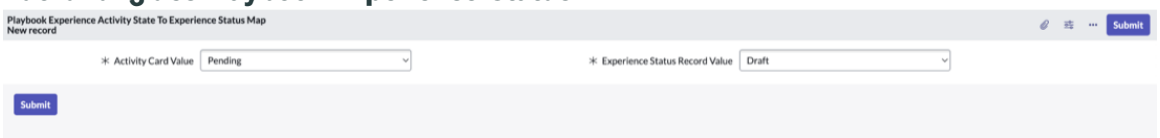
9. Die Zuordnung kann bidirektional sein. Ordnen Sie die Status unter Aktivitätsstatus auch der zugehörigen Experience-Liste korrekt zu. Dieser Schritt ist die umgekehrte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtung des vorherigen Schritts. In diesem Fall wird auf der linken Seite der Status der Aktivitätskarte angezeigt, und auf der rechten Seite der Status der Antwortaufgabe.

Zuordnung des Playbook-Experience-Status



Details

- Tag-Zeile: E-Mail Senden
- Symbol: Umschlagumriss (in der Anwenderoberfläche nicht angezeigt)
- Titel: **Aktivität** > **Aktivitätsinstanz** > **Bezeichnung**an. Hier haben wir die Bezeichnung der Aktivitätsinstanz ausgewählt. Bei diesem Dot-Walking wird der Bezeichnungswert zur Laufzeit dynamisch als Titel ersetzt.
- Beschreibung: **Aktivität** > **Aktivitätsinstanz** > **Beschreibung**an. Hier haben wir die Beschreibung der Aktivitätsinstanz ausgewählt. Bei diesem Dot-Walking wird der Bezeichnungswert zur Laufzeit dynamisch als Titel ersetzt.
- Titel des Status „Ausstehend“: E-Mail-Benachrichtigung senden. Dies ist der Titel, wenn sich die Aktivität im Status „Ausstehend“ befindet.
- Beschreibung des Status „Ausstehend“: Fordert vor dem Senden die Bestätigung des Betreffs und des Texts der E-Mail auf. Dies ist die Beschreibung der Aktivitätskarte, wenn der Status „Ausstehende Datensatzfelder“ lautet: In diesem Beispiel sind Datensatzfelder ausgewählt.

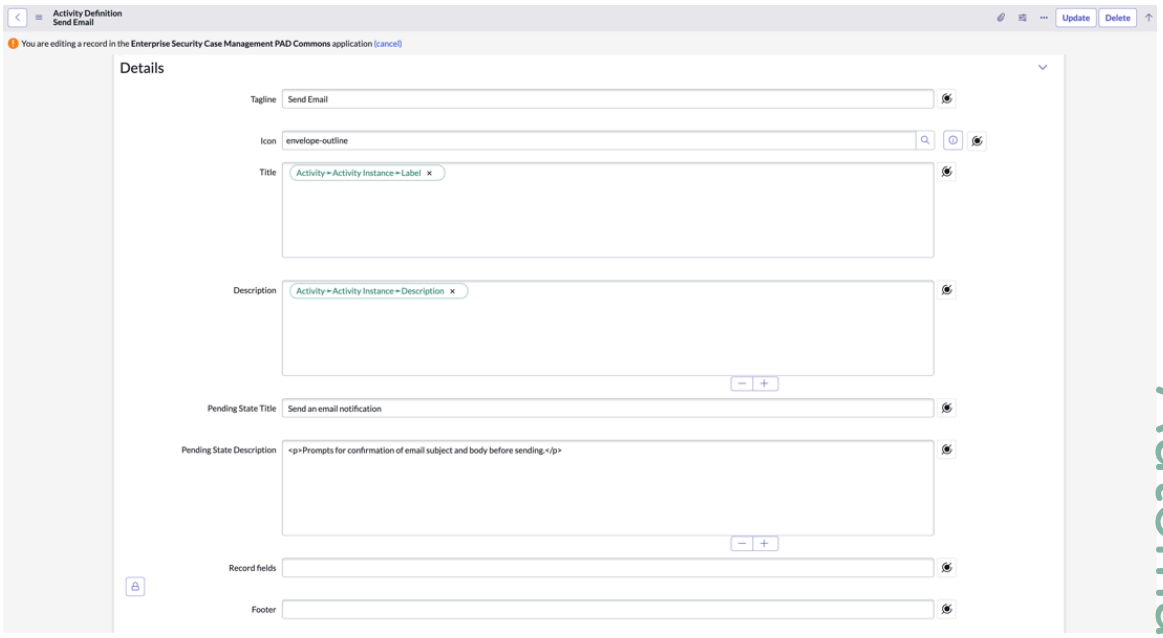
  Datensatzfelder sind eine kommagetrennte Liste von Feldnamen, die für den zugehörigen Datensatz in einer Name-Wert-Paarliste angezeigt werden sollen. Daten werden auf dem Server vorab abgerufen, Dot-Walking wird unterstützt und **CanRead()** #Berechtigungen werden für jedes Feld ausgewertet.

- Fußzeile: Für dieses Beispiel ist keine Fußzeile definiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fußzeile ist ein Text in einem grauen Bereich der Kartenfußzeile. Sie können dem angezeigten alle aussagekräftigen Informationen hinzufügen.

Aktivitätsdefinition: E-Mail Senden

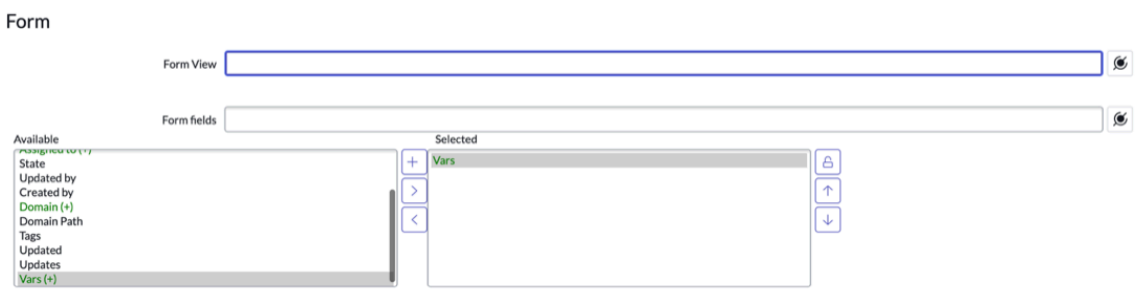


Formular

- Formularansicht: Collect_Data
- Formularfelder:

In diesem Beispiel wird die Ansicht „Collect_Data“ verwendet, um die Felder anzuzeigen, die dem Anwender zur Eingabe von Eingaben angezeigt werden müssen. Die Ansicht „Collect_Data“ ist eine von der Plattform bereitgestellte Ansicht, die der Flow-Datentabelle entspricht. Alternativ können Sie die Formularansicht leer lassen und VARs aus der Liste der für Formularfelder verfügbaren Werte auswählen. (Klicken Sie auf das Schlosssymbol, um die Liste der verfügbaren Werte zu öffnen.)

Formularansicht



Anhänge

Beispiel:

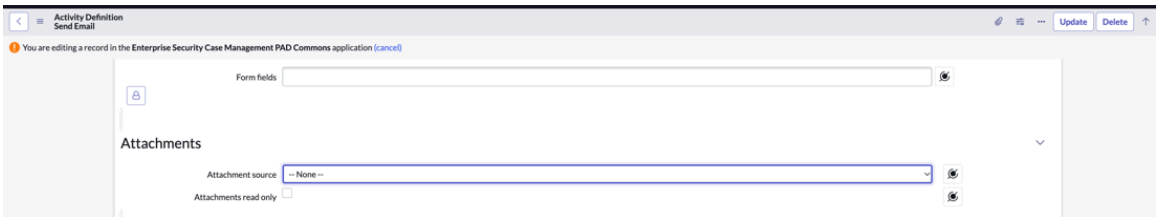
- Anhangsquelle ist leer.
- Anhang schreibgeschützt nicht ausgewählt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Anhangsquelle: Dropdown-Liste. Welche Anhänge auf der Karte angezeigt werden sollen: Diejenigen, die an den übergeordneten Datensatz, den zugehörigen Datensatz oder keinen angehängt sind.
2. Anhang schreibgeschützt: „Wahr“ oder „falsch“. Verhindern Sie, dass der Anwender die vorhandenen Anhänge umbenennt oder löscht.

Aktivitätsdefinition: E-Mail Senden



Features

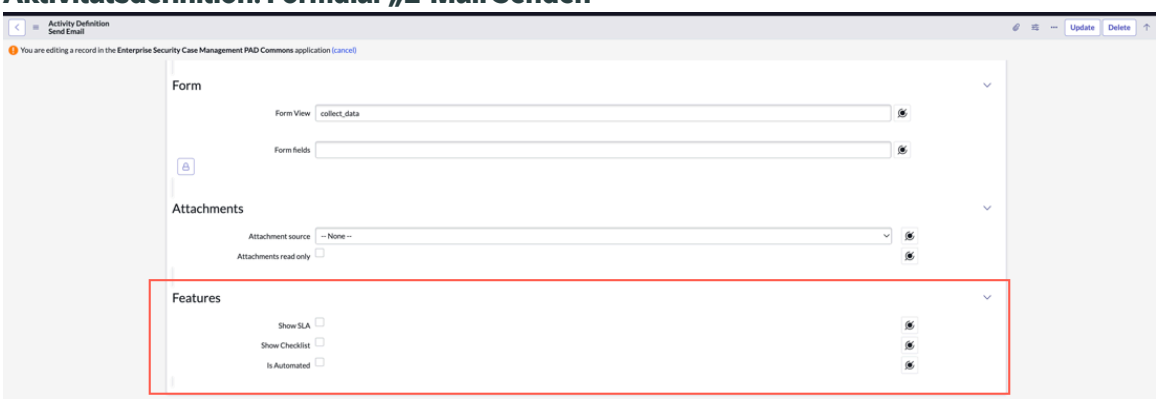
In diesem Beispiel

- SLA anzeigen – gelöscht
- Prüfliste Anzeigen – Gelöscht
- Ist Automatisiert – Gelöscht

SLA anzeigen: Wahr/falsch. Rendert einen SLA-Timer im Header der Karte für den zugehörigen Datensatz. Das SLA wird gemäß dem SLA-Konfigurationsdatensatz ausgewählt, der in der Playbook-Konfiguration angegeben ist.

1. Prüfliste anzeigen#– wahr oder falsch. Rendert alle Prüflisten, die an den zugehörigen Datensatz angehängt sind. Die Prüfliste kann bearbeitet werden, und Änderungen werden gespeichert, ohne dass eine deklarative Aktion erforderlich ist.
2. Ist automatisiert: Wahr oder falsch. Bei „wahr“ wird der **Tagline** #Und **Symbol** #Wird mit dem Text überschrieben **Automatisierte Aufgabe** Und ein automatisiertes Symbol.

Aktivitätsdefinition: Formular „E-Mail Senden“



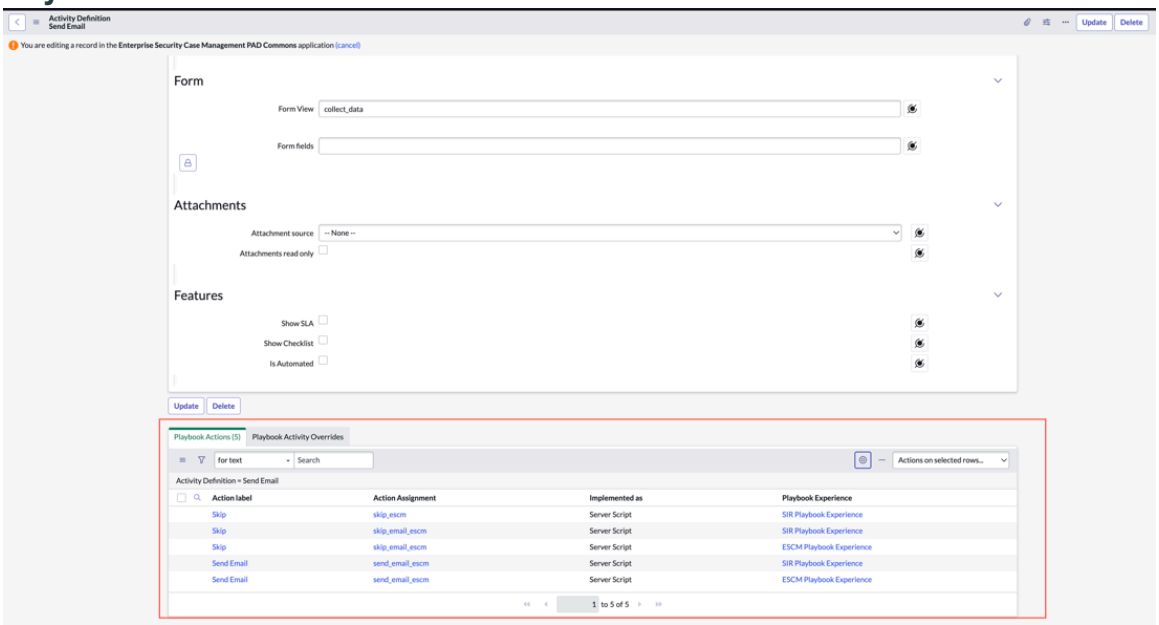
Playbook-Aktionen in Aktivitätsdefinition

Dieser Abschnitt enthält die Aktionen, die auf der Aktivitätskarte gerendert werden. Dieses Beispiel hat **Überspringen** , Und **E-Mail Senden** Als Aktionen.

Um der Aktivitätskarte eine neue Aktion hinzuzufügen, müssen Sie einen Datensatz in erstellen **Playbook-Aktionen** Zugehörige Liste unten auf der Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook-Aktionen



1. Klicken Sie auf **Neu**.
2. Wählen Sie eine vorhandene Aktivitätsaktion für das Feld „Aktionszuweisung“ aus.
3. Wählen Sie Aus **SIR-Playbook-Experience** Für Playbook-Experience-Feld.

Erstellen Sie eine Aktivitätsaktion

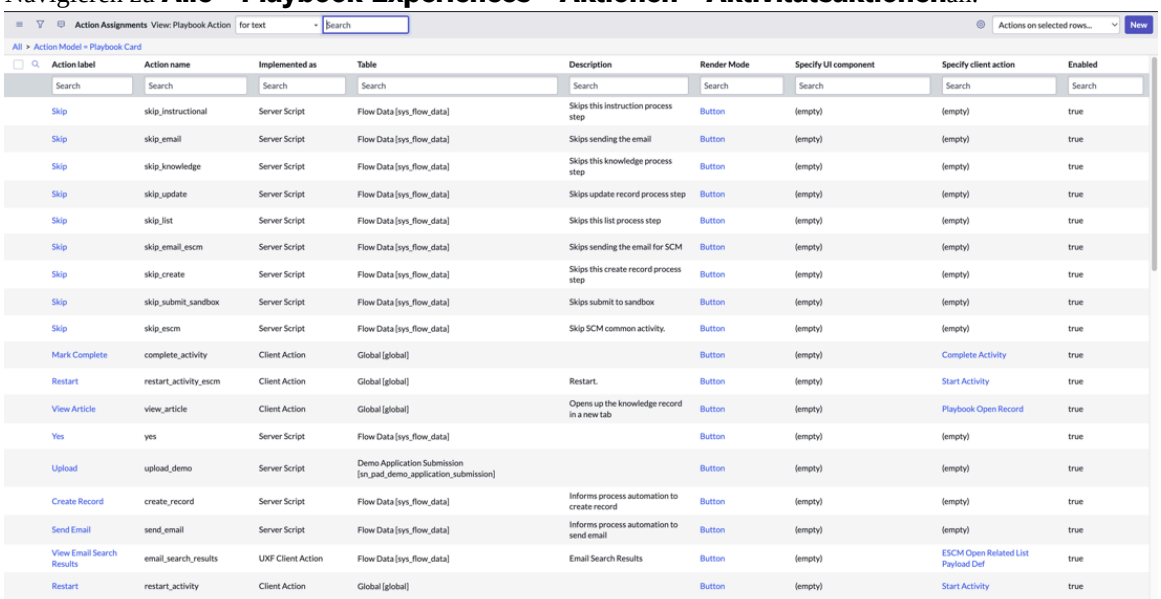
Im Folgenden finden Sie das Verfahren zum Erstellen einer Aktivitätsaktion.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Playbook-Experiences** > **Aktionen** > **Aktivitätsaktionen**an.



2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Siehe ServiceNow AI Platform Dokumentation, um zu erfahren, wie diese Aktionen erstellt werden. In diesem Beispiel ist „Überspringen“ als Serverskript implementiert.

3. **Playbook-Überschreibung:**

   Wenn Sie den vorhandenen Aktivitäts-Experience-Typ überschreiben möchten, ist dies möglich. Weitere Informationen finden Sie unter ServiceNow AI Platform Dokumentation. Keine Playbook-Überschreibungen für dieses Beispiel.

An CSF X Sandbox übermitteln

„An CSF senden X Sandbox“ ist ein Beispiel für einen Aktivitätsdefinitionsprozess.

Standard

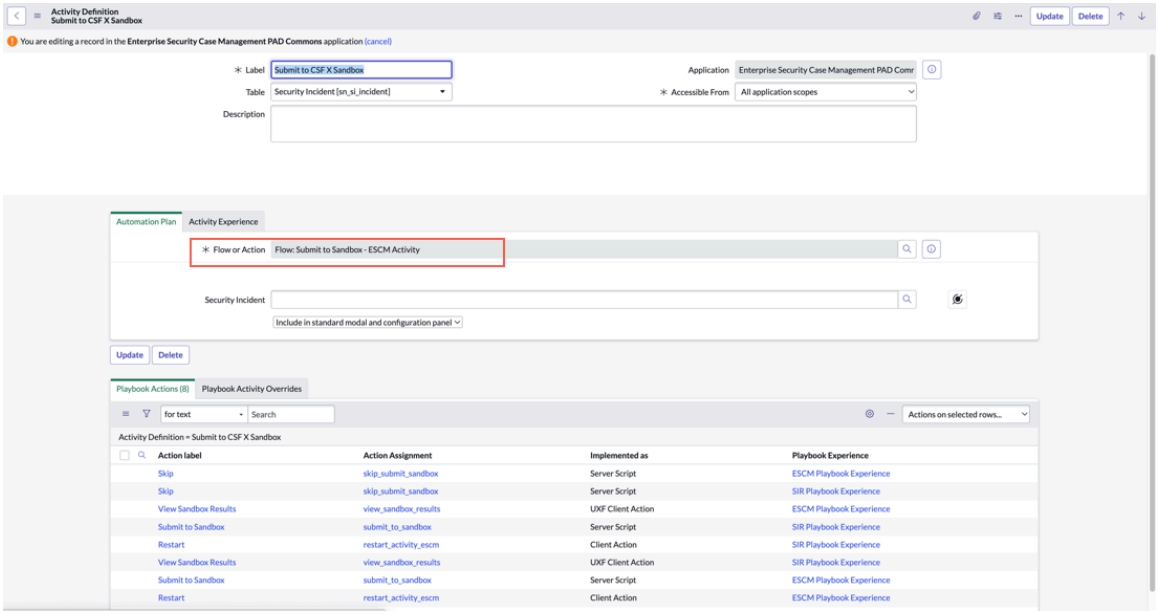
Die grundlegenden Details erfassen den Namen (Bezeichnung), die Anwendung, die Beschreibung, die Tabelle und, von welcher aus alle Anwendungen darauf zugegriffen werden kann.

Fügen Sie den Automatisierungsplan und die Aktivitätenerfahrung hinzu, und übermitteln Sie ihn. Bearbeiten Sie das Dokument nach der Übermittlung, um weitere Details für jede Registerkarte hinzuzufügen.

Automatisierungsplan

Der Automatisierungsplan ordnet die mit dem Flow Designer erstellte Back-End-Aktion/-Subflow zu. In diesem Beispiel wird verwendet **An Sandbox senden – ESCM-Aktivität** Subflow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieser Subflow ermöglicht das Senden der schädlichen erkennbaren Elemente an die Sandbox. Alle Eingabefelder und Ausgabefelder sind definiert.

Security Incident ist das Eingabefeld.

Aktivitäts-Experience

In diesem Beispiel **Datensatz** Typ ist ausgewählt.

Zugeordneter Datensatz

Der zugeordnete Datensatz dient zum Speichern der zugeordneten Daten, die sich auf die aktuelle Aktivität beziehen. Dadurch würden die Laufzeitdaten sowie der Status der Experience erfasst.

- Zugeordnete Tabelle: Flow-Daten
- Zugeordneter Datensatz: VL
- Experience-Statustabelle: Flow-Daten
- Experience-Statusdatensatz: VL

Details

- Tag-Zeile: E-Mail Senden
- Symbol: Umschlagumriss
- Titel: **Aktivität** > **Aktivitätsinstanz** > **Bezeichnung**an. Hier haben wir die Bezeichnung der Aktivitätsinstanz ausgewählt. Dieses Dot-Walking ersetzt den Bezeichnungswert zur Laufzeit dynamisch als Titel.
- Beschreibung: VL (Subflow-Ausgabe ist zugeordnet)
- Titel des Status „Ausstehend“: Leer
- Beschreibung des Status „Ausstehend“: Leer
- Datensatz-Felder
- Footer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular

- Formularansicht: Leer
- Formularfelder: Leer

Anhänge

Beispiel:

- Anhangsquelle: Keine
- Anhang schreibgeschützt: Deaktiviert

1. Anhangsquelle: Dies ist eine Dropdown-Liste. Welche Anhänge auf der Karte angezeigt werden sollen: Diejenigen, die an den übergeordneten Datensatz, den zugehörigen Datensatz oder keinen angehängt sind.
2. Anhang schreibgeschützt: Dies ist „wahr“/„falsch“. Verhindern Sie, dass der Anwender die vorhandenen Anhänge umbenennt oder löscht.

Features

In diesem Beispiel

- SLA anzeigen – deaktiviert
- Prüfliste Anzeigen – Deaktiviert
- Ist Automatisiert: Deaktiviert

Playbook-Aktionen in Aktivitätsdefinition

Dieser Abschnitt enthält die Aktionen, die auf der Aktivitätskarte gerendert werden.

Dieses Beispiel enthält die Aktionen „Überspringen“, „Sandbox-Ergebnisse anzeigen“, „an Sandbox senden“ und „Neu starten“.

Um der Aktivitätskarte eine neue Aktion hinzuzufügen, müssen Sie einen neuen Datensatz in der zugehörigen Liste Playbook-Aktionen erstellen, die unten auf der Seite vorhanden ist.

Playbook-Überschreibung

Keine Playbook-Überschreibungen für dieses Beispiel.

Beispiel-Playbooks für SIR Workspace

Sie können Playbooks für SIR Workspace schnell und einfach erstellen oder konfigurieren, ohne komplizierten Code zu schreiben. Sie können diese Playbooks verwenden, um Sicherheitsbedrohungen Schritt für Schritt zu lösen. Sie können den Security Incident-Playbook-Flow automatisch oder manuell aufrufen.

Die Security Incident Response stellt die folgenden Playbooks mit dem Basissystem bereit:

- Playbook für manuelles Phishing
- Playbook für automatisiertes Phishing
- Playbook für manuelle Malware

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Playbook für automatisierte Malware
- Playbook für fehlgeschlagene Anmeldung – Handbuch

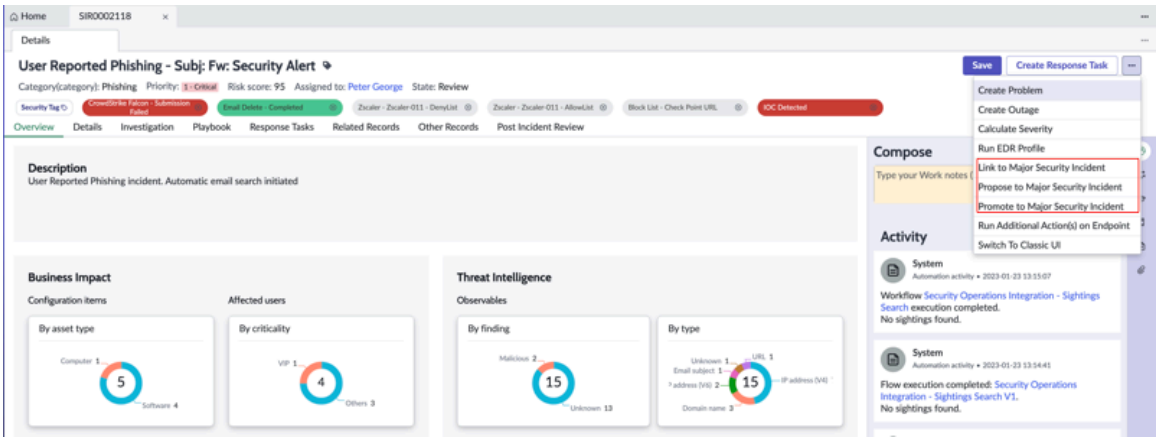
Mit MSI-Datensätzen arbeiten

Mit dem Arbeitsbereich „Security Incident Response“ können Sie Security Incidents als schwerwiegende Security Incidents vorschlagen, heraufstufen oder verknüpfen, wenn die Incidents als kritische Bedrohung für die Organisation identifiziert werden.

Nach der Installation Management schwerwiegender Sicherheits-Incidents(MSIM) auf Ihrem ServiceNow AI Platform Instanz können Sie dann den Übergang von Security Incidents zu schwerwiegenden Incidents verarbeiten.

Die Management schwerwiegender Sicherheits-Incidents(MSIM) UI-Aktionen werden oben rechts im Security Incident-Formularbanner des SIR-Arbeitsbereichs angezeigt. Wählen Sie die UI-Aktion nach Bedarf aus.

Hinweis:
Einige Aktionen sind kontextbezogen. Beispielsweise ist die Aktion „Verknüpfung aufheben“ nur verfügbar, wenn der Security Incident bereits vorgeschlagen, heraufgestuft oder mit einem schwerwiegenden Security Incident verknüpft ist.



Als schwerwiegenden Security Incident vorschlagen

Schlagen Sie einen Security Incident als schwerwiegenden Security Incident (MSI) vor.

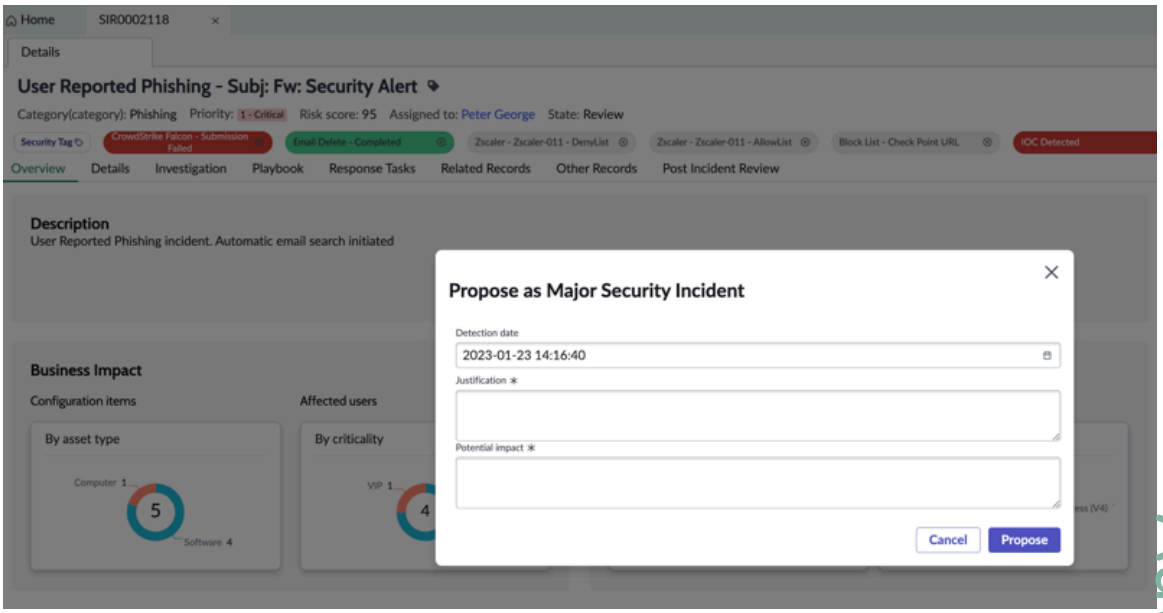
Vorbereitungen

Erforderliche Rolle: sn_si.Analyst.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen Security Incident.
3. Klicken Sie Auf **Schwerwiegenden Security Incident vorschlagen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie im Formular die Felder aus, z. B. Erkennungsdatum, Begründung und potenzielle Auswirkung.
5. Klicken Sie auf **Vorschlagen**.
   Der Incident-Datensatz wird als Kandidat für schwerwiegende Security Incidents vorgeschlagen. Nachdem der Incident-Datensatz als Kandidat für schwerwiegenden Security Incident vorgeschlagen wurde, **Kandidat Für Schwerwiegenden Security Incident** Tag wird angewendet und auf dem Banner des Security Incident-Formulars angezeigt.

> **Hinweis:**
> Klicken Sie Auf **Verknüpfung mit schwerwiegendem Security Incident aufheben** Um die Verknüpfung des Incident aufzuheben, wenn Sie keinen Vorschlag machen möchten oder keine kritischen Auswirkungen hat. Die Verknüpfung des Incident wird aufgehoben und in der Listenansicht dem Sicherheitsanalysten zur Korrektur angezeigt.

Zu schwerwiegendem Security Incident heraufstufen

Einen Security Incident zu einem schwerwiegenden Security Incident heraufstufen.

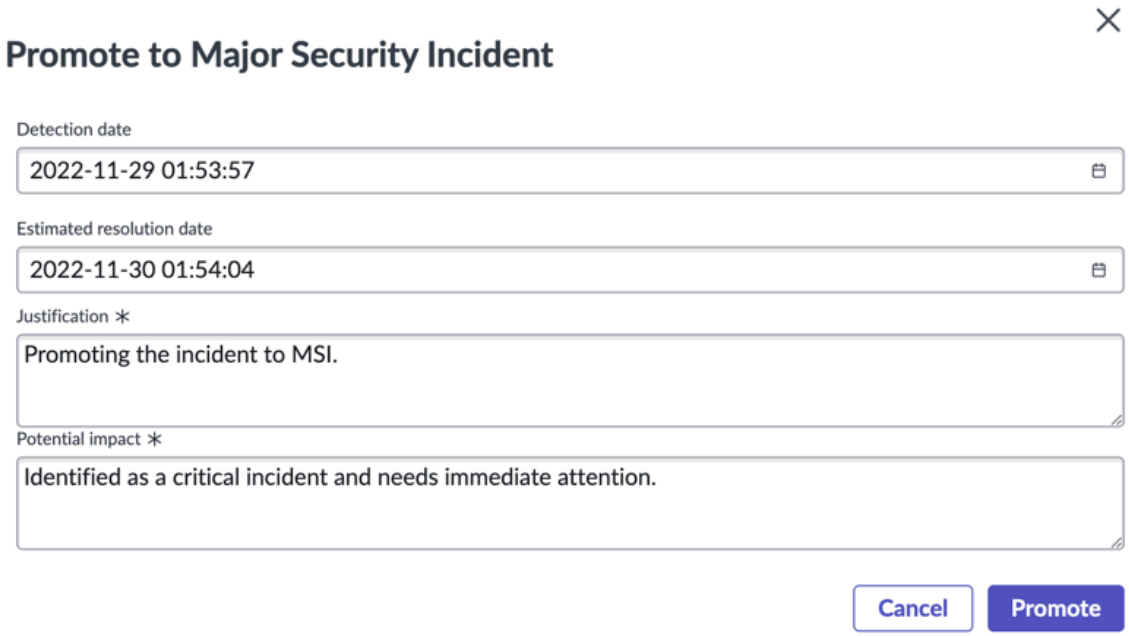
Vorbereitungen

Erforderliche Rolle: sn_si.Analyst.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen Security Incident.
3. Klicken Sie Auf **Zu schwerwiegendem Security Incident heraufstufen** .
4. Füllen Sie im Formular die Felder aus, z. B. Erkennungsdatum, Geschätztes Lösungsdatum, Begründung und potenzielle Auswirkung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie Auf **Heraufstufen** .
   Der Incident-Datensatz wird als schwerwiegender Security Incident heraufgestuft.
   Nachdem der Incident-Datensatz als schwerwiegender Security Incident heraufgestuft wurde, **Schwerwiegender Security Incident** Tag wird angewendet und auf dem Formularbanner angezeigt.

> **Hinweis:**
> Sie können die Verknüpfung des schwerwiegenden Security Incidents auch aufheben, wenn der Incident nicht kritisch ist. Der Incident wird dann aufgehoben und in der Listenansicht für die Korrektur durch Sicherheitsanalysten aufgeführt.

Mit schwerwiegendem Security Incident verknüpfen

Verknüpfen Sie einen Security Incident mit einem schwerwiegenden Security Incident als untergeordnete Security Incidents.

Vorbereitungen

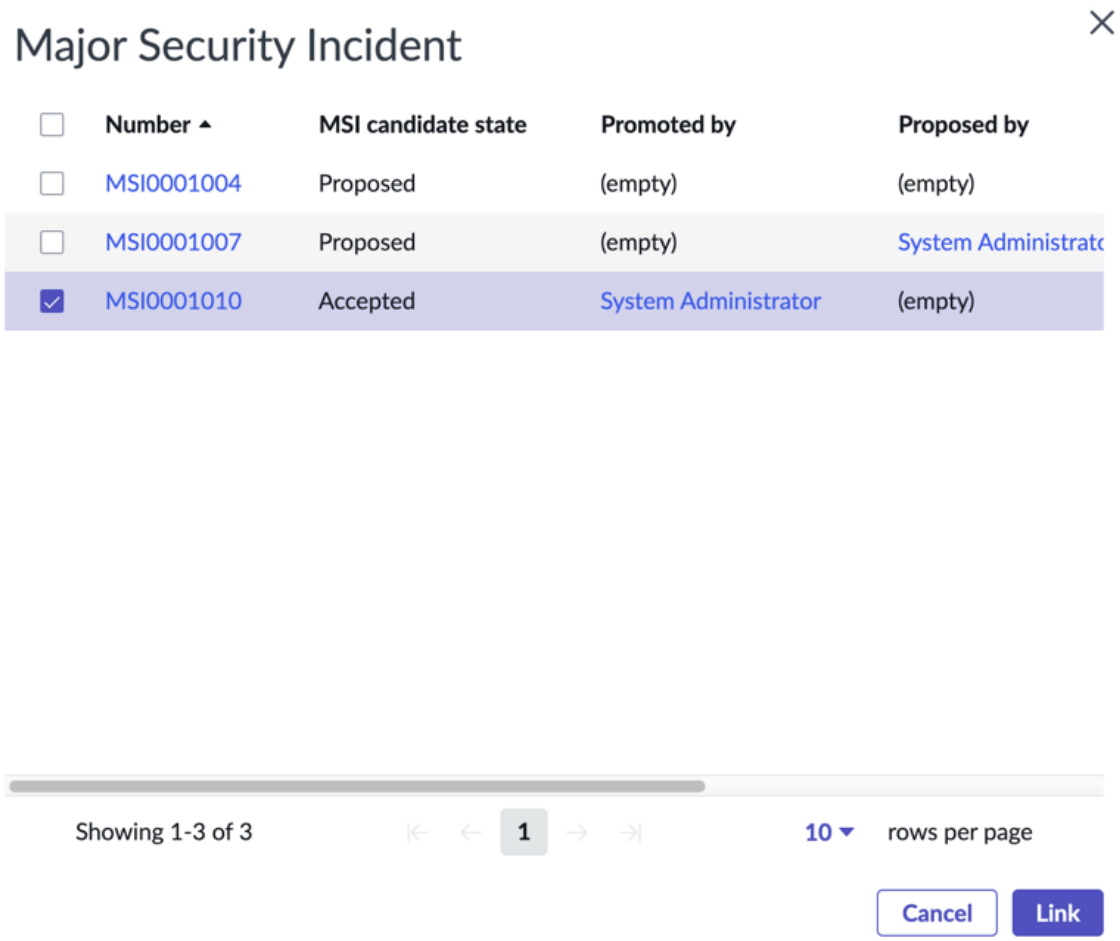
Erforderliche Rolle: sn_si.Analyst.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Öffnen Sie einen Security Incident.
3. Klicken Sie Auf **Link zu schwerwiegendem Security Incident** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

4. Wählen Sie die Incidents aus, die mit einem schwerwiegenden Security Incident verknüpft werden sollen.
5. Klicken Sie Auf **Link** .
6. Der Incident-Datensatz ist als untergeordneter Incident des schwerwiegenden Security Incident verknüpft. Nachdem der Incident als untergeordneter Incident mit einem schwerwiegenden Security Incident verknüpft wurde, **Schwerwiegender Security Incident** Tag wird angewendet und auf dem Formularbanner angezeigt.

Arbeiten mit Formular-UI-Aktionen

Im Folgenden finden Sie die UI-Aktionen, die im Security Incident-Formular angezeigt werden.

So navigieren Sie zu den Formular-UI-Aktionen:

1. Gehe zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Wählen Sie einen Security Incident in der Listenansicht aus.
3. Alle UI-Aktionen sind in der oberen rechten Ecke des Security Incident-Formulars vorhanden.

UI-Aktionen des Arbeitsbereichsformulars

Feldname	Beschreibung
Diskutieren	Erstellen oder starten Sie eine Sidebar-Diskussion für den Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

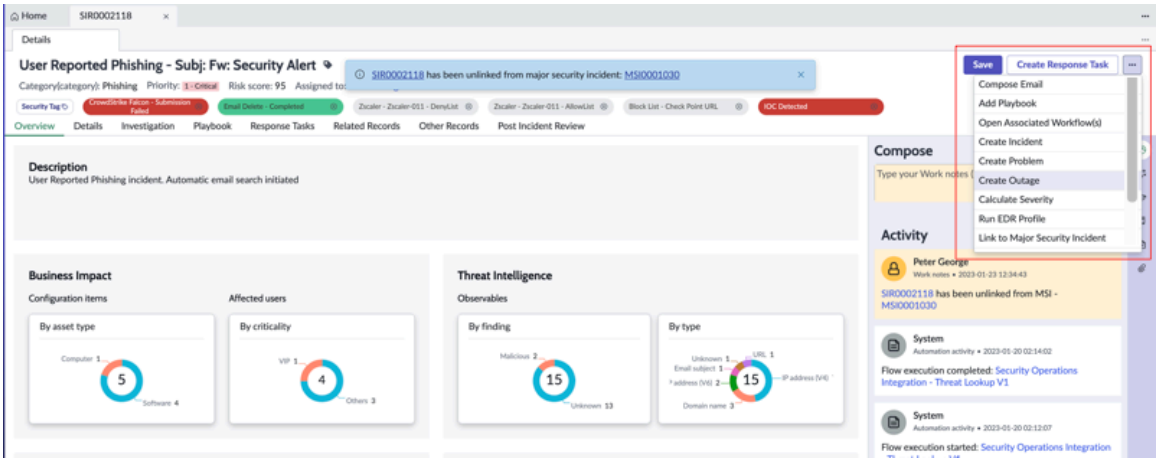
Feldname	Beschreibung
Speichern	Speichern oder aktualisieren Sie den Security Incident Response-Datensatz, nachdem Sie Änderungen vorgenommen haben.
Antwortaufgabe erstellen	Erstellen Sie eine Antwortaufgabe für den Security Incident.
Verfassen Sie E-Mails	Verfassen Sie E-Mails für den Security Incident.
Playbook hinzufügen	Fügen Sie das Playbook für den Security Incident manuell hinzu.
Incident erstellen	Erstellen Sie einen Incident innerhalb des Security Incident.
Kundenservicefall erstellen	Erstellen Sie einen Kundenservicefall für den Security Incident, der vom Kundenservice-Management-Team (CSM) nachverfolgt wird. **Hinweis:** Diese Option ist nur verfügbar, wenn Customer Service Management (CSM) installiert ist.
Zugeordnete Wokflows öffnen	Öffnen Sie alle Workflow-Kontexte, die dem Security Incident zugeordnet sind. Diese Option ist nur sichtbar, wenn Workflows vorhanden sind.
Change Request erstellen	Erstellen Sie eine Change-Anforderung innerhalb des Security Incident.
Problem erstellen	Erstellen Sie ein Problem innerhalb des Security Incident.
Ausfall erstellen	Erstellen Sie einen Ausfall innerhalb des Security Incident.
Schweregrad berechnen	Berechnen Sie den Schweregrad eines Security Incidents mithilfe vordefinierter Rechner. Der Schweregrad wird basierend auf den vordefinierten Regeln in den Rechnern berechnet. Der Schweregrad eines Incidents basiert auf der Risikopunktzahl, der Geschäftsauswirkung und der Priorität.
EDR-Profil ausführen	Wählen Sie das EDR-Profil für die erforderliche Integration aus, und führen Sie es aus. **Hinweis:** Diese Option ist nur verfügbar, wenn Integrationen installiert sind.
Mit schwerwiegendem Security Incident verknüpfen	Verknüpfen Sie einen Security Incident mit einem schwerwiegenden Security Incident.
Risikoereignis melden	Melden Sie diesen Security Incident als Risikoereignis an das Risikomanagementteam. Das Risikomanagementteam analysiert das Ereignis und stellt sicher, dass solche Ereignisse und die zugehörigen Verluste nicht erneut auftreten. **Hinweis:** Diese Option ist nur verfügbar, wenn Risikomanagement installiert ist.
Verknüpfung mit schwerwiegendem Security Incident aufheben	Verknüpfung mit schwerwiegendem Security Incident aufheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldname	Beschreibung
Als schwerwiegenden Security Incident vorschlagen	Schlagen Sie einen Security Incident als schwerwiegenden Security Incident vor.
Zu schwerwiegendem Security Incident heraufstufen	Einen Security Incident als schwerwiegenden Security Incident heraufstufen.
Zusätzliche Aktion(en) für Endpunkt ausführen	Führen Sie zusätzliche Aktionen für den Endpunkt aus. **Hinweis:** Diese Option ist nur verfügbar, wenn Endpunktintegrationen installiert sind. Beispiel: FireEye HX
Neues Ereignis in MISP erstellen	Erstellen und ändern Sie Ereignisse in MISP automatisch oder manuell. **Hinweis:** Diese Option ist nur verfügbar, wenn die MISP-Integration installiert ist.
MITRE ATT&K-Technik zuordnen	Ordnen Sie dem Security Incident MITRE ATT&K-Techniken zu. **Hinweis:** Diese Option ist verfügbar, wenn MITRE ATT&K installiert ist.
MITRE ATT&K-Informationen anzeigen	Zeigt die MITRE ATT&K-Informationen an, die dem Security Incident zugeordnet sind. **Hinweis:** Diese Option ist verfügbar, wenn MITRE ATT&K installiert ist.
Dem Sicherheitsfall hinzufügen	Fügen Sie den Security Incident einem vorhandenen oder neuen Sicherheitsfall hinzu. **Hinweis:** Diese Option ist verfügbar, wenn Threat Intel installiert ist.
Zu klassischer UI wechseln	Ermöglichen Sie dem Analysten, zwischen klassischer und neuer Anwenderoberfläche zu wechseln, damit der Analysten auch an den vorhandenen Funktionalitäten arbeiten kann, die im neuen Arbeitsbereich noch nicht verfügbar sind.
Abbrechen	Brechen Sie einen Security Incident ab. Nachdem Sie ausgewählt haben **Abbrechen** Alle zugehörigen Datensätze wie Antwortaufgaben und untergeordnete Security Incidents werden ebenfalls abgebrochen.
Löschen	Löschen Sie einen Security Incident-Datensatz.

4. Klicken Sie auf eine Security Incident-Nummer, um den Security Incident-Datensatz anzuzeigen. Die UI-Aktionen werden oben auf der Seite angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Workflow zum Abschluss von Security Incidents

Schließen Sie den Security Incident, indem Sie den Incident-Status aktualisieren.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

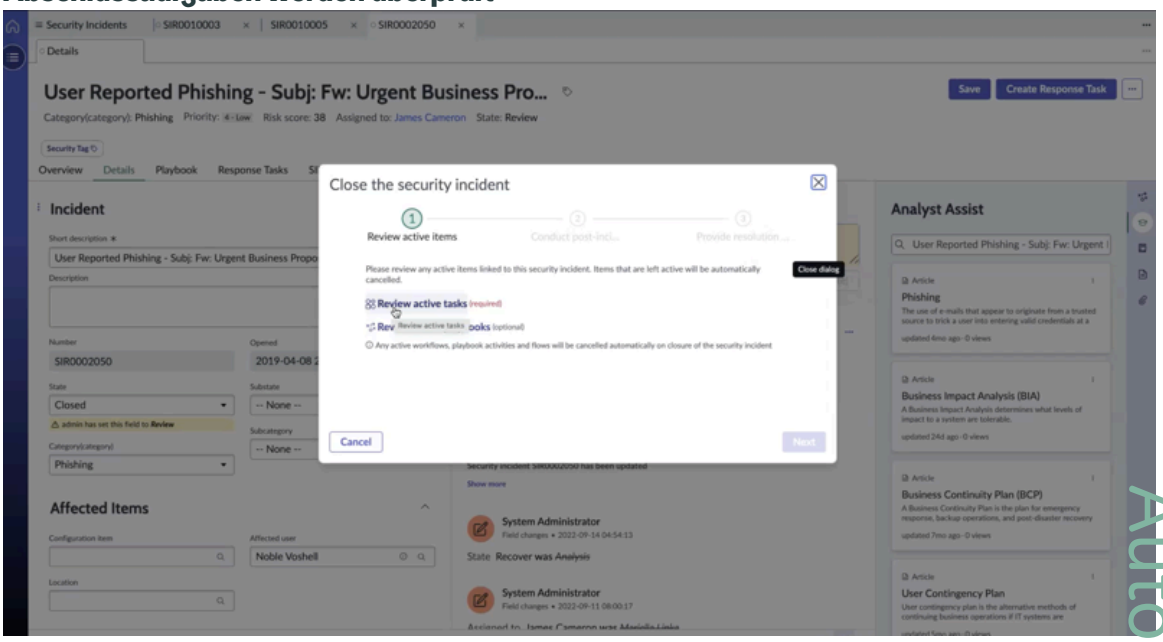
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Wechseln Sie zum Beispiel zu **Listen** > **Security Incidents** > **Offene Incidents**an.
3. Öffnen Sie einen Incident, den Sie schließen möchten.
4. Wechseln Sie zu **Details** Registerkarte.
5. Führen Sie einen Drilldown zum Incident-Status durch, und wählen Sie aus **Schließen** .
6. Führen Sie die Abschlussaktivitäten aus.

    - Dies ist ein obligatorischer Schritt zum Überprüfen einer Aufgabe, bevor ein Security Incident geschlossen wird. Alle Antwortaufgaben müssen vom Analysten überprüft und geschlossen oder abgebrochen werden, bevor sie als Security Incident geschlossen werden. Wenn der Analyst auf klickt **Überprüfen Sie aktive Aufgaben** , Führt der Anwender zu **Antwortaufgaben** Registerkarte. Eine Sitzungsnachricht wird angezeigt, die Sie auffordert, einen Security Incident zu schließen. Klicken Sie Auf **Fahren Sie fort** .
    - Klicken Sie auf **Fortsetzen**. Der erste Schritt – Überprüfen aktiver Aufgaben beim Schließen des Security Incident ist abgeschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

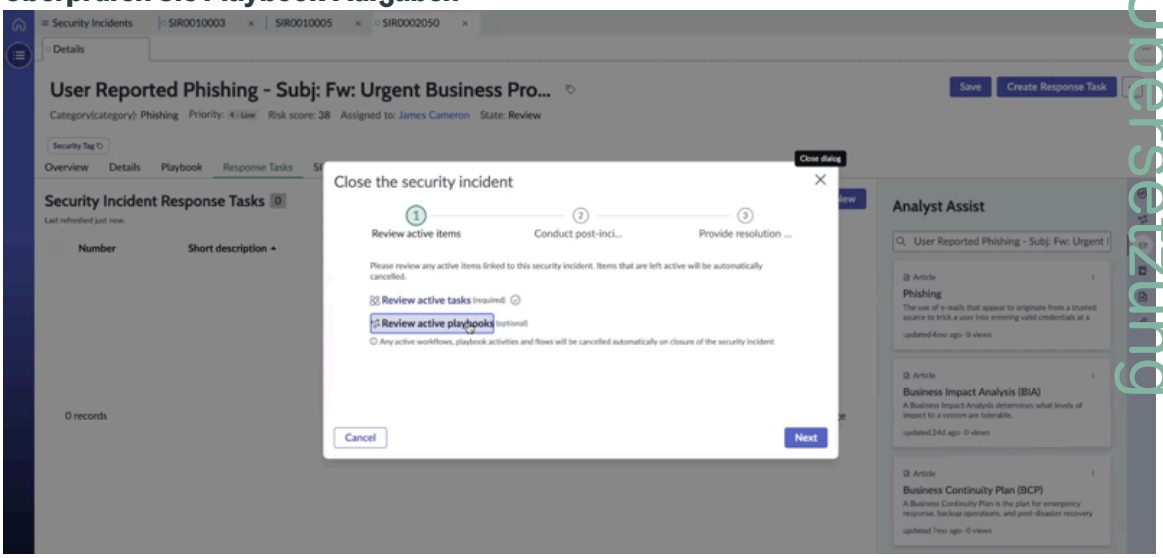
Abschlussaufgaben werden überprüft



- Wechseln Sie zum nächsten Schritt, um die aktiven Playbooks für den Analysten zu überprüfen. Dies ist ein optionaler Schritt. Sie können auf den Link klicken, um die aktive Playbook-Aufgabe zu überprüfen und nach Bedarf zu schließen.

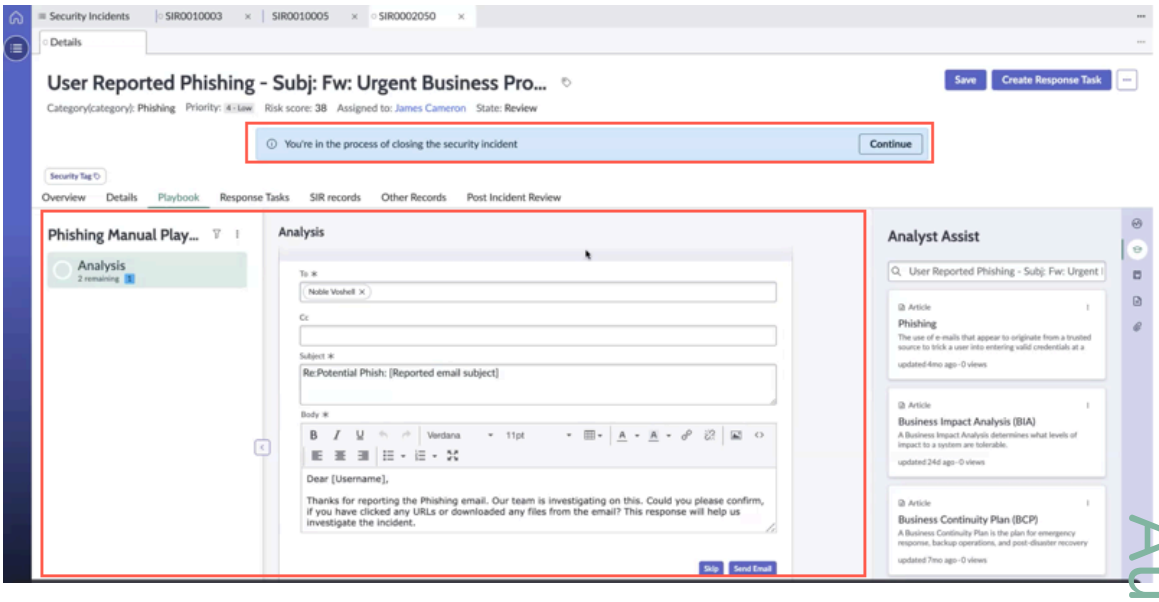
Hinweis:
Alle aktiven Workflows, Playbook-Aktivitäten und Flows werden beim Schließen des Security Incident automatisch abgebrochen.

Überprüfen Sie Playbook-Aufgaben



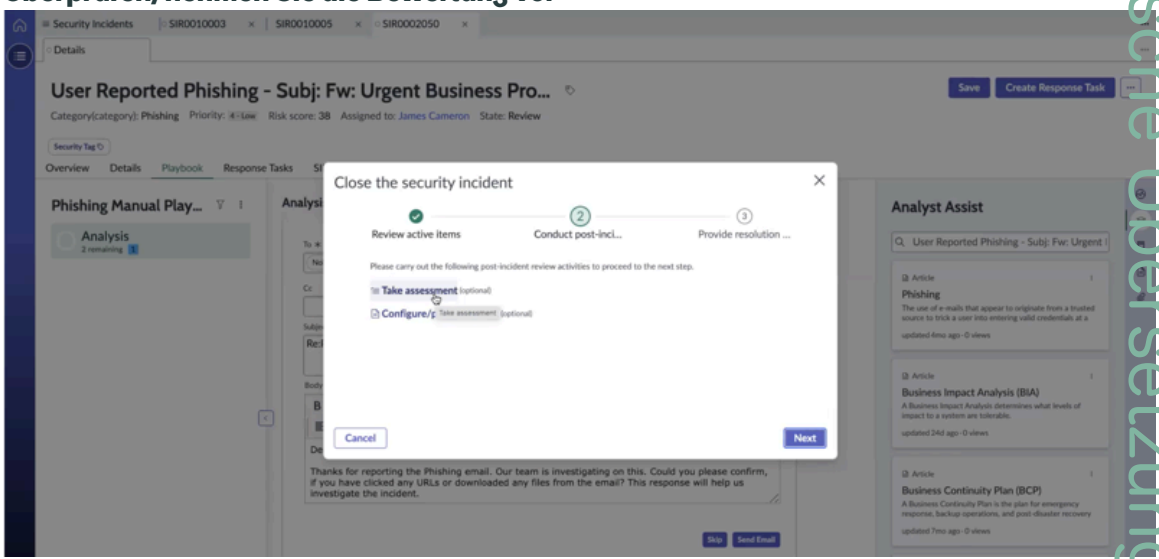
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



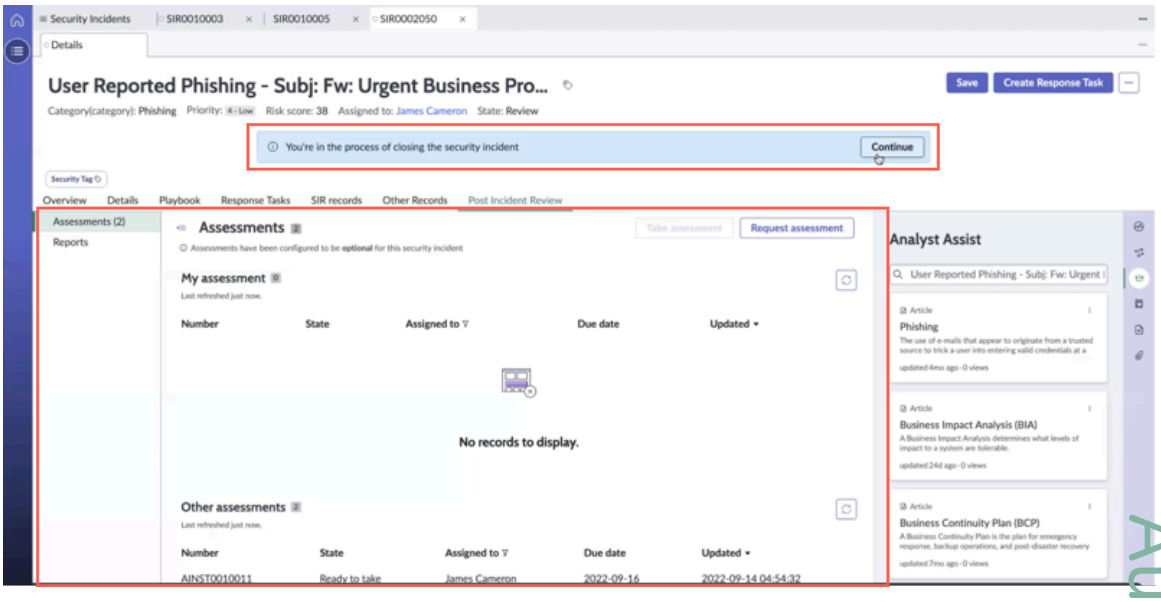
- Bericht zur Überprüfung nach Incident: Sie werden jetzt zur Überprüfung der Aktivitäten nach Incident verschoben, um mit dem Abschluss fortzufahren. Wenn die Bewertung optional ist, überspringen Sie den Schritt, oder wenn die Bewertung obligatorisch ist, führen Sie die Bewertung durch, und schließen Sie sie ab.

Überprüfen/nehmen Sie die Bewertung vor

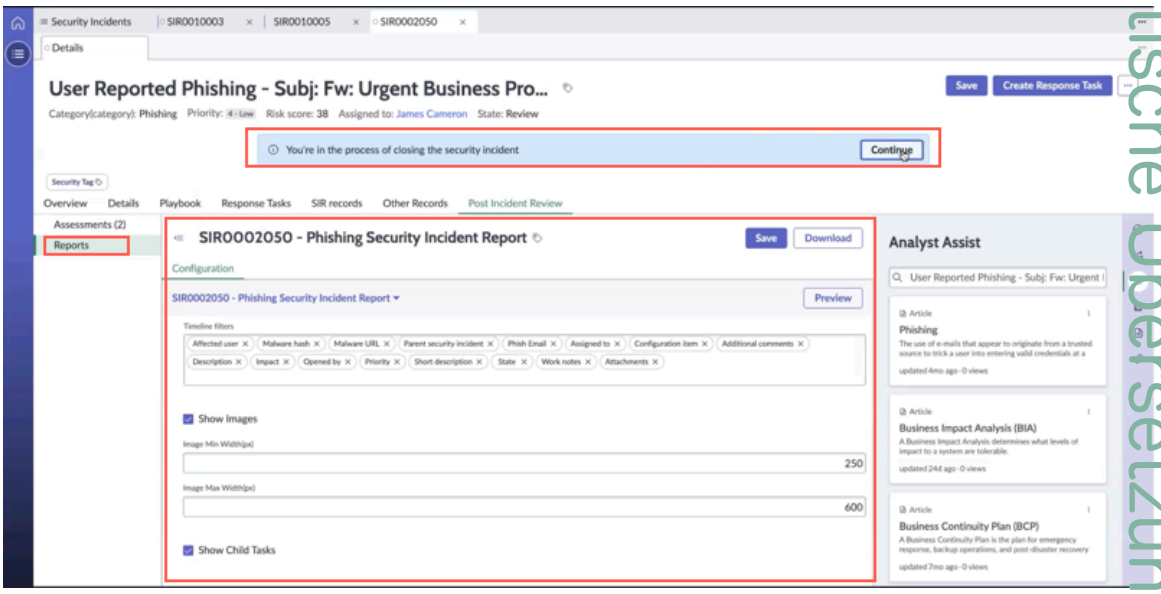


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Bericht konfigurieren/in der Vorschau anzeigen: Dies ist erneut ein optionaler Schritt. Klicken Sie auf den Link, um den Bericht zu überprüfen und mit fortzufahren **Als Nächstes** Schritt.

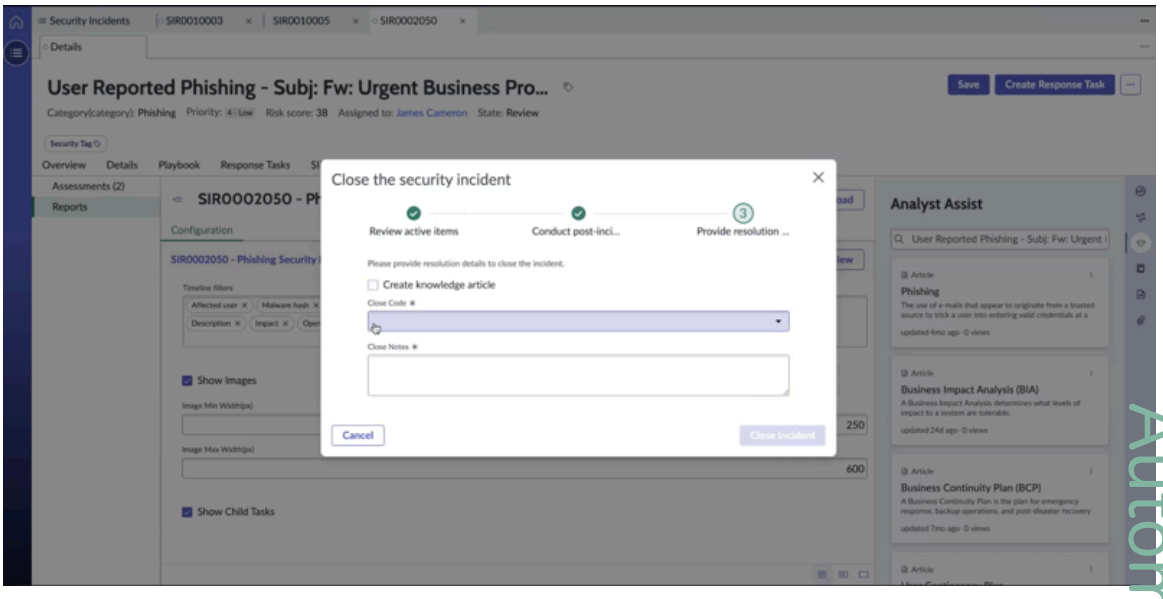


- Lösungsdetails angeben: Der Analysten kann das Kontrollkästchen aktivieren, um Wissensartikel automatisch zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geben Sie den Abschlusscode und die Abschlussnotizen an, und klicken Sie auf **Schließen Sie den Incident** .



Hinweis:
Zufällig, wenn der Analyst abbricht **Schließen Sie den Security Incident** Dialogfeld, dann kann der Analyst zu navigieren **Details** Registerkarte und ändern Sie den Incident-Status in **Schließen** Um mit dem Abschluss fortzufahren.

SIR Workspace-Dashboards anzeigen

In diesem Abschnitt werden die wichtigen Metriken zur Analyse von vorgestellt Security Incident Response Prozesse, z. B. neue Security Incidents oder das durchschnittliche Alter offener Security Incidents.

In der klassischen UI sind einige Standard-Dashboards unter Homepage und verfügbar Performance Analytics Dashboards, die verfügbar sind, wenn Performance Analytics Für Security Incident Response Plugin ist installiert. Alle sind jetzt im neuen Arbeitsbereich unter verfügbar **SIR-Dashboards** Abschnitt.

Standard-Dashboards unter der Homepage :

- Security Incident Response – Übersicht
  - Analystenübersicht
  - Managerübersicht (in zukünftigen Releases unterstützt)
  - CISO-Übersicht (in zukünftigen Releases unterstützt)
- **Platform Analytics für** *`Security Incident Response`*
  - Security Incident-Explorer
  - CISO-Dashboard (zukünftiges Release)
  - Security Incident-Management
  - KPIs von Security Incident-Management Premium
  - Effizienz von Security Operations
  - Kontextbezogene Analytics – SI-Dashboard

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Dashboards werden möglicherweise in Standard- und Plattform-Analytics für Security Incident Response-Dashboards wie CISO-Dashboard wiederholt. Wenn das Plugin installiert ist, werden in diesen Dashboards zusätzliche Inhalte angezeigt und sind nicht als Duplikat verfügbar.

Anwender müssen das Plugin für die Dashboards installieren, die unter Platform Analytics für Security Incident Response-Dashboards aufgeführt sind, um im Arbeitsbereich vorhanden zu sein. Andernfalls sind nur die Standard-Dashboards verfügbar.

In der aktuellen Version von SIR-Arbeitsbereich, Die folgenden Dashboards sind unter verfügbar **SIR-Dashboards** Abschnitt. Die anderen fehlenden Dashboards sind in späteren Releases verfügbar.

Security Incident Response-Dashboards

Dashboard	Beschreibung
Standard-Dashboard	
Sicherheitsanalyst – Übersicht	Mit diesem Dashboard können Sicherheitsanalysten Security Incidents basierend auf der Arbeit des Analysten mit kritischer Priorität, der Arbeit mit hoher Priorität, den Security Incidents, die dem Analysten zugewiesen sind, den den Analysten zugewiesenen Aufgaben und der Incident-Anzahl zusammenfassen.
Performance Analytics (PA) für Security Incident Response-Dashboards	
Security Incident-Explorer	Mit diesem Dashboard können Sicherheitsmanager und Analysten Security Incidents zusammengefasst und gruppiert nach Kategorie, Unterkategorie, Standort, Priorität und Geschäftsauswirkung anzeigen. Mit diesen Ansichten erhalten Manager und Analysten schnell Einblicke in die Häufigkeit, mit der Angriffe auftreten und welche Business-Services betroffen sind.
Security Incident-Management	Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents problemlos nachverfolgen, von der ersten Analyse/Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung.
CISO-Dashboard	Unterstützung für zukünftiges Release vorgeschlagen.
Effizienz von Security Operations	Mit diesem Dashboard können Manager und Analysten allgemeine Effizienzmetriken anzeigen und die Leistung des SOC messen.
KPIs von Security Incident-Management Premium	Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents nachverfolgen und anzeigen, von der ersten Analyse/Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung.
Kontextbezogene Analytics – S	Mit diesem Dashboard können Manager und Analysten die offenen Security Incidents, das durchschnittliche Alter offener Security Incidents,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response-Dashboards (Fortsetzung)

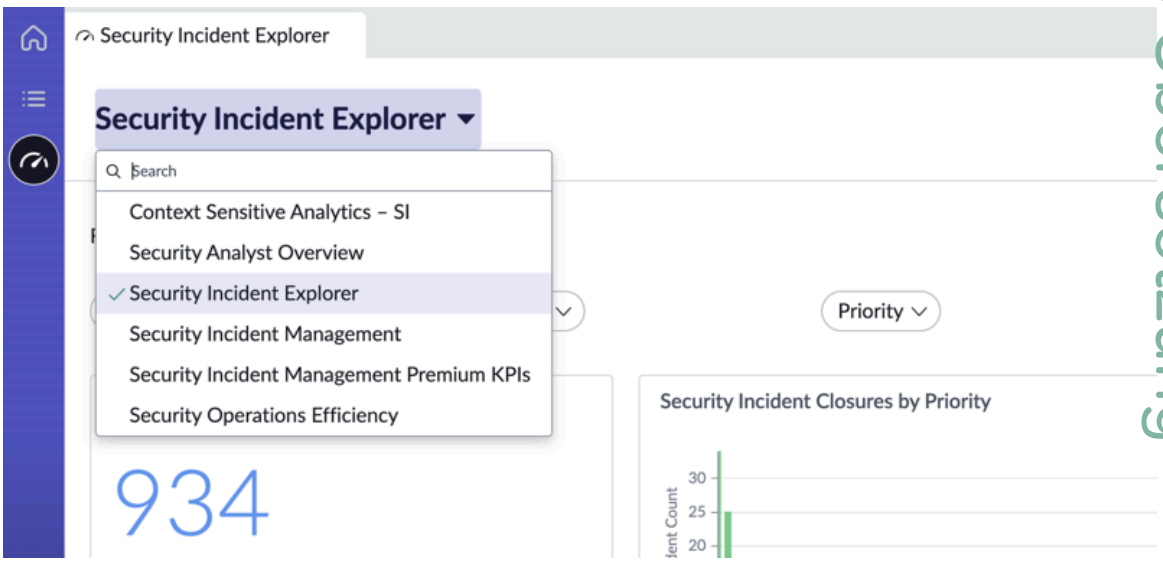
Dashboard	Beschreibung
	die durchschnittliche Abschlusszeit von Security Incidents, den Prozentsatz der Security Incidents, die am selben Tag geöffnet und geschlossen wurden, und den Prozentsatz der Incidents anzeigen, die in den letzten 5 Tagen und 30 Tagen nicht aktualisiert wurden.

Greifen Sie auf SIR- und PA-Dashboards zu

Die **SIR-Dashboards** Symbol, das auf der linken Seite der Homepage des Arbeitsbereichs angezeigt wird.

Hinweis:
Anwender mit Zugriff „sn_si.Manager“ oder „sn_si.admin“ können die Dashboards bearbeiten. Die Anwender müssen sich im selben Umfang wie die Dashboards befinden, die der Anwender bearbeiten möchte. Beispielsweise ist das Übersichts-Dashboard für Sicherheitsanalysten im SIR-Arbeitsbereich verfügbar. Dann sollte sich der Anwender auch im selben SIR-Arbeitsbereich befinden, um die Änderungen am Dashboard vorzunehmen.

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Management-Arbeitsbereich**an.
2. Klicken Sie auf **SIR-Dashboards** Symbol.
3. Wählen Sie das gewünschte Dashboard aus der Dropdown-Liste aus.



Sie können die Dashboards bearbeiten, den Dashboards neue Elemente hinzufügen und eigene Dashboards erstellen. Weitere Informationen zur Verwendung von Dashboards finden Sie unter Arbeiten mit reaktionsfähigen Dashboards

Zeigen Sie das Dashboard „Sicherheitsanalystenübersicht“ an

Mit diesem Dashboard können Sicherheitsanalysten Security Incidents basierend auf der Arbeit von Analysten mit kritischer Priorität, der Arbeit mit hoher Priorität, den Security Incidents, die dem Analysten zugewiesen sind, den den Analysten zugewiesenen Aufgaben und der Incident-Anzahl zusammenfassen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

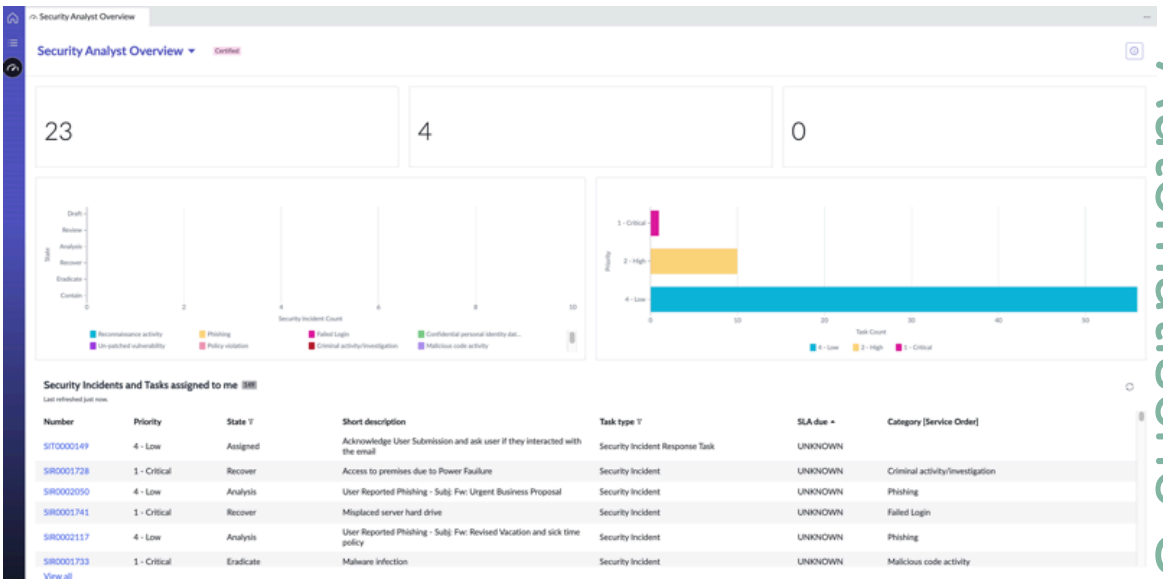
Vorbereitungen

Standardmäßig wird das Dashboard „Sicherheitsanalystenübersicht“ für Anwender mit Zugriff „sn_si.Analyst“ angezeigt.

Erforderliche Rolle: sn_si.Analyst (Lesen), sn_si.Manager oder sn_si.admin (Schreiben)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**an.
2. Klicken Sie Auf **SIR-Dashboards** Symbol, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie Aus **Sicherheitsanalyst – Übersicht** Aus der Dropdown-Liste.



Zeigen Sie das Dashboard „Sicherheitsanalystenübersicht“ an, um weitere Aktionen zu erhalten. Detaillierte Informationen zum Dashboard „Sicherheitsanalystenübersicht“ finden Sie unter Security Incident Response Platform Analytics-Lösungen.

Zeigen Sie das Dashboard „Security Incident Explorer“ an

Mit diesem Dashboard können Sicherheitsmanager Security Incidents zusammengefasst und nach Kategorie, Unterkategorie, Standort, Priorität und Geschäftsauswirkungen gruppiert anzeigen.

Vorbereitungen

Standardmäßig wird das Dashboard „Security Incident Explorer“ für die Anwender mit sn_si.Manager-Zugriff angezeigt.

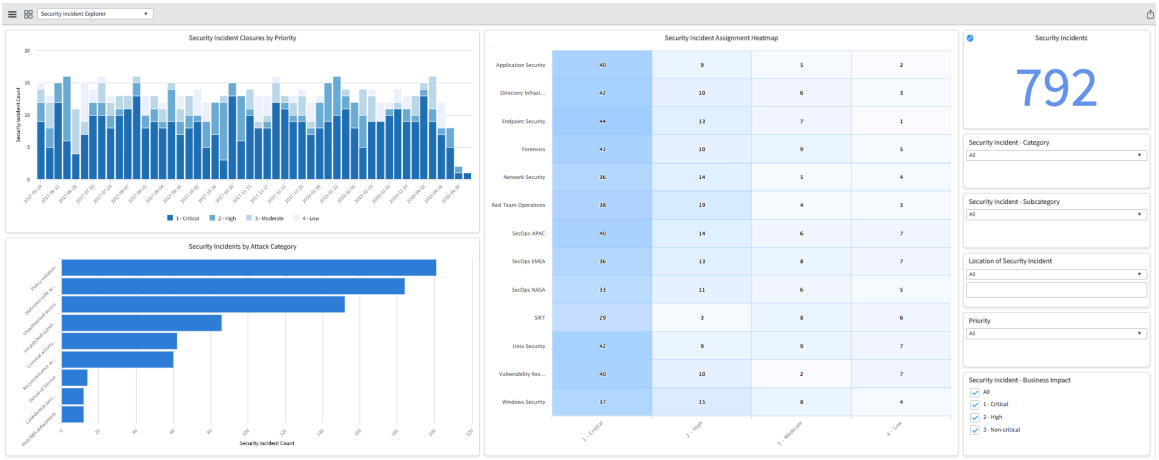
Erforderliche Rolle: sn_si.Analyst (Lesen), sn_si.Manager oder sn_si.admin (Schreiben)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**an.
2. Klicken Sie Auf **SIR-Dashboards** Symbol, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie Aus **Security Incident-Explorer** Aus der Dropdown-Liste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zeigen Sie das Dashboard „Security Incident Explorer“ an, um weitere Aktionen zu erhalten. Detaillierte Informationen zum Dashboard „Security Incident Explorer“ finden Sie unter Dashboard „Security Incident Explorer“

Im aktuellen Release wird die folgende Liste von Berichten im Dashboard „Security Incident Explorer“ nicht unterstützt:

- Heatmap für Security Incident-Zuweisung: Heatmap-Visualisierung ist nicht verfügbar.
- Security Incident-Zuordnung: Kartenvisualisierung ist nicht verfügbar.

Zeigen Sie das Dashboard „Security Incident Management“ an

Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents problemlos nachverfolgen, von der ersten Analyse/Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung.

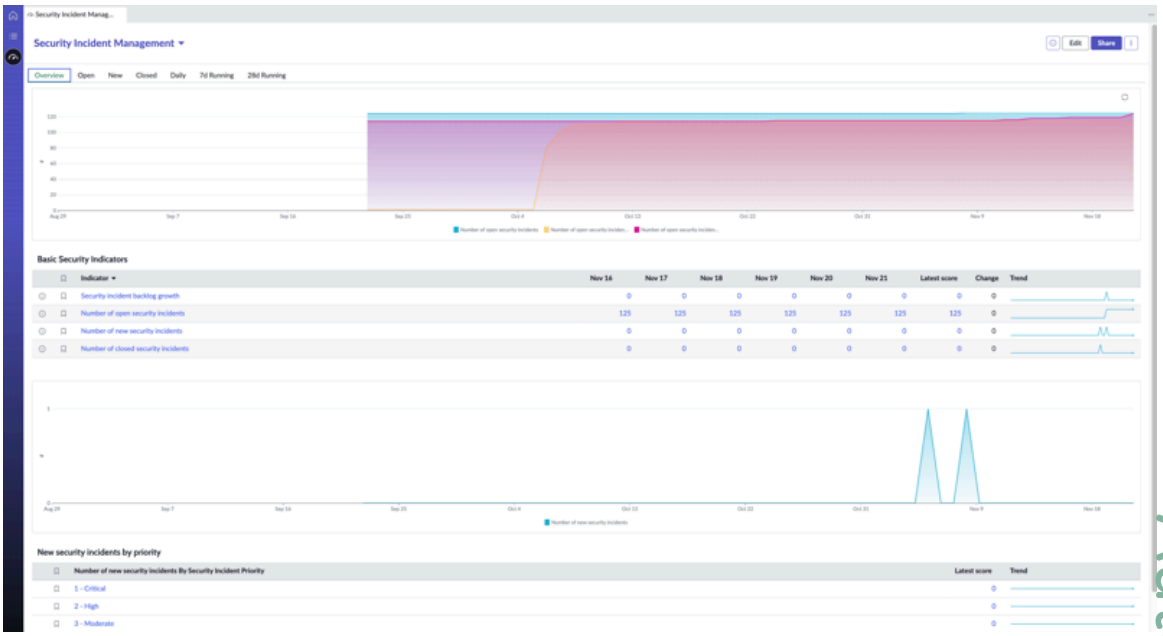
Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**an.
2. Klicken Sie Auf **SIR-Dashboards** Symbol, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie Aus **Security Incident-Management** Aus der Dropdown-Liste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zeigen Sie das Dashboard „Security Incident Management“ an, um weitere Aktionen zu erhalten. Detaillierte Informationen zum Dashboard „Security Incident Management“ finden Sie unter Dashboard „Security Incident Management“

Zeigen Sie das Dashboard „Security Operations-Effizienz“ an

Manager des Security Operations Center (SOC) können allgemeine Effizienzmetriken anzeigen und die individuelle Leistung der SOC-Teammitglieder in der Organisation messen.

Vorbereitungen

Im aktuellen Release wird der folgende Bericht im Dashboard „Security Operations-Effizienz“ nicht unterstützt:

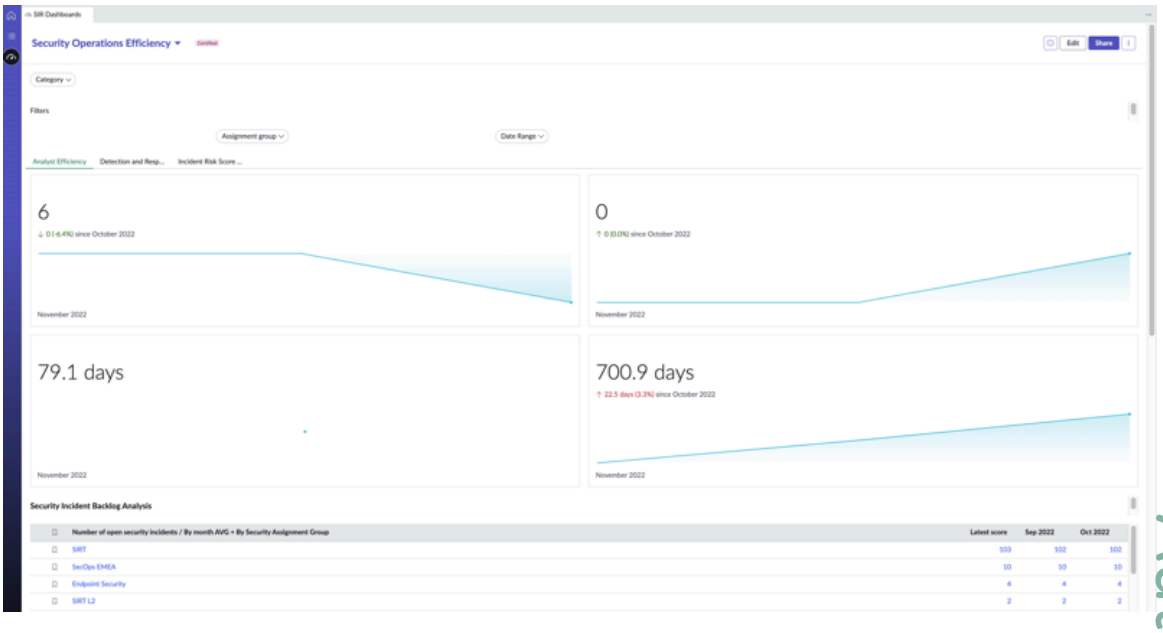
- Analyse der Security Incident-Phase – Workbench ist nicht verfügbar

Erforderliche Rolle: sn_si.Analyst (Lesen), sn_si.Manager oder sn_si.admin (schreiben)

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Security Incident Response**an.
2. Klicken Sie Auf **SIR-Dashboards** Symbol, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie Aus **Effizienz Von Security Operations** Aus der Dropdown-Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zeigen Sie das Dashboard „Effizienz von Security Operations“ an, um weitere Aktionen zu erhalten. Detaillierte Informationen zum Dashboard „Effizienz von Security Operations“ finden Sie unter Dashboard „Effizienz von Security Operations“

Zeigen Sie das Dashboard „Security Incident Response Premium-KPIs“ an

Mit diesem Dashboard können Sicherheitsmanager das Volumen, die Leistung und den Fortschritt von Security Incidents nachverfolgen und anzeigen, von der ersten Analyse/Erkennung bis zur Eindämmung, Beseitigung und Wiederherstellung.

Vorbereitungen

Im aktuellen Release wird die folgende Liste von Berichten im Dashboard „Security Incident Response Premium-KPIs“ nicht unterstützt:

- Nach Status verarbeiten: Workbench ist nicht verfügbar
- Prozess nach Alter: Workbench ist nicht verfügbar
- Security Incidents, die seit mehr als 30 Tagen offen sind, nach Zuweisungsgruppe und Status – Heatmap-Visualisierung ist nicht verfügbar.
- Security Incidents, die seit mehr als 30 Tagen nach Zuweisungsgruppe und Status nicht aktualisiert wurden – Heatmap-Visualisierung ist nicht verfügbar.
- Security Incidents mit Beauftragtem, der nicht aktiv ist – Heatmap-Visualisierung ist nicht verfügbar.

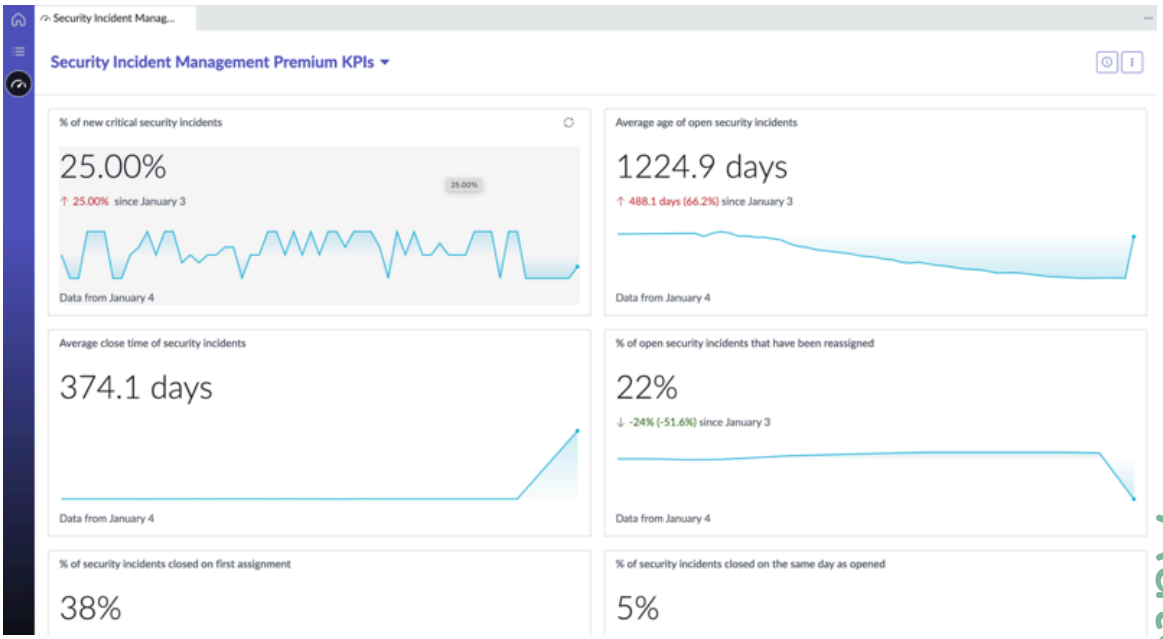
Erforderliche Rolle: sn_si.Analyst (Lesen), sn_si.Manager oder sn_si.admin (schreiben)

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**an.
2. Klicken Sie Auf **SIR-Dashboards** Symbol, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie Aus **Premium-KPIs für Security Incident Response** Aus der Dropdown-Liste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Zeigen Sie das Dashboard „Security Incident Response Premium-KPIs“ an, um weitere Aktionen zu erhalten. Detaillierte Informationen zum Dashboard „Security Incident Response Premium-KPIs“ finden Sie unter Security Incident Management Premium-Dashboard

Kontextbezogene Analytics anzeigen – SI-Dashboard

Mit diesem Dashboard können Manager und Analysten die offenen Security Incidents, das durchschnittliche Alter offener Security Incidents, die durchschnittliche Abschlusszeit von Security Incidents, den Prozentsatz der Security Incidents, die am selben Tag geöffnet und geschlossen wurden, und den Prozentsatz der Incidents anzeigen, die in den letzten 5 Tagen und 30 Tagen nicht aktualisiert wurden.

Vorbereitungen

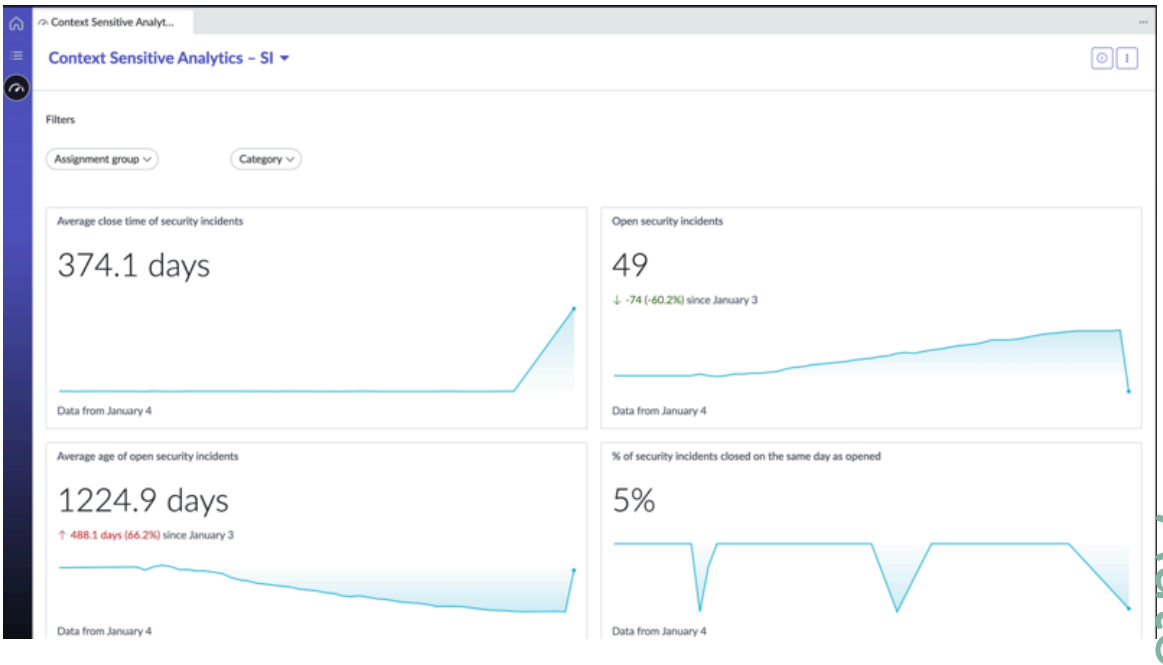
Erforderliche Rolle: sn_si.Analyst (Lesen), sn_si.Manager oder sn_si.admin (schreiben)

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**an.
2. Klicken Sie Auf **SIR-Dashboards** Symbol, das auf der linken Seite der Arbeitsbereichs-Homepage angezeigt wird.
3. Wählen Sie Aus **Kontextbezogene Analytics: SI** Aus der Dropdown-Liste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Zeigen Sie das Dashboard „kontextbezogene Analytics – SI“ für weitere Aktionen an.

Zeigen Sie das CISO-Dashboard an

Dieses Dashboard bietet Chief Information Security Officers (CISOs) in Form von grafischen Diagrammen einen allgemeinen Überblick über Security Incidents und wöchentliche Incident-Trends in der Instanz. Diese Diagramme helfen Ihnen, die Leistung des Security Operations Center (SOC) effektiv anzuzeigen und zu analysieren.

Vorbereitungen

- Erforderliche Rolle: sn_si.admin und sn_si.ciso – Incidents bearbeiten und anzeigen.
- Stellen Sie sicher, dass die App Performance Analytics für Security Incident Response installiert ist.

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Das CISO-Dashboard und das CISO-Übersichts-Dashboard waren in der klassischen Anwenderoberfläche zwei verschiedene. Aber jetzt wurden die Fähigkeiten der beiden Dashboards unter dem CISO-Dashboard zusammengeführt.

Das CISO-Dashboard bietet wöchentlich wichtige Einblicke zu Ihren Security Incidents. Sie können Indikatoren einrichten und Daten-Snapshots der Incidents erfassen, die den Bedingungen in den Indikatoreigenschaften entsprechen. Die gesammelten Daten werden dann mithilfe von Widgets im Dashboard visualisiert.

Sie können die wöchentlichen Trends mithilfe der Widgets im CISO-Dashboard visualisieren. Die Daten oder Statistiken für die Trends Ihrer Security Incidents werden aus den wöchentlichen Incident-Indikatoreigenschaften erfasst, die von der Organisation definiert werden. Mithilfe der folgenden Diagramme können Sie wichtige Einblicke gewinnen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

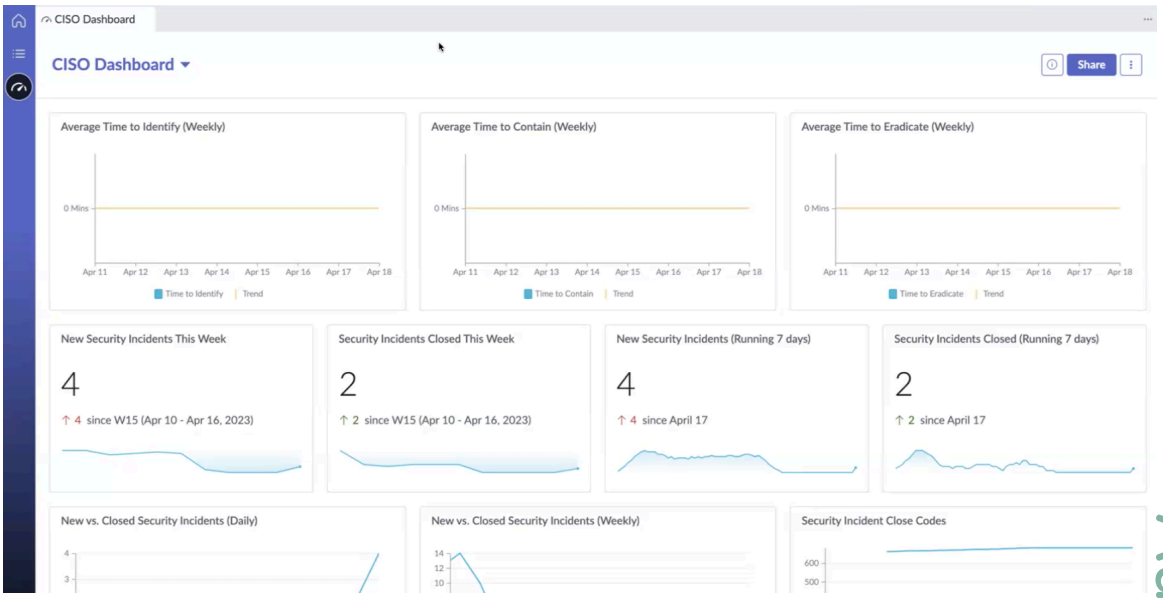
- **Durchschnittliche Zeit bis zur Identifizierung (wöchentlich)** : Dieses Diagramm veranschaulicht die durchschnittliche wöchentliche Zeit, die zur Identifizierung eines Security Incidents benötigt wird.
- **Durchschnittliche Zeit bis zur Eindämmung (wöchentlich)** : Dieses Diagramm veranschaulicht die durchschnittliche wöchentliche Zeit, die zur Eindämmung eines Security Incidents benötigt wird.
- **Durchschnittliche Zeit bis zur Beseitigung (wöchentlich)** : Dieses Diagramm veranschaulicht die durchschnittliche wöchentliche Zeit, die zur Beseitigung eines Security Incidents benötigt wird.
- **Neue Security Incidents diese Woche** : Dieses Diagramm zeigt die Anzahl der neuen Security Incidents in dieser Woche.
- **Diese Woche geschlossene Security Incidents** : Dieses Diagramm zeigt die Anzahl der in dieser Woche geschlossenen Security Incidents.
- **Neue Security Incidents (Ausführung 7 Tage)** : Dieses Diagramm zeigt die Anzahl der neuen Security Incidents, die eine Woche lang ausgeführt werden.
- **Geschlossene Security Incidents (Ausführung 7 Tage)** : Dieses Diagramm zeigt die Anzahl der neuen Security Incidents, die geschlossen wurden, aber eine Woche lang ausgeführt werden.
- **Neue vs. Geschlossene Incidents (täglich)** : Dieses Diagramm veranschaulicht den Vergleich zwischen den täglichen neuen Security Incidents und den täglich geschlossenen Security Incidents.
- **Neue vs. Geschlossene Incidents (wöchentlich)** : Dieses Diagramm veranschaulicht den Vergleich zwischen den wöchentlichen neuen Security Incidents und den wöchentlich geschlossenen Security Incidents.
- **Codes Für Geschlossene Security Incidents** : Dieses Diagramm veranschaulicht die geschlossenen Codes der Security Incidents.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**an.
2. Klicken Sie auf **SIR-Dashboards** Symbol auf der linken Seite der Arbeitsbereichs-Homepage.
3. Wählen Sie Aus **CISO-Dashboard** Aus der Dropdown-Liste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Zeigen Sie das CISO-Dashboard für weitere Aktionen an.

Zeigen Sie das Dashboard „CISO-Reporting-Übersicht“ an

Dieses Dashboard bietet Chief Information Security Officers (CISOs) in Form von grafischen Diagrammen eine allgemeine Berichterstellungsübersicht über Security Incidents und wöchentliche Incident-Trends in der Instanz. Diese Diagramme helfen Ihnen, die Leistung des Security Operations Center (SOC) effektiv anzuzeigen und zu analysieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin und sn_si.ciso – Incidents bearbeiten und anzeigen.

Warum und wann dieser Vorgang ausgeführt wird

Das Dashboard „CISO-Reporting-Übersicht“ bietet wöchentlich wichtige Einblicke zu den Security Incidents, und Sie können die wöchentlichen Trends mithilfe von Widgets visualisieren. Mithilfe der folgenden Diagramme können Sie wichtige Einblicke in das CISO-Reporting erhalten:

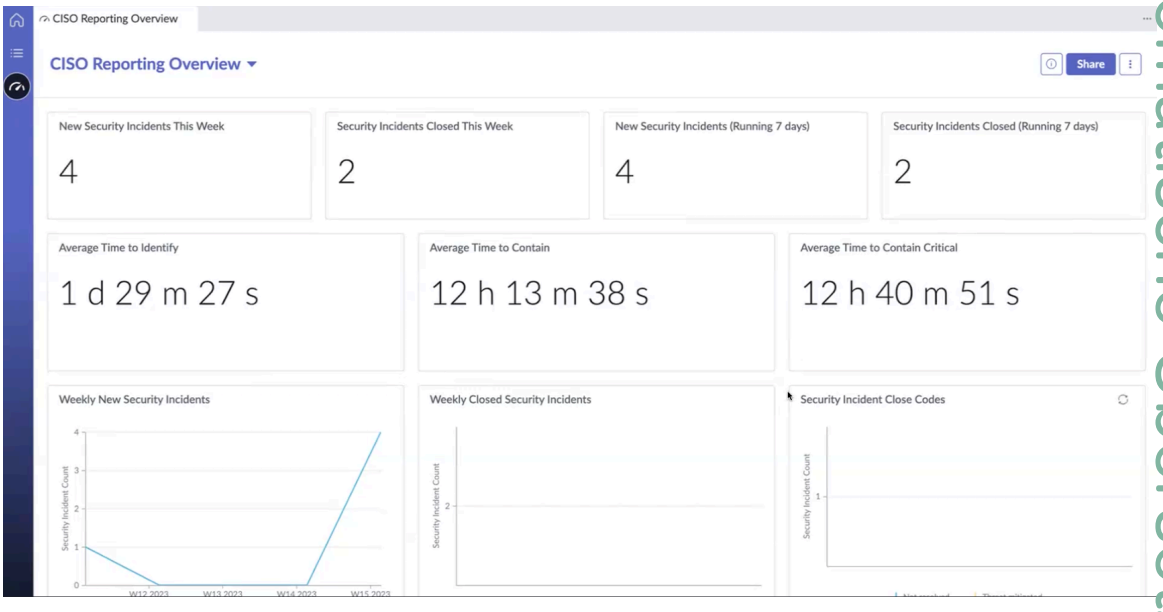
- **Neue Security Incidents diese Woche** : Diese Kachel zeigt den Bericht über die Anzahl der neuen Security Incidents diese Woche an.
- **Diese Woche geschlossene Security Incidents** : Diese Kachel zeigt den Bericht über die Anzahl der in dieser Woche geschlossenen Security Incidents an.
- **Neue Security Incidents (Ausführung 7 Tage)** : Diese Kachel zeigt den Bericht über die Anzahl der neuen Security Incidents an, die eine Woche lang ausgeführt werden.
- **Geschlossene Security Incidents (Ausführung 7 Tage)** : Diese Kachel zeigt den Bericht über die Anzahl der neuen Security Incidents an, die geschlossen wurden, aber eine Woche lang ausgeführt werden.
- **Durchschnittliche Zeit bis zur Identifizierung** : Diese Kachel zeigt den Bericht über die durchschnittliche wöchentliche Zeit an, die zur Identifizierung von Security Incidents benötigt wurde.
- **Durchschnittliche Zeit bis zur Eindämmung** : Diese Kachel zeigt den Bericht über die durchschnittliche wöchentliche Zeit an, die zur Eindämmung von Security Incidents benötigt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Durchschnittliche Zeit bis zur Eindämmung kritischer Elemente** : Diese Kachel zeigt den Bericht über die durchschnittliche wöchentliche Zeit an, die benötigt wurde, um kritische Security Incidents einzudämmen.
- **Wöchentliche Neue Security Incidents** : Dieses Diagramm veranschaulicht den Bericht der wöchentlichen neuen Security Incidents.
- **Wöchentlich Geschlossene Security Incidents** : Dieses Diagramm veranschaulicht den Bericht der wöchentlich geschlossenen Security Incidents.
- **Codes Für Geschlossene Security Incidents** : Dieses Diagramm veranschaulicht den Bericht der geschlossenen Codes der Security Incidents.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**an.
2. Klicken Sie auf **SIR-Dashboards** Symbol auf der linken Seite der Arbeitsbereich-Homepage.
3. Wählen Sie Aus **CISO-Reporting-Übersicht** Aus der Dropdown-Liste.



4. Zeigen Sie das CISO-Reporting-Dashboard an, um weitere Aktionen zu erhalten.

Automatische Übersetzung

Zeigen Sie das Dashboard „Security Incident Manager-Übersicht“ an

Dieses Dashboard bietet Managern einen allgemeinen Überblick über die Security Incidents mit kritischer oder hoher Priorität auf Teamebene, SLAs, die in 24 Stunden ablaufen, und wöchentliche Incident-Trends in der Instanz in Form von Berichten und grafischen Diagrammen.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin: Dashboard zum Bearbeiten und Anzeigen.
- sn_si.Manager: Dashboard anzeigen.

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Security Incidents mit kritischer oder hoher Priorität oder SLAs analysieren, die sofortige Aufmerksamkeit erfordern. Sie können die wöchentlichen Trends auch mithilfe der Widgets im Dashboard „Security Incident Manager – Übersicht“ visualisieren. Die Daten

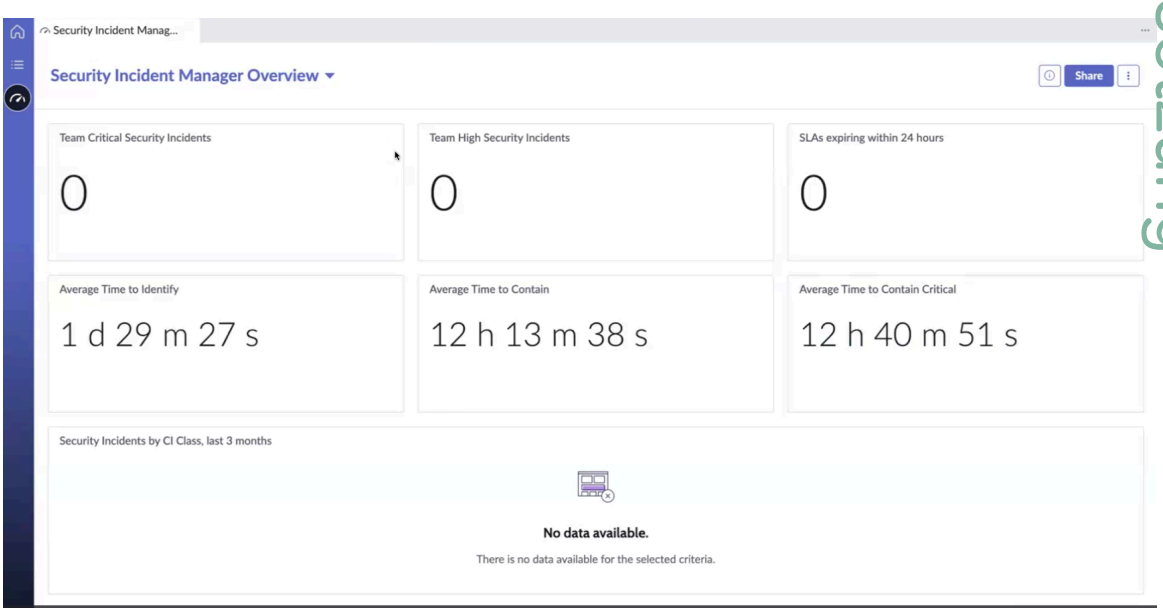
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

oder Statistiken für die wöchentlichen oder monatlichen Trends Ihrer Security Incidents werden aus den Tabellen der Incidents erfasst, die von der Organisation definiert werden. Mithilfe der folgenden Diagramme können Sie wichtige Einblicke gewinnen:

- **Kritische Security Incidents Des Teams** : Diese Kachel zeigt die Anzahl der kritischen Security Incidents für das Team in dieser Woche an.
- **Team High Security Incidents** : Diese Kachel zeigt die Anzahl der Incidents mit hoher Sicherheit für das Team in dieser Woche an.
- **SLAs, die innerhalb von 24 Stunden ablaufen** : Diese Kachel zeigt die Anzahl der SLAs an, die innerhalb von 24 Stunden ablaufen.
- **Durchschnittliche Zeit bis zur Identifizierung** : Diese Kachel zeigt die durchschnittliche wöchentliche Zeit an, die zur Identifizierung von Security Incidents benötigt wurde.
- **Durchschnittliche Zeit bis zur Eindämmung** : Diese Kachel zeigt die durchschnittliche wöchentliche Zeit an, die zur Eindämmung von Security Incidents benötigt wird.
- **Durchschnittliche Zeit bis zur Eindämmung kritischer Elemente** : Diese Kachel zeigt die durchschnittliche wöchentliche Zeit an, die benötigt wird, um kritische Security Incidents einzudämmen.
- **Security Incident nach CI-Klasse, letzte 3 Monate** : Dieses Diagramm veranschaulicht die Trends aller Security Incidents basierend auf der CI-Klasse für die letzten drei Monate.
- **Trend aller Security Incidents nach Kategorie** : Dieses Diagramm veranschaulicht die Trends aller Security Incidents basierend auf der Kategorie.
- **Trend aller Security Incidents nach Priorität** : Dieses Diagramm veranschaulicht die Trends aller Security Incidents basierend auf der Priorität.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Security Incident Response**an.
2. Klicken Sie auf **SIR-Dashboards** Symbol auf der linken Seite der Arbeitsbereich-Homepage.
3. Wählen Sie Aus **Security Incident Manager – Übersicht** Aus der Dropdown-Liste.



4. Zeigen Sie die Security Incident Manager-Übersicht für weitere Aktionen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie das Dashboard „Security Incident Response Health“ an

Die Dashboard-Funktion „Security Incident Response Health“ bietet eine zentrale Ansicht kritischer Aspekte im Zusammenhang mit der Implementierung des Prozesses zur Reaktion auf Incidents, aufgetretenen Problemen/Fehlern und Leistungsmetriken. Es dient als wichtiges Tool für die Überwachung und Optimierung der Effektivität der Fähigkeiten zur Reaktion auf Security Incidents einer Organisation.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.Analyst oder sn_si.Analytics_read – Dashboard anzeigen.

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Integrität der Security Incidents mithilfe der Widgets und Trenddiagramme für jede Anwendung überwachen. Diese Statistiken bieten eine umfassende Integritätspunktzahl, die den Konfigurationsstatus und die Effektivität der Korrektur in den SIR-Anwendungen beschreibt. Das Dashboard Security Incident Response Health unterstützt die folgenden vier Registerkarten:

- **Prozess** : Auf der Registerkarte wird wöchentlich eine Zusammenfassung aller Incidents aus verschiedenen Warnungssensoren angezeigt.
- **Implementierung** : Auf dieser Registerkarte werden die Anpassungen angezeigt, die Kunden in ihren Instanzen durchführen und Skripteinbindungen, Business-Regeln, Flows und Upgrades abdecken.
- **Probleme/Fehler** : Auf der Registerkarte werden Widgets angezeigt, die Fehler in Integrationsprozessen, Diskrepanzen bei der Erfassung von Incident-Rohdaten, ausgehende HTTP-Fehler in SIR-Anwendungen und alle Probleme hervorheben, die während der Ausführung von Playbooks auftreten.
- **Leistung** : Auf dieser Registerkarte werden die Leistungsprobleme in den SIR-Anwendungen angezeigt, einschließlich langsamer Leistungsabfragen, Geschäftsregeln und Skripts.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Wählen Sie aus **SIR-Dashboards** Symbol auf der SIR-Arbeitsbereich-Homepage.
3. Wählen Sie Aus **Dashboard „Security Incident Response – Integrität“** Aus der Dropdown-Liste.
4. Wählen Sie aus **Prozess** Registerkarte, um die Anzahl der Security Incidents anzuzeigen, die wöchentlich für jeden Warnungssensor im Diagramm ausgelöst wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Prozess“

Sie können die folgenden Aufgaben ausführen:

a. Wählen Sie einen Warnungssensor im Diagramm aus, um die KPI-Details der Anzahl der Security Incidents anzuzeigen, die von Warnungssensoren in einer Woche ausgelöst wurden.

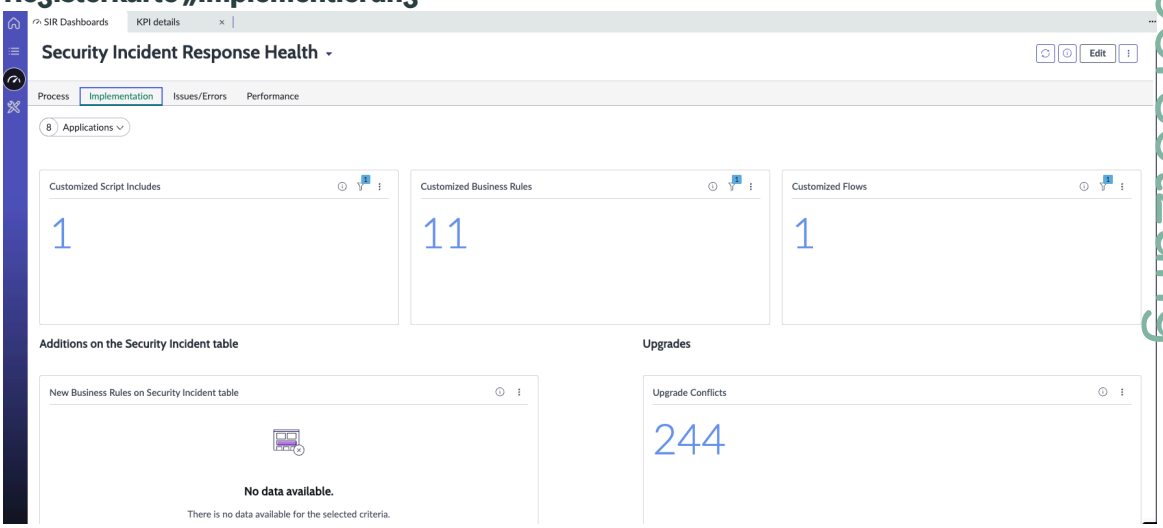
b. Um die KPI-Details für eine bestimmte Woche abzurufen, verwenden Sie **Kalender** Option.

c. Um die vom Warnungssensor ausgelösten Security Incidents zu vergleichen, wählen Sie aus **Datensätze Vergleichen** Option.

d. Um den Diagrammtyp, die Zeitreihe oder die Analyse zu verwenden, wählen Sie aus **Diagrammoptionen** .

5. Wählen Sie aus **Implementierung** Registerkarte, um die Anzahl der Anpassungen anzuzeigen, die für die Security Incidents in den Security Incident Response-Anwendungen erstellt wurden.

Registerkarte „Implementierung“



Implementierung Registerkarte:

Sie können das zusammengefasste Dashboard für die Anzahl der Anpassungen anzeigen, die für jede Incident Response-Anwendung erstellt wurden.

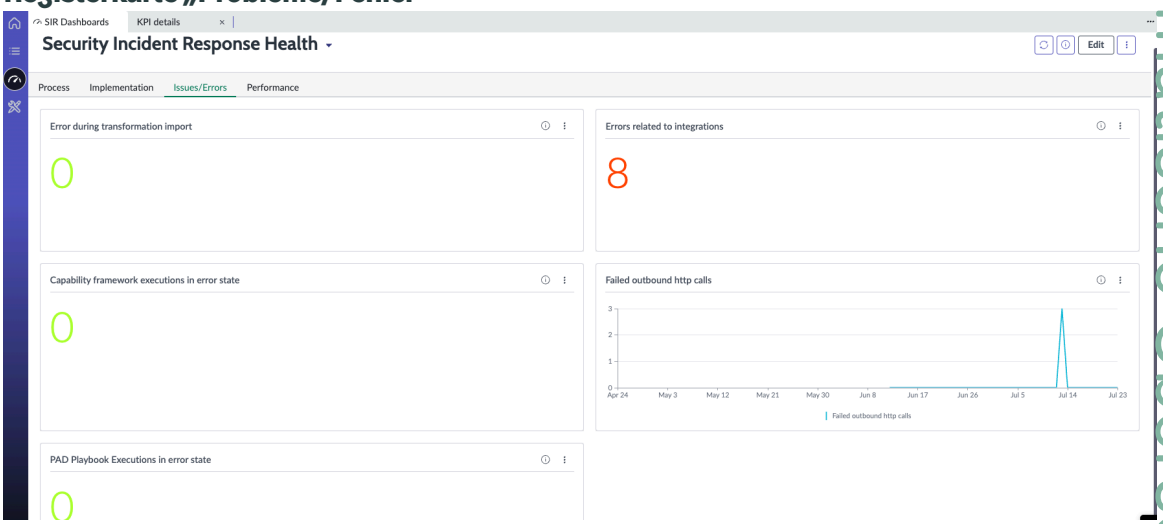
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Anwenderdefinierte Skripteinbindungen** : Dieses Widget zeigt die Anzahl der anwenderdefinierten Skripts an, die basierend auf Ihren Anforderungen in den SIR-Anwendungen hinzugefügt wurden.
- **Anwenderdefinierte Business-Regeln** : Dieses Widget zeigt die Anzahl der anwenderdefinierten Business-Regeln an, die basierend auf Ihren Anforderungen in den SIR-Anwendungen hinzugefügt wurden.
- **Anwenderdefinierte Flows** : Dieses Widget zeigt die Anzahl der anwenderdefinierten Flows an, die basierend auf Ihren Anforderungen in den SIR-Anwendungen hinzugefügt wurden.
- **Neue Business-Regel in der Security Incident-Tabelle** : Dieses Widget zeigt die Anzahl der Business-Regeln an, die in der Tabelle „Security Incident“ erstellt wurden.
- **Upgrade-Konflikte** : Dieses Widget zeigt die Anzahl der Konflikte an, die während Upgrades in den SIR-Anwendungen ausgelöst wurden.

6. Wählen Sie aus **Probleme/Fehler** Registerkarte, um die Anzahl der Probleme oder Fehler anzuzeigen, die in den Security Incident Response-Anwendungen ausgelöst wurden.

Registerkarte „Probleme/Fehler“



Probleme/Fehler Registerkarte:

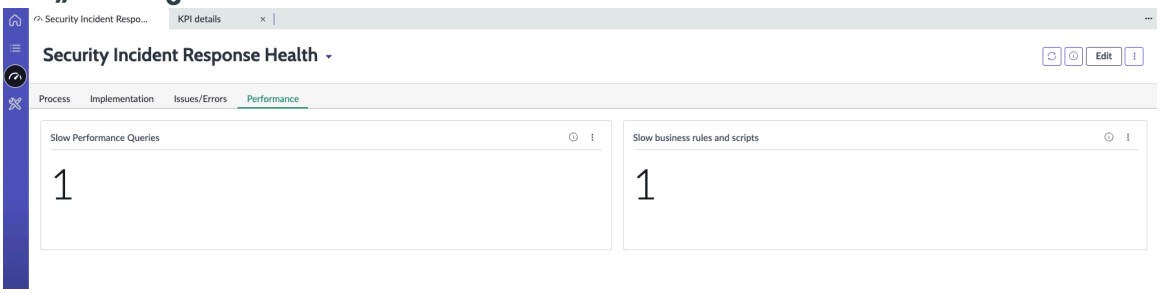
Sie können das zusammengefasste Dashboard für Probleme oder Fehler in den Security Incident Response-Anwendungen anzeigen.

- **Fehler beim Transformationsimport** : Dieses Widget zeigt die Anzahl der Fehler an, die während des Transformationsimports in SIR-Anwendungen ausgelöst wurden.
- **Fehler im Zusammenhang mit Integrationen** : Dieses Widget zeigt die Anzahl der Fehler an, die während der SIR-Integrationen ausgelöst wurden.
- **Fähigkeits-Framework-Ausführungen im Fehlerstatus** : Dieses Widget zeigt die Anzahl der Fehler an, die während der Ausführungen des Fähigkeits-Frameworks in SIR-Anwendungen ausgelöst wurden.
- **Ausgehende HTTP-Aufrufe fehlgeschlagen** : Dieses Widget zeigt die Anzahl der fehlgeschlagenen ausgehenden HTTP-Aufrufe an, die in den SIR-Anwendungen ausgelöst wurden.
- **PAD-Playbook-Ausführungen im Fehlerstatus** : Dieses Widget zeigt die Anzahl der PAD-Playbook-Ausführungsfehler an, die in den SIR-Anwendungen ausgelöst wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie aus **Leistung** Registerkarte, um die Anzahl der Leistungsprobleme anzuzeigen, die in den Security Incident Response-Anwendungen ausgelöst wurden.

Tab „Leistung“



Leistung Registerkarte:

Sie können das zusammengefasste Dashboard für Leistungsprobleme in den Security Incident Response-Anwendungen anzeigen.

- **Abfragen Mit Langsamer Leistung** : Dieses Widget zeigt die Anzahl der Leistungsabfragen in den SIR-Anwendungen an, deren durchschnittliche Ausführungszeit größer als 10 ms ist und im Durchschnitt 1000 oder mehr Ausführungen beträgt.
- **Langsame Geschäftsregeln und Skripts** : Dieses Widget zeigt die Anzahl der Business-Regeln und Skripts in den SIR-Anwendungen an, deren durchschnittliche Ausführungszeit größer als 10 ms ist und im Durchschnitt 1000 oder mehr Ausführungen beträgt.

8. Sie können verwenden **Aktualisieren** Symbol zum Aktualisieren der Daten im Dashboard „Integrität der Security Incident Response“.
9. Sie können verwenden **Zeigen Sie Dashboard-Details an** Symbol zum Anzeigen der Details des Dashboards für die Integrität der Security Incident Response.
10. Sie können verwenden **Bearbeiten** Option zum Ändern der Details des Dashboard „Security Incident Response – Integrität“.
11. Sie können verwenden **Mehr** Option zum Ausführen zusätzlicher Aktionen im Dashboard „Integrität der Security Incident Response“.

Security Incident-Erstellung

Security Incidents können manuell über das Formular oder automatisch über Sicherheitsereignisse erstellt werden, die von integrierten Warnungstools von Drittanbietern wie Splunk empfangen werden.

Wichtig:
Die neuesten Funktionen in Security Incident Response Sind ausschließlich in verfügbar Arbeitsbereich für Security Incident Response. Installieren oder aktualisieren Sie auf den neuesten Security Incident Response Oder Arbeitsbereich für Security Incident Response Version für den Zugriff auf und die Nutzung von Funktionen wie Schichtübergabe, Risikobewertungsrechner usw.

Wenn Sie eine Sicherheitsrolle haben, können Sie eine der folgenden Methoden verwenden, um Security Incidents manuell zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Methoden zum manuellen Erstellen von Security Incidents

Methode	Beschreibung
Manuell aus der Security Incident-Liste erstellt	Klicken Sie in der Liste Security Incident auf **Neu** Um einen neuen Security Incident zu erstellen.
Manuell aus dem Security Incident-Katalog erstellt	Sie können Security Incidents erstellen, indem Sie aus Kategorien von Sicherheitsbedrohungen auswählen, die im Security Incident-Katalog definiert sind.
Incident-Management	Klicken Sie im Incident-Formular in Incident-Management auf **Erstellen Sie Einen Security Incident** Um einen neuen Security Incident zu erstellen.
Manuell aus einer Sicherheitsanforderung konvertiert	Klicken Sie im Formular „Sicherheitsanforderung“ auf **In Security Incident konvertieren** Um einen neuen Security Incident zu erstellen.
Manuell aus einer Ereignismanagement-Warnung erstellt	Klicken Sie im Formular „Ereignismanagement-Warnungen“ auf **Erstellen Sie einen Security Incident** Dient zum Erstellen eines neuen Security Incidents aus einer Warnung.
Manuell aus einer Warnung erstellt	Klicken Sie im Formular „Ereignismanagement-Warnung“ auf **Erstellen Sie Einen Security Incident** Um einen neuen Security Incident zu erstellen.
Manuell aus einem Schwachstellendatensatz konvertiert (wenn das Plugin „Vulnerability Response“ aktiviert ist)	Klicken Sie im Formular „Schwachstellenelemente“ auf **Erstellen Sie Einen Security Incident** Um einen neuen Security Incident zu erstellen.

Automatische Erstellung von Security Incidents

Im Allgemeinen sind Sicherheitsadministratoren für die Einrichtung von Warnungsregeln verantwortlich, die zum automatischen Generieren von Security Incidents verwendet werden.

Sicherheitsadministratormethode zum Erstellen von Security Incidents

Methode	Beschreibung
Wird automatisch mithilfe von Warnungsregeln erstellt	Security Incidents können basierend auf Warnungsregeln erstellt werden, die in definiert sind Ereignismanagement in Ihrem Rechenzentrum Anwendung.

Manuelle Erstellung von Security Incidents

Sie können einen Security Incident aus dem Security Incident-Formular sowie aus mehreren anderen Formularen erstellen.

Sie können Security Incidents basierend auf einem vorhandenen Datensatz aus den folgenden Formularen erstellen:

- Aus einer beliebigen Security Incident-Liste
- Incident-Formular
- Ereignismanagement Warnungsformular
- Formular „angreifbare Elemente“
- Formular „Sicherheitsanforderung“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Security Incident aus der Liste Security Incident

Zusätzlich zu automatischen Methoden zum Erstellen von Security Incidents können Sie sie bei Bedarf manuell erstellen.

Dieses Video zeigt einen visuellen Überblick darüber, wie Sie einen Security Incident aus der Liste Security Incident erstellen können.

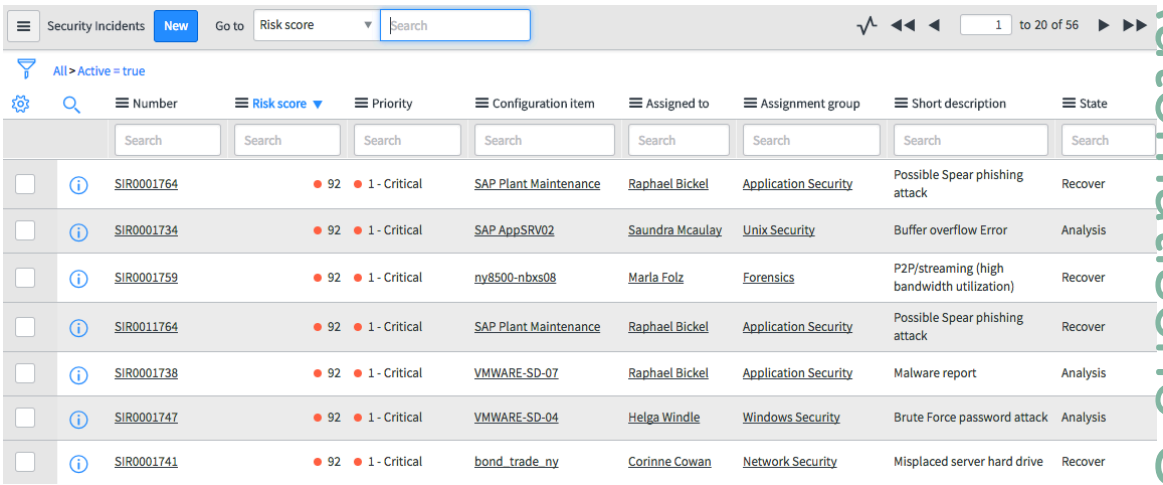
Erstellen Sie einen Security Incident aus der Liste Security Incident

Vorbereitungen

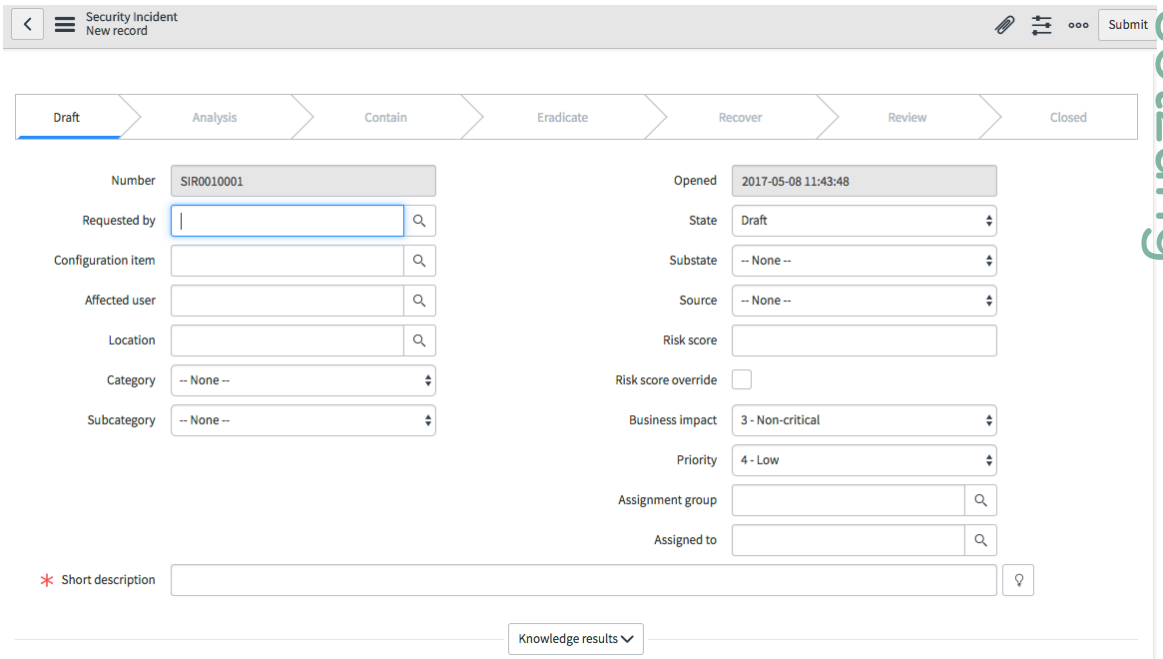
Erforderliche Rolle: sn_si.Basic

Prozedur

1. Navigieren Sie zu einer beliebigen Security Incident-Liste (z. B. **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**) an.



2. Klicken Sie auf **Neu**.



3. Füllen Sie im Formular die Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sicherheits-Tag auswählen	Wählen Sie bei Bedarf eine aus Sicherheits-Tag Um dem Datensatz Metadaten hinzuzufügen oder zu identifizieren, wer Zugriff auf diesen Security Incident-Datensatz haben soll. Dieses Feld wird erst angezeigt, nachdem der Security Incident gespeichert wurde.
Anzahl	[Schreibgeschützt] die Nummer des Security Incidents.
Angefordert von	Die Person, die die auszuführende Arbeit anfordert.
Konfigurationselement	Der Server, Computer, Router oder ein anderes Konfigurationselement, das vom Sicherheitsproblem betroffen ist.
Betroffener Anwender	Die vom Sicherheitsproblem betroffene Person.
Standort	Der Standort der anfordernden Person oder Ressource. Wenn ein **Konfigurationselement** Ist nicht ausgewählt, ist dieses Feld mit dem Standort der anfordernden Person vorab ausgefüllt.
Kategorie	Die Kategorie, die den Typ des Sicherheitsproblems identifiziert. Wenn eine Kategorie ausgewählt ist, wird beim Speichern des Datensatzes ein Workflow zur Analyse dieses Problems ausgeführt. Beispiel: Wenn Sie auswählen **Denial of Service** , Der Workflow „Security Incident – Denial of Service – Vorlage“ wird ausgeführt. Weitere Informationen finden Sie unter Workflow-Vorlagen für Security Incident Response.
Unterkategorie	Die Unterkategorie, die das Problem weiter definiert.
Geöffnet	[Schreibgeschützt] zeigt Datum und Uhrzeit der Eröffnung des Incident an.
Status	Der aktuelle Status des Security Incidents. Bei der Erstellung von Security Incidents ist dieses Feld standardmäßig auf festgelegt **Entwurf** .
Substatus	Gibt an, ob der Security Incident ein ausstehendes Problem oder einen Change enthält.
Quelle	Gibt die Quelle des Security Incidents an, z. B. E-Mail, Telefonanruf oder Netzwerküberwachung.
Warnungssensor	Sicherheitsintegration, über die Sie Warnungs- oder Ereignisdaten wie CarbonBlack, CrowdStrike, McAfee usw. erfassen.
Warnungsregel	Die Regel im Sicherheitsprodukt, die die Erstellung dieses Security Incidents ausgelöst hat.
Risikopunktzahl	Zeigt die für diesen Security Incident berechnete Risikopunktzahl an. Der Wert basiert auf der Priorität des Security Incidents, dem Typ des Security Incidents (Denial of Service, Spear Phishing oder schädliche Codeaktivität) und der Anzahl der Quellen, die für einen Indikator eine fehlgeschlagene Reputationspunktzahl ausgelöst haben. Die Risikopunktzahl hilft bei der Priorisierung der Security Incident-Arbeit für Analysten. Mit drei Security Incident-Eigenschaften können Sie einen farbcodierten Punkt weiter festlegen, der neben der Risikopunktzahl in der Listenansicht angezeigt wird, um sie leichter zu identifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn Sie Änderungen an bestimmten Feldern im Security Incident vornehmen, z. B. **Geschäftsauswirkung** Oder **Priorität** , Und speichern Sie den Datensatz, **Risikopunktzahl** Wird automatisch neu berechnet und angezeigt. Der Change wird auch in den Arbeitsnotizen und in der zugehörigen Liste „Audits der Risikopunktzahl“ berücksichtigt. **Hinweis:** Die Risikopunktzahl wird auch neu berechnet, wenn betroffene Anwender einem Security Incident, betroffenen Services oder angreifbaren Elementen zugeordnet sind. Sie können auch manuell einen neuen eingeben **Risikopunktzahl** . Dies kann nützlich sein, wenn Sie einen bestimmten Security Incident ganz oben in der Liste der Security Incidents lassen möchten, die Sie analysieren. Wenn Sie einen neuen eingeben **Risikopunktzahl** , **Überschreibung der Risikopunktzahl** Das Kontrollkästchen ist automatisch aktiviert. Unabhängig von den im Security Incident vorgenommenen Änderungen wird eine manuell eingegebene Risikopunktzahl nicht automatisch neu berechnet. **Hinweis:** Wenn Sie Ihre Instanz von einem früheren Release aktualisiert haben, wurden Risikopunktzahlen für alle Ihre offenen Security Incidents berechnet. Weitere Informationen finden Sie unter Verstehen von Security Incident-Rechnern.
Überschreibung der Risikopunktzahl	Aktivieren Sie dieses Kontrollkästchen, um die automatische Aktualisierung der Risikopunktzahl zu überschreiben. Die Überschreibung wird in den Arbeitsnotizen berücksichtigt.
Geschäftsauswirkung	Wählen Sie die Wichtigkeit dieses Security Incidents für Ihr Unternehmen aus. Der Standardwert ist nicht kritisch. Wenn Sie nach dem Speichern des Security Incident-Datensatzes den Wert in ändern **Priorität** Gefunden/oder **Risiko** Felder, die **Geschäftsauswirkung** Wird neu berechnet.
Priorität	Wählen Sie die Reihenfolge aus, in der dieser Security Incident behandelt werden soll, basierend auf der Dringlichkeit. Wenn dieser Wert nach dem Speichern des Datensatzes geändert wird, kann dies sich auf auswirken **Geschäftsauswirkung** Berechnung.
Zuweisungsgruppe	Die Gruppe, der dieser Security Incident zugewiesen ist.
Zugewiesen an	Die Person, die der Analyse dieses Security Incidents zugewiesen ist. Zuweisungen können manuell oder automatisch durchgeführt werden. Weitere Informationen finden Sie unter Sicherheitsanalysten werden zugewiesen.
Kurzbeschreibung	Eine kurze Beschreibung des Security Incidents.
Wissensergebnisse	Während Sie die Kurzbeschreibung eingeben, werden Links zu zugehörigen Artikeln aus der Knowledge Base angezeigt. Das Scannen der Informationen könnte Ihr Problem lösen.

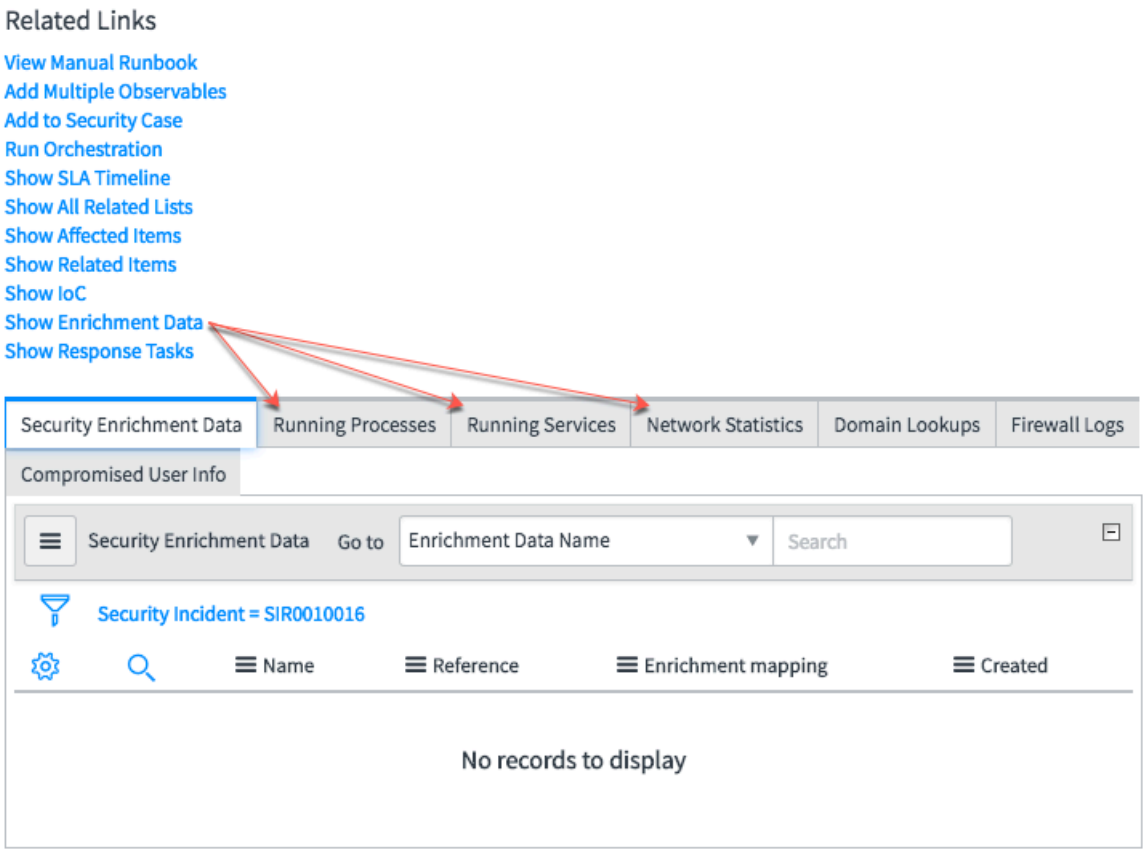
4. Klicken Sie mit der rechten Maustaste in den Datensatzheader, und wählen Sie aus **Speichern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie dem Security Incident ein neues CI hinzugefügt haben, werden die folgenden Integrations-Workflows automatisch ausgeführt:

- Security Operations – Flow „Laufende Prozesse Abrufen“. Dieser Workflow ruft eine Liste der laufenden Prozesse für ein Konfigurationselement (Configuration Item, CI) von einem Host oder Endpunkt ab.
- Security Incident Response – Workflow „laufende Services abrufen“. Dieser Workflow ruft eine Liste der laufenden Services von Windows-basierten CIs ab.
- Security Operations-Integrationen – Flow „Netzwerkstatistiken abrufen“. Dieser Workflow ruft eine Liste aktiver Netzwerkverbindungen von einem Host oder Endpunkt ab.

5. Um die von diesen Workflows abgerufenen Informationen anzuzeigen, klicken Sie auf **Anreicherungsdaten Anzeigen** Zugehöriger Link, und klicken Sie dann auf eine der angegebenen Registerkarten.



Automatische Übersetzung

Hinweis:
Zusätzliche Workflows werden basierend auf den Drittanbieterintegrationen ausgeführt, die Sie wie folgt aktiviert haben Security Operations Carbon Black-Integration – Flow Für Laufende Prozesse Abrufen

Zugehörige Informationen

Setup von Security Incident Response

Erstellen Sie einen Security Incident aus dem Security Incident-Katalog

Anwender in Ihrem Unternehmen können den Security Incident-Katalog verwenden, um verschiedene Arten von sicherheitsbezogenen Analysen anzufordern.

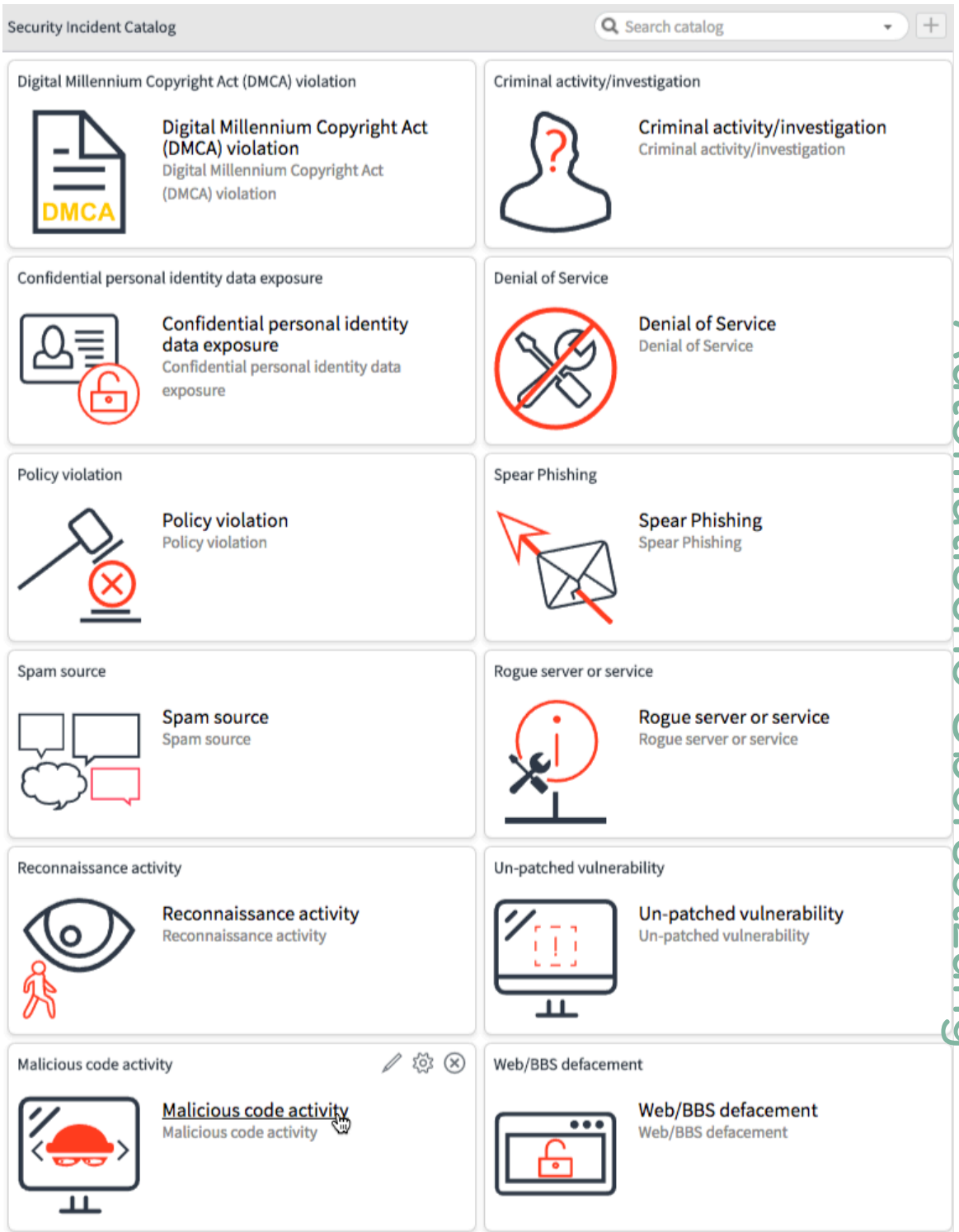
Vorbereitungen

Erforderliche Rolle: keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

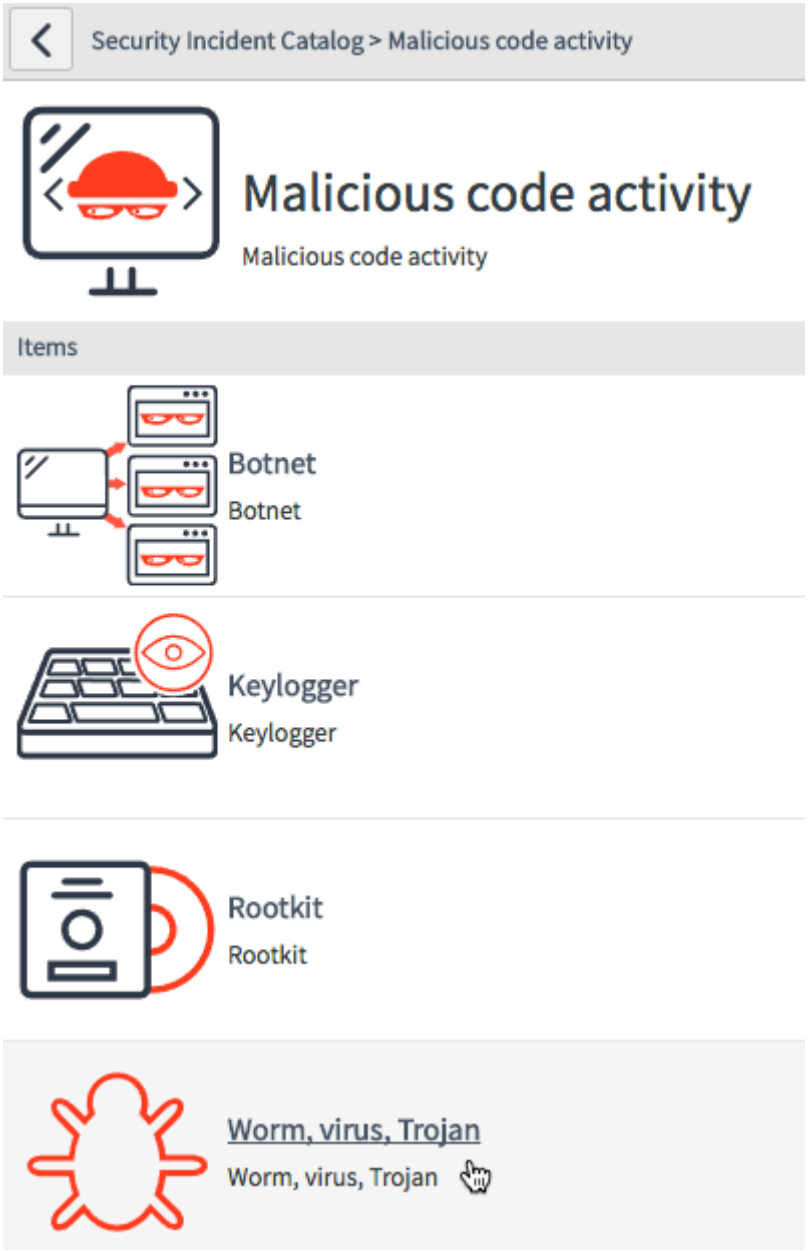
1. Navigieren zu **Alle** > **Self-Service** > **Security Incident-Katalog**an.



2. Klicken Sie auf das Katalogelement, für das Sie eine Anforderung stellen möchten.
   Wenn das Element, das Sie im Hauptkatalog ausgewählt haben, Unterkategorien enthält, wird die Liste angezeigt. Im folgenden Beispiel: **Schädliche Codeaktivität** Wurde ausgewählt.

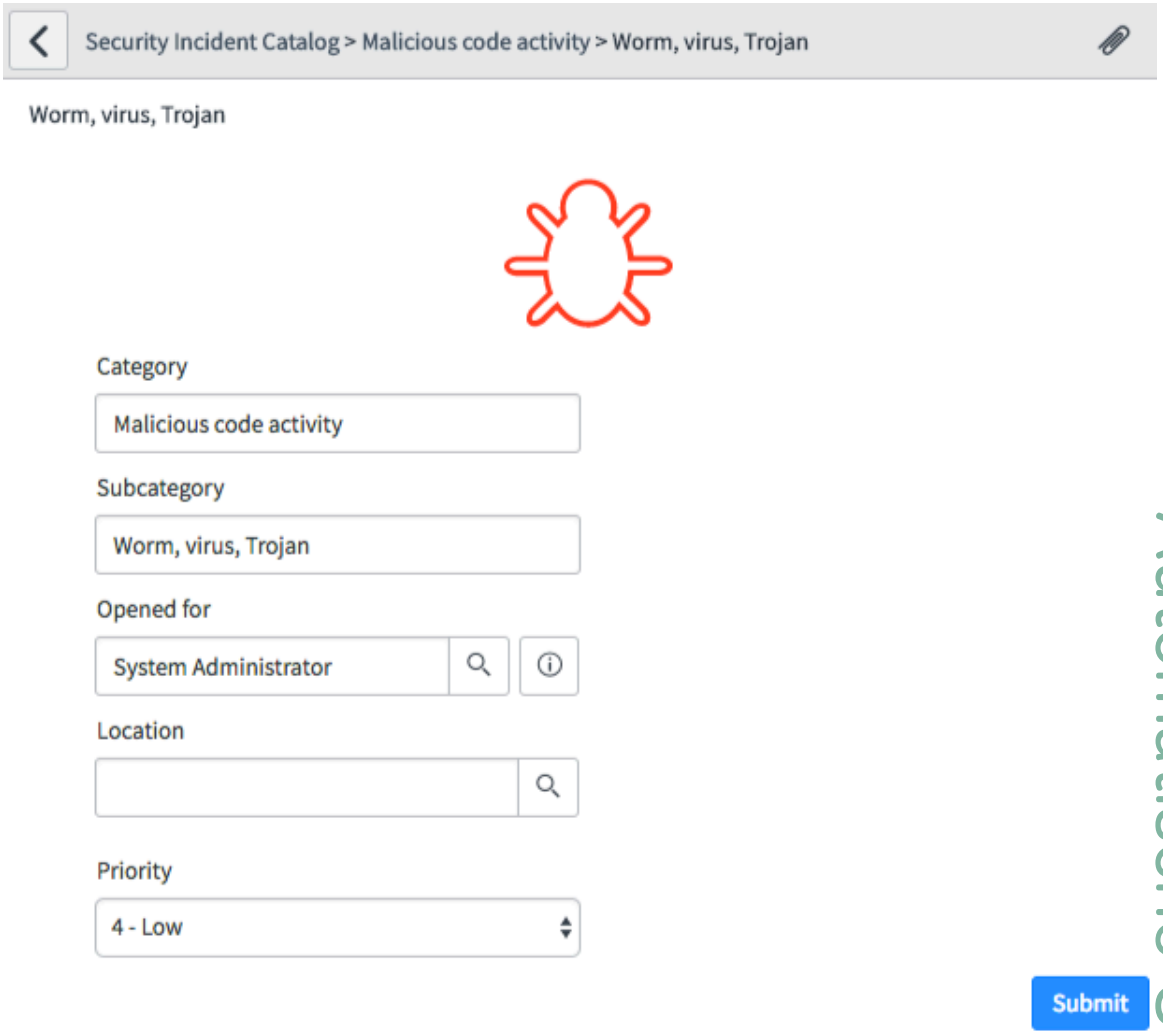
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf die Unterkategorie, die am besten dem Typ der Anforderung entspricht, die Sie stellen möchten.
In diesem Beispiel ist **Wurm, Virus, Trojaner** Unterkategorie wurde ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie die Informationen für die Anforderung ein, und klicken Sie auf **Übermitteln** .
   Die Anforderung wird an Ihre Security Incident-Abteilung gesendet.
5. Nachdem Sie die Anforderung übermittelt haben, können Sie ihren Fortschritt nachverfolgen, indem Sie zu navigieren **Self-Service** > **Meine Anforderungen**, Und Eingabe der Anforderungsnummer.

Erstellen Sie einen Security Incident aus einer Ereignismanagement-Warnung

Wenn Ereignismanagement aktiviert ist, können Sie Security Incidents manuell über das Warnungsformular erstellen.

Vorbereitungen

Das Ereignismanagement-Plugin erfordert ein separates Abonnement und muss von ServiceNow-Mitarbeitern aktiviert werden. Dieses Plugin enthält Demodaten und aktiviert zugehörige Plugins, wenn sie nicht bereits aktiv sind. Service Analytics wird automatisch aktiviert, wenn Ereignismanagement aktiviert ist.
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**an.
2. Klicken Sie auf die **Nummer** der Warnung.
3. Klicken Sie Auf **Erstellen Sie einen Security Incident** .
4. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Erstellung von Security Incidents

Überwachungstools von Drittparteien wie Splunk können in integriert werden Security Incident Response Damit aus diesen Tools importierte Sicherheitsereignisse automatisch Security Incidents generieren. Sie können auch Daten aus Drittanbietertools in Sicherheitswarnungen importieren.

Zum Integrieren von Warnungsüberwachungstools in Security Incident Response, Sie müssen verwenden REST-API Zum Schreiben in die Tabelle „Security Incident-Import“ [sn_si_Incident_Import]. Dann mit **Security Incident-Transformation** Transformationszuordnungen , Die Quelltabelle des Importsatzes wird Feldern in der Tabelle „Ziel-Security Incident“ [sn_si.incident] zugeordnet.

Wenn Sie versuchen, CI-Datensätze zu importieren, die von der Transformationszuordnung nicht erkannt werden, überprüft das Transformationszuordnungsskript den Datensatz auf Folgendes (in dieser Reihenfolge), um eine Übereinstimmung zu erzielen:

- sys_id
- CI-Name
- Vollqualifizierter Domänenname
- IP-Adresse

Hinweis:
Wenn Sie finden, dass **Security Incident-Transformation** Transformationszuordnung ist für das von Ihnen verwendete Drittanbieter-Warnungstool für die Warnungsüberwachung nicht ausreichend. Duplizieren Sie die Transformationszuordnung, erstellen Sie eine neue, und bearbeiten Sie die Felder nach Bedarf.

Aus Events und Warnungen erstellte Security Incidents

Wenn Ereignisse aus Warnungsüberwachungstools importiert werden, werden sie zuerst von verarbeitet EreignismanagementUnd gruppiert in Warnungen. Diese Warnungen können verwendet werden, um Security Incidents basierend auf anpassbaren Warnungsregeln zu erstellen, oder manuell überprüft werden, um die Warnungen auszuwählen, die als Security Incident untersucht werden sollen.

Sie finden eine Beispiel-Warnungsregel namens **Erstellen Sie Security Incidents aus kritischen Warnungen** In WarnungsregelnModul von EreignismanagementAnwendung. Diese Warnungsregel erstellt automatisch Security Incidents, wenn kritische sicherheitsbezogene Ereignisse von innerhalb empfangen werden ServiceNow Oder aus Überwachungsanwendungen von Drittparteien. Nachdem der Security Incident erstellt wurde, wird er aktualisiert, wenn neue Ereignisse empfangen werden. Sie können die Aufgabenvorlage in der Warnungsregel ändern, um die Anfangswerte für den von dieser Warnungsregel erstellten Security Incident zu ändern. Um jede unterschiedliche Vielfalt von Security Incidents zu verarbeiten, die Sie erstellen möchten, können Sie andere Warnungsregeln mit verschiedenen Bedingungen definieren.

Alternativ können Sie, wenn Sie ein Anwender mit der Rolle „Sicherheitsadministrator“ sind, einen Security Incident manuell erstellen, indem Sie auf klicken **Erstellen Sie Einen Security Incident** Schaltfläche aus jeder verdächtigen Warnung.

Es ist wichtig, dass die von externen Tools empfangenen Ereignisse die folgenden Informationen enthalten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Knoten, der auf den Namen, die IP-Adresse oder die sys_ID des CI festgelegt ist, das zur betroffenen Ressource wird.
- Die Ereignisklassifizierung ist auf „Sicherheit“ festgelegt, um sie von anderen IT-Ereignissen zu unterscheiden.
- Die Ereignisbeschreibung, die die Beschreibung des Security Incidents ausfüllt.
- Die zusätzlichen Informationen können zusätzliche Informationen enthalten, die nicht in die zuvor aufgeführten Felder oder andere Ereignisfelder passen, z. B. Kategorie, Angriffsvektoren, Rückgabe-URL oder Korrelations-ID. Das Format ist eine Zeichenfolge, die Feldnamen zusammen mit ihren Werten im folgenden JSON-Format auflistet:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

Hinweis:
Wenn das Feld im Security Incident, in dem der Spaltenname mit dem fieldName übereinstimmt, für jedes Feld- und Wertpaar leer ist, wird es auf fieldValue festgelegt. Wenn das Feld im Security Incident nicht leer ist, wird es nicht geändert. In beiden Fällen werden das Ereignis und alle in den zusätzlichen Informationen codierten Felder und Werte in einem Arbeitsnotizeneintrag aufgezeichnet, der das Ereignis beschreibt. Wenn sich im Security Incident nichts ändert, wird kein Arbeitsnotizeneintrag erstellt.
Alle Felder in einem Security Incident, einschließlich anwenderdefinierter Felder, die Sie der Tabelle hinzufügen, können festgelegt werden.

Daten wurden in Sicherheitswarnungen importiert

Wenn ein Ereignis mit weiteren JSON-codierten Daten erstellt wird, werden diese Daten in ein Feld mit einem Namen importiert, der dem Feldnamen dieses Werts in den JSON-Daten entspricht.

Wenn Sie Daten in Ihrer Überwachungssoftware von Drittanbietern (z. B. Splunk) haben, die nicht im Basissystem vorhanden sind, können Sie der Tabelle „Warnung“ neue Felder hinzufügen, um den Datenimport aufzunehmen. Das JSON-Format zum Importieren von Daten in Warnungen entspricht dem Format, das zum Erstellen von Security Incidents aus Ereignissen und Warnungen verwendet wird:

```
{ "fieldName" : "fieldValue", "fieldName" : "fieldValue" }
```

Der einzige Unterschied besteht darin, dass die Daten im Feld immer mit dem fieldValue überschrieben werden.

Wenn die Sicherheitsereignisdaten importiert werden, werden die Felder in der Warnungstabelle mit übereinstimmenden Feldnamen ausgefüllt. Wenn die Warnung später in einen Security Incident umgewandelt wird, füllen dieselben zusätzlichen Informationsdaten übereinstimmende Felder im Security Incident aus.

Erstellen Sie Security Incidents aus vom Anwender gemeldeten Phishing-E-Mails

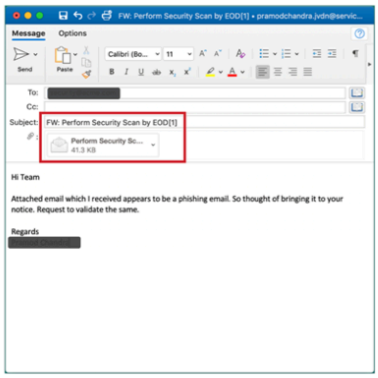
Verwenden Sie diese Funktion, um Security Incidents aus vom Anwender gemeldeten Phishing-E-Mails zu erstellen.

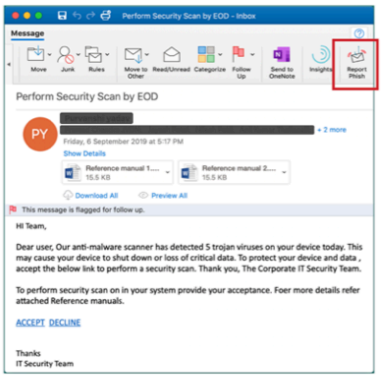
Die erweiterte Funktionalität „von Anwendern gemeldete Phishing“ umfasst Zusammenfassungsfunktionen, E-Mail-Header-Extraktion und Konfiguration.

- Anwender können Phishing-E-Mails auf verschiedene Arten melden:
  - E-Mails können als Anhänge weitergeleitet werden.
  - Wenn **PhishAlarm** Plugin (früher Wombat) wurde mit dem Microsoft Outlook-Client konfiguriert. Anwender können:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

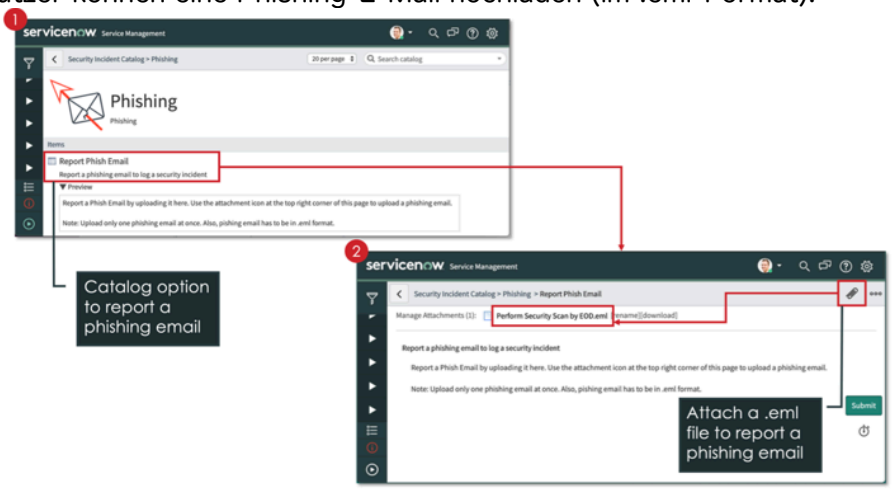
- Klicken Sie auf **Phishing Melden** Schaltfläche.
- Leiten Sie Phishing-E-Mails von einem Mobilgerät mit weiter **Phishing Melden** Option.


Desktop


Desktop

Mobile

- Benutzer können eine Phishing-E-Mail hochladen (im .eml-Format).



- Vom Anwender gemeldete Phishing-Einbindungen **Geschäftslogik der Zusammenfassung** Identifiziert doppelte Phishing-E-Mails, die von Anwendern in einer Organisation gemeldet wurden. Anwender können diese Fähigkeit verwenden, um:
  - Fassen Sie doppelte oder ähnliche von Anwendern gemeldete Phishing-Incidents zusammen (vom Unternehmen initiierte Phishing-Kampagnen).
  - Vermeiden Sie die Selektierung doppelter von Anwendern gemeldeter Phishing-Incidents, und reduzieren Sie den manuellen Aufwand für die Konsolidierung von Incidents.
  - Ermöglichen Sie Sicherheitsanalysten, an einem einzelnen Anwender gemeldeten Phishing-Incident zu arbeiten.
- Stellt Phishing-E-Mail-Header innerhalb des vom Anwender gemeldeten Phishing-Incidents bereit.
  - Sicherheitsanalysten können innerhalb des Incident nach wichtigen E-Mail-Header-Informationen suchen.
  - Manueller Aufwand beim Sammeln von Headerinformationen aus anderen Quellen ist nicht mehr erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die ursprünglich übermittelte Phishing-E-Mail wird als gespeichert **Phishing-E-Mail-Datensatz** In einer neuen Tabelle.
- Sicherheitsanalysten können Details der ursprünglichen Phishing-E-Mail anzeigen, z. B. Inhalt, Header und Ursprung von Phishing-E-Mails.
- Sicherheitsadministratoren können bestimmte Erweiterungen konfigurieren und vornehmen, darunter:
  - Konfigurationen zum Extrahieren von E-Mail-Kopfzeilen aus dem E-Mail-Text (**Phishing Melden** Übermittlungen).
  - Filter zum Erfassen ausgewählter Header.
  - Konfigurationen zur Verarbeitung der Zuordnung von über- und untergeordneten Incidents, wenn doppelte Phishing-E-Mail-Datensätze identifiziert werden.
  - Flow Designer-Konfigurationen zum Ändern der Geschäftslogik der Zusammenfassung basierend auf den Anforderungen.

Richten Sie Erfassungsregeln für vom Anwender gemeldetes Phishing ein

Als Anwender mit `sn_si.admin` Rolle können Sie E-Mail-Übereinstimmungsregeln definieren, um von Anwendern gemeldete Phishing-E-Mails basierend auf bestimmten Kriterien zu filtern. Sie können beispielsweise eine Regel definieren, bei der alle E-Mails entweder direkt oder über die Schaltfläche Phishing melden an gesendet werden `security@acme.com` Werden als vom Anwender gemeldete Phishing-E-Mails kategorisiert. Weitere Informationen finden Sie unter Richten Sie Erfassungsregeln für vom Anwender gemeldetes Phishing ein.

Definieren Sie vom Anwender gemeldete Phishing-Eigenschaften

Definieren Sie die Headerinformationen, die aus vom Anwender gemeldeten Phishing-E-Mails erfasst werden müssen. Weitere Informationen finden Sie unter Definieren Sie vom Anwender gemeldete Phishing-Eigenschaften

Phishing-E-Mail-Datensätze, die aus vom Anwender gemeldeten Phishing-E-Mails erstellt wurden

Vom Anwender gemeldete Phishing-E-Mails werden basierend auf den definierten E-Mail-Übereinstimmungsregeln in Security Incidents konvertiert. Weitere Informationen finden Sie unter Phishing-E-Mail-Datensätze, die aus vom Anwender gemeldeten Phishing-E-Mails erstellt wurden.

Wandeln Sie Phishing-E-Mails in Security Incident um

Der Flow Phishing-E-Mail in Security Incident umwandeln konvertiert oder wandelt Phishing-E-Mail-Datensätze in Security Incidents um. Weitere Informationen finden Sie unter Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents.

Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden

Zeigen Sie die Details des Security Incident-Datensatzes an, einschließlich der zugehörigen Listen, Arbeitsnotizen und anderer wichtiger Informationen. Weitere Informationen finden Sie unter Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Komponenten und Plugins

Die Funktion „von Anwendern gemeldetes Phishing“, die in diesem Release verfügbar ist, ist eine erweiterte Version der vorhandenen von Anwendern gemeldeten Phishing-Funktionalität, die im London-Release verfügbar ist. Siehe **Erstellen Sie Regeln, um von Anwendern gemeldete Phishing-Angriffe zu validieren** Thema in der London-Dokumentation für Details.

Wichtige Installationsanweisungen

Diese Erweiterung ersetzt das vorhandene von Anwendern gemeldete Phishing-Design. Das neue Design enthält die folgenden Updates:

- Die vorhandenen **Vom Anwender Gemeldetes Phishing** Eingehende E-Mail-Aktionen (Typ = Weiterleiten und Typ = Neu) wurden deaktiviert.
- Ein neuer **Phishing-E-Mail Erstellen** Eingehende Aktion ist jetzt verfügbar.
- Die Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents Ist ein neuer Flow, der die Geschäftslogik für die Erstellung und Zusammenfassung von Security Incidents für das neue Design enthält. Sie müssen diesen Flow aktivieren, damit das neue Design wirksam wird.
- Die vorhandenen von Anwendern gemeldeten Phishing-Regeln wurden während des Upgrades beibehalten.

Hinweis:
Wenn Sie anwenderdefinierte Aktionen für eingehende E-Mails und anwenderdefinierte Workflows für von Anwendern gemeldete Phishing-Übermittlungen verwenden, müssen Sie sowohl das alte als auch das neue Design auf in Konflikt stehende oder sich überschneidende Funktionalitäten überprüfen.

Vom Anwender gemeldete Details zur Phishing-Erweiterung : Im Folgenden finden Sie die Details der Erweiterung:

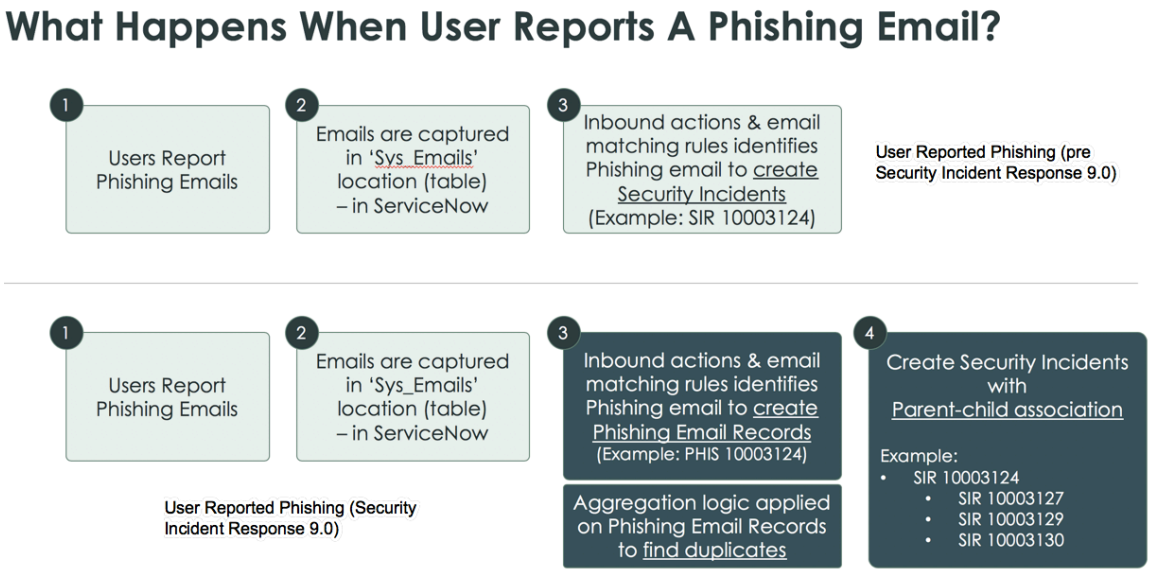
- Phishing-E-Mails auf verschiedene Arten melden: Siehe Erstellen Sie Security Incidents aus vom Anwender gemeldeten Phishing-E-Mails Für Details. Die Phishing-E-Mail wird dann in verschoben `sn_si_Phishing_email` Tabelle.
- Phishing-E-Mail-Datensätze erstellen: Wenn die E-Mail-Übereinstimmungsregeln erfüllt sind (siehe Richten Sie Erfassungsregeln für vom Anwender gemeldetes Phishing ein), **Phishing-E-Mail Erstellen** Mit der eingehenden Aktion wird ein Phishing-E-Mail-Datensatz erstellt. Die analysierten E-Mail-Header werden im cm gespeichert `sn_si_Phishing_email_Header` Tabelle und ist der Phishing-E-Mail als zugehörige Liste zugeordnet.
- Zusammenfassung ähnlicher Phishing-Datensätze in einem einzelnen Security Incident: Der Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents Flow erstellt Security Incidents aus den Phishing-E-Mail-Datensätzen und fasst ähnliche Datensätze in einem einzelnen Incident zusammen. Die Zusammenfassungsbedingungen können nach Bedarf in diesem Flow geändert werden.

Hinweis:

- Die **Vom Anwender Gemeldetes Phishing** Eingehende Aktionen, die vor Release Security Incident Response 9,0 verfügbar sind, sind jetzt deaktiviert. Security Incidents werden nicht mehr über die deaktivierten eingehenden Aktionen erstellt.
- Die Anwendung Security Operations-Spoke muss installiert sein, damit das neue Design wirksam wird. Dies umfasst Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents Flow, der standardmäßig in einem inaktiven Status verfügbar ist. Aktivieren Sie diesen Flow, um Security Incidents aus den Phishing-E-Mail-Datensätzen zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt die Unterschiede zwischen dem alten und dem neuen Design:



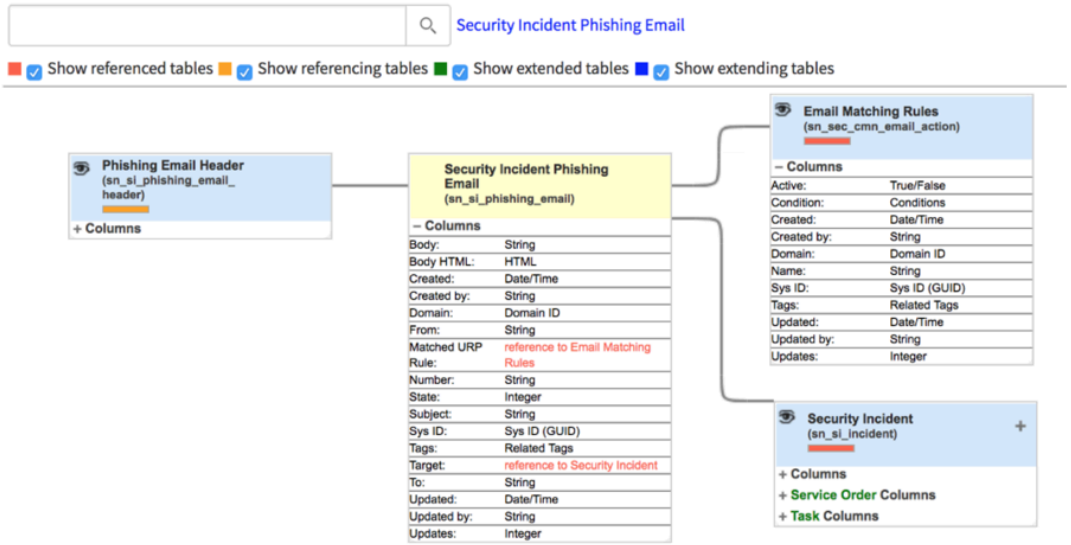
Zur Verwendung der erweiterten Funktion „von Anwendern gemeldete Phishing“ sind die folgenden Plugins und Komponenten erforderlich:

- Sicherheitssupport Allgemein (`sn_sec_cmn`): Enthält:
  - Eingehende Aktion
  - Neues E-Mail-Benutzer-ReportedPhishing-Skript
  - Erfassungsregeltabelle
- Security Incident Response (sn_si): Enthält:
  - Security Incident-Tabelle (sn_si_Incident)
  - Tabelle „Sicherheits-Phishing-E-Mails“ (sn_si_Phishing_email)
  - Tabelle „Sicherheits-Phishing-E-Mail-Header“ (sn_si_Phishing_email_Header)
  - EML-Upload-Datensatzersteller
- Security Operations-Spoke

  Flows und Subflows für die Zusammenfassung von E-Mails und die Umwandlung von Phishing-E-Mails in Security Incidents.

Die folgende Abbildung zeigt die neue Phishing-E-Mail-Tabelle mit Verweisen auf die übereinstimmende URP-Regel und den Ziel-Security Incident-Datensatz (sn_si_Incident).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Richten Sie Erfassungsregeln für vom Anwender gemeldetes Phishing ein

Als Anwender mit `sn_si.admin` Rolle können Sie E-Mail-Übereinstimmungsregeln definieren, um von Anwendern gemeldete Phishing-E-Mails basierend auf bestimmten Kriterien zu filtern. Sie können beispielsweise eine Regel definieren, bei der alle E-Mails entweder direkt oder über die Schaltfläche Phishing melden an gesendet werden `security@acme.com` Werden als vom Anwender gemeldete Phishing-E-Mails kategorisiert.

Vorbereitungen

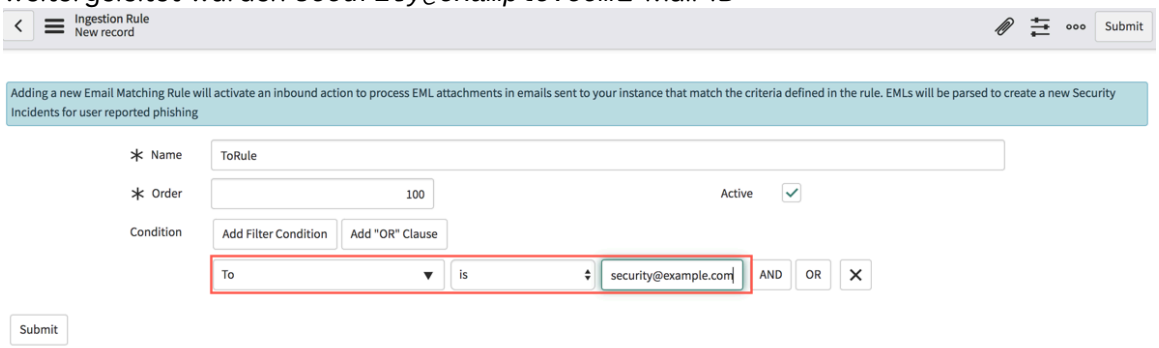
Erforderliche Rolle: sn_si.admin

Prozedur

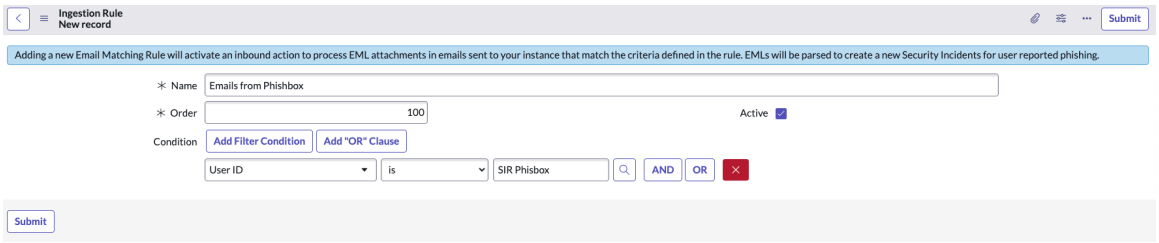
1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Erfassungsregeln – von Anwender gemeldetes Phishing**an.
2. Klicken Sie Auf **Neu** Dient zum Erstellen einer neuen E-Mail-Übereinstimmungsregel.
3. Geben Sie einen Namen ein, und definieren Sie eine oder mehrere Bedingungen für die Regel.
4. Klicken Sie Auf **Übermitteln** Zum Speichern der Regel.
   Im Folgenden finden Sie einige Beispielregeln:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Zu Regel** : Filtern Sie E-Mails, die direkt gesendet oder an weitergeleitet wurden *security@example.com*E-Mail-ID



- **Anwender-ID-Regel**: Filtern Sie E-Mails, die von einer bestimmten E-Mail-ID gesendet wurden



Definieren Sie vom Anwender gemeldete Phishing-Eigenschaften

Definieren Sie die Headerinformationen, die aus vom Anwender gemeldeten Phishing-E-Mails erfasst werden müssen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie diese Optionen, um die folgenden von Anwendern gemeldeten Phishing-Einstellungen zu konfigurieren.

- Konfiguration zum Extrahieren von E-Mail-Kopfzeilen aus dem E-Mail-Text. (**Phishing Melden** Übermittlungen.)
- Filter zum Auswählen von Headern.
- Aktivieren oder deaktivieren Sie die Zuordnung von über- und untergeordneten Elementen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Eigenschaften des vom Anwender gemeldeten Phishing**an.

2. Geben Sie die Konfiguration zum Extrahieren von E-Mail-Headern aus dem E-Mail-Text an:
   - Geben Sie eine Zeichenfolge ein, die den Anfang des E-Mail-Headers identifiziert.
   - Geben Sie eine Zeichenfolge ein, die das Ende des E-Mail-Headers identifiziert.

   Hinweis:
   Wenden Sie diese Einstellungen nur auf Header an, die als Teil des E-Mail-Texts der Phishing-E-Mail erfasst wurden. Beispiel: Wenn **PhishAlarm** Plugin (früher Wombat) wurde mit dem Microsoft Outlook-Client konfiguriert, wenn der Anwender auf klickt **Phishing Melden** Schaltfläche, werden die E-Mail-Header gemäß der hier definierten Konfiguration erfasst. Die Headerinformationen werden nicht erfasst, wenn die Phishing-E-Mail als Anhang weitergeleitet wird.

3. Geben Sie Filter an, um Header zu eliminieren, die für die Untersuchung des Security Incidents nicht erforderlich sind.

   Geben Sie eine kommagetrennte Liste der E-Mail-Header ein, die aus der vom Anwender gemeldeten Phishing-E-Mail erfasst werden müssen. Wenn Sie hier keinen Wert angeben, werden alle Headerinformationen erfasst.

4. Aktivieren oder deaktivieren Sie die Zuordnung von über- und untergeordneten Elementen. Standardmäßig ist **Ja** Option ist aktiviert. Wählen Sie Aus **Ja** Gibt an, dass untergeordnete Security Incidents erstellt werden müssen, wenn vom Anwender gemeldete Phishing-E-Mails aggregiert werden. Wenn Sie auswählen **Nein** , Untergeordnete Security Incidents werden nicht erstellt, aber die vom Anwender gemeldeten Phishing-E-Mails werden dem Security Incident zugeordnet, und der Security Incident-Datensatz wird aktualisiert. Siehe Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents Um weitere Informationen darüber zu erhalten, wie die untergeordneten Security Incidents erstellt werden.

5. Aktivieren oder deaktivieren Sie die Option zum Anzeigen des Phishing-E-Mail-Inhalts im HTML-Format. Standardmäßig ist **Ja** Option ist aktiviert. Wählen Sie Aus **Ja** Zum Anzeigen des Phishing-E-Mail-Inhalts im HTML-Format. Wenn Sie auswählen **Nein** , Der E-Mail-Inhalt im HTML-Format ist in einem Phishing-Datensatz nicht sichtbar.

Phishing-E-Mail-Datensätze, die aus vom Anwender gemeldeten Phishing-E-Mails erstellt wurden

Vom Anwender gemeldete Phishing-E-Mails werden basierend auf den definierten E-Mail-Übereinstimmungsregeln in Security Incidents konvertiert.

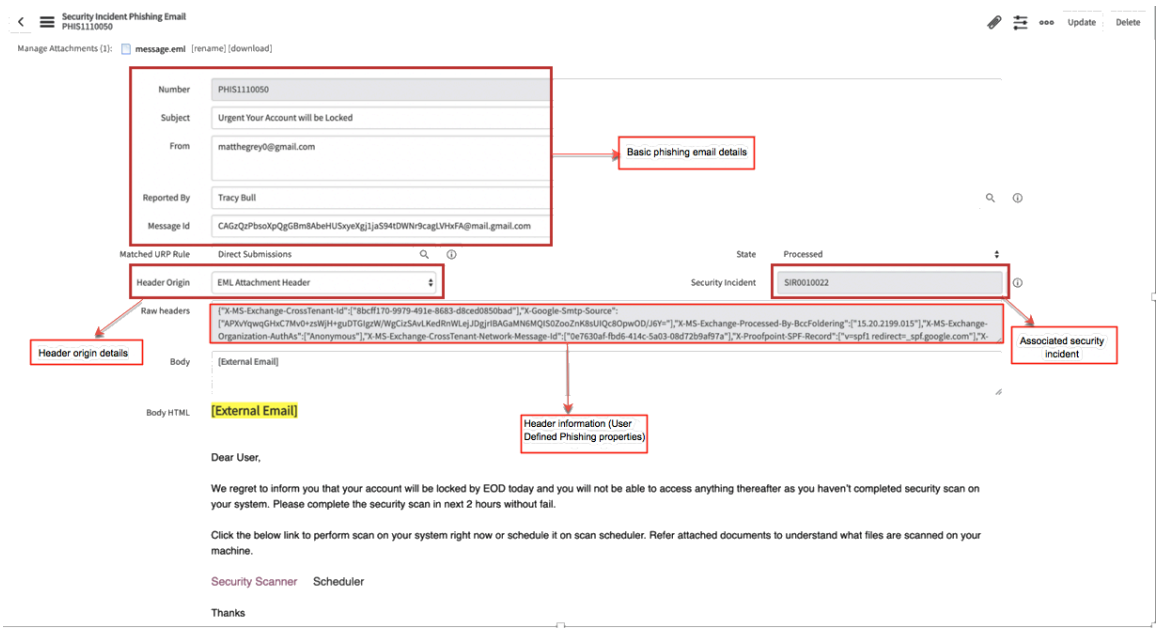
Wenn eine neue Phishing-E-Mail gemeldet wird, werden die folgenden Aktionen ausgeführt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein E-Mail-Datensatz wird in erstellt `sys_email` Tabelle.
- Die **Phishing-E-Mail Erstellen** Die eingehende Aktion wird für den E-Mail-Datensatz ausgeführt und verwendet die E-Mail-Abgleichsregeln (siehe Richten Sie Erfassungsregeln für vom Anwender gemeldetes Phishing ein), um zu bestimmen, ob es sich um eine Phishing-E-Mail handelt.
- Wenn es als Phishing-E-Mail identifiziert wurde, wird ein Phishing-E-Mail-Datensatz in erstellt sn_si_Phishing_email Tabelle.
- Schließlich die Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents Flow wird angewendet, um den Phishing-E-Mail-Datensatz in einen Security Incident zu konvertieren.

Um die E-Mail-Details anzuzeigen, navigieren Sie zu **Security Incident** > **Alle Phishing-E-Mails anzeigen**an. Eine Liste der Phishing-E-Mail-Datensätze wird angezeigt. Klicken Sie auf den Datumslink in der Spalte erstellt, um den E-Mail-Datensatz anzuzeigen.

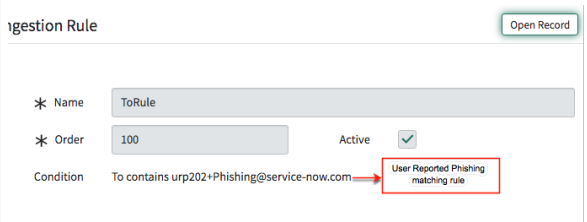


Details Zu Security Incident-Phishing-E-Mail

Feldname	Beschreibung
Anzahl	Die Nummer, die der vom Anwender gemeldeten Phishing-E-Mail zugewiesen ist.
Betreff	Betreff der E-Mail Die Betreffregel ist in simulierten Phishing-Kampagnen oder -Tests nützlich. In diesem Fall senden Organisationen trügerische E-Mails an ihre eigenen Mitarbeiter, um ihre Reaktion auf Phishing- und ähnliche E-Mail-Angriffe zu testen. In simulierten Phishing-E-Mail-Tests, wenn der Microsoft Outlook-E-Mail-Client mit dem **PhishAlarm** Plugin (früher Wombat) wird verwendet. Der Anwender kann auf klicken **Phishing Melden** Schaltfläche zum Melden der Phishing-E-Mail. Die E-Mail wird mit an das Security Operations-Team gesendet **Simuliertes Phishing** An den Betreff der E-Mail angehängt. Dies wird verwendet, um die E-Mail als simulierte Phishing-E-Mail zu identifizieren.

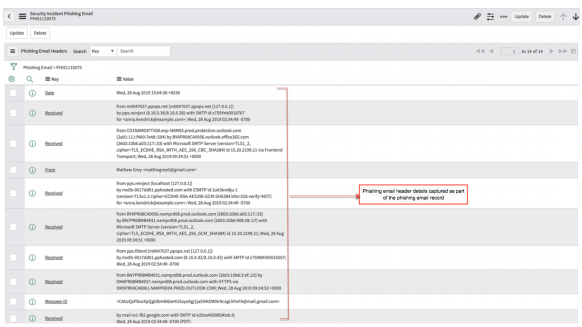
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details Zu Security Incident-Phishing-E-Mail (Fortsetzung)

Feldname	Beschreibung
Von	Die E-Mail-Adresse, von der diese Phishing-E-Mail stammt. Diese Informationen sind verfügbar, wenn die Phishing-E-Mail als EML-Dateianhang weitergeleitet wird oder wenn die ursprünglichen Header in die E-Mail eingebettet sind. Wenn der Anwender die Phishing-E-Mail direkt weitergeleitet hat, ist die Absenderadresse möglicherweise nicht verfügbar.
Gemeldet von	Die E-Mail-ID des Anwenders, der diese Phishing-E-Mail gemeldet hat. Klicken Sie auf **Informationen** Symbol zum Anzeigen zusätzlicher Details.
Nachrichten-ID	Die der Nachricht zugewiesene ID.
Übereinstimmende URP-Regel	Die vom Anwender gemeldete Phishing-Regel, die auf diese E-Mail angewendet werden soll. Klicken Sie auf das Informationssymbol, um zusätzliche Details anzuzeigen.
 Wie Sie in diesem Beispiel sehen können, die **Bedingung** Das Feld zeigt an, dass die ToRule auf diese E-Mail angewendet wird und ein Security Incident erstellt wird. Siehe Richten Sie Erfassungsregeln für vom Anwender gemeldetes Phishing ein Weitere Informationen zum Definieren von E-Mail-Übereinstimmungsregeln.	
Status	Wenn ein neuer Phishing-E-Mail-Datensatz in erstellt wird sn_si_Phishing_email Tabelle, ist das Feld Status auf festgelegt **Neu** . Wenn dieser E-Mail-Datensatz in einen Security Incident konvertiert wird (siehe Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents) Wird das Feld Status auf aktualisiert **Verarbeitet** .
Header-Ursprung	Dieses Feld gibt an, wie die E-Mail-Header stammen oder wie der Anwender die Phishing-E-Mail gemeldet hat: • **E-Mail-Header** : Der Anwender hat die Phishing-E-Mail an das Security Operations-Team weitergeleitet. • **E-Mail-Textkörper:** ○ Der Anwender hat auf geklickt **Phishing Melden** Option (wenn **PhishAlarm** Plugin (früher Wombat) wurde mit dem E-Mail-Client konfiguriert.) ○ Basierend auf der definierten Phishing-Regel „vom Anwender gemeldet“ wird die Phishing-E-Mail an das Security Operations-Team weitergeleitet. • **EML-Anhangsheader** :

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details Zu Security Incident-Phishing-E-Mail (Fortsetzung)

Feldname	Beschreibung
	○ Anhang: Der Anwender hat die E-Mail als Anhang (EML-Datei) weitergeleitet. ○ Servicekatalog-Übermittlung: Der Anwender hat die E-Mail als EML-Datei auf den Desktop heruntergeladen und sie dann an einen angegebenen Speicherort hochgeladen. Der Security Incident wird dann aus der E-Mail erstellt. • **EML-Anhangstext** : ○ Der Anwender hat auf geklickt **Phishing Melden** Option (wenn **PhishAlarm** Plugin (früher Wombat) wurde mit dem E-Mail-Client konfiguriert.) ○ Basierend auf der definierten Phishing-Regel „vom Anwender gemeldet“ wird die Phishing-E-Mail als Anhang an das Security Operations-Team weitergeleitet.
Security Incident	Dieses Feld ist leer, wenn die vom Anwender gemeldete Phishing-E-Mail erstmals gemeldet wird. Wenn Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents Flow wurde ausgeführt. Diese E-Mail wird in einen Security Incident-Datensatz konvertiert, und die Nummer dieses Datensatzes wird hier angezeigt.
Rohe Header	Dieses Feld zeigt die vollständigen Header-Informationen an, die aus der E-Mail extrahiert wurden, wie in definiert Definieren Sie vom Anwender gemeldete Phishing-Eigenschaften Seite. Die Header werden in Schlüssel-Wert-Paare analysiert und in der Liste „Phishing-E-Mail-Header“ angezeigt.
	
Textkörper	Dies ist der Text der vom Anwender gemeldeten Phishing-E-Mail.

Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents

Die **Phishing-E-Mail in Security Incident umwandeln** Flow ist ein neuer Flow, der Phishing-E-Mail-Datensätze in Security Incidents konvertiert oder umwandelt.

Vorbereitungen

Hinweis:

Um die Funktionalität „von Anwendern gemeldetes Phishing“ zu aktivieren, müssen Sie eine Kopie des Flows#und erstellenAktivieren IT. Wenn Sie anwenderdefinierte eingehende Aktionen und anwenderdefinierte Flows erstellt haben, um vom Anwender gemeldete Phishing-Übermittlungen zu verarbeiten, sind hier vorgeschlagene Flow-Änderungen nicht erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erforderliche Rolle: sn_si.admin
- Flow Designer-Spoke muss installiert sein.

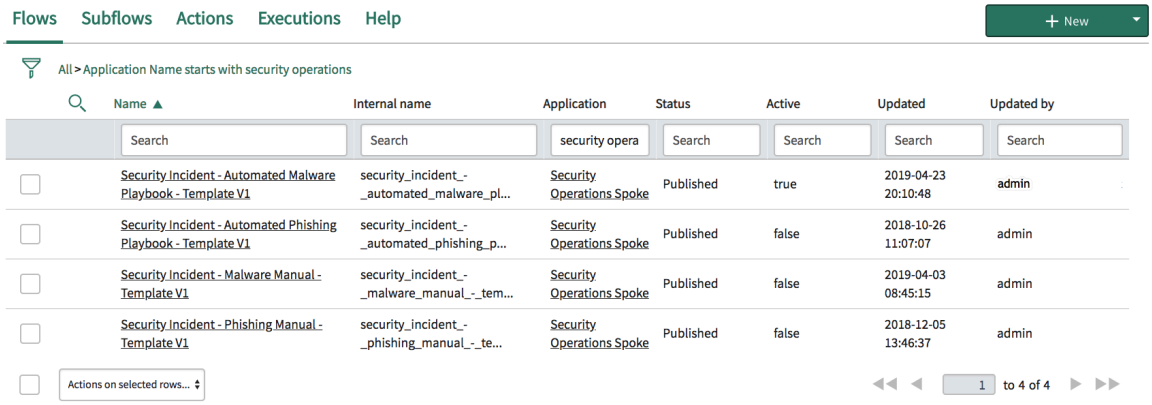
Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird automatisch gestartet, wenn ein Anwender einen Phishing-E-Mail-Datensatz mit dem Status auf gemeldet hat **Neu** Wird erstellt. Dieser Flow enthält die Logik für:

- Aggregieren Sie Security Incidents.
- Aktualisieren Sie Security Incidents mit relevanten Notizen.
- Fügen Sie Headerdaten hinzu.
- Erstellen Sie nach Bedarf untergeordnete Incidents.

Prozedur

- Navigieren zu **Flow Designer** > **Designer** Zum Anzeigen der mit der Security Operations-Spoke verfügbaren Flows.

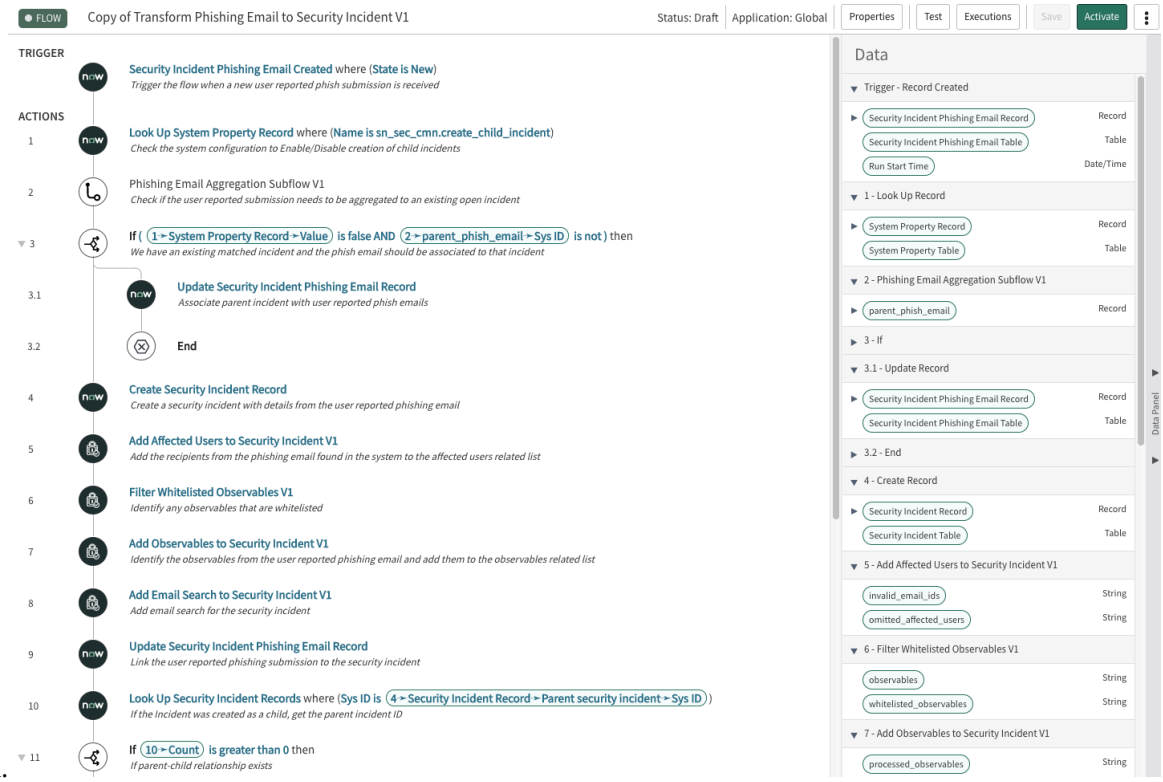


- Klicken Sie auf **Phishing-E-Mails in Security Incidents umwandeln** Link zum Anzeigen des Flows.
- Dieser Flow wird mit dem Basissystem bereitgestellt und befindet sich in **Schreibgeschützt** Modus und kann nicht verwendet werden.

  Klicken Sie auf das Symbol mehr , Erstellen Sie eine Kopie des Flows, und öffnen Sie ihn für Ihre Verwendung. Sie können jetzt Änderungen an Ihrem Flow vornehmen, z. B. Auslöserbedingungen oder -Aktionen ändern oder Aktionen hinzufügen und entfernen. Nachdem Sie die erforderlichen Änderungen vorgenommen haben, müssen Sie aktivieren (siehe

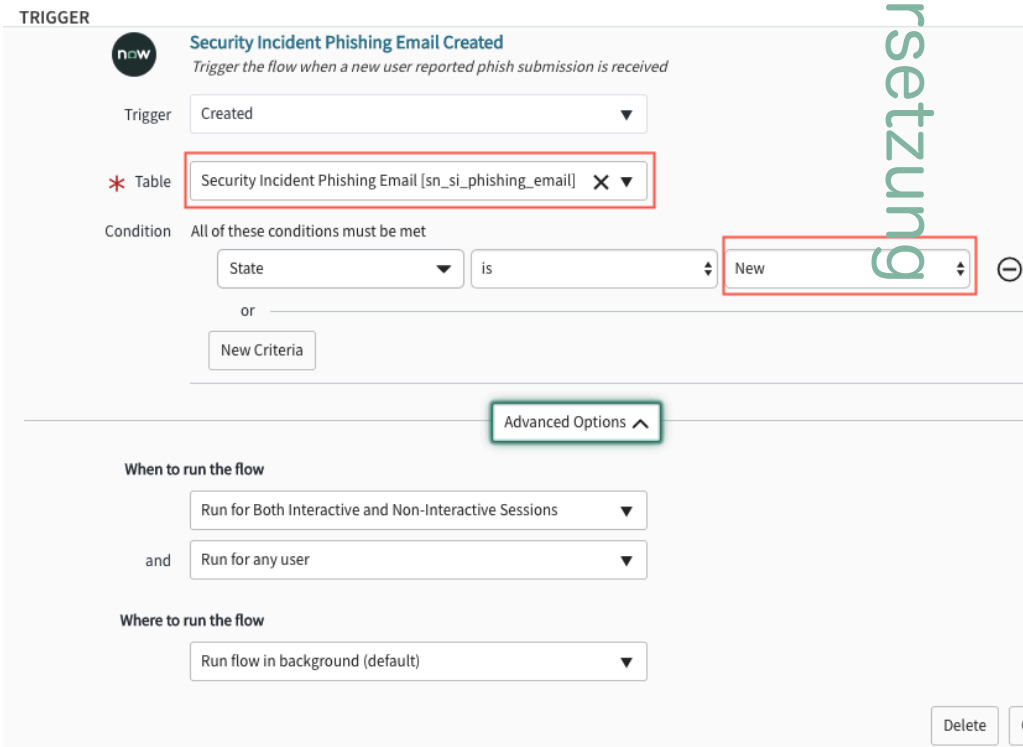
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie einen Security Incident Response Flow) Den Flow, damit er ausgeführt werden kann.



Diese Abbildung zeigt den Auslöser und die mit dem Flow ausgeführten Schritte. Im rechten Bereich wird der Daten-Flow angezeigt. Klicken Sie auf ein Symbol, um den Schritt zu erweitern und die Details anzuzeigen.

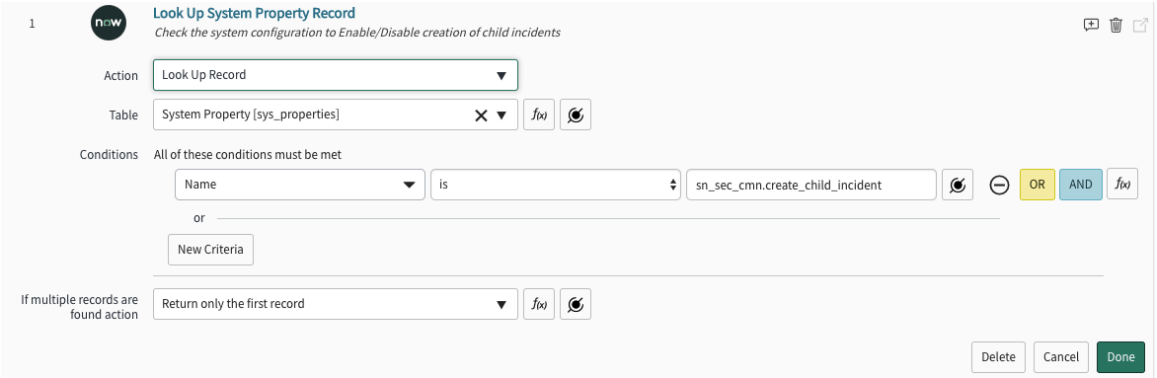
- Klicken Sie auf **Auslöser** Symbol.
  Im ersten Schritt definieren oder legen Sie den Auslöser für den Flow fest. Geben Sie die Bedingungen für den Auslöser und die Aufgabe an, die ausgeführt werden sollen, wenn die Bedingungen erfüllt sind. Dieser Flow wird initiiert, wenn ein **Neu** Datensatz wird in hochgeladen sn_si_Phishing_emailTabelle.



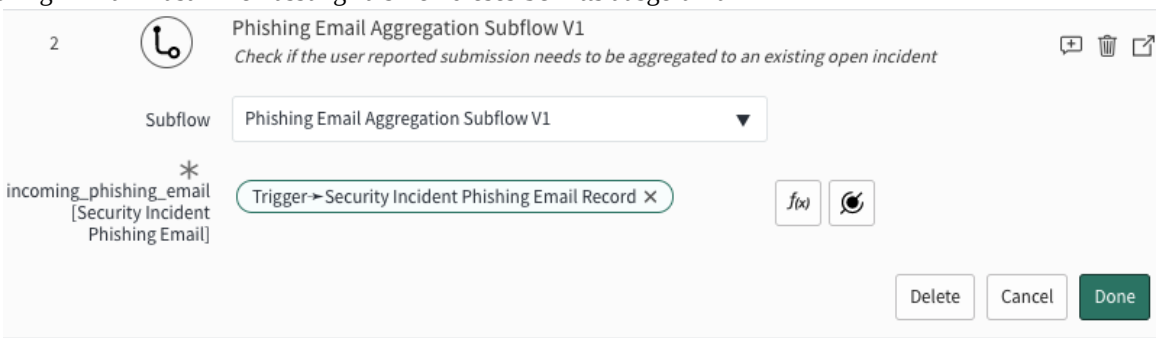
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

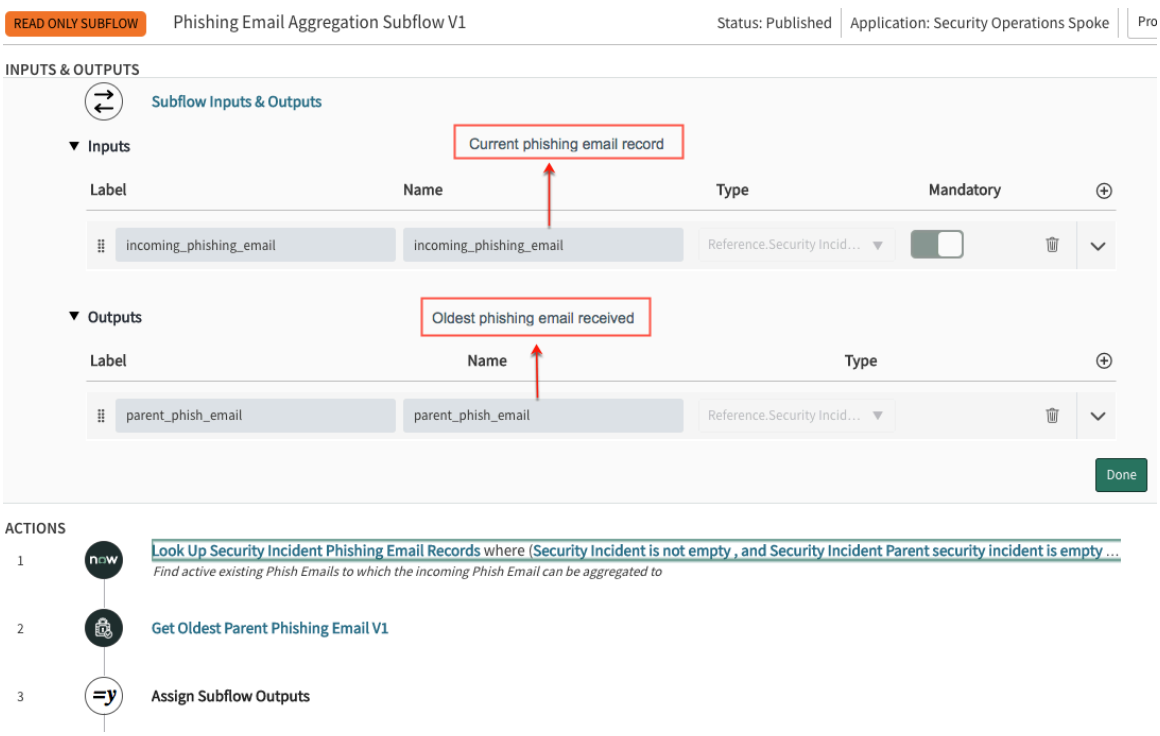
- In Schritt 1 überprüft der Flow, ob der **Untergeordnete Incidents für aggregierte E-Mail-Übermittlungen erstellen?** Kennzeichnung ist in aktiviert oder deaktiviert Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents Seite.



- In Schritt 2 wird der älteste übergeordnete Security Incident identifiziert. Beachten Sie das Symbol in Schritt 2. Dies gibt an, dass der Subflow „Phishing-E-Mail-Zusammenfassung“ als Teil dieses Schritts ausgeführt wird.

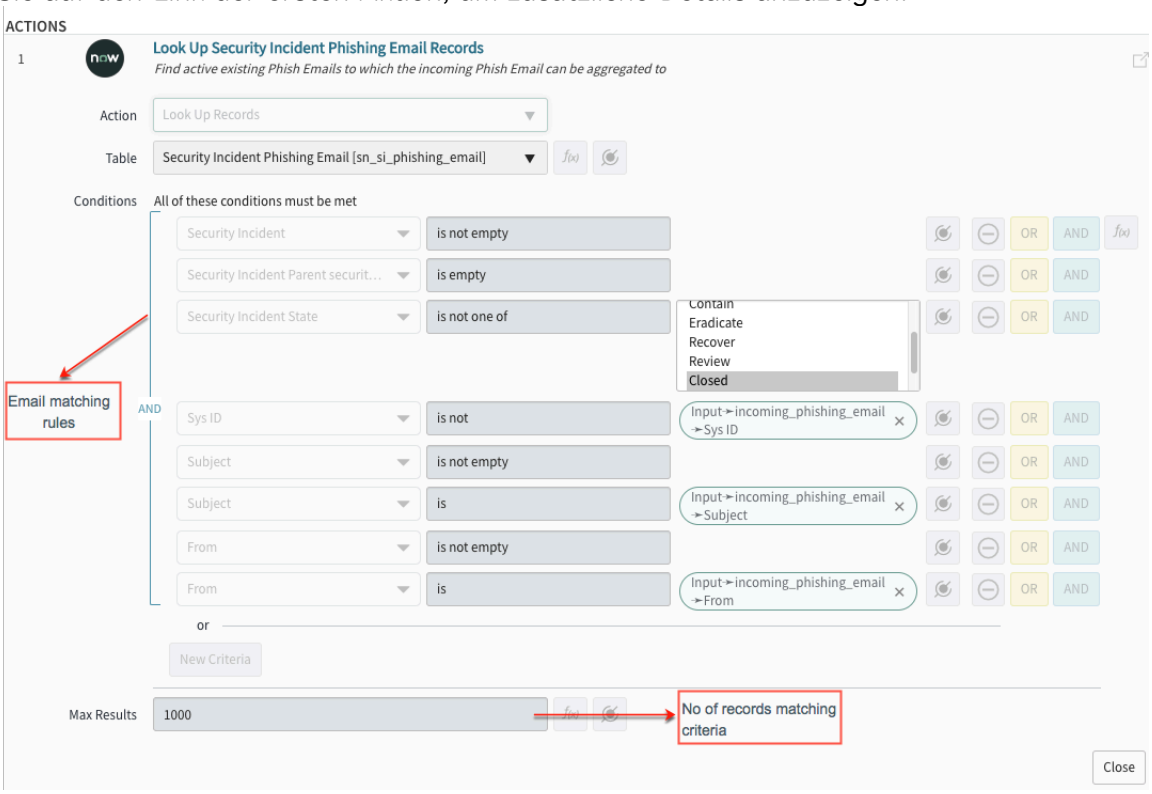


Klicken Sie auf das Aktionsdesigner-Symbol, um eine detaillierte Ansicht der Aktion anzuzeigen. Dieser Subflow überprüft die Phishing-E-Mail und gleicht sie basierend auf den angegebenen Kriterien mit einem vorhandenen Security Incident ab.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese beiden Aktionen werden ausgeführt, wenn dieser Subflow ausgeführt wird. Klicken Sie auf den Link der ersten Aktion, um zusätzliche Details anzuzeigen.



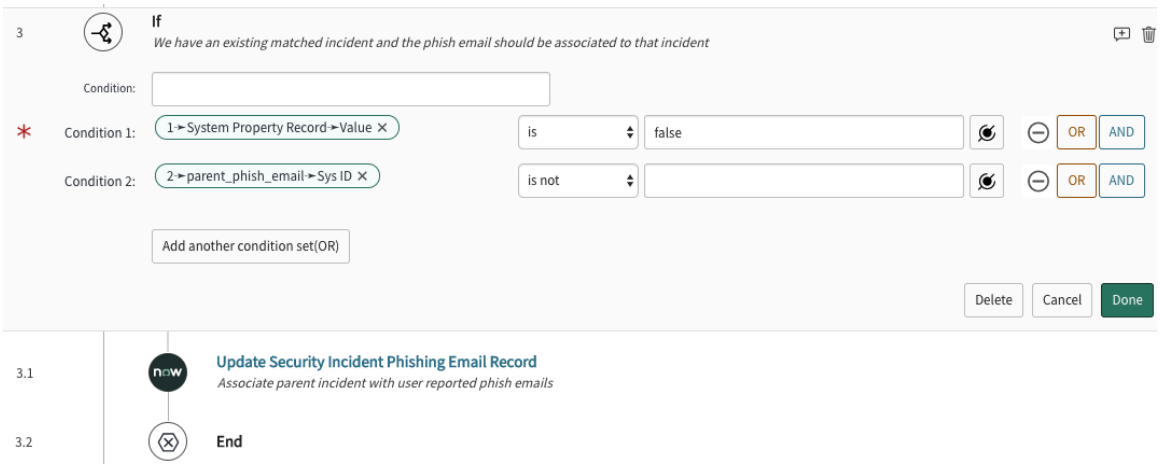
Diese Aktion überprüft die E-Mails, die den Kriterien für die neue eingehende E-Mail entsprechen, basierend auf folgenden Bedingungen:

- Status des Security Incidents ist nicht **Geschlossen** .
- Betreff- oder Absenderwert entsprechen den definierten Bedingungen für E-Mail-Übereinstimmungsregeln (siehe Richten Sie Erfassungsregeln für vom Anwender gemeldetes Phishing ein).

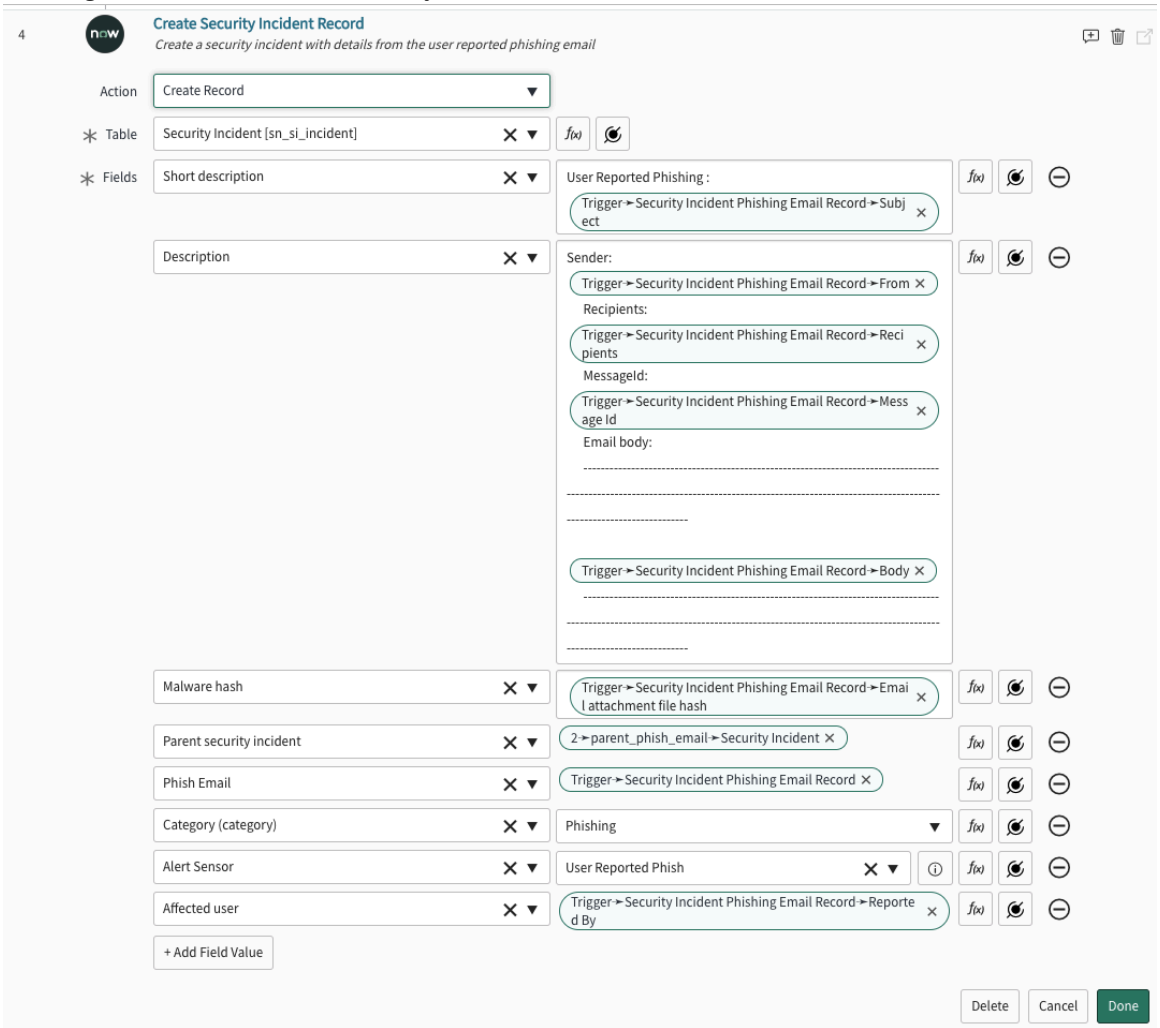
Wenn diese Bedingungen erfüllt sind, wird die Anzahl der Datensätze angezeigt, die den Kriterien im Feld Max. Ergebnisse entsprechen. Der älteste oder erste Datensatz in der Liste wird als übergeordneter Datensatz festgelegt, für den die Security Incidents aggregiert werden.

- Schritt 3 gilt nur, wenn **Untergeordnete Incidents für aggregierte E-Mail-Übermittlungen erstellen?** Kennzeichnung wurde auf festgelegt **Nein** In Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents Seite.
  In diesem Fall wird die Phishing-E-Mail dem Security Incident-Datensatz zugeordnet, und der Flow endet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

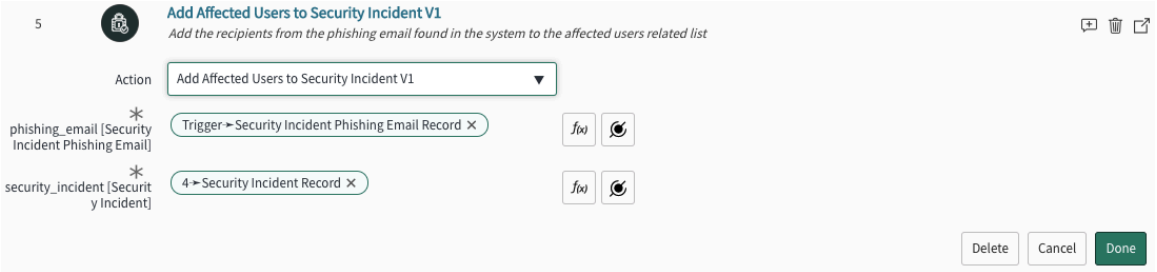


- Wenn **Untergeordnete Incidents für aggregierte E-Mail-Übermittlungen erstellen?** Wurde auf festgelegt **Ja** , Der Flow wird weiterhin ausgeführt, und basierend auf der vom Anwender gemeldeten Phishing-E-Mail wird ein neuer Security Incident erstellt.

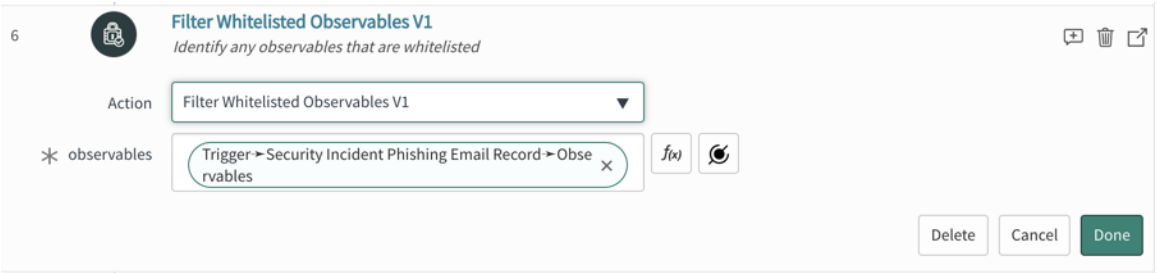


- In Schritt 5 werden Anwender, die die Phishing-E-Mail erhalten haben (Mitarbeiter in den Listen an und CC der Phishing-E-Mail) der zugehörigen Liste Betroffene Anwender im Security Incident-Datensatz hinzugefügt.

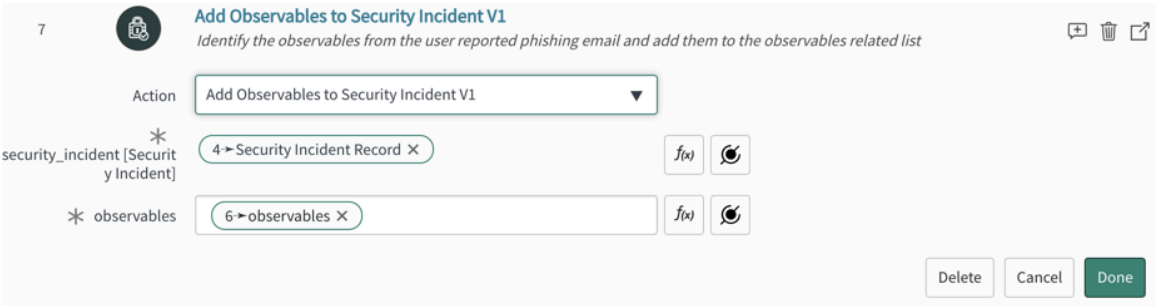
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



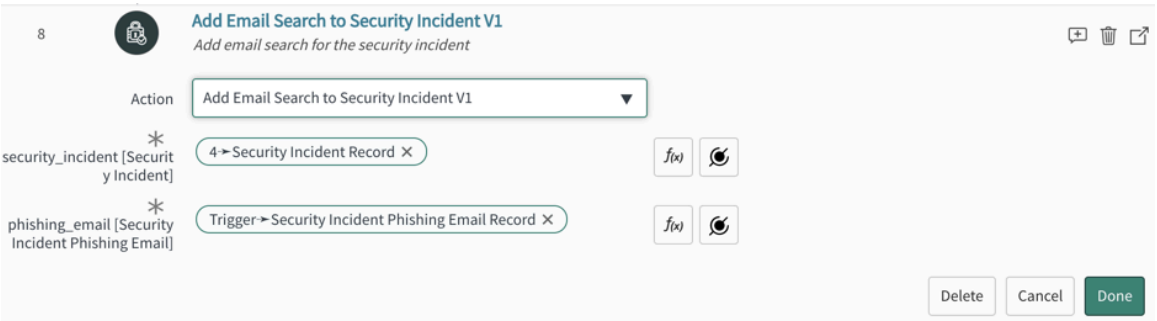
- In Schritt 6 werden erkennbare Elemente mit Allow-Liste aus der Liste der erkennbaren Elemente im Security Incident gefiltert.
  Diese zulässigen erkennbaren Elemente werden dem Security Incident nicht hinzugefügt.



- In Schritt 7 werden unbekannte erkennbare Elemente aus der vom Anwender gemeldeten Phishing-E-Mail identifiziert und der zugehörigen Liste erkennbarer Elemente hinzugefügt.

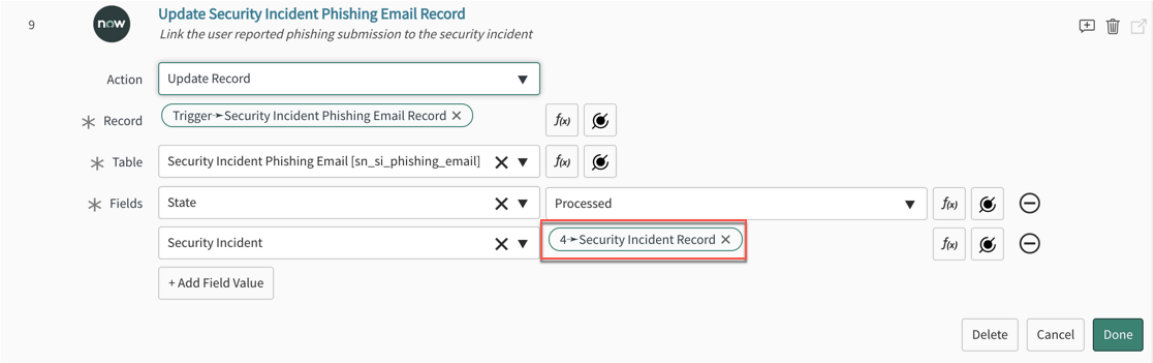


- In Schritt 8 wird eine E-Mail-Suchabfrage generiert, die eine Kombination aus dem Betreff und der Absenderadresse der E-Mail ist.
  Diese Informationen sind nützlich, um die Mitarbeiter in der Organisation zu identifizieren, denen ein Phishing ausgesetzt wurde.

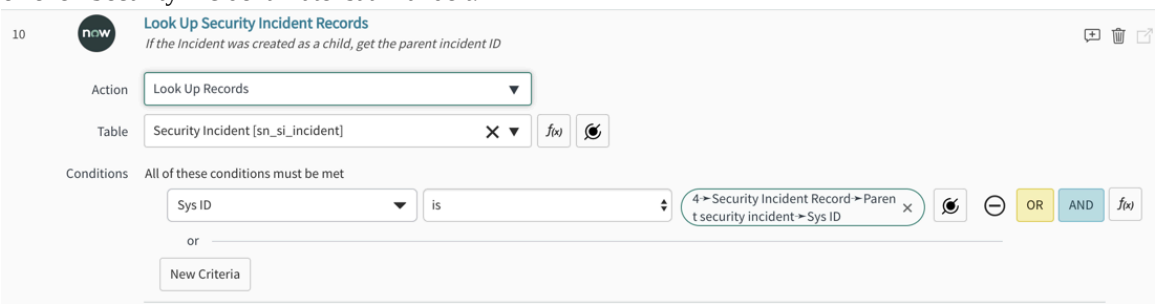


- In Schritt 9 wird die vom Anwender gemeldete Phishing-E-Mail dem Security Incident zugeordnet, und der Security Incident-Datensatz (erstellt in Schritt 4) wird aktualisiert.

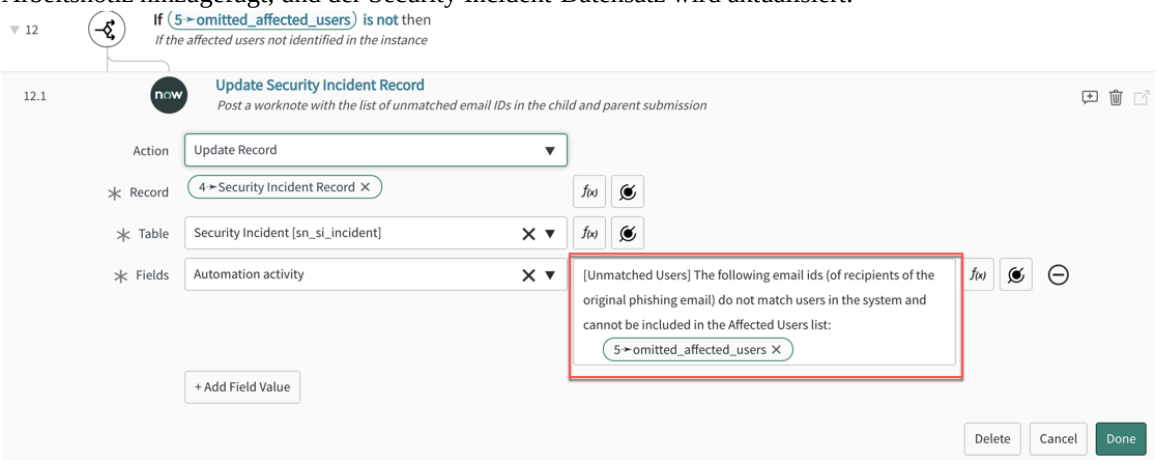
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- In Schritt 10 wird der übergeordnete Security Incident identifiziert, und überprüft, ob es sich um einen offenen Security Incident-Datensatz handelt.

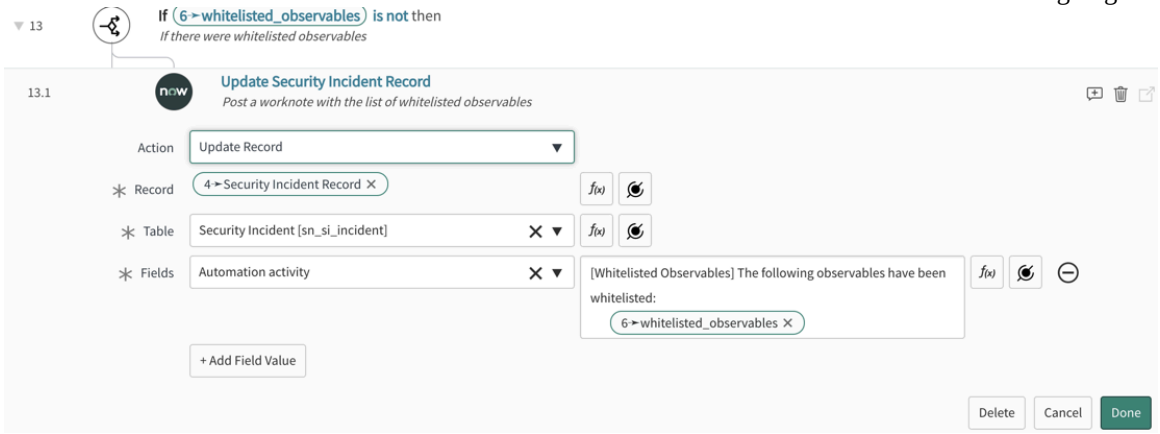


- Wenn die übergeordnete Sicherheit aktiv ist, werden dem untergeordneten Element und den übergeordneten Security Incident-Datensätzen Notizen hinzugefügt, die angeben, wie sie einander zugeordnet sind.
- Wenn in Schritt 12 keine betroffenen Anwender gefunden wurden (in Schritt 5 des Flows), wird eine Arbeitsnotiz hinzugefügt, und der Security Incident-Datensatz wird aktualisiert.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

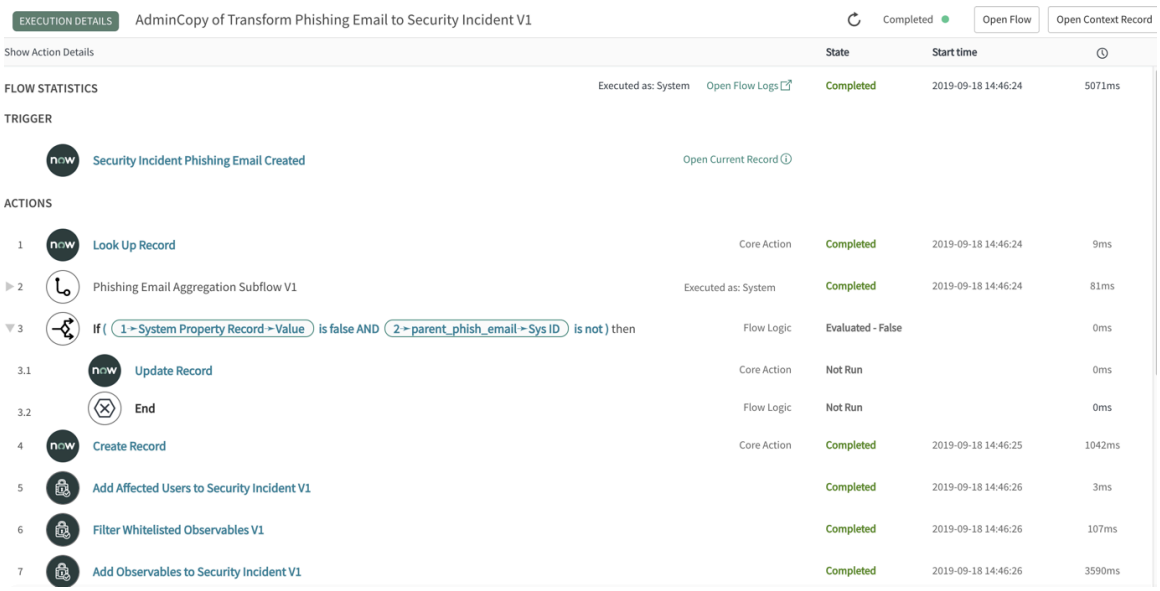
- In Schritt 13 wird eine Arbeitsnotiz mit der Liste der erkennbaren Elemente mit Allow-Liste hinzugefügt.



Nächste Maßnahme

Sie können auf klicken **Testen** Um die Aktionen im Flow zu simulieren, bevor er veröffentlicht wird. Klicken Sie nach dem Testen des Flows auf **Aktivieren** Dient zum Aktivieren des Flows, damit er ausgeführt werden kann.

Klicken Sie Auf **Ausführungen** Zum Anzeigen der Ausführungsdetails des Flows.



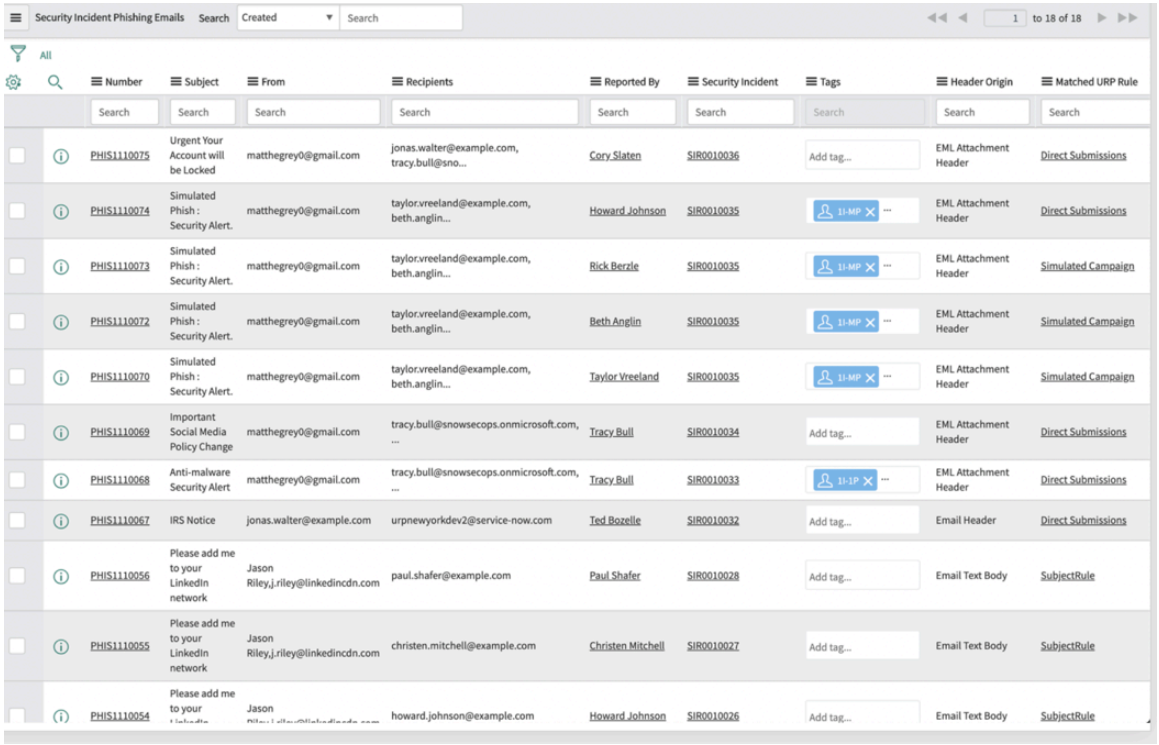
Wenn der Flow ausgeführt wurde, wird der Phishing-E-Mail-Datensatz in einen Security Incident konvertiert. Siehe Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden

Security Incident-Datensätze, die aus Phishing-E-Mail-Datensätzen erstellt wurden

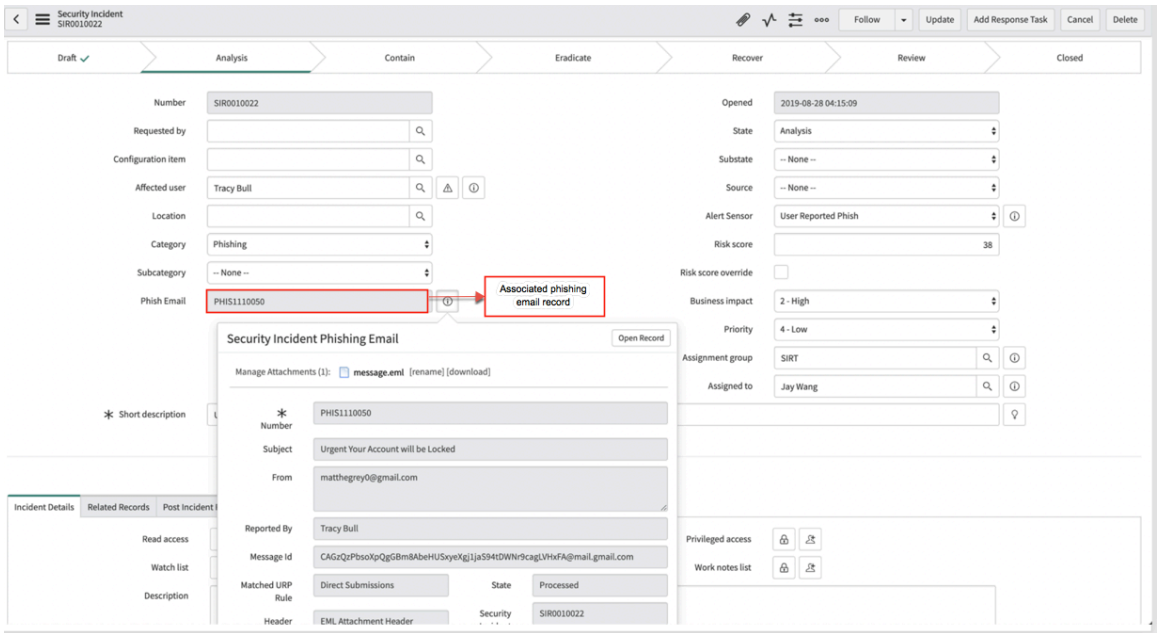
In gespeicherte Phishing-E-Mail-Datensätze `sn_si_Phishing_email` Tabellen werden in Security Incident-Datensätze konvertiert.

Um den Security Incident anzuzeigen, der dem Phishing-E-Mail-Datensatz zugeordnet ist, klicken Sie auf **Security Incident** > **Phishing-E-Mail** > **Alle Phishing-E-Mails anzeigen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Klicken Sie auf den Link in der Spalte Security Incident, der dem Phishing-E-Mail-Datensatz zugeordnet ist. Die Security Incident-Details werden angezeigt.



Zugehörige Listen

Scrollen Sie nach unten zum Abschnitt zugehörige Links des Security Incidents, und klicken Sie auf **Alle zugehörigen Listen anzeigen** . Zeigen Sie Details wie untergeordnete Security Incidents, betroffene Anwender und zugehörige Phishing-E-Mails an.

Untergeordnete Security Incidents

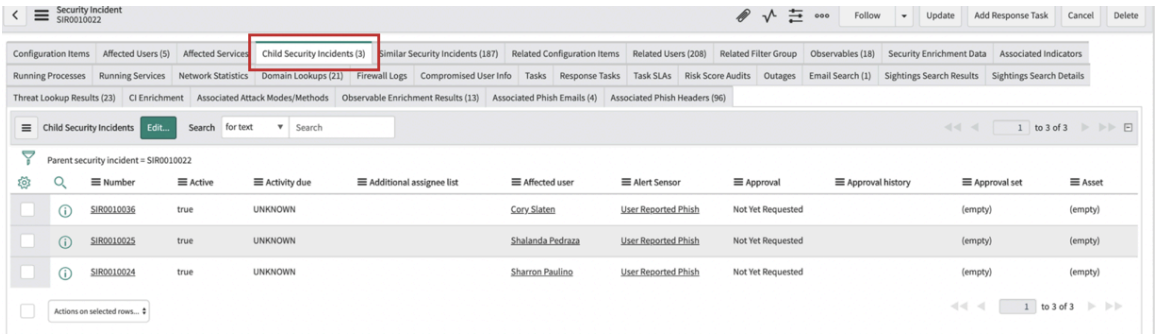
Klicken Sie auf **Untergeordnete Security Incidents** Registerkarte. Sie können eine Liste der untergeordneten Security Incidents anzeigen, die dem übergeordneten Security Incident zugeordnet sind, basierend auf der angewendeten Zusammenfassungslogik. Für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

jeden hinzugefügten untergeordneten Datensatz wird dem übergeordneten Datensatz eine automatisierte Systemaktivität (im Abschnitt Arbeitsnotiz) hinzugefügt. Dadurch wird der Sicherheitsanalyst über den zusammengefassten untergeordneten Datensatz benachrichtigt.

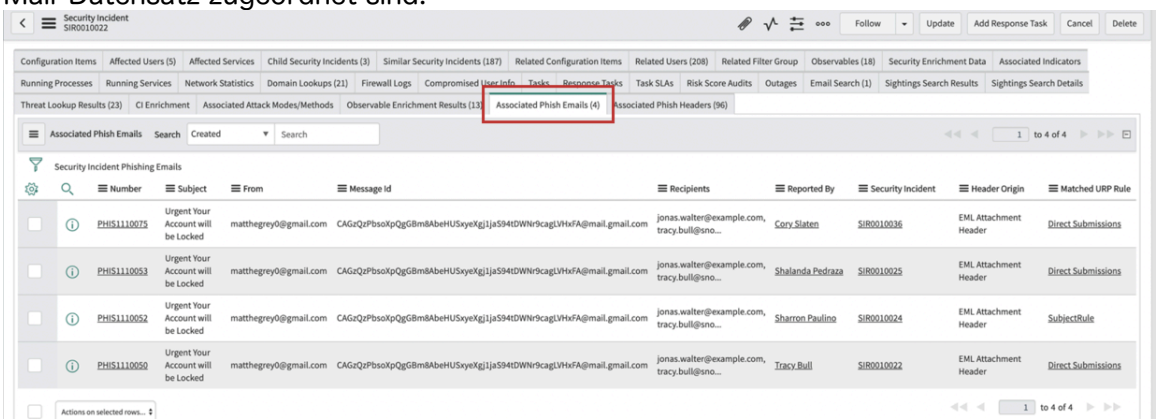
Hinweis:

Sie können die untergeordneten Security Incidents hier nur anzeigen, wenn die **Erstellen Sie untergeordnete Incidents für aggregierte E-Mail-Übermittlungen** Kennzeichnung ist auf festgelegt **Ja** Auf der Seite „vom Anwender gemeldete Phishing-Eigenschaften“. Details siehe Definieren Sie vom Anwender gemeldete Phishing-Eigenschaften.



Zugehörige Phishing-E-Mails

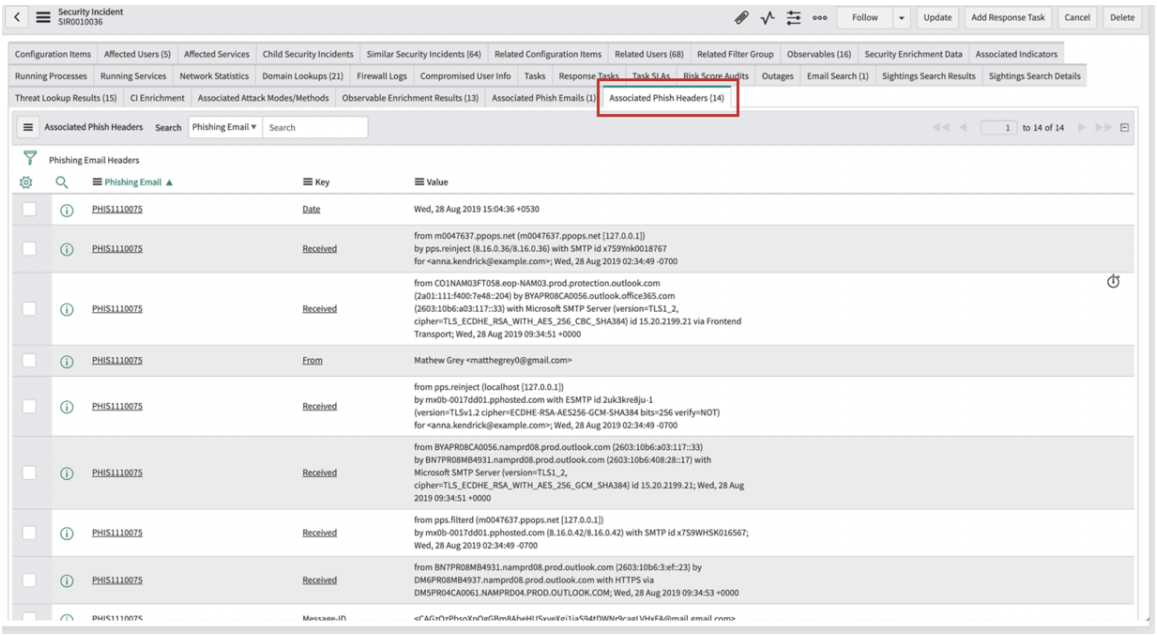
Klicken Sie auf **Zugehörige Phishing-E-Mails** Registerkarte. Sie sehen eine Liste der Phishing-E-Mail-Datensätze (doppelte Datensätze), die dem übergeordneten Phishing-E-Mail-Datensatz zugeordnet sind.



Zugeordnete Phishing-E-Mail-Header

Klicken Sie auf **Zugehörige Phishing-E-Mails** Registerkarte. Sie sehen die Phishing-E-Mail-Header-Details, die als Teil des Security Incidents erfasst wurden. Sie können die Rollup-Header aller untergeordneten Datensätze und Phishing-E-Mail-Datensätze anzeigen, die zum übergeordneten Security Incident aggregiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

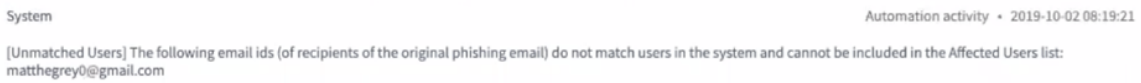


Zulässige Liste erkennbarer Elemente

Als Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents Flow wird ausgeführt. Sie können den Status des Security Incidents überwachen. Wenn bestimmte erkennbare Elemente als zulässige erkennbare Elemente markiert sind, werden sie nicht der zugehörigen Liste erkennbarer Elemente hinzugefügt. Durch Markieren der erkennbaren Elemente in der Allow-Liste können Sie sicherstellen, dass nur die wichtigen Details angezeigt werden. Beispiel: Wenn www.google.com Ist eine der URLs, die als zulässige Liste markiert wurde, wird die folgende Systemnachricht angezeigt. Zulässige Listen erkennbarer Elemente stellen sicher, dass nur die wichtigen erkennbaren Elemente überwacht werden.

Erfassung nicht abgeglichener Anwender

Einige E-Mail-IDs in den Listen an und CC der Phishing-E-Mail gehören möglicherweise nicht zu Anwendern in der Organisation. Diese E-Mail-IDs werden als nicht übereinstimmende Anwender kategorisiert und sind nicht in der zugehörigen Liste „Betroffene Anwender“ enthalten. Eine Arbeitsnotiz, die angibt, dass dies nicht übereinstimmende Anwender sind, wird angezeigt.

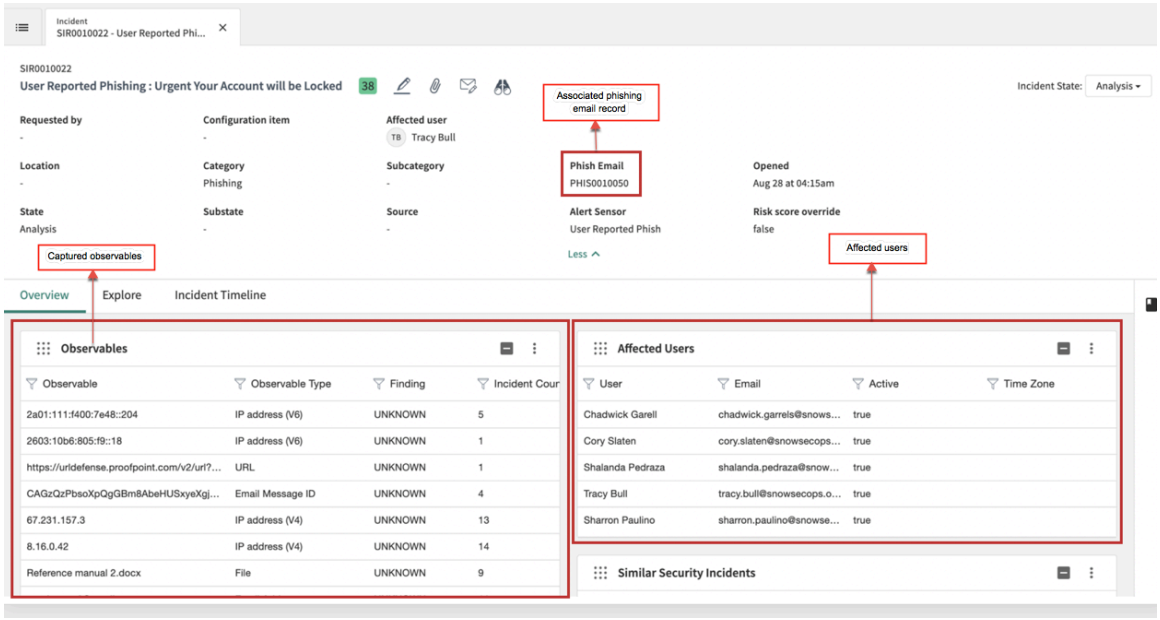


Anwender hat Phishing im Arbeitsbereich des Sicherheitsanalysten gemeldet

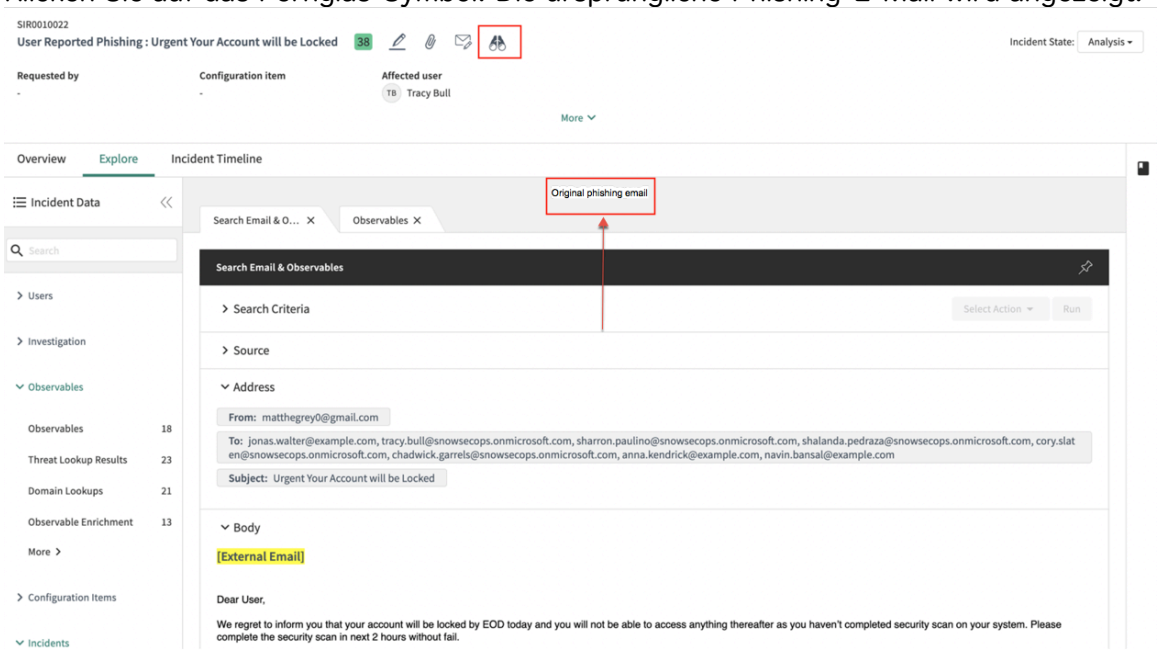
Sie können Security Incidents anzeigen, die den Phishing-E-Mail-Datensätzen im Arbeitsbereich des Sicherheitsanalysten zugeordnet sind.

Navigieren zu **Security Incident** > **Neue UI**an. Der Arbeitsbereich wird in einer separaten Browserregisterkarte geöffnet. Klicken Sie auf den Security Incident, der dem Phishing-E-Mail-Datensatz zugeordnet ist, um den Security Incident anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

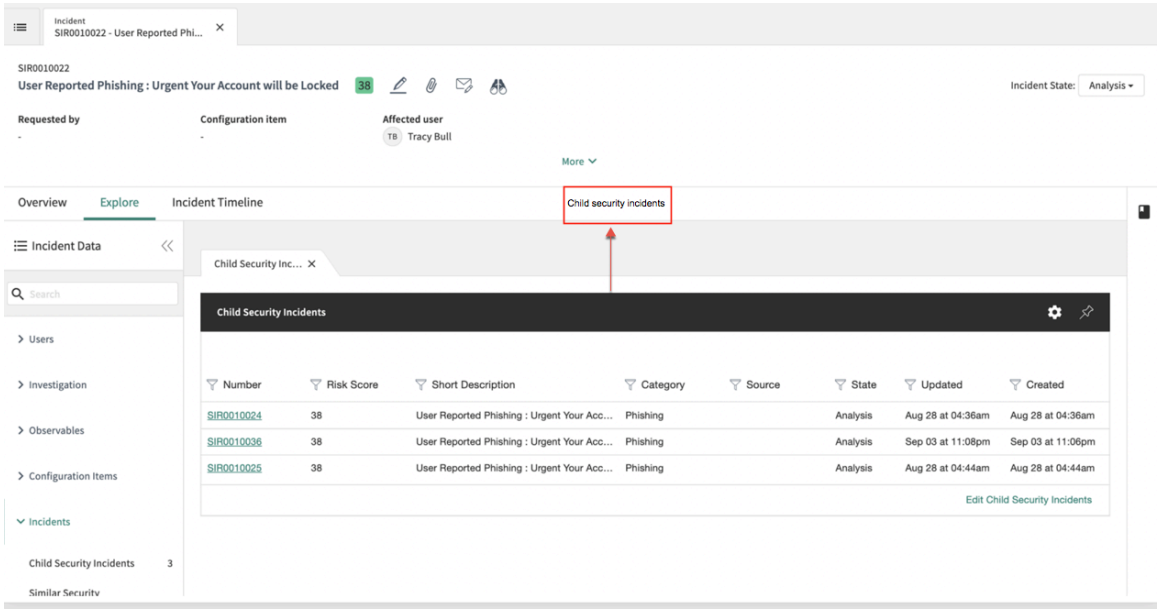


Klicken Sie auf das Fernglas-Symbol. Die ursprüngliche Phishing-E-Mail wird angezeigt.

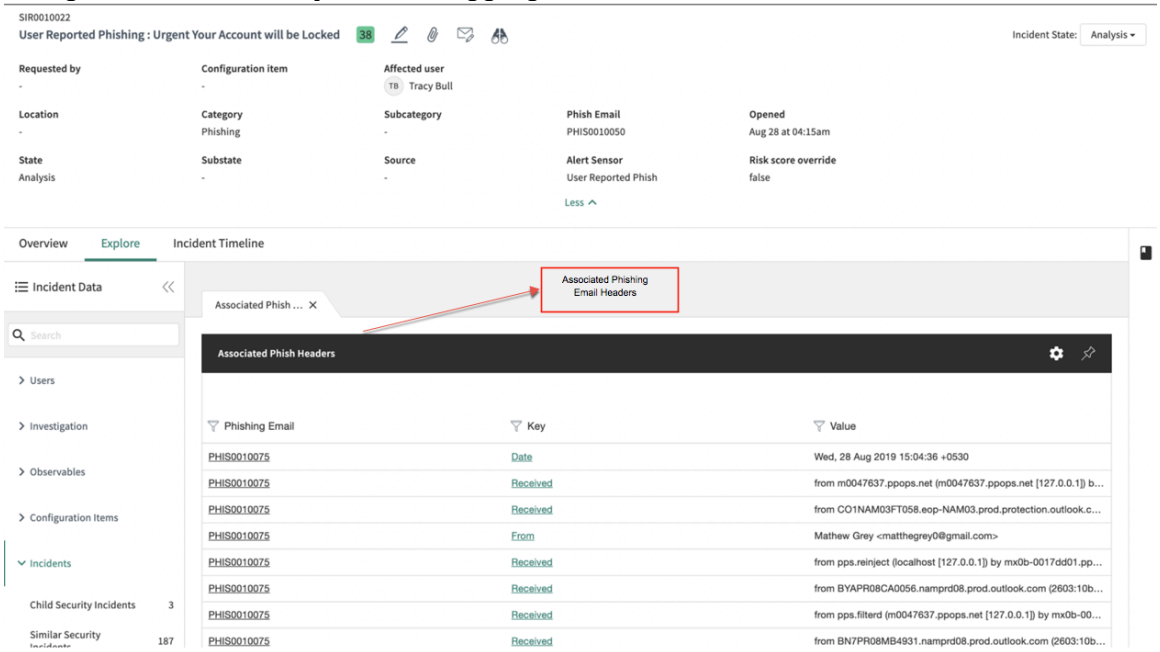


In **Erkunden** Klicken Sie auf die Registerkarte **Incidents** > **Untergeordnete Security Incidents**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

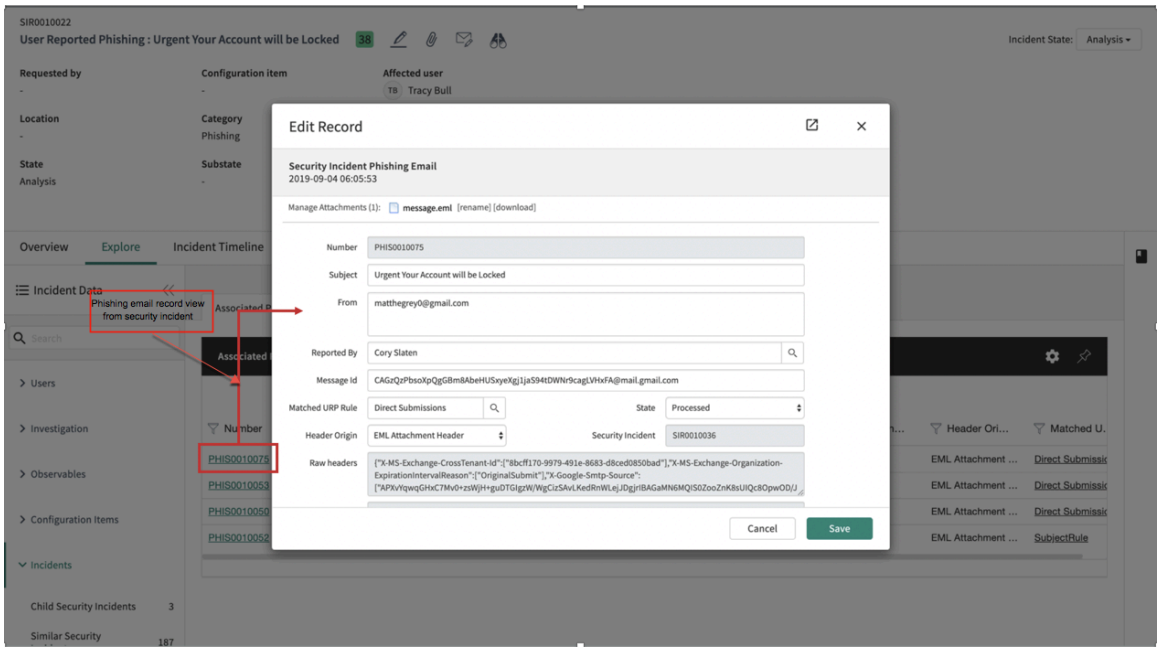


Klicken **Incidents** > **Zugehörige Phishing-Header** > an. Sie können die Rollup-Header aller untergeordneten Datensätze und Phishing-E-Mail-Datensätze anzeigen, die zum übergeordneten Security Incident aggregiert sind.

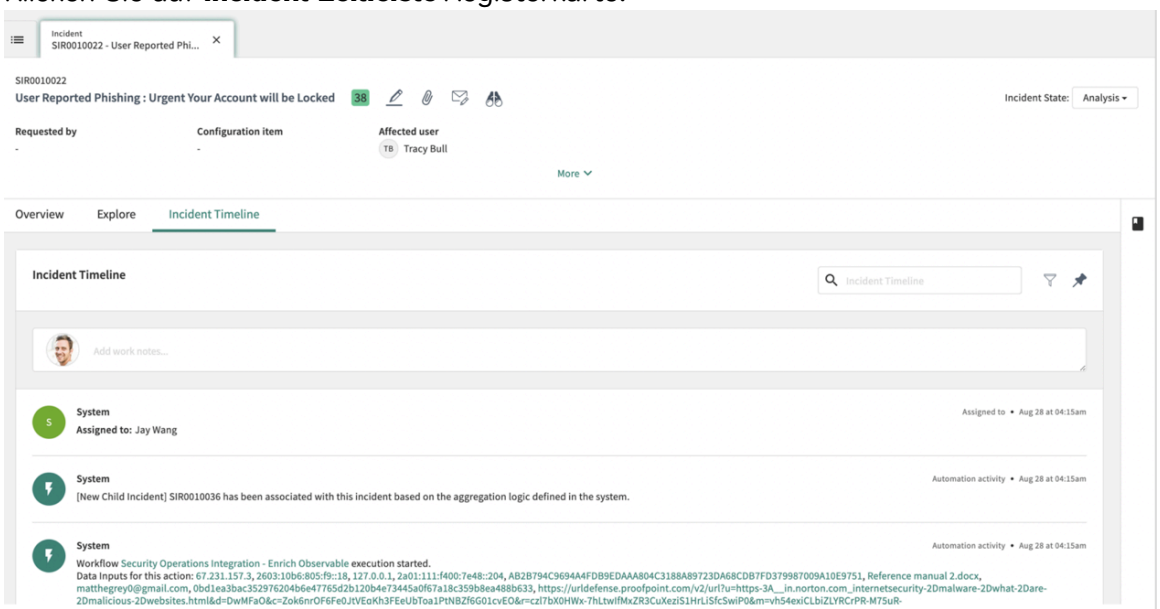


Klicken Sie auf den Phishing-E-Mail-Link, um den Phishing-E-Mail-Datensatz anzuzeigen, der dem Security Incident zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Klicken Sie auf **Incident-Zeitleiste** Registerkarte.



Sie können die Systemupdates anzeigen, die Folgendes hervorheben:

- Doppelte untergeordnete Datensätze identifiziert.
- Zulässige Liste erkennbarer Elemente.
- Nicht übereinstimmende Anwender, die die Phishing-E-Mail erhalten haben, aber nicht zur Liste „Betroffene Anwender“ gehören.

Häufige Fragen

In diesem Abschnitt werden einige der häufig gestellten Fragen zur erweiterten Funktion „von Anwendern gemeldete Phishing“ behandelt.

1. Ich habe die neue Security Incident Response-Spoke installiert, kann jedoch keine von Anwendern gemeldeten Phishing-Incidents anzeigen.

   Standardmäßig wurde die Phishing-Funktionalität „vom Anwender gemeldet“ deaktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um diese Funktion zu aktivieren, müssen Sie eine Kopie des schreibgeschützten erstellen Transformieren Sie vom Anwender gemeldete Phishing-E-Mails in Security Incidents Führen Sie einen Flow durch, und aktivieren Sie ihn vor der Verwendung.

2. Welche Vorsichtsmaßnahmen werden beim Erfassen von Phishing-E-Mails und ihrer Umwandlung in Security Incidents verwendet, um schädliche Links und Anhänge in den Phishing-E-Mails zu behandeln?

   Die ServiceNow Der Antivirus-Scanner scannt solche schädlichen Anhänge und Links. Um jedoch sicherzustellen, dass Sicherheitsanalysten die Incidents genau untersuchen können, ist die Security Incident Response Die Anwendung erfasst alle Artefakte, die Teil einer Phishing-E-Mail sind. Die Phishing-Funktionalität „vom Anwender gemeldet“ schaltet die schädlichen Links in der Phishing-E-Mail jedoch stummgeschaltet, damit Sicherheitsanalysten nicht versehentlich auf diese Links klicken. In Bezug auf schädliche Anhänge müssen Sicherheitsanalysten beim Herunterladen vorsichtig sein.

3. Erfassen wir alle schädlichen Dateien, die Teil der Phishing-E-Mails sind, zur Ergänzung von Security Incidents?

   Ja, wir erfassen alle Dateien aus den Phishing-E-Mails. Sie können diese Details anzeigen, die als Teil erkennbarer Security Incident-Elemente in Form eines Datei-Hash verfügbar sind.

4. Senden wir schädliche Dateien und Links aus Phishing-E-Mails zur Untersuchung an eine Sandbox-Instanz?

   Derzeit unterstützen wir keine sofort einsatzbereiten Sandbox-Integrationen zur Untersuchung schädlicher Dateien und Links.

5. Gibt es ein Zeitfenster oder einen Auslöser, der die Dauer definiert, in der eingehende doppelte Phishing-E-Mail-Datensätze einem übergeordneten Security Incident zugeordnet werden?

   Doppelte Phishing-E-Mail-Datensätze werden nur zu einem aktiven übergeordneten Security Incident zusammengefasst. Wenn der übergeordnete Incident geschlossen oder abgebrochen wird, wird die eingehende neue doppelte Phishing-E-Mail als neuer Security Incident erstellt. In diesem Szenario können Sie jedoch innerhalb des neuen Security Incidents den geschlossenen oder abgebrochenen übergeordneten Security Incident in anzeigen **Ähnlicher Security Incident** Zugehörige Liste.

   Hinweis:
   Dieses Verhalten kann mit dem Flow Designer konfiguriert werden.

6. Unterstützt die Phishing-Funktion für Anwenderberichte nur die Verwendung von Microsoft Outlook **PhishAlarm** Plugin (früher Wombat) zum Erfassen von E-Mail-Header-Details?

   Die vom Anwender gemeldete Funktionalität wurde entwickelt, um E-Mail-Header zu analysieren und entspricht den RFC822-Standards. Also ähnlich wie **PhishAlarm** Plugin (früher Wombat), alle anderen Microsoft Outlook-Plugins, die E-Mail-Header basierend auf RFC822-Standards erfassen, werden unterstützt.

Datensatzerstellung aus Security Incidents

Nachdem Sie einen Security Incident erstellt und gespeichert haben, können Sie daraus einen Change Request (CHG), einen Incident (INC) oder einen Problem (PRB)-Datensatz erstellen. Sie können auch einen Kundenservicefall aus jedem Security Incident erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Change, einen Incident oder ein Problem aus einem Security Incident

Nachdem Sie einen Security Incident erstellt und gespeichert haben, können Sie daraus einen Change Request (CHG), einen Incident (INC) oder einen Problem (PRB)-Datensatz erstellen.

Vorbereitungen

Erforderliche Rolle: sn.si_Basic oder höher

Prozedur

1. Öffnen Sie einen Security Incident mit einer dieser Methoden.
   - Öffnen Sie einen auslaufenden Security Incident, indem Sie zu navigieren **Security Incident** > **Nicht zugewiesen** > **Incidents**, Und klicken Sie auf einen Security Incident.
   - Erstellen Sie einen Security Incident, indem Sie zu navigieren **Security Incident** > **Nicht zugewiesen** > **Incidents**, Klicken Sie auf **Neu** , Füllen Sie das Formular aus, und speichern Sie den Datensatz.
2. Klicken Sie mit der rechten Maustaste in die Header-Leiste des Security Incidents, und klicken Sie auf eine der folgenden Optionen:
   - **Change erstellen**
   - **Incident erstellen**
   - **Problem erstellen**

   Hinweis:
   Diese Auswahl gilt nur, wenn die Popup-Eigenschaft (sn_vul.Popup) aktiviert ist. Wenn Sie auf eine dieser Schaltflächen klicken, wird ein Vorschaufenster geöffnet, in dem Sie die Informationen aus dem Security Incident anzeigen, der zum Erstellen des Change, Incidents oder Problems verwendet wird. Das heißt das Konfigurationselement, sein Standort, seine Priorität und die kurzen und langen Beschreibungen. Wenn Sie eine Change-Anforderung erstellen, können Sie bearbeiten **Priorität** , **Kurzbeschreibung** , Und **Beschreibung** Felder. Wenn Sie einen Incident erstellen, können Sie bearbeiten **Auswirkung** , **Dringlichkeit** , **Kurzbeschreibung** Und **Beschreibung** Felder. Die Felder im Bildschirm „zugehöriger Security Incident“ sind nicht betroffen.
3. Klicken Sie Auf **Übermitteln** Um den Change, den Incident oder das Problem zu erstellen.

Erstellt einen Kundenservicefall aus einem Security Incident

Security Incident Response Wird mit einer Standardfeldzuordnung geliefert, die einen Security Incident einem zugeordnet Kundenservice(CS) Fall. Sie können einen CS-Fall aus jedem Security Incident erstellen und bearbeiten **Priorität** , Und fügen Sie auch hinzu **Optionale Notizen** .

Vorbereitungen

Erforderliche Rolle: sn_si.Basic und sn_customerservice_Agent

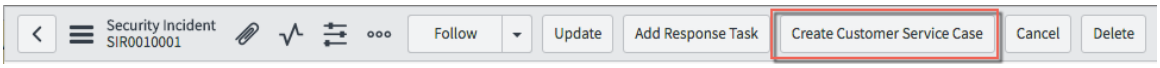
Hinweis:
Die Kundenservice Plugin muss aktiviert sein, um diese Aufgabe auszuführen.

Prozedur

1. Navigieren Sie zu **Security Incident** .
2. Öffnen Sie den Security Incident, dem Sie einen CS-Fall hinzufügen möchten.
3. Klicken Sie Auf **Erstellen Sie Einen Kundenservicefall** Im oberen Header.

Automatische Übersetzung

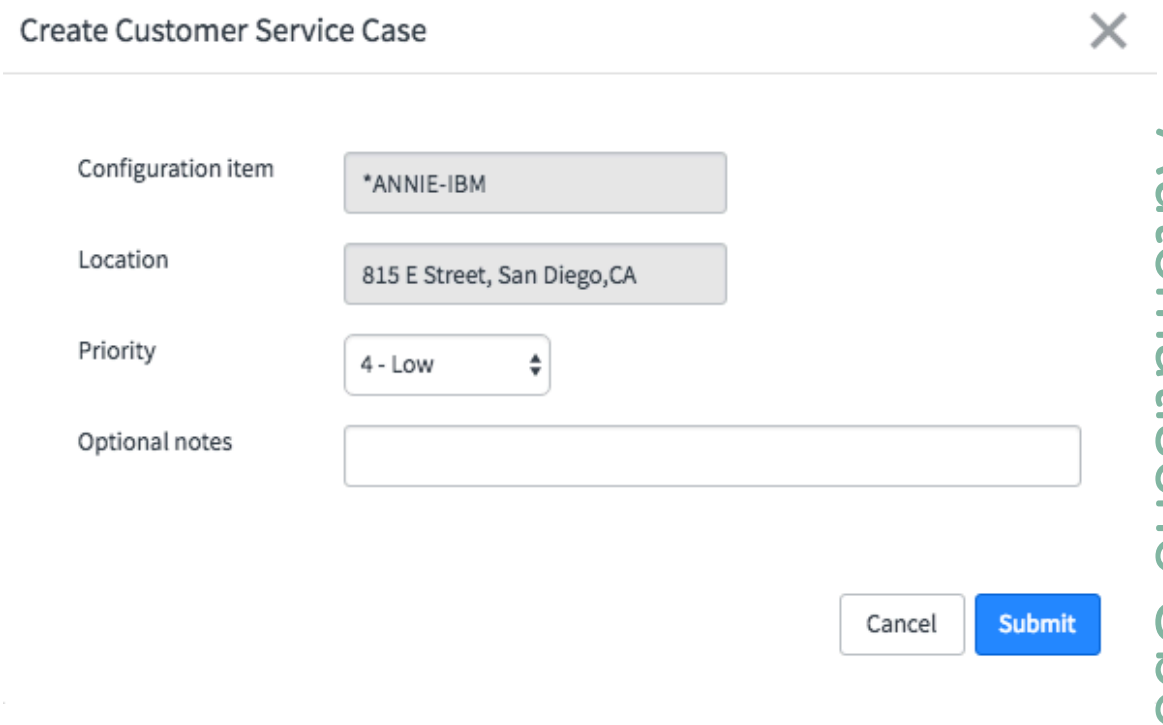
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Popup-Fenster wird basierend auf Ihrer Feldzuordnung mit Informationen aus dem Security Incident gefüllt.

4. Sie können einen neuen auswählen **Priorität** Und fügen Sie beliebige hinzu **Optionale Notizen** .

Hinweis:
Die **Priorität** Feld überschreibt die Standardeinstellung. Die **Optionale Notizen** Werden an den Incident angehängt.



5. Klicken Sie auf **Absenden**.
Ein CS-Fall wird erstellt und in der zugehörigen Liste Kundenservicefälle im Security Incident angezeigt.
6. Sie können auf den Link CS-Fall klicken, um den Fall nachzuverfolgen.

Zugehörige Informationen

Kundenservice-Fallmanagement

Fügen Sie einem Sicherheitsfall einen Security Incident hinzu

Wenn Sie feststellen, dass ein Security Incident eine höhere Analyseebene erfordert, fügen Sie ihn einem neuen oder vorhandenen Fall hinzu.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

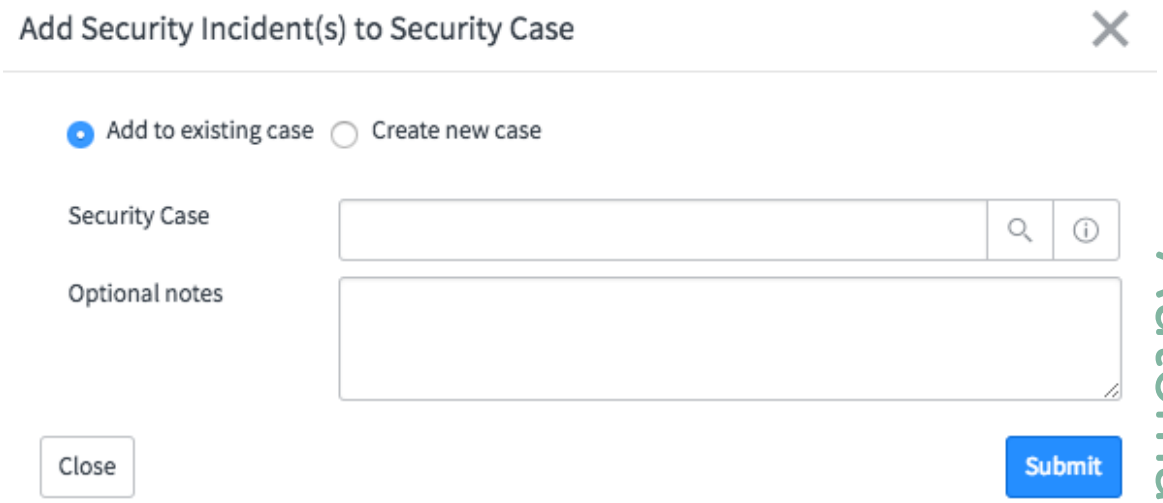
Erforderliche Rolle: sn_si.admin, sn_ti.case_user_write

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zu dem Security Incident, der eine Eskalation erfordert, indem Sie auf klicken **Security Incident** > **Incidents** > **Mir zugewiesen**, Und öffnen Sie den Security Incident.
2. Klicken Sie auf **Dem Sicherheitsfall hinzufügen** Zugehöriger Link.
   Die **Fügen Sie Security Incident(s) dem Sicherheitsfall hinzu** Dialogfeld wird geöffnet.



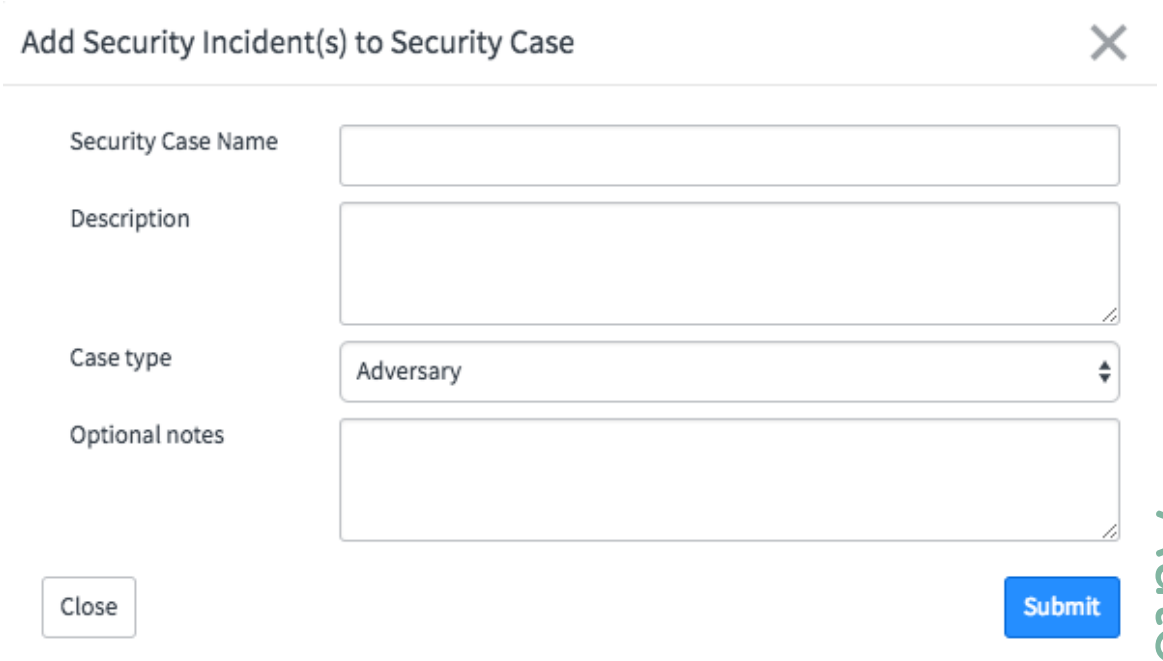
3. Wenn Ihnen ein Fall zugewiesen ist, dem Sie diesen Security Incident hinzufügen möchten, füllen Sie die entsprechenden Felder aus, und klicken Sie dann auf **Übermitteln** .

Feld	Beschreibung
Sicherheitsfall	Wählen Sie den Sicherheitsfall aus.
Optionale Notizen	Geben Sie bei Bedarf zusätzliche Notizen ein, die für den Fallanalysten von Wert wären.

4. Wenn Ihnen ein oder mehrere Fälle zugewiesen sind, Sie aber einen neuen Fall erstellen und ihm den Security Incident zuweisen möchten, klicken Sie auf **Erstellen Sie einen neuen Fall** Zum Anzeigen zusätzlicher Felder.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Wenn Ihnen keine Fälle zugewiesen sind, wird zuerst der Bildschirm oben geöffnet.

5. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Name Des Sicherheitsfalls	Geben Sie den Namen des neuen Sicherheitsfalls ein.
Beschreibung	Geben Sie eine Beschreibung für den Fall ein.
Falltyp	Wählen Sie den Typ des untersuchten Falls aus.
Optionale Notizen	Geben Sie bei Bedarf zusätzliche Notizen ein, die für den Fallanalysten von Wert wären.

6. Klicken Sie auf **Absenden**.
Oben im Security Incident wird eine Nachricht mit einem Link zum neuen Fall angezeigt.

Zugehörige Informationen

Security Case Management

Erstellen Sie Antwortaufgaben

Nachdem ein Security Incident erstellt wurde, können Sie Antwortaufgaben erstellen, um separate Aktionen nachzuverfolgen, die zur Reaktion auf das Sicherheitsproblem ausgeführt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.Basic

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zum entsprechenden Speicherort, um den Security Incident zu öffnen, für den Sie Aufgaben erstellen möchten.
   Zum Beispiel:
   - Um eine Antwortaufgabe basierend auf einem Ihnen zugewiesenen Security Incident zu erstellen, wählen Sie aus **Security Incident** > **Incidents** > **Mir zugewiesen**an.
   - Um eine Antwortaufgabe basierend auf einem Security Incident zu erstellen, der Ihrem Team zugewiesen ist, wählen Sie aus **Security Incident** > **Incidents** > **Dem Team zugewiesen** > **Incidents**an.
   - Um eine Antwortaufgabe basierend auf einem nicht zugewiesenen Security Incident zu erstellen, wählen Sie aus **Security Incident** > **Incidents** > **Nicht zugewiesene Incidents**an.
2. Öffnen Sie den Security Incident, für den Sie Antwortaufgaben hinzufügen möchten.
3. Klicken Sie auf **Fügen Sie Eine Antwortaufgabe Hinzu** Schaltfläche im Formularheader.

   Hinweis:
   Klicken Sie auf , um eine andere Aufgabe zu erstellen **Aufgaben** Registerkarte in der zugehörigen Liste „Incident“.

4. Füllen Sie die entsprechenden Felder im Formular aus.

Security Incident

Feld	Beschreibung
Sicherheits-Tag auswählen	Wenn Sie eingerichtet und aktiviert haben Sicherheits-Tags , Sie können ein oder mehrere Tags auswählen, um dem Datensatz Metadaten hinzuzufügen, oder den Vertraulichkeitsgrad der Antwortaufgabe angeben. Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt.
Anzahl	[Schreibgeschützt] automatisch generiert Security Incident Response Nummer.
Übergeordnet	[Schreibgeschützt] die Nummer des zugehörigen Security Incidents.
Konfigurationselement	Das Konfigurationselement (die Ressource), das vom Sicherheitsproblem betroffen ist.
Betroffener Anwender	Die vom Sicherheitsproblem betroffene Person.
Priorität	Die Priorität, mit der bestimmt wird, wann diese Aufgabe ausgeführt wird.
Status	Der aktuelle Status der Sicherheitsantwortaufgabe. Bei der Aufgabenerstellung ist dieses Feld standardmäßig auf festgelegt **Entwurf** .
Kompetenzen	Die zur Ausführung dieser Aufgabe erforderliche Kompetenz. Klicken Sie auf das Schlosssymbol, und wählen Sie die erforderliche Kompetenz aus. Nachdem Sie Ihre Auswahl abgeschlossen haben, klicken Sie erneut auf das Schlosssymbol.
Zuweisungsgruppe	Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird.
Zugewiesen an	Die Person, die der Ausführung der Aufgabe zugewiesen ist.
Kurzbeschreibung	Eine Beschreibung von Security Incident Response Aufgabe.
Beschreibung	Eine Beschreibung für die ausgewählte Aufgabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sichere Notizen	Die Arbeitsnotizen, die verschlüsselt und für den Kunden nicht sichtbar sind.
Arbeitsnotizen	Die Arbeitsnotizen, die für den Kunden nicht sichtbar sind.
Zusätzliche Anmerkungen	Kommentare, die Sie für den Kunden sichtbar sein möchten.

5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Hinweis:
Nachdem Sie erstellt haben Security Incident Response-Aufgaben können Sie sie mit einer der folgenden Anwendungen unter anzeigen **Antwortaufgaben** Modul:

- **Mir zugewiesen** .
- **Dem Team zugewiesen** .
- **Offene Aufgaben anzeigen**
- **Alle Aufgaben anzeigen**
- **Nicht Zugewiesene Aufgaben** .

Verwalten Sie Predictive Intelligence für von Anwendern gemeldetes Phishing

Die Funktion „Predictive Intelligence für von Anwendern gemeldetes Phishing“ bietet eine bedeutende Lösung für die Selektierung und Priorisierung von von Anwendern gemeldeten Phishing-E-Mails.

In diesem Abschnitt wird Folgendes beschrieben:

- Predictive Intelligence für Phishing-Meldungen von Anwendern
- Erforderliche Komponenten und Plugins
- Endgültige Urteilsgenerierung für vom Anwender gemeldetes Phishing
- Fehlerbehebung bei Predictive Intelligence für vom Anwender gemeldetes Phishing

Predictive Intelligence für Phishing-Meldungen von Anwendern

Diese Funktion unterstützt Sicherheitsanalysten bei der Selektierung und Priorisierung von von Anwendern gemeldeten Phishing-E-Mails.

Das Predictive Intelligence-Framework bietet Lösungen zum Trainieren des Systems, um Datenergebnisse vorherzusagen, zu empfehlen und zu organisieren. Weitere Informationen zu Predictive Intelligence finden Sie unter Predictive Intelligence . Mit diesem Framework können Sie Modelle erstellen, um automatisch vorherzusagen, ob ein Anwender meldete Phishing-E-Mails verdächtig oder legitim ist.

Mithilfe historischer Daten von vom Anwender gemeldeten Phishing-Security Incidents (E-Mail-Header, E-Mail-Text und Selektierungsergebnisse, die über die Abschlusscodes für Security Incidents erfasst werden) können Sicherheitsanalysten das System trainieren, um eingehende von Anwendern gemeldete Phishing-Übermittlungen als Übermittlungen zu klassifizieren, die weiter selektiert werden müssen (wahrscheinlich verdächtig) und als legitime Übermittlungen.

Durch die automatische Selektierung eingehender E-Mails können Sicherheitsanalysten die Incident-Warteschlange einfach priorisieren und sich vor allem auf Incidents konzentrieren, die wahrscheinlich ein Risiko für die Organisation darstellen, und weniger Aufwand für E-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mails aufwenden, die sehr wahrscheinlich falsch positiv sind. Das Vorhersageergebnis bietet auch eine Konfidenzpunktzahl für die Klassifizierung, um eine granulare Priorisierung zu ermöglichen.

Erforderliche Komponenten und Plugins

Um Predictive Intelligence für von Anwendern gemeldetes Phishing zu verwenden, müssen Sie die folgenden Anwendungen installieren

Plugin-Name	Mindestversion
Security Incident Response	9.0.1 oder 10.0.2
Predictive Intelligence	Orlando-Version
Predictive Intelligence für Phishing-Meldungen von Anwendern	10.0.2

Hinweis:
Die folgenden neuen Erweiterungen sind mit Security Incident Response 10.4 verfügbar:

- Die Möglichkeit, Abschlusscodes aus anwenderdefinierten Feldern für das Modelltraining auszuwählen.
- Die Möglichkeit, Vorhersagen nach der Modellerstellung explizit zu aktivieren.
- Die Möglichkeit, ein endgültiges Urteil über die vom Anwender gemeldete Phishing-Übermittlung mithilfe einer Entscheidungstabelle zu generieren. (Erfordert Security Operations-Spoke 10.3,0)

Um die neuen Erweiterungen zu verwenden, müssen Sie die folgenden Anwendungen aktualisieren:

Plugin-Name	Upgrade auf
Security Incident Response	10.0.4
Predictive Intelligence für Phishing-Meldungen von Anwendern	10.3.1

Neue und aktualisierte Tabellen

- sn_Sir_ml_URP_config (Neu): Enthält die Konfiguration für die URP ML-Anwendung.
- sn_Sir_ml_URP_Feature (Neu): Datensätze, die aus der E-Mail-Tabelle „sn_si_Phishing“ extrahiert wurden.
- sn_Sir_ml_URP_Feature_Import (Neu): Wird verwendet, um historische Phishing-E-Mail-Daten hochzuladen.
- sn_si_Incident (aktualisiert): Die folgenden neuen Felder wurden hinzugefügt:
  - Vorhersage akzeptiert
  - Ergebnis der Vorhersage
  - Vertrauensbewertung
- **Skripteinbindungen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- URPMLUtil: Ruft die Konfiguration ab, führt einen Vorhersageauftrag aus und verfolgt den Vorhersageprozess.
- URPMLProcessor: Extrahiert und verarbeitet Daten aus der Tabelle „sn_si_Phishing_email“.
- URPMLAction: Führt einen Flow aus, um das Vorhersageergebnis zu akzeptieren.

Endgültige Urteilsgenerierung für vom Anwender gemeldetes Phishing

Security Incident Response-Teams können jetzt basierend auf den Ergebnissen von Predictive Intelligence- und Bedrohungsanreicherungsintegrationen das finalisierte Urteil für einen von Anwendern gemeldeten Phishing-Datensatz vorantreiben.

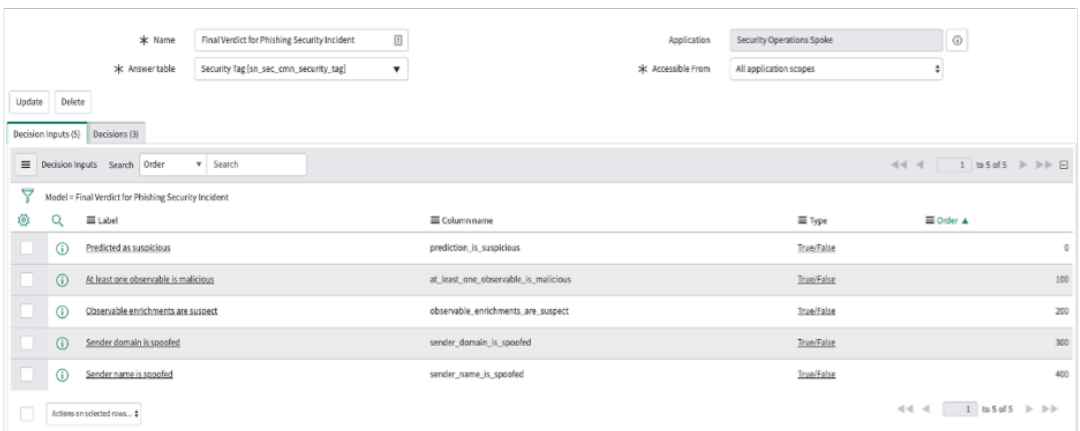
Diese endgültige Urteilsgenerierung wird über ein Entscheidungstabellenkonstrukt aktiviert und in einem Flow genutzt.

Voraussetzungen

Stellen Sie sicher, dass alle Plugins in aufgeführt sind Erforderliche Komponenten und Plugins Wurden installiert.

Navigieren zu **Predictive Intelligence für Phishing** > **Endgültiges Urteil** > **Endgültiges Urteil für Phishing Security Incident**an.

Die **Entscheidungseingaben** Die Registerkarte zeigt die verschiedenen Bedingungen, die ausgewertet wurden, um zum endgültigen Urteil zu gelangen.



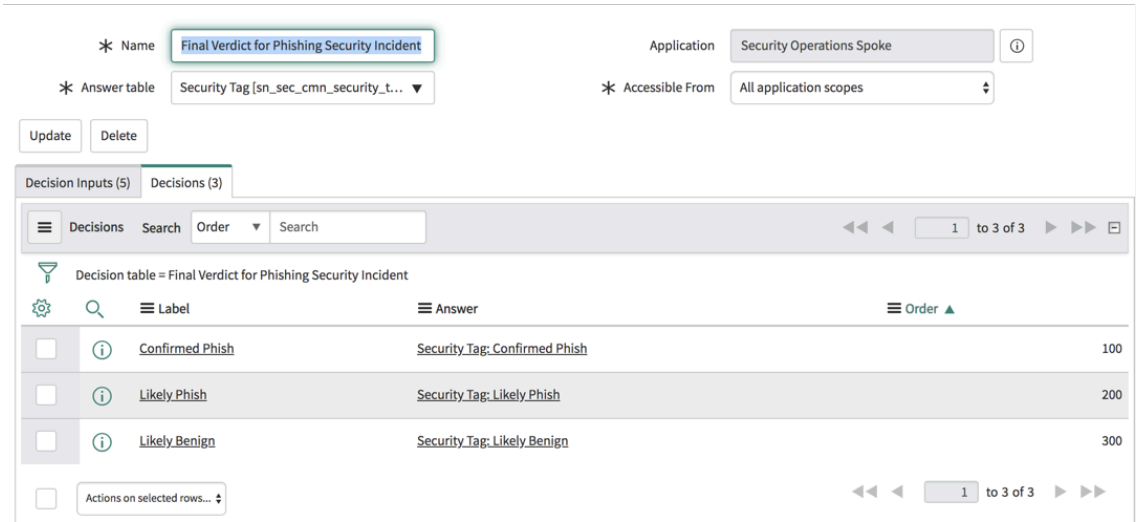
Die folgenden Bedingungen sind mit dem Basissystem verfügbar:

- Als verdächtig vorhergesagt: Wenn Predictive Intelligence die Phishing-E-Mail als klassifiziert hat **Verdächtig** .
- Mindestens ein erkennbares Element ist schädlich: Wenn ein erkennbares Element, das am Security Incident beteiligt ist (z. B. URL, Domäne, IP, Hash), als klassifiziert wurde **Böswillig** Nach Threat Intelligence-Quellen.
- Anreicherung erkennbarer Elemente ist verdächtig: Wenn Anreicherung erkennbarer Elemente (z. B. Aktualität der Phishing-Domänenregistrierung, Land der Phishing-Domänenregistrierung) als verdächtig gilt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Absenderdomäne wird gefälscht: Wenn der Verdacht besteht, dass die E-Mail-Domäne des Phisher eine vertrauenswürdige Domäne vortäuscht.
- Absendername wird gefälscht: Wenn die E-Mail-Adresse des Phisher vermutet wird, dass ein vertrauenswürdiger Mitarbeiter einer Organisation gefälscht wird.

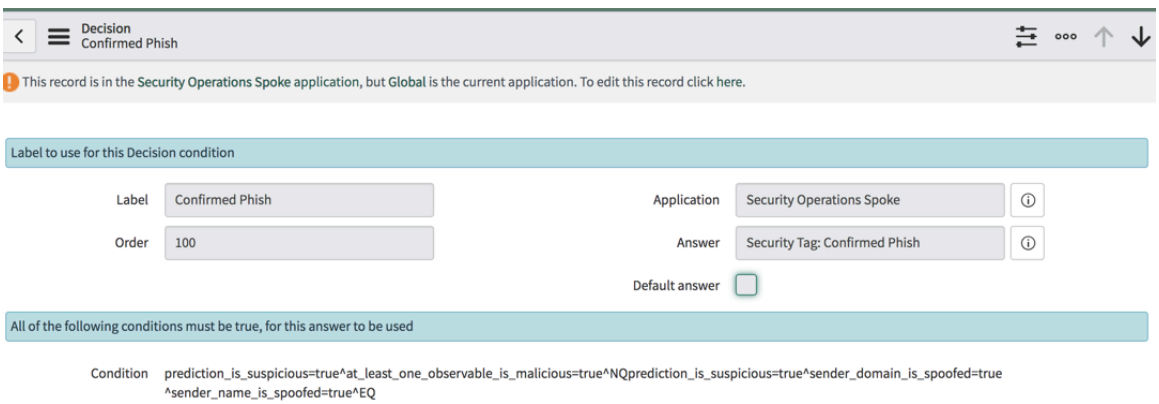
Die **Entscheidungen** Auf der Registerkarte werden die endgültigen Urteilsoptionen angezeigt, die für einen bestimmten Security Incident erreicht werden können.



Die folgenden Entscheidungen sind mit dem Basissystem verfügbar:

- Bestätigtes Phishing: Wenn die Bedingungen zum endgültigen Urteil als bestätigte Phishing-E-Mail geführt haben.
- Wahrscheinlich Phishing: Wenn die Bedingungen zum endgültigen Urteil als potenzieller Phishing-Versuch geführt haben.
- Wahrscheinlich gutartig: Wenn die Bedingungen zum endgültigen Urteil als gutartige Übermittlung geführt haben.

Sie können die Bedingungen anzeigen, die für jede der endgültigen Urteilsoptionen ausgewertet wurden. Klicken Sie auf den Bezeichnungslink, um die Bedingungen anzuzeigen.



Sie können die mit dem Basissystem bereitgestellte Entscheidungstabelle anpassen oder eine eigene Entscheidungstabelle erstellen. Diese Entscheidungstabelle kann in Security Incident Response-Playbooks verwendet werden. Die **Endgültiges Urteil für Phishing**

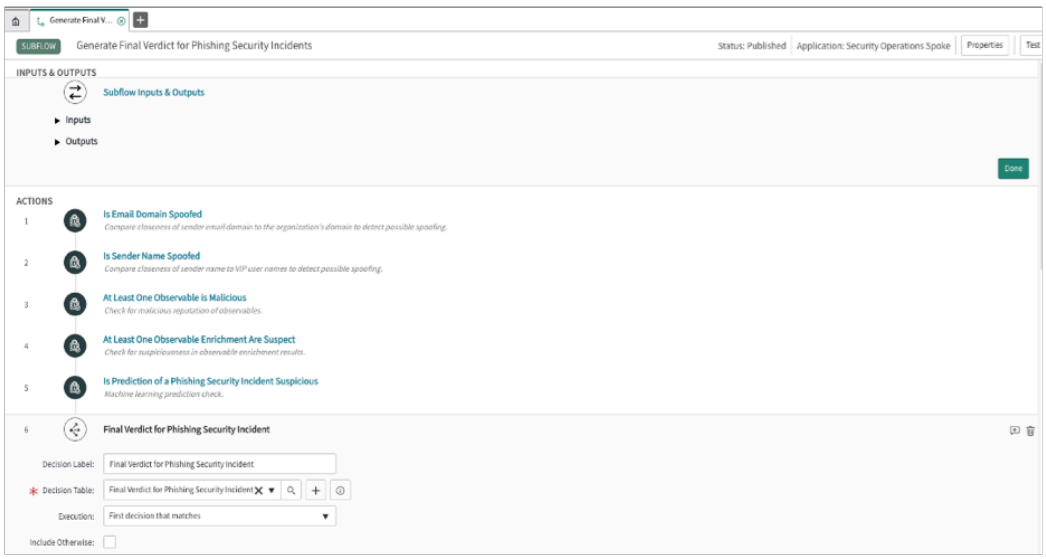
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incidents generieren subflow ist mit dem Basissystem verfügbar. Dieser Subflow generiert automatisch das endgültige Urteil für einen Phishing-Security Incident und wendet basierend auf dieser Entscheidung ein Sicherheits-Tag an. Sie können diesen Subflow als Teil von einschließen **Automatisiertes Phishing** playbook.

Die Eingaben für diesen Subflow sind:

- Incident_ID: Die SYS-ID des Phishing-Security Incidents.
- c_Level_names: Kommagetrennte Liste von Namen (z. B. Namen von Führungskräften in der Organisation), die wahrscheinlich beim Phishing-Angriff gefälscht werden.
- Trusted_Domains: Kommagetrennte Liste vertrauenswürdiger E-Mail-Domänen.
- Anreicherung_keywords: Kommagetrennte Liste von Stichwörtern, die die böswillige Haltung des erkennbaren Elements aus Anreicherungsergebnissen angeben.
- Sender_email (optional): Die E-Mail-Adresse des Absenders der Phishing-E-Mail.

Die Ausgabe dieses Flows kann sein **Phishing Bestätigt** , **Wahrscheinlich Phishing** , Oder **Wahrscheinlich Gutartig** .



Fehlerbehebung bei Predictive Intelligence für vom Anwender gemeldetes Phishing

In diesem Abschnitt werden einige häufige Problemszenarien behandelt.

- Problem: Ich kann die Predictive Intelligence-Konfiguration nicht ändern.

  Lösung: Überprüfen Sie, ob Sie dazu berechtigt sind. Sie müssen sich als Anwender mit der Rolle „ml_admin“ anmelden, um Schwellenwerte zu ändern. Einige Szenarien erfordern möglicherweise sogar höhere Berechtigungen, z. B. müssen Sie die Grenze für Trainingsdaten ändern. Für solche Szenarien müssen Sie sich an den Kundensupport wenden, um Hilfe zu erhalten.

- Problem: Das Modelltraining ist fehlgeschlagen.

  Lösung: Überprüfen Sie, ob die URLs des ML-Planers eingerichtet wurden. Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften** Und überprüfen Sie, ob `Glide.Shared_Service_Scheduler.url` Eigenschaft wurde konfiguriert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Problem: Vorhersageergebnisse sind für einen Security Incident nicht verfügbar.

  Lösung:

  - Überprüfen Sie, ob die Vorhersage-URL in eingerichtet wurde `Glide.Prediction_Service.url` Systemeigenschaft und stellen Sie sicher, dass das Rechenzentrum mit der URL übereinstimmt.
  - Überprüfen Sie, ob die geplante Aufgabe „vom Anwender gemeldete Phishing-E-Mail vorhersagen“ aktiv ist.

Konfigurieren Sie Predictive Intelligence für vom Anwender gemeldetes Phishing

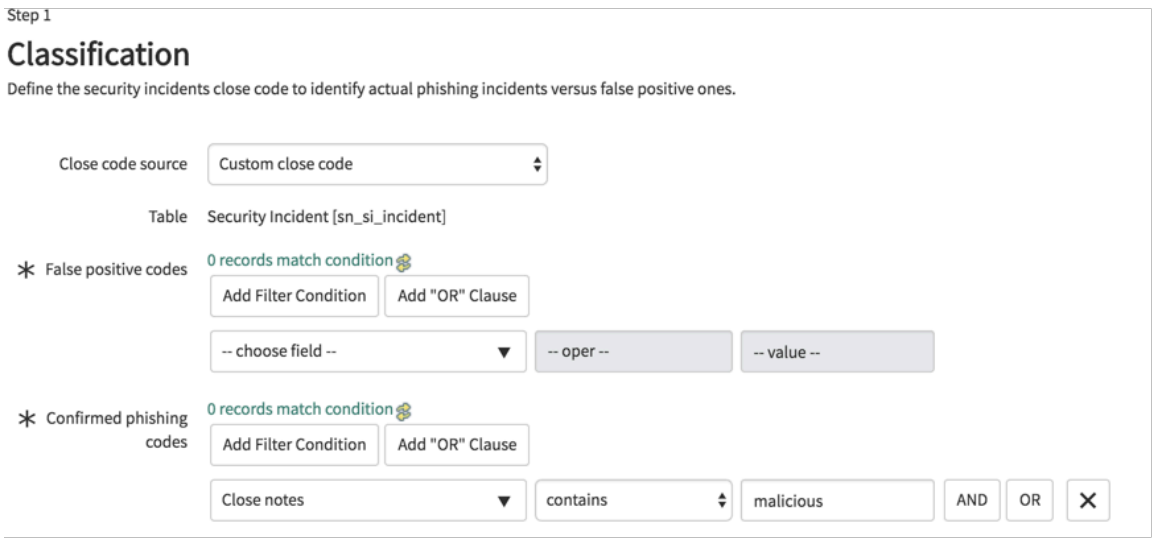
Konfigurieren und bereiten Sie das Modell vor, um von Anwendern gemeldete Phishing-E-Mails zu identifizieren.

Vorbereitungen

Erforderliche Rolle: ml_admin

Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence für Phishing** > **Konfiguration**an.
2. Wählen Sie in Schritt 1 der Konfiguration eine der folgenden Optionen aus der Liste Abschlusscodequelle aus:
   - Standard-Abschlusscode: Wählen Sie diese Option aus, um die Standard-Abschlusscodes für Security Incidents anzugeben, die vom Schulungsmodell zur Identifizierung schädlicher und legitimer E-Mails verwendet werden müssen. Klicken Sie auf das Schlosssymbol, und wählen Sie einen oder mehrere falsch positive Codes oder bestätigte Phishing-Codes aus.
   - Anwenderdefinierter Abschlusscode: Wählen Sie die Option Anwenderdefinierter Abschlusscode aus, wenn Sie Abschlusscodes aus anwenderdefinierten Feldern definieren möchten, die als Teil Ihrer vorhandenen Incident-Antwortverfahren verwendet werden können. Um einen Abschlusscode zu definieren, wählen Sie ein Feld aus der Tabelle „Security Incident“ aus, und geben Sie eine oder mehrere Filterbedingungen an.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Importieren Sie in Schritt 2 Verlaufsdaten, die zum Trainieren des Modells verwendet werden können. Wählen Sie die Datenquelle für den Import der Verlaufsdaten aus. Dies kann sein:
   - Vom Anwender gemeldete Phishing-E-Mail-Tabelle: Sie können die Anzahl der Datensätze anzeigen, die als Verlaufsdaten importiert werden können. Wählen Sie diese Option aus, und klicken Sie auf **Importieren** .
   - Anwenderdefinierte Datenquelle: Sie können eine einzelne formatierte CSV-Datei anhängen, die Verlaufsdatensätze enthält. Wählen Sie die Datei aus, und klicken Sie auf **Importieren** .

   Hinweis:
   Die CSV-Datei, die Sie importieren, muss die folgenden Header enthalten:
   - Bezeichnung
   - Header
   - Haupttext

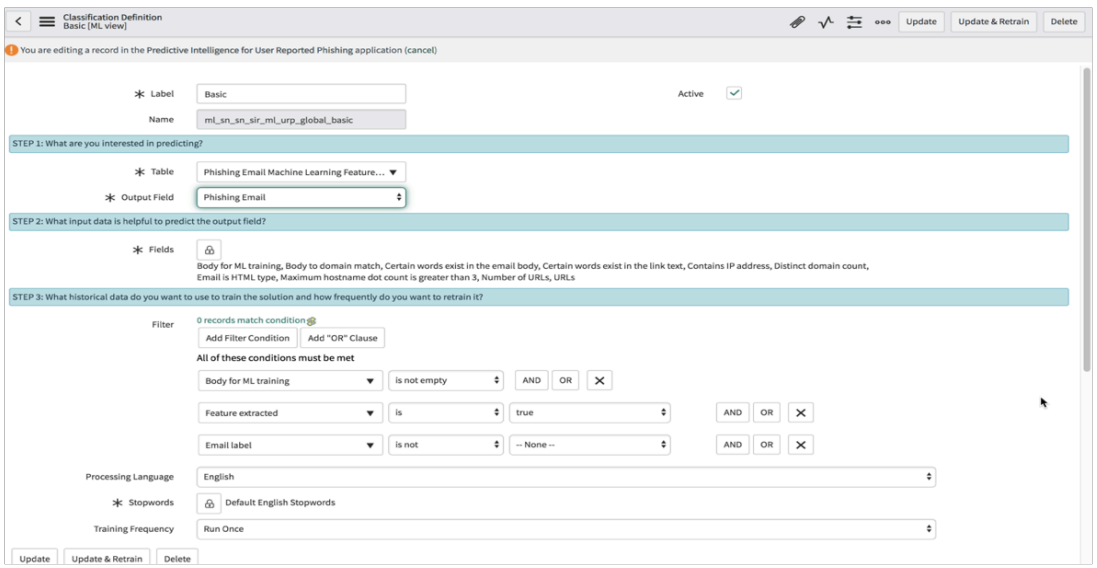
   Jeder Datensatz muss in der Spalte Bezeichnung in der CSV-Datei ein schädliches oder legitimes Tag enthalten.

   Klicken Sie Auf **Import Abbrechen** Um den Import der Daten zu beenden. Der Importprozess wird abgebrochen, und alle Datensätze, die bisher importiert wurden, werden gelöscht.

4. Nachdem Sie die Verlaufsdaten importiert haben, klicken Sie auf den Link, um die Seite zu aktualisieren. Sie können dann entweder weitere Trainingsdaten importieren oder mit dem nächsten Schritt fortfahren.
5. Überprüfen Sie in Schritt 3, ob die Anzahl der für das Training verfügbaren Datensätze die Mindestanforderungen an Schwellenwerte erfüllt.

   Hinweis:
   Die Standardwerte für die maximale und minimale Anzahl von Schulungsdatensätzen werden angezeigt. Diese Schwellenwerte können in geändert werden Eigenschaften Der Plattform Für Maschinelles Lernen Seite. Wenden Sie sich an den Kundensupport, um Unterstützung zu erhalten.

6. Wenn die Trainingsdaten ausreichen, klicken Sie auf **Modell trainieren** .
   Sie können die Eingaben für das Training auf dem folgenden Bildschirm aktualisieren.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Zu den Vorhersageeingaben, die Sie ändern können, gehören:
   - Was möchten Sie vorhersagen?
   - Welche Eingabedaten helfen bei der Vorhersage des Ausgabefelds?
   - Welche Verlaufsdaten möchten Sie zum Trainieren der Lösung verwenden, und wie häufig möchten Sie sie erneut trainieren?

   Die Standardwerte für diese Eingaben werden angezeigt. Sie können sie ändern und auf eine der folgenden Optionen klicken:
   - **Aktualisieren** : Aktualisiert die Trainingsmodelldefinition.
   - **Aktualisieren Und Erneut Trainieren** : Aktualisiert die Trainingsmodelldefinition und trainiert das Modell erneut (löst aus **Modell Trainieren** Funktion).
8. Wenn Sie das Training des Modells abgeschlossen haben, klicken Sie abschließend auf **Aktivieren Sie Die Vorhersage** Kontrollkästchen.
   Vorhersagen werden jetzt für jeden von Anwendern gemeldeten Phishing-Datensatz mit diesem Modell bereitgestellt. Wenn Sie die Bereitstellung von Vorhersagen für die vom Anwender gemeldeten Phishing-Datensätze beenden möchten, löschen Sie **Aktivieren Sie Die Vorhersage** Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Deaktivieren** .

Sicherheitsanalysten werden zugewiesen

Abhängig von Ihren Einstellungen in SIR Bildschirm „Administrationskonfiguration“ können Sie Security Incidents manuell, automatisch mithilfe eines Workflows oder automatisch mithilfe der automatischen Zuweisung zuweisen.

Manuelle Analystenzuweisung

Sie können konfigurieren Security Incident Response Bildschirm „Administrationskonfiguration“, der erfordert, dass Sicherheitsanalysten manuell zugewiesen werden, wann immer jemand oder der SIR Die Anwendung erstellt einen Security Incident oder generiert eine Security Response-Aufgabe.

Wenn ein Security Incident oder eine Antwortaufgabe nicht automatisch zugewiesen werden kann, können Sie festlegen SIR Bildschirm „Administrationskonfiguration“, um die manuelle Zuweisung von Sicherheitsanalysten zu erfordern. Dies ist eine gute Wahl, wenn Sie eine begrenzte Anzahl von Sicherheitsanalysten haben, um Anforderungen abzuschließen, oder wenn Sie sie einfach nicht automatisch zuweisen möchten.

Workflow-basierte Sicherheitsanalystenzuweisung

Sie können konfigurieren Security Incident Response Bildschirm „Administrationskonfiguration“ zur Verwendung eines ausgewählten Workflows zum Zuweisen des Sicherheitsanalysten, wenn jemand oder die SIR-Anwendung einen Security Incident oder eine Security Response-Aufgabe erstellt.

Im Konfigurationsbildschirm „Security Incident Administration“ können Sie einen Workflow verwenden, um jedem Security Incident oder jeder Security Response-Aufgabe einen Analysten zuzuweisen. Diese Option ist eine gute Wahl für Organisationen, die einen anwenderdefinierten Prozess zur Lösung von Sicherheitsproblemen verwenden oder anderweitig über einen automatisierbaren Prozess verfügen.

Automatische Zuweisung von Sicherheitsanalysten

Sie können konfigurieren Security Incident Response Bildschirm „Administrationskonfiguration“ zum automatischen Zuweisen des Sicherheitsanalysten, wann immer jemand oder der SIR Die Anwendung erstellt einen Security Incident oder eine Security Response-Aufgabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit der automatischen Zuweisung können Sie basierend auf den Anforderungen Ihrer Organisation die Kriterien definieren, nach denen Analysten automatisch Security Incidents zugewiesen werden.

Automatische Zuweisung von Service Desk-Mitarbeitern basierend auf Mitarbeiterbewertungen

Wenn die automatische Zuweisung aktiviert ist und ein Security Incident oder eine Antwortaufgabe erstellt wird, werden die folgenden Aktionen ausgeführt:

- Die verfügbaren Sicherheitsanalysten werden basierend auf den in der Konfiguration definierten Kriterien ausgewertet.
- Der Aufgabe wird automatisch ein entsprechender Sicherheitsanalyst zugewiesen.
- Die Aufgabe wird in den Status **Zugewiesen** versetzt.

Wenn die Konfiguration so eingerichtet ist, dass mehr als ein Satz von Bedingungen berücksichtigt werden, z. B. Kompetenzen, Standort, Zeitzone oder Gruppenabdeckungsbereich, werden die Sicherheitsanalysten basierend auf den Einstellungen für die Gewichtungseigenschaft und anderen Kriterien bewertet. Diese Konfigurationseinstellungen helfen Ihnen, Service Desk-Mitarbeiter basierend auf optionalen Eigenschaften automatisch zuzuweisen. Die berechneten Bewertungen werden verwendet, um den besten Service Desk-Mitarbeiter für den Security Incident oder die Antwortaufgabe zu bestimmen. Jede Kombination von bewertungsbasierten Methoden kann im Anwendungskonfigurationsbildschirm aktiviert werden.

Beim Erstellen einer Aufgabe wird eine Bewertung für jeden Typ der aktivierten Auswahlkriterien für alle verfügbaren Außendienstmitarbeiter berechnet. Der Service Desk-Mitarbeiter, dessen Gesamtbewertung die höchste ist, wird für die automatische Zuweisung berücksichtigt.

Die Einstellungen für die Gewichtungseigenschaften für die automatische Zuweisung, gefunden in **Security Incident** > **Administration** > **Eigenschaften**, Sind in den Bewertungsberechnungen enthalten.

Mit diesen Werten können Sie Prioritäten für die Auswahlkriterien für die automatische Zuweisung festlegen, die für Ihre Organisation wichtiger sind. Legen Sie die Prioritätswerte zwischen 1 (weniger wichtig) und 10 (wichtig) fest.

Ein Beispiel dafür, wie sich die Gewichtungseigenschaften auf die Bewertungen der Außendienstmitarbeiter auswirken, finden Sie unter Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe mehrerer Auswahlkriterien.

Bereitschaftsplanung

Die Anwendung Bereitschaftsplanung hilft Ihnen, dafür zu sorgen, dass Mitglieder des dedizierten Support-Teams bereit stehen, um Probleme schon bei der Entstehung zu beheben. Sie können Rufbereitschaftszeitpläne, Dienstplanrotationen und Eskalationsrichtlinien einrichten, Benachrichtigungen für eine Gruppe eskalieren und den aktuellen Kontakt für eine Eskalation bestimmen. Die Anwendung identifiziert das zugewiesene und verfügbare Mitglied einer Supportgruppe, z. B. beim Zuweisen eines Incident. Weitere Informationen finden Sie unter On-Call Scheduling . Die Bereitschaftsplanung für Security Incident Response funktioniert auf dieselbe Weise.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Zuweisung von Außendienstmitarbeitern mithilfe des Standorts

Service Desk-Mitarbeiter können basierend auf dem Heimatstandort in ihrem Anwenderdatensatz und dem Standort der Aufgaben automatisch zugewiesen werden.

Die automatische Zuweisung nach Standort wird ausgeführt, wenn **Bei der automatischen Auswahl von Service Desk-Mitarbeitern wird der Standort der Konfiguration von Service Desk-Mitarbeitern berücksichtigt** Option ist aktiviert.

Wenn eine Aufgabe (Security Incident oder Antwortaufgabe) erstellt wird, wird der Service Desk-Mitarbeiter berücksichtigt, der dem Aufgabenstandort am nächsten ist. Wenn die Anwendung so konfiguriert ist, dass nur der Standort berücksichtigt wird, wird dem nächsten Service Desk-Mitarbeiter die Aufgabe automatisch zugewiesen.

Wenn eine Aufgabe erstellt wird, werden Mitarbeiterstandorte mit den folgenden Bereichen verglichen, um die Bewertung der einzelnen Mitarbeiterstandorte zu bestimmen.

Berechnung der Standortberechnung

Entfernung (km) vom Außendienstmitarbeiter zur Aufgabe	Bewertung
0 bis 0,1	1
0,11 bis 0,5	0.9
0,51 bis 5	0,7
5,1 bis 10	0,5
10,1 bis 20	0,4
20,1 bis 30	0,3
30,1 bis 40	0,2
40,1 bis 100	0.1
>100	0

Wenn die Anwendung so konfiguriert ist, dass andere Auswahlkriterien verwendet werden, z. B. Kompetenzen, Zeitzone oder Zeitplan, werden die Bewertungen aller Auswahlkriterien gewichtet und zusammengefasst. Der Service Desk-Mitarbeiter mit der höchsten Gesamtbewertung wird für die Aufgabe automatisch zugewiesen. Details siehe Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe mehrerer Auswahlkriterien.

Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe von Kompetenzen

Service Desk-Mitarbeiter können basierend auf ihren Kompetenzen und den Kompetenzen, die für die Ausführung der Aufgabe erforderlich sind, automatisch zugewiesen werden. Weisen Sie ihren Anwenderdatensätzen mithilfe von Kompetenzen zu **Kompetenzen** > **Anwender**an.

Die automatische Zuweisung nach Kompetenzen kann durchgeführt werden, wenn der **Die automatische Auswahl von Service Desk-Mitarbeitern für Aufgaben erfordert Kompetenzen** Konfigurationsoption ist auf festgelegt **Alle** Oder **Einige** .

Wenn eine Aufgabe, die Kompetenzen enthält, automatisch zugewiesen wird, werden die Kompetenzen eines Service Desk-Mitarbeiters mit den Kompetenzen verglichen, die für die Ausführung der Aufgabe erforderlich sind. Eine Bewertung wird basierend auf der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsoption für Kompetenzen berechnet. Wenn die Option auf **einige** festgelegt ist, wird der Außendienstmitarbeiter mit der besten Übereinstimmung der Fähigkeiten der Aufgabe automatisch zugewiesen. Wenn die Option auf **alle** festgelegt ist, werden nur Außendienstmitarbeiter berücksichtigt, die alle erforderlichen Fähigkeiten besitzen. Wenn keine Service Desk-Mitarbeiter über alle Kompetenzen verfügen, die zur Ausführung der Aufgabe erforderlich sind, wird niemand automatisch zugewiesen.

Eine Kompetenzbewertung wird wie folgt berechnet:

Skills_agent/Skills_task

Wobei:

- Skills_agent die Anzahl der Fähigkeiten des Außendienstmitarbeiters ist, die den für die Aufgabe erforderlichen Fähigkeiten entsprechen.
- Skills_task die Gesamtanzahl der für die Aufgabe erforderlichen Fähigkeiten ist.

Wenn eine Aufgabe beispielsweise vier Fähigkeiten erfordert und Außendienstmitarbeiter A drei davon und Außendienstmitarbeiter B zwei davon besitzt, dann ist die:

- Kompetenzbewertung des Service Desk-Mitarbeiters = 3/4 oder 0,75
- Kompetenzbewertung Service Desk-Mitarbeiter B = 2/4 oder 0,5

Wenn die Anwendung so konfiguriert ist, dass andere Auswahlkriterien verwendet werden, z. B. Standort oder Zeitzone, werden die Bewertungen aller Auswahlkriterien gewichtet und zusammengefasst. Für die Aufgabe wird der Service Desk-Mitarbeiter mit der höchsten Gesamtbewertung ausgewählt. Details siehe Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe mehrerer Auswahlkriterien.

Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe von Zeitzonen

Service Desk-Mitarbeiter können basierend auf der in ihren Anwenderdatensätzen definierten Zeitzone und der Zeitzone der Aufgaben automatisch zugewiesen werden.

Wenn **Bei der automatischen Auswahl von Service Desk-Mitarbeitern wird die Zeitzone für die Aufgabe berücksichtigt** Die Konfigurationsoption ist aktiviert. Die automatische Zuweisung nach Zeitzone kann durchgeführt werden.

Wenn eine Aufgabe erstellt wird, werden Service Desk-Mitarbeiter in der Zeitzone berücksichtigt, die der Aufgabenzeitzone am nächsten liegt. Wenn die Anwendung so konfiguriert ist, dass nur eine Zeitzone berücksichtigt wird, kann der Aufgabe nur ein Service Desk-Mitarbeiter in derselben Zeitzone automatisch zugewiesen werden.

Hinweis:
Es ist wichtig, dass die Zeitzonen für den Service Desk-Mitarbeiter und die Aufgabe korrekt festgelegt sind.

Wenn eine Aufgabe erstellt wird, werden Service Desk-Mitarbeiter basierend auf der Zeitzone der Aufgabe und der Zeitzone des Service Desk-Mitarbeiters mit der folgenden Formel bewertet:

1 - [abs(Task_tz – Agent_tz) ÷ 12]

wobei:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- abs die mathematische Funktion ist, um den absoluten Wert zu berechnen.
- Task_tz der Versatz zwischen der Zeitzone der Aufgabe und GMT ist.
- Agent_tz der Versatz zwischen der Zeitzone des Außendienstmitarbeiters und GMT ist.

Beispielsweise wird eine Aufgabe in New York City (GMT-4) erstellt, und zwei Außendienstmitarbeiter stehen zur Verfügung, um die Aufgabe auszuführen, einer in Los Angeles (GMT-7) und einer in Paris, Frankreich (GMT + 1).

Die Bewertung des Außendienstmitarbeiters in Los Angeles wird wie folgt berechnet:

1 - abs((-4) - (-7)) ÷ 12 oder 0,75

Die Bewertung des Außendienstmitarbeiters in Paris wird wie folgt berechnet:

1 - abs((-4) - (+1)) ÷ 12 oder 0,58

Wenn die automatische Zuweisung der Aufgabe also nur auf der Zeitzone basiert, wird sie dem Service Desk-Mitarbeiter aus Los Angeles zugewiesen.

Wenn die Anwendung so konfiguriert ist, dass andere Auswahlkriterien verwendet werden, z. B. Kompetenzen oder Standort, werden die Bewertungen aller Auswahlkriterien gewichtet und summiert. Für die Aufgabe wird der Service Desk-Mitarbeiter mit der höchsten Gesamtbewertung ausgewählt. Details siehe Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe mehrerer Auswahlkriterien.

Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe von Gruppenabdeckungsbereichen

Service Desk-Mitarbeiter können basierend auf dem in ihren Anwenderdatensätzen definierten Gruppenabdeckungsbereich automatisch zugewiesen werden.

Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe mehrerer Auswahlkriterien

Wenn eine Aufgabe erstellt wird, werden die Mitarbeiterbewertungen berechnet. Weitere Informationen finden Sie unter:

- Automatische Zuweisung von Außendienstmitarbeitern mithilfe des Standorts
- Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe von Kompetenzen
- Automatische Zuweisung von Service Desk-Mitarbeitern mithilfe von Zeitzonen

Die automatische Zuweisung basiert auf der folgenden Berechnung:

(Criteria_1-Bewertung x Criteria_1-Gewichtung) + (Criteria_2-Bewertung x Criteria_2-Gewichtung) + (Criteria_3-Bewertung x Criteria_3-Gewichtung) / Anzahl der verwendeten Kriterientypen, wobei:

Anzahl der verwendeten Kriteriumtypen = 1, 2 oder 3, abhängig von den verwendeten Einstellungen für Standort, Fähigkeiten und Zeitzone.

In diesem Beispiel wird die automatische Zuweisung von Außendienstmitarbeitern basierend auf Standort und Fähigkeiten berechnet. Das Beispiel basiert auf folgenden Annahmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Konfigurationsoption **Bei der automatischen Auswahl von Agenten wird deren Standort berücksichtigt** ist für die Anwendung aktiviert.
- Die Konfigurationsoption **Für die automatische Auswahl von Agenten für Aufgaben müssen Fähigkeiten von Agenten vorhanden sein** ist für die Anwendung aktiviert.
- Die Eigenschaft **Gewichtung der Fertigkeit** ist für die Anwendung auf 10 festgelegt.
- Die Eigenschaft **Standortgewichtung** ist für die Anwendung auf 5 festgelegt.
- Außendienstmitarbeiter A und B stehen zur Verfügung, um eine Aufgabe auszuführen, und die Aufgabe erfordert vier spezifische Fähigkeiten.
- Service Desk-Mitarbeiter Ein Standort ist 8 Meilen vom Standort der Aufgabe entfernt und verfügt über drei der vier erforderlichen Kompetenzen.
- Der Standort von Service Desk-Mitarbeiter B ist eine Viertelmeile vom Standort entfernt und verfügt über zwei der erforderlichen Kompetenzen.

Bei der automatischen Zuweisung für die Service Desk-Mitarbeiter wird diese Berechnung verwendet: [(Standortbewertung x Standortgewichtung) + (Kompetenzbewertung x Kompetenzgewichtung)]/ 2

- Die Berechnung der automatischen Zuweisung für Service Desk-Mitarbeiter A lautet: [(0,7 x 0,5) + (0,75 x 1)]/ 2 = 0,55
- Die Berechnung der automatischen Zuweisung für Service Desk-Mitarbeiter B lautet: [(0,9 x 0,5) + (0,5 x 1)]/ 2 = 0,475

In diesem Beispiel wird Service Desk-Mitarbeiter A die Aufgabe automatisch zugewiesen.

Process Mining-Arbeitsbereich für Security Incident Response

Process Mining scannt Security Incident-Audit-Protokolle und identifiziert Faktoren, die zu Ineffizienzen beitragen, z. B. mehrere Neuzuweisungen, verlängerte Wartezeiten und Zeiträume der Inaktivität für Security Incidents. Organisationen können diese Informationen verwenden, um die Ineffizienzen zu beheben.

Mit Process Mining können Sie die folgenden Verbesserungsmöglichkeiten für Ihre Security Incidents identifizieren.

Möglichkeiten mit Process Mining

Verkaufschance	Beschreibung
Incidents mit mindestens zwei Zuweisungsgruppenänderungen	Incidents, für die sich die Zuweisungsgruppe mindestens zweimal geändert hat.
SIRT (max. Wiederholungen ist 2)	
Die Eskalation von Incidents an hohe Priorität hat mehr als 5 Stunden gedauert	Incidents, für die die Priorität nach fünf Stunden an eine höhere Priorität eskaliert wurde.
Die Analyse der Incidents dauerte mehr als 5 Stunden.	Incidents, die sich länger als fünf Stunden im Analysestatus befanden.
Incidents, die innerhalb von 30 Minuten analysiert wurden	Incidents, die sich weniger als 30 Minuten im Analysestatus befanden.
Überprüfen (max. Wiederholungen: 2)	Incidents, die zweimal in den Status „Überprüfen“ verschoben wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Möglichkeiten mit Process Mining (Fortsetzung)

Verkaufschance	Beschreibung
Beseitigen (max. Wiederholungen: 2)	Incidents, die zweimal in den Status „Beseitigen“ verschoben wurden.

Das Process Mining-Inhaltspaket für Security Incident Response Fügt ein vorgefertigtes Projekt hinzu, das eine vordefinierte Prozessmodelldefinition für Security Incidents enthält. Informationen zum Erstellen eines Projekts finden Sie unter Erstellen Sie ein Process Mining-Projekt für Security Incidents.

Hinweis:
Dient zur Verwendung von Process Mining in Security Incident Response, Laden Sie das Inhaltspaket herunter, und installieren Sie es. Weitere Informationen finden Sie unter Content pack for Security Incident Response .

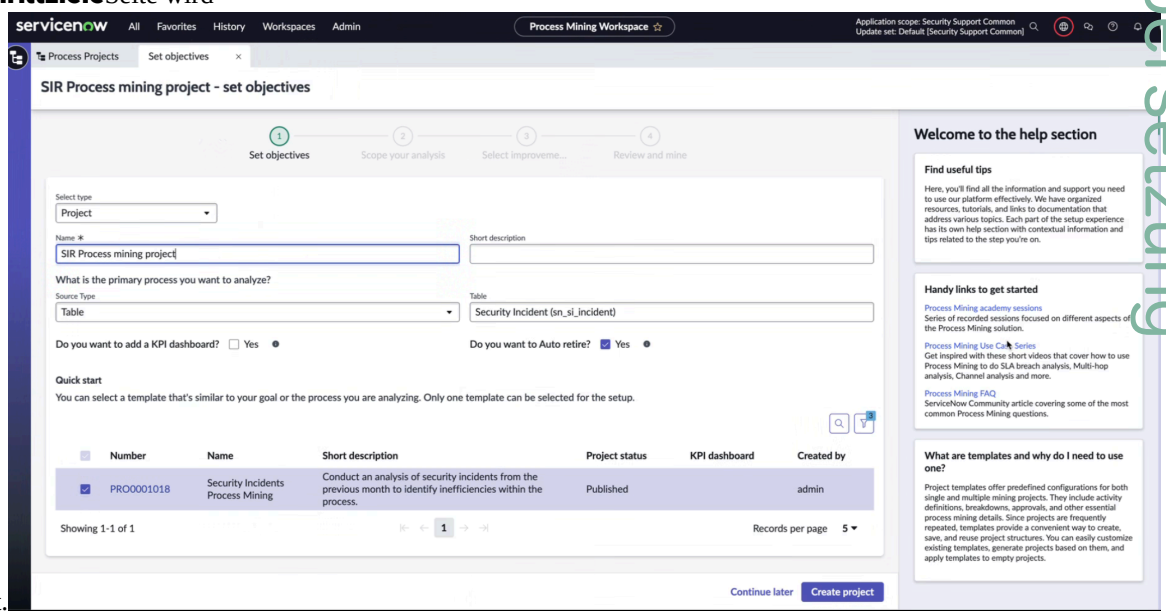
Erstellen Sie ein Process Mining-Projekt für Security Incidents

Erstellen Sie ein Projekt im Process Mining-Arbeitsbereich mit den Definitionen für vorgefertigte Prozessmodelle aus dem Inhaltspaket, um Audit-Protokolle von Security Incident-Datensätzen zu durchsuchen und Ineffizienzen im Lebenszyklus Ihres Security Incident zu identifizieren.

Vorbereitungen
Erforderliche Rolle: sn_Process_Optimization_Analyst und sn_si_read

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Process Mining-Arbeitsbereich**an.
2. Wählen Sie Aus **Erstellen Sie Ein Neues Projekt** .
   Die **Schrittziele**Seite wird



geöffnet.

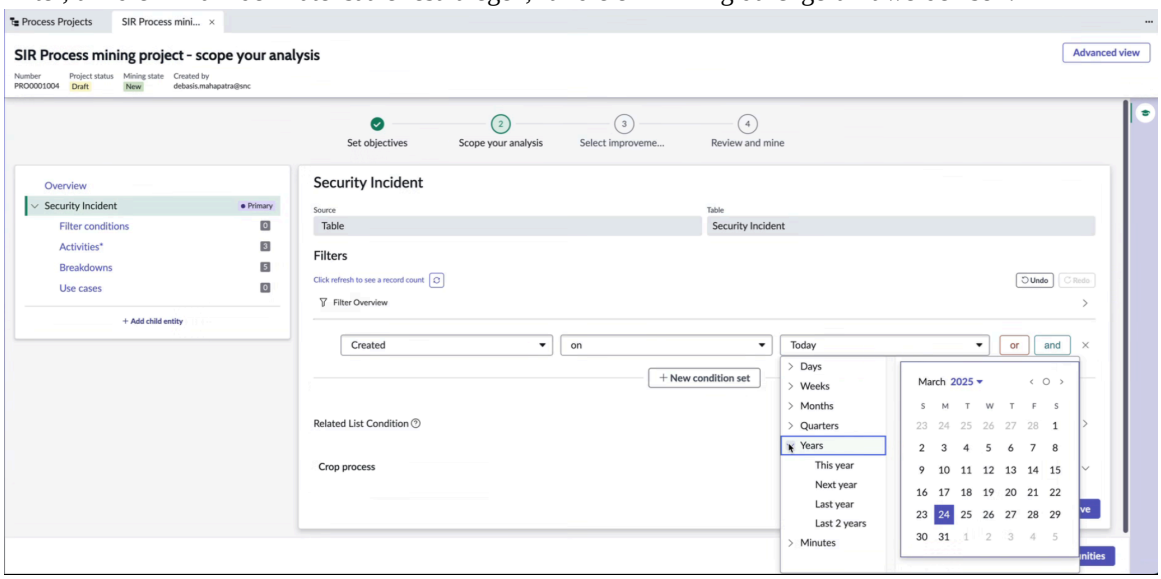
3. Geben Sie einen Namen für das Process Mining-Projekt in ein **Name** .
4. **Wahlweise:** Fügen Sie in eine Kurzbeschreibung zu Ihrem Projekt hinzu **Kurzbeschreibung** .
5. Wählen Sie Aus **Quelltyp** Als Tabelle.
6. Wählen Sie aus Security Incident (sn_si_Incident) In **Tabelle** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie die Standardvorlage und dann aus **Erstellen Sie ein Projekt** .
   Das Projekt-Dashboard wird mit allen konfigurierten Einstellungen angezeigt.

8. Wählen Sie Bearbeiten ( ) Symbol, das entspricht **Umfang der Analyse** Und konfigurieren Sie die Filter, um die Anzahl der Datensätze festzulegen, für die ein Mining durchgeführt werden soll.



9. Wählen Sie Aus **Wählen Sie Verbesserungsmöglichkeiten aus** Und konfigurieren Sie die Verbesserungen für Ihre Security Incidents.
   Eine Liste der Verbesserungsmöglichkeiten wird angezeigt. Informationen zum Konfigurieren von Verbesserungsmöglichkeiten finden Sie unter Working with improvement opportunities .

10. Wählen Sie Aus **Überprüfen und Mining durchführen** Und wählen Sie dann aus **Mining für Projekt durchführen** .

11. Wählen Sie Aus **Beispiel-Mining** Oder **Vollständiges Mining** .

12. Wählen Sie Aus **Bestätigen Und Mining Durchführen** Um das Mining zu starten.
    Das Mining startet, und der Status des Mining wird angezeigt.

Process Mining-Anwendungsfälle für Security Incidents

Die folgenden Process Mining-Anwendungsfälle bieten verschiedene Analysemethoden, mit denen Sie Ineffizienzen während der Lösung Ihrer Security Incidents identifizieren können.

Multi-Hop-Analyse

Security Incidents, die mehrmals verschiedenen Teams zugewiesen werden, können zu einer Verzögerung bei der Lösung führen. Indem Sie die Gründe für Neuzuweisungen für solche Security Incidents analysieren und die Incidents länger anhalten, können Sie die Gesamteffizienz verbessern.

Im Folgenden finden Sie Beispielschritte zum Abrufen der Liste der Security Incidents, die längere Routen beanspruchten:

1. Navigieren zu **Arbeitsbereiche** > **Process Mining-Arbeitsbereich**an.
2. Wählen Sie Aus **Zuweisungsgruppe** .
3. Öffnen Sie ein Projekt, und navigieren Sie zu **Workbench Für Analysten** .

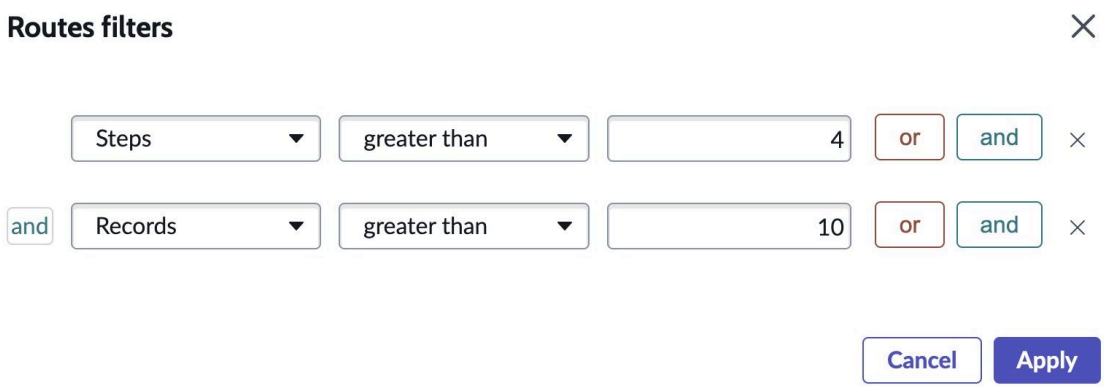
   Wenn Sie ein Mining-Prozessoptimierungsprojekt öffnen, wird standardmäßig die Workbench für Analysten geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie Aus **Variationsanalyse** .
5. Wählen Sie den Filter aus ( ) Symbol, und legen Sie den Filter ähnlich wie folgt fest:
   - Schritte, die größer sind als die durchschnittliche Anzahl von Schritten.
   - Datensätze, die größer sind als die Mindestanzahl von Datensätzen, die eine längere Route beanspruchen.

Hinweis:
Sie können die Werte entsprechend Ihren Anforderungen konfigurieren.



6. Wählen Sie **Übernehmen**.

   Alle Datensätze, die den Filterkriterien entsprechen, werden angezeigt. Wählen Sie einen Datensatz aus, um die Abschlussroute des Datensatzes anzuzeigen.
7. Wählen Sie einen Datensatz und dann aus **Route Anzeigen** .

   Die vom Datensatz durchzogene Route wird angezeigt. Sie können diese Route verwenden, um den Schritt zu identifizieren, bei dem die Incidents länger als erwartet angehalten wurden.

SLA-Verstoßanalyse

Sie können Process Mining verwenden, um Security Incidents zu analysieren, die gegen ein bestimmtes SLA (Service Level Agreement) verstoßen haben.

Im Folgenden finden Sie Beispielschritte zum Abrufen der Liste der Security Incidents, die gegen das SLA verstoßen:

1. Navigieren zu **Arbeitsbereiche** > **Process Mining-Arbeitsbereich**an.
2. Öffnen Sie ein Projekt, und navigieren Sie zu **Workbench Für Analysten** .

   Wenn Sie ein Mining-Prozessoptimierungsprojekt öffnen, wird standardmäßig die Workbench für Analysten geöffnet.
3. Wählen Sie unter Erweiterte Filter die Option aus **Bedingungen** .
4. Wählen Sie den entsprechenden Pfeil aus **Bedingung Für Zugehörige Liste** .
5. Legen Sie die Bedingungen ähnlich wie folgt fest:
   - Verwenden Sie **Wählen Sie Aus** Liste, um auszuwählen `Aufgaben-SLA` Tabelle.
   - Legen Sie den Wert von fest **Größer als oder gleich** Feld bis `1` .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie den Wert von fest **Wurde nicht eingehalten** Bis **Wahr** .
- Um Security Incidents zu identifizieren, die gegen ein bestimmtes SLA verstoßen haben, legen Sie einen fest **SLA-Definition** Filter.

6. Wählen Sie **Übernehmen**.

   Alle Datensätze, die den Bedingungen entsprechen, werden angezeigt. Wählen Sie einen Datensatz aus, um die Route des Datensatzes für die Analyse anzuzeigen.

Prioritätsanalyse

Sie können das Process Mining verwenden, um den vorhandenen Prioritätszuweisungsprozess für Ihre Security Incidents zu überprüfen und zu verbessern.

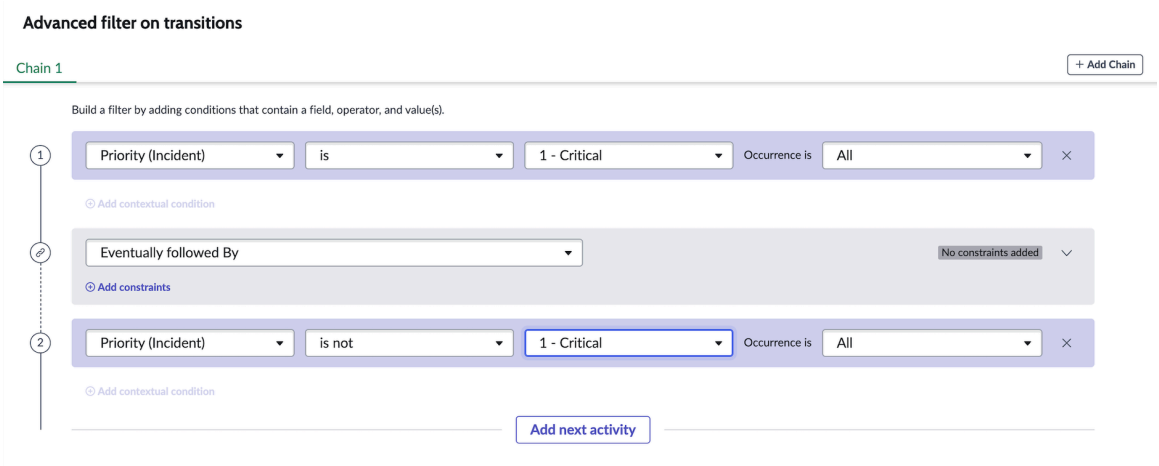
Im Folgenden finden Sie Beispielschritte zum Abrufen der Liste der Security Incidents, für die die Priorität geändert wurde:

1. Navigieren zu **Arbeitsbereiche** > **Process Mining-Arbeitsbereich**an.
2. Öffnen Sie ein Projekt, und navigieren Sie zu **Workbench Für Analysten** .

   Wenn Sie ein Mining-Prozessoptimierungsprojekt öffnen, wird standardmäßig die Workbench für Analysten geöffnet.

3. Wählen Sie **Priorität** aus.
4. Wählen Sie unter Erweiterte Filter die Option aus **Übergänge** .
5. In **Erweiterter Filter für Übergänge** , Konfigurieren Sie Folgendes:
   a. Legen Sie die Priorität auf 1 fest – Kritisch.
   b. Wählen Sie Aus **Schließlich gefolgt von**
   c. Priorität ist nicht 1 – Kritisch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie Aus **Alle Ketten anwenden** .

   Die Karte zeigt alle Security Incidents, denen eine Priorität 1 zugewiesen wurde und deren Priorität später gesenkt wurde.

Engpassanalyse

Sie können das Process Mining verwenden, um die Statusübergänge Ihrer Security Incidents zu überprüfen. Diese Analyse identifiziert die nicht üblichen Übergänge und die dadurch verursachte Zeitverzögerung.

Im Folgenden finden Sie Beispielschritte zum Durchführen der Engpassanalyse:

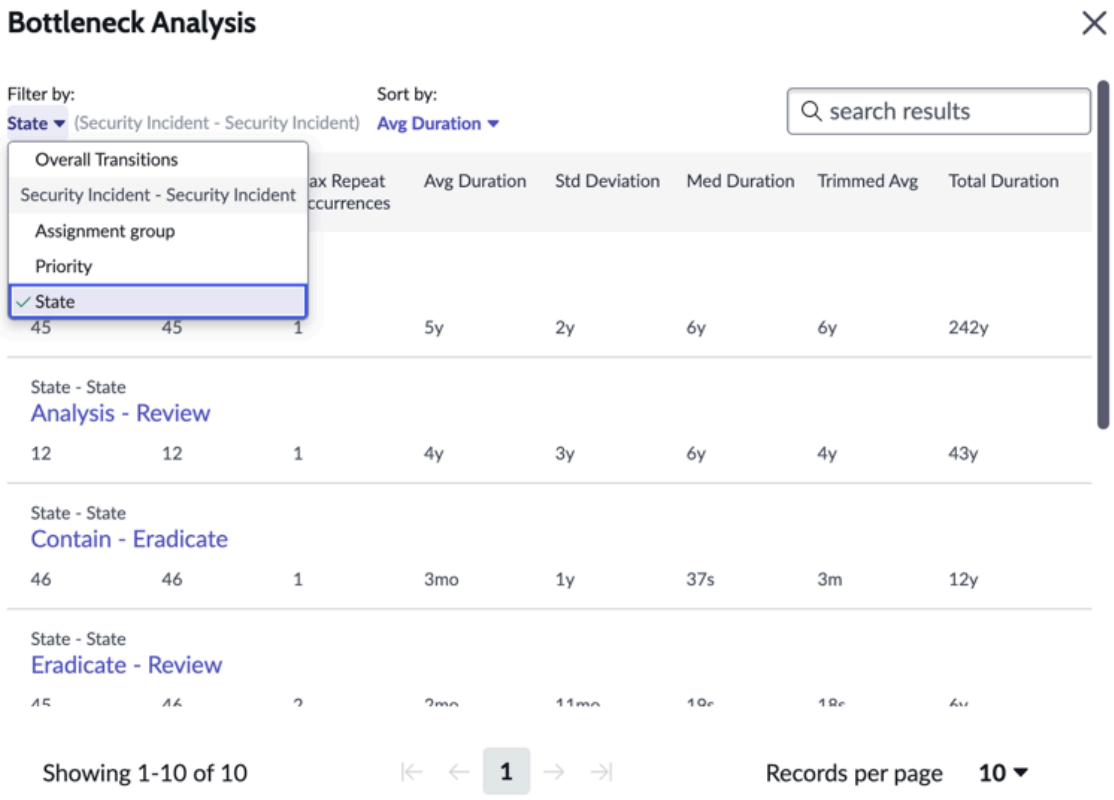
1. Navigieren zu **Arbeitsbereiche** > **Process Mining-Arbeitsbereich**an.
2. Öffnen Sie ein Projekt, und navigieren Sie zu **Workbench Für Analysten** .

   Wenn Sie ein Mining-Prozessoptimierungsprojekt öffnen, wird standardmäßig die Workbench für Analysten geöffnet.

3. Wählen Sie Aus **Engpassanalyse** Von **Modelloptionen** .

   Auf dem Bildschirm werden die Statusübergänge für die Security Incidents angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie aus **Filtern nach** Um Engpassübergänge zu identifizieren. Alternativ können Sie die Suchleiste verwenden, um nach Engpassübergängen zu suchen. Um beispielsweise Incidents zu identifizieren, die aus dem Status „Geschlossen“ in andere status verschoben wurden, verwenden Sie „Geschlossen“ oder „Geschlossen –“.

Lange Zeit bis zum Start als Lösung

Sie können das Process Mining verwenden, um die Incidents zu überprüfen, die lange dauern, bis sie in den Status „Entwurf“ gelangen, dann aber in relativ kürzerer Zeit geschlossen wurden.

Im Folgenden finden Sie Beispielschritte zur Identifizierung von Security Incidents, die sich länger als zwei Tage im Status Entwurf befanden und innerhalb von 30 Minuten nach dem Wechsel in den Status Analyse geschlossen wurden:

1. Navigieren zu **Arbeitsbereiche** > **Process Mining-Arbeitsbereich**an.
2. Öffnen Sie ein Projekt, und navigieren Sie zu **Workbench Für Analysten** .

   Wenn Sie ein Mining-Prozessoptimierungsprojekt öffnen, wird standardmäßig die Workbench für Analysten geöffnet.
3. Wählen Sie unter Erweiterte Filter die Option aus **Übergänge** .
4. In **Erweiterter Filter für Übergänge** , Konfigurieren Sie Folgendes:
   a. Festlegen `Status (Incident)` Ist `Entwurf` .
   b. Wählen Sie Aus **Schließlich gefolgt von**
   c. Wählen Sie Aus **Fügen Sie Einschränkungen hinzu** Und festgelegt **Von** Als `2` Tage.
   d. Wählen Sie Aus **Fügen Sie die nächste Aktivität hinzu** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Festlegen Status (Incident) Ist in Analyse .

f. Wählen Sie Aus **Schließlich gefolgt von**

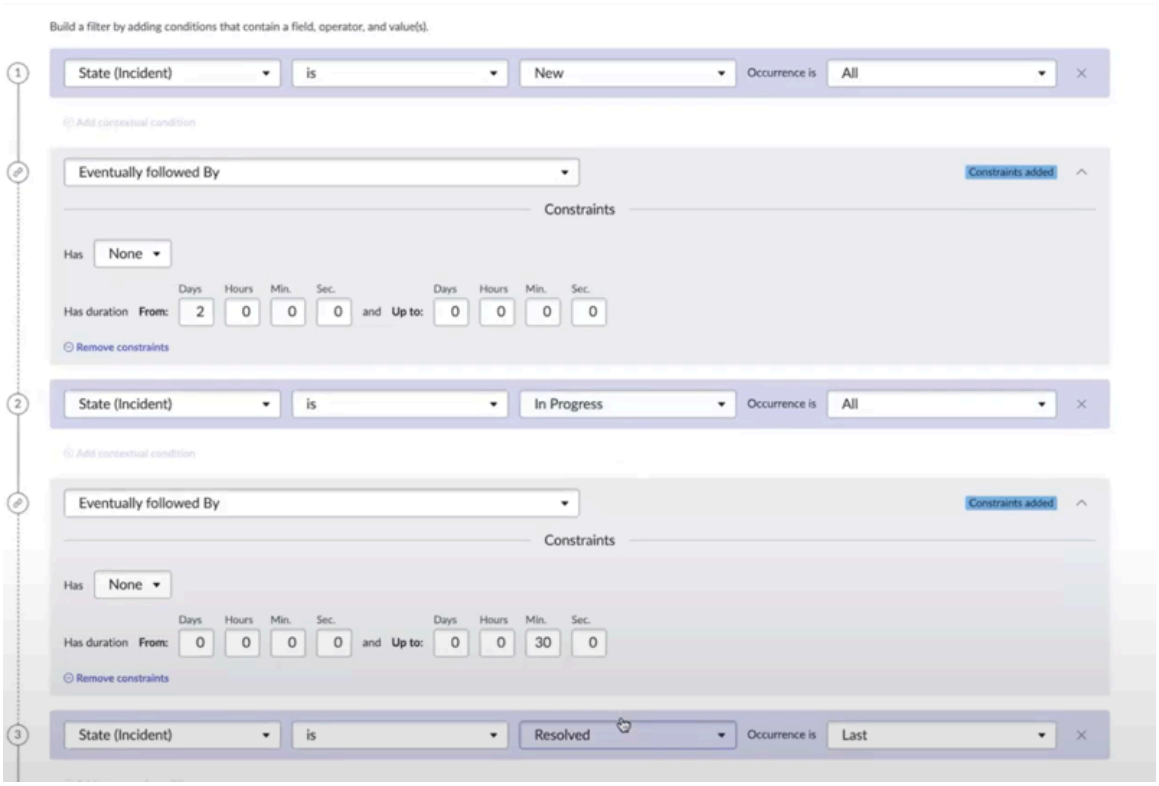
g. Wählen Sie Aus **Fügen Sie Einschränkungen hinzu** Und festgelegt **Bis zu** Als 30 Minuten.

h. Wählen Sie Aus **Fügen Sie die nächste Aktivität hinzu** .

i. Wählen Sie Aus **Schließlich gefolgt von**

j. Wählen Sie Aus **Fügen Sie Einschränkungen hinzu** Und festgelegt **Bis zu** Als 30 Minuten.

k. Festlegen Status (Incident) Ist Geschlossen .



5. Wählen Sie Aus **Alle Ketten anwenden** .

6. Wählen Sie Aus **Aufgliederungsfilter** Und sortieren nach **Längste Durchschnittliche Dauer** .

Security Incidents und eingehende Anforderungen verwalten

Nachdem ein Security Incident erstellt wurde, gibt es zahlreiche Arten von Informationen, die hinzugefügt und angezeigt werden können, während Ihre Analyse des Problems auf die Lösung hinarbeitet.

Wichtig:
Die neuesten Funktionen in Security Incident Response Sind ausschließlich in verfügbar Arbeitsbereich für Security Incident Response. Installieren oder aktualisieren Sie auf den neuesten Security Incident Response Oder Arbeitsbereich für Security Incident Response Version für den Zugriff auf und die Nutzung von Funktionen wie Schichtübergabe, Risikobewertungsrechner usw.

In diesem Abschnitt wird Folgendes beschrieben:

- Erstellen Sie eine eingehende Anforderung
- Verwalten Sie erkennbare Elemente
- Verwalten Sie Suchen und Scans

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Berechnen Sie den Schweregrad eines Security Incidents
- Verwalten Sie Aktivitäten nach dem Incident
- Schließen Sie Security Incidents

Erstellen Sie eine eingehende Anforderung

Im Gegensatz zu Security Incidents haben eingehende Anforderungen im Allgemeinen eine niedrigere Priorität. Anforderungen für eine Suche, einen Scan oder ein neues Abzeichen sind Beispiele für eingehende Anforderungen.

Vorbereitungen

Erforderliche Rollen: sn_si.Basic-Rolle oder höher

Prozedur

1. Navigieren Sie zu einem der Anforderungsformulare.
   Beispiel: **Alle** > **Security Incident** > **Eingehende Anfragen** > **Mir zugewiesen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Sicherheitsanforderung

Feld	Beschreibung
Anzahl	[Schreibgeschützt] die automatisch generierte Sicherheitsanforderungsnummer.
Unternehmen	Das Unternehmen der anfordernden Person.
Standort	Der CI-Standort, falls zutreffend. Dieses Feld ist vorab ausgefüllt, wenn das CI ausgewählt wird.
Konfigurationselement	Das von der Anforderung betroffene Konfigurationselement.
Priorität	Die Priorität der Anforderung.
Geöffnet	[Schreibgeschützt] Datum und Uhrzeit des Öffnens der Anforderung.
Status	Der aktuelle Status der Sicherheitsanforderung. Bei der Erstellung der Sicherheitsanforderung ist dieses Feld standardmäßig auf festgelegt **Entwurf** .
Zuweisungsgruppe	Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird.
Zugewiesen an	Die Person, die der Ausführung der Arbeit zugewiesen ist.
Kurzbeschreibung	Eine kurze Beschreibung der Sicherheitsanforderung, die für die anfordernde Person sichtbar ist.
Beschreibung	Die vollständige Beschreibung der Anforderung, die für die anfordernde Person sichtbar ist.
Arbeitsnotizen	Arbeitsnotizen, die für die anfordernde Person sichtbar sind.

4. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.
5. Wenn Sie die Anforderung zu einem Security Incident eskalieren müssen, klicken Sie auf **In Security Incident konvertieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie erkennbare Elemente

Erkennbare Elemente sind Artefakte, die in einem Netzwerk oder Betriebssystem gefunden werden und wahrscheinlich auf einen Angriff hinweisen. Typische erkennbare Elemente sind IP-Adressen, MD5-Hashes von Malware-Dateien oder URLs oder Domänennamen. Threat Intelligence Tabellendaten erkennbarer Elemente sind innerhalb eines Security Incidents verfügbar.

Informationen zu erkennbaren Elementen umfassen Wert, Typ, Kontext und Zeitstempel.

Sie können erkennbare Elemente manuell oder automatisch über Suchanforderungen erstellen oder löschen.

Ein neuer **Ergebnis** Spalte wurde zu hinzugefügt **Ergebnisse Der Bedrohungssuche** Registerkarte. Mögliche Werte sind: Böswillig und Unbekannt.

Wenn eine IOC-Suchanforderung kein erkennbares Security Incident-Element findet, wird es als Unbekannt bezeichnet.

Wenn eine IOC-Suchanforderung einen Security Incident erkennt, wird er als böswillig bezeichnet.

Während eines Upgrades haben vorhandene Elemente die **Ergebnis** Spalte auf schädlich festgelegt.

Hinweis:
Während Threat Intelligence Tabellendaten erkennbarer Elemente sind Teil eines Security Incidents, keine andere Interaktion mit Threat Intelligence Modul ist enthalten. Für vollständige Bedrohungsfunktionalität die Threat Intelligence Plugin ist als Abonnement verfügbar.

Zugehörige Informationen

Erstellen Sie ein erkennbares Security Incident-Element

IOC-Informationen für einen Security Incident anzeigen

Sie können IOC-Informationen anzeigen, z. B. Suchergebnisse für erkennbare Elemente und Sichtungen, die einem Security Incident zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie IOC-bezogene Informationen anzeigen möchten.
2. Klicken Sie auf **IOC anzeigen** Zugehöriger Link.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

Registerkarte	Beschreibung
Erkennbare Elemente	Zeigen Sie dem Security Incident zugeordnete erkennbare Elemente an, fügen Sie sie manuell hinzu oder bearbeiten Sie sie. Weitere Informationen finden Sie unter Verwalten Sie erkennbare Elemente.
Zugehörige Indikatoren	Wenn Threat Intelligence Ist aktiviert, können Sie alle anderen Indikatoren anzeigen, die einem der gleichen Bedrohungsdatensätze zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte	Beschreibung
Ergebnisse der Sichtungssuche	Enthält Sichtungssuchergebnisse.
Details einer Sichtungssuche	Enthält Details zum Sichtungssuchdatensatz.
Bedrohungssuchen	Speichert Ergänzungsdaten aus Malware-Erkennungssystemen. Diese Registerkarte wird nur angezeigt, wenn Threat Intelligence Plugin ist installiert.
Zugehörige Angriffsmodi/-methoden	Wenn Threat Intelligence Ist aktiviert, können Sie alle anderen Angriffstypen anzeigen, die einem der gleichen Bedrohungsdatensätze zugeordnet sind.
Anforderungen für Sicherheitsprüfung	Wenn Threat Intelligence Ist aktiviert, können Sie Scan- und Suchanforderungen anzeigen, die an den Security Incident angehängt sind.
Ressourcen mit ähnlichem IoC	Wenn Threat Intelligence Ist aktiviert, können Sie alle anderen Ressourcen mit ähnlichen Indikatoren anzeigen.
Anwender mit ähnlichem IoC	Wenn Threat Intelligence Ist aktiviert, können Sie alle anderen Anwender mit ähnlichen Indikatoren anzeigen.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Betroffene Elemente anzeigen
   - Zugehörige Elemente anzeigen
   - Ergänzungsdaten anzeigen
   - Antwortaufgaben anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Erstellen Sie ein erkennbares Security Incident-Element

Sie können ein erkennbares Element in einem Security Incident erstellen und anzeigen und entsprechende Maßnahmen ergreifen. Wenn im Security Incident erkennbare Elemente verfügbar sind, ist dies skalierbar und reduziert die Antwortzeit.

Vorbereitungen

Erforderliche Rolle:

- sn_ti_erkennbares Element.schreiben (schreiben)
- sn_ti_Observable.read (lesen)
- sn_ti_Observable.admin (löschen)

Prozedur

1. Navigieren Sie zu **Security Incident** .
2. Wählen Sie einen Incident aus.
3. Klicken Sie Auf **Erkennbare Security Incident-Elemente** Registerkarte „zugehörige Liste“.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die entsprechenden Felder im Formular aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Klassifizierungs-Tag auswählen	Wenn Sie eingerichtet und aktiviert haben Sicherheits-Tags Um dem Datensatz Metadaten hinzuzufügen, können Sie ein oder mehrere Tags auswählen, um den Grad der Empfindlichkeit des erkennbaren Elements anzugeben. Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt.
Wert	Der Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist. **Hinweis:** Wenn ein Bedrohungsscan durchgeführt wird Bei einer IP-Adresse oder einem Hash, bei der Malware oder einem anderen Fehler zurückgegeben wurde, wird die IP-Adresse oder der Hash-Wert automatisch der Tabelle des erkennbaren Elements [sn_ti_observable] hinzugefügt. Daher kann sie über das Formular „erkennbare Elemente“ gesucht werden.
Typ des erkennbaren Elements	Wählen Sie die Klassifizierung erkennbarer Elemente aus, z. B. eine IP-Adresse oder einen Datei-Hash. Diese Typen erkennbarer Elemente sind in definiert **Typen Erkennbarer Elemente** Modul.
Incident-Anzahl	Gibt an, wie oft der Wert des erkennbaren Elements aufgetreten ist.
Ist Zusammensetzung	Dieses Feld wird erst angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde. Wenn **Typ Des Erkennbaren Elements** Ist auf alles andere festgelegt **Zusammensetzung Erkennbarer Elemente** , Und dieses neue erkennbare Element ist eine Zusammensetzung, aktivieren Sie dieses Kontrollkästchen. Wenn **Typ Des Erkennbaren Elements** Ist bereits auf festgelegt **Zusammensetzung Erkennbarer Elemente** , Das Kontrollkästchen ist aktiviert und schreibgeschützt. Eine Zusammensetzung eines erkennbaren Elements ist ein erkennbares Element, das untergeordnete erkennbare Elemente enthält.
Ergebnis	Wählen Sie eine der folgenden Optionen aus: ○ **Böswillig** : Gibt an, dass das erkennbare Element für die Organisation schädlich ist. ○ **Verdächtig** : Gibt an, dass das erkennbare Element für die Organisation schädlich sein könnte. ○ **Bereinigen** : Gibt an, dass das erkennbare Element für die Organisation nicht schädlich ist. ○ **Unbekannt** : Gibt an, dass wir das Ergebnis des erkennbaren Elements noch bestimmen müssen. ○ Standardwert: Unbekannt. Weitere Informationen finden Sie unter Rechner für Funde der Bedrohungssuche.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Nach einem Upgrade werden vorhandene erkennbare Elemente als schädlich markiert.
Operator	Dieses Feld wird nur angezeigt, wenn **Ist Zusammensetzung** Das Kontrollkästchen ist aktiviert. Abhängig von Ihrer Einstellung in diesem Feld werden die erkennbaren Elemente und ihre untergeordneten Elemente bei der Entscheidung berücksichtigt, ob ein zugeordneter Indikator vorhanden ist. Legen Sie dieses Feld auf fest **UND** Wenn alle untergeordneten erkennbaren Elemente vorhanden sein müssen, damit ein zugehöriger Indikator als vorhanden betrachtet wird. Legen Sie sie auf fest **ODER** Ob eines der untergeordneten erkennbaren Elemente vorhanden ist, damit ein zugehöriger Indikator als vorhanden betrachtet wird.
Darf nicht vorhanden sein	Dieses Feld wird erst angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde. Wenn diese Option ausgewählt ist, gibt dieses Feld an, dass das Fehlen des erkennbaren Elements das potenzielle Problem ist (z. B. ein fehlender Registrierungsschlüssel).
Standort	Mithilfe der Einstellungen in zwei Eigenschaften und einer Skripteinbindungsdefinition können Sie laden Laden Sie weitere IOC-Daten In diesem Feld.
Notizen	Geben Sie zusätzliche Notizen zum erkennbaren Element ein.

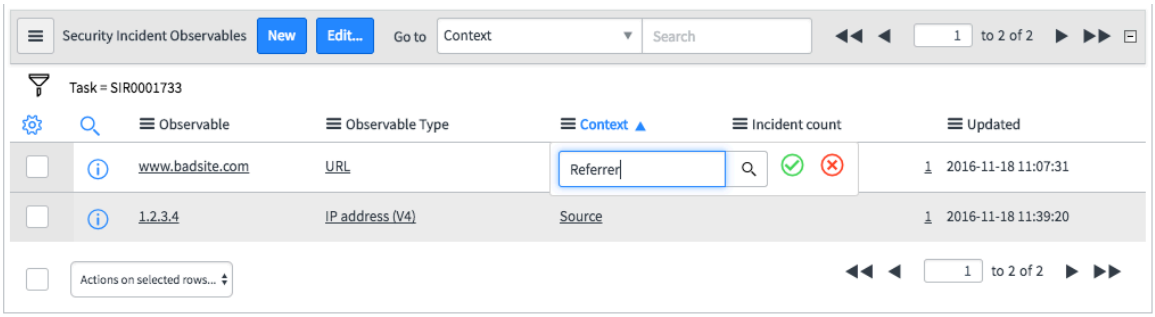
6. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**. Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

Zugehörige Liste	Beschreibung
Zugehörige Indikatoren	Listet Indikatoren auf, die von der Bedrohungsquelle identifiziert wurden.
Zugehörige Aufgaben	Listet Changes auf, die dem erkennbaren Element zugeordnet sind.
Untergeordnete erkennbare Elemente	Listet zugehörige erkennbare Elemente auf, die von der Bedrohungsquelle identifiziert wurden.
Übereinstimmende Ressourcen für IP	Wenn das erkennbare Element eine IP-Adresse ist, werden in dieser Liste alle Ressourcen (Konfigurationselemente) angezeigt, die eine übereinstimmende IP-Adresse haben.
Quelle erkennbare Elemente	Listet die Quellen dieses erkennbaren Elements zusammen mit dem Konfidenzniveau der Quelle auf.
Sicherheitsanmerkungen	Listet Sicherheitsanmerkungen auf, die diesem erkennbaren Element hinzugefügt wurden.

7. Zurück zum Security Incident sind die folgenden Informationen verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie dem Security Incident ein erkennbares Element hinzufügen, sucht das System nach anderen Konfigurationselementen oder Anwendern, die ihm zugeordnet sind. Die **Zugehörige Konfigurationselemente** Und **Zugehörige Anwender** Registerkarten der zugehörigen Liste werden entsprechend aktualisiert.



Spalte	Definition
Erkennbares Element	Der Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist.
Erkennbarer Typ	Der spezifische Typ des erkennbaren Elements.
Kontext	Vom Anwender ausgewählt. Die Auswahlmöglichkeiten lauten wie folgt: ○ IP: Quelle oder Ziel **Hinweis:** Wenn Threat Intelligence Und Palo Alto Networks – Firewall Sind aktiviert, verursacht das Ändern oder Hinzufügen eines Werts zu diesem Feld die Protokolldaten-Flow Abrufen Security Operations Palo Alto Networks – Protokolldaten Abrufen Auszuführender Workflow. Der Workflow ruft angereicherte Bedrohungsprotokolldaten von der Firewall ab und hängt sie an den Security Incident an. Die Informationen werden auch analysiert und in angezeigt Firewall-Protokolle Abschnitt unter **Ergänzungsdaten** Registerkarte. ○ URL: Referrer **Hinweis:** Wenn der Anwender auf einen Link in einer Phishing-E-Mail klickt, ist ein Referrer die URL des letzten Jumps, bevor auf die Malware-URL zugegriffen wird.
Incident-Anzahl	Die Anzahl der Incidents, in denen dieses erkennbare Element angezeigt wird. Dieser Wert wird automatisch aktualisiert, wenn das erkennbare Element manuell oder über einen Workflow einem anderen Incident hinzugefügt wird.
Aktualisiert	Daten und Uhrzeit der letzten Aktualisierung der Liste.

Hinweis:
Wenn Threat Intelligence Das Plugin ist installiert. Sie können das erkennbare Element auch in anzeigen **Erkennbare Elemente** Liste in **IOC-Repository** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Bearbeiten Sie eine Security Incident-Liste erkennbarer Elemente

Fügen Sie mehrere erkennbare Security Incidents hinzu S

Verwalten Sie erkennbare Dateielemente

„Erkennbare Dateielemente verwalten“ bietet strenge Sicherheitsmaßnahmen zum Speichern verdächtiger Dateien und aktiviert die erkennbaren Dateitypen für die Sandbox-Integration.

Vorbereitungen

Erforderliche Rolle: sn_ti_böswillig_attachment_Access (Upload)

Laden Sie die erkennbaren Dateitypen hoch:

- Automatisch: Wenn Security Incidents für die Phishing-E-Mails erstellt werden, werden die Anhänge in der Phishing-E-Mail als erkennbare Dateitypen erstellt.
- Manuell: Ein Sicherheitsanalyst kann die verdächtigen Dateien auch hochladen, um erkennbare Dateitypen zu erstellen.

Warum und wann dieser Vorgang ausgeführt wird

Sie können erkennbare Dateitypen für einen Security Incident erstellen und anzeigen. Die verdächtigen Dateien, die Teil der erkennbaren Elemente sind, werden an einem bestimmten Ort gespeichert, auf den der Sicherheitsanalyst zugreifen kann, um die Datei nur mit einer bestimmten Rolle herunterzuladen.

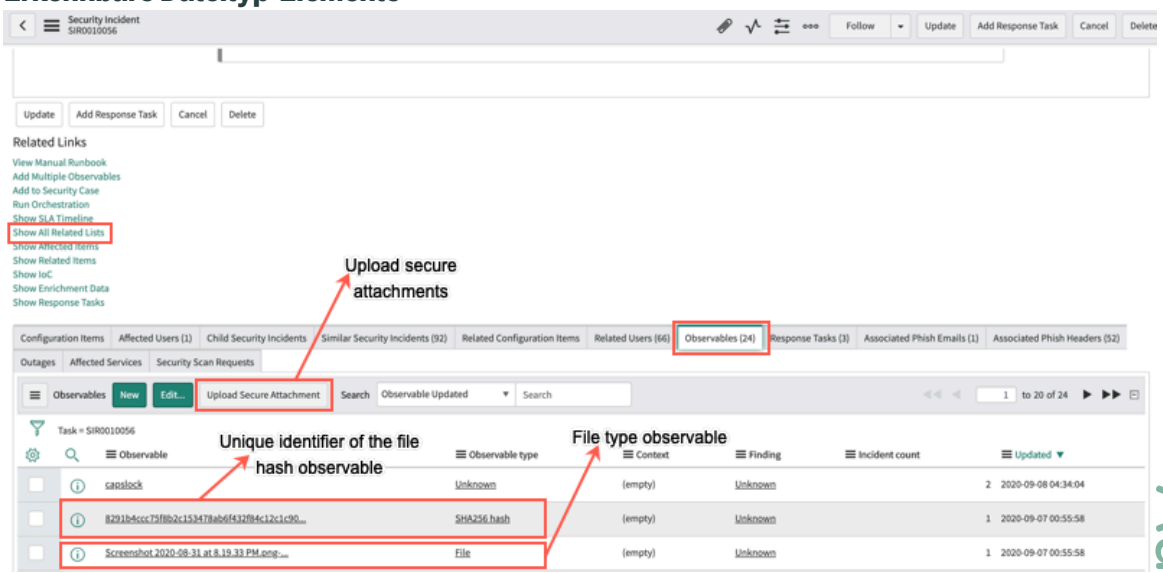
Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie Aus **Erkennbare Elemente** Von **Alle Zugehörigen Listen Anzeigen** Registerkarte.

   Wenn die Phishing-E-Mail Anhänge enthält, werden diese Anhänge standardmäßig als erkennbare Dateitypen im entsprechenden Security Incident erstellt. Jeder Anhang wird als zwei erkennbare Elemente wie Dateityp und Datei-Hash-Element erstellt.
3. So laden Sie die sicheren Anhänge manuell hoch:
   - Klicken Sie Auf **Sicheren Anhang Hochladen** .
   - Klicken Sie unter sichere Anhänge hochladen auf **Wählen Sie die Datei aus** Zum Hochladen einer oder mehrerer Dateien. Jede Datei wird als einzelner Datensatz erkennbarer Elemente betrachtet.
   - Klicken Sie Auf **Datei Erkennbare Elemente Erstellen** Zum Erstellen des Dateityps erkennbare Elemente, z. B. das eine ist der Dateityp und das andere der Datei-Hash, der ein eindeutiger Bezeichner ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennbare Dateityp-Elemente



Wählen Sie den Dateityp des erkennbaren Elements aus, das für weitere Integrationen wie Sandbox oder Bedrohungssuche verarbeitet werden soll. Darüber hinaus können Sie die Anhänge auch aus dem Dateityp „erkennbares Element“ herunterladen.

Hinweis:

Die Bedrohungssuche (VirusTotal) ruft die Datei aus den gesicherten Anhängen für die neuen erkennbaren Dateitypen ab, und die folgenden Systemeigenschaften gelten nicht für die neuen erkennbaren Dateitypen.

- sn_ti.scan.delete_attachment_after_hash
- sn_ti.scan.use_file_hash

Als Schnellreferenz wird der Dateityp erkennbares Element dem erkennbaren Hash-Element als untergeordnetes Element zugeordnet, und das erkennbare Hash-Element wird dem erkennbaren Element der Datei als untergeordnetes Element zugeordnet.

Wenn die Phishing-E-Mail-Anhänge die definierte Größe überschreiten, werden die erkennbaren Elemente nicht erstellt. Sie müssen die Systemeigenschaften ändern, um größere Dateien zu unterstützen.

Systemeigenschaften für Dateigröße

Systemeigenschaft	Beschreibung
glide.email.inbound.max_total_attachment_size_bytes	Wenn Sie die Phishing-E-Mail direkt weiterleiten, verwenden Sie diesen Systemeigenschaftswert, um die Dateigröße von 18 MB auf eine gewünschte Dateigröße zu erhöhen.
Com.Glide.attachment.max_get_size	Wenn Sie die Phishing-E-Mail als Anhang weiterleiten, verwenden Sie diesen Systemeigenschaftswert, um die folgenden Systemeigenschaften im globalen Bereich zu erstellen, um die Dateigröße von 5 MB auf die gewünschte Größe zu erhöhen.

Sie können auch wie folgt ein neues erkennbares Element vom Dateityp erstellen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf **Neu**.

b. Wählen Sie aus **Typkategorie des erkennbaren Elements: Datei**

c. Klicken Sie Auf **Hochladen** Zum Anhängen einer Datei.

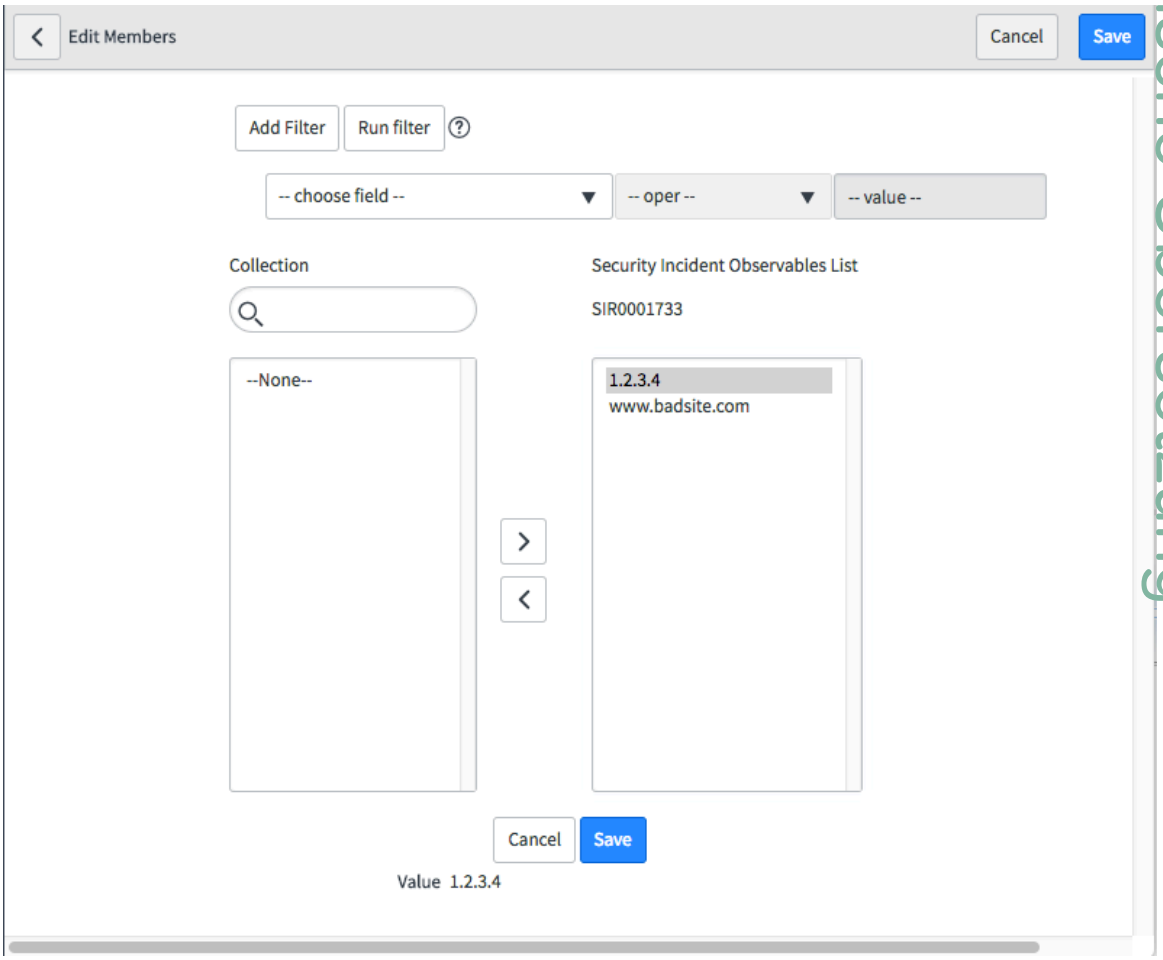
Bearbeiten Sie eine Security Incident-Liste erkennbarer Elemente

Sie können bearbeiten, welche erkennbaren Elemente in der Liste, die einem Security Incident zugeordnet sind, angezeigt werden sollen.

Vorbereitungen
Erforderliche Rolle: sn_si.Basic

Prozedur

1. Navigieren Sie zu **Security Incident** .
2. Wählen Sie einen Incident aus.
3. Klicken Sie Auf **Erkennbare Security Incident-Elemente** Registerkarte „zugehörige Liste“.
4. Klicken Sie auf **Bearbeiten**.
5. Fügen Sie der Liste erkennbare Elemente hinzu, oder entfernen Sie sie.
   Erstellen Sie einen Filter für lange Listen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Speichern**.

Hinweis:
Wenn Sie dem Security Incident ein erkennbares Element hinzufügen, sucht das System nach anderen Konfigurationselementen oder Anwendern, die ihm zugeordnet sind. Die **Zugehörige Konfigurationselemente** Und **Zugehörige Anwender** Registerkarten der zugehörigen Liste werden entsprechend aktualisiert. Auch, wenn Threat Intelligence Plugin ist aktiviert, und Sie haben mindestens eines Security Incident Response-Integrationen Integrationsimplementierung aktiviert, der Integration von Security Operations: Fähigkeit zur Bedrohungssuche Führt einen oder mehrere Workflows aus, und für die von Ihnen hinzugefügten erkennbaren Elemente werden nach Bedrohungssicherheit gesucht. Die Ergebnisse werden in angezeigt **Ergebnisse Der Bedrohungssuche** Registerkarte.

Zugehörige Informationen

Fügen Sie mehrere erkennbare Security Incidents hinzu S

Erstellen Sie ein erkennbares Security Incident-Element

Fügen Sie mehrere erkennbare Security Incidents hinzu S

Um Zeit zu sparen, können Sie der Liste erkennbarer Security Incident-Elemente mehrere erkennbare Security Incident-Elemente hinzufügen.

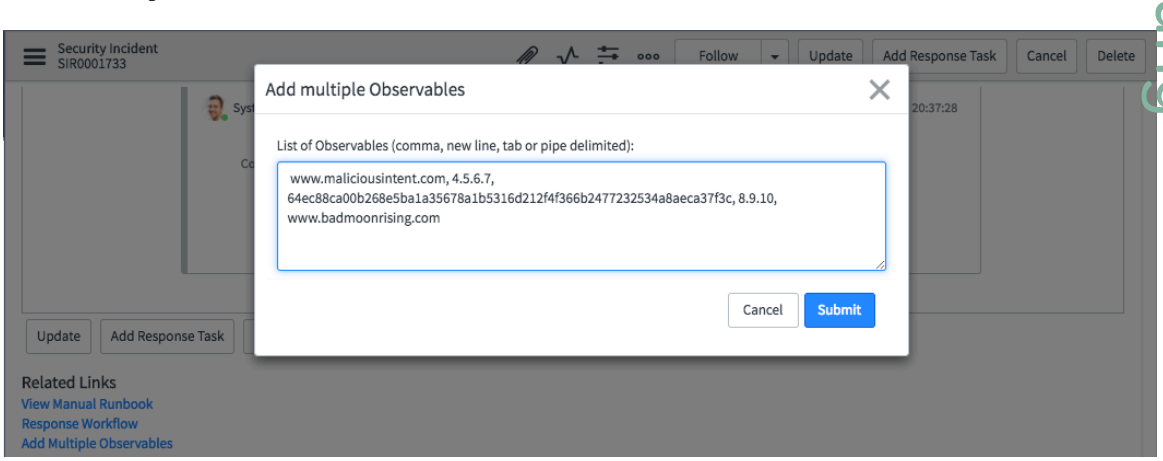
Vorbereitungen

Erforderliche Rolle: sn_ti_write

Hinweis:
Beim Hinzufügen mehrerer erkennbarer Security Incident-Elemente werden Duplikate während der Verarbeitung ignoriert.

Prozedur

1. Navigieren Sie zu **Security Incident** .
2. Wählen Sie einen Incident aus.
3. Klicken Sie auf **Fügen Sie Mehrere Erkennbare Elemente Hinzu** Zugehöriger Link.
4. Geben Sie mehrere erkennbare Elemente ein, oder fügen Sie sie ein.
   Einträge können einen beliebigen erkennbaren Typ haben. Akzeptierte Formate sind: Komma, neue Zeile, Registerkarte oder Pipe-Trennzeichen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie dem Security Incident ein erkennbares Element hinzufügen, sucht das System nach anderen Konfigurationselementen oder Anwendern, die ihm zugeordnet sind. Die **Zugehörige Konfigurationselemente** Und **Zugehörige Anwender** Registerkarten der zugehörigen Liste werden entsprechend aktualisiert.

Hinweis: Werte erkennbarer Elemente, die nicht automatisch erkannt werden, werden dem Typ „Unbekannt“ zugewiesen.

5. Klicken Sie auf **Absenden**.

Automatische Ergänzung der Protokolldaten für erkennbare Security Incidents

Wenn bestimmte Anwendungen und Integrationen eingerichtet sind, einschließlich Threat Intelligence Und Palo Alto Networks – Firewall Integration: Informationen zu erkennbaren Elementen in einem Security Incident können automatisch mit Bedrohungsprotokolldaten ergänzt werden, wenn die Quell-IP für ihre erkennbaren Elemente geändert wird.

Wenn eine Änderung auftritt, initiiert eine Business-Regel einen Workflow, der Daten aus Bedrohungsprotokollen in Ihrer Firewall abruft und die Informationen erkennbarer Elemente im Security Incident ergänzt.

Bevor erkennbare Elemente angereichert werden können, müssen die folgenden Schritte ausgeführt werden.

- Threat Intelligence Muss aktiviert sein.
- Die Palo Alto Networks-Firewall Die Integration muss aktiviert und konfiguriert sein. Dies kann auch sein Richten Sie SSH-Anmeldeinformationen für den MID-Server ein.

Nachdem dieses Setup abgeschlossen wurde, führt das Ändern der Quell-IP von erkennbaren Elementen, die einem Security Incident zugeordnet sind, dazu, dass eine Geschäftsregel ausgeführt wird **Security Operations Palo Alto Networks – Protokolldaten Abrufen** Workflow. Workflow-Aktivitäten stellen eine Suchabfrage in der Firewall in die Warteschlange und geben eine Auftrags-ID zurück, mit der Bedrohungsprotokolldaten aus der Firewall abgerufen und als XML-Datei an den Security Incident angehängt werden.

Zugehörige Informationen

Abrufen des Autofokus-Sitzungsinformationsanreicherungs-Flows

Palo Alto Networks Firewall-Startprogramm-Workflow

Security Operations Palo Alto Networks – Wert-Workflow überprüfen und blockieren

Protokolldaten-Flow Abrufen

Wildfire-Datenanreicherungs-Flow abrufen

Veröffentlichen Sie erkennbare Elemente in einer Beobachtungsliste einer Drittpartei

Sie können ein oder mehrere erkennbare Elemente oder zugehörige Indikatoren in einer Beobachtungsliste einer Drittpartei veröffentlichen. Derzeit ist CrowdStrike Falcon Host die einzige Implementierung, die diese Funktionalität unterstützt.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

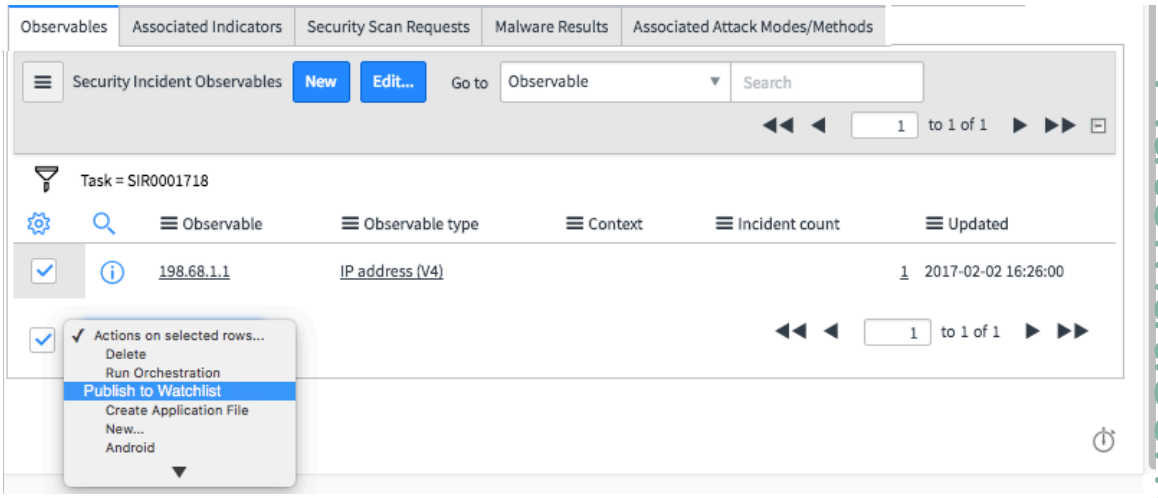
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

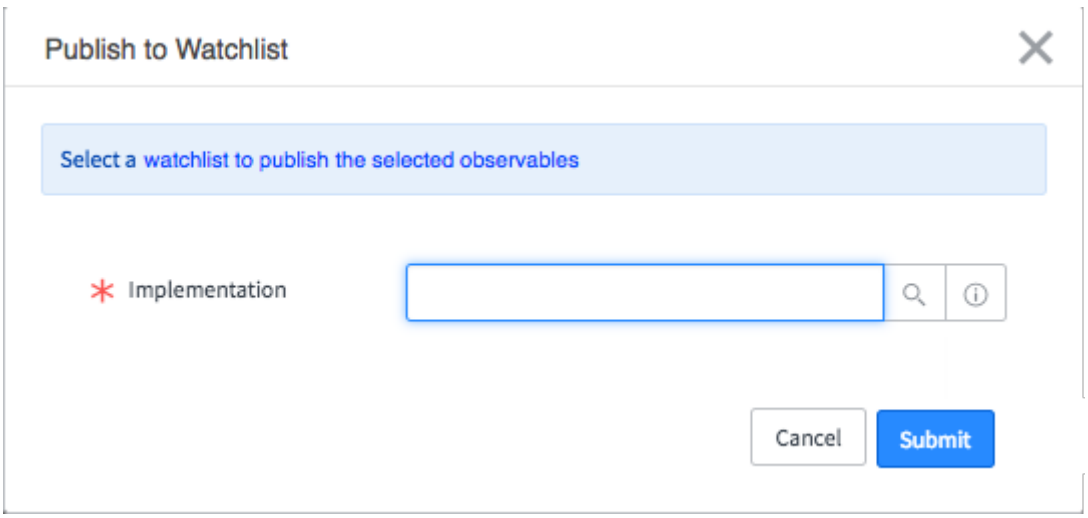
Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie Aus **Erkennbare Elemente** Von **Zugehörige Liste** Registerkarte.
3. Klicken Sie Auf **In Beobachtungsliste veröffentlichen** In **Aktionen für ausgewählte Zeilen...** Dropdown-Menü.



Das Dialogfeld wird angezeigt.



4. Geben Sie die Implementierung ein, oder wählen Sie sie aus.

Hinweis:
Ein Workflow wird von ausgelöst Integration von Security Operations: Funktion „in Beobachtungsliste veröffentlichen“ Wenn Sie die CrowdStrike Falcon Host-Implementierung auswählen.

5. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie Suchen und Scans

Sie können Suchen und Schwachstellen-Scans von Security Incidents und aus dem Security Incident-Katalog durchführen, um potenzielle Bedrohungen und Schwachstellen zu identifizieren.

Senden Sie eine IOC-Suchanforderung aus einem Security Incident

Eine IOC-Suche wird automatisch ausgeführt, wenn erkennbare Elemente einem Security Incident hinzugefügt werden. Wenn Ihr Security Incident Anhänge enthält, können Sie sie auch per Knopfdruck finden.

Vorbereitungen

Für automatische IOC-Suchen, die Threat Intelligence Plugin muss aktiviert sein.

Erforderliche Rolle: sn_si.Basic

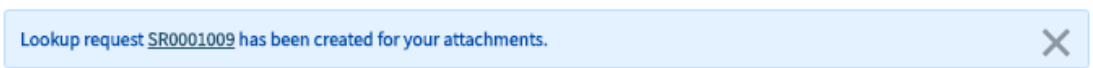
Hinweis:
Standardmäßig ist **Suchtyp** Für **Datei** Ist inaktiv.

Prozedur

1. Erstellen Sie einen neuen Security Incident Oder öffnen Sie eine vorhandene, wenn Sie neue Dateien daran anhängen möchten.
2. Klicken Sie auf das Büroklammersymbol im Formularheader, und hängen Sie eine oder mehrere Dateien an.
3. Wenn Sie Ihre Einträge im Formular abgeschlossen haben, klicken Sie mit der rechten Maustaste auf den Formularheader, und klicken Sie auf **Speichern** .
   Nachdem der Datensatz gespeichert wurde, wird ein **Suchen Sie nach Anhängen** Schaltfläche wird angezeigt.
4. Klicken Sie Auf **Suchen Sie nach Anhängen** .

   Hinweis:
   Die Arbeitsnotizen unter **Incident-Details** Melden Sie den Fortschritt des Suchprozesses.

5. Sie können auf die Suchnummer am Ende der Nachricht klicken, um den Suchdatensatz anzuzeigen.
   Sie können auf den Referenzlink „Suchen“ klicken, um detaillierte Ergebnisse anzuzeigen.



Senden Sie eine IOC-Suchanforderung von Security Incident Catalog

Wenn Security Incident Response Das Plugin ist aktiviert. Sie können Bedrohungssuchen für Dateien, Hash-Werte, URLs und IP-Adressen aus dem Security Incident-Katalog übermitteln. Die Anforderungen werden übermittelt, und Sie können die Ergebnisse in anzeigen **Meine Anforderungen** Modul.

Vorbereitungen

Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird

Für den Standardsuchtyp werden für jede Suchquelle, die im Suchdatensatz aufgeführt ist, automatisch Suchvorgänge durchgeführt. Die Ergebnisse der Suchanforderung sind in verfügbar **Meine Anforderungen** Modul.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Self-Service** > **Security Incident-Katalog**an.
2. Klicken Sie Auf **IOC-Suche** .
3. Klicken Sie Auf **Suchen Sie nach Dateien, Hash-Werten, URLs oder IP-Adressen** .
4. Geben Sie mindestens eine der folgenden Optionen ein:

IOC-Suchanforderung

Zu suchendes Element	Beschreibung
Dateien	Klicken Sie auf das Büroklammersymbol, suchen Sie die Dateien, die Sie suchen möchten, und hängen Sie sie an. **Hinweis:** Standardmäßig ist **Suchtyp** Für **Datei** Ist inaktiv. Dateien werden als Hash-Wert konvertiert und übermittelt.
URLs	In **URLs** Geben Sie die URLs, die Sie suchen möchten, durch Kommas getrennt ein. Beispiel: www.abc.com,www.xyz.net.
IP-Adressen	In **IP-Adressen** Geben Sie die IP-Adressen, die Sie suchen möchten, durch Kommas getrennt ein.
Hash-Werte	In **Hash-Werte** Geben Sie die Hash-Werte, die Sie suchen möchten, durch Kommas getrennt ein. **Hinweis:** Wenn **Suchtyp** Für **Datei** Ist inaktiv, dieser Wert ist die Standardaktion für beide **Datei** Und **Hash-Werte** .

5. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Übermitteln** .
6. Um den Status und/oder die Ergebnisse der Suchvorgänge anzuzeigen, navigieren Sie zu **Self-Service** > **Meine Anforderungen**an.
7. Klicken Sie auf die SR-Nummer für die Anforderung.
   Die Arbeitsnotizen unter **Aktivität** Listen Sie die während der Suche ausgeführten Aufgaben auf, einschließlich der Erstellung einzelner Suchvorgänge für jede Datei, jeden Hash-Wert, jede URL oder jede IP-Adresse und die Suchergebnisse.

Senden Sie eine Schwachstellen-Scan-Anforderung von einem Security Incident

Wenn Ihr Security Incident über ein oder mehrere Konfigurationselemente (Server, Computer usw.) verfügt, können sie über auf Schwachstellen gescannt werden Security Incident Response Formular.

Vorbereitungen

Das Vulnerability Response-Plugin muss aktiviert sein.

Erforderliche Rolle: sn_si.write

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

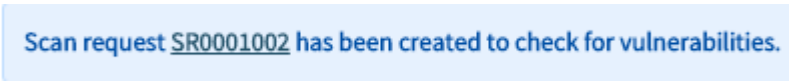
Prozedur

1. Erstellen Sie einen Security Incident Und schließen Sie mindestens eine Ressource ein.
   Sie können auch einen vorhandenen Incident öffnen, der Konfigurationselemente enthält.
2. Wenn Sie Ihre Einträge im Formular abgeschlossen haben, klicken Sie mit der rechten Maustaste auf den Formularheader, und klicken Sie auf **Speichern** .
   Nachdem der Datensatz gespeichert wurde, wird ein **Suchen Sie nach Schwachstellen** Der zugehörige Link wird angezeigt.

   Hinweis:
   Wenn **Suchen Sie nach Schwachstellen** Zugehörige Liste wird nicht angezeigt. Sie müssen zu navigieren **Schwachstelle** > **Scanner**, Richten Sie mindestens einen Scanner ein, und legen Sie den Standardwert auf fest **Wahr** .
3. Klicken Sie Auf **Suchen Sie nach Schwachstellen** .

   Hinweis:

   Oben im Security Incident-Formular wird eine Nachricht mit einem Link zum Scan-Datensatz angezeigt.

4. Sie können auf die Nummer der Scan-Anforderung klicken, um den Scan-Datensatz anzuzeigen.
   Die Incident-Details zeigen die Ergebnisse des Scans im Datensatz der Sicherheitsscan-Anforderung.

Senden Sie eine Anforderung zum Schwachstellen-Scan aus dem Security Incident Response-Katalog

Sie können Schwachstellen-Scans für CIs und IP-Adressen von übermitteln Security Incident Response Katalog. Die Anforderungen werden übermittelt, und Sie können die Ergebnisse in anzeigen **Meine Anforderungen** Modul.

Vorbereitungen

Erforderliche Rolle: keine

Prozedur

1. Navigieren zu **Alle** > **Self-Service** > **Security Incident-Katalog**an.
2. Klicken Sie Auf **Schwachstellen-Scan** .
3. Klicken Sie Auf **Scan-Konfigurationselement und IP-Adressen** .
4. Geben Sie mindestens eine der folgenden Elemente ein, die gescannt werden sollen.

Schwachstellen-Scanner

Zu scannendes Element	Beschreibung
Konfigurationselement	In **Konfigurationselement zum Scannen** Feld das zu scannende CI auswählen.
IP-Adressen	In **Zu scannende IP-Adressen** Geben Sie die IP-Adressen durch Kommas getrennt ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wenn Sie Ihre Auswahl getroffen haben, klicken Sie auf **Übermitteln** .
   Wenn ein erkennbares Element gefunden wird, wird ein Indikator gemäß STIXX-Standards erstellt.
6. Um den Status und/oder die Ergebnisse der Scans anzuzeigen, navigieren Sie zu **Self-Service** > **Meine Anforderungen**an.
7. Klicken Sie auf die SR-Nummer für die Anforderung.
   Die Arbeitsnotizen unter **Aktivitäten** Listen Sie die während des Scans ausgeführten Aufgaben auf, einschließlich der Erstellung einzelner Scans für jedes CI oder jede IP-Adresse und der Ergebnisse der Scans.

Definieren Sie neue Orchestrationen bei Bedarf

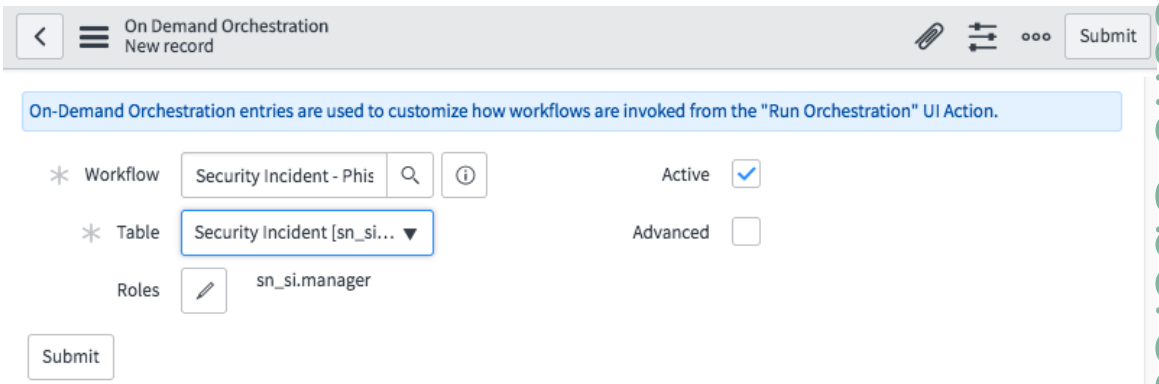
Im Basissystem können Sie Orchestrationen bei Bedarf auswählen, die vordefinierte Workflows ausführen. Sie können neue Orchestrationen bei Bedarf definieren, um anzupassen, wie Workflows über aufgerufen werden **Orchestration Ausführen** Auswahllisten.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Orchestration bei Bedarf**
2. Klicken Sie auf **Neu**.



3. Füllen Sie die Felder entsprechend aus.

Orchestration bei Bedarf

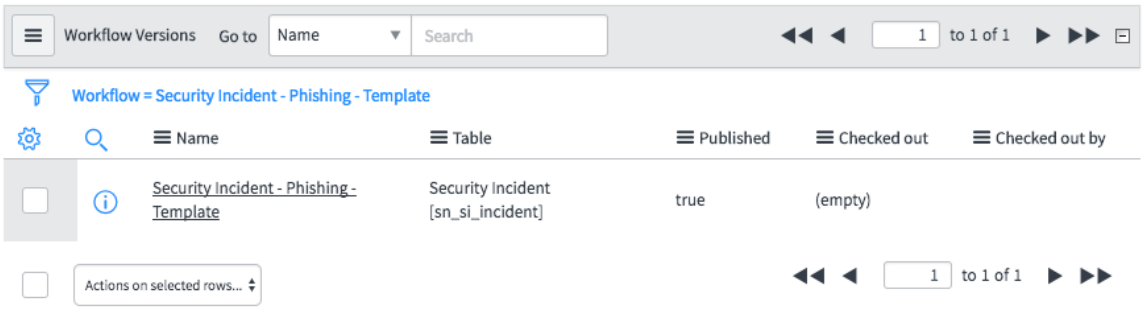
Feld	Beschreibung
Workflow	Wählen Sie den Workflow aus, der in aufgenommen werden soll **Orchestration Ausführen** Auswahlliste.
Tabelle	Wählen Sie die Tabelle aus, für die der ausgewählte Workflow ausgeführt wird. Wenn die Tabelle nicht mit der für den ausgewählten Workflow konfigurierten Tabelle übereinstimmt, müssen Sie auswählen **Erweitert** Aktivieren Sie das Kontrollkästchen, und ändern Sie **Ausführungsskript** Um den richtigen Datensatz bei der Ausführung an den Workflow zu übergeben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Rollen	Wählen Sie bei Bedarf zusätzliche Rollen aus, um einzuschränken, wer diesen Workflow in sehen kann **Orchestration Ausführen** Auswahlliste.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diesen Orchestration-Datensatz bei Bedarf zu aktivieren.
Erweitert	Aktivieren Sie dieses Kontrollkästchen, um das Ausführungsskript so zu ändern, dass es den richtigen Datensatz an die ausgewählte Tabelle für diesen Workflow übergibt.
Ausführungsskript	Ändern Sie das Ausführungsskript so, dass es den richtigen Datensatz an die ausgewählte Tabelle für diesen Workflow übergibt. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Erweitert** aktiviert ist.

4. Klicken Sie mit der rechten Maustaste in den Datensatzheader, und wählen Sie aus **Speichern** .
Die **Workflow-Versionen** Zugehörige Liste wird angezeigt.



5. Wenn Sie zusätzliche Änderungen am Workflow vornehmen müssen, müssen Sie ihn auschecken.

Zugehörige Informationen

Arbeiten Sie mit Workflow-Versionen

Registrieren Sie neue Security Operations-Anwendungen Für Orchestration bei Bedarf

Im Basissystem werden Security Operations-Anwendungen automatisch registriert, wenn sie aktiviert werden. Mit der Registrierung können die den Anwendungen zugeordneten Workflows für Orchestration-Anforderungen bei Bedarf verfügbar sein. Bei Bedarf können Sie neue Anwendungen definieren und ihnen Workflows für die Orchestration bei Bedarf zuordnen.

Vorbereitungen

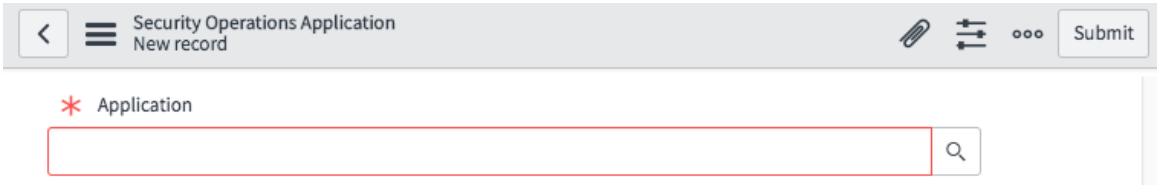
Erforderliche Rolle: sn_si.write

Prozedur

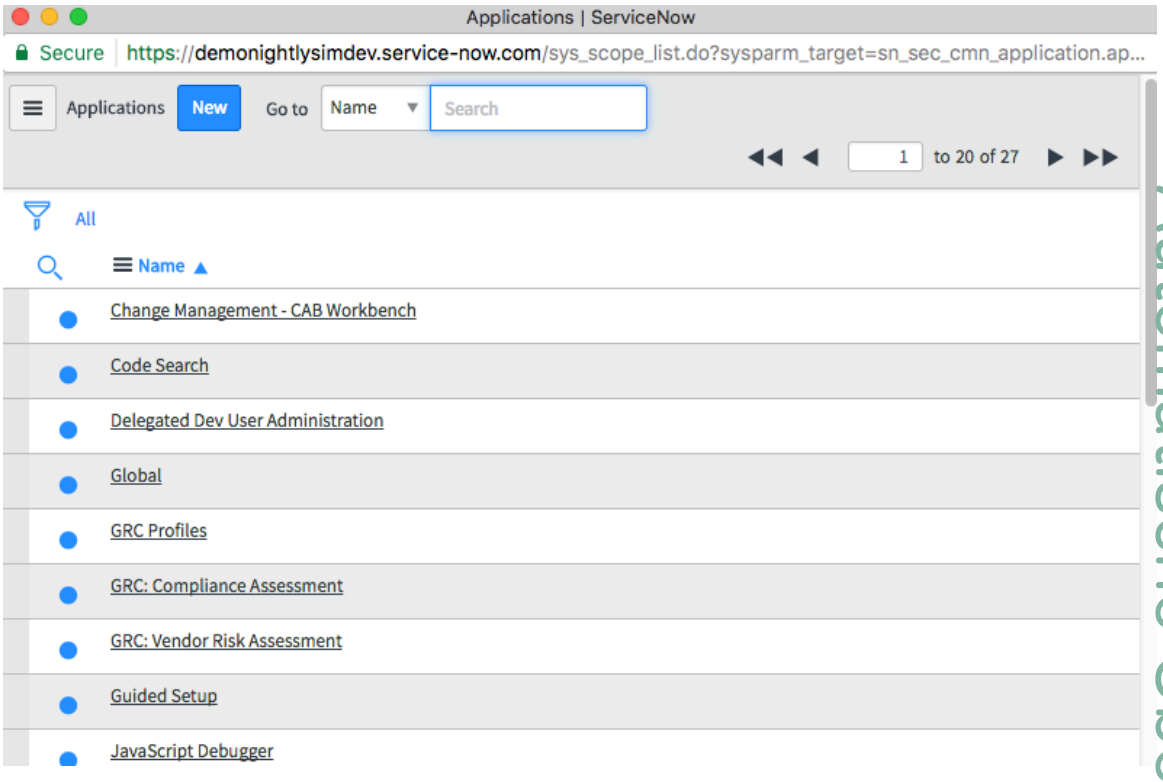
1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **SecOps-Applikationsregistrierung**, Und klicken Sie auf **Anwendung Registrieren** .
Der Bildschirm Security Operations-Anwendung wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



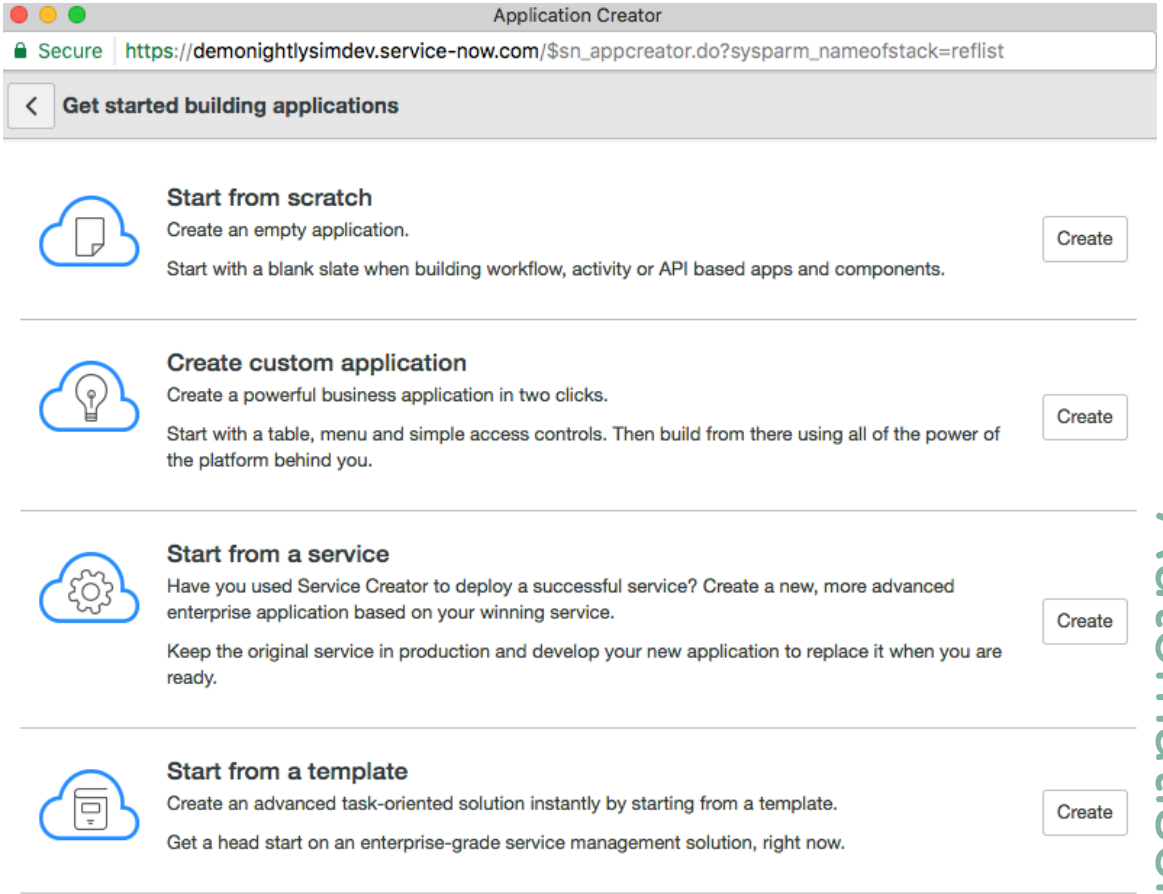
2. In **Anwendung** Klicken Sie auf das Suchsymbol (Lupe).
   Der Bildschirm Anwendungen wird angezeigt.



3. Klicken Sie auf **Neu**.
   Der Bildschirm Anwendungsersteller wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Die angezeigten Optionen hängen von den von Ihnen aktivierten Anwendungen ab. Detaillierte Informationen zum Erstellen neuer Anwendungen finden Sie unter Building applications .

4. Nachdem die Anwendung generiert wurde, können Sie Skripts zum Einrichten der Orchestration bei Bedarf erstellen.

Hinweis:
Das Einrichten der bedarfsgesteuerten Orchestration für neue Anwendungen erfordert fortgeschrittene technische Kenntnisse über Skripterstellung und Erstellung von Auslösern für die Skripts (Geschäftsregeln, UI-Aktion, Workflows usw.). Weitere Informationen erhalten Sie von ServiceNow Professionelle Services.

Fügen Sie einem Security Incident Informationen hinzu

Nachdem ein Security Incident erstellt wurde, können Sie weitere Details hinzufügen, um die Analyse zu unterstützen, z. B. Zugriffsrollen und verschiedene Arten von Notizen.

Vorbereitungen
Erforderliche Rolle: sn_si.Basic

Prozedur

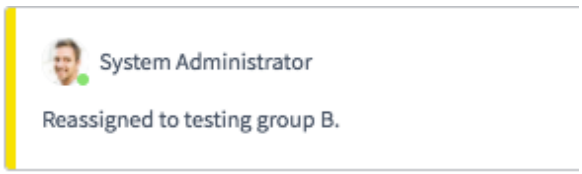
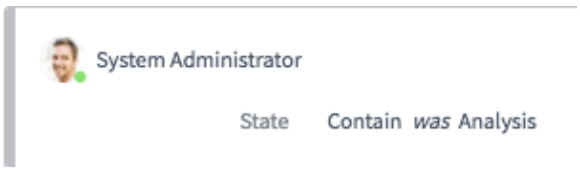
1. Wenn er nicht bereits geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. Klicken Sie auf **Incident-Details** Registerkarte.
3. Füllen Sie die Felder nach Bedarf aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Lesezugriff	Gibt einem Anwender mit **Spezieller Zugriff** Rollenlesezugriff auf den Security Incident. Der Anwender kann Arbeitsnotizen lesen und schreiben. **Hinweis:** ○ Wenn ein Anwender beidem hinzugefügt wird **Lesezugriff** Und **Privilegierter Zugriff** Listet auf, dann nur die **Privilegierter Zugriff** Berechtigungen bleiben erhalten. ○ Anwender mit der Rolle „sn_si.admin“ können sowohl den Lesezugriff als auch den privilegierten Zugriff ändern.
Beobachtungsliste	Klicken Sie auf das Sperrsymbol, um Anwender hinzuzufügen, die benachrichtigt werden, wenn Änderungen am Security Incident auftreten. Nachdem das Feld entsperrt wurde, sind Optionen zum Hinzufügen oder Entfernen mehrerer Anwender oder zum Eingeben von Anwender-E-Mail-Adressen verfügbar. Wenn Sie Ihre Einträge abgeschlossen haben, klicken Sie auf das Schlosssymbol, um das Feld zu sperren.
Privilegierter Zugriff	Gibt einem Anwender mit **Spezieller Zugriff** Rollen-Lese- und Schreibzugriff auf alle Felder des Security Incident außer **Zugewiesen an** . Anwender mit speziellen Zugriffsrollen haben ein eigenes Modul, das alle ihnen zugewiesenen Security Incidents enthält. Für sie sind keine anderen Module verfügbar. Niemand sonst kann sehen **Für mich sichtbar** Modul. **Hinweis:** Nur ein zugewiesener Anwender oder jemand mit einer Sicherheitsrolle (z. B. sn_si_Analyst oder sn_si.admin) kann ändern **Zugewiesen an** Feld. Wenn ein Anwender beidem hinzugefügt wird **Lesezugriff** Und **Privilegierter Zugriff** Listet auf, dann nur die **Privilegierter Zugriff** Berechtigungen bleiben erhalten.
Arbeitsnotizenliste	Klicken Sie auf das Schlosssymbol ( ) Zum Hinzufügen von Anwendern, die benachrichtigt werden, wenn neue Arbeitsnotizen hinzugefügt werden. Nachdem das Feld entsperrt wurde, sind Optionen zum Hinzufügen oder Entfernen

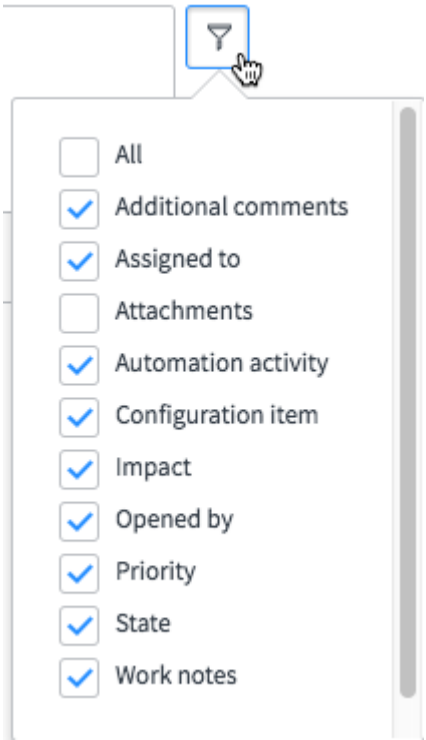
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	mehrerer Anwender oder zum Eingeben von Anwender-E-Mail-Adressen verfügbar. Wenn Sie Ihre Einträge abgeschlossen haben, klicken Sie auf das Schlosssymbol, um das Feld zu sperren.
Beschreibung	Geben Sie eine vollständige Beschreibung des Security Incidents zusammen mit allen Informationen ein, die bei der Suche nach der Ursache oder der Lösung des Problems helfen können.
Sichere Notizen	Nur Anwenderrollen mit sn_si.admin und sn_si.Analyst können die sicheren Notizen anzeigen oder bearbeiten.
Arbeitsnotizen	Geben Sie Arbeitsnotizen ein, die für den Kunden nicht sichtbar sind. Arbeitsnotizen werden in angezeigt **Aktivität** Bereich.
Aktivität	Zeigt Informationen, die manuell in Arbeitsnotizen eingegeben wurden, und alle dynamisch aktualisierten Aufgabenaktivitäten (Aktionen, Kommentare, Arbeitsnotizen usw.) in zugehörigen Datensätzen für diesen Security Incident an. Arbeitsnotizen werden mit einem gelben Farbband angezeigt.  Automatisch generierte Notizen werden mit einem grauen Farbband angezeigt. 

4. Sie können die Arten von Informationen einschränken, die in angezeigt werden **Aktivität** Durch Klicken auf den Filter ( )-Symbol.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Die **Automatisierungsaktivität** Mit dem Kontrollkästchen können Sie alle Ergänzungen einschließen, die von diesem Security Incident durchgeführt werden, einschließlich Workflow-Aktivitäten, Updates der Risikopunktzahl usw.

5. Klicken Sie auf eine der folgenden Registerkarten, um den Security Incident weiter zu aktualisieren:
   - Zugehörige Datensätze
   - Überprüfung nach Incident
   - Abschlussinformationen
6. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Fügen Sie einem Security Incident zugehörige Probleme, Changes und Incidents hinzu

Sie können vorhandene Security Incidents zugehörige Datensätze wie Probleme, Changes und Incidents hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_si.Basic

Prozedur

1. Wenn er nicht bereits geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. Klicken Sie auf **Zugehörige Datensätze** Registerkarte.
3. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Problem	Wählen Sie einen Problemdatensatz (PRB) aus, der das zugrunde liegende Problem löst, das die Erstellung dieses Security Incidents verursacht hat. Die PRBS für diesen Incident

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	werden normalerweise erstellt, indem Sie mit der rechten Maustaste auf den Header des Security Incident-Formulars klicken und auswählen **Problem Erstellen** .
Übergeordnet	Wählen Sie einen Aufgabendatensatz aus, der sich auf das zugrunde liegende Problem bezieht, das die Erstellung dieses Security Incidents verursacht hat.
Übergeordneter Security Incident	Wählen Sie einen Security Incident-Datensatz aus, der sich auf das zugrunde liegende Problem bezieht, das die Erstellung dieses Security Incidents verursacht hat. Weitere Informationen finden Sie unter Beziehungen zwischen über- und untergeordneten Security Incidents.
Incident	Wählen Sie einen Incident-Datensatz (INC) aus, der das zugrunde liegende Problem löst, das die Erstellung dieses Security Incidents verursacht hat. Der Incident wird normalerweise erstellt, indem Sie mit der rechten Maustaste in den Header des Security Incident-Formulars klicken und auswählen **Incident Erstellen** .
Change-Anforderung	Wählen Sie einen Change Request-Datensatz (CHG) aus, der das zugrunde liegende Problem löst, das die Erstellung dieses Security Incidents verursacht hat. Die Change-Anforderung wird normalerweise erstellt, indem Sie mit der rechten Maustaste in den Header des Security Incident-Formulars klicken und auswählen **Erstellen Sie Einen Change** .

4. Klicken Sie auf eine der folgenden Registerkarten, um den Security Incident weiter zu aktualisieren:
   - Incident Details
   - Überprüfung nach Incident
   - Abschlussinformationen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Rufen Sie einen Prozess-Dump für einen angereicherten Prozess in Windows auf

Ein Sicherheitsanalyst kann einen Prozess-Dump für einen bestimmten Prozess ausführen, in eine Datei ablegen und an einer freigegebenen Website in einem internen Netzwerk veröffentlichen. Ein Analyst kann dann einen Prozess mit der Deny-Liste anzeigen, der in einem Security Incident rot hervorgehoben wird, und zusätzliche Analysen durchführen.

Vorbereitungen

Folgendes ist erforderlich:

- Ein Client, auf dem Windows Vista oder höher ausgeführt wird, oder ein Server, auf dem Windows Server 2008 oder höher ausgeführt wird.
- Das Befehlszeilendienstprogramm ProcDump wurde mit einer Systemumgebungsvariable installiert, die auf den Pfad der ausführbaren procdump-Datei verweist. Der Name der Variable muss PROCDUMP sein. Dieser Name wird in einem powershell-Skript verwendet.

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren Sie zum Security Incident mit dem angereicherten Prozess, für den Sie einen procdump aufrufen möchten, indem Sie auf klicken **Alle** > **Security Incident** > **Offene Incidents anzeigen**, Und öffnen Sie einen Security Incident.
2. Klicken Sie auf **Ergänzungsdaten** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Laufende Prozesse Abrufen** Ergänzungsdatensatz.
4. Aktivieren Sie die Kontrollkästchen für die laufenden Prozesse, für die Sie einen Procdump ausführen möchten, klicken Sie unten in der Liste auf die Dropdown-Liste Aktionen für ausgewählte Zeilen, und klicken Sie auf **Procdump Ausführen** .
   Ein **Prodump-Workflow für ausgewählten Prozess initiiert** Die Meldung wird oben in der Liste und angezeigt **Security Incident Response: Procdump ausführen** Workflow-Ausführungen.

Zeigen Sie Informationen in einem Security Incident an

Über die zugehörigen Links können Sie mehrere andere Aktionen für einen vorhandenen Security Incident ausführen.

Vorbereitungen

Erforderliche Rolle: sn_si.Basic

Prozedur

1. Wenn er nicht bereits geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. Innerhalb Von **Zugehörige Links** , Sie können die folgenden Aufgaben ausführen:

Option	Bezeichnung
Manuelles Runbook anzeigen	Zeigen Sie eine Liste der für diesen Security Incident verfügbaren Runbooks an.
Antwort-Workflow	Zeigen Sie alle diesem Incident zugeordneten Workflows an.
Mehrere erkennbare Elemente hinzufügen	Fügt eine Liste erkennbarer Elemente in Komma-, neuen Zeilen-, Tab- oder Pipe-getrennten Formaten hinzu.
Dem Sicherheitsfall hinzufügen	Fügt den Security Incident einem oder mehreren Sicherheitsfällen hinzu. Sie können auch einen neuen Sicherheitsfall erstellen und diesen Security Incident hinzufügen.
QRadar-IP-Zusammenfassungen abrufen	Wenn eine QRadar-Integration verfügbar ist und gültige CIs, Quell- und Ziel-IP-Adressen enthält, löst sie die QRadar-Workflows aus und zeigt die Ergebnisse in Arbeitsnotizen an.
Orchestration ausführen	Wählen Sie einen Security Operations-Workflow aus, und führen Sie ihn aus.
View SLA timeline	Sie können eine SLA-Zeitleiste aus einem Aufgaben-SLA-Datensatz oder aus einer SLA-Definition anzeigen.
Alle zugehörigen Listen anzeigen	Zeigt alle zugehörigen Standardlisten und alle manuell hinzugefügten Listen an. **Hinweis:** Manuell hinzugefügte Elemente sind nur in dieser Ansicht verfügbar.
Betroffene Elemente anzeigen	Zeigt die Listen der CIs, Anwender und Services an, die direkt von diesem Incident betroffen sind

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Zugehörige Elemente anzeigen	Zeigt die Listen der zugehörigen Incidents, CIs, Anwender und Gruppen an, die von diesem Incident betroffen sind.
IoC anzeigen	Zeigt die Listen der erkennbaren Elemente, Indikatoren, Malware, Modi und Methoden sowie Sicherheitsscananforderungen an, die diesem Incident zugeordnet sind.
Ergänzungsdaten anzeigen	Zeigt die Listen von Ergänzungsdaten, Prozessen, Services, Statistiken, Suchen an Firewall-Protokolle und gefährdete Anwenderinformationen, die diesem Incident zugeordnet sind.
Antwortaufgaben anzeigen	Zeigt die Listen der Aufgaben, SLAs, Audits der Risikopunktzahl, Ausfälle und Exchange-Suchen an, die diesem Incident zugeordnet sind.
Details im externen System anzeigen	Wenn dieser Security Incident direkt oder durch Ereignisse aus einer externen Anwendung generiert wurde und ein Link zu den Ursprungsdaten bereitgestellt wurde, wird der **Zeigen Sie Details im externen System an** Aktion öffnet die URL. Sie können die Protokolle anzeigen und durchsuchen, die diesen Incident generiert haben.
Suchen Sie nach Schwachstellen	Wenn Vulnerability Response Ist aktiviert, und Sie haben mindestens ein betroffenes CI für den Security Incident ausgewählt. Sie können eine Scan-Anforderung senden, um festzustellen, welche Schwachstellen im CI vorhanden sind.

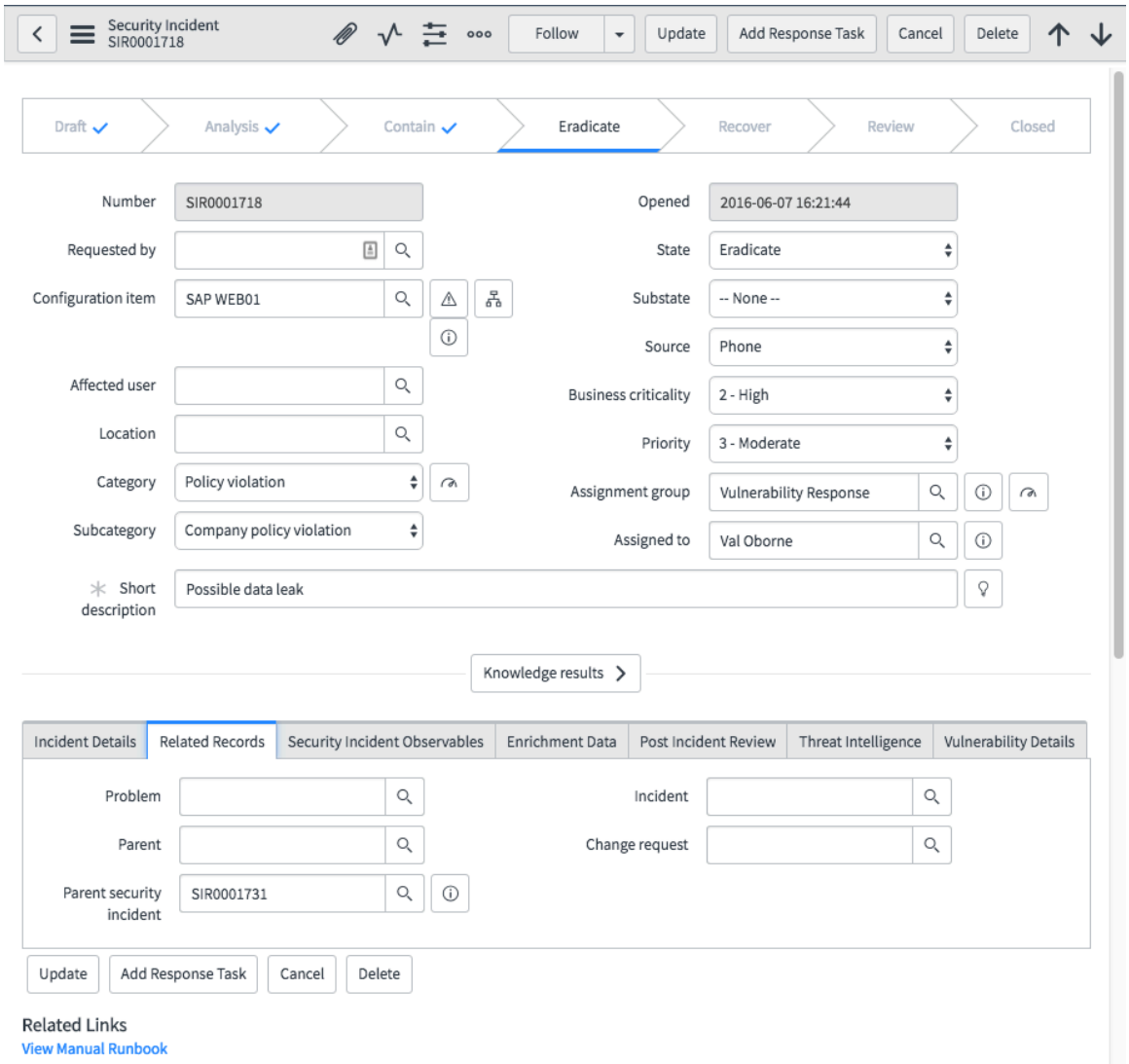
Beziehungen zwischen über- und untergeordneten Security Incidents

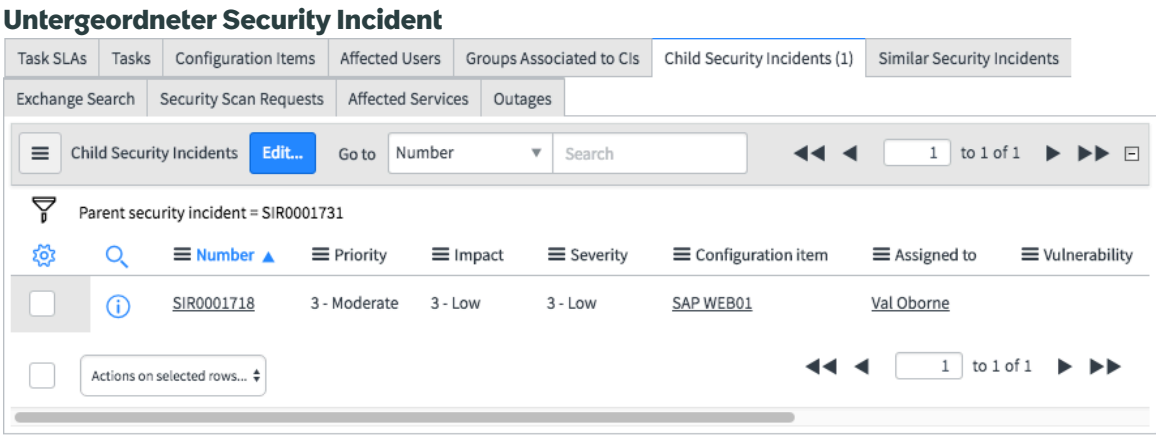
Sie können die Auswirkungen eines bestimmten Problems mithilfe von über- und untergeordneten Security Incident-Beziehungen in zuordnen und nachverfolgen Security Incident Response.

Mit **Zugehörige Datensätze** Registerkarte können Sie hinzufügen **Übergeordneter Security Incident** Problem an beliebig Security Incident Response Formular. Diese Funktion macht den Incident automatisch zu einem untergeordneten Element, das in angezeigt wird **Zugehörige Listen: Untergeordnete Security Incidents** Registerkarte des übergeordneten Problems.

Hinweis:
Sie können einen vorhandenen übergeordneten Security Incident nicht zu einem eigenen untergeordneten Element machen, indem Sie für beide Incidents dieselbe Nummer verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



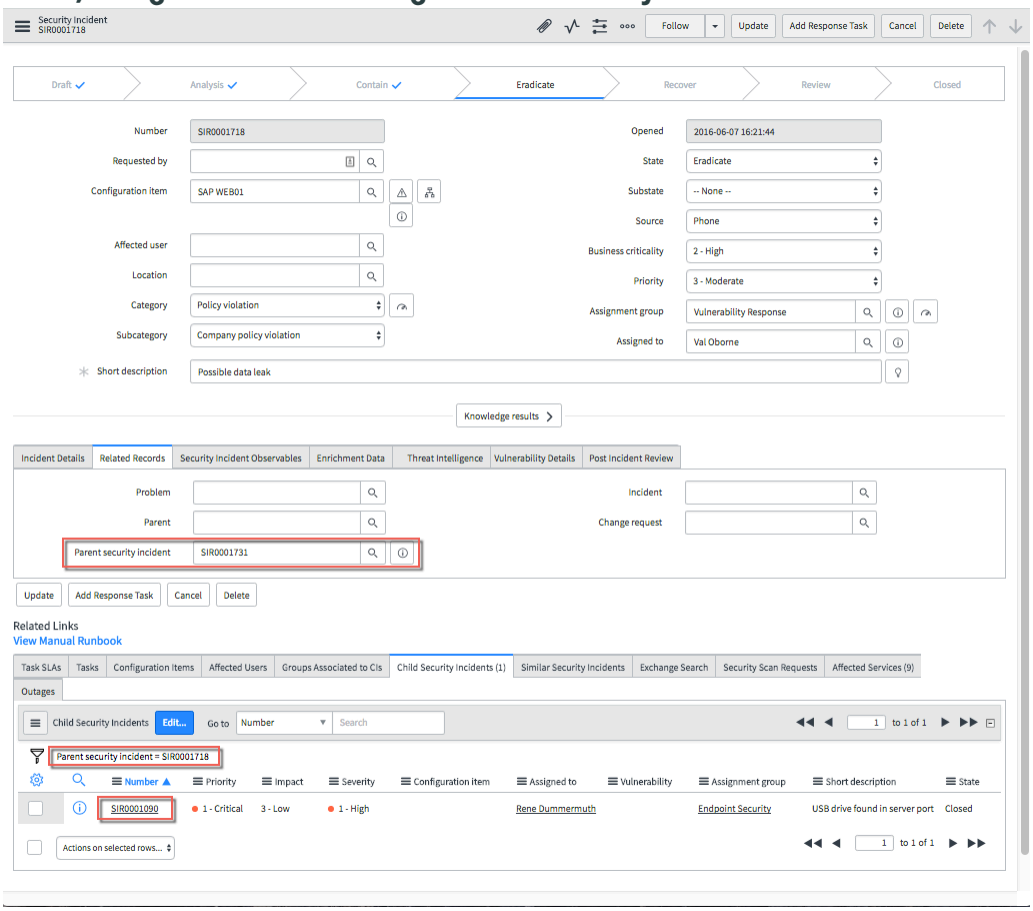


Sie können eine oder mehrere hinzufügen **Untergeordnete Security Incidents** Auch in einen beliebigen Security Incident-Datensatz mit **Bearbeiten** Schaltfläche in **Untergeordnete Security Incidents** Registerkarte. Im folgenden Beispiel sind alle drei Datensätze verbunden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Groß-, übergeordnete und untergeordnete Security Incidents



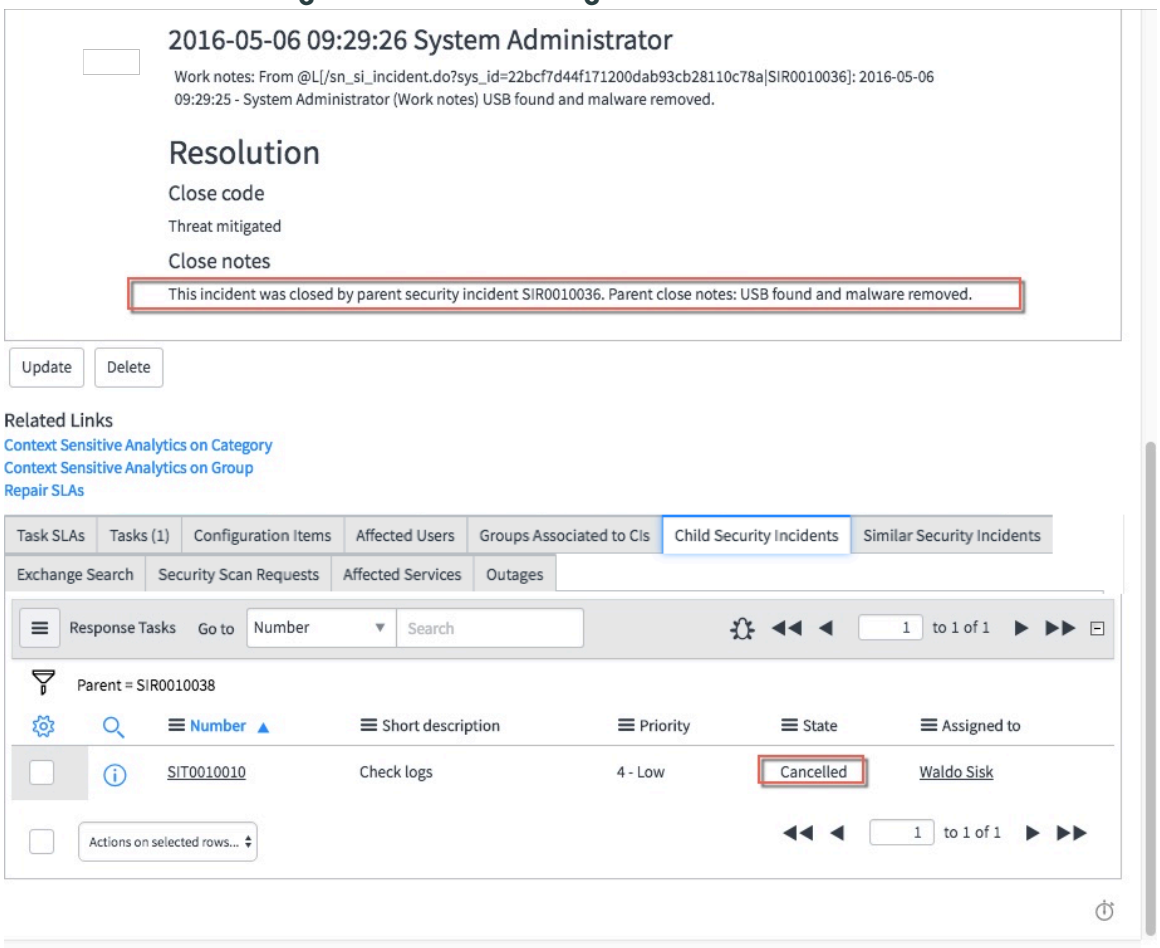
Hinweis:

- Alle im übergeordneten Element aufgezeichneten Arbeitsnotizen werden an alle aktiven untergeordneten Elemente in weitergegeben **Aktivitäten** Unter **Incident-Details** Registerkarte.
- Die **Übergeordnet** Das Feld wird verwendet, um den Security Incident einem übergeordneten Datensatz zuzuordnen, z. B. einem schwerwiegenden Incident, einem Problem oder einer Change-Anforderung, der sich außerhalb des Security Incident-Moduls befindet. Zum Gruppieren mehrerer Security Incidents zu einem Haupt-Security Incident, der **Übergeordneter Security Incident** Feld wird verwendet.

Wenn ein übergeordnetes Element geschlossen oder abgebrochen wird, werden alle aktiven untergeordneten Elemente ebenfalls geschlossen oder abgebrochen. Alle aktiven **Antwortaufgaben** Für die untergeordneten Incidents werden abgebrochen. Wenn keine anderen offen sind **Aufgaben** , Der untergeordnete Incident wird geschlossen. Wenn geschlossen, wird **Incident-Interview Veröffentlichen** Zeichnet den Abschluss und die im gefundenen Informationen auf **Abschlussinformationen** Registerkarte wird vom übergeordneten Element an die untergeordneten Elemente weitergegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schließen Sie die untergeordnete Antwortaufgabe



Zeigen Sie betroffene Elemente für einen Security Incident an

Sie können betroffene Elemente anzeigen, z. B. CIs, betroffene Anwender und betroffene Services, die einem Security Incident zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: sn_si.Basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie betroffene Elemente anzeigen möchten.
2. Klicken Sie auf **Betroffene Elemente Anzeigen** Zugehöriger Link.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

Registerkarte	Beschreibung
Konfigurationselemente	Betroffene Konfigurationselemente (CI). Nachdem betroffene CIs identifiziert wurden, können Sie betroffene Ressourcen manuell aus dieser zugehörigen Liste hinzufügen.
Betroffene Anwender	Nachdem betroffene Anwender identifiziert wurden, können Sie betroffene Anwender manuell aus dieser zugehörigen Liste hinzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte	Beschreibung
Betroffene Services	Zeigen Sie Business-Services an, die dem Security Incident zugeordnet sind, oder fügen Sie sie hinzu. **Hinweis:** Wenn ein betroffenes CI hinzugefügt wird, nachdem der Security Incident geöffnet wurde, empfiehlt es sich, mit der rechten Maustaste in den Formularheader zu klicken und auszuwählen **Aktualisieren Sie Die Betroffenen Services** .

Hinweis:
Wenn Integration Von Security Operations: Laufende Prozesse Abrufen Die Integrationsfähigkeit ist aktiv, und Sie fügen einem Security Incident, dem, ein CI hinzu Laufende Prozesse Abrufen Workflow wird ausgeführt und ruft eine Liste der laufenden Prozesse für das CI ab.

Wenn Integration Von Security Operations: Host Isolieren Die Integrationsfähigkeit ist aktiv. Sie können ein oder mehrere CIs auswählen und ihre Systemverbindungen auf andere Geräte beschränken. Aktivieren Sie dazu die Kontrollkästchen für die CIs, und klicken Sie auf **Host Isolieren** Von **Aktionen für ausgewählte Zeilen** Auswahlliste.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Zugehörige Elemente anzeigen
   - IoC anzeigen
   - Ergänzungsdaten anzeigen
   - Antwortaufgaben anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Zeigen Sie zugehörige Elemente für einen Security Incident an

Sie können zugehörige Elemente anzeigen, z. B. ähnliche und untergeordnete Security Incidents, zugehörige Anwender, Schwachstellengruppen und angreifbare Elemente, die einem Security Incident zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie zugehörige Elemente anzeigen möchten.
2. Klicken Sie auf **Zugehörige Elemente Anzeigen** Zugehöriger Link.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

Registerkarte	Beschreibung
Untergeordnete Security Incidents	Wählen Sie einen Aufgabendatensatz im Zusammenhang mit dem Problem aus, das die Erstellung dieses Security Incident verursacht hat.
Ähnliche Security Incidents	Zeigen Sie alle anderen Security Incidents an, die einem der gleichen Datensätze erkennbarer Elemente zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte	Beschreibung
Zugehörige Configuration Items	Zeigt eine Liste von Security Incidents an, die Konfigurationselemente mit demselben erkennbaren Element wie dieser Security Incident enthalten. Diese Liste kann mit gefiltert werden **CI-Ausschlüsse** Filtergruppe. Wenn einem Security Incident ein erkennbares Element hinzugefügt wird, wird diese Liste automatisch aktualisiert. Standardmäßig werden erkennbare Elemente mit dem Kontexttyp „Ziel“ ausgeschlossen.
Zugehörige Anwender	Zeigt eine Liste von Security Incidents an, die Anwender mit denselben erkennbaren Elementen wie dieser Security Incident enthalten. Diese Liste kann mit gefiltert werden **Anwenderausschluss** Filtergruppe. Wenn einem Security Incident ein erkennbares Element hinzugefügt wird, wird diese Liste automatisch aktualisiert. Standardmäßig werden erkennbare Elemente mit dem Kontexttyp „Ziel“ ausgeschlossen.
Zugehörige Filtergruppe	Nachdem Konfigurationselemente identifiziert wurden, werden alle übereinstimmenden CI- oder Filtergruppen automatisch hinzugefügt.
Schwachstellengruppen	Wenn Vulnerability Response Ist aktiviert, können Sie Schwachstellengruppen anzeigen, die diesem Security Incident zugeordnet sind.
Angreifbare Elemente	Wenn Vulnerability Response Ist aktiviert, können Sie Schwachstellen-Elemente anzeigen, die diesem Security Incident zugeordnet sind.
Risiken	Wenn eines der Core-Risikomanagement-Plugins (Richtlinien- und Compliance-Management, Audit, Management oder Risikomanagement) aktiviert ist, können Sie Risiken im Zusammenhang mit dem Security Incident anzeigen oder hinzufügen. Sie können diese zugehörige Liste über das Kontextmenü des Formularheaders unter hinzufügen **Konfigurieren** > **Zugehörige Listen**an.
Konfigurationselement-Ereignisse	Wenn Ereignismanagement Ist aktiviert, können Sie Ereignisse anzeigen.
Konfigurationselementwarnungen	Wenn Ereignismanagement Ist aktiviert, können Sie Warnungen anzeigen.
Kundenservicefälle	Wenn Kundenservice Ist aktiviert, können Sie anzeigen Kundenservice Fallinformationen.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Betroffene Elemente anzeigen
   - IoC anzeigen
   - Ergänzungsdaten anzeigen
   - Antwortaufgaben anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Ergänzungsdaten für einen Security Incident an

Sie können Ergänzungsdaten anzeigen, z. B. laufende Prozesse, laufende Services und Netzwerkstatistiken, die einem Security Incident zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie Ergänzungsdaten anzeigen möchten.
2. Klicken Sie auf **Anreicherungsdaten Anzeigen** Zugehöriger Link.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

Hinweis:
Rohdatendetails werden in einem Anhang zum Ergänzungsdatensatz gespeichert. Wenn die Feldgrenze überschritten wird, werden die angezeigten Details gekürzt.

Registerkarte	Beschreibung
Laufende Prozesse	Speichert die von erstellten Datensätze Security Incident Response **Laufende Prozesse Abrufen** Workflow.
Laufende Services	Speichert die von erstellten Datensätze Security Incident Response **Laufende Services Abrufen** Workflow.
Netzwerkstatistiken	Speichert die von erstellten Datensätze Security Incident Response **Rufen Sie Netzwerkstatistiken Ab** Workflow.
Domänensuchen	Wenn WhoisXML-API-Integration Plugin ist aktiviert und speichert die von einer Whois-Suche erstellten Datensätze.
Firewall-Protokolle	Speichert Ergänzungsdaten aus Firewall-Protokollen, z. B. den Firewall-Protokollen des Palo Alto-Netzwerks.
Info zu gefährdetem Anwender	Speichert Accounts, die identifiziert wurden, dass sie durch eine Gefährdung gefährdet wurden? Suchen.

Hinweis: Der **Sicherheitsanreicherungsdaten** Auf der Registerkarte werden Rohanreicherungsdaten von angezeigt Security Incident Response Workflows, z. B. Abrufen von Netzwerkstatistiken oder laufende Prozesse. Diese Registerkarte kann angezeigt werden, indem Sie auf klicken **Alle Zugehörigen Listen Anzeigen** Zugehöriger Link.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Betroffene Elemente anzeigen
   - Zugehörige Elemente anzeigen
   - IoC anzeigen
   - Antwortaufgaben anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Informationen zur Antwortaufgabe für einen Security Incident an

Sie können Informationen zu Antwortaufgaben anzeigen, z. B. Aufgaben-SLAs, Risikopunktzahlaudits und Ausfälle, die einem Security Incident zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie Antwortaufgaben anzeigen möchten.
2. Klicken Sie auf **Antwortaufgaben Anzeigen** Zugehöriger Link.
3. Klicken Sie auf eine der zugehörigen Listen, um Informationen für den Security Incident anzuzeigen oder hinzuzufügen.

Registerkarte	Beschreibung
Aufgaben	Zeigt Aufgaben an, die bereits für den Security Incident definiert sind. Sie können eine Antwortaufgabe manuell erstellen.
Antwortaufgaben	Zeigt Aktionen an, die als Reaktion auf den Security Incident ausgeführt werden sollen.
Aufgaben-SLAs	Zeigen Sie aktive Aufgaben-SLAs an, die für den Security Incident definiert wurden, oder fügen Sie sie hinzu.
Risikopunktzahl-Audits	Ein Audit-Datensatz für jede Instanz einer geänderten Risikopunktzahl.
Ausfälle	Zeigen Sie neue Ausfalldatensätze an, die dem Security Incident zugeordnet sind, oder fügen Sie sie manuell hinzu.
E-Mail-Suche	Eine Liste von Datensätzen, die Suchkriterien zum Ausführen von Abfragen auf einem E-Mail-Server wie Microsoft enthält ®Exchange Server (basierend auf der installierten Implementierung) und speichert die empfangenen Ergebnisse. **Hinweis:** Wenn Integration von Security Operations: Funktion „E-Mail suchen und löschen“ Ist nicht aktiv, der **E-Mail-Suche** Zugehöriger Link wird nicht angezeigt.

4. Klicken Sie auf einen der folgenden zugehörigen Links, um den Security Incident weiter zu aktualisieren:
   - Betroffene Elemente anzeigen
   - Zugehörige Elemente anzeigen
   - IoC anzeigen
   - Ergänzungsdaten anzeigen
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

Zeigen Sie zugehörige Ereignisse und Warnungen in Security Incidents an

Während an einem Security Incident gearbeitet wird, können Sie die Details der Ereignisse anzeigen. Bei Warnungen können Sie diese Warnungen anzeigen und bestätigen und nach Bedarf Incidents oder Security Incidents daraus erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Das Support-Plugin „Security Incident Response Event Management“ muss aktiviert sein.

Erforderliche Rolle: si.sn_Agent

Prozedur

1. Navigieren Sie zu einer beliebigen Security Incident-Liste (z. B. **Alle** > **Security Incident** > **Incidents** > **Nicht zugewiesene Incidents**) an.
2. Wenn die von dem angezeigten Security Incident betroffenen Ressourcen innerhalb der letzten 24 Stunden Warnungen oder Ereignisse erhalten haben, werden eine oder beide der folgenden zugehörigen Listen angezeigt.
   - Security Incident-CI-Warnungen
   - Security Incident-CI-Ereignisse
3. Klicken Sie auf die zugehörige Liste, die Sie anzeigen möchten.

Zugehörige Liste	Beschreibung
Security Incident-CI-Warnungen	Sie können Details für Warnungen anzeigen, die innerhalb der letzten 24 Stunden empfangen wurden. Sie haben die Möglichkeit, auf zu klicken **Bestätigen** Um anzugeben, dass Sie die Warnung kennen und verarbeitet wird. Verwenden **Schließen** Um anzugeben, dass die Warnung nicht wichtig ist.
Security Incident-CI-Ereignisse	Sie können Details für Ereignisse anzeigen, die innerhalb der letzten 24 Stunden empfangen wurden.

Zeigen Sie die Zuordnung von Security Incident zu Kundenservicefall an

Security Incident Response Wird mit einer Standardfeldzuordnung geliefert, die einen Security Incident einem zugeordnet Kundenservice Fall. Sie können die Standardzuordnung für Security Incident zu CS-Fall anzeigen.

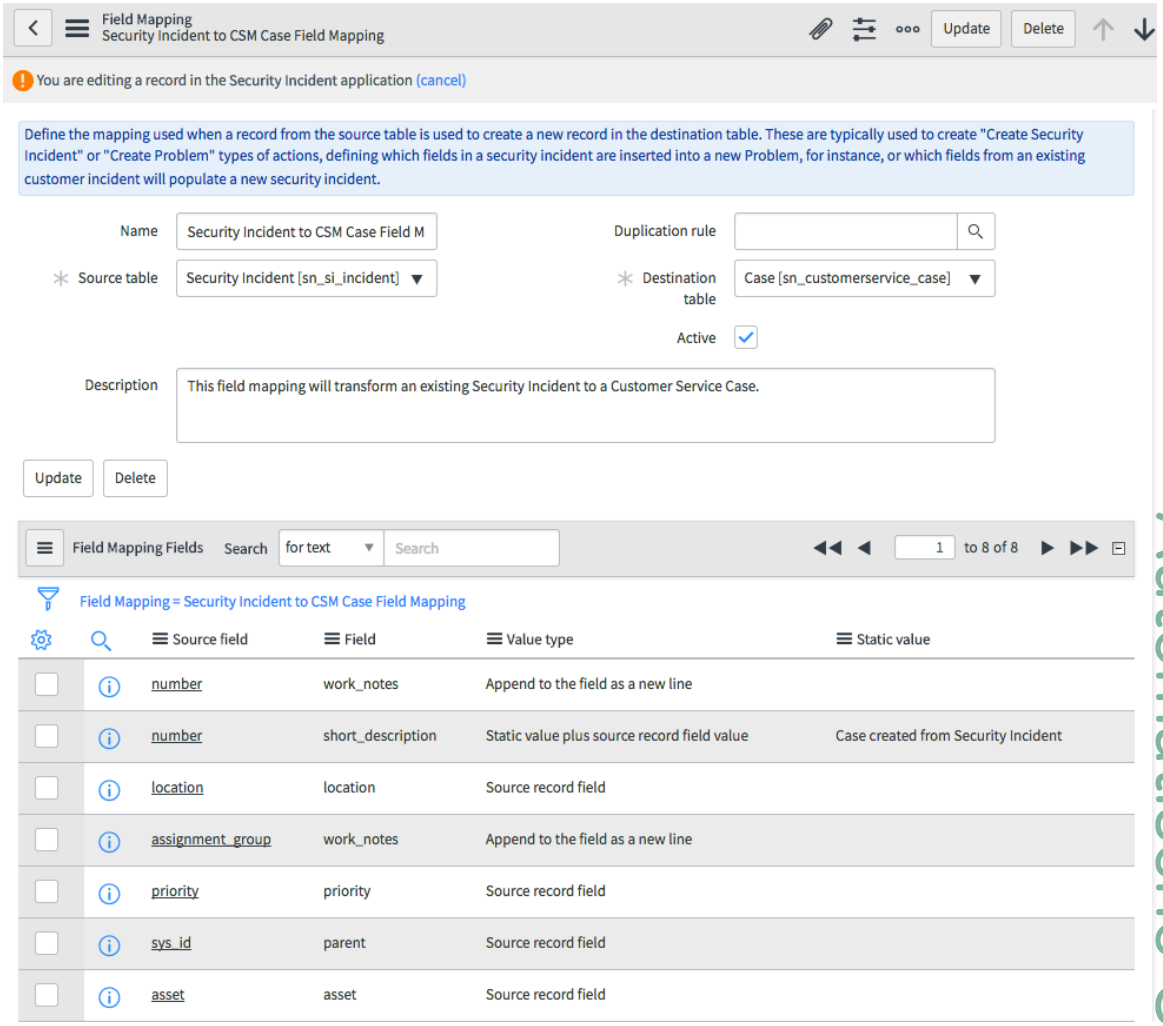
Vorbereitungen

Erforderliche Rolle: Sec_cmn.read

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Feldzuordnung**an.
2. Klicken Sie Auf **Zuordnung von Security Incident zu CSM-Fall** Zum Anzeigen der Standardzuordnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Sie können die Zuordnung nach Bedarf bearbeiten.
4. Wenn Sie Ihre Änderungen abgeschlossen haben, klicken Sie auf **Aktualisieren** .

Zeigen Sie ein Security Incident Response-Runbook an

Runbooks bieten Ihnen Zugriff auf Verfahren im Zusammenhang mit Aufgaben, an denen Sie arbeiten.

Vorbereitungen

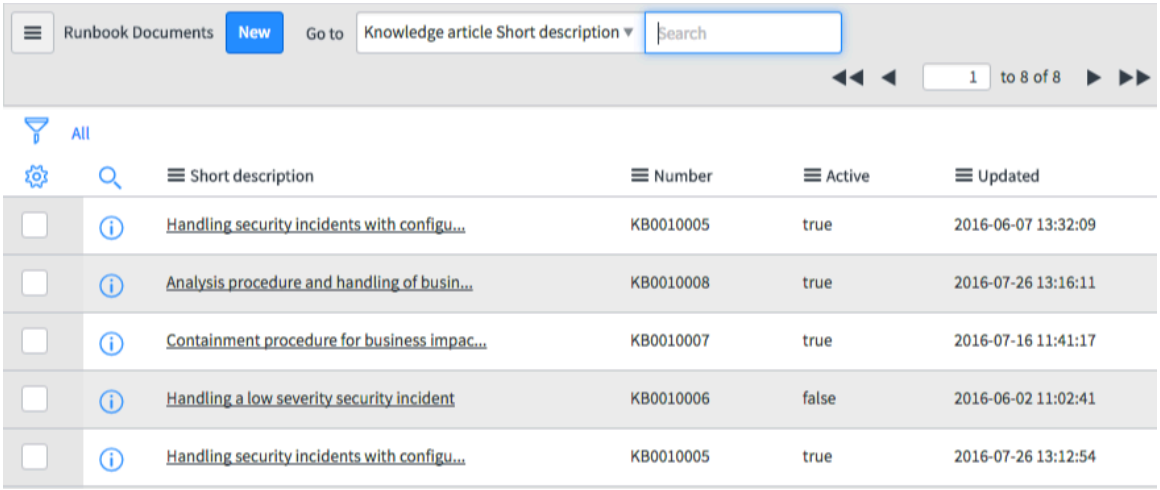
Erforderliche Rolle: sn.si.Knowledge_admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Manuelles Runbook** > **Runbook-Dokumente anzeigen**an.
2. Wählen Sie ein Runbook aus der Liste aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf, um ein Runbook zu erstellen **Neu** .
   Weitere Informationen finden Sie unter Erstellen Sie ein Runbook .

Identifizieren Sie alle Konfigurationselemente, die von einem Security Incident betroffen sind

Wenn Sie wissen, welche Ressource (Server, Desktop oder anderes Konfigurationselement) hinter einem Security Incident steckt und zugehörige Ressourcen und Business-Services identifizieren möchten, die betroffen sein können, können Sie die Business Service Management (BSM)-Zuordnung verwenden.

Vorbereitungen
Erforderliche Rolle: admin oder sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Die BSM-Zuordnung zeigt die vor- und nachgelagerten Abhängigkeiten für ein ausgewähltes Stamm-CI an.

Es gibt zwei Methoden, mit denen Sie die BSM-Zuordnung für ein CI anzeigen können:

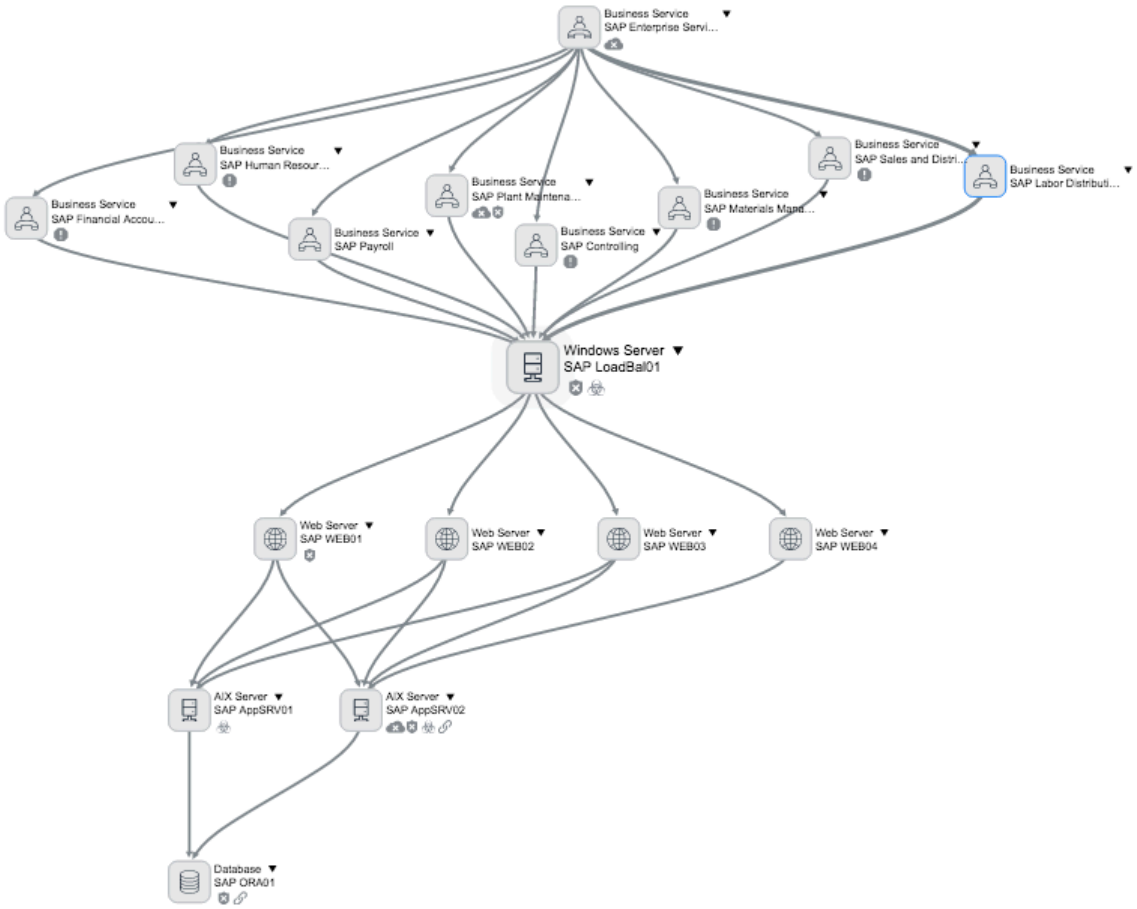
- Wenn Sie CIs aus dem Kontext einer Aufgabe anzeigen möchten, zeigen Sie sie im Security Incident-Formular an.
- Wenn Sie CIs nicht aus Aufgabensicht anzeigen möchten, zeigen Sie sie in der Navigationsleiste an.

Prozedur

1. Füllen Sie im Formular „Security Incident“ aus **Konfigurationselement** Und klicken Sie auf das BSM Map-Symbol ( ).
   Der BSM-Kartenbildschirm zeigt die Karte für den letzten Incident an, auf den Sie im Incident-Management zugegriffen haben, oder den letzten Security Incident, auf den Sie im Security Incident-Management zugegriffen haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Klicken Sie auf die Symbole neben einem Konfigurationselement, um verschiedene Arten von Details zur Ressource (Server, Desktop oder anderes CI) anzuzeigen.
   Klicken Sie beispielsweise auf (⚠), um Warnungen anzuzeigen, die dem CI zugeordnet sind.

   Hinweis:
   Um eine Liste aller verfügbaren Symbole anzuzeigen, klicken Sie auf **Filter** Über der BSM-Zuordnung und erweitern **Filteraufgabentypen** .

3. Um die Karte in verschiedenen Konfigurationen anzuordnen, wählen Sie eines der oben aufgeführten Formate aus (**Vertikal** , **Horizontal** , **Radial**), oder klicken Sie auf **Filter** Zum Filtern der Karte für eine einfachere Anzeige.

4. Wenn Sie die BSM-Karte über das Security Incident-Formular geöffnet haben, können Sie dem Security Incident ein abhängiges CI hinzufügen, indem Sie mit der rechten Maustaste auf das CI klicken und auswählen **Fügen Sie betroffene CIs hinzu** .
   Sie können auch mehrere CIs gleichzeitig hinzufügen. Ziehen Sie ein Feld um die CIs, die Sie hinzufügen möchten, klicken Sie mit der rechten Maustaste auf das Feld, und wählen Sie aus **Fügen Sie betroffene CIs hinzu** .
   Die CIs werden der zugehörigen Liste Betroffene CIs des Security Incidents hinzugefügt.

Berechnen Sie den Schweregrad eines Security Incidents

Sie können den Schweregrad eines Security Incidents mithilfe vordefinierter Rechner berechnen.

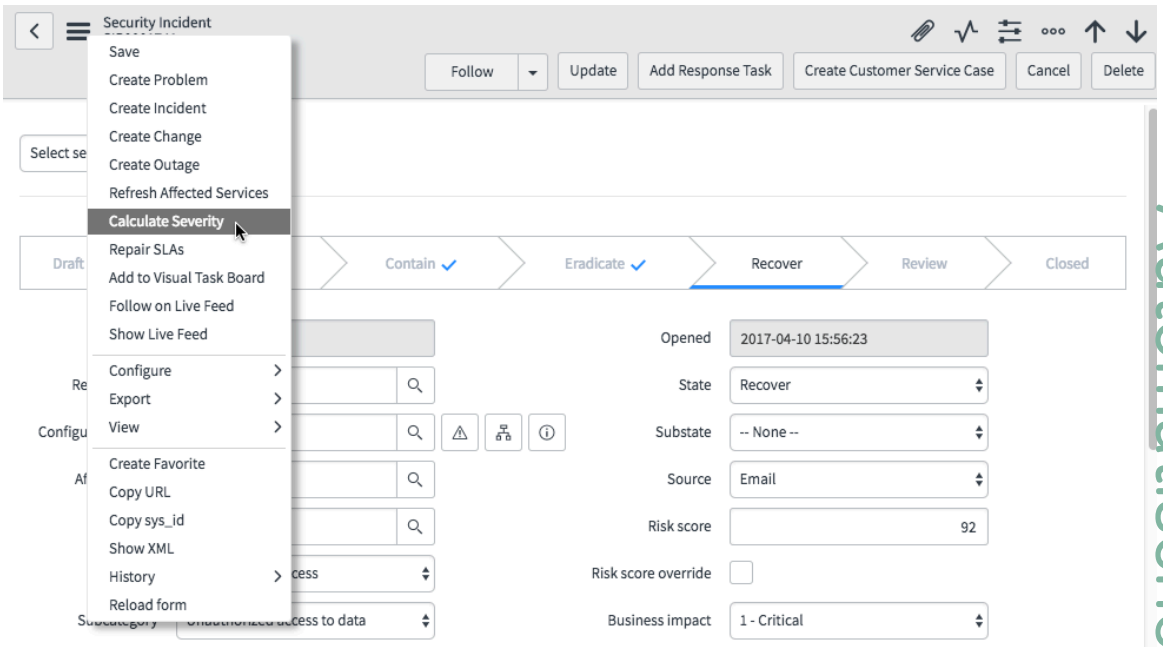
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Basic

Prozedur

1. Wenn er noch nicht geöffnet ist, öffnen Sie den Security Incident, für den Sie den Schweregrad berechnen möchten.
2. Klicken Sie auf das Kontextmenü des Formularheaders, und wählen Sie aus **Schweregrad Berechnen** :



Der Schweregrad wird basierend auf den vordefinierten Regeln für Basisrechner berechnet. Weitere Informationen finden Sie unter Verstehen von Security Incident-Rechnern.

Suchen und löschen Sie Phishing-E-Mails

Das Löschen von Phishing-E-Mails kann dazu beitragen, das Risiko eines bestimmten Angriffs in einer Organisation zu reduzieren. Sie können Phishing-E-Mails auf Ihrem E-Mail-Server verwalten, indem Sie sie durchsuchen, Genehmigungen erteilen und löschen.

Vorbereitungen
Erforderliche Rollen: sn_sec_cmn.cap_email_read

Sie können bestimmen, wie viele Anwender von einem Phishing-Angriff betroffen waren, indem Sie einen E-Mail-Datensatz abfragen, der einem Security Incident zugeordnet ist.

Unterstützte Software:

- Microsoft ®Exchange Server 2010

Einschränkung: Beim Durchsuchen des Textkörpers von E-Mails können Sie maximal 1.500 Postfächer durchsuchen.

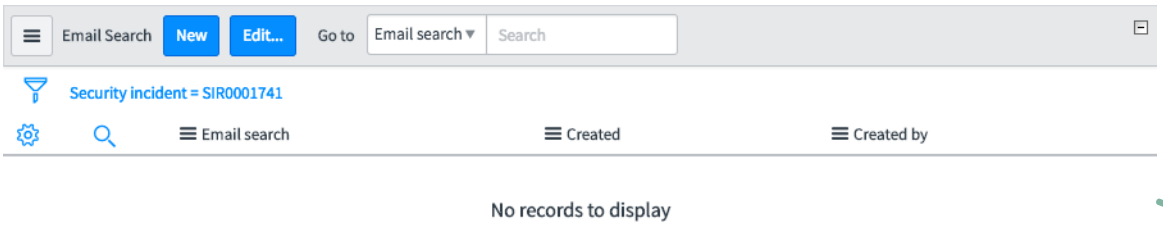
Warum und wann dieser Vorgang ausgeführt wird
Diese Funktion wird von verwendet Integration von Security Operations – Flow für E-Mail-Suche und -Löschung Um eine Abfrage für Ihren E-Mail-Server auszuführen. Abhängig von den von Ihnen ausgewählten Suchkriterien identifiziert die Suche alle E-Mails innerhalb eines Phishing-Angriffs und gibt die Gesamtzahl der betroffenen E-Mails oder Details aus den betroffenen E-Mails zurück.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

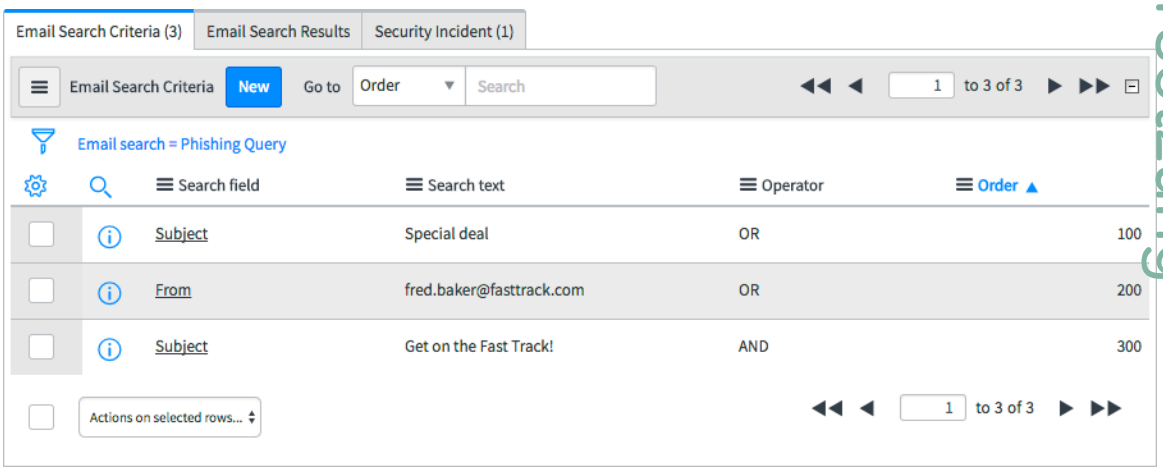
1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**an.
2. Wählen Sie einen Security Incident aus.
3. Wenn **E-Mail-Suche** Die zugehörige Liste ist nicht sichtbar. Klicken Sie auf **Alle Zugehörigen Links Anzeigen** Zugehöriger Link.
4. Klicken Sie auf **E-Mail-Suche** Zugehörige Liste.



5. Klicken Sie auf **Neu**.
6. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Name	Name der Suchabfrage
Abfrage von Kriterium	Eine Vorschau der Abfrage, die auf dem E-Mail-Server ausgeführt wird. Wird aus allen zugehörigen aktiven Suchkriteriendatensätzen generiert.
Beschreibung	Beschreiben Sie, wonach die Suchabfrage sucht.

7. Klicken Sie mit der rechten Maustaste in die Formularkopfzeile, und wählen Sie **Speichern** aus.



8. Klicken Sie auf **E-Mail-Suchkriterien** Registerkarte und klicken Sie auf **Neu** .
9. Füllen Sie die Felder entsprechend aus, oder bearbeiten Sie sie.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
E-Mail-Suche	Zeigt den Namen der E-Mail-Suche an. Sie können sie bei Bedarf ändern.
Suchfeld	Feld, das auf dem E-Mail-Server gesucht werden soll. Das Suchfeld hat die folgenden Auswahlmöglichkeiten: **Betreff** Dieses Kriterium sucht nach E-Mails, die den in angegebenen Betreffzeilentext enthalten **Suchtext** Feld. Für E-Mails, die diese Suchkriterien erfüllen, werden die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail zurückgegeben, einschließlich Empfangsdatum der E-Mail, Lesestatus der E-Mail, Empfänger und Nachrichten-ID. **Von** Dieses Kriterium sucht nach E-Mails, die die vollständige E-Mail-Adresse des Absenders (z. B. jane.doe@abc.com) enthalten, die in angegeben ist **Suchtext** Feld. Für E-Mails, die diese Suchkriterien erfüllen, werden die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail zurückgegeben, einschließlich Empfangsdatum der E-Mail, Lesestatus der E-Mail, Empfänger und Nachrichten-ID. **Hinweis:** Sie können nicht verwenden **Von** Und **Empfänger** Felder in derselben Abfrage. **Empfänger** Dieses Kriterium sucht nach E-Mails, die die vollständige E-Mail-Adresse des Empfängers (z. B. john.doe@abc.com) enthalten, die in angegeben ist **Suchtext** Feld. Außerdem wird in den Feldern „an“, „CC“ und „Bcc“ nach E-Mails gesucht. Für E-Mails, die diese Suchkriterien erfüllen, werden die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail

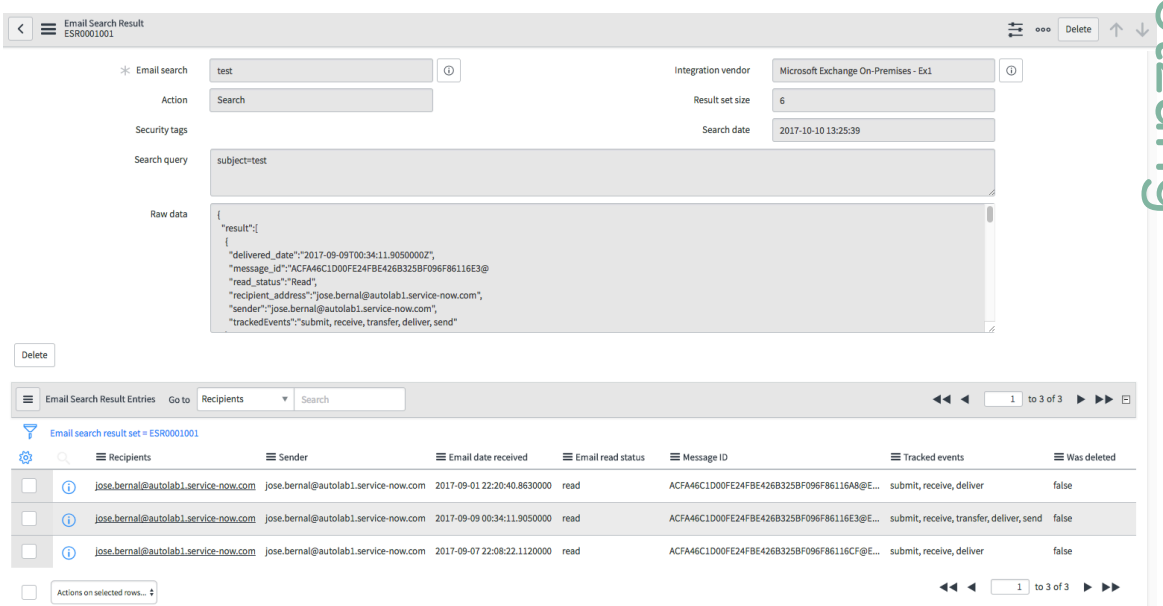
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	zurückgegeben, einschließlich Empfangsdatum der E-Mail, Lesestatus der E-Mail, Empfänger und Nachrichten-ID. **Hinweis:** Sie können nicht verwenden **Von** Und **Empfänger** Felder in derselben Abfrage. **Textkörper** Dieses Kriterium sucht nach E-Mails, die den in angegebenen Textkörper enthalten **Suchtext** Feld. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben. **Hinweis:** Beim Durchsuchen des Textkörpers von E-Mails können Sie maximal 1.500 Postfächer durchsuchen. **Cc:** Dieses Kriterium sucht nach E-Mails, die die vollständige CC-E-Mail-Adresse (z. B. jane.doe@abc.com) enthalten, die in angegeben ist **Suchtext** Feld. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben. **Bcc:** Dieses Kriterium sucht nach E-Mails, die die vollständige Bcc-E-Mail-Adresse (z. B. jane.doe@abc.com) enthalten, die in angegeben ist **Suchtext** Feld. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben. **Anhang** Dieses Kriterium sucht nach E-Mails, die entweder den Namen der Anhangsdatei oder den in angegebenen Anhangsinhalt enthalten **Suchtext** Feld. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Beim Durchsuchen der Anhangsinhalte werden nur nur nur-Text-Anhänge unterstützt. **Aufbewahrungsrichtlinie** Dieses Kriterium sucht nach E-Mails, die Aufbewahrungsrichtliniennummern enthalten, die in angegeben sind **Suchtext** Feld. Für E-Mails, die diese Suchkriterien erfüllen, wird die Gesamtzahl der Phishing-E-Mails zurückgegeben.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diese E-Mail-Suchabfrage zu aktivieren.
Operator	Mögliche Werte sind UND UND ODER. Sie können definieren, wie Suchkriterien kombiniert werden, um sie auf dem E-Mail-Server auszuführen.
Reihenfolge	Die Reihenfolge, in der die Suchabfrage aus den Suchkriterien erstellt wird.
Suchtext	Der Text, nach dem gesucht werden soll. Einfache Anführungszeichen, doppelte Anführungszeichen und Doppelpunkte werden nicht unterstützt.

10. Klicken Sie auf **Absenden**.
11. Wiederholen Sie den Vorgang nach Bedarf, um zusätzliche Suchkriterien zu definieren.
12. Sie können die Ergebnisse der Suche anzeigen, indem Sie auf klicken **E-Mail-Suchergebnisse** Registerkarte.

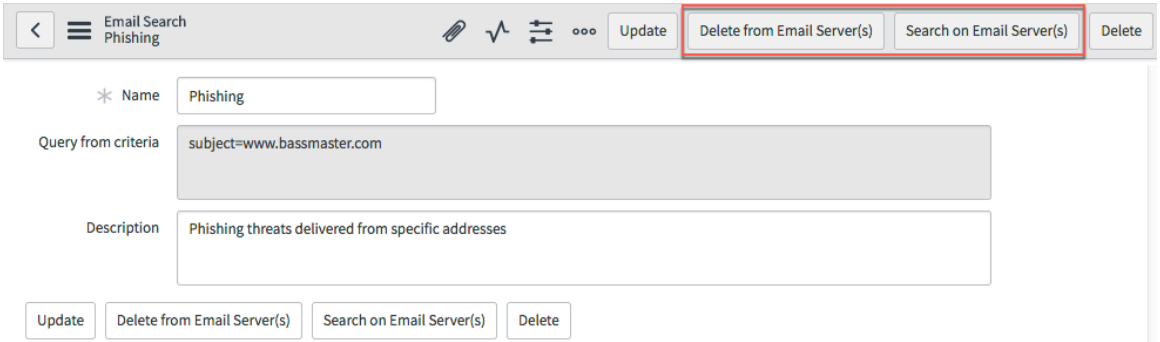


Jede Zeile des Formulars „E-Mail-Suchergebniseinträge“ stellt eine separate E-Mail dar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Nachdem Sie einen Suchkriteriendatensatz erstellt haben, werden im Formular „E-Mail-Suche“ zwei Schaltflächen angezeigt: **Aus E-Mail-Server(n) löschen** Und **E-Mail-Server suchen** .



14. Um auf dem ausgewählten Server nach E-Mails zu suchen, die die von Ihnen definierten Suchkriterien erfüllen, klicken Sie auf **E-Mail-Server suchen** .

Erstellen Sie einen Security Incident-wissensartikel

Während Sie mit Security Incidents und Antwortaufgaben arbeiten, werden automatisch Wissensartikel angezeigt, um relevante Informationen zu der von Ihnen ausgeführten Aufgabe zu erhalten. Ihre Organisation kann Artikel in der Security Incident Knowledge Base erstellen und verwalten.

Vorbereitungen

Erforderliche Rolle: sn_si.Knowledge_admin

Warum und wann dieser Vorgang ausgeführt wird

Wissensartikel geben Sicherheitsinformationen frei, dokumentieren die Arten von Cyberbedrohungen, denen Ihre Organisation ausgesetzt ist, und bieten Antworten und Antworten auf diese Bedrohungen.

Bei Bedarf können Sie Wissensartikel in Runbooks organisieren, die Zuordnungen zwischen den Artikeln und bestimmten Aufgaben erstellen. Sie können beispielsweise ein Runbook mit Bedingungen konfigurieren, die dazu führen, dass ein Knowledge Base-artikel über Phishing angezeigt wird, wenn Sie einen Security Incident für einen Phishing-Angriff erstellen. Weitere Informationen finden Sie unter Erstellen Sie ein Security Incident Response-Runbook.

Wissensartikel in Runbooks können auch bestimmten Aufgaben in einem Playbook zugeordnet werden. Weitere Informationen finden Sie unter Ordnen Sie einen wissensartikel einer Playbook-Aufgabe zu.

Die Vorteile von Wissensartikeln umfassen die folgenden.

- Mitarbeiter haben eine Informationsquelle, die sich leicht durchsuchen lässt.
- Informationen können auf dem neuesten Stand gehalten werden, da Wissensartikel einen definierten Lebenszyklus haben: Erstellen, überprüfen und aktualisieren, veröffentlichen und stilllegen.
- Wenn Sie eine Sicherheitsanforderung, einen Incident oder eine Antwortaufgabe manuell erstellen, wird während Sie die Kurzbeschreibung eingeben, eine Liste der relevanten Artikel angezeigt.

Hinweis:
Es ist wichtig, jeder Security Incident Knowledge Base einen Wissensmanager zuzuweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Katalog & Wissen** > **Wissen**an.
2. Klicken Sie auf das Symbol Artikel erstellen ( ).
3. Füllen Sie die entsprechenden Felder im Formular aus.

Wissensformular

Feld	Beschreibung
Anzahl	Die automatisch generierte KB-Nummer.
Knowledge Base	Die für diesen Artikel ausgewählte Knowledge Base.
Kategorie	Die Kategorie für diesen Artikel.
Veröffentlicht	Wann dieser wissensartikel veröffentlicht wurde. Dieser Wert wird festgelegt, wenn der artikel erstellt wird, und aktualisiert, wenn der artikel veröffentlicht wird.
Gültig bis	Wann dieser wissensartikel abläuft. Dieser artikel wird nach diesem Datum oder wenn kein Datum ausgewählt ist, nicht in Suchergebnissen angezeigt.
Bild	Ein Bild, das bei der Suche über das Legacy-Wissensportal neben dem artikel angezeigt wird.
Workflow	[Schreibgeschützt] Der Veröffentlichungsstatus des Artikels, z. B. Entwurf oder Veröffentlicht. Wann Neuer artikel wird eingefügt Von einem vorhandenen artikel wird der Status des neuen artikels auf zurückgesetzt **Entwurf** .
Quelle	Die Aufgabe, für die dieser Knowledge Base-Artikel erstellt wurde, als Reaktion darauf, falls vorhanden. Dieses Feld wird automatisch festgelegt, wenn Sie den Knowledge Base-Artikel aus einem Aufgabendatensatz erstellen.
Link zu Anhang	Kontrollkästchen zum automatischen Herunterladen einer angehängten Datei, wenn ein Benutzer auf den Artikel zugreift, anstatt die Artikelansicht zu öffnen. Fügen Sie dem artikel einen Anhang hinzu, um diese Option zu verwenden.
Anhänge anzeigen	Kontrollkästchen zum Anzeigen von Anlagen für Benutzer, die diesen Knowledge Base-Artikel anzeigen. Anhänge werden unter dem Artikeltext angezeigt. Fügen Sie dem Artikel einen oder mehrere Anhänge hinzu, um diese Option zu verwenden.
Kurzbeschreibung	Der Titel des Artikels. Dieser Titel erscheint beim Durchsuchen der Knowledge Base-Artikel oben im Artikel.
Text	Inhalt für den Artikel. Verwenden Sie den WYSIWYG-HTML-Editor, um Inhalte zu erstellen. Beim Durchsuchen von Knowledge Base-Artikeln wird eine Vorschau des Inhalts angezeigt.

Hinweis:
Wenn Sie eine erstellen wissensartikel, der einer Playbook-Aufgabe zugeordnet werden soll , Legen Sie fest **Knowledge Base** Feld bis **Security Incident Response Runbook** .

4. Klicken **einreichen** um den Artikel zu erstellen.

Nächste Maßnahme

Alle zusätzlichen Schritte, die zum Veröffentlichen des artikels erforderlich sind, z. B. Genehmigungen, hängen von ab Veröffentlichungs-Workflow Für die Knowledge Base.

Zugehörige Informationen

Erstellen Sie ein Security Incident Response-Runbook

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eskalieren Sie einen Security Incident

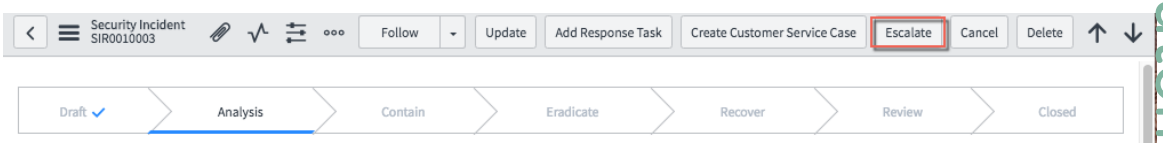
Wenn für einen Security Incident ein Eskalationspfad vorhanden ist, ist die Schaltfläche Eskalation im Header des Security Incidents verfügbar.

Vorbereitungen

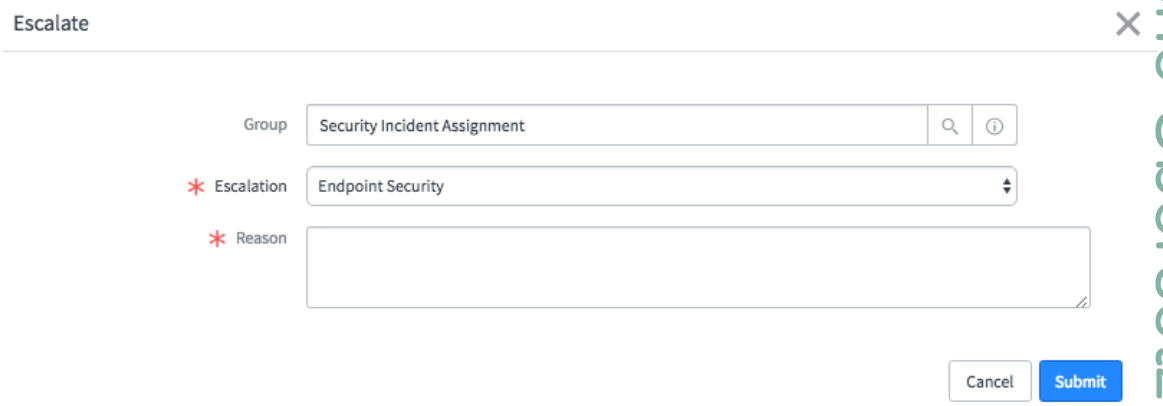
Erforderliche Rolle: sn_si.admin
Sie müssen eine Eskalationsgruppe erstellt haben, um diese Schaltfläche anzuzeigen. Weitere Informationen finden Sie unter Erstellen Sie einen Security Operations Anwenderdefinierte Eskalationsgruppe.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**an.
2. Öffnen Sie den Incident, den Sie eskalieren möchten.
3. Klicken Sie auf **Eskalieren** Schaltfläche.



4. Wählen Sie eine Eskalationsgruppe aus.
5. Geben Sie einen Grund für die Eskalation ein.



6. Klicken Sie auf **Absenden**.
   Updates **Zuweisungsgruppe** Und **Zugewiesen an** Für den Security Incident.

Verwalten Sie Aktivitäten nach dem Incident

Basierend auf den Anforderungen Ihres Unternehmens ist häufig eine Überprüfung der Herkunft und Bearbeitung von Security Incidents erforderlich.

Die Überprüfung nach IncidentFunktionalität in ServiceNow Stellt viele Tools zur Automatisierung, Nachverfolgung, Auditierung und Vereinfachung dieses Prozesses bereit.

In diesem Abschnitt wird Folgendes beschrieben:

- Weisen Sie Rollen für die Überprüfung nach Incident zu
- Konfigurieren Sie eine Bewertungsauslöserbedingung
- Führen Sie eine Fragebogenbasierte Überprüfung nach Incident durch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie PIR-Zuweisungsregeln
- Prüfbericht nach Incident

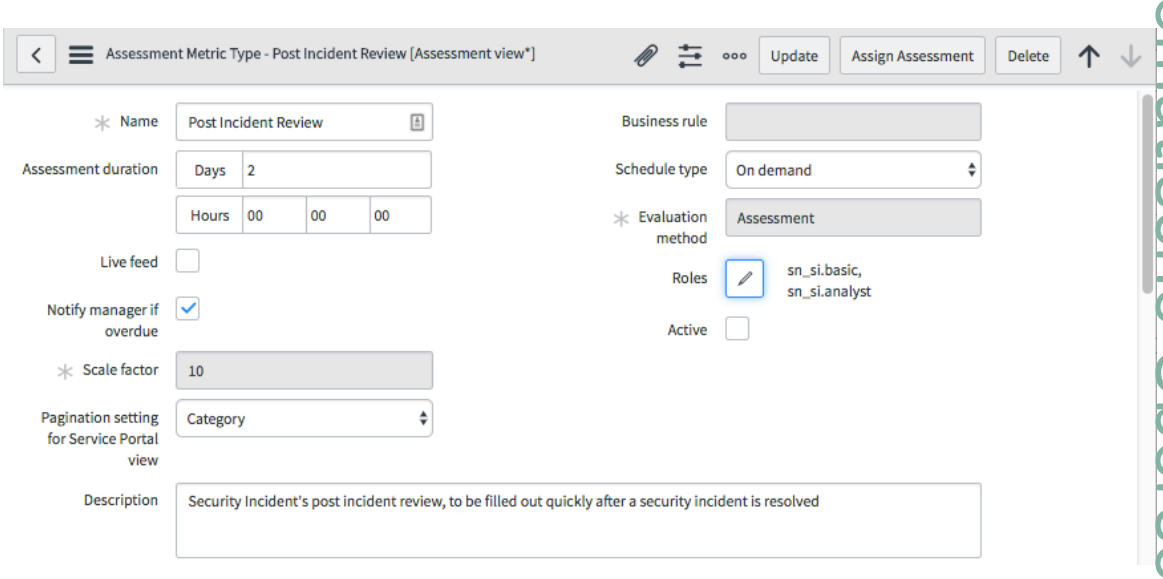
Weisen Sie Rollen für die Überprüfung nach Incident zu

Sie können Fragen auf bestimmte vordefinierte Gruppen ausrichten, indem Sie den Kategorien der Nachprüfung von Incidents (PIR) Rollen zuweisen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Bewertungen** > **Metrikdefinition** > **Typen**an.
2. Unter **Typen** Spalte, suchen Sie nach **Überprüfung Nach Incident** Datensatz.
3. Öffnen Sie den Datensatz.
4. Weisen Sie dieser Fragekategorie eine oder mehrere Rollen zu.



5. Klicken Sie auf **Aktualisieren**.
6. Navigieren zu **Anwenderadministration** > **Anwender**an.
7. Wählen Sie einen Anwender aus
8. Fügen Sie dem Anwenderdatensatz eine oder mehrere Metriktyprollen hinzu.

> **Hinweis:**
> Die Rollen müssen den Rollen entsprechen, die in der Kategorie „Überprüfung nach Incident“ zugewiesen sind.

Prüfbericht nach Incident

Mit der Funktion „Berichte nach Incident-Überprüfung“ (PIR) können Sie Berichte nach Incident-Überprüfung über die Registerkarte „Überprüfung nach Incident“ einrichten und herunterladen.

Der Sicherheitsadministrator kann die Berichtsvorlagen erstellen und konfigurieren und diese Vorlagen mithilfe der Berichtskonfiguration dem Security Incident zuordnen. Ein Sicherheitsanalyst kann den Bericht dann anzeigen oder herunterladen, nachdem der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident gelöst wurde und der Status in den Status „Überprüfen“ aktualisiert wurde.

Ein PDF-Bericht wird generiert und an den Security Incident angehängt, wenn der Incident nach erfolgreicher Konfiguration in den Status Geschlossen versetzt wird.

Hinweis:
Die Berichtsfunktion ist anwendbar und wird von Orlando Patch9 unterstützt.

Um Ihre Berichte zur Überprüfung nach Incident anzupassen, müssen Sie die folgende Konfiguration vornehmen.

1. **Berichtsvorlagen** : Anpassen und konfigurieren Sie die folgenden Berichtsvorlagenfunktionen, um dem Bericht zusätzliche Informationen hinzuzufügen:
   a. Zeitachse
   b. Branding
   c. Vorlagenskripts
2. **Berichtkonfiguration**

In diesem Abschnitt wird das Konfigurationsverfahren beschrieben:

Berichtsvorlagen

Verwenden Sie#den###Abschnitt Berichtsvorlagen, um primäre und zusätzliche Berichtsvorlagen zu erstellen, die#auf#die Security Incidents angewendet werden#, um##den##Bericht zur Überprüfung nach Incident zu generieren. Sie können###den Bericht basierend auf Ihren Anforderungen formatieren und konfigurieren. #Die Vorlagen helfen Ihnen auch, die Bewertungsdetails in die Vorlage aufzunehmen.

Im Folgenden sind einige optionale Schritte aufgeführt, die beim Erstellen der Vorlage ausgeführt werden können:

1. Branding-Informationen werden konfiguriert.
2. Seitengröße und Seitenrand einrichten.
3. Hinzufügen von Security Incident-bezogenen Feldern (anwenderdefiniert und Standard).
4. Mit den folgenden vordefinierten anwenderdefinierten Token:
   a. *$sessionUser*: Gibt#den angemeldeten Anwendernamen zurück
   b. *$date*:#Gibt#das aktuelle Datum zurück
   c. *$if_not_null_start#&#$if_not_null_end*Wenn diese Tags für Felder verwendet werden, werden die Tags nur angezeigt, wenn der Wert vorhanden ist. #Beispiel:
      - *${if_not_null_start:problem}*
      - *Problem Category: ${problem.category}*
      - *${if_not_null_end:problem}*
5. Einschließlich der zugehörigen Listendaten mithilfe der Vorlagenskripts. Weitere Informationen finden Sie im Abschnitt unten auf **Vorlagenskripts** .
6. Einschließlich der Zeitleisteninformationen mithilfe der Zeitleistenfilter. Weitere Informationen finden Sie im Abschnitt unten auf **Zeitleiste** .
7. Verwalten und Formatieren des Vorlageninhalts wie Anhänge, Tabellen und Bilder.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die erweiterten Funktionen der Symbolleiste für Berichtsvorlagen sind nur ab der Paris-Release-Version verfügbar.

Schlüsselpunkte der Berichtsvorlagen:

1. Die an die Berichtsvorlage angehängten Bilder werden im Bericht „Überprüfung nach Incident##“ nur angezeigt, wenn sie in der Tabelle „sys_attachment“ enthalten sind.

   Hinweis:
   Bilder, die aus der Tabelle „DB_image“ ausgewählt wurden, werden nicht im Nachprüfungsbericht für Incidents angezeigt.

2. Videos werden im Bericht zur Überprüfung nach Incident nicht unterstützt.
3. Die URL in der PDF-Datei kann nicht angeklickt werden. Aktivieren, dass die URLs nicht anklickbar sind (.) Ist als (Punkt) gekennzeichnet.
4. Der Bericht wird nicht generiert, wenn die Größe der Berichtsvorlage 50 MB überschreitet.
5. Die für den Inhalt der Berichtsvorlage ausgewählte Schriftartfamilie wird nicht auf die PDF-Datei angewendet, wenn sie vom PDF-Generator nicht unterstützt wird.

   Hinweis:
   Wenn die entsprechende Schriftart nicht vorhanden ist, identifiziert der PDF-Generator die alternative nächstgelegene Schriftart und generiert dann die PDF-Datei.

6. Wenn Sie höhere Seitenmargenwerte angeben, ist das Generieren des Berichts zur Überprüfung nach Incident fehlgeschlagen. Beispiel: Oberer und unterer Rand > 450#und linker und rechter Rand > 450.
7. Wenn in der Berichtsvorlage ein großer Text ohne Leerzeichen enthalten ist, kann der Text gekürzt werden. Zeigen Sie eine Vorschau des Texts an, und ändern Sie ihn entsprechend.

Der Sicherheitsadministrator kann mit eine Vorschau des Berichts anzeigen **Vorschau Des Berichts Anzeigen** Schaltfläche, die auf der Seite „Berichtsvorlage“ verfügbar ist.

Hinweis:

Wählen Sie einen Security Incident aus, um eine Vorschau eines Berichts mit dieser Vorlage anzuzeigen Option und klicken Sie auf **Vorschau Des Berichts Anzeigen** .

Branding

Sie können den Namen der Branding-Vorlage, das Kopf-#und#Fußzeilenbild, den Kopf- und Fußzeilentext hinzufügen, Seitenzahlen generieren und den Branding-Datensatz nach der Erstellung in die Berichtsvorlage aufnehmen.

Im Folgenden finden Sie ein Beispiel für#das Branding-Berichtsformat:

Schlüsselpunkte des Brandings für Berichtsvorlagen:

1. Die maximal zulässige Größe für Kopf- und Fußzeilenbild beträgt 5 MB. Wenn die Größe den angegebenen Grenzwert überschreitet, wird im Security Incident die Fehlermeldung „Bildformat kann nicht erkannt werden“ angezeigt.
2. Die Länge des Fußzeilentexts ist auf 100 Zeichen beschränkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wenn sich der Text des Fußzeilenbilds und der Berichtsinhalt während der Vorschau überschneiden, müssen Sie Änderungen am Branding-Datensatz vornehmen.

b. Wenn der Fußzeilentext einen URL-Link enthält, kann er sich mit dem Fußzeilenbild überschneiden. Zeigen Sie eine Vorschau an, und korrigieren Sie sie nach Bedarf.

Zeitachse

Mit der Zeitleistenkonfiguration können Sie die Zeitleistenfilter nach#Bedarf erstellen und ändern. Sie können##die Aktivitätstypen filtern, die in den Bericht aufgenommen werden sollen, konfigurieren, ob die untergeordneten Aufgaben in den Bericht aufgenommen oder ausgeschlossen werden sollen, und konfigurieren, ob die Bilder in den Bericht aufgenommen oder ausgeschlossen werden sollen.

Wenn Sie eine Zeitleistenkonfiguration verwenden und ausfüllen möchten, müssen Sie das Tag wie unten beschrieben hinzufügen: `${timeline:timeline name}`. Zwei###Beispiel-Zeitleistenkonfigurationen werden##im Setup bereitgestellt, die in#der#Phishing-Berichtsvorlage und der Standardberichtsvorlage verwendet werden. #Sie können die Konfigurationen ändern und wiederverwenden.

Vorlagenskripts

Verwenden Sie die Vorlagenskripts, um die zugehörigen Listendaten, Datums- und Zeitstempel und alle anderen Daten einzubeziehen, die nicht direkt DOT-Walking-fähig sind. Im Folgenden finden Sie ein Beispiel:

Erstellen Sie ein Vorlagenskript, um die zugehörige Liste in der Berichtsvorlage anzuzeigen :

1. Um die zugehörigen Listendaten vorzubereiten, rufen Sie die Methode „PostIncidentReportUtils.fetchRelatedListDataForReport“ auf.
2. Um die Schritt1-Daten im Tabellenformat und -Stil darzustellen, rufen Sie die Methode ReportTemplateUtil.constructTablefunction auf.

Wenn Sie ein Vorlagenskript verwenden und ausfüllen möchten, müssen Sie das Tag-Vorlagenskript-Tag als hinzufügen `${template_script:script name}`.

Im Folgenden finden Sie einige Beispielvorlagenskripts, die zum Konfigurieren und Ändern Ihrer Berichte nach Incident bereitgestellt werden.

Skriptname	Beschreibung
Formatted_current_date	Gibt das aktuelle lokale Datum und die aktuelle Uhrzeit im Format DMMJJJ 00,00 AM oder PM zurück. Beispiel: 21. Januar 2021 15:51 PM PST.
si_affected_users	Gibt die betroffenen Anwender aus der zugehörigen Liste in einem tabellarischen Formular zurück.
si_Assessments	Gibt die Ergebnisse der Bewertung nach dem Incident in einem tabellarischen Formular zurück.
si_Associated_Phish_email	Gibt die zugehörigen Phishing-E-Mails aus der zugehörigen Liste in tabellarischer Form zurück.
si_Associated_Phish_Header	Gibt die zugeordneten Phishing-Header aus der zugehörigen Liste in tabellarischer Form zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Skriptname	Beschreibung
si_Business_Critikality	Gibt einen farbcodierten Geschäftsrelevanzwert zurück.
si_böswillig_erkennbare Elemente	Gibt die schädlichen erkennbaren Elemente aus der zugehörigen Liste in tabellarischer Form zurück.
si_observables	Gibt die erkennbaren Elemente aus der zugehörigen Liste in tabellarischer Form zurück.
si_Priority	Gibt einen farbcodierten Prioritätswert zurück.
si_response_Tasks	Gibt die Antwortaufgaben aus der zugehörigen Liste in einem tabellarischen Formular zurück.
si_time_to_Identify	Gibt die aufgewendete Dauer im Status Entwurf und Analyse zurück.
si_time_to_Resolve	Gibt die Zeit bis zur Lösung des Incident zurück.

Schlüsselpunkte der Berichtsvorlagenskripts:

1. Wenn eine zugehörige Liste mit mehr als 5 Spalten hinzugefügt wird, werden die Tabellendaten während der PDF-Generierung gekürzt. ##Die Mindestbreite jeder Spalte ist auf 124 px festgelegt.
2. Wenn ein Vorlagenskript den Inhalt#aufgrund technischer Probleme nicht in die Berichtsvorlage laden kann, wird im Bericht die Fehlermeldung „Fehler beim Auswerten des Vorlagenskripts“ angezeigt, und der Sicherheitsadministrator muss die Richtigkeit des Skripts bewerten, um das Problem zu beheben.
3. si_Assessments: Standardmäßig werden alle Bewertungskategorien dem Bericht hinzugefügt. Der Sicherheitsadministrator kann#die Daten filtern, indem er das Vorlagenskript nach Bedarf ändert. Fügen Sie hinzu `categories: sys_id1, # sys_id2;` Parameter zum Filtern der Daten.
4. Zeit bis zur Lösung und Zeit bis zur Identifizierung von Skripts: Verwenden Sie die Definitionsdatensätze, die Teil der zugehörigen Liste der Metriken sind. Wenn die Definitionsdatensätze#für den Security Incident nicht verfügbar sind, erstellen oder fügen Sie diese Definitionsdatensätze hinzu, um die Werte für die beiden Felder auszufüllen.

Hinweis:

Standardmäßig hat der Sicherheitsadministrator keinen Zugriff zum Anzeigen der Versionsdatensätze#einer Tabelle. Sie müssen die Administratorrolle hinzufügen, um auf die Versionsdatensätze zuzugreifen und zur vorherigen Version zurückzukehren.

Berichtkonfiguration

Verwenden Sie den Abschnitt „Berichtskonfiguration“, um die Bedingungen einzurichten und die Berichtsvorlagen auf#die#Security Incidents anzuwenden. Sie können einen primären Bericht und eine oder mehrere zusätzliche Berichtsvorlagen derselben Bedingung hinzufügen.

Im Folgenden finden Sie eine Beispielbedingung, die bereitgestellt wird, um die Phishing-Berichtsvorlage auf Incidents der Phishing-Kategorie##anzuwenden, und die andere, um die Standardberichtsvorlage auf alle Security Incidents anzuwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

##Die Standardberichtsvorlage wird auf die Security Incidents angewendet#, wenn die Bedingungen nicht erfüllt sind.

Verfahren zum Deaktivieren der neuen Implementierung

1. Deaktivieren Sie die folgenden Business-Regeln:
   a. PIR-PDF generieren
   b. Erstellen Sie Wissen Zu Abschluss Neu
2. Aktivieren Sie die folgenden Business-Regeln:
   a. PIR generieren, wenn überprüft und geschlossen wird
   b. Erstellen Sie Wissen Zum Abschluss
   c. [PIR bei Abschluss/Abbrechen/Löschen neu starten]
3. UI-Regel aktivieren, *`Hide PIR field when empty`*.
4. Wechseln Sie zum Formularlayout im Security Incident-Formular. Unter **Überprüfung Nach Incident** Abschnitt:
   a. Entfernen Sie die PIR-Berichtsauswahl aus dem PIR-Abschnitt
   b. Fügen Sie dem PIR-Abschnitt das Feld „Bericht nach Incident“ hinzu

Konfigurieren Sie die Berichtseigenschaften für die Nachprüfung von Incidents (PIR) für untergeordnete Security Incidents

Sie haben die Möglichkeit, die folgenden zwei PIR-Berichtseigenschaften für untergeordnete Security Incidents zu konfigurieren:

- **sn_si.generate_pir_Report_for_Child_si**
- **sn_si.include_child_si_timeline_in_pir**

Hinweis:
Benutzer mit der Rolle „Systemadministrator“ [admin] können die Eigenschaften anzeigen. Benutzer mit der Rolle „Sicherheitsadministrator“ [sn_si.admin] können sie ändern.

Konfigurieren Sie PIR-Berichtseigenschaften für untergeordnete Security Incidents

Eigenschaft	Monatlich
sn_si.generate_pir_Report_for_Child_si	Option zum Aktivieren der Generierung von PIR-Berichten (Post Incident Review) für untergeordnete Security Incidents. • **Typ**: true | false • **Standardwert**: false • **Standort** : Navigieren Sie zu alle > Systemeigenschaften > alle Eigenschaften.
sn_si.include_child_si_timeline_in_pir	Option, um die Zeitleiste der untergeordneten Security Incidents in den PIR-Bericht des übergeordneten Security Incidents aufzunehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie PIR-Berichtseigenschaften für untergeordnete Security Incidents (Fortsetzung)

Eigenschaft	Monatlich
	• **Typ**: true | false • **Standardwert**: false • **Standort** : Navigieren Sie zu alle > Systemeigenschaften > alle Eigenschaften.

Verwalten Sie Den Überprüfungsbericht Nach Dem Incident

Der Bericht „Überprüfung nach Incident verwalten“ enthält die Informationen, die vom Sicherheitsadministrator konfiguriert und angewendet wurden, und die Sicherheitsanalysten können die Zeitleistenfilter zur Laufzeit ändern und herunterladen.

Vorbereitungen
Erforderliche Rolle: sn.si_Analyst

Warum und wann dieser Vorgang ausgeführt wird
Der Sicherheitsanalyst kann entweder die verfügbaren primären oder zusätzlichen Berichtsvorlagen auswählen, die Zeitleistenfilter konfigurieren, eine Vorschau anzeigen und den Bericht herunterladen. Der Sicherheitsanalyst kann den Bericht auch direkt mit der zuletzt angewendeten Zeitleistenkonfiguration herunterladen.

Der Sicherheitsanalyst kann über die Registerkarte Überprüfung nach Incident auf die Berichte zugreifen.

Prozedur

1. Navigieren Sie zum Security Incident im Status Überprüfen.
2. Klicken Sie Auf **Überprüfung Nach Incident** Registerkarte.
3. Wenn sich der Security Incident in befindet **Überprüfen** status:
   Berichtsvorlage:
   - Standardmäßig wird die primäre Berichtsvorlage, die auf der Einrichtungsseite konfiguriert wurde, auf den Security Incident angewendet und kann heruntergeladen werden.
   - Der Analyst kann andere Berichte aus der Dropdown-Liste auswählen, um den Bericht zu konfigurieren und herunterzuladen.
4. **Konfigurieren/Vorschau:**

   Ein Sicherheitsanalyst kann eine Vorschau der Berichtsvorlagenkonfiguration anzeigen und ändern. In der aktuellen Konfiguration kann der Sicherheitsanalyst nur die Zeitleistenfilter ändern.

   Wenn die Konfiguration für den primären Bericht geändert wird, bevor der Security Incident geschlossen wird, wird der Überprüfungsbericht nach dem Incident, der an den Security Incident angehängt ist, gemäß den vom Sicherheitsanalysten vorgenommenen Änderungen aktualisiert. Nach dem Abschluss kann der Analyst die Konfiguration ändern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und den Bericht unterwegs herunterladen. Der angehängte Bericht würde jedoch der letzten Konfiguration vor dem Abschluss entsprechen.

Führen Sie die folgenden Schritte aus, um den Bericht zu konfigurieren/in der Vorschau anzuzeigen:

a. Wählen Sie die gewünschte Berichtsvorlage aus **Berichtsvorlage** Dropdown-Liste auf der **Überprüfung Nach Incident** Registerkarte.

b. Klicken Sie Auf **Konfigurieren/Vorschau Anzeigen** Registerkarte.

c. **Aktualisieren** Oder konfigurieren Sie die Zeitleistenfilter nach Bedarf.

d. Verwenden Sie **Bilder Anzeigen** Kontrollkästchen zum Einbeziehen oder Ausschließen der Bilder in die Zeitleiste. Wenn diese Option deaktiviert ist, werden nur die Namen der Bilder im Zeitleistenabschnitt enthalten.

e. Verwenden Sie **Untergeordnete Aufgaben Anzeigen** Kontrollkästchen zum Auflisten aller untergeordneten Aufgaben, die dem Security Incident zugeordnet sind.

5. **Speichern** Die Konfiguration, und klicken Sie auf **Vorschau** Registerkarte, um eine Vorschau des Berichts anzuzeigen und herunterzuladen.

6. Klicken Sie Auf **Herunterladen** Um den Bericht direkt herunterzuladen.

Konfigurieren Sie eine Bewertungsauslöserbedingung

Definieren Sie Regelbedingungen, und generieren Sie erforderliche und optionale Bewertungen für bestimmte Security Incidents.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Hinweis:
Um die Funktion „Auslöserbedingungen für Bewertung nach Incident“ zu verwenden, müssen Sie ein Upgrade auf durchführen Security Incident Response11.0. Vor dem Upgrade müssen Sie alle Anpassungen rückgängig machen, die für den Metriktyp „Überprüfung nach Incident“ und die Auslöserbedingungen vorgenommen wurden. Darüber hinaus müssen Sie möglicherweise auch die Anpassungen rückgängig machen, die an den Geschäftsregeln vorgenommen wurden, die für die Überprüfung nach Incident spezifisch sind.

- Erfordern Sie den Abschluss der Bewertungen
- Store-Beauftragter

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Überprüfung nach Incident – Bewertungen-Setup**an.

2. In **Bewertungsauslöserbedingungen Konfigurieren** Klicken Sie auf Abschnitt **Konfigurieren** .

Hinweis:
Im Formular „Bewertungskonfigurationen“ und im Abschnitt „Bewertungskonfigurationen“ die **Generieren Sie Bewertungen** Das Kontrollkästchen ist standardmäßig aktiviert.

- Wenn Sie das Kontrollkästchen aktivieren, wird für jeden Security Incident eine optionale Bewertung erstellt.
- Wenn Sie das Kontrollkästchen deaktivieren, werden die Bewertungen nicht generiert. Die Bewertungsregeln werden nicht angezeigt, und Sie können keine Bedingungen für die Security Incidents konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Geben Sie im Formular „Bewertungskonfigurationen“ im Abschnitt Bedingungen die erforderlichen Informationen an.

   a. In **Name** Feld den Regelnamen angeben.

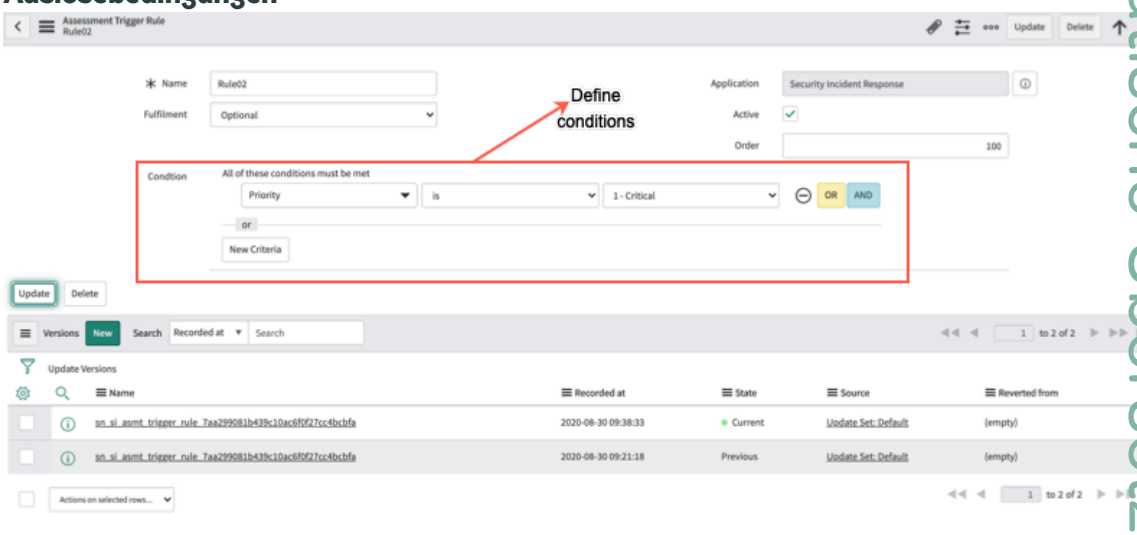
   b. In **Erfüllung** Feld den Erfüllungstyp angeben.

   c. Um eine Bedingung zu konfigurieren, klicken Sie auf den Regeldatensatz, und definieren Sie Bedingungen in **Bedingung** Feld.

Hinweis:

- Wenn Sie eine Regel erstellen, ohne eine Bedingung in zu definieren **Bedingung** Wird die Bedingung als „wahr“ ausgewertet, und die Regel gilt für alle Security Incidents.
- Sie können eine bestimmte Regel definieren, um die Bewertungen entweder obligatorisch oder optional zu machen, und die Bewertungen werden für die verbleibenden Security Incidents nicht generiert, die nicht den definierten Regeln entsprechen.

Auslösebedingungen



Beispiele für Bewertungsauslöserbedingungen

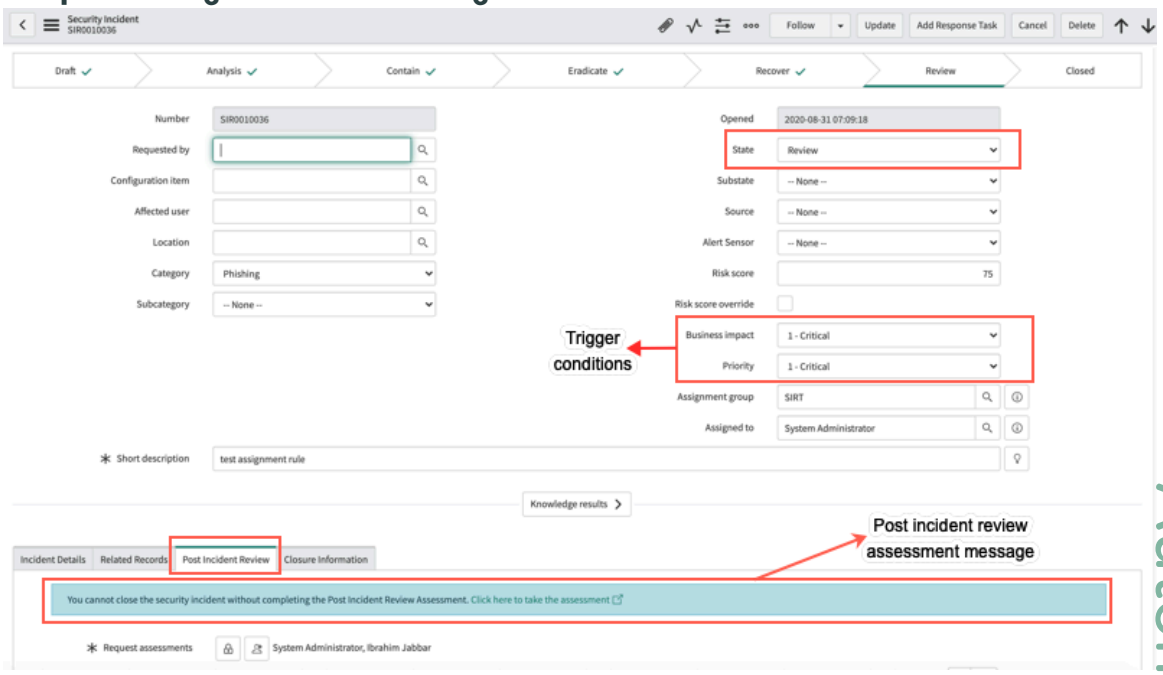
Die folgenden Beispiele zeigen verschiedene Szenarien, wie obligatorische und optionale Bewertungsauslöserbedingungen generiert werden.

- Generieren Sie im Formular „Bewertungsauslöserbedingung“ obligatorische Bewertungen, wenn die Option ist **Priorität** Und **Geschäftsauswirkung** Für einen Security Incident ist auf festgelegt **Kritisch** Auf der **Bewertungsauslöserregel** Seite. In einem solchen Szenario können die Sicherheitsanalysten den Incident erst schließen, wenn die obligatorischen Bewertungen abgeschlossen sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für obligatorische Bewertung



- Wie Sie in diesem Beispiel sehen können, wenn sich ein Security Incident in einem befindet **Überprüfen** status: Sicherheitsanalysten können den Security Incident nicht schließen, ohne den abzuschließen **Bewertung Der Überprüfung Nach Incident** . Ein Bewertungslink ist verfügbar, um die Bewertung an die Sicherheitsanalysten weiterzuleiten, die dem Incident zugewiesen sind (oder die die Bewertung angefordert haben).
- Generieren Sie im Formular „Bewertungsauslöserbedingung“ optionale Bewertungen, wenn die **Priorität** Und **Geschäftsauswirkung** Für einen Security Incident ist auf festgelegt **Hoch** . Wenn die Sicherheitsanalysten in diesem Beispiel die Bewertungen nicht abschließen und den Security Incident nicht schließen, werden die Bewertungen automatisch abgebrochen.
- Wenn die obligatorischen oder optionalen Bewertungen nicht mit dem Security Incident übereinstimmen, werden für solche Security Incidents keine Bewertungen generiert. Ein Sicherheitsanalyst kann den Security Incident schließen, ohne die Bewertung der Überprüfung nach dem Incident abzuschließen.

Führen Sie eine Fragebogenbasierte Überprüfung nach Incident durch

Sie können entscheiden, dass eine Überprüfung des Security Incident nach dem Incident gerechtfertigt ist. Eine Überprüfung nach Incident beschreibt, was passiert ist, hilft bei der Bestimmung des Incident-Auftretens und identifiziert, wie er in Zukunft vermieden oder behandelt werden kann.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.Manager, sn_si.Analyst

Hinweis:

Jeder Anwender kann unabhängig von seiner Rolle an einem Fragebogen zur Überprüfung nach Incident teilnehmen. Rollen können einer Überprüfung zugewiesen werden.

Warum und wann dieser Vorgang ausgeführt wird

Die ServiceNow Security Incident Response Die Anwendung kann die Erfassung von Informationen zur Überprüfung nach dem Incident von allen an einem Security Incident beteiligten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Personen mithilfe von Fragebogen automatisieren. Wenn Sie sich entscheiden, einen Fragebogen als Teil einer Überprüfung nach Incident zu verwenden, wird eine Liste von Fragen, die für den Security Incident relevant sind, an die anwenderdefinierte Liste der Teilnehmer gesendet. Wenn jeder Anwender den Fragebogen ausfüllt, wird der Bericht nach dem Incident automatisch generiert. Der Bericht fasst alle Informationen im Zusammenhang mit dem Security Incident sowie alle Antworten auf die Überprüfung nach dem Incident zusammen.

Eine erste Liste von Fragen wird mit dem Basissystem bereitgestellt, sie können jedoch angepasst werden. Sie können Kategorien erstellen und ihnen neue Fragen hinzufügen oder einzelne Fragen innerhalb vorhandener Kategorien ändern. Sie können Fragen basierend auf Rollen stellen. Sie können definieren, wann bestimmte Fragen gestellt werden. Es können Fragen geben, die Sie nur für Ihre UNIX-Server stellen, z. B. oder nur, wenn kriminelle Aktivitäten vorliegen. Sie können Fragen definieren, die abhängig von der Antwort auf eine andere Frage oder dem Wert in einem Feld im Formular gestellt werden. Es kann sogar Fragen geben, die vollständig durch Abfragen der Datenbank ausgefüllt werden.

Nachdem der Security Incident gelöst und in verschoben wurde **Überprüfen** status, Bewertungen werden für alle zugewiesenen Anwender und Anwender generiert, die direkt aus hinzugefügt werden **Bewertungen anfordern** Liste.

Der Fragebogen kann ein hilfreiches Tool zum Sammeln von Informationen über die Behandlung des Security Incidents aus verschiedenen Quellen sein.

Während der Überprüfung können Sie der Liste weitere Anwender hinzufügen oder vorhandene Anwender aus der Liste entfernen, es sei denn, sie haben bereits mit dem Ausfüllen des Fragebogens begonnen. Wenn Sie der Liste neue Anwender hinzufügen, erhalten sie die Fragen, wenn der Datensatz gespeichert wird. Der Security Incident kann erst geschlossen werden, wenn alle Fragebogen abgeschlossen wurden. Wenn Fragebogen von jedem Anwender ausgefüllt werden, wird der Bericht nach dem Incident automatisch generiert (und erneut generiert) und auf der angezeigt **Überprüfung Nach Incident** Registerkarte.

So starten Sie eine Überprüfung nach dem Incident:

Prozedur

1. Erstellen Sie einen Security Incident , Oder öffnen Sie eine vorhandene, indem Sie zu navigieren **Security Incident** > **Incidents** > **Mir zugewiesen (oder dem Team zugewiesen oder nicht zugewiesene Incidents)**an.
2. Klicken Sie auf **Überprüfung Nach Incident** Registerkarte.
3. Die **Bewertungen anfordern** Das Feld ist standardmäßig auf die Person in festgelegt **Zugewiesen an** Feld.
   Klicken Sie auf das Sperrsymbol, um der Überprüfungsliste weitere Anwender hinzuzufügen. Nachdem das Feld entsperrt wurde, sind Optionen zum Hinzufügen oder Entfernen mehrerer Anwender, Rollen oder zum Eingeben von Anwender-E-Mail-Adressen verfügbar.
4. Wenn Sie Ihre Einträge abgeschlossen haben, klicken Sie auf das Schlosssymbol, um das Feld zu sperren.

Hinweis:
Sie können auch Bedingungen definieren, die bei Erfüllung in einem Security Incident dazu führen können, dass bestimmte Anwender automatisch zu hinzugefügt werden **Bewertungen anfordern** Feld für diesen Security Incident. Beispiel: Wenn ein Security Incident ist **Kategorie** Wird in geändert **Phishing** , Bestimmte Personen, die über Fachkenntnisse in Phishing-Bedrohungen verfügen, können der Liste der Überprüfung nach Incident hinzugefügt werden. Weitere Informationen finden Sie unter Erstellen Sie PIR-Zuweisungsregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Aktualisieren**.
   Wenn der Incident in geht **Überprüfen** status (oder sofort, wenn er sich bereits im befindet **Überprüfen** status) erhält jeder der Anwender in der Überprüfungsliste einen ersten E-Mail-Benachrichtigung . Erinnerungen werden gesendet, wenn sich das Fälligkeitsdatum nähert. Wenn jeder Anwender über den E-Mail-Link oder über die Website auf den Fragebogen zugreift **Überprüfung nach Incident** > **Meine ausstehenden Überprüfungen**, Die angezeigten Fragen stammen aus allen Kategorien, die zu diesem Security Incident passen. Wenn neue Anwender der Überprüfungsliste hinzugefügt werden, bevor das Fälligkeitsdatum erreicht ist, werden ihnen Benachrichtigungen gesendet, wenn der Security Incident gespeichert wird.

   Wenn Anwender ihre Fragebogen ausfüllen, werden die Daten im Bericht nach dem Incident zusammengestellt und der Bericht in angezeigt **Überprüfung Nach Incident** Registerkarte. Die Fragebogendaten werden in angezeigt **Ergebnisse** Registerkarte.

Erstellen Sie Fragebogenkategorien für die Überprüfung nach Incidents

Sie können die Fragebogenkategorien verwenden, die im Basissystem enthalten sind, oder eigene Kategorien erstellen.

Vorbereitungen
Erforderliche Rolle: sn.si_admin

Warum und wann dieser Vorgang ausgeführt wird
So erstellen Sie eine neue Kategorie von Fragen:

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Überprüfung nach Incident**an.
2. Klicken Sie Auf **Überprüfen Sie Fragen** .
   Eine Liste von Kategorien wird zusammen mit ihrer Reihenfolge und Filtern angezeigt, die definieren, unter welchen Bedingungen die Fragen gestellt werden (z. B. nur, wenn die Kategorie Security Incident lautet) `Kriminelle Aktivität`). Jede Kategorie ist ein Abschnitt im Fragebogen zur Überprüfung nach Incident, und die Fragen in jeder Kategorie werden nur berücksichtigt, wenn der Security Incident dem Bedingungsfilter entspricht. Für eine Kategorie von Fragen, die nur für Linux-Server gelten, richten Sie beispielsweise einen Filter ein, der Security Incidents ausgewählt hat, bei denen der betroffene Ressourcentyp Linux-Server war. In dieser Kategorie erstellen Sie dann alle Fragen, die erforderlich sind, wenn sich ein Security Incident auf einem Linux-Server befand. Sie verwenden eine der im Basissystem bereitgestellten Kategorien oder erstellen eine neue Kategorie. Bei diesem Verfahren wird davon ausgegangen, dass Sie eine neue Kategorie erstellen möchten, bevor Sie Fragen definieren.
3. Klicken Sie Auf **Neu** In der Liste der Kategorien.
4. Füllen Sie die entsprechenden Felder im Formular aus.

Security Incident

Feld	Beschreibung
Name	Name für die Kategorie, die im Security Incident-Fragebogen angezeigt wird.
Typ	Die Überprüfung nach Incident ist der Standard.
Stakeholder erstellen	Nicht verwendet von Security Incident Response.
Tabelle	Dieses Feld wird automatisch zugewiesen, sobald das Formular übermittelt wurde.
Filter	Geben Sie die Bedingung ein, die bestimmt, wann Fragen in dieser Kategorie verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn ein Security Incident-Datensatz mit diesem Filter übereinstimmt, werden die Fragen in eine Überprüfung nach dem Incident für diesen Security Incident aufgenommen. Filter können beliebige Daten im Datensatz oder in anderen Datensätzen verwenden, die mit diesem Datensatz verknüpft sind. Zum Beispiel die Abteilung des Managers des anfordernden Anwenders.
Anwendung	Umfangsanwendung für den Incident.
Gewichtung	Numerischer Wert, der die Bedeutung dieser Metrik im Vergleich zu anderen Metriken in derselben Kategorie darstellt. Standardmäßig beträgt die Gewichtung 10.
Metriken Insgesamt	Anzahl der von der Kategorie verwendeten Metriken.
Beschreibung	Beschreibung des Fragebogens.

5. Klicken Sie Auf **Übermitteln** Zum Speichern der Kategorie.

Verfassen Sie Fragen zur Überprüfung nach dem Incident

Sie können die Fragen verwenden, die im Basissystem enthalten sind, oder eigene Fragen erstellen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Die Methoden zum Sammeln von Informationen zur Überprüfung nach Incident können in Form von Fragen oder als Daten erfolgen, die automatisch mithilfe von Skripts erfasst werden.

Fragen können von den Antworten auf andere Fragen abhängen. Sie können beispielsweise fragen, ob alle erforderlichen Protokolle verfügbar waren. Wenn die Antwort „Nein“ lautet, stellen Sie eine Folgefrage, um festzustellen, welche der erforderlichen Protokolle nicht aktiviert wurden.

Geskriptete Datensammlung, auch Skriptmetriken genannt, erfasst Daten im Zusammenhang mit dem Security Incident über von Ihnen geschriebene Skripts. Diese Aktion kann weit über die Daten im Security Incident-Datensatz selbst hinausgehen. Beispielsweise könnte eine Skriptmetrik die letzte Ausfallzeit für einen Server erfassen, der von diesem Security Incident betroffen ist.

Schließlich können Sie die beiden Typen mischen. Fragen können Standardwerte aus einem Skript oder einfach aus einem Feld im Security Incident-Datensatz haben. Wenn Sie einen verwenden Standardantwort von··· Art der Frage: Sie können auswählen, ob der Anwender die Frage immer beantworten soll – wobei der Standardwert ihm einen Anfangswert gibt – oder ob dem Anwender nur die Frage gestellt werden soll, wenn das Skript oder Feld leer ist.

So erstellen Sie eine neue Frage:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Überprüfung nach Incident**an.
2. Klicken Sie auf die Kategorie, für die Sie eine neue Frage erstellen möchten.
3. Klicken Sie auf **Bewertungsmetriken** Registerkarte.
4. Klicken Sie auf **Neu**.
   Sie können auch auf eine vorhandene Frage klicken, um sie zu ändern.
5. Füllen Sie die entsprechenden Felder im Formular aus.

Metrikformular

Feld	Beschreibung
Name	Name der Metrik (Frage oder Skript). Wenn die Metrik eine geskriptete Datensammlung ist, wird dieser Name im Bericht nach dem Incident angezeigt.
Kategorie	Die Kategorie, zu der die Metrik gehört. Das System füllt diese Kategorie automatisch auf, wenn Sie eine neue Metrik aus dem Formular „Metrikkategorie“ erstellen. **Hinweis:** Sie können die Kategorie nicht ändern, wenn das Feld **Abhängig von** gesetzt ist oder eine andere Metrik von dieser Metrik abhängt.
Methode	Gibt den Typ der Metrik wie folgt an: ○ *`Assessment`*: Eine Frage ohne Standardwert. Es gibt mehrere Datentypen, die in definiert werden können **Datentyp** Feld auf der **Feldtyp** Registerkarte, z. B. Kontrollkästchen, Auswahllisten, Texteingabe. ○ *`Script`*: Geskriptete Metrik. Erhält Werte durch Schreiben eines benutzerdefinierten Skripts. Die *`Script`*Methode ist kompatibel mit **Dauer** , **Nummer** , Und **Prozentsatz** Datentypen. ○ *`Default answer from field`*: Eine Frage, bei der die Standardantwort aus einem ausgewählten Feld im Security Incident stammt. Wenn Sie diese Option auswählen, werden dem zwei Felder hinzugefügt **Allgemein** Registerkarte: ▪ *`Default answer`*: Wählen Sie das Feld im Security Incident aus, das die Standardantwort für die Frage enthält. Beispiel: Für die Frage „Wer hat diesen Incident ursprünglich gemeldet?“, die **Angefordert von** Feld wäre wahrscheinlich eine Auswahl. ▪ *`Ask question`*: Gibt an, wann die Frage gestellt werden soll: Immer oder nur, wenn **Standardantwort** Feld ist leer. Im obigen Beispiel wird die Frage gestellt, wenn der **Angefordert von** Feld ist leer. ○ *`Default answer from script`*: Eine Frage, bei der die Standardantwort aus einem Skript stammt. Die Antwort kann eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Zahl, eine Zeichenfolge oder ein Prozentsatz sein. Die **Allgemein** Registerkarte fügt ein Feld hinzu: *`Ask question`*: Wie angibt, wann die Frage gestellt werden soll: Immer oder nur, wenn das Skript keine Standardantwort bereitstellt. Das Skript wird in der Registerkarte **Feldtyp** definiert. **Hinweis:** Wenn Sie einen auswählen **Datentyp** Das mit dem ausgewählten nicht kompatibel ist **Methode** , Ändert das System automatisch **Methode** Auf einen kompatiblen Wert.
Gewichtung	[Erforderlich] Numerischer Wert, der die Bedeutung dieser Metrik im Vergleich zu anderen Metriken in derselben Kategorie darstellt. Standardmäßig beträgt die Gewichtung 10. Dieses Feld ist sichtbar und erforderlich, es sein denn der **Datentyp** ist **Datum**, **Datum/Zeit** oder **Zeichenfolge**. Diese Datentypen werden nicht in die Ergebnisberechnungen einbezogen.
Reihenfolge	[Erforderlich] Numerischer Wert, der die Reihenfolge der Metrikfrage in Bewertungsfragebögen in Relation zu anderen Metrikfragen in derselben Kategorie bestimmt. Die Metrik mit dem kleinsten Wert für die Reihenfolge erscheint als erste Frage im Kategoriebereich. Standardmäßig ist die Reihenfolge 100. **Hinweis:** Es spielt keine Rolle, welchen Wert für die Reihenfolge Sie für Metriken mit der Skriptmethode verwenden, da sie nicht in Fragebögen angezeigt werden.
Aktiv	Kontrollkästchen, das bestimmt, ob diese Metrik verwendet wird. Wenn das Kontrollkästchen nicht aktiviert ist, ist der Metrikdatensatz so, als wäre er nicht vorhanden.
Obligatorisch	Checkbox, die die Metrikfrage für Bewertungsfragebogen obligatorisch (ausgewählt) oder optional (deaktiviert) macht. Benutzer können Fragebögen erst einreichen, wenn sie gültige Antworten auf alle obligatorischen Fragen geben, die durch eine rote Feldstatusanzeige gekennzeichnet sind. Dieses Feld ist nur sichtbar, wenn **Abhängig von** Feld ist leer, und der Datentyp ist nicht **Kontrollkästchen** .

6. Klicken Sie auf **Allgemein** Registerkarte und füllen Sie die Felder entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Allgemein“

Feld	Beschreibung
Frage	Text, der als Frage zu Fragebogen zur Überprüfung von Security Incidents verwendet werden soll. Geben Sie eine klare, einfache Frage ein, die einfach zu beantworten ist, z. B. **Wie haben wir den Incident eingedämmt**
Beschreibung	Informationen zur Metrik und deren Auswertung. Wenn `Method`Ist **Bewertung** , Fügen Sie Details hinzu, die Anwendern helfen, zu verstehen, wie sie die Frage beantworten. Dieser Text wird als Hinweis angezeigt, wenn ein Benutzer auf den Fragentext im Fragebogen verweist.
Hängt von ab und wird angezeigt, wenn	Wählen Sie eine Frage im aus **Abhängig von** Feld, von dem die aktuelle Frage abhängt. Zum Beispiel die Frage „welche zusätzlichen Protokolle wurden benötigt?“ Hängt von der Frage „waren alle erforderlichen Protokolle verfügbar?“ ab. Als Nächstes verwenden Sie **Wird angezeigt, wenn** Feld, das identifiziert, wann die abhängige Frage in Fragebogen angezeigt werden soll. Beispiel: Wenn Sie möchten, dass die abhängige Frage nur gestellt wird, wenn der Anwender antwortet **Nein** Zu „waren alle erforderlichen Protokolle verfügbar?“ Frage, wählen Sie aus **Nein** In **Wird angezeigt, wenn** Feld. **Hinweis:** Das System verhindert die Erstellung rekursiver Abhängigkeiten zwischen Metriken. Wenn beispielsweise Metrik A von Metrik B abhängt, kann Metrik B nicht von Metrik A abhängen.

7. Klicken Sie auf **Feldtyp** Registerkarte und füllen Sie die Felder entsprechend aus.

Registerkarte „Feldtyp“

Feld	Beschreibung
Datentyp	Der Datentyp der erwarteten Antwort, von der die Liste der verfügbaren Typen für die ausgewählte Methode abhängt. Wenn die Methode **Bewertung** ist, bestimmt der Datentyp, wie Benutzer die entsprechende Frage in Fragebögen beantworten. Wenn die Methode **Skript** ist, bestimmt der Datentyp, wie das System die Bewertungsergebnisse berechnet. **Hinweis:** Wenn eine andere Metrik von dieser Metrik abhängt, kann der Datentyp nicht geändert werden.
Antworten zufällig	Kontrollkästchen, das bestimmt, ob die Antwortoptionen für diese Metrikfrage jedes Mal in zufälliger Reihenfolge angezeigt werden sollen, wenn ein Anwender einen Bewertungsfragebogen öffnet, der die Frage enthält. Die Antworteinstellung kann von der Reihenfolge beeinflusst werden, in der Antwortoptionen angezeigt werden. Dies kann zu verzerrten Ergebnissen führen. Durch Randomisieren von Antwortmöglichkeiten kann diese Verzerrung vermieden werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dieses Feld ist nur sichtbar, wenn Sie auswählen **Likert-Skala** Oder **Auswahl** In **Datentyp** Feld.
Abhängiges Plugin	[Erforderlich, wenn *Method*Ist **Skript** .] Plugin, das die im Skript abgefragten Tabellen enthält. Das System führt das Metrikskript nur dann aus, wenn das Plugin aktiv ist. Die standardmäßig verfügbaren Werte sind **Asset Management**, **CMDB**, **Kern**, **Cost Management**, **Procurement** und **Software Asset Management**. Dieses Feld ist nur sichtbar, wenn *Method*lst **Skript** . **Hinweis:** ◦ Wenn der Core-Standardwert verwendet wird, wird das Skript immer ausgeführt. ◦ Wenn Sie Administrator sind, können Sie dem Feld weitere Plugins-Auswahlmöglichkeiten hinzufügen.
Skaladefinition	Eine Einstellung, die bestimmt, ob kleinere oder größere numerische Werte einer guten Bewertung bei den Bewertungsergebnisberechnungen entsprechen. Wählen Sie Aus **Niedrig** Wenn weniger numerische Werte besser sind, z. B. für eine Metrik, die die Anzahl der Fehler für einen Lieferanten misst. Wählen Sie **Hoch**, wenn größere numerische Werte besser sind, z. B. für eine Metrik, die die Benutzerzufriedenheit auf einer Skala von eins bis fünf misst. Der Standardwert ist **Hoch**. Dieses Feld ist sichtbar und erforderlich, es sei denn *Data type*lst **Datum** , **Datum/Uhrzeit** , Oder **Zeichenfolge** . Die Ergebnisse für diese Datentypen werden nicht in die Ergebnisberechnungen einbezogen.
Min.	Niedrigster numerischer Wert, der als Antwortoption bei Assessments oder als skalierter Wert in einer Skriptmetrik verwendet werden soll. Dieses Feld ist nur sichtbar und nur erforderlich, wenn bestimmte Datentypen ausgewählt sind. Wenn der Datentyp ist **Auswahl** Oder **Likert-Skala** , Dieses Feld ist schreibgeschützt und wird automatisch basierend auf der kleinsten Metrikdefinition festgelegt *Value*.
Max.	Höchster numerischer Wert, der als Antwortoption oder skalierter Wert verwendet werden soll. Dieses Feld ist nur sichtbar und nur erforderlich, wenn bestimmte Datentypen ausgewählt sind. Wenn der Datentyp ist **Auswahl** Oder **Likert-Skala** , Dieses Feld ist schreibgeschützt und wird automatisch basierend auf der größten Metrikdefinition festgelegt *Value*.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Skript	Skript, das die gewünschten Systeminformationen abruft. Das Skript verfügt über eine Eingabevariable, die mit der ID des Security Incident (primär) festgelegt ist, und drei mögliche Ausgabevariablen, die vom Skript festgelegt werden: String_result, scaled_result und actual_result. Wenn der Datentyp „Zeichenfolge“ ist, ist nur „string_result“ erforderlich. Dieses Feld ist sichtbar und erforderlich, wenn *Method*lst **Skript** , Oder der Standardwert stammt aus einem Skript.
Vorlage	Ein vordefinierter Satz allgemeiner Antworten, die für die Frage verwendet werden sollen. Beispielsweise würde eine Häufigkeitsvorlage wahrscheinlich mit dem Wert „nie“ beginnen und bis zum obersten Wert „immer“ reichen. Dieses Feld ist nur sichtbar und erforderlich, wenn *Data type*lst **Vorlage** . **Hinweis:** Wenn eine andere Metrik von dieser Metrik abhängt, kann die Vorlage nicht geändert werden.

8. **Wahlweise:** Wenn Sie Ihre Einträge abgeschlossen haben, klicken Sie auf **Aktualisieren** .

Erstellen Sie PIR-Zuweisungsregeln

Zusätzlich zum manuellen Hinzufügen von Anwendern nach der Überprüfung von Incidents für einen Security Incident können Sie Zuweisungsregeln für das automatische Hinzufügen von Anwendern zur Liste definieren.

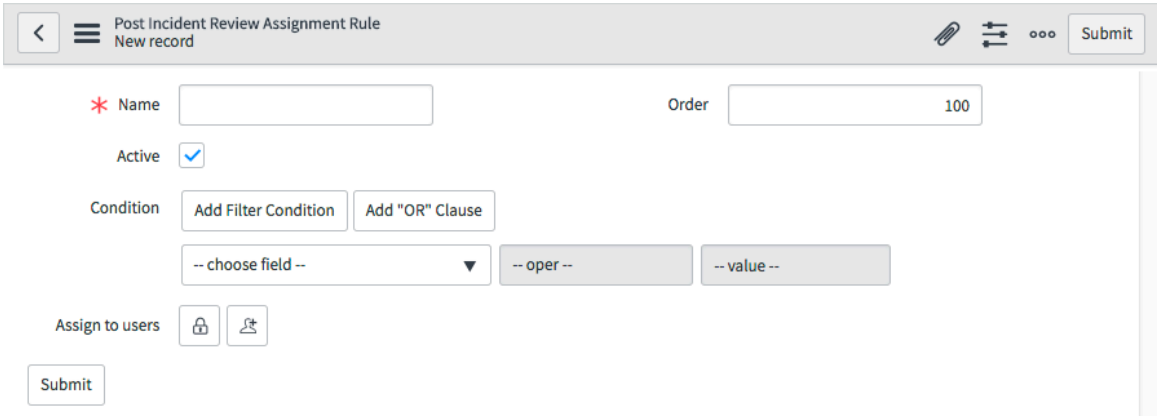
Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.Manager, sn_si.Analyst

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration** > **Überprüfung nach Incident – Bewertungen-Setup**an.
2. Führen Sie einen Drilldown zu **Anwenderzuweisungsregeln** Abschnitt.
3. Klicken Sie auf **Konfigurieren**.
4. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Zuweisungsregel.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Regel zu aktivieren.
Reihenfolge	Geben Sie einen numerischen Wert ein, um anzugeben, wo in der Liste der Zuweisungsregeln diese Regel angezeigt werden soll. Niedrigere Zahlen werden oben in der Liste angezeigt. **Hinweis:** Nur die erste übereinstimmende Zuweisungsregel wird ausgeführt, und nur die in dieser Regel definierten Anwender werden der Bewertungsliste hinzugefügt.
Bedingung	Verwenden Sie den Bedingungsgenerator Zum Definieren der Bedingungen, die im Security Incident erfüllt sein müssen, damit diese Regel ausgeführt wird. Weitere Informationen finden Sie im folgenden Beispiel.
Zu Anwendern zuweisen	Klicken Sie auf das Sperrsymbol, um der Überprüfungsliste Anwender hinzuzufügen. Nachdem das Feld entsperrt wurde, sind Optionen zum Hinzufügen oder Entfernen mehrerer Anwender, Rollen oder zum Eingeben von Anwender-E-Mail-Adressen verfügbar.

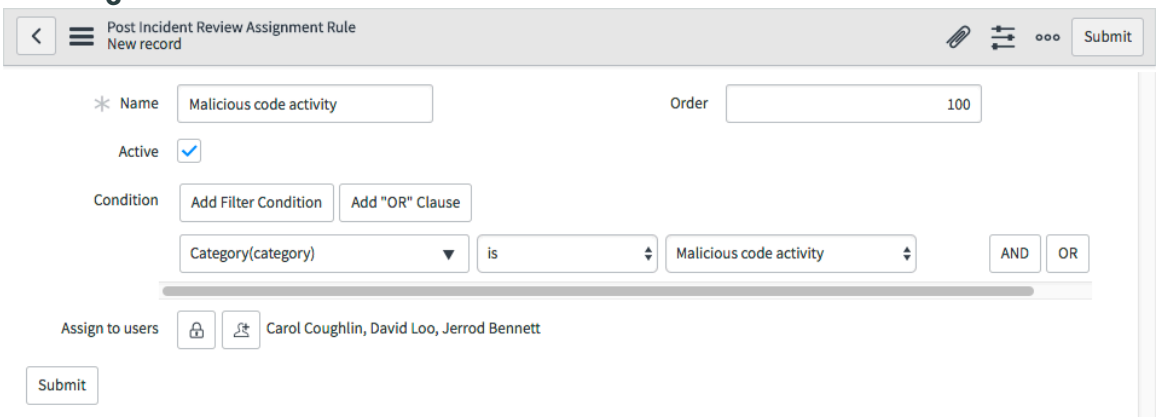
6. Klicken Sie auf **Absenden**.

Example: Böswillige Code-Aktivität

In der hier angezeigten Zuweisungsregel für die Überprüfung nach Incident, wenn ein Security Incident mit angezeigt wird **Kategorie** Feld auf festgelegt **Schädliche Codeaktivität** Übergänge zu **Überprüfen** status, die drei identifizierten Anwender (die zufällig Experten im Umgang mit schädlichen Code-Aktivitäten sind) werden der Liste der Anwender hinzugefügt, die den Fragebogen zur Überprüfung nach dem Incident für diesen Security Incident erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Böswillige Code-Aktivität



Schließen Sie Security Incidents

Wenn ein Security Incident in den Status „Überprüfen“ übergegangen ist, kann er geschlossen und ein entsprechender Abschlusscode eingegeben werden. Abschlusscodes können später durchsucht werden, um den Standort zu erleichtern.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:

In vorherigen Versionen von Security Incident Response, Anwender können Security Incidents oder Anforderungen als Spam schließen. In Istanbul Release, die Spam-Option ist nicht mehr verfügbar. Spam Security Incidents oder Anforderungen können je nach Bedarf abgebrochen oder gelöscht werden.

Prozedur

1. Wenn der Security Incident, den Sie schließen möchten, noch nicht geöffnet ist, navigieren Sie zu **Security Incident** > **Incidents** > **Alle Incidents anzeigen**, Und suchen Sie den Security Incident, den Sie schließen möchten.

   Hinweis:

   Wenn vorhanden Bewertungen der Überprüfung nach Incident Die für diesen Security Incident nicht abgeschlossen wurden, kann der Security Incident nicht geschlossen werden. Zurück zu **Security Incident** > **Überprüfung nach Incident** > **Alle unvollständigen Überprüfungen**, Suchen Sie die unvollständigen Überprüfungen, und bitten Sie die Überprüfer entweder, ihre Überprüfungen abzuschließen, oder brechen Sie die verbleibenden Bewertungen ab.

2. Klicken Sie auf **Abschlussinformationen** Registerkarte und füllen Sie die Felder entsprechend aus.

Security Incident

Feld	Beschreibung
Wissensartikel erstellen	Wählen Sie dieses Feld aus, um automatisch einen Entwurf für einen Knowledge Base-artikel zu erstellen, der den Inhalt der Überprüfung nach Incident enthält.
Abschlusscode	Wählen Sie den Abschlusscode aus, der den Grund, aus dem Sie diesen Security Incident schließen, am besten beschreibt. ○ Untersuchung abgeschlossen ○ Bedrohung gemindert ○ Schwachstelle gepatcht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Ungültige Schwachstelle ○ Nicht behandelt ○ Falsch positiv
Geschlossen von	Zeigt den Anwender an, der den Security Incident nach der Aktualisierung des Datensatzes geschlossen hat.
Geschlossen	Zeigt Datum und Uhrzeit des Abschlusses nach der Aktualisierung des Datensatzes an.
Abschlussnotizen	Geben Sie zusätzliche Notizen ein, die das Ergebnis des Schließens dieses Security Incident beschreiben.

3. Klicken Sie auf **Aktualisieren**.
4. Der zugewiesene Anwender kann manuell ändern **Status** Bis **Geschlossen** .
   Wenn ein übergeordneter Incident geschlossen wird, werden alle Antwortaufgaben, die zum untergeordneten Incident gehören, abgebrochen. Wenn keine anderen Arten von Aufgaben vorhanden sind, wird auch der untergeordnete Incident geschlossen.

Fügen Sie einem Security Incident Abschlussinformationen hinzu

Wenn sich ein Security Incident im Status „Überprüfen“ oder „Geschlossen“ befindet, können Sie Informationen zum Abschluss eingeben.

Vorbereitungen

Erforderliche Rolle: sn_si.Basic

Prozedur

1. Wenn er nicht bereits geöffnet ist, öffnen Sie den Security Incident, den Sie aktualisieren möchten.
2. Klicken Sie auf **Zugehörige Datensätze** Registerkarte.
3. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Wissensartikel erstellen	Aktivieren Sie dieses Kontrollkästchen, um einen wissensartikel mithilfe des Inhalts des Berichts nach dem Incident zu generieren.
Abschlusscode	Wählen Sie den Abschlusscode aus, der den Grund für das Schließen des Security Incidents am besten beschreibt.
Geschlossen von	[Schreibgeschützt] zeigt den Anwender an, der den Security Incident geschlossen hat.
Geschlossen	[Schreibgeschützt] zeigt Datum und Uhrzeit des Schließens des Security Incident an.
Abschlussnotizen	Wie der Security Incident geschlossen wurde, einschließlich gelernter Lektionen, Lösung usw.

4. Klicken Sie auf eine der folgenden Registerkarten, um den Security Incident weiter zu aktualisieren:
   - Incident Details
   - Überprüfung nach Incident
5. Klicken Sie, nachdem Sie alle Eingaben vorgenommen haben, auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschränken Sie den Zugriff auf Security Incidents

Verwalten Sie den Zugriff auf Security Incidents, die vertrauliche Informationen enthalten. Sie können Security Incident-Einschränkungen erzwingen, um zu bestimmen, wer auf einen bestimmten Incident zugreifen kann, und den Zugriff nur auf bestimmte Anwender oder Gruppen beschränken.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

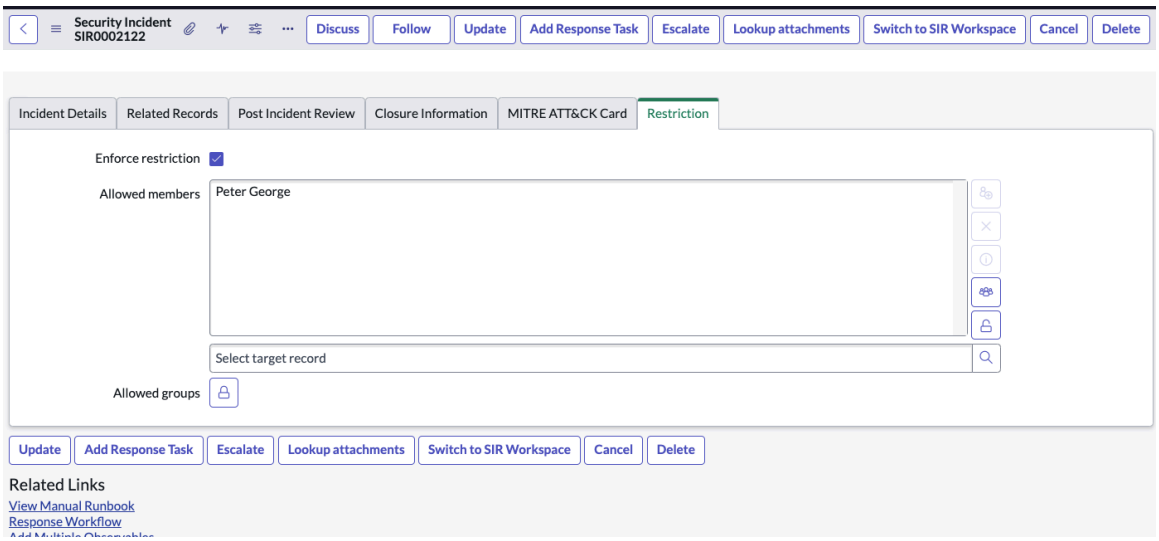
Warum und wann dieser Vorgang ausgeführt wird

Mit Security Incident-Einschränkungen können Sie ausblenden, dass andere Anwender in einer bestimmten Organisation auf kritische Security Incidents zugreifen. Mit diesen Einschränkungen können Sie eine detailliertere Möglichkeit zur Steuerung der Security Incidents bereitstellen, auf die ein Anwender zugreifen kann. Sie können eine Security Incident-Einschränkung erzwingen, indem Sie aktivieren **Einschränkung erzwingen** Kontrollkästchen und dann die Anwender oder Gruppen auswählen, die auf den bestimmten Security Incident zugreifen dürfen.

Nachdem Sie die Einschränkung für bestimmte Security Incidents durchgesetzt und den Zugriff auf bestimmte Anwender oder Gruppen beschränkt haben, können alle übrigen Anwender in Ihrer Organisation nicht auf diese Security Incidents zugreifen, auch wenn sie nach einem bestimmten eingeschränkten Security Incident suchen.

Prozedur

1. Öffnen Sie einen Security Incident, den Sie einschränken möchten.
2. Wenn Sie die klassische UI verwenden, gehen Sie wie folgt vor:
   a. Klicken Sie auf **Einschränkung** Registerkarte.
   b. Wählen Sie aus **Einschränkung erzwingen** Kontrollkästchen, um die Einschränkung des Security Incidents zu aktivieren.



   c. Klicken Sie im Feld zulässige Mitglieder auf Symbol zum Auswählen der Anwender, die auf den Security Incident zugreifen können.
   d. Wählen Sie aus Symbol, um sich selbst als zulässiger Anwender hinzuzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Wählen Sie aus Symbol zum Hinzufügen oder Entfernen von Anwendern.

f. Klicken Sie im Feld zulässige Gruppen auf Symbol zum Auswählen der Gruppen, die auf den Security Incident zugreifen können.

g. Wählen Sie aus Symbol zum Hinzufügen oder Entfernen von Gruppen.

> **Hinweis:**
> Nach **Einschränkung erzwingen** Das Kontrollkästchen ist für den Security Incident aktiviert. Nur sn_si.admin und zulässige Mitglieder oder Gruppen haben Zugriff auf den Security Incident.

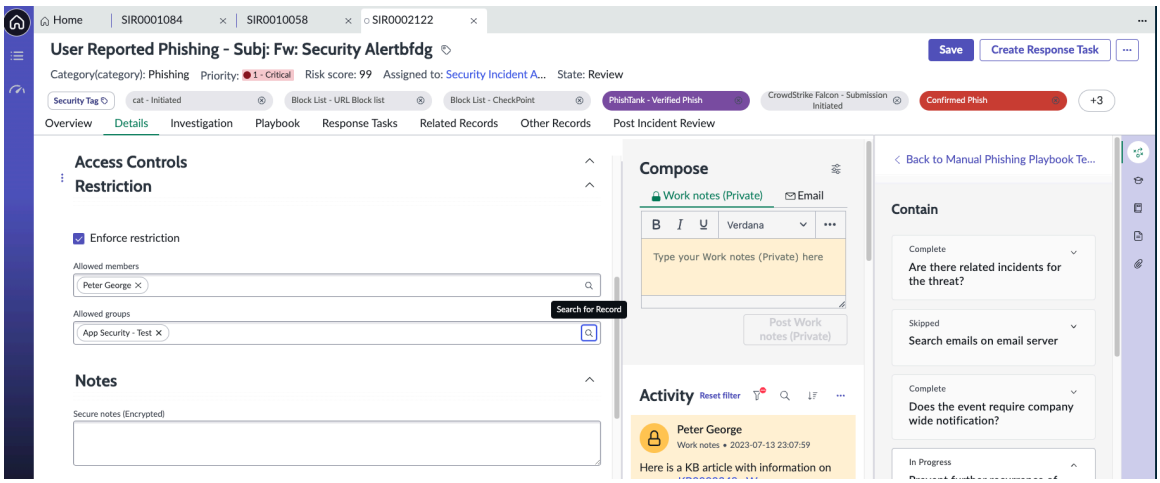
h. Klicken Sie auf **Aktualisieren**.

3. Wenn Sie SIR Workspace verwenden, gehen Sie wie folgt vor:

a. Klicken Sie im Security Incident auf **Details** Registerkarte.

b. Scrollen Sie nach unten, und klicken Sie auf **Einschränkung** Abschnitt.

c. Wählen Sie aus **Einschränkung erzwingen** Kontrollkästchen, um die Einschränkung des Security Incidents zu aktivieren.



d. Wählen Sie im Feld zulässige Mitglieder die Anwender aus, die über die Suchoption auf den Security Incident zugreifen können.

e. Wählen Sie im Feld zulässige Gruppen die Gruppen aus, die über die Suchoption auf den Security Incident zugreifen können.

> **Hinweis:**
> Nach **Einschränkung erzwingen** Das Kontrollkästchen ist für den Security Incident aktiviert. Nur sn_si.admin und zulässige Mitglieder oder Gruppen haben Zugriff auf den Security Incident.

f. Klicken Sie auf **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie Sicherheitsbedrohungen mit Sicherheitsanalyst-Arbeitsbereich

Security Incident Response Enthält eine neue Anwenderoberfläche namens Sicherheitsanalyst-Arbeitsbereich Das leistungsstarke Tools zur Unterstützung der Analyse enthält, einschließlich Playbook, PEEK-Ansicht und Registerkarten für die Bearbeitung mehrerer Security Incidents.

Speziell für Sicherheitsanalysten entwickelt, die leistungsstarken Tools in Sicherheitsanalyst-Arbeitsbereich Ermöglichen Sie es Ihnen, das ständig wachsende Datenvolumen im Zusammenhang mit Security Incidents zu analysieren. Und automatisierte Aktionen reduzieren die Zeit für die Untersuchung von Security Incidents erheblich, was der Unterschied zwischen dem Stoppen eines Angriffs und dem Erleiden eines Verstoßes sein kann.

Vor der Verwendung von Sicherheitsanalyst-Arbeitsbereich

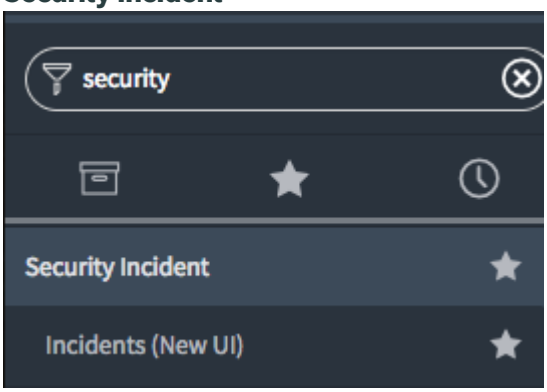
Bevor Sie mit der Verwendung von beginnen können Sicherheitsanalyst-Arbeitsbereich, Sie müssen sicherstellen, dass in Ihrer Instanz mindestens London Patch 3 installiert ist, Sie über die richtigen Rollen verfügen und verfügen Die UI-Anwendung „Security Incident Response“ wurde aus heruntergeladen ServiceNow Storean.

Hinweis:
Wenn Ihre Instanz eine ältere Version als London Patch 3 ausführt, müssen Sie das UI-Plugin „Security Incident Response“ über das HI-Kundenservice-System anfordern.

Auf Sicherheitsanalyst-Arbeitsbereich zugreifen

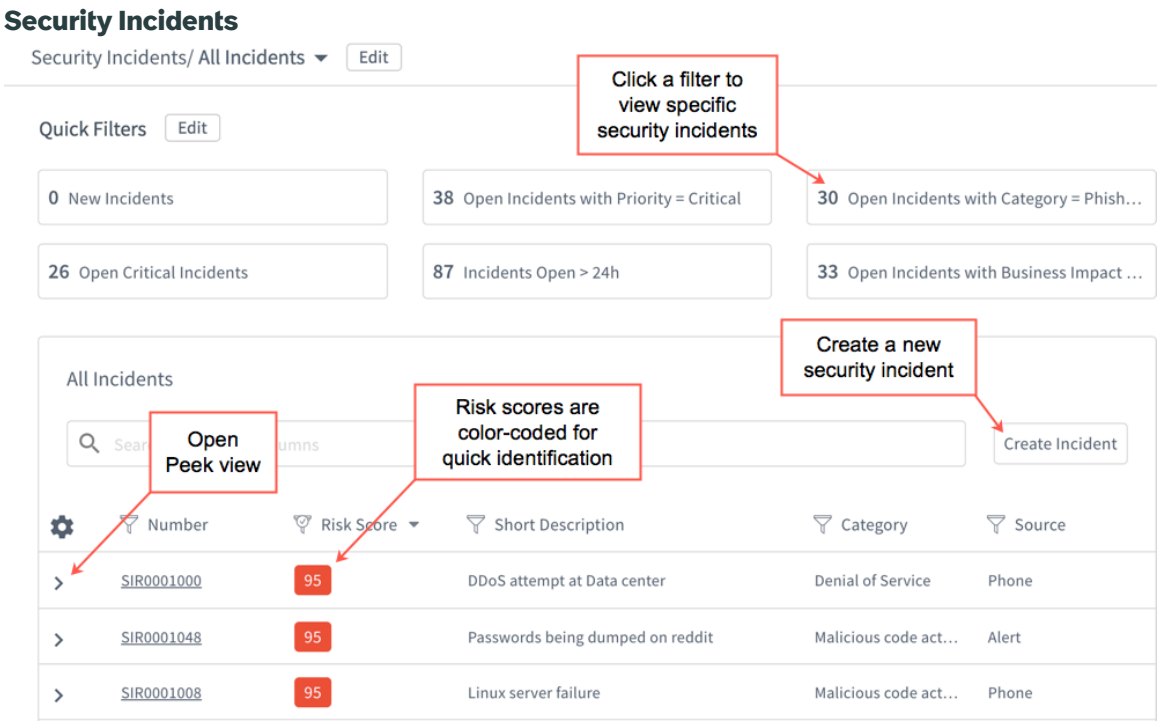
Um auf diesen neuen Arbeitsbereich zuzugreifen, navigieren Sie zu **Security Incident** > **Incidents (neue UI)**an.

Security Incident



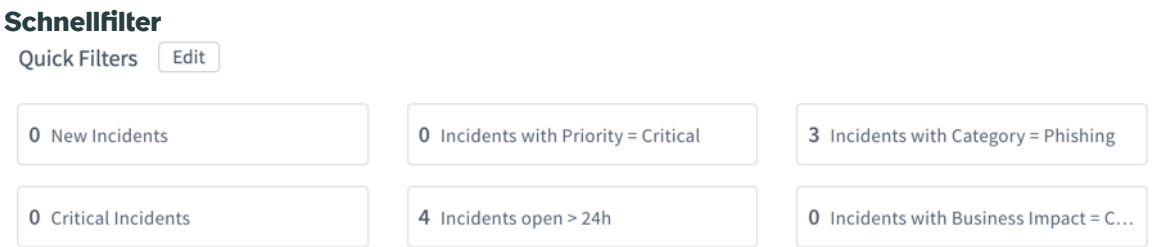
Der Arbeitsbereich wird in einer separaten Browserregisterkarte geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Suchen Sie mit Schnellfiltern nach den Security Incidents, die Sie analysieren möchten

Die Sicherheitsanalyst-Arbeitsbereich Stellt mehrere Tools zum Filtern der Liste der Security Incidents bereit, damit Sie schnell die Security Incidents finden können, die Sie analysieren möchten. Mit den Schnellfiltern können Sie eine Teilmenge der Security Incidents basierend auf den Kriterien im Filter auswählen.



Klicken Sie einfach auf den Schnellfilter, den Sie verwenden möchten.

Hinweis:
Sie können auf klicken **Bearbeiten** Schaltfläche zum Identifizieren, welche Schnellfilter auf dem Listenbildschirm angezeigt werden sollen. Mindestens ein Filter muss ausgewählt werden, maximal sechs.

Sie können zusätzliche Schnellfilter sowie primäre Filter für definieren Sicherheitsanalyst-Arbeitsbereich, Mit der klassischen Umgebung. Weitere Informationen finden Sie unter Richten Sie primäre und sekundäre Filter für ein Sicherheitsanalyst-Arbeitsbereich.

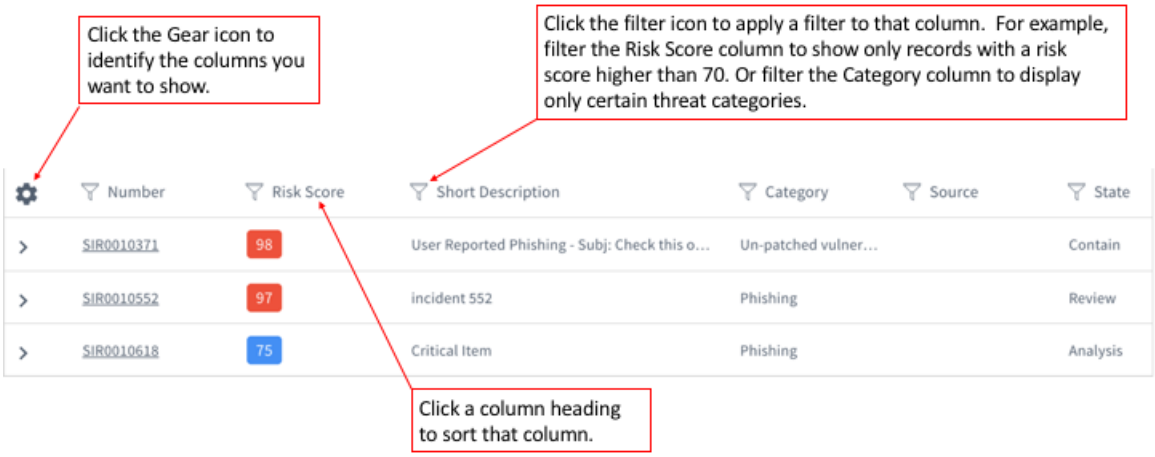
Personalisieren Sie die Security Incident-Liste

Wie bei allen Listen in Ihrer Instanz, die Sicherheitsanalyst-Arbeitsbereich Stellt Tools zum Personalisieren der Liste und zum Sortieren der angezeigten Informationen entsprechend Ihren Analyseanforderungen bereit.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

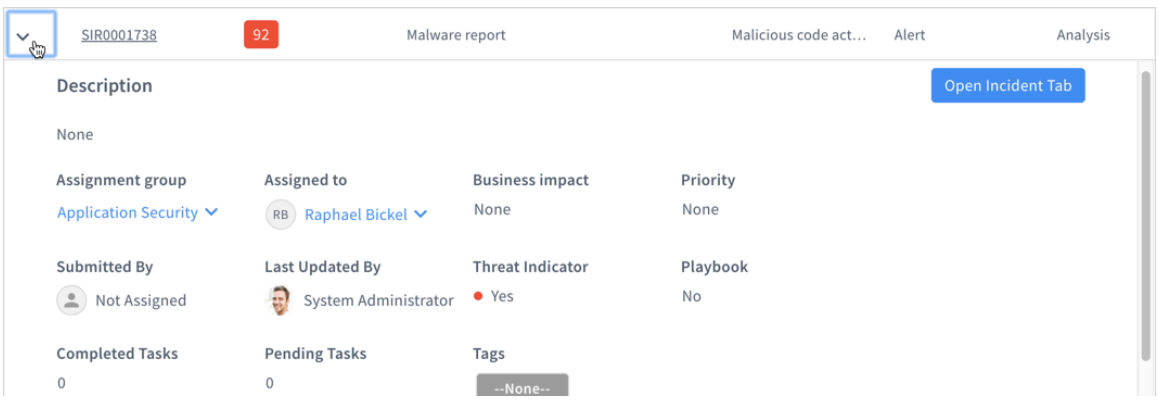
Personalisieren Sie die Security Incident-Liste



Sparen Sie Zeit mit der Peek-Ansicht

Bevor Sie einen Security Incident-Datensatz öffnen, können Sie mit der Peek-Ansicht Zeit sparen. Mit dieser Funktion können Sie wichtige Sicherheitsartefakte schnell finden, ohne die gesamte Seite neu laden zu müssen. Klicken Sie einfach auf **>** Symbol links neben einer Security Incident-Nummer, um einen Blick zu werfen.

PEEK-Ansicht

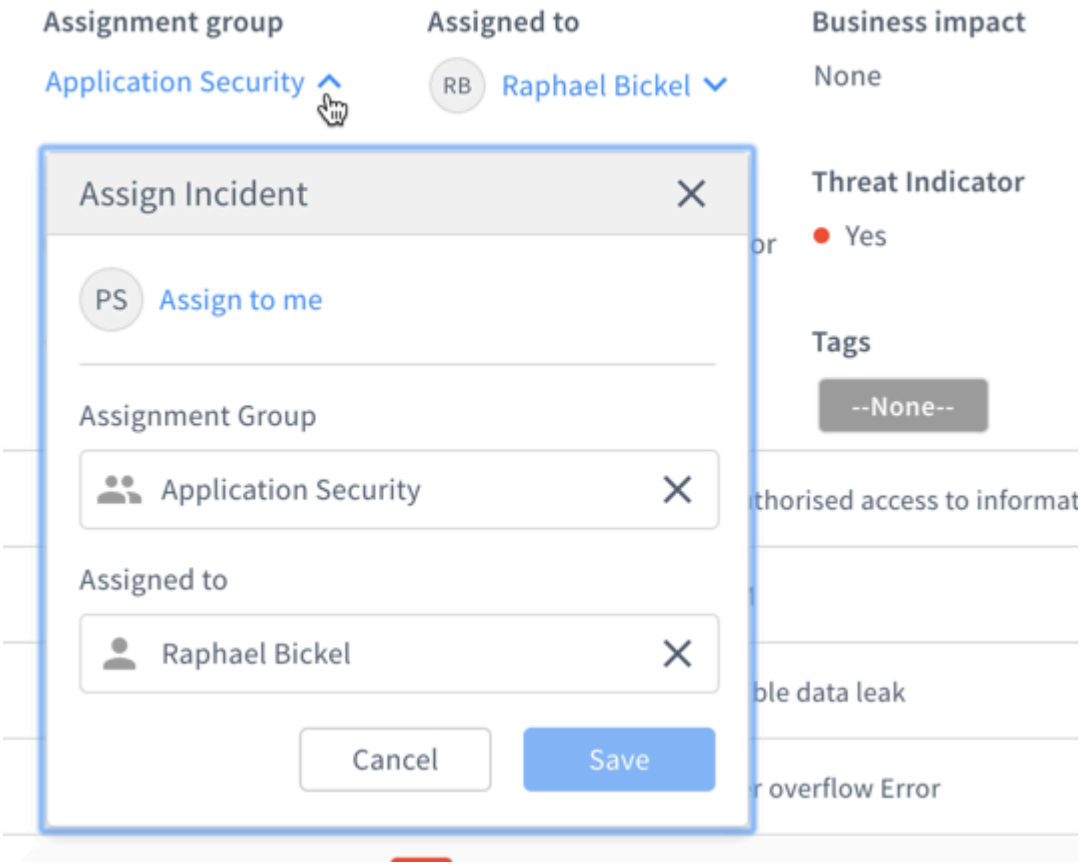


Die PEEK-Ansicht bietet einen Snapshot wichtiger Informationen in einer einzigen Ansicht. Diese Ansicht kann wertvolle Zeit sparen, wenn Sie mit mehreren Incidents arbeiten. Sie können auf bestimmte Felder auf die Abwärtspfeile klicken, um aktuelle Aktualisierungen vorzunehmen, z. B. das Zuweisen einer Zuweisungsgruppe oder eines bestimmten Analysten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details der Ansicht anzeigen



Führen Sie schnelle Aktionen für einen Security Incident aus

Nachdem Sie einen bestimmten Security Incident ausgewählt und geöffnet haben, können Sie Zeitersparnisaktionen für den Datensatz ausführen.

- Wenn Ihr Security Incident geöffnet ist, klicken Sie auf **Bearbeiten Sie Den Datensatz** Symbol, um schnelle Änderungen an einem der Felder vorzunehmen. Wenn der Datensatz geschlossen ist, können Sie nur sein Tag ändern.
- Klicken Sie Auf **Verwalten Sie Anhänge** Zum Anhängen von Dateien an den Security Incident. Sie können angehängte Dateien auch herunterladen oder entfernen und die auf die Anhänge angewendete Verschlüsselung bearbeiten.
- Klicken Sie Auf **E-Mail Verfassen** Dient zum Senden einer schnell-E-Mail an einen Kollegen. E-Mails können Freiform sein, oder Sie können E-Mails senden, die aus einer Liste von Vorlagen ausgewählt wurden. Gesendete E-Mails und empfangene Antworten werden in der Incident-Zeitleiste erfasst.

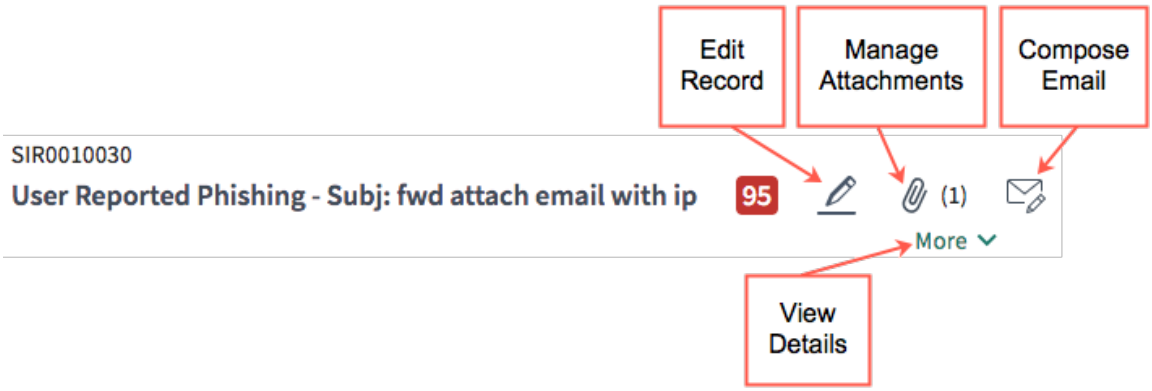
  Hinweis:
  Sie können anwenderdefinierte Vorlagen erstellen, die wiederverwendbare Inhalte für E-Mails und E-Mail-Benachrichtigungen enthalten. Variablen können zum Einfügen von Informationen verwendet werden, die für den Security Incident oder die Warnung spezifisch sind, z. B. Betreffzeile, Priorität oder Bedrohungskategorie. Verwenden Sie die Tabelle „Security Incident“ [sn_si_Incident] für E-Mails und E-Mail-Benachrichtigungen im Zusammenhang mit Security Incident Response. Weitere Informationen finden Sie unter E-Mail-Vorlagen

- Klicken Sie Auf **Mehr** Dient zum Anzeigen eines schnellen Snapshots des Security Incidents, z. B. Beschreibung, Geschäftsauswirkung und Priorität. Sie können auch auf den Abwärtspfeil in klicken **Zuweisungsgruppe** Und **Zugewiesen an** Felder zum Vornehmen von On-the-fly-Änderungen an diesen Feldern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

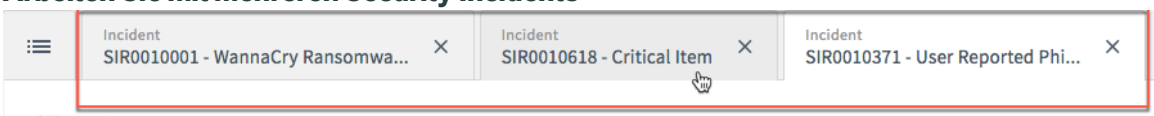
Zuweisungsgruppe



Arbeiten Sie mit mehreren Security Incidents

Die Benutzeroberfläche mit Registerkarten ermöglicht es Ihnen, mehrere Security Incidents gleichzeitig offen zu halten, sodass Sie mit einem einzigen Klick zwischen ihnen wechseln können. Dies kann Zeit sparen und Ihnen das Gesamtbild anzeigen, wenn Bedrohungen aus mehreren Quellen identifiziert werden.

Arbeiten Sie mit mehreren Security Incidents



Zeigen Sie Analyseinformationen auf den Security Incident-Registerkarten an

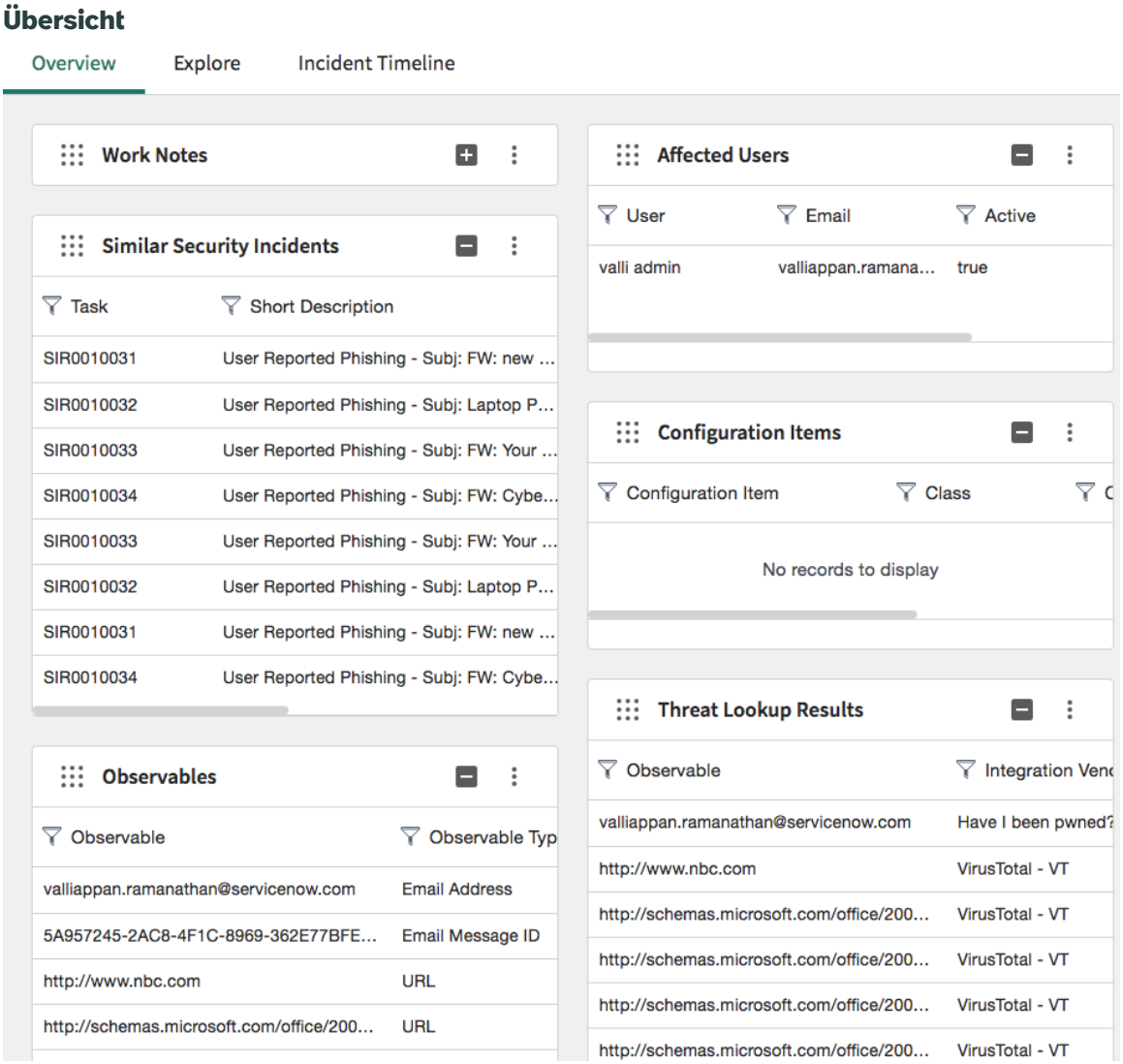
Wenn Sie einen Security Incident-Datensatz öffnen, werden drei Registerkarten angezeigt:

- Übersicht
- Untersuchen
- Incident-Zeitleiste

Registerkarte „Übersicht“

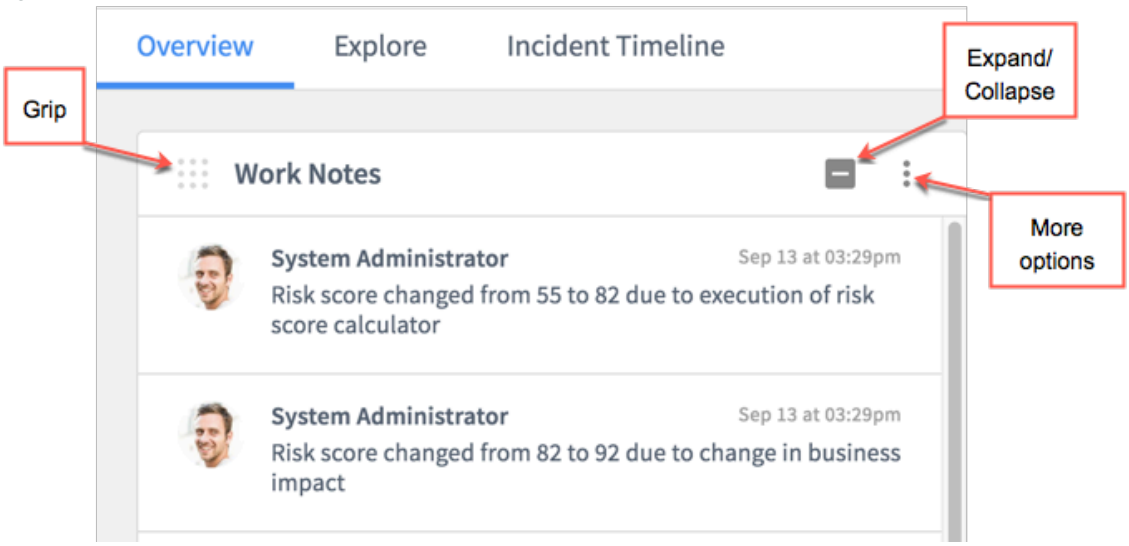
Verwenden Sie **Übersicht** Registerkarte zum Anzeigen von Informationen in einem Security Incident an einem einzelnen Ort. Es muss keine andere Anwendung oder Konsole geöffnet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Kacheln, die auf angezeigt werden **Übersicht** Registerkarten können angepasst werden. Sie können sie nach Bedarf reduzieren und erweitern und verschieben, indem Sie ziehen **Greifen** Symbol. Klicken Sie auf **Weitere Optionen** Symbol zum Löschen einer Kachel oder zum Ändern des Überschriftentexts.

Registerkarte „Übersicht“



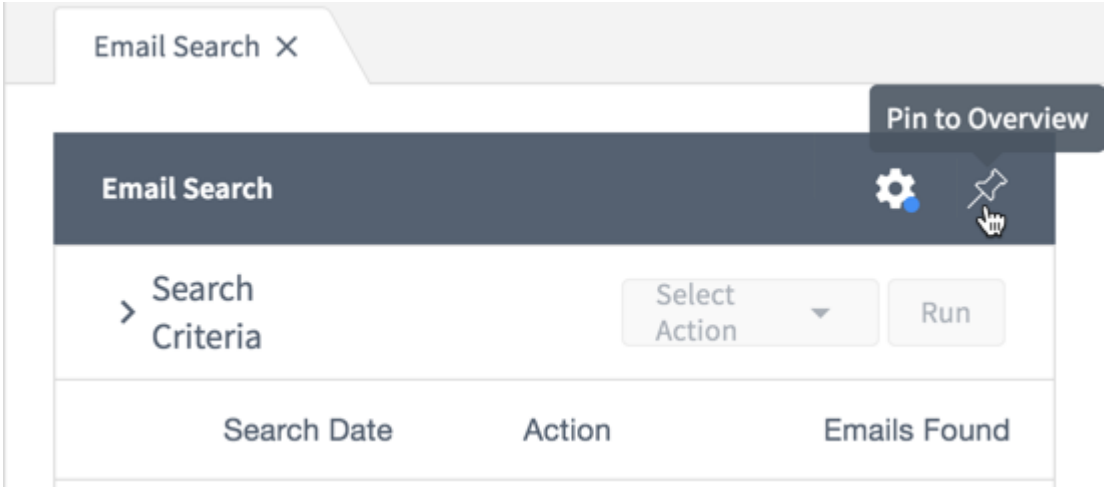
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erkunden“

Konfigurieren Sie die auf der angezeigten Kacheln **Übersicht** Registerkarte mit **Erkunden** Registerkarte. Wählen Sie einfach im linken Bereich die Kacheln aus, die Sie anzeigen möchten, und klicken Sie auf **Anheften** Symbol. Angeheftete Kacheln werden automatisch in angezeigt **Übersicht** Registerkarte.

Registerkarte „Exportieren“



Der linke Bereich von **Erkunden** Die Registerkarte enthält eine Vielzahl von Informationen, die Sie im anzeigen können **Übersicht** Registerkarte. Erweitern Sie beispielsweise **Erkennbare Elemente** Um diese zugehörigen Listen anzuzeigen.

- Erkennbare Elemente
- Bedrohungssuche – Ergebnisse
- Ergebnisse Des Sicherheitsscans
- Domänensuchen
- Ergänzung erkennbarer Elemente

Zusätzliche zugehörige Listen sind unter verfügbar **Anwender** , **Konfigurationselemente** , Und **Incidents** .

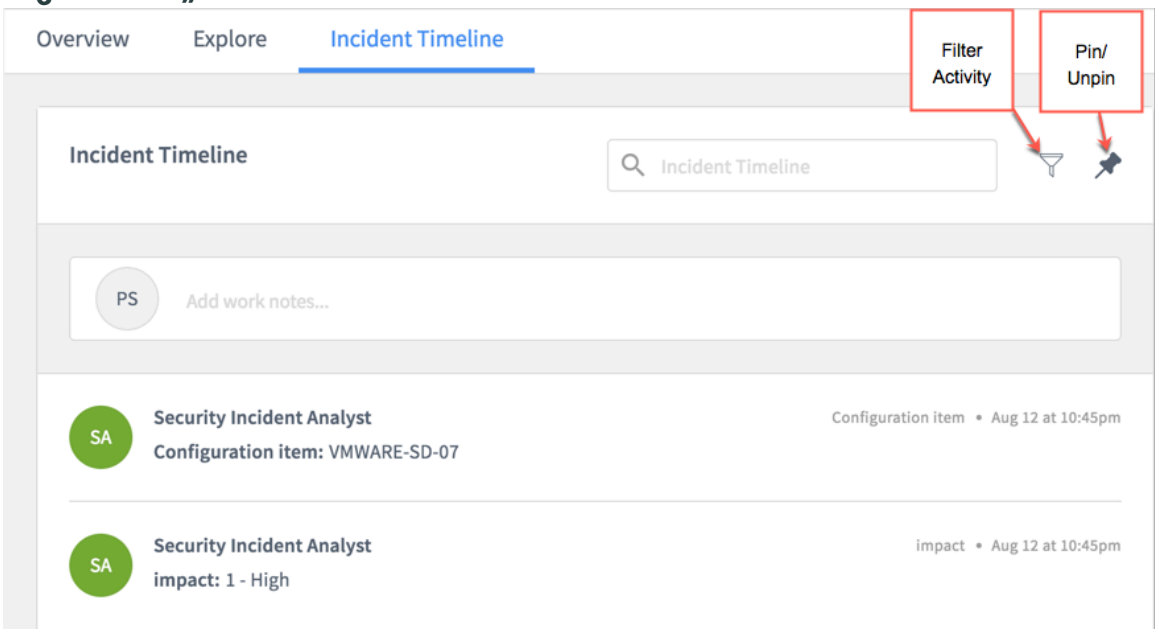
Registerkarte „Incident-Zeitleiste“

Verwenden Sie **Incident-Zeitleiste** Registerkarte während Ihrer Untersuchung zu Nachverfolgungszwecken. Jedes Mal, wenn eine Aktion für einen Security Incident ausgeführt wird, zeichnet das System sie in der Incident-Zeitleiste auf.

- Sie können der Zeitleiste auch manuell Arbeitsnotizen hinzufügen, indem Sie sie in eingeben **Fügen Sie Arbeitsnotizen hinzu** Kästchen und Klicken auf **Veröffentlichen** .
- Sie können mithilfe des Suchfelds nach einer bestimmten Zeitleistenaktivität suchen.
- Die **Filteraktivität** Mit dem Symbol können Sie nur die Arten von Zeitleistenaktivitäten anzeigen, die Sie anzeigen möchten (z. B. nur Incidents, die von einem bestimmten Analysten erstellt wurden).
- Sie können die Incident-Zeitleiste hinzufügen oder daraus entfernen **Übersicht** Registerkarte mit **Anheften/Lösen** Symbol.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Incident-Zeitleiste“



Behandeln Sie Security Incidents mit dem Playbook

Lösen Sie bestimmte Arten von Sicherheitsbedrohungen Schritt für Schritt mit den integrierten Sicherheitsanalysten-Playbooks. Beispielsweise kann ein Analyst das Playbook verwenden, um Phishing-Angriffe und Bedrohungen zu lösen, die durch schädliche Codeaktivitäten verursacht wurden. Weitere Informationen finden Sie unter Lösen Sie Sicherheitsbedrohungen mit dem Playbook.

Lösen Sie Sicherheitsbedrohungen mit dem Playbook

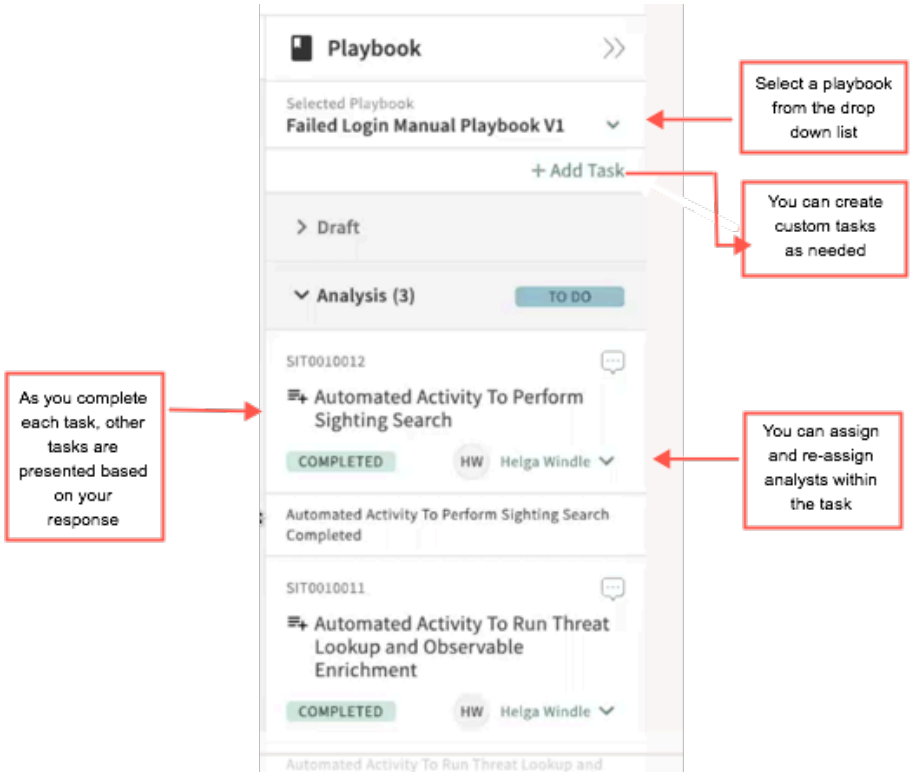
Verwenden Sie das Playbook, um bestimmte Arten von Sicherheitsbedrohungen Schritt für Schritt zu lösen. Sie können beispielsweise Phishing-Angriffe und Bedrohungen lösen, die durch schädliche Codeaktivitäten verursacht wurden, mithilfe von Playbooks.

Vorbereitungen
Erforderliche Rolle: sn_si.admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Jede Gruppe von Aufgaben (Analyse, Eindämmung usw.) führt Sie durch eine Reihe von Fragen und anderen Aktivitäten zur Lösung der Bedrohung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

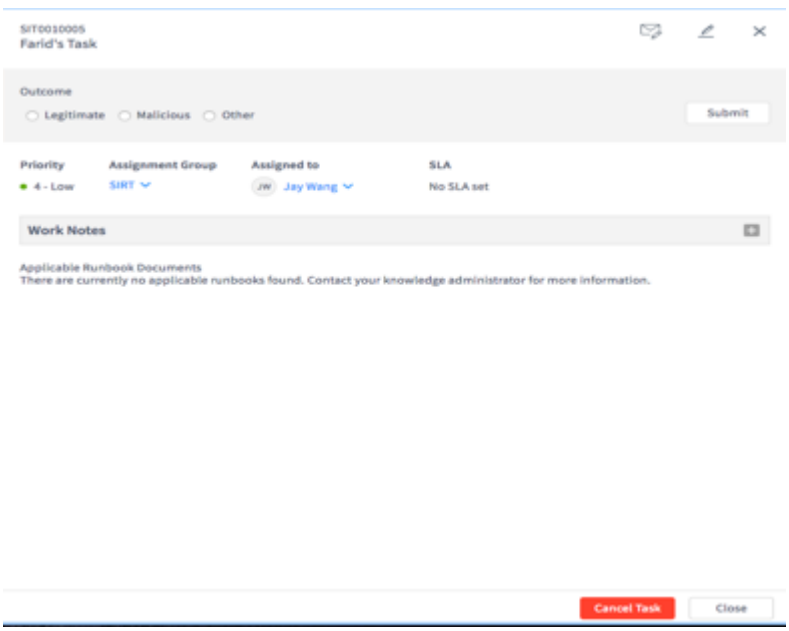
Playbook



Geben Sie während der Bearbeitung jeder Aufgabe Arbeitsnotizen ein, um ähnliche Angriffe in der Zukunft zu analysieren. Nachdem eine Bedrohung identifiziert wurde, können Sie auch Informationen im Playbook verwenden, um die Bedrohung unter Quarantäne zu stellen, ähnlich betroffene Assets zu isolieren und Malware zu entfernen.

Wissensartikel, die in jeder Aufgabe enthalten sind, enthalten Tipps und andere Informationen, die Sie bei der Durchführung der erforderlichen Schritte unterstützen.

Wissensartikel



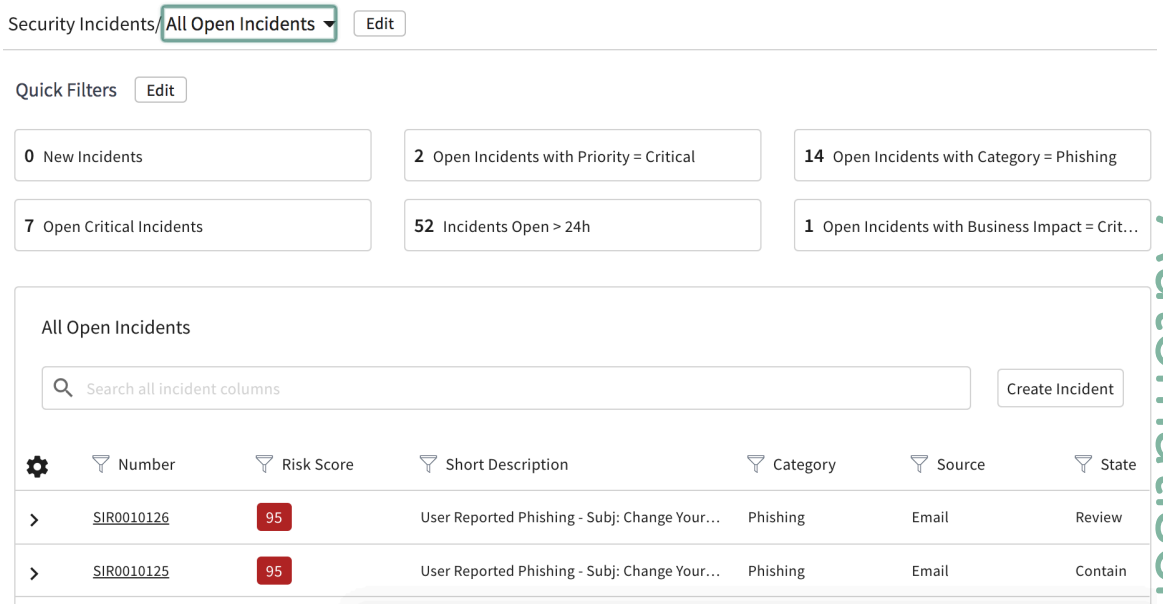
Das Basissystem enthält Wissensartikel für jede der Playbook-Aufgaben. Sie können jedoch Schreiben Sie Ihre eigenen Wissensartikel Und Ordnen Sie sie Playbook-Aufgaben zu .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Ein Beispiel für die Verwendung des Playbooks zur Analyse und Lösung einer bestimmten Bedrohung finden Sie unter Auflösen von von Anwendern gemeldeten Phishing-Angriffen mit dem Playbook.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents (neue UI)**an.
   Der Bildschirm Security Incidents zeigt Security Incidents an, die Ihnen zugewiesen wurden.

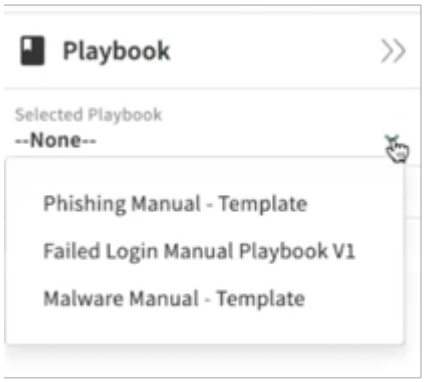


2. Sie können auf klicken **Mir zugewiesen** Auswahlliste zum Auswählen eines anderen Filters, z. B. alle offenen Incidents oder alle nicht zugewiesenen Incidents.
   Alternativ können Sie auf einen der Schnellfilter klicken, um Security Incidents eines bestimmten Typs anzuzeigen, z. B. nur kritische Incidents.
3. Klicken Sie auf den Security Incident, den Sie analysieren möchten.

   Erwägen Sie die Priorisierung von Security Incidents mit hoch Risikopunktzahlen .
4. Wenn der Playbook-Bereich am rechten Rand des Bildschirms geschlossen ist, klicken Sie auf das Playbook-Symbol ( ), um es zu öffnen.
   Wenn dem Security Incident kein Playbook zugewiesen ist, können Sie ein Playbook aus der Auswahlliste „ausgewähltes Playbook“ wie unten gezeigt auswählen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können dem Security Incident auch ein anderes Playbook zuweisen. Informationen zum Einbeziehen eines Playbooks in die ausgewählte Playbook-Auswahlliste oder zum Ändern des Playbooks für einen Security Incident finden Sie unter Aktivieren Sie Playbooks für die Analystenauswahl Für Details.

Das für den Typ der Sicherheitsbedrohung spezifische Playbook wird geöffnet. Sie ist in Kategorien ähnlicher Aufgaben unterteilt. Sie verwenden beispielsweise die Aufgaben in der **Analyse** Gruppe, um die Gültigkeit und den Umfang der Bedrohung zu bestimmen. Die **Enthalten** Die Gruppe enthält Aufgaben zum Isolieren der Bedrohung für einen bestimmten Anwender oder ein bestimmtes Asset. Die Aufgaben in **Beseitigen** Die Gruppe führt Sie durch den Prozess zum Entfernen der Malware oder zum erneuten Mapping des Hosts.

5. Klicken Sie auf die erste Gruppe (**Analyse**), und klicken Sie dann auf die erste Aufgabe im Playbook.
6. Befolgen Sie die Anweisungen in der Aufgabe.
   - Einige Aufgaben stellen eine Frage, z. B. „ist E-Mail Teil der Kampagne?“ Führen Sie die erforderliche Analyse durch, um die Frage zu beantworten, und wählen Sie aus **Ja** Oder **Nein** .
   - Wenn Sie haben Definierte Wissensartikel und verknüpfte sie Playbook-Aufgaben , Die Artikel werden angezeigt, wenn Sie mit der Arbeit an einer Aufgabe beginnen.
   - Einige Aufgaben sind Übergangsaufgaben. Sie weisen Sie einfach an, eine Aktion auszuführen, z. B. erkennbare Elemente zu einem Security Incident hinzuzufügen. Nachdem Sie die Aktion abgeschlossen haben, klicken Sie auf **Als abgeschlossen markieren** .

   Wenn Sie Aufgaben abschließen, werden Ihnen nachfolgende Aufgaben basierend auf den von Ihnen getroffenen Auswahlmöglichkeiten angezeigt. Ausgegraute Gruppen (z. B. **Wiederherstellen** , **Überprüfen** , Usw.) kann durch Ihre Auswahlmöglichkeiten aktiviert werden.
7. Arbeiten Sie an jeder Ihnen vorgelegten Aufgabe weiter, bis Sie alle Aufgaben zur Lösung der Bedrohung und zum Schließen des Security Incidents abgeschlossen haben.

Zugehörige Informationen

Fügen Sie dem Playbook eine anwenderdefinierte Aufgabe hinzu

Auflösen von von Anwendern gemeldeten Phishing-Angriffen mit dem Playbook

Das Phishing-Playbook führt Sie durch die Aufgaben, die für die Analyse und Lösung eines Phishing-Angriffs erforderlich sind, der von einem der Mitarbeiter Ihres Unternehmens gemeldet wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

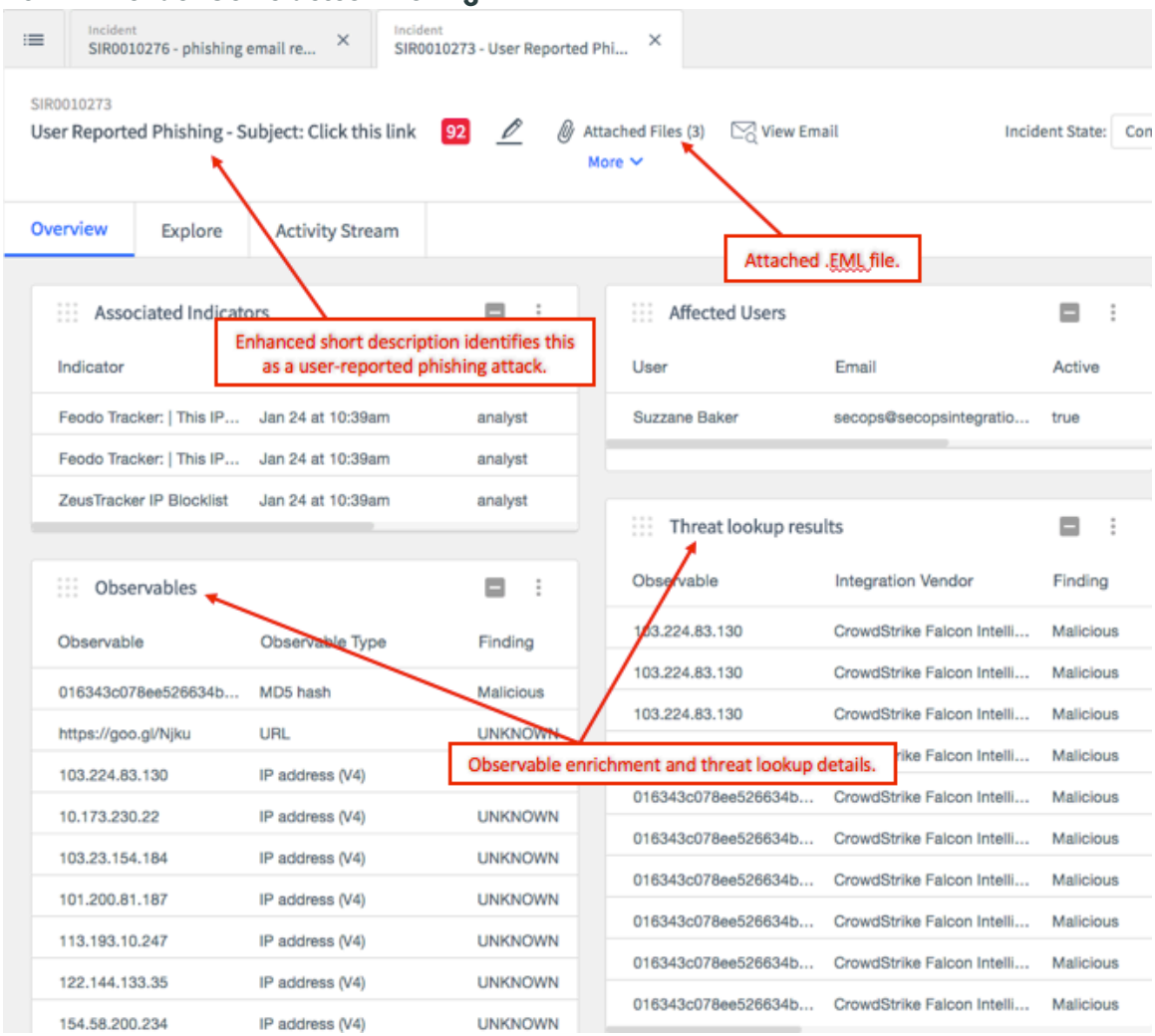
Wie Security Incidents aus von Anwendern gemeldeten Phishing-Angriffen erstellt werden

Während des Setups von Security Incident Response erstellt Ihr Systemadministrator eine Reihe von E-Mail-Übereinstimmungsregeln Die E-Mails identifizieren kann, die Anzeichen eines Phishing-Angriffs enthalten. Wenn Mitarbeiter eine verdächtige E-Mail erhalten, die die allgemeinen Anzeichen eines Phishing-Angriffs enthält (wie in Ihren Sicherheitsrichtlinien definiert), können sie sie sie als EML-Anhang an die von Ihrer Organisation definierte Phishing-E-Mail-Adresse senden.

Wenn die E-Mail an die Phishing-E-Mail-Adresse empfangen wird, wird der EML-Anhang analysiert, und seine Informationen werden mit den E-Mail-Übereinstimmungsregeln verglichen. Wenn eine Übereinstimmung gefunden wird, wird ein Security Incident mit den folgenden Informationen erstellt:

- Die Kurzbeschreibung enthält vom Anwender gemeldetes Phishing, gefolgt vom tatsächlichen Betreff aus der ursprünglichen E-Mail.
- Die EML-Datei wird an den Security Incident angehängt.
- Wenn die EML erkennbare Elemente enthielt, werden sie analysiert, und Ergänzungs- und Bedrohungssuchen werden automatisch durchgeführt.

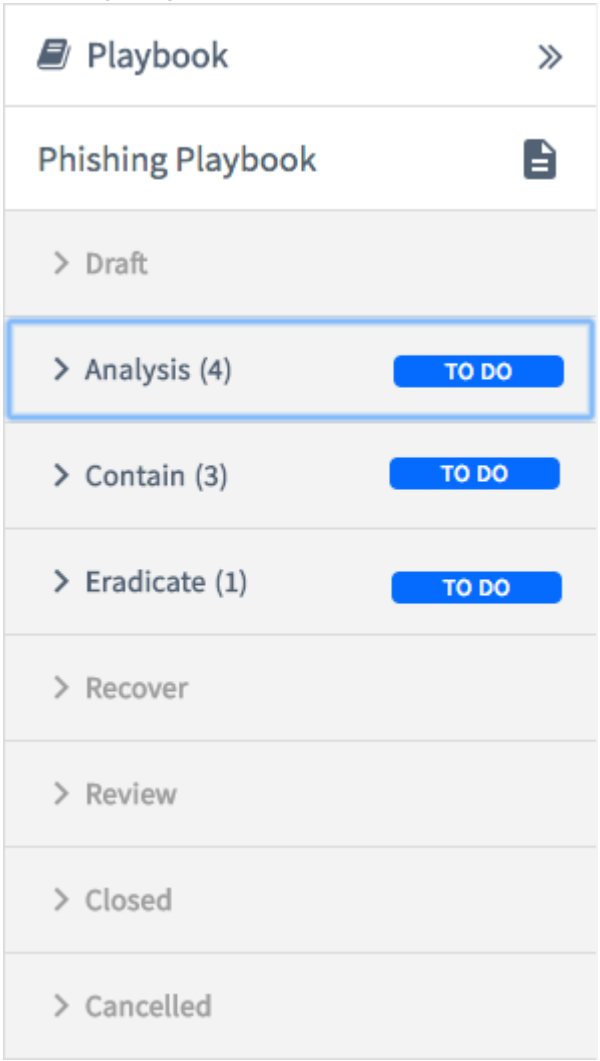
Vom Anwender Gemeldetes Phishing



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein Security Incident der Phishing-Kategorie geöffnet wird, ist das Phishing-Playbook automatisch verfügbar. Klicken Sie einfach auf das Playbook-Symbol ( ), um das Playbook zu öffnen.

Phishing-Playbook



Das Phishing-Playbook enthält Aufgaben, mit denen Sie eine Phishing-Bedrohung analysieren, eindämmen und beseitigen können. Die Aufgaben sind in status organisiert (z. B. **Analyse** , **Enthalten** , Und so weiter). Wenn alle Aufgaben für einen Status abgeschlossen wurden, führt Sie das Playbook zum nächsten Status.

Security Incident-Details werden analysiert

Wenn sich der Security Incident im Status „Analyse“ befindet, erhalten Sie Aufgaben zur Durchführung einer grundlegenden Untersuchung des Incident, einschließlich:

- Bestimmung der Gültigkeit des Incident.
- Untersuchung der Auswirkungen der potenziellen Bedrohung.
- Koordination einer effektiven Reaktion auf den Incident.

Während der Bearbeitung der Aufgaben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Machen Sie sich mit den Wissensartikeln vertraut.
- Öffnen Sie den E-Mail-Anhang, und untersuchen Sie ihn auf Anzeichen allgemeiner Phishing-Elemente.
- Überprüfen Sie die Ergebnisse der Bedrohungssuche.

Enthält den Security Incident

Wenn sich der Security Incident in befindet **Enthalten** status erhalten Sie Aufgaben, um die Details der E-Mail zu überprüfen. Um sicherzustellen, dass Bedrohungen nicht in Ihre Organisation gelangen können, aktualisieren Sie Ihre Netzwerkschutzmaßnahmen in Form von Signaturen und Regeln für Intrusion Defense System (IDS) und Intrusion Prevention System (IPS).

Während der Bearbeitung der Aufgaben:

- Ergreifen Sie Maßnahmen, um die Auswirkungen von Bedrohungen zu begrenzen, z. B. das Isolieren der betroffenen Geräte.
- Überprüfen Sie die an die E-Mail angehängten erkennbaren Elemente.
- Bestimmen Sie, ob E-Mail-Inhalte einer bekannten Bedrohung zugeordnet sind, einschließlich:
  - URL
  - E-Mail-Absender
  - Phishing-URL
  - IP-Adresse des SMTP-Servers des Absenders

Malware wird beseitigt

Nachdem Sie aktualisierte Signaturen und Regeln für Ihre Virenschutzlösung bereitgestellt haben, verwenden Sie die Aufgaben in **Beseitigen** status, um zu bestimmen, ob Malware vorhanden ist, und sie entsprechend zu behandeln.

Während Sie die Aufgaben durcharbeiten:

- Scannen Sie die Endpunkte der betroffenen Geräte auf das Vorhandensein von Malware.
- Entfernen Sie alle gefundenen Malware.
- Löschen Sie als letztes Mittel die Hostgeräte, und erstellen Sie ein neues Image.

Security Incident wird überprüft

Wenn Sie bei der Ausführung der Analyseaufgaben festgestellt haben, dass ein Phishing-Angriff ein falscher Alarm war, wird der Security Incident zu verschoben **Überprüfen** geben sie an, und Sie müssen Ihre Anwender benachrichtigen, damit sie wissen, dass es sicher ist, den E-Mail-Anhang zu öffnen.

Security Incident wird geschlossen

Wenn alle Aufgaben im Playbook abgeschlossen sind, wird der Security Incident in verschoben **Geschlossen** status. Sie müssen Abschlusskommentare eingeben, bevor der Incident geschlossen werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident wird abgebrochen

Wenn sich ein Security Incident in befindet **Überprüfen** Und Sie haben Ihre Anwender erfolgreich darüber informiert, dass die E-Mail keine Bedrohung darstellt, d. h. **Abgebrochen** der status wird aktiv, und Sie können den Security Incident abbrechen.

Hinweis:
Die Wiederherstellungsaufgabe wird im Phishing-Playbook nicht verwendet.

Ordnen Sie einen wissensartikel einer Playbook-Aufgabe zu

Während Sie Sicherheitsbedrohungen mit analysieren Security Incident Response playbook: Sie können Wissensartikel für jede Aufgabe anzeigen, wenn sie von Ihrer Organisation definiert wurde. Wenn keine Wissensartikel vorhanden sind, können Sie sie erstellen und Playbook-Aufgaben zuordnen.

Vorbereitungen

Wie Sie das Playbook in verwenden Security Incident Response, Notieren Sie sich den Text, der jeder Aufgabe zugeordnet ist. Beispielsweise ist die erste Aufgabe in der Phishing-Kategorie **Wurde Der Mitarbeiter Gewarnt?** Dies ist die Kurzbeschreibung der Aufgabe. Sie benötigen diesen Text (genau so, wie er im Playbook angezeigt wird), um der Aufgabe einen wissensartikel zuzuordnen.

Erforderliche Rolle: sn_Sir.Knowledge_admin und entweder sn_si.admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Katalog & Wissen** > **Wissen**an.
2. Erstellen und veröffentlichen Sie einen wissensartikel für eine bestimmte Playbook-Aufgabe.
3. Navigieren zu **Security Incident** > **Manuelles Runbook** > **Neues Runbook erstellen**an.
4. Erstellen Sie ein Runbook, indem Sie die folgenden Informationen eingeben:

Feld	Beschreibung
Wissensartikel	Wählen Sie den veröffentlichten wissensartikel aus, den Sie der Playbook-Aufgabe zuordnen möchten.
Tabelle	Wählen Sie Aus Security Incident Response Aufgabe [sn_si_Task].
Bedingung	Legen Sie den Bedingungsgenerator fest auf: ○ **Option:** Wählen Sie Aus **Kurzbeschreibung** . ○ **Operator:** Wählen Sie Aus **Ist** . ○ **Eingabewert:** Geben Sie die Kurzbeschreibung für die Aufgabe genau so ein, wie sie im Playbook angezeigt wird.

5. Klicken Sie auf **Absenden**.
   Wenn Sie das Playbook das nächste Mal ausführen und diese Aufgabe auswählen, wird der zugehörige wissensartikel angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erstellen Sie einen Security Incident-wissensartikel

Erstellen Sie ein Security Incident Response-Runbook

Fügen Sie dem Playbook eine anwenderdefinierte Aufgabe hinzu

Die Sicherheitsanalyst-Arbeitsbereich Das Basissystem enthält eine Reihe von Aufgaben für jede Bedrohungskategorie. Sie können anwenderdefinierte Aufgaben erstellen, die den individuellen Anforderungen Ihres Systems oder Ihrer Kunden entsprechen.

Vorbereitungen

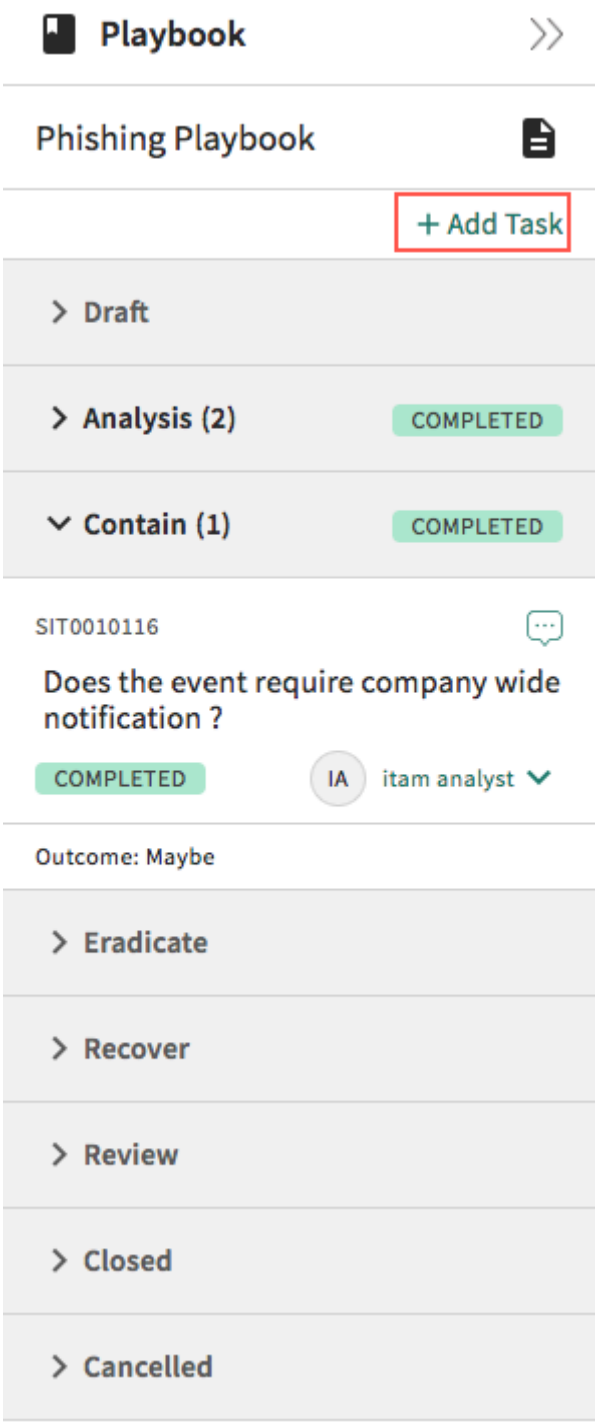
Erforderliche Rolle: sn_si.Basic oder Security_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

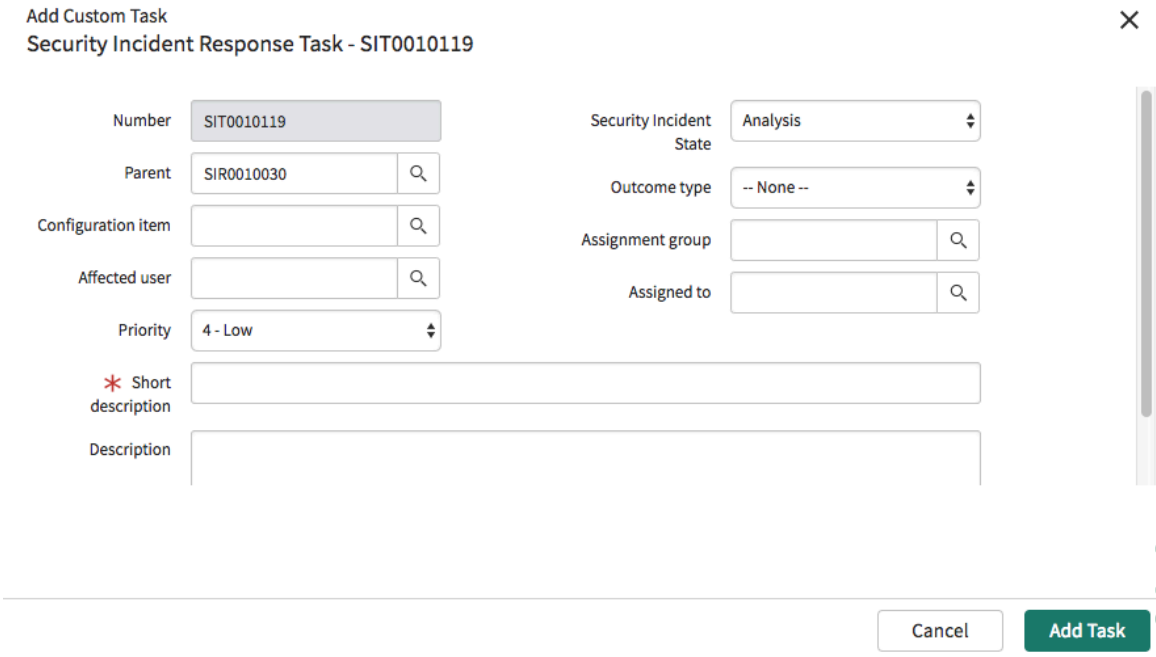
Prozedur

1. Klicken Sie bei geöffnetem Playbook auf **Aufgabe Hinzufügen** .



Der Bildschirm „Anwenderdefinierte Aufgabe hinzufügen“ wird geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Anzahl	[Schreibgeschützt] die automatisch generierte Security Incident-Aufgabennummer.
Übergeordnet	Die Nummer des zugehörigen Security Incidents.
Konfigurationselement	Das vom Sicherheitsproblem betroffene Konfigurationselement, falls vorhanden.
Betroffener Anwender	Der vom Sicherheitsproblem betroffene Anwender, falls vorhanden.
Priorität	Wählen Sie die Priorität aus, mit der bestimmt wird, wann diese Aufgabe ausgeführt werden soll.
Status des Security Incidents	Der aktuelle Status der Sicherheitsantwortaufgabe. Sie können bei Bedarf einen zukünftigen Status auswählen.
Ergebnistyp	Wenn Sie über die Rolle sn_si.Basic verfügen, wählen Sie aus **Ja/Nein** Als Ergebnistyp. Wenn Sie über die Rolle Security_admin verfügen, können Sie einen anwenderdefinierten Ergebnistyp mit mehreren anwenderdefinierten Ausgabewerten erstellen. Sie können beispielsweise eine Aufgabe mit abhängigen Werten basierend auf der Bedrohungskategorie definieren. Weitere Informationen finden Sie unter Auswahllisten
Zuweisungsgruppe	Die Zuweisungsgruppe, aus der der zugewiesene Mitarbeiter ausgewählt wird.
Zugewiesen an	Die Person, die der Ausführung der Aufgabe zugewiesen ist.
Kurzbeschreibung	Eine Beschreibung der Security Incident-Playbook-Aufgabe.
Beschreibung	Geben Sie eine Beschreibung für die ausgewählte Aufgabe ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wenn Sie Ihre Einträge abgeschlossen haben, klicken Sie auf **Aufgabe Hinzufügen** .
   Die Aufgabe wird nach der aktuellen Aufgabe in das Playbook eingefügt.

Sichtungen sucht nach von Anwendern gemeldeten Phishing- und Malware-Angriffen

Führen Sie Sichtungssuchen für E-Mails oder erkennbare Elemente durch, um festzustellen, wie oft bestimmte Arten von Angriffen, z. B. Phishing-Angriffe oder Kommunikation mit einer schädlichen IP oder URL, in Ihrem Netzwerk auftreten. Jedes Vorkommen wird als Sichtung betrachtet. Sichtungssuchen nach erkennbaren Elementen müssen für Ihre Protokollspeicher oder Security Information and Event Management (SIEM) konfiguriert werden.

So verwenden Sie die Sichtungssuchfunktion, um Phishing-Anwender zu finden und erkennbare Phishing- und Malware-Elemente im Protokollspeicher in Ihrem Netzwerk nachzuverfolgen.

Sehen Sie sich dieses dreiminütige Video an, um zu erfahren, wie Sie die Sichtungssuchfunktion verwenden, um Phishing- und Malware-Elemente innerhalb des Protokollspeichers in Ihrem Netzwerk zu finden.

Die folgenden Begriffe werden verwendet, um von Anwendern gemeldete Phishing-Angriffe zu beschreiben:

- Phishing-Anwender: Ein Anwender, der eine Phishing-E-Mail erhalten hat.
- Opferanwender: Ein Anwender, der mit der Phishing-URL interagiert hat, normalerweise durch Klicken auf einen Link in der Phishing-E-Mail. Diese Aktion stellt dem Angreifer potenziell Anmeldeinformationen zur Verfügung.

Wenn Sie mit der Analyse eines Phishing-Incidents beginnen, können Sie dies Führen Sie eine E-Mail-Sichtungssuche durch Oder Führen Sie eine Sichtungssuche für erkennbare Elemente durch Um andere Anwender in Ihrer Organisation zu identifizieren, die von demselben Phishing-Angriff betroffen sind. Durchsuchen Sie Ihre Protokollspeicher, um Phishing- und Opferanwender zu identifizieren. Nachdem Sie die Liste der betroffenen Anwender identifiziert haben, erstellen Sie untergeordnete Security Incidents, um mithilfe der in verfügbaren Tools umfassende Verfahren zur Reaktion auf Incidents durchzuführen Security Incident Response.

Hinweis:
Sie können auch den folgenden Ansatz verwenden, um eine Sichtungssuche durchzuführen:

- Navigieren zu **Security Incidents** > **Alle Incidents anzeigen** Und klicken Sie auf einen Security Incident.
- Klicken Sie Auf **IOC anzeigen** Unter zugehörige Links. Eine Liste der erkennbaren Elemente wird angezeigt.
- Wählen Sie ein erkennbares Element aus der Liste und aus der aus **Aktionen** Wählen Sie eine der folgenden Optionen aus:
  - Sichtungssuche für Webdatenverkehr ausführen
  - Sichtungssuche für E-Mail-Datenverkehr ausführen
- Geben Sie den Zeitrahmen an, und klicken Sie auf **Suchen** Um eine Sichtungssuche durchzuführen.

Gespeicherte Sichtungssuchkonfigurationen

Konfigurieren Sie Sichtungssuchen, und erstellen Sie gespeicherte Konfigurationen für SIEMs oder andere Protokollspeicher für Instanzen erkennbarer Elemente, um das Vorhandensein schädlicher erkennbarer Elemente in Ihrer Umgebung zu bestimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Gespeicherte Suchen und Inplace-Abfragen werden nur für Splunk-Integration unterstützt.

Zugehörige Informationen

Erstellen Sie Konfigurationsdatensätze für Sichtungssuche

Führen Sie eine E-Mail-Sichtungssuche nach von Anwendern gemeldeten Phishing-Angriffen durch

Suchen Sie basierend auf erkennbaren Elementen wie E-Mail-Betreff, Absendername oder Nachrichten-ID nach Anwendern, die Phishing-E-Mails erhalten haben. Sie können diese Phishing-E-Mails dann in Ihrer Organisation eindämmen und löschen.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Durchsuchen Sie die Splunk-E-Mail-Datenverkehrsprotokolle, um die Liste der Empfänger einer verdächtigen E-Mail zu erfassen. Die Suche kann anhand des E-Mail-Absenders, der E-Mail-Nachrichten-ID oder des E-Mail-Betreffs durchgeführt werden, der einem Security Incident zugeordnet ist.

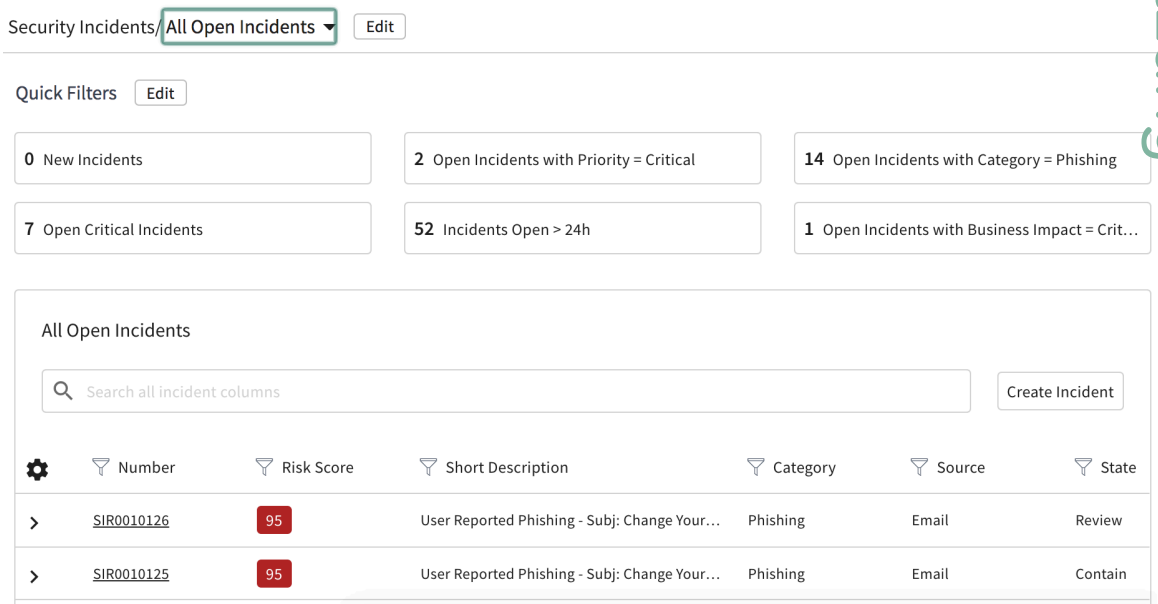
Hinweis:

- Diese Implementierung der Sichtungssuche nach E-Mail-basierten erkennbaren Elementen wurde nur mit dem Splunk Enterprise-Protokollspeicher getestet.
- Die Splunk-Protokollereignisse müssen mit dem Common Information Model (CIM) konform sein, damit die Sichtungssuchabfrage genaue Ergebnisse zurückgibt.

Prozedur

1. Navigieren Sie zu , um die Ihrem Team zugewiesenen Security Incidents anzuzeigen **Security Incident** > **Incidents (neue UI)**an.
2. Von **Security Incidents** Wählen Sie einen der Filter aus, z. B. alle **Offene Incidents** , **Alle Ihnen zugewiesenen Incidents** , Oder **Alle Incidents** .

   Um Security Incidents eines bestimmten Typs anzuzeigen, z. B. kritische Incidents oder Phishing-E-Mails, klicken Sie auf einen der **Schnellfilter** .

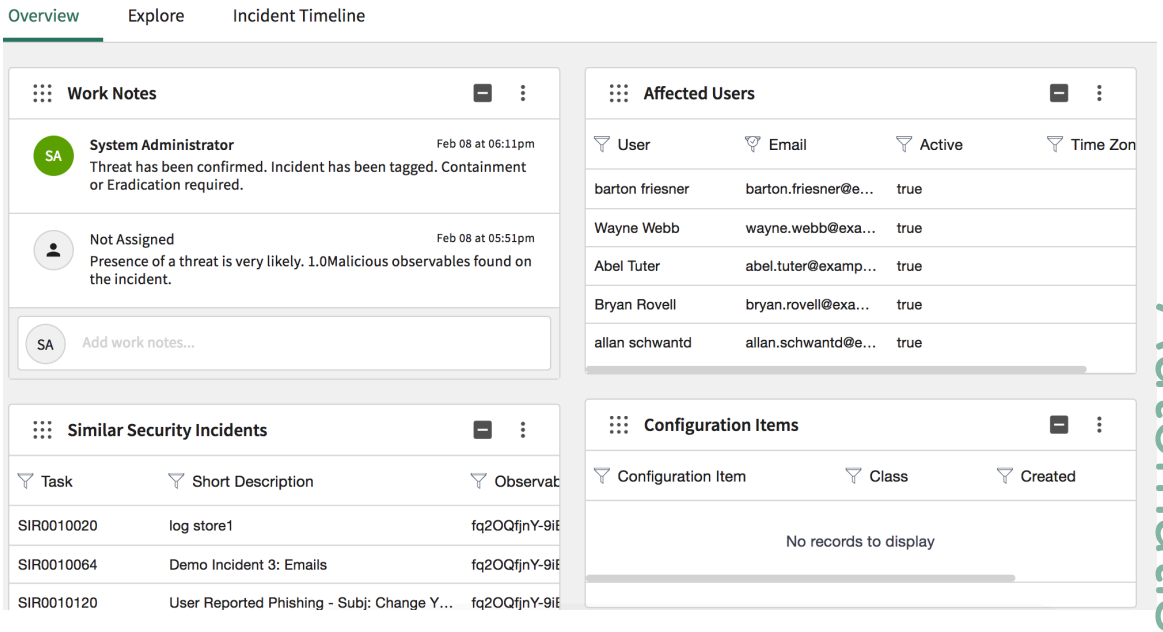


Automatische Übersetzung

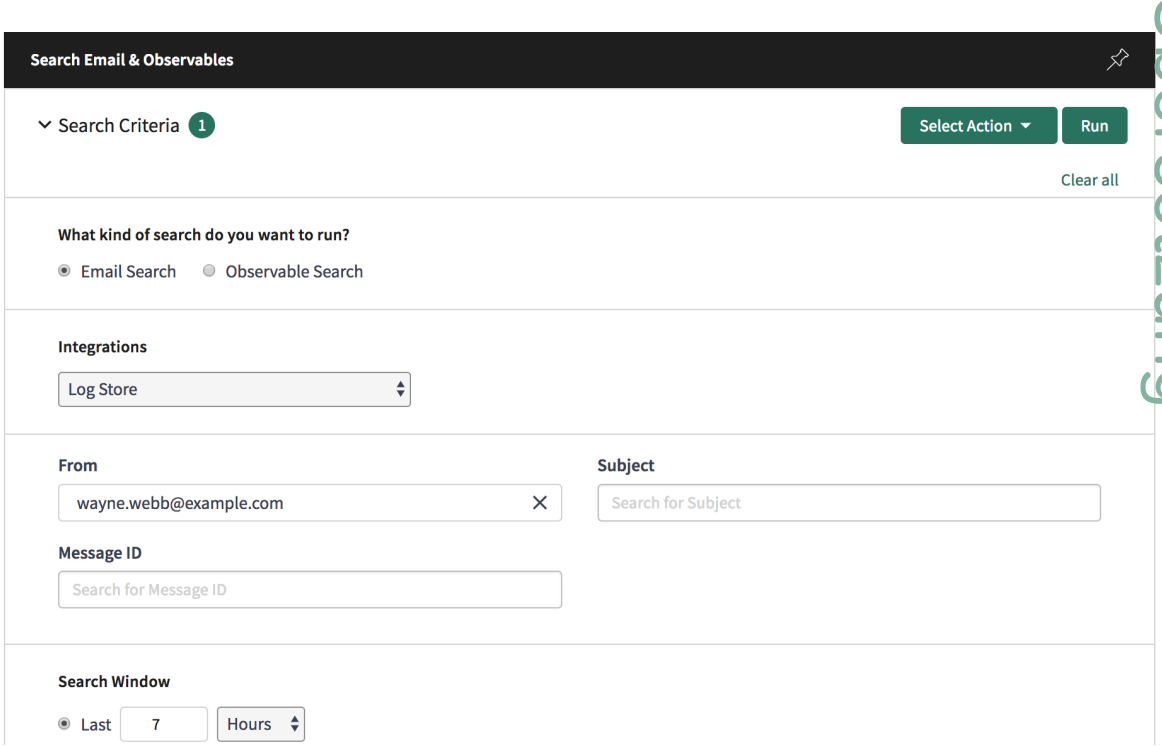
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf den Security Incident, den Sie analysieren möchten.

   Die Registerkarte Übersicht bietet eine Übersicht über den Security Incident, einschließlich einer Liste erkennbarer Elemente, betroffener Anwender und ähnlicher Security Incidents.



4. Klicken Sie auf **Erkunden** Registerkarte.
5. Unter **Incident-Daten** , Navigieren Sie zu **Ermittlung** > **Suchen Sie E-Mail Und Erkennbare Elemente**an.



6. Erweitern Sie den Abschnitt Suchkriterien.
7. Wählen Sie Aus **E-Mail-Suche** Als Typ der Suche, die Sie ausführen möchten, und geben Sie die restlichen Suchkriterien an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Suchkriterien“

Feld	Beschreibung
Integrationen	Integrationstyp. Wählen Sie Aus **Protokollspeicher** Aus der Liste. **Hinweis:** Diese Funktion wird nur mit dem Splunk-Protokollspeicher unterstützt.
Von	Vollständige E-Mail-Adresse des Absenders (z. B. jane.doe@example.com).
Nachrichten-ID	E-Mail-Nachrichten-ID aus dem Protokollspeicher.
Betreff	Betreff der Phishing-E-Mail.
Suchfenster	Zeitfenster für die Suche (z. B. die letzten 24 Stunden).

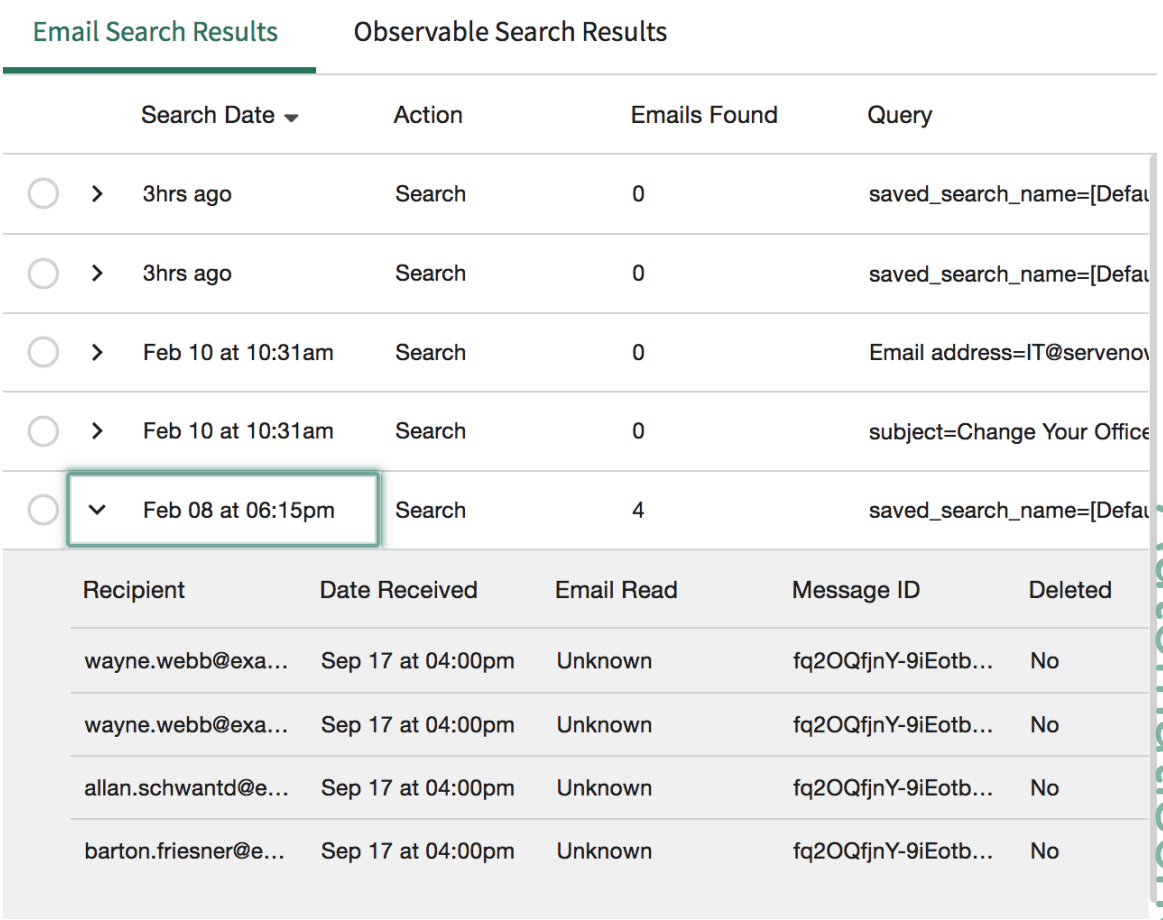
8. Von **Wählen Sie Aktion Aus** Liste, wählen Sie aus **Suchen** Und klicken Sie dann auf **Ausführen** .

   Der Splunk-Protokollspeicher wird anhand der von Ihnen eingegebenen Kriterien durchsucht, und die Anwender, die vom Phishing-Angriff betroffen sind, werden im angezeigt **E-Mail-Suchergebnisse** Registerkarte. Die Gesamtzahl der Phishing-E-Mails und die Details jeder E-Mail, einschließlich Empfangsdatum, Empfänger und Nachrichten-ID, werden angezeigt.

9. Um die Liste der Anwender anzuzeigen, die die Phishing-E-Mail erhalten haben, klicken Sie auf **>** Symbol in der Spalte „Suchdatum“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Um eine Liste der Anwender anzuzeigen, die die E-Mail erhalten haben, navigieren Sie zu **Anwender** > **Betroffene Anwender**an.

    Die Spalte Phishing User (Phishing User) identifiziert die E-Mail-Empfänger.

    Hinweis:
    Auf der Seite „Betroffene Anwender“ werden nur die Anwenderdatensätze angezeigt, die in der ServiceNow-Instanz vorhanden sind.

11. Um die Anwender, die Ziele des Phishing-Angriffs sind, weiter zu untersuchen, gehen Sie wie folgt vor:

    a. Aktivieren Sie die Kontrollkästchen neben den Anwendernamen.

    b. Wählen Sie in der Liste aus **Untergeordneten Security Incident Erstellen** , Und klicken Sie auf **Ausführen** .

    Eine Meldung zeigt an, dass ein untergeordneter Security Incident erstellt wurde. Klicken Sie auf , um die untergeordneten Security Incidents anzuzeigen, die einem übergeordneten Incident zugeordnet sind **Erkunden** Registerkarte und navigieren Sie zu **Incidents** > **Untergeordnete Security Incidents**an.

Ergebnisse

Die Liste der Phishing-Anwender wird angezeigt.

Führen Sie eine Sichtungssuche für erkennbare Elemente nach von Anwendern gemeldeten Phishing- und Malware-Angriffen durch

Führen Sie Sichtungssuchen nach erkennbaren Elementen durch, um herauszufinden, wie viele Anwender innerhalb eines bestimmten Zeitraums eine schädliche oder verdächtige Website besucht haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Netzwerkdatenverkehrssuche für erkennbare Elemente wie die URL, den Zielhost oder die Ziel-IP-Adresse durchführen, die einem Security Incident zugeordnet sind.

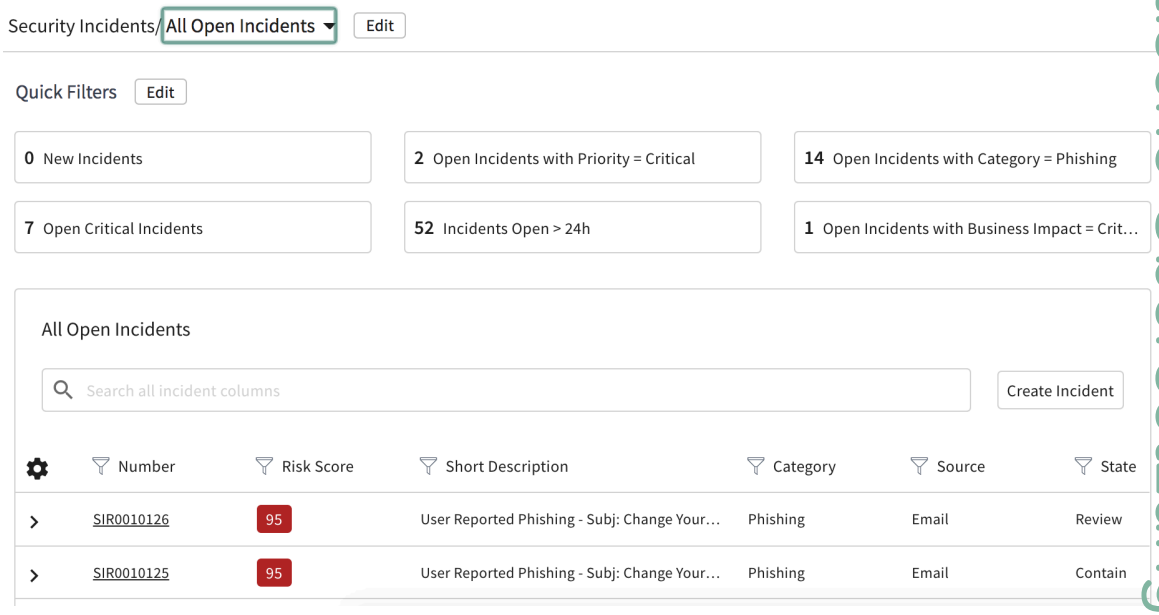
Hinweis:

- Diese Implementierung der Sichtungssuche nach erkennbaren Elementen wurde nur mit dem Splunk Enterprise-Protokollspeicher getestet.
- Die Splunk-Protokollereignisse müssen mit dem Common Information Model (CIM) konform sein, damit die Sichtungssuchabfrage genaue Ergebnisse zurückgibt.

Prozedur

1. Navigieren Sie zu , um die Security Incidents anzuzeigen, die Ihrem Team zugewiesen sind **Security Incident** > **Incidents (neue UI)**an.
2. Von **Security Incidents** Wählen Sie einen anderen Filter aus, z. B. alle **Mir zugewiesene Incidents** , **Alle Offenen Incidents** , Oder **Alle Incidents** .

   Um Security Incidents eines bestimmten Typs anzuzeigen, z. B. kritische Incidents oder Phishing-E-Mails, klicken Sie auf einen der **Schnellfilter** .

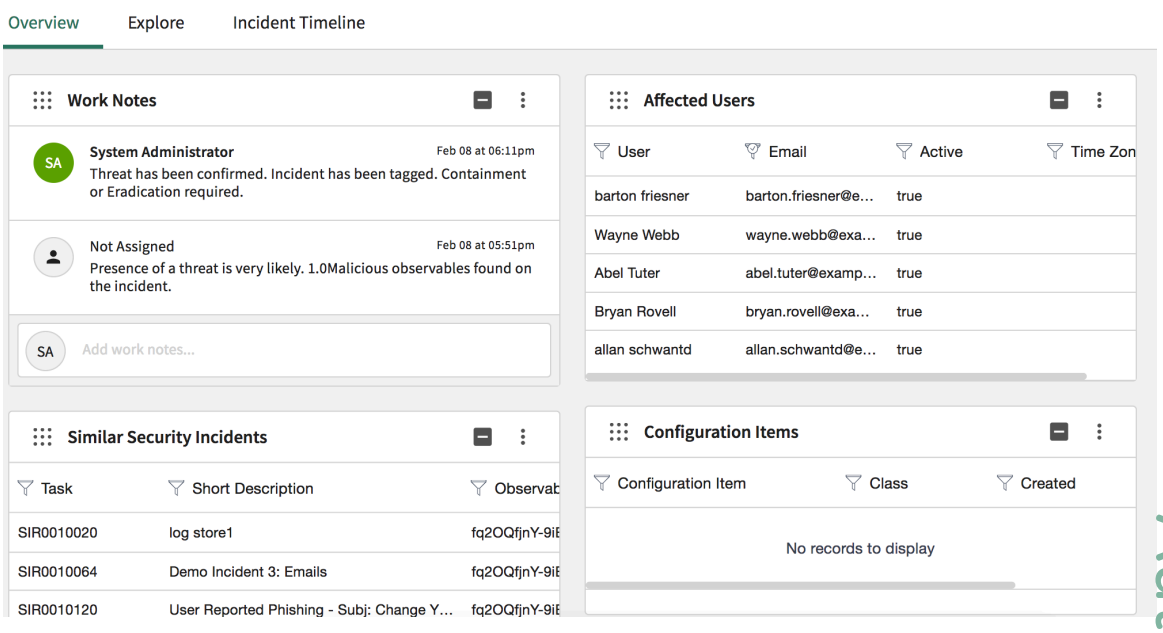


3. Klicken Sie auf den Security Incident, den Sie analysieren möchten.

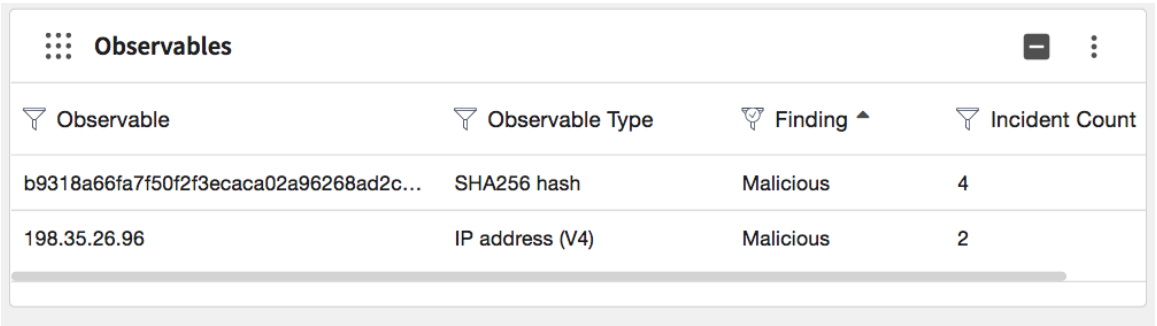
   Sie können eine Übersicht über den Security Incident anzeigen, einschließlich einer Liste erkennbarer Elemente, betroffener Anwender und ähnlicher Security Incidents.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

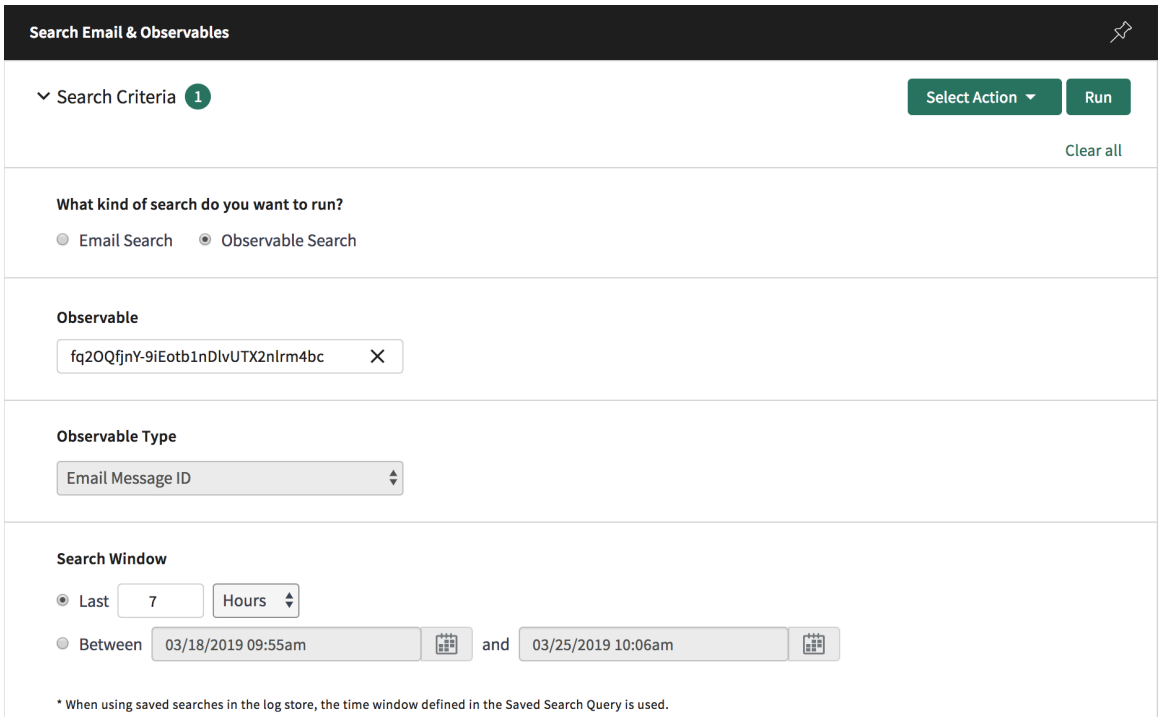


Beachten Sie im Abschnitt „erkennbare Elemente“, dass die Spalte „erkennbares Element“ die E-Mail-Adresse, den Betreff und die URL anzeigt. Beachten Sie auch, dass die Spalte „Ergebnis“ zeigt, dass die URL automatisch gescannt wurde, als die Phishing-E-Mail übermittelt wurde, und dass sie als schädliche URL bekannt ist. Die Spalte Incident-Anzahl zeigt die anderen Incidents an, die dasselbe erkennbare Element teilen. Diese Artefakte zeigen an, dass Sie wahrscheinlich bereit sind, mit Eindämmungsverfahren für diesen Phishing-Angriff fortzufahren, einschließlich der Bestimmung, wie viele Anwender in der Organisation betroffen waren.

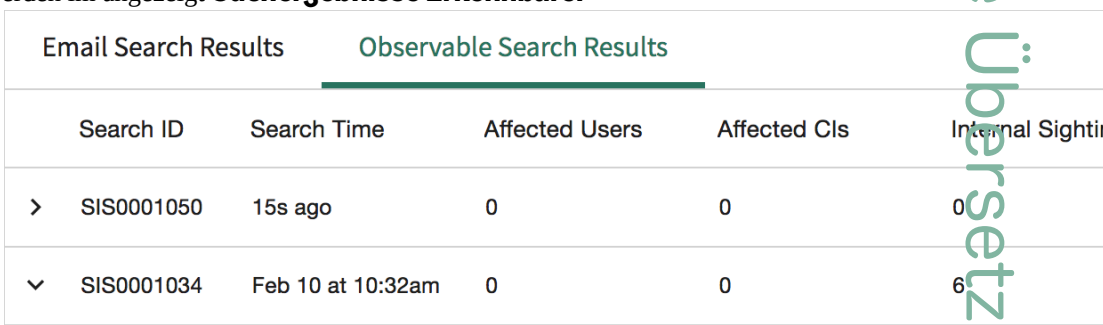


4. Navigieren zu **Untersuchen** > **Ermittlung** > **Suchen Sie E-Mail Und Erkennbare Elemente**an.
5. Erweitern Sie den Abschnitt Suchkriterien, und klicken Sie auf **Suche Erkennbarer Elemente** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Geben Sie das erkennbare Element, nach dem Sie suchen, und ein Zeitfenster für die Suche ein (z. B. letzte 24 Stunden).
7. Von **Wählen Sie Aktion Aus** Liste, wählen Sie aus **Suchen** .
   Der Splunk-Protokollspeicher wird anhand der von Ihnen eingegebenen Kriterien durchsucht, und die wichtigsten Anwender, die von dem böswilligen Angriff betroffen sind, werden im angezeigt **Suchergebnisse Erkennbarer Elemente**Registerkarte.



8. Um die Anwender anzuzeigen, die die E-Mail erhalten haben, navigieren Sie zu **Anwender** > **Betroffene Anwender**an.

   Die Spalte Phishing-Anwender identifiziert die Empfänger der Phishing-E-Mail, und die Spalte Anwenderinteraktion identifiziert Anwender, die auf eine Phishing-URL geklickt oder mit einer verdächtigen E-Mail-Adresse interagiert haben. Die Spalte Anwenderinteraktion wird auf „wahr“ oder „falsch“ festgelegt, je nachdem, ob der Anwender auf den schädlichen Link oder die schädliche IP geklickt hat.

   Hinweis:
   Auf der Seite „Betroffene Anwender“ werden nur die Anwenderdatensätze angezeigt, die in der ServiceNow-Instanz vorhanden sind.

9. So untersuchen Sie die Anwender, die auf die Phishing-E-Mail geklickt und ihre Anmeldeinformationen potenziell gefährdet haben:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Aktivieren Sie sowohl in den Spalten Phishing User (Phishing-Anwender) als auch Anwenderinteraktion die Kontrollkästchen neben den angezeigten Anwendernamen **Wahr** .

b. Klicken Sie Auf **Untergeordneten Security Incident Erstellen** Und klicken Sie dann auf **Ausführen** .
Eine Meldung zeigt an, dass ein untergeordneter Security Incident erstellt wurde. Klicken Sie auf , um die untergeordneten Security Incidents anzuzeigen, die einem übergeordneten Incident zugeordnet sind **Erkunden** Registerkarte und navigieren Sie zu **Incidents** > **Untergeordnete Security Incidents**an.

Ergebnisse
Die Liste der Phishing-Anwender wird angezeigt.

Erstellen Sie Konfigurationsdatensätze für Sichtungssuche

Erstellen Sie mehrere Sichtungssuchkonfigurationsdatensätze, und verwenden Sie sie, wenn Sie mehrere Protokollspeicher abfragen oder die Suchparameter ändern.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

- Das CIM-Add-on muss auf der Splunk-Instanz installiert sein.
- Gespeicherte Suchen und Inplace-Abfragen werden nur für Splunk-Integration unterstützt.

Warum und wann dieser Vorgang ausgeführt wird
Sie können auch Konfigurationsdatensätze für Sichtungssuche erstellen, um sie aufzurufen Gespeicherte Suchen Im Splunk Enterprise-Protokollspeicher.

Hinweis:
Die Suchkonfigurationsabfragen basieren auf Splunk-Protokolldaten, um Splunk Common Information Model (CIM)-konform zu sein.

Mit gespeicherten Suchkonfigurationen können Sie:

- Erstellen Sie anwenderdefinierte Suchen, die mehrere Ereignisdatensätze kombinieren.
- Designeffiziente und effektive Suchen.
- Verwenden Sie parametrisierte Eingaben in der gespeicherten Splunk-Suche.

Das Basissystem enthält die Beispielkonfigurationen, wie in dieser Abbildung gezeigt:

Gespeicherte Suchkonfigurationen

Name	Observable type	Search	Is saved search
Search	Search	Search	Search
Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

Die gespeicherten Such- und Inplace-Konfigurationsabfragen sind Beispielabfragen und können durch entsprechende Parameter für Ihre Umgebung ersetzt werden. Erstellen Sie nach Bedarf zusätzliche gespeicherte Suchkonfigurationen. Wenn Sie eine gespeicherte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchkonfiguration definieren, müssen der Name und die Parameter in der Suchabfrage mit der gespeicherten Konfiguration übereinstimmen, die in Ihrer Splunk-Instanz definiert ist. Wenn der Name und die Parameter nicht identisch sind, werden bei einer Sichtungssuche möglicherweise keine genauen Ergebnisse angezeigt.

Hinweis:
Navigieren Sie in Ihrer Splunk-Instanz zur Seite Suchen, Berichte und Warnungen, und suchen Sie Ihre gespeicherte Suchabfrage. Klicken Sie auf **Berechtigungen** Link, um zur Seite „Berechtigungen“ zu navigieren. Wählen Sie aus **Alle Apps** Optionsschaltfläche und aktivieren Sie **Leseberechtigung** Option für **Alle** . Dadurch wird der Wert der Spalte „Freigeben“ für Ihre gespeicherte Suchabfrage von „Privat“ in „App“ geändert. Wenn dies nicht festgelegt ist, gibt die gespeicherte Suchabfrage möglicherweise keine Ergebnisse zurück.

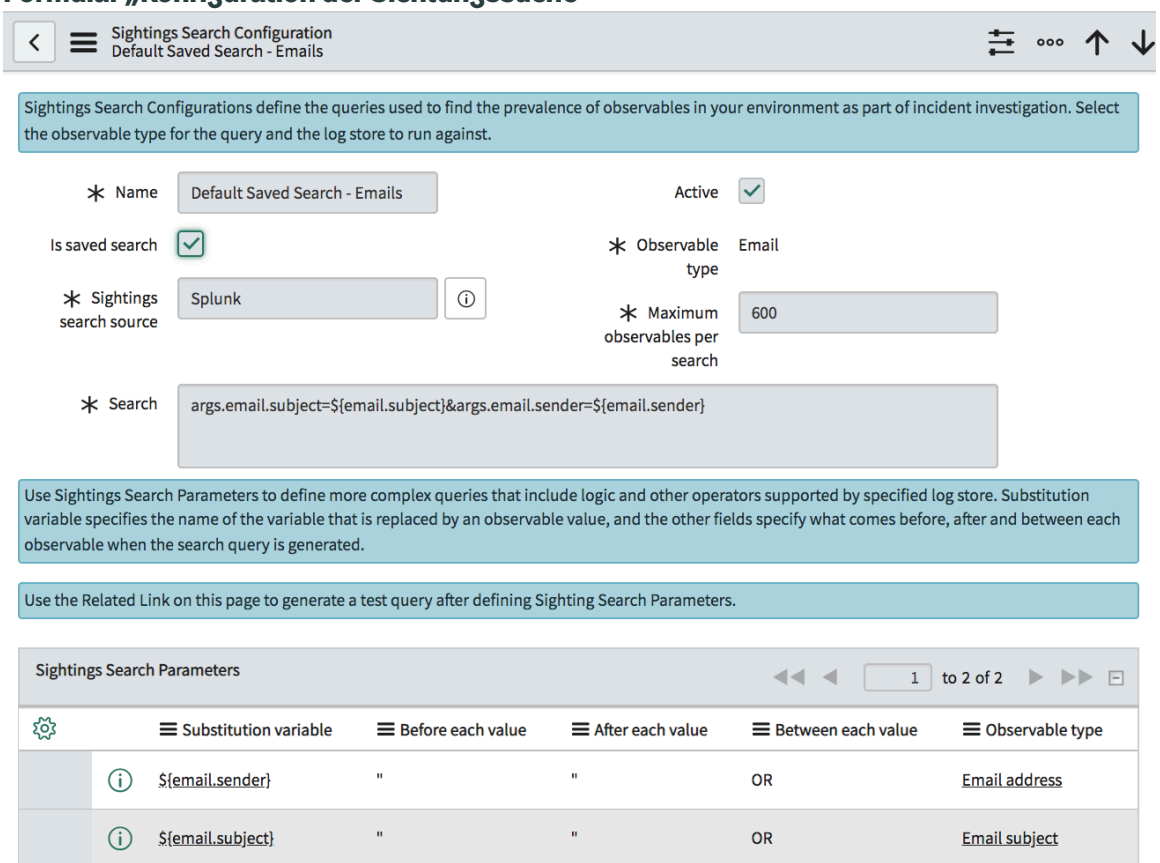
So überprüfen Sie, ob die gespeicherte Suchkonfiguration mit der in Ihrer Splunk-Instanz definierten Konfiguration übereinstimmt:

1. Navigieren zu **Einstellungen** > **Suchen, Berichte und Warnungen**an.
2. Ändern **App-Kontext** Bis **Alle** .

   Eine Liste der Suchberichte wird angezeigt.
3. Bestätigen Sie, dass die gespeicherte Suchabfrage in der Liste vorhanden ist.

Beispielsweise enthält das Formular „Sichtungssuchkonfiguration“ die E-Mail-Adresse und den E-Mail-Absender als Suchparameter:

Formular „Konfiguration der Sichtungssuche“



Definieren Sie in Ihrer Splunk-Instanz die gespeicherte Suche mit dem gleichen Namen, der standardmäßig gespeicherten Suche – E-Mails und den gleichen Suchparametern für die E-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mail-Adresse und den E-Mail-Betreff. Wenn Name und Suchparameter nicht identisch sind, wird bei der Sichtungssuche kein genaues Ergebnis generiert.

Prozedur

1. Navigieren zu **Security Operations** > **Integrationen** > **Sichtungssuche – Konfiguration** Und erstellen Sie einen neuen Datensatz (Feldbeschreibungen finden Sie in der Tabelle).

Formular „Konfiguration der Sichtungssuche“

Feld	Beschreibung
Name	Name der Konfiguration
Ist gespeicherte Suche	Wenn Sie diese Option auswählen, wird eine gespeicherte Suchkonfiguration erstellt.
Sichtungssuchquelle	Die Quelle für die Sichtungssuche. Wählen Sie den Splunk-Protokollspeicher als Quelle aus.
Aktiv	Option für den gespeicherten Suchstatus. Nur aktive Suchkonfigurationen können verwendet werden, um eine Sichtungssuche durchzuführen.
Typ des erkennbaren Elements	Der Typ des erkennbaren Elements kann ein beliebiger Typ des erkennbaren Elements sein, z. B. IP, Hash-Wert, URL, Domänenname usw.
Maximale erkennbare Elemente pro Suche	Maximale Anzahl erkennbarer Elemente, die von der Suche zurückgegeben werden sollen.
Suchen	Die Standardsuchzeichenfolge ist `$(erkennbares Element)` , Sie können jedoch Ihre eigene Suchabfrage definieren, indem Sie Parameter angeben, die vom Splunk-Protokollspeicher unterstützt werden.

2. Klicken Sie auf **Absenden**.

Ergebnisse
Sie haben einen Konfigurationsdatensatz für die Sichtungssuche erstellt.

Nächste Maßnahme
Klicken Sie nach dem Definieren der Suchabfrage auf **Testabfrage Für Sichtungssuche Generieren** , Und geben Sie eine Liste erkennbarer Werte an, um eine Testabfrage basierend auf dieser gespeicherten Suchkonfiguration zu generieren.

Playbook-Ressourcen

Security Incident Response bietet eine umfangreiche Reihe von Playbook-Ressourcen, einschließlich einer umfassenden Bibliothek von Playbooks, Subflows und Aktionen. Sie können Playbooks schnell und einfach erstellen oder konfigurieren, ohne komplizierten Code zu schreiben. Sie können diese Playbooks verwenden, um Sicherheitsbedrohungen Schritt für Schritt zu lösen.

Playbook-Ressourcen umfassen Folgendes:

Security Incident Response Playbooks	Playbook-Aktionen für Security Incident Response
Die mit dem Basissystem bereitgestellten Playbooks sollen den Untersuchungsprozess für Security Incidents beschleunigen,	Komplexe Aktionen, die für die Erstellung von Playbooks kritisch sind, sind als verfügbar **Aktionsbibliotheken** . Mit diesen Aktionsbibliotheken können

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response Playbooks	Playbook-Aktionen für Security Incident Response
indem komplexe und alltägliche Aufgaben automatisiert werden. Playbooks sind in hohem Maße konfigurierbar und werden mit der Flow Designer-Technologie von ServiceNow erstellt. Kopieren Sie zum Konfigurieren das mit dem Basissystem bereitgestellte Playbook, und ändern Sie es mithilfe der einfachen grafischen Drag-and-Drop-Oberfläche. Weitere Informationen finden Sie unter Security Incident Response Playbooks.	Sicherheitsadministratoren Playbooks erstellen, ohne komplizierten Code zu schreiben. Weitere Informationen finden Sie unter Playbook-Aktionen für Security Incident Response.

Aktivieren Sie einen Security Incident Response Flow

Sicherheitsadministratoren und Flow-Designer können verwenden Security Incident Response Flows zur Automatisierung des Prozesses zur Lösung von Security Incidents in der Organisation.

Vorbereitungen

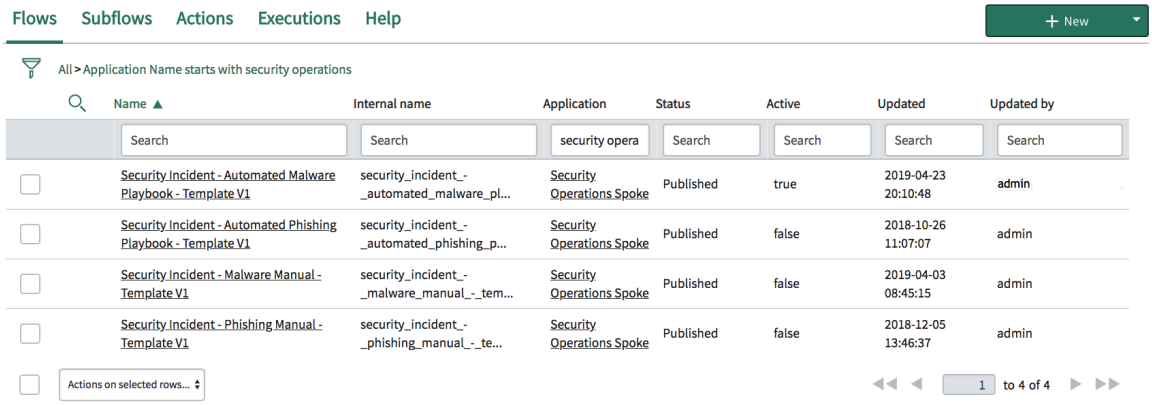
Erforderliche Rolle: sn_si.admin, action_Designer und Flow_Designer

Warum und wann dieser Vorgang ausgeführt wird

Die mit dem Basissystem bereitgestellten Flows befinden sich in einem inaktiven Status. Aktivieren Sie diese Flows, bevor Sie sie verwenden.

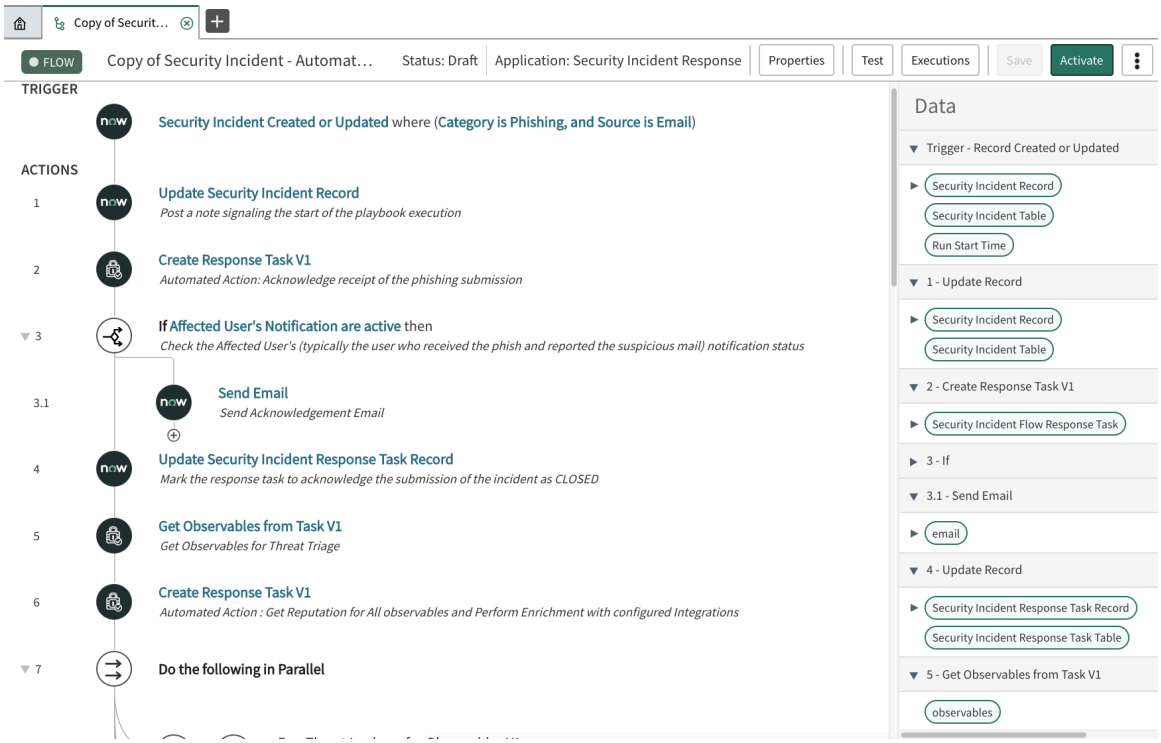
Prozedur

1. Herunterladen und installieren Die Security Operations Spoke-Anwendung.
   Diese Spoke-Anwendung bietet Sicherheitsvorgangsaktionen, die Sie beim Definieren verwenden können Security Incident Response Flows.
2. Navigieren zu **Flow Designer** > **Designer** Und suchen Sie nach Security Operations Spoke-Anwendung zum Anzeigen der Security Incident-bezogenen Flows.



   Beachten Sie, dass die Flows den Status „veröffentlicht“ haben und inaktiv sind.
3. Wenn Sie beispielsweise den Flow Automated Malware Playbook aktivieren möchten, klicken Sie auf **Security Incident – Playbook für automatisiertes Phishing – Vorlage V1** Link zum Anzeigen des Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Sie können die mit dem Basissystem bereitgestellten Flows nicht bearbeiten, da es sich um schreibgeschützte Flows handelt. Sie können diese Flows unverändert verwenden oder eine Kopie erstellen und sie nach Bedarf ändern.

4. Klicken Sie Auf **Aktivieren** Zum Aktivieren des Flows.

Ergebnisse

Der Flow „Playbook für automatisiertes Phishing“ ist aktiv und einsatzbereit.

Security Incident Response Playbooks

Sie können den Security Incident-Playbook-Flow automatisch oder manuell aufrufen.

Ein Playbook ist nur sichtbar, wenn mindestens ein Playbook einem Security Incident zugeordnet ist. Die Playbook-Komponente funktioniert nur für die vom Prozessautomatisierungs-Designer (PAD) erstellten Prozesse und nicht für die vom Flow Designer erstellten Flows. Für die vorhandenen Flow Designer-fähigen Flows funktioniert es weiterhin, und die Aktivitäten werden weiterhin als Antwortaufgaben gerendert.

Security Incident Response Unterstützt zwei Arten von Playbooks:

- Prozessbasierte Playbooks
- Flow-basierte Playbooks

Neben den aufgeführten Playbooks gibt es auch Subflows in der Security Operations-Spoke, die über das Flows-Playbook aufgerufen werden können. Ransomware ist einer dieser Subflows.

Aktivieren Sie diese Flows, bevor Sie sie verwenden. Weitere Informationen finden Sie unter Aktivieren Sie einen Security Incident Response-Flow .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozessbasierte Playbooks

Die Playbook-Komponente funktioniert nur für integrierte Playbooks Workflow-Studio Und nicht für Flows. Vorhandene Flow-basierte Playbooks funktionieren jedoch weiterhin, und die Aktivitäten werden weiterhin als Antwortaufgaben gerendert.

Security Incident Response Stellt die folgenden Playbooks mit dem Basissystem bereit.

Playbook für manuelles Phishing

Das Manual Phishing Playbook bietet Ihren Analysten Schritt-für-Schritt-Anleitungen, wie sie bestimmte Arten von Sicherheitsbedrohungen in Ihren Phishing-Aktivitäten manuell lösen können.

Übersicht

Die Vorlage „Manuelles Phishing-Playbook“ dient dazu, die Phishing-Antwortaufgaben manuell auszuführen, und enthält eine Reihe von Aktionen, die Auslöserbedingungen enthalten. Sie können die PAD-Vorlagen verwenden, um die Schritte im Phishing-Antwort-Playbook auszuführen und diese Incidents effizient zu lösen.

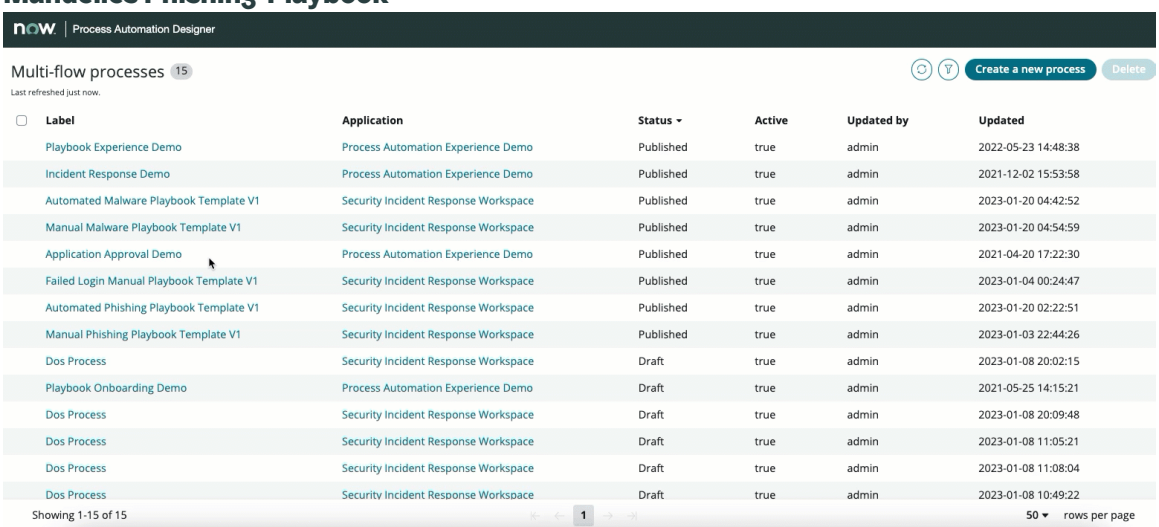
Dieses Playbook kann verwendet werden, wenn ein Security Incident erstellt oder aktualisiert wird. Sie müssen das Playbook für manuelles Phishing im Prozessautomatisierungs-Designer (PAD) aktivieren und dann alle Aufgaben ausführen, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

Die folgenden Phasen der Prozessdefinition entsprechen dem Status des Security Incidents:

- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Phase enthält Aktivitäten.

Manuelles Phishing-Playbook



Sobald Sie eine Aufgabe in einer Phase als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Phase

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

abgeschlossen haben, können Sie zur nächsten Phase wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie Aufgaben und Phasen abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für jede Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die von Ihnen eingegebenen Details in allen Phasen zu überprüfen. Sie können ein beliebiges Feld bearbeiten oder auf Fertigstellen klicken, um den Prozess zum Erstellen der Berechtigung abzuschließen.

Erstellen Sie Playbooks für manuelles Phishing in Workflow-Studio

Verwenden Sie diese Schritte, um Playbooks für manuelles Phishing in zu erstellen Workflow-Studio.

Vorbereitungen

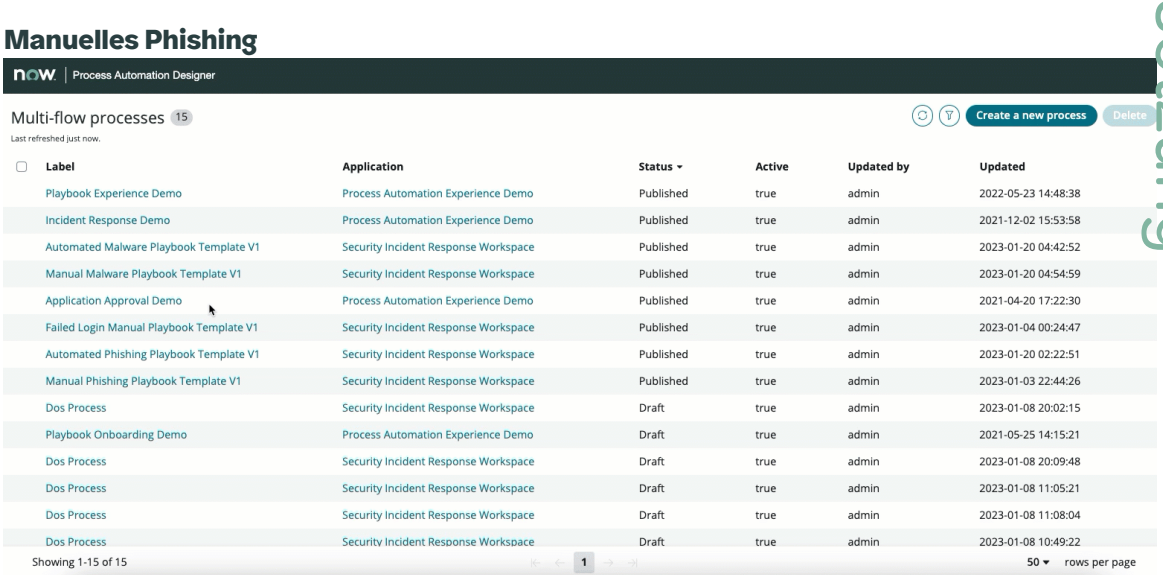
Erforderliche Rolle: sn_si.admin oder sn_si.Manager

Prozedur

1. Klicken **Alle** > **Prozessautomatisierungs-Designer** > > **Neu** Und wählen Sie aus **Playbook** .

   Beispiel: Manuelle Phishing-Playbook-Vorlage V1.

2. Geben Sie einen Namen für das Playbook, die Beschreibung und die Anwendung ein, für die das Playbook erstellt wird.
3. Klicken Sie Auf **Wählen Sie einen Auslöser aus** .
4. Wählen Sie Aus **Definieren Sie Ihre eigenen Bedingungen für die Ausführung Ihres Prozesses** , Und wählen Sie die Auslöserbedingung aus, wenn Ihr Playbook ausgeführt werden muss.
5. Klicken Sie Auf **Legen Sie Ihre Auslöserbedingungen fest** .
6. Wählen Sie die Bedingungen aus, die definiert werden sollen, wann Ihr Playbook ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslöserbedingung ist beispielsweise, wenn ein Security Incident der Kategorie Phishing erstellt wird.



7. Klicken Sie Auf **Wechseln Sie zu Designer** .
8. Um mit dem Entwerfen Ihres automatisierten Prozesses zu beginnen, klicken Sie auf **Fügen Sie eine neue Phase hinzu** .

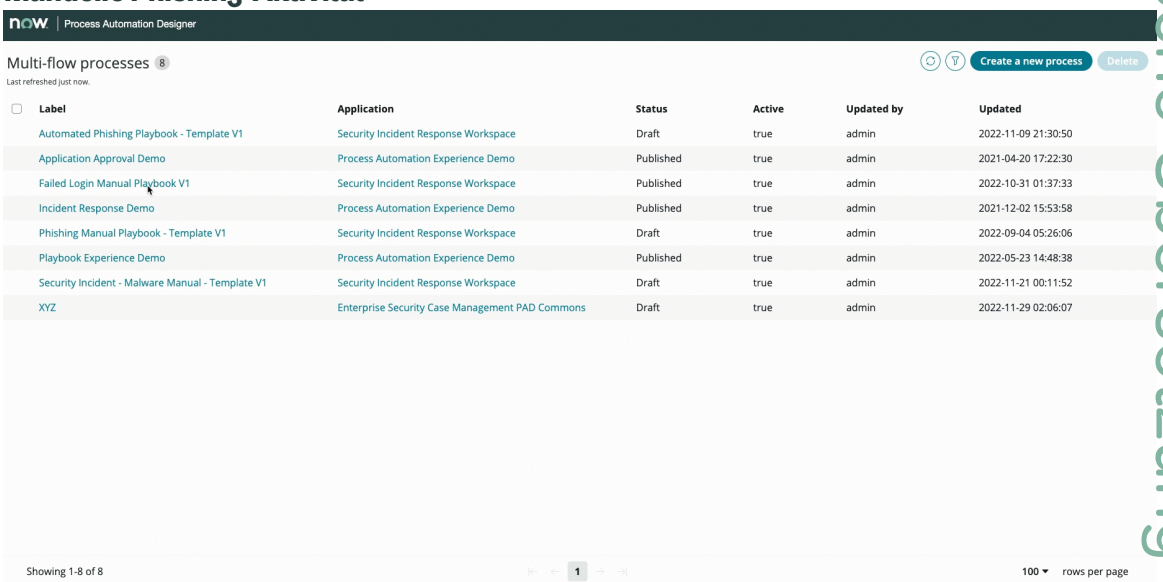
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Bereich für Phaseneigenschaften wird auf der rechten Seite der Anwenderoberfläche geöffnet.

9. Geben Sie im Bereich „Phaseneigenschaften“ die folgenden Details ein: **Name** , **Beschreibung** , **Ausführungsbedingung** , Und **Geben Sie an, wann begonnen werden soll** .
   Die **Ausführungsbedingung** Und **Geben Sie an, wann begonnen werden soll** Felder geben an, wann die Phase ausgeführt würde.
10. Klicken Sie Auf **Speichern und schließen** .
11. Um eine weitere Phase hinzuzufügen, klicken Sie auf **Fügen Sie eine weitere Phase hinzu** .
    Ebenso können Sie beliebig viele Phasen erstellen. In diesem Beispiel können Sie eine Phase für „Analyse“, „Eindämmen“, „Auslöschen“ und „Überprüfen“ erstellen. Im folgenden Beispiel: **Analyse** Phase startet sofort und hat keine Ausführungsbedingung. **Enthalten** Phasenstart, nachdem die vorherige Phase abgeschlossen ist und eine Ausführungsbedingung aufweist, die auf dem Ergebnis einer Aktivität in der vorherigen Phase basiert.
    Nach dem Hinzufügen der Phasen müssen Sie Prozessaktivitäten für jede Phase hinzufügen.
12. Klicken Sie Auf **Fügen Sie eine weitere Aktivität hinzu** Unter einer bestimmten Phase (z. B. Analysephase).
    Das Popup-Fenster Aktivität hinzufügen wird geöffnet.
    a. Wählen Sie im Popup-Fenster Aktivität hinzufügen die erforderliche Aktivitätsdefinition aus.
13. Klicken Sie Auf **Erstellen Sie eine neue Aktivität** .
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Phasen weiter konfiguriert werden. Ebenso können Sie unter jeder Phase weitere Prozessaktivitäten erstellen.

Manuelle Phishing-Aktivität



14. Fügen Sie im Bereich „Aktivitätseigenschaften“ eine Ausführungsbedingung hinzu, und geben Sie an, wann die Aktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) werden angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie Auf **Zeigen Sie alle Eigenschaften an** Und aktivieren Sie **Erweiterte Eigenschaften** Umschalten, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Fügen Sie parallele Aktivitäten hinzu

Wenn **Zeitpunkt für den Start** Feld ist auf festgelegt **Mit Vorherigem** , Dann können parallele Aktivitäten initiiert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für den Wechsel von einer Phase zur nächsten

Wenn keine Ausführungsbedingung definiert ist, werden die Phasen und Aktivitäten sequenziell ausgeführt.

Sie können die Ausführungsbedingung verwenden, um Aktivitäten oder Phasen zu überspringen. In diesem Beispiel **Phase „Eindämmen“ beginnt, wenn das Ergebnis von „enthält die E-Mail Bedrohungsindikatoren?“ vorliegt Ist ja** .

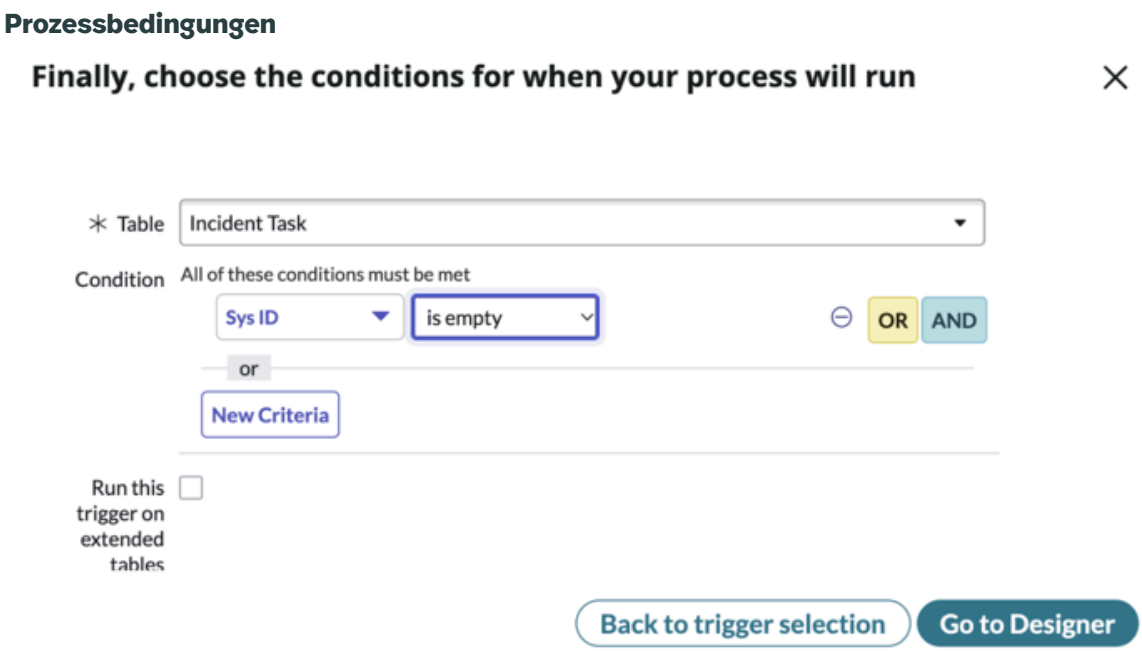
Um von einer Phase in eine andere zu wechseln, können Sie die bereitgestellte Plattform verwenden **Aktivitätsdefinition: Datensatz aktualisieren** . Dadurch wird das Statusfeld des Security Incidents aktualisiert und die Playbook-Ausführung mit der nächsten Phase fortgesetzt.

Die Herausforderung bei dieser Aktivitätsdefinition besteht jedoch darin, dass, wenn sich das Playbook in der Analysephase befindet und der Anwender den Status manuell auf „Überprüfen“ aktualisiert hat, die Aktivität „Datensatz aktualisieren“ den Status erneut in „Eindämmen“ ändert, um die Ausführung des Playbooks fortzusetzen. Dadurch wird der manuelle Change überschrieben.

Um dies zu überwinden, wird im Basissystem eine Aktivitätsdefinition namens genannt **Aufgabenstatus Aktualisieren** Ist angegeben. Diese Aktivität überschreibt den Status des Security Incidents nicht, wenn der aktuelle Status des Sicherheitsstatus der Phase im Playbook voraus ist.

Erstellen Sie eine Prozessdefinition mit Dummy-Auslöserbedingung

Eine Prozessdefinition erfordert immer eine Auslöserbedingung. Wenn Sie sich jedoch nicht sicher sind, wann der Prozess ausgelöst werden soll, können Sie trotzdem eine Prozessdefinition mit einer Dummy-Auslöserbedingung erstellen. Legen Sie die Auslöserbedingung als fest **sys_ID ist leer** . Diese Bedingung wird nie erfüllt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit dem manuellen Phishing-Playbook

Verwenden Sie diese Schritte, um zu erfahren, wie Sie das Playbook für manuelles Phishing im SIR Analyst Workspace und seine Fähigkeiten verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Manager oder sn_si.Analyst

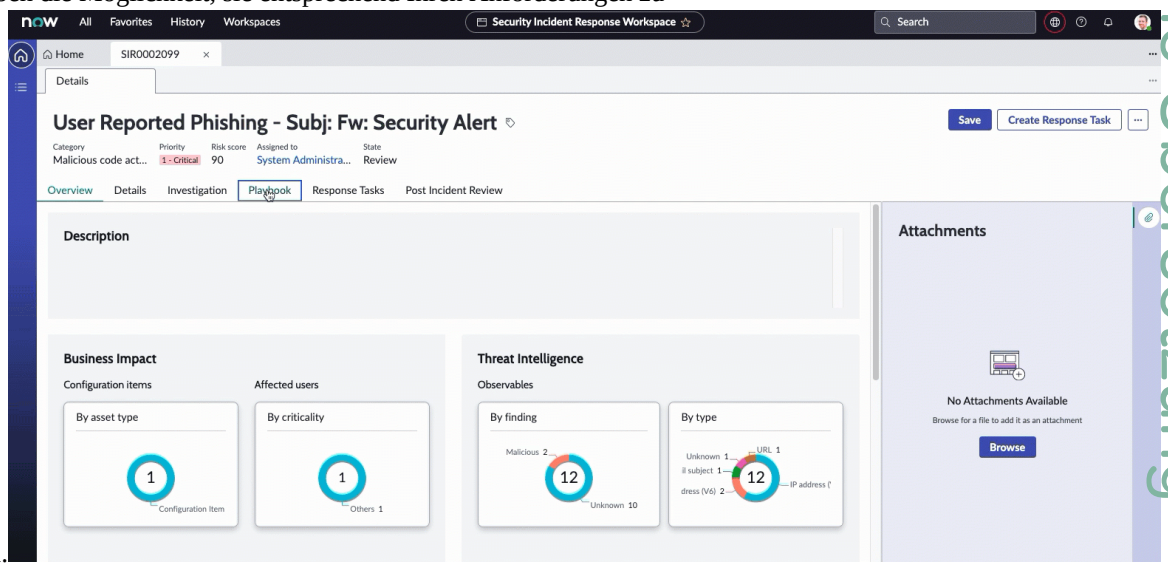
Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf **Playbook** Registerkarte.

   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incidents und die Risikopunktzahl anzeigen.

   Hinweis:
   Wenn keine Playbooks aufgeführt sind, müssen Sie zum PAD wechseln und zulassen, dass sie es im anzeigen können **Playbook** Registerkarte.

3. Klicken Sie auf **Manuelles Phishing-Playbook** .
4. Klicken Sie auf die einzelnen Phasen, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie Auf **Analyse** Um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen. Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern.



6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase ausgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn noch eine Aktivität oder Anwenderaktion vorhanden ist, die Sie ausführen müssen, wird sie in der jeweiligen Phase angezeigt.
7. Wenn in einer der Phasen noch eine Aktivität oder Anwenderaktion erforderlich ist, klicken Sie auf die entsprechende Phase, und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Arbeitsbereich-Playbook-Zusammenfassung

Im Folgenden wird die Prozesszusammenfassung beschrieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verstehen Sie das veraltete Flow-basierte Playbook.
- Listen Sie mögliche Aktivitäten und Phasen nach der Analyse des Flows auf. Suchen Sie nach den Schritten, in denen True Orchestration erstellt werden kann.
- Führen Sie jede Aktivität aus, und überprüfen Sie, ob die vom Basissystem bereitgestellte Aktivitätsdefinition den Anwendungsfall erfüllen kann oder nicht.
- Listen Sie Aktivitätsanwendungsfälle auf, für die neue Aktivitätsdefinitionen implementiert werden müssen. Klassifizieren – interaktiv, nicht interaktiv oder automatisiert. So erstellen Sie eine Aktivitätsdefinition:
  - Erstellen Sie einen Subflow oder eine Aktion für den Anwendungsfall.
  - Entscheiden Sie, ob die zugehörigen Daten in der Flow-Datentabelle oder einer anwenderdefinierten Tabelle erfasst werden müssen.
  - Wenn Sie eine Flow-Datentabelle verwenden, erstellen Sie in eine Flow-Datendefinition **sys_Flow_Data_Definition** . Wählen Sie beim Erstellen eines Flow-Datensatzes im Subflow die erstellte Flow-Datendefinition aus.
  - Erstellen Sie einen **Aktivitätsdefinition** .
  - Ordnen Sie den Automatisierungsplan zu.
  - Füllen Sie aus **Aktivitäts-Experience** Eigenschaften.
  - Erstellen Sie eine Aktion unter Playbook-Aktionen. Es muss eine Aktivitätsaktion vorhanden sein, um sie der Aktivitätsdefinition zuzuweisen.
  - Um die Standardkarten-Experience basierend auf dem ausgewählten Experience-Typ zu überschreiben, fügen Sie die Playbook-Überschreibung mithilfe des Aktivitäts-UI-Konzepts hinzu.
- Einige Aktivitäten können durchgeführt werden, um sowohl automatisch als auch interaktiv zu verarbeiten, indem die Kennzeichnung „Warten auf Anwendereingabe“ im Subflow verwendet wird. Diese Eingabe kann beim Konfigurieren der Aktivität in der Prozessdefinition übergeben werden.
- Nachdem Sie alle für Ihren Prozess erforderlichen Aktivitätsdefinitionen haben, beginnen Sie mit der Erstellung der Prozessdefinition mit Workflow-Studio.

Playbook für automatisiertes Phishing

Das Playbook für automatisiertes Phishing bietet Ihren Analysten Schritt-für-Schritt-Anleitungen, wie sie bestimmte Arten von Sicherheitsbedrohungen in Ihren automatisierten Phishing-Aktivitäten lösen könnten.

Übersicht

Die Playbook-Vorlage für automatisiertes Phishing dient der Automatisierung der Phishing-Antwortaufgaben und enthält eine Reihe von Aktionen, die Auslöserbedingungen enthalten. Sie können die Playbook-Vorlagen in verwenden Workflow-Studio Automatisieren Sie die Schritte im Phishing-Antwort-Playbook und lösen Sie diese Incidents effizient. Diese Playbook-Vorlage enthält eine Sequenz wiederverwendbarer Aktionen, die auf Phishing-Angriffe reagieren sollen. Jeder Flow hat einen Auslöser (Bedingung), eine Sequenz von Aktionen und Subflows, die Sie kommentieren können.

In diesem Playbook gibt es keine Anwenderinteraktion, wenn die Kategorie eines Security Incidents auf Phishing festgelegt ist. Dieses Playbook kann verwendet werden, wenn ein Security Incident erstellt oder aktualisiert wird. Sie müssen das Playbook für automatisiertes Phishing in aktivieren Workflow-Studio, Und dieses Playbook führt automatisch alle Aufgaben aus, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

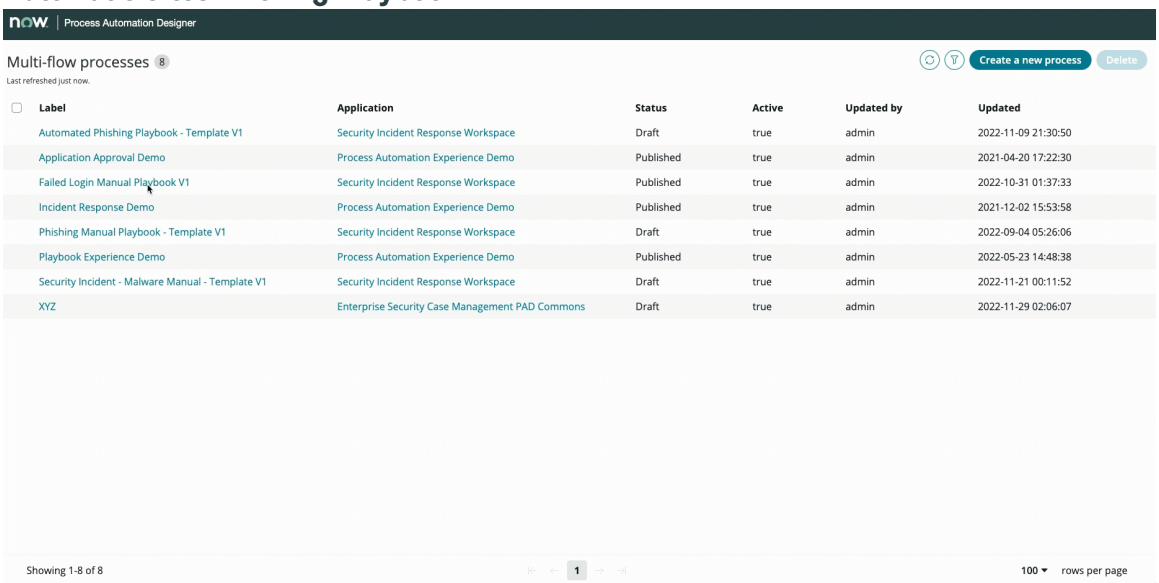
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Phasen der Prozessdefinition entsprechen dem Status des Security Incidents:

- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Phase enthält Aktivitäten.

Automatisiertes Phishing-Playbook



Sobald Sie eine Aufgabe in einer Phase als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Phase abgeschlossen haben, können Sie zur nächsten Phase wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie Aufgaben und Phasen abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für jede Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die von Ihnen eingegebenen Details in allen Phasen zu überprüfen. Sie können ein beliebiges Feld bearbeiten oder auf Fertigstellen klicken, um den Prozess zum Erstellen der Berechtigung abzuschließen.

Erstellen Sie Prozesse für automatisiertes Phishing in PAD

Verwenden Sie diese Schritte, um Prozesse für automatisiertes Phishing im Prozessautomatisierungs-Designer (PAD) zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Manager

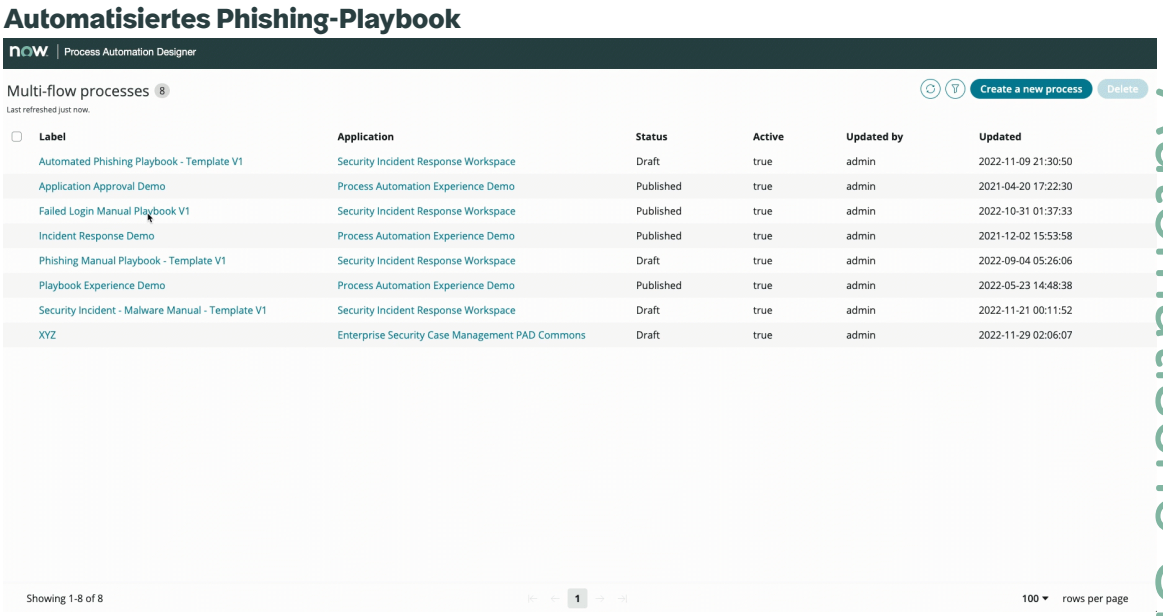
Prozedur

1. Klicken **Alle** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**an.

   Beispiel: Playbook-Vorlage für automatisiertes Phishing V1.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Geben Sie einen Namen für den Prozess, die Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken Sie Auf **Wählen Sie einen Auslöser aus** .
4. Wählen Sie Aus **Definieren Sie Ihre eigenen Bedingungen für die Ausführung Ihres Prozesses** , Und wählen Sie die Auslöserbedingung aus, wenn Ihr Prozess ausgeführt werden muss.
5. Klicken Sie Auf **Legen Sie Ihre Auslöserbedingungen fest** .
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslöserbedingung ist beispielsweise, wenn ein Security Incident der Kategorie Phishing erstellt wird.



7. Klicken Sie Auf **Wechseln Sie zu Designer** .
   Die Seite Prozessautomatisierungs-Designer wird geöffnet.
8. Um mit dem Entwerfen Ihres automatisierten Prozesses zu beginnen, klicken Sie auf **Fügen Sie eine neue Phase hinzu** .
   Der Bereich für Phaseneigenschaften wird auf der rechten Seite der Anwenderoberfläche geöffnet.
9. Geben Sie im Bereich „Phaseneigenschaften“ die folgenden Details ein: **Name** , **Beschreibung** , **Ausführungsbedingung** , Und **Geben Sie an, wann begonnen werden soll** .
   Die **Ausführungsbedingung** Und **Geben Sie an, wann begonnen werden soll** Felder geben an, wann die Phase ausgeführt würde.
10. Klicken Sie Auf **Speichern und schließen** .
11. Um eine weitere Phase hinzuzufügen, klicken Sie auf **Fügen Sie eine weitere Phase hinzu** .
    Ebenso können Sie beliebig viele Phasen erstellen. In diesem Beispiel können Sie eine Phase für „Analyse“, „Eindämmen“, „Auslöschen“ und „Überprüfen“ erstellen. Im folgenden Beispiel: **Analyse** Phase startet sofort und hat keine Ausführungsbedingung. **Enthalten** Phasenstart, nachdem die vorherige Phase abgeschlossen ist und eine Ausführungsbedingung aufweist, die auf dem Ergebnis einer Aktivität in der vorherigen Phase basiert.
    Nach dem Hinzufügen der Phasen müssen Sie Prozessaktivitäten für jede Phase hinzufügen.
12. Klicken Sie Auf **Fügen Sie eine weitere Prozessaktivität hinzu** Unter einer bestimmten Phase (z. B. Analysephase).
    Das Popup-Fenster Aktivität hinzufügen wird geöffnet.

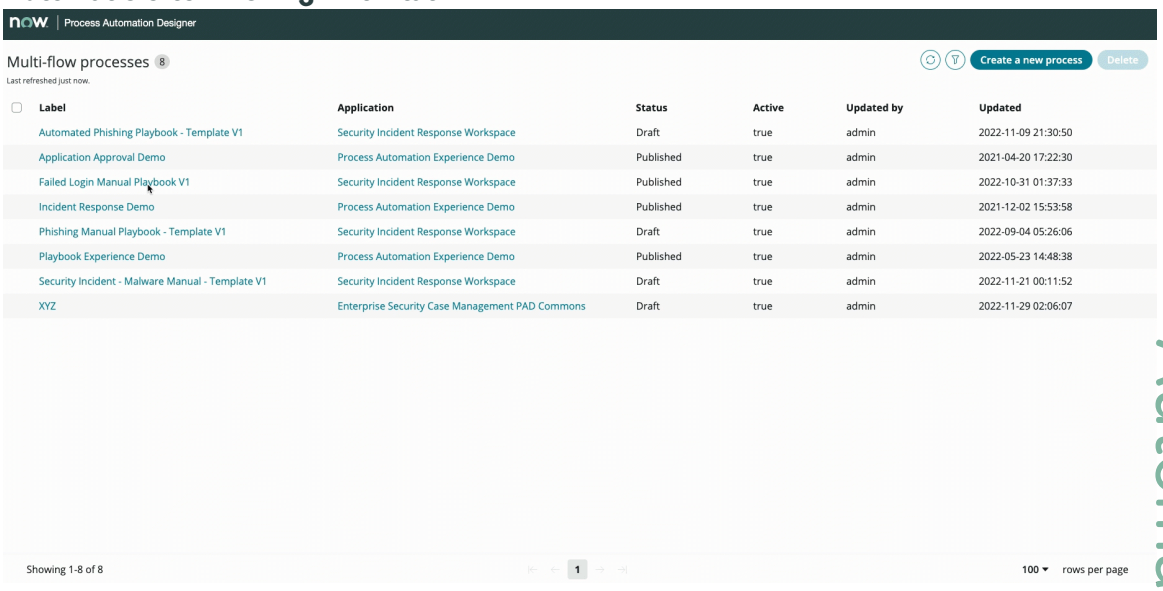
    a. Wählen Sie im Popup-Fenster Aktivität hinzufügen die erforderliche Aktivitätsdefinition aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Klicken Sie Auf **Erstellen Sie eine neue Aktivität** .
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Phasen weiter konfiguriert werden. Ebenso können Sie unter jeder Phase weitere Prozessaktivitäten erstellen.

Automatisierte Phishing-Aktivität



14. Fügen Sie im Bereich „Aktivitätseigenschaften“ eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) werden angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie Auf **Zeigen Sie alle Eigenschaften an** Und aktivieren Sie **Erweiterte Eigenschaften** Umschalten, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Mit dem Playbook für automatisiertes Phishing

Verwenden Sie diese Schritte, um zu erfahren, wie Sie das Playbook für automatisiertes Phishing im SIR Analyst Workspace und seine Fähigkeiten verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Manager oder sn_si.Analyst

Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf **Playbook** Registerkarte.

   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incidents und die Risikopunktzahl anzeigen.

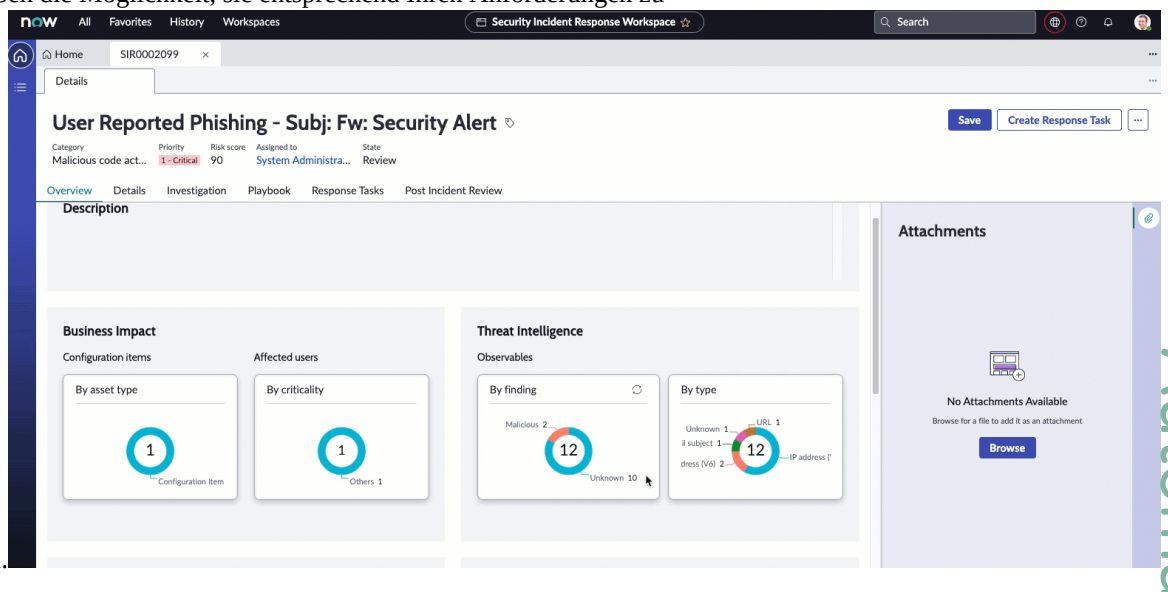
   Hinweis:
   Wenn keine Playbooks aufgeführt sind, müssen Sie zum PAD wechseln und zulassen, dass sie es im anzeigen können **Playbook** Registerkarte.

3. Klicken Sie auf **Playbook Für Automatisiertes Phishing** .
   Für automatisiertes Phishing werden die Aufgaben für den Security Incident automatisch ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die einzelnen Phasen, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie Auf **Analyse** Um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen. Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern.



6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase ausgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn noch eine Aktivität oder Anwenderaktion vorhanden ist, die Sie ausführen müssen, wird sie in der jeweiligen Phase angezeigt.
7. Wenn in einer der Phasen noch eine Aktivität oder Anwenderaktion erforderlich ist, klicken Sie auf die entsprechende Phase, und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Playbook für manuelle Malware

Das Manuelle Malware-Playbook bietet Schritt-für-Schritt-Anleitungen, wie Analysten Malware-Warnungen effizienter manuell lösen können.

Die Vorlage „Manuelles Malware-Playbook“ dient dazu, die Schritte für die Verarbeitung von Malware-Warnungen vom Endpunkt oder Netzwerk manuell auszuführen. Sie können die Playbook-Vorlagen in verwenden Workflow-Studio Um die Schritte im manuellen Malware-Playbook auszuführen und diese Warnungen effizient zu lösen. Dieses Playbook enthält Auslöserbedingungen, eine Sequenz von Aktionen und Subflows, die Sie kommentieren können. Dieses Playbook enthält eine Sequenz wiederverwendbarer Aktionen, die auf Malware-Angriffe reagieren sollen. Jeder Flow hat einen Auslöser (Bedingung), eine Sequenz von Aktionen und Subflows für Anmerkungen.

Dieses Playbook kann verwendet werden, wenn Malware erstellt oder aktualisiert wird. Sie müssen das manuelle Malware-Playbook in aktivieren Workflow-Studio Und erstellen Sie alle Aufgaben, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

Die folgenden Phasen der Prozessdefinition entsprechen dem Malware-Warnungsstatus:

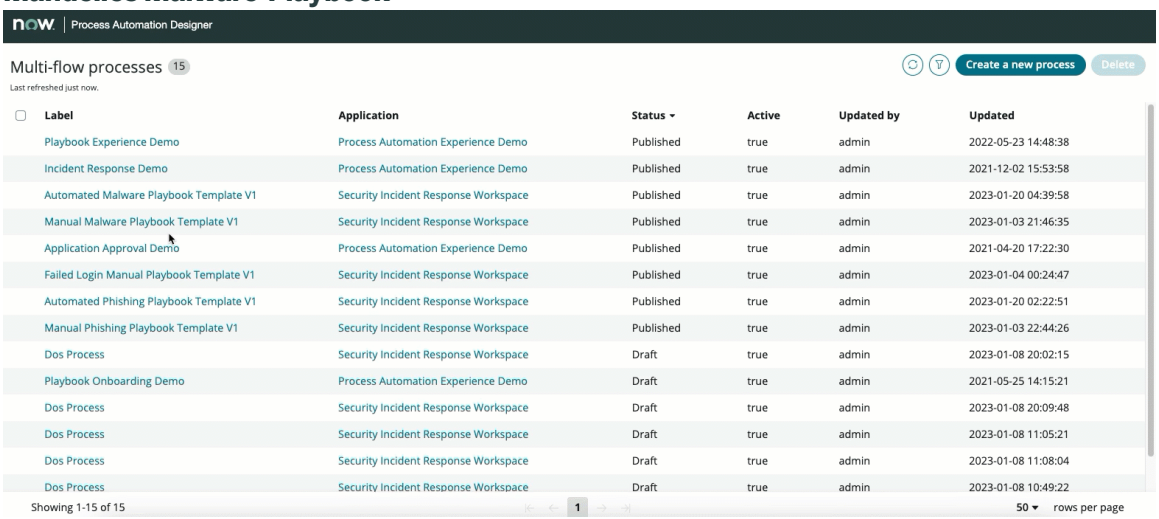
- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Phase enthält Aktivitäten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Manuelles Malware-Playbook



Nachdem Sie eine Aufgabe in einer Phase als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Phase abgeschlossen haben, können Sie zur nächsten Phase wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie Aufgaben und Phasen abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für jede Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die von Ihnen eingegebenen Details in allen Phasen zu überprüfen. Sie können ein beliebiges Feld bearbeiten oder auf Fertigstellen klicken, um den Prozess zum Erstellen der Berechtigung abzuschließen.

Erstellen Sie Prozesse für manuelle Malware in PAD

Verwenden Sie diese Schritte, um Prozesse für manuelle Malware im Prozessautomatisierungs-Designer (PAD) zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Manager

Prozedur

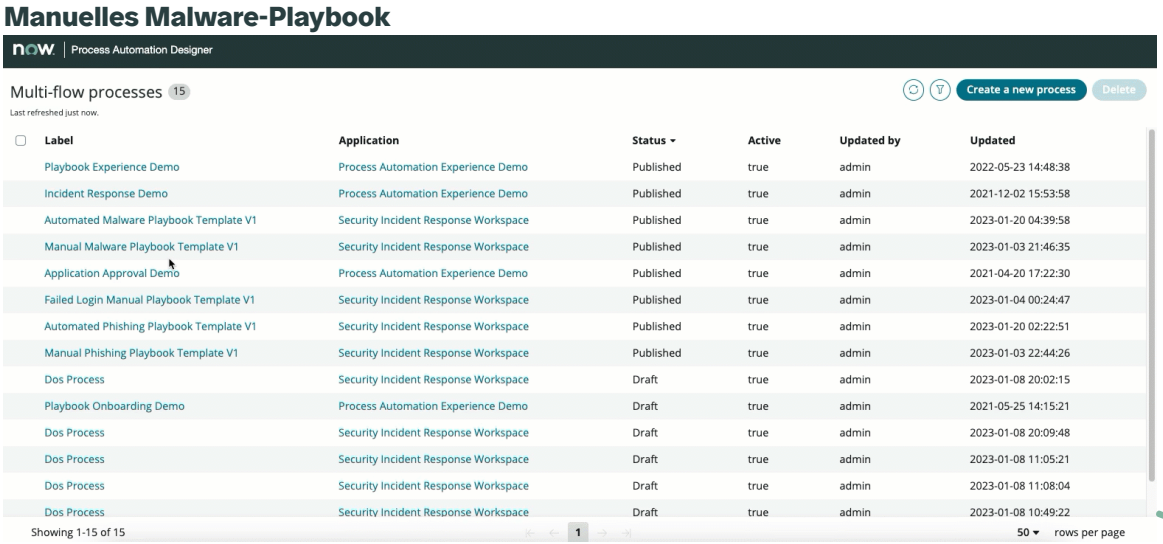
1. Klicken **Alle** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**an.

   Beispiel: Manuelle Malware-Playbook-Vorlage V1.

2. Geben Sie einen Namen für den Prozess, die Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken Sie Auf **Wählen Sie einen Auslöser aus** .
4. Wählen Sie Aus **Definieren Sie Ihre eigenen Bedingungen für die Ausführung Ihres Prozesses** , Und wählen Sie die Auslöserbedingung aus, wenn Ihr Prozess ausgeführt werden muss.
5. Klicken Sie Auf **Legen Sie Ihre Auslöserbedingungen fest** .
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslöserbedingung ist beispielsweise, wenn ein Security Incident der Kategorie Phishing erstellt wird.

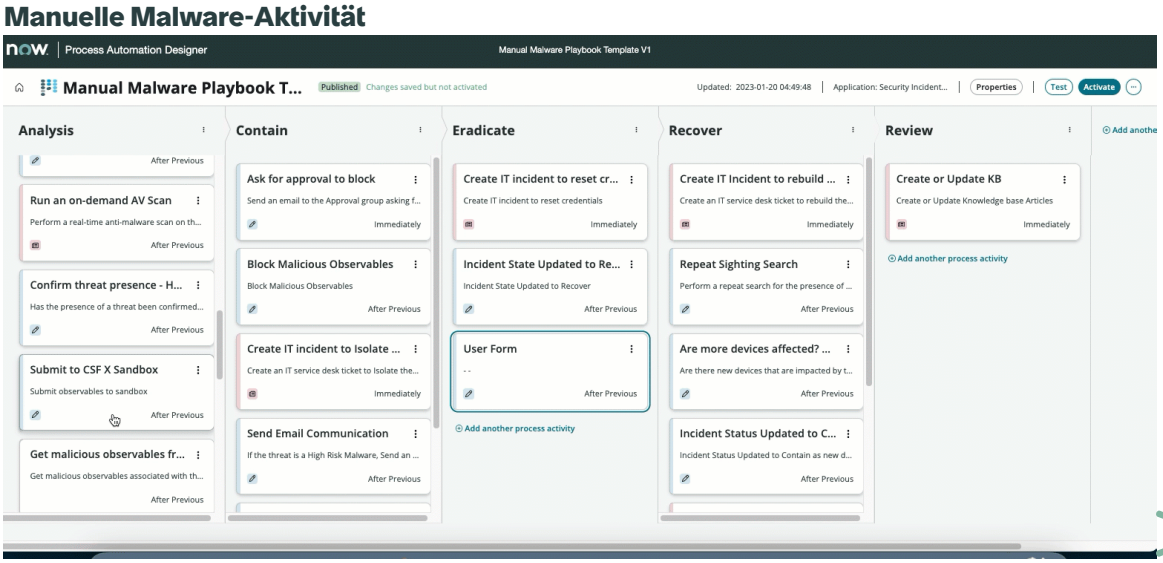
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie Auf **Wechseln Sie zu Designer** .
   Die Seite Prozessautomatisierungs-Designer wird geöffnet.
8. Um mit dem Entwerfen Ihres automatisierten Prozesses zu beginnen, klicken Sie auf **Fügen Sie eine neue Phase hinzu** .
   Der Bereich für Phaseneigenschaften wird auf der rechten Seite der Anwenderoberfläche geöffnet.
9. Geben Sie im Bereich „Phaseneigenschaften“ die folgenden Details ein: **Name** , **Beschreibung** , **Ausführungsbedingung** , Und **Geben Sie an, wann begonnen werden soll** .
   Die **Ausführungsbedingung** Und **Geben Sie an, wann begonnen werden soll** Felder geben an, wann die Phase ausgeführt würde.
10. Klicken Sie Auf **Speichern und schließen** .
11. Um eine weitere Phase hinzuzufügen, klicken Sie auf **Fügen Sie eine weitere Phase hinzu** .
    Ebenso können Sie beliebig viele Phasen erstellen. In diesem Beispiel können Sie eine Phase für „Analyse“, „Eindämmen“, „Auslöschen“ und „Überprüfen“ erstellen. Im folgenden Beispiel: **Analyse** Phase startet sofort und hat keine Ausführungsbedingung. **Enthalten** Phasenstart, nachdem die vorherige Phase abgeschlossen ist und eine Ausführungsbedingung aufweist, die auf dem Ergebnis einer Aktivität in der vorherigen Phase basiert.
    Nach dem Hinzufügen der Phasen müssen Sie Prozessaktivitäten für jede Phase hinzufügen.
12. Klicken Sie Auf **Fügen Sie eine weitere Prozessaktivität hinzu** Unter einer bestimmten Phase (z. B. Analysephase).
    Das Popup-Fenster Aktivität hinzufügen wird geöffnet.
    a. Wählen Sie im Popup-Fenster Aktivität hinzufügen die erforderliche Aktivitätsdefinition aus.
13. Klicken Sie Auf **Erstellen Sie eine neue Aktivität** .
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Phasen weiter konfiguriert werden. Ebenso können Sie unter jeder Phase weitere Prozessaktivitäten erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



14. Fügen Sie im Bereich „Aktivitätseigenschaften“ eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) werden angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie Auf **Zeigen Sie alle Eigenschaften an** Und aktivieren Sie **Erweiterte Eigenschaften** Umschalten, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Mit dem manuellen Malware-Playbook

Verwenden Sie diese Schritte, um zu erfahren, wie Sie das manuelle Malware-Playbook im SIR Analyst Workspace und seine Fähigkeiten verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Manager oder sn_si.Analyst

Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf **Playbook** Registerkarte.

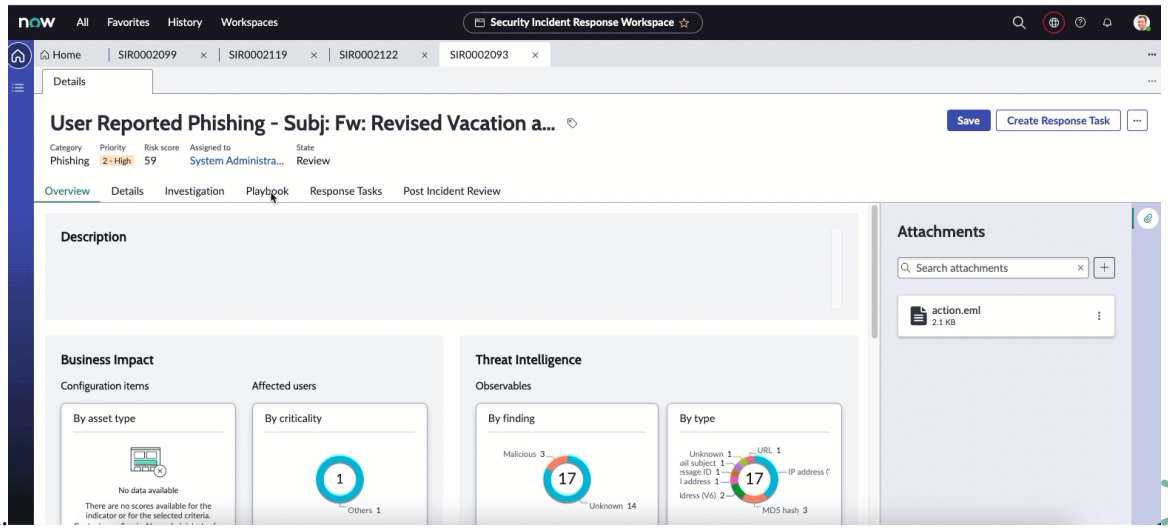
   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incidents und die Risikopunktzahl anzeigen.

   Hinweis:
   Wenn keine Playbooks aufgeführt sind, müssen Sie zum PAD wechseln und zulassen, dass sie es im anzeigen können **Playbook** Registerkarte.

3. Klicken Sie auf **Manuelles Malware-Playbook** .
   Bei manueller Malware werden die Aufgaben für den Security Incident automatisch ausgeführt.
4. Klicken Sie auf die einzelnen Phasen, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie Auf **Analyse** Um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern.



6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase ausgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn noch eine Aktivität oder Anwenderaktion vorhanden ist, die Sie ausführen müssen, wird sie in der jeweiligen Phase angezeigt.
7. Wenn in einer der Phasen noch eine Aktivität oder Anwenderaktion erforderlich ist, klicken Sie auf die entsprechende Phase, und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Playbook für automatisierte Malware

Das automatisierte Malware-Playbook bietet eine Sequenz automatisierter Schritte, mit denen Analysten Malware-Warnungen effizienter lösen können.

Die Playbook-Vorlage für automatisierte Malware dient der Automatisierung der Schritte, die bei der Verarbeitung von Malware-Warnungen vom Endpunkt oder Netzwerk erforderlich sind. Sie können die Playbook-Vorlagen in verwenden Workflow-Studio Automatisieren Sie die Schritte im Playbook für automatisierte Malware und lösen Sie diese Warnungen effizient. Dieses Playbook enthält Auslöserbedingungen, eine Sequenz von Aktionen und Subflows, die Sie kommentieren können. Dieses Playbook enthält eine Sequenz wiederverwendbarer Aktionen, die auf Malware-Angriffe reagieren sollen. Jeder Flow hat einen Auslöser (Bedingung), eine Sequenz von Aktionen und Subflows für Anmerkungen.

Dieses Playbook kann verwendet werden, wenn ein Security Incident erstellt oder aktualisiert wird. Sie müssen das automatisierte Malware-Playbook in aktivieren Workflow-Studio, Und dieses Playbook führt automatisch alle Aufgaben aus, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

Die folgenden Phasen der Prozessdefinition entsprechen dem Status des Security Incidents:

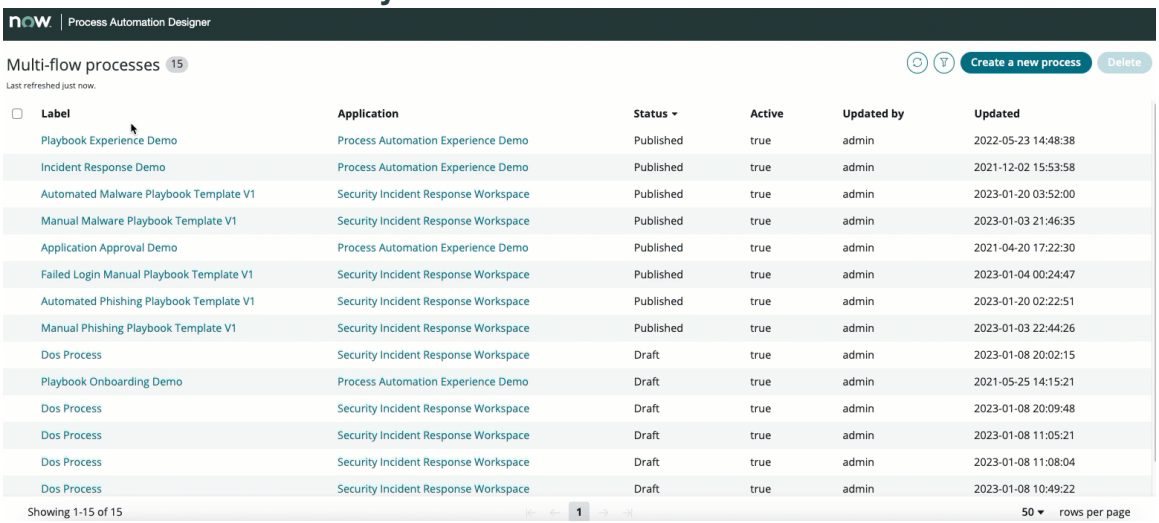
- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Phase enthält Aktivitäten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatisiertes Malware-Playbook



Sobald Sie eine Aufgabe in einer Phase als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Phase abgeschlossen haben, können Sie zur nächsten Phase wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie Aufgaben und Phasen abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für jede Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die von Ihnen eingegebenen Details in allen Phasen zu überprüfen. Sie können ein beliebiges Feld bearbeiten oder auf Fertigstellen klicken, um den Prozess zum Erstellen der Berechtigung abzuschließen.

Erstellen Sie Prozesse automatisierte Malware in PAD

Verwenden Sie diese Schritte, um Prozesse für automatisierte Malware im Prozessautomatisierungs-Designer (PAD) zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Manager

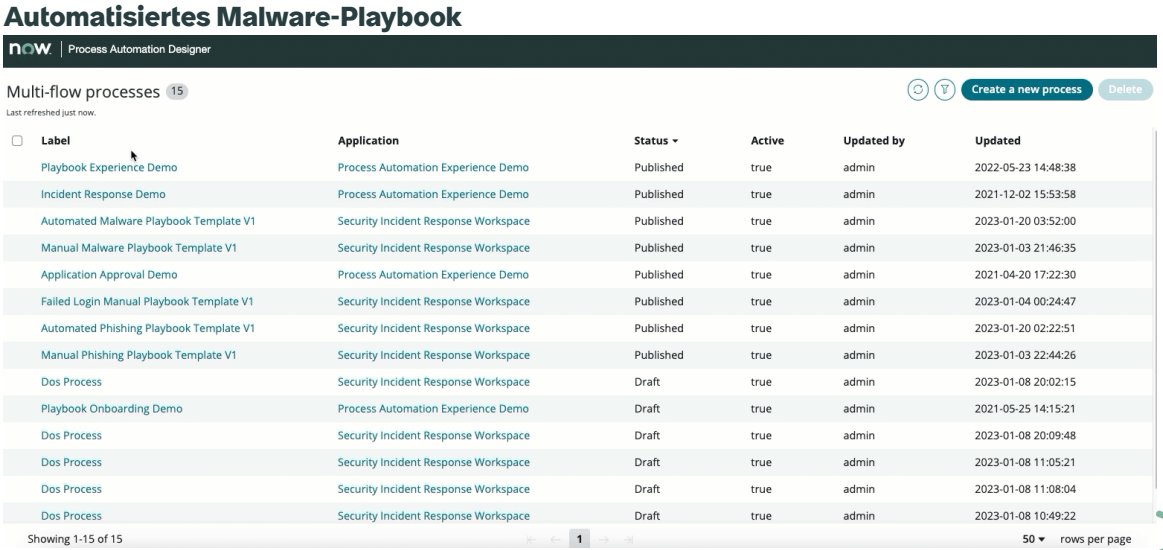
Prozedur

1. Klicken **Alle** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**an.

   Beispiel: Automatisierte Malware-Playbook-Vorlage V1.

2. Geben Sie einen Namen für den Prozess, die Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken Sie Auf **Wählen Sie einen Auslöser aus** .
4. Wählen Sie Aus **Definieren Sie Ihre eigenen Bedingungen für die Ausführung Ihres Prozesses** , Und wählen Sie die Auslöserbedingung aus, wenn Ihr Prozess ausgeführt werden muss.
5. Klicken Sie Auf **Legen Sie Ihre Auslöserbedingungen fest** .
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslöserbedingung ist beispielsweise, wenn ein Security Incident der Kategorie Phishing erstellt wird.

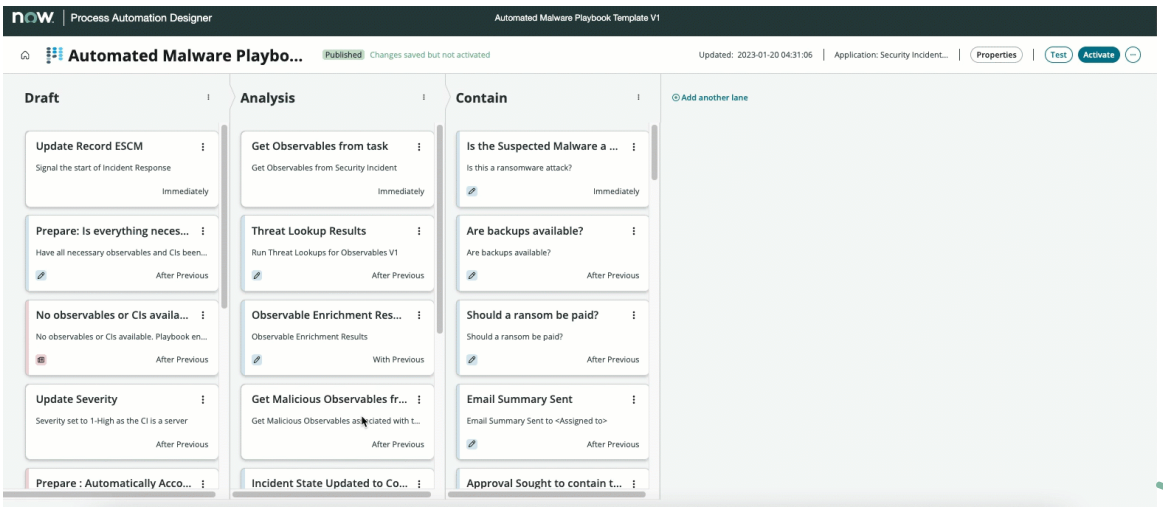
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie Auf **Wechseln Sie zu Designer** .
   Die Seite Prozessautomatisierungs-Designer wird geöffnet.
8. Um mit dem Entwerfen Ihres automatisierten Prozesses zu beginnen, klicken Sie auf **Fügen Sie eine neue Phase hinzu** .
   Der Bereich für Phaseneigenschaften wird auf der rechten Seite der Anwenderoberfläche geöffnet.
9. Geben Sie im Bereich „Phaseneigenschaften“ die folgenden Details ein: **Name** , **Beschreibung** , **Ausführungsbedingung** , Und **Geben Sie an, wann begonnen werden soll** .
   Die **Ausführungsbedingung** Und **Geben Sie an, wann begonnen werden soll** Felder geben an, wann die Phase ausgeführt würde.
10. Klicken Sie Auf **Speichern und schließen** .
11. Um eine weitere Phase hinzuzufügen, klicken Sie auf **Fügen Sie eine weitere Phase hinzu** .
    Ebenso können Sie beliebig viele Phasen erstellen. In diesem Beispiel können Sie eine Phase für „Analyse“, „Eindämmen“, „Auslöschen“ und „Überprüfen“ erstellen. Im folgenden Beispiel: **Analyse** Phase startet sofort und hat keine Ausführungsbedingung. **Enthalten** Phasenstart, nachdem die vorherige Phase abgeschlossen ist und eine Ausführungsbedingung aufweist, die auf dem Ergebnis einer Aktivität in der vorherigen Phase basiert.
    Nach dem Hinzufügen der Phasen müssen Sie Prozessaktivitäten für jede Phase hinzufügen.
12. Klicken Sie Auf **Fügen Sie eine weitere Prozessaktivität hinzu** Unter einer bestimmten Phase (z. B. Analysephase).
    Das Popup-Fenster Aktivität hinzufügen wird geöffnet.
    a. Wählen Sie im Popup-Fenster Aktivität hinzufügen die erforderliche Aktivitätsdefinition aus.
13. Klicken Sie Auf **Erstellen Sie eine neue Aktivität** .
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Phasen weiter konfiguriert werden. Ebenso können Sie unter jeder Phase weitere Prozessaktivitäten erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatisierte Malware-Aktivität



14. Fügen Sie im Bereich „Aktivitätseigenschaften“ eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) werden angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie Auf **Zeigen Sie alle Eigenschaften an** Und aktivieren Sie **Erweiterte Eigenschaften** Umschalten, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Mit dem automatisierten Malware-Playbook

Verwenden Sie diese Schritte, um zu erfahren, wie Sie das Playbook für automatisierte Malware im SIR Analyst Workspace und seine Fähigkeiten verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Manager oder sn_si.Analyst

Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf **Playbook** Registerkarte.

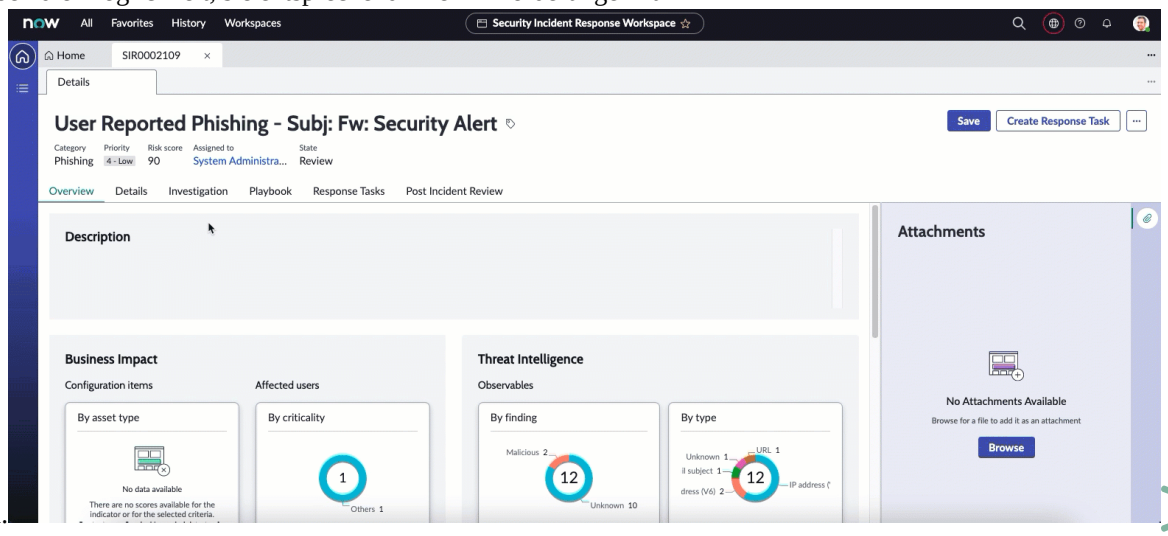
   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incidents und die Risikopunktzahl anzeigen.

   Hinweis:
   Wenn keine Playbooks aufgeführt sind, müssen Sie zum PAD wechseln und zulassen, dass sie es im anzeigen können **Playbook** Registerkarte.

3. Klicken Sie auf **Automatisiertes Malware-Playbook** .
   Bei automatisierter Malware werden die Aufgaben für den Security Incident automatisch ausgeführt.
4. Klicken Sie auf die einzelnen Phasen, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie Auf **Analyse** Um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern.



6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase ausgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn noch eine Aktivität oder Anwenderaktion vorhanden ist, die Sie ausführen müssen, wird sie in der jeweiligen Phase angezeigt.
7. Wenn in einer der Phasen noch eine Aktivität oder Anwenderaktion erforderlich ist, klicken Sie auf die entsprechende Phase, und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Playbook für fehlgeschlagene Anmeldung – Handbuch

Das Playbook „Handbuch für fehlgeschlagene Anmeldungen“ bietet Anleitungen und hilft, die Untersuchung von Security Incidents für fehlgeschlagene Anmeldungen zu optimieren.

Wenn ein Anwender bestimmte nicht erfolgreiche Anmeldeversuche (gemäß SIM-Konfiguration) vornimmt, wird ein Security Incident erstellt. Diese nicht erfolgreichen Anmeldeversuche können entweder falsch positive Ergebnisse sein oder Versuche von Angreifern sein, Zugriff auf Anwender-E-Mail-Accounts zu erhalten.

Sie können die Playbook-Vorlagen in verwenden Workflow-Studio Um die Schritte im Playbook für fehlgeschlagene Anmeldungen auszuführen und Security Incidents für fehlgeschlagene Anmeldungen effizient zu lösen. Dieses Playbook enthält Auslöserbedingungen, eine Sequenz von Aktionen und Subflows, die Sie kommentieren können. Dieses Playbook enthält eine Sequenz wiederverwendbarer Aktionen, die auf Security Incidents mit fehlgeschlagener Anmeldung reagieren sollen. Jeder Flow hat einen Auslöser (Bedingung), eine Sequenz von Aktionen und Subflows für Anmerkungen.

Dieses Playbook kann verwendet werden, wenn ein Security Incident für die fehlgeschlagene Anmeldung erstellt oder aktualisiert wird. Sie müssen das Playbook „Manuelle fehlgeschlagene Anmeldung“ in aktivieren Workflow-Studio Und erstellen Sie alle Aufgaben, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

Die folgenden Phasen der Prozessdefinition entsprechen dem Status des Security Incidents:

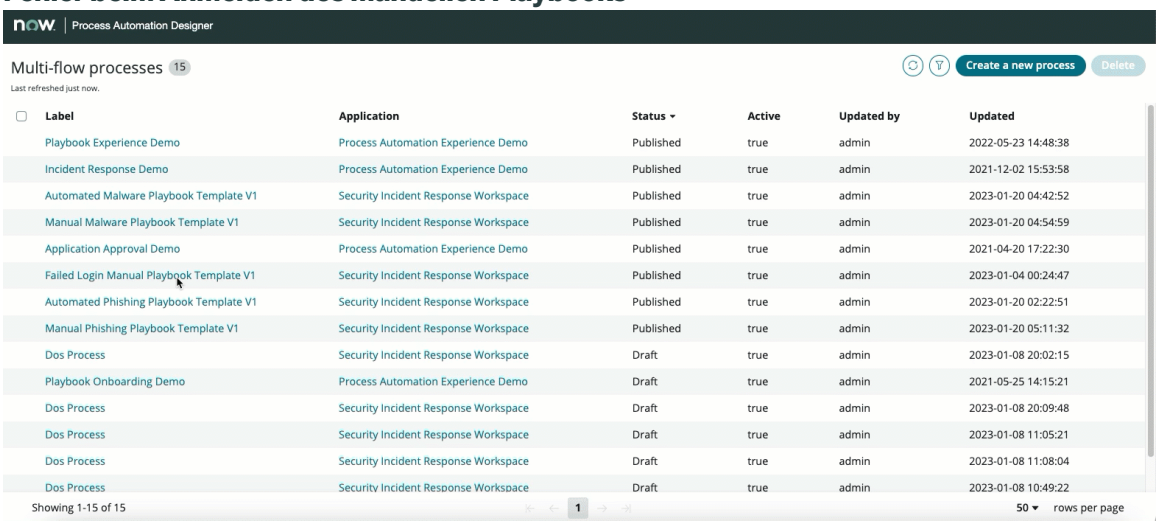
- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Phase enthält Aktivitäten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler beim Anmelden des manuellen Playbooks



Sobald Sie eine Aufgabe in einer Phase als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Phase abgeschlossen haben, können Sie zur nächsten Phase wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie Aufgaben und Phasen abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für jede Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die von Ihnen eingegebenen Details in allen Phasen zu überprüfen. Sie können ein beliebiges Feld bearbeiten oder auf Fertigstellen klicken, um den Prozess zum Erstellen der Berechtigung abzuschließen.

Erstellen Sie Prozesse für das Handbuch für fehlgeschlagene Anmeldung in PAD

Verwenden Sie diese Schritte, um Prozesse für das Handbuch für fehlgeschlagene Anmeldung im Prozessautomatisierungs-Designer (PAD) zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Manager

Prozedur

1. Klicken **Alle** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**an.

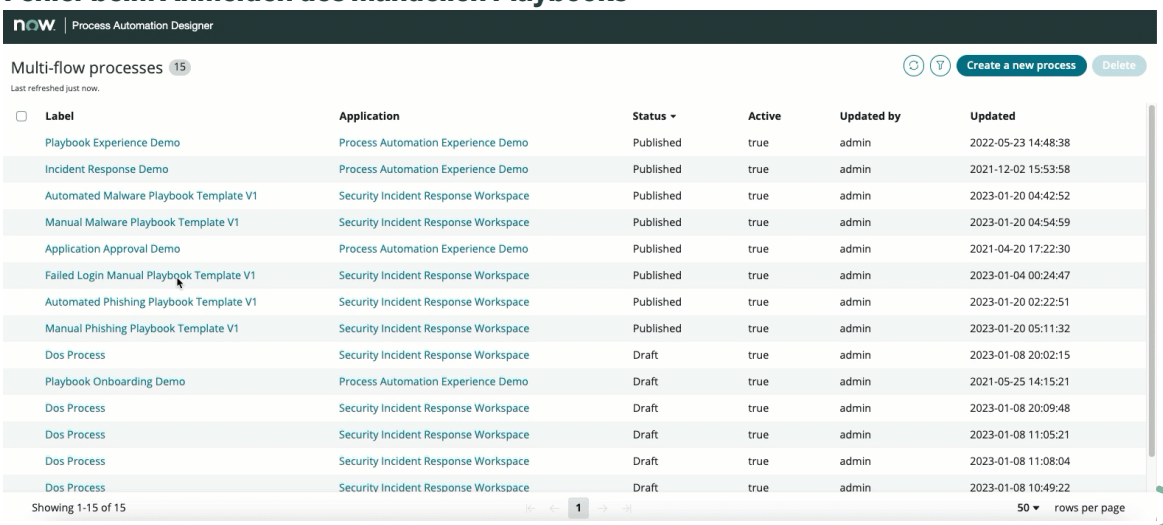
   Beispiel: Fehlgeschlagene Anmeldung – Manuelle Playbook-Vorlage V1.

2. Geben Sie einen Namen für den Prozess, die Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.
3. Klicken Sie Auf **Wählen Sie einen Auslöser aus** .
4. Wählen Sie Aus **Definieren Sie Ihre eigenen Bedingungen für die Ausführung Ihres Prozesses** , Und wählen Sie die Auslöserbedingung aus, wenn Ihr Prozess ausgeführt werden muss.
5. Klicken Sie Auf **Legen Sie Ihre Auslöserbedingungen fest** .
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
   Die Auslöserbedingung ist beispielsweise, wenn ein Security Incident der Kategorie Phishing erstellt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

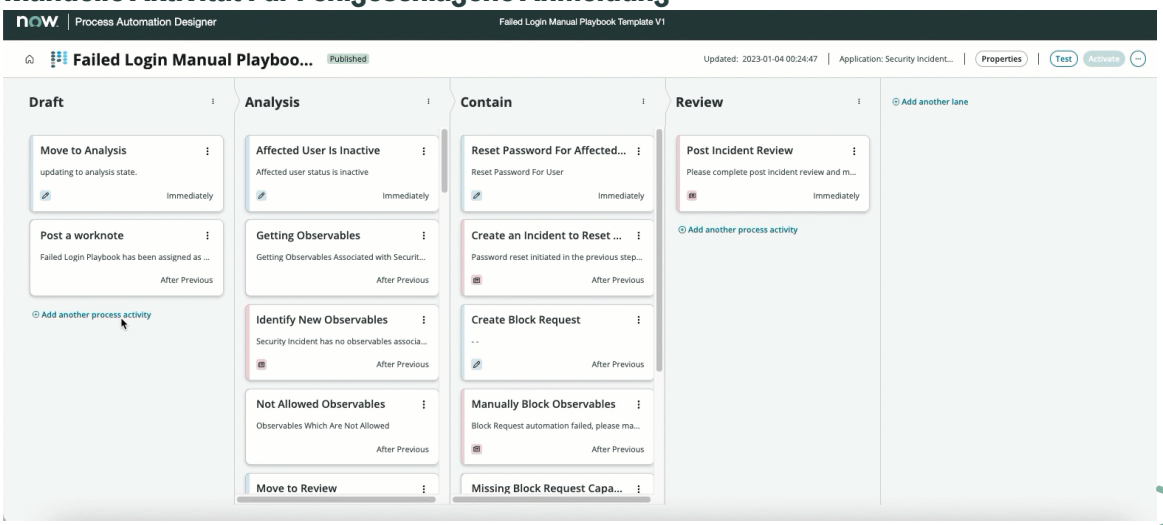
Fehler beim Anmelden des manuellen Playbooks



7. Klicken Sie Auf **Wechseln Sie zu Designer** .
   Die Seite Prozessautomatisierungs-Designer wird geöffnet.
8. Um mit dem Entwerfen Ihres automatisierten Prozesses zu beginnen, klicken Sie auf **Fügen Sie eine neue Phase hinzu** .
   Der Bereich für Phaseneigenschaften wird auf der rechten Seite der Anwenderoberfläche geöffnet.
9. Geben Sie im Bereich „Phaseneigenschaften“ die folgenden Details ein: **Name** , **Beschreibung** , **Ausführungsbedingung** , Und **Geben Sie an, wann begonnen werden soll** .
   Die **Ausführungsbedingung** Und **Geben Sie an, wann begonnen werden soll** Felder geben an, wann die Phase ausgeführt würde.
10. Klicken Sie Auf **Speichern und schließen** .
11. Um eine weitere Phase hinzuzufügen, klicken Sie auf **Fügen Sie eine weitere Phase hinzu** .
    Ebenso können Sie beliebig viele Phasen erstellen. In diesem Beispiel können Sie eine Phase für „Analyse“, „Eindämmen“, „Auslöschen“ und „Überprüfen“ erstellen. Im folgenden Beispiel: **Analyse** Phase startet sofort und hat keine Ausführungsbedingung. **Enthalten** Phasenstart, nachdem die vorherige Phase abgeschlossen ist und eine Ausführungsbedingung aufweist, die auf dem Ergebnis einer Aktivität in der vorherigen Phase basiert.
    Nach dem Hinzufügen der Phasen müssen Sie Prozessaktivitäten für jede Phase hinzufügen.
12. Klicken Sie Auf **Fügen Sie eine weitere Prozessaktivität hinzu** Unter einer bestimmten Phase (z. B. Analysephase).
    Das Popup-Fenster Aktivität hinzufügen wird geöffnet.
    a. Wählen Sie im Popup-Fenster Aktivität hinzufügen die erforderliche Aktivitätsdefinition aus.
13. Klicken Sie Auf **Erstellen Sie eine neue Aktivität** .
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Phasen weiter konfiguriert werden. Ebenso können Sie unter jeder Phase weitere Prozessaktivitäten erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Manuelle Aktivität Für Fehlgeschlagene Anmeldung



14. Fügen Sie im Bereich „Aktivitätseigenschaften“ eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) werden angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie Auf **Zeigen Sie alle Eigenschaften an** Und aktivieren Sie **Erweiterte Eigenschaften** Umschalten, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Verwenden des Playbooks „Manuelle fehlgeschlagene Anmeldung“

Verwenden Sie diese Schritte, um zu erfahren, wie Sie das Playbook Manuelle fehlgeschlagene Anmeldung im SIR Analyst Workspace und seine Fähigkeiten verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Manager oder sn_si.Analyst

Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich einen Security Incident.
2. Klicken Sie auf **Playbook** Registerkarte.

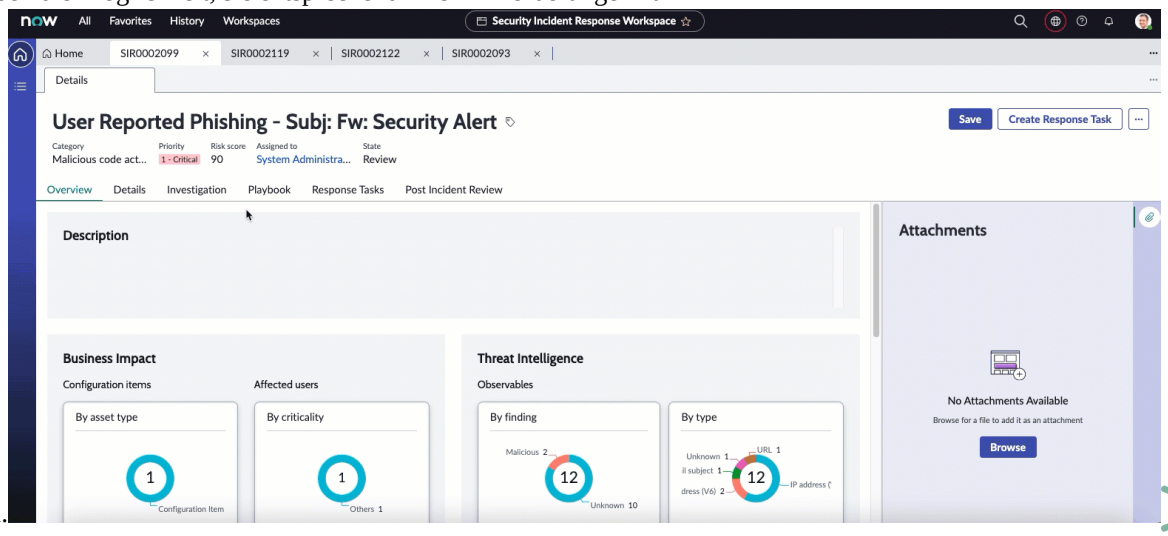
   Sie können die Playbooks anzeigen, die für den Security Incident aktiviert wurden. Sie können auch Details wie die Kategorie des Security Incidents und die Risikopunktzahl anzeigen.

   Hinweis:
   Wenn keine Playbooks aufgeführt sind, müssen Sie zum PAD wechseln und zulassen, dass sie es im anzeigen können **Playbook** Registerkarte.

3. Klicken Sie auf **Fehler Beim Anmelden Des Manuellen Playbooks** .
   Bei fehlgeschlagener Anmeldung werden die Aufgaben für den Security Incident automatisch ausgeführt.
4. Klicken Sie auf die einzelnen Phasen, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie Auf **Analyse** Um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern.



6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase ausgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn noch eine Aktivität oder Anwenderaktion vorhanden ist, die Sie ausführen müssen, wird sie in der jeweiligen Phase angezeigt.
7. Wenn in einer der Phasen noch eine Aktivität oder Anwenderaktion erforderlich ist, klicken Sie auf die entsprechende Phase, und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Flow-basierte Playbooks

Mit Flow Designer können Sicherheitsadministratoren und Flow Design-Autoren einfacher von manuellen oder undokumentierten Playbooks zu automatisierten und wiederholbaren Playbooks wechseln. Die Drag-and-Drop-Funktion bietet Flexibilität beim Verschieben von Objekten, Bedingungsprüfungen, parallelen Verzweigungen, Entscheidungstabellen und mehr.

Security Incident Response Stellt die folgenden Playbooks mit dem Basissystem bereit.

Neben den aufgeführten Playbooks gibt es auch Subflows in der Security Operations-Spoke, die über das Flows-Playbook aufgerufen werden können. Ransomware ist einer dieser Subflows.

Aktivieren Sie diese Flows, bevor Sie sie verwenden. Weitere Informationen finden Sie unter Aktivieren Sie einen Security Incident Response-Flow .

Playbook für automatisiertes Phishing

Das Playbook für automatisiertes Phishing hilft Ihnen, bestimmte Arten von Sicherheitsbedrohungen Schritt für Schritt zu lösen. Mit den Flow Designer-Vorlagen können Sie die Schritte im Phishing-Antwort-Playbook automatisieren und Incidents schnell und effizient lösen.

Sie können mit Flow Designer erstellte Vorlagen verwenden, um die Aufgaben in zu automatisieren Phishing-Antwort-Playbook Zum Analysieren und Lösen von Phishing-Angriffen in Ihrer Organisation.

Das Phishing-Antwort-Playbook enthält die folgenden Flows und Subflows:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Security Incident – Vorlage für automatisierte Phishing-Antwort: Diese Vorlage dient der Automatisierung der Phishing-Antwortaufgaben und enthält eine Reihe von Aktionen, einschließlich eines Auslösers.
- Security Incident – manuelle Phishing-Vorlage: Diese Vorlage ist der vorhandene manuelle Phishing-Antwort-Workflow. Legen Sie die Kategorie auf Phishing fest, um den Flow zu aktivieren.

Diese Vorlagen enthalten eine Sequenz wiederverwendbarer Aktionen, die auf Phishing-Angriffe reagieren sollen. Jeder Flow hat einen Auslöser (Bedingung), eine Sequenz von Aktionen und Subflows, die Sie zur Lesbarkeit kommentieren können. Um auf diese Flows zuzugreifen, müssen Sie installieren Security Operations-Spoke .

Hinweis:
Aktivieren Sie diese Vorlagen, bevor Sie sie verwenden können. Siehe Aktivieren Sie einen Security Incident Response-Flow Für Details.

- Bedrohungssuchen für erkennbare Elemente ausführen: Führt Bedrohungssuchen ausgewählter erkennbarer Elemente durch.
- Erkennbare Elemente anreichern: Ermöglicht das Anreichern erkennbarer Elemente mit zusätzlichen Informationen aus verschiedenen Quellen.
- Auswirkung auf Phishing-E-Mails bewerten: Ermöglicht Ihnen, die Auswirkungen der Phishing-E-Mail zu bewerten. Wenn Sie eine E-Mail an die Phishing-E-Mail-Adresse erhalten, analysiert dieser Subflow den EML-Anhang und vergleicht die Informationen mit den E-Mail-Übereinstimmungsregeln.
- Phishing-E-Mails beseitigen: Ermöglicht Ihnen das Löschen oder Löschen von Phishing-E-Mails, um das Risiko eines bestimmten Angriffs zu reduzieren.
- Sichtungssuche für erkennbare Elemente ausführen: Bestimmt die Verbreitung einer Bedrohung im Zeitverlauf oder testet Korrekturmaßnahmen oder Beseitigungsmaßnahmen.
- Blockanforderungen erstellen: Blockiert die Kommunikation mit erkennbaren Elementen, die dem Incident zugeordnet sind.

Diese Subflows stellen eine Reihe wiederverwendbarer Vorgänge dar, die Sie in mehreren Playbooks verwenden können. Sie können diese Subflows verwenden, um anwenderdefinierte Vorlagen (Flows) entsprechend Ihren Anforderungen zu definieren.

Befolgen Sie zum Erstellen anwenderdefinierter Vorlagen (Flows) die Anweisungen in Flows .

Führen Sie den Playbook-Flow für automatisierte Phishing-Antworten aus

Mit dem Flow Designer können Sie Aufgaben im Playbook definieren und automatisieren, um Phishing-Angriffe auf Ihre Organisation zu analysieren und zu lösen.

Vorbereitungen

- Erforderliche Rolle: sn_si.admin, Flow_Designer und action_Designer
- Installieren und konfigurieren Sie die folgenden Integrationen mit den richtigen Anmeldeinformationen:
  - Anforderung Blockieren (Security Operations Palo Alto Networks NGFW-Integration)
  - Ergänzung erkennbarer Elemente
  - Sichtungssuche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bedrohungssuche
- Microsoft Office Exchange

Warum und wann dieser Vorgang ausgeführt wird

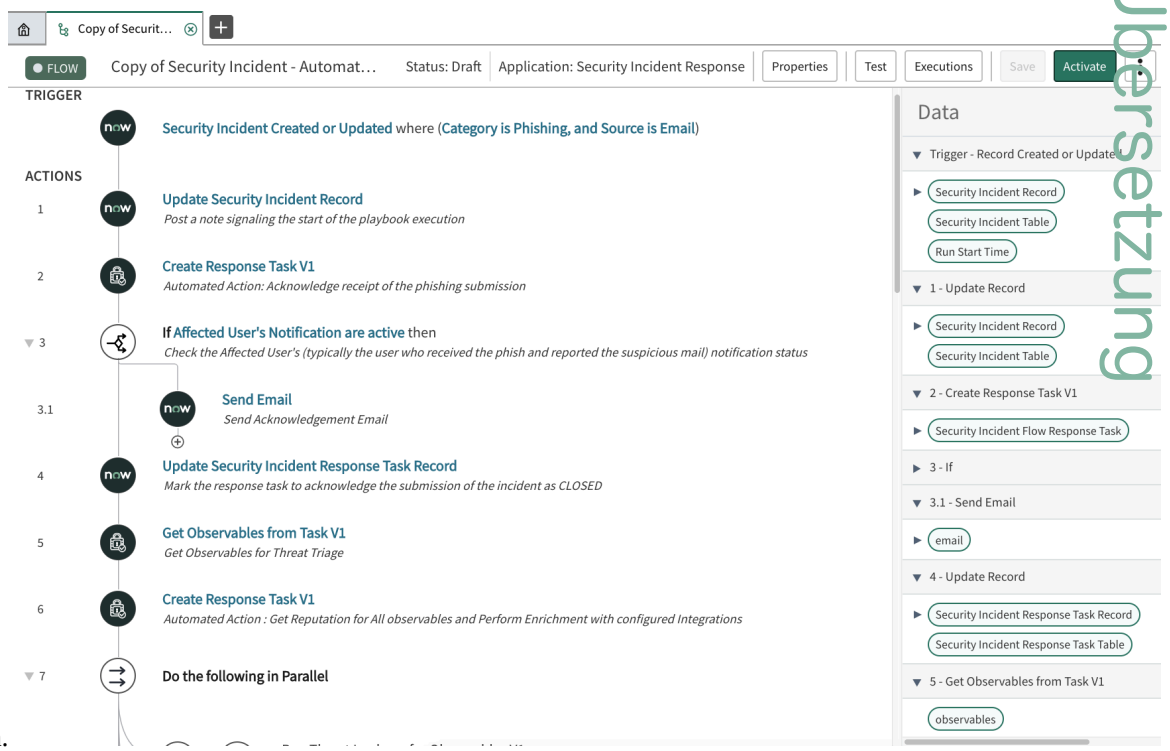
Wenn Mitarbeiter eine verdächtige E-Mail erhalten, die die allgemeinen Anzeichen eines Phishing-Angriffs enthält (wie in Ihren Sicherheitsrichtlinien definiert), können sie sie sie als EML-Anhang an die von Ihrer Organisation definierte Phishing-E-Mail-Adresse senden. Mit den im Flow des automatisierten Phishing-Playbooks definierten Aufgaben können Sie eine Phishing-Bedrohung selektieren, analysieren, eindämmen und beseitigen. Diese Aufgaben können als Teil verschiedener Incident-status aufgerufen werden (z. B. „Analyse“, „Einhalten“ usw.). Wenn ein Phishing-Security Incident erstellt wird, kann der automatisierte Phishing-Flow automatisch ausgelöst werden. Mit Flow Designer können Sie die Details der verschiedenen Aktionen zur Reaktion auf Incidents anzeigen, während sie aufgerufen werden.

Hinweis:
Der Playbook-Flow „Security Incident – automatisierte Phishing-Antwort – Vorlage V1“ ist schreibgeschützt. Sie können eine Kopie des Flows erstellen und nach Bedarf Änderungen vornehmen.

Die folgenden Schritte beschreiben, wie Sie eine Kopie der Phishing-Playbook-Vorlage erstellen, und führen Sie durch einige der Aufgaben im Flow.

Prozedur

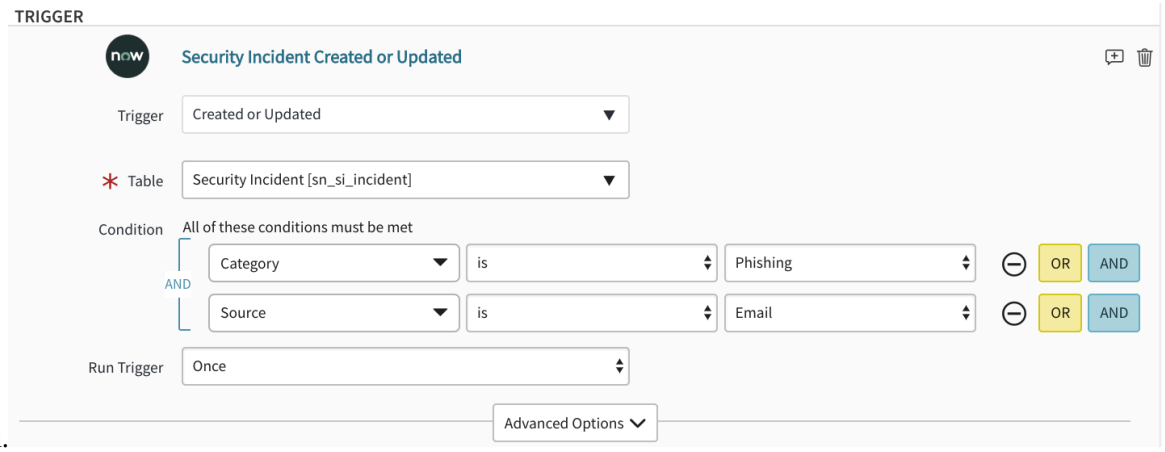
1. Navigieren zu **Alle** > **Flow Designer** > **Designer** Zum Anzeigen der mit verfügbaren Flows Security Operations Spoke.
2. Klicken Sie auf **Security Incident: Vorlage für automatisierte Phishing-Antwort VI** Link.
3. Klicken Sie auf der Flow-Seite auf das Symbol mehr , Erstellen Sie eine Kopie des Flows, und öffnen Sie ihn für Ihre Verwendung.
   Sie können die Auslöserbedingungen ändern, Aktionen hinzufügen oder entfernen und andere Änderungen am Flow vornehmen.



Diese Abbildung zeigt die Auslöserbedingungen und die Schritte, die der Flow ausführt. Im rechten Bereich wird der Daten-Flow angezeigt. Klicken Sie auf ein Symbol, um den Schritt zu erweitern und die Details anzuzeigen.

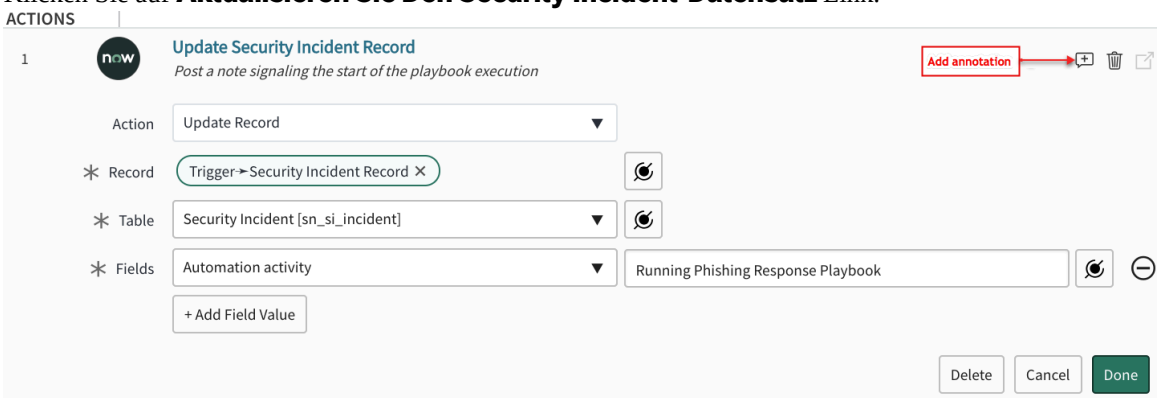
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Auslöser** Symbol.
   Im ersten Schritt definieren oder legen Sie den Auslöser für den Flow fest. Geben Sie die Bedingungen für den Auslöser an und wie oft der Flow den Auslöser ausführen soll.



   Wenn die im Flow definierten Bedingungen (Kategorie ist Phishing und Quelle ist E-Mail) im Incident-Datensatz erfüllt sind, werden die Aufgaben im automatisierten Phishing-Flow sequenziell ausgeführt. Sie können den Auslöser ändern, Anmerkungen hinzufügen, Bedingungen hinzufügen oder löschen usw.

5. Klicken Sie auf **Aktualisieren Sie Den Security Incident-Datensatz** Link.

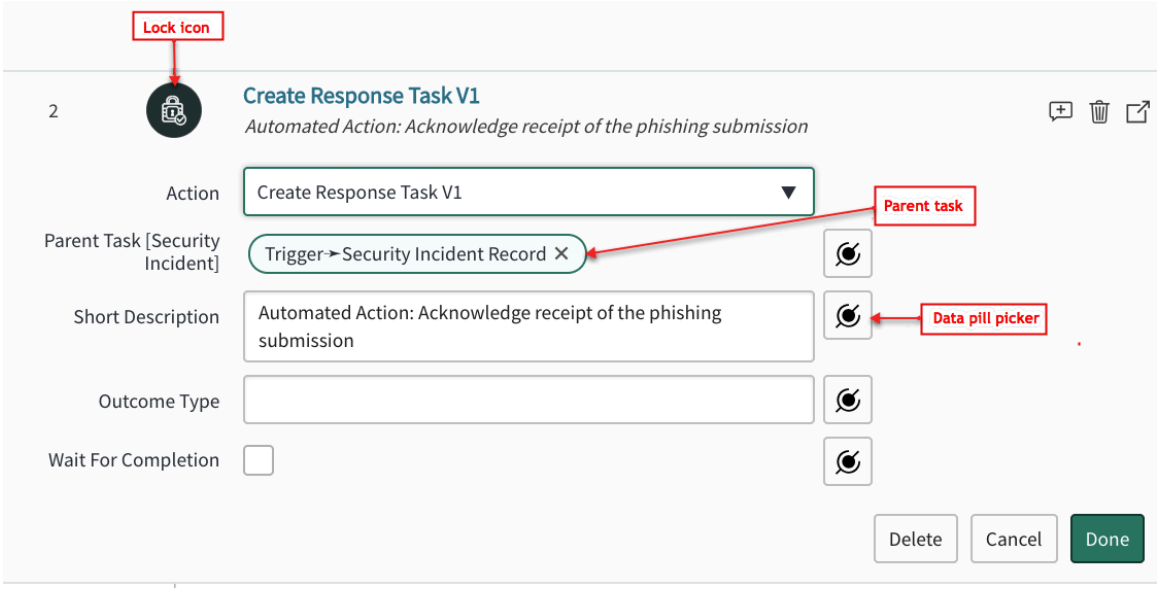


   Die Aktualisierung des Security Incident-Datensatzes ist der erste Schritt im Flow. Klicken Sie auf das Anmerkungssymbol Um dem Sicherheitsanalysten eine Notiz hinzuzufügen, die angibt, dass ein Phishing-Incident aufgetreten ist und der automatisierte Phishing-Playbook-Flow mit der Ausführung begonnen hat.

6. Fahren Sie mit Schritt 2 im Flow fort, und klicken Sie auf **Erstellen Sie Eine Antwortaufgabe** Link.

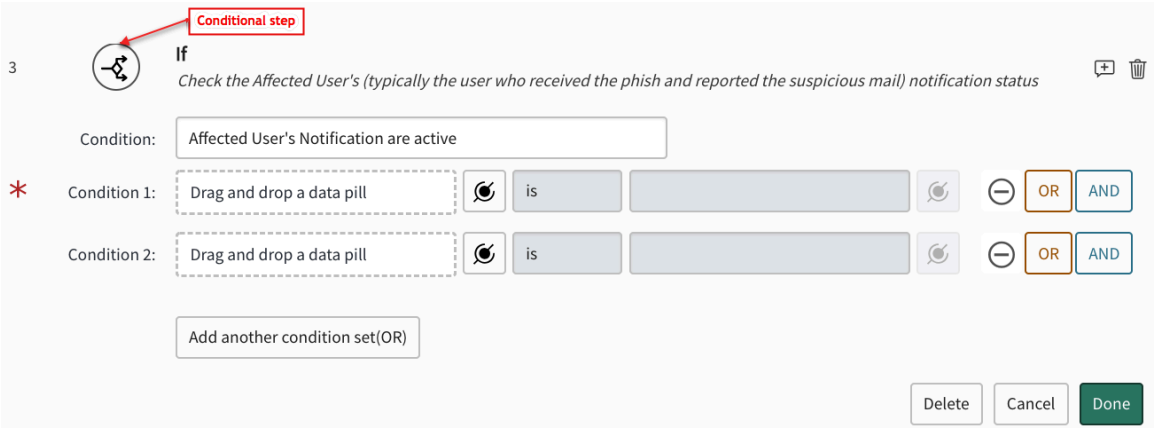
   In diesem Schritt erstellt der Flow eine automatisierte Antwortaufgabe, um den Eingang an den einreichenden Incident oder den betroffenen Anwender zu bestätigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



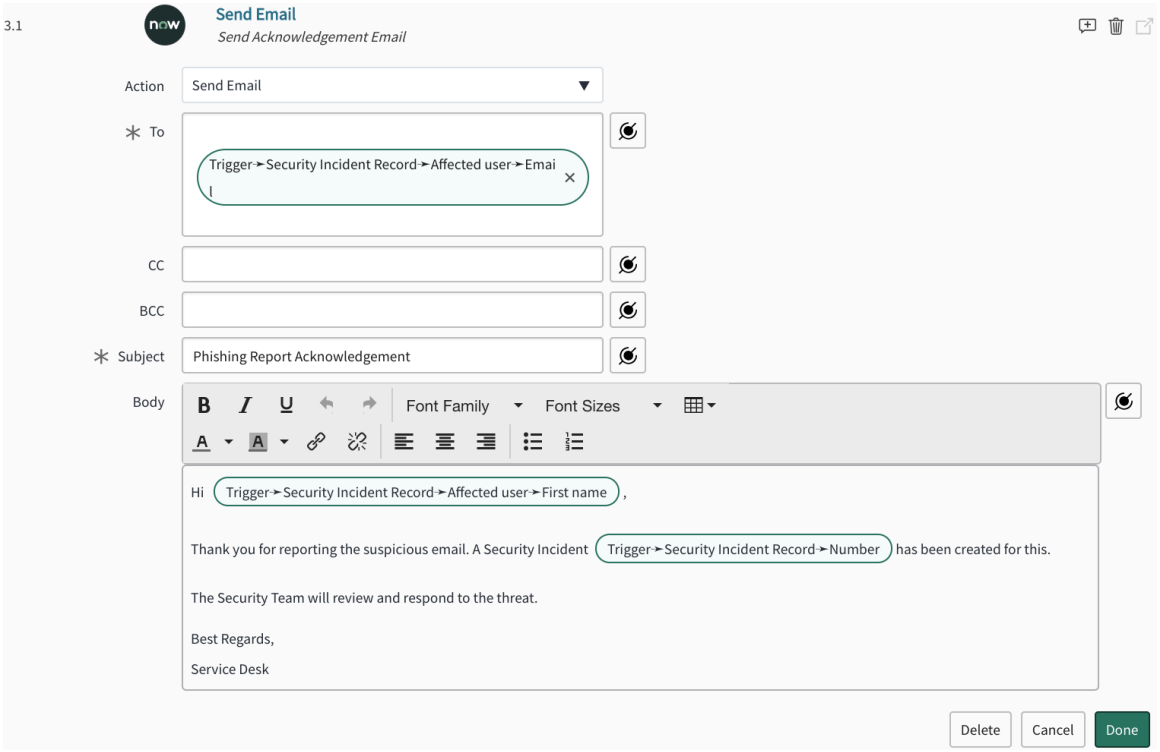
Beachten Sie **Übergeordnete Aufgabe [Security Incident]** Feld verweist auf den übergeordneten Datensatz, der diesem Schritt zugeordnet ist. Sie können einen beliebigen Referenzdatensatz mithilfe des Symbols für die Datenpillenauswahl auswählen Oder ziehen Sie das relevante Referenzelement aus dem rechten Bereich. Beachten Sie das Sperrsymbol . Das Schlosssymbol zeigt an, dass für den Schritt kein Anwendereingriff erforderlich ist.

7. In Schritt 3 erfasst der Flow zusätzliche Details des betroffenen Anwenders (normalerweise des Anwenders, der den Incident übermittelt hat), um sicherzustellen, dass eine Benachrichtigung erfolgreich gesendet werden kann.
Sie können Bedingungen angeben, um zu überprüfen, ob der Status des betroffenen Anwenders aktiv ist und der Anwender Benachrichtigungen erhalten kann.



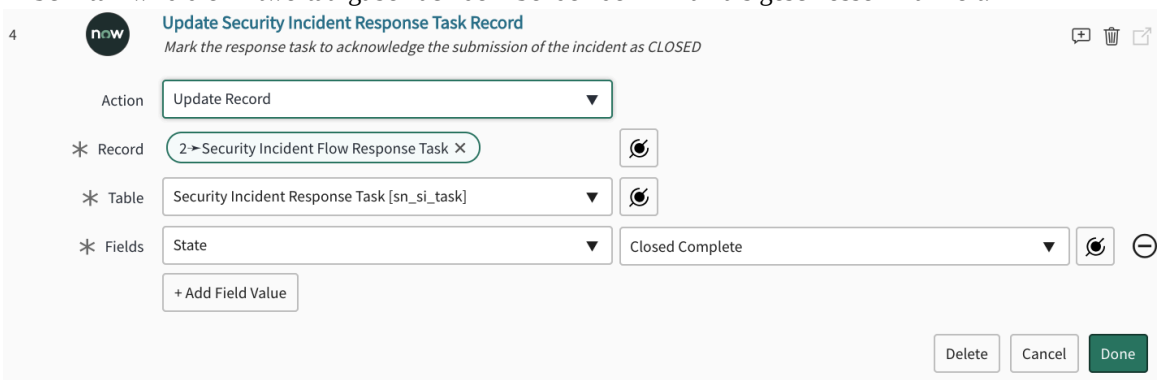
Beachten Sie das Symbol für bedingten Schritt In Schritt 3. Der Flow führt den nächsten Schritt (3,1) nur aus, wenn die angegebenen Bedingungen erfüllt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

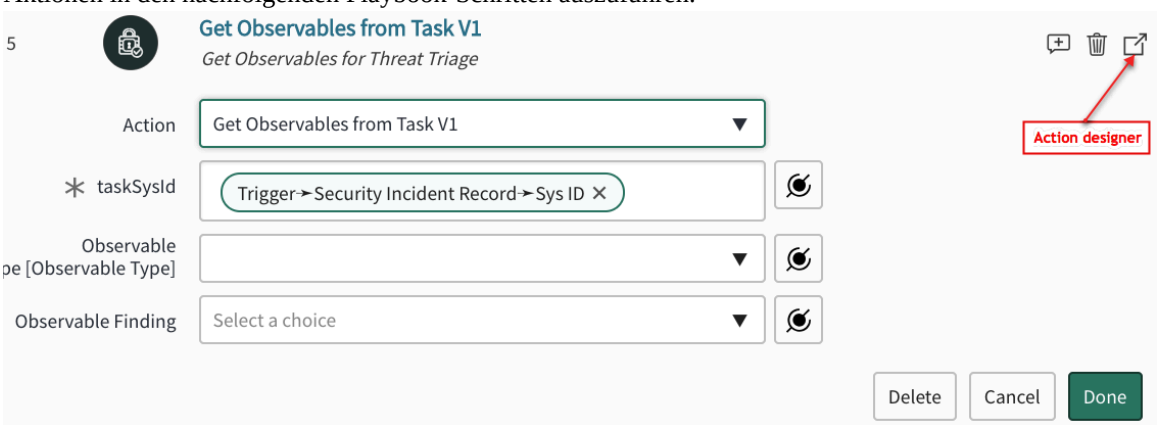


Wenn die in Schritt 3 definierten Bedingungen erfolgreich erfüllt wurden, wird die E-Mail gesendet.

8. In Schritt 4 wird die Antwortaufgabe nach dem Senden der E-Mail als geschlossen markiert.



9. In Schritt 5 werden alle am Incident beteiligten erkennbaren Elemente (z. B. E-Mail-Betreff, E-Mail-Adresse, von der die Phishing-E-Mail gesendet wurde, Phishing-URL) oder erkennbare Elemente, die zu einer ausgewählten Kategorie (Hash, Datei oder Domäne) gehören, gesammelt, um zusätzliche automatisierte Aktionen in den nachfolgenden Playbook-Schritten auszuführen.

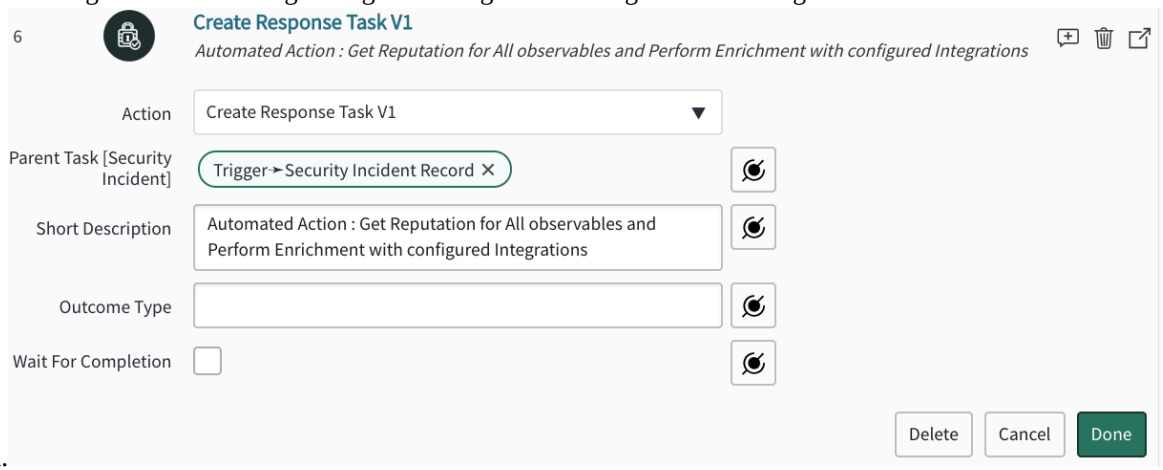


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

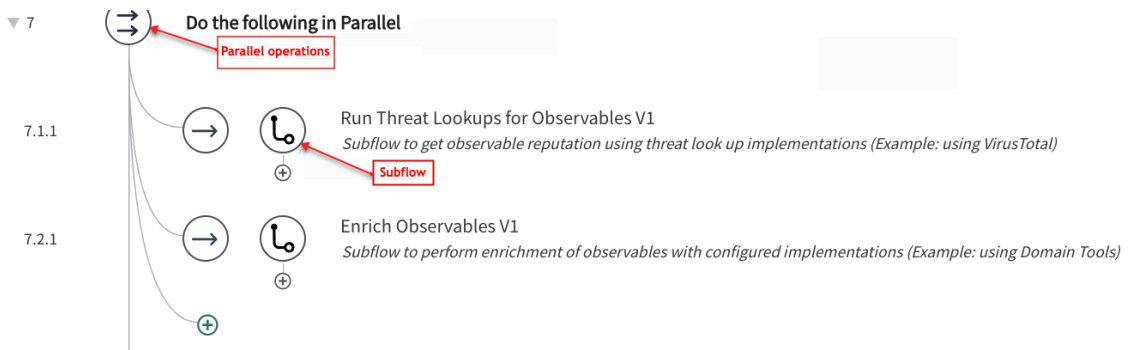
Klicken Sie auf das Aktionsdesigner-Symbol Um eine detaillierte Ansicht der Aktion anzuzeigen.

Um anzuzeigen Aktionsdesigner Erweitern Sie einen Schritt im Flow, und klicken Sie auf das Aktionsdesigner-Symbol.

10. In Schritt 6 wird eine automatisierte Antwortaufgabe erstellt.
Diese Aufgabe erfasst den Beginn des Prozesses, bei dem die Reputation aller erkennbaren Elemente abgerufen und die Ergänzung mit konfigurierten Integrationen durchgeführt wird.

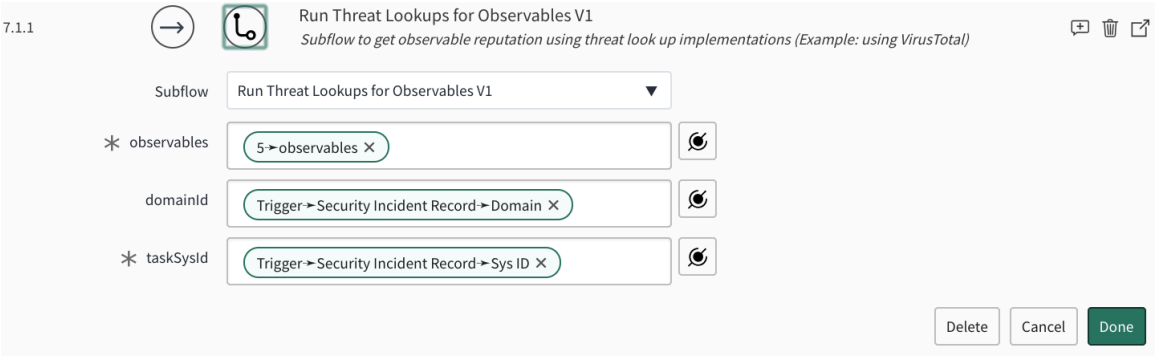


11. In Schritt 7 werden zwei Subflows genannt:
    - Bedrohungssuchen für erkennbare Elemente ausführen: Dieser Subflow wird verwendet, um die Reputation aller erkennbaren Elemente mithilfe von Bedrohungssuche-Implementierungen abzurufen.
    - Erkennbare Elemente anreichern: Dieser Subflow wird verwendet, um die Anreicherung erkennbarer Elemente mit konfigurierten Implementierungen durchzuführen.



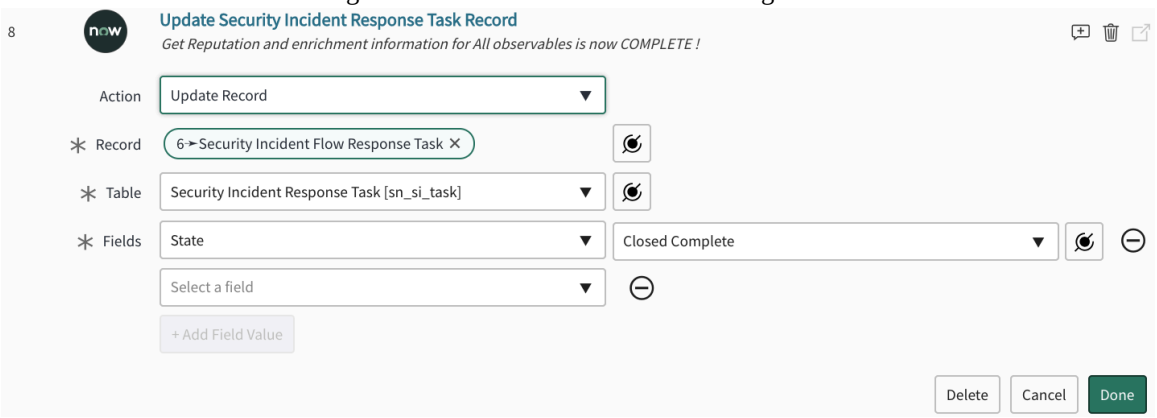
Beachten Sie die Symbole für diese Aufgabe. Das Symbol für parallele Vorgänge Gibt an, dass sowohl die Aufgaben parallel als auch das Subflow-Symbol ausgeführt werden Gibt an, dass die ausgeführte Aufgabe ein Subflow ist, wie unten gezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

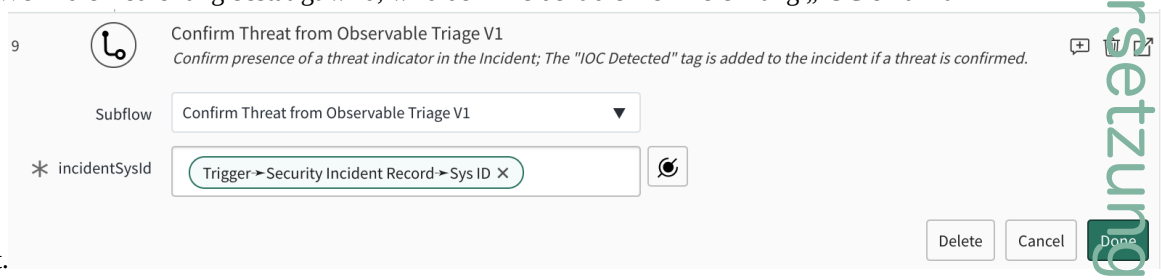


Beachten Sie die Zahl 5 im Feld erkennbare Elemente. Dies gibt an, dass die Bedrohungssuche für erkennbare Elemente ausgeführt wird, die in Schritt 5 abgerufen wurden. Dieser Subflow ruft wiederum vorhandene Workflows und Aktionen auf, wie in angezeigt Subflow-Designer .

12. In Schritt 8 wird die Antwortaufgabe nach Abschluss der Subflows als geschlossen markiert.

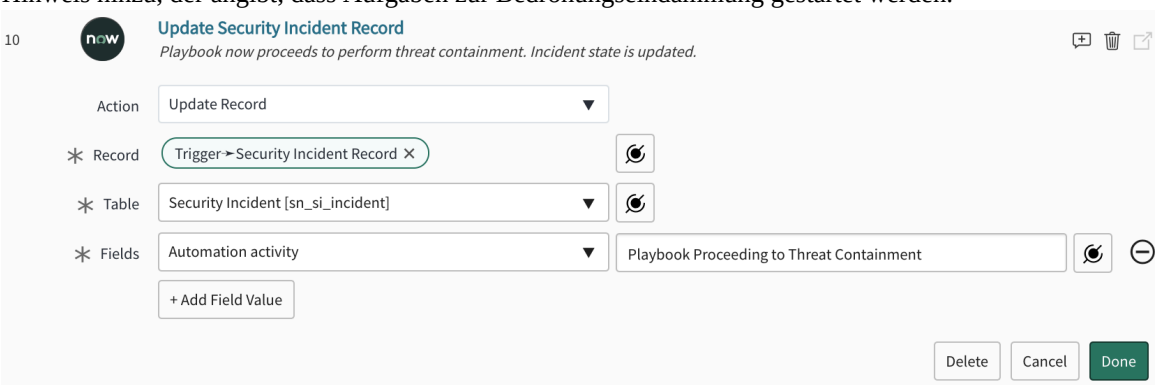


13. In Schritt 9 wird der Subflow „Bedrohung durch Selektierung erkennbarer Elemente bestätigen“ aufgerufen. Dieser Subflow wird verwendet, um das Vorhandensein eines Bedrohungsindikators im Incident zu bestätigen. Wenn die Bedrohung bestätigt wird, wird dem Incident die Kennzeichnung „IOC erkannt“



hinzugefügt.

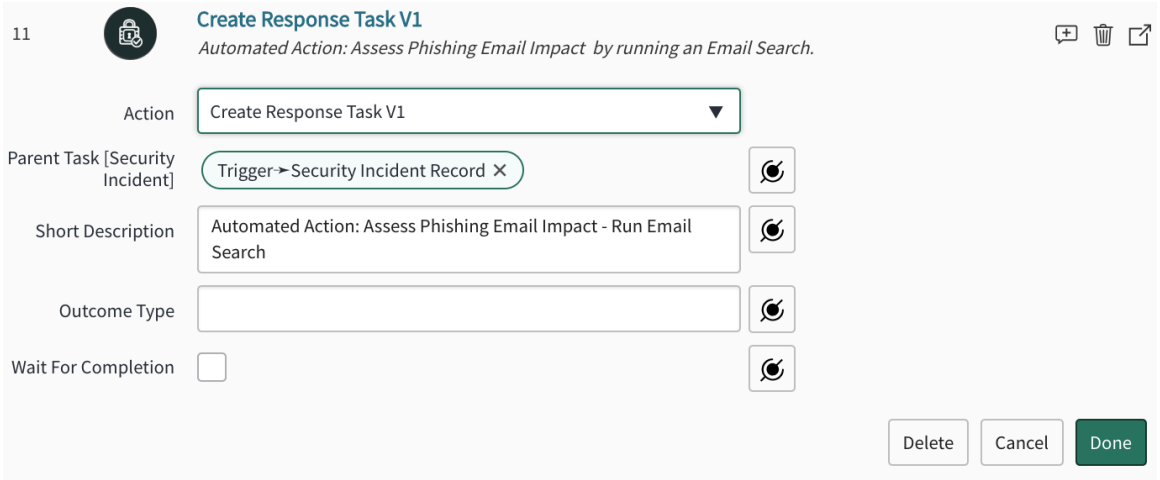
14. Wenn die Bedrohung bestätigt wurde, aktualisieren Sie in Schritt 10 den Security Incident und fügen einen Hinweis hinzu, der angibt, dass Aufgaben zur Bedrohungseindämmung gestartet werden.



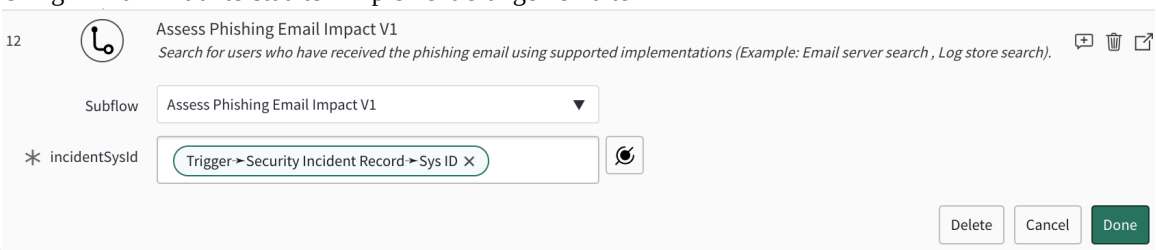
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

15. Schritt 11 ist eine automatisierte Antwortaufgabe, die den Start und Abschluss der Aufgabe erfasst, mit der die Auswirkungen der Phishing-E-Mails bewertet werden.

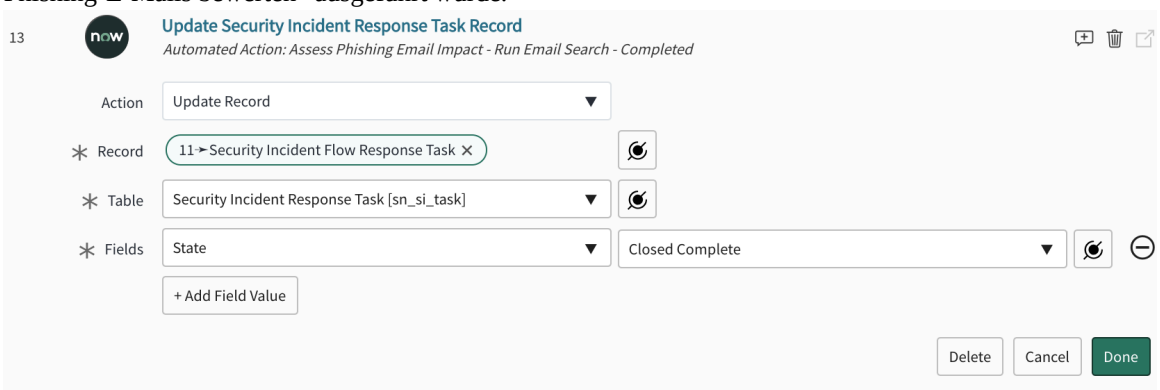


16. In Schritt 12 wird der Subflow Phishing-E-Mail-Auswirkung bewerten aufgerufen. Dieser Subflow wird verwendet, um nach Anwendern zu suchen, die die Phishing-E-Mail mit unterstützten Implementierungen erhalten

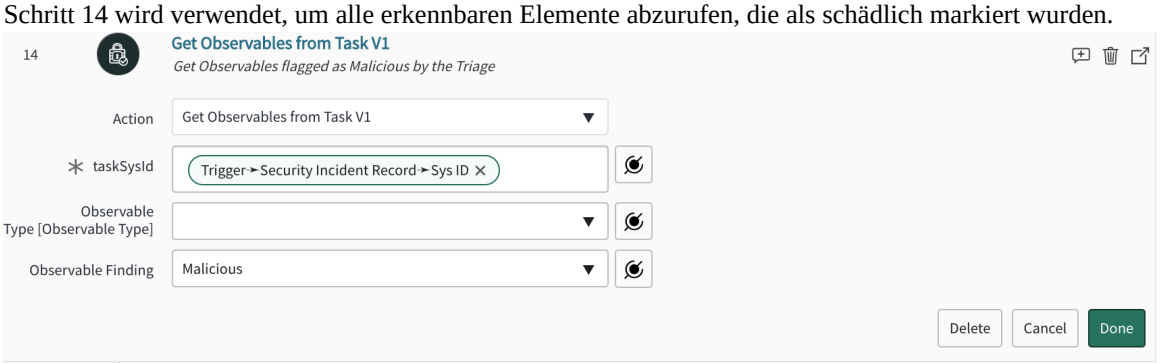


haben.

17. In Schritt 13 wird die Aufgabe als geschlossen markiert, um anzuzeigen, dass der Subflow „Auswirkung auf Phishing-E-Mails bewerten“ ausgeführt wurde.

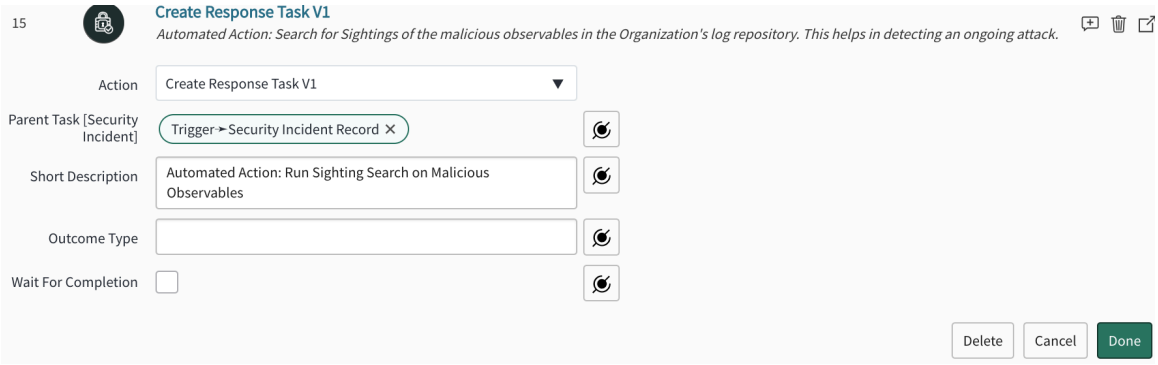


18. Schritt 14 wird verwendet, um alle erkennbaren Elemente abzurufen, die als schädlich markiert wurden.

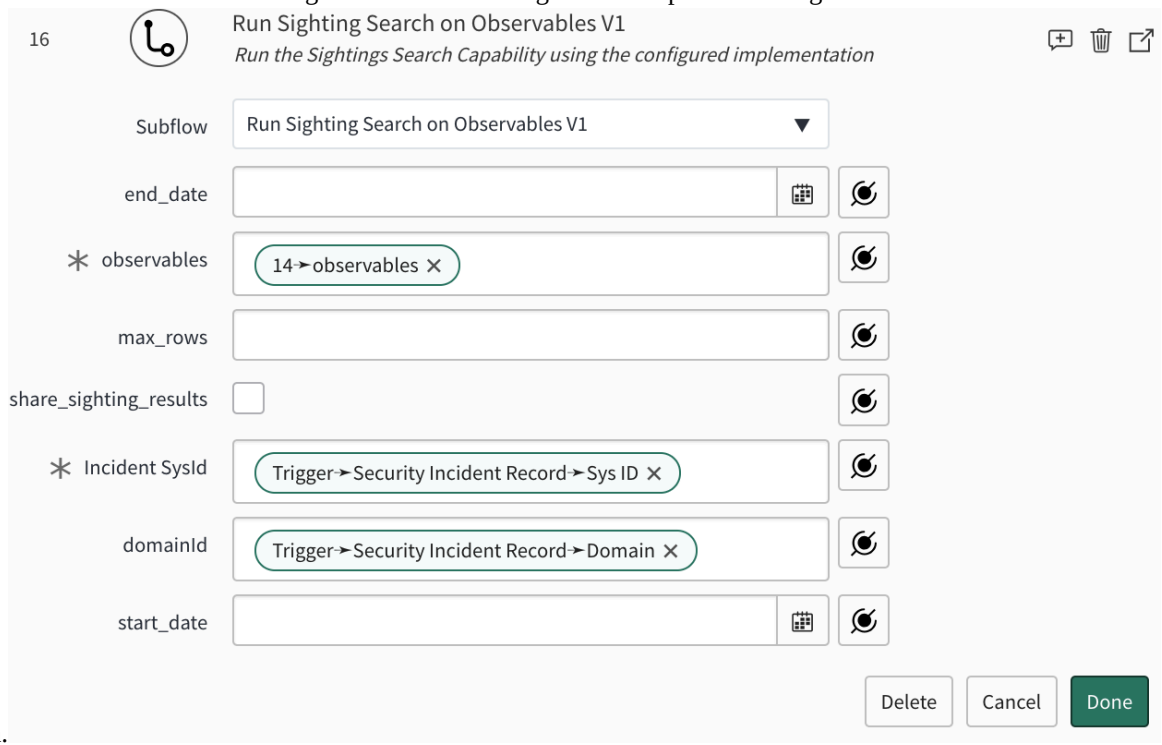


19. Schritt 15 ist eine automatisierte Antwortaufgabe, die den Start und Abschluss der Sichtungssuche nach erkennbaren Elementen erfasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

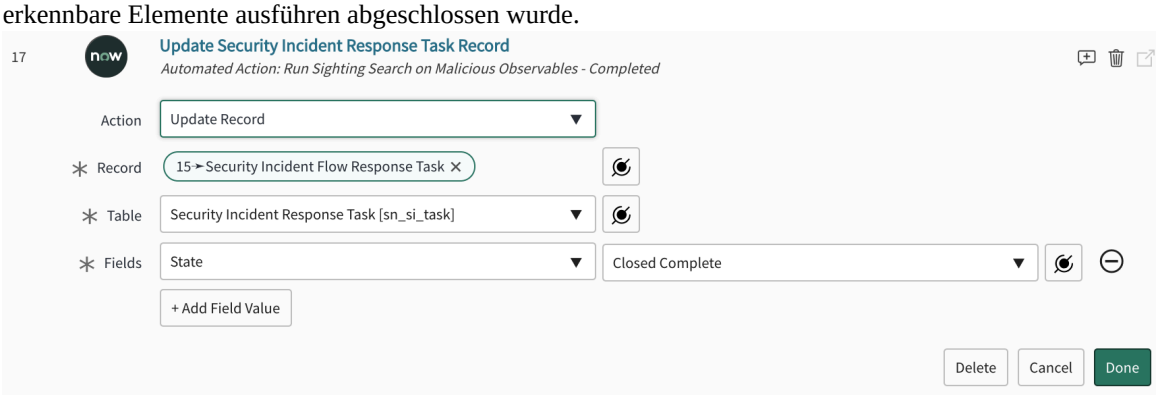


20. In Schritt 16 wird der Subflow Sichtungssuche für erkennbare Elemente ausführen aufgerufen. Dieser Subflow führt eine Sichtungssuche mit der konfigurierten Implementierung



durch.

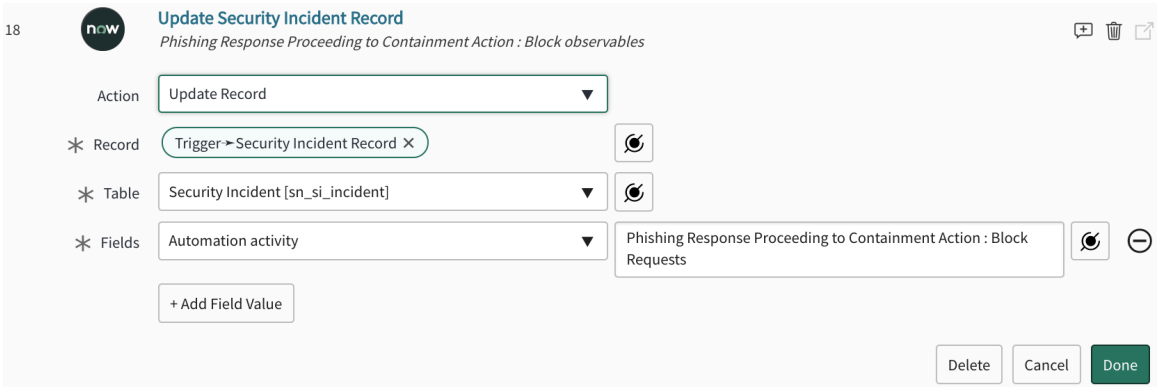
21. In Schritt 17 wird die Aufgabe als geschlossen markiert, um anzuzeigen, dass der Subflow Sichtungssuche für erkennbare Elemente ausführen abgeschlossen wurde.



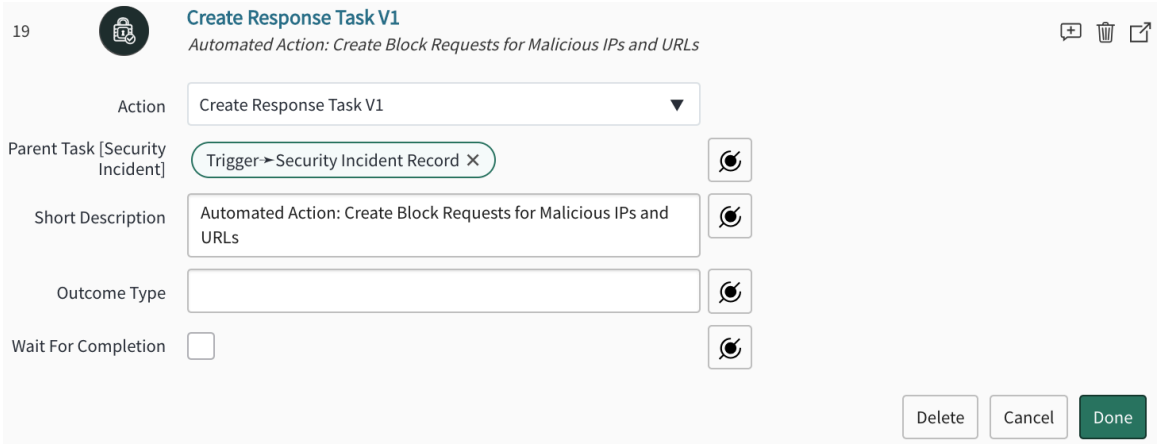
22. Nachdem Sie die schädlichen erkennbaren Elemente identifiziert haben, aktualisieren Sie in Schritt 18 den Security Incident-Datensatz, um anzuzeigen, dass die Eindämmungsmaßnahmen jetzt beginnen.

Automatische Übersetzung

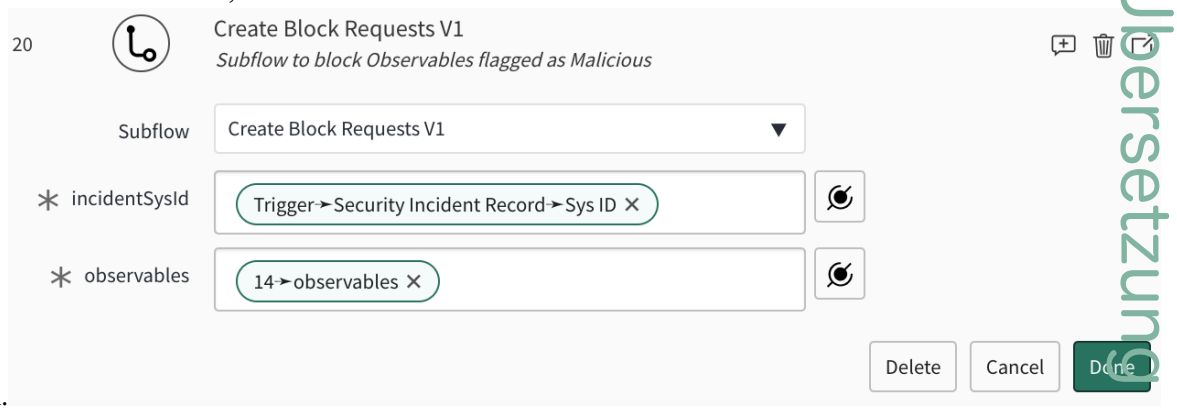
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



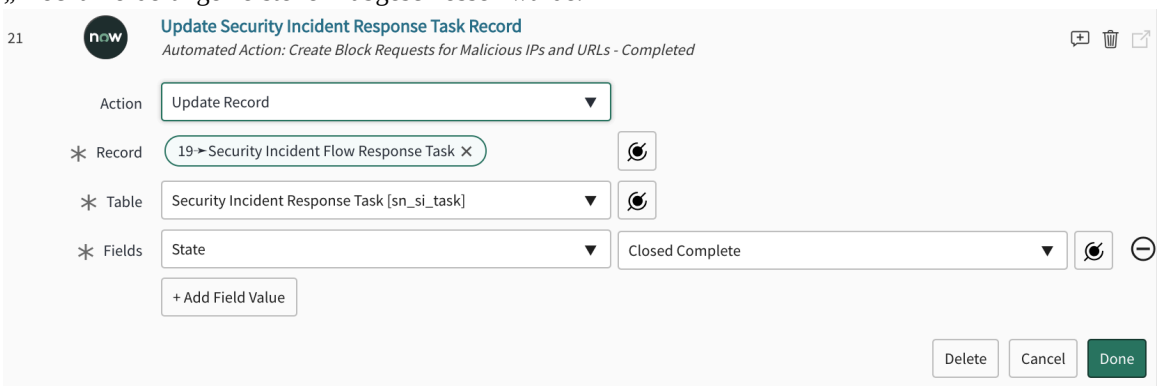
23. Schritt 19 ist eine automatisierte Antwortaufgabe, die den Start und Abschluss der Aufgabe zum Blockieren von Anforderungen erfasst.



24. In Schritt 20 wird der Subflow „Blockanforderungen erstellen“ aufgerufen. Dieser Subflow wird verwendet, um schädliche erkennbare Elemente zu blockieren.



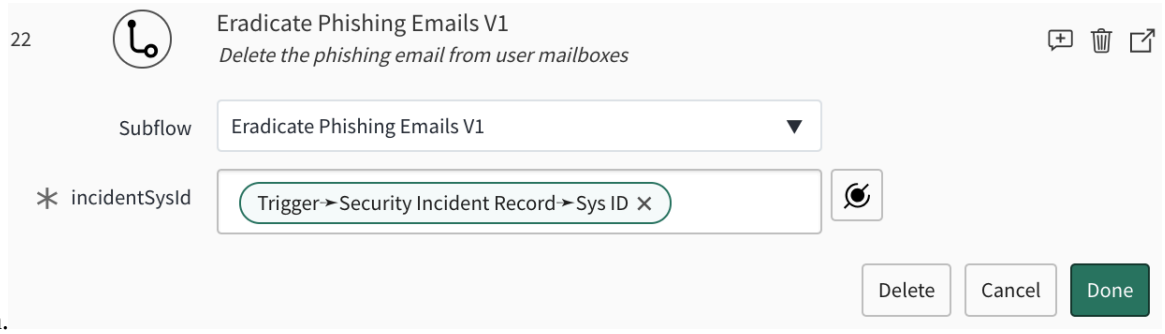
25. In Schritt 21 wird die Aufgabe als geschlossen markiert, um anzuzeigen, dass der Subflow „Blockanforderungen erstellen“ abgeschlossen wurde.



Automatische Übersetzung

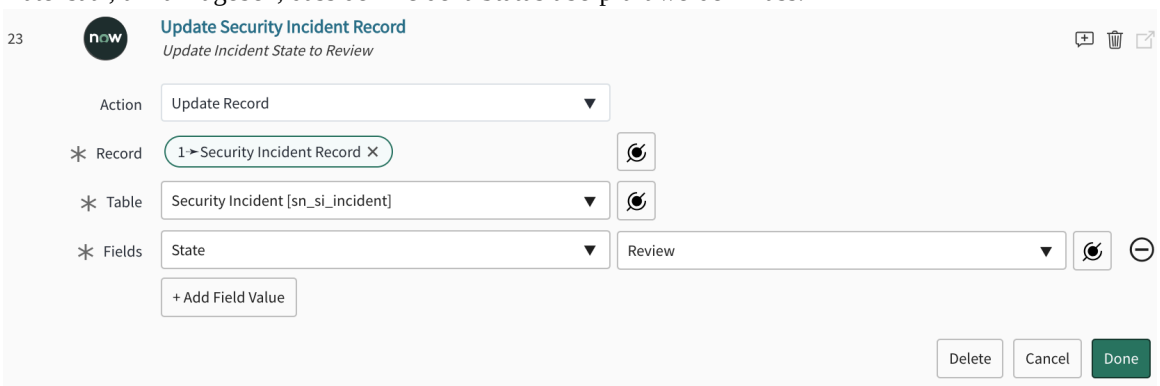
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

26. In Schritt 22 wird der Subflow Phishing-E-Mails löschen aufgerufen.
Dieser Subflow wird verwendet, um Phishing-E-Mails aus Anwenderpostfächern zu

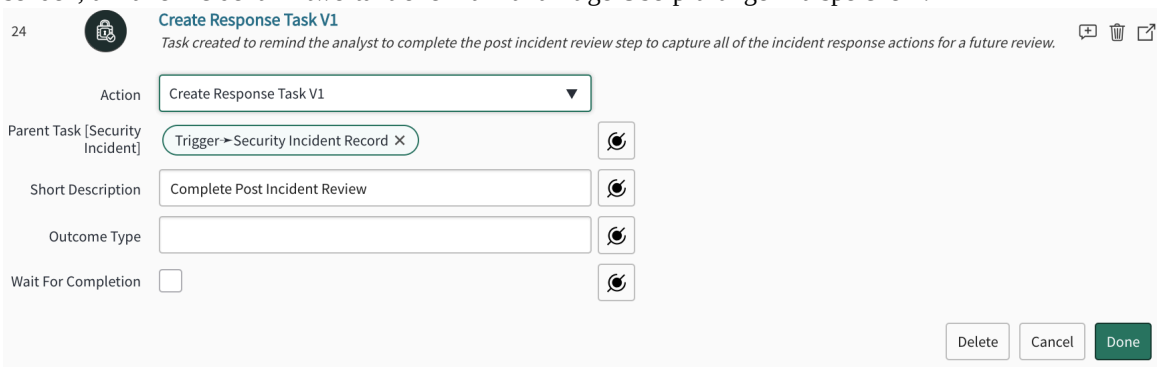


löschen.

27. Nachdem die Phishing-E-Mails gelöscht wurden, aktualisieren Sie in Schritt 23 den Security Incident-Datensatz, um anzugeben, dass der Incident-Status überprüft werden muss.



28. Im letzten Schritt erstellt der Flow eine automatisierte Antwortaufgabe.
Diese Aufgabe wird verwendet, um eine Erinnerung an den Sicherheitsanalysten zu senden, um alle Incident-Antwortaktionen für zukünftige Überprüfungen zu speichern.

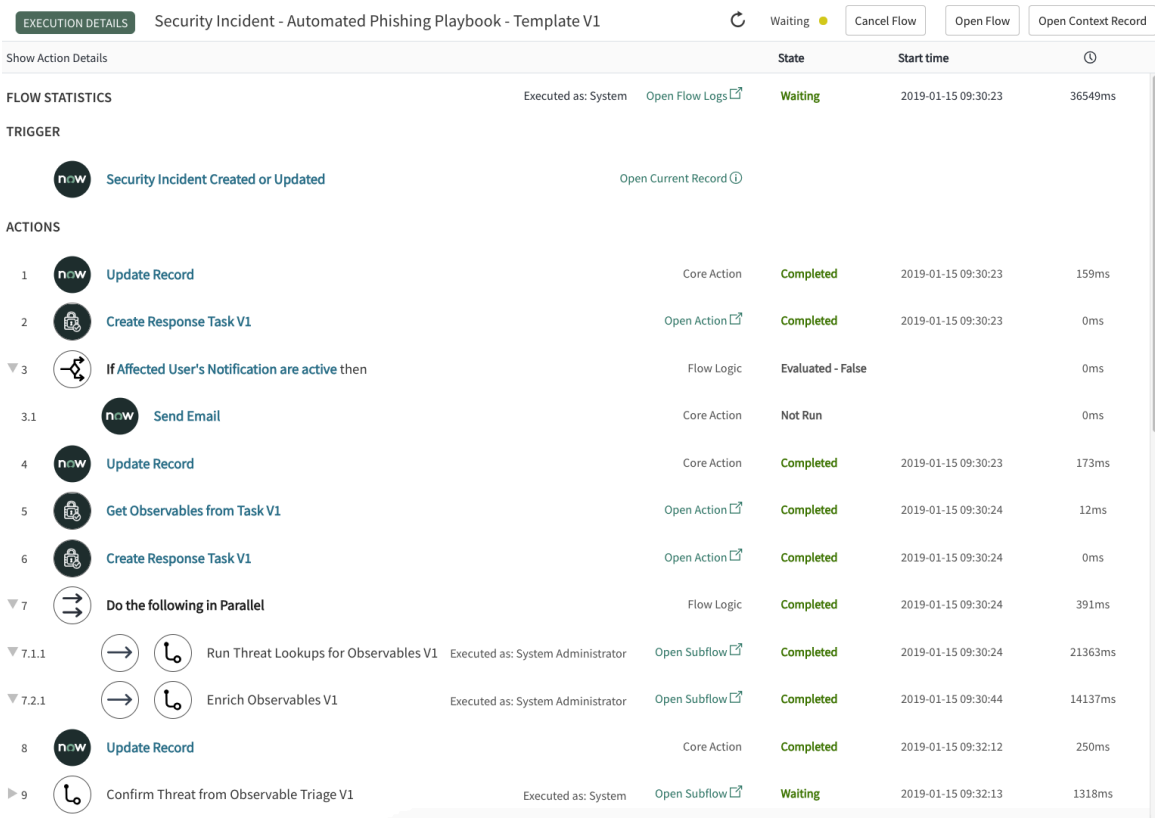


Nächste Maßnahme

Sie können auf klicken **Testen** Um die Aktionen im Flow zu simulieren, bevor Sie ihn veröffentlichen. Klicken Sie nach dem Testen des Flows auf **Aktivieren** Um den Flow zu aktivieren und auszuführen.

Klicken Sie Auf **Ausführungen** Zum Anzeigen der Ausführungsdetails des Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



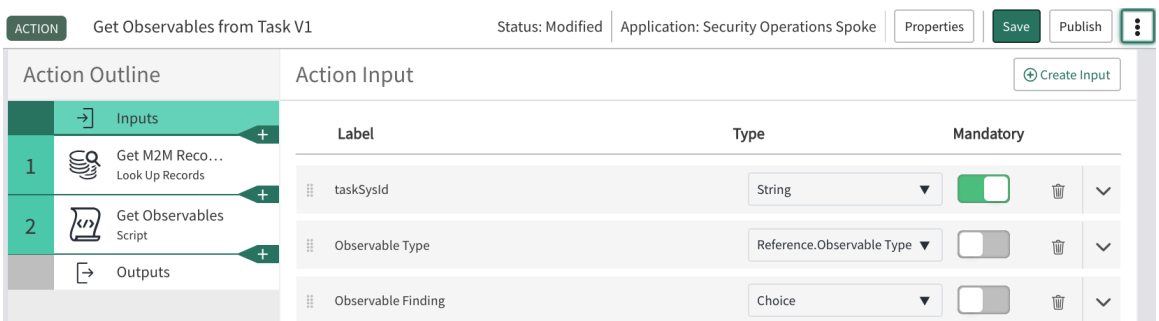
Zeigen Sie den Flow-Aktionsdesigner des Playbooks für automatisierte Phishing-Antworten an

Sie können Detailinformationen zum Aktionsdesigner anzeigen, um detaillierte Informationen zu den Aktionen anzuzeigen, die für einen bestimmten Schritt im Playbook-Flow für automatisierte Phishing-Antworten ausgeführt werden.

Auf dieser Seite wird die Aktionsdesigner-Seite für den Schritt „erkennbare Elemente aus Aufgabe abrufen“ beschrieben. Wählen Sie eine Aufgabe im Bereich Aktionsgliederung aus, um die Details anzuzeigen.

Aktionseingabe

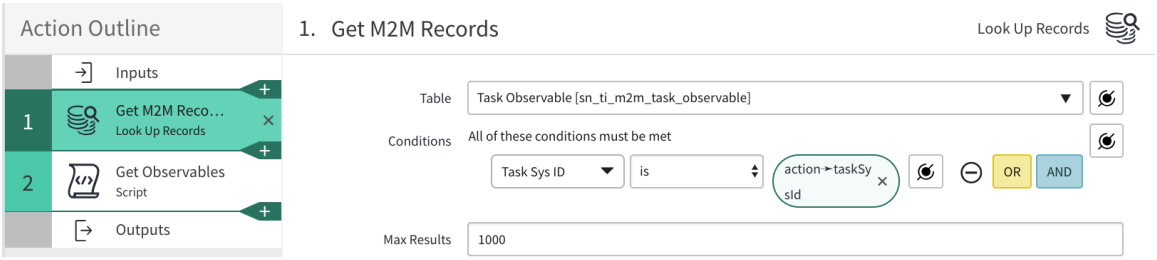
Dieser Abschnitt zeigt Details zur Erstellung der Aktion, einschließlich der Incident-ID, des Typs des erkennbaren Elements (Hash oder IP) und des Ergebnisses erkennbarer Elemente (nur schädliche E-Mails).



M2M-Datensätze abrufen

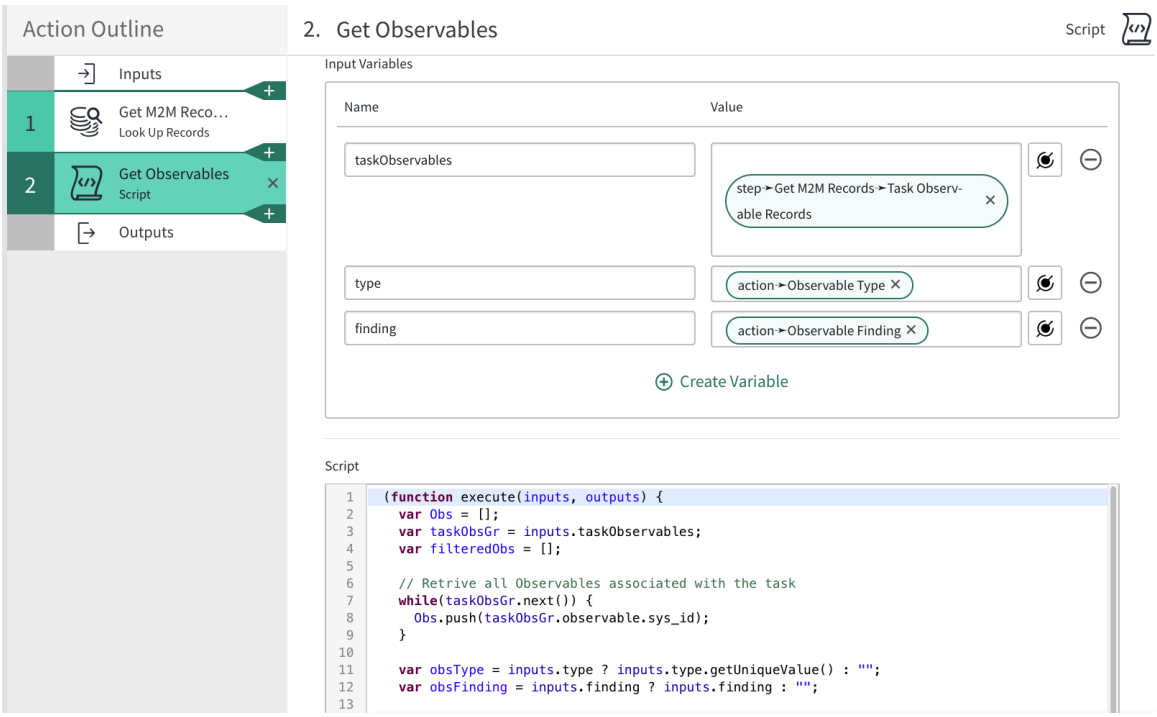
In diesem Abschnitt werden die Bedingungen angezeigt, die für die Suche nach erkennbaren Elementen in einer angegebenen Tabelle definiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Erkennbare Elemente abrufen

In diesem Abschnitt wird das Skript angezeigt, das zum Abrufen erkennbarer Elemente basierend auf den angegebenen Filterbedingungen verwendet wird. Schließlich werden die erkennbaren Elemente, die diese Kriterien erfüllen, und die Anzahl angezeigt.



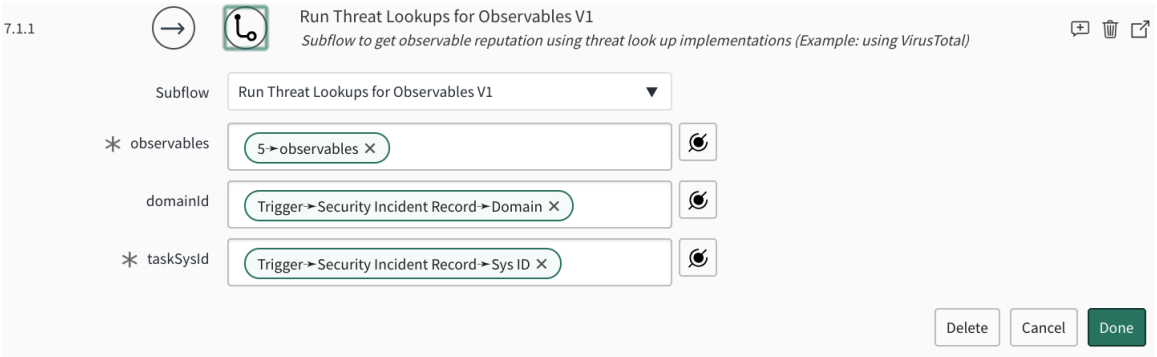
Hinweis:
Alle in diesem Flow definierten Aktionen sind wiederverwendbar und können entsprechend Ihren Anforderungen geändert werden.

Zeigen Sie den Subflow-Designer des Playbooks für automatisierte Phishing-Antworten an

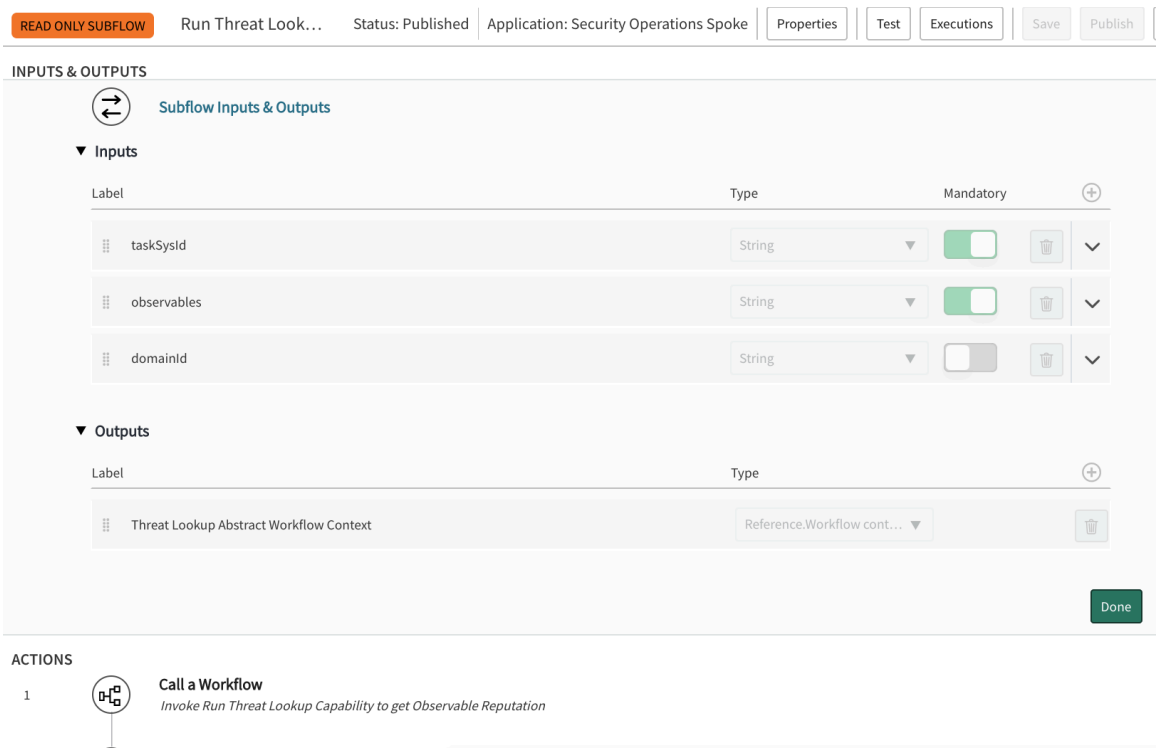
Sie können Detailinformationen zum Subflow-Designer anzeigen, um detaillierte Informationen zum Subflow anzuzeigen, der als Teil des automatisierten Phishing-Antwort-Playbook-Flows ausgeführt wird.

Sie können den Subflow-Designer starten, um zusätzliche Details eines Subflows anzuzeigen. Die Subflow-Designer-Seite für den Subflow „Bedrohungssuchen für erkennbare Elemente ausführen“ wird hier angezeigt. Wählen Sie aus Symbol in der folgenden Abbildung zum Anzeigen des Subflow-Designers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Auf der Seite „Subflow-Designer“ können Sie die Eingaben und Ausgaben für diesen Subflow sowie die zugrunde liegenden Workflow-Aktionen anzeigen, die ausgeführt werden.



Hinweis:
Dieser Subflow ist schreibgeschützt und kann nicht bearbeitet werden. Sie können dem Schritt Subflows hinzufügen oder löschen, den Subflow jedoch nicht ändern.

Playbook für automatisierte Malware

Das automatisierte Malware-Playbook bietet eine Sequenz automatisierter Schritte, mit denen Sie Malware-Warnungen schnell und effizient lösen können.

Verwenden Sie den Malware-Playbook-Flow, um die Schritte für die Verarbeitung von Malware-Warnungen vom Endpunkt oder Netzwerk zu automatisieren. Die Flow-Vorlage enthält Auslöserbedingungen, eine Sequenz von Aktionen und Subflows, die zur Lesbarkeit kommentiert werden.

Diese Vorlagen enthalten eine Sequenz wiederverwendbarer Aktionen, die auf Phishing-Angriffe reagieren sollen. Jeder Flow hat einen Auslöser (Bedingung), eine Sequenz von Aktionen und Subflows, die zur Lesbarkeit kommentiert werden. Um auf diese Flows zuzugreifen, müssen Sie installieren Security Operations-Spoke Und Security Operations Palo Alto Networks: Wildfire-App aus der ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie müssen diese Vorlagen aktivieren, bevor Sie sie verwenden können.

Die folgenden Flows und Subflows sind enthalten:

- Security Incident – Playbook-Vorlage für automatisierte Malware: Diese Vorlage dient der Automatisierung der Antworten auf Malware-Warnungen und enthält eine Reihe von Aktionen, einschließlich eines Auslösers.
- Security Incident – Manuelle Malware-Vorlage: Diese Vorlage ist der vorhandene manuelle Malware-Antwort-Workflow, der aktiviert wird, wenn die Kategorie auf schädliche Code-Aktivität festgelegt ist.

Subflows

- Bedrohung durch erkennbares Element bestätigen: Überprüft, ob die erkennbaren Elemente böswillig sind und behoben werden müssen.
- Incident-Schweregrad festlegen: Legt einen Schweregradstatus für den Incident fest.
- Ransomware-Playbook: Bestimmt, ob es sich um einen Ransomware-Angriff handelt.

Diese Subflows stellen eine Reihe wiederverwendbarer Vorgänge dar, die in mehreren Playbooks verwendet werden können. Sie können diese Subflows verwenden, um anwenderdefinierte Vorlagen (Flows) entsprechend Ihren Anforderungen zu definieren.

Befolgen Sie zum Erstellen anwenderdefinierter Vorlagen (Flows) die Anweisungen in Flows .

Führen Sie den automatisierten Malware-Playbook-Flow aus

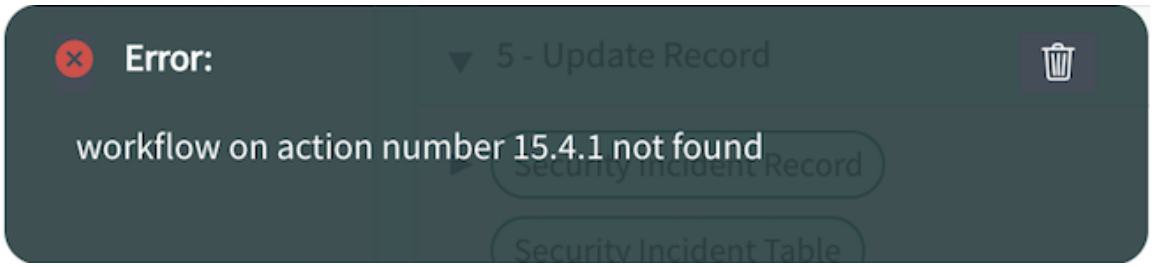
Verwenden Sie diesen Flow, um Aufgaben im Playbook zu automatisieren, um Malware-Angriffe auf Ihre Organisation zu analysieren und zu beheben.

Vorbereitungen

- Erforderliche Rolle: sn_si.admin, Flow_Designer und action_Designer
- Installieren und konfigurieren Sie die folgenden Integrationen mit den richtigen Anmeldeinformationen:
  - Palo Alto Networks Wildfire für Security Operations
  - Sichtungssuche (Splunk)
  - Anforderungen Blockieren
  - Bedrohungssuche
  - Erkennbare Elemente ergänzen

  Vergewissern Sie sich, dass diese Integrationen ordnungsgemäß funktionieren Aktivieren Die Playbook-Vorlage für Security Incident – automatisierte Malware.
- Security Operations Palo Alto Networks Wildfire-App: Um auf den automatisierten Malware-Playbook-Flow zuzugreifen, müssen Sie die App Security Operations Spoke und Security Operations Palo Alto Networks – Wildfire aus dem installieren ServiceNow Store. Wenn die Security Operations Palo Alto Networks Wildfire-App nicht installiert ist, wird der Fehler „Workflow für Aktionsnummer 15.4.1 nicht gefunden“ angezeigt, wie unten gezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie diese App nicht installieren möchten, löschen Sie die Schritte **15.2, 15.3 und 15,4** Aus dem automatisierten Malware-Playbook-Flow.

- Stellen Sie sicher, dass die folgenden Bedingungen erfüllt wurden:
  - Der Security Incident wurde einem Sicherheitsanalysten zugewiesen, der der entsprechenden Genehmigungsgruppe angehört.
  - Der Sicherheitsanalyst, der den Incident bearbeitet, muss über eine gültige E-Mail-Adresse verfügen.
  - Die erforderlichen Konfigurationselemente und erkennbaren Elemente wurden dem Security Incident hinzugefügt.
- Für **Schritt 21 (Genehmigung anfordern)** , Ändern Sie die Gruppe von **Security Incident-Zuweisung** An Ihre bevorzugte Gruppe.
- Schritt 21 des Flows ist ein obligatorischer Aufgabengenehmigungsschritt, bei dem eine Genehmigungsanforderung an den Administrator gesendet wird. Um die Anforderung zu genehmigen, muss der Administrator zur Seite „Aufgabengenehmigungen“ navigieren und das Feld Status auf festlegen **Genehmigt** . Wenn die Aufgabe nicht genehmigt wird, kann der Flow Designer nicht fortfahren, und der Prozess endet.

Warum und wann dieser Vorgang ausgeführt wird

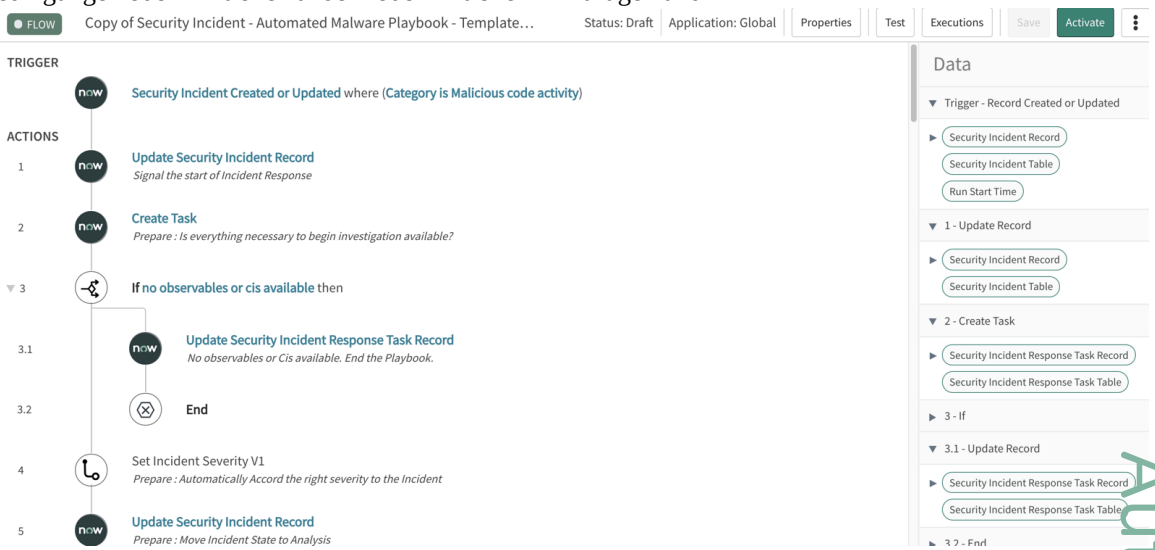
Wenn eine schädliche Codeaktivität im Netzwerk erkannt wird, wird ein Security Incident erstellt, und der automatisierte Malware-Playbook-Flow wird gestartet. Sie können die im automatisierten Malware-Playbook-Flow definierten Aufgaben verwenden, um die Bedrohung zu selektieren, zu analysieren, einzudämmen und zu beseitigen.

Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Designer** Zum Anzeigen der mit der Security Operations-Spoke verfügbaren Flows.
2. Klicken Sie auf **Security Incident – automatisierte Malware-Playbook-Vorlage VI** Link.
3. Klicken Sie auf der Flow-Seite auf das Symbol mehr , Erstellen Sie eine Kopie des Flows, und öffnen Sie ihn für Ihre Verwendung.

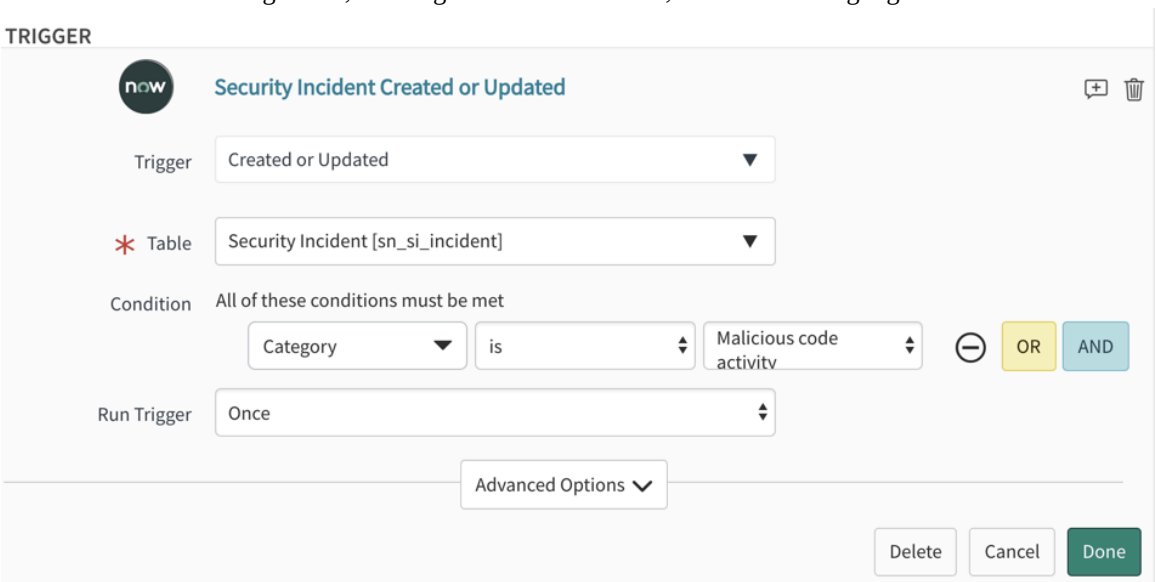
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können jetzt Änderungen an Ihrem Flow vornehmen, z. B. Auslöserbedingungen oder -Aktionen ändern oder Aktionen hinzufügen und entfernen.



Dies zeigt den Auslöser und die Schritte, die mit dem Flow ausgeführt werden. Im rechten Bereich wird der Daten-Flow angezeigt. Klicken Sie auf ein Symbol, um den Schritt zu erweitern und die Details anzuzeigen.

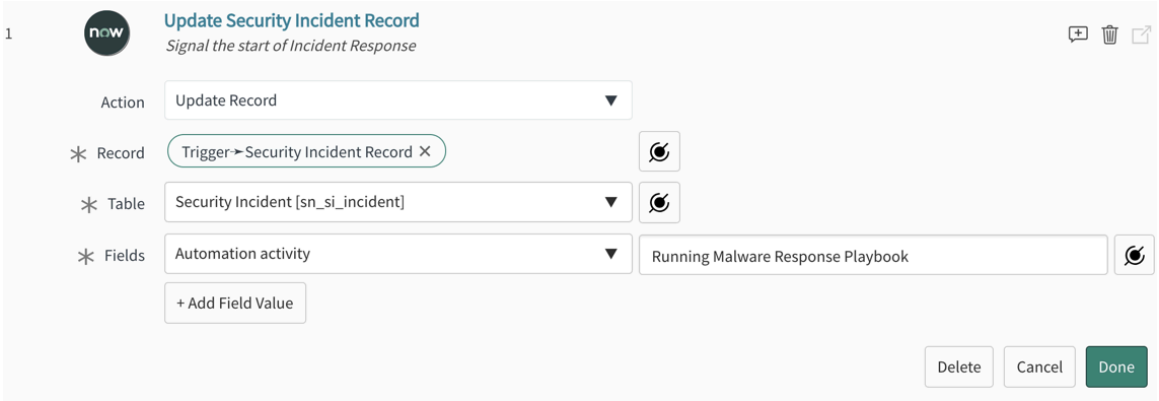
4. Klicken Sie auf **Auslöser** Symbol.
   Im ersten Schritt definieren oder legen Sie den Auslöser für den Flow fest. Geben Sie die Bedingungen für den Auslöser und die Aufgabe an, die ausgeführt werden sollen, wenn die Bedingungen erfüllt sind.



Wenn die im Flow definierte Bedingung (Kategorie ist böswillige Code-Aktivität) im Incident-Datensatz erfüllt ist, werden die Aufgaben im automatisierten Phishing-Flow sequenziell ausgeführt. Sie können den Auslöser ändern, Anmerkungen hinzufügen, Bedingungen hinzufügen oder löschen usw.

5. Der erste Schritt im Flow ist **Aktualisieren Sie Den Security Incident-Datensatz** .

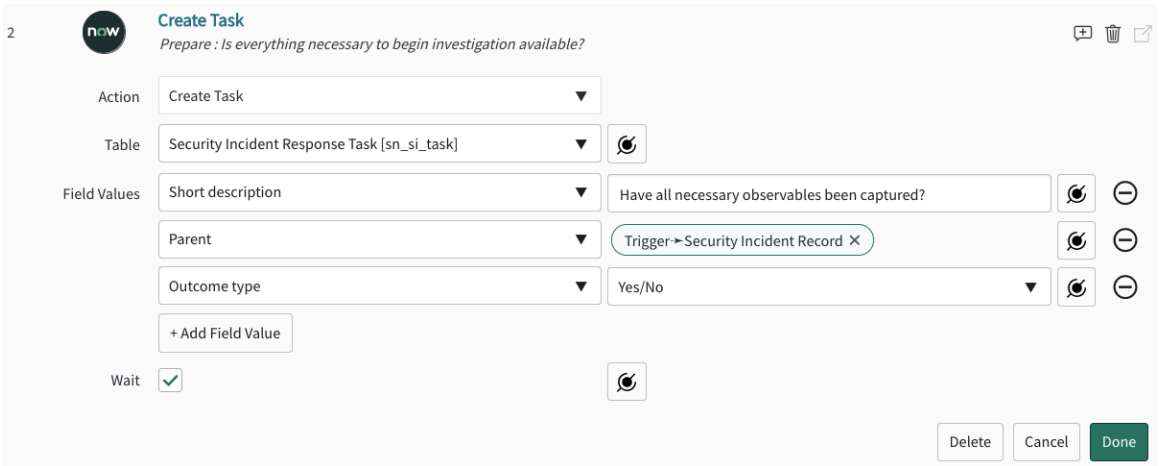
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Klicken Sie auf den Link und dann auf das Anmerkungssymbol Um dem Sicherheitsanalysten eine Notiz hinzuzufügen, die darauf hinweist, dass schädliche Code-Aktivitäten aufgetreten sind und der automatisierte Playbook-Flow für Malware-Antworten mit der Ausführung begonnen hat.

6. Fahren Sie mit Schritt 2 im Flow fort, und klicken Sie auf **Aufgabe Erstellen** Link.

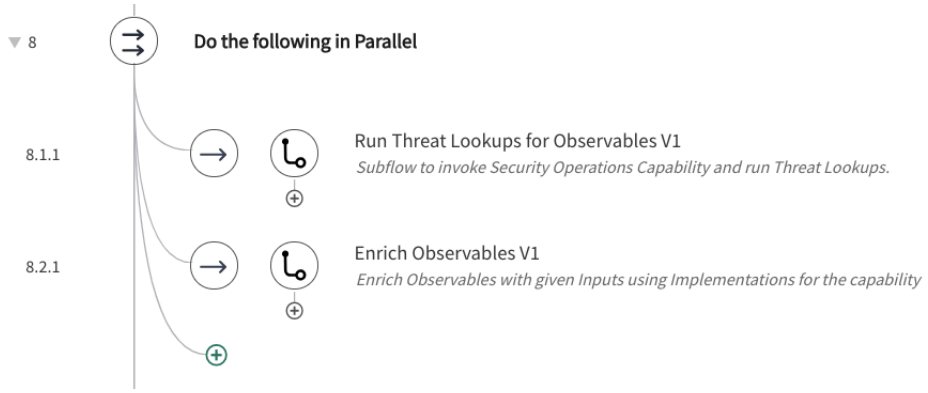
   In diesem Schritt wird eine automatisierte Antwortaufgabe erstellt, um zu überprüfen, ob alle erforderlichen erkennbaren Elemente erfasst wurden und ob die Untersuchung beginnen kann.



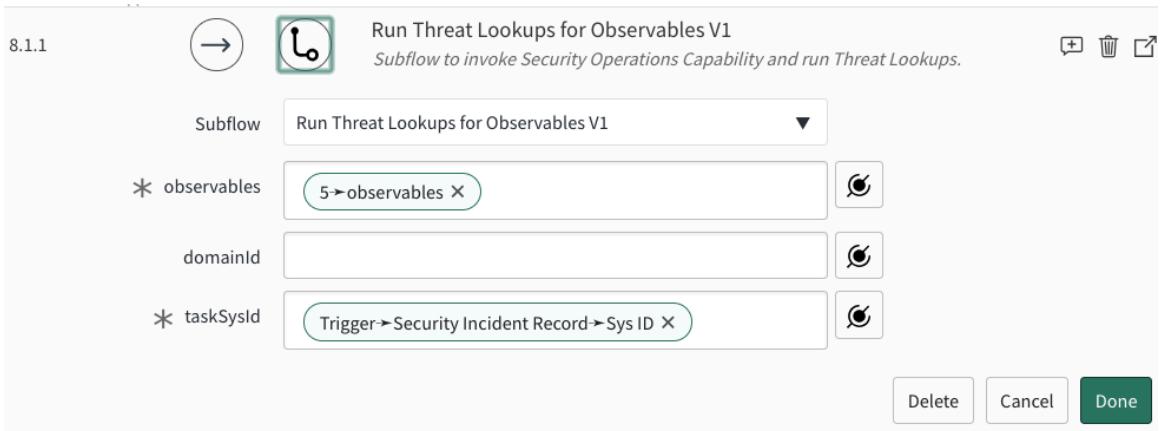
7. Wenn der Ergebnistyp ist **Nein** , Gibt an, dass keine erkennbaren Elemente und CIs zum Initiieren der Untersuchung verfügbar sind.
   Aktualisieren Sie den Security Incident-Datensatz, um anzugeben, dass das Playbook nicht fortfahren kann.
8. Wenn der Ergebnistyp ist **Ja** , Der Subflow „Incident-Schweregrad festlegen“ weist dem Security Incident automatisch den richtigen Schweregrad zu.
9. Im nächsten Schritt wird der Security Incident-Datensatz aktualisiert.
10. Im nächsten Schritt werden alle am Incident oder einer ausgewählten Kategorie beteiligten erkennbaren Elemente erfasst, um in den nachfolgenden Playbook-Schritten zusätzliche automatisierte Aktionen auszuführen.
11. Im nächsten Schritt wird eine automatisierte Antwortaufgabe erstellt.
    Diese Aufgabe erfasst den Beginn des Prozesses, bei dem die Reputation aller erkennbaren Elemente abgerufen und die Ergänzung mit konfigurierten Integrationen durchgeführt wird.
12. In Schritt 8 werden zwei Subflows genannt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bedrohungssuchen für erkennbare Elemente ausführen: Dieser Subflow wird verwendet, um die Reputation aller erkennbaren Elemente mithilfe von Bedrohungssuche-Implementierungen abzurufen.
- Erkennbare Elemente anreichern: Dieser Subflow wird verwendet, um die Anreicherung erkennbarer Elemente mit konfigurierten Implementierungen durchzuführen.



Beachten Sie die Symbole für diese Aufgabe. Das Symbol für parallele Vorgänge Gibt an, dass sowohl die Aufgaben parallel als auch das Subflow-Symbol ausgeführt werden Gibt an, dass die ausgeführte Aufgabe ein Subflow ist, wie unten gezeigt:



Beachten Sie die Zahl 5 im Feld erkennbare Elemente. Dies gibt an, dass die Bedrohungssuche für erkennbare Elemente ausgeführt wird, die in Schritt 5 abgerufen wurden. Dieser Subflow ruft wiederum vorhandene Workflows und Aktionen auf.

13. Im nächsten Schritt wird die Aktion Datensätze suchen ausführen ausgeführt.
Diese Aktion wird verwendet, um Workflow-Kontextdatensätze zu suchen, bei denen die übergeordneten Workflows einer der folgenden sein können.
    - Bedrohungssuche – abstrakter Workflow-Kontext
    - Anreicherung erkennbarer Elemente – abstrakter Workflow-Kontext
14. Im nächsten Schritt werden die Reputation- und Ergänzungsergebnisse für alle 8 Datensätze überprüft.
15. Überprüfen Sie die nächsten Schritte weiter:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Security Incident-Datensatz aktualisieren: Aktualisiert den Security Incident-Datensatz, um anzugeben, dass die Reputationssuche- und Ergänzungsaktivitäten abgeschlossen wurden.

b. Erkennbare Elemente aus Aufgabe abrufen: Ruft alle schädlichen erkennbaren Elemente ab, die dem Security Incident zugeordnet sind.

c. Aufgabe erstellen: Überprüft und bestätigt, ob die automatisierten Selektierungsausführungen erfolgreich waren.

16. Wenn erkennbare Elemente als schädlich gekennzeichnet wurden:

a. Security Incident-Datensatz aktualisieren: Veröffentlichen Sie eine Arbeitsnotiz, die angibt, dass eine Bedrohung erkannt wurde.

b. Eingabeabfrage aus erkennbaren Elementen erstellen: Wenn mehr als zehn erkennbare Elemente als schädlich gekennzeichnet wurden, wird der Subflow „Sichtungssuche nach erkennbaren Elementen“ (in Splunk oder Carbon Black) ausgeführt.

17. Wenn die erkennbaren Elemente nicht als schädlich gekennzeichnet sind, wird der Flow mit den folgenden Schritten fortgesetzt:

a. Security Incident-Datensatz aktualisieren: Veröffentlichen Sie eine Arbeitsnotiz, die angibt, dass keine Bedrohung erkannt wurde

b. Erkennbare Elemente aus Aufgabe abrufen: Identifiziert alle SHA256-Hash-IDs aus dem Incident.

c. Datensätze erkennbarer Elemente suchen: Sucht nach Datensätzen, die diese Kriterien erfüllen.

18. Überprüfen Sie die nächsten Schritte weiter:

a. Für jedes schädliche erkennbare Element **Security Operations Palo Alto Networks – Wildfire-Datenanreicherung Abrufen** Workflow wird ausgeführt.

b. Überprüft die Untersuchungsergebnisse, um festzustellen, ob sie zufriedenstellend sind.
Eine Antwortaufgabe wird erstellt, um zu überprüfen, ob es sich bei der vermuteten Malware um einen Ransomware-Angriff handelt. Wenn ja, wird der Subflow „Ransomware-Playbook“ ausgeführt.

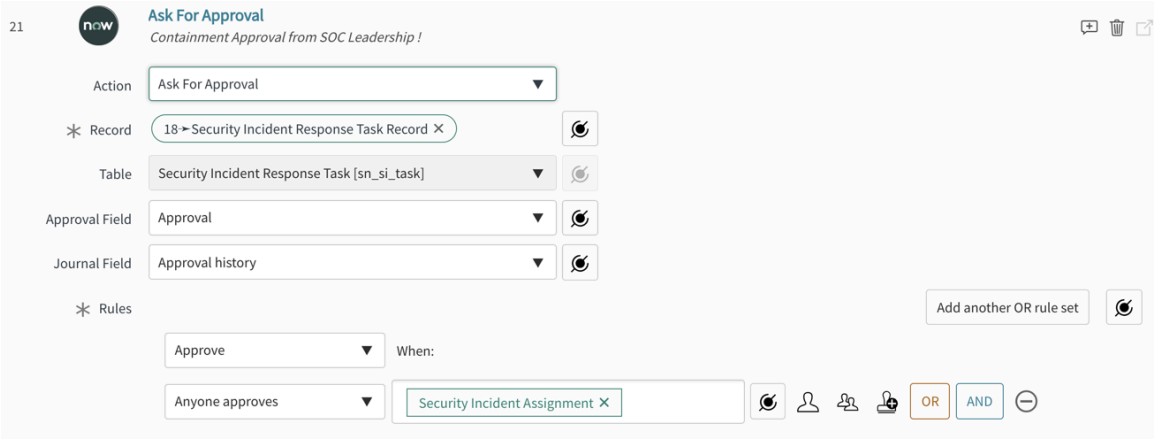
c. Im nächsten Schritt wird eine E-Mail mit einer Zusammenfassung der Analyse und der Anforderung zur Genehmigung zum Initiieren von Eindämmungsverfahren gesendet.

d. Eine Aufgabe wird erstellt, um Details der angeforderten Genehmigung zu erfassen.

e. Der nächste Schritt besteht darin, den Security Incident-Datensatz zu aktualisieren.
Veröffentlichen Sie eine Arbeitsnotiz, die den Sicherheitsanalysten darüber informiert, dass die Genehmigungsanforderung gestellt wurde.

f. Fordert die Genehmigung zur Eindämmung der Malware-Angriffe von Ihrem SOC-Manager an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Wenn vom Flow eine Genehmigungsanforderung generiert wird, wird die Arbeitsnotiz mit der folgenden Nachricht aktualisiert:

Es wurde eine Genehmigungsanforderung für <task id> gestellt, um mit der Eindämmung fortzufahren. Um diese Aufgabe zu genehmigen, führen Sie als SOC-Manager die folgenden Schritte manuell aus:

- Navigieren Sie zur Seite Aufgabengenehmigungen.
- Sie sehen die Liste der Genehmigungen. Klicken Sie auf die <task id>, die genehmigt werden soll.
- Ändern Sie den Status in **Genehmigen** Und speichern Sie die aktualisierte <task id>.

g. Im nächsten Schritt wird der Security Incident-Datensatz aktualisiert, um den Genehmigungsstatus nachzuverfolgen.

h. Als Nächstes wird eine Aufgabe erstellt, um Containment-Verfahren zu initiieren.

i. Der Subflow „Blockanforderungen für schädliche erkennbare Elemente erstellen“ ausführen wird ausgeführt, und ein Incident-Datensatz wird mit einer Anforderung zum Neuaufbau des infizierten Geräts und seiner Assets erstellt.

j. Als Nächstes wird eine Aufgabe erstellt, um die Sichtungssuche auszuführen, um zu bestätigen, ob die Umgebung sicher ist.
Die Sichtungssuche wird wiederholt, bis keine Sichtungen gefunden werden.

k. Als Nächstes wird eine Aufgabe erstellt, die angibt, dass der Security Incident-Datensatz zur Überprüfung bereit ist.

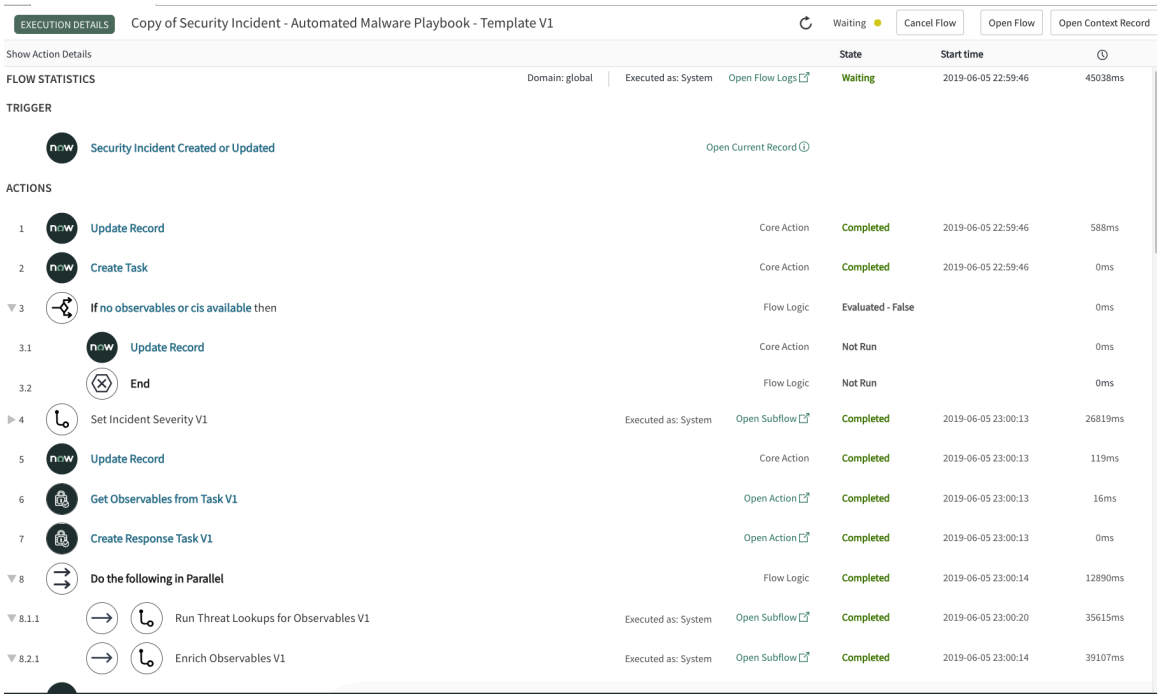
l. Schließlich wird der Datensatz aktualisiert und in die Phase „Überprüfen“ verschoben.

Nächste Maßnahme

Sie können auf klicken **Testen** Um die Aktionen im Flow zu simulieren, bevor er veröffentlicht wird. Klicken Sie nach dem Testen des Flows auf **Aktivieren** Dient zum Aktivieren des Flows, damit er ausgeführt werden kann.

Klicken Sie Auf **Ausführungen** Zum Anzeigen der Ausführungsdetails des Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Playbook für fehlgeschlagene Anmeldung – Handbuch

Wenn ein Anwender bestimmte nicht erfolgreiche Anmeldeversuche (gemäß der SIM-Konfiguration) unternimmt, wird ein Security Incident erstellt.

Diese nicht erfolgreichen Anmeldeversuche können entweder falsch positive Ergebnisse sein oder Versuche von Angreifern sein, Zugriff auf Anwender-E-Mail-Accounts zu erhalten. In solchen Szenarien kann das Playbook „Manuelle fehlgeschlagene Anmeldung“ Anleitungen bieten und dazu beitragen, die Untersuchung fehlgeschlagener Anmelde-Security Incidents zu optimieren.

Voraussetzungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Spoke: Security Operations-Spoke installieren (sn_sec_Spoke)

Wichtige Funktionen

Das Playbook für fehlgeschlagene Anmeldung umfasst die folgenden Funktionen zur Untersuchung von Security Incidents:

1. Überprüft, ob der betroffene Anwender ein aktiver/inaktiver Anwender ist
2. Filtert erkennbare Elemente in der Liste der zulässigen Elemente
3. Bereichert die erkennbaren Elemente
4. Führt eine automatisierte Bedrohungssuche durch.
5. Sendet eine automatisierte E-Mail an den Anwender, um den fehlgeschlagenen Anmeldeversuch zu bestätigen.
6. Weist dem Analysten Aufgaben zu, um den Anwenderzugriff zu untersuchen
7. Identifiziert schädliche erkennbare Elemente und blockiert IPs und URLs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Setzt das Anwenderpasswort zurück.
9. Aktualisiert den Status des Security Incidents
10. Weist einem Sicherheitsanalysten Aufgaben zu, um die Überprüfung nach dem Incident durchzuführen.

Fähigkeiten erforderlich

- Bedrohungssuche (Virensumme, Hybridanalyse)
- Anreicherung erkennbarer Elemente (Whois, ReverseWhois)
- Sichtungssuche (Splunk, QRadar)
- Blockierung erkennbarer Elemente (Prüfpunkt, Palo Alto)

Weitere Informationen finden Sie unter ServiceNow-Store .

Sicherheitsanalysten-Experience

Informationen zur schrittweisen Lösung von Sicherheitsbedrohungen finden Sie unter Lösen Sie Sicherheitsbedrohungen mit dem Playbook.

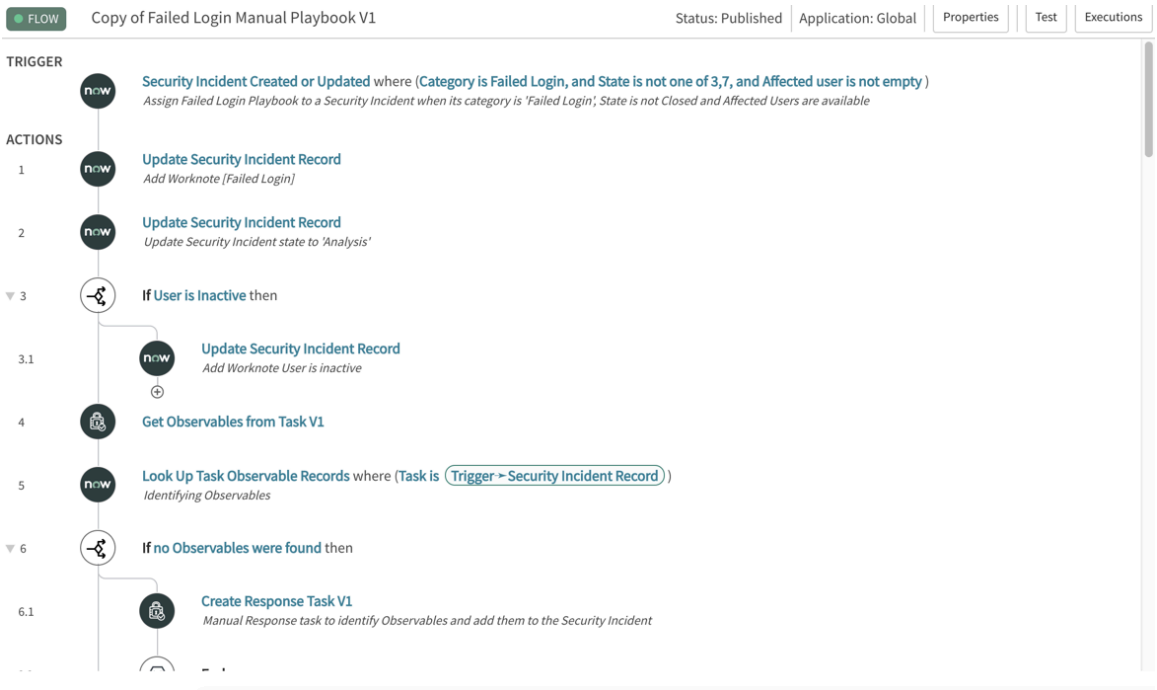
Playbook für fehlgeschlagene Anmeldung mit Flow Designer-Fähigkeiten verwenden

Erste Schritte

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Flow Designer** > **Designer** Und klicken Sie auf **Anmeldung Fehlgeschlagen** playbook.
3. Erstellen Sie eine Kopie der folgenden Flows, um das Playbook für fehlgeschlagene Anmeldung zu kopieren und die erforderlichen Änderungen vorzunehmen. (Dies ist ein optionaler Schritt. Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen daran vorzunehmen).
   - Fehler bei der Anmeldung – Manuelles Playbook V1
   - Fehlgeschlagene Anmeldung: Analysieren Sie die Antwort des Anwenders, und aktualisieren Sie die Antwortaufgabe V1
4. Nehmen Sie die erforderlichen Änderungen entsprechend Ihren Anforderungen vor. (Dies ist ein optionaler Schritt. Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen daran vorzunehmen).
5. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie Änderungen gemäß Ihren Anforderungen vorgenommen haben.

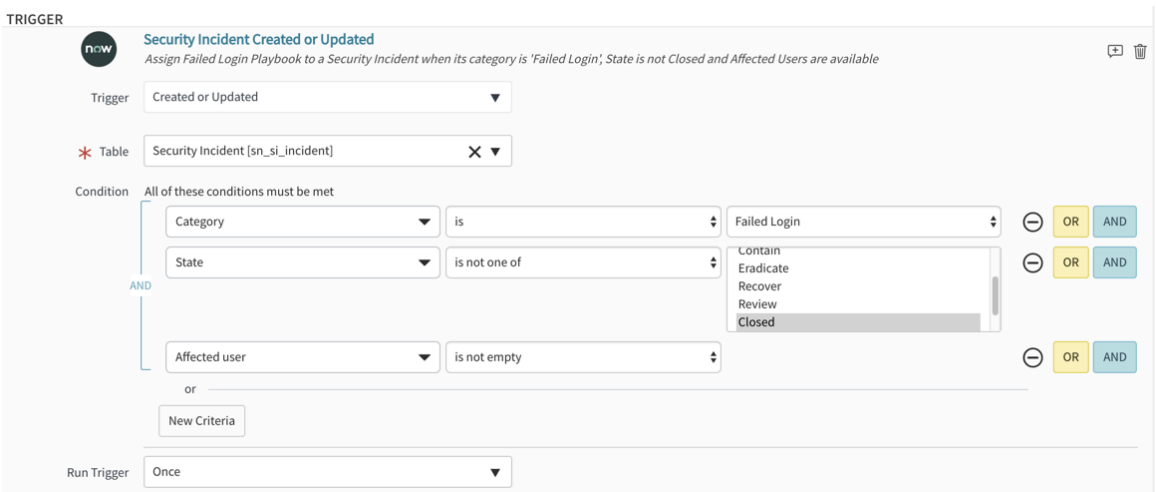
Die folgende Abbildung zeigt eine Kopie des Playbooks „Manuelle fehlgeschlagene Anmeldung“. Überprüfen Sie die folgenden Schritte, um ein Verständnis der verschiedenen Aktionen im Playbook zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:

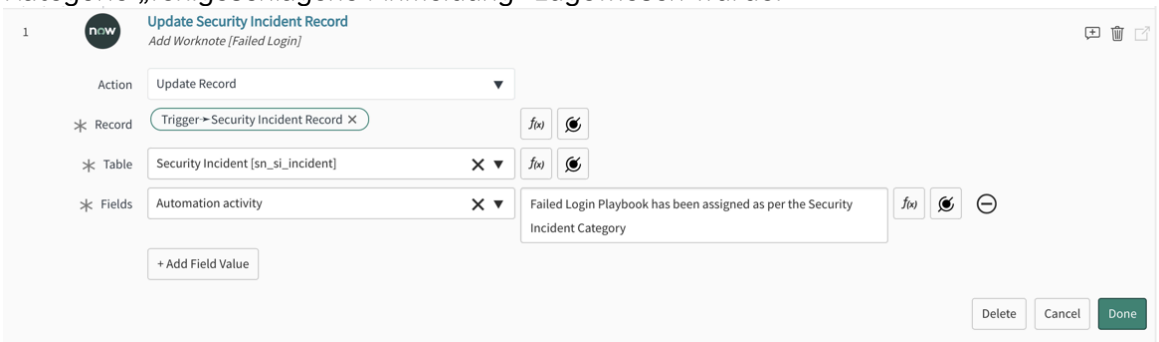
- Kategorie ist „fehlgeschlagene Anmeldung“
- Hat mindestens einen betroffenen Anwender
- Security Incident wurde nicht geschlossen oder abgebrochen



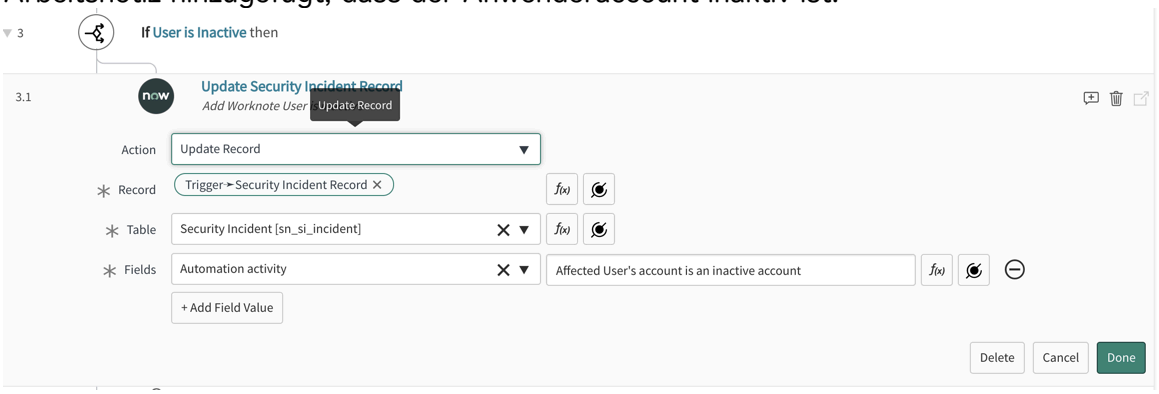
Die folgenden Schritte führen Sie durch die Aktionen, Aufgaben und Subflows, die im Playbook „Manuelle fehlgeschlagene Anmeldung“ verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wenn die Ausführung des Playbooks beginnt, wird das Playbook in Schritt 1 automatisch mit einer Arbeitsnotiz aktualisiert, die anzeigt, dass der Security Incident mit der Kategorie „fehlgeschlagene Anmeldung“ zugewiesen wurde.



2. In Schritt 2 wird das Playbook aktualisiert und in den Status „Analyse“ versetzt.
3. In Schritt 3 überprüft das Playbook, ob der betroffene Anwender ein aktiver oder inaktiver Anwender ist. Wenn der Anwender inaktiv ist, wird dem Security Incident eine Arbeitsnotiz hinzugefügt, dass der Anwenderaccount inaktiv ist.



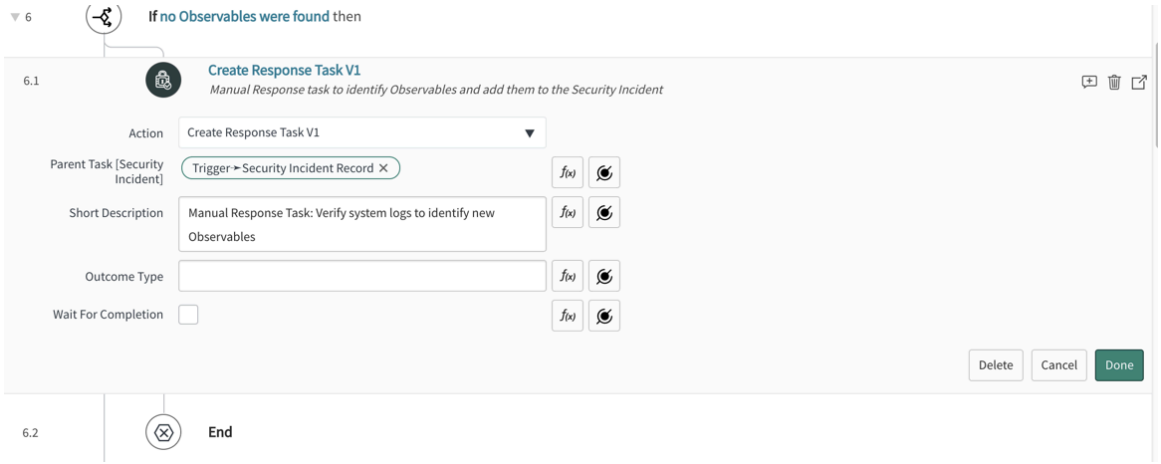
Hinweis:

In Schritt 3 des Flows prüft der Flow inaktive Anwender in `sn_si_Incident` Tabelle verfügbar in ServiceNow. Dieser Schritt wird als Leitfaden bereitgestellt und muss für Ihre spezifische Umgebung geändert werden. Wenn Sie diese Funktionalität verwenden möchten, empfehlen wir Ihnen, in Ihrer Umgebung eine Active Directory-Integration einzurichten. Sie können mit Ihrer Active Directory-Integration den Anwenderstatus ermitteln. Je nach Antwort können Sie die nächsten Schritte für Ihr Playbook entwerfen.

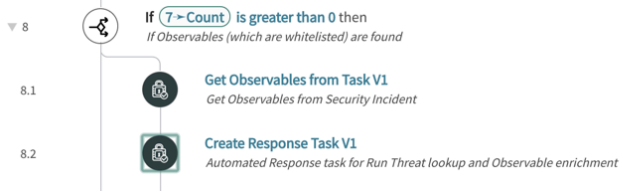
Wenn Sie keine Active Directory-Integration haben, ersetzen Sie diesen Schritt durch eine manuelle Aufgabe, die der Sicherheitsanalysten mit dem IT-Team zusammenarbeiten kann, um den Anwender zu blockieren und mit den restlichen Schritten im Playbook fortzufahren.

4. In Schritt 4 werden die erkennbaren Elemente für den Security Incident abgerufen.
5. In Schritt 5 werden die erkennbaren Elemente identifiziert.
6. Wenn keine erkennbaren Elemente gefunden werden, wird in Schritt 6 eine manuelle Antwortaufgabe erstellt, und der Flow endet.

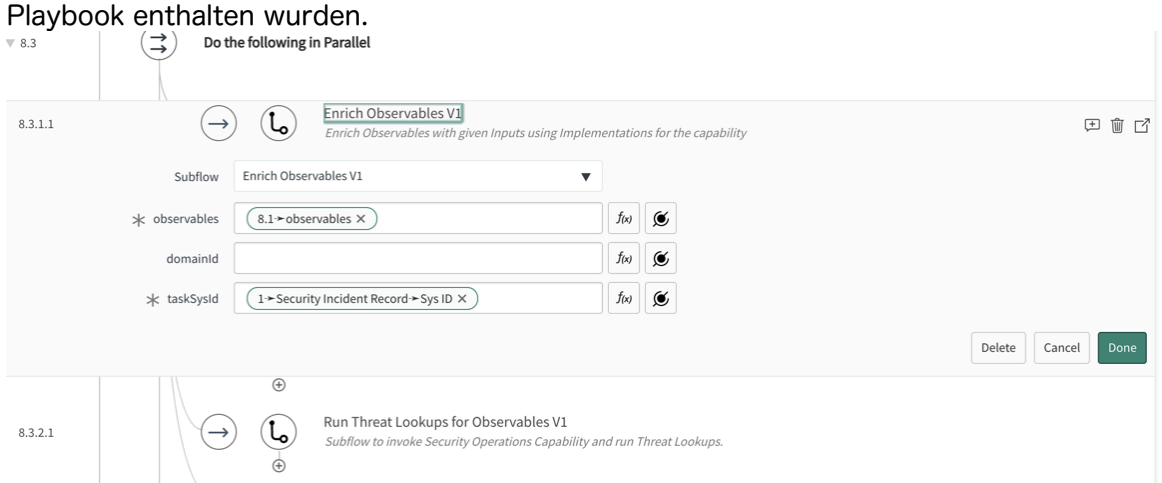
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Wenn erkennbare Elemente in Schritt 7 gefunden werden, werden erkennbare Elemente identifiziert, die nicht zulässig sind.
8. Wenn mindestens eines der erkennbaren Elemente nicht zulässig ist, werden die folgenden Schritte ausgeführt:
   a. Die Schritte 8,1 und 8,2 werden ausgeführt. Erkennbare Elemente werden abgerufen, und eine automatisierte Antwortaufgabe wird initiiert.



   b. Nachdem die automatisierte Aufgabe erstellt wurde, wird Schritt 8,3 (8.3.1.1 und 8,3.2,1) ausgeführt, und die Integrationen „erkennbare Elemente anreichern“ und „Bedrohungssuche“ werden ausgeführt. Beachten Sie, dass dies Subflows sind, die im Playbook enthalten wurden.



   c. In Schritt 8,4 wird der Security Incident-Datensatz aktualisiert, nachdem die Integrationen abgeschlossen wurden.
   d. In Schritt 8,5 wird eine neue Antwortaufgabe erstellt, um die nächste automatisierte Aufgabe anzugeben, die ausgeführt wird.
   e. In Schritt 8,6 wird die Integration der Sichtungssuche für die erkennbaren Elemente ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Nachdem der Subflow „Sichtungssuche“ abgeschlossen wurde, wird der Security Incident in Schritt 8,7 aktualisiert.

g. In Schritt 8,8 werden die erkennbaren Elemente überprüft, um festzustellen, ob sie böswillig sind.

h. Wenn die erkennbaren Elemente nicht schädlich sind und der Anwenderaccount aktiv ist, wird eine automatisierte E-Mail an den Anwender gesendet, um die fehlgeschlagenen Anmeldeversuche erneut zu bestätigen. Eine manuelle Antwortaufgabe wird erstellt, um die erkennbaren Elemente zu identifizieren und dem Security Incident hinzuzufügen. Das Playbook endet dann in dieser Phase.

i. Wenn die erkennbaren Elemente schädlich sind, werden drei Antwortaufgaben erstellt:

i. Zur Bestätigung wird eine automatisierte E-Mail an den Anwender gesendet **(Ja oder Nein)** Die nicht erfolgreichen Anmeldeversuche. Wenn der Anwender mit „Ja“ antwortet:

1. Der Status des Security Incidents wird auf aktualisiert **Enthalten** .
2. Eine automatisierte E-Mail wird an den Anwender gesendet, um das Passwort zurückzusetzen.
3. Der Subflow „Passwort zurücksetzen“ wird initiiert, und eine E-Mail wird an den Anwender gesendet, wenn die Aufgabe abgeschlossen wurde.

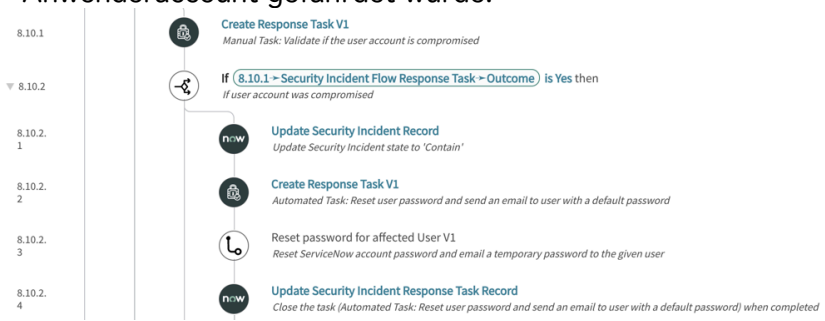
Hinweis:

Der Schritt „Passwort zurücksetzen“ wird als Leitfaden bereitgestellt. Die Schritte im Flow setzen das Passwort für den Account des Anwenders im ServiceNow-System zurück. Der Prozess zum Zurücksetzen des Passworts kann jedoch je nach Umgebung unterschiedlich sein. Sie können mit Ihrer Active Directory-Integration überprüfen, ob das Passwort von Anwendern automatisch zurückgesetzt wird. Wenn Sie keine Active Directory-Integration haben, ersetzen Sie diesen Schritt durch eine manuelle Aufgabe, die der Sicherheitsanalysten mit dem jeweiligen IT-Team zusammenarbeiten kann, um das Passwort des Anwenders zurückzusetzen und mit den restlichen Schritten im Playbook fortzufahren, nachdem die entsprechende Aufgabe abgeschlossen wurde.

ii. Wenn der Anwender mit „Nein“ antwortet, wird eine automatisierte E-Mail an den Anwender gesendet, um die Antwort erneut zu bestätigen. Der Sicherheitsanalyst muss die entsprechenden Maßnahmen manuell ergreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

iii. Wenn der Anwender nicht auf die automatisierte E-Mail antwortet, muss der Sicherheitsanalyst den Security Incident manuell aktualisieren und eine Antwort bereitstellen. Eine manuelle Aufgabe wird erstellt, um zu validieren, ob der Anwenderaccount gefährdet wurde.



9. In Schritt 8.10.3 wird der Status des Security Incident aktualisiert.
10. In Schritt 8.10.4 wird eine automatisierte Aufgabe erstellt, um zu überprüfen, ob die Funktionsimplementierung „Blockanforderungen für schädliche IPs und URLs erstellen“ verfügbar ist. Wenn die Fähigkeitsimplementierung verfügbar ist, wird der Subflow „Blockanforderungen erstellen“ ausgeführt. Wenn dies nicht verfügbar ist, wird der Security Incident aktualisiert, und eine Arbeitsnotiz wird veröffentlicht, um anzuzeigen, dass die Fähigkeitsimplementierung nicht verfügbar ist.
11. In Schritt 9 wird der Security Incident aktualisiert, und der Status wird auf festgelegt **Überprüfen** .
12. In Schritt 10 wird eine Antwortaufgabe erstellt, damit der Anwender die Überprüfung nach dem Incident abschließen kann, bevor er die Aufgabe schließt.

Playbook für die Automatisierung untergeordneter Security Incidents

Doppelte Security Incidents werden als untergeordnete Security Incidents kategorisiert und in den übergeordneten Security Incidents zusammengefasst.

Das Playbook für die Automatisierung von untergeordneten Security Incidents trägt dazu bei, den Zeitaufwand für die Untersuchung und das Schließen doppelter Security Incidents zu reduzieren. Dieses Playbook führt automatisch einen Rollup bestimmter eindeutiger Artefakte des untergeordneten Security Incidents (erkennbare Elemente, betroffene Anwender, CIs) zum übergeordneten Security Incident durch.

Voraussetzungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Spoke: Security Operations-Spoke installieren (sn_sec_Spoke)

Wichtige Funktionen

Das Playbook für untergeordnete Automatisierung umfasst die folgenden Fähigkeiten:

1. Verschiebt den Security Incident in **Analyse** Phase.
2. Eliminiert Duplikate und fügt dem übergeordneten Security Incident die betroffenen Anwender und CIs hinzu (Rollup).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Fügt dem übergeordneten Security Incident erkennbare Elemente aus dem untergeordneten Incident hinzu.
4. Schließt oder bricht den untergeordneten Security Incident ab, wenn der übergeordnete Security Incident geschlossen wird.

Fähigkeiten erforderlich

Weitere Informationen finden Sie unter ServiceNow-Store .

Sicherheitsanalysten-Experience

Informationen zur schrittweisen Lösung von Sicherheitsbedrohungen finden Sie unter Lösen Sie Sicherheitsbedrohungen mit dem Playbook.

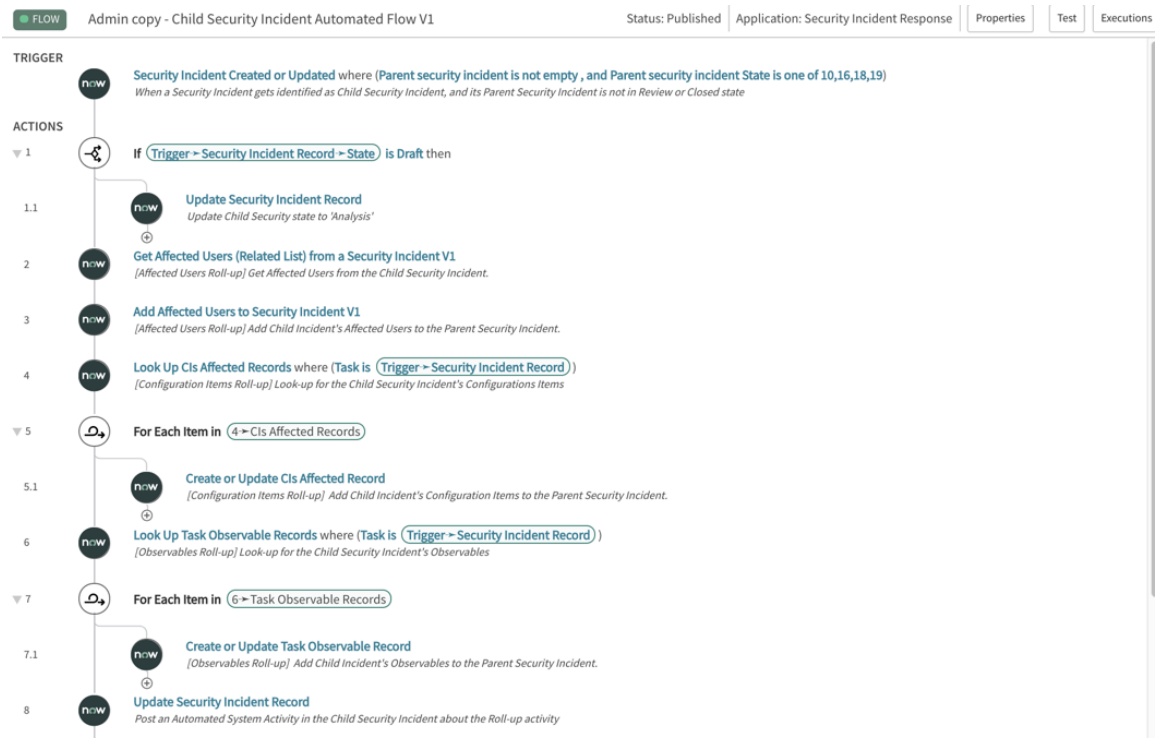
Tieferes Verständnis des Playbooks für die Automatisierung untergeordneter Security Incidents mit Flow Designer-Fähigkeiten

Erste Schritte

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Flow Designer** > **Designer** Und klicken Sie auf das Playbook für fehlgeschlagene Anmeldung.
3. Erstellen Sie eine Kopie des Playbooks für die Automatisierung untergeordneter Security Incidents, und nehmen Sie die erforderlichen Änderungen vor. (Dies ist ein optionaler Schritt. Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen daran vorzunehmen).
4. Nehmen Sie die erforderlichen Änderungen entsprechend Ihren Anforderungen vor. (Dies ist ein optionaler Schritt. Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen daran vorzunehmen).
5. Aktivieren Sie das Playbook.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie den kopierten Flow, nachdem Sie Änderungen gemäß Ihren Anforderungen vorgenommen haben.

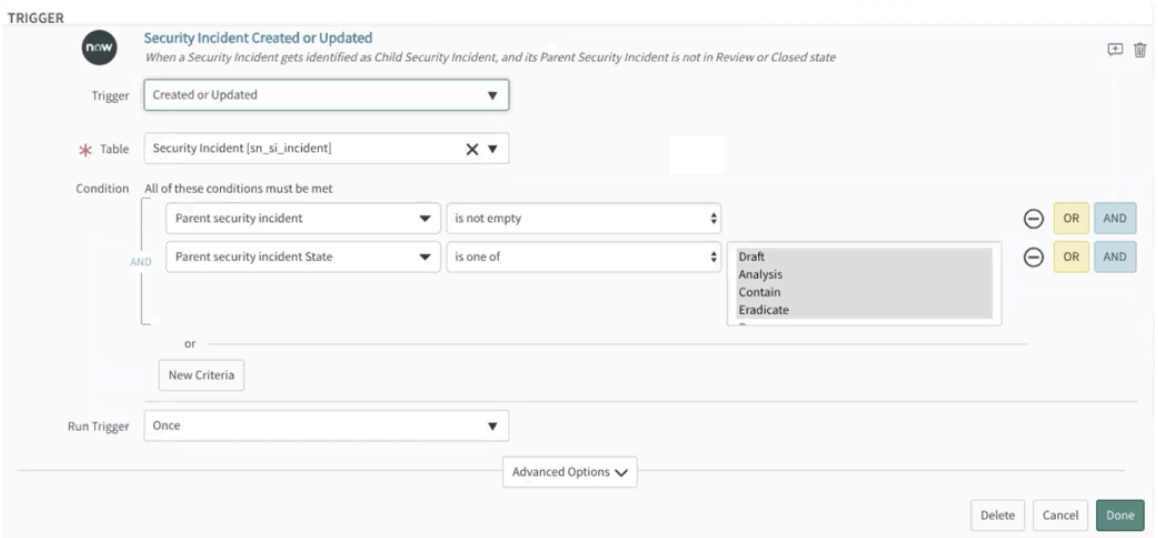
Die folgende Abbildung zeigt eine Kopie des Playbooks für die Automatisierung untergeordneter Security Incidents. Überprüfen Sie die folgenden Schritte, um ein Verständnis der verschiedenen Aktionen im Playbook zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieses Playbook wird ausgelöst, wenn:

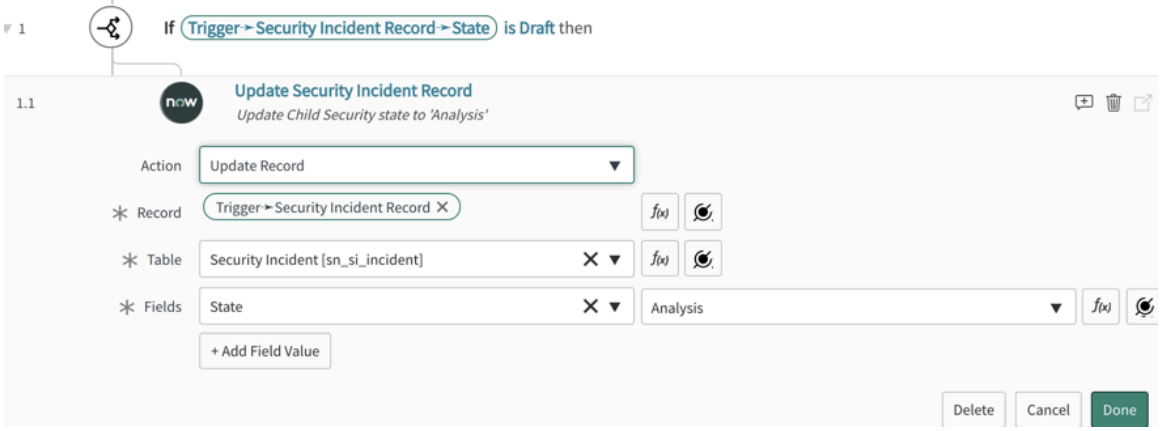
- Das Feld „übergeordneter Security Incident“ ist nicht leer.
- Der übergeordnete Security Incident befindet sich im Status „Entwurf“, „Analyse“, „Eindämmen“ oder „Beseitigen“.



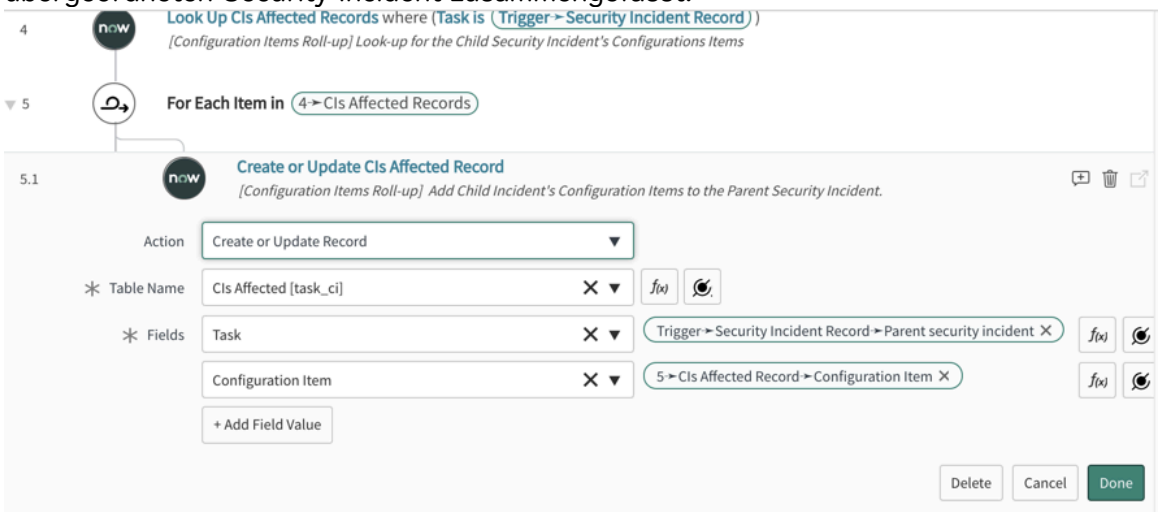
Die folgenden Schritte führen Sie durch die Aktionen und Aufgaben, die im Playbook „Automatisierung untergeordneter Security Incidents“ verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wenn das Playbook mit der Ausführung beginnt, wird es in Schritt 1 aktualisiert und in den Status „Entwurf“ versetzt, wenn sich der Security Incident im Status „Analyse“ befindet.

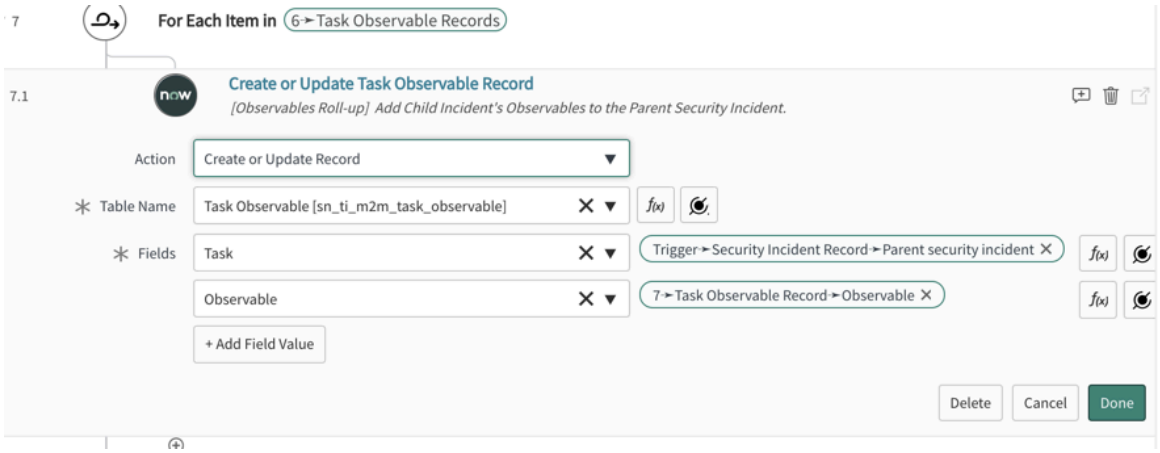


2. In den Schritten 2 und 3 werden betroffene Anwender für den Security Incident abgerufen und zum übergeordneten Security Incident zusammengefasst. Alle doppelten Anwender werden eliminiert.
3. In den Schritten 4 und 5 werden Konfigurationselemente abgerufen, die dem untergeordneten Security Incident zugeordnet sind, und eindeutige CIs werden zum übergeordneten Security Incident zusammengefasst.



4. In den Schritten 6 und 7 werden erkennbare Elemente abgerufen, die dem untergeordneten Security Incident zugeordnet sind, und eindeutige erkennbare Elemente werden zum übergeordneten Security Incident zusammengefasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. In den Schritten 8 und 9 werden automatisierte Arbeitsnotizen in den übergeordneten und untergeordneten Security Incidents veröffentlicht, die angeben, dass die betroffenen Anwender, Konfigurationselemente und erkennbaren Elemente vom untergeordneten zum übergeordneten Security Incident zusammengefasst wurden.

Playbook für Office 365 – schädliche Datei erkannt

Dieses Playbook bietet systematische Korrekturschritte für die Untersuchung schädlicher Dateien, die in Office 365 erkannt wurden.

Wenn schädliche Dateien in Office 365 erkannt werden, können Sie das Playbook 365 – schädliche Datei erkannt im Flow Designer verwenden, um Anleitungen zu erhalten und die Untersuchung dieser schädlichen Dateien zu optimieren.

Richten Sie das Playbook für erkannte Office Malicous-Datei ein

Führen Sie die folgenden Schritte aus, um das Playbook für erkannte Office Malicous-Datei einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

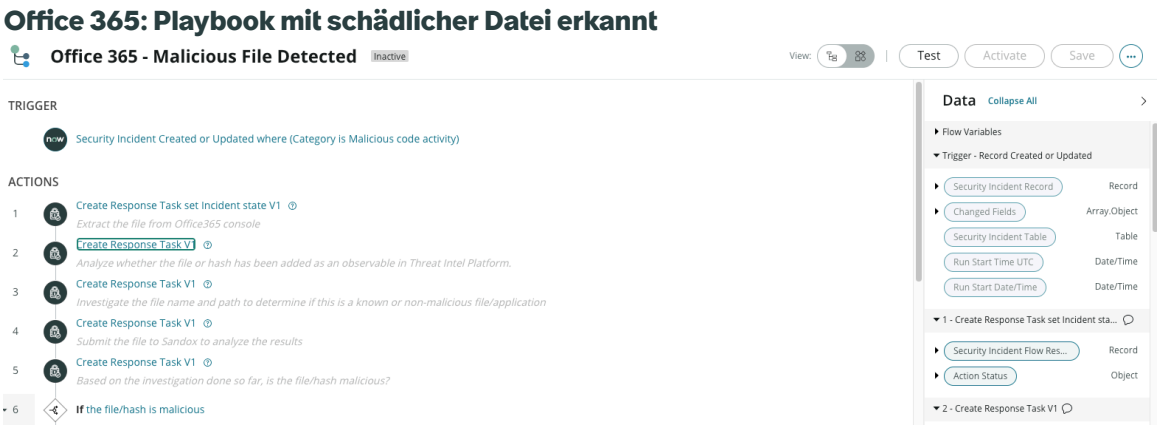
Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

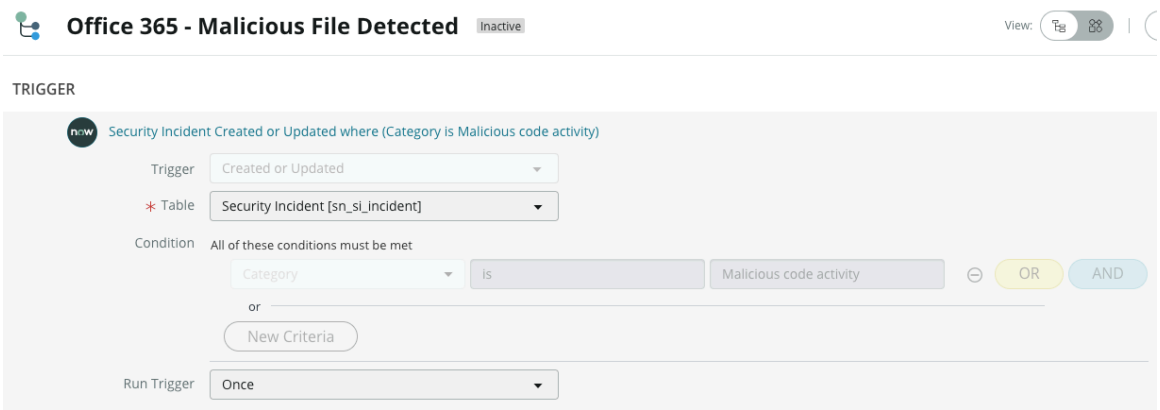
1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Office 365: Schädliche Datei Erkannt** playbook.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows „Office 365 – schädliche Datei erkannt“ erstellen und die erforderlichen Änderungen vornehmen.

   Klicken Sie auf , um eine Kopie des Playbook-Flows zu erstellen Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der verwendet wird **Kategorie** Ist **Schädliche Codeaktivität** .



Verwenden Sie das Playbook „erkannte schädliche Office 365-Datei“

Verwenden Sie dieses Playbook, um schädliche Dateien zu untersuchen, die in Office 365 erkannt wurden. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die im Playbook „erkannte schädliche Datei für Office 365“ verfügbar sind.

Vorbereitungen

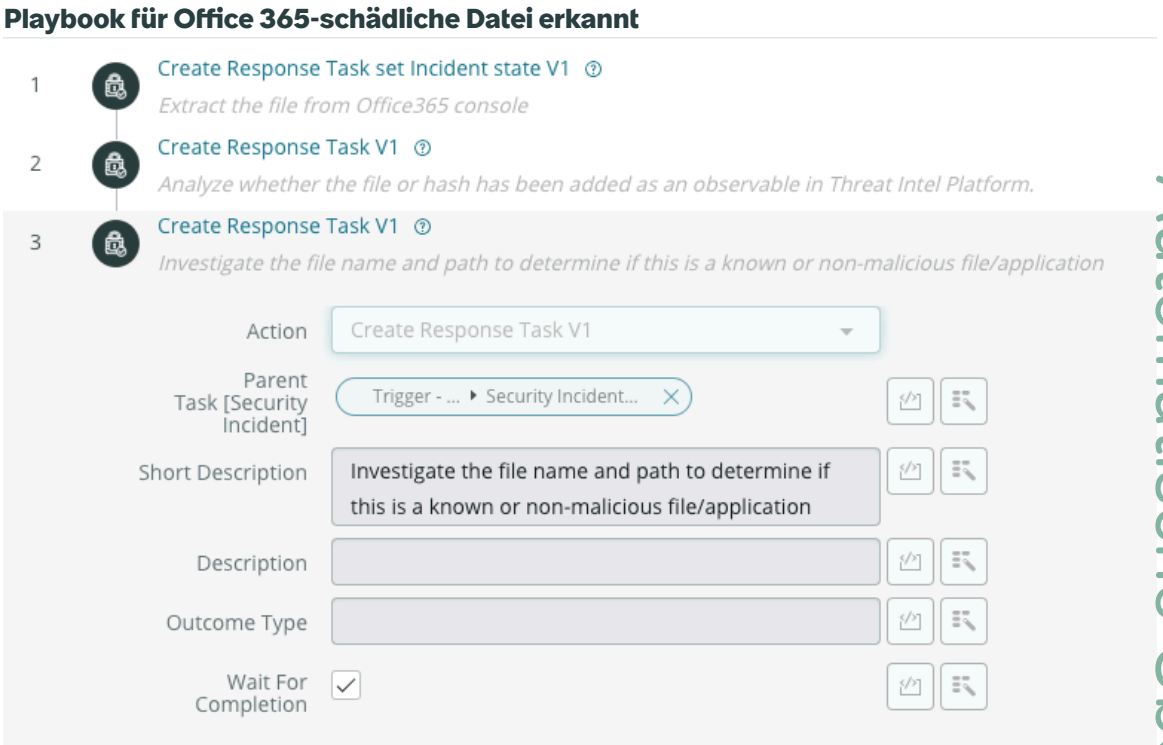
Erforderliche Rolle:

- sn_si.admin
- flow_designer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, müssen Sie in Aktion 1 die schädliche Datei aus der Office 365-Konsole extrahieren.
2. In Aktion 2 müssen Sie analysieren, ob die Datei oder der Hash als erkennbares Element in der Threat Intel Platform hinzugefügt wurde.
3. In Aktion 3 müssen Sie den Dateinamen und Pfad untersuchen, um festzustellen, ob es sich um eine bekannte oder nicht schädliche Datei/Anwendung handelt.



4. In Aktion 4 müssen Sie die Datei zur Analyse der Ergebnisse an Sandbox senden.
5. In Aktion 5 müssen Sie basierend auf der bisher durchgeführten Untersuchung überprüfen, ob die Datei oder der Hash böswillig ist oder nicht.
   Wenn die Datei oder der Hash nicht schädlich ist, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow endet.
6. Wenn die Datei oder der Hash in Aktion 6 schädlich ist, werden die Aktionen 7 und 8 ausgeführt.
7. In Aktion 7 müssen Sie sich an den Endanwender wenden, um eine gültige geschäftliche Begründung zu erhalten, warum er eine schädliche Datei auf dem Gerät hat.
   Wenn die Datei oder der Hash böswillig ist, können Sie die bereits vorhandene E-Mail-Vorlage im Playbook verwenden, um dem Endanwender eine Klärung anzufordern.
8. In Aktion 8 müssen Sie überprüfen, ob der Endanwender eine gültige geschäftliche Begründung angegeben hat oder nicht.
   Wenn der Endanwender eine gültige geschäftliche Begründung angegeben hat, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow endet.
9. Wenn der Anwender in Aktion 9 keine gültige geschäftliche Begründung angegeben hat, werden die Aktionen 10, 11 und 12 ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Da in Aktion 10 keine gültige geschäftliche Begründung vorhanden ist, können Sie die schädliche Datei oder den schädlichen Hash zur Überprüfung an das Threat Intel-Team weiterleiten.
11. In Aktion 11 müssen Sie das Malware-Bytes-Scannerskript ausführen, um zu überprüfen, ob die Datei oder der Hash schädlich ist.
12. In Aktion 12 müssen Sie eine forensische Analyse durchführen, um zu überprüfen, ob die Datei oder der Hash schädlich ist.
13. In Aktion 13 wird eine Antwortaufgabe erstellt, damit der Anwender die Überprüfung nach dem Incident abschließen kann, bevor er die Aufgabe schließt.

Playbook für Wiederholungserkennung

Mit diesem Playbook können Sie feststellen, ob die Reaktion auf Incidents in der Vergangenheit für einen genauen oder ähnlichen Phishing-Bericht bereitgestellt wurde und automatisch ähnlich am neuen Bericht arbeitet.

Das Playbook „Wiederholungserkennung“ überprüft, ob der neu gemeldete Phishing-Incident einem früheren Incident ähnelt. Wenn die Wiederholungserkennung identifiziert wird, werden der übereinstimmende Security Incident und die Lösungsdetails dem Analysten mitgeteilt, der ihn für den neu gemeldeten Incident verwenden kann, was zu einer schnellen Korrektur des Security Incidents führt.

Richten Sie das Playbook für Wiederholungserkennung ein

Führen Sie die folgenden Schritte aus, um das Playbook für Wiederholungserkennung einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*). Sie haben die Möglichkeit, die folgenden Systemeigenschaften zu ändern:

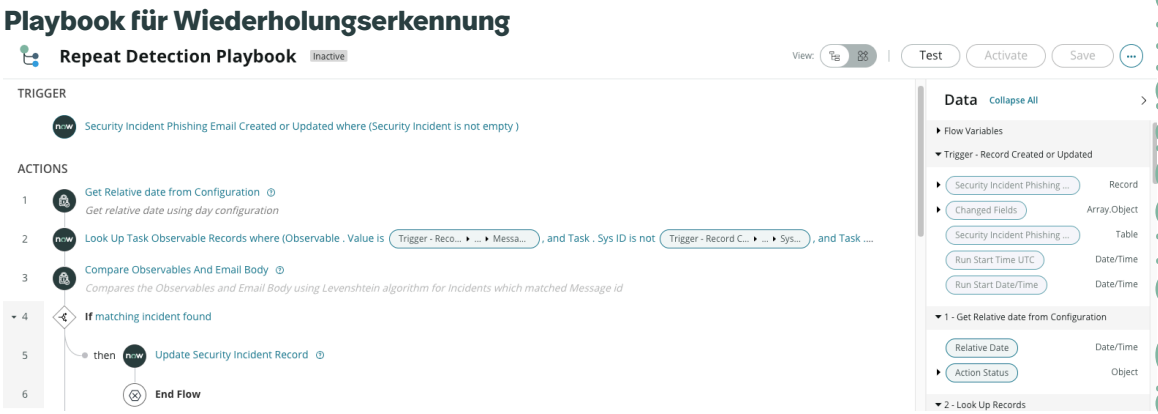
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *sn_sec_Spoke.similarphish.earlyterminationscore*
- *sn_sec_Spoke.similarphish.lookbackdays*
- *sn_sec_Spoke.similarphish.maxcomparisonsize*
- *sn_sec_Spoke.similarphish.minmatchscore*

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Erkennung Wiederholen** playbook.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows für Wiederholungserkennung erstellen und die erforderlichen Änderungen vornehmen.

   Klicken Sie auf , um eine Kopie des Playbook-Flows zu erstellen Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

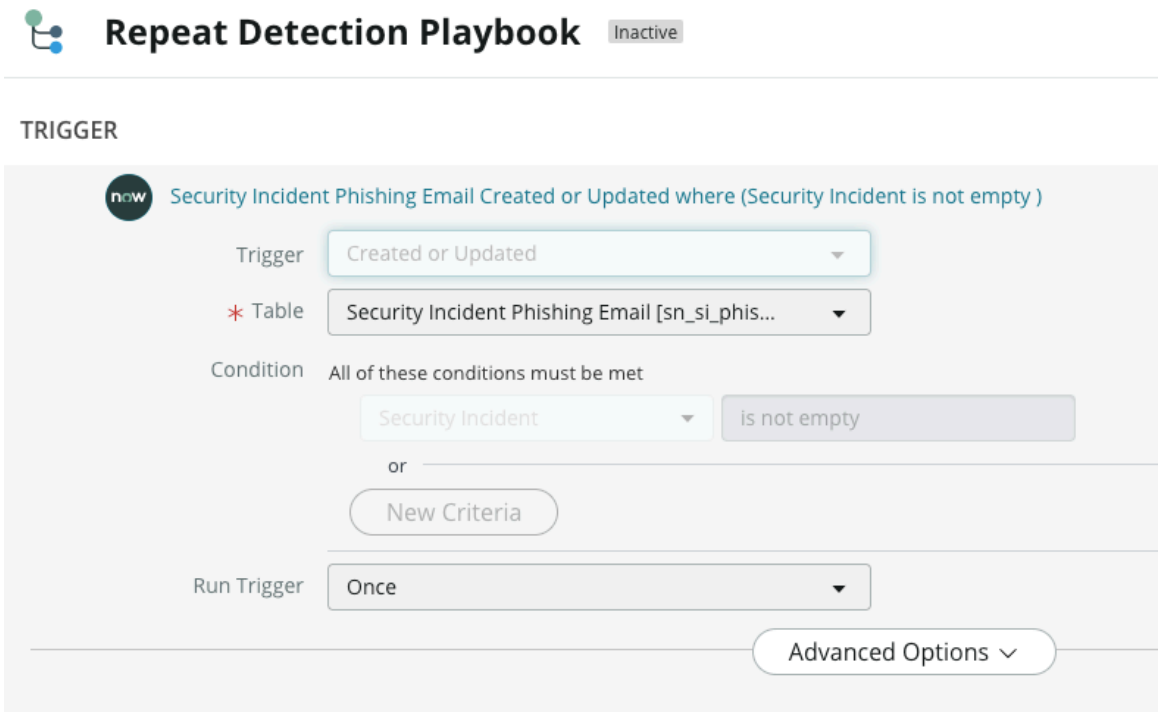
   

4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst, wenn **Security Incident Ist nicht leer** .



Verwenden Sie das Playbook für Wiederholungserkennung

Verwenden Sie dieses Playbook, um zu untersuchen, ob die Reaktion auf Incidents in der Vergangenheit für einen genauen oder ähnlichen Phishing-Bericht bereitgestellt wurde und automatisch ähnlich am neuen Bericht arbeitet. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die im Playbook „Wiederholungserkennung“ verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

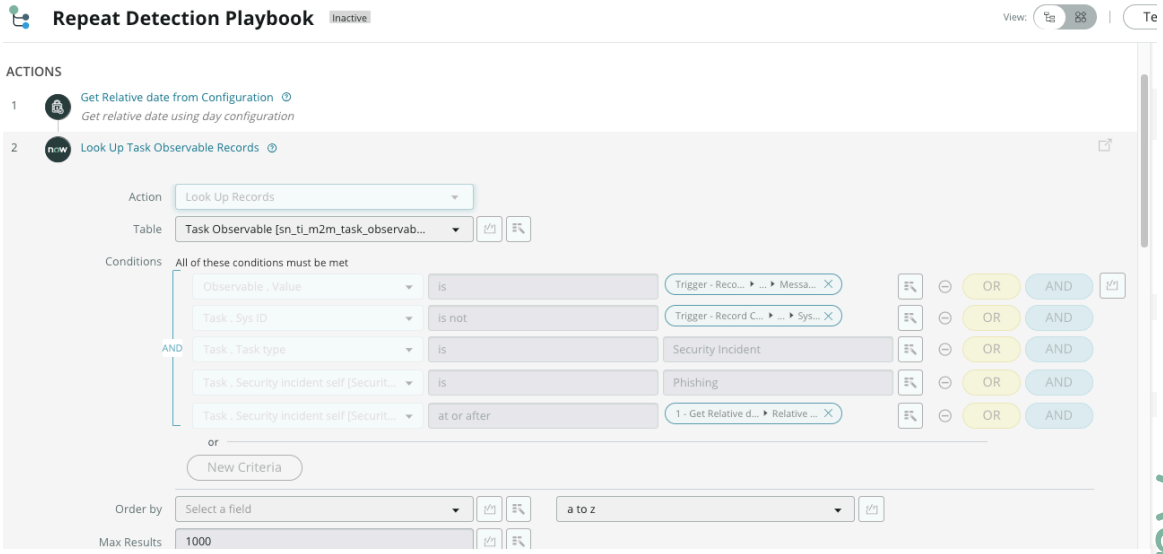
- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, ruft das Playbook in Aktion 1 das relative Datum des Security Incident mithilfe der Tageskonfiguration ab.
2. In Aktion 2 sucht das Playbook nach den Datensätzen des erkennbaren Aufgabenelements in der Tabelle `sn_ti_m2m_Task_Observable` Die dem Incident basierend auf der Nachrichten-ID entsprechen.

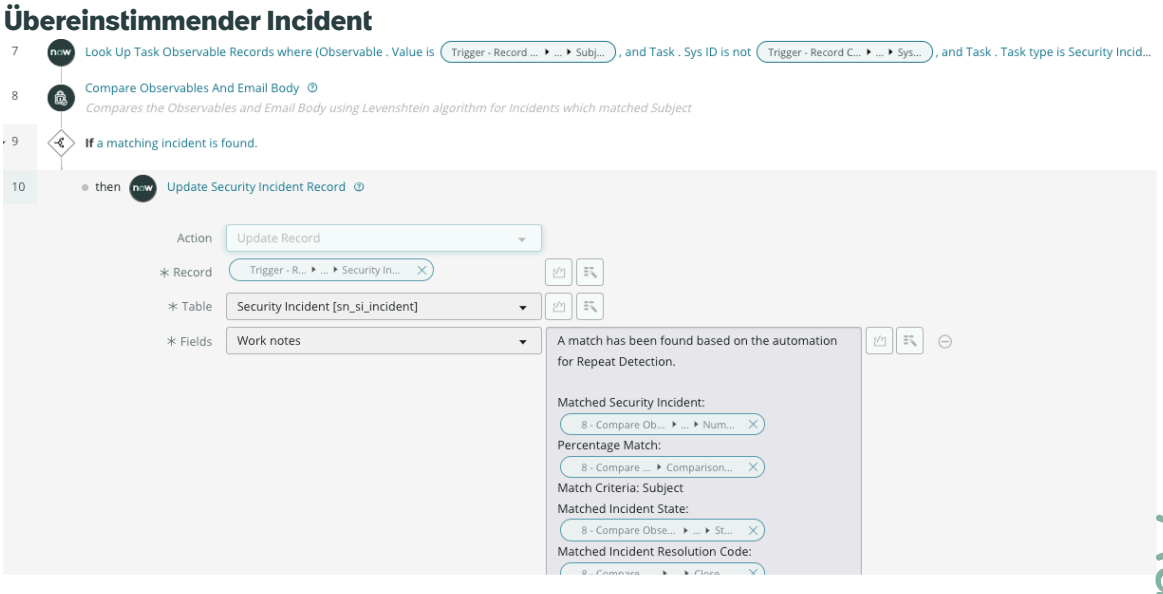
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook für Wiederholungserkennung



3. In Aktion 3 vergleicht das Playbook die erkennbaren Aufgaben und den E-Mail-Text mithilfe des Levenshtein-Algorithmus für Incidents, die der Nachrichten-ID entsprechen.
4. In Aktion 4 überprüft das Playbook basierend auf der bisher durchgeführten Untersuchung, ob der übereinstimmende Incident basierend auf der Nachrichten-ID gefunden wird oder nicht.
   Wenn in Aktion 5 der übereinstimmende Incident gefunden wird, aktualisiert das Playbook automatisch die Arbeitsnotiz, dass eine Übereinstimmung gefunden wurde, basierend auf der Automatisierung für die Wiederholungserkennung. In Aktion 6 endet der Flow.
5. Wenn der übereinstimmende Incident nicht gefunden wird, sucht das Playbook in Aktion 7 nach den Datensätzen des erkennbaren Aufgabenelements in der Tabelle `sn_ti_m2m_Task_Observable` Die dem Incident basierend auf dem Betreff entsprechen.
6. In Aktion 8 vergleicht das Playbook die erkennbaren Aufgabenelemente und den E-Mail-Text mithilfe des Levenshtein-Algorithmus für Incidents, die dem Betreff entsprechen.
7. In Aktion 9 überprüft das Playbook, ob der übereinstimmende Incident gefunden wurde oder nicht.
   Wenn in Aktion 10 der übereinstimmende Incident gefunden wird, aktualisiert das Playbook automatisch die Arbeitsnotiz, dass eine Übereinstimmung gefunden wurde, basierend auf der Automatisierung für die Wiederholungserkennung. In Aktion 11 endet der Flow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. In Aktion 12 sucht das Playbook nach den Datensätzen des erkennbaren Aufgabenelements in der Tabelle `sn_ti_m2m_Task_Observable` Die dem Incident basierend auf der Adresse entsprechen.
9. In Aktion 13 vergleicht das Playbook die erkennbaren Aufgabenelemente und den E-Mail-Text mithilfe des Levenshtein-Algorithmus für Incidents, die der Adresse entsprechen.
10. In Aktion 14 überprüft das Playbook, ob der übereinstimmende Incident basierend auf der Adresse gefunden wird oder nicht.
    Wenn in Aktion 15 der übereinstimmende Incident gefunden wird, aktualisiert das Playbook automatisch die Arbeitsnotiz, dass eine Übereinstimmung gefunden wurde, basierend auf der Automatisierung für die Wiederholungserkennung. In Aktion 16 endet der Flow.

Playbook für gefälschte E-Mails (mit demselben Anzeigenamen)

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung gefälschter E-Mails, die ausgelöst werden, wenn gefälschte Namen für E-Mails an die Mitarbeiter der Organisation gesendet werden.

Richten Sie das Playbook für gefälschte E-Mails ein

Führen Sie die folgenden Schritte aus, um das Playbook für gefälschte E-Mails einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

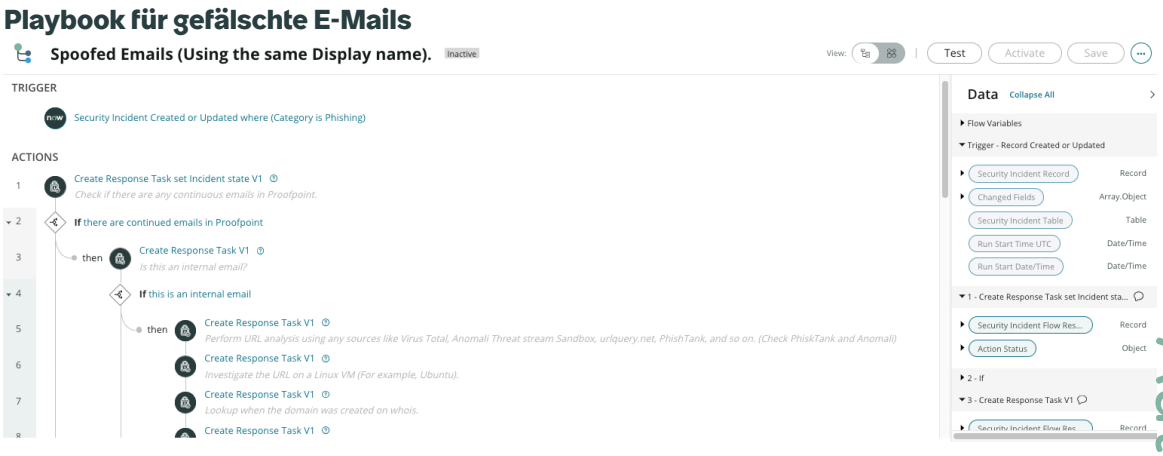
Stellen Sie sicher, dass Sie die Security Operations-Spoke (`sn_sec_Spoke`).

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Gefälschte E-Mails (mit demselben Anzeigenamen)** playbook.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows für Wiederholungserkennung erstellen und die erforderlichen Änderungen vornehmen.

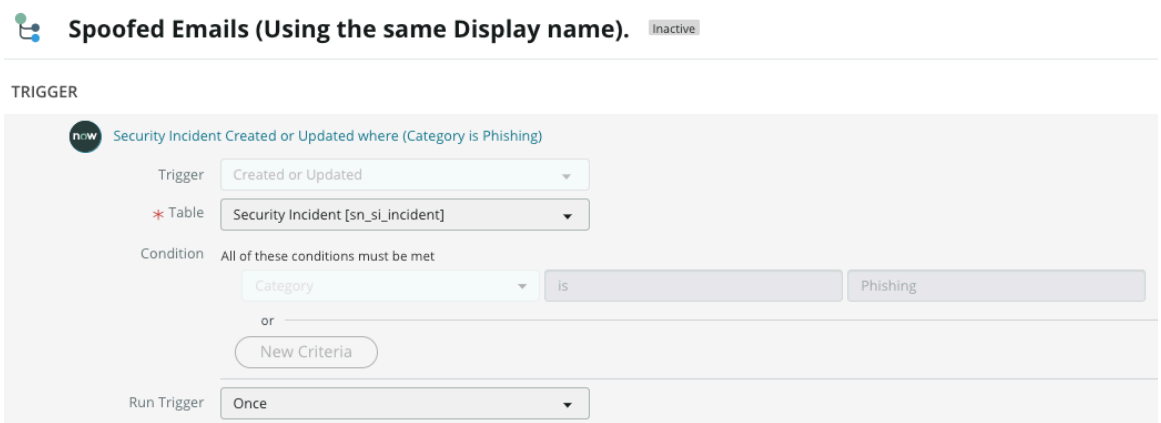
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie auf , um eine Kopie des Playbook-Flows zu erstellen Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.



4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der verwendet wird **Kategorie** Ist **Phishing** .



Verwenden Sie das Playbook „gefälschte E-Mails“ (mit demselben Anzeigenamen)

Verwenden Sie dieses Playbook, um gefälschte E-Mails zu untersuchen, die ausgelöst werden, wenn gefälschte Namen für E-Mails an die Mitarbeiter der Organisation gesendet werden. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die im Playbook „gefälschte E-Mails“ (mit demselben Anzeigenamen) verfügbar sind.

Vorbereitungen
Erforderliche Rolle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

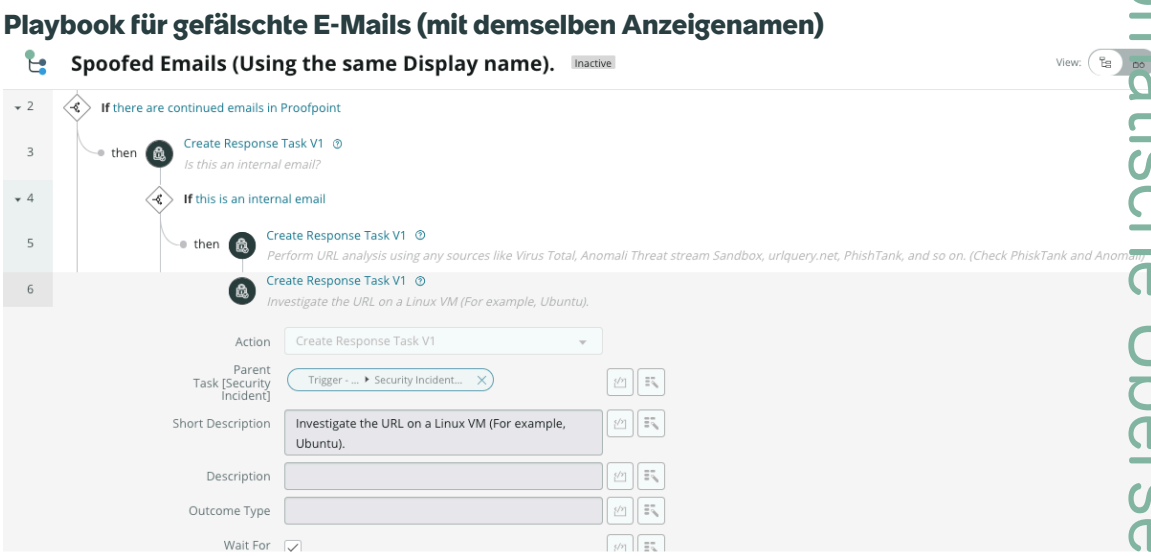
- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, müssen Sie in Aktion 1 überprüfen, ob in Proofpoint fortlaufende gefälschte E-Mails vorhanden sind.
2. Wenn in Aktion 2 kontinuierliche E-Mails in Proofpoint vorhanden sind, überprüfen Sie, ob dies eine interne gefälschte E-Mail ist oder nicht.
3. Wenn es sich in Aktion 3 um eine interne gefälschte E-Mail handelt, führen Sie die folgenden Aktionen aus:

   a. In Aktion 5 müssen Sie URL-Analysen mit beliebigen Quellen wie Virus Total, Anomali-Bedrohungsstrom Sandbox, urlquery.net, PhishTank durchführen (überprüfen Sie z. B. PhiskTank und Anomali).

   b. In Aktion 6 müssen Sie die URL auf einer Linux-VM (z. B. Ubuntu) untersuchen.

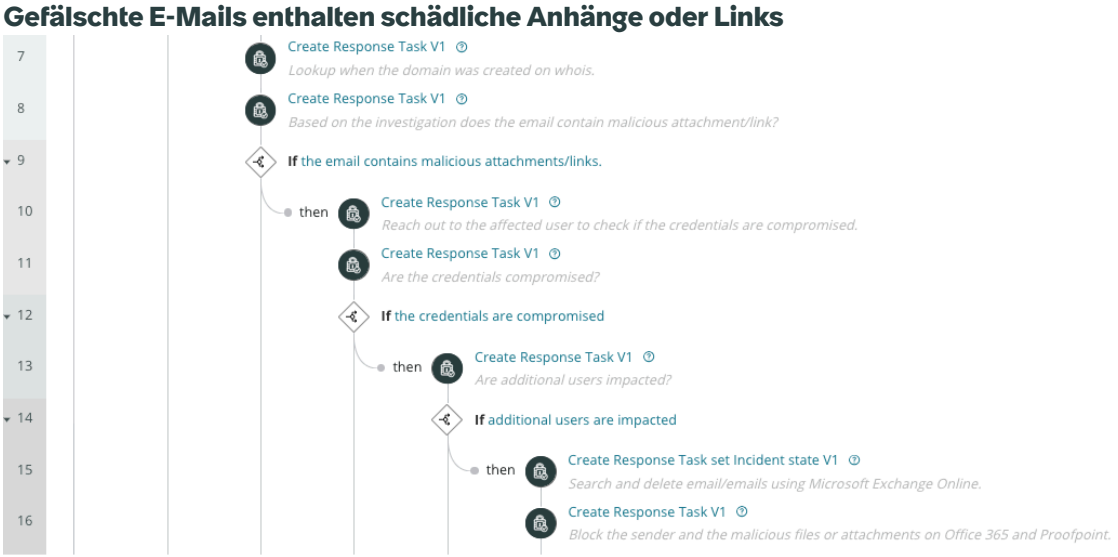


   c. In Aktion 7 müssen Sie suchen, wann die Domäne in WHOIS erstellt wurde.
   Suchen Sie nach kürzlich registrierten Domänen (innerhalb der letzten Woche), die verdächtig sind und eine hohe Wahrscheinlichkeit von Phishing-Angriffen haben.

   d. In Aktion 8 müssen Sie basierend auf der bisher durchgeführten Untersuchung überprüfen, ob diese E-Mail einen böswilligen Anhang oder Link enthält.
   Wenn diese E-Mail keinen böswilligen Anhang oder Link enthält, wird der Flow beendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Führen Sie in Aktion 9 die folgenden Aktionen aus, wenn die E-Mail schädliche Anhänge oder Links enthält.

i. In Aktion 10 müssen Sie sich an den betroffenen Anwender wenden, um zu überprüfen, ob die Anmeldeinformationen gefährdet sind. Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den betroffenen Anwender zu kontaktieren.

ii. In Aktion 11 müssen Sie basierend auf der E-Mail-Antwort überprüfen, ob die Anmeldeinformationen gefährdet sind. Wenn die Anmeldeinformationen nicht gefährdet wurden, endet der Flow.

1. Wenn in Aktion 12 die Anmeldeinformationen gefährdet sind, müssen Sie in Aktion 13 überprüfen, ob zusätzliche Anwender betroffen sind. Wenn keine zusätzlichen Anwender betroffen sind, endet der Flow.

2. Führen Sie in Aktion 14 die folgenden Aktionen aus, wenn zusätzliche Anwender betroffen sind:

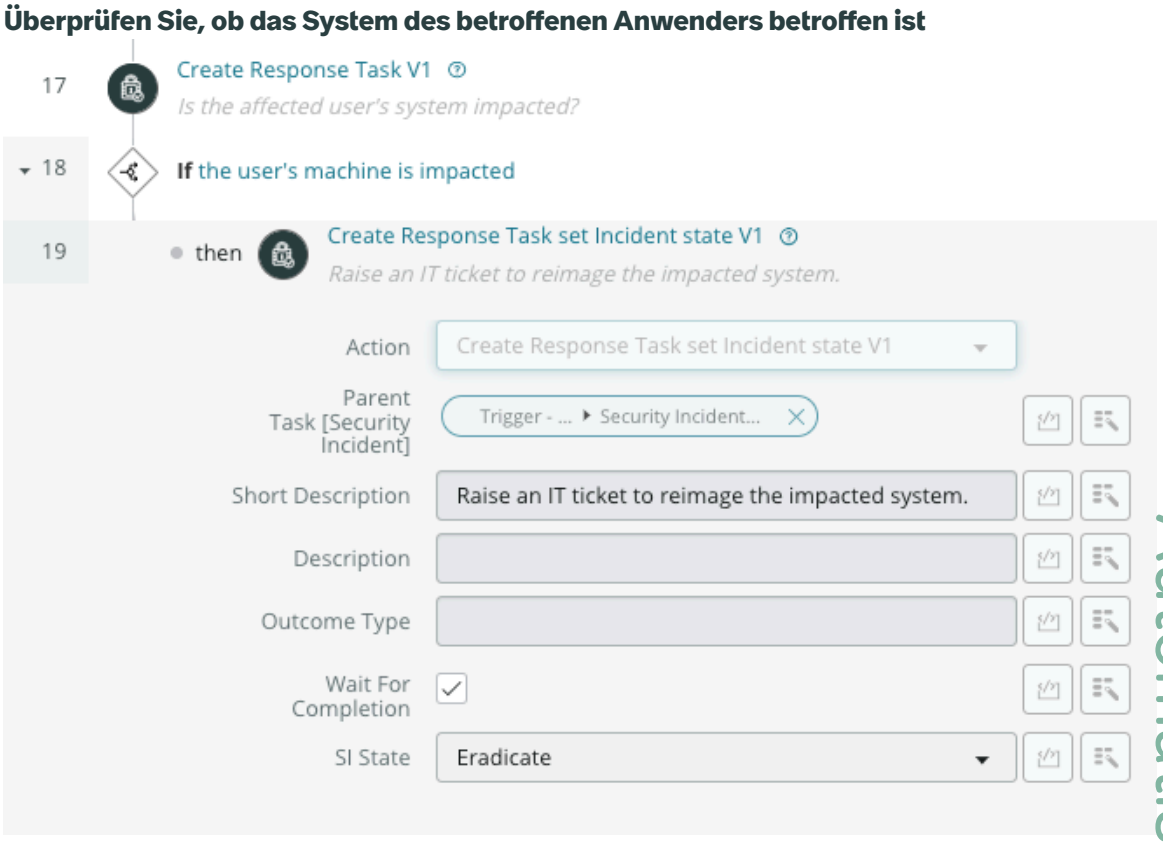
a. In Aktion 15 müssen Sie E-Mails mit Microsoft Exchange Online suchen und löschen.

b. In Aktion 16 müssen Sie den Absender und die schädlichen Dateien oder Anhänge in Office 365 und Proofpoint blockieren.

4. Wenn es sich in Aktion 17 nicht um eine interne gefälschte E-Mail handelt, müssen Sie überprüfen, ob das System des betroffenen Anwenders betroffen ist.

5. Wenn in Aktion 18 das System des Anwenders betroffen ist, erstellen Sie in Aktion 19 ein IT-Ticket, um das betroffene System neu zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. In Aktion 20 wird eine Antwortaufgabe erstellt, mit der Sie die Überprüfung nach dem Incident abschließen können, bevor Sie die Aufgabe schließen.

Playbook für Endpunkterkennung

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Malware-Warnungen, die auf einem Host oder Endpunkt ausgelöst wurden (z. B. Erkennung schädlicher Dateien).

Wenn CrowdStrike-Warnungen auf einem Host oder Endpunkt ausgelöst werden, können Sie das Playbook „Endpunkterkennung“ im Flow Designer verwenden, um Anleitungen zu erhalten und die Untersuchung dieser schädlichen Dateien zu optimieren.

Richten Sie das Playbook für die Endpunkterkennung ein

Führen Sie die folgenden Schritte aus, um das Playbook für die Endpunkterkennung einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

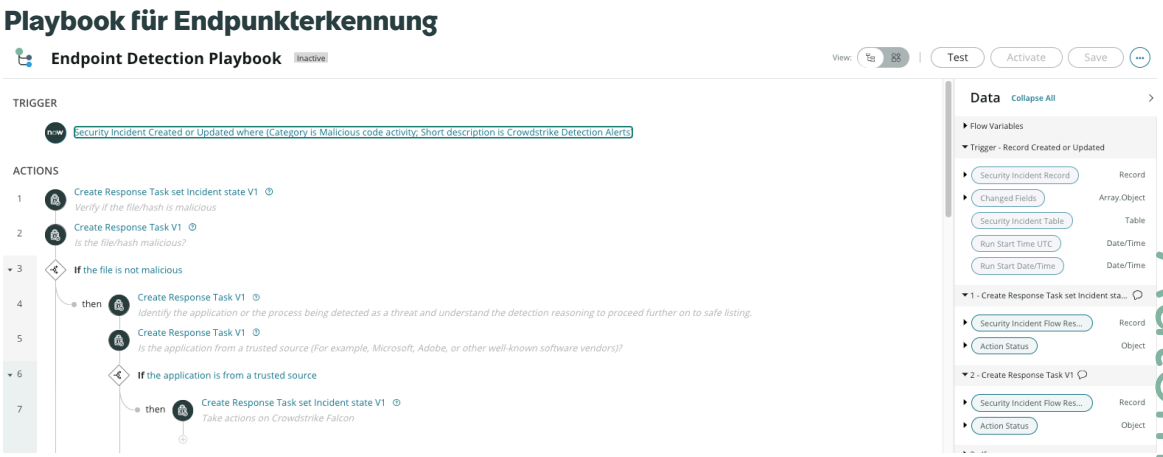
1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Endpunkterkennung** playbook.

Automatische Übersetzung

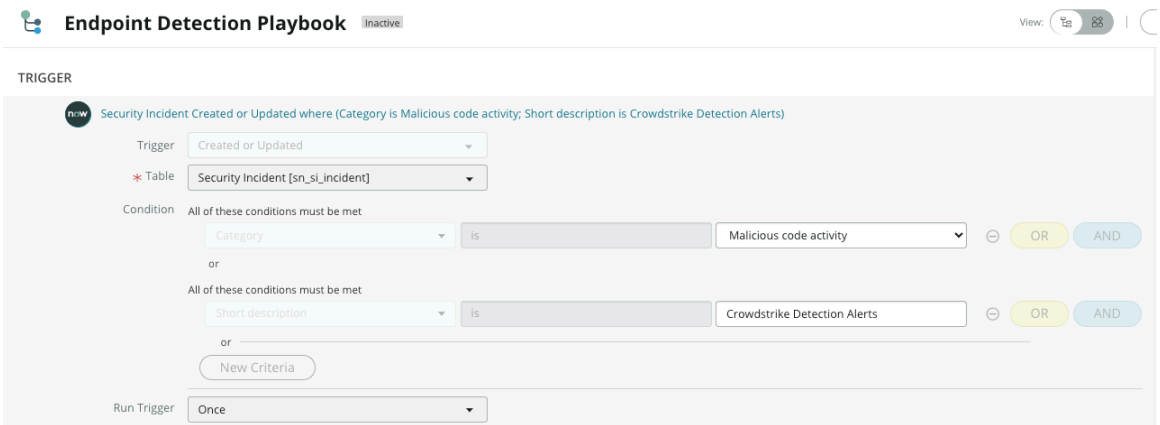
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows für die Endpunkterkennung erstellen und die erforderlichen Änderungen vornehmen.

   Klicken Sie auf , um eine Kopie des Playbook-Flows zu erstellen Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.



4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:
   - **Kategorie** Ist **Schädliche Codeaktivität** .
   - **Kurzbeschreibung** Ist **CrowdStrike-Erkennungswarnungen** .



Verwenden Sie das Playbook „Endpunkterkennung“

Verwenden Sie dieses Playbook, um Malware-Warnungen zu untersuchen, die auf einem Host oder Endpunkt ausgelöst wurden. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die im Playbook „Endpunkterkennung“ verfügbar sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

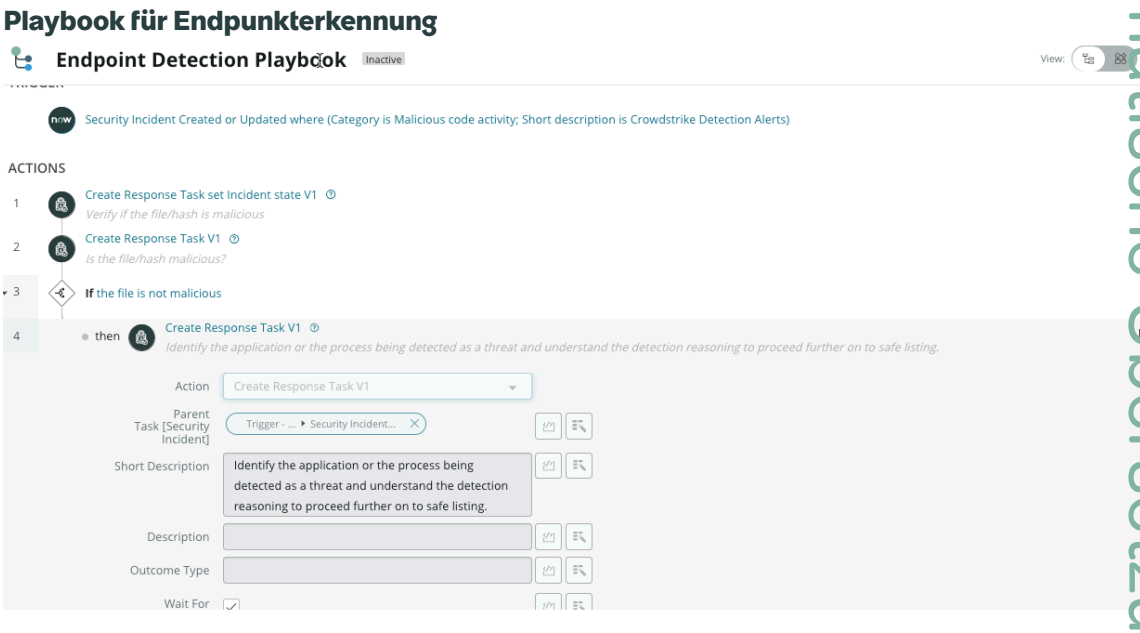
- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, müssen Sie in Aktion 1 überprüfen, ob die Datei oder der Hash schädlich ist, indem Sie die Ergebnisse der Bedrohungssuche in SIR analysieren und informationen von VirusTotal, Wildfire, ThreatCrowd usw. sammeln
2. In Aktion 2 müssen Sie überprüfen, ob die Datei oder der Hash schädlich ist oder nicht.
3. Führen Sie in Aktion 3 die folgenden Aktionen aus, wenn die Datei oder der Hash schädlich ist:

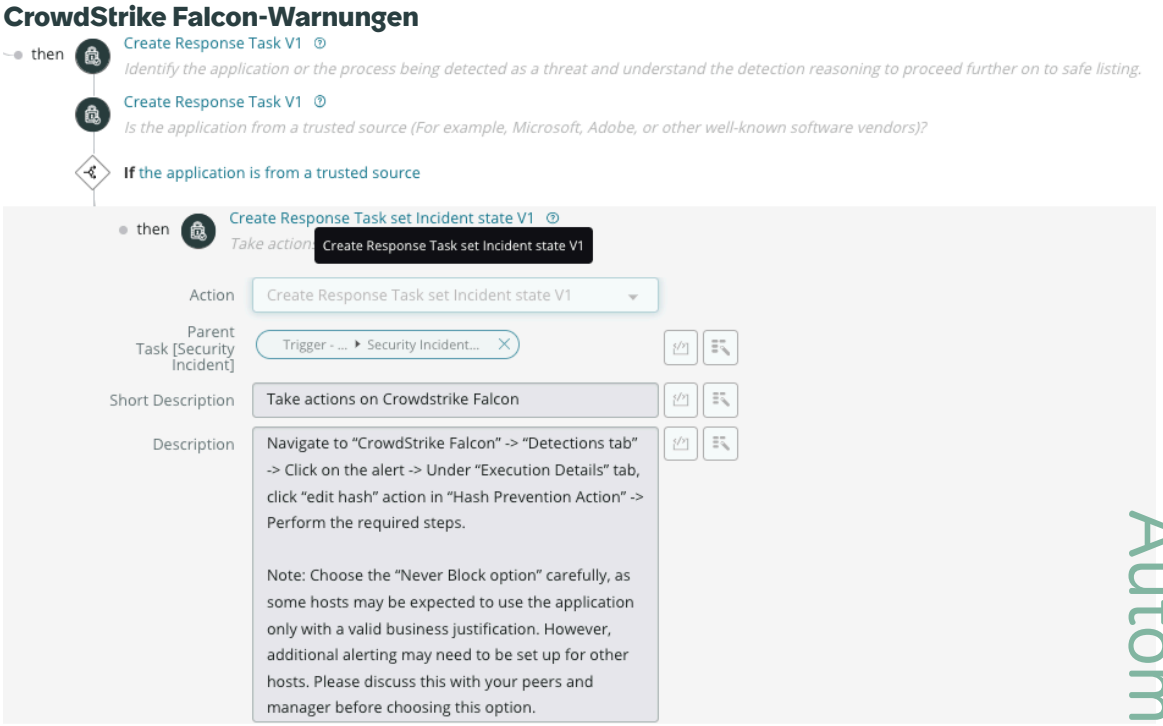
   a. In Aktion 4 müssen Sie die erkannte Anwendung oder den Prozess als Bedrohung identifizieren und Informationen über die Erkennungsgründe sammeln, um mit der sicheren Liste fortzufahren.



   b. In Aktion 5 müssen Sie überprüfen, ob die Anwendung aus einer vertrauenswürdigen Quelle stammt (z. B. Microsoft, Adobe oder andere bekannte Softwareanbieter).

   c. Wenn die Anwendung in Aktion 6 aus einer vertrauenswürdigen Quelle stammt, müssen Sie Maßnahmen für die CrowdStrike Falcon-Warnungen ergreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Führen Sie in Aktion 7 die folgenden Aktionen aus:

i. Navigieren zu **CrowdStrike Falcon** > **Erkennungen** Registerkarte

ii. Klicken Sie auf die CrowdStrike Falcon-Warnung.

iii. Klicken Sie auf der Registerkarte Ausführungsdetails auf **Bearbeiten Sie Den Hash** Aktion in Hash-Präventionsaktion.

iv. Führen Sie die erforderlichen Schritte aus.

> **Hinweis:**
> Wählen Sie aus **Nie Blockieren** Option vorsichtig, da nur bestimmte Hosts die Anwendung mit einer gültigen geschäftlichen Begründung verwenden dürfen. Möglicherweise müssen jedoch zusätzliche Warnungen für andere Hosts eingerichtet werden.

e. Wenn die Anwendung in Aktion 8 nicht aus einer vertrauenswürdigen Quelle stammt, müssen Sie auswählen, ob Sie auf die Datei oder Anwendung lokal vom Gerät verzichten möchten.
Wenn Sie in Aktion 10 auf die Datei oder Anwendung lokal vom Gerät verzichten möchten, führen Sie die folgenden Aktionen aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Navigieren Sie in Aktion 11 zu **Dateien In Quarantäne** Und filtern Sie den Endpunkt, indem Sie nach dem Gerätenamen suchen.

ii. Wählen Sie die Datei aus, auf die lokal verzichtet werden muss, und klicken Sie auf **Release** .

Hinweis:

- Die Datei wird weiterhin auf diesem bestimmten Endpunkt ausgeführt. Die Erkennung und Quarantäne erfolgt jedoch weiterhin auf allen anderen Hosts.
- Wählen Sie den entsprechenden Dateinamen und -Status aus, um die Quarantänedatei auf mehreren Hosts Massenfreigabe zu geben. Klicken Sie auf **Wählen Sie Aus** , Und wählen Sie aus **Release** .

Wenn Sie in Aktion 12 nicht auf die Datei oder Anwendung lokal vom Gerät verzichten möchten, können Sie den Anwender zum IT-Support umleiten, um die Installation der genehmigten Anwendungen anzufordern.

4. Wenn die Datei oder der Hash in Aktion 14 nicht böswillig ist, führen Sie die folgenden Aktionen aus:

a. In Aktion 15 müssen Sie anhand der Rolle des Anwenders (Abteilung oder Position, die vertrauliche Informationen verarbeitet), der Art der Anwendung (Ransomware, Rootkit usw.) und der Auswirkung der Anwendung (wie viele Anwender betroffen waren) bestimmen, ob die Datei/der Hash ein hohes Risiko oder ein geringes Risiko aufweist.

b. Wenn die Datei in Aktion 16 eine Datei mit hohem Risiko ist, führen Sie die folgenden Aktionen aus:

i. Überprüfen Sie in Aktion 17 die Ergebnisse mit dem Threat Intel-Team.

ii. Führen Sie in Aktion 18 den Malware-Byte-Scan für die Datei aus.

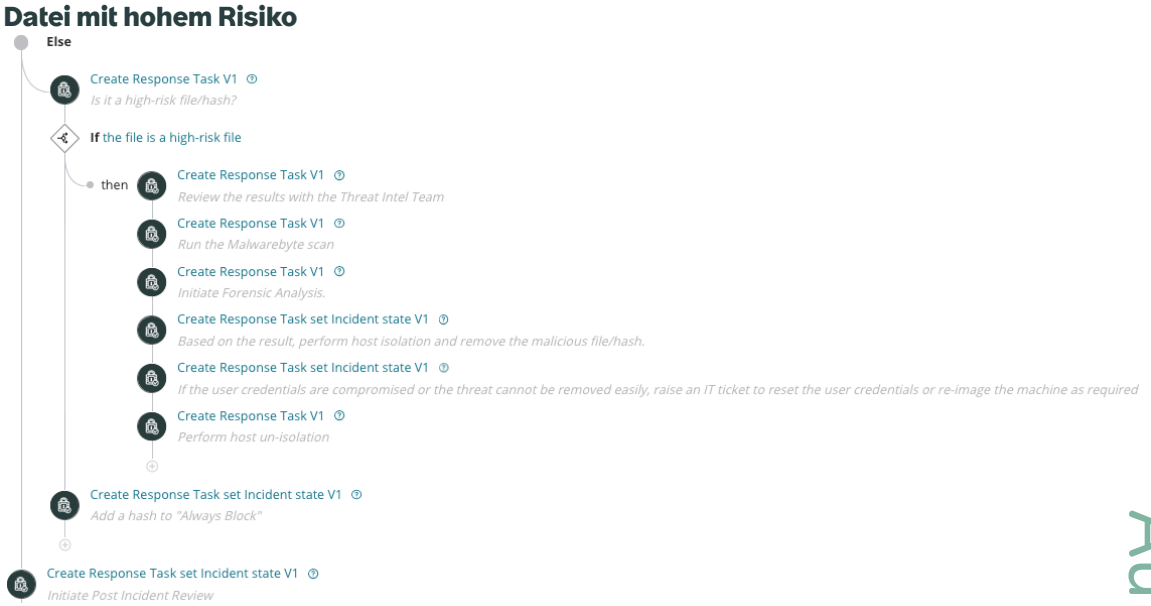
iii. Initiieren Sie in Aktion 19 die forensische Analyse.

iv. Führen Sie in Aktion 20 basierend auf dem Ergebnis der forensischen Analyse die Host-Isolierung durch, und entfernen Sie die schädliche Datei/den schädlichen Hash.

v. Wenn in Aktion 21 die Anwenderanmeldeinformationen gefährdet sind oder die Bedrohung nicht einfach entfernt werden kann, erstellen Sie ein IT-Ticket, um die Anwenderanmeldeinformationen zurückzusetzen oder den Computer nach Bedarf neu zu erstellen.

vi. Heben Sie in Aktion 22 die Host-Isolierung auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Wenn die Datei in Aktion 23 keine Datei mit hohem Risiko ist, führen Sie die folgenden Aktionen aus:

i. Navigieren zu **CrowdStrike Falcon** > **Konfigurationen** Registerkarte

ii. Navigieren Sie auf der Registerkarte Konfigurationen zu **Präventions-Hashes** > > **Hash Hochladen** > **Fügen Sie den Hash hinzu**an.

iii. Wählen Sie das erforderliche Betriebssystem aus, und wählen Sie aus **Immer Blockieren** .

5. In Aktion 24 wird eine Antwortaufgabe erstellt, damit der Anwender die Überprüfung nach dem Incident abschließen kann, bevor er die Aufgabe schließt.

Playbook für mögliches Passwortspray

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Passwortspray-Warnungen, die durch mehrere fehlgeschlagene Anmeldungen ausgelöst wurden (zu viele Authentifizierungsfehler von mehr als einer IP-Adresse für denselben Anwender).

Richten Sie das Playbook „mögliches Passwortspray“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „mögliches Passwortspray“ einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

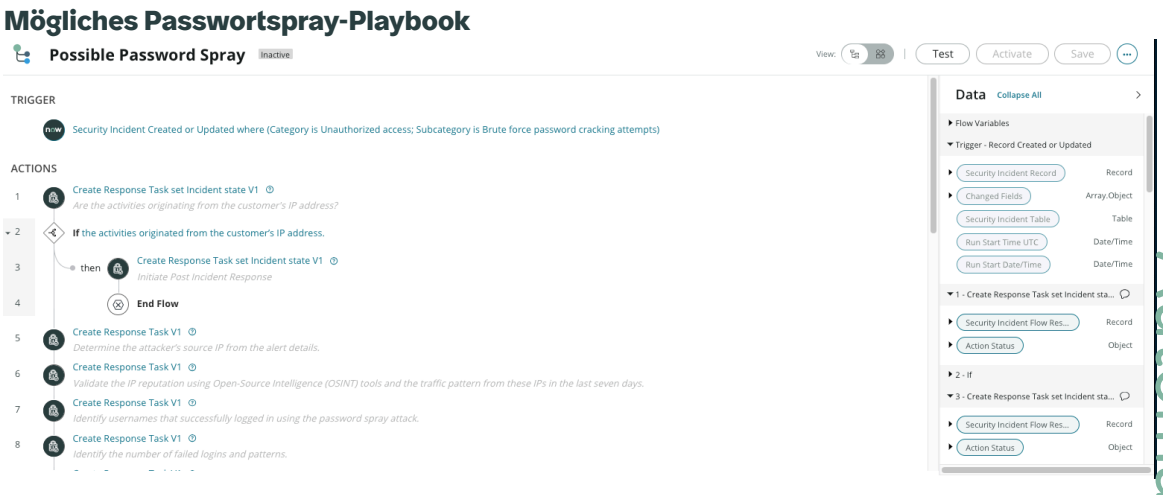
1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.

2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Mögliches Passwortspray** playbook.

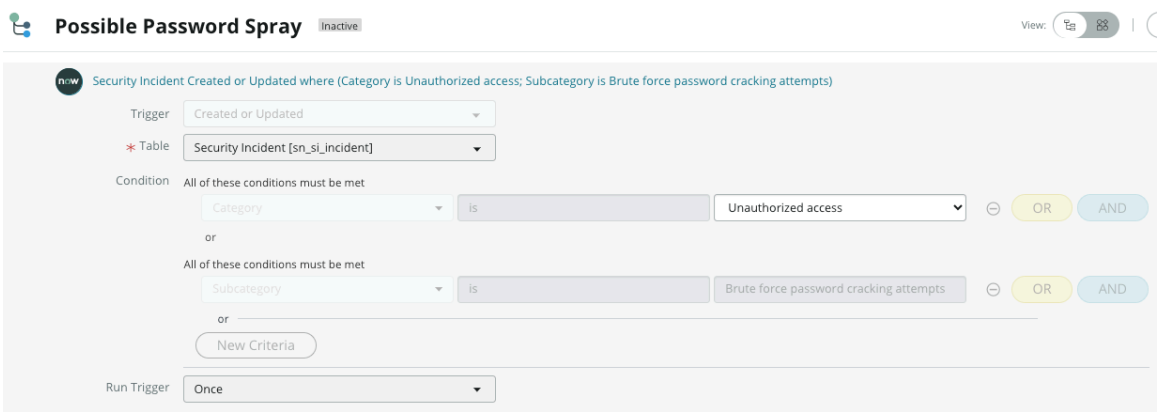
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Sie können eine Kopie des möglichen Passwortspray-Playbook-Flows erstellen und die erforderlichen Änderungen vornehmen.

   Klicken Sie auf , um eine Kopie des Playbook-Flows zu erstellen Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.



4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:
   - **Kategorie** Ist **Nicht autorisierter Zugriff** .
   - **Unterkategorie** Ist **Brute-Force-Passwortknackversuche** .



Verwenden Sie das Playbook „mögliches Passwortspray“

Verwenden Sie dieses Playbook, um Passwortspray-Warnungen zu untersuchen, die durch mehrere fehlgeschlagene Anmeldungen ausgelöst wurden (zu viele Authentifizierungsfehler von mehr als einer IP-Adresse für denselben Anwender). Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die im Playbook „mögliches Passwortspray“ verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

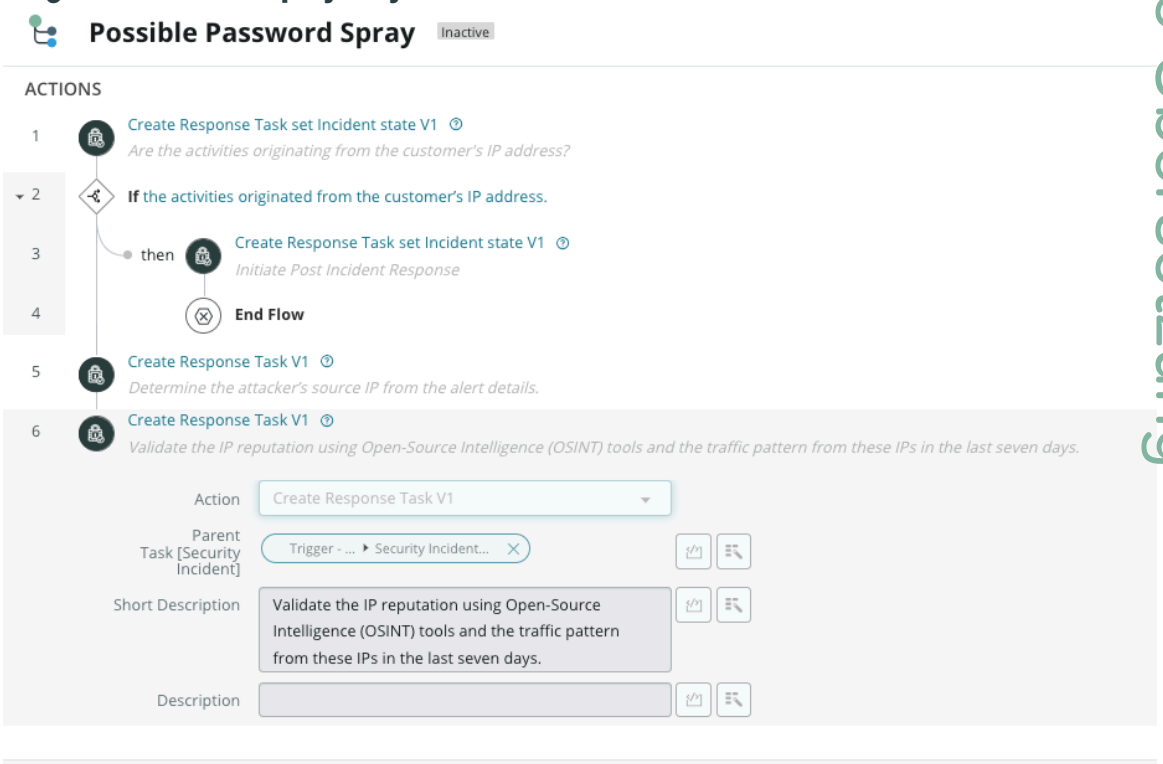
- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Wenn das Playbook ausgelöst wird und mit der Ausführung beginnt, müssen Sie in Aktion 1 überprüfen, ob die Aktivitäten von der IP-Adresse des Kunden stammen.
   Identifizieren Sie die IP-Adressen, die den Passwortspray-Angriff ausführen. Verwenden Sie beispielsweise die TXIDs (Transaktions-IDs) aus der Warnung, und suchen Sie sie anhand der F5-Protokolle.
2. Führen Sie in Aktion 2 die folgenden Aktionen aus, wenn die Aktivitäten von der IP-Adresse des Kunden stammen:
   a. In Aktion 3 müssen Sie eine Überprüfung des möglichen Passwortspray-Angriffs nach dem Incident initiieren.
   b. In Aktion 4 endet der Flow.
3. Wenn die Aktivitäten in Aktion 5 nicht von der IP-Adresse des Kunden stammen, bestimmen Sie die Quell-IP des Angreifers anhand der Warnungsdetails.
4. In Aktion 6 müssen Sie die IP-Reputation mithilfe von Open-Source Intelligence (OSINT)-Tools und das Datenverkehrsmuster dieser IPs in den letzten sieben Tagen validieren.

Mögliches Passwortspray-Playbook



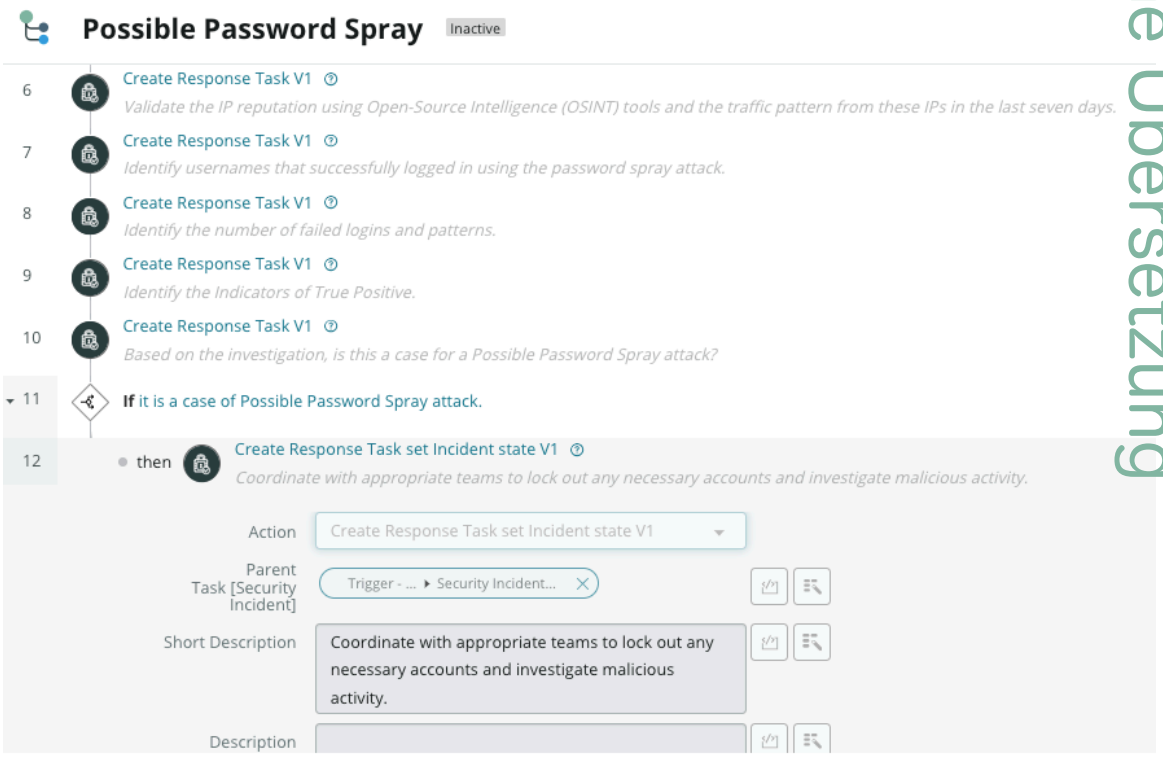
5. In Aktion 7 müssen Sie die Anwendernamen identifizieren, die sich erfolgreich mit dem Password Spray Attack angemeldet haben.
6. In Aktion 8 müssen Sie die Anzahl der fehlgeschlagenen Anmeldungen und Muster identifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. In Aktion 9 müssen Sie die Indikatoren für „wahr positiv“ identifizieren.
   - Überprüfen Sie den Datenverkehr von den Quell-IPs in den letzten 60 Tagen. Kein historischer Datenverkehr kann ein Hinweis auf ein wirklich positives Ergebnis sein.
   - Überprüfen Sie die Anwendernamen-Muster mit Authentifizierungsfehlern und die Anzahl. Je höher die Anzahl, desto höher ist die Wahrscheinlichkeit, dass es sich um ein wirklich positives Ergebnis handelt.
   - Der Anwendername sieht wie eine Wörterbuchbasis aus (von A bis Z) und kann allgemeine Administratornamen wie admin, sysadmin, root usw. haben
   - Derselbe Anwendername kann verschiedene Muster im Sprayangriff haben, z. B. dieselbe Warnung kann Fehler für john.doe, Johnd, jdoe, john_doe, jdoe7 usw. aufweisen. gibt an, dass Angreifer das Anwendernamen-Muster basierend auf allgemeinen Anwendungsfällen erraten.
   - Beachten Sie den Anwender-Agent und die URIs aus den F5-Protokollen im obigen Schritt, und überprüfen Sie, ob sich die IOCs auf die Red Condor-Warnungen beziehen. Wenn sie übereinstimmen, ist es ein wirklich positives Ereignis.
8. In Aktion 10 müssen Sie basierend auf der bisher durchgeführten Untersuchung überprüfen, ob es sich um einen möglichen Passwortspray-Angriff handelt oder nicht.
9. Führen Sie in Aktion 11 die folgenden Aktionen aus, wenn dies ein möglicher Passwortspray-Angriff ist:

   a. In Aktion 12 müssen Sie sich mit den entsprechenden Teams abstimmen, um erforderliche Accounts zu sperren und böswillige Aktivitäten zu untersuchen.

Mögliches Passwortspray-Playbook



   b. In Aktion 13 müssen Sie eine Überprüfung des möglichen Passwortspray-Angriffs nach dem Incident initiieren.

   c. In Aktion 14 endet der Flow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. In Aktion 15 müssen Sie überprüfen, ob dies kein Fall eines möglichen Passwortspray-Angriffs ist.
11. Wenn es sich in Aktion 16 nicht um einen möglichen Passwortspray-Angriff handelt, führen Sie die folgenden Aktionen aus:
    a. In Aktion 17 müssen Sie die bisherigen Ergebnisse dokumentieren.
    b. In Aktion 18 müssen Sie eine Überprüfung des möglichen Passwortspray-Angriffs nach dem Incident initiieren.
    c. In Aktion 19 endet der Flow.
12. In Aktion 20 müssen Sie sich an die Kollegen und den GIR-Manager wenden, um Anleitungen zu erhalten.
13. In Aktion 21 wird eine Antwortaufgabe erstellt, um die Überprüfung nach dem Incident abzuschließen, bevor die Aufgabe geschlossen wird.

Playbook für T1003 – Tools zum Entwerfen von Anmeldeinformationen erkennen

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung eines Incident mit Aktivitäten zum Dumping von Anmeldeinformationen.

Richten Sie das Playbook „T1003 – Tools zum Entwerfen von Anmeldeinformationen erkennen“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „T1003 – Tools zum Entwerfen von Anmeldeinformationen erkennen“ einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

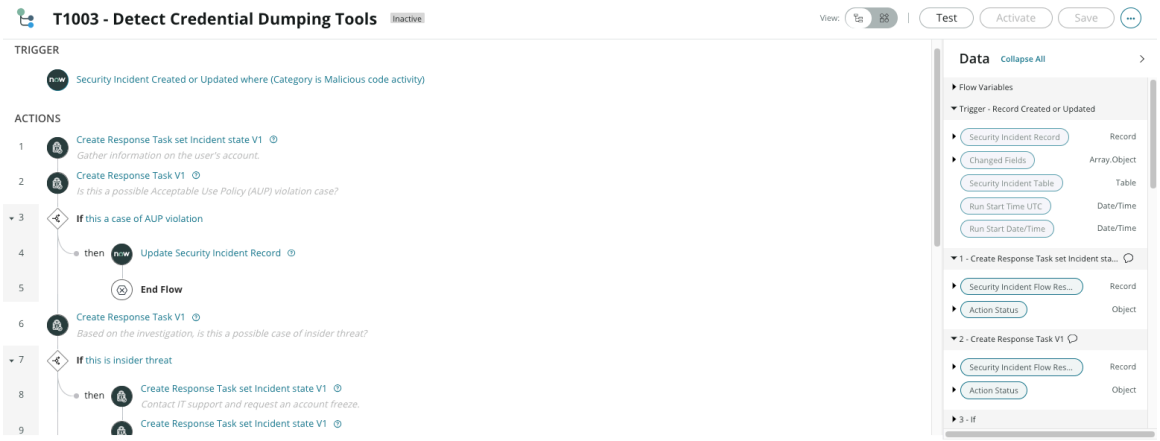
Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **T1003: Tools zum Dumping von Anmeldeinformationen erkennen** playbook.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows „T1003 – Tools für das Entwerfen von Anmeldeinformationen erkennen“ erstellen und die erforderlichen Änderungen vornehmen.

   Klicken Sie auf , um eine Kopie des Playbook-Flows zu erstellen Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

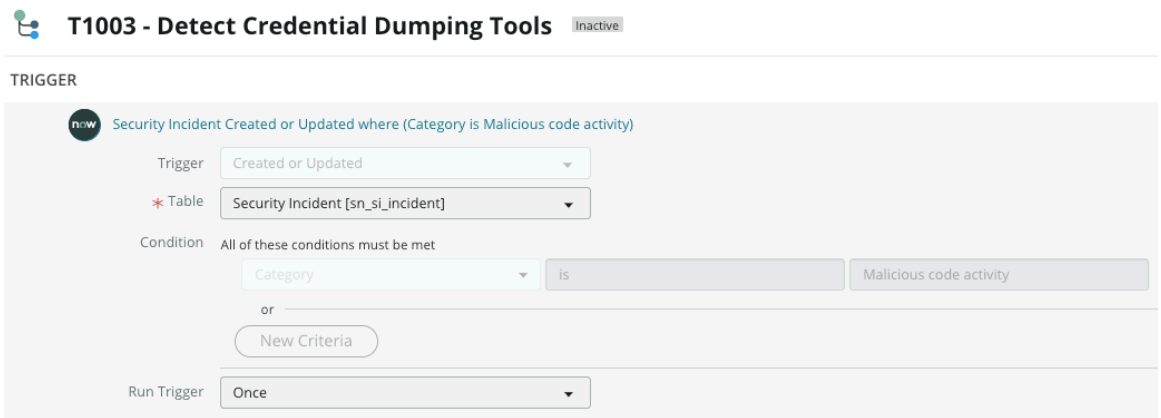
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

T1003 – Playbook für Tools zum Entwerfen von Anmeldeinformationen erkennen



4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der verwendet wird **Kategorie** Ist **Schädliche Codeaktivität** .



Verwenden Sie das Playbook T1003 – Tools zum Entwerfen von Anmeldeinformationen erkennen

Verwenden Sie dieses Playbook, um einen Incident mit Aktivitäten zum Dumping von Anmeldeinformationen zu untersuchen. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die im Playbook T1003 – Tools für Anmeldeinformationsdumping erkennen verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

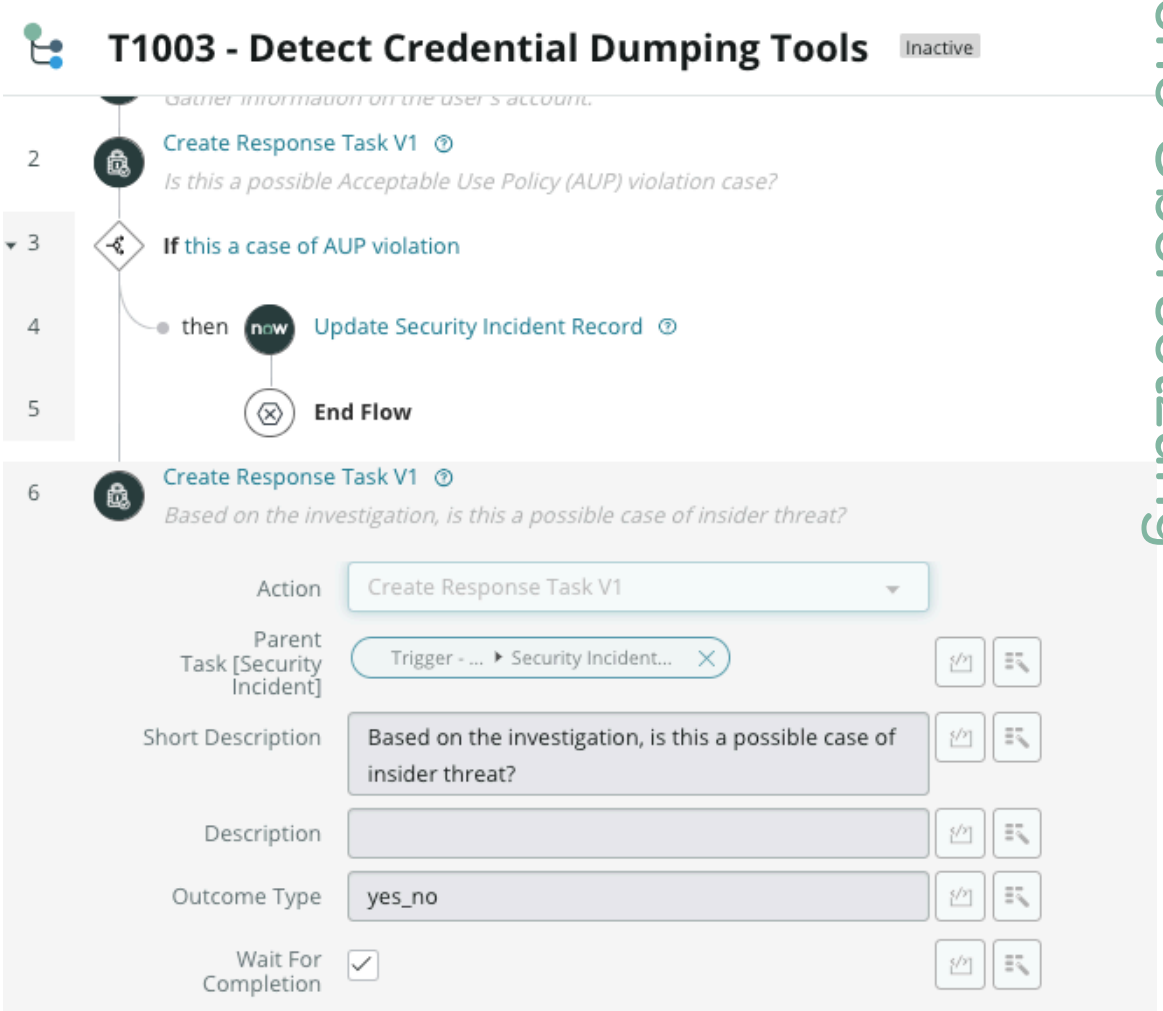
Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, müssen Sie in Aktion 1 Informationen zum Account des Anwenders sammeln.
   - Sie müssen die Hostaktivität überprüfen, um nach verdächtigen Aktivitäten zu suchen.
   - Sie müssen den Besitzer des Servers/Endpunkts/der VM identifizieren und die mit dem Tool korrelierenden Daten erfassen.
   - Sie müssen Informationen zu den anderen Accounts des Anwenders sammeln.
2. In Aktion 2 müssen Sie überprüfen, ob es sich um einen möglichen Verstoßfall (Acceptable Use Policy, AUP) handelt.
   Sie können eine Peer-Review mit den gesammelten Nachweisen durchführen und sich an Ihren regionalen Incident-Manager wenden, ob Sie sich an den Anwender wenden möchten.
3. Wenn es sich in Aktion 3 um einen Verstoß gegen die Richtlinie zur zulässigen Verwendung (Acceptable Use Policy, AUP) handelt, führen Sie die folgenden Aktionen aus:
   a. In Aktion 4 müssen Sie den Security Incident aktualisieren, dass es sich um einen AUP-Verstoß handelt
   b. In Aktion 5 endet der Flow.
4. In Aktion 6 müssen Sie basierend auf der bisher durchgeführten Untersuchung überprüfen, ob es sich um einen möglichen Fall einer internen Bedrohung handelt oder nicht.

T1003 – Playbook für Tools zum Entwerfen von Anmeldeinformationen erkennen



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Führen Sie in Aktion 7 die folgenden Aktionen aus, wenn es sich um einen Fall einer internen Bedrohung handelt:

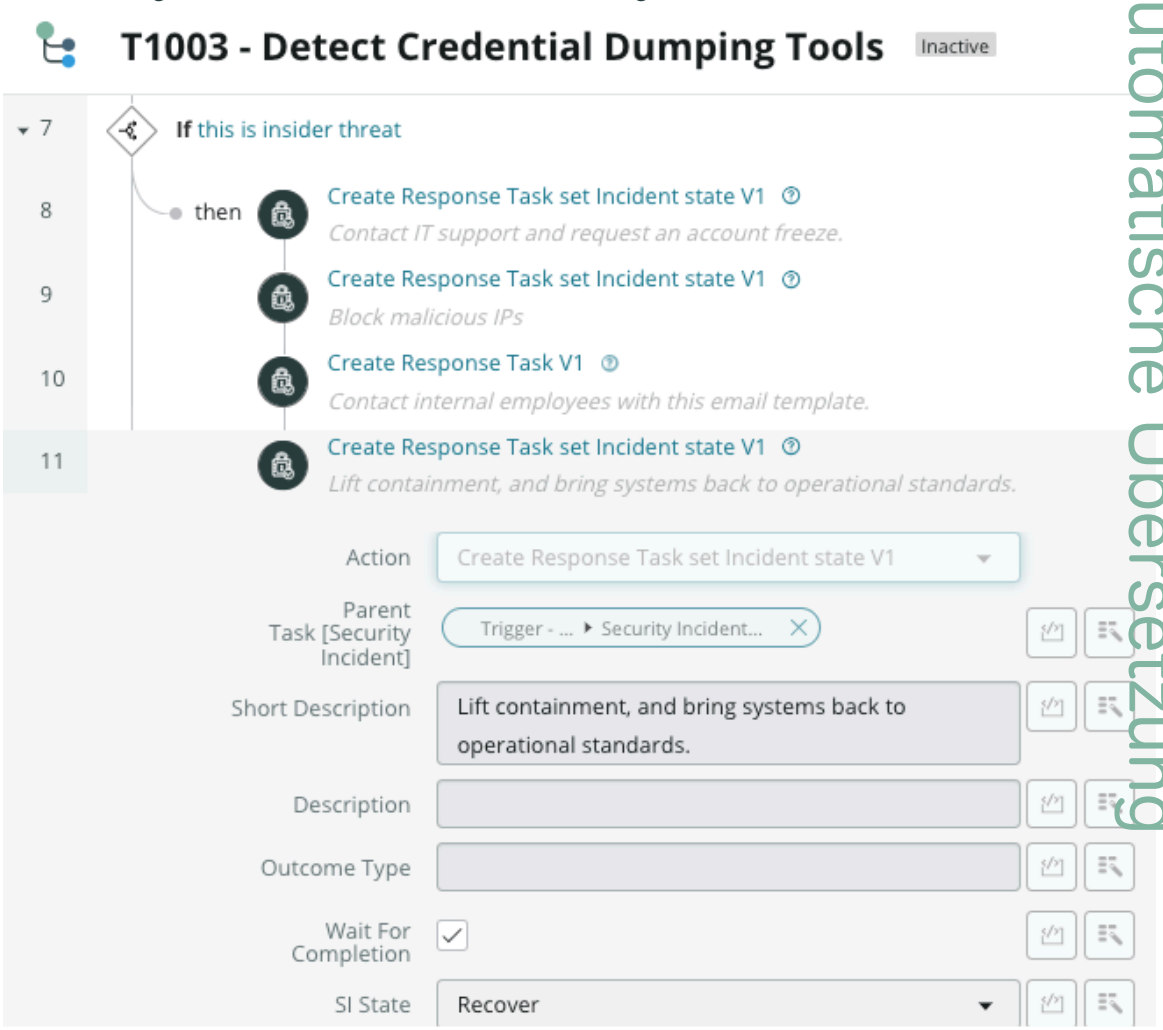
   a. In Aktion 8 müssen Sie sich an den IT-Support wenden und eine Kontosperrung anfordern.

   b. In Aktion 9 müssen Sie schädliche IPs blockieren.

   c. In Aktion 10 müssen Sie interne Mitarbeiter per E-Mail kontaktieren.
   Sie können die bereitgestellte E-Mail-Vorlage verwenden, um Ihre internen Mitarbeiter zu kontaktieren.

   d. In Aktion 11 müssen Sie die Eindämmung aufheben und die Systeme wieder auf Betriebsstandards zurücksetzen.
   Der Flow endet.

Antwortaufgaben zum Aufheben der Eindämmung



6. Wenn es sich in Aktion 12 nicht um eine interne Bedrohung handelt, müssen Sie in Aktion 13 eine Peer-Review durchführen, um festzustellen, ob dies der Ausschlussliste hinzugefügt werden muss.
   Der Flow endet.

7. In Aktion 14 wird eine Antwortaufgabe erstellt, um die Überprüfung nach dem Incident abzuschließen, bevor die Aufgabe geschlossen wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook für Spoofing-Erkennung der E-Mail-Domäne

Dieses Playbook hilft bei der frühzeitigen Selektierung von von von Anwendern gemeldeten Phishing-Übermittlungen, indem es den Analysten auf die Möglichkeit einer Look-like-Domäne in der E-Mail-Adresse des Phisher aufmerksam macht.

Das Playbook „Spoofing-Erkennung für E-Mail-Domäne“ sucht nach einer Ähnlichkeitsübereinstimmung zwischen der Absender-E-Mail-Domäne des Phisher mit einem vertrauenswürdigen Domänennamen, der im Repository erkennbarer Elemente vorhanden ist. Wenn eine gefälschte Übereinstimmung der Absender-E-Mail-Domäne vom Playbook identifiziert wurde, werden die Analysten mit einem Tag benachrichtigt.

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Incident-Untersuchung bietet. Jeder Entscheidungspunkt im Playbook wurde in eine ergebnisgesteuerte Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis solcher Aufgaben.

Richten Sie das Playbook „E-Mail-Spoof-Erkennung“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „E-Mail-Spoof-Erkennung“ einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

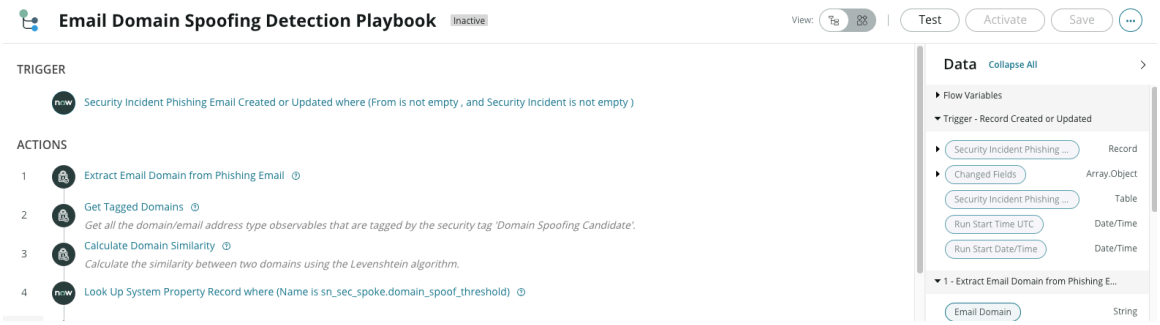
Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Playbook für E-Mail-Domänen-Spoofing-Erkennung** playbook.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows „E-Mail-Domänen-Spoofing-Erkennung“ erstellen und die erforderlichen Änderungen vornehmen.

   Klicken Sie auf , um eine Kopie des Playbook-Flows zu erstellen Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

   Playbook für E-Mail-Domänen-Spoofing-Erkennung

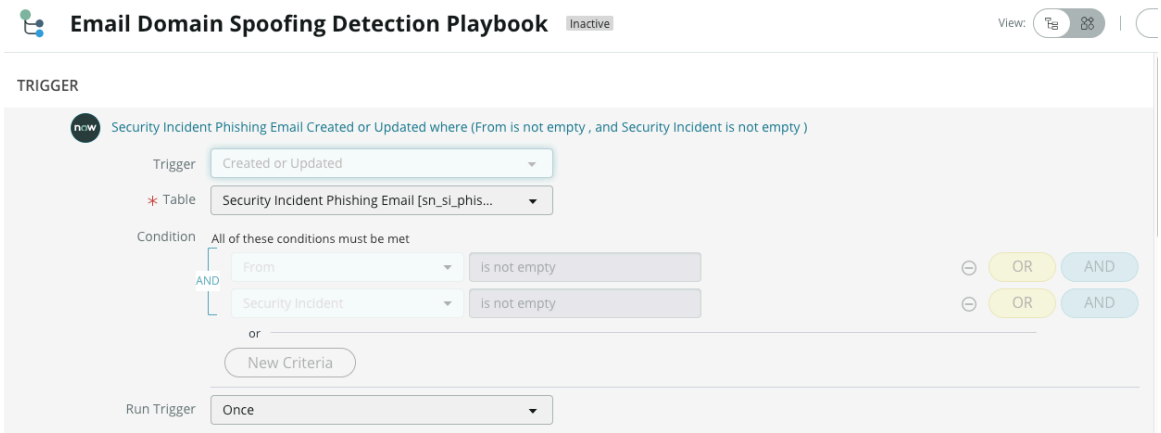
   

4. Aktivieren Sie die Playbooks.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
- Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:
   - **Von** Ist nicht **Leer** .
   - **Security Incident** Ist nicht **Leer** .



Verwenden Sie das Playbook „Spoofing-Erkennung für E-Mail-Domäne“

Verwenden Sie dieses Playbook, um eine Ähnlichkeitsübereinstimmung zwischen der Absender-E-Mail-Domäne des Phisher und einem vertrauenswürdigen Domänennamen im Repository erkennbarer Elemente zu finden. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die im Playbook „E-Mail-Domänen-Spoofing-Erkennung“ verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

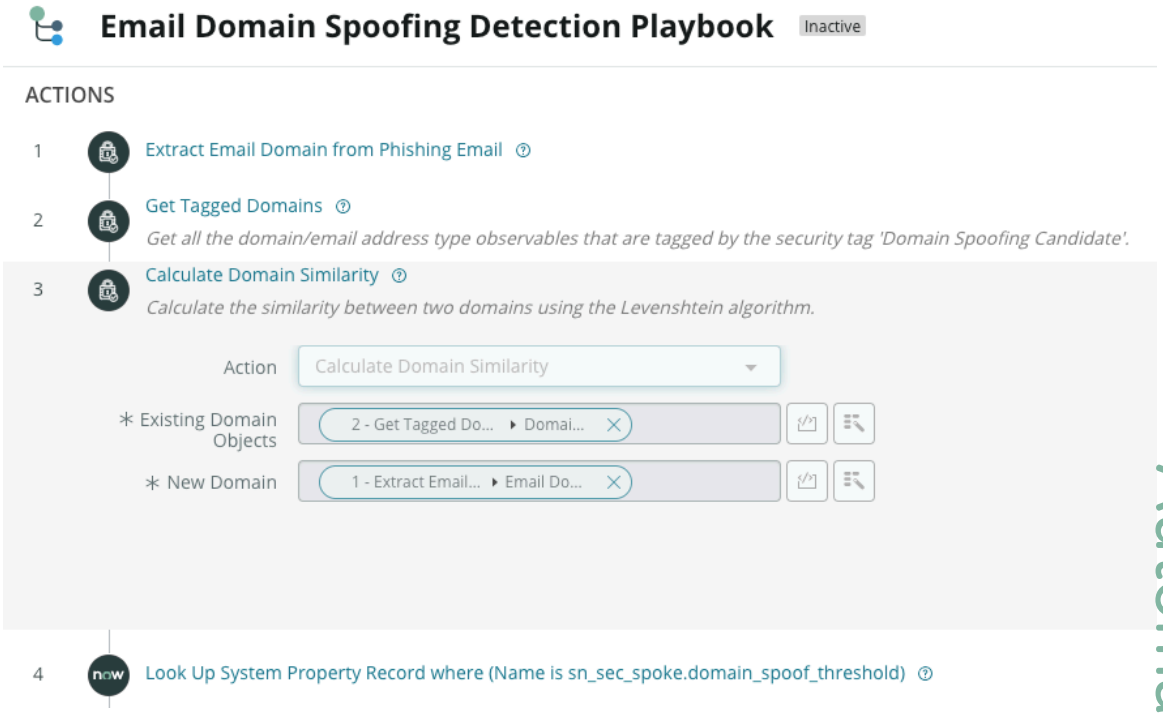
Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, extrahiert das Playbook in Aktion 1 die E-Mail-Domäne aus der Phishing-E-Mail.
2. In Aktion 2 ruft das Playbook alle erkennbaren Elemente vom Typ Domäne/E-Mail-Adresse ab, die vom Sicherheits-Tag „Domänen-Spoofing-Kandidat“ gekennzeichnet sind.
3. In Aktion 3 berechnet das Playbook die Ähnlichkeit zwischen der getaggten Domäne und der E-Mail-Domäne mithilfe des Levenshtein-Algorithmus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

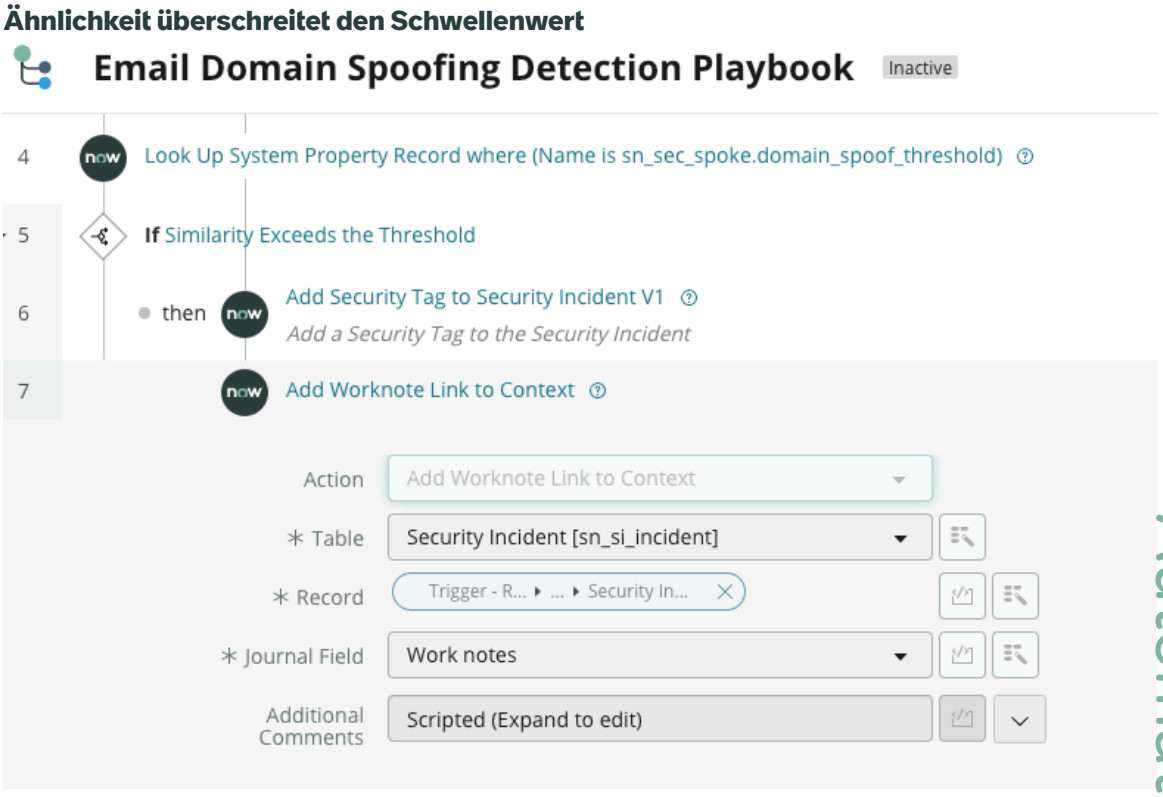
Playbook für E-Mail-Domänen-Spoofing-Erkennung



4. In Aktion 4 sucht das Playbook basierend auf den folgenden Bedingungen nach dem Systemeigenschaftsdatensatz:
   - Name ist sn_sec_Spoke.Domain_Spoof_threshold, (ODER)
   - Der Name liegt von a bis z. Wenn mehrere Datensätze gefunden werden, wird nur der erste Datensatz zurückgegeben.
5. In Aktion 5 überprüft das Playbook basierend auf der bisher durchgeführten Untersuchung, ob die Ähnlichkeit der beiden Domänen den Schwellenwert überschreitet oder nicht.
   Wenn die Ähnlichkeit der beiden Domänen den Schwellenwert nicht überschreitet, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow endet. Wenn die Ähnlichkeit der beiden Domänen den Schwellenwert überschreitet, werden die Aktionen 6 und 7 ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. In Aktion 6 fügt das Playbook dem Security Incident das Sicherheits-Tag „E-Mail-Domäne Spoofing“ hinzu.
7. In Aktion 7 fügt das Playbook dem Kontext mithilfe der Skriptoption einen Arbeitsnotizlink hinzu.
8. In Aktion 8 endet der Flow.

Playbook für Tippfehler besetzte Domäne

Dieses Playbook bietet systematische Verfahren für die Untersuchung falsch geschriebener Domänen und die Zusammenarbeit mit der Rechtsabteilung der Organisation bei Abnahmen. Tippfehlerdomänen sind absichtlich falsch geschriebene Domänennamen, die legitimen Domänen sehr ähnlich sind. Angreifer nutzen Rechtschreibfehler, um sie zu einer ungewollten Website zur finanziellen Ausnutzung oder anderen böswilligen Aktivitäten zu leiten.

Die Tippfehler besetzten Domänen werden dem Security Operations-Team aus verschiedenen Quellen gemeldet, z. B. Lösungen zum Schutz vor digitalen Risiken (digitale Schatten) und Bedrohungsintelligenz-Plattformen (Anomali Threatstream). Nachdem ein Security Incident erstellt wurde, hilft diese Lösung zu identifizieren, ob die Domäne tatsächlich eine Tippbesatzungsdomäne ist. Wenn es sich um eine Tippfehlerbesatzungsdomäne handelt, kann der Analysten sie der Rechtsabteilung melden, damit weitere Maßnahmen ergriffen werden können.

Der Workflow wird basierend auf einem vorhandenen Playbook erstellt, das einen konsistenten und effizienten Ansatz für die Incident-Untersuchung bietet. Jeder Entscheidungspunkt im Playbook wurde in eine ergebnisgesteuerte Aufgabe konvertiert, und der Flow ändert die Richtung basierend auf dem Ergebnis solcher Aufgaben.

Richten Sie das Playbook „Tippbesatzungsdomäne“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „Tippbesatzungsdomäne“ einzurichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

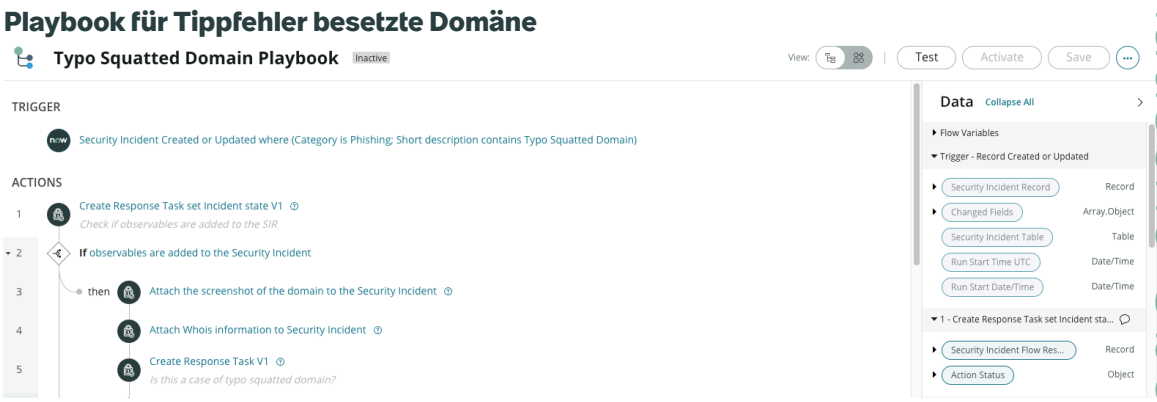
- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Tippfehler Besetzte Domäne** playbook.
3. **Wahlweise:** Sie können eine Kopie des Playbook-Flows für Tippfehlerbesatzungen erstellen und die erforderlichen Änderungen vornehmen.

   (Optional) Klicken Sie auf , um eine Kopie des Playbook-Flows zu erstellen Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

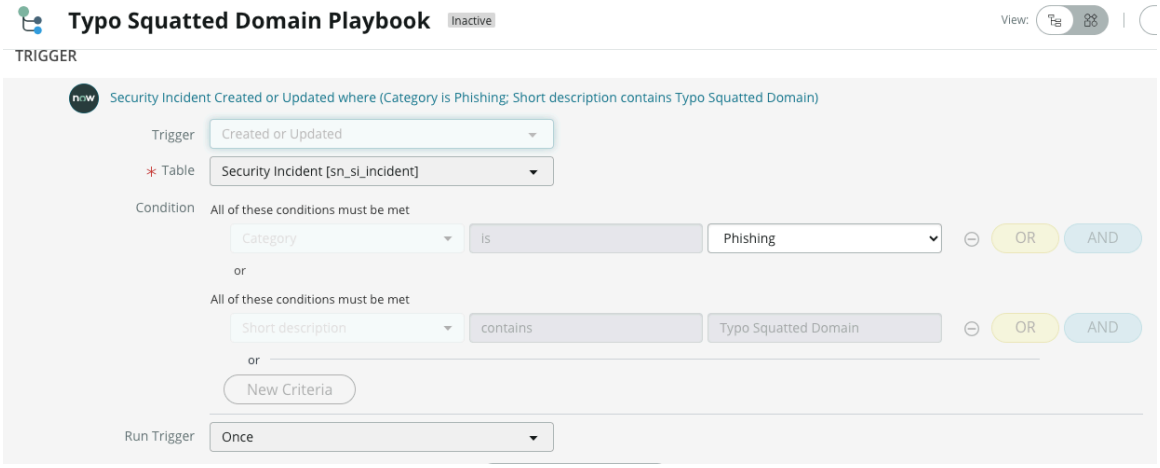


4. Aktivieren Sie die Playbooks.
   - Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   - Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Kategorie** Ist **Phishing** .
- **Kurzbeschreibung** Enthält **Tippfehler Besetzte Domäne** .



Verwenden Sie das Playbook für Tippfehlerbesatzungsdomäne

Verwenden Sie dieses Playbook, um falsch geschriebene Domänen zu untersuchen und mit der Rechtsabteilung der Organisation zusammenzuarbeiten, um Aufnahmen zu machen. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die im Playbook „Tippbesatzte Domäne“ verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

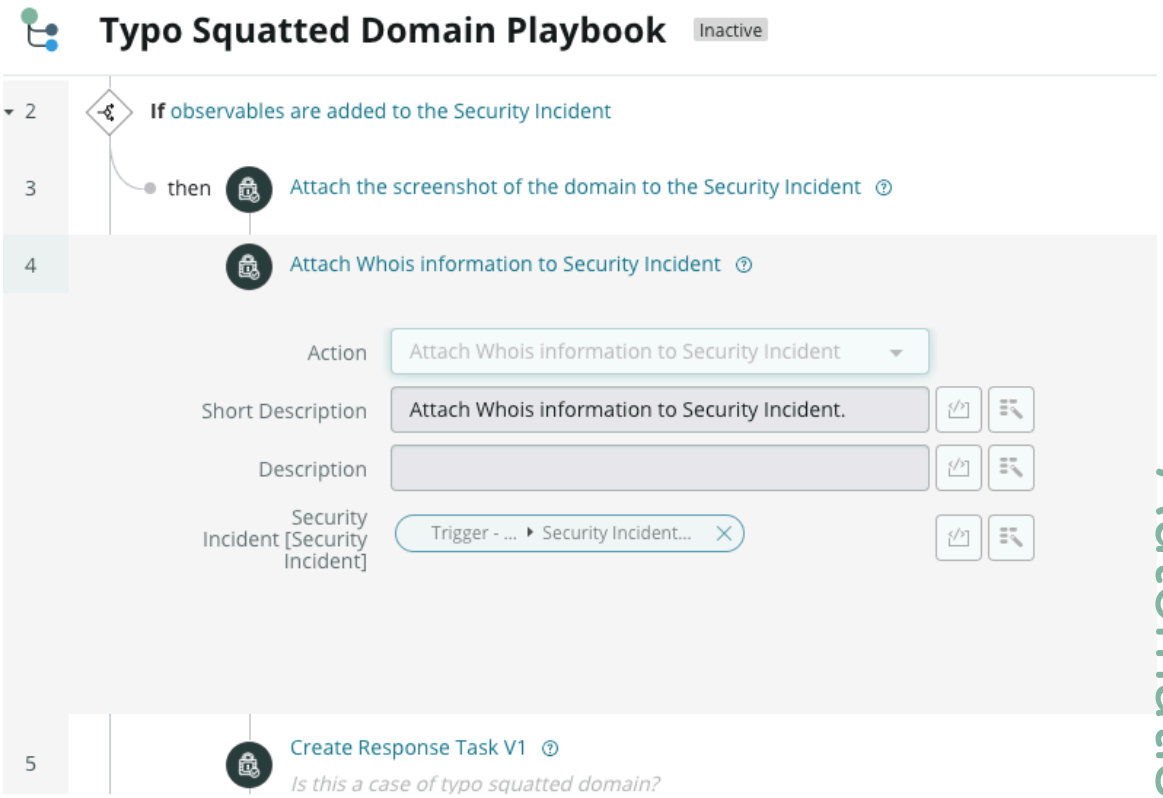
Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, müssen Sie in Aktion 1 überprüfen, ob die erkennbaren Elemente der Security Incident Response (SIR) hinzugefügt werden.
   Wenn die erkennbaren Elemente nicht zu SIR hinzugefügt werden, fügen Sie die erkennbaren Elemente hinzu, bevor Sie fortfahren. Wenn die erkennbaren Elemente nicht verfügbar sind, wird Aktion 10 ausgeführt, und der Security Incident wird geschlossen.
2. Wenn in Aktion 2 die erkennbaren Elemente dem Security Incident hinzugefügt werden, werden die folgenden Aktionen ausgeführt.
3. In Aktion 3 müssen Sie den Screenshot der Domäne mit Tippfehler an den Security Incident anhängen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook für Tippfehler besetzte Domäne



4. In Aktion 4 müssen Sie die Whois-Informationen an den Security Incident anhängen.
5. In Aktion 5 überprüft das Playbook basierend auf der bisher durchgeführten Untersuchung, ob es sich um einen Fall einer Tippbesatzungsdomäne handelt oder nicht.
   Wenn dies kein Fall einer Domäne mit Tippfehler ist, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow endet.
6. Wenn dies in Aktion 6 ein Fall einer Domäne mit Tippfehler ist, wird Aktion 7 ausgeführt.
7. In Aktion 7 müssen Sie eine E-Mail senden, die Rechtsabteilung und andere erforderliche Teams darüber informieren, dass es sich um einen Fall einer Domäne mit Tippfehler handelt, und die erforderlichen Maßnahmen ergreifen, um sie zu beseitigen.
   Wenn dies kein Fall einer Domäne mit Tippfehler ist, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow endet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fall einer Domäne mit Tippfehlerbesatz

8. In Aktion 9 wird eine Antwortaufgabe erstellt, mit der Sie die Überprüfung nach dem Incident abschließen können, bevor Sie die Aufgabe schließen.

Playbook für Anmeldeinformations-Sniffing

Dieses Playbook bietet Systemkorrekturschritte zum Untersuchen eines Incidents mit Aktivitäten zum Sniffing von Anmeldeinformationen, die über durchgeführt werden `sys_installation_exit`Tabelle in einer ServiceNow-Instanz.

Das Playbook „Anmeldeinformations-Sniffing“ bietet ein Skriptfeld zum Verarbeiten der Datenbankanmeldungen (DB), Single Sign-on (SSO) und LDAP (Lightweight Directory Access Protocol), indem die Datensätze auf verwendet werden `sys_installation_exit`Tabelle. Diese privilegierten Skripting-Felder ermöglichen das Abhören von Anwenderanforderungen und Parametern während der Anmeldung an die Instanzen, einschließlich Anwenderanmeldeinformationen wie Anwendername und Passwort.

Ein böswilliger Anwender kann ein Skript erstellen, um die Anwenderanforderungen abzuhören und diese Anforderungen in der Instanz zu protokollieren. Die `sys_installation_exit`Die Tabelle in einer Instanz definiert die Regeln für die Verarbeitung der an- und Abmeldeaktivitäten aller Anwender in dieser Instanz.

Richten Sie das Playbook „Anmeldeinformations-Sniffing“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „Anmeldeinformations-Sniffing“ einzurichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

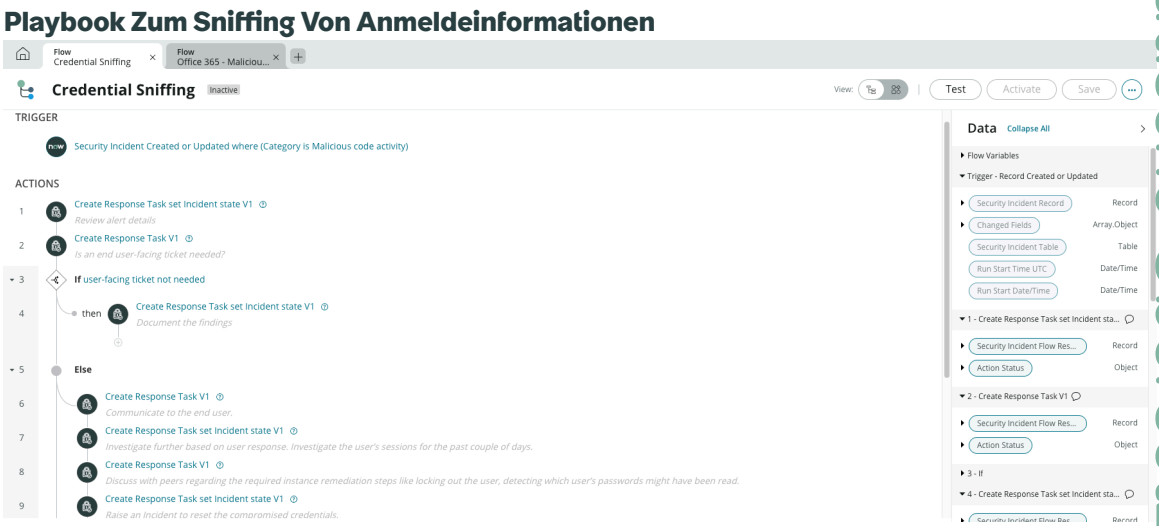
- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Sniffing Von Anmeldeinformationen** playbook.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „Anmeldeinformations-Sniffing“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie aus Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.



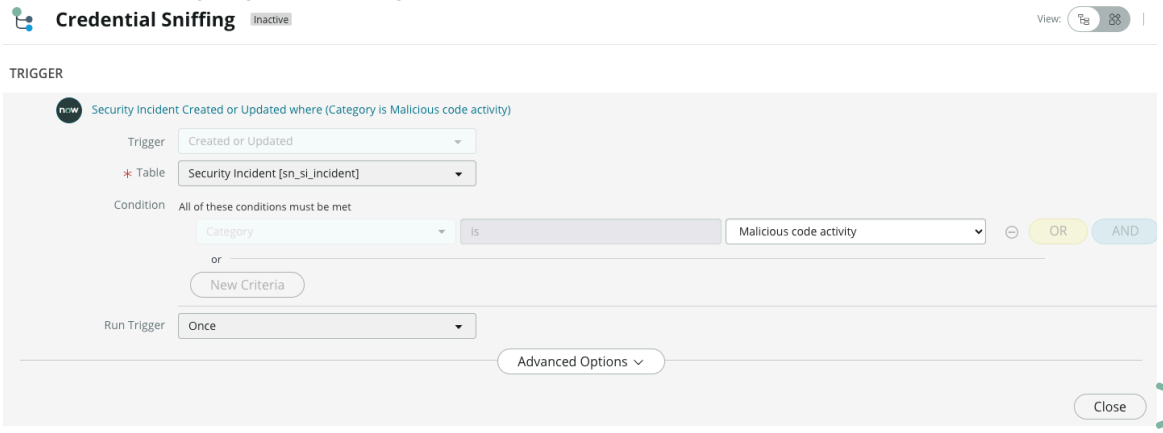
4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der verwendet wird **Kategorie** Ist **Schädliche Codeaktivität** .

Auslöserbedingung für Sniffing von Anmeldeinformationen



Verwenden Sie das Playbook „Anmeldeinformations-Sniffing“

Verwenden Sie dieses Playbook, um einen Incident zu untersuchen, der Aktivitäten zum Sniffing von Anmeldeinformationen umfasst, die über durchgeführt werden *sys_installation_exit*Tabelle in einer ServiceNow-Instanz. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Anmeldeinformations-Sniffing“ verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, überprüfen Sie in Aktion 1 die folgenden Warnungsdetails.
   - Instanz
   - Sitzungs-ID
   - Transaktion-ID
   - _RAW: Stellt das gesamte Skript bereit.

   Beispielskript:

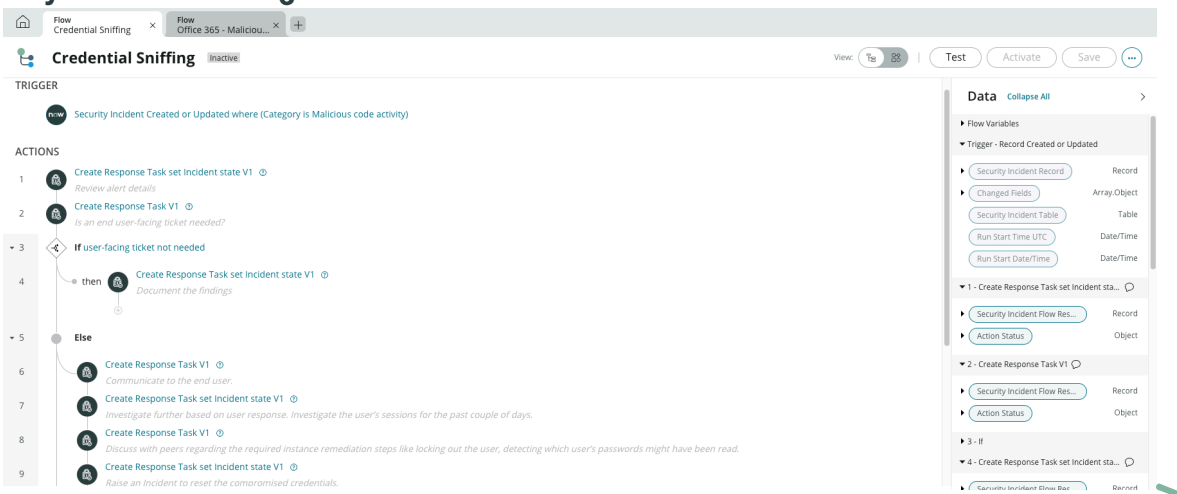
   ```
   Var pass= request.getParameter(“user_password”);
   Gs.log(pass);
   ```

2. Überprüfen Sie in Aktion 2 basierend auf den bisher erfassten Daten, ob für diese Warnung ein Endanwenderticket erforderlich ist oder nicht.
3. Wenn die Warnung in Aktion 3 kein Endanwenderticket erfordert, dokumentieren Sie in Aktion 4 die bisherigen Ergebnisse.
   Der Flow endet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook Zum Sniffing Von Anmeldeinformationen



4. Wenn die Warnung in Aktion 5 ein Endanwenderticket erfordert, führen Sie die folgenden Schritte aus:

   a. Informieren Sie den Endanwender in Aktion 6, dass die Warnung ein Endanwenderticket erfordert.

   b. Untersuchen Sie in Aktion 7 basierend auf der Antwort des Anwenders und den Sitzungen des Anwenders in den letzten Tagen weiter.

   c. Besprechen Sie in Aktion 8 mit Kollegen die Korrekturschritte für die Instanz, z. B. das Sperren des Anwenders und das Erkennen der Passwörter des Anwenders, die möglicherweise gelesen wurden.

   d. Lösen Sie in Aktion 9 einen Incident oder ein Ticket aus, um die Anmeldeinformationen des gefährdeten Anwenders zurückzusetzen.

   e. Heben Sie in Aktion 10 die Eindämmung auf, und bringen Sie die Systeme wieder auf Betriebsstandards zurück
   Der Flow endet.

5. Schließen Sie in Aktion 11 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für T1070 – Windows-Ereignisprotokolle gelöscht

Dieses Playbook bietet Korrekturschritte zur Untersuchung von Incidents, die Ereignistypen nachverfolgen, bei denen der Anwender Sicherheitsprotokolle entfernt. Wenn das Sicherheitsprotokoll gelöscht wird, werden die Ereignisse 517 und 1102 unabhängig vom Status der Audit-Systemereignisrichtlinie protokolliert.

Diese Warnung kann die folgenden Ereignistypen nachverfolgen:

- **Ereignis 517** : Die Felder Primär. Anwendername und Client-Anwendername geben den Anwender an, der das Protokoll gelöscht hat. Der primäre Anwendername entspricht dem System, und der Anwendername des Clients gibt den Anwender an, der das Protokoll gelöscht hat.
- **Ereignis 1102** : Die Felder „Account-Name“ und „Domänenname“ geben den Anwender an, der das Protokoll gelöscht hat. Mit der Anmelde-ID können Sie rückwärts mit dem Anmeldereignis und anderen während derselben Anmeldesitzung protokollierten Ereignissen korrelieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie das Playbook T1070 – gelöschte Windows-Ereignisprotokolle ein

Führen Sie die folgenden Schritte aus, um das Playbook T1070 – gelöschte Windows-Ereignisprotokolle einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **T1070: Windows-Ereignisprotokolle gelöscht** playbook.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows T1070 – gelöschte Windows-Ereignisprotokolle, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie aus ••• Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

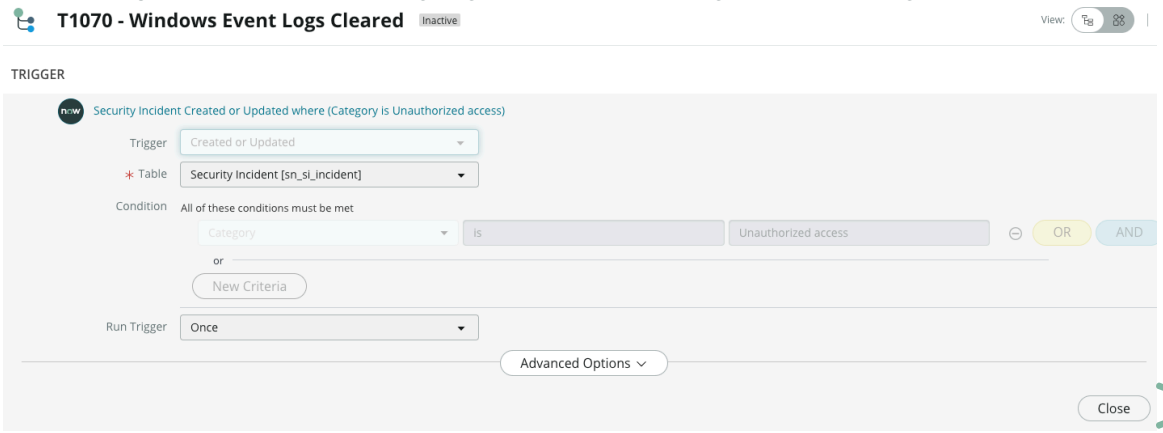
4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der verwendet wird **Kategorie** Ist **Nicht autorisierter Zugriff** .

T1070: Playbook-Auslöserbedingung für Windows-Ereignisprotokolle gelöscht



Verwenden Sie das Playbook T1070 – gelöschte Windows-Ereignisprotokolle

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die Ereignistypen nachverfolgen, bei denen der Anwender Sicherheitsprotokolle entfernt. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook T1070 – gelöschte Windows-Ereignisprotokolle verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, rufen Sie in Aktion 1 die Anwenderdetails aus der Warnung ab.
2. Überprüfen Sie in Aktion 2, ob der Anwender identifiziert wurde oder nicht.
3. Wenn der Anwender in Aktion 3 nicht identifiziert wurde, führen Sie die folgenden Schritte aus:

   a. Überprüfen Sie in Aktion 4 die CMDB (Configuration Management Database) auf Details zum Hostbesitzer.

   b. Überprüfen Sie in Aktion 5, ob der Anwender aus der CMDB identifiziert wurde oder nicht.

      Wenn der Anwender aus der CMDB identifiziert wurde, wird in Aktion 5 eine manuelle Antwortaufgabe erstellt, und der Flow endet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wenn der Anwender in Aktion 6 nicht über die CMDB identifiziert wurde, führen Sie die folgenden Schritte aus:

i. Erstellen Sie in Aktion 7 einen Incident, um den Systembesitzer und die Person zu identifizieren, die die Protokolle gelöscht hat.

ii. Überprüfen Sie in Aktion 8, ob der Anwender nach dem Auslösen eines Incident identifiziert wurde oder nicht.

Wenn der Anwender nach dem Auslösen eines Incident identifiziert wurde, wird in Aktion 8 eine manuelle Antwortaufgabe erstellt, und der Flow endet.

iii. Wenn der Anwender in Aktion 9 nach dem Auslösen eines Incident nicht identifiziert wurde, führen Sie die folgenden Schritte aus:

1. Besprechen Sie in Aktion 10 die nächste Vorgehensweise mit Kollegen.

2. Isolieren Sie in Aktion 11 das Hostsystem.

3. Entfernen Sie in Aktion 12 alle unerwünschten Dateien, die möglicherweise erstellt wurden, und löschen Sie die nicht autorisierten Accounts.

4. Heben Sie in Aktion 13 die Eindämmung auf, und bringen Sie die Systeme wieder auf Betriebsstandards zurück.

5. Schließen Sie in Aktion 14 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

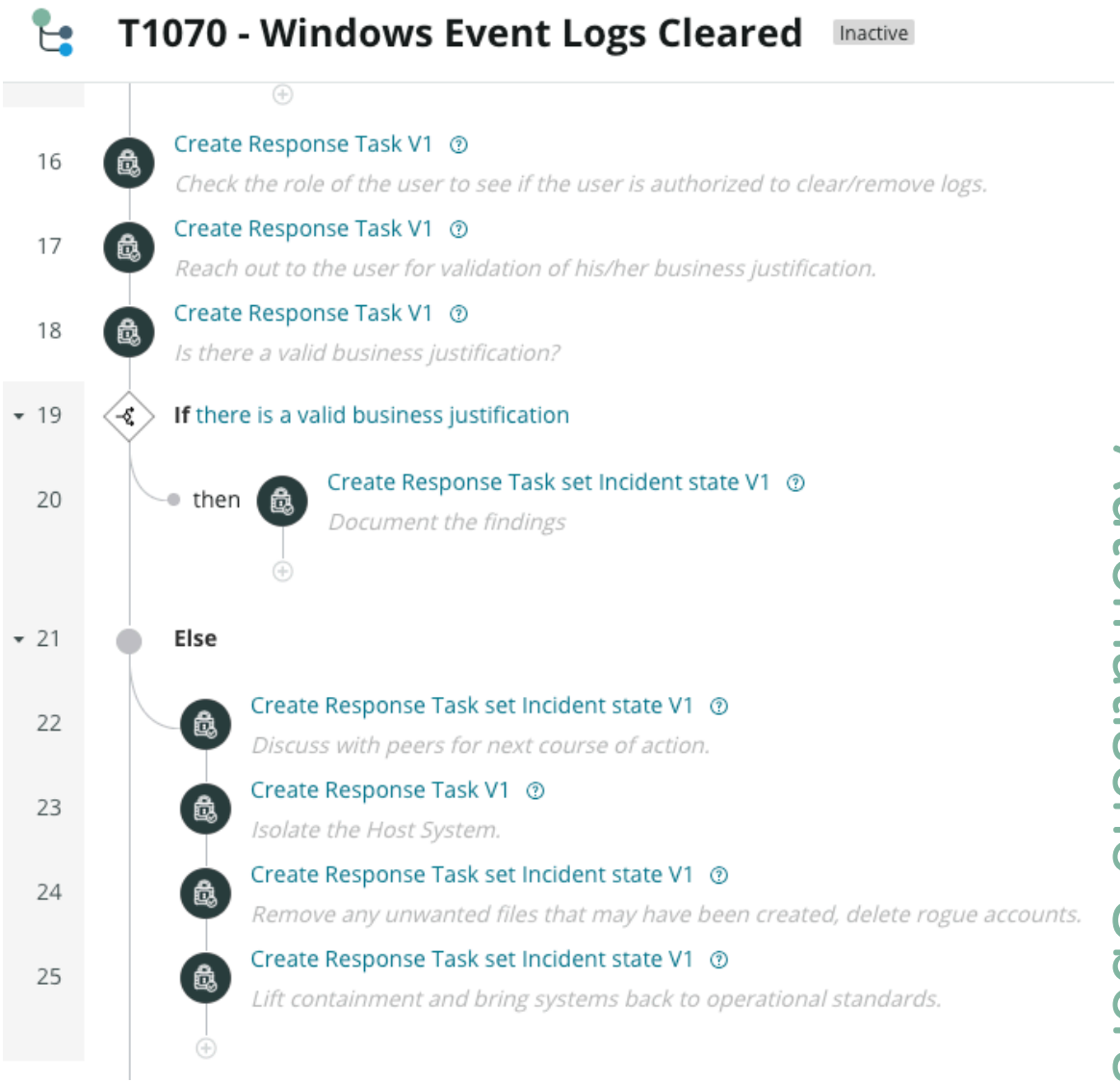
In Aktion 15 endet der Flow.

4. Wenn der Anwender in Aktion 16 identifiziert wurde, überprüfen Sie die Rolle des Anwenders, um festzustellen, ob der Anwender berechtigt ist, Protokolle zu löschen oder zu entfernen.

5. Wenden Sie sich in Aktion 17 an den Anwender, um seine geschäftliche Begründung zu validieren. Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Anwender zu kontaktieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit dem Playbook T1070 – Windows-Ereignisprotokolle wurde gelöscht



Automatische Übersetzung

6. Überprüfen Sie in Aktion 18, ob eine gültige geschäftliche Begründung angegeben wurde oder nicht.
7. Wenn in Aktion 19 eine gültige geschäftliche Begründung angegeben wurde, dokumentieren Sie in Aktion 20 die bisherigen Ergebnisse.
   Der Flow endet.
8. Wenn in Aktion 21 keine gültige geschäftliche Begründung angegeben wurde, führen Sie die folgenden Schritte aus:

   a. Besprechen Sie in Aktion 22 die nächste Vorgehensweise mit Kollegen.

   b. Isolieren Sie in Aktion 23 das Hostsystem.

   c. Entfernen Sie in Aktion 24 alle unerwünschten Dateien, die möglicherweise erstellt wurden, und löschen Sie die nicht autorisierten Accounts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Heben Sie in Aktion 25 die Eindämmung auf, und bringen Sie die Systeme wieder auf Betriebsstandards zurück.
Der Flow endet.

9. Schließen Sie in Aktion 26 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für OSquery der externen Adresse in der Datei „/etc/Hosts“

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, die darauf hinweisen, dass ein interner Hostname oder eine interne Domäne einer externen IP-Adresse im lokalen DNS (/etc/Hosts) eines Linux-Servers zugewiesen wurde.

Richten Sie die OSquery der externen Adresse im Datei „/etc/Hosts“-Playbook ein

Führen Sie die folgenden Schritte aus, um die OSquery der externen Adresse im Datei „/etc/Hosts“-Playbook einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

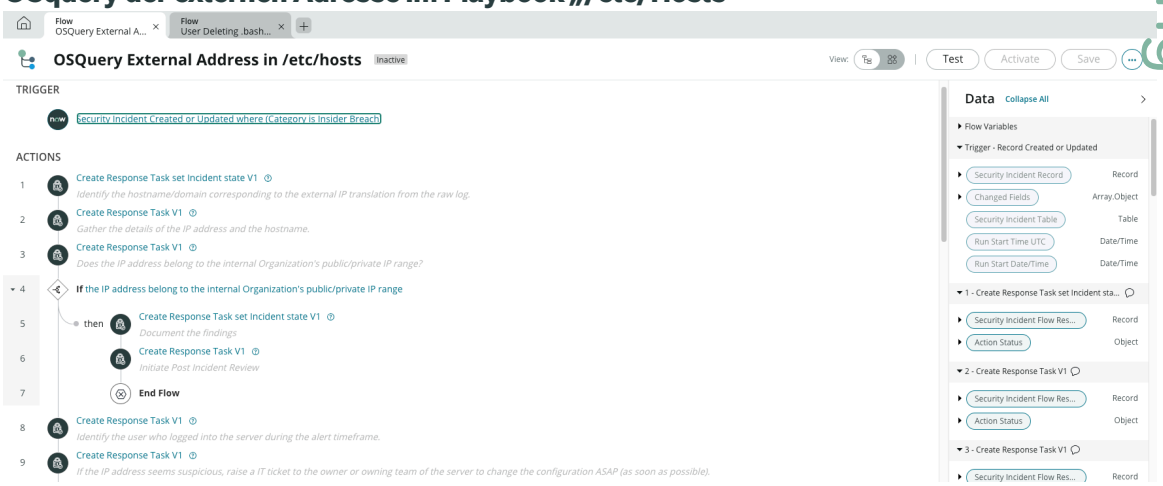
1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.

2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Externe OSquery-Adresse in /etc/Hosts** playbook.

3. Wahlweise: Erstellen Sie eine Kopie der externen OSquery-Adresse im Playbook-Flow „/etc/Hosts“, und nehmen Sie die erforderlichen Änderungen vor.

(Optional) Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie aus Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

OSquery der externen Adresse im Playbook „/etc/Hosts“



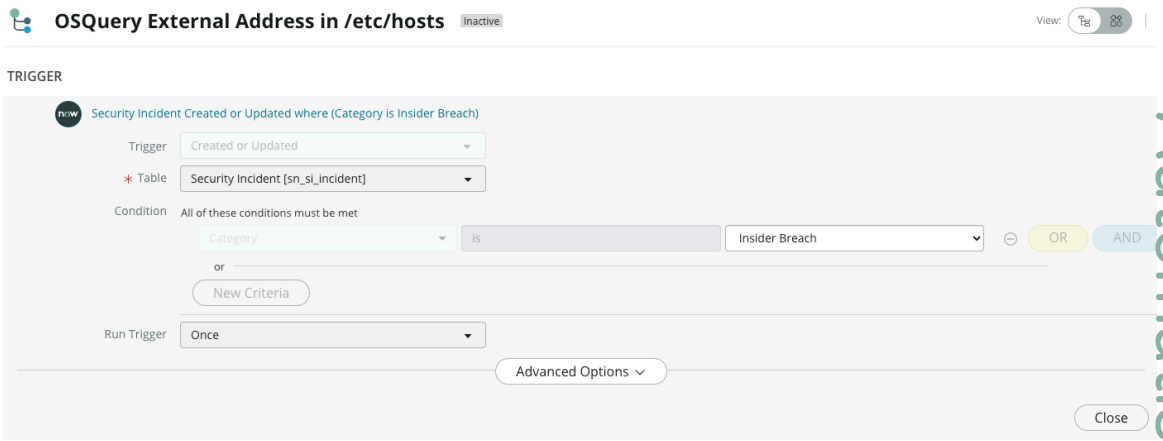
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der verwendet wird **Kategorie** Ist **Insider-Verstoß** .

OSquery der externen Adresse in der Playbook-Auslöserbedingung „/etc/Hosts“



Verwenden Sie die OSquery der externen Adresse im Datei „/etc/Hosts“-Playbook

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die darauf hinweisen, dass ein interner Hostname oder eine interne Domäne einer externen IP-Adresse im lokalen DNS (/etc/Hosts) eines Linux-Servers zugewiesen wurde. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die in der OSquery der externen Adresse im Datei-Playbook /etc/Hosts verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

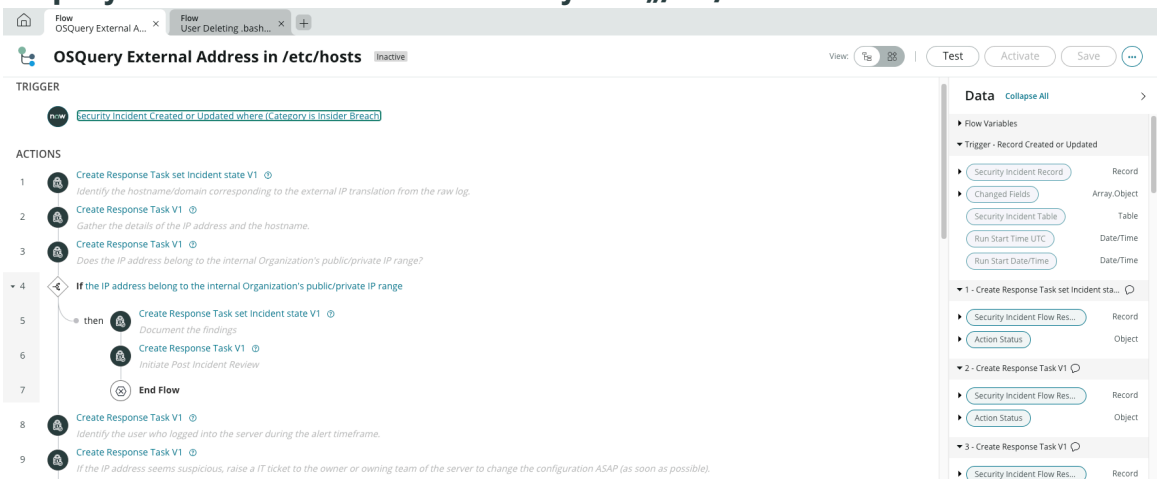
Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, identifizieren Sie in Aktion 1 den Hostnamen oder Domänennamen, der der externen IP-Übersetzung aus dem Rohprotokoll entspricht.
2. Erfassen Sie in Aktion 2 die Details der IP-Adresse und des Hostnamens.
3. Überprüfen Sie in Aktion 3, ob diese IP-Adresse zum öffentlichen/privaten IP-Bereich der internen Organisation gehört oder nicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OSquery der externen Adresse im Datei-Playbook „/etc/Hosts“



4. Führen Sie in Aktion 4 die folgenden Schritte aus, wenn die IP-Adresse zum öffentlichen/privaten IP-Bereich der internen Organisation gehört:

   a. Dokumentieren Sie in Aktion 5 die bisherigen Ergebnisse.

   b. Initiieren Sie in Aktion 6 eine Überprüfung nach Incident.
   In Aktion 7 endet der Flow nach der Überprüfung nach dem Incident.

5. Wenn die IP-Adresse nicht zum öffentlichen/privaten IP-Bereich der internen Organisation gehört, identifizieren Sie in Aktion 8 den Anwender, der sich während des Warnungszeitrahmens beim Server angemeldet hat.
6. Wenn die IP-Adresse in Aktion 9 verdächtig erscheint, erstellen Sie ein IT-Ticket an den Besitzer oder das Serverteam, um die Konfiguration so bald wie möglich zu ändern.
7. Überprüfen Sie in Aktion 10, ob vor und nach dem Hinzufügen des DNS-Eintrags schädliche Aktivitäten auf dem Server aufgetreten sind.
8. Überprüfen Sie in Aktion 11 auf Verbindungen mit der externen IP-Adresse vom Server.
9. Dokumentieren Sie in Aktion 12 die bisherigen Ergebnisse.
10. Überprüfen Sie in Aktion 13, ob die Besitzer- oder Teaminformationen verfügbar sind oder nicht.
11. Führen Sie in Aktion 14 die folgenden Schritte aus, wenn die Besitzer- oder Teaminformationen verfügbar sind:

    a. Wenden Sie sich in Aktion 15 an den Besitzer oder das Serverteam, um zu sehen, ob er die Aktivität erkennt.
    Sie können die bereitgestellte E-Mail-Vorlage verwenden, um sich an den Besitzer oder das Team des Servers zu wenden.

    b. Überprüfen Sie in Aktion 16, ob der Besitzer oder das Team eine gültige geschäftliche Begründung angegeben hat oder nicht.

    c. Wenn der angegebene Besitzer oder das angegebene Team in Aktion 17 keine gültige geschäftliche Begründung angegeben hat, endet der Flow.
    Wenn der Besitzer oder das Team jedoch eine gültige geschäftliche Begründung angegeben hat, führen Sie die folgenden Schritte aus:

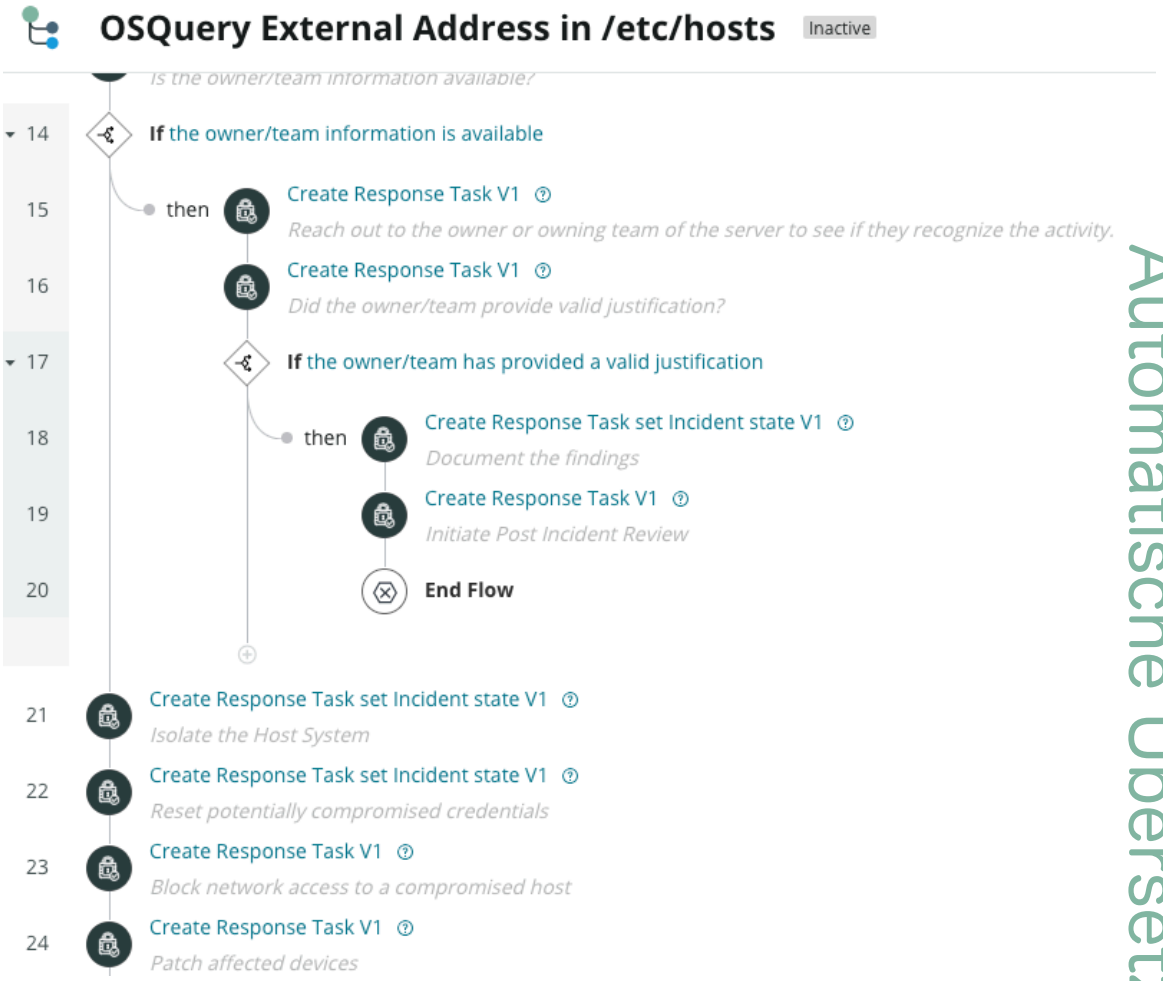
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Dokumentieren Sie in Aktion 18 die bisherigen Ergebnisse.

ii. Initiieren Sie in Aktion 19 eine Überprüfung nach Incident.

In Aktion 20 endet der Flow nach der Überprüfung nach dem Incident.

Verwendung der OSquery der externen Adresse im Datei-Playbook „/etc/Hosts“



12. Wenn in Aktion 21 die Besitzer- oder Teaminformationen nicht verfügbar sind, isolieren Sie das Hostsystem.
13. Setzen Sie in Aktion 22 die potenziell gefährdeten Anmeldeinformationen zurück.
14. Blockieren Sie in Aktion 23 den Netzwerkzugriff auf den gefährdeten Host.
15. In Aktion 24 patchen Sie die betroffenen Geräte.
16. Heben Sie in Aktion 25 die Eindämmung auf, und bringen Sie Systeme wieder auf Betriebsstandards zurück.
17. Schließen Sie in Aktion 26 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für Anwender, der Bash-Verlauf löscht – Cloud

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, die darauf hinweisen, ob jemand versucht hat, den Bash-Verlauf zu entfernen (`.Bash_history`) Datei von einem Linux-Server.

Hinweis:
Sie müssen diese Warnung vorsichtig mindern, da diese Warnungen selten ausgelöst werden und potenziell auf eine interne Bedrohung hindeuten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie das Playbook „Anwender löschen Bash-Verlauf“ ein

Führen Sie die folgenden Schritte aus, um das Playbook „Anwender löschen Bash-Verlauf“ einzurichten.

Vorbereitungen
Erforderliche Rolle:

- sn_si.admin
- flow_designer

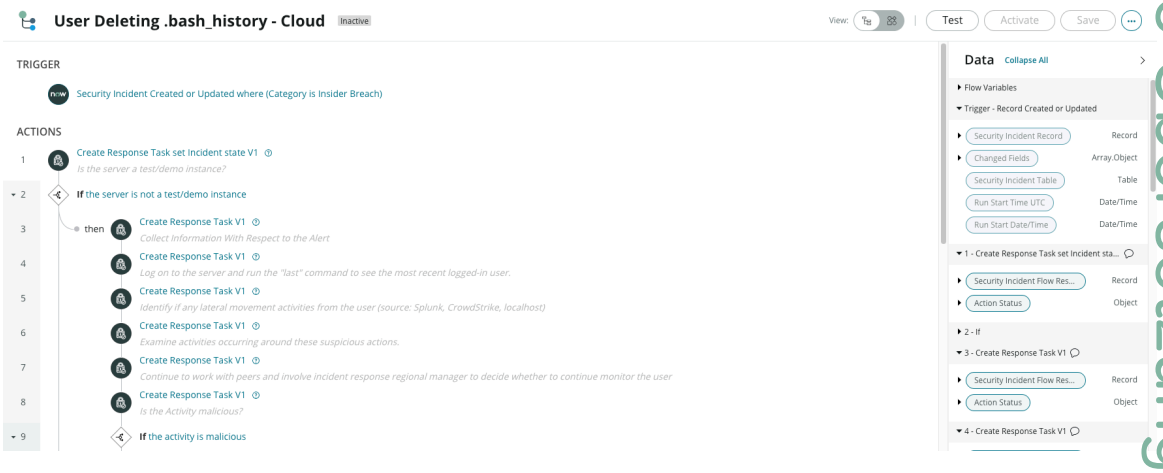
Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Anwender löscht .bash_history – Cloud** playbook.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „Anwender löschen“ .bash_history – Cloud, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie aus Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

Anwender löscht Bash-Verlauf – Cloud-Playbook

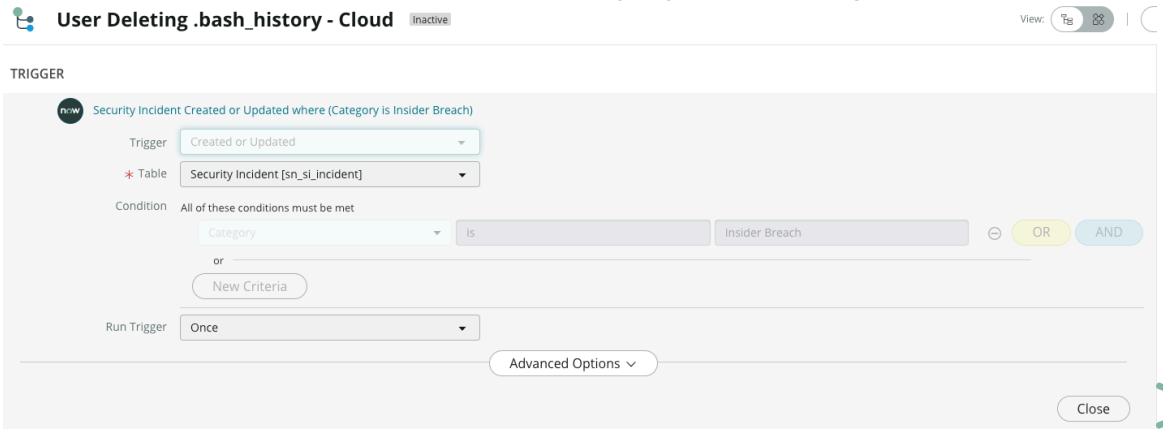


4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der verwendet wird **Kategorie** Ist **Insider-Verstoß** .

Anwender löscht Bash-Verlauf – Auslöserbedingung für Cloud-Playbook



Verwenden Sie das Playbook „Anwender löschen Bash-Verlauf“

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die darauf hinweisen, ob jemand versucht hat, die Bash-Verlaufsdatei von einem Linux-Server zu entfernen. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die in der Registerkarte Anwender Löschen des Bash-Verlaufs (verfügbar sind `.Bash_history`) Playbook.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, überprüfen Sie in Aktion 1, ob der Server eine Test- oder Demo-Instanz ist.
2. Wenn der Server in Aktion 2 keine Test- oder Demo-Instanz ist, führen Sie die folgenden Schritte aus:

   a. Erfassen Sie in Aktion 3 die folgenden Informationen für die Warnung:
      - Anwendername
      - IP-Adresse
      - Böswillige Befehle, die versuchen, den Bash-Verlauf zu löschen
      - Alle vom Anwender ausgeführten Befehle, falls in den CrowdStrike-Protokollen verfügbar.

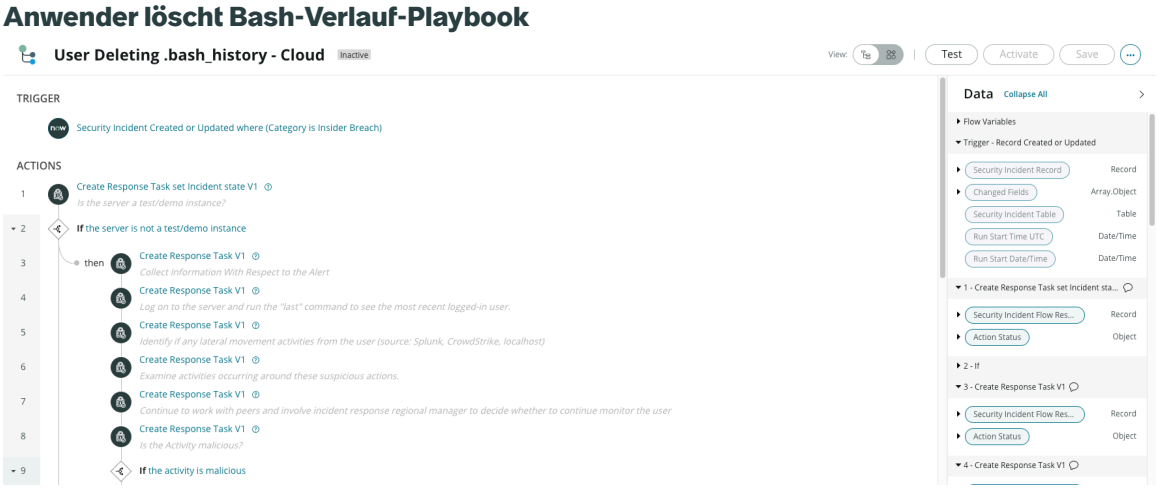
   b. Melden Sie sich in Aktion 4 beim Server an, und führen Sie aus `Zuletzt` Befehl zum Anzeigen des zuletzt angemeldeten Anwenders.

   c. Identifizieren Sie in Aktion 5, ob der Anwender laterale Bewegungsaktivitäten hatte (Quelle: Splunk, CrowdStrike, localhost).

   d. Untersuchen Sie in Aktion 6 die Aktivitäten im Zusammenhang mit diesen verdächtigen Aktionen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. In Aktion 7 arbeiten Sie weiter mit Kollegen, und beziehen Sie den Regional Manager für die Reaktion auf Incidents in die Entscheidung ein, ob der Anwender weiterhin überwacht werden soll.

f. Bestimmen Sie in Aktion 8, ob die Aktivität böswillig ist oder nicht.

g. Führen Sie in Aktion 9 die folgenden Schritte aus, wenn die Aktivität böswillig ist:

i. Wenden Sie sich in Aktion 10 während der Untersuchung an DEN IT-Support, und fordern Sie eine Sperrung des Accounts an.

ii. Stellen Sie in Aktion 11 sicher, dass die Instanz in einen normalen Status ohne böswillige Aktivitäten wiederhergestellt wird.

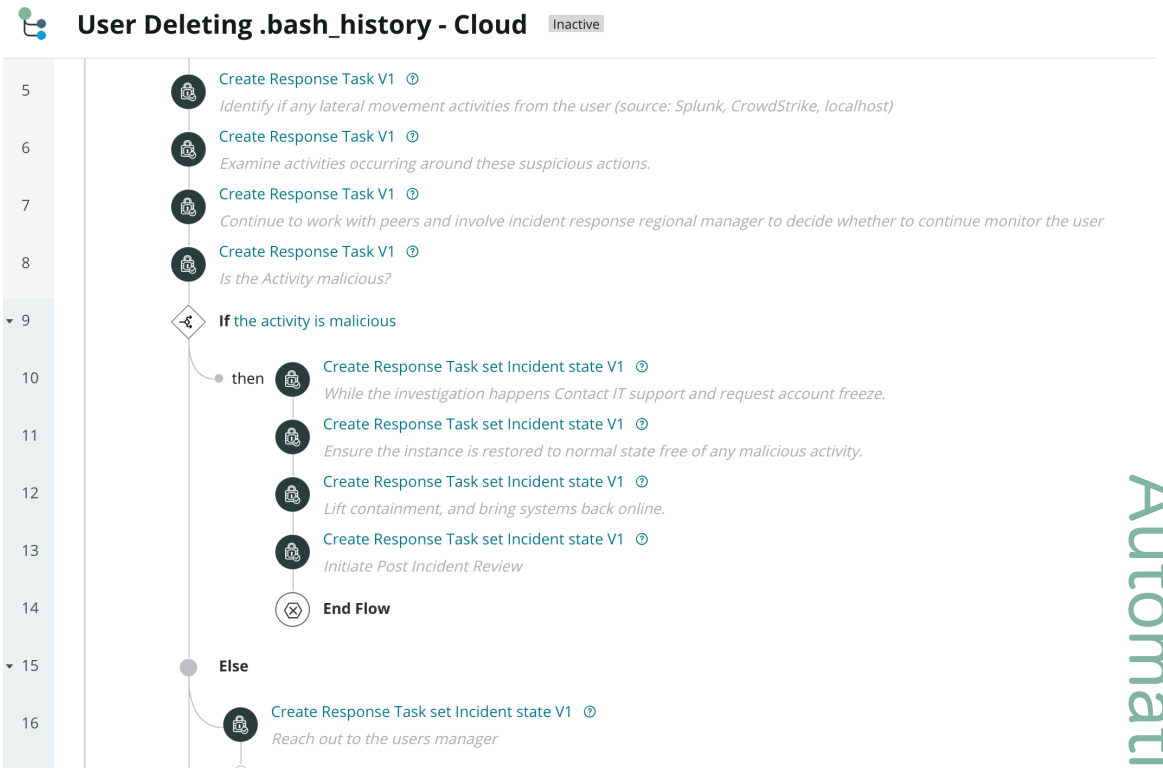
iii. Heben Sie in Aktion 12 die Eindämmung auf, und bringen Sie Systeme wieder auf Betriebsstandards zurück.

iv. Initiieren Sie in Aktion 13 eine Überprüfung nach dem Incident.

In Aktion 14 endet der Flow nach der Überprüfung nach dem Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden des Playbooks „Anwender löschen Bash-Verlauf“



h. Wenn die Aktivität in Aktion 15 nicht böswillig ist, wenden Sie sich in Aktion 16 an den Vorgesetzten des Anwenders.
Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Manager des Anwenders zu kontaktieren und ihn über den empfohlenen Ansatz zu informieren.

3. Dokumentieren Sie in Aktion 17 die bisherigen Ergebnisse.

4. Schließen Sie in Aktion 18 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für erfolgreiche VPN-Versuche aus den Service-Accounts – Corp/Cloud

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, die erfolgreiche Anmeldeversuche von Service-Accounts über VPN nachverfolgen. Service-Accounts dürfen keine Anmeldungsereignisse aus einem VPN haben, und solche Ereignisse können Indikatoren für Brute Force oder mögliche Offenlegung der Anmeldeinformationen des Accounts sein.

Richten Sie die erfolgreichen VPN-Versuche im Playbook „Service-Accounts“ ein

Führen Sie die folgenden Schritte aus, um die erfolgreichen VPN-Versuche über das Playbook „Service-Accounts“ einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Automatische Übersetzung

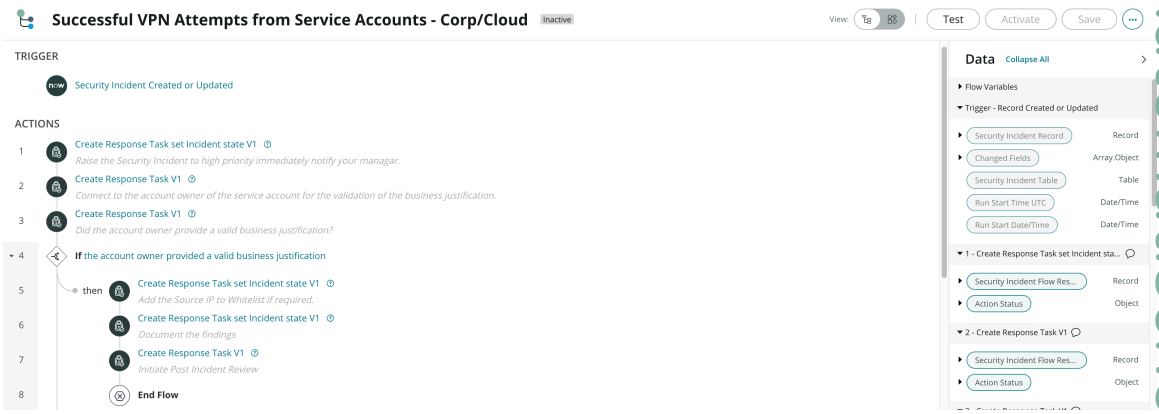
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Erfolgreiche VPN-Versuche von den Service-Accounts** playbook.
3. **Wahlweise:** Erstellen Sie eine Kopie der erfolgreichen VPN-Versuche aus dem Playbook-Flow „Service-Accounts“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie aus Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

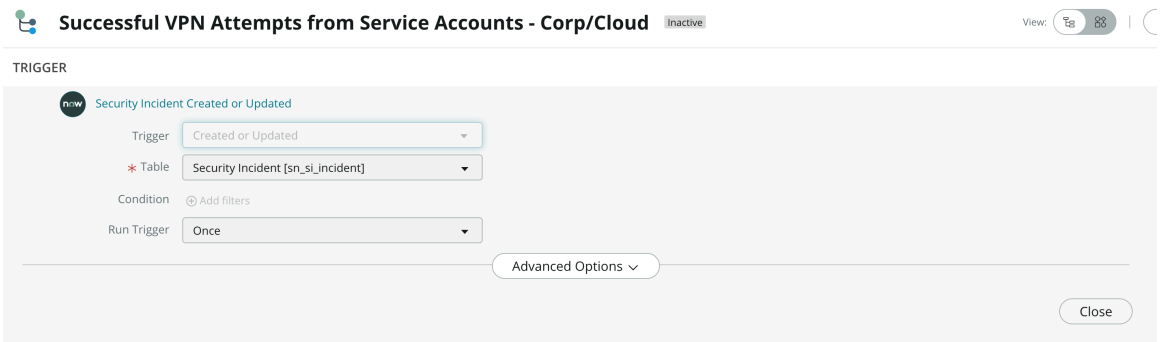
   Erfolgreiche VPN-Versuche aus dem Playbook „Service-Accounts – Corp/Cloud“

4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der Security Incident basierend auf Ihren erforderlichen Bedingungen erstellt oder aktualisiert wird. Beispiel: Wann **Kategorie** Ist **Insider-Verstoß** .

   Erfolgreiche VPN-Versuche über die Auslöserbedingung „Service-Accounts – Corp/Cloud-Playbook“

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die erfolgreichen VPN-Versuche aus dem Playbook „Service-Accounts“

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, die erfolgreiche Anmeldeversuche von Service-Accounts über VPN nachverfolgen. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die in den erfolgreichen VPN-Versuchen aus dem Playbook „Service-Accounts“ verfügbar sind.

Vorbereitungen

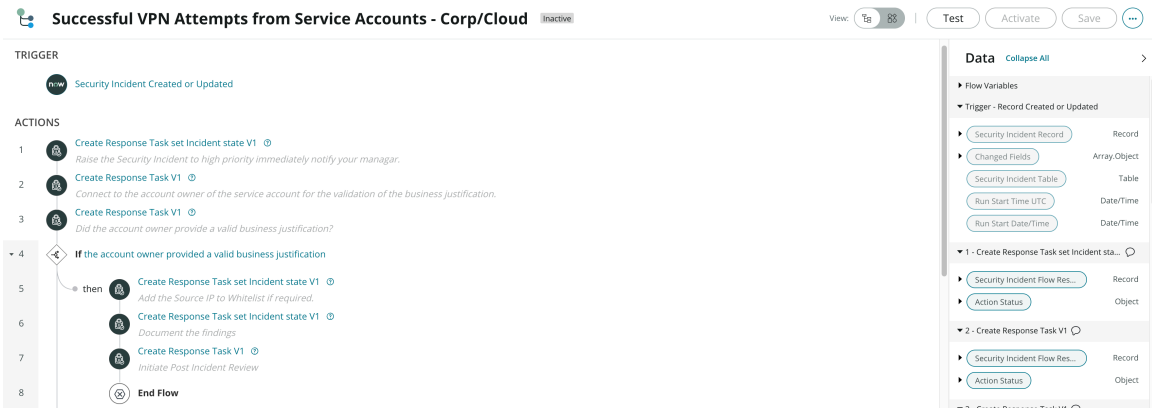
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, heben Sie den Security Incident in Aktion 1 auf hohe Priorität an, und benachrichtigen Sie sofort Ihren Vorgesetzten.
2. Wenden Sie sich in Aktion 2 an den Besitzer des Service-Accounts, um die geschäftliche Begründung zu validieren.
   Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Besitzer des Service-Accounts zu kontaktieren, um die geschäftliche Begründung zu validieren.
3. Überprüfen Sie in Aktion 3, ob der Service-Account-Besitzer eine gültige geschäftliche Begründung angegeben hat.

Erfolgreiche VPN-Versuche aus dem Playbook „Service-Accounts – Corp/Cloud“



4. Führen Sie in Aktion 4 die folgenden Schritte aus, wenn der Service-Account-Besitzer eine gültige geschäftliche Begründung angegeben hat:

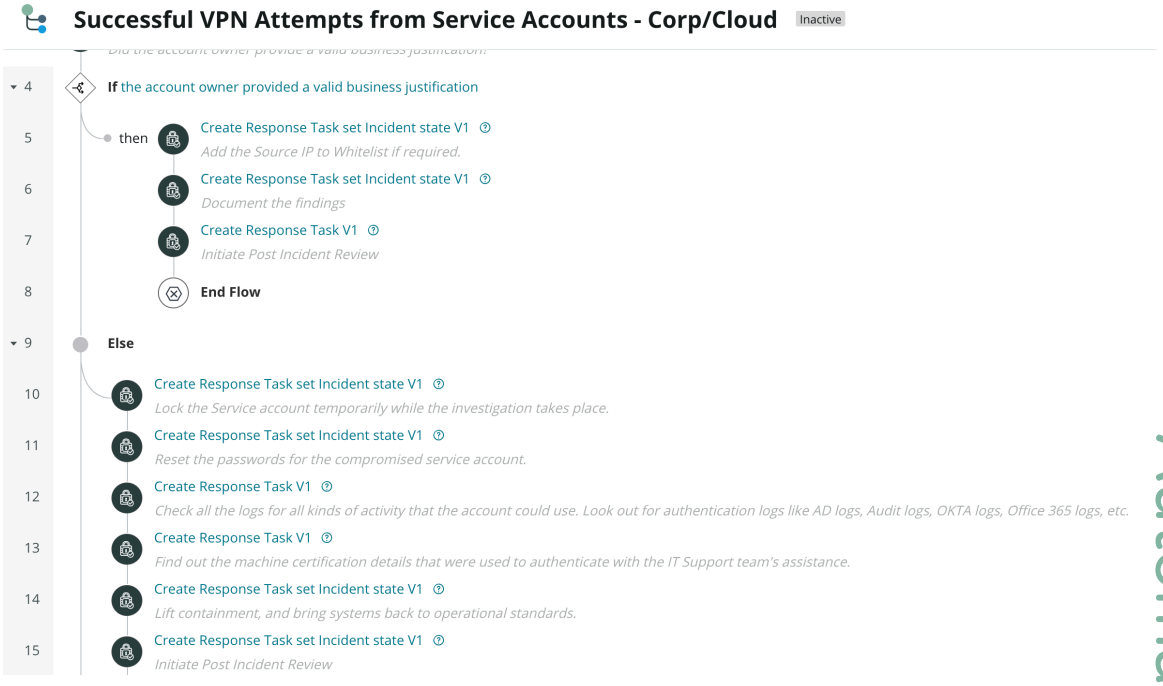
   a. Fügen Sie in Aktion 5 die Quell-IP bei Bedarf der Liste Zulassen hinzu.

   b. Dokumentieren Sie in Aktion 6 die bisherigen Ergebnisse.

   c. Initiieren Sie in Aktion 7 eine Überprüfung nach Incident.
   In Aktion 8 endet der Flow nach der Überprüfung nach dem Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwendung der erfolgreichen VPN-Versuche aus dem Playbook „Service-Accounts – Corp/Cloud“



5. Führen Sie in Aktion 9 die folgenden Schritte aus, wenn der Service-Account-Besitzer keine gültige geschäftliche Begründung angegeben hat:

   a. Sperren Sie in Aktion 10 den Service-Account vorübergehend, während die Untersuchung stattfindet.

   b. Setzen Sie in Aktion 11 die Passwörter für den gefährdeten Service-Account zurück.

   c. Überprüfen Sie in Aktion 12 die Protokolle auf alle Arten von Aktivitäten, die der Account verwenden könnte.
   Achten Sie auf Authentifizierungsprotokolle wie Active Directory-Protokolle, Audit-Protokolle, Okta-Protokolle, Office 365-Protokolle usw.

   d. Suchen Sie in Aktion 13 nach den Computerzertifizierungsdetails, die zur Authentifizierung mit Unterstützung des IT-Support-Teams verwendet werden.

   e. Heben Sie in Aktion 14 die Eindämmung auf, und bringen Sie Systeme wieder auf Betriebsstandards zurück.

   f. Schließen Sie in Aktion 15 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für versuchten Zugriff auf deaktivierte Accounts

Dieses Playbook wird ausgelöst, wenn ein Mitarbeiter, dessen Account beendet, deaktiviert oder getrennt wird, versucht, sich mit seinen Anmeldeinformationen anzumelden. Der Identitätsstatus des Anwenders in Sail Point wird im Allgemeinen am Kündigungsdatum in „deaktiviert“ aktualisiert.

30 Tage sind die ideale Zeit ab dem Kündigungsdatum, bis die IT in einen getrennten Status aktualisiert wird. Sie können die Geschäftslogik in Sail Point verwenden, um die RSA-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Accounts zu löschen und die Active Directory (AD)-Gruppenmitgliedschaften nach 30 Tagen zu entfernen.

Richten Sie das Playbook für deaktivierten Account für versuchten Zugriff ein

Führen Sie die folgenden Schritte aus, um das Playbook für deaktivierten Account für versuchten Zugriff einzurichten.

Vorbereitungen
Erforderliche Rolle:

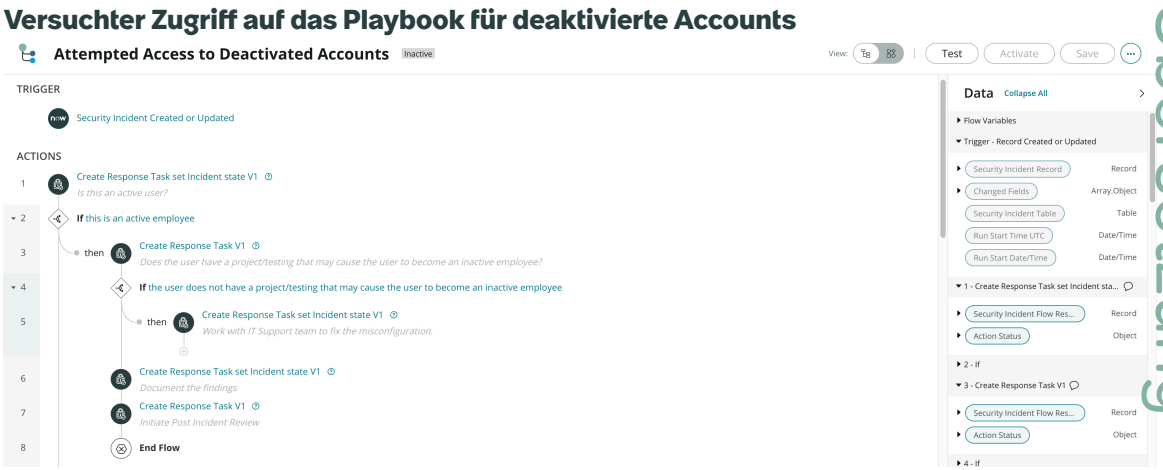
- sn_si.admin
- flow_designer

Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Versuchter Zugriff – Deaktivierter Account** playbook.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „versuchter Zugriff – deaktivierter Account“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie aus Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

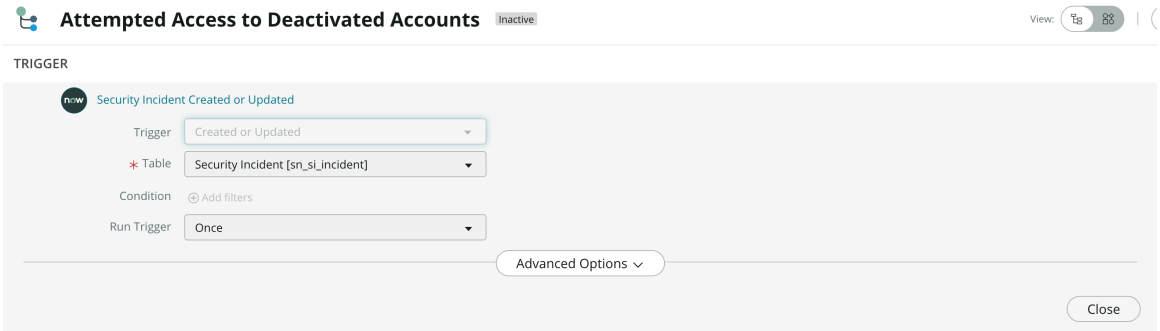


4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst, wenn der Security Incident basierend auf Ihren erforderlichen Bedingungen erstellt oder aktualisiert wird. Beispiel: Wann **Kategorie** Ist **Insider-Verstoß**

Auslöserbedingung für versuchten Zugriff auf deaktivierte Accounts-Playbook



Verwenden Sie das Playbook „versuchter Zugriff auf deaktivierte Accounts“

Verwenden Sie dieses Playbook, wenn ein Mitarbeiter, dessen Account beendet, deaktiviert oder getrennt wurde, versucht, sich mit seinen Anmeldeinformationen anzumelden. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „versuchter Zugriff auf deaktivierte Accounts“ verfügbar sind.

Vorbereitungen

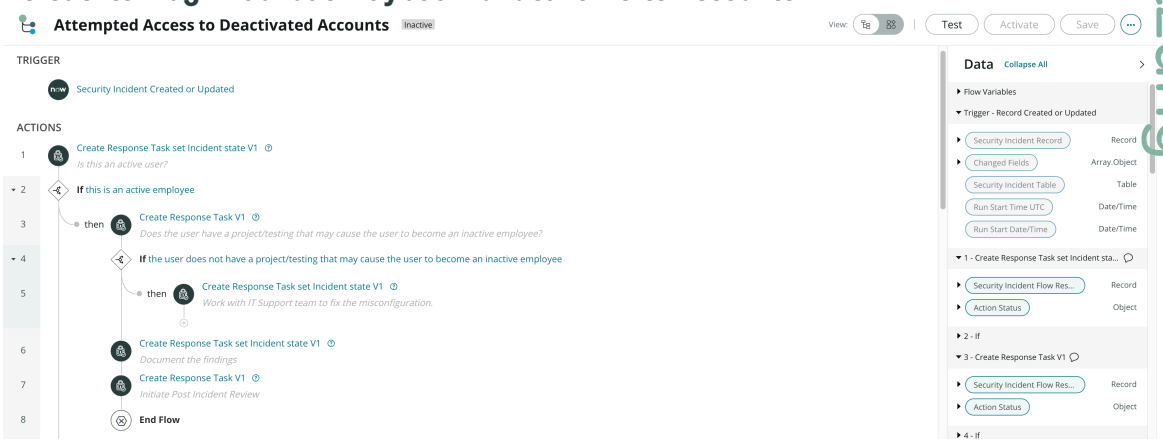
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, überprüfen Sie in Aktion 1, ob der versuchte Zugriff auf die deaktivierten Accounts von einem aktiven Anwender erfolgt ist.
2. Überprüfen Sie in Aktion 2, ob der versuchte Zugriff auf die deaktivierten Accounts von einem aktiven Mitarbeiter erfolgt ist.

Versuchter Zugriff auf das Playbook für deaktivierte Accounts



3. Wenn der versuchte Zugriff auf die deaktivierten Accounts von einem aktiven Mitarbeiter erfolgt ist, führen Sie die folgenden Schritte aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Überprüfen Sie in Aktion 3, ob der Anwender ein Projekt oder einen Testfall hatte, der dazu geführt hat, dass der Anwender ein inaktiver Mitarbeiter wurde.

b. Wenn der Anwender in Aktion 4 keinen Projekt- oder Testfall hatte, der dazu geführt hat, dass der Anwender inaktiver Mitarbeiter wurde, arbeiten Sie mit dem IT-Support-Team zusammen, um die Fehlkonfiguration zu beheben.
Der Flow endet.

c. Wenn der Anwender in Aktion 5 einen Projekt- oder Testfall hatte, der dazu geführt hat, dass der Anwender ein inaktiver Mitarbeiter wurde, führen Sie die folgenden Schritte aus:

i. Dokumentieren Sie in Aktion 6 die bisherigen Ergebnisse.

ii. Initiieren Sie in Aktion 7 eine Überprüfung nach Incident.

In Aktion 8 endet der Flow nach der Überprüfung nach dem Incident.

4. Führen Sie in Aktion 9 die folgenden Schritte aus, wenn der versuchte Zugriff auf den deaktivierten Account nicht von einem aktiven Mitarbeiter vorgenommen wurde:

a. Überprüfen Sie in Aktion 10, ob sich der Anwender erfolgreich angemeldet hat.

b. Überprüfen Sie in Aktion 11, wann der Mitarbeiter aus dem Onboarding entlassen wurde.

c. Untersuchen Sie in Aktion 12 die Ereignisse in Splunk, um die Aktivitäten des Anwenders während des Zeitraums zu untersuchen.

d. Bestimmen Sie in Aktion 13 basierend auf der bisherigen Untersuchung, ob der Anwender Daten exfiltriert hat.

e. Führen Sie in Aktion 14 die folgenden Schritte aus, wenn der Anwender keine Daten exfiltriert hat:

i. Arbeiten Sie in Aktion 15 mit dem IT-Support-Team zusammen, um aktive Sitzungen zu beenden und die Accounts zu deaktivieren.

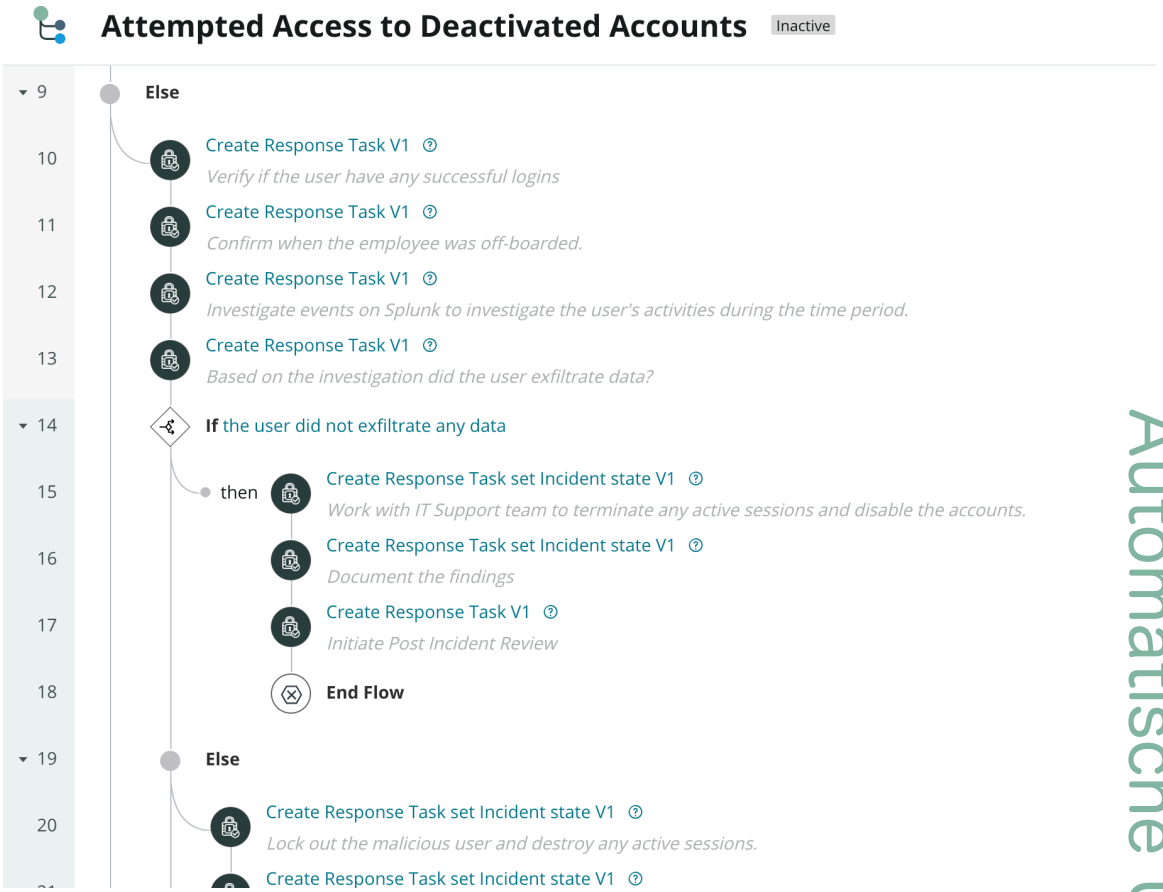
ii. Dokumentieren Sie in Aktion 16 die bisherigen Ergebnisse.

iii. Initiieren Sie in Aktion 17 eine Überprüfung nach dem Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In Aktion 18 endet der Flow nach der Überprüfung nach dem Incident.

Verwenden des Playbooks „versuchter Zugriff auf deaktivierte Accounts“



5. Wenn der Anwender in Aktion 19 Daten exfiltriert hat, gehen Sie wie folgt vor:

a. Sperren Sie in Aktion 20 den böswilligen Anwender aus, und löschen Sie alle aktiven Sitzungen.

b. Arbeiten Sie in Aktion 21 mit dem IT-Support-Team zusammen, um alle Accounts zu deaktivieren.

c. Stellen Sie in Aktion 22 sicher, dass die Ressourcen auf den normalen Status zurückgesetzt und frei von böswilligen Aktivitäten sind.
Sie können die Ressourcen bei Bedarf neu erstellen.

d. Heben Sie in Aktion 23 die Eindämmung auf, und bringen Sie Systeme wieder auf Betriebsstandards zurück.

e. Schließen Sie in Aktion 24 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für T1003 – Verteidigungsflucht – Mimikatz DCShadow

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, bei denen vermutet wird, dass sie durch Mimikatz DCShadow verursacht wurden. DCShadow ist eine Funktion in Mimikatz, die das Verhalten eines Domänencontrollers (eines Servers, der Active Directory steuert) simuliert, um seine eigenen Daten einzufügen, wobei die meisten Standardsicherheitskontrollen (einschließlich SIEMs) umgangen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mimikatz DCShadow hilft dem Angreifer, einen Rogue Domain Controller (DC) einzurichten, der Teil des Active Directory (AD) wird. Nach der Registrierung kann es als legitime DC fungieren und Schäden verursachen.

Richten Sie das Playbook T1003 – Verteidigungsflucht – Mimikatz DCShadow ein

Führen Sie die folgenden Schritte aus, um das Playbook T1003 – Defense Evasion – Mimikatz DCShadow einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

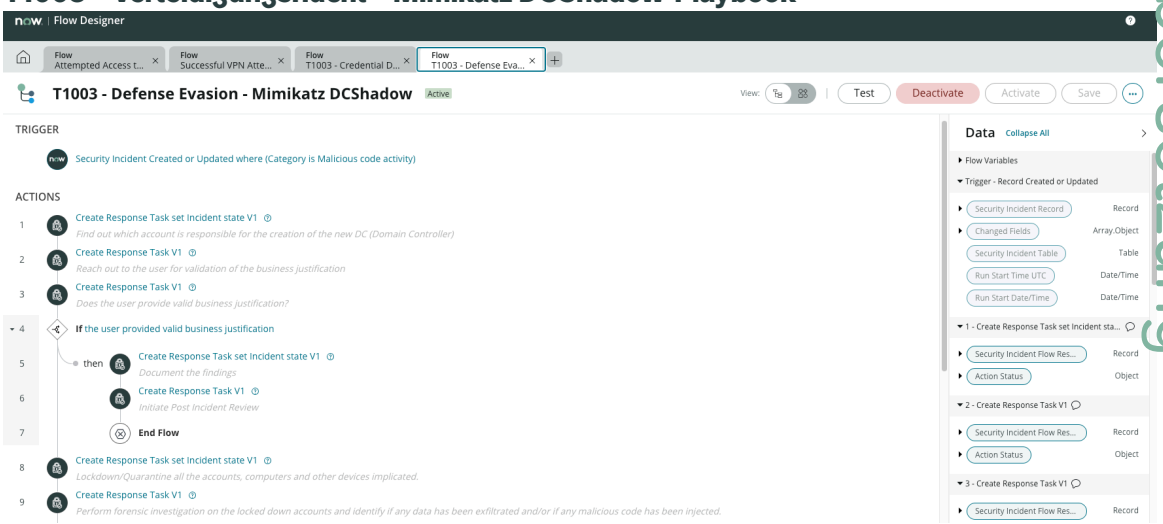
Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **T1003 – Verteidigungsflucht – Mimikatz DCShadow** playbook.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „T1003 – Verteidigungsflucht – Mimikatz DCShadow“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie aus Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

   T1003 – Verteidigungsflucht – Mimikatz DCShadow-Playbook

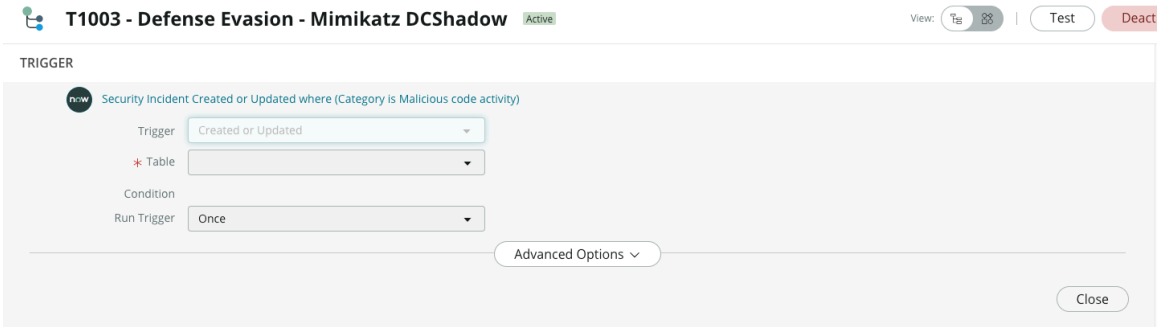


4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der verwendet wird **Kategorie** Ist **Schädliche Codeaktivität** .

T1003 – Abwehrflucht – Auslöserbedingung für Mimikatz DCShadow-Playbook



Verwenden Sie das Playbook T1003 – Verteidigungsflucht – Mimikatz DCShadow

Verwenden Sie dieses Playbook, um Security Incidents zu untersuchen, bei denen vermutet wird, dass sie durch Mimikatz DCShadow verursacht wurden. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die im Playbook T1003 – Verteidigungsflucht – Mimikatz DCShadow verfügbar sind.

Vorbereitungen

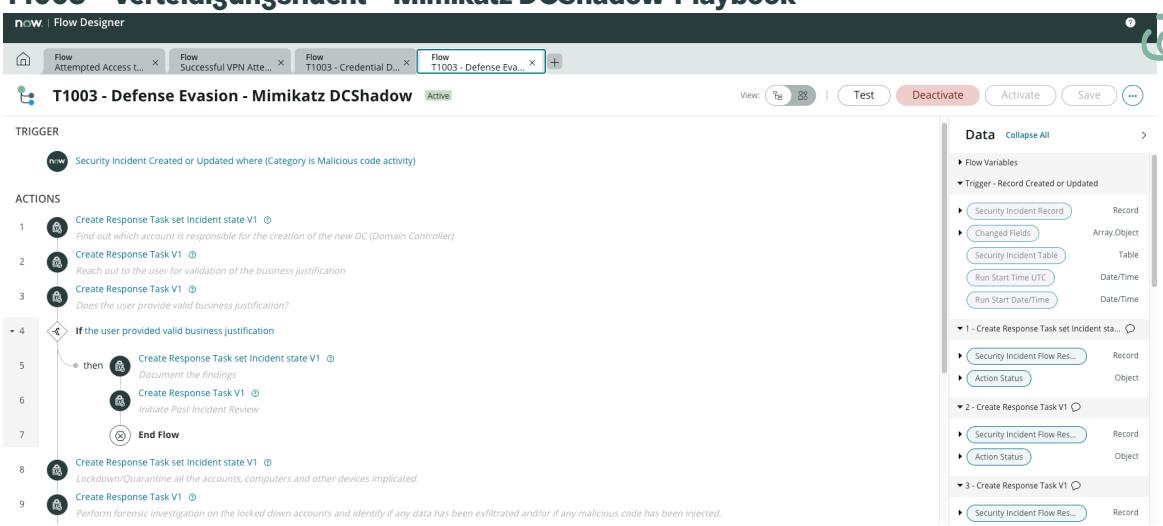
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, finden Sie in Aktion 1 heraus, welcher Account für die Erstellung des neuen DC (Domänencontrollers) verantwortlich ist.
2. Wenden Sie sich in Aktion 2 an den Anwender, um die geschäftliche Begründung zu validieren. Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den Anwender zu kontaktieren.
3. Überprüfen Sie in Aktion 3, ob der Anwender eine gültige geschäftliche Begründung angegeben hat.
4. Führen Sie in Aktion 4 die folgenden Schritte aus, wenn der Anwender eine gültige geschäftliche Begründung angegeben hat:

T1003 – Verteidigungsflucht – Mimikatz DCShadow-Playbook



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Dokumentieren Sie in Aktion 5 die bisherigen Ergebnisse.

b. Initiieren Sie in Aktion 6 eine Überprüfung nach Incident.
In Aktion 7 endet der Flow nach der Überprüfung nach dem Incident.

5. Wenn der Anwender in Aktion 8 keine gültige geschäftliche Begründung angegeben hat, führen Sie die folgenden Schritte aus:

a. Sperren oder Quarantäne Sie in Aktion 9 alle Accounts, Computer und anderen beteiligten Geräte.

b. Führen Sie in Aktion 10 eine forensische Untersuchung der gesperrten Accounts durch, und identifizieren Sie, ob Daten exfiltriert wurden oder böswilliger Code injiziert wurde.

c. Führen Sie in Aktion 11 ein neues Image für die betroffenen Ressourcen durch.

d. Heben Sie in Aktion 12 die Eindämmung auf, und bringen Sie Systeme wieder auf Betriebsstandards zurück.

e. Schließen Sie in Aktion 13 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für T1003 – Dumping von Anmeldeinformationen – Mimikatz DCSync

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents, bei denen vermutet wird, dass sie durch Mimikatz DCSync verursacht wurden. Dieses Playbook wird ausgelöst, wenn einer der Mimikatz-Funktionen funktioniert (`Lsadump::dcsync`) Wird verwendet. Die Funktion wird normalerweise auf angegriffenen Domänencontrollern (DC) verwendet.

Mimikatz ist ein beliebtes Hacking-Tool, mit dem Anwender Befehle ausgeben können, mit denen vertrauliche Daten aus dem angegriffenen System abgerufen werden können. Die vertraulichen Daten umfassen Passwörter, ihre Hashes und andere.

Hinweis:
Dies ist eine Warnung mit hoher Genauigkeit, von der angenommen wird, dass sie selten ausgelöst wird. Wenn er ausgelöst wird, sollten Sie ein Senior-Teammitglied oder einen Manager sofort benachrichtigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie das Playbook T1003 – Anmeldeinformationsdumping – Mimikatz DCsync ein

Führen Sie die folgenden Schritte aus, um das Playbook T1003 – Anmeldeinformationsdumping – Mimikatz DCsync einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

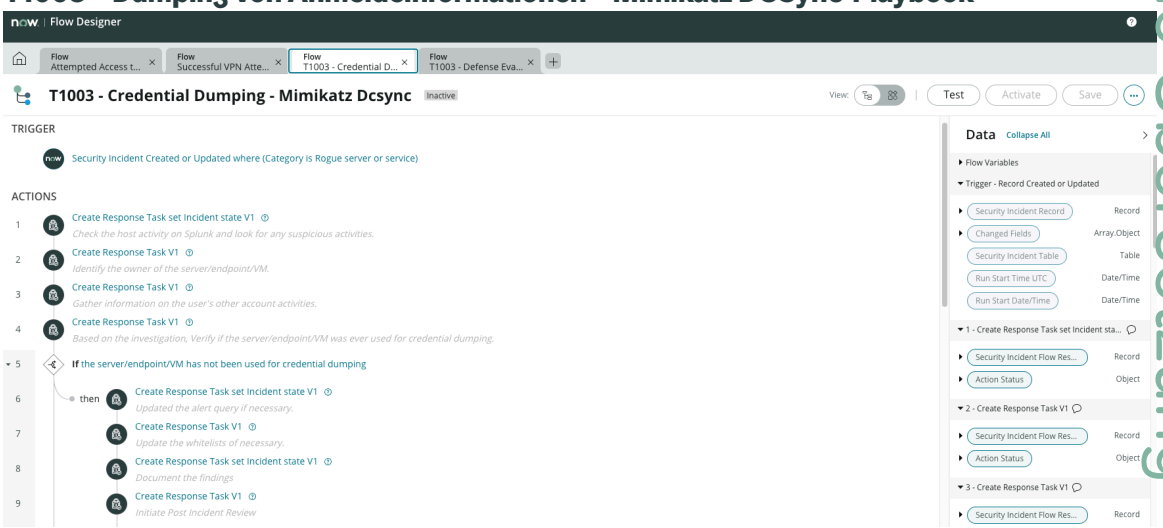
Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **T1003 – Dumping von Anmeldeinformationen – Mimikatz DCsync** playbook.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „T1003 – Anmeldeinformationsdumping – Mimikatz DCsync“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie aus Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

   T1003 – Dumping von Anmeldeinformationen – Mimikatz DCSync-Playbook

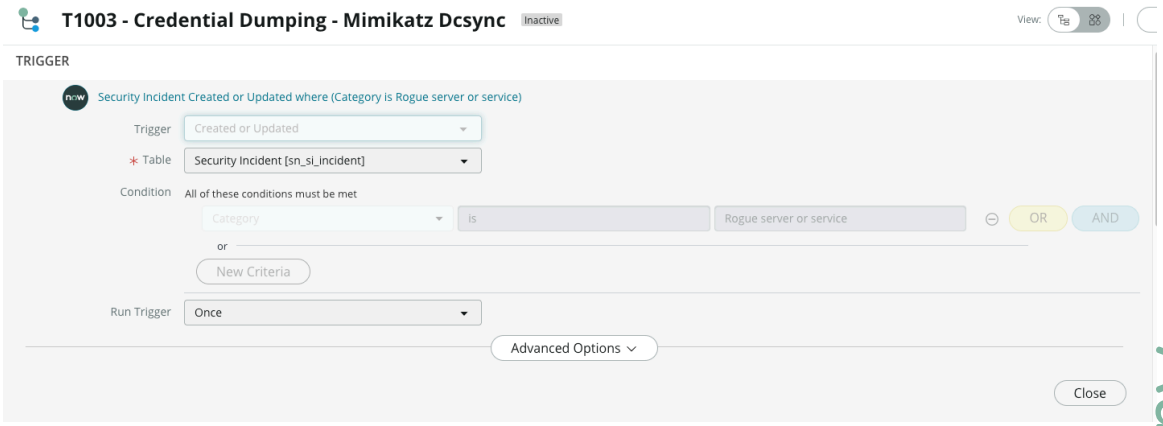
4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der verwendet wird **Kategorie** Ist **Nicht autorisierter Server oder Service** .

T1003 – Dumping von Anmeldeinformationen – Mimikatz DCSync-Playbook-Auslöserbedingung



Verwenden Sie das Playbook T1003 – Anmeldeinformationsdumping – Mimikatz DCsync

Verwenden Sie dieses Playbook, um Incidents zu untersuchen, bei denen vermutet wird, dass sie durch Mimikatz DCSync verursacht wurden. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die im Playbook T1003 – Anmeldeinformationsdumping – Mimikatz DCsync verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

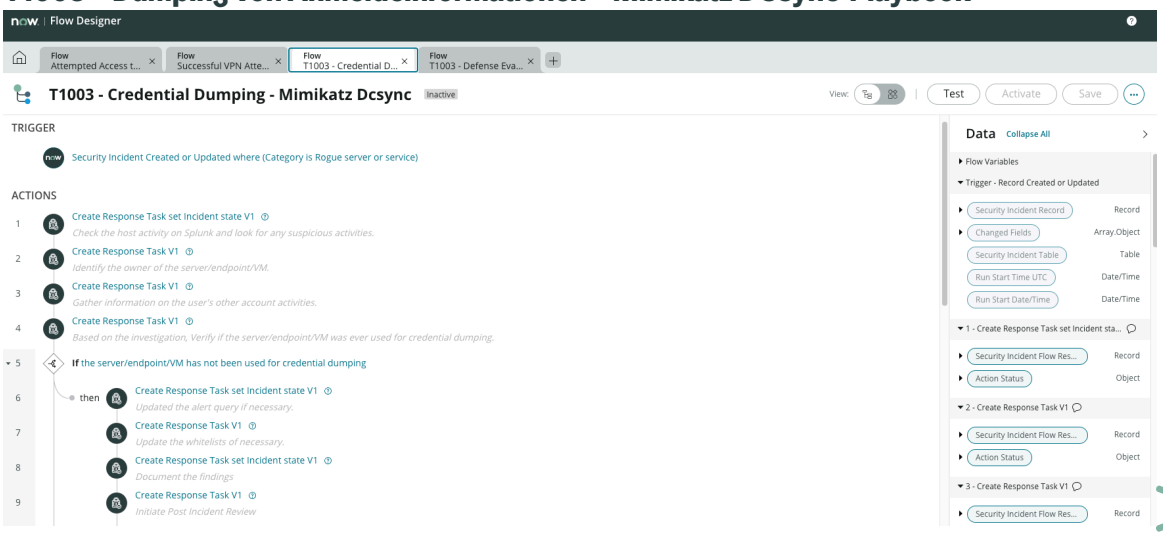
- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, überprüfen Sie in Aktion 1 die Hostaktivität in Splunk, und suchen Sie nach verdächtigen Aktivitäten.
2. Identifizieren Sie in Aktion 2 den Besitzer des Servers/Endpunkts/der VM.
   Wenn der Anwender online ist, führen Sie den CrowdStrike EDR aus, um einen besseren Umfang der Systemaktivitäten zu erfassen.
3. Sammeln Sie in Aktion 3 Informationen zu den anderen Account-Aktivitäten des Anwenders.
4. Überprüfen Sie in Aktion 4 basierend auf der Untersuchung, ob der Server/Endpunkt/die VM jemals für das Dumping von Anmeldeinformationen verwendet wurde.
5. Führen Sie in Aktion 5 die folgenden Aktionen aus, wenn der Server/Endpunkt/die VM nicht für das Dumping von Anmeldeinformationen verwendet wurde:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

T1003 – Dumping von Anmeldeinformationen – Mimikatz DCsync-Playbook



a. Aktualisieren Sie in Aktion 6 bei Bedarf die Warnungsabfrage.

b. Aktualisieren Sie in Aktion 7 bei Bedarf die Allow-Liste.

c. Dokumentieren Sie in Aktion 8 die bisherigen Ergebnisse.

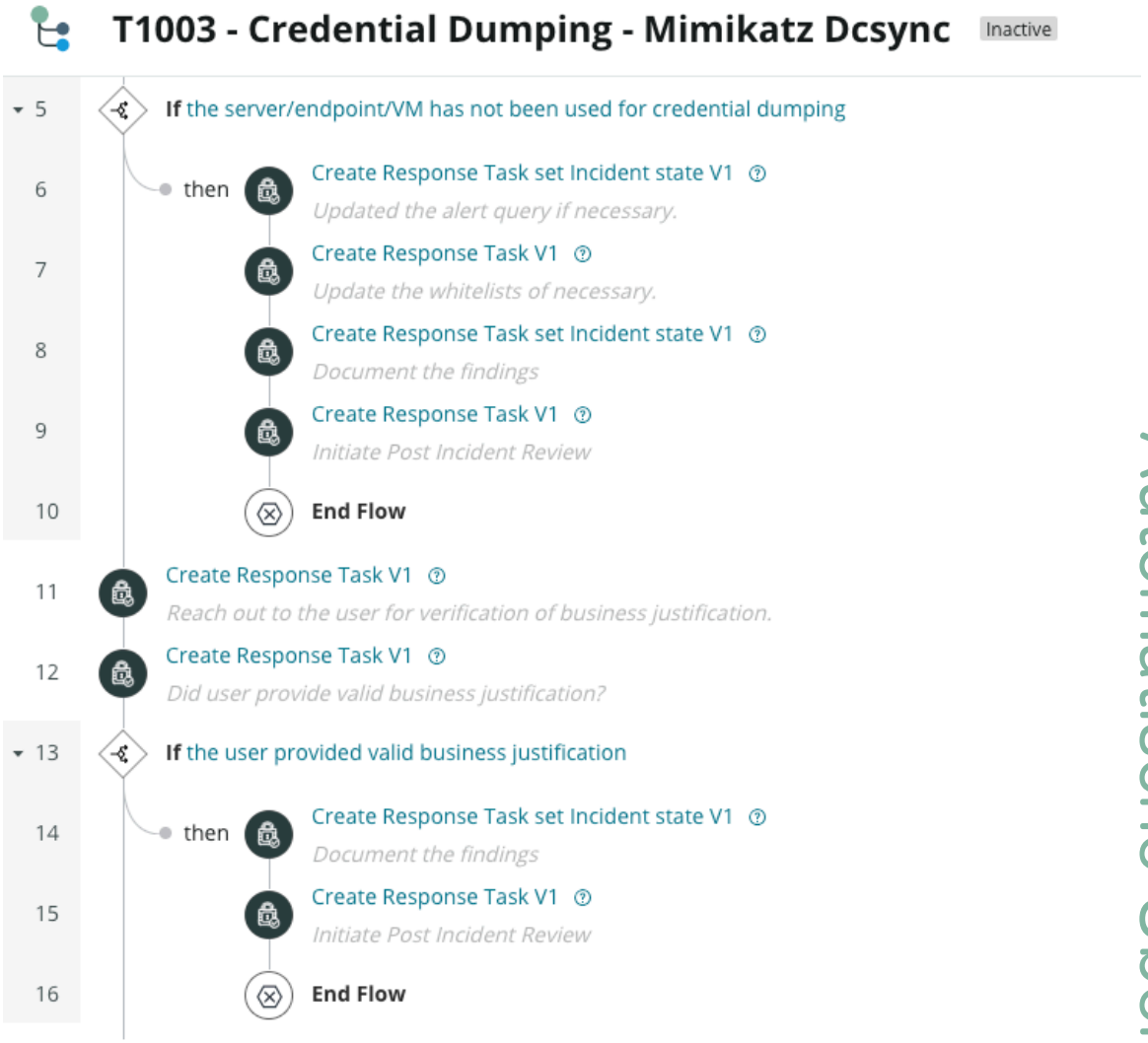
d. Initiieren Sie in Aktion 9 eine Überprüfung nach Incident.
In Aktion 10 endet der Flow.

6. Wenn der Server/Endpunkt/die VM für das Dumping von Anmeldeinformationen verwendet wurde, wenden Sie sich in Aktion 11 an den Anwender.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden des Playbooks T1003 – Anmeldeinformationsdumping – Mimikatz DCsync



7. Wenden Sie sich in Aktion 12 an den Anwender, um die geschäftliche Begründung zu validieren.
8. Wenn der Anwender in Aktion 13 eine gültige geschäftliche Begründung angegeben hat, führen Sie die folgenden Aktionen aus:

   a. Dokumentieren Sie in Aktion 14 die bisherigen Ergebnisse.

   b. Initiieren Sie in Aktion 15 eine Überprüfung nach Incident.
   In Aktion 16 endet der Flow.

9. Wenn der Anwender keine gültige geschäftliche Begründung angegeben hat, stellen Sie das System in Aktion 17 unter Quarantäne.
10. Entfernen Sie in Aktion 18 alle unerwünschten Dateien, die möglicherweise von den nicht autorisierten Accounts erstellt oder gelöscht wurden.
11. Heben Sie in Aktion 19 die Eindämmung auf, und bringen Sie Systeme wieder auf Betriebsstandards zurück.
12. Schließen Sie in Aktion 20 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook für Fehler bei der Okta-Anwenderanmeldung über mehrere IPs

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents für Fehler bei der Anwenderanmeldung in Okta.

Das Playbook „Fehler bei der Okta-Anwenderanmeldung von mehreren IPs“ enthält Anweisungen zur Analyse der Warnung, wenn ServiceNow-Account-Fehler in Okta von mehreren nicht-ServiceNow-IPs aus beobachtet werden. Die Warnung im Zusammenhang mit diesem Playbook überprüft die Okta-Protokolle. Es wird eine Warnung ausgelöst, wenn ein Anmeldefehler für ServiceNow-Anwender-IDs aus mehr als drei nicht-ServiceNow-IP-Bereichen innerhalb von 1 Stunde auftritt.

Richten Sie das Playbook „Fehler bei der Okta-Anwenderanmeldung“ über mehrere IPs ein

Führen Sie die folgenden Schritte aus, um das Playbook „Fehler bei der Okta-Anwenderanmeldung über mehrere IPs“ einzurichten.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

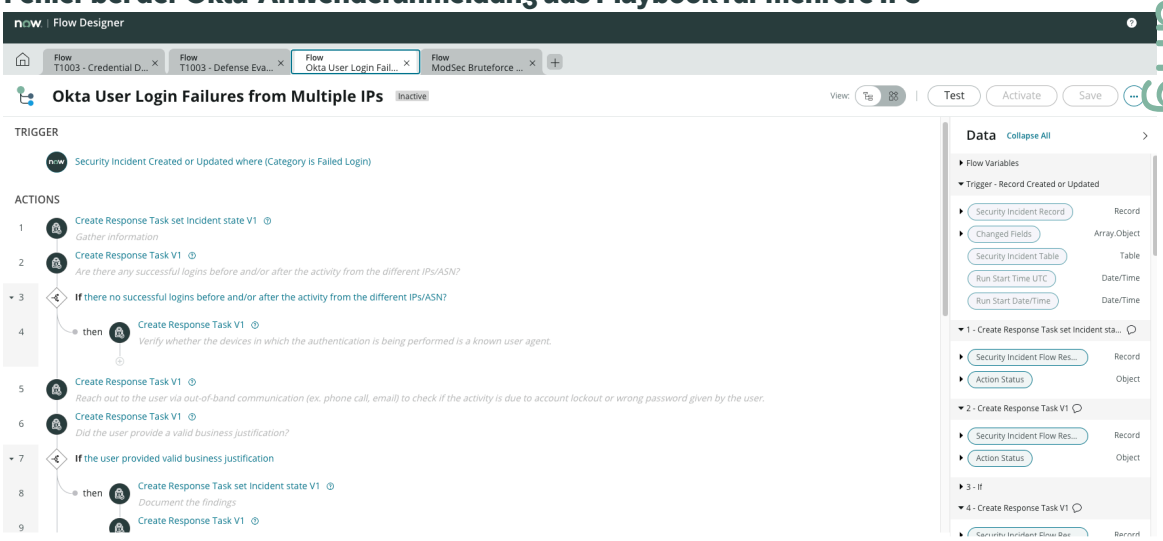
Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **Fehler bei der Okta-Anwenderanmeldung über mehrere IPs** playbook.
3. **Wahlweise:** Erstellen Sie eine Kopie des Playbook-Flows „Fehler bei der Okta-Anwenderanmeldung aus mehreren IPs“, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie aus Symbol und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

Fehler bei der Okta-Anwenderanmeldung aus Playbook für mehrere IPs



4. Aktivieren Sie die Playbooks.

Automatische Übersetzung

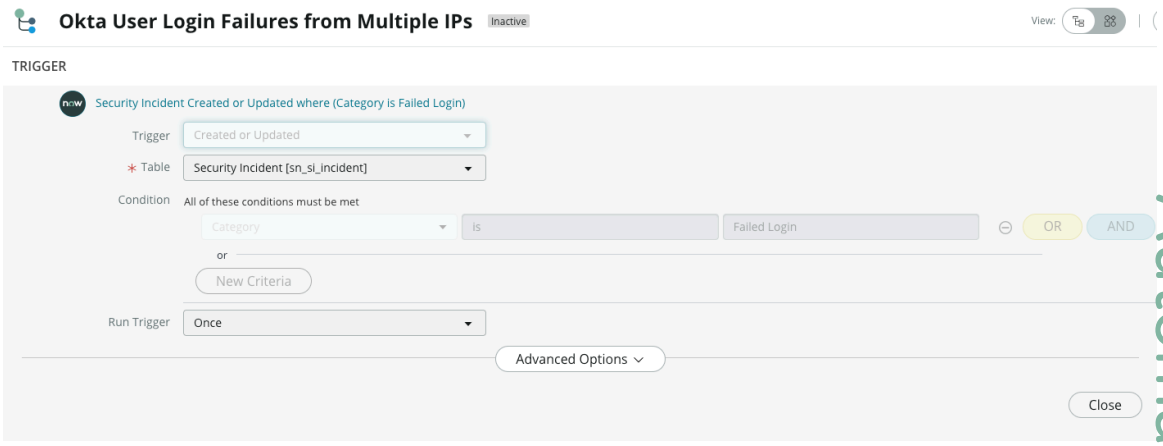
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.

b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn der verwendet wird **Kategorie** Ist **Anmeldung Fehlgeschlagen** .

Auslöserbedingung für Okta-Anwenderanmeldungsfehler aus Playbook für mehrere IPs



Verwenden Sie das Playbook „Fehler bei der Okta-Anwenderanmeldung aus mehreren IPs“

Verwenden Sie dieses Playbook, um Security Incidents auf Fehler bei der Anwenderanmeldung in Okta zu untersuchen. Die folgenden Schritte geben Ihnen einen Überblick über die Aktionen, Aufgaben und Subflows, die im Playbook „Fehler bei der Okta-Anwenderanmeldung von mehreren IPs“ verfügbar sind.

Vorbereitungen

Erforderliche Rolle:

- sn_si.admin
- flow_designer

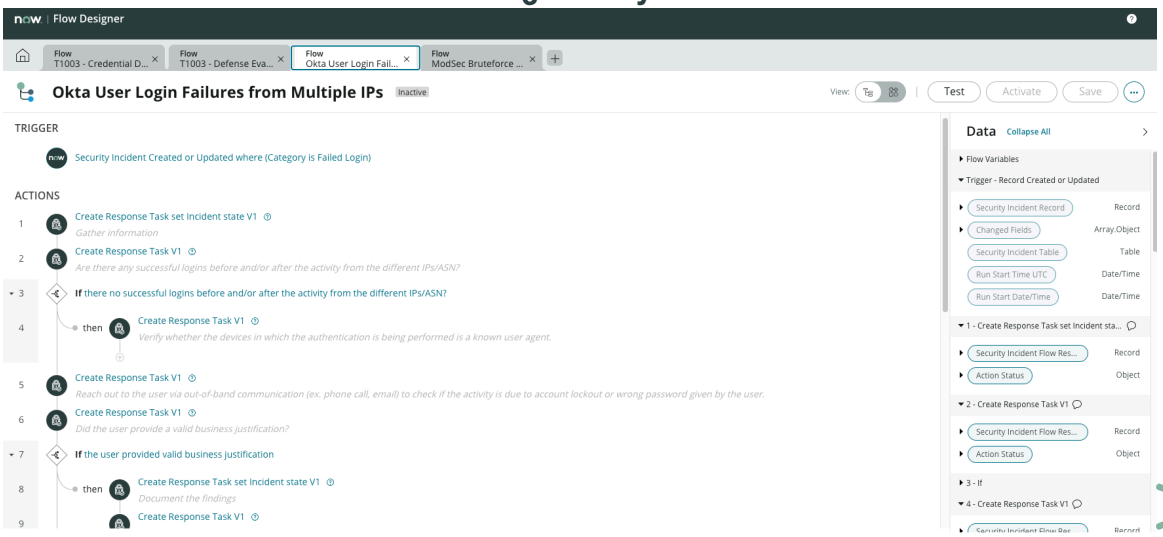
Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, führen Sie in Aktion 1 die folgenden Aufgaben aus:
   - Identifizieren Sie den Anwender-Account, der angestrebt wird.
   - Überprüfen Sie das IP-Subnetz, und überprüfen Sie, ob alle zum selben Besitzer der autonomen Systemnummer (ASN) gehören.
2. Überprüfen Sie in Aktion 2, ob vor oder nach der Aktivität von den verschiedenen IPs/ASNs erfolgreiche Anmeldungen durchgeführt wurden.
3. Wenn es in Aktion 3 keine erfolgreichen Anmeldungen vor oder nach der Aktivität von den verschiedenen IPs/ASNs gab, überprüfen Sie in Aktion 4, ob die Geräte, auf denen die Authentifizierung durchgeführt wird, bekannte Anwender-Agents sind.
   Wenn die Geräte von bekannten Anwenderagenten authentifiziert werden, endet der Flow.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehler bei der Okta-Anwenderanmeldung aus Playbook für mehrere IPs



4. Wenden Sie sich in Aktion 5 basierend auf der Untersuchung über Out-of-Band-Kommunikation (z. B. Telefonanruf oder E-Mail) an den Anwender, um zu überprüfen, ob die Aktivität auf eine Kontosperrung oder ein falsches Passwort des Anwenders zurückzuführen ist.
5. Überprüfen Sie in Aktion 6, ob der Anwender eine gültige geschäftliche Begründung angegeben hat.
6. Wenn der Anwender in Aktion 7 eine gültige geschäftliche Begründung angegeben hat, führen Sie die folgenden Aufgaben aus.

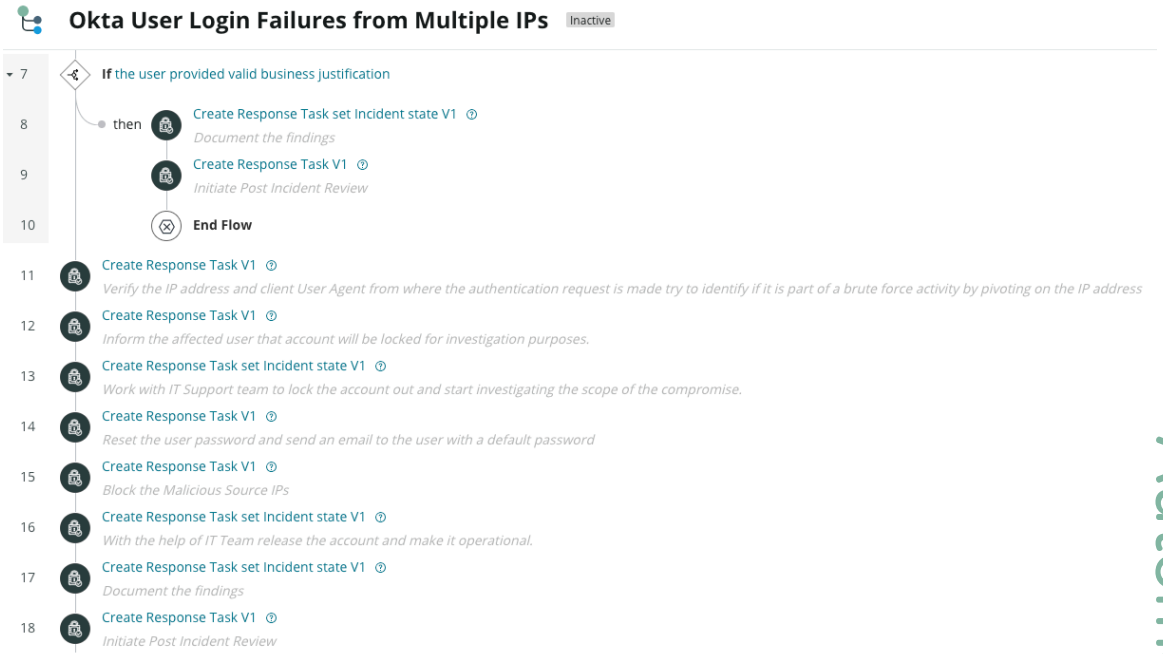
    a. Erstellen Sie in Aktion 8 eine Antwortaufgabe, um die bisherigen Ergebnisse zu dokumentieren.

    b. Erstellen Sie in Aktion 9 eine Antwort, um eine Überprüfung nach Incident zu initiieren.
    In Aktion 10 endet der Flow.

7. Überprüfen Sie in Aktion 11 die IP-Adresse und den Client-Anwender-Agent, von dem aus die Authentifizierungsanforderung gestellt wird, und versuchen Sie, zu identifizieren, ob sie Teil einer Brute-Force-Aktivität ist, indem Sie auf die IP-Adresse drehen.
8. Informieren Sie in Aktion 12 den betroffenen Anwender, dass der Account zu Untersuchungszwecken gesperrt wird.
Sie können die bereitgestellte E-Mail-Vorlage verwenden, um den betroffenen Anwender zu informieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden des Playbooks „Fehler bei der Okta-Anwenderanmeldung aus mehreren IPs“



9. Arbeiten Sie in Aktion 13 mit dem IT-Support-Team zusammen, um den Account zu sperren, und beginnen Sie mit der Untersuchung des Umfangs der Gefährdung.
10. Setzen Sie in Aktion 14 das Anwenderpasswort zurück, und senden Sie eine E-Mail mit dem Standardpasswort an den Anwender.
11. Blockieren Sie in Aktion 15 die schädlichen Quell-IPs.
12. In Aktion 16 erhalten Sie Hilfe vom IT-Supportteam, um den Account freizugeben und wieder auf Betriebsstandards zurückzusetzen.
13. Dokumentieren Sie in Aktion 17 die bisherigen Ergebnisse.
14. Schließen Sie in Aktion 18 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook für ModSec-Brute-Force nach IP-Burst

Dieses Playbook bietet systematische Korrekturschritte zur Untersuchung von Incidents von Brute-Force-Versuchen auf den Anmeldeseiten von mehreren von ModSec erkannten IPs. Die Ereignisbedingungen können in der ModSec-Richtlinie selbst festgelegt werden und löst eine Warnung in Splunk aus, wenn das Ereignis in ModSec erstellt wird.

Dieses Playbook hilft bei der Erkennung abnormaler Datenverkehrsanzahlen auf der Anmeldeseite. In diesem Beispiel sollten zwei aufeinanderfolgende Bursts von mehr als 50 Treffern/Minute von einer IP-Adresse zur Anmeldeseite stammen, was auf einen Brute-Force-Versuch hinweist, sich anzumelden.

Richten Sie das ModSec Brute Force by IP Burst-Playbook ein

Führen Sie die folgenden Schritte aus, um das ModSec Brute Force by IP Burst-Playbook einzurichten.

Vorbereitungen
Erforderliche Rolle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_si.admin
- flow_designer

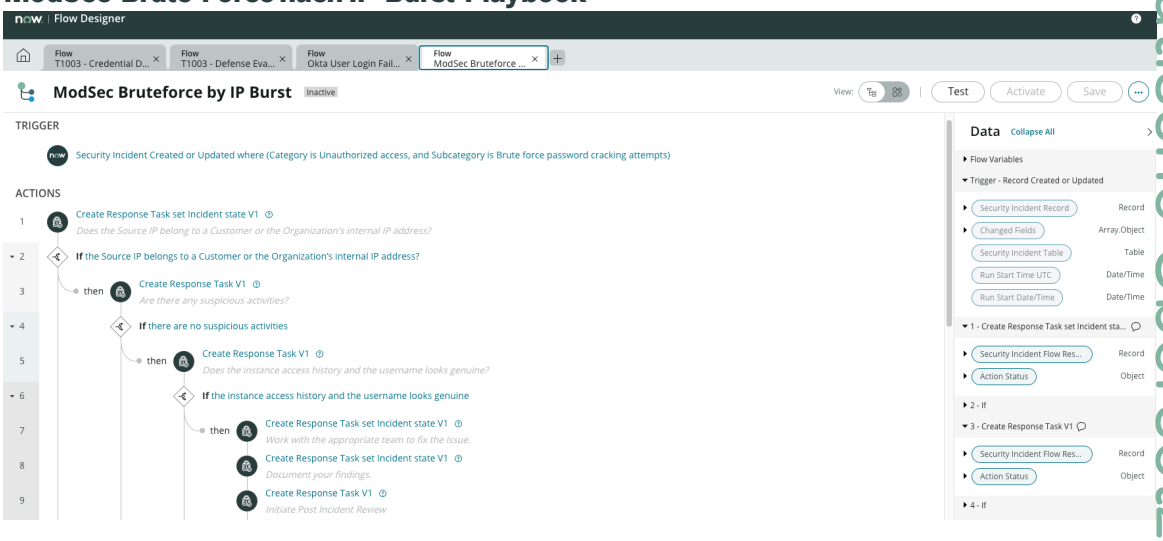
Stellen Sie sicher, dass Sie die Security Operations-Spoke (*sn_sec_Spoke*).

Prozedur

1. Melden Sie sich als Anwender mit den Rollen sn_si.user und Flow_Designer an.
2. Navigieren zu **Alle** > **Flow Designer** Und wählen Sie aus **ModSec BRuteforce nach IP-Burst** playbook.
3. **Wahlweise:** Erstellen Sie eine Kopie des ModSec BRuteforce by IP Burst-Playbook-Flows, und nehmen Sie die erforderlichen Änderungen vor.

   (Optional) Um eine Kopie des Playbook-Flows zu erstellen, wählen Sie das Menüsymbol „weitere Aktionen“ ( ) Und wählen Sie aus **Flow kopieren** . Führen Sie diesen Schritt nur aus, wenn Sie planen, den Flow anzupassen oder bestimmte Änderungen vorzunehmen.

   ModSec-Brute-Force nach IP-Burst-Playbook

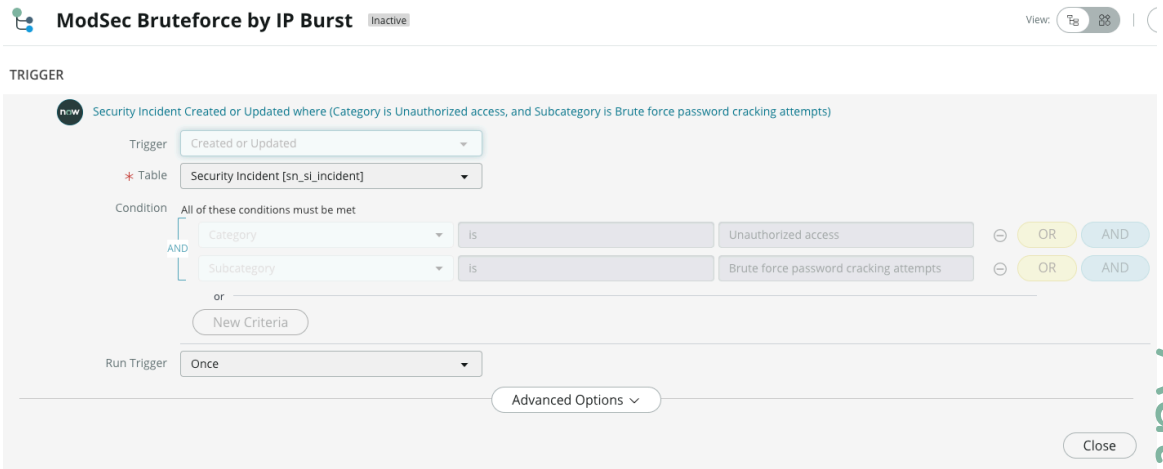
4. Aktivieren Sie die Playbooks.
   a. Aktivieren Sie den Haupt-Flow, um das im Basissystem verfügbare Playbook zu verwenden.
   b. Aktivieren Sie die kopierten Flows, nachdem Sie die erforderlichen Änderungen vorgenommen haben.
5. Legen Sie ein fest **Auslöserbedingung** Für das Playbook.
   Dieses Playbook wird ausgelöst und dem Security Incident zugeordnet, wenn die folgenden Bedingungen erfüllt sind:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Kategorie** Ist **Nicht autorisierter Zugriff** .
- **Unterkategorie** Ist **Brute-Force-Passwortknackversuche** .

ModSec-Brute-Force nach IP-Burst-Playbook-Auslöserbedingung



Verwenden Sie das ModSec Brute Force by IP Burst-Playbook

Verwenden Sie dieses Playbook, um Incidents von Brute-Force-Versuchen auf den Anmeldeseiten von mehreren von ModSec erkannten IPs zu untersuchen. Die folgenden Schritte geben Ihnen einen Rundgang durch die Aktionen, Aufgaben und Subflows, die im ModSec Brute Force by IP Burst-Playbook verfügbar sind.

Vorbereitungen

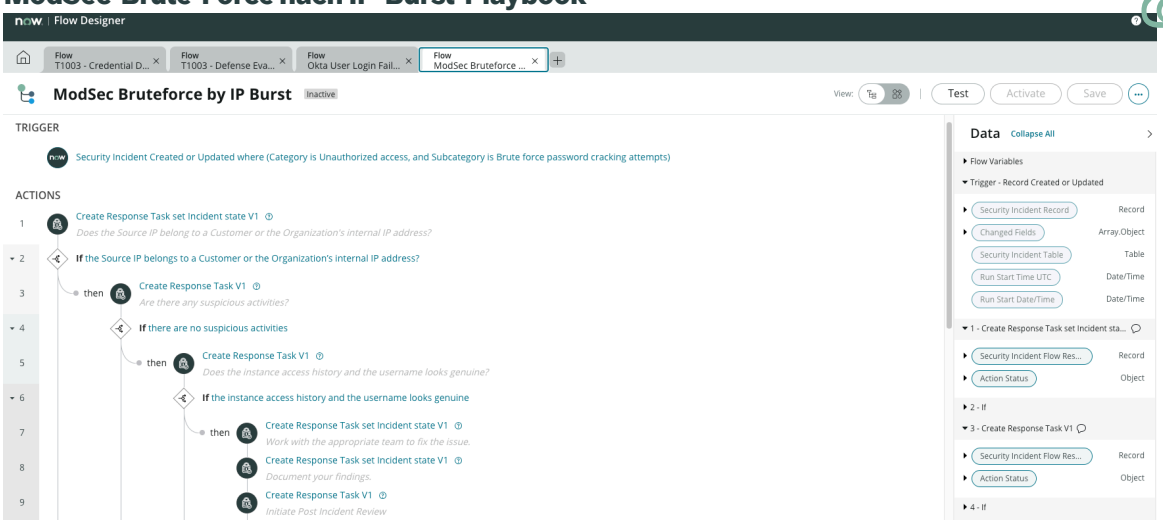
Erforderliche Rolle:

- sn_si.admin
- flow_designer

Prozedur

1. Wenn das Playbook ausgelöst wird und die Ausführung beginnt, überprüfen Sie in Aktion 1, ob die Quell-IP zu einem Kunden oder zur internen IP-Adresse der Organisation gehört.
2. Führen Sie in Aktion 2 die folgenden Schritte aus, wenn die Quell-IP zu einem Kunden oder zur internen IP-Adresse der Organisation gehört:

ModSec-Brute-Force nach IP-Burst-Playbook



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Überprüfen Sie in Aktion 3, ob verdächtige Aktivitäten vorhanden sind.

- Überprüfen Sie die Aktivität der Quell-IP in den letzten Tagen. Wenn die IP vernachlässigbarer Datenverkehr hatte, weist dies auf einen tatsächlichen Angriff hin.
- Überprüfen Sie die Sprachanwendernamen. Überprüfen Sie beispielsweise, ob die Anwendernamen in alphabetischer Reihenfolge angeordnet sind.
- Suchen Sie nach generischen Accountnamen, die beteiligt sind. Beispiel: Admin, sysadmin, root, Administrator, und andere Anwendungsaccount-Namen.

Wenn keine verdächtigen Aktivitäten vorhanden sind, endet der Flow.

b. Wenn in Aktion 4 verdächtige Aktivitäten aufgetreten sind, überprüfen Sie in Aktion 5, ob der Instanzzugriffsverlauf und der Anwendername echt aussehen.

Überprüfen Sie *Appnode*Protokolliert alle Anzeichen eines Fehlers. Es können SAML-, SSO- oder LDAP-Fehlgeschlagen-Ereignisse vorliegen, die auf ein Betriebsproblem zurückzuführen sein können.

Wenn der Instanzzugriffsverlauf und der Anwendername nicht authentisch aussehen, endet der Flow.

c. Wenn in Aktion 6 der Instanzzugriffsverlauf und der Anwendername echt aussehen, führen Sie die folgenden Schritte aus:

i. Koordinieren Sie sich in Aktion 7 mit dem entsprechenden Team, um das Problem zu beheben.

ii. Dokumentieren Sie in Aktion 8 die bisherigen Ergebnisse.

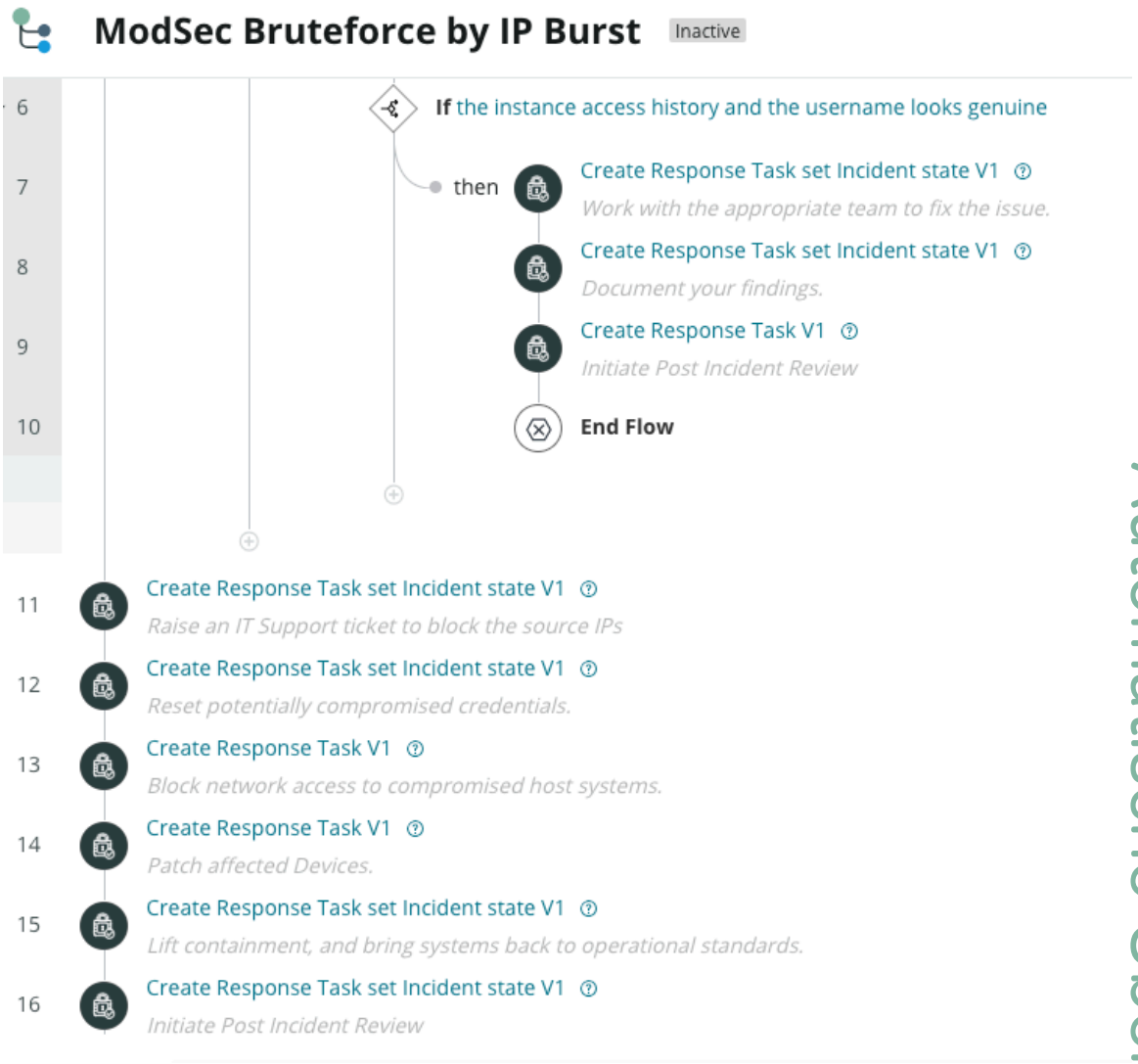
iii. Schließen Sie in Aktion 9 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

In Aktion 10 endet der Flow.

3. Wenn die Quell-IP nicht zu einem Kunden oder der internen IP-Adresse der Organisation gehört, erstellen Sie in Aktion 11 ein IT-Support-Ticket, um die Quell-IPs zu blockieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden des ModSec Brute Force by IP Burst-Playbooks



4. Setzen Sie in Aktion 12 die potenziell gefährdeten Anmeldeinformationen zurück.
5. Blockieren Sie in Aktion 13 den Netzwerkzugriff auf gefährdete Hostsysteme.
6. In Aktion 14 patchen Sie die betroffenen Geräte.
7. Heben Sie in Aktion 15 die Eindämmung auf, und bringen Sie die Systeme wieder auf Betriebsstandards zurück.
8. Schließen Sie in Aktion 16 die Überprüfung nach dem Incident ab, bevor Sie die Aufgabe schließen.

Playbook-Aktionen für Security Incident Response

In diesem Abschnitt werden die Aktionen beschrieben, die in der Flow Designer-Aktionsbibliothek bereitgestellt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	Beschreibung	Beispielszenario	
Fügen Sie dem Security Incident ein Sicherheits-Tag hinzu	Verwenden Sie diese Aktion, um mithilfe der Flow Designer-Logik automatisch ein Sicherheits-Tag hinzuzufügen.	Wenn der Flow ein IOC erkennt, wird der **IOC erkannt** Tag kann mit dieser Aktion automatisch hinzugefügt werden. **Flow** :	• Eingabe: Security Incident, Sicherheits-Tag • Ausgabe: Nicht zutreffend
Fügen Sie dem Security Incident erkennbare Elemente hinzu	Verwenden Sie diese Aktion, um einem ausgewählten Security Incident erkennbare Elemente hinzuzufügen. • Standardmäßig ist die Liste der erkennbaren Elemente durch das Komma (,) getrennt, dies kann jedoch geändert werden. Sie können ein anderes einzelnes Sonderzeichen als Trennzeichen angeben. Beim Hinzufügen erkennbarer Elemente wird der Typ (URL, IP-Adresse, Hash) automatisch festgelegt. • Wenn die erkennbaren Elemente dem Security Incident hinzugefügt werden, wird der Typ (URL, IP-Adresse, Hash) automatisch festgelegt. • Wenn die erkennbaren Elemente hinzugefügt werden, identifiziert die Option „zulässige Liste erkennbarer Elemente filtern“ die zulässigen		• Eingabe: ◦ Security Incident ◦ Erkennbare Elemente ◦ Trennzeichen ◦ Filtern Sie die zulässigen Listen erkennbarer Elemente, und veröffentlichen Sie die Aktivitätsnotiz • Ausgabe: Nicht zutreffend

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	Beschreibung	Beispielszenario	
	Listenelemente und fügt sie nicht der zugehörigen Liste erkennbarer Elemente des Security Incidents hinzu. Eine automatisierte Systemaktivität (Antwort) wird hinzugefügt, um anzuzeigen, dass diese erkennbaren Elemente entfernt wurden.		
Ruft betroffene Anwender (zugehörige Listen) aus mehreren Security Incidents ab V1	Ruft alle betroffenen Anwender ab, die in der zugehörigen Liste Betroffene Anwender für die angegebenen Security Incidents aufgeführt sind.	Sie können übergeordnete Security Incidents mit mehreren untergeordneten Security Incidents haben. Verwenden Sie diese Aktion, um ein Rollup für betroffene Anwender aus allen untergeordneten Security Incidents zu den entsprechenden übergeordneten Security Incidents durchzuführen. Nur eindeutige betroffene Anwender werden zusammengefasst, und alle Duplikate werden entfernt.	• Eingabe: Security Incidents • Ausgabe: ◦ Betroffener Anwender ◦ count
Ruft betroffene Anwender aus mehreren Security Incidents ab	Ruft den primären betroffenen Anwender für den angegebenen Security Incident ab. Die betroffenen Anwender aus der zugehörigen Liste Betroffene Anwender sind nicht enthalten.	• Senden Sie bei der Untersuchung eines Phishing-Security Incidents eine E-Mail an die primären betroffenen Anwender (die den Phishing-Incident gemeldet haben), um zu bestätigen, ob einer der Anwender auf die schädlichen Links in der Phishing-E-Mail geklickt hat. • Aktualisieren Sie den Schweregrad oder die Risikopunktzahl	• Eingabe: Security Incidents • Ausgabe: ◦ Betroffene Anwender ◦ count

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	Beschreibung	Beispielszenario	
		des übergeordneten Security Incidents basierend auf der Anzahl der primär betroffenen Anwender.	
Ruft betroffene Anwender (zugehörige Liste) aus einem Security Incident ab	Ruft alle betroffenen Anwender ab, die in der zugehörigen Liste Betroffene Anwender für einen angegebenen Security Incident aufgeführt sind.		• Eingabe: Security Incidents • Ausgabe: ◦ Betroffene Anwender ◦ count
Fügen Sie dem Security Incident betroffene Anwender hinzu	Fügt alle betroffenen Anwender einem Security Incident hinzu.	Angenommen, Sie haben einen übergeordneten Security Incident mit mehreren untergeordneten Security Incidents. Sie können diese Aktion verwenden, um betroffene Anwender aus allen untergeordneten Security Incidents zum entsprechenden übergeordneten Security Incident zusammenzufassen. Nur eindeutige betroffene Anwender werden zusammengefasst, und alle Duplikate werden entfernt.	• Eingabe: ◦ Security Incident ◦ Anwender • Ausgabe: Nicht zutreffend
Rufen Sie Konfigurationselemente der betroffenen Anwender ab	Ruft die Konfigurationselemente (Configuration Items, CIs) aller betroffenen Anwender ab.	In Phishing- oder Malware-Szenarien können Sie diese Aktion verwenden, um die zugehörige Liste Betroffene Configuration Items (CI) zu aktualisieren und die CIs zu untersuchen. Sie können dann den Schweregrad oder die Risikopunktzahl des Security Incidents basierend auf der Anzahl der identifizierten CIs aktualisieren.	• Eingabe: Anwender • Ausgabe: ◦ Konfigurationselemente ◦ count

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	Beschreibung	Beispielszenario	
Ruft alle untergeordneten Security Incidents für einen Security Incident ab	Ruft alle untergeordneten Security Incidents ab, die sich auf einen bestimmten übergeordneten Security Incident beziehen.	Beispielszenario: Verwenden Sie diese Aktion, um: • Aktualisieren Sie den Status der untergeordneten Security Incidents, wenn der entsprechende Status der übergeordneten Security Incidents aktualisiert wird. • Aktualisieren Sie den Schweregrad oder die Risikopunktzahl des Security Incidents automatisch basierend auf der Anzahl der untergeordneten Security Incidents.	• Eingabe: ◦ Security Incident ◦ Incident-Status • Ausgabe: ◦ Untergeordneter Security Incident ◦ count
Konfigurationselemente für die erkennbaren Elemente abrufen (IP-Adresse eingeben)	Ruft alle Konfigurationselemente (Configuration Items, CIs) für erkennbare Elemente vom Typ „IP-Adresse“ ab.	Ein erkennbares IP-Adresse kann einem Konfigurationselement zugeordnet werden. Zum Beispiel die IP-Adresse eines Servers. Wenn Sie diese Aktion verwenden, können Sie Informationen für den Server abrufen.	• Eingabe: ip-Adresse des erkennbaren Elements • Ausgabe: ◦ Konfigurationselemente ◦ count
Ist erkennbares Element böswillig	Bestätigt das Vorhandensein eines oder mehrerer schädlicher erkennbarer Elemente in einer Reihe von erkennbaren Elementen.	Nachdem die Bedrohungssuche abgeschlossen wurde und Sie das Vorhandensein schädlicher erkennbarer Elemente identifiziert haben, können Sie den Schweregrad oder die Risikopunktzahl eines Security Incidents erhöhen.	• Eingabe: Security Incident • Ausgabe: Böswillig (wahr/falsch)
Senden Sie eine E-Mail, um die Anwenderinteraktion zu bestätigen	Sendet eine E-Mail als Antwort auf eine Anwenderantwort.	Wenn ein Anwender mehrmals versucht, sich bei einer Anwendung anzumelden, führt dies zu einem fehlgeschlagenen Anmeldeszenario.	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	Beschreibung	Beispielszenario	
		In diesem Fall wird eine E-Mail an den Anwender gesendet, um zu bestätigen, ob der Anwender versucht hat, sich anzumelden oder nicht. Je nach Anwenderantwort (Ja oder Nein) können verschiedene Aktionen ausgeführt werden. **Flow** : Manuelles Playbook für fehlgeschlagene Anmeldung	
Filtern Sie erkennbare Elemente der zulässigen Liste heraus	Verwenden Sie diese Aktion, um das Auflisten erkennbarer Elemente aus einem bestimmten Satz erkennbarer Elemente zuzulassen.	Sie können bestimmte erkennbare Elemente identifizieren, die aus einer Reihe erkennbarer Elemente ignoriert werden können. Diese erkennbaren Elemente werden bei der Lösung des Security Incident nicht berücksichtigt.	• Eingabe: Security Incident • Ausgabe: ◦ Zulässige Liste erkennbarer Elemente ◦ count
Passwort für betroffene Anwender zurücksetzen	Verwenden Sie diese Aktion, um das Passwort für betroffene Anwender zurückzusetzen.	Wenn ein Anwenderaccount gehackt wurde oder ein Anwender die Zurücksetzung eines Passworts anfordert, wird eine E-Mail an den Anwender gesendet, um das Passwort zurückzusetzen. **Flow** : Manuelles Playbook für fehlgeschlagene Anmeldung.	
Anwendergruppe für betroffenen Anwender abrufen	Ruft die Anwendergruppendetails der betroffenen Anwender ab.	Wenn in einer Organisation zwei oder mehr Anwender Phishing-E-Mails melden, können Sie die Gruppe herausfinden, zu der sie gehören, und feststellen, ob weitere Anwender betroffen waren	• Eingabe: Anwender • Ausgabe: ◦ Anwendergruppen ◦ count

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Visuelle Darstellung der Berichterstellung für Security Incident Response

Sicherheitsmanager können die allgemeinen grafischen Oberflächen wie Karten und Baumpläne verwenden, um Problembereiche zu identifizieren.

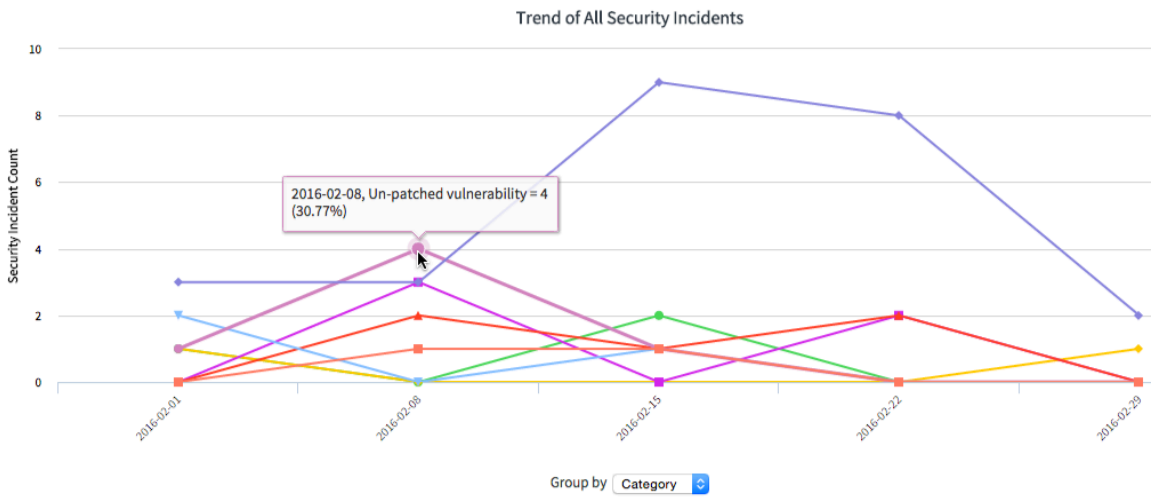
Zum Anzeigen Security Incident Response Explorer-Dashboard in Arbeitsbereich für Security Incident Response Weitere Informationen finden Sie unter SIR Workspace-Dashboards anzeigen.

Security Incident Response-Dashboard „Übersicht“

Die Security Incident Response Das Übersichts-Dashboard bietet einen Überblick über die Aktivitäten von Security Incidents, Trends und Berichte sowie Drilldowns zu bestimmten Daten.

Das Modul Übersicht zeigt Security Incident-Informationen an, die auf die Rolle des Anwenders zugeschnitten sind. Sie können auf einen beliebigen Teil eines Diagramms zeigen (Balken, Kreis, Datenpunkt, Heatmap usw.), um allgemeine Daten anzuzeigen, die für diesen Teil spezifisch sind. Siehe folgende Abbildung. Wenn Sie auf einen Teil eines Berichts klicken, wird eine Liste mit detaillierten Informationen geöffnet.

Trend aller Security Incidents



Sicherheitsvorfallmanager – Übersicht

Benutzer mit den Rollen Security Incident-Administrator und Security Incident-Manager zeigen die Security Incident Manager-Übersicht an. Enthält die folgenden Berichte im Basissystem.

Security Incident Manager – Übersichtsberichte

Name	Visuell	Beschreibung
Team Security Incidents mit Priorität „Kritisch“	Einzelne Punktzahl	Die Anzahl der kritischen Security Incidents, die dem Team zugewiesen sind.
Team Security Incidents mit Priorität „Hoch“	Einzelne Punktzahl	Die Anzahl der Incidents mit hoher Sicherheit, die dem Team zugewiesen sind.
In 24 Stunden ablaufende SLAs	Einzelne Punktzahl	Die Anzahl der SLAs, die innerhalb der nächsten 24 Stunden ablaufen.
Risiko vs. Schweregrad	Heatmap	Die Verteilung der Security Incidents, die dem Team zugewiesen sind, nach Risiko und Schweregrad.
Security Incidents nach CI-Klasse, letzte 3 Monate	Balkendiagramm	Die Anzahl der Security Incidents, die dem Team nach Konfigurationselementklasse zugewiesen sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Manager – Übersichtsberichte (Fortsetzung)

Name	Visuell	Beschreibung
Trend aller Security Incidents	Trend	Stellt die Anzahl der empfangenen Security Incidents nach Kategorie oder Priorität dar.
Security Incidents Mit Nicht Autorisiertem Zugriff	Balkendiagramm	Zeigt die Typen der im Laufe der Zeit empfangenen Security Incident-Kategorien an.
Durchschnittliche Zeit bis zur Eindämmung	Einzelne Punktzahl	Die durchschnittliche Zeit, die benötigt wird, um alle Security Incidents einzudämmen.
Durchschnittliche Zeit bis zur Eindämmung kritischer Elemente	Einzelne Punktzahl	Die durchschnittliche Zeit, die benötigt wird, um alle kritischen Security Incidents einzudämmen.
Durchschnittliche Zeit bis zur Identität	Einzelne Punktzahl	Die durchschnittliche Zeit, die zur Identifizierung aller Security Incidents benötigt wird.

Sicherheitsanalyst – Übersicht

Benutzer mit der Rolle „Security Incident Analyst“ zeigen die Sicherheitsanalyst-Übersicht an. Enthält die folgenden Berichte im Basissystem.

Sicherheitsanalystenübersicht – Berichte

Name	Visuell	Beschreibung
Meine Arbeit mit kritischer Priorität	Einzelne Punktzahl	Die Anzahl der mir zugewiesenen kritischen Security Incidents.
Meine Arbeit mit hoher Priorität	Einzelne Punktzahl	Die Anzahl der mir zugewiesenen Incidents mit hoher Sicherheit.
Meine in 24 Stunden ablaufenden SLAs	Einzelne Punktzahl	Die Anzahl der mir zugewiesenen SLAs, die innerhalb der nächsten 24 Stunden ablaufen.
Mir zugewiesene Security Incidents	Balkendiagramm	Mir zugewiesene Security Incidents nach Incident-Status oder -Kategorie.
Mir zugewiesene Arbeit nach Typ	Balkendiagramm	Mir zugewiesene Sicherheitsaufgaben (Incidents, Aufgaben oder Anforderungen) nach Typ oder Priorität.
Mir zugewiesene Security Incidents, Anforderungen, Aufgaben	Liste	Eine Liste aller mir zugewiesenen Security Incidents, Sicherheitsanforderungen und Aufgaben.
Ort des Security Incidents	Karte	Regionaler Standort der Security Incidents.
Anzahl	Karte	Anzahl der Security Incidents pro Region.
Min./Max. Anzahl	Farbspektrum-Balken	Die minimale und maximale Anzahl von Security Incidents pro Region, dargestellt durch einen Farbspektrumbalken.
Prozentsatz der Anzahl	Karte	Prozentsatz der Gesamtanzahl der Incidents pro Region.

Security Incident-CISO-Übersicht mit aktivierter Security Incident Analytics

Wenn Security Incident Analytics Das Plugin ist aktiviert. Benutzer mit den Rollen Security Incident CISO und Systemadministrator zeigen die Security Incident CISO-Übersicht an. Die folgenden CISO-Berichte werden im Basissystem bereitgestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident-CISO-Übersichtsberichte (mit aktivierter Security Incident Analytics)

Name	Visuell	Beschreibung
Neue Security Incidents diese Woche	Einzelne Punktzahl	Die Anzahl der neuen Security Incidents, die in der aktuellen Woche empfangen wurden.
Diese Woche geschlossene Security Incidents	Einzelne Punktzahl	Die Anzahl der in der aktuellen Woche geschlossenen Security Incidents.
Neue Security Incidents (Ausführung 7 Tage)	Einzelne Punktzahl	Die Anzahl der innerhalb der letzten 7 Tage geöffneten Security Incidents.
Geschlossene Security Incidents (Ausführung 7 Tage)	Einzelne Punktzahl	Die Anzahl der innerhalb der letzten 7 Tage geschlossenen Security Incidents.
Tägliche neue Security Incidents vs. Geschlossene Security Incidents	Trend	Anzahl neuer und geschlossener Security Incidents im Zeitverlauf nach Tag.
Wöchentliche neue Security Incidents vs. Geschlossene Security Incidents	Trend	Neue und geschlossene Security Incidents im Zeitverlauf nach Woche.
Lösungscode für Security Incident	Trend	Vollständige Anzahl der Abschlusscodes im Zeitverlauf.
Security Incident – Geschäftsauswirkung	Verzeichnisübersicht	Business-Services mit Security Incidents mit verfügbaren Gruppierungen nach Geschäftsrelevanz.
Durchschnittliche Zeit bis Eindämmung (wöchentlich)	Trend	Die durchschnittliche Zeit von 7 Tagen, die benötigt wird, um einen Security Incident im Laufe der Zeit einzudämmen.
Durchschnittliche Zeit bis Beseitigung (wöchentlich)	Trend	Die durchschnittliche Zeit von 7 Tagen, die zur Beseitigung eines Security Incidents im Laufe der Zeit benötigt wird.
Durchschnittliche Zeit bis Identifizierung (wöchentlich)	Trend	Die durchschnittliche Zeit von 7 Tagen, die zur Identifizierung eines Security Incidents im Laufe der Zeit benötigt wird.
Ort des Security Incidents	Karte	Regionaler Standort der Security Incidents.
Anzahl	Karte	Anzahl der Security Incidents pro Region.
Min./Max. Anzahl	Farbspektrum-Balken	Die minimale und maximale Anzahl von Security Incidents pro Region, dargestellt durch einen Farbspektrumbalken.
Prozentsatz der Anzahl	Karte	Prozentsatz der Gesamtanzahl der Incidents pro Region.

Security Incident-CISO-Übersicht ohne aktivierte Security Incident Analytics

Wenn Security Incident Analytics Plugin ist nicht aktiviert, Benutzer mit den Rollen Security Incident CISO und Systemadministrator zeigen die Security Incident CISO Reporting-Übersicht an. Die folgenden CISO-Berichte werden im Basissystem bereitgestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident-CISO-Übersichtsberichte (ohne aktivierte Security Incident Analytics)

Name	Visuell	Beschreibung
Neue Security Incidents diese Woche	Einzelne Punktzahl	Die Anzahl der neuen Security Incidents, die in der aktuellen Woche geöffnet wurden.
Diese Woche geschlossene Security Incidents	Einzelne Punktzahl	Die Anzahl der in der aktuellen Woche geschlossenen Security Incidents.
Neue Security Incidents (Ausführung 7 Tage)	Einzelne Punktzahl	Die Anzahl der innerhalb der letzten 7 Tage geöffneten Security Incidents.
Geschlossene Security Incidents (Ausführung 7 Tage)	Einzelne Punktzahl	Die Anzahl der innerhalb der letzten 7 Tage geschlossenen Security Incidents.
Wöchentliche neue Security Incidents	Trend	Die neuen Security Incidents, die wöchentlich geöffnet wurden.
Wöchentliche geschlossene Security Incidents	Trend	Die wöchentlich geschlossenen Security Incidents.
Lösungscodes für Security Incident	Trend	Abschlusscodes für Security Incidents im Zeitverlauf.
Business Services mit Sicherheitsvorfällen – Geschäftsauswirkung	Verzeichnisübersicht	Business-Services mit Security Incidents mit verfügbaren Gruppierungen nach Geschäftsrelevanz.
Durchschnittliche Zeit bis zur Eindämmung	Einzelne Punktzahl	Die durchschnittliche Zeit, die benötigt wird, um alle Security Incidents einzudämmen.
Durchschnittliche Zeit bis zur Eindämmung kritischer Elemente	Einzelne Punktzahl	Die durchschnittliche Zeit, die benötigt wird, um alle kritischen Security Incidents einzudämmen.
Durchschnittliche Zeit bis zur Identität	Einzelne Punktzahl	Die durchschnittliche Zeit, die zur Identifizierung aller Security Incidents benötigt wird.

Hinweis:
Die Security Incident Response Das Basissystem enthält Performance Analytics-Lösungen zum Anzeigen vorkonfigurierter Best Practice-Dashboards. Die Dashboards enthalten wichtige Metriken für die Analyse Ihres Prozesses in Security Incident Response, z. B. neue Sicherheitsvorfälle oder das durchschnittliche Alter offener Sicherheitsvorfälle. Weitere Informationen und Installationsanweisungen finden Sie unter Security Incident Response Platform Analytics-Lösungen.

Greifen Sie Auf Den Security Incident Response Explorer Zu

Sie können auf zugreifen Security Incident Response Explorer-Dashboard zum Anzeigen von Security Incident-Aktivitäten, um Problembereiche sofort zu erkennen und Probleme schnell zu lösen.

Vorbereitungen
Erforderliche Rollen:

- sn_si.admin (zum Schreiben)
- sn_si_Basic (zum Lesen)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Self-Service** > **Homepage** Oder navigieren Sie zu **Self-Service** > **Dashboards**an.
2. Wählen Sie Security Incident Explorer aus der Berichtsliste aus.

Ergebnisse

Die Security Incident Response Explorer-Dashboard wird angezeigt.

Nächste Maßnahme

Zum Anzeigen Security Incident Response Explorer-Dashboard in Arbeitsbereich für Security Incident Response Weitere Informationen finden Sie unter SIR Workspace-Dashboards anzeigen.

Security Incident-Zuordnung

Die Security Incident-Karte stellt Daten nach geografischem Standort bereit. Die Weltkarte wird in jedem Bereich hervorgehoben, in dem ein Incident auftritt. Wenn Security Incident Analytics Das Plugin ist aktiviert. Sie können die Zuordnung von Security Incidents zu hinzufügen Security Incident ResponseÜbersicht. Nachdem sie hinzugefügt wurde, können Sie die Karte konfigurieren, indem Sie die Kartenfilter ändern.

Fügen Sie Zuordnung zu hinzu Security Incident ResponseÜbersicht

Sie können die Karte zu hinzufügen Security Incident ResponseÜbersicht zum Anzeigen von Security Incident-Daten nach geografischem Standort. Mit einer Karte können Sie nach Standort Detailinformationen zu Security Incidents anzeigen.

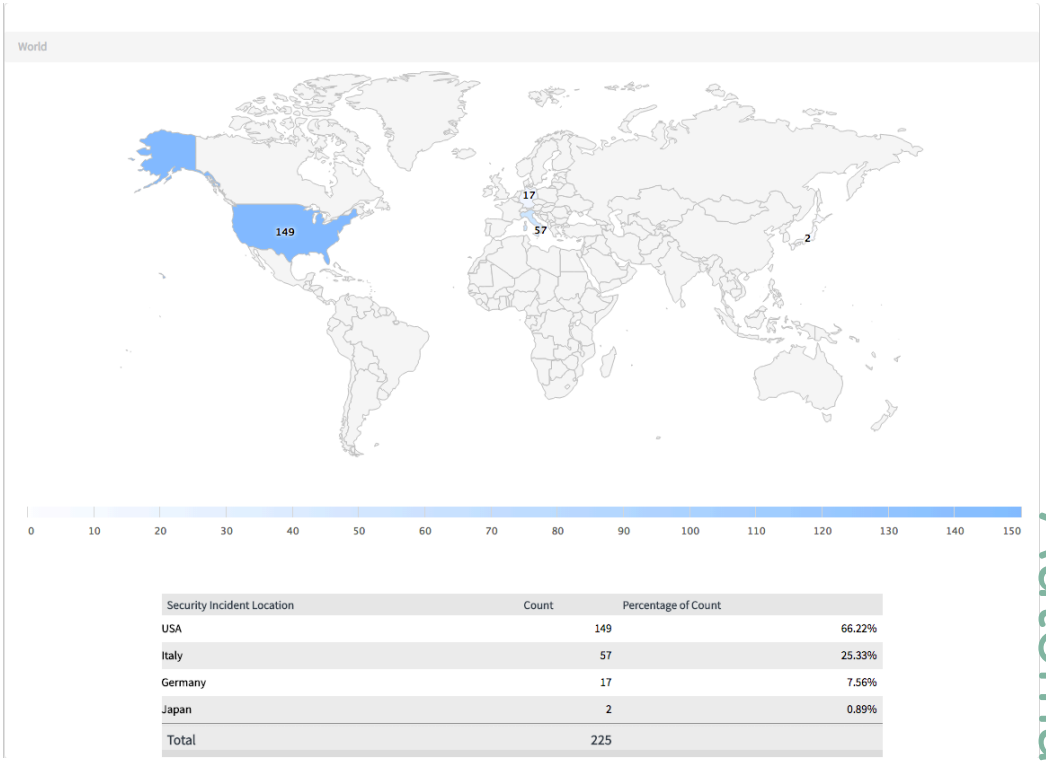
Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Übersicht**an.
2. Klicken Sie Auf **Fügen Sie Inhalt hinzu** In der oberen linken Ecke der Seite, um das Steuerelement für die Widget-Auswahl zu öffnen.
3. Klicken Sie im ersten Auswahlfeld auf **Berichte** .
4. Klicken Sie im zweiten Auswahlfeld auf **Security Incident** .
5. Klicken Sie im dritten Auswahlfeld auf **Zuordnung von Security Incidents** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Security Incident Location	Count	Percentage of Count
USA	149	66.22%
Italy	57	25.33%
Germany	17	7.56%
Japan	2	0.89%
Total	225	

6. Klicken Sie unten auf dem Bildschirm auf die Stelle auf dem Bildschirm, die Sie dem Bericht hinzufügen möchten.
7. Schließen Sie **Fügen Sie Inhalt hinzu** Feld.

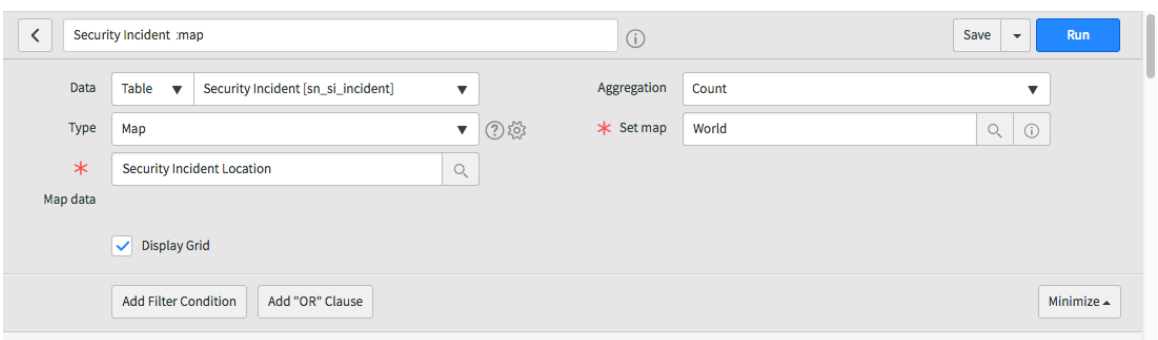
Ändern Sie die Security Incident-Zuordnung

Administratoren in der globalen Domäne können mithilfe von Filtern ändern, wie die Security Incident-Zuordnung Security Incidents behandelt.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Berichte** > **Administration** > **Alle**an.
2. Suchen Sie nach **Zuordnung von Security Incidents** .
3. Klicken Sie Auf **Bearbeiten Sie Den Bericht** .



4. Klicken Sie Auf **Fügen Sie Eine Filterbedingung Hinzu** Zum Hinzufügen oder Bearbeiten von Filtern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie Auf **Ausführen** Um die angewendeten Änderungen anzuzeigen.
6. Klicken Sie auf **Speichern**.

Security Incident-Verzeichnisse

Wenn Security Incident Analytics Das Plugin ist aktiviert. Sie können dem die Tabellen Security Incident – Serviceauswirkung und Security Incident – Echtzeit hinzufügen Security Incident ResponseÜbersicht. Nachdem sie hinzugefügt wurden, können Sie die Verzeichniszuordnungen konfigurieren, indem Sie die Verzeichniskategorien und -Indikatoren ändern.

Fügen Sie der Übersicht über Security Incident Response Baumstrukturen hinzu

Baumstrukturen zeigen hierarchische (strukturierte) Daten als Satz geschachtelter Rechtecke an. Jeder Verzweigung der Struktur wird ein Rechteck zugewiesen, das dann mit kleineren Rechtecken gekachelt wird, die Unterverzweigungen darstellen. Mit Baumstrukturen können Sie Security Incident-Informationen auf dynamische und ansprechende Weise anzeigen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

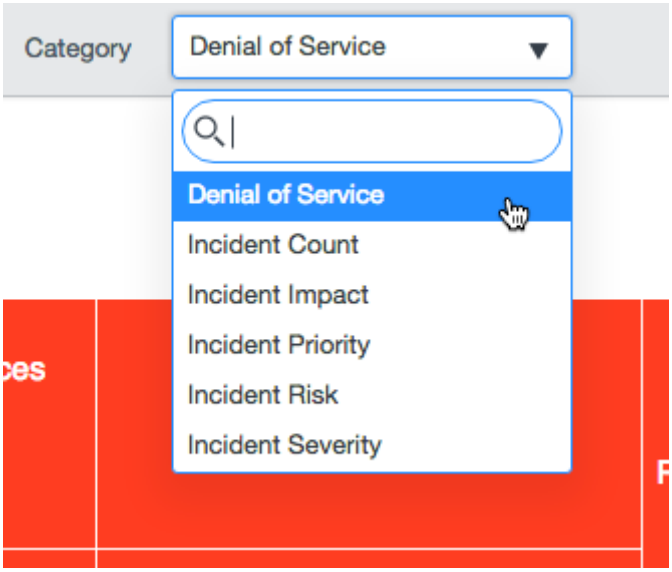
Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Übersicht**an.
2. Klicken Sie Auf **Fügen Sie Inhalt hinzu** In der oberen linken Ecke der Seite, um das Steuerelement für die Widget-Auswahl zu öffnen.
3. Klicken Sie im ersten Auswahlfeld auf **Baumübersicht** .
4. Wählen Sie im zweiten Auswahlfeld die Baumkarte aus der folgenden Liste aus, die Sie einfügen möchten:
   - Security Incident: Serviceauswirkung
   - Security Incident: Echtzeit
   - Security Incident: Geschäftsauswirkung
   - Bedeutung Der Schwachstelle

   Hinweis:
   Die Struktur „Geschäftsauswirkung“ wird auf der angezeigt Security Incident Response Homepage standardmäßig. Für die Verzeichnisse „Serviceauswirkung“ und „Echtzeit“ muss das Plugin „Security Incident Analytics“ aktiviert sein.
5. Wählen Sie im dritten Auswahlfeld die Ebene der Granularität der Informationen aus, die Sie für die ausgewählte Baumstruktur abrufen möchten.

   Hinweis:
   Wählen Sie für die Treemap Security Incident – Serviceauswirkung die Option aus **Security Incident** Im dritten Auswahlfeld. Diese Auswahl bietet eine Dropdown-Liste mit mehreren Datenkategorien.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Klicken Sie unten im Bildschirm auf die Position auf dem Bildschirm, an der Sie die Anzeige hinzufügen möchten.
7. Schließen Sie **Fügen Sie Inhalt hinzu** Feld.

Erstellen oder aktualisieren Sie eine Baumordnerkategorie

Sie können die vordefinierten Kategorien für die Security Incident-Verzeichnisse ändern oder Kategorien nach Bedarf erstellen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Die Treemaps verwenden Performance Analytics als Datenquelle. Das Performance Analytics-Modul erfordert ein separates Plugin.

Warum und wann dieser Vorgang ausgeführt wird

Im Basissystem sind Baumstrukturkategorien wie Incident-Risiko, Denial of Service und Incident-Schweregrad enthalten. Sie können diese Kategorien nach Bedarf ändern oder weitere Kategorien definieren.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Administration**, Und öffnen Sie die Baumstrukturdefinition, für die Sie Kategorien konfigurieren möchten:
   - **Servicerelevanz-Reportingdefinition**
   - **Echtzeitdefinition**
2. **Wahlweise:** Ändern Sie den Namen der Baumstrukturdefinition.
   Im Basissystem lautet der Standardname für die Definition der Serviceauswirkungsstruktur **Security Incident** . Der Standardname für die Echtzeit-Strukturzuordnungsdefinition ist **Security Incident: Echtzeit** .
3. Ändern Sie nicht, wenn Sie keine anwenderdefinierte Baumübersicht verwenden **PA-Indikatorgruppe** Wert.
4. Um die Strukturzuordnungsdefinition zu deaktivieren, löschen Sie **Aktiv** Kontrollkästchen.
   Wenn Sie beispielsweise die Kategorie „Denial of Service“ im Dashboard „Systemauswirkung“ deaktivieren, ist diese Baumordnerkategorie nicht verfügbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. In **Verzeichniskategorien** Zugehörige Liste wählen Sie eine Kategorie aus, die Sie ändern möchten, oder klicken Sie auf **Neu** Um eine neue Kategorie zu erstellen.
6. Füllen Sie die Felder aus.

Formular „Baumordnerkategorie“

Feld	Beschreibung
Name	Der Name, der für die Kategorie in angezeigt wird **Kategorien** Liste über der Baumstruktur.
Reihenfolge	Die Reihenfolge, in der die Kategorie in angezeigt wird **Kategorien** Liste über der Baumstruktur.
Verzeichnisübersicht	Der Name der Baumkarte, die diese Kategorie verwendet.
Farbe	Die Farbe, die für diese Kategorie in der Baumübersicht angezeigt wird.
Aktiv	Auswählen, um diese Kategorie zu aktivieren.
Beschreibung	Eine Beschreibung der Kategorie.
Für alle Rollen sichtbar	Wählen Sie diese Option aus, um diese Kategorie für alle Anwender unabhängig von ihrer Rolle sichtbar zu machen.
Rollen	Wenn Sie nicht ausgewählt haben **Für alle Rollen sichtbar** Aktivieren Sie das Kontrollkästchen, um die Rollen auszuwählen, die diese Kategorie anzeigen können.

7. Klicken Sie auf **Absenden** oder **Aktualisieren**.

Erstellen oder aktualisieren Sie einen Treemap-Indikator

Sie können die vordefinierten Indikatoren für eine Baumordnerkategorie ändern oder neue Indikatoren erstellen. Für jeden Indikator können Sie seine Datenquelle konfigurieren und angeben, wie Listen von Security Incidents aus Baumstrukturen geöffnet werden, die mit dem Indikator angezeigt werden.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Die Treemaps verwenden Performance Analytics als Datenquelle. Das Performance Analytics-Modul erfordert ein separates Plugin.

Prozedur

1. Öffnen Sie die Baumstrukturdefinition, für die Sie Indikatoren konfigurieren möchten.
2. In **Verzeichniskategorien** Zugehörige Liste wählen Sie die Kategorie aus, für die Sie Indikatoren konfigurieren möchten.
3. In **Indikatoren Für Die Strukturzuordnung** Zugehörige Liste wählen Sie einen Indikator aus, der geändert werden soll, oder klicken Sie auf **Neu** Um einen neuen Indikator zu erstellen.
4. Füllen Sie die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Strukturzuordnungsindikator“

Feld	Beschreibung
Name	Der Name, der für den Indikator in angezeigt wird **Indikatoren** Liste im Dashboard „Serviceauswirkung“.
Kurzbeschreibung	Eine Beschreibung, die für den Indikator in angezeigt wird **Indikatoren** Liste über der Baumstruktur.
Ergebnisgrenzwert	Die maximale Anzahl zulässiger Ergebnisse. Die Obergrenze ist 100.
Ergebnisgenauigkeit	Die Anzahl der Stellen, die nach dem Dezimalpunkt angezeigt werden sollen. Dieses Feld wird nur für die Echtzeit-Strukturzuordnungsdefinition angezeigt.
Aktiv	Kontrollkästchen zum Aktivieren dieses Indikators.
Kategorie	Der auf dem vorherigen Bildschirm eingegebene Kategoriename.
Wegbeschreibung	Gibt an, ob die Kachel auf der Baumkarte minimiert oder maximiert ist. Dieses Feld wird nur für die Echtzeit-Strukturzuordnungsdefinition angezeigt.
Einheit	Die Maßeinheit, die für die Metrik verwendet werden soll. Dieses Feld wird nur für die Echtzeitdefinition angezeigt.
Automatisches Aktualisierungsintervall	Wie häufig die Baumstruktur aktualisiert werden soll.
Reihenfolge	Die Reihenfolge, in der der Indikator angezeigt wird **Indikatoren** Liste über der Baumstruktur.

5. Klicken Sie auf **Datenquellenkonfiguration** Registerkarte und konfigurieren Sie eine der folgenden Datenquellenoptionen für den Indikator.

6. Klicken Sie auf **Klicken Sie Durch** Und geben Sie an, wie Listen von Security Incidents über die Baumübersicht geöffnet werden.
   a. In **Klicken Sie durch URL-Navigationstyp** Feld auswählen, ob die Liste der Security Incidents in einem neuen Fenster, im selben Fenster oder in einem Dialogfeld geöffnet werden soll.
   b. **Wahlweise:** In **Klicken Sie durch das URL-Skript** Feld, ändern Sie bei Bedarf das Beispielskript.
7. Klicken Sie auf **Absenden** oder **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie einer Übersicht Diagramme zur Bedeutung von Schwachstellen hinzu

Wenn Vulnerability Response Das Plugin ist aktiviert. Sie können der Übersicht Diagramme zur Definition der Schwachstellenbedeutung und andere Visualisierungen hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren Sie zur Übersichtsseite, der Sie die Schwachstellen-Bedeutungsanzeige hinzufügen möchten.
2. Klicken Sie Auf **Fügen Sie Inhalt hinzu** In der oberen linken Ecke der Seite, um das Steuerelement für die Widget-Auswahl zu öffnen.
3. Treffen Sie in den drei Auswahlfeldern die Auswahl abhängig von der Anzeige (Strukturzuordnung oder Punktzahlbericht), die Sie hinzufügen möchten:
   - Um die Strukturzuordnung der Schwachstellenbedeutung hinzuzufügen, treffen Sie die folgenden Auswahlmöglichkeiten:
     - Verzeichnisübersicht
     - Bedeutung Der Schwachstelle
     - Bedeutung Der Schwachstelle
   - Um den Bericht „Schwachstellenbedeutung Punktzahl“ hinzuzufügen, treffen Sie die folgenden Auswahlmöglichkeiten:
     - Performance Analytics
     - Punktzahl
     - Services mit Bedeutung für Schwachstellen
4. Klicken Sie auf die Position auf dem Bildschirm, an der Sie die Anzeige hinzufügen möchten.
5. Schließen Sie **Fügen Sie Inhalt hinzu** Feld.

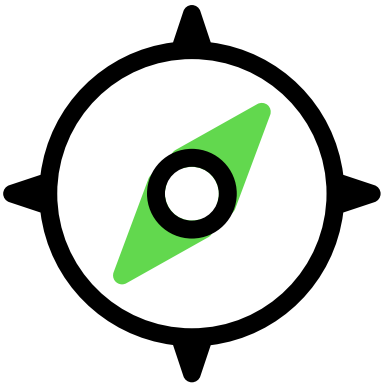
Management schwerwiegender Sicherheits-Incidents

Die ServiceNow® Management schwerwiegender Sicherheits-Incidents Die Anwendung verfolgt den Fortschritt von Major Security Incident(MSI) von der Discovery über die Analyse, Vorschlagen, Heraufstufen und Verknüpfen von Security Incidents bis zum Abschluss.

Management schwerwiegender Sicherheits-Incidents

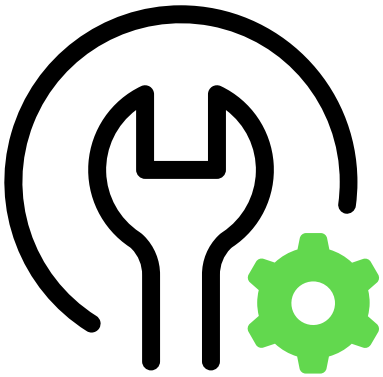
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



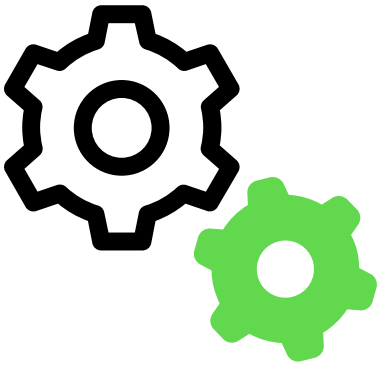
Erfahren Sie, wie Analysten, Administratoren und Manager das Management schwerwiegender Security Incidents (MSIM) verwenden

Konfigurieren



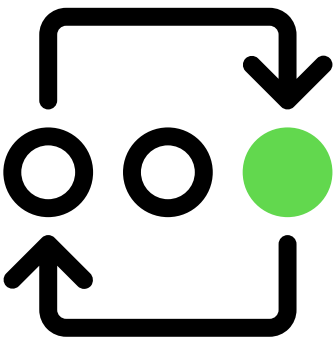
Planen und konfigurieren Sie Ihre Implementierung

Integrieren



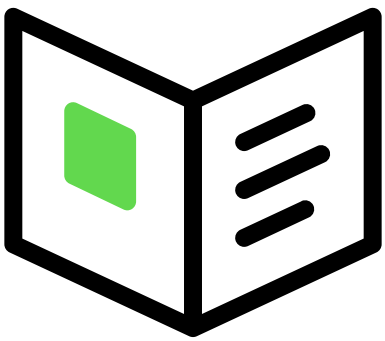
Erweitern Sie MSIM-Fähigkeiten durch Integration mit anderen Microsoft Anwendungen

Verwalten



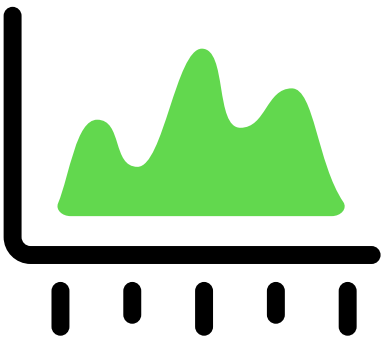
Administrationsaufgaben zum Taggen von Incident-Datensätzen und Konfigurieren von Bezeichnungen

Verwenden



Über das Arbeitsbereichsmanagement können Sie Datensätze für schwerwiegende Security Incidents vorschlagen, heraufstufen, verknüpfen und ablehnen

Statusberichte



Überwachen Sie Incident-bezogene Aufgaben, und verbessern Sie Prozesse durch Metriken, Trenddiagramme und Berichte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Fähigkeiten		
Konfigurieren Sie Informationen zum Rollup von Datensätzen		

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Security Operations-Apps im Store anfordern

Wenn Sie neu sind Security Operations Kunde am Rome Oder besuchen Sie später die ServiceNow Store Website zum Anzeigen der verfügbaren Apps und Informationen zum Senden von Anforderungen an den Store.

Problembehandlung und Hilfe

- Management schwerwiegender Sicherheits-Incidents -forum auf der ServiceNow Community an.
- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Management Schwerwiegender Security Incidents Erkunden

Erkunden Management schwerwiegender Sicherheits-Incidents Um zu verstehen, wie die Anwendung bei der Nachverfolgung kritischer Security Incidents mit hoher Priorität funktioniert, die als Bedrohung für die Organisation identifiziert werden.

In diesem Abschnitt erfahren Sie mehr über die wichtigsten Funktionen und verschiedenen Rollen, die bei der Arbeit mit Datensätzen schwerwiegender Security Incidents beteiligt sind. In diesem Abschnitt erfahren Sie auch, wie Sie mit der Anwendung, den Voraussetzungen und den Plugins beginnen, die für die Arbeit mit der Anwendung erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Management schwerwiegender Sicherheits-Incidents

Verfolgen und verwalten Sie verschiedene Aktivitäten, die normalerweise Teil der Lösung eines schwerwiegenden Security Incident durch sind Management schwerwiegender Sicherheits-Incidents. Über einen intuitiven Arbeitsbereich können Incident-Manager und Personen, die an einem Incident arbeiten, Incidents vorschlagen und zu schwerwiegenden Incidents heraufstufen, Aktivitäten schwerwiegender Security Incidents nachverfolgen und einfach mit Kollegen zusammenarbeiten.

Übersicht

Die Funktionen für das Management schwerwiegender Security Incidents funktionieren in Verbindung mit den vorhandenen Security Incident Response-Produktfunktionen. Dies umfasst die Fähigkeit eines Sicherheitsanalysten, einen Standard-Security Incident zu einem schwerwiegenden Security Incident zu eskalieren, sodass die neuen Produktfunktionen zur Unterstützung des Korrekturprozesses verfügbar sind.

Nachdem Sie auf installiert haben ServiceNow Instanz kann ein Security Incident-Analyst:

- Schlagen Sie dem Kandidaten für einen schwerwiegenden Security Incident einen Security Incident vor, um einen Überprüfungsprozess zu initiieren, ob ein schwerwiegender Security Incident erstellt werden muss.
- Einen Security Incident direkt zu einem schwerwiegenden Security Incident heraufstufen, ohne dass ein zusätzlicher Überprüfungsprozess erforderlich ist.
- Lehnen Sie einen Security Incident ab, der als schwerwiegender Security Incident (MSI) vorgeschlagen wird.
- Verknüpfen Sie einen Security Incident als untergeordneten Incident mit dem schwerwiegenden Security Incident (MSI), damit alle Security Incidents bearbeitet werden können.

Schlüsselfunktionen

Management schwerwiegender Security Incidents (MSIM) verbessert den Korrekturprozess für schwerwiegende Security Incidents mit den folgenden Funktionen:

- Dedizierter Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents, der für die Anwenderrolle „Manager für schwerwiegende Security Incidents“ konzipiert ist.
- Organisieren Sie Antwortaufgaben für mehrere „untergeordnete“ Security Incidents.
- Automatisieren Sie die Erstellung von Zusammenarbeitsordnern und Chatkommunikationskanälen, nachdem ein schwerwiegender Security Incident erstellt wurde, sowie die Archivierung im Rahmen des Incident-Abschlusses.
- Datei-Explorer-Komponente zum Organisieren und Nachverfolgen der Sammlung von Artefakten (Dateien) im Zusammenhang mit dem schwerwiegenden Security Incident über einen Microsoft SharePoint Integration.
- Komponenten des Chatkanalmanagers und des Aktivitätenstroms zur Verwaltung der Kommunikation in mehreren Sicherheits-, IT- und Funktionsgruppen über einen Microsoft Teams Integration.

Arbeitsbereichskomponenten

Die Management schwerwiegender Sicherheits-Incidents Das Produkt enthält mehrere neue Arbeitsbereichskomponenten und Anwenderoberflächenseiten, die die wichtigsten Funktionen bieten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Dedizierter Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents, der speziell für die Anwenderrolle „Manager für schwerwiegende Security Incidents“ konzipiert ist.
- Organisieren Sie Antwortaufgaben für mehrere untergeordnete Security Incidents.
- Automatisieren Sie die Erstellung von Zusammenarbeitsordnern und Chatkommunikationskanälen, nachdem ein schwerwiegender Security Incident erstellt wurde, sowie die Archivierung im Rahmen des Incident-Abschlusses.
- Datei-Explorer-Komponente zum Organisieren und Nachverfolgen der Sammlung von Artefakten (Dateien) im Zusammenhang mit dem schwerwiegenden Security Incident über einen Microsoft SharePoint Integration.
- Komponenten des Chatkanalmanagers und des Aktivitätenstroms zur Verwaltung der Kommunikation in mehreren Sicherheits-, IT- und Funktionsgruppen über einen Microsoft Teams Integration.

Unterstützte Versionen des Management schwerwiegender Security Incidents

Management schwerwiegender Sicherheits-Incidents(MSIM) Erfordert ServiceNow AI Platform® Rom-Version.

Diese Funktion unterstützt Microsoft Teams, Der ein Chat-zentrierter Arbeitsbereich in ist Microsoft Office 365 suite. Früher Microsoft Teams War eine separate Installation von Microsoft Office 365 Anwendungen.

Unterstützt ServiceNow AI Platform Versionen

Diese Funktion wird in unterstützt Rome Und spätere Releases.

Folgendes Security Operations Anwendungen sind der Standard Security Incident Response Plugins, die wahrscheinlich für die meisten Anwender installiert werden, wenn sie bereits verwenden Security Incident Response(SIR). Wenn nicht installiert, müssen Sie über installieren und aktivieren ServiceNow Store. Installieren und aktivieren Sie jeweils eine Anwendung in der angegebenen Reihenfolge, um eine reibungslose Installation zu gewährleisten:

1. Security Incident Response: Com.snc.si_dep ist das abhängige Plugin. Durch die Installation dieses Plugins werden die anderen Security Operations-Anwendungen aktiviert.
2. Sicherheits-Integrations-Framework
3. Security Support Common
4. Security Support Common Orchestration

Erste Schritte mit MSIM

Überprüfen Sie die folgenden Informationen, bevor Sie mit arbeiten Management schwerwiegender Sicherheits-Incidents.

Erforderliche Rolle: sn_msi.Workspace_admin.

Für eine einfache Installation und Konfiguration von Management schwerwiegender Sicherheits-Incidents Anwendung müssen Sie möglicherweise überprüfen, ob die folgenden Plugins aktiviert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Ein Update-Satz (KB1289784) Ist im Schnellstartleitfaden für das Management schwerwiegender Security Incidents verfügbar, um Anwendern eine einfache Konfigurationseinrichtung zu erleichtern. Sie müssen den Update-Satz importieren, nachdem Sie die Anwendungsinstallation abgeschlossen haben. Befolgen Sie das Verfahren, das in der Schnellstartanleitung (Schritt 2) im Abschnitt „Begleitdokumente“ in der MSIM-Anwendung beschrieben ist, die sich im ServiceNow Store befindet.

Voraussetzung

Aufgabe	Beschreibung
Bevor Sie mit der Anwendung beginnen, stellen Sie sicher, dass Sie über die erforderlichen abhängigen Plugins verfügen.	Installieren Sie als ersten Schritt: • ServiceNow IntegrationHub-Installationsprogramm (com.glide.hub.integrations) • ServiceNow® IntegrationHub Laufzeit (com.glide.hub.integration.runtime). • ServiceNow® IntegrationHub Action Step - REST (com.glide.hub.action_step.rest) • ServiceNow® IntegrationHub Aktionsvorlage – Datenstrom (com.Glide.Hub.action_type.datastream) • ServiceNow® IntegrationHub Flow Designer – dynamische Eingaben (com.Glide.Hub.Dynamic_input) **Hinweis:** Wenn Sie nicht über die erforderlichen Berechtigungen für eine der aufgeführten verfügen ServiceNow® IntegrationHub Plugins erstellen und dann ein Support-Ticket erstellen, um diese erforderlichen Anwendungen zu installieren.
Stellen Sie sicher, dass Sie über den erforderlichen Zugriff für die Installation verfügen Microsoft SharePoint Spoke und Microsoft Teams Graph Spoke. **Hinweis:** Die oben aufgeführten sind die primären abhängigen Anwendungen, mit denen Sie beginnen können Management schwerwiegender Sicherheits-Incidents.	Vor der Installation Microsoft SharePoint Spoke und Microsoft Teams Graph Spoke, stellen Sie sicher, dass Sie über den erforderlichen Zugriff auf verfügen ServiceNow IntegrationHub Anwendungen. **Hinweis:** Microsoft SharePoint Spoke und Microsoft Teams Graph Spoke sind abhängige Anwendungen von ServiceNow® IntegrationHub Anwendungen.

Prüfliste für MSIM Setup

Vor der Verwendung von ServiceNow® Management schwerwiegender Sicherheits-Incidents(MSIM)-Anwendung: Laden Sie die Anwendung aus dem herunter ServiceNow® Store.

Verfolgen Sie Ihren Fortschritt beim Setup, der Installation und der Konfiguration aus der folgenden Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die Rollen, die für zugewiesen sind Management schwerwiegender Sicherheits-Incidents Anwendungen werden in den folgenden Abschnitten aufgeführt. Weitere Informationen finden Sie unter Management schwerwiegender Sicherheits-Incidents Rollen.

Verwenden Sie die folgende Prüfliste, um Sie durch die End-to-End-Schritte zur Installation und Konfiguration zu führen Management schwerwiegender Sicherheits-Incidents Anwendung.

Prüfliste

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Management schwerwiegender Sicherheits-Incidents Die Anwendung wird über installiert und aktiviert ServiceNow® Store.	Management schwerwiegender Sicherheits-Incidents v1.1.1 ist für verfügbar ServiceNow® Store. Befolgen Sie diese Anweisungen: Lädt eine Anwendung aus dem herunter ServiceNow Storean.
Überprüfen Sie, ob die folgenden Anwendungen in der angegebenen Reihenfolge installiert sind.	Die folgenden Anwendungen werden nach der Installation standardmäßig installiert Management schwerwiegender Sicherheits-Incidents Anwendung in der aktuellen Release-Version der Anwendung: • File Explorer Core für Security Operations v1.1.1 • Microsoft SharePoint File Explorer Connector für Security Operations v1.1.1 • File Explorer Komponente für Security Operations v1.0.0 • Microsoft Teams Chat-Connector für Security Operations v1.0.0 • Chat-Core für Security Operations v1.0.0 • Major Security Incident Antwort v1.1.1 • EVAM-Karte für Chat für Zusammenarbeit für MSIM Arbeitsbereich v1.0.0 (diese Anwendung ist nur für die UI-Visualisierungen im Anwendungshintergrund für eingerichtet Management schwerwiegender Sicherheits-Incidents Arbeitsbereich) • UI-Komponente des Aufgabenorganisators für Management schwerwiegender Sicherheits-Incidents Arbeitsbereich 1.0.0 • Security Incident Response V12.8.1
Überprüfen Sie, ob die Anwenderrollen zugewiesen sind Major Security Incident Entsprechend.	Im Folgenden finden Sie die Rollen, die während des gesamten Incident-Lebenszyklus von beteiligt sind Major Security Incident Korrekturprozess:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	• MSI-Administrator [sn_msi.Workspace_admin] • MSI-Manager [sn_msi.Workspace_Manager] • MSI-Responder [sn_msi.Workspace_Responder Detaillierte Informationen zu den einzelnen Rollen finden Sie unter Management schwerwiegender Sicherheits-Incidents Rollen.
Überprüfen Sie, ob Sie das Setup erfolgreich durchgeführt haben Microsoft SharePoint v1.0.0-Konfiguration.	Microsoft SharePoint Verwaltet Sites, Ordner, Dateien, Gruppen und Anwender in Microsoft SharePoint. Hinzufügen Microsoft SharePoint Daten an Ihren ServiceNow® Instanz. Dazu müssen Sie Graph- und Rest-Verbindungen einrichten. Informationen finden Sie unter Microsoft SharePoint-Spoke v1.1.2 Dokumentation zum Einrichten der Konfiguration VON REST- und Graph-Verbindungen. Stellen Sie eine Graph- und REST-Verbindung her, um eine Verbindung mit herzustellen ServiceNow® Instanz von Microsoft SharePoint.
Überprüfen Sie, ob Sie einen erstellt haben Microsoft SharePoint Site zum Erstellen einer Dokumentbibliothek.	Erstellen Sie einen Microsoft SharePoint Website, falls erforderlich, oder Sie können eine vorhandene Website verwenden, um unsere Dokumentbibliothek zu erstellen.
Stellen Sie sicher, dass Sie eine Dokumentbibliothek unter erstellt haben Microsoft SharePoint Website.	Erstellen Sie eine dedizierte Dokumentbibliothek unter einer neuen oder vorhandenen Microsoft SharePoint Website.
Überprüfen Sie, ob den Anwendern die erforderlichen Berechtigungen bereitgestellt und den erforderlichen Anwendergruppen in zugewiesen werden Microsoft SharePoint.	Verwalten Sie den Zugriff von Microsoft SharePoint Site für verschiedene Anwender und Anwendergruppen.
Überprüfen Sie, ob Sie erstellt und konfiguriert haben Microsoft SharePoint Laufwerk und erforderliche Konfigurationseinstellungen.	Richten Sie ein, um die Laufwerkskonfigurationen zu überprüfen Microsoft SharePoint Datei-Explorer-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	Connector, Ordner- und Dateiaktionen und Ordnervorlagen: • Konfigurieren Sie Den Datei-Explorer Repository Laufwerk: Verbindung aus erstellen Microsoft SharePoint Bis ServiceNow® Instanz. • Konfigurieren Sie Ordner- und Dateiaktionseinstellungen: Konfigurieren und steuern Sie die einzelnen Ordner- und Dateiaktionen, die in der Datei-Explorer-Komponente angezeigt werden. • Erstellen Sie Ordnervorlagen: Konfigurieren Sie diese Option, um eindeutige Ordner für verschiedene Typen schwerwiegender Security Incidents zu erstellen.
Überprüfen Sie, ob Sie erfolgreich eine Verbindung zur Microsoft Teams Chat Connector-Anwendung hergestellt haben.	Dient zum Herstellen einer Verbindung der Microsoft Teams Chat Connector-Anwendung mit ServiceNow® Führen Sie das hier erläuterte Verfahren aus: Stellen Sie eine ms Teams Graph-Verbindung auf her ServiceNow AI Platform.
Überprüfen Sie, ob Sie Microsoft Teams mit konfiguriert haben ServiceNow AI Platform®Instanzen und erstellte Verbindungen und Anmeldeinformationskonfigurationen.	Zur Verifizierung Microsoft Teams Konfiguration mit ServiceNow® Führen Sie das hier erläuterte Verfahren aus: • Stellen Sie eine ms Teams Graph-Verbindung auf her ServiceNow AI Platform • Erstellen Sie eine Chat-Kanalvorlage
Überprüfen Sie, ob die Einstellungen für Administration schwerwiegender Security Incidents – Konfiguration erfolgreich sind.	Als MSI-Administrator müssen Sie Folgendes können: • Bestimmen Sie, ob Sicherheitsanalysten den Incident vorschlagen und heraufstufen und andere Security Incidents verknüpfen können. • Aktivieren oder deaktivieren Sie die Benachrichtigungen, wenn ein Incident vorgeschlagen oder heraufgestuft wird. Möglichkeit, Standardvorlagennachrichten zu bearbeiten. • Konfigurieren Sie Sicherheits-Tags, die auf der Schnittstelle von Sicherheitsanalysten angezeigt werden, um die Incidents zu unterscheiden, die als Kandidat für schwerwiegende Security

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	Incidents vorgeschlagen oder zu einem schwerwiegenden Security Incident heraufgestuft wurden.
Überprüfen Sie, ob die Einstellungen für Administration schwerwiegender Security Incidents – Benachrichtigungen erfolgreich sind.	Lösen Sie als MSI-Administrator E-Mail-Benachrichtigungen aus, wenn ein Security Incident vorgeschlagen wird, und werden an alle Anwender und Gruppen gesendet, die für die Benachrichtigungsliste konfiguriert sind. Weitere Informationen finden Sie unter Legen Sie Benachrichtigungseinstellungen für fest MSIM.

Management schwerwiegender Sicherheits-Incidents Rollen

Weisen Sie Rollen zu, um sicherzustellen, dass Anwender alle erforderlichen Aktionen in der MSIM-Anwendung ausführen können.

Rollen für Management schwerwiegender Incidents

Rollentyp	Rolle	Beschreibung
MSI-Administrator	sn_msi.Workspace_admin	Kann ich installieren und konfigurieren Management schwerwiegender Incidents Und richten Sie die abhängigen Anwendungen wie ein File Explorer(FE), Microsoft Teams- und Chatkanalkonfiguration, Arbeitsbereich-Setup und MSI-Administration: Setup von Konfigurationen und Benachrichtigungen. So richten Sie ein: • Datei-Explorer (FE)-Komponente: ◦ Konfigurieren Sie das Datei-Repository. ◦ Konfigurieren Sie Datei- und Ordneraktionen, die in der Datei-Explorer-Komponente der Registerkarte Zusammenarbeit im Arbeitsbereich „Management schwerwiegender Security Incidents“ bereitgestellt werden. ◦ Erstellen Sie die Stammordner und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen für Management schwerwiegender Incidents (Fortsetzung)

Rollentyp	Rolle	Beschreibung
		Unterordner, und gewähren Sie Zugriff auf die Unterordner. • Chat-Kanalverwaltung ○ Aktivieren und konfigurieren Microsoft Teams Durch Validierung Microsoft Teams Verbindung. ○ Erstellen Sie Chatteams und Chatkanäle, fügen Sie Anwender hinzu, und weisen Sie Anwender den verschiedenen Anwendergruppen zu. • MSI-Administration: ○ Konfigurationen: Konfigurieren Sie die Aktionen von Sicherheitsanalysten, Benachrichtigungen, die gesendet werden, wenn Incidents vorgeschlagen und heraufgestuft werden, und zeigen Sie Tags für die Security Incidents an. ○ Benachrichtigungen: Automatisieren Sie den E-Mail-Benachrichtigungsprozess und Anwenderbenachrichtigungen, wenn ein Security Incident entweder vorgeschlagen oder als schwerwiegender Security Incident heraufgestuft wird.
MSI-Manager	sn_msi.Workspace_Manager	• Zeigen Sie den Zugriff auf die Konfigurationseinstellungsseite für das Management schwerwiegender Security Incidents an. Darf keine der Konfigurationseinstellungen ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollen für Management schwerwiegender Incidents (Fortsetzung)

Rollentyp	Rolle	Beschreibung
		• Zeigen Sie Incident-Datensatzdaten in an, und bearbeiten Sie sie **Details** , **Zusammenarbeit** , Und **Aufgabenorganisator** Registerkarten von Management schwerwiegender Incidents Arbeitsbereich. • Heben Sie den Security Incident zu einem schwerwiegenden Security Incident hoch. • Konfigurieren Sie Datei- und Ordneraktionen, die in der Datei-Explorer-Komponente auf der verfügbar sind **Zusammenarbeit** Registerkarte von Management schwerwiegender Incidents Arbeitsbereich. • Verknüpfen und Aufheben der Verknüpfung zusätzlicher Datensätze mit schwerwiegenden Security Incidents über den Arbeitsbereich.
MSI-Beantworter	sn_msi.Workspace_Responder	• Optionale Rolle zum Anzeigen, Bearbeiten und Beantworten schwerwiegender Security Incidents in **Details** und **Aufgaben** Registerkarten von Management schwerwiegender Incidents Arbeitsbereich. • Verknüpfen und Aufheben der Verknüpfung zusätzlicher Datensätze mit schwerwiegenden Security Incidents über den Arbeitsbereich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration Management schwerwiegender Sicherheits-Incidents

Erweitern Sie die Fähigkeiten von Management schwerwiegender Sicherheits-Incidents Und stellen Sie eine Verbindung mit her ServiceNow AI Platform Instanz durch Integration mit Microsoft Anwendungen.

Wichtig:
Ein Update-Satz (KB1289784) Ist im Schnellstartleitfaden für das Management schwerwiegender Security Incidents verfügbar, um Anwendern eine einfache Konfigurationseinrichtung zu erleichtern. Sie müssen den Update-Satz importieren, nachdem Sie die Anwendungsinstallation abgeschlossen haben. Befolgen Sie das Verfahren, das in der Schnellstartanleitung (Schritt 2) im Abschnitt „Begleitdokumente“ in der MSIM-Anwendung beschrieben ist, die sich im ServiceNow Store befindet.

Management schwerwiegender Sicherheits-Incidents mit Microsoft SharePoint integrieren

Integrieren Sie Ihr Microsoft SharePoint Mit Management schwerwiegender Sicherheits-Incidents.

Registrieren Sie eine neue Anwendung im Azure-Portal für SharePoint-Verbindungen

Registrieren Sie eine neue Anwendung im Azure-Portal für Microsoft SharePoint Integration.

Vorbereitungen
Erforderliche Rolle: administrator, Azure-Administrator

Prozedur

1. Melden Sie sich bei an Microsoft Azure Portal, das Ihren Microsoft-Account als Azure-Administrator verwendet.
2. Navigieren zu **Azure-Services** > **Anwendungsregistrierung** > **Neue Registrierung**an.

   Hinweis:
   Wenn Sie nicht finden, navigieren Sie zu **Azure-Services** Und suchen Sie nach **App-Registrierung** .

3. Geben Sie den Namen der Anwendung ein.
   Beispiel: Microsoft SharePoint Diagramm.
4. Wählen Sie Aus **Unterstützte Account-Typen: Nur Accounts in diesem Organisationsverzeichnis (nur Service Now – einzelner Mandant**).
5. Wählen Sie Aus **Web** Geben Sie aus der Dropdown-Liste unter dem Feld Umleitungs-URI (optional) ein.
6. Geben Sie Ein ServiceNow AI Platform® Instanzumleitungs-URL im Feld zulässige Umleitungs-URL.
   Beispiel: `https://<InstanceName>.service-now.com/oauth_redirect.do` .
7. Klicken Sie auf **Registrieren** Und stellen Sie sicher, dass die Seite mit angezeigt wird **Übersicht** Abschnitt.
8. Notieren Sie sich das Client-ID Und Mandanten-ID Von **Essentials** Abschnitt der Übersichtsseite.
9. Unter **API-Berechtigungen** , Fügen Sie die Microsoft Graph-Berechtigung hinzu:
   a. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
   b. Wählen Sie **Microsoft Graph** aus.
   c. Wählen Sie Aus **Anwendungsberechtigungen** .
   d. Von **Sites** Liste, wählen Sie aus **Sites.Ausgewählt** Berechtigung.
   e. Klicken Sie auf **Berechtigungen hinzufügen**.
10. Unter **API-Berechtigungen** , Fügen Sie die SharePoint-Berechtigung hinzu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.

b. Wählen Sie Aus **SharePoint** .

c. Wählen Sie Aus **Anwendungsberechtigungen** .

d. Von **Sites** Liste auswählen **Sites.Ausgewählt** Berechtigung.

e. Klicken Sie auf **Berechtigungen hinzufügen**.

11. Klicken Sie nach dem Hinzufügen der Berechtigungen auf **Erteilen Sie die Zustimmung des Administrators** .
Alle Berechtigungen sind jetzt vom Administrator genehmigt.

Verwenden Sie Zertifikate für die Authentifizierung

Fordern Sie ein Zugriffstoken mit Zertifikatanmeldeinformationen an.

Vorbereitungen

1. Sie können entweder ein selbst signiertes Zertifikat oder ein VON DER CA ausgestelltes Zertifikat verwenden. Sie können ein selbst signiertes Zertifikat erstellen, indem Sie das PowerShell-Skript wie in beschrieben ausführen Einrichten einer Azure AD-App für den nur-App-Zugriff . Das Skript generiert zwei Dateien: .PFX-Datei und .CER-Datei.

   Hinweis:
   Stellen Sie sicher, dass Sie das Passwort kennen, das zum Verschlüsseln des privaten Schlüssels verwendet wird, um die PFX-Datei und die CER-Datei zu generieren.

2. Verwenden Sie die PFX-Datei, um eine Java Key Store-Datei (JKS) zu erstellen.

   Hinweis:
   Stellen Sie sicher, dass Sie das Passwort kennen, das zum Generieren der JKS-Datei aus der PFX-Datei verwendet wird.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie zu **App-Registrierungen** Im Azure AD-Portal.
2. Klicken Sie Auf **Zertifikate und Geheimnisse** Von **Verwalten** Abschnitt.
3. In **Zertifikate** Klicken Sie auf die Registerkarte **Zertifikat Hochladen** .
4. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Laden Sie ein Zertifikat (öffentlicher Schlüssel) mit einem der folgenden Dateitypen hoch: .Cer, .pem, .crt	.CER-Datei, die Sie mit dem PowerShell-Skript generiert haben.
Beschreibung	Beschreibung des Zertifikats.

5. Klicken Sie auf **Hinzufügen**.
Das Zertifikat wird hochgeladen, und seine Details werden unter angezeigt **Zertifikate** Registerkarte.
6. Kopieren Sie **Fingerabdruck** Wert des hochgeladenen Zertifikats.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die **Fingerabdruck** Wert ist ein hexadezimaler Wert.

7. Codieren Sie **Fingerabdruck** Wert für einen Base64-Wert, und notieren Sie den Wert zur späteren Verwendung.

Hinweis:
Sie können ein Hexadezimal-zu-Base64-Konvertertool (Hex-zu-Base64) verwenden, um zu codieren **Fingerabdruck** Wert für einen Base64-Wert.

Konfigurieren Microsoft SharePoint Mit Management schwerwiegender Sicherheits-Incidents

Einrichten Management schwerwiegender Sicherheits-Incidents Mit Microsoft SharePoint Verbindung.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

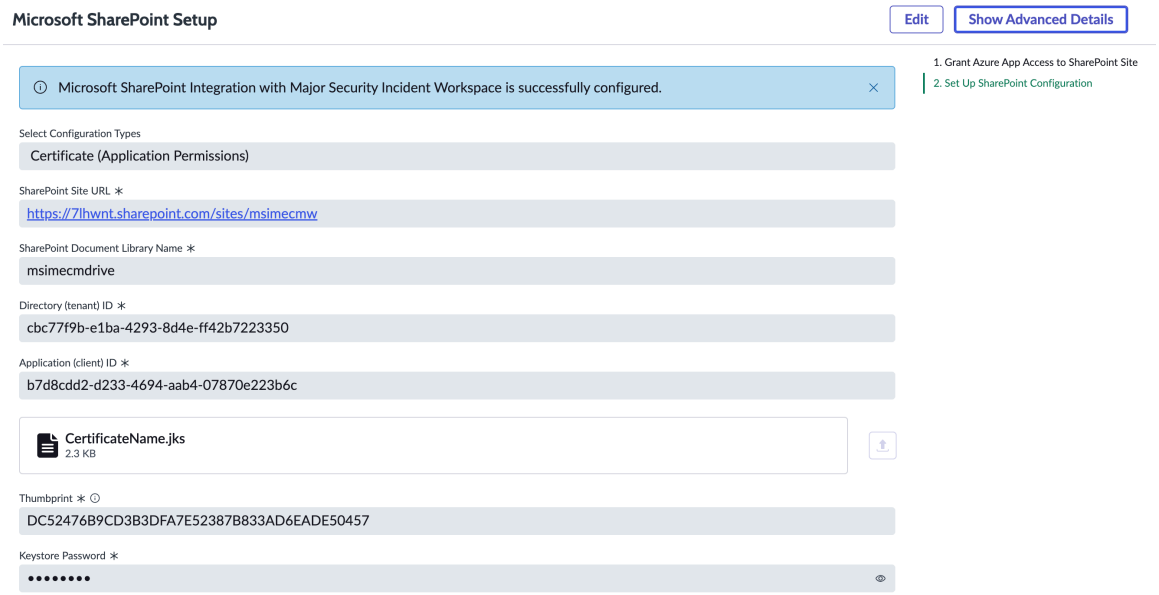
1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Administration**an.
2. Wählen Sie Aus **Dokumentzusammenarbeit** , Und dann **Microsoft SharePoint-Setup** .
3. Wählen Sie Aus **Gewähren Sie Azure App-Zugriff auf die SharePoint-Website** Aus dem Kontextmenü.
4. Gewähren Sie Zugriff auf Ihre registrierte Anwendung mit einer der folgenden Methoden: Curl-Befehle, Azure CLI oder PowerShell.

Hinweis:
- Der Azure-Administrator muss die Zugriffskonfiguration bereitstellen.
- Erteilen Sie der registrierten Anwendung die Berechtigung Sites.FullControl.all.
- Entfernen Sie die Berechtigung Sites.Vollsteuerung.alle, wenn der Zugriff erfolgreich gewährt wurde.

5. Wählen Sie Aus **Richten Sie die SharePoint-Konfiguration ein** Aus dem Kontextmenü.
6. Wählen Sie einen Konfigurationstyp in aus **Wählen Sie Konfigurationstypen Aus** , Und konfigurieren Sie Folgendes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zertifikat (Anwendungsberechtigungen)



SharePoint-Einstellungen für Zertifikat

Feld	Beschreibung
URL der SharePoint-Website	Die Microsoft SharePoint Website-URL.
Name der SharePoint-Dokumentbibliothek	Name des Microsoft SharePoint Dokumentbibliothek.
Verzeichnis-ID (Mandant)	Der eindeutige Bezeichner Ihrer Azure Active Directory-Instanz.
Anwendungs-ID (Client)	Der eindeutige Bezeichner Ihrer in Azure registrierten Anwendung.
Zertifikat hochladen	Die Zertifikatdatei für die Authentifizierung.
Fingerabdruck	Der Fingerabdruck für das Zertifikat.
Schlüsselspeicher-Passwort	Das Schlüsselspeicher-Passwort für den Zugriff auf den Fingerabdruck des Zertifikats.

- Geheimer Client-Schlüssel (Anwendungsberechtigungen)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SharePoint-Einstellungen für geheimes Client

Feld	Beschreibung
URL der SharePoint-Website	Die Microsoft SharePoint Website-URL.
Name der SharePoint-Dokumentbibliothek	Name des Microsoft SharePoint Dokumentbibliothek.
Verzeichnis-ID (Mandant)	Der eindeutige Bezeichner Ihrer Azure Active Directory-Instanz.
Anwendungs-ID (Client)	Der eindeutige Bezeichner Ihrer in Azure registrierten Anwendung.
Geheimer Clientschlüssel	Die geheime Zeichenfolge der Anwendung, die zum anfordern eines Tokens verwendet wird.

7. Wählen Sie Aus **OAuth-Token konfigurieren und abrufen** .
   Eine Anmeldeaufforderung mit Details zu Ihrem Microsoft-Account wird angezeigt.
8. Geben Sie Ihre Microsoft-Account-Details an, und melden Sie sich an.
   Eine erfolgreiche Meldung wird angezeigt, und die Verbindung wird hergestellt.

Management schwerwiegender Sicherheits-Incidents mit Microsoft Teams integrieren

Integrieren Sie Ihr Microsoft Teams Mit Management schwerwiegender Sicherheits-Incidents.

- Registrieren Sie eine neue Anwendung im Azure-Portal für Microsoft Teams Verbindungen
- Konfigurieren Microsoft Teams Verbindung mit herstellen Management schwerwiegender Sicherheits-Incidents

Registrieren Sie eine neue Anwendung im Azure-Portal für Microsoft Teams Verbindungen

Registrieren Sie eine neue Anwendung im Azure-Portal für Microsoft Teams Integration und Zugriff auf die Azure-App gewähren.

Vorbereitungen

Hinweis:
Wenn Sie möchten, können Sie dieselbe Anwendung verwenden, die Sie für SharePoint erstellt haben, um die Microsoft Teams Graph-Verbindung herzustellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: administrator, Azure-Administrator

Prozedur

1. Melden Sie sich mit Ihrem Microsoft-Account beim Azure-Portal an.
2. Navigieren zu **Azure-Services** > **Anwendungsregistrierung** > **Neue Registrierung**an.
3. Geben Sie den Namen der Anwendung ein.
   Beispiel: Microsoft Teams Graph.
4. Wählen Sie Aus **Unterstützter Account-Typ: Accounts nur in diesem Organisationsverzeichnis (nur Service Now – einzelner Mandant)** .
5. Wählen Sie Aus **Web** Geben Sie aus der Dropdown-Liste unter der Umleitungs-URL ein.
6. Geben Sie Ein ServiceNow AI Platform® Instanzumleitungs-URL im Feld zulässige Umleitungs-URL.
   Beispiel: https://<<InstanceName>>.service-now.com/oauth_redirect.do
7. Klicken Sie auf **Registrieren** Und stellen Sie sicher, dass die Seite mit angezeigt wird **Übersicht** Abschnitt.
8. Notieren Sie sich das Client-ID Und Mandanten-ID Von **Essentials** Abschnitt in **Übersicht** Seite.
9. Sie können entweder Schritt 6,1 oder Schritt 6,2 ausführen, um das Verfahren zum Herstellen einer Verbindung mit abzuschließen ServiceNow Instanz.

Konfigurieren Microsoft Teams Verbindung mit herstellen Management schwerwiegender Sicherheits-Incidents

Einrichten Management schwerwiegender Sicherheits-Incidents Mit Microsoft Teams Verbindung.

Vorbereitungen

Voraussetzung: Stellen Sie sicher, dass Sie eine Anwendung in Azure Active Directory mit den erforderlichen Delegierungsberechtigungen registriert haben.

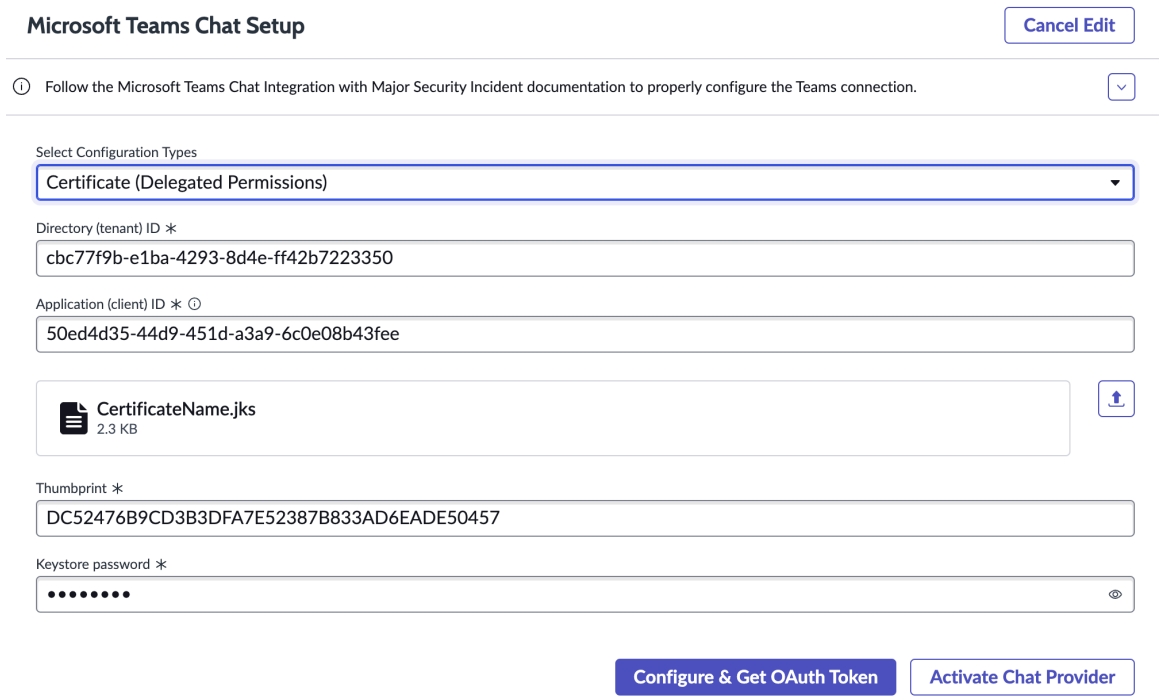
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Administration**an.
2. Wählen Sie Aus **Chat-Zusammenarbeit** , Und dann **Microsoft Teams-Setup** .
3. Wählen Sie im einen Konfigurationstyp aus **Wählen Sie Konfigurationstypen Aus** Und konfigurieren Sie Folgendes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zertifikat (Delegierte Berechtigungen)



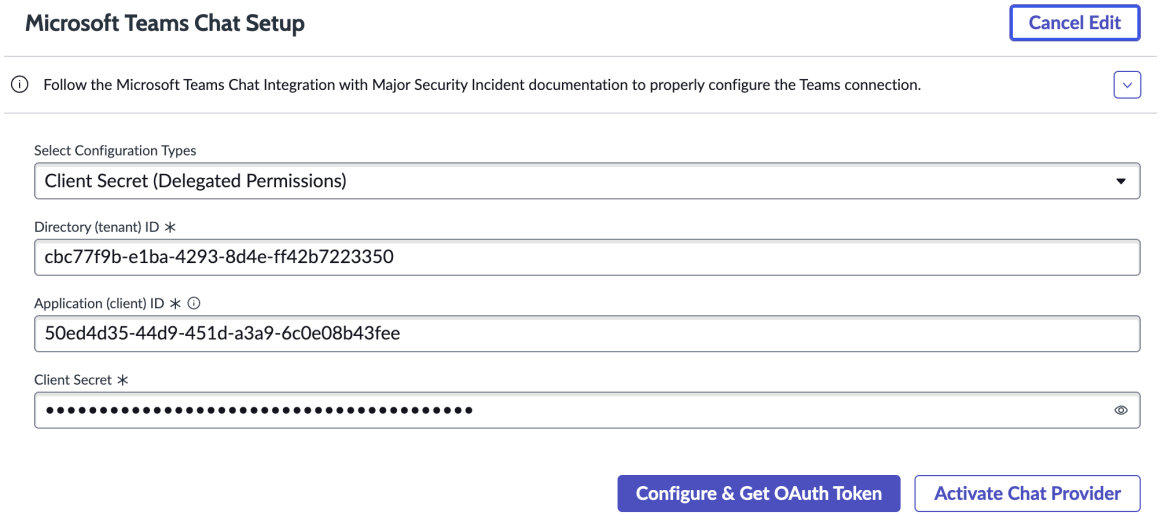
Microsoft Teams-Einstellungen für Zertifikat

Feld	Beschreibung
Verzeichnis-ID (Mandant)	Der eindeutige Bezeichner Ihrer Azure Active Directory-Instanz.
Anwendungs-ID (Client)	Der eindeutige Bezeichner Ihrer in Azure registrierten Anwendung.
Zertifikat hochladen	Die Zertifikatdatei für die Authentifizierung.
Fingerabdruck	Der Fingerabdruck für das Zertifikat.
Schlüsselspeicher-Passwort	Das Schlüsselspeicher-Passwort für den Zugriff auf den Fingerabdruck des Zertifikats.

- Geheimer Client-Schlüssel (Delegierte Berechtigungen)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Microsoft Teams-Einstellungen für geheimes Client

Feld	Beschreibung
Verzeichnis-ID (Mandant)	Der eindeutige Bezeichner Ihrer Azure Active Directory-Instanz.
Anwendungs-ID (Client)	Der eindeutige Bezeichner Ihrer in Azure registrierten Anwendung.
Geheimer Clientschlüssel	Die geheime Zeichenfolge der Anwendung, die zum anfordern eines Tokens verwendet wird.

4. Wählen Sie Aus **OAuth-Token konfigurieren und abrufen** .
   Eine Anmeldeaufforderung mit Details zu Ihrem Microsoft-Account wird angezeigt.
5. Geben Sie Ihre Microsoft-Account-Details an, und melden Sie sich an.
   Eine erfolgreiche Meldung wird angezeigt, und die Verbindung wird hergestellt.
6. Wählen Sie Aus **Aktivieren Sie Den Chatanbieter** Zum Aktivieren Microsoft Teams Verbindung.
7. **Wahlweise:** Wählen Sie Aus **Erweiterte Details Anzeigen** Zum Anzeigen der Konfigurationsdetails.

Stellen Sie eine ms Teams Graph-Verbindung auf her ServiceNow AI Platform

Integrieren ServiceNow AI Platform Instanz und Microsoft Teams Account durch Einrichtung eines Microsoft Teams Graph Verbindung.

Vorbereitungen

Wenn Sie möchten, können Sie dieselbe Anwendung verwenden, die Sie für SharePoint erstellt haben, um die Microsoft Teams Graph-Verbindung herzustellen.

Erforderliche Rolle: administrator, Azure-Administrator

Registrieren Sie eine neue Anwendung in Azure for Microsoft Teams Graph Connection

Prozedur

1. Melden Sie sich bei an Azure Portal mit Ihrem Microsoft Account.
2. Navigieren zu **Azure-Services** > **Anwendungsregistrierung** > **Neue Registrierung**an.
3. Geben Sie den Namen der Anwendung ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Microsoft Teams Graph.

4. Wählen Sie den entsprechenden aus **Unterstützte Account-Typen** Option, die für Ihre Organisation gilt. Wählen Sie beispielsweise aus **Accounts nur in diesem Organisationsverzeichnis (nur Service Now – einzelner Mandant)** Option.

   Hinweis:
   Informationen zu unterstützten Account-Typen finden Sie unter Registrieren Sie eine Anwendung bei der Microsoft Identity Platform .

5. Wählen Sie Aus **Web** Geben Sie aus der Dropdown-Liste unter der Umleitungs-URL ein.
6. Geben Sie Ein ServiceNow AI Platform Instanzumleitungs-URL im Feld zulässige Umleitungs-URL. Beispiel: Https://<<InstanceName>>.service-now.com/oauth_redirect.do
7. Klicken Sie Auf **Registrieren** Um Ihre neue Anwendung zu registrieren und sicherzustellen, dass die Seite mit angezeigt wird **Übersicht** Abschnitt.

Verwenden von Zertifikaten für die Authentifizierung

Fordern Sie ein Zugriffstoken mit Zertifikatanmeldeinformationen an.

Vorbereitungen

1. Sie können entweder ein selbst signiertes Zertifikat oder ein VON DER CA ausgestelltes Zertifikat verwenden. Sie können ein selbst signiertes Zertifikat erstellen, indem Sie das PowerShell-Skript wie in beschrieben ausführen Einrichten einer Azure AD-App für den nur-App-Zugriff . Das Skript generiert zwei Dateien: .PFX-Datei und .CER-Datei.

   Hinweis:
   Stellen Sie sicher, dass Sie das Passwort kennen, das zum Verschlüsseln des privaten Schlüssels verwendet wird, um die PFX-Datei und die CER-Datei zu generieren.

2. Verwenden Sie die PFX-Datei, um eine Java Key Store-Datei (JKS) zu erstellen.

   Hinweis:
   Stellen Sie sicher, dass Sie das Passwort kennen, das zum Generieren der JKS-Datei aus der PFX-Datei verwendet wird.

Erforderliche Rolle: Administrator

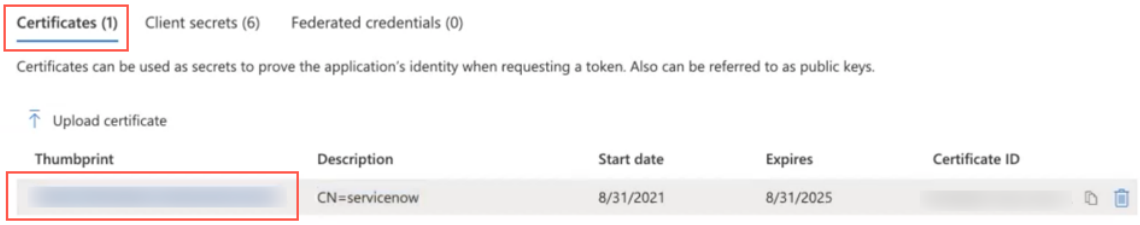
Prozedur

1. Navigieren Sie zu **App-Registrierungen** Im Azure AD-Portal.
2. Klicken Sie Auf **Zertifikate und Geheimnisse** Von **Verwalten** Abschnitt.
3. In **Zertifikate** Klicken Sie auf die Registerkarte **Zertifikat Hochladen** .
4. Füllen Sie diese Werte im Formular aus.

Feld	Beschreibung
Laden Sie ein Zertifikat (öffentlicher Schlüssel) mit einem der folgenden Dateitypen hoch: .Cer, .pem, .crt	.CER-Datei, die Sie mit dem PowerShell-Skript generiert haben.
Beschreibung	Beschreibung des Zertifikats.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Hinzufügen**.
   Das Zertifikat wird hochgeladen, und seine Details werden unter angezeigt **Zertifikate** Registerkarte.
6. Kopieren Sie **Fingerabdruck** Wert des hochgeladenen Zertifikats.
   Die **Fingerabdruck** Wert ist ein hexadezimaler Wert.



7. Codieren Sie **Fingerabdruck** Wert für einen Base64-Wert, und notieren Sie den Wert zur späteren Verwendung.

Hinweis:
Sie können ein Hexadezimal-zu-Base64-Konvertertool (Hex-zu-Base64) verwenden, um zu codieren **Fingerabdruck** Wert für einen Base64-Wert.

Hängen Sie ein Java Key Store-Zertifikat für MS Teams an

Aktivieren Sie die JWT-Bearer-Token-Authentifizierung, indem Sie ein gültiges Java Key Store (JKS)-Zertifikat anhängen.

Vorbereitungen

Melden Sie sich bei Ihrer ServiceNow-Instanz an, um das folgende Verfahren auszuführen.

- Gültiges Java Key Store-Zertifikat
- Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Systemdefinition** > **Zertifikate**an.
2. Öffnen Sie den Datensatz **Microsoft Teams Connector-Zertifikat** .
   Stellen Sie sicher, dass Sie den Standarddatensatz verwenden **Microsoft Teams Connector-Zertifikat** Nur.
3. Geben Sie das Passwort ein, das der JKS-Datei in zugeordnet ist **Schlüsselspeicher-Passwort** .
4. Klicken Sie auf das Anhangssymbol ( ) Und hängen Sie das von Ihnen generierte JKS-Zertifikat an.
   Weitere Informationen finden Sie unter .
5. Klicken Sie Auf **Validiert Speicher/Zertifikate** .
6. Klicken Sie auf **Aktualisieren**.

Konfigurieren Sie den JWT-Signaturschlüssel für MS Teams

Erstellen Sie einen JSON Web Token (JWT)-Signaturschlüssel, der Ihrem Java Key Store-Zertifikat zugewiesen werden soll.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **System-OAuth** > **JWT-Schlüssel**an.
2. Öffnen Sie den Datensatz **Microsoft Teams Connector JWT** .
3. Geben Sie das Passwort ein, das zum Verschlüsseln des privaten Schlüssels verwendet wird, um die PFX-Datei und die CER-Datei in zu generieren **Signaturschlüsselpasswort** .
4. Klicken Sie auf **Aktualisieren**.

Konfigurieren Sie den JWT-Provider für MS Teams

Fügen Sie Ihrer ServiceNow-Instanz einen JSON-Webtoken-Anbieter (JWT) hinzu.

Vorbereitungen

- Kopieren Sie den Wert von , und zeichnen Sie ihn auf **Anwendungs-ID (Client)** Und **Verzeichnis-ID (Mandant)** Der Anwendung, die Sie im Azure-Portal registriert hatten.

- Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **System-OAuth** > **JWT-Anbieter**an.
2. Öffnen Sie den Datensatz **Ms Teams-Connector-JWT-Provider** .
3. Geben Sie Werte für ein **iss** , **Untergeordnet** , Und **aud** In der zugehörigen Liste „Standardansprüche“.

Feld	Wert
aud	Microsoft Online-URL in diesem Format: `https://login.microsoftonline.com/<tenant-id>/oauth2/Token` . Ersetzen `<tenant-id>` Mit **Verzeichnis-ID (Mandant)** Wert Ihrer Anwendung wurde im Azure-Portal registriert.
iss	**Anwendungs-ID (Client)** Der Anwendung, die Sie im Azure-Portal registriert hatten.
Untergeordnet	**Anwendungs-ID (Client)** Der Anwendung, die Sie im Azure-Portal registriert hatten.

4. Klicken Sie auf **Aktualisieren**.

Stellen Sie eine Verbindung mithilfe von Zertifikaten her

Stellen Sie mithilfe von Zertifikaten eine Verbindung zwischen der neu erstellten Microsoft Teams Graph-Anwendung her.

Vorbereitungen

Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse Für Verbindungen Und Anmeldeinformationen**an.
2. Öffnen **Microsoft Teams-Spoke** .
3. Ändern Sie den Feldwert **Konfigurationsvorlage: MSIM Microsoft Teams ConnectorAutorisierungscodevorlage** Und speichern Sie das Formular.

   Hinweis:
   Diese Vorlage enthält die delegierte API-Berechtigung, die für die MSTeams-Integration erforderlich ist.

4. Klicken Sie im Abschnitt zugehörige Links auf Erstellen **Neue Verbindung Und Anmeldeinformationen** .
5. Klicken Sie Auf **OAuth-Token erstellen und abrufen** .
   Eine Fehlermeldung mit der Aufforderung „401 – nicht autorisiert“ wird angezeigt.
6. Laden Sie das Formular neu, und öffnen Sie den Datensatz in der zugehörigen Liste „Verbindungen“.
7. Geben Sie die Base64-codierte ein **Fingerabdruck** Wert in **Codierter Fingerabdruck Des Zertifikats** Attribut in **Attribute** Abschnitt.

   Hinweis:
   Der Fingerabdruckwert ist ein Hexadezimalwert. Sie können ein hexadezimales Konvertierungstool zu Base64 (Hex zu Base64) verwenden, um den Thumbprint-Wert in einen Base64-Wert zu codieren.

8. Navigieren zu **System-OAuth** > **Applikationsregistrierung**
9. Öffnen **Autorisierungscode für MSIM Microsoft Teams Connector** Datensatz.
10. Ändern Sie das OAuth-API-Skript: **OAuthUtilJWTMSTeamsConnector** .
11. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**an.
12. Öffnen Sie den Datensatz **MSIM Microsoft Teams Connector-Anmeldeinformationen** .
13. Klicken Sie unter zugehörige Links auf **OAuth-Token abrufen** .
    Bei Erfolg werden der Azure-Anwendung die folgenden API-Berechtigungen hinzugefügt.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now
openid	Delegated	Sign users in	No	Granted for Service Now
Team.Create	Delegated	Create teams	No	Granted for Service Now
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geheimer Client-Wert wird verwendet

Verwenden Sie den geheimen Clientwert, um den Registrierungsdatensatz der Graph-Anwendung zu konfigurieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie zu **App-Registrierungen** Im Azure AD-Portal.
2. Klicken Sie Auf **Zertifikate und Geheimnisse** Von **Verwalten** Abschnitt.
3. Klicken Sie auf **New client secret** (Neuer geheimer Clientschlüssel).
4. Kopieren Sie das erstellte geheime Clientgeheimnis, und notieren Sie es **Wert** Feld.

Stellen Sie eine Verbindung mithilfe des geheimen Clientschlüssels her

Stellen Sie eine Verbindung zwischen der neu erstellten Microsoft Teams Graph-Anwendung mit her ServiceNow AI Platform Instanz.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse Für Verbindungen Und Anmeldeinformationen**an.
2. Öffnen **Microsoft Teams-Spoke** .
3. Ändern Sie den Feldwert **Konfigurationsvorlage: MSIM Microsoft Teams ConnectorAutorisierungscodevorlage** Und speichern Sie das Formular.

   Hinweis:
   Diese Vorlage enthält die delegierte API-Berechtigung, die für die MSTeams-Integration erforderlich ist.

4. Klicken Sie im Abschnitt zugehörige Links auf Erstellen **Neue Verbindung Und Anmeldeinformationen** .
5. Klicken Sie Auf **OAuth-Token erstellen und abrufen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei Erfolg werden der Azure-Anwendung die folgenden API-Berechtigungen hinzugefügt.

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (13)				•••
Channel.Create	Delegated	Create channels	Yes	Granted for Service Now •••
Channel.Delete.All	Delegated	Delete channels	Yes	Granted for Service Now •••
Channel.ReadBasic.All	Delegated	Read the names and descriptions of channels	No	Granted for Service Now •••
ChannelMember.ReadWrite.All	Delegated	Add and remove members from channels	Yes	Granted for Service Now •••
ChannelMessage.Read.All	Delegated	Read user channel messages	Yes	Granted for Service Now •••
ChannelSettings.ReadWrite.All	Delegated	Read and write the names, descriptions, and settings of ch...	Yes	Granted for Service Now •••
offline_access	Delegated	Maintain access to data you have given it access to	No	Granted for Service Now •••
openid	Delegated	Sign users in	No	Granted for Service Now •••
Team.Create	Delegated	Create teams	No	Granted for Service Now •••
TeamMember.ReadWrite.All	Delegated	Add and remove members from teams	Yes	Granted for Service Now •••
TeamSettings.ReadWrite.All	Delegated	Read and change teams' settings	Yes	Granted for Service Now •••
User.Read	Delegated	Sign in and read user profile	No	Granted for Service Now •••
User.Read.All	Delegated	Read all users' full profiles	Yes	Granted for Service Now •••

Aktivieren Sie den MS Teams-Chat-Connector für den MS Teams Graph-Spoke-Anwender

Wenn Sie bereits ein Anwender sind, befolgen Sie die in diesem Abschnitt beschriebenen Schritte, um den Microsoft Teams Chat Connector für den MS Teams Graph Spoke-Anwender zu aktivieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

Wenn Sie bereits ein Microsoft Teams Graph-Spoke-Anwender sind, führen Sie die folgenden Schritte aus:

- Navigieren Sie zu Ihrer registrierten Anwendung im Azure-Portal, das von der Microsoft Teams Graph-Spoke verwendet wird.
- Navigieren Sie zu **API-Berechtigungen** Abschnitt zum Konfigurieren der erforderlichen API-Berechtigungen.
- Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
- Wählen Sie **Microsoft Graph** aus.
- Um die Anwendung Microsoft Teams Connector zu verwenden, müssen Sie Ihrer Anwendung über das Azure-Portal zwei weitere delegierte Berechtigungen hinzufügen: „ChannelMember.ReadWrite.all“ und „teammember.ReadWrite.all“.
- Klicken Sie nach dem Hinzufügen der oben erforderlichen Berechtigungen auf **Erteilen Sie die Zustimmung des Administrators** .

Konfigurieren Sie MS Teams auf *ServiceNow AI Platform***Instanz für einen vorhandenen Anwender:**

- Navigieren Sie zu **Aliasse Für Verbindungen Und Anmeldeinformationen** .
- Wählen Sie Aus **Microsoft Teams-Spoke** Datensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wählen Sie den Anmeldeinformationsdatensatz aus, der der Microsoft Teams-Spoke zugeordnet ist.
- Klicken Sie Auf **OAuth-Token abrufen** . Eine Bestätigungsmeldung zeigt an, dass das OAuth-Aktualisierungstoken verfügbar ist.

Als vorhandener Anwender haben Sie jetzt die Integration der Microsoft Teams Chat Connector-Anwendung mit der Microsoft Teams Graph API abgeschlossen.

Management schwerwiegender Sicherheits-Incidents Telefonkonferenzintegration

Mit Management schwerwiegender Sicherheits-Incidents Integration von Telefonkonferenzen können Sie mit Ihren Kunden und Peer-Mitarbeitern zusammenarbeiten, um Kundenprobleme mithilfe der Video- und Bildschirmfreigabeoptionen in zu lösen Microsoft Teams, Cisco Webex, Oder Zoom Aus der MSIM-Anwendung.

Die Management schwerwiegender Sicherheits-Incidents Mit der Integration von Telefonkonferenzen können Sie den Konferenzkommunikationskanal in integrieren Notify Kommunikationskanal durch Verwalten und Initiieren von Microsoft Teams, Cisco Webex, Oder Zoom Besprechung direkt von Management schwerwiegender Sicherheits-Incidents Anwendung.

Als MSI-Manager können Sie die Integration der MSIM-Telefonkonferenz zum Initiieren verwenden Microsoft Teams, Cisco Webex Oder Zoom Besprechungen. Integrieren Sie Management schwerwiegender Sicherheits-Incidents Telefonkonferenz mit den externen Service Providern als Kommunikationskanal, um sich mit den Stakeholdern zu treffen, um die schwerwiegenden Security Incidents zu lösen.

Schlüsselfunktionen

Die Major Security Incident Die Integration von Management-Telefonkonferenzen bietet die folgenden wichtigen Funktionen:

- MSI-Manager können einen initiieren Microsoft Teams, Cisco Webex, Oder Zoom Telefonkonferenz direkt aus dem schwerwiegenden Security Incident.
- Laden Sie zusätzliche Teilnehmer zum Anruf ein.
- Zeigen Sie Anrufaufzeichnungen und Chat-Details an.
- Sendet Einladungen an Teilnehmer per E-Mail und Microsoft Teams Chat.

Konferenzanruf starten

Starten Sie eine Telefonkonferenz aus einer Aufgabe oder einer wichtigen Sicherheitsaufgabe, indem Sie einen oder mehrere Anwender zur Teilnahme an einer Telefonkonferenz einladen. Die Telefonkonferenz wird nur gestartet, wenn mindestens zwei Teilnehmer beitreten.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

Stellen Sie sicher, dass Sie im Folgendes ausgeführt haben ServiceNow® Instanz:

- Installiert und aktiviert Notify Plugin (com.snc.notify).
- Hat installiert Notify UI-Komponenten für die App „konfigurierbare Arbeitsbereiche“.
- Das Plugin „visuelles Taskboard“ (com.devsnc.snb_vtb) wurde installiert und aktiviert.

Weitere Informationen finden Sie unter IntegrationHub anfordern .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

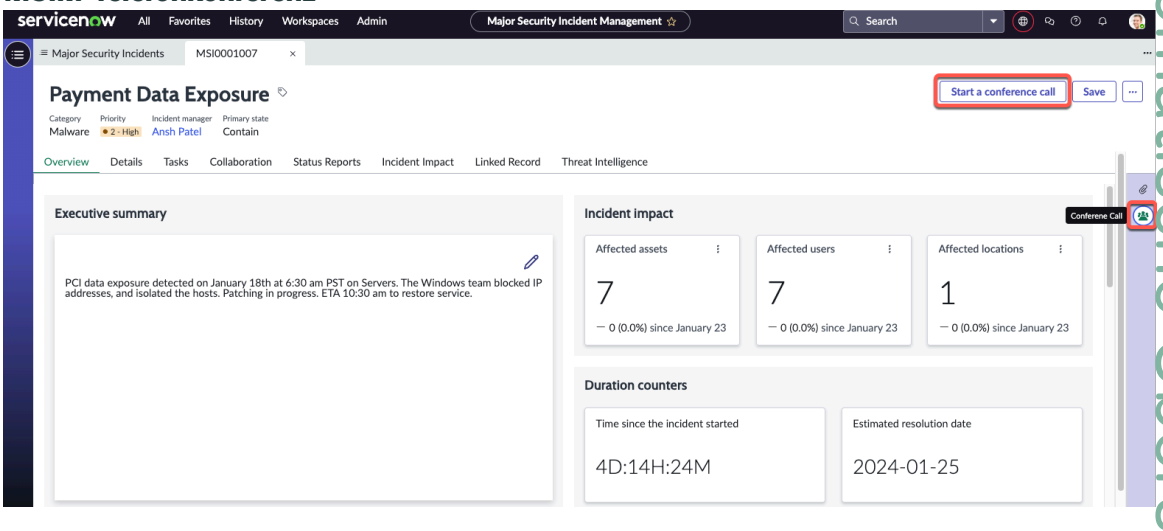
Die Anrufteilnehmer können Folgendes umfassen:

- Anwender, denen bestimmte Verantwortlichkeiten zugewiesen wurden.
- Ad-hoc- oder On-Demand-Kontakte
- Andere Drittparteikontakte

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**an.
2. Wählen Sie in der Liste schwerwiegender Security Incident einen schwerwiegenden Security Incident aus.
3. Wählen Sie aus **Starten Sie eine Telefonkonferenz** Aktion.
4. Sie können auch eine Telefonkonferenz starten, indem Sie auswählen Symbol im rechten Kontextmenü und Auswahl des +-Symbols.
   Das Popup-Fenster „Telefonkonferenz starten“ wird angezeigt.

MSIM-Telefonkonferenz



5. Wählen Sie im Feld Konferenzbrücke eine aus **Konferenzbrücke** Über die Sie eine Verbindung herstellen möchten.
   Zum Beispiel Microsoft Team, Zoom oder Cisco Webex.
6. Geben Sie im Feld Titel einen Titel an, der den Grund für die Telefonkonferenz beschreibt.
7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Telefonkonferenz aus.
   Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen oder die Teilnehmer aus auszuwählen **Empfehlungen** Liste, die Teilnehmerempfehlungen enthält, die der Telefonkonferenz hinzugefügt werden können.

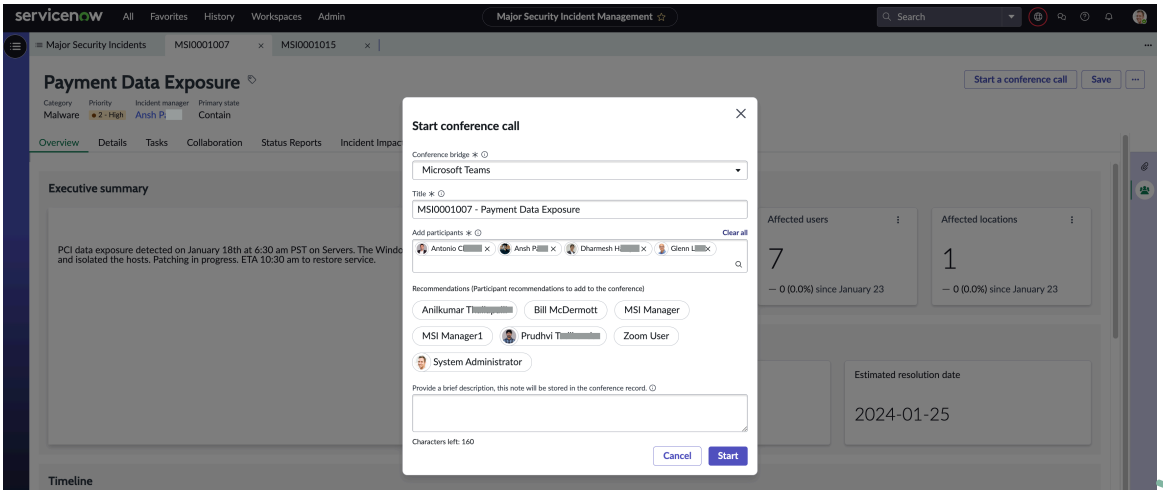
   Der Anwender (Host), der die Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle Anwender, die dem schwerwiegenden Security Incident zugeordnet sind, sind standardmäßig unter verfügbar **Empfehlungen** Liste.

Hinweis:
Stellen Sie sicher, dass die ausgewählten Teilnehmer über eine gültige E-Mail-Adresse verfügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konferenzanruf starten



8. Nachdem Sie die Teilnehmer ausgewählt haben, geben Sie im Feld Beschreibung eine kurze Beschreibung des Grunds für den Beginn der Telefonkonferenz an.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.
9. Nachdem die Teilnehmerliste abgeschlossen ist, wählen Sie aus **Starten** .
   Die Telefonkonferenz beginnt in der ausgewählten Konferenzbrücke. Alle Teilnehmer werden per E-Mail benachrichtigt, und sie werden auch über die entsprechende Konferenzbrücke benachrichtigt, die ausgewählt wurde.
10. Wählen Sie aus **Klicken Sie hier** Option neben dem schwerwiegenden Security Incident, an der Telefonkonferenz teilzunehmen.
    Die Teilnehmer können den Link aus der E-Mail-Benachrichtigung oder die Benachrichtigung aus der ausgewählten Konferenzbrücke verwenden, um an der Telefonkonferenz teilzunehmen.
11. Öffnen Sie den zugehörigen schwerwiegenden Security Incident, um die Telefonkonferenzdetails anzuzeigen. Wenn der endgültige Teilnehmer die Konferenz verlässt, endet die Telefonkonferenz, oder wählen Sie aus **Anruf beenden** Um die Telefonkonferenz zu beenden.

Einer Telefonkonferenz Teilnehmer hinzufügen

Fügen Sie einer Telefonkonferenz mithilfe der Suchoption im Teilnehmer hinzu **Telefonkonferenz starten** Popup zum Suchen und Hinzufügen der erforderlichen Teilnehmer. Sie können Teilnehmer auch hinzufügen, indem Sie die Teilnehmer aus der Empfehlungsliste auswählen, die Teilnehmerempfehlungen enthält, die der Telefonkonferenz hinzugefügt werden können.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

Warum und wann dieser Vorgang ausgeführt wird

Der Anwender (Host), der die Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle Anwender, die dem schwerwiegenden Security Incident zugeordnet sind, sind standardmäßig in der Empfehlungsliste verfügbar.

Die Anrufteilnehmer können Folgendes umfassen:

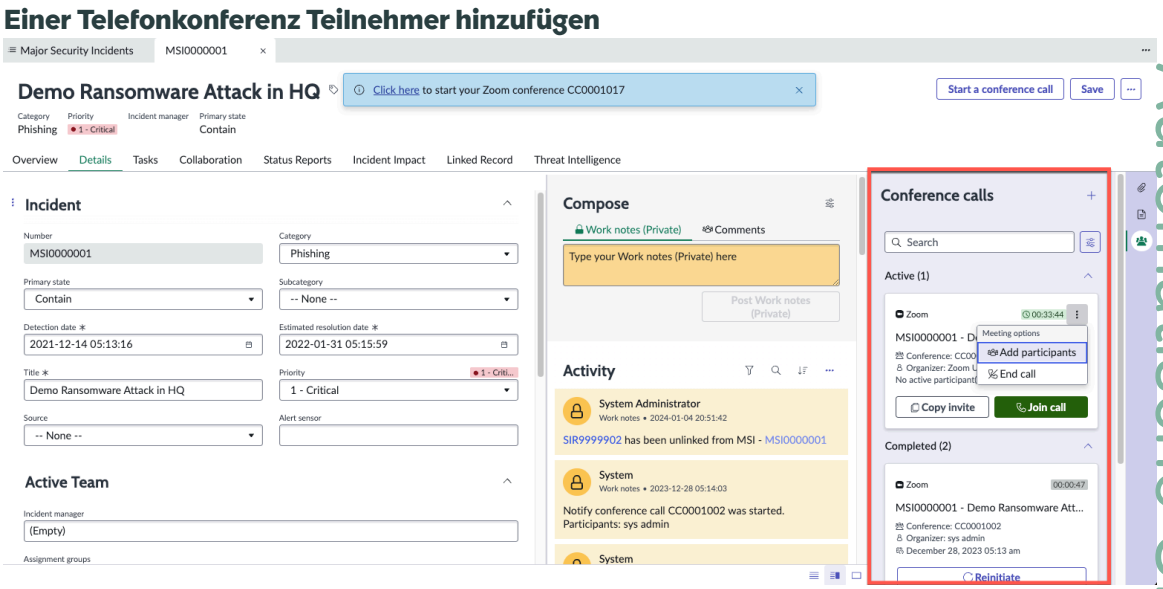
- Anwender, denen bestimmte Verantwortlichkeiten zugewiesen wurden.
- Ad-hoc- oder On-Demand-Kontakte
- Andere Drittparteikontakte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**an.
2. Wählen Sie in der Liste schwerwiegender Security Incident den schwerwiegenden Security Incident aus, den Sie in der Telefonkonferenz lösen möchten.
3. Wählen Sie aus Symbol im rechten Kontextmenü, um die Details der Telefonkonferenzen anzuzeigen. Dies umfasst Details wie Name der Konferenzbrücke, Name des Organisators, Datum, Uhrzeit, Dauer des Anrufs, aktive und inaktive Teilnehmer.
4. Wählen Sie Aus Wählen Sie neben der aktiven Telefonkonferenz die aus **Fügen Sie Teilnehmer Hinzu** Option.



5. Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen oder die Teilnehmer aus auszuwählen **Empfehlungen** Liste, die Teilnehmerempfehlungen enthält, die der Telefonkonferenz hinzugefügt werden können.
6. Nachdem Sie die Teilnehmer ausgewählt haben, geben Sie im Feld Beschreibung eine kurze Beschreibung des Grunds für den Beginn der Telefonkonferenz an.
   Alle Teilnehmer werden per E-Mail benachrichtigt, und sie werden auch über die entsprechende Konferenzbrücke benachrichtigt, die ausgewählt wurde. Die Teilnehmer können den Link aus der E-Mail-Benachrichtigung oder die Benachrichtigung aus der ausgewählten Konferenzbrücke verwenden, um an der Telefonkonferenz teilzunehmen.
7. Alternativ können Sie Teilnehmer hinzufügen, indem Sie auswählen **Kopieren Sie die Einladung** Option im Abschnitt Telefonkonferenzen im rechten Kontextmenü, und Sie können sie für die erforderlichen Teilnehmer freigeben.

Schalten Sie Teilnehmer in einer Telefonkonferenz stummschalten

Als MSI-Manager oder Moderator einer Telefonkonferenz haben Sie die Möglichkeit, einen bestimmten Teilnehmer oder alle Teilnehmer der Telefonkonferenz stummzuschalten.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

Stellen Sie vor Beginn dieses Verfahrens sicher, dass eine aktive Telefonkonferenz mit mindestens einem Teilnehmer vorhanden ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**an.
2. Wählen Sie in der Liste schwerwiegender Security Incident den schwerwiegenden Security Incident aus, den Sie in der Telefonkonferenz lösen möchten.
3. Wählen Sie aus Symbol im rechten Kontextmenü, um die Details der Telefonkonferenzen anzuzeigen.
4. Wählen Sie Aus **Nehmen Sie am Anruf Teil** Auf der aktiven Konferenzbrücke.
5. Wählen Sie nach dem Beitritt zur Telefonkonferenz einen Teilnehmer aus, den Sie stummschalten möchten, und wählen Sie ihn aus **Stummschalten** Auf der Konferenzbrücke.
6. Wählen Sie aus, um alle Teilnehmer der Telefonkonferenz stummzuschalten **Teilnehmer** Wählen Sie in den Besprechungssteuerungen und aus **Alle Stummschalten** .

Telefonkonferenzdetails anzeigen

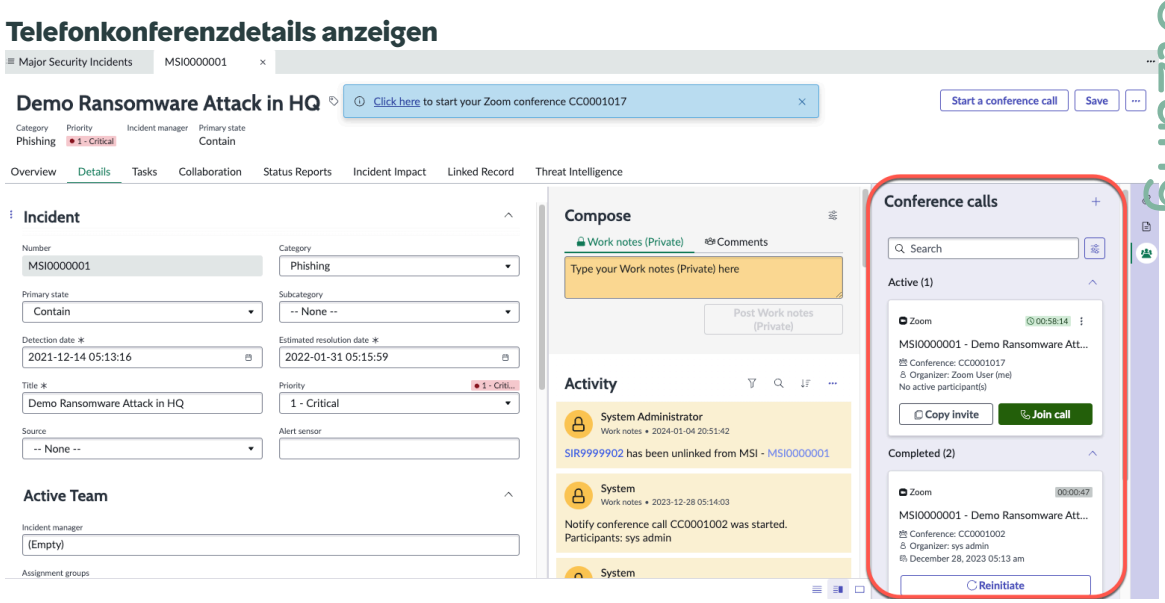
Telefonkonferenzen werden als Systemaktivitäten im Abschnitt „Aktivität“ des schwerwiegenden Security Incidents und auch in der zugehörigen Liste „Telefonkonferenzen“ aufgeführt. Sie können Details wie Name der Konferenzbrücke, Name des Organisators, Datum, Uhrzeit, Dauer des Anrufs, aktive und inaktive Teilnehmer anzeigen.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**an.
2. Wählen Sie in der Liste schwerwiegender Security Incident den schwerwiegenden Security Incident aus, den Sie in der Telefonkonferenz lösen möchten.
3. Wählen Sie aus Symbol im rechten Kontextmenü, um die Details der Telefonkonferenzen anzuzeigen. Dies umfasst Details wie Name der Konferenzbrücke, Name des Organisators, Datum, Uhrzeit, Dauer des Anrufs, aktive und inaktive Teilnehmer.



4. Sie können die Suchoption verwenden, um nach einer bestimmten Telefonkonferenz zu suchen. Es können mehrere Anrufe für denselben schwerwiegenden Security Incident geben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Um Teilnehmer zu einer Telefonkonferenz hinzuzufügen, wählen Sie aus ⋮ Wählen Sie neben der aktiven Telefonkonferenz die aus **Fügen Sie Teilnehmer Hinzu** Option.
6. Sie können auch Teilnehmer hinzufügen, indem Sie verwenden **Kopieren Sie die Einladung** Option und Freigabe des Links für die erforderlichen Teilnehmer.
7. Um an einer Telefonkonferenz teilzunehmen, navigieren Sie zum Abschnitt aktiv, und wählen Sie aus **Nehmen Sie am Anruf Teil** Option der erforderlichen Telefonkonferenz.
8. Um eine Telefonkonferenz zu beenden, wählen Sie aus ⋮ Wählen Sie neben der aktiven Telefonkonferenz die aus **Anruf beenden** Option.
9. Um eine Telefonkonferenz neu zu starten, navigieren Sie zum Abschnitt Abgeschlossen, und wählen Sie aus **Erneut Initiieren** Option der erforderlichen Telefonkonferenz.

Integrieren Sie MSIM-Telefonkonferenzen mit Microsoft Teams

Die Telefonkonferenz Microsoft Teams Mit der Integration können Sie eine verwalten und initiieren Microsoft Teams Telefonkonferenz direkt von einem schwerwiegenden Security Incident.

Schlüsselfunktionen

- Start und Ende Microsoft Teams Telefonkonferenzen direkt von schwerwiegenden Security Incidents oder einer Aufgabe aus der Workbench für schwerwiegende Sicherheit.
- Verwalten Sie einen Microsoft Teams Telefonkonferenz durch Hinzufügen oder Entfernen von Teilnehmern.

Voraussetzungen

Vergewissern Sie sich, dass Sie Folgendes installiert haben IntegrationHub Plugins auf Ihrem ServiceNow Instanz.

- Notify Plugin (com.snc.notify)
- Microsoft Teams Plugin „Communications Spoke“ (sn_msteams_com_spk).
- Plugin „Azure Active Directory-Anwenderzuordnung“ (sn_now_Azure).
- Notify UI-Komponenten für konfigurierbare Arbeitsbereiche

Weitere Informationen finden Sie unter IntegrationHub anfordern .

Konfiguration

- Zum Konfigurieren der MSIM-Telefonkonferenz Microsoft Teams Integration mit der vorkonfigurierten App, siehe Integrate Notify connector pre-published app with Microsoft Teams .
- Zum Konfigurieren der MSIM-Telefonkonferenz Microsoft Teams Integration mit der selbst konfigurierten App, siehe Integrating Notify connector self-configured app with Microsoft Teams .

Verwenden Sie die MSIM-Telefonkonferenz Microsoft Teams Integration

Die folgenden Schritte zeigen Ihnen, wie Sie einen verwalten und initiieren können Microsoft Teams Telefonkonferenz direkt von einem schwerwiegenden Security Incident.

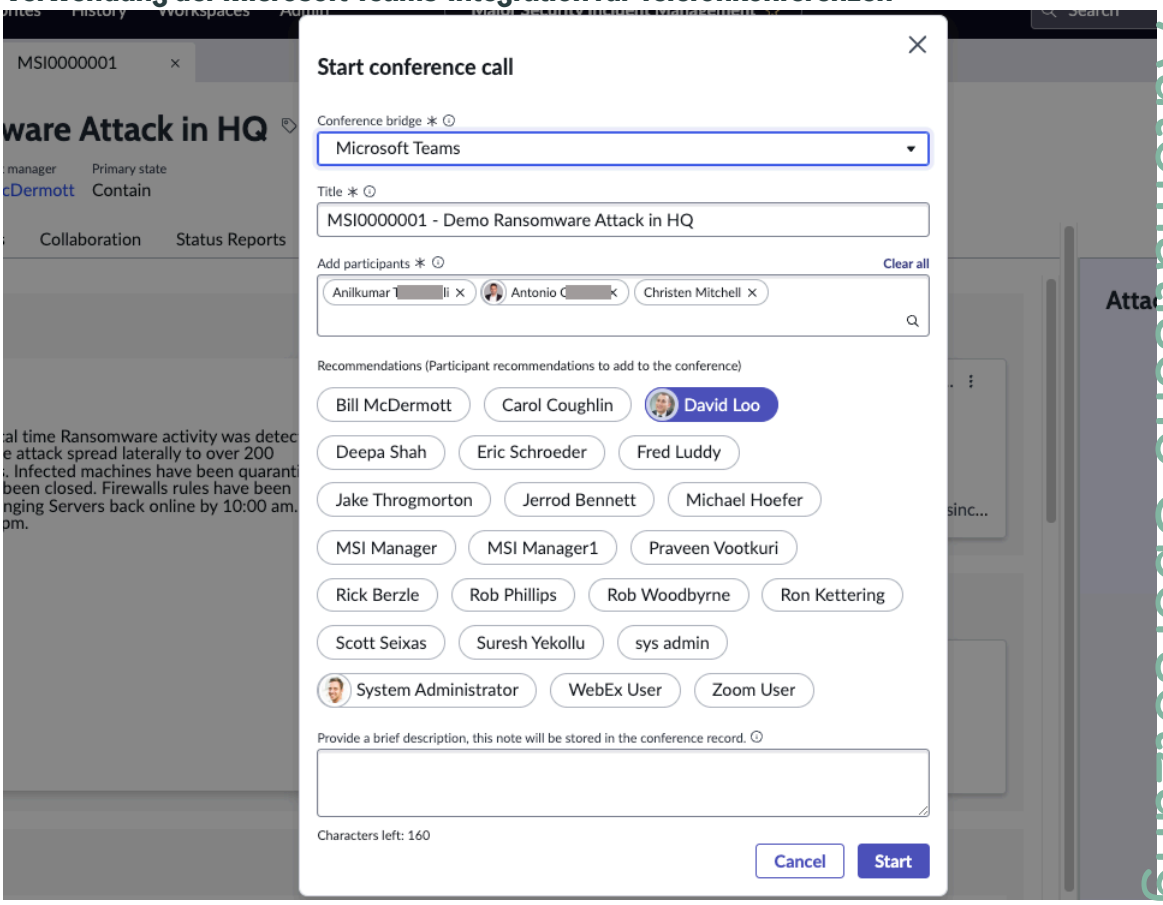
Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_Manager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**an.
2. Wählen Sie in der Liste schwerwiegender Security Incident einen schwerwiegenden Security Incident aus.
3. Wählen Sie aus **Starten Sie eine Telefonkonferenz** Aktion.
4. Sie können auch eine Telefonkonferenz starten, indem Sie auswählen Symbol im rechten Kontextmenü und Auswahl des +-Symbols.
   Das Popup-Fenster „Telefonkonferenz starten“ wird angezeigt.
5. Wählen Sie Aus **Microsoft Teams** Als Konferenzbrücke, über die Sie eine Verbindung herstellen möchten.
6. Geben Sie im Feld Titel einen Titel an, der den Grund für die Microsoft Teams-Telefonkonferenz beschreibt.

Verwendung der Microsoft Teams-Integration für Telefonkonferenzen



Automatische Übersetzung

7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Microsoft Teams-Telefonkonferenz aus. Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen oder die Teilnehmer aus auszuwählen **Empfehlungen** Liste, die Teilnehmerempfehlungen enthält, die der Microsoft Teams-Telefonkonferenz hinzugefügt werden können.

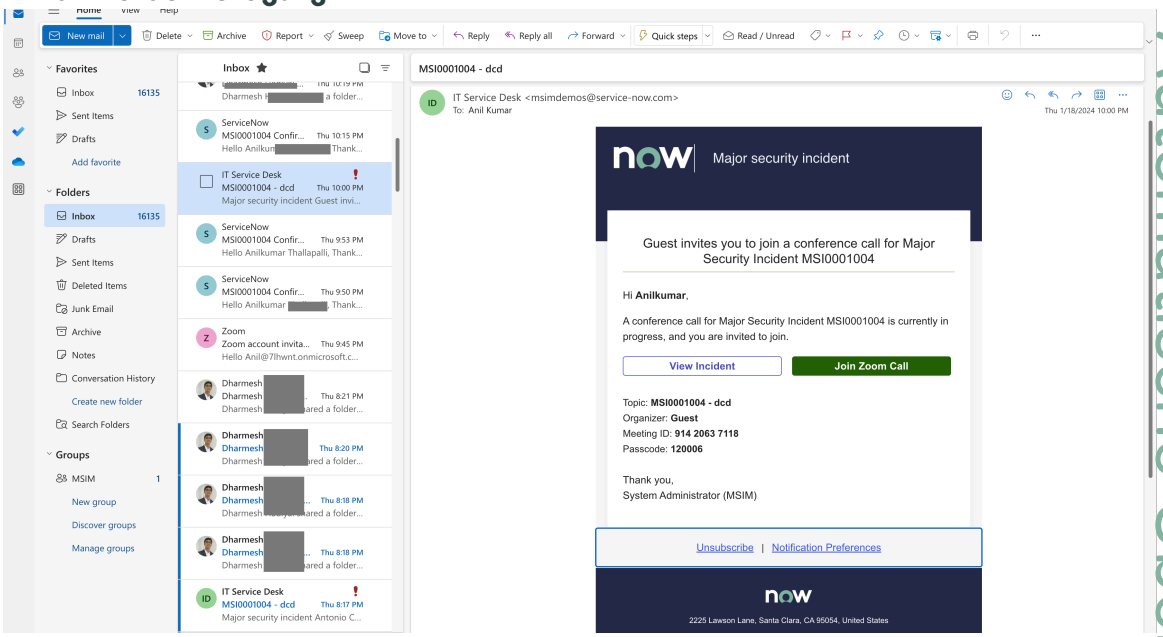
   Der Anwender (Host), der die Microsoft Teams-Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle Anwender, die dem schwerwiegenden Security Incident zugeordnet sind, sind standardmäßig unter verfügbar **Empfehlungen** Liste.

Hinweis:
Stellen Sie sicher, dass die ausgewählten Teilnehmer über eine gültige E-Mail-Adresse verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Nachdem Sie die Teilnehmer ausgewählt haben, geben Sie im Feld Beschreibung eine kurze Beschreibung des Grunds für den Beginn der Telefonkonferenz an.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.
9. Nachdem die Teilnehmerliste abgeschlossen ist, wählen Sie aus **Starten** .
   Die Telefonkonferenz beginnt in der Microsoft Teams-App. Alle Teilnehmer werden per E-Mail von der MSIM-App benachrichtigt, und die andere Benachrichtigung wird über einen Bot in der Microsoft Teams-App gesendet.
10. Wählen Sie aus **Klicken Sie hier** Option neben dem schwerwiegenden Security Incident, an der Telefonkonferenz in der Microsoft Teams-App teilzunehmen.
    Die Teilnehmer können den Link aus der MSIM-E-Mail-Benachrichtigung oder die Benachrichtigung aus der Microsoft Teams-App verwenden, um am Anruf teilzunehmen.

E-Mail-Benachrichtigung



11. Öffnen Sie den zugehörigen schwerwiegenden Security Incident im MSIM-Arbeitsbereich, um die Telefonkonferenzdetails anzuzeigen.

    Wenn der endgültige Teilnehmer den Anruf verlässt, wird die Telefonkonferenz beendet, oder wählen Sie aus **Anruf beenden** Im Abschnitt Telefonkonferenz, um die Telefonkonferenz zu beenden.

Automatische Übersetzung

Integrieren Sie MSIM-Telefonkonferenzen mit Zoom

Die Telefonkonferenz Zoom Mit der Integration können Sie eine verwalten und initiieren Zoom Telefonkonferenz direkt von einem schwerwiegenden Security Incident.

Schlüsselfunktionen

- Start und Ende Zoom Besprechungen direkt aus einem beliebigen Aufgabendatensatz, z. B. einem schwerwiegenden Security Incident, einem Change oder sogar aus der Workbench für schwerwiegende Incidents.
- Verwalten Zoom Besprechungen durch Hinzufügen oder Entfernen von Teilnehmern.
- Verfolgen und melden Sie Besprechungsdetails wie Besprechungsdauer und Teilnehmer zur weiteren Analyse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Vergewissern Sie sich, dass Sie Folgendes installiert haben IntegrationHub Plugins auf Ihrem ServiceNow Instanz.

- Notify Plugin (com.snc.notify)
- Zoom Spoke (sn_Zoom_Spoke)
- Notify Zoom (sn_Notify_Zoom)
- Notify UI-Komponenten für konfigurierbare Arbeitsbereiche

Weitere Informationen finden Sie unter IntegrationHub anfordern .

Konfiguration

Zum Konfigurieren der MSIM-Telefonkonferenz Zoom Integration mit Notify Kommunikationskanal, siehe Configure Notify Zoom connector in Notify .

Verwenden Sie die MSIM-Telefonkonferenz Zoom Integration

Die folgenden Schritte zeigen Ihnen, wie Sie einen verwalten und initiieren können Zoom Telefonkonferenz direkt von einem schwerwiegenden Security Incident.

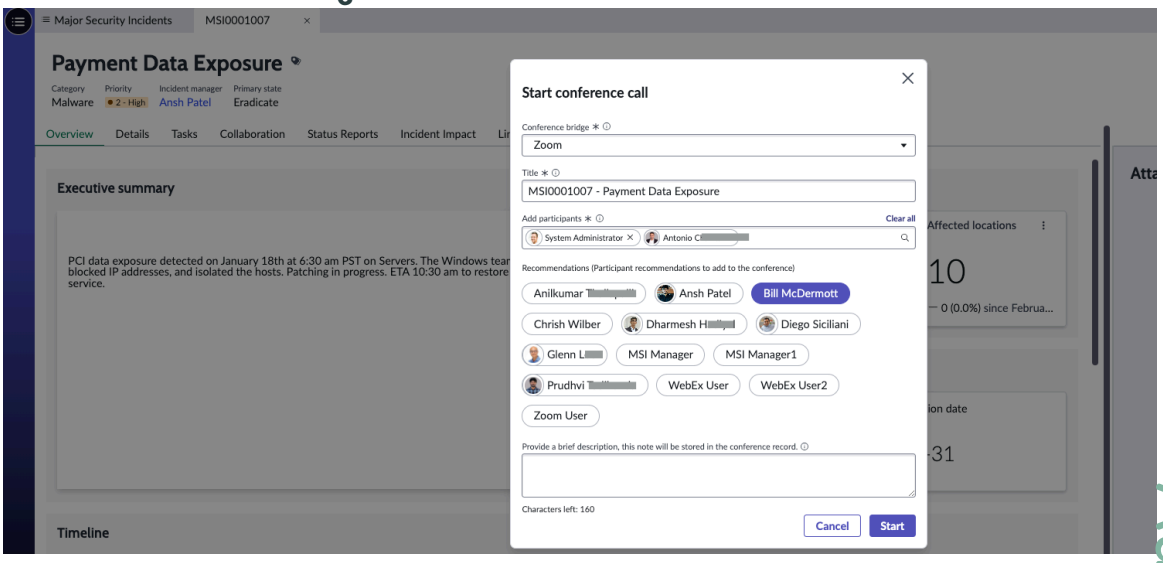
Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**an.
2. Wählen Sie in der Liste schwerwiegender Security Incident einen schwerwiegenden Security Incident aus.
3. Klicken Sie auf **Starten Sie eine Telefonkonferenz** Aktion.
4. Sie können auch eine Telefonkonferenz starten, indem Sie auf klicken Symbol im rechten Kontextmenü und Auswahl des +-Symbols.
   Das Popup-Fenster „Telefonkonferenz starten“ wird angezeigt.
5. Wählen Sie Aus **Zoom** Als Konferenzbrücke, über die Sie eine Verbindung herstellen möchten.
6. Geben Sie im Feld Titel einen Titel an, der den Grund für die Zoom-Telefonkonferenz beschreibt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden der Zoom-Integration für Telefonkonferenzen



7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Zoom-Telefonkonferenz aus.
   Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen oder die Teilnehmer aus auszuwählen **Empfehlungen** Liste, die Teilnehmerempfehlungen enthält, die der Zoom-Telefonkonferenz hinzugefügt werden können.

   Der Anwender (Host), der die Zoom-Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle Anwender, die dem schwerwiegenden Security Incident zugeordnet sind, sind standardmäßig unter verfügbar **Empfehlungen** Liste.

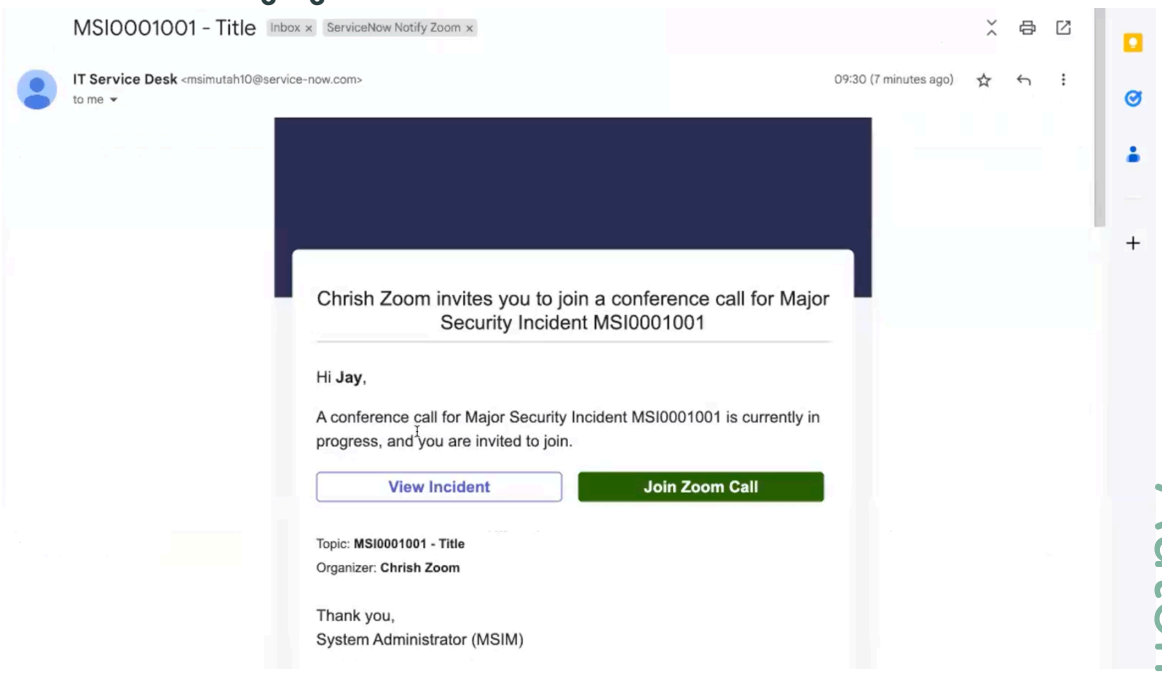
   Hinweis:
   Stellen Sie sicher, dass die ausgewählten Teilnehmer über eine gültige E-Mail-Adresse verfügen.

8. Nachdem Sie die Teilnehmer ausgewählt haben, geben Sie im Feld Beschreibung eine kurze Beschreibung des Grunds für den Beginn der Telefonkonferenz an.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.
9. Nachdem die Teilnehmerliste abgeschlossen ist, klicken Sie auf **Starten** .
   Die Telefonkonferenz beginnt in der Zoom-App. Alle Teilnehmer werden über zwei E-Mails benachrichtigt. Eine E-Mail wird über die MSIM-App an die Teilnehmer gesendet, die andere E-Mail wird über die Zoom-Konferenzbrücke gesendet.
10. Wählen Sie aus **Klicken Sie hier** Option neben dem schwerwiegenden Security Incident zur Teilnahme an der Telefonkonferenz in der Zoom-App.
    Die Teilnehmer können den Link aus der MSIM-E-Mail-Benachrichtigung oder die Benachrichtigung aus der Zoom-App verwenden, um am Anruf teilzunehmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Benachrichtigung



11. Öffnen Sie den zugehörigen schwerwiegenden Security Incident im MSIM-Arbeitsbereich, um die Telefonkonferenzdetails anzuzeigen.

    Wenn der endgültige Teilnehmer den Anruf verlässt, wird die Telefonkonferenz beendet, oder wählen Sie aus **Anruf beenden** Im Abschnitt Telefonkonferenz, um die Telefonkonferenz zu beenden.

    Wenn die Telefonkonferenz aufgezeichnet wurde, ist die Aufzeichnung nach einiger Zeit im Abschnitt Telefonkonferenz des zugehörigen schwerwiegenden Security Incidents verfügbar.

Integrieren Sie MSIM-Telefonkonferenzen mit Cisco Webex

Die MSIM-Telefonkonferenz Cisco Webex Mit der Integration können Sie eine verwalten und initiieren Cisco Webex Telefonkonferenz direkt von einem schwerwiegenden Security Incident.

Schlüsselfunktionen

- Start und Ende Cisco Webex Besprechungen direkt von schwerwiegenden Security Incidents.
- Verwalten Sie einen Cisco Webex Besprechung durch Hinzufügen oder Entfernen von Teilnehmern.

Voraussetzungen

Vergewissern Sie sich, dass Sie Folgendes installiert haben IntegrationHub Plugins auf Ihrem ServiceNow Instanz.

- Notify Plugin (com.snc.notify)
- Notify Cisco Webex Connector (sn_Notify_webex)
- Cisco Webex Teams-Spoke (sn_cisco_Teams_spk)
- Notify UI-Komponenten für konfigurierbare Arbeitsbereiche

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter IntegrationHub anfordern .

Konfiguration

Zum Konfigurieren der MSIM-Telefonkonferenz Cisco Webex Integration mit Notify Kommunikationskanal, siehe Configure Notify Cisco Webex Connector .

Verwenden Sie die Telefonkonferenzen Cisco Webex Integration

Die folgenden Schritte zeigen Ihnen, wie Sie einen verwalten und initiieren können Cisco Webex Telefonkonferenz direkt von einem schwerwiegenden Security Incident.

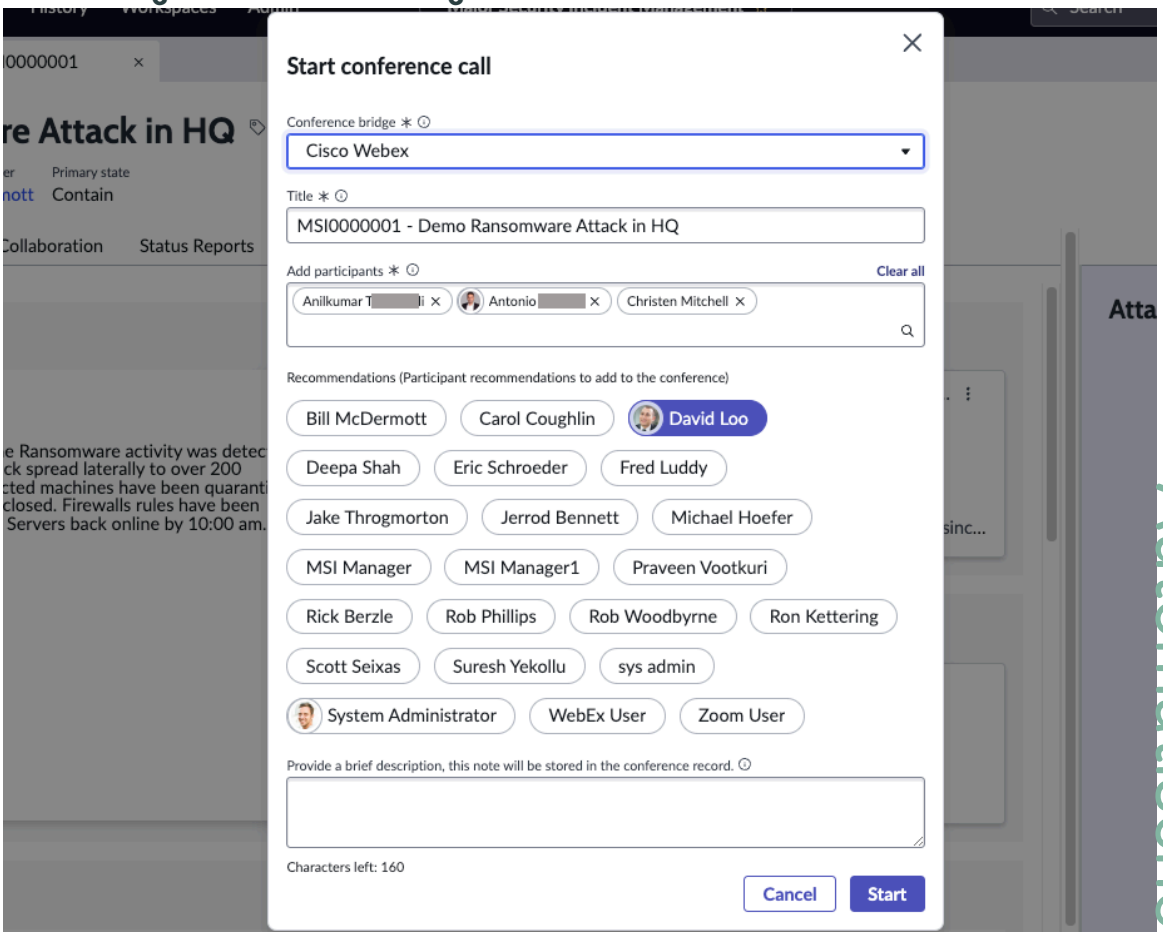
Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_Manager

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents**an.
2. Wählen Sie in der Liste schwerwiegender Security Incident einen schwerwiegenden Security Incident aus.
3. Wählen Sie aus **Starten Sie eine Telefonkonferenz** Aktion.
4. Sie können auch eine Telefonkonferenz starten, indem Sie auswählen Symbol im rechten Kontextmenü und Auswahl des +-Symbols.
   Das Popup-Fenster „Telefonkonferenz starten“ wird angezeigt.
5. Wählen Sie Aus **Cisco Webex** Als Konferenzbrücke, über die Sie eine Verbindung herstellen möchten.
6. Geben Sie im Feld Titel einen Titel an, der den Grund für die Cisco Webex-Telefonkonferenz beschreibt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwendung der Cisco Webex-Integration für Telefonkonferenzen



7. Wählen Sie im Feld Teilnehmer hinzufügen die Teilnehmer für die Cisco Webex-Telefonkonferenz aus. Sie können die Suchoption verwenden, um die erforderlichen Teilnehmer zu suchen und hinzuzufügen oder die Teilnehmer aus auszuwählen **Empfehlungen** Liste, die Teilnehmerempfehlungen enthält, die der Cisco Webex-Telefonkonferenz hinzugefügt werden können.

   Der Anwender (Host), der die Cisco Webex-Telefonkonferenz initiiert, wird automatisch der Liste der ausgewählten Teilnehmer hinzugefügt. Alle Anwender, die dem schwerwiegenden Security Incident zugeordnet sind, sind standardmäßig unter verfügbar **Empfehlungen** Liste.

   Hinweis:
   Stellen Sie sicher, dass die ausgewählten Teilnehmer über eine gültige E-Mail-Adresse verfügen.

8. Nachdem Sie die Teilnehmer ausgewählt haben, geben Sie im Feld Beschreibung eine kurze Beschreibung des Grunds für den Beginn der Telefonkonferenz an.
   Die von Ihnen angegebene Beschreibung wird dem Konferenzdatensatz hinzugefügt.

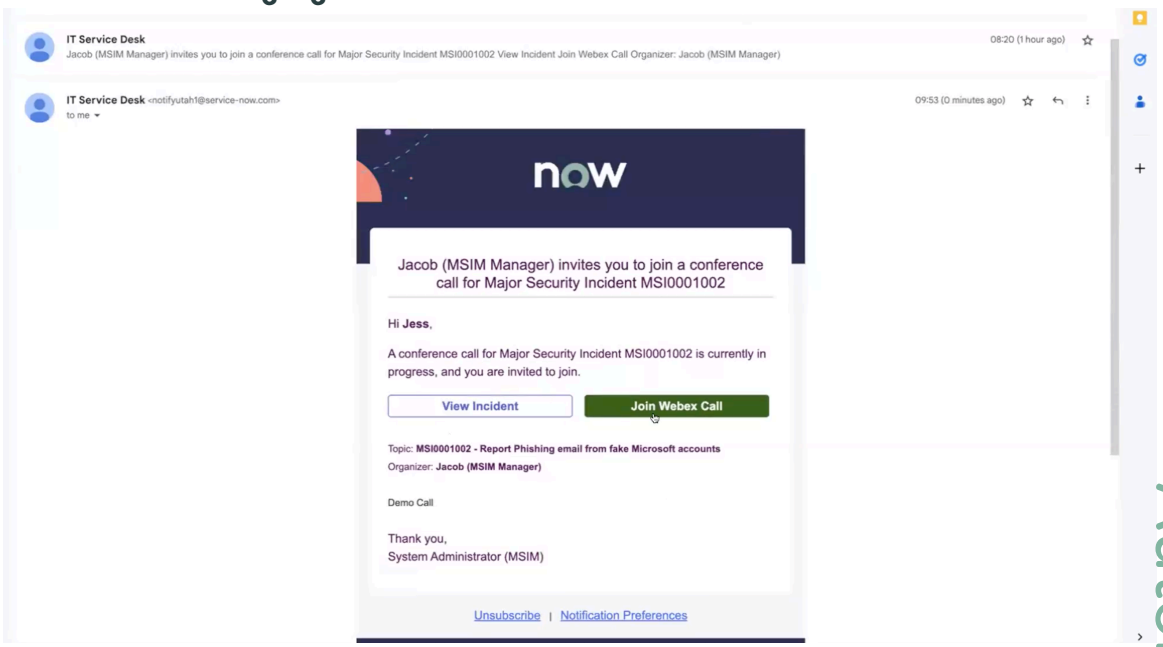
9. Nachdem die Teilnehmerliste abgeschlossen ist, wählen Sie aus **Starten** .
   Die Telefonkonferenz beginnt in der Cisco Webex-App. Alle Teilnehmer werden über zwei E-Mails benachrichtigt. Eine E-Mail wird über die MSIM-App an die Teilnehmer gesendet, die andere E-Mail wird über die Cisco Webex-Konferenzbrücke gesendet.

10. Wählen Sie aus **Klicken Sie hier** Option neben dem schwerwiegenden Security Incident, an der Telefonkonferenz in der Cisco Webex-App teilzunehmen.
    Die Teilnehmer können den Link aus der MSIM-E-Mail-Benachrichtigung oder die Benachrichtigung aus der Cisco Webex-App verwenden, um an dem Anruf teilzunehmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Benachrichtigung



11. Öffnen Sie den zugehörigen schwerwiegenden Security Incident im MSIM-Arbeitsbereich, um die Telefonkonferenzdetails anzuzeigen.

    Wenn der endgültige Teilnehmer den Anruf verlässt, wird die Telefonkonferenz beendet, oder wählen Sie aus **Anruf beenden** Im Abschnitt Telefonkonferenz, um die Telefonkonferenz zu beenden.

    Wenn die Telefonkonferenz aufgezeichnet wurde, ist die Aufzeichnung nach einiger Zeit im Abschnitt Telefonkonferenz des zugehörigen schwerwiegenden Security Incidents verfügbar.

Management schwerwiegender Sicherheits-Incidents konfigurieren

Installieren und konfigurieren Management schwerwiegender Sicherheits-Incidents Anwendung.

Wichtig:

- Um schnell mit zu beginnen Management schwerwiegender Sicherheits-Incidents-Konfiguration finden Sie unter Schnellstartleitfaden für Management schwerwiegender Security Incidents (MSIM) Im ServiceNow Store.
- Nach der Installation von Management schwerwiegender Sicherheits-Incidents App, stellen Sie sicher, dass Sie den Update-Satz in importieren KB1289784 Zum Laden der teilweise vorkonfigurierten Dateien.

In diesem Abschnitt erfahren Sie, wie Sie die für die Arbeit mit erforderlichen Konfigurationen einrichten Major Security Incident Datensätze durch Integration mit anderen externen Microsoft Anwendungen, mit denen Verbindungen hergestellt werden sollen ServiceNow Instanz.

Konfigurieren Sie Die Datei-Explorer-Komponente

Die Komponente „Datei-Explorer-Arbeitsbereich“ organisiert und verfolgt die Sammlung von Artefakten (Dateien) im Zusammenhang mit einem schwerwiegenden Security Incident. Es wurde entwickelt, um die Integration mit einem beliebigen Dateihosting-Anbieter von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Drittparteien wie zu unterstützen Microsoft SharePoint In Management schwerwiegender Sicherheits-Incidents Arbeitsbereich.

- File Explorer Komponente: Bietet eine grafische Anwenderoberfläche zum Anzeigen des Dateisystems und ermöglicht Anwendern die Ausführung von Dateivorgängen.
- File Explorer Core: Stellt eine Abstraktionsebene bereit, mit der die Datei-Explorer-Komponente das Dateisystem anzeigen und verschiedene Dateivorgänge ausführen kann, ohne etwas über den zugrunde liegenden Connector zu wissen, der für die Kommunikation mit externen Repositorys verwendet wird.
- File Explorer Microsoft SharePoint Connector-Anwendung: Stellt die Implementierungsmodule bereit, die zum Nachverfolgen und Abrufen von Dateien/Ordnermetadaten von erforderlich sind Microsoft SharePoint Dokumentbibliothek und Dateivorgänge ausführen.

Die File Explorer Die Kernkomponente stellt eine Basisinfrastruktur bereit, die für die verschiedenen Connector-Anwendungen für die Dateifreigabe erforderlich ist, um ihre Verbindungseigenschaften zu definieren.

Sie müssen das Datei-Repository-Laufwerk und den Datei-Repository-Anbieter installieren und konfigurieren, indem Sie die Verbindungseigenschaften hinzufügen, um die Dateimetadaten aus einem Dateihosting-Provider-Speicherort abzurufen.

Für diese aktuelle Version von File Explorer, Diese Anweisungen umfassen das Konfigurieren und Abonnieren einer abrufenden Datei Metadaten Z. B. Microsoft SharePoint Datei- und Ordneraktualisierungen, Dateivorgänge und Protokollierungsdateiaktivität. Ein festgelegt Microsoft SharePoint Die Dokumentbibliothek und die zugehörige Laufwerkskonfiguration sind erforderlich, um einzelne Ordner zu erstellen, die für einen schwerwiegenden Security Incident spezifisch sind.

File Explorer Ermöglicht auch Connector-Anwendungen wie Microsoft SharePoint. Sie können dieses Beispiel verwenden, um seine Dateivorgangsimplementierungen zu konfigurieren, z. B. **Herunterladen** oder **Umbenennen** Ordner- und Dateiaktionen werden in der Komponente des Datei-Explorer-Arbeitsbereichs aktiviert. Diese Aktionen werden mit den integrierten Flow Designer-Subflows aktiviert und ausgeführt. Weitere Informationen finden Sie unter Einstellungen für Ordner- und Dateiaktion .

File Explorer Konfiguration Enthält das folgende Setup:

- Konfigurieren Sie Den Datei-Explorer Repository Laufwerk
- Konfigurieren Sie Ordner- und Dateiaktionseinstellungen
- Erstellen Sie Ordnervorlagen

Erste Schritte mit dem Datei-Explorer

Überprüfen Sie die folgenden Informationen, bevor Sie mit arbeiten File Explorer Komponente.

Überprüfen Sie die folgenden Informationen, bevor Sie mit dem Herstellen der Verbindung mit beginnen Microsoft SharePoint, Erstellen von Ordner- und Dateiaktionen und Erstellen von Ordnervorlagen für die Datei-Explorer-Komponente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Name	Beschreibung
Microsoft SharePoint Spoke, Version 2.0.2 für ServiceNow® IntegrationHub.	Verwenden **sn_sp_Spoke** Plugin-ID, die gesucht und installiert werden soll Microsoft SharePoint Spoke. Die Installation dieses Plugins bietet Flows und Aktionen zur Automatisierung von Zusammenarbeit, Dokumentverwaltung und Anwenderzugriffsrechten in Microsoft SharePoint.
Datei-Explorer-Komponente v1.1.0	Verwenden **sn_file_Explorer** Plugin-ID zum Suchen und Installieren der Datei-Explorer-Komponente v1.1.0 Die Installation dieses Plugins bietet eine grafische Anwenderoberfläche zum Durchsuchen des Dateisystems, das im Datei-Explorer-Core verfügbar ist.
Datei-Explorer Core für Security Operations v1.1.1	Verwenden **sn_fe** Plugin-ID zum Suchen und Installieren des Datei-Explorer Core. Die Installation dieses Plugins stellt eine Basisinfrastruktur zur Integration mit einem beliebigen Dateihosting-Anbieter von Drittparteien bereit.
Microsoft SharePoint Datei-Explorer-Connector für Security Operations v1.1.1	Verwenden **sn_fe_sharepoint** Plugin-ID, die gesucht und installiert werden soll Microsoft SharePoint Datei-Explorer-Connector. Durch die Installation dieses Plugins wird verwaltet Microsoft SharePoint Dateien/Ordner mit Datei-Explorer.

Konfigurieren Sie Den Datei-Explorer Repository Laufwerk

Die Microsoft SharePoint Connector bietet verschiedene Funktionen, die in implementiert werden sollen Microsoft SharePoint Datei-Explorer-Funktionen durch Verwaltung und Nachverfolgung der Dateimetadaten.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Schwerwiegender Security Incident** > **Dateiexplorer** > **Datei-Repository-Konfiguration**an.
2. Füllen Sie die folgenden Felder wie in der folgenden Tabelle beschrieben aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

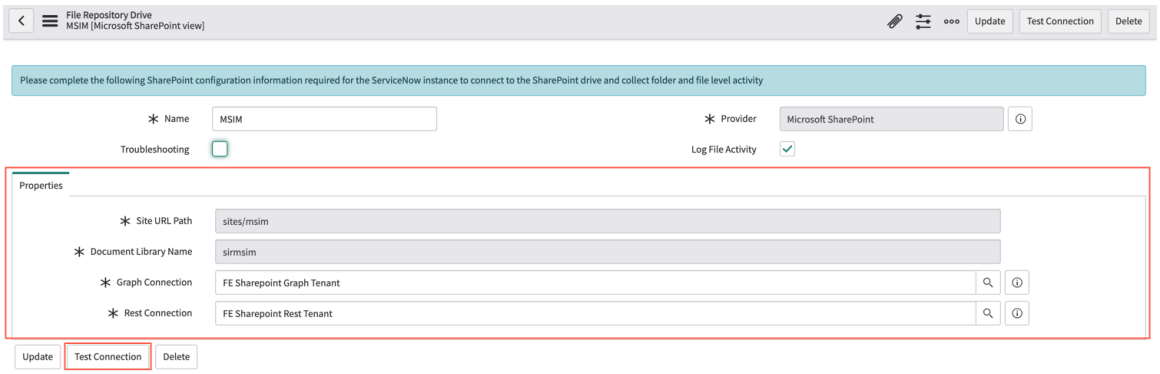
Feldname	Feldbeschreibung
Name	Name des Datei-Repository-Datensatzes, der die Nutzung identifiziert. Beispiel: MSIM.
Anbieter	Name des Anbieters, der der Drittanbieter des Dateihosting-Repositorys ist. Beispiel: Microsoft SharePoint.
Eigenschaften	
Website-URL-Pfad	Geben Sie ein Microsoft SharePoint URL mit einem bestimmten Websitepfad. Geben Sie nur den relativen Pfad zur Website an, und möglicherweise ist keine vollständige Website-URL erforderlich. Beispiel: Sites/MSIM.
Name der Dokumentbibliothek	Erstellen Sie eine Dokumentbibliothek unter Microsoft SharePoint Site und geben Sie hier denselben Namen der Dokumentbibliothek an. Dies wäre dieselbe Dokumentbibliothek, die Sie in erstellt haben Microsoft SharePoint Setup des Connector-Laufwerks.
Graph-Verbindung	Wählen Sie den Datei-Explorer Graph-Mandantendatensatz aus. Weitere Informationen zur Konfiguration der Mandantenverbindung finden Sie unter Microsoft SharePoint-Spoke .
REST-Verbindung	Wählen Sie den REST-Mandantendatensatz des Datei-Explorers aus. Weitere Informationen zur Konfiguration der Mandantenverbindung finden Sie unter Microsoft SharePoint-Spoke .

3. Wählen Sie **Speichern**.
4. Klicken **Testverbindung** Registerkarte zum Testen der Verbindung und Validieren der Konfigurationseigenschaften des Datei-Repository-Laufwerks.

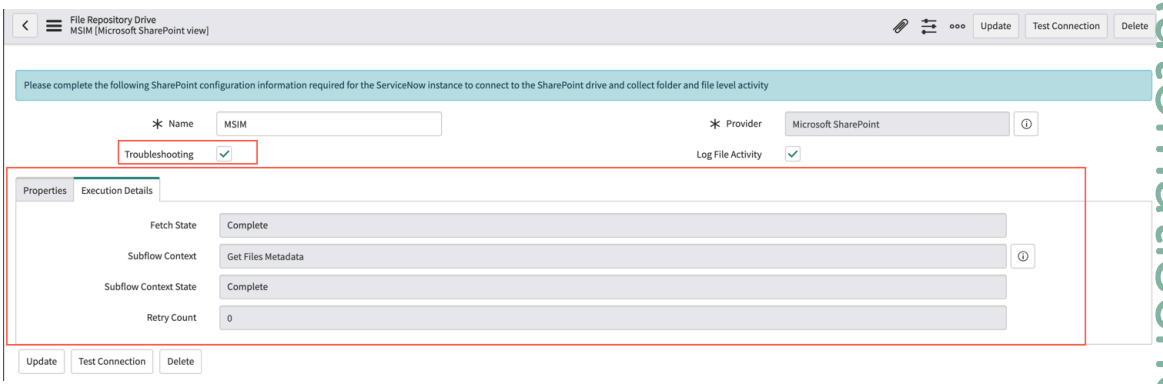
   Hinweis:
   Vor **Wird Aktiviert** Das Datei-Repository, stellen Sie sicher, dass die entsprechende Dokumentbibliothek in Microsoft SharePoint Hat keine Ordner- oder Dateidaten.

5. Klicken Sie Auf **Aktivieren** Zum Aktivieren des Datei-Repositorys.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie aus **Problembehandlung** Kontrollkästchen zum Überprüfen des Datei-Repositorys **Ausführungsdetails** Und verifizieren Sie **Status abrufen** Ist abgeschlossen, und stellen Sie sicher, dass die Microsoft SharePoint Laufwerksabonnements werden erstellt, und der Status ist „Abgeschlossen“.



Hinweis:
Mit **Verbindung Testen** Schaltfläche, entweder MSI-Administrator oder MSI-Manager kann nur die Datei-Repository-Konfiguration validieren.

Konfigurieren Sie Ordner- und Dateiaktionseinstellungen

C Konfigurieren Die Ordner- und Dateiaktionen, die Sie über die Datei-Explorer-Komponente im Arbeitsbereich „Management schwerwiegender Security Incidents“ aktivieren möchten , Mithilfe der Setup-Seite für Ordner- und Dateiaktionseinstellungen . Als MSI-Administrator können Sie die einzelnen Ordner- und Dateiaktionen steuern, die in der Datei-Explorer-Komponente angezeigt werden.

Vorbereitungen

Im Folgenden finden Sie die implementierten Dateivorgangsfunktionen in der Datei-Explorer-Komponente mit ServiceNow® Flow Designer:

Dateivorgangsfähigkeiten

Dateivorgang	Beschreibung
Öffnen Sie in Microsoft SharePoint	Öffnet eine neue Browserregisterkarte zum Anzeigen Microsoft SharePoint Dateiansicht der Dokumentbibliothek

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateivorgangsfähigkeiten (Fortsetzung)

Dateivorgang	Beschreibung
Ordner erstellen	Möglichkeit, zusätzliche Ad-hoc-Ordner zu erstellen, nachdem der schwerwiegende Security Incident erstellt wurde.
Ordner umbenennen	Möglichkeit, die erstellten Ordner umzubenennen.
Datei verschieben	Ermöglicht Ihnen das Verschieben von Dateien zwischen Ordnern in der Datei-Explorer-Komponente des Arbeitsbereichs, was zu einer Verschiebung von Dateien in führt Microsoft SharePoint
Suchen Sie Die Datei	Zeigt den Ordnerspeicherort bei Verwendung von an **Letzte** Ansicht des Datei-Explorers.
Datei löschen	Löschen Sie die Datei.
Ordner löschen	Löschen Sie den Ordner.
Datei herunterladen	Lädt die Datei auf der vorhandenen Browserregisterkarte des MSIM-Arbeitsbereichs herunter, um sie schnell anzuzeigen.
Benennen Sie Die Datei Um	Benennt die Datei um.

Hinweis:

1. Alle aufgeführten Aktionen sind derzeit standardmäßig aktiviert. Sie müssen bearbeiten **Dateiaktionseinstellungen** Wenn bestimmte Aktionen nicht angezeigt werden sollen. Alle Einstellungen sind derzeit für alle Anwender global, Dies bedeutet, dass keine Aktionen für eine Teilmenge der Anwender mit einer bestimmten Rolle aktiviert werden können.
2. **Anwenderzugriff Widerrufen** und **Berechtigungen hinzufügen** Aktionen sind systembezogene Aktionen. Es wird empfohlen, diese Dateiaktionen nicht zu ändern.

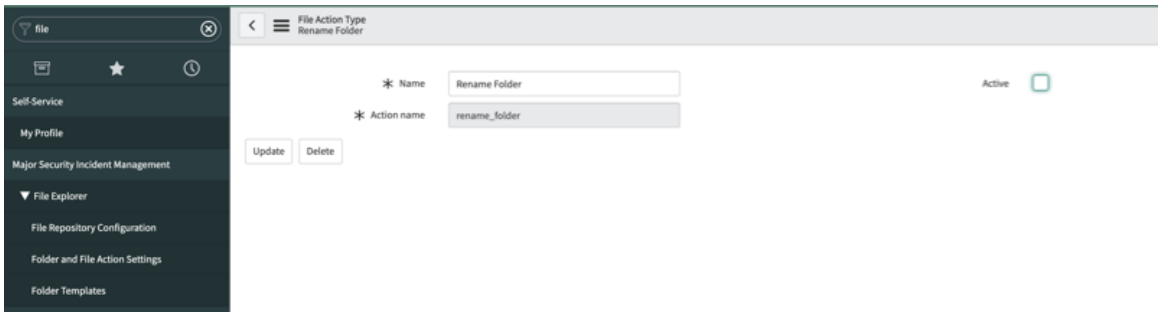
Das folgende Beispiel Verfahren Beschreibt einen der Funktionen für Dateivorgänge Ja Zum Deaktivieren bestimmter Ordner- und Dateiaktionen während der Konfiguration des Datei-Explorer-Repositorys. Dieses Verfahren gilt für alle anderen Aktionen, die möglicherweise bearbeitet werden müssen :

Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Dateiexplorer** > **Einstellungen für Ordner- und Dateiaktionen**an.
2. Wählen Sie den gewünschten Datensatz aus, um die Ordner- bzw. Dateiaktion zu aktivieren oder zu deaktivieren.
3. Auswahl Aufheben Die **Aktiv** Kontrollkästchen zum Deaktivieren der Ordner- und Dateiaktion.

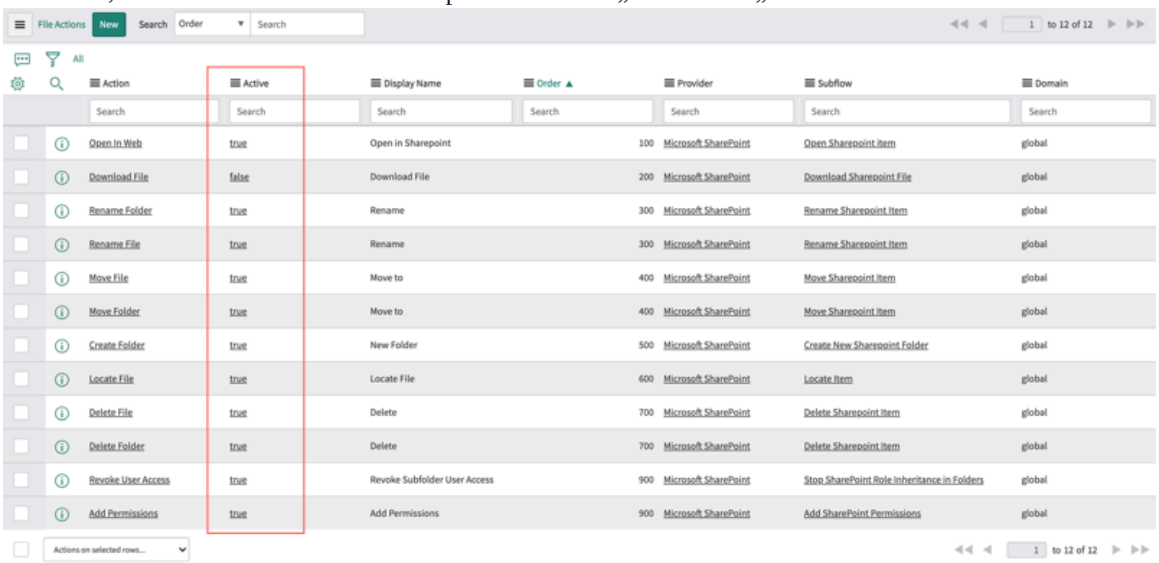
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



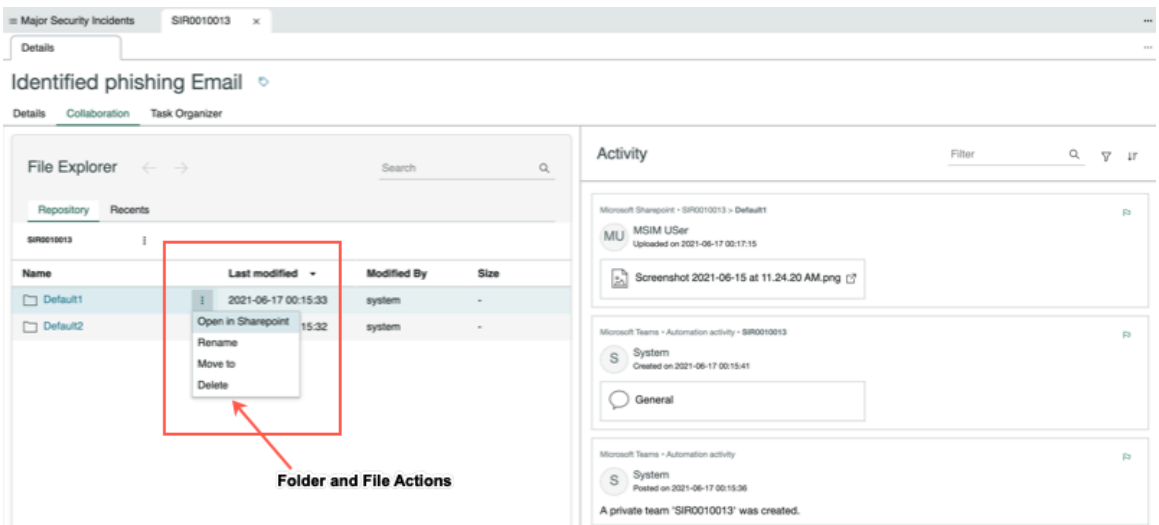
4. **Aktualisieren** Der Laufwerksdatensatz.

Hinweis:

Sie können die Dateiaktion auch direkt aus der Liste der angezeigten Dateivorgänge ausführen, indem Sie auswählen **Aktiv** Spaltenwerte auf „wahr“ oder „falsch“.



Wenn die ausgeführte Dateiaktion deaktiviert ist, wird die Aktion nicht in angezeigt **Kollaborationen** Registerkarte von **Management schwerwiegender Sicherheits-Incidents** Arbeitsbereich.



Erstellen Sie Ordnervorlagen

Verwenden Sie Ordnervorlagen, um automatisch eindeutige Ordner für verschiedene Typen schwerwiegender Security Incidents zu erstellen. Die Ordnervorlagen in der Datei-Explorer-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponente werden verwendet, um eine Basisordnerstruktur für den Security Incident in zu erstellen Microsoft SharePoint.

Vorbereitungen

Als MSI-Administrator definieren Sie die anfängliche Ordnerstruktur, die erforderlich ist, um die Zusammenarbeit zwischen verschiedenen Incident-Beantworter-Gruppen zu ermöglichen, und weisen entsprechende Zugriffsrechte auf Unterordnerebene zu. Mehrere Konfigurationen können für verschiedene erstellt werden Major Security Incident Typen, die einen Bedingungsgenerator für bestimmte verwenden Major Security IncidentFeldwerte, die den Zugriff auf verschiedene Anwender und Anwendergruppen auf jeder Unterordnerebene ermöglichen.

Hinweis:
Diese Ordnervorlagen werden von allen schwerwiegenden Security Incidents verwendet, die die im Bedingungsgenerator angegebenen Bedingungen erfüllen. Es wird empfohlen, Incident-Feldvariablen wie Incident-Nummer oder -Kategorie zu verwenden, um eindeutige Stammordnernamen zu erstellen, die einen Satz von Unterordnern mit allgemeinen Ordnernamen für einen schwerwiegenden Security Incident von ähnlichen Ordnern mit diesen Namen unterscheiden, die Teil eines anderen schwerwiegenden Security Incidents sind.

Die definierte Ordnervorlagenkonfiguration wird nur dann auf den schwerwiegenden Security Incident angewendet, wenn die Bedingung erfüllt ist.

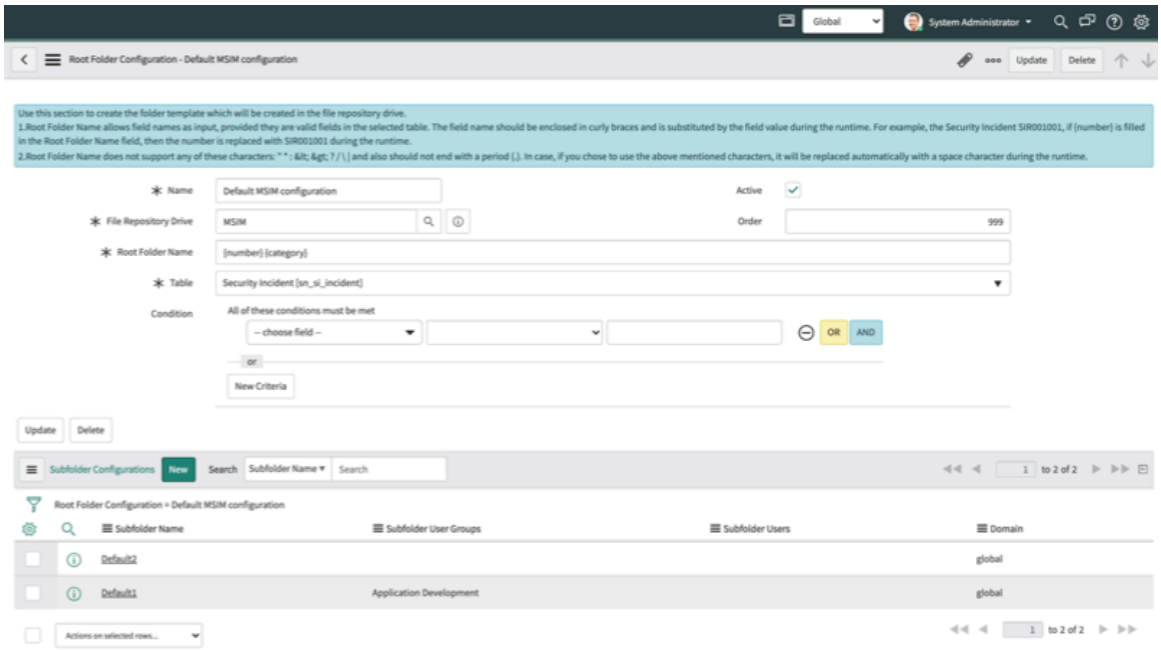
Hinweis:
Eine Basissystemkonfiguration (ohne Unterordner) wird auf alle Security Incidents angewendet. Sie können diese Standardkonfiguration entweder bearbeiten, um bestimmte Unterordner einzubeziehen, oder eine neue Konfiguration basierend auf einem angegebenen Satz von Feldwerten für schwerwiegende Security Incidents erstellen. Beispiel: Kategorie = schädliche Codeaktivität.

Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

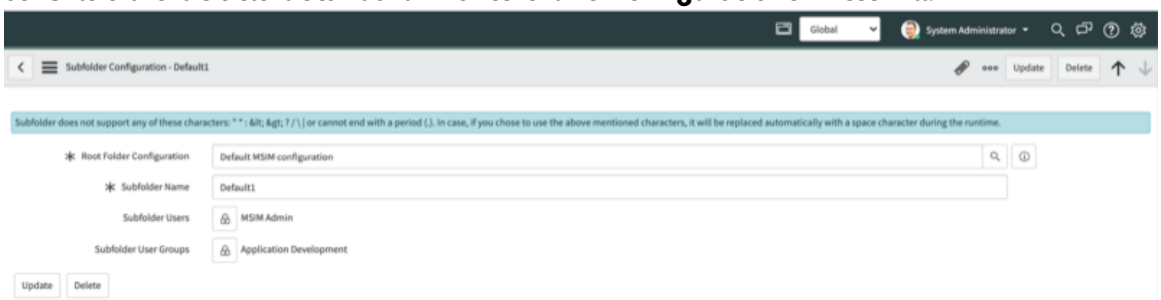
1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **Dateiexplorer** > **Ordnervorlagen**an.
2. Klicken **Neu** Für Stammordnerkonfiguration.
3. Füllen Sie die Felder im Formular aus.
4. Definieren Sie den Security Incident **Bedingung** Werte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. **Aktualisieren** Der Datensatz.
   Die Unterordner werden mit den definierten Werten erstellt.

6. Klicken Sie auf die gewünschte **Unterordner** .
   Wenn Sie keinen Unterordner mit einem entsprechenden Namen erstellen, werden die Namen der Unterordner als erstellt **Standard** In **Unterordnerkonfigurationen** Abschnitt.



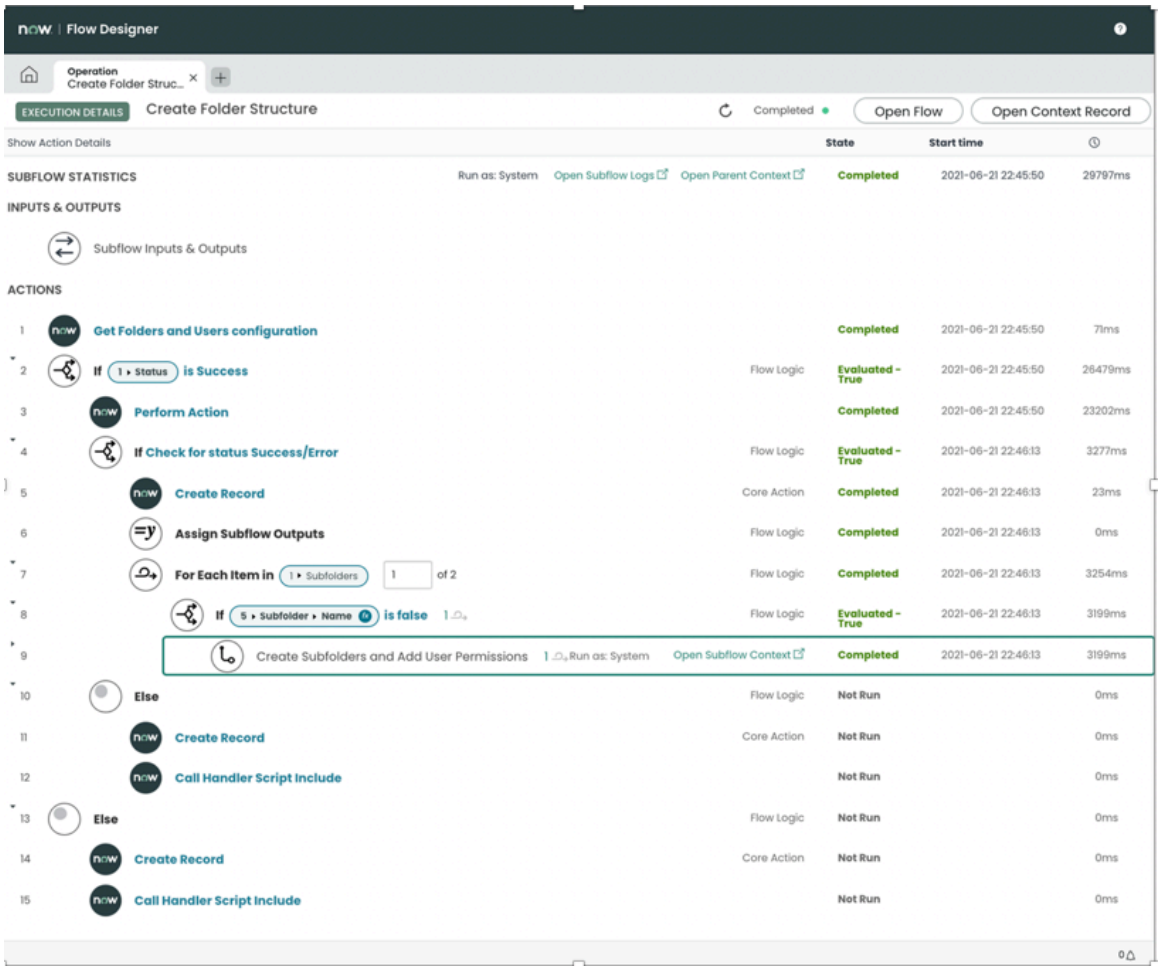
Dieselbe Ordnerstruktur wird automatisch in erstellt Microsoft SharePoint Mit denselben Zugriffsberechtigungen, die auf konfiguriert sind **Ordnervorlagen** Seite.

Hinweis:

- **Stammordnername** Erlaubt Feldvariablennamen als Eingabe, sofern es sich um gültige Felder in der ausgewählten Tabelle handelt. Der Feldname muss in geschweiften Klammern eingeschlossen werden und wird während der Laufzeit der Flow-Ausführung durch den Feldwert ersetzt. Beispiel: Die Variable „Security Incident SIR001001“, wenn {number} in konfiguriert ist **Stammordnername** Dann wird die Zahl während der Laufzeit durch SIR001001 ersetzt.
- **Stammordnername** Unterstützt keines der folgenden Zeichen: „ * : < > ? / \ | und darf nicht mit einem Punkt (.) enden. Wenn Sie die oben genannten Zeichen verwenden, werden sie während der Laufzeit automatisch durch ein Leerzeichen ersetzt.
- Wenn **Stammordner** Und **Unterordner** Der Name überschreitet den definierten Grenzwert (256 Zeichen), dann wird der Ordnername gekürzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Folgenden finden Sie die Ausführungszeit des Subflows „Ordnerstruktur erstellen“:



File Explorer Aktivitätenstrom im Arbeitsbereich

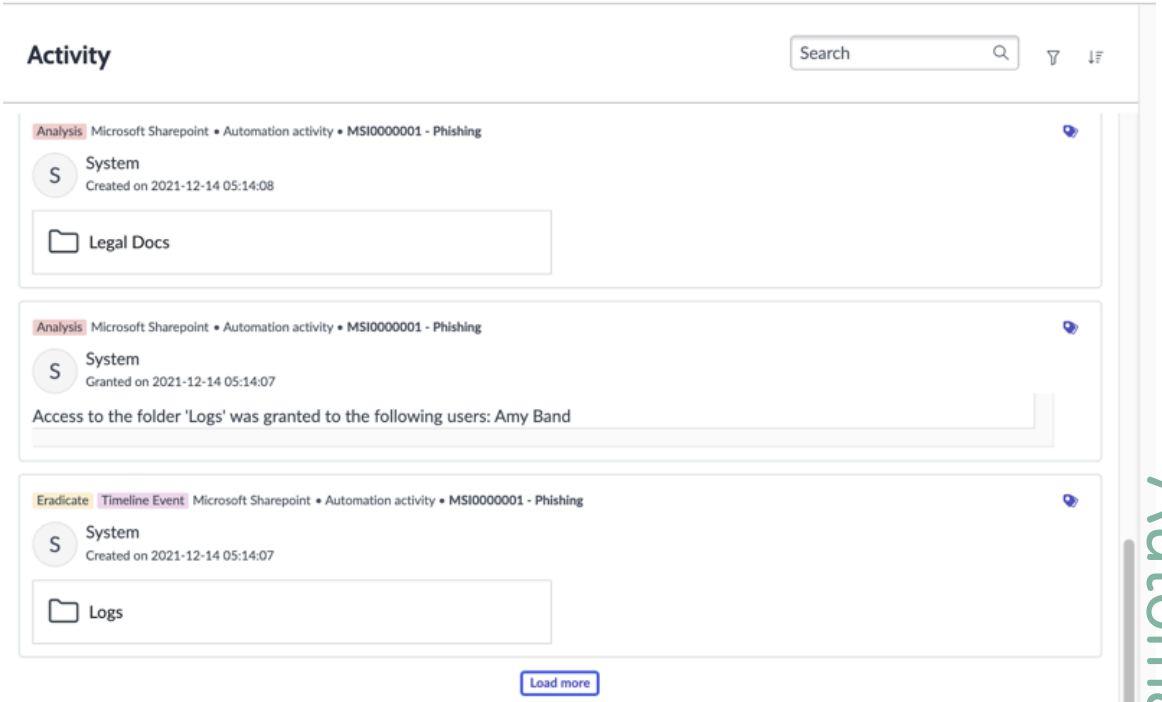
Verwenden Sie den Abschnitt „Datei-Explorer“ von Management schwerwiegender Sicherheits-Incidents Arbeitsbereich zum Anzeigen der Ordner und Dateien in der Reihenfolge, in der sie erstellt wurden Microsoft SharePoint Dokumentbibliothek.

Der Aktivitätenstrom listet alle Veröffentlichungen der Automatisierungsaktivität auf, wann immer Ordner- und Dateiaktivitäten oder Protokolle während der auftreten Major Security Incident Lösung. Die Aktivitätenstromstruktur ist im gleichen Format wie ausgerichtet Microsoft SharePoint Bibliothek, die die erstellten Ordner anzeigt und welche Anwender oder Anwendergruppen diesen Ordnern zugewiesen wurden.

Mit dem Aktivitätenstrom können Arbeitsbereichsmanager und andere Anwender oder Anwendergruppen effektiv kommunizieren und zusammenarbeiten und die Aktivitäten auflisten, die für ausgeführt wurden Microsoft SharePoint Ordner und Dateien, überwachen den Status des Incident, veröffentlichen Sie die Notizen, oder fügen Sie zusätzliche Kommentare zum Incident-Datensatz hinzu. Die Arbeitsbereichsmanager

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können basierend auf der zuletzt aktualisierten Aktivität abholen und



arbeiten.

File Explorer-Problembehandlung

Der Abschnitt „Fehlerbehebung“ kann Ihnen helfen, einige der technischen Probleme zu beheben, die beim Einrichten auftreten können File Explorer Komponente.

Informationen zu geplanten Aufgaben, Systemeigenschaften und finden Sie im folgenden Abschnitt File Explorer Flow Designer-Subflows im Detail.

Geplante Aufgaben für File Explorer

Geplante Aufgaben sind automatisierte Aufgaben, die ausgeführt werden, um die Benachrichtigungen von zu verarbeiten Microsoft SharePoint, Erfassen Sie die Dateimetadaten in ServiceNow Instanz und verlängern Sie die Datei-Repository-Abonnements nach einem wiederkehrenden Zeitplan.

Geplante Aufgaben sind automatisierte Aufgaben, die im Hintergrund ausgeführt werden, um:

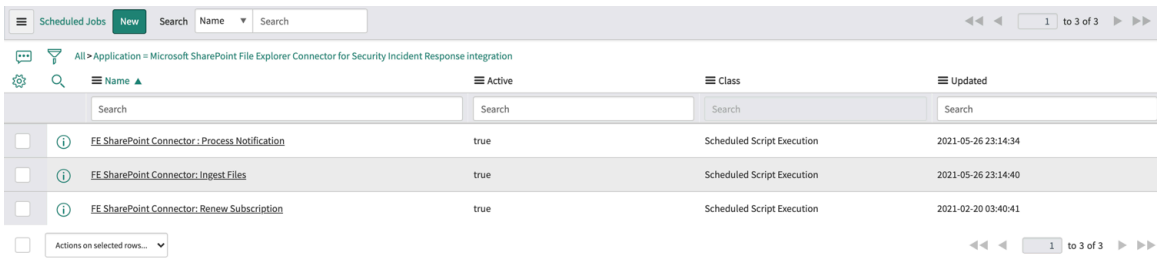
- Verarbeiten Sie die Benachrichtigungen von Microsoft Microsoft SharePoint.
- Erfassen Sie die Dateimetadaten in ServiceNow AI Platform Instanz.
- Verlängern Sie das Abonnement mit Microsoft SharePoint Dokumentbibliothek zum Empfangen von Benachrichtigungen.

Auftrag	Beschreibung
Microsoft SharePoint File Explorer Connector: Prozessbenachrichtigung	Wird alle 30 Sekunden ausgeführt und ist für das Lesen der Benachrichtigungen verantwortlich, die angeben, dass Änderungen an der abonnierten Dokumentbibliothek aufgetreten sind, und den

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auftrag	Beschreibung
	Status von Laufwerken (sn_fe_file_repo_Drive) als ausstehend markieren.
Microsoft SharePoint File Explorer Connector: Dateien Erfassen	Wird alle 30 Sekunden ausgeführt und hauptsächlich für die Verarbeitung der Laufwerke (sn_fe_file_repo_Drive) verantwortlich, die sich im Status „Ausstehend“ befinden, und ruft die Delta-Dateiänderungen aus dem konfigurierten ab Microsoft SharePoint Dokumentbibliothek seit dem letzten Abruf.
Microsoft SharePoint File Explorer: Abonnement Verlängern	Wird alle 10 Minuten ausgeführt und ist für die Verlängerung von verantwortlich Microsoft SharePoint Dokumentbibliotheksabonnement einen Tag vor dem Ablaufdatum. Normalerweise laufen diese Abonnements in 30 Tagen ab.



Verfügbare Datei-Explorer-Systemeigenschaften

Im Folgenden sind die verfügbar Microsoft SharePoint Systemeigenschaften des Datei-Explorer-Connectors.

Systemeigenschaften

Eigenschaftsname	Beschreibung
sn_fe_sharepoint.max_retry_count	Steuert die Häufigkeit von Versuchen, die verwendet werden Microsoft SharePoint Die Connector-Anwendung hat versucht, das fehlerhafte Laufwerk abzurufen oder das fehlgeschlagene Abonnement zu verlängern. Der Standardwert für die Häufigkeit ist auf 50 festgelegt.
sn_fe_sharepoint.retry_After_seconds	Zeitintervall zwischen jedem Versuch, das fehlerhafte Laufwerk abzurufen oder das Abonnement zu verlängern. Der Standardwert ist auf 900 Sekunden oder 15 Minuten festgelegt.
sn_fe_sharepoint.max_Subscription_expiration_time	Maximaler Abonnementablaufzeitraum in Tagen für Microsoft SharePoint. Der standardmäßige Ablaufzeitraum ist auf 30 Tage festgelegt.

File Explorer Flow Designer-Subflows

Im Folgenden finden Sie die Flow Designer-Subflows, die mit installiert werden Microsoft SharePoint File Explorer Connector.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subflows

Name	Beschreibung
Hinzufügen Microsoft SharePoint Berechtigungen	Erteilt bestimmten Anwendern Bearbeitungsberechtigung für einen bestimmten Ordner.
Laufwerksabonnement Erstellen	Abonniert mit konfiguriertem Microsoft SharePoint Dokumentbibliothek zum Empfangen von Benachrichtigungen über Aktualisierungen in der Dokumentbibliothek.
Neu Erstellen Microsoft SharePoint Ordner	Erstellt eine neue Microsoft SharePoint Ordner unter einem bestimmten übergeordneten Ordner.
Löschen Microsoft SharePoint Element	Löscht Microsoft SharePoint Dateien und Ordner.
Herunterladen Microsoft SharePoint Datei	Gibt die Download-URL von zurück Microsoft SharePoint Dateien
Dateimetadaten Abrufen	Abonniert und ruft die Änderungen ab Microsoft SharePoint Dokumentbibliothek.
Verschieben Microsoft SharePoint Element	Verschiebt Microsoft SharePoint Dateien/Ordner im Zielordner
Öffnen Microsoft SharePoint Element	Gibt die Web-URL von zurück Microsoft SharePoint Datei/Ordner, die/der in einem Browser geöffnet werden soll.
Laufwerksabonnement Verlängern	Verlängert das Abonnement mit Microsoft SharePoint Dokumentbibliothek.
Erstellen Sie Eine Ordnerstruktur	Folgt den Ordnervorlagenkonfigurationen und erstellt die Ordnerstruktur auf Microsoft SharePoint Dokumentbibliothek.

Microsoft Teams konfigurieren

Konfigurieren Management schwerwiegender Sicherheits-Incidents Mit Microsoft Teams Was bei der Kommunikation über den Chat zur Lösung hilft Major Security Incident.

Konfigurieren und abonnieren von Microsoft Teams Die Chat-Umgebung, das Abrufen von Chat-Konversationen aus den angegebenen Kanälen und das Archivieren des Teams und der zugehörigen Kanäle sind Teil des Incident-Abschlussprozesses. Ein festgelegt Microsoft Teams Umgebung und zugehörige Microsoft Teams Graph Die API-Konfiguration ist erforderlich, um einzelne Kanäle zu erstellen, die spezifisch für sind Major Security Incident.

Um Microsoft Teams zu konfigurieren, aktivieren Sie Teams als Chatanbieter. Sie können dann Chatkanäle für die verschiedenen Stakeholder und Gruppen erstellen, die über Aktivitäten kommunizieren, und Chatkonversationen nachverfolgen, um zu lösen Major Security Incident. Die Konfiguration der Microsoft Teams- und Microsoft Graph-API umfasst:

- Stellen Sie eine ms Teams Graph-Verbindung auf her ServiceNow AI Platform
- Aktivieren Sie MS Teams als Chatanbieter
- Erstellen Sie eine Chat-Kanalvorlage
- Zeigen Sie Die Aktivität Der Chat-Nachricht An

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte mit Microsoft Teams

Überprüfen Sie die folgenden Informationen, bevor Sie mit arbeiten Microsoft Teams Als Connector-Anwendung.

Stellen Sie sicher, dass die folgenden Plugins installiert sind, bevor Sie mit der Einrichtung, Aktivierung und Validierung beginnen Microsoft Teams Richten Sie Verbindungen ein.

Benötigte Plugins

Name	Beschreibung
Chat-Integration mit Security Incident Management	Verwenden **sn_Chat_collab_Core** Plugin-ID, die gesucht und installiert werden soll Microsoft Teams Chat. Durch die Installation dieses Plugins können Sie die Chat-Aktivität für Drittanbieteranwendungen wie Microsoft Teams (oder Slack und andere Drittanbieterchat-Anwendungen) nachverfolgen.
Microsoft Teams Chat Connector für Security Incident Management	Verwenden **sn_ms_Teams_Connector** Plugin-ID zum Suchen und Installieren von Microsoft Teams Chat Connector für das Management schwerwiegender Security Incidents. Durch die Installation dieses Plugins können Sie die Chataktivitäten mithilfe der spezifischen Zusammenarbeitskomponente nachverfolgen Microsoft Teams.
Microsoft Teams Graph-Spoke	Durch die Installation dieses Plugins wird eine Graph-Spoke-Verbindung mit hergestellt Microsoft Teams. Weitere Informationen finden Sie unter Microsoft Teams Graph-Spoke

Aktivieren Sie MS Teams als Chatanbieter

Aktivieren Microsoft Teams Durch Validierung von Microsoft Teams Verbindung.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_admin

Sobald die Verbindung aktiviert und validiert wurde, wird eine Informationsnachricht angezeigt, dass die Anbieterverbindung erfolgreich validiert wurde. Sie können die Kanalkonfiguration ändern, indem Sie Anwender hinzufügen und entfernen und möglicherweise weitere Kanäle hinzufügen oder vorhandene Kanäle umbenennen.

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Konfiguration des Chat-Providers**an.
2. Wählen Sie Aus **Microsoft Teams-Datensatz** .
3. Klicken Sie Auf **Validieren Sie Die Verbindung** .
   Eine Bestätigungsmeldung zeigt an, dass die Provider-Verbindung erfolgreich validiert wurde.
4. Wählen Sie Aus **Aktiv** Kontrollkästchen zum Aktivieren des Anbieterdatensatzes.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Bestätigungsnachricht zeigt an, dass die Anbieterverbindung erfolgreich validiert wurde.

5. **Speichern** Das Formular, nachdem Sie die Konfiguration des Chatanbieters aktiviert haben.
   Mit dieser Verbindung zwischen Microsoft Teams und ServiceNow AI Platform Instanz wurde erfolgreich eingerichtet.

Erstellen Sie eine Chat-Kanalvorlage

Konfigurieren Sie Chatteams und Kanalvorlagen, um Chatteams und Kanäle für die Zusammenarbeit zu erstellen, die Chatkonversationen nachzuverfolgen und diesen Chatkanälen Anwender und Anwendergruppen hinzuzufügen. Diese Kanalvorlagen werden in Microsoft Teams erstellt, wenn ein schwerwiegender Security Incident heraufgestuft wird.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Chat-Kanal** > **Kanalvorlagen**an.
2. Klicken Sie im Formular „Chat-Kanalkonfiguration“ auf **Neu** Im Formularheader.
3. Füllen Sie im Formular die Felder aus.

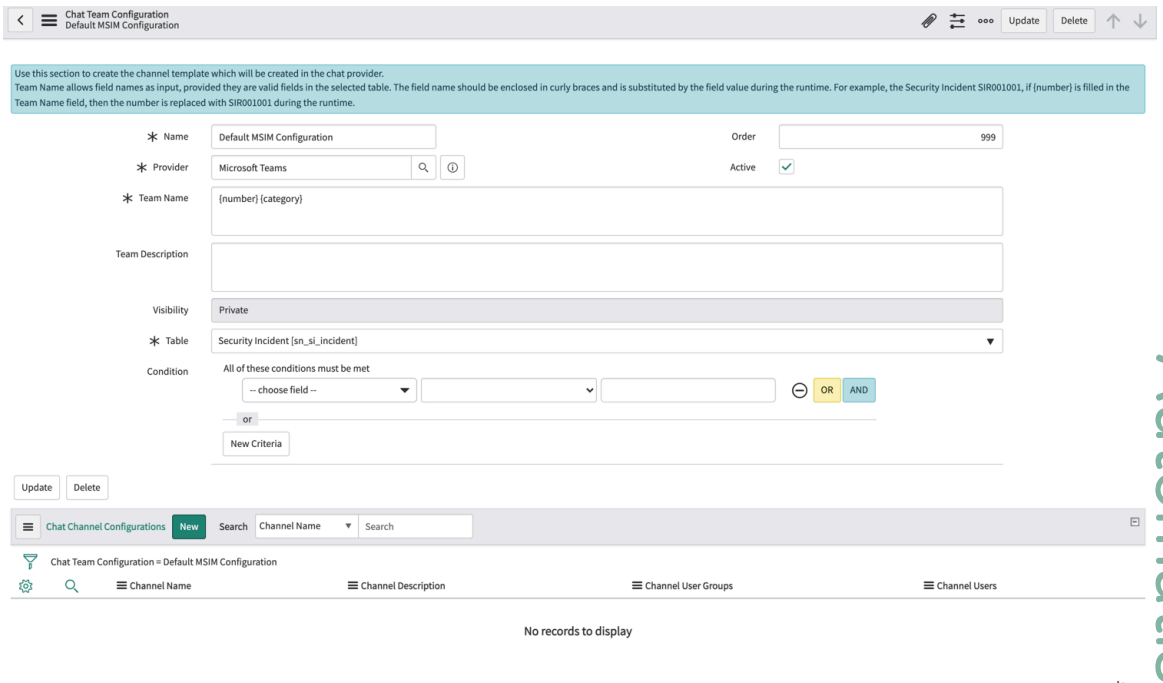
Formular „Chat-Teamkonfiguration“

Feld	Beschreibung
Name	Name des Ordners.
Anbieter	Microsoft Teams.
Teamname	Name für das Team, z. B. im Format {number}-{category}. **Hinweis:** Der hier angegebene Teamname wird für alle Datensätze schwerwiegender Security Incidents verwendet. Um sicherzustellen, dass der tatsächliche Microsoft-Teamname in der MS Teams-Anwendung angezeigt wird und einen eindeutigen Namenswert für verschiedene schwerwiegende Security Incidents aufweist, wird empfohlen, einen eindeutigen Incident-Feldwert zu verwenden, z. B. die Incident-Nummer {number}. Wie im Screenshot-Beispiel gezeigt, würden {number} gefolgt von einem Trennzeichen „-“ und der Feldvariable „{category}“ eine eindeutige Nummer und eine Beschreibung des schwerwiegenden Security Incidents bereitstellen, für den Microsoft Teams erstellt wird, z. B. {number} - {category}.
Teambeschreibung	Optionale Beschreibung des Teams.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tabelle	Schwerwiegender Security Incident (sn_msi_Incident).



4. Klicken Sie auf **Absenden**.
5. Navigieren Sie zum Abschnitt Chatkanalkonfiguration.
6. Klicken **Neu** Dient zum Erstellen einer neuen Chat-Kanalkonfiguration.
7. Geben Sie ein **Konfiguration des Chat-Teams** und **Kanalname**an.

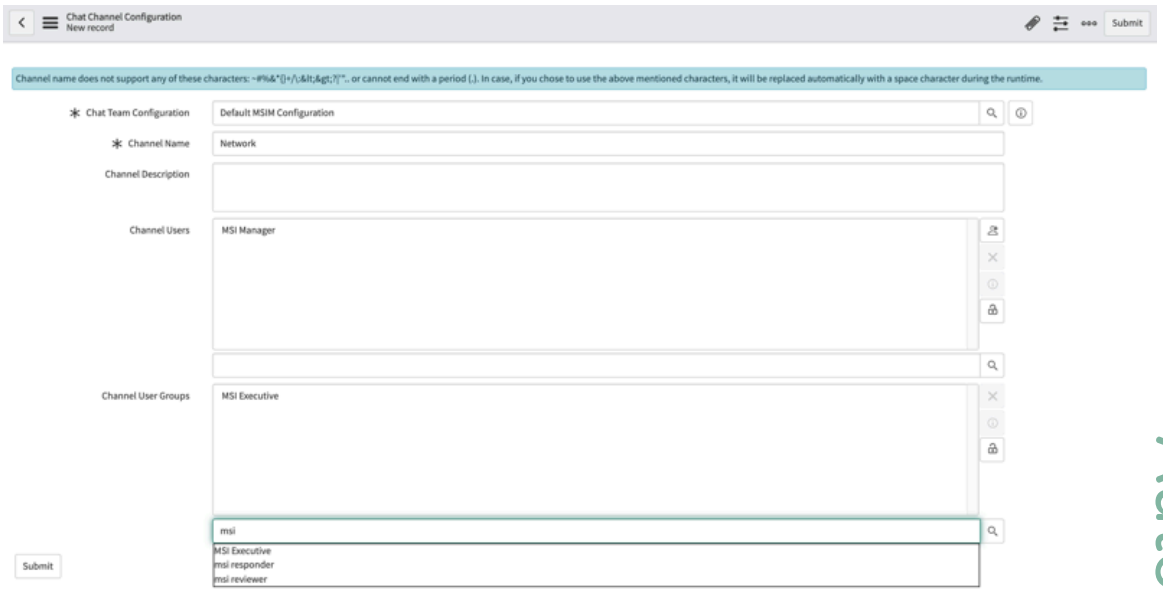
> **Hinweis:**
> Der neue Kanal, den Sie hier erstellt haben, ist auch Ihr Kanalname in Microsoft Teams. Sie können nach demselben Kanal suchen und Ihre Konversationen hinzufügen.

8. Fügen Sie die Systemeigenschaft **Kanalanwender** und **Kanalanwendergruppen** Aus der Suchliste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Absenden Der neue Konfigurationsdatensatz des Chatkanals.



Ergebnisse

Der Chatkanal wird jetzt erstellt, und die Anwender werden diesen Chatkanalgruppen zugewiesen. Sie können die Aktivitäten des Zusammenarbeits-Chats sowohl in anzeigen Microsoft Teams Und im Aktivitätenstrom „Zusammenarbeit“ des MSIM-Arbeitsbereichs mit der Hierarchiestruktur des organisierten Chatkanals, wie in der Konfiguration des Chatkanals-Anbieters konfiguriert.

Zeigen Sie Die Aktivität Der Chat-Nachricht An

Die Aktivität der Chat-Nachricht wird aufgezeichnet und auf der Registerkarte Zusammenarbeit des Arbeitsbereichs „Management schwerwiegender Security Incidents“ angezeigt.

Die Aktivität „Chat-Nachricht“ enthält alle Chat-Konversationen, die zwischen den Teilnehmern und verschiedenen Anwendergruppen stattgefunden haben.

Ms Teams Chat Connector – Problembehandlung für MSIM

Informationen zu geplanten Aufgaben, Systemeigenschaften und Microsoft Teams Flow Designer-Subflows finden Sie im Abschnitt „Fehlerbehebung für Microsoft Teams Chat Connector“.

Überprüfen Sie in jedem Fall, ob der Chat-Connector geplante Aufgaben verarbeitet, wenn die Zusammenarbeits-Chat-Nachrichten nicht in Microsoft Team und im externen Zusammenarbeits-Aktivitätenstrom des MSIM-Arbeitsbereichs veröffentlicht werden.

Geplante Aufgaben für Microsoft Teams

Geplante Aufgaben sind automatisierte Aufgaben, die ausgeführt werden, um die Benachrichtigungen von zu verarbeiten Microsoft Teams Chat-Connector und verlängern Sie die Microsoft Teams-Abonnements nach einem wiederkehrenden Zeitplan.

Erforderliche Rolle: admin.

- **Ms Teams Chat Connector: Prozessbenachrichtigung**

  Für jedes Chat-Nachrichtenereignis wird eine Benachrichtigung empfangen, die die Ressourcen-ID und die Benachrichtigung enthält, die in einer Tabelle gespeichert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sind. Eine geplante Aufgabe wird alle 30 Sekunden ausgeführt, um unverarbeitete Benachrichtigungen auszuwählen und die Microsoft Teams-API abzufragen, um den tatsächlichen Nachrichteninhalt abzurufen, der weiter in einer anderen Tabelle gespeichert wird.

- **Ms Teams Chat Connector: Abonnements verlängern**

  Für jeden Kanal im Team werden Abonnements erstellt, um über die erstellten, aktualisierten und gelöschten Ereignisse benachrichtigt zu werden. Dieses Abonnement ist nur für 60 Minuten aktiv. Die Abonnements werden alle 25 Minuten über den Auftrag Microsoft Teams Connector: Benachrichtigungszeitplan verlängern verlängert.

Microsoft Teams Funktionaler Flow Des Chat-Connectors

Zeigen Sie diesen Abschnitt an, um zu verstehen Microsoft Teams Zugehörige Flow Designer-Subflows, die zum Verwalten der Erstellung von Chatkanälen und des Anwenderzugriffs aus einem schwerwiegenden Security Incident verwendet werden.

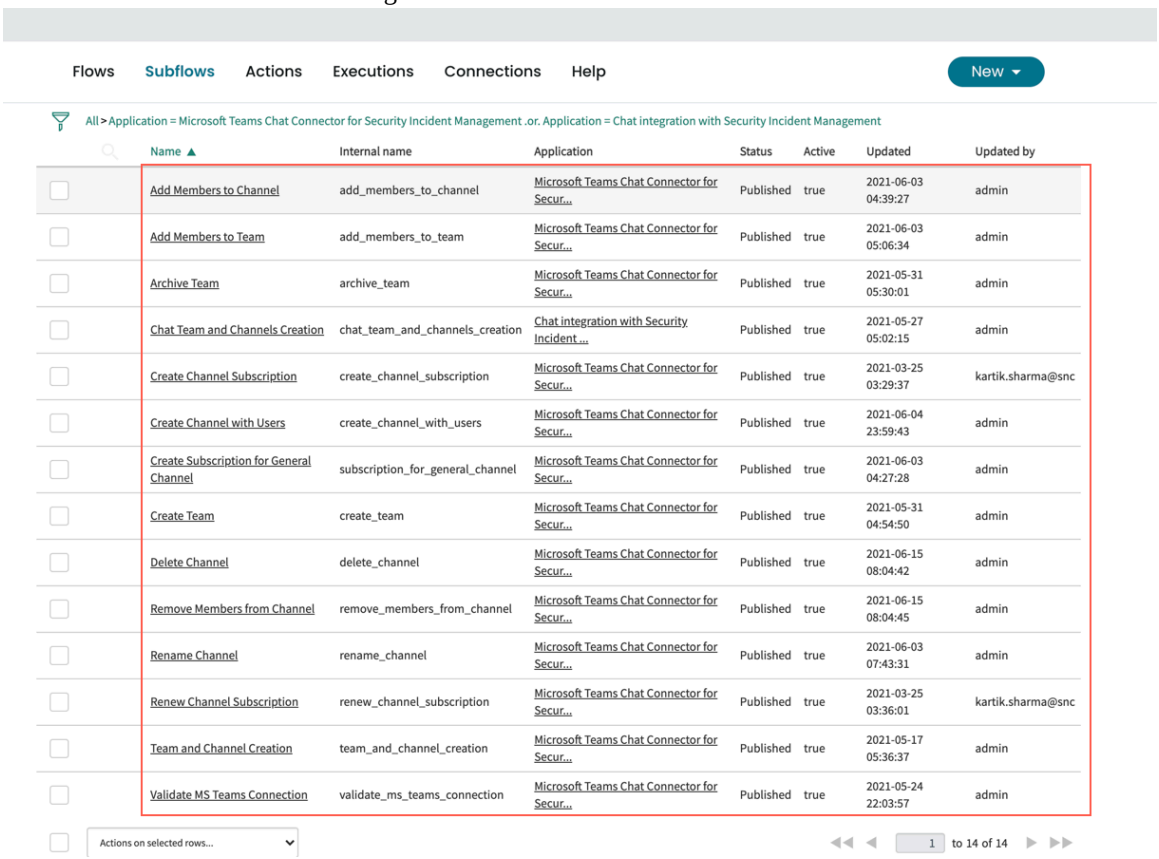
Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Flow Designer**an.
2. Mitglieder zu Kanal hinzufügen
3. Fügen Sie dem Team Mitglieder hinzu
4. Team archivieren
5. Erstellung von Chatteams und Kanälen
6. Erstellen Sie Ein Kanalabonnement
7. Erstellen Sie einen Kanal mit Anwendern
8. Abonnement für allgemeinen Kanal erstellen
9. Team erstellen
10. Kanal löschen
11. Entfernen Sie Mitglieder aus dem Kanal
12. Benennen Sie Den Kanal Um
13. Kanalabonnement Verlängern
14. Team- und Kanalerstellung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

15. Validiert die MS Teams-Verbindung



Konfigurieren Sie den Slack-Chat-Connector für schwerwiegende Security Incidents

Integrieren Sie und arbeiten Sie mit zusammen Slack Zum Lösen eines schwerwiegenden Security Incidents zum Anzeigen und Filtern von Zusammenarbeits-Chat-Aktivitäten.

Konfigurieren und abonnieren von Slack Die Chat-Umgebung, das Abrufen von Chat-Konversationen aus den angegebenen Kanälen und die Archivierung des Slack und der zugehörigen Kanäle sind Teil des Incident-Abschlussprozesses. Ein festgelegt Slack Umgebung und zugehörige Slack Die API-Konfiguration ist erforderlich, um einzelne Kanäle zu erstellen, die spezifisch für sind Major Security Incident.

Um Slack zu konfigurieren, aktivieren Sie Slack als Chatanbieter. Sie können dann Chatkanäle für die verschiedenen Stakeholder und Gruppen erstellen, die über Aktivitäten kommunizieren, und Chatkonversationen nachverfolgen, um zu lösen Major Security Incident. Die Slack Und Slack API-Konfiguration umfasst:

- Erste Schritte mit der Konfiguration des Slack-Chat-Connectors
- Aktivieren Sie Slack als Kanalanbieter
- Erstellen Sie eine Chatkanalvorlage für Slack
- Zeigen Sie Chat-Nachrichtenaktivitäten in Slack an

Erste Schritte mit der Konfiguration des Slack-Chat-Connectors

Überprüfen Sie die folgenden Informationen, bevor Sie mit arbeiten Slack Als Connector-Anwendung.

Stellen Sie sicher, dass die folgenden Plugins installiert sind, bevor Sie mit der Einrichtung, Aktivierung und Validierung beginnen Slack Richten Sie Verbindungen ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benötigte Plugins

Name	Beschreibung
Slack Chat-Connector für Security Incident Management	Verwenden **sn_Slack_Connector** Plugin-ID, die gesucht und installiert werden soll Slack Connector für Management schwerwiegender Security Incidents. Durch die Installation dieses Plugins können Sie die Chataktivitäten mithilfe der spezifischen Zusammenarbeitskomponente nachverfolgen Slack.
Slack-Spoke	Durch die Installation dieses Plugins wird eine Spoke-Verbindung mit hergestellt Slack. Weitere Informationen finden Sie unter Slack Spoke

Erstellen Sie eine Chatkanalvorlage für Slack

Konfigurieren Sie Chatteams und Kanalvorlagen, um Chatteams und Kanäle für die Zusammenarbeit zu erstellen, die Chatkonversationen nachzuverfolgen und diesen Chatkanälen Anwender und Anwendergruppen hinzuzufügen. Diese Kanalvorlagen werden in erstellt Slack Wenn ein schwerwiegender Security Incident heraufgestuft wird.

Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_admin

Warum und wann dieser Vorgang ausgeführt wird
Der neue Kanal, den Sie erstellen, ist Ihr Kanalname in Slack Auch. Sie können nach demselben Kanal suchen und Ihre Konversationen hinzufügen.

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **Chat-Kanal** > **Kanalvorlagen**an.
2. Wählen Sie Aus **Slack-Kanalkonfiguration** Zum Anzeigen der Slack-Konfigurationsdetails.
3. Wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren der Konfiguration des Slack-Chatkanals.
4. Geben Sie im Feld Teamname die MSI-Nummer und den Codenamen an.

   Standardmäßig wird allen Slack-Kanälen die Incident-Nummer vorangestellt. Beispiel: `MSI000000 – {Kanalname}` . Sie können das Präfix in ein beliebiges Feld Ihrer Wahl in diesem Format ändern: `{Field_Name}` .

   Hinweis:
   Der hier angegebene Teamname wird für alle Datensätze schwerwiegender Security Incidents verwendet. Um zu überprüfen, ob tatsächlich ist Slack Wird in angezeigt Slack Anwendung und hat einen eindeutigen Namenswert für verschiedene schwerwiegende Security Incidents. Es wird empfohlen, einen Incident-Feldwert zu verwenden, der eindeutig ist, z. B. `MSI000000 – {Kanalname}` .
5. Klicken Sie mit der rechten Maustaste auf die Konfiguration, und wählen Sie aus **Speichern** .
6. Navigieren Sie zum Abschnitt Chatkanalkonfiguration.
7. Auswahlvorgang **Neu** Dient zum Erstellen einer neuen Chat-Kanalkonfiguration.
8. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wählen Sie **Absenden**.

Ergebnisse

Der Chatkanal wird jetzt erstellt, und die Anwender werden diesen Chatkanalgruppen zugewiesen. Sie können die Aktivitäten des Zusammenarbeits-Chats sowohl in anzeigen Slack Und im Aktivitätenstrom „Zusammenarbeit“ des MSIM-Arbeitsbereichs mit der Hierarchiestruktur des organisierten Chatkanals, wie in der Konfiguration des Chatkanals-Anbieters konfiguriert.

Aktivieren Sie Slack als Kanalanbieter

Aktivieren Slack Durch Validierung von Slack Verbindung.

Vorbereitungen

Erforderliche Rolle:

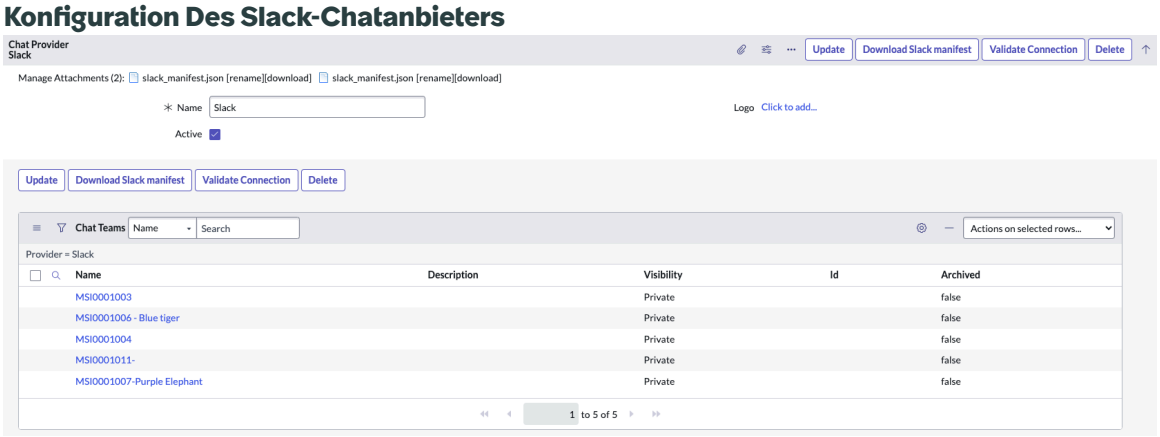
- sn_msi.Workspace_admin – Schreiben
- sn_msi.chat_collab_provider: Lesen

Sobald die Verbindung aktiviert und validiert wurde, wird eine Informationsnachricht angezeigt, dass die Anbieterverbindung erfolgreich validiert wurde. Sie können die Kanalkonfiguration ändern, indem Sie Anwender hinzufügen und entfernen und möglicherweise weitere Kanäle hinzufügen oder vorhandene Kanäle umbenennen.

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **Chat-Kanal** > **Konfiguration des Chat-Providers**an.
2. Wählen Sie Aus **Slack** Zum Öffnen der Konfiguration des Slack-Chatanbieters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie Aus **Laden Sie das Slack-Manifest herunter** Um herunterzuladen Slack_manifest.JSON Datei.
   Die Slack_manifest.JSON Die Datei enthält die vollständige Konfiguration für das Slack-Setup und ermöglicht Ihnen die automatische Konfiguration von Slack. Sie müssen diese JSON-Datei in die Slack-Konfiguration hochladen.
4. Öffnen Sie Slack_manifest.JSON Datei, und führen Sie die folgenden Schritte aus:
   a. Wechseln Sie zu api.slack.com/apps URL in Ihrem Webbrowser.
   b. Wählen Sie Aus **Erstellen Sie Eine Neue App** Aktion.
   c. Wählen Sie im Popup-Fenster „App erstellen“ die Option aus **Aus einem App-Manifest** Option.
   d. Wählen Sie im Popup-Fenster Arbeitsbereich auswählen, um Ihre App zu entwickeln, einen Arbeitsbereich aus der Liste aus, und wählen Sie aus **Als Nächstes** .
   Beispiel: MSIM Slack-Arbeitsbereich.
   e. Wählen Sie im Popup-Fenster „App-Manifest eingeben“ unten die Option aus **JSON** Und kopieren Sie den Code aus der Slack_manifest.JSON Datei.
   f. Wählen Sie **Weiter**.
   g. Wählen Sie im Popup-Fenster Zusammenfassung überprüfen und App erstellen die Option aus **Erstellen** .
   Jetzt wurde Ihre App erstellt.
   h. Wählen Sie auf der Seite „Basisinformationen“ die Option aus **In Arbeitsbereich installieren** .
   Der Slack-Integrations-Bot fordert Ihre Berechtigung für den Zugriff auf den MSIM Slack-Arbeitsbereich an.
   i. Wählen Sie **Genehmigen** aus.
   j. Geben Sie im Abschnitt App-Anmeldeinformationen die Details ein, indem Sie zurück zur ServiceNow-Instanz navigieren.
   k. Auswahlvorgang **Alle** > **Slack-Konfigurationen**an.
   Sie benötigen die Rolle sn_msi.Workspace_admin für diese Aktion.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

l. Wählen Sie ein aus **Signaturgeheimnis** Eigenschaft.

m. Kopieren Sie das Signaturgeheimnis, und fügen Sie es in den Abschnitt „App-Anmeldeinformationen“ von Slack ein.

n. Navigieren Sie in der ServiceNow-Instanz zu **Alle** > **Flow Designer**an.

o. Navigieren zu **Verbindungen** > **Slack** > **Details anzeigen** > **Konfigurieren**an.

p. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Verbindungsname	Name dieser Verbindung. Beispiel: Slack.
Verbindungs-URL	URL dieser Verbindung. Beispiel: https://slack.com
Anmeldeinformationsname	Name der Anmeldeinformationen. Beispiel: Slack-Anmeldeinformationen.
OAuth-Name	Name des OAuth. Beispiel: Slack OAuth.
OAuth-Client-ID	Die Client-ID, die für den Account generiert wurde, den Sie in Slack erstellt haben.
OAuth-Client-Geheimnis	Das geheime Clientgeheimnis für den Account, den Sie in Slack erstellt haben.
OAuth-Umleitungs-URL	Name der OAuth-Umleitungsinstanz. Beispiel: msimslack.service-now.com/oauth_redirect.do

q. Wählen Sie Aus **OAuth-Token konfigurieren und abrufen** .
Der Slack-Integrations-Bot fordert Ihre Berechtigung für den Zugriff auf den MSIM Slack-Arbeitsbereich an.

r. Wählen Sie **Genehmigen** aus.
Das OAuth-Zugriffstoken ist verfügbar und läuft am <YYYY-MM-DD> <HH:MM:SS> ab.

5. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **Chat-Kanal** > **Konfiguration des Chat-Providers**an.
6. Wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren des Chatanbieterdatensatzes.
7. Wählen Sie Aus **Validieren Sie Die Verbindung** Um die Verbindung zu testen.
Eine Bestätigungsnachricht zeigt an, dass die Anbieterverbindung erfolgreich validiert wurde.
8. Klicken Sie mit der rechten Maustaste auf den Datensatz, und wählen Sie aus **Speichern** .
Danach die Verbindung zwischen Slack und ServiceNow AI Platform Instanz wurde erfolgreich eingerichtet.
9. Navigieren zu **api.slack.com/apps** > **Features** > **OAuth und Berechtigungen**an.

a. Überprüfen Sie, ob alle Umfänge korrekt sind.

b. Navigieren zu **Features** > **Ereignisabonnements**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie im Feld Anforderungs-URL die Option aus **Wiederholen Sie Den Vorgang** .
Sie können eine verifizierte Nachricht sehen.

d. Wählen Sie **Speichern**.

Zeigen Sie Chat-Nachrichtenaktivitäten in Slack an

Die Aktivität der Chat-Nachricht wird aufgezeichnet und auf der Registerkarte Zusammenarbeit des Arbeitsbereichs „Management schwerwiegender Security Incidents“ angezeigt.

Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Aktivität „Chat-Nachricht“ enthält alle Chat-Konversationen, die zwischen den Teilnehmern und verschiedenen Anwendergruppen stattgefunden haben. Weitere Informationen finden Sie unter Verwalten Sie die Kommunikation von Chatkanälen mit Slack.

Management schwerwiegender Sicherheits-Incidents – Administration

Planen und konfigurieren Sie Ihre Management schwerwiegender Sicherheits-Incidents-Implementierung.

Sie können die folgenden Aspekte von konfigurieren Management schwerwiegender Sicherheits-Incidents Verwaltung:

Aktivieren Sie Vorschlag, Heraufstufung und Verknüpfung schwerwiegender Security Incidents

Ermöglichen Sie Anwendern die Entscheidung, Incidents als schwerwiegende Security Incidents vorzuschlagen oder heraufzustufen. Verfolgen Sie einfach alle Incidents im Zusammenhang mit einem schwerwiegenden Security Incident, indem Sie zulassen, dass Security Incidents mit dem übergeordneten oder untergeordneten Incident verknüpft werden.

Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**an.
2. Ermöglichen Sie Anwendern, einen Security Incident für einen schwerwiegenden Security Incident vorzuschlagen, indem Sie auswählen **Schwerwiegenden Security Incident Vorschlagen** Kontrollkästchen im Abschnitt SIR/VR-Arbeitsbereichsaktionen.
3. Ermöglichen Sie Anwendern, einen Security Incident zu einem schwerwiegenden Security Incident hochzustufen, indem Sie auswählen **Zu schwerwiegendem Security Incident heraufstufen** Kontrollkästchen.
4. Aktivieren Sie die Verknüpfung eines Security Incidents mit einem schwerwiegenden Security Incident, damit sie gemeinsam nachverfolgt werden können, indem Sie auswählen **Link zu schwerwiegendem Security Incident** Kontrollkästchen.
5. Wählen Sie **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Markieren Sie Security Incidents als schwerwiegende Security Incidents

Kennzeichnen Sie die Security Incidents oder angreifbaren Datensätze als schwerwiegenden Security Incident, wenn der Incident vorgeschlagen oder heraufgestuft wird. Wenn ein Security Incident vorgeschlagen wird, wird der Incident-Datensatz als Kandidat für schwerwiegenden Security Incident bezeichnet. Wenn eine Sicherheit heraufgestuft wird, wird der Incident-Datensatz als schwerwiegender Security Incident mit dem Status akzeptiert bezeichnet.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**an.
2. Aktivieren **Bezeichnungen Anzeigen** Aktivieren Sie das Kontrollkästchen, um den vorgeschlagenen Incident-Kandidaten als schwerwiegenden Security Incident zu bezeichnen, indem Sie auswählen **Bezeichnungsname: Als Kandidat Vorschlagen** Suchen Sie das Feld, und wählen Sie Kandidat für schwerwiegenden Security Incident im aus **SIR/VR-Arbeitsbereichsbezeichnungen** Abschnitt.
3. Aktivieren **Bezeichnungen Anzeigen** Aktivieren Sie das Kontrollkästchen, um den heraufgestuften Incident-Kandidaten als schwerwiegenden Security Incident zu bezeichnen, indem Sie auswählen **Bezeichnungsname: Heraufstufung zu schwerwiegendem Security Incident** Suchen Sie das Feld , und wählen Sie schwerwiegender Security Incident im aus **SIR/VR-Arbeitsbereichsbezeichnungen** Abschnitt.
4. Wählen Sie **Aktualisieren**.

Konfigurieren Sie Bezeichnungen für schwerwiegende Security Incidents

Konfigurieren Sie Bezeichnungen im Management schwerwiegender Security Incidents, um anwenderdefinierte Bezeichnungen zu erstellen und die externen Zusammenarbeitsaktivitäten und -Aufgaben im Aktivitätenstrom zu filtern. Die verschiedenen Arten implementierter Bezeichnungen sind Status- und Zeitleistenbezeichnungen.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**an.
2. Aktivieren **Bezeichnungen Anzeigen** Kontrollkästchen zum Aktivieren der Kennzeichnung verschiedener Incident-status wie „Analyse“, „Eindämmen“, „Beseitigen“, „Wiederherstellen“, „Überprüfen“, Zeitleistenereignis in **MSIM-Arbeitsbereichsbezeichnungen (Anzeige in Zusammenarbeitsaktivitäten und -Aufgaben)** Abschnitt.
3. Wählen Sie **Aktualisieren**.

Konfigurieren Sie Bezeichnungen für schwerwiegende Security Incidents

Konfigurieren Sie verschiedene Arten von Bezeichnungen, um die Incident-status besser zu filtern und anzuzeigen. Bezeichnungen für schwerwiegende Security Incidents bieten die Flexibilität, die Zusammenarbeitsaktivitäten und -Aufgaben der Incident-Datensätze zu bezeichnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_admin

Sie können die Bezeichnungen über das Bezeichnungssymbol auswählen oder deaktivieren, das im Abschnitt „Aktivitätenstrom“ des Abschnitts „Zusammenarbeits- und Aufgabenorganisator“ des MSIM-Arbeitsbereichs verfügbar ist.

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **MSI-Bezeichnungen**an.
2. Klicken Sie Auf **Neu** Um eine neue Bezeichnung zu erstellen.
3. Füllen Sie das Formular mit aus **Bezeichnungsname** Und **Bezeichnungsfarbe** .
4. Klicken Sie Auf **Bezeichnung Erstellen** .
5. Als Teil des Basissystems sind im Folgenden die konfigurierten Bezeichnungen für jeden Incident-Status aufgeführt, und Sie können den Bezeichnungsnamen oder die Farbe nicht ändern:
   - Analyse
   - Beinhalten
   - Beseitigen
   - Prüfung
   - Wiederherstellen
   - Zeitleistenereignis

   Hinweis:
   Sie können die anwenderdefinierten Bezeichnungen und ihre Eigenschaften ändern.

Konfigurieren Sie Zeitleistenkategorien für schwerwiegende Security Incidents

Konfigurieren und weisen Sie Ihren schwerwiegenden Security Incidents Zeitleistenkategorien wie Bedrohung, Antwort oder Anwenderdefiniert zu, indem Sie den Abschnitt Zeitleiste auf der Registerkarte Übersicht verwenden.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Zeitleistenkategorien**an.
   Die folgenden Zeitleistenkategorien werden als Teil des Basissystems bereitgestellt:
   - **Anwenderdefiniert** .
   - **Antwort** .
   - **Bedrohung** .
2. Führen Sie die folgenden Schritte aus, um eine vorhandene Zeitleisten-Ereigniskategorie zu ändern:
   a. Wählen Sie eine Ereigniskategorie der Zeitleiste aus der Liste aus.
   b. Sie können den Namen der Ereigniskategorie der Zeitleiste ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Sie können die Ereignisfarbe ändern und eine andere Farbe für Ihre Ereigniskategorie der Zeitleiste auswählen.

d. Wählen Sie **Aktualisieren**.

3. Führen Sie die folgenden Schritte aus, um eine neue Ereigniskategorie der Zeitleiste zu erstellen:

a. Wählen Sie **Neu**.

b. Geben Sie im Feld Name einen Namen für die Ereigniskategorie Zeitleiste ein.

c. Wählen Sie im Feld Ereignisfarbe mithilfe der Dropdown-Liste eine Farbe für die Ereigniszeitleistenkategorie aus.

d. Wählen Sie **Absenden**.

Legen Sie Benachrichtigungseinstellungen für fest MSIM

Automatisieren Sie den E-Mail-Benachrichtigungsprozess, und benachrichtigen Sie die Anwender, wenn ein Security Incident entweder vorgeschlagen oder zu einem Kandidaten für schwerwiegenden Security Incident heraufgestuft wird.

Erforderliche Rolle: sn_msi.Workspace_admin.

Die Benachrichtigungen werden nur ausgelöst, wenn ein Security Incident vorgeschlagen und an alle Anwender und Gruppen gesendet wird, die für die Benachrichtigungsliste konfiguriert sind. Standardmäßig wird die E-Mail-Benachrichtigung von dem Anwender empfangen, der den Security Incident als Kandidaten für schwerwiegenden Security Incident vorgeschlagen hat.

Benachrichtigung: Security Incident vorgeschlagen (SI) als schwerwiegender Security Incident (MSI)

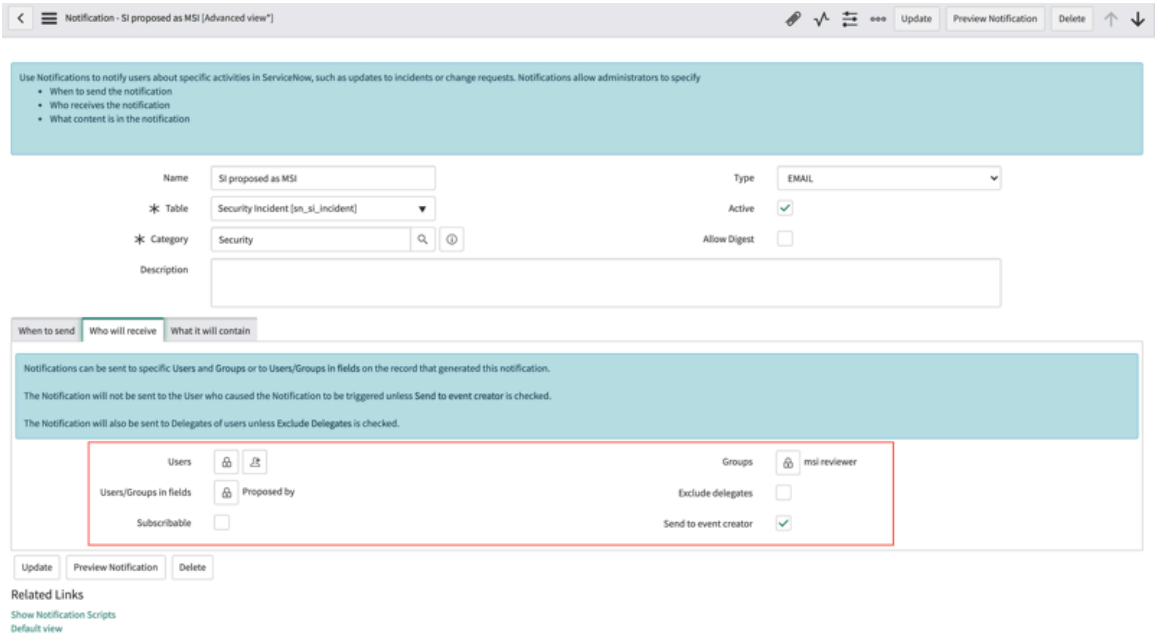
Wer erhält:

- Standardmäßig **MSI-Prüfer** Der Gruppenname wird erstellt, und jeder Anwender, der dieser Gruppe hinzugefügt wird, hat die Berechtigung, ein zu sein **MSIM-Manager** Und die Anwender, die dieser Gruppe angehören, erhalten die Benachrichtigungs-E-Mails.
- Jeder bestimmte Anwender, der zu hinzugefügt wird **Anwender** Die Liste erhält auch die Benachrichtigungs-E-Mails.

Inhalt:

Wenn Sie den E-Mail-Inhalt ändern möchten, z. B. den Text der E-Mail, der den Betreff oder die Nachrichten-HTML enthält, müssen Sie über die Systemadministrator-Rolle verfügen oder als Systemadministrator und nicht als MSI-Administrator zugewiesen sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Benachrichtigung: Security Incident als schwerwiegender Security Incident (MSI) heraufgestuft

Diese Benachrichtigung wird ausgelöst, wenn ein Security Incident heraufgestuft wird und wenn der Datei-Explorer und verwendet wird Microsoft Teams Basisstruktur wird erstellt. Standardmäßig wird diese Benachrichtigung von dem Anwender empfangen, der den Security Incident zu einem schwerwiegenden Security Incident heraufgestuft hat.

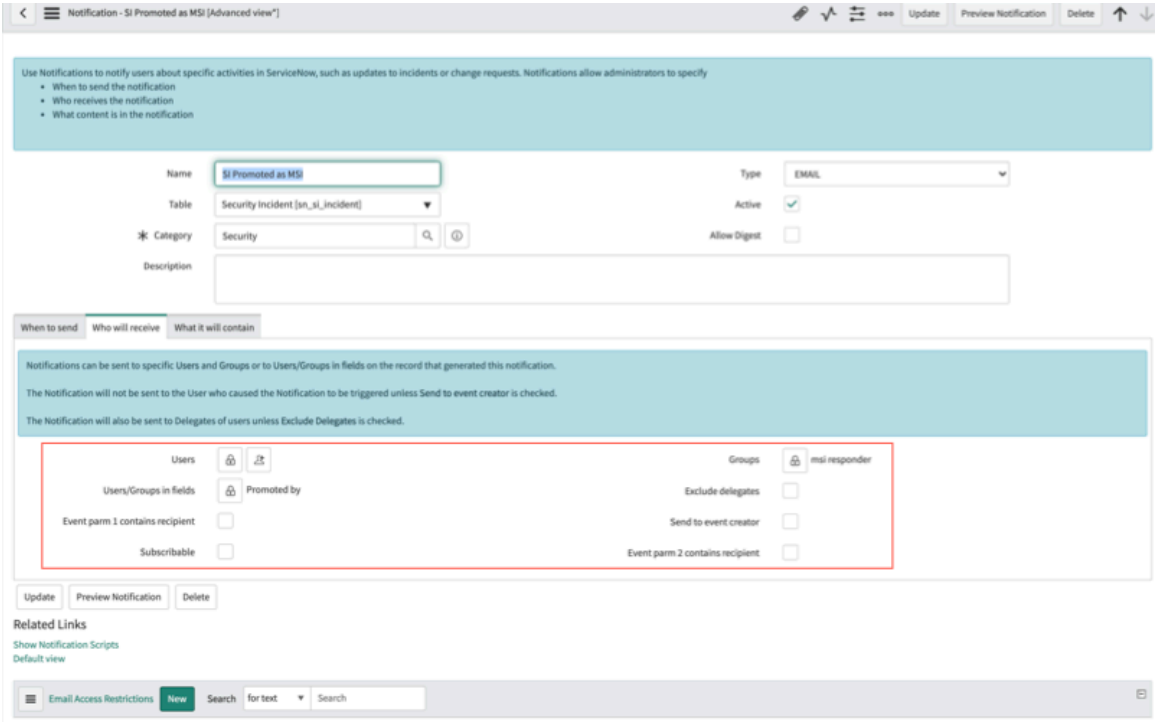
Empfänger

- Standardmäßig A **Gruppe** Nach Name **MSI-Beantworter** Wird erstellt, und jeder Anwender, der dieser Gruppe hinzugefügt wird, hat die Berechtigung **MSIM-Beantworter** Die Rolle und alle Anwender, die dieser Gruppe angehören, erhalten die Benachrichtigungs-E-Mail.
- Jeder bestimmte Anwender, der zu hinzugefügt wird **Anwender** Die Liste erhält auch die Benachrichtigungs-E-Mails.

Was wird enthalten

Wenn Sie den E-Mail-Inhalt ändern möchten, z. B. den Text der E-Mail, der den Betreff oder die Nachrichten-HTML enthält, müssen Sie über die Systemadministrator-Rolle verfügen oder als Systemadministrator und nicht als MSI-Administrator zugewiesen sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Konfigurieren Sie MSI-Abschlussaktivitäten

Legen Sie Aktionen fest, die automatisch ausgeführt werden, wenn ein schwerwiegender Security Incident geschlossen wird. Erhöhen Sie die Sicherheit, indem Sie den Zugriff auf Ordner mit Lösungsinformationen automatisch archivieren und entfernen.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Konfigurationen**an.
2. Archivieren Sie Chatkommunikation im Zusammenhang mit der Lösung des Incident, indem Sie auswählen **Archivieren Sie Zusammenarbeitskanäle** Kontrollkästchen im Abschnitt automatisierte Abschlussaktionen.
3. Entfernen Sie Ordner, die Material im Zusammenhang mit der Lösung des Incident enthalten, indem Sie auswählen **Entfernen Sie Zusammenarbeitsordner** Kontrollkästchen.
4. Wählen Sie **Aktualisieren**.

Management schwerwiegender Sicherheits-Incidents-Arbeitsbereich

Management schwerwiegender Sicherheits-Incidents Bietet einen dedizierten Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents, die speziell für den konzipiert sind Major Security Incident manager.

Arbeiten Sie einfach an Aktivitäten zusammen, die zur Lösung schwerwiegender Security Incidents beitragen, indem Sie Dateien und Ordner freigeben und anzeigen, Incident-Aufgaben anzeigen und aktualisieren, und kommunizieren Sie über dedizierte Chatkanäle mit denjenigen, die an dem Incident arbeiten.

Management schwerwiegender Security Incidents (MSIM) bietet einen Mechanismus zum Nachverfolgen und Lösen schwerwiegender Security Incidents. MSIM funktioniert in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbindung mit den vorhandenen Produktfunktionen für Security Incidents und Vulnerability Response und verbessert den Korrekturprozess für schwerwiegende Security Incidents mit den folgenden Funktionen:

- Dedizierter Arbeitsbereich für die Verwaltung schwerwiegender Security Incidents, der speziell für die Anwenderrolle „Manager für schwerwiegende Security Incidents“ konzipiert ist.
- Organisieren Sie Aufgaben zur Reaktion auf schwerwiegende Security Incidents, einschließlich Aufgaben, die für verknüpfte Security Incidents und Schwachstellengruppen nachverfolgt werden.
- Automatisieren Sie die Erstellung von Zusammenarbeitsordnern und Chatkommunikationskanälen, sobald ein schwerwiegender Security Incident erstellt wurde, sowie die Archivierung im Rahmen des Incident-Abschlusses.
- Datei-Explorer-Komponente zum Organisieren und Nachverfolgen der Sammlung von Artefakten (Dateien) im Zusammenhang mit dem schwerwiegenden Security Incident über einen Microsoft SharePoint Integration.
- Komponenten des Chatkanalmanagers und des Aktivitätenstroms zur Verwaltung der Kommunikation in mehreren Sicherheits-, IT- und Funktionsgruppen über einen Microsoft Teams Integration.
- Zusammenfassungsberichte über Auswirkungs- und Fortschrittsmetriken für schwerwiegende Security Incidents, einschließlich Rollup betroffener Assets, Anwender, Standorte und Teamressourcen sowie Zeitleiste wichtiger Incident-Meilensteine.

Verwenden Sie den MSIM-Arbeitsbereich, um schwerwiegende Security Incidents nachzuverfolgen und zu lösen:

1. Zeigen Sie die Trenddiagramme und den Fortschritt des schwerwiegenden Security Incidents an.
2. Verfolgen und organisieren Sie Microsoft SharePoint-Dateiaktivitäten über den MSIM-Arbeitsbereich.
3. Verfolgen und organisieren Sie Microsoft Teams-Chataktivitäten über den MSIM-Arbeitsbereich.
4. Zeigen Sie Incident-Details über den MSIM-Arbeitsbereich an, und aktualisieren Sie sie.
5. Filtern Sie Zusammenarbeitsaktivitäten im Aktivitätenstrom des MSIM-Arbeitsbereichs.

Management schwerwiegender Sicherheits-Incidents verwenden

Manager können verwenden Management schwerwiegender Sicherheits-Incidents Arbeitsbereich zum Anzeigen der vorgeschlagenen, heraufgestuften, verknüpften und abgelehnten Incident-Datensätze und zum Nachverfolgen der zugehörigen Aktivitäten.

Incident-Datensätze vorschlagen, heraufstufen und verknüpfen

Schlagen Sie Security Incidents als schwerwiegende Security Incidents vor, wenn Incidents als kritische Bedrohung für die Organisation identifiziert werden.

Sobald das Management schwerwiegender Security Incidents auf Ihrem installiert ist ServiceNow Instanz können Sie den Übergang von Security Incidents zu schwerwiegenden Incidents wie folgt behandeln:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Schlagen Sie dem Kandidaten für einen schwerwiegenden Security Incident einen Security Incident vor, um einen Überprüfungsprozess zu initiieren.
- Einen Security Incident ohne Überprüfungsprozess direkt zu einem schwerwiegenden Security Incident heraufstufen.
- Lehnen Sie einen Security Incident ab, der als schwerwiegender Security Incident vorgeschlagen wird.

Sie können einen Security Incident auch als untergeordneten Incident mit dem schwerwiegenden Security Incident verknüpfen, sodass alle zugehörigen Security Incidents gemeinsam nachverfolgt werden können.

Als vorschlagen Major Security Incident

Schlagen Sie einem schwerwiegenden Security Incident einen Security Incident vor.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Listen**an.
2. Wählen Sie den Security Incident in der zugehörigen Kategorie aus, den Sie als schwerwiegenden Security Incident vorschlagen möchten.
3. Wählen Sie aus **Weitere Aktionen** Symbol und wählen Sie aus **Als schwerwiegenden Security Incident vorschlagen** .
4. Füllen Sie die Felder im Dialogfeld als schwerwiegenden Security Incident vorschlagen aus.
   a. **Erkennungsdatum** : Datum, an dem der schwerwiegende Security Incident erstmals erstellt oder vorgeschlagen wurde.
   b. **Begründung** : Geben Sie die Begründung für den Vorschlag des Incident an.
   c. **Potenzielle Auswirkung** : Geben Sie die Auswirkung des Incident an.
5. Wählen Sie Aus **Vorschlagen** .

Ergebnisse

Der Incident wird vorgeschlagen, und die folgenden Aktionen werden ausgeführt:

- Im Security Incident-Datensatz wird eine Verifizierungsbanner-Nachricht angezeigt, und das definierte Tag „schwerwiegender Security Incident“ wird angezeigt.
- Der Datensatz wird in der zugehörigen Liste schwerwiegender Security Incident im Incident-Datensatz mit dem Status „Vorgeschlagen“ und in der Liste der MSIM-Arbeitsbereichskandidaten angezeigt.
- Der Abschnitt „Aktivität“ im MSIM-Arbeitsbereich zeigt, dass der Security Incident als schwerwiegender Security Incident heraufgestuft werden soll.
- Eine Nachricht wird an diejenigen in der definierten Benachrichtigungsliste gesendet, die einen Link zum Incident-Datensatz und zur Registerkarte Details für den Incident enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zu heraufstufen Major Security Incident

Einen Security Incident zu einem schwerwiegenden Security Incident heraufstufen oder heraufgestufte Vorschläge über ablehnen Management schwerwiegender Sicherheits-Incidents(MSIM)-Arbeitsbereich.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response** > **Security Incidents** > **Listen**an.
2. Wählen Sie den Security Incident in der zugehörigen Kategorie aus, den Sie als schwerwiegenden Security Incident heraufstufen möchten.
   Überprüfen Sie die Details des Security Incidents im Abschnitt „Details“, oder zeigen Sie erweiterte Details im Incident-Datensatz auf einer separaten Registerkarte an, indem Sie auf klicken **Zeigen Sie weitere Details an** .
3. Wählen Sie aus **Weitere Aktionen** Symbol und wählen Sie aus **Zu schwerwiegendem Security Incident heraufstufen** .
4. Füllen Sie die Felder im Dialogfeld schwerwiegenden Security Incident heraufstufen aus.

   a. **Erkennungsdatum** : Datum, an dem der schwerwiegende Security Incident erstmals erstellt oder vorgeschlagen wurde.

   b. **Geschätztes Lösungsdatum** : Das geschätzte Lösungsdatum, bis zu dem der schwerwiegende Security Incident voraussichtlich gelöst wird.

   c. **Codename** : Wählen Sie den Codenamen für den schwerwiegenden Security Incident aus.
   Beispiel: Blue Tiger.

   d. **Kategorie** : Wählen Sie die Kategorie für den schwerwiegenden Security Incident aus.
   Beispiel: Fehlkonfiguration.

   e. **Begründung** : Geben Sie die Begründung für den Vorschlag des Incident an.

   f. **Potenzielle Auswirkung** : Geben Sie die Auswirkung des Incident an.

5. Wählen Sie Aus **Vorschlagen** .
6. Heben Sie den Security Incident entweder hoch, oder lehnen Sie den Heraufstufungsvorschlag ab.
   - Klicken Sie auf, um den Incident hochzustufen **Zu schwerwiegendem Security Incident heraufstufen** .
   - Klicken Sie auf, um den Heraufstufungsvorschlag abzulehnen **Als schwerwiegenden Security Incident ablehnen** .
7. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

- Wenn Sie den Heraufstufungsvorschlag abgelehnt haben, wird der Incident nicht heraufgestuft, und der Incident-Eintrag wird auf die Registerkarte abgelehnt verschoben.
- Wenn Sie den Incident heraufgestuft haben, wird der Incident-Eintrag auf die Registerkarte Öffnen verschoben, und im Sicherheitsdatensatz wird ein Tag angezeigt, das angibt, dass es sich um einen schwerwiegenden Security Incident handelt.
- Die Entscheidung wird im Abschnitt „Aktivität“ des MSIM-Arbeitsbereichs aufgeführt.

Sobald ein Incident heraufgestuft wurde, wird die Standardkonfiguration angewendet.

- Eine Ordnerstruktur wird basierend auf der Ordnervorlagenkonfiguration erstellt.
- Chatkanäle werden basierend auf der Kanalkonfiguration erstellt.
- Eine E-Mail-Nachricht wird an die festgelegten Anwender gesendet. Die Standardbenachrichtigung enthält einen Link zum schwerwiegenden Security Incident und Details zum Incident. Die designierten Anwender haben jetzt auch Zugriff auf die Zusammenarbeitsressourcen. Daher enthält die Benachrichtigung auch den Microsoft Team-Namen und einen Link zu Microsoft SharePoint-Ordnern im Zusammenhang mit dem Incident.

Verknüpfen mit Major Security Incident

Verknüpfen Sie Security Incidents mit einem schwerwiegenden Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_admin

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident in der zugehörigen Kategorie aus, den Sie mit dem schwerwiegenden Security Incident verknüpfen möchten.
3. Wählen Sie aus **Zusätzliche Aktionen** Symbol und wählen Sie aus **Link zu schwerwiegendem Security Incident** .
4. Wählen Sie den schwerwiegenden Security Incident aus, mit dem Sie verknüpfen möchten.
   a. Wählen Sie im Dialogfeld das Symbol mit der Liste suchen.
   b. Wählen Sie den schwerwiegenden Security Incident aus, mit dem Sie verknüpfen möchten.
   c. Wählen Sie **OK**.
5. Wählen Sie Aus **Vorschlagen** .

Ergebnisse

Der Vorschlag wird übermittelt, und die folgenden Aktionen werden ausgeführt:

- Im Security Incident-Datensatz wird eine Verifizierungsbanner-Nachricht angezeigt, und das definierte Tag „schwerwiegender Security Incident“ wird neben angezeigt **Wählen Sie das Sicherheits-Tag aus** Feld.
- In **Details** Registerkarte für den schwerwiegenden Security Incident in Management schwerwiegender Sicherheits-Incidents, Die Dropdown-Liste „Datensatznummer“ enthält beide Incidents.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Datensatz wird in der zugehörigen Liste schwerwiegender Security Incident des Incident-Datensatzes mit dem Status „Vorgeschlagen“ angezeigt.
- Eine Nachricht wird an diejenigen in der definierten Benachrichtigungsliste gesendet, die einen Link zum Incident-Datensatz und zur Registerkarte Details für den Incident enthält.
- Die **Aktivität** Im Abschnitt im MSIM-Arbeitsbereich wird angezeigt, dass der Security Incident dem schwerwiegenden Security Incident als untergeordneter Security Incident mit einem Link hinzugefügt wurde.

Verwenden der MSI-Listenansicht im MSIM-Arbeitsbereich

Mit der Listenansicht im MSIM-Arbeitsbereich können Sie vorgeschlagene, heraufgestufte und abgelehnte schwerwiegende Security Incidents anzeigen.

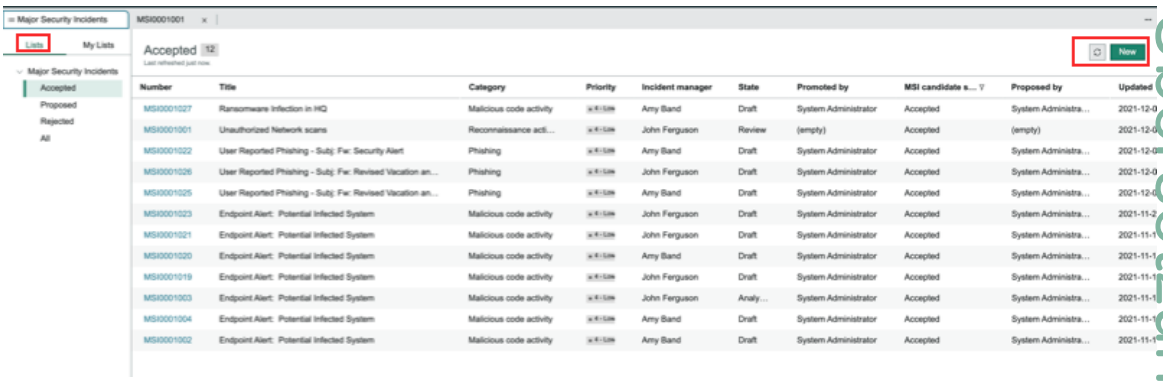
Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

Sie können auch neue Incidents mit erstellen **Neu** Schaltfläche, die in der oberen rechten Ecke des Arbeitsbereichs verfügbar ist.

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSIM-Arbeitsbereich**an.
2. Wählen Sie die Registerkarte Listen aus, um die Listenansicht anzuzeigen.



3. Wählen Sie Aus **Meine Listen** Um eine eigene Liste schwerwiegender Security Incidents zu erstellen.
4. In der folgenden Tabelle finden Sie, was Sie in der Listenansicht tun können:

Aufgabe	Beschreibung
Meine Listen	Erstellen Sie neue MSI-Datensatzlisten, und zeigen Sie die von Ihnen erstellten Listen an.
Legen Sie Filter für eine Spalte in einer Liste fest	Wählen Sie eine Spalte aus, und erweitern Sie das Menü „vertikale Punkte“, um Optionen anzuzeigen, die die Daten in der Spalte weiter filtern.
Filtern Sie Elemente aus einer Zeile in einer Spalte heraus, oder gleichen Sie Elemente ab	Wählen Sie eine Zelle in einer Spalte aus, und verfeinern Sie die angezeigten Daten, indem Sie eine auswählen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	○ Übereinstimmung anzeigen: Zeigen Sie nur Elemente an, die dem ausgewählten Element in der Spalte entsprechen. ○ Herausfiltern: Filtert die Elemente aus der Spalte heraus, die dem ausgewählten Element in der entsprechenden Spalte entsprechen.
Liste neu laden	Aktualisieren Sie die Listen, und zeigen Sie die vollständigen Listen an, die aktualisiert wurden.
Neu	Erstellen Sie einen neuen MSI-Datensatz.

Anzeigen Major Security Incident Auswirkungsmetriken

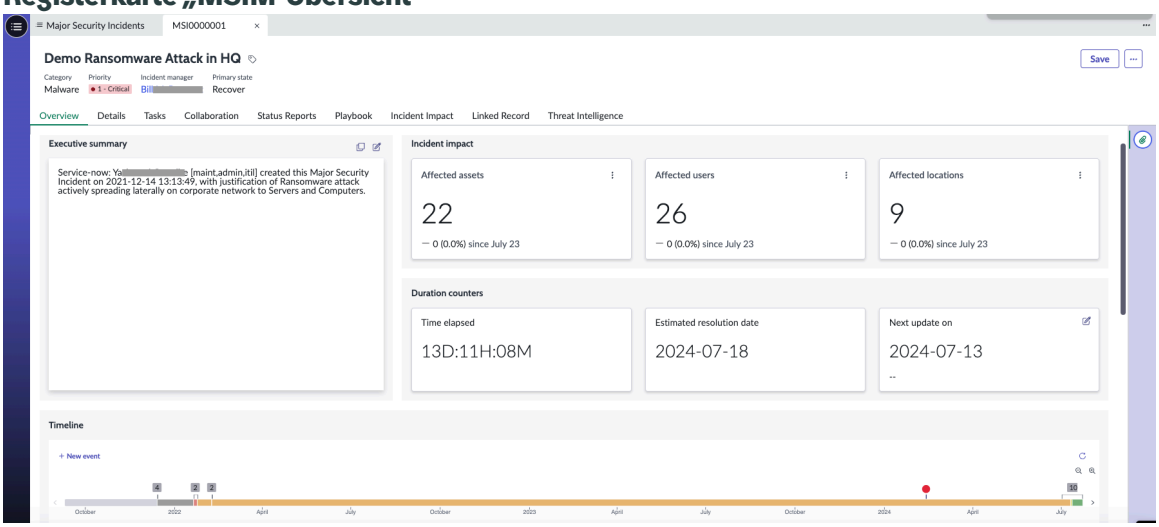
Bietet aktuelle Zusammenfassungsberichte über die Auswirkungen und den Fortschritt schwerwiegender Security Incidents, was ein wichtiger Aspekt bei der Verwaltung schwerwiegender Security Incidents mithilfe des neuen Arbeitsbereichs ist.

Die **Übersicht** Die Registerkarte enthält die relevanten Metriken zum Verwalten des Umfangs und Fortschritts des Incident, einschließlich eines Rollups betroffener Assets, Anwender, Standorte und Teamressourcen sowie der Zeitleiste wichtiger Incident-Meilensteine.

Die Zeitleiste bietet eine horizontale Ansicht wichtiger Ereignisse und Meilensteine, die im Rahmen der spezifischen Lösung schwerwiegender Security Incidents aufgetreten sind. Die Zeitleistenkomponente wird oben auf allen Registerkarten des Arbeitsbereichs „Management schwerwiegender Security Incidents“ angezeigt, mit der Möglichkeit, sie zur Anzeige nach Bedarf zu reduzieren und zu erweitern. Die dargestellten Ereignisdaten werden aktualisiert und aktualisiert, wenn festgelegte Meilensteinereignisse oder Meilensteine hinzugefügt oder aktualisiert werden.

Jedes Ereignis oder Meilenstein wird mit einer anderen Zeitleistenereignistypoption angezeigt, um die Anzahl und den Typ der Ereignisse oder Meilensteine zu identifizieren. Zum Beispiel NOW-Datensatzaktualisierungen, Zusammenarbeitsaktivitäten. Darüber hinaus wird der Zeitraum für die verschiedenen status schwerwiegender Security Incidents automatisch nachverfolgt und in farbcodierten Bereichen angezeigt, die zusammen mit der Dauer der einzelnen Incident-Status angezeigt werden.

Registerkarte „MSIM-Übersicht“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kurzzusammenfassung und Auswirkung auf Incidents

Aufgabe	Beschreibung
Kurzübersicht	Eine kurze Zusammenfassung des schwerwiegenden Security Incidents mit Anwendernamen, Anwenderrolle und Zeitstempeldetails. • Sie können die Zusammenfassung ändern, indem Sie auswählen **Bearbeiten** Symbol. Nachdem Sie die erforderlichen Änderungen vorgenommen haben, wählen Sie aus **Aktualisieren** Option. • Um die Kurzzusammenfassung zu kopieren und in einen schwerwiegenden Security Incident einzufügen, wählen Sie aus **Kopieren** Symbol und fügen Sie die Zusammenfassung in den erforderlichen schwerwiegenden Security Incident ein.
Incident Impact	Diese Komponenten zeigen die betroffenen Ressourcen basierend auf einem Rollup aller aktiven Aufgaben und verknüpften Incidents mit identifizierten Assets, Anwendern, Standorten und zugewiesenen Teammitgliedern an. Die betroffenen Ressourcen sind: • **Betroffene Assets** • **Betroffene Anwender** • **Betroffene Standorte** Wenn Sie die Zahlenwerte auswählen, können Sie Detailinformationen zu den betroffenen Assets, Anwendern und Standortdetails anzeigen und die zugehörigen Aufgaben im anzeigen **Incident-Auswirkung** Registerkarte des Arbeitsbereichs. Basierend auf dem ausgewählten Link zum Incident-Auswirkungstyp werden die zugehörigen Incident-Details wie Aufgabentyp und Beschreibung, Zuweisungsgruppe und Incident-Status in angezeigt **Incident Impact** Registerkarte des MSIM-Arbeitsbereichs.
Dauerzähler	Diese Komponenten zeigen die Dauer des schwerwiegenden Security Incidents an. Die betroffenen Ressourcen sind:

Automatische Übersetzung

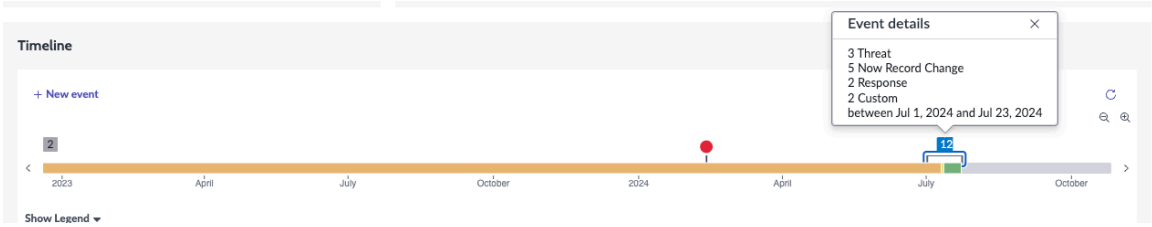
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kurzzusammenfassung und Auswirkung auf Incidents (Fortsetzung)

Aufgabe	Beschreibung
	• **Verstrichene Zeit** : Zeigt die Zeit an, die seit der Erkennung des schwerwiegenden Security Incidents verstrichen ist. • **Geschätztes Lösungsdatum** : Zeigt das geschätzte Lösungsdatum an, bis zu dem der schwerwiegende Security Incident voraussichtlich gelöst wird. • **Nächstes Update am** : Datum und Uhrzeit des nächsten Updates zur Lösung des schwerwiegenden Security Incident. Beispiel: 17:00 Uhr EST am 25. März 2024. Sie können ändern **Nächstes Update am** Indem Sie auswählen **Bearbeiten** Symbol. Wählen Sie das neue Datum und die neue Uhrzeit aus, und wählen Sie aus **Aktualisieren** .

Sie können die Anzeige bestimmter Ereignistypen für Zeitleistenindikatoren und Zeitleistenbereiche entsprechend aktivieren oder deaktivieren, indem Sie die Umschaltflächen für Filter verwenden.

Zeitachse



In der folgenden Tabelle finden Sie zusätzliche Funktionen, die mit der Zeitleistenkomponente verfügbar sind.

Zusätzliche Fähigkeiten der Zeitleistenkomponente

Aufgabe	Beschreibung
Neues Ereignis	Erstellt neue anwenderdefinierte Ereignisse und ordnet diese Ereignisse dem MSI-Datensatz zu. Dies hilft beim Erstellen von Ereignissen für vergangene und zukünftige Daten, die andernfalls möglicherweise nicht über eine gekennzeichnete Aufgabe, eine Änderung des Datensatzstatus oder eine gekennzeichnete Zusammenarbeitsaktivität erfasst werden, die standardmäßig auf der Zeitleiste angezeigt werden.
Neu laden	Aktualisiert die Zeitleistenereignisse, um die neuesten Updates anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Fähigkeiten der Zeitleistenkomponente (Fortsetzung)

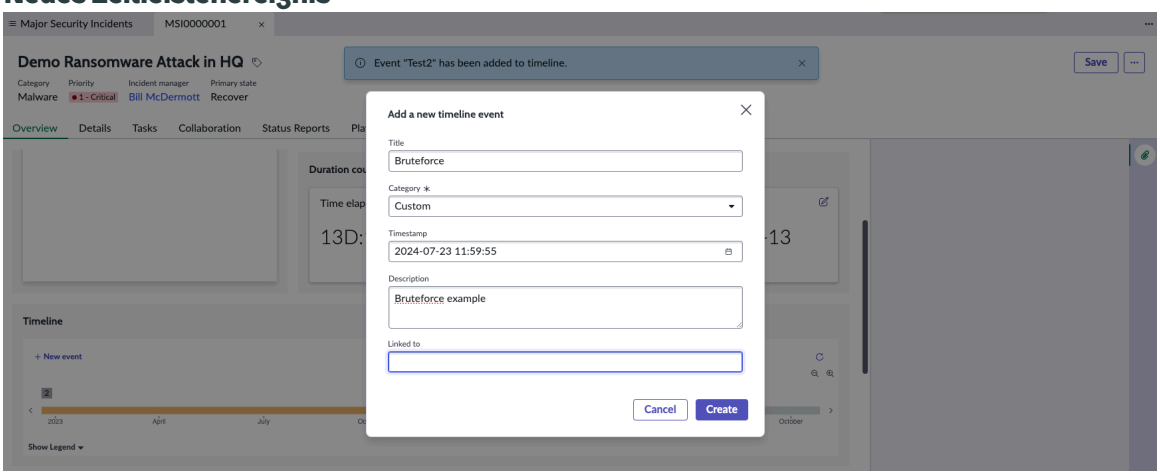
Aufgabe	Beschreibung
Zeitleistenindikatoren	Listet die verschiedenen Ereignistypen auf, z. B. Änderungen im Now-Datensatz-Feld, bezeichnete Zusammenarbeitsaktivitäten und andere (anwenderdefiniert), zusammen mit den Symbolen und der Gesamtzahl der Ereignisse, die in Bezug auf jeden Ereignistypindikator aufgetreten sind. Mit dem Folienindikator können Sie alle Ereignisse für einen bestimmten Ereignistyp aktivieren oder deaktivieren.
Legende Anzeigen	Wählen Sie diese Option aus, um die Dropdown-Legende mit verschiedenen Arten von Zeitleistenindikatoren anzuzeigen.
Fortschrittsbalken der Zeitleiste	Zeigt den Gesamtfortschritt des Incidents über festgelegte Zeitleistenereignisse oder Meilensteine an, die innerhalb der verschiedenen angezeigten Zeitleistenbereiche aufgetreten sind. Sie können auch einen Ereignistyp mit einer Ereigniskategorie verknüpfen. Nachdem Sie sie verknüpft haben, werden die Ereignisdetails an beiden Stellen in der Zeitleiste aktualisiert.
Zeitleistenbereiche	Zeigt verschiedene Incident-Statustypen und -Dauer an, während der Incident während des gesamten Lebenszyklus schwerwiegender Security Incidents voranschreitet. Aktivieren oder deaktivieren Sie ein bestimmtes Ereignis basierend auf dem Incident-Status.

Erstellen Sie ein Zeitleistenereignis

Führen Sie die folgenden Schritte aus, um ein neues Zeitleistenereignis zu erstellen:

1. Navigieren Sie auf der Registerkarte Übersicht zu **Zeitleiste** Abschnitt.
2. Auswahlvorgang **+ Neues Ereignis**an.
3. Füllen Sie die Felder im Popup-Fenster Neues Zeitleistenereignis hinzufügen aus.

Neues Zeitleistenereignis



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
Titel	Geben Sie den Titel für das Zeitleistenereignis ein.
Kategorie	Wählen Sie eine Kategorie für das Zeitleistenereignis aus. Die folgenden Kategorien werden als Teil des Basissystems bereitgestellt, und Sie können eine basierend auf Ihren Anforderungen auswählen. ○ **Anwenderdefiniert** . ○ **Antwort** . ○ **Bedrohung** . Informationen zum Hinzufügen oder Konfigurieren einer Ereigniskategorie in der Zeitleiste finden Sie unter Konfigurieren Sie Zeitleistenkategorien für schwerwiegende Security Incidents.
Zeitstempel	Wählen Sie das Datum und die Uhrzeit des Zeitleistenereignisses mithilfe des Zeitstempelkalenders aus. Sie können der Zeitleiste Ereignisse vor und nach dem Startdatum hinzufügen.
Beschreibung	Geben Sie eine kurze Beschreibung des Zeitleistenereignisses an.
Verknüpft mit	Option zum Verknüpfen des Zeitleistenereignisses mit einem Datensatz für schwerwiegende Security Incidents.

4. Auswahlvorgang **Erstellen**an.
5. Sie können verwenden **Vergrößern** Und **Verkleinern** Symbole zum Vergrößern oder Verkleinern der Zeitleisten-Fortschrittsleiste, einschließlich der Anzeige einzelner Ereignisse, wenn Zahlen angezeigt werden, um mehrere Ereignisse in unmittelbarer Nähe darzustellen.

   Sie können auch die standardmäßige Zoomstufe hinzufügen, um alle Ereignisse anzuzeigen.
6. Wählen Sie aus **Aktualisieren** Symbol zum Anzeigen der neuesten Zeitleistenereignisse.

Anzeigen Major Security Incident Trenddiagramme

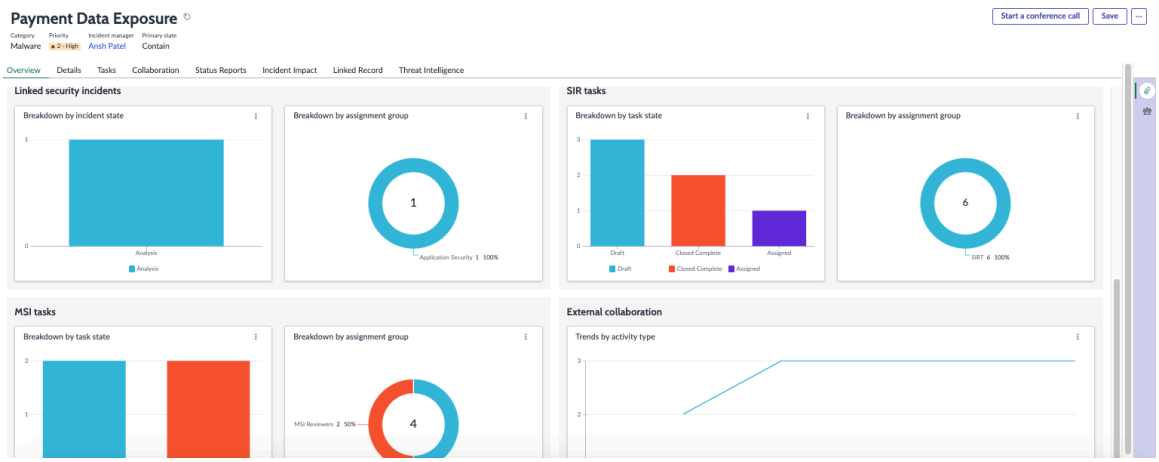
Zeigen Sie die Fortschrittsmetriken für schwerwiegende Auswirkungen auf Security Incidents als Balkendiagramme und Diagramme an.

Zusätzlich zur Visualisierung der Incident-Zeitleiste und des Fortschrittstrenddiagramms **Übersicht** Die Registerkarte bietet relevante Auswirkungsmetriken zum Verwalten des sich ändernden Umfangs des Incident, einschließlich Rollup betroffener Assets, Anwender, Standorte und Teamressourcen.

Die in den Visualisierungskomponenten angezeigten Anzahlen basieren auf aktiven Aufgaben für verknüpfte Security Incident Response (SIR)-Incidents. Wenn Aufgaben geöffnet und geschlossen werden, ändern sich diese Anzahlen in Bezug auf Art und Umfang der verbleibenden geplanten Aktivität für den schwerwiegenden Security Incident, um die Trends darzustellen, die in den Trenddiagramm-Visualisierungskomponenten angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „MSIM-Übersicht“ – Auswirkungsmetriken



In der folgenden Tabelle finden Sie die UI-Aktionen, die Sie über ausführen können **Übersicht** Abschnitt:

Übersichts-UI-Abschnitte

Titel	Beschreibung
Zeit	Zeigt den Zeitraum in Tagen an, ab dem der schwerwiegende Security Incident aktiv ist. Die Zeit wird basierend auf berechnet **Erkennungsdatum** In eingegeben **Details** Registerkarte des Arbeitsbereichs. Das Erkennungsdatum wird häufig anfänglich erfasst, wenn der schwerwiegende Security Incident zuerst erstellt oder vorgeschlagen wurde. Wenn dieses Datum geändert wird, wird die Uhrzeit automatisch berechnet, aktualisiert und im Format Tage: Stunden: Minuten, z. B. 20D: 13H: 58M. angezeigt **Geschätztes Lösungsdatum**: Das Datum, bis zu dem das Incident-Lösungsdatum voraussichtlich gelöst wird. Dieses Datum wird häufig anfänglich erfasst, wenn der schwerwiegende Security Incident erstmals erstellt oder heraufgestuft wurde. Das Datum wird basierend auf dem in angegebenen geschätzten Datum aktualisiert und aktualisiert **Details** Registerkarte des Arbeitsbereichs. Wenn das geschätzte Datum nicht im Abschnitt „Details“ angegeben ist, wird in diesem Abschnitt „Bindestrich“ ohne Datumswert angezeigt.
Aktives Team	Zeigt die verschiedenen Antwortteams und Teammitglieder aus jedem Team an, die aktiv an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersichts-UI-Abschnitte (Fortsetzung)

Titel	Beschreibung
	dem schwerwiegenden Security Incident und den zugehörigen Aufgaben arbeiten. **Aktives Team** Trend: Zeigt das Trenddiagramm jedes Teams und seiner Teammitglieder an, die in regelmäßigen Intervallen aktiv an dem schwerwiegenden Security Incident und zugehörigen Aufgaben arbeiten. **Hinweis:** Zeigen Sie die zugewiesenen aktiven Gruppen aus dem an **Details** Registerkarte des Arbeitsbereichs.
Verknüpfte SIR-Incidents	**Nach Incident-Status**: Zeigen Sie die Verteilung verknüpfter Security Incidents basierend auf einem Incident-Status an, z. B. „Analyse“, „Eindämmen“, „Beseitigen“, „Wiederherstellen“ oder „Überprüfen“. **Trends nach Incident-Status**: Gibt außerdem die Trendansicht an, wie die Anzahl der verknüpften Incidents basierend auf dem Incident-Status voranschreitet. Wenn Sie die einzelnen Incident-Statusverknüpfungen auswählen, können Sie direkt im die verknüpften Security Incident-Details navigieren und anzeigen **Verknüpfte SI/VI** Registerkarte des Arbeitsbereichs. Dieser Abschnitt wird automatisch aktualisiert und aktualisiert, wenn Änderungen an den zugrunde liegenden Incidents auftreten.
SIR-Aufgaben	Zeigt aktive Aufgabensummen an, die über SIR-Incidents mit dem MSI-Datensatz verknüpft sind. • **Nach Aufgabenstatus**: Zeigen Sie die Incident-Antwortaufgaben basierend auf dem Incident-Status an, z. B. Entwurf, Zugewiesen, in Bearbeitung, Abgeschlossen. Dieses Verteilungsdiagramm ermöglicht eine weitere Verteilungsaufgliederung nach Zuweisungsgruppen. Wenn Sie die einzelnen Aufgabenstatus auswählen, können Sie eine gefilterte Liste nach Status der Incident-Aufgabe im anzeigen **Aufgaben** Registerkarte des Arbeitsbereichs. In der gefilterten Ansicht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersichts-UI-Abschnitte (Fortsetzung)

Titel	Beschreibung
	können Sie einzelne Aufgabendetails anzeigen und aktualisieren. • **In Bearbeitung befindliche Aufgaben nach Incident-Statusbezeichnung**: Zeigt aktive Aufgaben und Gruppen basierend auf der Incident-Statusbezeichnung an, die in den Komponenten des Aufgabenorganisators angewendet werden muss. Diese Standardbezeichnungen haben Werte wie Analyse, Eindämmen, Beseitigen, Wiederherstellen oder Überprüfen, um die Art der beteiligten Aufgabe anzugeben. • **Überfällig**: Zeigt die Security Incident Response-Aufgaben an, die aktiv sind und das Fälligkeitsdatum überschritten haben. Sie können die Details aller überfälligen Aufgaben anzeigen, indem Sie die Gesamtzahl der überfälligen Aufgaben auswählen und automatisch zur Registerkarte Aufgaben navigieren. • **Trends nach Aufgabenstatus**: Zeigen Sie den Fortschrittstrend sowohl der in Arbeit befindlichen als auch der geschlossenen Antwortaufgaben über die Incident-Dauer an. **Hinweis:** Das Trenddiagramm ruft die neuesten Daten basierend auf der geplanten Aufgabe ab. Sie können das Datenabrufzeitintervall nach Bedarf konfigurieren oder ändern.
MSI-Aufgaben	Zeigt insgesamt aktive Aufgaben an, die direkt im MSI-Datensatz erstellt wurden (und dies sind keine verknüpften Antwortaufgaben): **Nach Aufgabenstatus:** Zeigen Sie die erstellten Aufgaben für schwerwiegende Security Incidents, zugewiesenen Aufgaben und zugehörigen Informationen an. Wenn Sie die einzelnen Aufgabenstatus auswählen, können Sie eine gefilterte Liste nach Status der Incident-Aufgabe im anzeigen **Aufgaben** Registerkarte des Arbeitsbereichs. Die gefilterte Ansicht ermöglicht das Anzeigen und Aktualisieren einzelner Aufgabendetails.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersichts-UI-Abschnitte (Fortsetzung)

Titel	Beschreibung
Externe Zusammenarbeit	Zeigt Zusammenarbeitsaktivitäten insgesamt für alle bezeichneten Zusammenarbeitsaktivitäten aus dem Zusammenarbeitsaktivitäts-Stream an: • **Nach Incident-Statusbezeichnung:** Zeigen Sie die Daten der Zusammenarbeitsaktivitäten für Incidents an, die mit koordiniert werden Microsoft Teams Und Microsoft SharePoint Dateien und Ordner und werden mit Incident-Statusbezeichnungen wie „Analyse“, „Eindämmen“, „Beseitigen“ oder „Wiederherstellen“ von gekennzeichnet **Zusammenarbeit** Registerkarte des Arbeitsbereichs. • **Trends nach Aktivitätstyp**: Zeigt das Trenddiagramm für die Anzahl von an Microsoft Teams Und Microsoft SharePoint Dateien und Ordneraktivitäten über die Incident-Dauer.

Aktualisieren Major Security Incident Details

Zeigen Sie bestimmte Details im Zusammenhang mit dem schwerwiegenden Security Incident an, und aktualisieren Sie sie, z. B. Incident-Datensatzdetails, aktive Teamteilnehmer und das entsprechende Aktivitätsprotokoll.

Alle zugehörigen Details des schwerwiegenden Security Incidents werden in verschiedenen Formularabschnitten auf angezeigt **Details** Registerkarte des Arbeitsbereichs.
Zeigt die Details an, z. B. Incident-Datensatzdetails, aktive Teamteilnehmer und das entsprechende Aktivitätsprotokoll. Sie können auch die verknüpften SIR-Incidents, Details zu Schwachstellengruppen-Datensätzen und die Möglichkeit anzeigen, eine Aktivitätsveröffentlichung an alle verknüpften Incident-Datensätze zu übertragen.

Die Registerkarte „Details“ enthält hauptsächlich:

1. Formularfelder für schwerwiegenden Security Incident und Incident-bezogene UI-Abschnitte.
2. Aktivitätenstrom

Die folgende Tabelle enthält die Details der Formularfelder für schwerwiegende Security Incidents:

Formularabschnitte für schwerwiegenden Security Incident

Feld	Beschreibung
Incident	
Anzahl	Datensatznummer für schwerwiegenden Security Incident.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularabschnitte für schwerwiegenden Security Incident (Fortsetzung)

Feld	Beschreibung
Primärer Status	Der primäre Status des Datensatzes für schwerwiegende Security Incidents.
Erkennungsdatum	Das Datum, an dem der schwerwiegende Security Incident erstmals erstellt oder vorgeschlagen wurde. Wenn Sie das Erkennungsdatum auf der Registerkarte Details ändern, werden Datum und Uhrzeit des MSI automatisch berechnet, aktualisiert und auf der angezeigt **Zeit** > **Zeit seit Beginn des Incidents** Abschnitt auf der **Übersicht** Abschnitt des Arbeitsbereichs.
Titel	Titel des schwerwiegenden Security Incidents.
Codename	Codename für den schwerwiegenden Security Incident. Beispiel: Blue Tiger.
Nächstes Update am	Datum und Uhrzeit des nächsten Updates zur Lösung des schwerwiegenden Security Incidents. Beispiel: 17:00 Uhr EST am 25. März 2024.
Kategorie	Kategorie des schwerwiegenden Security Incidents.
Unterkategorie	Unterkategorietyp des schwerwiegenden Security Incidents.
Geschätztes Lösungsdatum	Das geschätzte Datum, an dem der Incident voraussichtlich gelöst wird. Der Standardwert beträgt 7 Tage ab dem Zeitpunkt der Erstellung eines schwerwiegenden Security Incidents.
Priorität	Priorität des schwerwiegenden Security Incidents.
Warnungssensor	Warnungssensor des schwerwiegenden Security Incidents. Beispiel: Vom Anwender gemeldetes Phishing.
Quelle	Quelle des schwerwiegenden Security Incidents.
Aktives Team	
Incident-Manager	Name des Incident-Managers.
Zuweisungsgruppen	Gibt die verschiedenen Antwortteams und Teammitglieder aus jedem Team an, die aktiv an dem schwerwiegenden Security Incident arbeiten.
Kandidat	
MSI-Kandidatenstatus	Gibt den Kandidatenstatus für schwerwiegenden Security Incident an, z. B. „vorgeschlagen“ oder „heraufgestuft“. Wenn der Incident heraufgestuft wird, wird der Status als akzeptiert angezeigt.
Heraufgestuft durch	Anwender, der den schwerwiegenden Security Incident heraufgestuft hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularabschnitte für schwerwiegenden Security Incident (Fortsetzung)

Feld	Beschreibung
Heraufgestuft	Datum, an dem der schwerwiegende Security Incident heraufgestuft wurde.
Begründung	Begründung des schwerwiegenden Security Incidents. Die Begründung muss die MSI-Nummer und den Codenamen enthalten.
Potenzieller Impact	Die potenziellen Auswirkungen und der Schweregrad des schwerwiegenden Security Incidents. Die potenziellen Auswirkungen sollten die MSI-Nummer und den Codenamen enthalten.
Beschränkung	
Beschränkung erzwingen	Wählen Sie diese Option aus, um Einschränkungen für bestimmte Einschränkungen für schwerwiegende Security Incidents durchzusetzen. Sie können Einschränkungen erzwingen, um die Ansicht zu beschränken oder den Zugriff nur auf bestimmte Anwender oder Gruppen zu ändern. Weitere Informationen finden Sie unter Beschränken Sie den Zugriff auf bestimmte schwerwiegende Security Incidents.
Zulässige Mitglieder	Liste der Anwender, die auf den schwerwiegenden Security Incident zugreifen können.
Zulässige Gruppen	Liste der Gruppen, die auf den schwerwiegenden Security Incident zugreifen können.
Andere Aktionen	
Anhang	Alle Anhänge im Zusammenhang mit dem schwerwiegenden Security Incident. Wählen Sie Aus **Wählen Sie Aus** Option zum Hinzufügen von Anhängen zum Incident.
Telefonkonferenz	Verwenden Sie Telefonkonferenzen mit externen Service Providern als Kommunikationskanal, um sich mit den Stakeholdern zu treffen, um die schwerwiegenden Security Incidents zu lösen. Weitere Informationen finden Sie unter Management schwerwiegender Sicherheits-Incidents Telefonkonferenzintegration

Aktivität :

Verwenden Sie den Abschnitt „Aktivität“, um Ihre Arbeitsnotizen und Kommentare hinzuzufügen, Ihre Aktivität privat zu veröffentlichen und zusätzliche Kommentare nach Bedarf im Abschnitt „Verfassen“ hinzuzufügen. Speichern Sie die Aktivität, nachdem Sie Ihre Arbeitsnotizen und Kommentare veröffentlicht haben, um die hinzugefügte Aktivität oder Arbeitsnotizen im Abschnitt „Aktivität“ anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wählen Sie aus **Mehr anzeigen** Link „Details“, um die Details eines bestimmten Security Incident-Datensatzes anzuzeigen, der diesem schwerwiegenden Security Incident zugeordnet ist.

Legen Sie Ihre Einstellungen fest, um die zugehörigen Aktivitäten anzuzeigen, z. B.:

1. **Filter** : Wählen Sie aus **Filtersätze** Symbol zum Festlegen von Filtern.

   Legen Sie Filter fest, um die Aktivitätskonversationen anzuzeigen, z. B. Aktivitäten, die in den Arbeitsnotizen hinzugefügt wurden, E-Mail, Zeitleiste und zusätzliche Kommentare.

2. **Gekennzeichnet** : Wählen Sie aus **Gekennzeichnet** Symbol zum Kennzeichnen der Aktivitäten.

   Kennzeichnen Sie alle wichtigen Aktivitätskonversationen, damit sie stets griffbereit sind.

Beschränken Sie den Zugriff auf bestimmte schwerwiegende Security Incidents

Verwalten Sie, wer schwerwiegende Security Incidents anzeigen oder ändern kann, die vertrauliche Informationen enthalten. Sie können Einschränkungen für schwerwiegende Security Incidents erzwingen, um zu bestimmen, wer Zugriff zum Anzeigen oder Ändern bestimmter Datensätze für schwerwiegende Security Incidents und zugehörige Listen hat, und den Lese- oder Schreibzugriff nur auf bestimmte Anwender oder Gruppen beschränken.

Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_Manager

Warum und wann dieser Vorgang ausgeführt wird
Mit Einschränkungen für schwerwiegende Security Incidents können Sie ausblenden, dass kritische schwerwiegende Security Incidents von allen Anwendern oder Gruppen in einer bestimmten Organisation aufgerufen oder geändert werden. Mit diesen Einschränkungen können Sie eine detailliertere Möglichkeit zur Steuerung der schwerwiegenden Security Incidents bereitstellen, die ein Anwender oder eine Gruppe anzeigen oder ändern kann. Sie können eine Einschränkung für schwerwiegende Security Incidents erzwingen, indem Sie auswählen **Einschränkung erzwingen** Aktivieren Sie das Kontrollkästchen, und wählen Sie die Anwender oder Gruppen aus, die den bestimmten schwerwiegenden Security Incident anzeigen oder ändern dürfen.

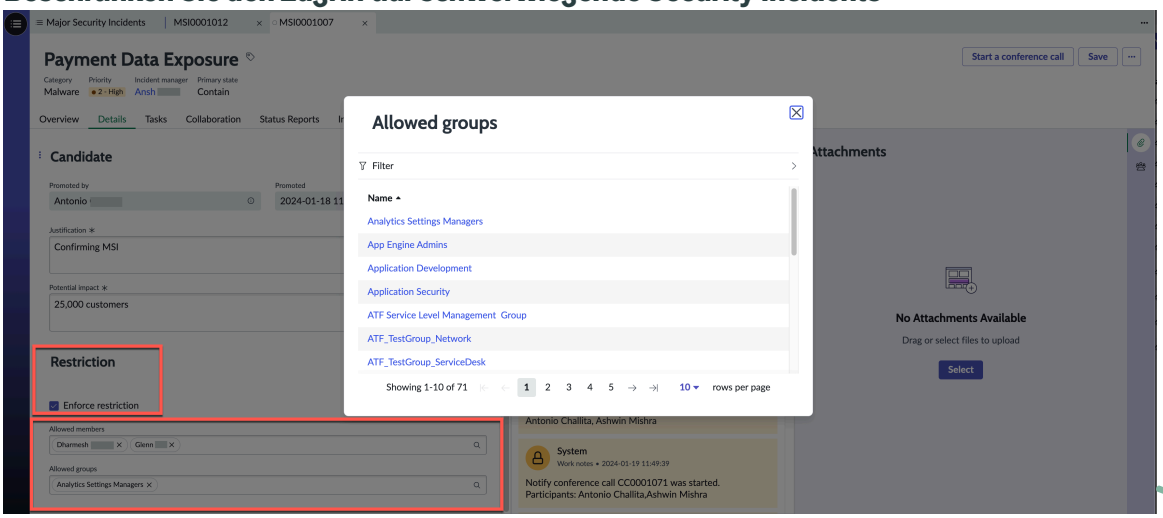
Nachdem Sie die Einschränkung für schwerwiegende Security Incidents oder zugehörige Listen für bestimmte Anwender oder Gruppen durchgesetzt haben, können alle verbleibenden Anwender oder Gruppen in Ihrer Organisation diese schwerwiegenden Security Incidents oder zugehörigen Listen nicht anzeigen oder ändern.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**an.
2. Wählen Sie aus **Listen** Anzeigen.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie die Registerkarte **Details** aus.
5. Scrollen Sie nach unten, und wählen Sie aus **Einschränkung** Abschnitt.
6. Wählen Sie aus **Einschränkung erzwingen** Kontrollkästchen, um die Einschränkung des schwerwiegenden Security Incidents zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschränken Sie den Zugriff auf schwerwiegende Security Incidents



7. Wählen Sie im Feld zulässige Mitglieder die Anwender aus, die den schwerwiegenden Security Incident mithilfe der Suchoption anzeigen oder ändern können.
8. Wählen Sie im Feld zulässige Gruppen die Gruppen aus, die den schwerwiegenden Security Incident mithilfe der Suchoption anzeigen oder ändern können.

Hinweis:
Nach **Einschränkung erzwingen** Das Kontrollkästchen ist für den schwerwiegenden Security Incident aktiviert. Nur sn_msi.Workspace_Manager und zulässige Mitglieder oder Gruppen haben Zugriff zum Anzeigen oder Ändern des schwerwiegenden Security Incidents.

9. Wählen Sie **Speichern**.

Verknüpfen Sie zusätzliche Datensätze mit Major Security Incident

Verwenden Sie im Arbeitsbereich die Funktion „Datensätze verknüpfen“, um zugehörige Security Incident-Datensätze und die zugehörigen untergeordneten Security Incidents, Korrekturaufgaben aus Vulnerability Response und Sicherheitsfälle aus Threat Intelligence mit einem zu verknüpfen Major Security Incident(MSI)-Datensatz.

Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_Manager und sn_msi.Workspace_Responder

Prozedur

1. Navigieren zu **Antwort Auf Schwerwiegende Security Incidents** > **MSIM-Arbeitsbereich**an.
2. Navigieren Sie zu **Listen** Ansicht, die im linken Bereich des Arbeitsbereichs angezeigt wird.
3. Klicken Sie Auf **Akzeptiert** Zum Auswählen der heraufgestuften Datensätze für schwerwiegende Security Incidents.
4. Wählen Sie in der Liste der heraufgestuften Datensätze den Incident-Datensatz aus, der verknüpft werden muss und sich nicht im Status Geschlossen befindet.
5. Klicken Sie Auf **Verknüpfte Datensätze** Registerkarte.
   Eine Dropdown-Liste wird bereitgestellt, um andere verknüpfte Datensatztabellen auszuwählen.
   Im Abschnitt „Verknüpfte Datensätze“ werden die verknüpften Datensätze und die zugehörigen Datensätze angezeigt, die mit dem schwerwiegenden Security Incident verknüpft waren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie die gewünschte Tabellenansicht aus der Liste aus, z. B. Security Incidents, Korrekturaufgaben (angreifbare Elemente) oder Sicherheitsfall.
   Basierend auf der Tabellenansicht der Auswahltyp-Datensätze werden die verknüpften Datensätze angezeigt, die mit den Datensätzen für schwerwiegende Security Incidents verknüpft sind.
7. Verknüpfen Sie einen Datensatz, der mit keinem MSI-Datensatz verknüpft ist und sich in befindet **Öffnen** geben sie an, indem Sie den Datensatz auswählen und auf klicken **Datensatz Verknüpfen** Oben rechts auf der Seite.

   Hinweis:
   Sie können einen Incident-Datensatz nicht mit einem MSI-Datensatz verknüpfen, wenn er sich im befindet **Geschlossen** status.

8. Wählen Sie den zu verknüpfenden Datensatz aus, und klicken Sie auf **Link** .
   Eine Bestätigungsnachricht zeigt an, dass der Datensatz erfolgreich verknüpft wurde und das Rollup der zugehörigen Datensätze im Hintergrund verarbeitet wird.

   Hinweis:
   Nachdem ein Datensatz verknüpft wurde, wird die Listenansicht automatisch aktualisiert und listet die aktualisierte Liste der Incident-Datensätze auf.

Zugehörige Informationen

Heben Sie die Verknüpfung von Datensätzen mit auf Major Security Incident

Heben Sie die Verknüpfung von Datensätzen mit auf Major Security Incident

Heben Sie im Arbeitsbereich Management schwerwiegender Security Incidents die Verknüpfung der Datensätze schwerwiegender Security Incidents im Abschnitt „Verknüpfte Datensätze“ auf.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager und sn_msi.Workspace_Responder

Hinweis:
Sie können die Verknüpfung eines einzelnen Datensatzes gleichzeitig nur aufheben. Nachdem Sie die Verknüpfung eines Datensatzes aufgehoben haben, werden die zugehörigen Rollup-Informationen aus den Abschnitten „Incident Impact“ und „Threat Intelligence“ im Arbeitsbereich entfernt, und die Aktion kann nicht rückgängig gemacht werden.

Weitere Informationen zu Rollup-Datensätzen finden Sie unter Rollup-Framework für MSIM.

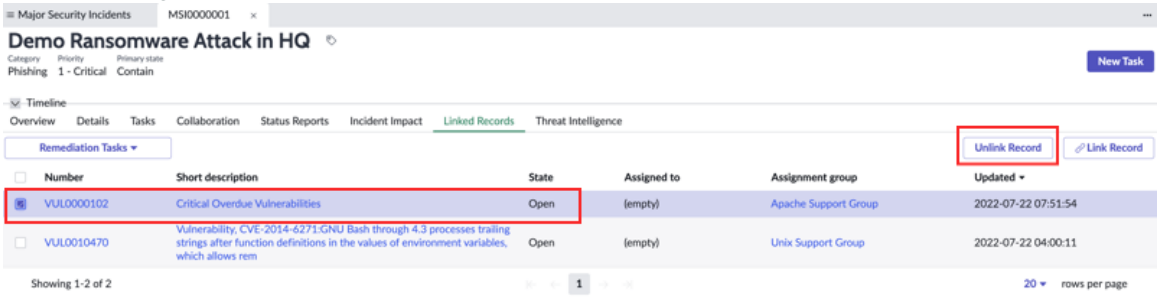
Prozedur

1. Navigieren zu **Antwort Auf Schwerwiegende Security Incidents** > **MSIM-Arbeitsbereich**an.
2. Navigieren Sie zu **Listen** Ansicht, die im linken Bereich des Arbeitsbereichs angezeigt wird.
3. Klicken Sie Auf **Akzeptiert** Zum Auswählen der heraufgestuften Datensätze für schwerwiegende Security Incidents.
4. Klicken Sie auf **Verknüpfte Datensätze** Registerkarte.
   In diesem Abschnitt werden die verknüpften Datensätze und die zugehörigen Datensätze angezeigt, die mit dem schwerwiegenden Security Incident verknüpft sind.
5. Wählen Sie die gewünschte Tabellenansicht aus, z. B. Security Incidents, Korrekturaufgaben (angreifbare Elemente) oder Sicherheitsfall.
6. Wählen Sie den Datensatz aus, dessen Verknüpfung mit der Listenansicht der Datensätze aufgehoben werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

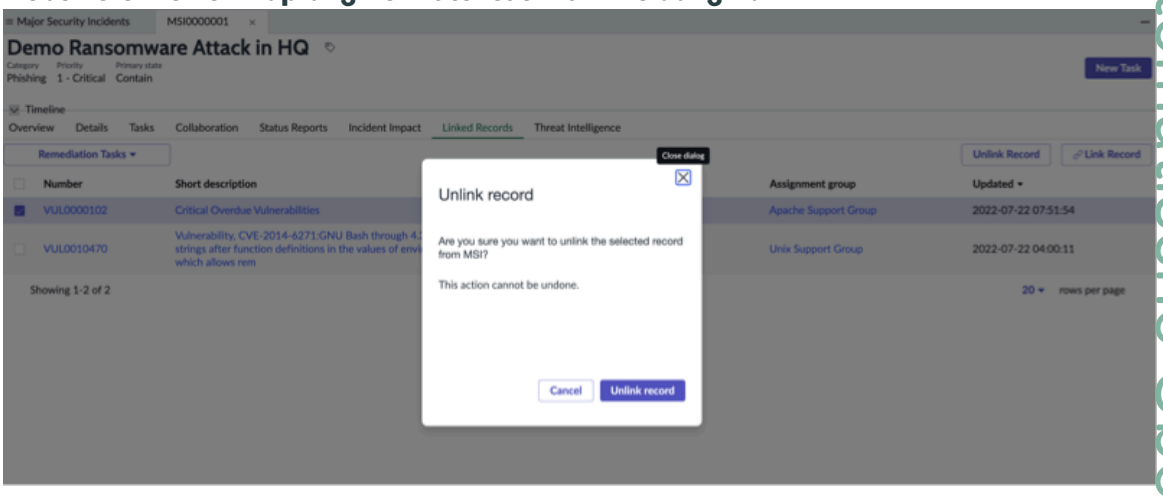
7. Klicken Sie Auf **Verknüpfung Des Datensatzes Aufheben** .

Verknüpfung von Datensatz aufheben



8. Eine Warnmeldung wird angezeigt, in der Sie gefragt werden, ob Sie die Verknüpfung des ausgewählten Datensatzes mit MSI aufheben möchten.

Heben Sie Die Verknüpfung Der Datensatzwarnmeldung Auf



9. Klicken Sie Auf **Verknüpfung Des Datensatzes Aufheben** .
Die Verknüpfung des Datensatzes wird aufgehoben, und sobald die Verknüpfung aufgehoben wurde, können die Änderungen nicht rückgängig gemacht werden. Die Listenansicht der verknüpften Datensätze wird nach dem Aufheben der Verknüpfung aktualisiert.

Zugehörige Informationen

Konfigurieren Sie verknüpfte Datensätze in Management schwerwiegender Sicherheits-Incidents

Konfigurieren Sie Rollup-Datensätze in Management schwerwiegender Sicherheits-Incidents

Verwalten Sie Aufgaben in einem Major Security Incident

Auf der Registerkarte Aufgabe können Sie alle Aufgaben, die einem schwerwiegenden Security Incident zugeordnet sind, im MSIM-Arbeitsbereich nachverfolgen und verwalten. Sie können die verschiedenen Aufgaben mithilfe des standardmäßigen visuellen Taskboards (Kanban-Ansicht) oder der Listenansicht anzeigen.

sn_msi.Workspace_Manager kann auf der Registerkarte Aufgaben Folgendes ausführen:

- Eine Aufgabe erstellen
- Aufgaben ändern

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

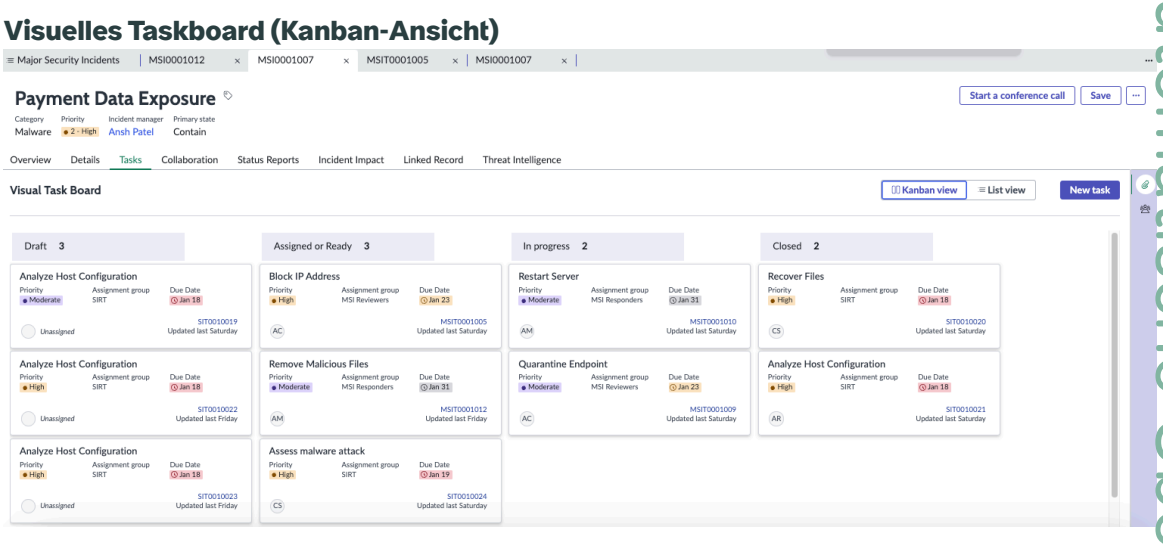
- Zeigen Sie Aufgaben an, und weisen Sie sie sich selbst oder anderen zu
- Löschen Sie Aufgaben

Hinweis:
Stellen Sie sicher, dass Sie installiert haben **MSIM VTB-Aufgabenkarte: 1,0.1v** App separat nach der Installation der MSIM-App.

Auf der Registerkarte Aufgaben werden die Details aller Aufgaben angezeigt, die einem schwerwiegenden Security Incident zugeordnet sind. Die Registerkarte Aufgabe unterstützt zwei Ansichten:

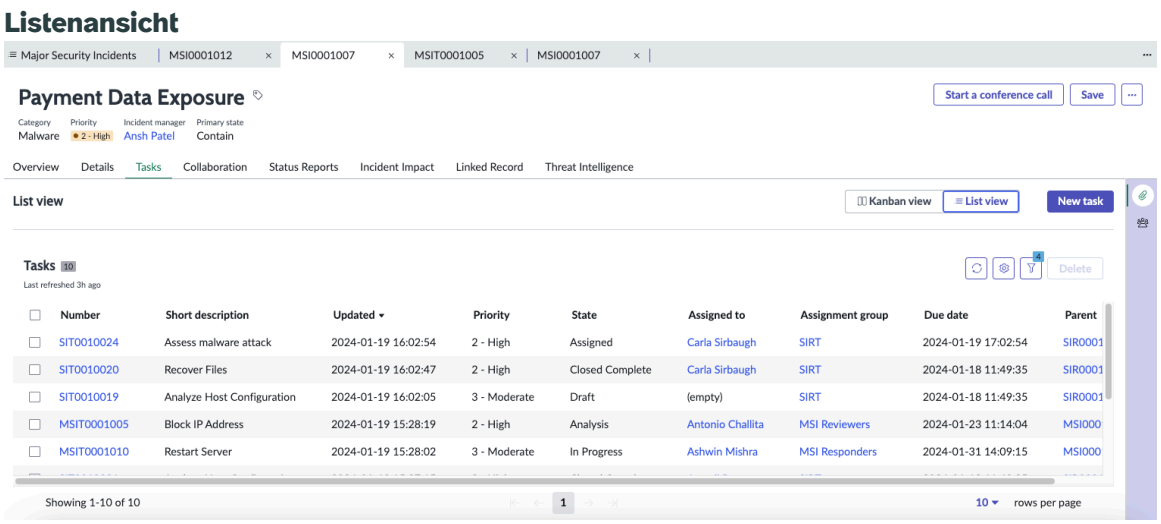
- **Visuelles Taskboard (Kanban-Ansicht)** :

  Zeigen Sie mehrere Aufgabendatensätze an, und aktualisieren Sie sie, die als Karten im visuellen Taskboard angezeigt werden, die basierend auf dem Status der Aufgaben im schwerwiegenden Security Incident zwischen Spuren verschoben werden können.



- **Listenansicht** :

  Zeigen Sie mehrere Aufgabendatensätze mit in Form von Listen an, und aktualisieren Sie sie. Mit diesen Listenkategorien und Filtern können Sie schnell die Aufgaben finden und nachverfolgen, an denen Sie bei einem schwerwiegenden Security Incident arbeiten müssen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die gekennzeichneten Aktivitäten werden zusammengefasst und im Abschnitt „Übersicht“ des schwerwiegenden Security Incident angezeigt. Im Abschnitt Übersicht ist ein Trenddiagramm verfügbar, um den Status der konsolidierten Aufgabenaktivitäten anzuzeigen.

Verwalten Sie Aufgaben mit dem visuellen Taskboard

Verfolgen und verwalten Sie alle Aufgaben, die einem schwerwiegenden Security Incident zugeordnet sind, mithilfe des visuellen Taskboards (Kanban-Ansicht).

Sie können das visuelle Taskboard verwenden, um die Karten schrittweise zwischen Spuren wie Entwurf, Zugewiesen oder bereit, in Bearbeitung und Geschlossen zu verschieben, je nach Status der Aufgaben. Ein Aktivitätenstrom auf der Tafel zeigt aktuelle Aktivitäten an, um Aufgabenänderungen einfach nachzuverfolgen. Sie können Aufgabenkarten aus jeder Tabelle hinzufügen, die die Aufgabe erweitert, um Aktualisierungen schnell nachzuverfolgen und schwerwiegende Security Incidents direkt über die Tafel zu bearbeiten.

Erstellen Sie eine Aufgabe mit dem visuellen Taskboard

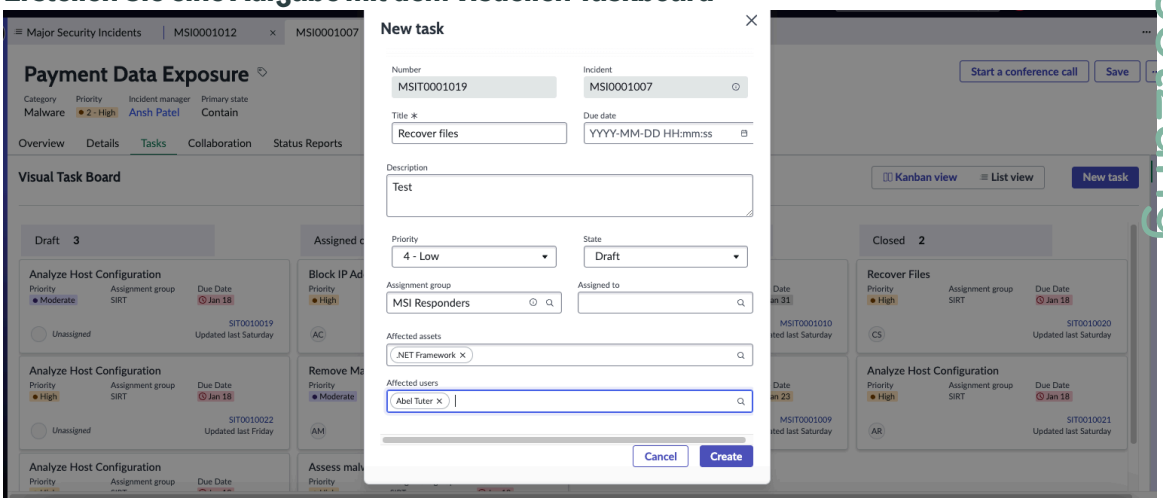
Erforderliche Rolle: sn_msi.Workspace_Manager.

Hinweis:
Stellen Sie sicher, dass Sie installiert haben **MSIM VTB-Aufgabenkarte: 1,0.1v** App separat nach der Installation der MSIM-App.

MSI-Manager können eine Aufgabe im visuellen Taskboard mit den folgenden Schritten erstellen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**an.
2. Wählen Sie aus **Listen** Anzeigen.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie aus **Aufgaben** Registerkarte.

Erstellen Sie eine Aufgabe mit dem visuellen Taskboard



5. Wählen Sie Aus **Kanban-Ansicht** , Und wählen Sie aus **Neue Aufgabe** .
6. Füllen Sie im Formular die Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anzahl	Eine eindeutige Nummer, die für die ausgewählte Aufgabe automatisch generiert wird. Dieses Feld kann nicht bearbeitet werden.
Incident	Nummer des schwerwiegenden Security Incidents. Dieses Feld kann nicht bearbeitet werden.
Titel	Geben Sie einen Namen für die Aufgabe an.
Fälligkeitsdatum	Wählen Sie ein Fälligkeitsdatum und eine Fälligkeitszeit für die Aufgabe aus, die abgeschlossen werden soll. Wählen Sie ein Datum mit aus **Kalender** Option und geben Sie die Zeit auf der an **Wählen Sie Zeit Aus** Abschnitt.
Beschreibung	Geben Sie eine eindeutige Beschreibung für die Aufgabe an.
Priorität	Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einen der folgenden Werte haben: ○ **Keine** ○ **1 – Kritisch** ○ **2 - Hoch** ○ **3 - Mittel** ○ **4 – Niedrig** ○ **5: Planung**
Status	Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein: ○ **Entwurf** ○ **Analyse** ○ **In Bearbeitung** ○ **Geschlossen** Der Standardstatus ist **Entwurf**.
Zuweisungsgruppe	Wählen Sie eine Zuweisungsgruppe des Anwenders aus, um die Aufgabe mithilfe der Suchoption zuzuweisen.
Zugewiesen an	Wählen Sie den Anwender aus, der die Aufgabe mithilfe der Suchoption zugewiesen werden soll.
Betroffene Assets	Wählen Sie die von der Aufgabe betroffenen Assets mithilfe der Suchoption aus.
Betroffene Anwender	Wählen Sie die von der Aufgabe betroffenen Anwender mithilfe der Suchoption aus.

7. Wählen Sie Aus **Erstellen** Um die Aufgabe zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie eine Aufgabe mit dem visuellen Taskboard an, und ändern Sie sie

Erforderliche Rolle: sn_msi.Workspace_Manager.

Hinweis:
Stellen Sie sicher, dass Sie installiert haben **MSIM VTB-Aufgabenkarte: 1,0.1v** App separat nach der Installation der MSIM-App.

MSI-Manager können die Details einer Aufgabe und Aktivitätsinformationen von den MSI-Beantwortern anzeigen und eine Aufgabe im visuellen Taskboard mithilfe der folgenden Schritte ändern:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**an.
2. Wählen Sie aus **Listen** Anzeigen.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie aus **Aufgaben** Und wählen Sie aus **Kanban-Ansicht** .
5. Wählen Sie die gewünschte Aufgabenkarte in einer der Spuren aus, um die Details der Aufgabe anzuzeigen.

   Die Aufgabenkarte kann sich in einer der Spalten befinden: Entwurf, Zugewiesen oder bereit, in Bearbeitung oder Geschlossen.
6. Im Abschnitt „Aufgabeninformationen“ können Sie die folgenden Details ändern:

Feld	Beschreibung
Anzahl	Eine eindeutige Nummer, die für die ausgewählte Aufgabe automatisch generiert wird. Dieses Feld kann nicht bearbeitet werden.
Incident	Nummer des schwerwiegenden Security Incidents. Dieses Feld kann nicht bearbeitet werden.
Titel	Geben Sie einen Namen für die Aufgabe an.
Fälligkeitsdatum	Wählen Sie ein Fälligkeitsdatum und eine Fälligkeitszeit für die Aufgabe aus, die abgeschlossen werden soll. Wählen Sie ein Datum mit aus **Kalender** Option und geben Sie die Zeit auf der an **Wählen Sie Zeit Aus** Abschnitt.
Beschreibung	Geben Sie eine eindeutige Beschreibung für die Aufgabe an.
Priorität	Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einen der folgenden Werte haben: ○ **Keine** ○ **1 – Kritisch** ○ **2 - Hoch** ○ **3 - Mittel** ○ **4 – Niedrig** ○ **5: Planung**

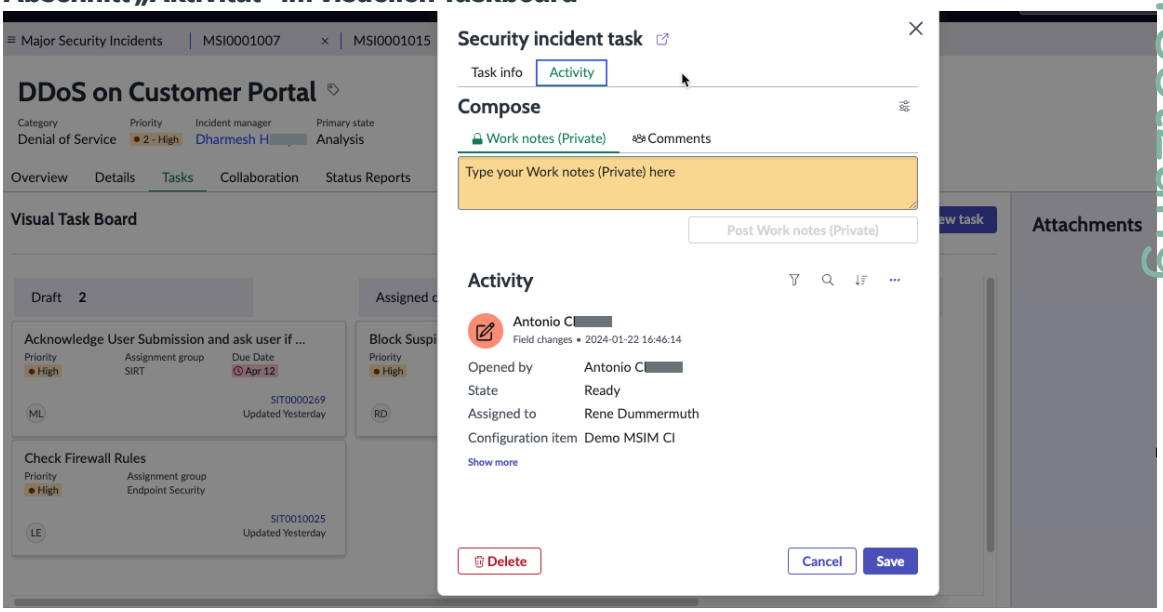
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein: ○ **Entwurf** ○ **Analyse** ○ **In Bearbeitung** ○ **Geschlossen** Der Standardstatus ist **Entwurf**.
Zuweisungsgruppe	Wählen Sie eine Zuweisungsgruppe des Anwenders aus, um die Aufgabe mithilfe der Suchoption zuzuweisen.
Zugewiesen an	Wählen Sie den Anwender aus, der die Aufgabe mithilfe der Suchoption zugewiesen werden soll.
Betroffene Assets	Wählen Sie die von der Aufgabe betroffenen Assets mithilfe der Suchoption aus.
Betroffene Anwender	Wählen Sie die von der Aufgabe betroffenen Anwender mithilfe der Suchoption aus.

7. Wählen Sie aus **Aktivität** Abschnitt zum Anzeigen der Aktivitätsdetails der MSI-Beantworter.

   Verwenden Sie den Abschnitt „Aktivität“, um Ihre Arbeitsnotizen und Kommentare hinzuzufügen, Ihre Aktivität privat zu veröffentlichen und zusätzliche Kommentare nach Bedarf im Abschnitt „Verfassen“ hinzuzufügen. Speichern Sie die Aktivität, nachdem Sie Ihre Arbeitsnotizen und Kommentare veröffentlicht haben, um die hinzugefügten Aktivitäten oder Arbeitsnotizen im Abschnitt „Aktivität“ anzuzeigen.

Abschnitt „Aktivität“ im visuellen Taskboard



Hinweis:
Wählen Sie aus **Mehr anzeigen** Link „Details“, um die Details eines bestimmten Security Incident-Datensatzes anzuzeigen, der diesem schwerwiegenden Security Incident zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Wählen Sie Aus **Speichern** Zum Aktualisieren der Aufgabeninformationen.

   Die Aufgabeninformationen werden sofort aktualisiert.

Löschen Sie eine Aufgabe mit dem visuellen Taskboard

Erforderliche Rolle: sn_msi.Workspace_Manager.

Hinweis:
Stellen Sie sicher, dass Sie installiert haben **MSIM VTB-Aufgabenkarte: 1,0.1v** App separat nach der Installation der MSIM-App.

MSI-Manager kann eine Aufgabe im visuellen Taskboard mit den folgenden Schritten löschen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**an.
2. Wählen Sie aus **Listen** Anzeigen.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie aus **Aufgaben** Und wählen Sie aus **Kanban-Ansicht**
5. Wählen Sie die Aufgabenkarte aus, die Sie löschen möchten.
6. Wählen Sie im Popup-Fenster „schwerwiegende Security Incident-Aufgabe“ die Option aus **Löschen** Option.

   Das Popup-Fenster „Aufgabe löschen“ wird angezeigt, in dem Sie aufgefordert werden, das Löschen der Aufgabe zu bestätigen.
7. Wählen Sie **Löschen**.

Verwalten Sie Aufgaben mit der Listenansicht

Verfolgen und verwalten Sie alle Aufgaben, die einem schwerwiegenden Security Incident zugeordnet sind, mithilfe der Listenansicht.

In der Listenansicht werden die Details aller Aufgaben angezeigt, die dem schwerwiegenden Security Incident zugeordnet sind, z. B. Aufgabennummer, Priorität, Aktueller Status, Zugewiesen an, zugewiesene Gruppe. Mit diesen Listenkategorien und Filtern können Sie schnell die erforderlichen Aufgaben finden und nachverfolgen, an denen Sie bei einem schwerwiegenden Security Incident arbeiten müssen.

Erstellen Sie eine Aufgabe mithilfe der Listenansicht

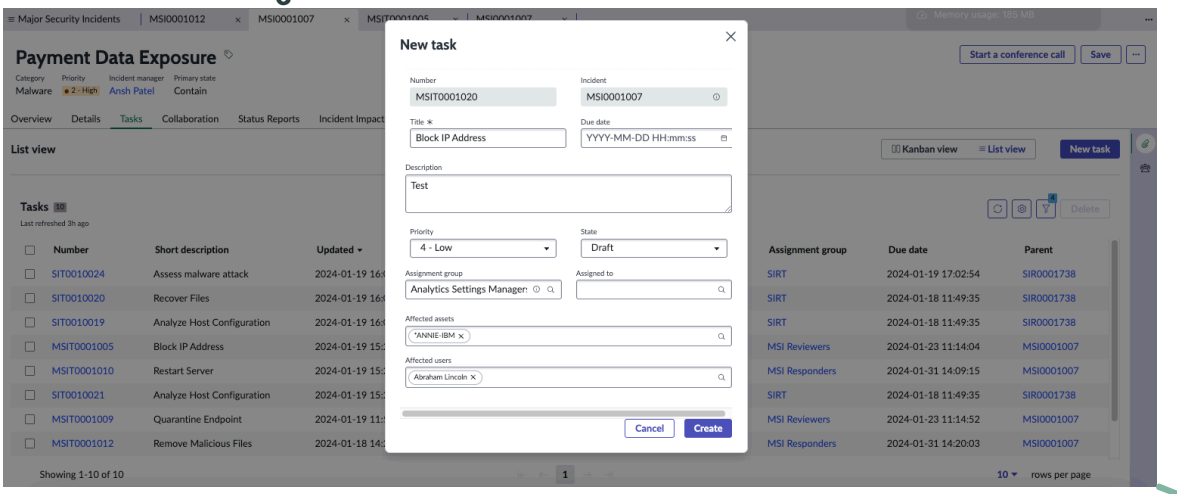
Erforderliche Rolle: sn_msi.Workspace_Manager.

MSI-Manager können eine Aufgabe in der Listenansicht mit den folgenden Schritten erstellen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**an.
2. Wählen Sie aus **Listen** Anzeigen.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie aus **Aufgaben** Registerkarte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Aufgabe mithilfe der Listenansicht



5. Wählen Sie Aus **Listenansicht** , Und wählen Sie aus **Neue Aufgabe** .

6. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Anzahl	Eine eindeutige Nummer, die für die ausgewählte Aufgabe automatisch generiert wird. Dieses Feld kann nicht bearbeitet werden.
Incident	Nummer des schwerwiegenden Security Incidents. Dieses Feld kann nicht bearbeitet werden.
Titel	Geben Sie einen Namen für die Aufgabe an.
Fälligkeitsdatum	Wählen Sie ein Fälligkeitsdatum und eine Fälligkeitszeit für die Aufgabe aus, die abgeschlossen werden soll. Wählen Sie ein Datum mit aus **Kalender** Option und geben Sie die Zeit auf der an **Wählen Sie Zeit Aus** Abschnitt.
Beschreibung	Geben Sie eine eindeutige Beschreibung für die Aufgabe an.
Priorität	Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einen der folgenden Werte haben: ○ **Keine** ○ **1 – Kritisch** ○ **2 - Hoch** ○ **3 - Mittel** ○ **4 – Niedrig** ○ **5: Planung**
Status	Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein: ○ **Entwurf** ○ **Analyse**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **In Bearbeitung** ○ **Geschlossen** Der Standardstatus ist **Entwurf**.
Zuweisungsgruppe	Wählen Sie eine Zuweisungsgruppe des Anwenders aus, um die Aufgabe mithilfe der Suchoption zuzuweisen.
Zugewiesen an	Wählen Sie den Anwender aus, der die Aufgabe mithilfe der Suchoption zugewiesen werden soll.
Betroffene Assets	Wählen Sie die von der Aufgabe betroffenen Assets mithilfe der Suchoption aus.
Betroffene Anwender	Wählen Sie die von der Aufgabe betroffenen Anwender mithilfe der Suchoption aus.

7. Wählen Sie Aus **Erstellen** Um die Aufgabe zu erstellen.

Zeigen Sie eine Aufgabe mit der Listenansicht an, und ändern Sie sie

Erforderliche Rolle: sn_msi.Workspace_Manager.

MSI-Manager können die Details einer Aufgabe und Aktivitätsinformationen von den MSI-Beantwortern anzeigen und eine Aufgabe in der Listenansicht mithilfe der folgenden Schritte ändern

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**an.
2. Wählen Sie aus **Listen** Anzeigen.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie aus **Aufgaben** Und wählen Sie aus **Listenansicht** .
5. Wählen Sie in der Listenansicht die gewünschte Aufgabe aus, um die Details der Aufgabe anzuzeigen.
6. Im Abschnitt „Aufgabeninformationen“ können Sie die folgenden Details ändern:

Feld	Beschreibung
Anzahl	Eine eindeutige Nummer, die für die ausgewählte Aufgabe automatisch generiert wird. Dieses Feld kann nicht bearbeitet werden.
Incident	Nummer des schwerwiegenden Security Incidents. Dieses Feld kann nicht bearbeitet werden.
Titel	Geben Sie einen Namen für die Aufgabe an.
Fälligkeitsdatum	Wählen Sie ein Fälligkeitsdatum und eine Fälligkeitszeit für die Aufgabe aus, die abgeschlossen werden soll. Wählen Sie ein Datum mit aus **Kalender** Option und geben Sie die Zeit auf der an **Wählen Sie Zeit Aus** Abschnitt.
Beschreibung	Geben Sie eine eindeutige Beschreibung für die Aufgabe an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

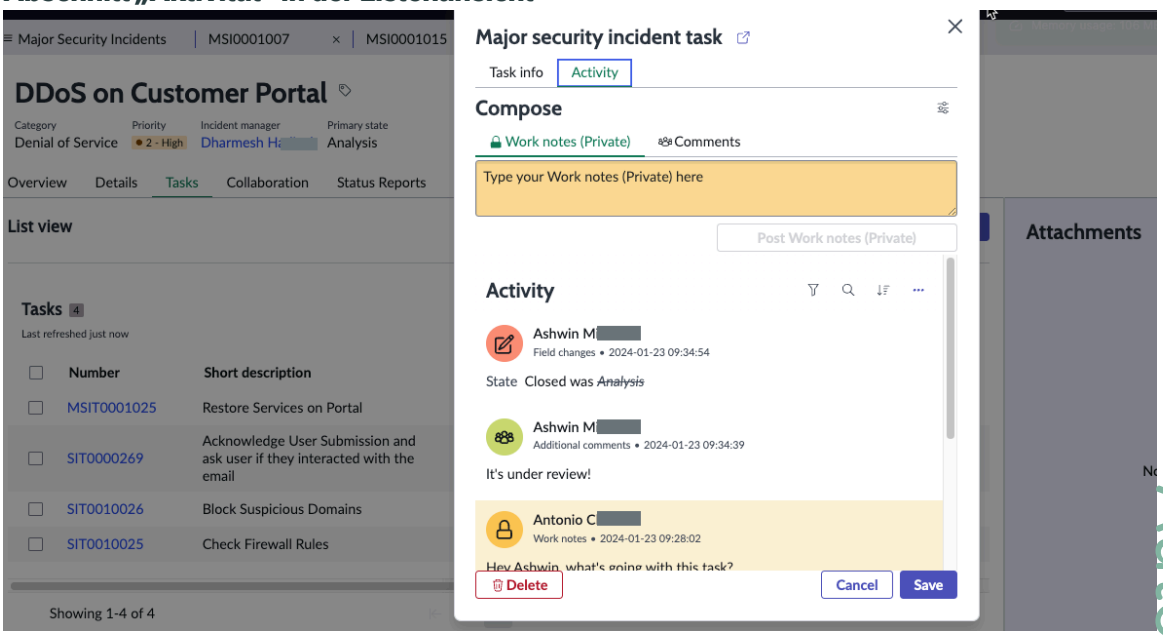
Feld	Beschreibung
Priorität	Wählen Sie die Priorität der Aufgabe aus, um zu bestimmen, wann die Aufgabe ausgeführt wird. Die Priorität kann einen der folgenden Werte haben: ○ **Keine** ○ **1 – Kritisch** ○ **2 - Hoch** ○ **3 - Mittel** ○ **4 – Niedrig** ○ **5: Planung**
Status	Wählen Sie den aktuellen Status der Aufgabe aus. Der Status kann einer der folgenden sein: ○ **Entwurf** ○ **Analyse** ○ **In Bearbeitung** ○ **Geschlossen** Der Standardstatus ist **Entwurf**.
Zuweisungsgruppe	Wählen Sie eine Zuweisungsgruppe des Anwenders aus, um die Aufgabe mithilfe der Suchoption zuzuweisen.
Zugewiesen an	Wählen Sie den Anwender aus, der die Aufgabe mithilfe der Suchoption zugewiesen werden soll.
Betroffene Assets	Wählen Sie die von der Aufgabe betroffenen Assets mithilfe der Suchoption aus.
Betroffene Anwender	Wählen Sie die von der Aufgabe betroffenen Anwender mithilfe der Suchoption aus.

7. Wählen Sie aus **Aktivität** Abschnitt zum Anzeigen der Aktivitätsdetails der MSI-Beantworter.

   Verwenden Sie den Abschnitt „Aktivität“, um Ihre Arbeitsnotizen und Kommentare hinzuzufügen, Ihre Aktivität privat zu veröffentlichen und zusätzliche Kommentare nach Bedarf im Abschnitt „Verfassen“ hinzuzufügen. Speichern Sie die Aktivität, nachdem Sie Ihre Arbeitsnotizen und Kommentare veröffentlicht haben, um die hinzugefügten Aktivitäten oder Arbeitsnotizen im Abschnitt „Aktivität“ anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt „Aktivität“ in der Listenansicht



Hinweis:
Wählen Sie aus **Mehr anzeigen** Link „Details“, um die Details eines bestimmten Security Incident-Datensatzes anzuzeigen, der diesem schwerwiegenden Security Incident zugeordnet ist.

8. Wählen Sie Aus **Speichern** Zum Aktualisieren der Aufgabeninformationen.

   Die Aufgabeninformationen werden sofort aktualisiert.

9. Sie können auch die folgenden Aktionen in der Listenansicht ausführen:
   a. Wählen Sie aus **Aktualisieren** Symbol zum Aktualisieren der Liste der Aufgaben in der Listenansicht.
   b. Wählen Sie aus **Einstellungen** -Symbol und verwenden Sie **Bearbeiten Sie Spalten** Option zum Ändern der Liste der Spalten, die in der Listenansicht angezeigt werden. Verwenden Sie **Breiten zurücksetzen** Option zum Zurücksetzen der Breiten der Spalten.

Löschen Sie eine Aufgabe mithilfe der Listenansicht

Erforderliche Rolle: sn_msi.Workspace_Manager.

MSI-Manager kann eine Aufgabe in der Listenansicht mit den folgenden Schritten löschen:

1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**an.
2. Wählen Sie aus **Listen** Anzeigen.
3. Wählen Sie den erforderlichen Datensatz für schwerwiegende Security Incidents aus.
4. Wählen Sie aus **Aufgaben** Registerkarte.
5. Wählen Sie Aus **Listenansicht** .
6. Wählen Sie eine Aufgabe aus der Liste aus, die Sie löschen möchten.
7. Wählen Sie im Popup-Fenster „schwerwiegende Security Incident-Aufgabe“ die Option aus **Löschen** Option.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Popup-Fenster „Aufgabe löschen“ wird angezeigt, in dem Sie aufgefordert werden, das Löschen der Aufgabe zu bestätigen.

8. Wählen Sie **Löschen**.

Verfolgen Sie Zusammenarbeitsaktivitäten über MSIM Arbeitsbereich

Verfolgen Sie Chat- und Dateiaktivitäten im Zusammenhang mit der Lösung schwerwiegender Security Incidents über den MSIM-Arbeitsbereich.

Aktivitäten werden mit koordiniert Microsoft Teams Chat und Microsoft SharePoint Dateien und Ordner und dann zurück in veröffentlicht Major Security IncidentÜber Integrationen.

Einmal Microsoft Teams Und Microsoft SharePoint sind in integriert Management schwerwiegender Sicherheits-Incidents, Können Sie verwenden MSIM Arbeitsbereich zum Nachverfolgen der Zusammenarbeit zwischen Anwendern der Reaktion auf Incidents und anderen Gruppen, die zur Lösung eines schwerwiegenden Security Incidents beitragen. Alle Aktualisierungen von Zusammenarbeitsordnern und -Dateien in Microsoft SharePoint Werden mit synchronisiert MSIM Arbeitsbereich File Explorer Und spiegelt sich auch in den Aktivitätenstrom-Komponenten wider.

Wenn ein Security Incident als schwerwiegender Security Incident heraufgestuft wird:

1. In wird eine Ordnerstruktur erstellt Microsoft SharePoint Basierend auf der Konfiguration der Ordnervorlage. Dieselbe Ordnerstruktur wird auf angezeigt File Explorer Komponente des Arbeitsbereichs.
2. Unter wird ein Team mit mehreren Kanälen erstellt Microsoft Teams Anwendung und dieselbe werden in der Komponente „Chat-Management“ des Arbeitsbereichs berücksichtigt.

Erforderliche Rolle: sn_msi.Workspace_Manager.

Interagieren Sie mit Dateien und Ordnern

Im Datei-Explorer wird das Dateisystem angezeigt, damit Sie Dateien und Ordner im Zusammenhang mit der Lösung des Incident anzeigen und mit ihnen interagieren können.

Zeigt die Datei und die Ordner an, die in Microsoft SharePoint für einen bestimmten Security Incident erfasst werden. Diese Ordner werden für diesen schwerwiegenden Security Incident automatisch in Microsoft SharePoint erstellt. Sie können diese standardmäßig erstellten Ordner verwenden, um bei Bedarf unterstützende Dateien hochzuladen. Sie können diese Dateien und Ordner nach Bedarf umbenennen, verschieben oder löschen.

Wenn Sie eine Datei in einen der Ordner hochladen, wird die Aktivität, die diesen Ordnern entspricht, automatisch den Datei-Explorer-Ordnern auf der Registerkarte Zusammenarbeit zugeordnet, und die Aktivität wird aufgezeichnet und im Abschnitt „Aktivität“ des Arbeitsbereichs „Management schwerwiegender Security Incidents“ angezeigt.

Hinweis:
Auf der **Zusammenarbeit** Registerkarte wird der Incident-Datensatz mit einer eindeutigen Incident-Nummer und Incident-Kategorie an die übergeordnete Datei in sharepoint angehängt.

1. **Repository-Ansicht** : Listet die Dateien und Ordner auf, die in Microsoft SharePoint für diesen bestimmten Security Incident aufgeführt sind. Für jede Datei oder jeden Ordner werden in der Repository-Ansicht Name, geändert von, zuletzt geändert und Größe angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Repository-Ansicht

Feld	Beschreibung
Öffnen Sie in SharePoint	Wählen Sie diese Option aus, die neben Ihrem schwerwiegenden Security Incident verfügbar ist. Klicken Sie auf den Link, um die Ordnerstruktur in Microsoft SharePoint auszuwählen und anzuzeigen.
Neuer Ordner	Wählen Sie diese Option aus, um nach Bedarf einen neuen Ordner zu erstellen. Nachdem Sie einen neuen Ordner erstellt haben, wird derselbe neue Ordner standardmäßig in Microsoft SharePoint erstellt und zugeordnet.

2. **Zuletzt** : Zeigt alle aktuellen Aktivitätsprotokolle an. Diese Protokolle enthalten sowohl Ihre SharePoint- als auch Datei-Explorer-Aktivitäten. Die letzten Aktivitäten sind normalerweise Ihre unterstützenden Dateien, die den übergeordneten Ordner enthalten.

   Im Folgenden finden Sie das Verfahren bis **Protokolldatei suchen:**

   a. Wählen Sie die entsprechende Datei aus, um die Details anzuzeigen.

   b. Klicken Sie Auf **Suchen Sie Die Datei** .

   Hinweis:
   Die Navigation und Details der übergeordneten Datei und der übergeordneten Ordner werden unter angezeigt **Zuletzt** Listenansichtsabschnitt. Sie können dieselbe Datei in SharePoint öffnen. Jedes Mal, wenn Sie die zugehörigen Protokolldateien oder Aktivitäten hochladen, werden alle diese Dateien und Aktivitäten sowohl in SharePoint als auch in Datei-Explorer angezeigt.

Verwalten Sie die Kommunikation von Chatkanälen mit Microsoft Teams

Der Chat-Kanal-Manager zeigt Microsoft Teams mit mehreren Kanälen an, die in der Microsoft Teams-Anwendung basierend auf dem Setup einer Konfigurationsvorlage erstellt wurden.

Diese konfigurierten Kanäle werden zusammen mit den Anwendern und Anwendergruppen, die ihnen zugewiesen sind, in der Komponente „Chat-Management“ angezeigt. Mit dem Chat-Channel-Manager können Sie Folgendes ausführen:

- **Verwalten Sie Chatkanäle**
- **Team umbenennen**
- **Teammitglieder verwalten**

Das Team und die Kanäle werden basierend auf der Chat-Kanalkonfiguration in Microsoft Teams erstellt.

Verwalten Sie Chatkanäle

Mit dem Chat-Kanal-Manager können Sie Chatkanäle erstellen, bearbeiten oder löschen. Führen Sie die folgenden Schritte aus, um einen Chatkanal in Microsoft Teams zu verwalten:

1. Wählen Sie aus **Zusammenarbeit** Registerkarte.
2. Navigieren zu **Chatkanalmanager** > **Neuen Kanal erstellen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Fügen Sie eine neue hinzu **Kanalname** , **Beschreibung** , Und wählen Sie aus **Mitglieder** Für den Kanal.
4. Wählen Sie **Erstellen** aus.

> **Hinweis:**
> Im Abschnitt „Microsoft Teams-Kanäle“ der Microsoft Teams-Anwendung wird ein neuer Kanaldatensatz erstellt, und derselbe Datensatz wird in MSIM wiedergegeben.

5. Um einen Chatkanal zu bearbeiten, wählen Sie in der Liste Chatkanal-Manager einen Chatkanal aus.
6. Sie können den Kanalnamen, die Mitgliederliste und die Gruppenmitgliederliste entsprechend Ihren Anforderungen ändern.
7. Wählen Sie **Speichern**.
8. Um einen Chatkanal zu löschen, wählen Sie in der Liste Chatkanal-Manager einen Chatkanal aus.
9. Wählen Sie Aus **Kanal Löschen** .

Team umbenennen

Führen Sie die folgenden Schritte aus, um ein Team in Microsoft Teams umzubenennen:

1. Wählen Sie aus **Zusammenarbeit** Registerkarte.
2. Navigieren zu **Chatkanalmanager** > **Team umbenennen**an.
3. Benennen Sie das Team im Feld Teamname entsprechend Ihren Anforderungen um.
4. Wählen Sie **Speichern**.

> **Hinweis:**
> Durch das Umbenennen des Teamnamens wird auch der Teamname in Microsoft Teams umbenannt.

Teammitglieder verwalten

Mit dem Chat-Kanal-Manager können Sie Teammitglieder in Microsoft Teams hinzufügen oder entfernen. Sie können Mitglieder auch über Gruppen hinzufügen. Führen Sie die folgenden Schritte aus, um Teammitglieder in Microsoft Teams zu verwalten:

1. Wählen Sie aus **Zusammenarbeit** Registerkarte.
2. Navigieren zu **Chatkanalmanager** > **Teammitglieder verwalten**an.
3. Fügen Sie im Feld Mitglieder Teammitglieder entsprechend Ihren Anforderungen Teammitglieder hinzu oder entfernen Sie sie.
4. Wählen Sie im Feld Mitglieder über Gruppen hinzufügen die Gruppen aus, die Sie in Microsoft Teams hinzufügen möchten.

> **Hinweis:**
> Wenn sich die Gruppenmitglieder bereits im Team befinden, werden diese Mitglieder nicht hinzugefügt.

5. Wählen Sie **Speichern**.

   Der Chat-Kanal-Manager zeigt die Details der Gesamtanzahl der Teammitglieder und die Anzahl der neuen Mitglieder an, die hinzugefügt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwalten Sie die Kommunikation von Chatkanälen mit Slack

Der Chat-Kanal-Manager zeigt Slack mit mehreren Kanälen an, die in der Slack-Anwendung basierend auf dem Setup einer Konfigurationsvorlage erstellt wurden.

Diese konfigurierten Kanäle werden zusammen mit den Anwendern und Anwendergruppen, die ihnen zugewiesen sind, in der Komponente „Chat-Management“ angezeigt. Mit dem Chat-Kanal-Manager können Sie Folgendes tun **Verwalten Sie Chatkanäle** . Das Team und die Kanäle werden basierend auf der Chat-Kanalkonfiguration in Slack erstellt.

Verwalten Sie Chatkanäle

Mit dem Chat-Kanal-Manager können Sie Chatkanäle in Slack erstellen, bearbeiten oder löschen. Führen Sie die folgenden Schritte aus, um einen Chatkanal zu verwalten:

1. Wählen Sie aus **Zusammenarbeit** Registerkarte.
2. Navigieren zu **Chatkanalmanager** > **Neuen Kanal erstellen**an.
3. Fügen Sie eine neue hinzu **Kanalname** , **Beschreibung** , Und wählen Sie aus **Mitglieder** Für den Kanal.
4. Wählen Sie **Erstellen** aus.

> **Hinweis:**
> Im Abschnitt „Slack-Kanäle“ der Slack-Anwendung wird ein neuer Kanaldatensatz erstellt, und derselbe Datensatz wird in MSIM wiedergegeben.

5. Um einen Chatkanal zu bearbeiten, wählen Sie in der Liste Chatkanal-Manager einen Chatkanal aus.
6. Sie können den Kanalnamen, die Mitgliederliste und die Gruppenmitgliederliste entsprechend Ihren Anforderungen ändern.
7. Wählen Sie **Speichern**.
8. Um einen Chatkanal zu löschen, wählen Sie in der Liste Chatkanal-Manager einen Chatkanal aus.
9. Wählen Sie Aus **Kanal Löschen** .

Verwalten Sie Aktivitätenstrom-Konversationen

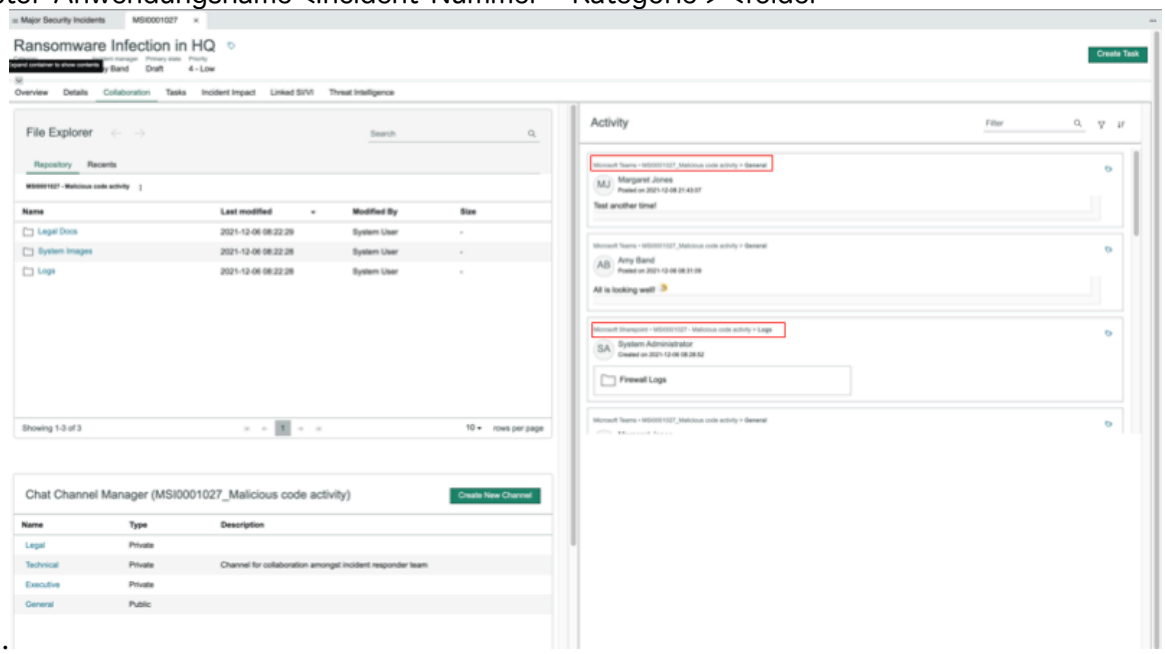
Zeigt alle Aktivitäten, Protokolle und Status an, die für ausgeführt wurden Microsoft SharePoint, Datei-Explorer und Microsoft Teams.

Wenn Sie eine bestimmte Aktivität anzeigen oder die Details der Zusammenarbeitsaktivität durchsuchen möchten, die zwischen verschiedenen Dateien und Ordnern und auch in Microsoft Teams interagiert wurden, können Sie die Filterfunktion verwenden, die oben rechts im Abschnitt „Aktivitätenstrom“ angezeigt wird, und die gewünschten Aktivitätsdetails suchen.

Ordner und Chatkonversationen, die für das Management schwerwiegender Security Incidents freigegeben werden, werden als Breadcrumbs mit folgender Struktur angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

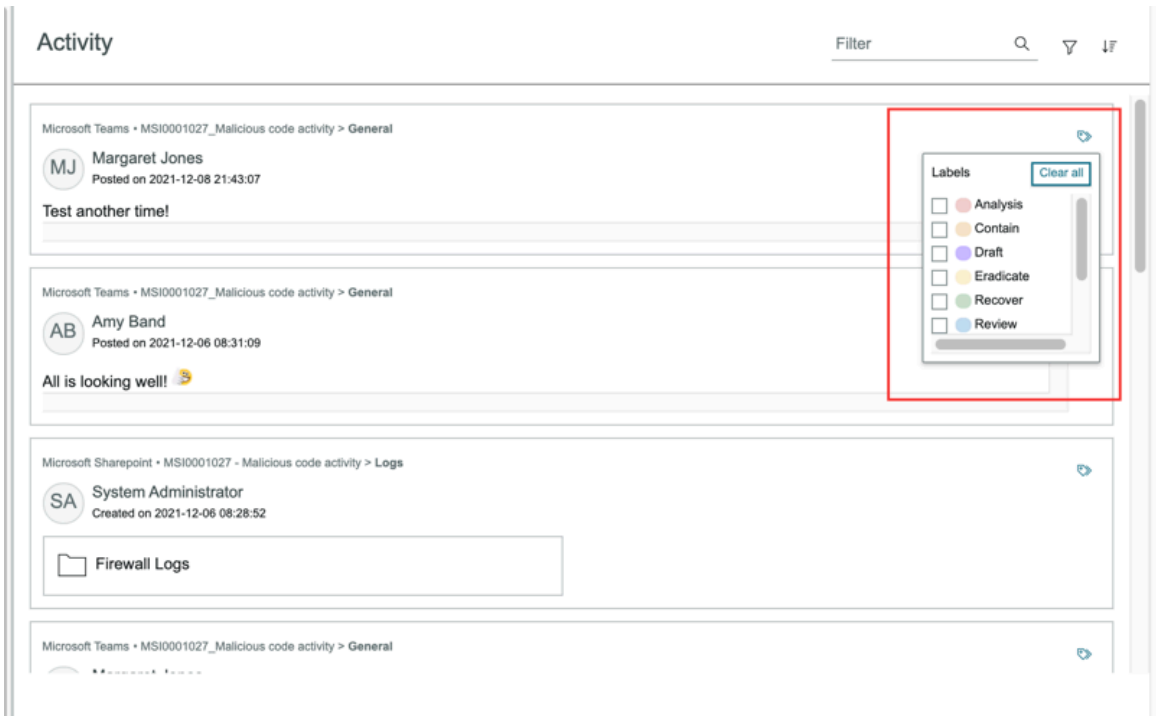
Connector-Anwendungsname <Incident-Nummer – Kategorie > <folder



name>).

Benennen Sie die Aktivitäten :

1. Klicken Sie auf **Bezeichnung** Symbol.
2. Aktivieren Sie das Kontrollkästchen entsprechende Incident-Aktivitätsbezeichnung, wie im folgenden Screenshot angezeigt.



3. Die gekennzeichneten Aktivitäten sind farbcodiert und als Fortschrittstrenddiagramm auf der dargestellt **Externe Zusammenarbeit** Abschnitt des Arbeitsbereichs.

Erstellen und verteilen MSIM Statusberichte

Als Major Security Incident manager, Sie können die verschiedenen Statusberichte erstellen und in verschiedenen Intervallen basierend auf der konfigurierten Berichtsvorlage oder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einem vorherigen Statusbericht während der Lösung schwerwiegender Security Incidents an verschiedene Stakeholder verteilen.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

Sie können eine Vorschau der zuvor konfigurierten Datenelemente des Zusammenfassungsberichts anzeigen, zusätzlichen Text oder eine Zusammenfassung hinzufügen, einzelne Berichtskomponenten nach Bedarf entfernen und die Richtigkeit und Vollständigkeit des Berichts überprüfen, bevor Sie ihn an verschiedene Stakeholder verteilen.

Erstellen Sie die Statusberichte, indem Sie die gewünschte Berichtsvorlage auswählen, die ursprünglich auf der Setup-Seite für MSI-Berichtsvorlagen konfiguriert wurde.

Prozedur

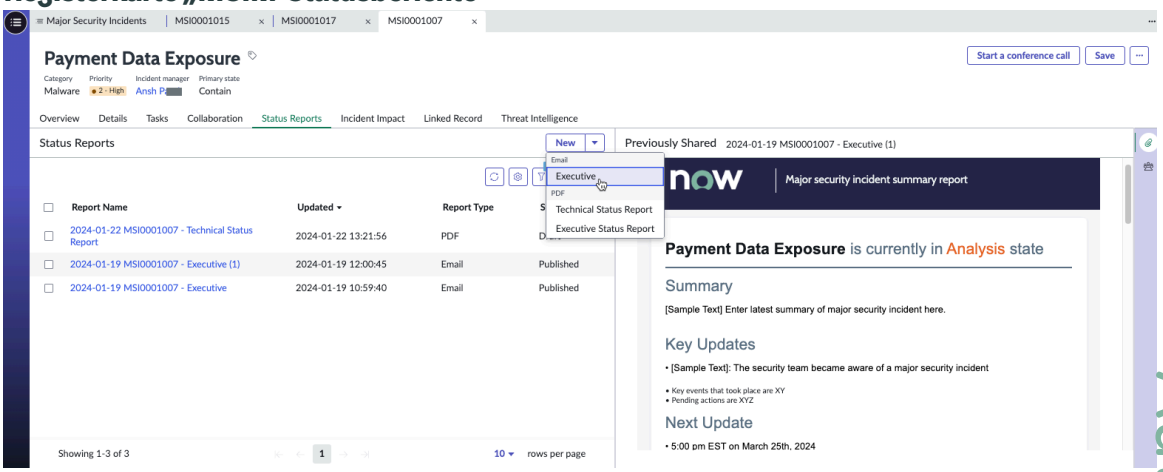
1. Navigieren zu **Arbeitsbereiche** > **Management schwerwiegender Sicherheits-Incidents** > **Schwerwiegende Security Incidents**an.
2. Wählen Sie aus **Listen** Anzeigen.
3. Wählen Sie den entsprechenden heraufgestuften MSI-Datensatz aus.
4. Wählen Sie aus **Statusberichte** Registerkarte.
   Die Registerkarte Statusberichte enthält drei verschiedene Arten von Unterabschnitten, z. B. unten.

Feld	Beschreibung
Berichtname	Name der Statusberichtvorlage. **Hinweis:** In der Ansicht Statusberichte werden die vorhandenen vordefinierten Berichtsvorlagen aufgelistet, die als Teil des Basissystems für die betroffene Persona verfügbar sind. Zum Beispiel Statusberichte für Führungskräfte per E-Mail (mobil-freundlich), Berichte zum technischen Status und Statusberichte für Führungskräfte als PDFs.
Aktualisiert	Das Datum, an dem die Berichtsvorlage zuletzt aktualisiert wurde.
Berichtstyp	Typ des Statusberichts. Der Statusbericht kann einen der folgenden Typen haben: ○ PDF ○ E-Mail
Status	Status der Statusberichte. Die Statusberichte können sich in einem der folgenden status befinden: ○ Entwurf ○ In der Warteschlange ○ Veröffentlicht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie den Typ des Statusberichts aus, den Sie anzeigen oder auswählen möchten **Neu** Dient zum Erstellen eines Statusberichts.

Registerkarte „MSIM-Statusberichte“



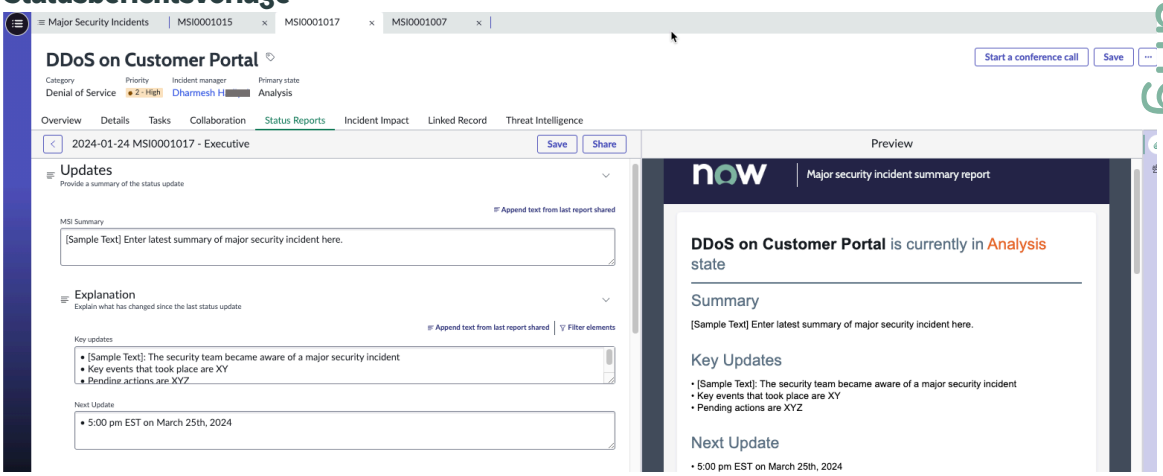
6. Wählen Sie einen der folgenden Statusberichtstypen aus der Liste aus.
   - **Führungskraft** E-Mail-Statusberichte, die für Mobilgeräte geeignet sind.
   - **Technischer Statusbericht** PDF
   - **Statusbericht Für Führungskräfte** PDF

Hinweis:
Wenn Sie eine gewünschte Berichtsvorlage auswählen, wird die Vorschau des ausgewählten Berichts sofort im rechten Bereich generiert. Sie können den ausgewählten Statusbericht des MSI anzeigen.

7. Füllen Sie in der Vorlage „E-Mail-Statusbericht für Führungskräfte“ die Abschnitte mit den Details des Statusberichts aus.

Hinweis:
Die Optionen, die Sie im Abschnitt „Statusberichte“ ausgewählt haben, sind die gleichen Optionen, die im Vorschaubericht gerendert werden.

Statusberichtsvorlage



8. Wählen Sie Aus **Speichern** Um die Aktualisierungen zu speichern, die Sie am Statusbericht vorgenommen haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wählen Sie Aus **Freigeben** Um den Statusbericht für interne und externe Stakeholder freizugeben.
   Das Dialogfeld Freigeben wird angezeigt.

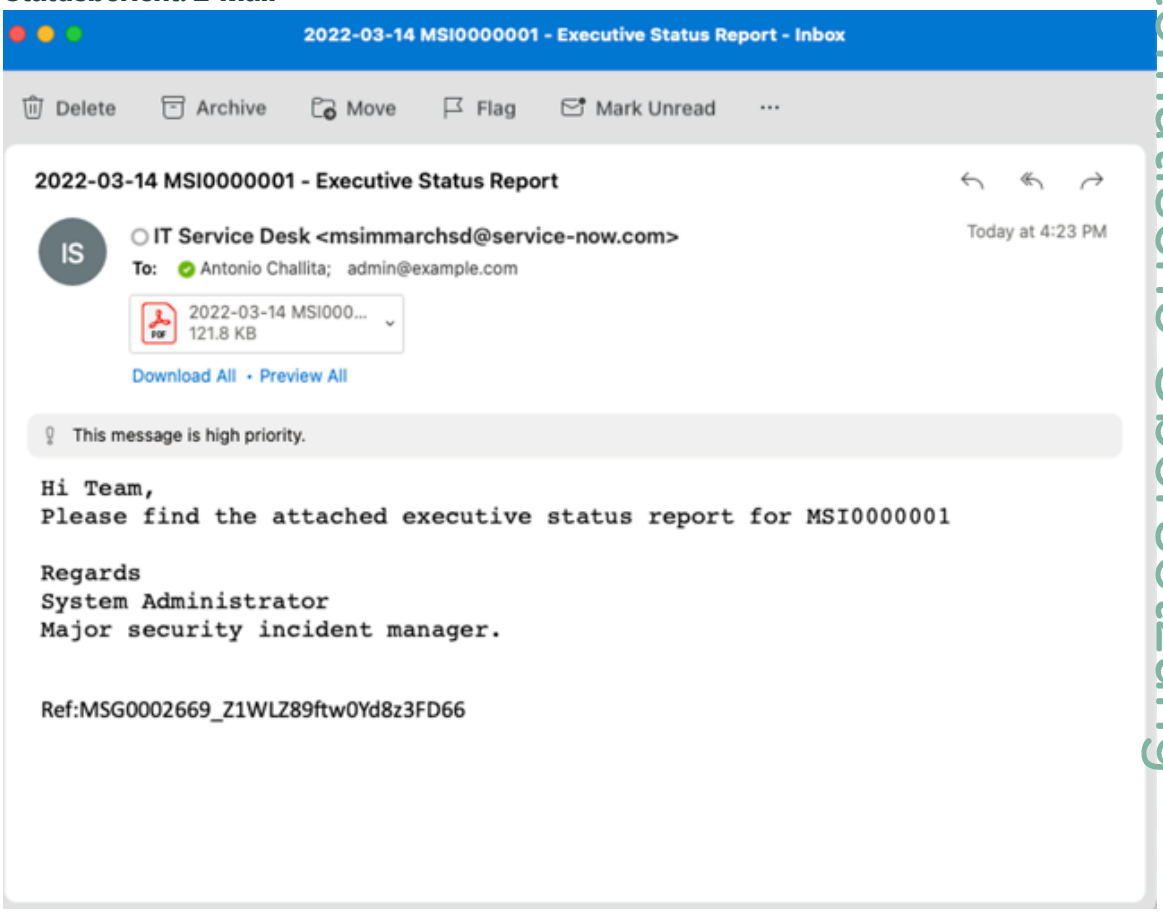
   a. Geben Sie im Feld Betreff den Betreff für den E-Mail-Bericht ein.

   b. Geben Sie im Feld interne Empfänger hinzufügen die Empfänger für den E-Mail-Bericht ein, und wählen Sie sie aus.

   c. Geben Sie im Feld externe Empfänger hinzufügen die E-Mail-Adresse oder DL der Empfänger für den E-Mail-Bericht ein.
   Sie können mehrere E-Mail-IDs mithilfe eines Kommas oder Semikolons hinzufügen.

10. Wählen Sie Aus **E-Mail-Bericht** .
    Eine E-Mail mit dem angehängten PDF-Statusbericht wird erfolgreich an den betreffenden Empfänger gesendet, damit er ihn verifizieren kann.

Statusbericht: E-Mail



11. Sie können auch die folgenden Aktionen auf der Registerkarte Statusberichte ausführen:

    a. Verwenden Sie **Aktualisieren** Aktion in der Ansicht „Statusberichte“, um die Liste der Statusberichte zu aktualisieren.

    b. Verwenden Sie **Listenaktionen** Aktion in der Ansicht „Statusberichte“ zum Bearbeiten von Spalten oder Zurücksetzen der Breiten der Liste „Statusberichte“.

    c. Verwenden Sie **Filter** Aktion in der Ansicht „Statusberichte“, um die Statusberichte basierend auf bestimmten Bedingungen zu filtern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Konfigurieren Major Security Incident Statusberichte

Verwalten MSIM Statusberichte

Statusberichte bieten vorkonfigurierte Trenddiagramme mit umsetzbaren Datenvisualisierungen, um Sicherheitsprozesse zu verbessern, die Lösungszeitleiste, die Anzahl der überfälligen Aufgaben und den Status jeder zugewiesenen Aufgabe zu messen und zu analysieren.

Konfigurieren Major Security Incident Statusberichte

Konfigurieren Sie Berichte zu schwerwiegenden Security Incidents, um die Berichte gemäß Ihren Geschäftsanforderungen während des gesamten Lebenszyklus des Korrekturprozesses für Datensätze zu schwerwiegenden Security Incidents einzurichten und herunterzuladen.

Sie können die Berichtsvorlagen mit einem bestimmten Format und Layout erstellen und diese Berichte mit der Funktion „Statusberichte“ des an Ihre spezifischen Anforderungen anpassen Management schwerwiegender Sicherheits-Incidents Arbeitsbereich.

Ein Anwender mit der Rolle „sn_msi.Workspace_Manager“ kann die Berichtsvorlagen erstellen und konfigurieren, die die Art der Berichtsinformationen beschreiben, die zum Generieren aller Statusberichte verwendet werden können, die für bestimmte Anwender wie Führungskräfte und Rechtsabteilungen freigegeben werden können, und diese Vorlagen den Datensätzen schwerwiegender Security Incidents zuordnen.

Um Ihre MSI-Statusberichte anzupassen, müssen Sie zuerst die Berichtsvorlagen mit einrichten **Berichtsvorlagen** . Mit Berichtsvorlagen können Sie die Berichtsvorlagentypen erstellen, die Berichtskomponenten für diese Berichtsvorlagen definieren, zusätzliche Informationen hinzufügen, visualisierte Daten erstellen, um den Umfang und die Fortschrittsmetriken nachzuverfolgen, zugehörige Listendaten hinzufügen und Statusberichte generieren.

Im Folgenden werden die Standardfelder beschrieben, die in allen Berichtsvorlagentypen bereitgestellt werden. Sie können die Berichtsvorlage basierend auf Ihren Anforderungen mithilfe von Abschnitten, Unterabschnitten und zugehörigen Elementen konfigurieren und formatieren:

Statusberichtskomponenten

Komponententyp	Beschreibung
Berichtstitel	Titel des Berichtstyps. Das Standardformat des Berichtstyps lautet beispielsweise: {MSI-Nummer} – {Stakeholder-Bericht für Führungskräfte} dargestellt als MSI0001001: Stakeholder-Bericht für Führungskräfte.
Name	Zeigt den Namen des Anwenders an, der den Bericht im Abschnitt „Statusberichte“ des Arbeitsbereichs „Management schwerwiegender Security Incidents“ generiert hat.
Zusammenfassung	Zeigt eine kurze Zusammenfassung des Berichts an.
Datum	Zeigt das Datum an, an dem der Bericht für den betreffenden Empfänger freigegeben wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Statusberichtskomponenten (Fortsetzung)

Komponententyp	Beschreibung
Fortschritt	Zeigt den Umfang und die Fortschrittsmetriken an, z. B. die verknüpften SIR-Incidents, Antwortaufgaben, ergänzende Aufgaben, externe Zusammenarbeit, Zeitleistenkomponenten, und letzte Zeitleistenereignisse.
Herausforderungen	In diesem Abschnitt wird eine kurze Beschreibung der Herausforderungen angezeigt, die während des Korrekturprozesses für schwerwiegende Security Incidents auftreten.
Nächste Schritte	In diesem Abschnitt wird eine kurze Beschreibung der nächsten Schritte zur Lösung des schwerwiegenden Security Incident angezeigt. Beispielsweise enthält der Unterabschnitt „aktives Team“ im Stakeholder-Bericht für Führungskräfte Informationen zum nächsten Schritt der Teamzuweisung, wer an der weiteren Analyse des Datensatzes für schwerwiegende Security Incidents beteiligt ist.
Andere Anpassungen	Die Berichtsvorlage bietet Ihnen auch die Möglichkeit, das Logo hochzuladen und die Kopf- und Fußzeilen im Bericht anzupassen.

Im Folgenden sind die Arten von Berichtskategorien aufgeführt, die eingerichtet und angezeigt werden können:

- **Führungskraft** E-Mail
- **Technischer Statusbericht** PDF
- **Statusbericht Für Führungskräfte** PDF

Die obigen Berichte sind konfiguriert und stehen dem Anwender zur Auswahl, Anzeige und Generierung des Berichts aus dem Arbeitsbereich „Management schwerwiegender Security Incidents“ zur Verfügung.

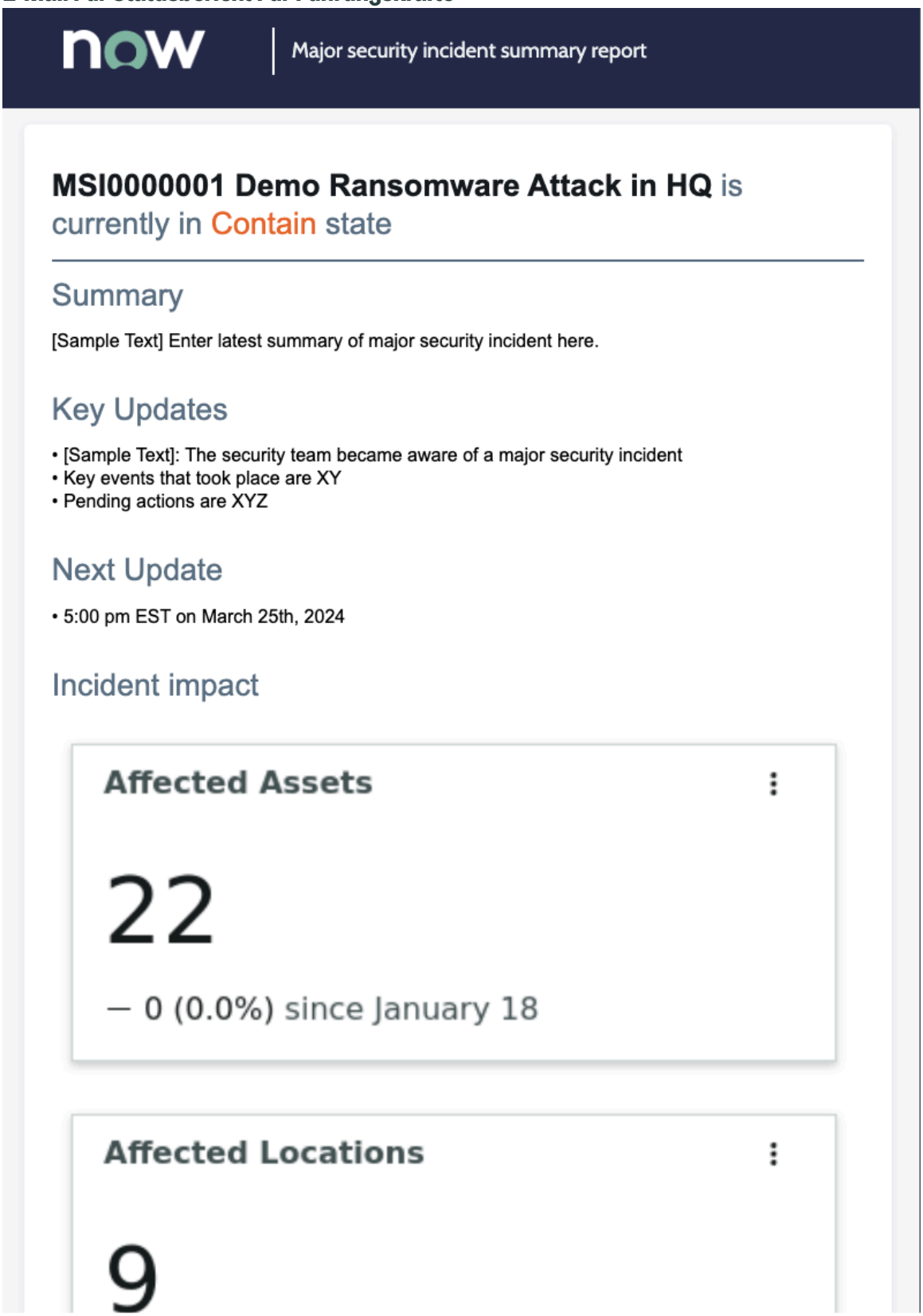
Mobile-freundliche Statusberichte für Führungskräfte – E-Mail

Die Statusberichte für Führungskräfte – E-Mail sind mobile-freundliche Statusberichte, die im E-Mail-Format generiert werden. Der Berichtsabschnitt enthält eine Zusammenfassung des Berichts, die Spalte „MSI-Dauer“, den Umfang/die Auswirkung des Incident, aktive Teammetriken, Fortschrittsmetriken, und Zeitleistenkomponenten, z. B. die letzten Zeitleistenereignisse für diesen spezifischen Datensatz für schwerwiegende Security Incidents.

Passen Sie die folgenden Berichtsvorlagenfunktionen an, und konfigurieren Sie sie, um dem Bericht zusätzliche Informationen hinzuzufügen. Ein Beispiel für einen E-Mail-Statusbericht für Führungskräfte wird unten zu Ihrer Referenz angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail Für Statusbericht Für Führungskräfte



Automatische Übersetzung

Statusberichte für Führungskräfte: PDF

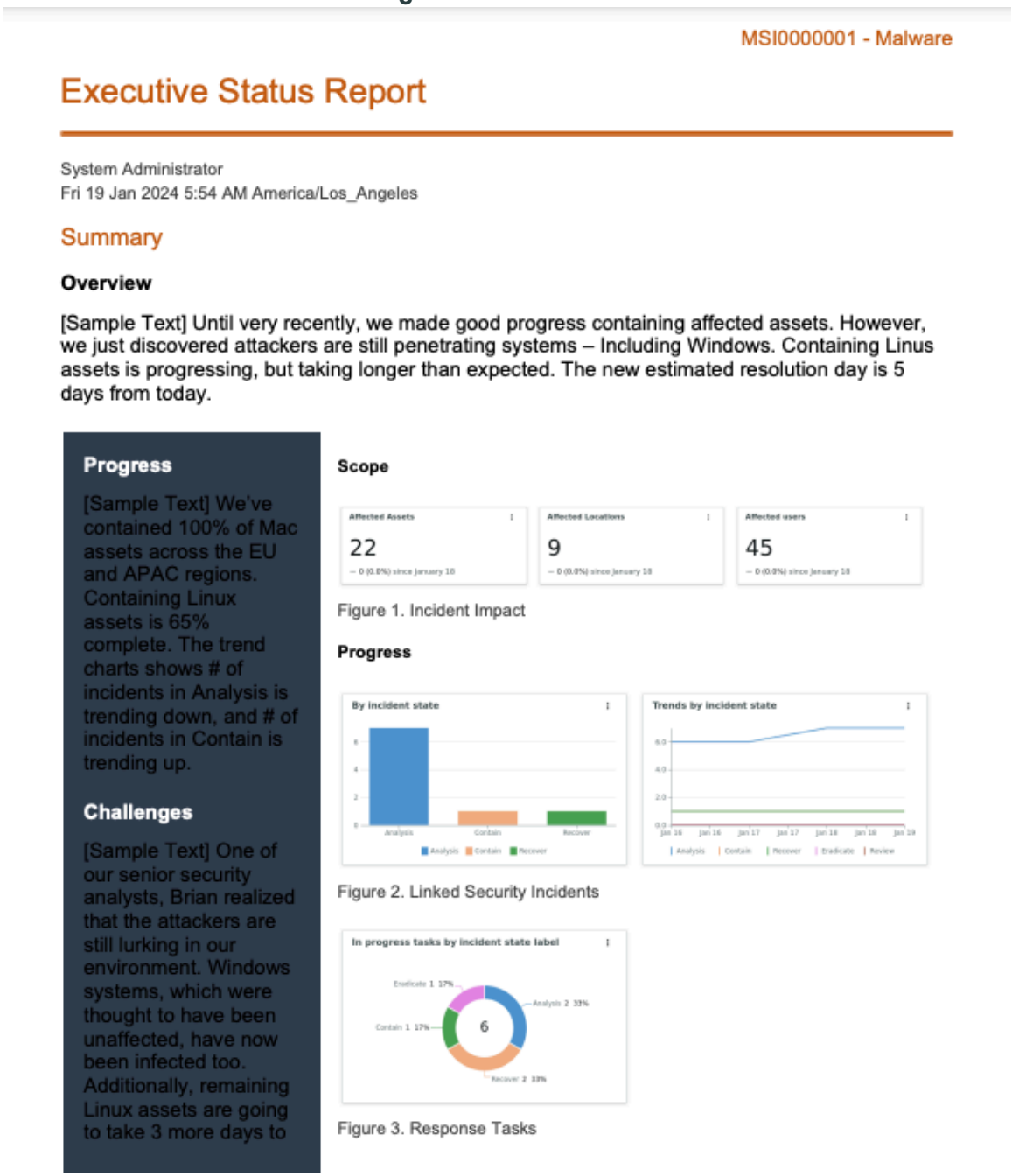
Die Statusberichte für Führungskräfte – PDF sind Statusberichte, die im PDF-Format generiert werden. Der Berichtsabschnitt enthält eine Zusammenfassung des Berichts, die Spalte „MSI-Dauer“, den Umfang/die Auswirkung des Incident, aktive Teammetriken,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fortschrittsmetriken, und Zeitleistenkomponenten, z. B. die letzten Zeitleistenereignisse für diesen spezifischen Datensatz für schwerwiegende Security Incidents.

Passen Sie die folgenden Berichtsvorlagenfunktionen an, und konfigurieren Sie sie, um dem Bericht zusätzliche Informationen hinzuzufügen. Ein Beispiel für einen Executive-Bericht wird unten zu Ihrer Referenz angezeigt.

PDF-Bericht zum Status der Führungskraft



MSI0000001 - Malware

Executive Status Report

System Administrator
Fri 19 Jan 2024 5:54 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

In progress tasks by incident state label
6

Figure 3. Response Tasks

Berichte zum technischen Status: PDF

Die technischen Statusberichte – PDF sind Statusberichte, die im PDF-Format generiert werden. Der Berichtsabschnitt enthält eine Zusammenfassung des Berichts, die Spalte „MSI-Dauer“, den Umfang/die Auswirkung des Incident, aktive Teammetriken, Fortschrittsmetriken, und Zeitleistenkomponenten, z. B. die letzten Zeitleistenereignisse für diesen bestimmten Datensatz für schwerwiegende Security Incidents, mit Aufgabenaktualisierungen und mit Aktivitäten bezeichnete, basierend auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Zuweisungsgruppe und der ausgewählten Tag-Bezeichnung seit der Generierung des letzten Statusberichts sowie zusätzliche Informationen wie Auswirkung auf Incidents und verknüpfte Incidents.

Passen Sie die Berichtsvorlage an, und konfigurieren Sie sie, um dem Bericht zusätzliche Informationen hinzuzufügen. Ein Beispiel für einen technischen Bericht, der die zusätzlichen Informationen enthält, z. B. die Auswirkung auf den Incident, ist unten als Referenz dargestellt, und der verbleibende Teil des Berichts ähnelt den Geschäftsberichten.

Technischer Statusbericht: PDF

MSI0000001 - Malware

System Admins Status Report

System Administrator
Fri 19 Jan 2024 6:00 AM America/Los_Angeles

Summary

Overview

[Sample Text] Until very recently, we made good progress containing affected assets. However, we just discovered attackers are still penetrating systems – Including Windows. Containing Linus assets is progressing, but taking longer than expected. The new estimated resolution day is 5 days from today.

Progress

[Sample Text] We've contained 100% of Mac assets across the EU and APAC regions. Containing Linux assets is 65% complete. The trend charts shows # of incidents in Analysis is trending down, and # of incidents in Contain is trending up.

Challenges

[Sample Text] One of our senior security analysts, Brian realized that the attackers are still lurking in our environment. Windows systems, which were thought to have been unaffected, have now been infected too. Additionally, remaining Linux assets are going to take 3 more days to

Scope

Affected Assets 22
Affected Locations 9
Affected users 45

Figure 1. Incident Impact

Progress

By incident state
Trends by incident state

Figure 2. Linked Security Incidents

Response Tasks by State
In progress tasks by incident state label

Die Berichtsvorlagenabschnitte enthalten verschiedene Unterabschnitte, die beschreiben, wie Sie die Berichtsunterabschnitte und ihre Elemente erstellen können, z. B.:

1. Branding: Fügen Sie Ihren Berichtsvorlagen Branding hinzu
2. Vorlagenskripts: Verwenden Sie Vorlagenskripts in Ihren Berichtsvorlagen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Verwenden Sie Visualisierungen in Berichtsvorlagen
4. Verwenden Sie Berichtslisten in Berichtsvorlagen

Erstellen Sie eine Berichtsvorlage

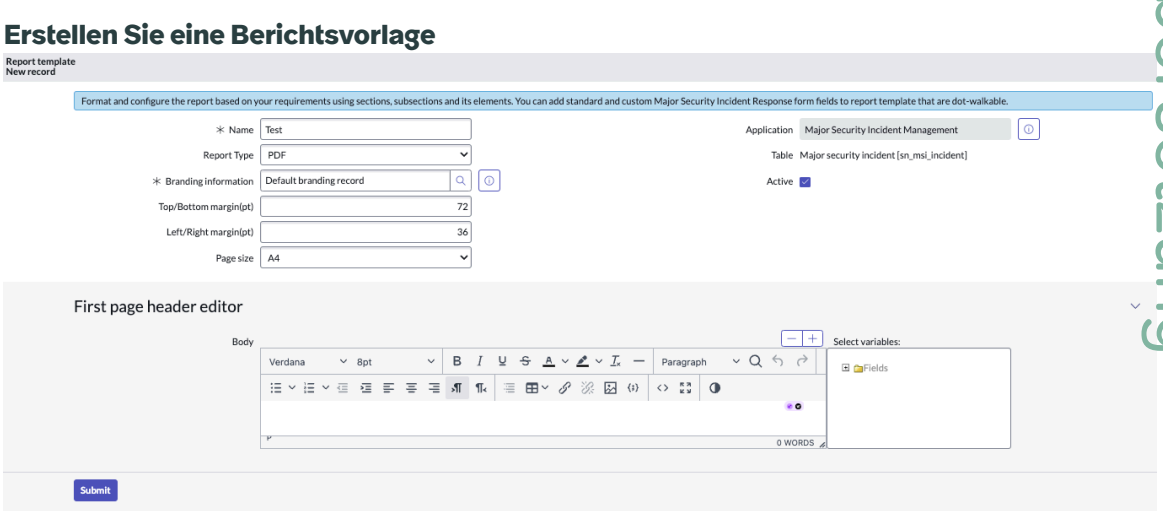
Erstellen Sie verschiedene Berichtsvorlagen, die auf die schwerwiegenden Security Incidents angewendet werden können, und generieren Sie einen Statusbericht. Sie können der Berichtsvorlage standardmäßige und anwenderdefinierte Formularfelder für die Reaktion auf schwerwiegende Security Incidents hinzufügen, die Dot-Walking-fähig sind. Darüber hinaus können Sie den Bericht basierend auf Ihren Anforderungen mithilfe von Abschnitten, Unterabschnitten und zugehörigen Elementen formatieren und konfigurieren.

Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_Manager

Warum und wann dieser Vorgang ausgeführt wird
Sie können Berichtskomponenten für Ihre Berichtsvorlagen definieren und zusätzliche Informationen bereitstellen. Erstellen Sie visualisierte Daten, um den Umfang und die Fortschrittsmetriken nachzuverfolgen, zugehörige Listendaten hinzuzufügen, eine Vorschau anzuzeigen und die Statusberichte zu generieren oder freizugeben.

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Seite „Setup des MSI-Statusberichts“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage die Option aus **Konfigurieren** .
3. Wählen Sie Aus **Neu** Dient zum Erstellen einer Berichtsvorlage.
4. Füllen Sie die Felder im Formular „Berichtsvorlage“ aus.



5. **Übermitteln** Der neue Berichtsvorlagendatensatz.
   Eine neue Berichtsvorlage wird auf der Seite „Berichtsvorlagen“ erstellt.

Zugehörige Informationen

Erstellen und verteilen MSIM Statusberichte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie Ihren Berichtsvorlagen Branding hinzu

Fügen Sie Ihren Berichten Branding hinzu. Sie können Kopf- und Fußzeilenbild sowie Kopf- und Fußzeilentext hinzufügen. Sie können diese Branding-Informationen in einen der Berichtsvorlagentypen einfügen, die Sie erstellen möchten, wenn Sie andere als die beiden vordefinierten Berichte erstellen möchten.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

Warum und wann dieser Vorgang ausgeführt wird

Die wichtigsten Überlegungen beim Hinzufügen von Branding zu Ihren Berichtsvorlagen lauten wie folgt:

- Laden Sie das Kopf- und Fußzeilenbild hoch, und richten Sie die Bildposition aus.
- Die maximale Größenbeschränkung für Kopf- und Fußzeilenbild beträgt 5 MB. Wenn die Größe den angegebenen Grenzwert überschreitet, wird im schwerwiegenden Security Incident die Fehlermeldung „Bildformat kann nicht erkannt werden“ angezeigt.
- Passen Sie die Höhe der Kopf- und Fußzeilenbilder an.
- Die Länge des Fußzeilentexts ist auf 100 Zeichen beschränkt.

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
2. Drilldown zu **Berichtsvorlage** > **Branding**an.
3. Wählen Sie **Konfigurieren**.
4. Wählen Sie Aus **Neu** Um Ihrer Berichtsvorlage ein Branding hinzuzufügen.
5. Füllen Sie die Felder im Formular „Branding-Vorlage“ aus.
6. Wählen Sie **Absenden**.
   Eine neue Branding-Vorlage wird auf der Seite Branding-Vorlagen erstellt.

Verwenden Sie Visualisierungen in Berichtsvorlagen

Verwenden Sie Berichts-Widgets, um UIB-Elemente (User Interface Builder) wie Datenvisualisierungen in die MSIM-Statusberichte zu definieren und einzubeziehen.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

Prozedur

1. Navigieren zu **Alle** > **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Seite „Setup des MSI-Statusberichts“ wird angezeigt.
2. Drilldown zu **Berichtsvorlage** > **Visualisierungen**an.
3. Wählen Sie **Konfigurieren**.
   Im Folgenden finden Sie die vordefinierten UIB-Visualisierungen als Teil des Basissystems, mit denen Sie Ihre Statusberichte konfigurieren und ändern können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erstellen Sie ein Visualisierungstyp-Element

Verwenden Sie Berichtslisten in Berichtsvorlagen

Verwenden Sie Berichtslisten, um die zugehörigen Listenartefakte zu definieren und einzubeziehen, um Listen in der PDF basierend auf Ihren konfigurierten MSI-Listendatensätzen zu generieren.

Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_Manager

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Seite „Setup des MSI-Statusberichts“ wird angezeigt.
2. Drilldown zu **Berichtsvorlage** > **Listen**an.
3. Wählen Sie **Konfigurieren**.
   Im Abschnitt „Listen der MSI-Statusberichte“ wird beschrieben, wie sich die einzelnen zugehörigen Listen seit der Erstellung des Incident auswirken. Im Folgenden finden Sie die vordefinierten MSI-Berichtslisten als Teil des Basissystems, mit denen Sie Ihre Statusberichte konfigurieren und ändern können.

Zugehörige Informationen

Erstellen Sie ein Listentypelement

Verwenden Sie Vorlagenskripts in Ihren Berichtsvorlagen

Erstellen Sie ein Skript, um die Daten der zugehörigen Listen, Datumsvorgänge und alle anderen Daten einzubeziehen, die nicht direkt per Dot-Walking ausgeführt werden können.

Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_Manager

Warum und wann dieser Vorgang ausgeführt wird
Sie können dieses vordefinierte Vorlagenskript in Ihren Berichtsvorlagen verwenden, um alle zugehörigen Daten einzubeziehen, nachdem die Berichtsvorlagen konfiguriert und angepasst wurden.

Erstellen Sie ein Vorlagenskript, um die zugehörigen Listendaten in der Berichtsvorlage anzuzeigen. Wenn Sie ein Vorlagenskript verwenden und ausfüllen möchten, müssen Sie das Tag-Vorlagenskript-Tag hinzufügen als: `${template_script:script Name}` .

Beispiel: `${template_script:msi_collab_cards}`

Hinweis:
Sie können die vordefinierten Vorlagenskripts nicht löschen. Eine Fehlermeldung wird angezeigt, wenn ein Anwender mit einer Administratorrolle versucht, einen Vorlagenskriptdatensatz zu löschen, wenn er einer Berichtsvorlage zugeordnet ist.

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Seite „Setup des MSI-Statusberichts“ wird angezeigt.
2. Drilldown zu **Berichtsvorlage** > **Vorlagenskripts**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Konfigurieren**.
   Im Folgenden finden Sie die vordefinierten Vorlagenskripts als Teil des Basissystems, mit denen Sie Ihre Statusberichte konfigurieren und ändern können.

   Hinweis:
   Sie können auch ein eigenes Vorlagenskript erstellen, um zusätzlich zu den aufgeführten Vorlagenskripts die Daten der zugehörigen Listen, Datumsvorgänge und andere Daten einzubeziehen, die nicht direkt per Dot-Walking ausgeführt werden können.

Zeigen Sie eine Vorschau der Berichtsvorlage an

Verwenden Sie die Vorschaufunktion, um eine Vorschau Ihrer Entwurfszeitberichtsvorlage anzuzeigen, um den Bericht während der Laufzeit aus zu generieren und für andere Stakeholder freizugeben Management schwerwiegender Sicherheits-Incidents Arbeitsbereich.

Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_Manager

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Seite „Setup des MSI-Statusberichts“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage die Option aus **Konfigurieren** .
3. Wählen Sie die gewünschte Berichtsvorlage aus.
4. Wählen Sie den Berichtstyp als aus **E-Mail** Oder **PDF** Basierend auf Ihren Anforderungen.
5. Wählen Sie aus **Speichern Sie den Bericht, und zeigen Sie eine Vorschau an** Aktion.

   Das Dialogfeld „Berichtsvorschau“ wird angezeigt.
6. Wählen Sie einen schwerwiegenden Security Incident mithilfe der Suchoption aus, um eine Vorschau eines Berichts mit der ausgewählten Vorlage anzuzeigen.
7. Wählen Sie Aus **Vorschau Des Berichts Anzeigen** .
   Der Bericht generiert eine Vorschau gemäß der ausgewählten Vorlagenkonfiguration. Wenn Sie den Berichtstyp als ausgewählt haben **E-Mail** , Dann wird die Vorschau im E-Mail-Vorlagenformat angezeigt. Die Statusberichte im E-Mail-Format sind für Mobilgeräte geeignet.

Erstellen Sie eine Berichtsabschnittsvorlage

Ein Bericht kann weiter in verschiedene Abschnitte unterteilt werden. Verwenden Sie den Abschnitt „Bericht“, um den Bericht in mehrere Abschnitte aufzugliedern und in der Reihenfolge neu zu organisieren.

Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_Manager

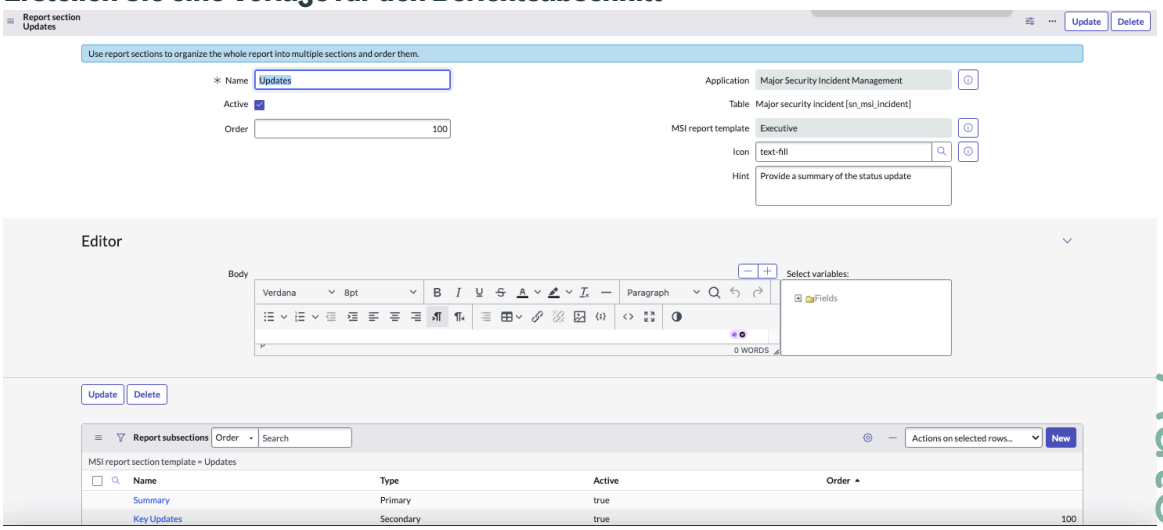
Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Seite „Setup des MSI-Statusberichts“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage die Option aus **Konfigurieren** .
3. Öffnen Sie eine vorhandene Berichtsvorlage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Navigieren zu **Berichtsabschnitte** > **Neu**an.
   Die neue Seite des Berichtsabschnitts wird angezeigt.

Erstellen Sie eine Vorlage für den Berichtsabschnitt



5. Füllen Sie die Felder im Vorlagenformular „Berichtsabschnitt“ aus.

6. Speichern Sie und **Übermitteln** Der neue Berichtsvorlagenabschnitt.

Erstellen Sie eine Berichtsunterabschnittsvorlage

Verwenden Sie den Berichtsunterabschnitt, um den Abschnitt weiter in mehrere Unterabschnitte zu organisieren und ihre Ausrichtung und Position mithilfe der verfügbaren Typen wie Textseitenbereich, Primär und Sekundär zu konfigurieren.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

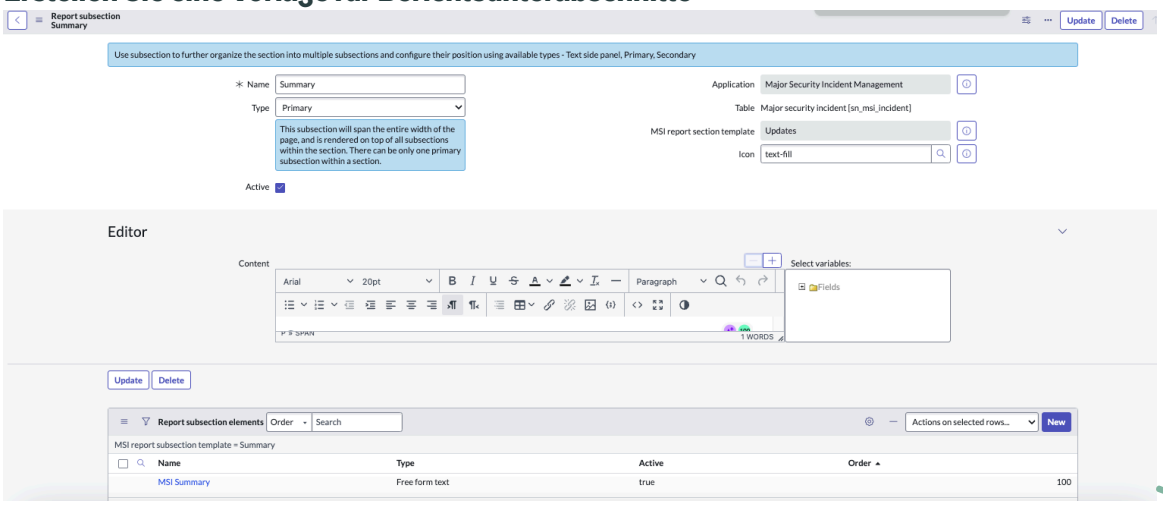
Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Seite „Setup des MSI-Statusberichts“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage die Option aus **Konfigurieren** .
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur Liste der entsprechenden Berichtsabschnitte.
4. Öffnen Sie in der Liste Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Navigieren zu **Berichtsunterabschnitte** > **Neu**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Vorlage für Berichtsunterabschnitte



6. Füllen Sie die Felder im Formular „Bericht“ aus.

7. Speichern Sie und **Übermitteln** Der neue Berichtsvorlagenabschnitt.

Erstellen Sie eine Elementvorlage für den Berichtsunterabschnitt

Verwenden Sie Unterabschnittselemente, um einen Unterabschnitt in mehrere Elemente weiter zu organisieren. Unterabschnittselemente helfen, Visualisierungen, Listen und Freiformtext deklarativer mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen zu definieren.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

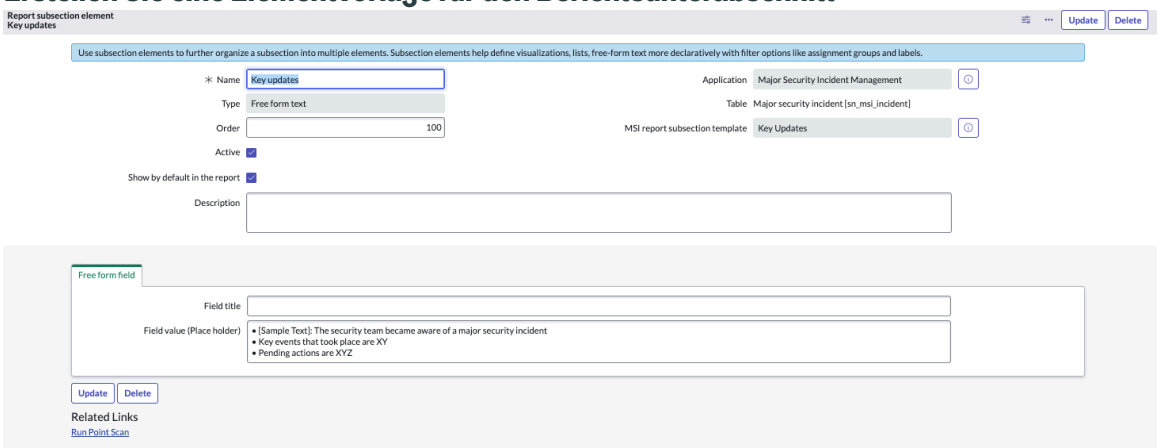
Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Seite „Setup des MSI-Statusberichts“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage die Option aus **Konfigurieren** .
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur Liste der entsprechenden Berichtsabschnitte.
4. Öffnen Sie in der Liste Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste Vorlage für den Berichtsabschnitt eine vorhandene Vorlage für den Berichtsunterabschnitt.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Elementvorlage für den Berichtsunterabschnitt



7. Füllen Sie die Felder im Formular „Elemente des Unterabschnitts Bericht“ aus.

8. Speichern Sie und **Aktualisieren** Der neue Berichtsvorlagenabschnitt.

Erstellen Sie ein Freiformtypelement

Erstellen Sie einen Freiform-Elementtyp, um den Freiform-Text mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer zu definieren.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Seite „Setup des MSI-Statusberichts“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage die Option aus **Konfigurieren** .
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur Liste der entsprechenden Berichtsabschnitte.
4. Öffnen Sie in der Liste Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste Vorlage für den Berichtsabschnitt eine vorhandene Vorlage für den Berichtsunterabschnitt.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**an.
7. Füllen Sie das Formular „Elemente des Berichtsunterabschnitts“ mit den erforderlichen Details aus, wie in erläutert Erstellen Sie eine Elementvorlage für den Berichtsunterabschnitt.
8. Navigieren Sie zum Elementtyp des Berichtsunterabschnitts, und wählen Sie aus **Freiformfeld** Option. Dadurch wird angezeigt **Freiformfeld** Abschnitt.
9. Füllen Sie die Felder auf der Registerkarte Freiform aus.

Erstellen Sie ein Visualisierungstyp-Element

Erstellen Sie einen Visualisierungselementtyp, um die Visualisierungselemente mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen deklarativer zu definieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

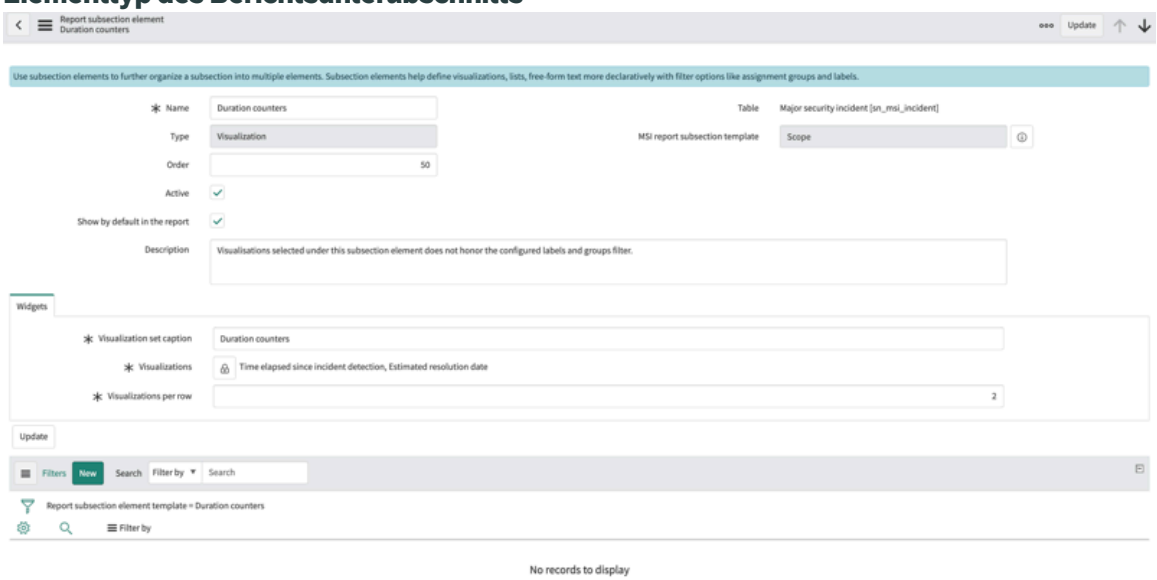
Erforderliche Rolle: sn_msi.Workspace_Manager

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Setup-Seite „MSI-Statusbericht“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage die Option aus **Konfigurieren** .
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur Liste der entsprechenden Berichtsabschnitte.
4. Öffnen Sie in der Liste Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste Vorlage für den Berichtsabschnitt eine vorhandene Vorlage für den Berichtsunterabschnitt.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**an.
7. Füllen Sie das Formular „Elemente des Berichtsunterabschnitts“ mit den erforderlichen Details aus, wie in erläutert Erstellen Sie eine Elementvorlage für den Berichtsunterabschnitt.
8. Navigieren Sie zum Elementtyp des Berichtsunterabschnitts, und wählen Sie aus **Visualisierung** Option. Dadurch wird angezeigt **Visualisierung** Abschnitt.
9. Füllen Sie die Felder im Visualisierungsformular aus.
10. Wählen Sie **Absenden**.

Example: Berichtvorlagen-Unterabschnittselementtyp für einen technischen Statusbericht

Elementtyp des Berichtsunterabschnitts



Erstellen Sie ein Listentypelement

Erstellen Sie ein Listentypelement, das die zugehörigen Listenelemente deklarativer mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen definiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Seite „Setup des MSI-Statusberichts“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage die Option aus **Konfigurieren** .
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur Liste der entsprechenden Berichtsabschnitte.
4. Öffnen Sie in der Liste Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste Vorlage für den Berichtsabschnitt eine vorhandene Vorlage für den Berichtsunterabschnitt.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**an.
7. Füllen Sie das Formular „Elemente des Berichtsunterabschnitts“ mit den erforderlichen Details aus, wie in erläutert Erstellen Sie eine Elementvorlage für den Berichtsunterabschnitt.
8. Navigieren Sie zum Elementtyp des Berichtsunterabschnitts, und wählen Sie aus **Liste** Option.
   Dadurch wird angezeigt **Listen** Abschnitt.
9. Füllen Sie die Felder im Listenformular aus.

Erstellen Sie ein anwenderdefiniertes Typelement

Erstellen Sie ein Listentypelement, das die zugehörigen Listenelemente deklarativer mit Filteroptionen wie Zuweisungsgruppen und Bezeichnungen definiert.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager

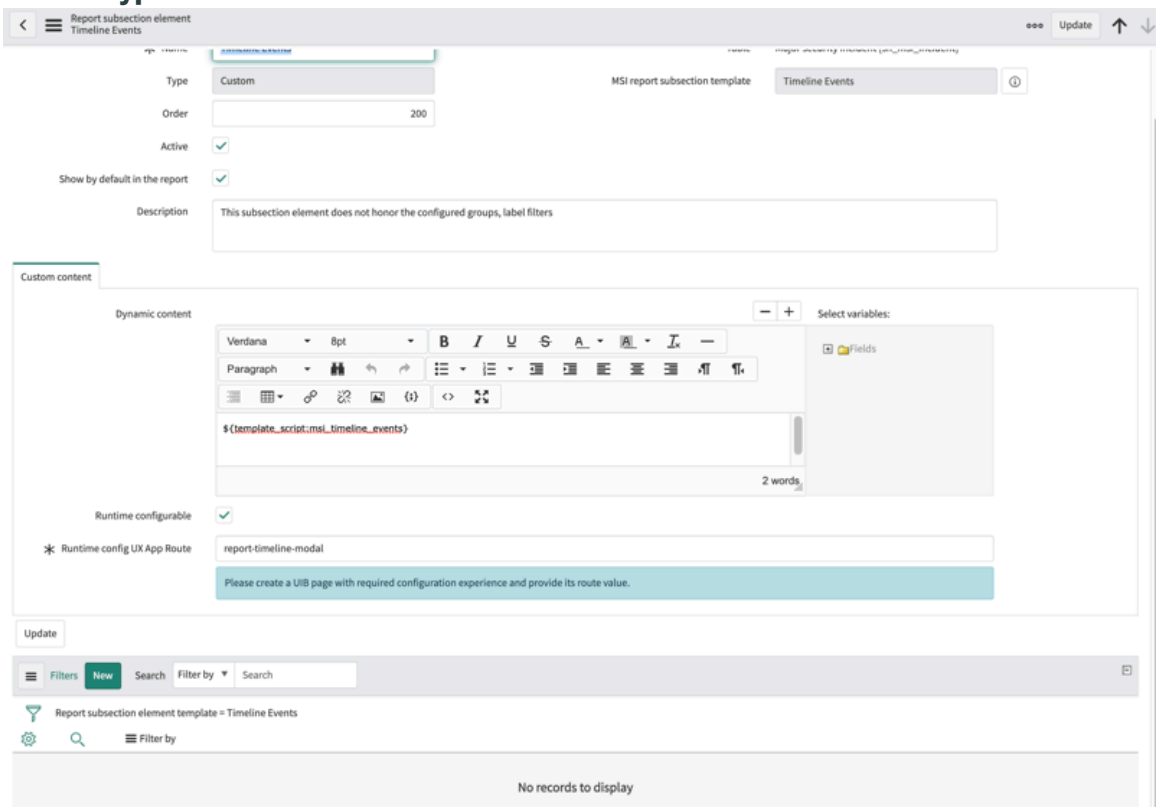
Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **MSI-Administration** > **Statusberichteinrichtung**an.
   Die Seite „Setup des MSI-Statusberichts“ wird angezeigt.
2. Wählen Sie im Abschnitt Berichtsvorlage die Option aus **Konfigurieren** .
3. Öffnen Sie eine vorhandene Berichtsvorlage, und navigieren Sie zur Liste der entsprechenden Berichtsabschnitte.
4. Öffnen Sie in der Liste Berichtsabschnitte eine vorhandene Berichtsabschnittsvorlage.
5. Öffnen Sie in der Liste Vorlage für den Berichtsabschnitt eine vorhandene Vorlage für den Berichtsunterabschnitt.
6. Navigieren zu **Berichtsunterabschnittselemente** > **Neu**an.
7. Füllen Sie das Formular „Elemente des Berichtsunterabschnitts“ mit den erforderlichen Details aus, wie in erläutert Erstellen Sie eine Elementvorlage für den Berichtsunterabschnitt.
8. Navigieren Sie zum Elementtyp des Berichtsunterabschnitts, und wählen Sie aus **Anwenderdefiniert** Option.
   Dadurch wird angezeigt **Anwenderdefinierter Inhalt** Abschnitt.
9. Füllen Sie die Felder im Formular „Anwenderdefinierter Inhalt“ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example: Im Folgenden finden Sie ein Beispiel für den Elementtyp „Berichtsvorlage – Unterabschnitt“ für einen technischen Statusbericht

Elementtyp des Berichtsunterabschnitts



Fügen Sie Systemeigenschaften hinzu

Fügen Sie Systemeigenschaften hinzu, um das Verhalten der MSIM-Anwendung zu steuern. Im Folgenden finden Sie die Standardsystemeigenschaften, die als Teil von eingeführt werden Management schwerwiegender Sicherheits-Incidents Statusberichte.

Systemeigenschaften

Eigenschaftsname	Beschreibung
sn_msi.Export_img	Verwenden Sie diese Eigenschaft, um den Export von Bildern zu steuern. Der Standardwert ist auf EIN festgelegt.
sn_msi.Export_img_log	Verwenden Sie diese Eigenschaft, um die Anmeldung bei der Browserkonsole zu aktivieren. Der Standardwert ist auf „AUS“ festgelegt.
sn_msi.Export_img_parallel_threshold	Verwenden Sie diese Eigenschaft, um die maximale Anzahl paralleler Anforderungen zum Generieren der Bilder aus Berichts-Widget-Konfigurationen zu steuern. Der Standardwert ist auf 14 festgelegt.
sn_msi.img_Export_log	Verwenden Sie diese Eigenschaft, um die Konsolenprotokolle im Browser zu aktivieren.
sn_msi.img_Export_poll_interval	Verwenden Sie diese Eigenschaft, um den Zeitabstand zwischen Abfragen zu steuern, der überprüft, ob das Bild generiert wird oder nicht. Die Standardzeit

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemeigenschaften (Fortsetzung)

Eigenschaftsname	Beschreibung
	des Abfrageintervalls ist auf 3000 Millisekunden festgelegt.
sn_msi.Export_Poll_Request_timeout	Verwenden Sie diese Eigenschaft, um die maximale Zeit zu steuern, die das System nach exportierten Bildern abfragen kann. Der Standardwert ist 120000 Millisekunden.
sn_msi.msi_Report_uib_Element_js_path	Verwenden Sie diese Eigenschaft, um den generischen Pfad zum Erfassen des Bildes aus dem UIB-Seitenteil zu steuern.
sn_msi.Report_default_style_objects	Verwenden Sie diese Eigenschaft, um die CSS der generierten PDFs zu ändern, z. B. Schriftgröße, Schriftfarbe oder Feldwert. Wenn sn_msi.Workspace_Manager beispielsweise die Schriftfarbe des linken Bereichs des generierten PDF-Statusberichts ändern möchte, kann der Arbeitsbereich-Manager die Schriftfarbe der Systemeigenschaft ändern und die PDF-Datei in einer gewünschten Ansicht rendern.

Playbooks Für Das Management Schwerwiegender Security Incidents

Sie können den Playbook-Flow für das Management schwerwiegender Security Incidents automatisch oder manuell aufrufen.

Ein Playbook ist nur sichtbar, wenn mindestens ein Playbook einem Security Incident zugeordnet ist. Die Playbook-Komponente wird nur für den erstellten Prozessautomatisierungs-Designer (PAD) unterstützt. Management schwerwiegender Security Incidents stellt das Playbook für Anfragen an die Rechtsabteilung mit dem Basissystem bereit.

Playbook für Anforderung an die Rechtsabteilung

Das Playbook für Anfragen an die Rechtsabteilung bietet Schritt-für-Schritt-Anleitungen, wie Sie die Rechtsabteilung über die neueste Zusammenfassung eines MSI informieren können, damit sie die SEC innerhalb des 4-tägigen Zeitrahmens benachrichtigen kann, der für wesentliche Verstöße erforderlich ist.

Übersicht

Als Incident-Manager können Sie das Playbook für Anfragen an die Rechtsabteilung verwenden, um die Rechtsabteilung über die neueste Zusammenfassung eines MSI zu informieren, damit sie die SEC über wesentliche Verstöße benachrichtigen kann. Sie können die Vorlagen des Prozessautomatisierungs-Designers (PAD) verwenden, um die Schritte im Playbook für Anfragen an die Rechtsabteilung auszuführen und die Rechtsabteilung entsprechend zu informieren.

Dieses Playbook kann verwendet werden, wenn ein schwerwiegender Security Incident erstellt oder aktualisiert wird. Sie müssen das Playbook für Anfragen an DIE Rechtsabteilung auf DEM PAD aktivieren und dann alle Aufgaben ausführen, z. B. Analyse, Eindämmung, Beseitigung und Überprüfung.

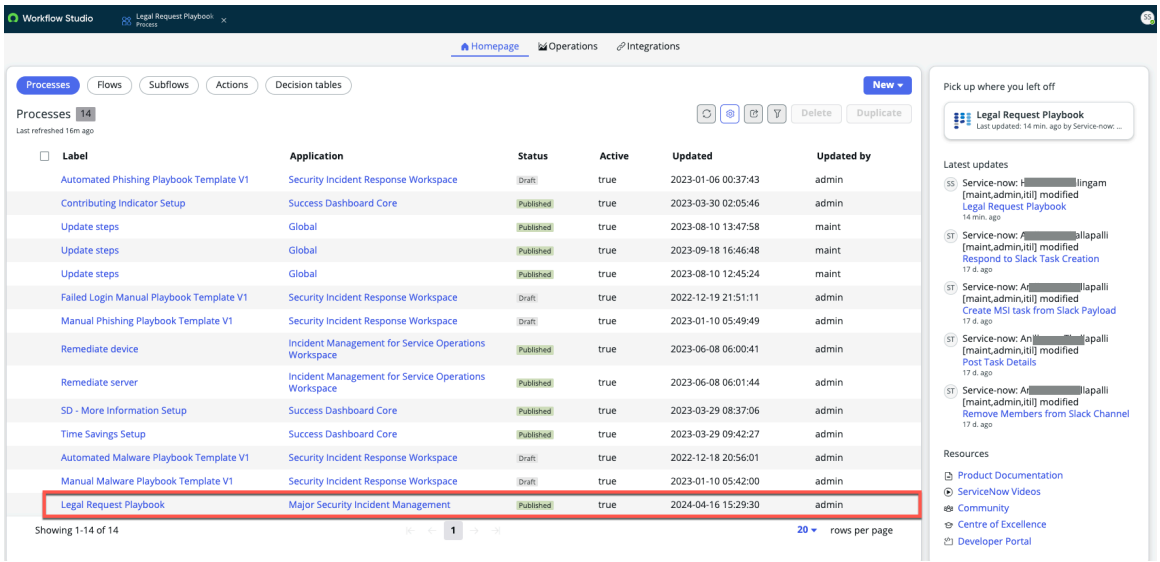
Die folgenden Spalten sind die Spuren der Prozessdefinition und entsprechen dem Status schwerwiegender Security Incidents:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Analyse
- Beinhalten
- Beseitigen
- Prüfung

Jede Spalte enthält bestimmte Aktivitäten.

Playbook für Anforderung an die Rechtsabteilung



Sobald Sie eine Aufgabe in einer Spalte als abgeschlossen markiert haben, können Sie zur nächsten Aufgabe wechseln. Sie können eine Aufgabe jederzeit speichern und zu einem späteren Zeitpunkt zum Playbook zurückkehren. Nachdem Sie alle Aufgaben in einer Spalte abgeschlossen haben, können Sie zur nächsten Spalte wechseln. Der Status wird im linken Bereich angezeigt, wenn Sie Aufgaben und Spuren abschließen. Ein Aktivitätsprotokoll auf der rechten Seite des Playbooks zeigt alle Daten an, die Sie für jede Aufgabe eingegeben haben.

Nachdem Sie alle Aufgaben abgeschlossen haben, werden Sie aufgefordert, die von Ihnen in allen Spuren eingegebenen Details zu überprüfen. Sie können ein beliebiges Feld bearbeiten oder auswählen **Beenden** Um den Prozess der Erstellung der Berechtigung abzuschließen.

Erstellen Sie Prozesse für das Playbook für Anfragen an die Rechtsabteilung

Verwenden Sie diese Schritte, um Prozesse für das Playbook für juristische Anforderungen im Prozessautomatisierungs-Designer (PAD) zu erstellen.

Vorbereitungen

Erforderliche Rolle: sn_msi.Workspace_Manager.

Prozedur

1. Klicken **Alle** > **Prozessautomatisierungs-Designer** > > **Einen neuen Prozess erstellen**an.

   Beispiel: Playbook für juristische Anforderung.

2. Geben Sie einen Namen für den Prozess, die Beschreibung und die Anwendung ein, für die der Prozess erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie Auf **Wählen Sie einen Auslöser aus** .
4. Wählen Sie Aus **Definieren Sie Ihre eigenen Bedingungen für die Ausführung Ihres Prozesses** , Und wählen Sie die Auslöserbedingung aus, wenn Ihr Prozess ausgeführt werden muss.
5. Klicken Sie Auf **Legen Sie Ihre Auslöserbedingungen fest** .
6. Wählen Sie die Bedingungen aus, um zu definieren, wann Ihr Prozess ausgeführt werden muss, indem Sie eine Tabelle auswählen und die Bedingungen ausfüllen.
7. Klicken Sie Auf **Wechseln Sie zu Designer** .
   Die Seite Prozessautomatisierungs-Designer wird geöffnet.
8. Um mit dem Entwerfen Ihres automatisierten Prozesses zu beginnen, klicken Sie auf **Fügen Sie eine neue Spalte hinzu** .
   Der Bereich „Spalteneigenschaften“ wird auf der rechten Seite der Anwenderoberfläche geöffnet.
9. Geben Sie im Bereich „Spalteneigenschaften“ die folgenden Details ein: **Name** , **Beschreibung** , **Ausführungsbedingung** , Und **Geben Sie an, wann begonnen werden soll** .
   Die **Ausführungsbedingung** Und **Geben Sie an, wann begonnen werden soll** Felder geben an, wann die Spalte ausgeführt würde.
10. Klicken Sie Auf **Speichern und schließen** .
11. Um eine weitere Spalte hinzuzufügen, klicken Sie auf **Fügen Sie eine weitere Spalte hinzu** .
    Ebenso können Sie beliebig viele Spuren erstellen. In diesem Beispiel können Sie eine Spalte für „Analyse“, „Eindämmen“, „Auslöschen“ und „Überprüfen“ erstellen. Im folgenden Beispiel: **Analyse** Spalte startet sofort und weist keine Ausführungsbedingung auf. **Enthalten** Spaltenstart, nachdem die vorherige Spalte abgeschlossen wurde und eine Ausführungsbedingung aufweist, die auf dem Ergebnis einer Aktivität in der vorherigen Spalte basiert.
    Nach dem Hinzufügen der Spuren müssen Sie Prozessaktivitäten für jede Spalte hinzufügen.
12. Klicken Sie Auf **Fügen Sie eine weitere Prozessaktivität hinzu** Unter einer bestimmten Spalte (z. B. Analysespalte).
    Das Popup-Fenster Aktivität hinzufügen wird geöffnet.
    a. Wählen Sie im Popup-Fenster Aktivität hinzufügen die erforderliche Aktivitätsdefinition aus.
13. Klicken Sie Auf **Erstellen Sie eine neue Aktivität** .
    Nachdem eine Aktivitätsdefinition hinzugefügt wurde, kann sie ähnlich wie Spuren weiter konfiguriert werden. Auf ähnliche Weise können Sie unter jeder Spalte weitere Prozessaktivitäten erstellen.
14. Fügen Sie im Bereich „Aktivitätseigenschaften“ eine Ausführungsbedingung hinzu, und geben Sie an, wann die Prozessaktivität gestartet werden soll.
15. Fügen Sie eine Ausführungsbedingung hinzu, und geben Sie an, wann gestartet werden soll.
    Alle für diese Aktivität erforderlichen Eingaben (enthält Eingaben im Automatisierungsplan, die konfiguriert sind) werden angezeigt. Sie können die Werte überschreiben oder die vorkonfigurierten Werte verwenden.
16. Klicken Sie Auf **Zeigen Sie alle Eigenschaften an** Und aktivieren Sie **Erweiterte Eigenschaften** Umschalten, um alle Aktivitäts-Experience-Felder aus der Aktivitätsdefinition anzuzeigen.

Mit dem Playbook für Anfragen an die Rechtsabteilung

Verwenden Sie diese Schritte, um zu erfahren, wie Sie das Playbook für Anfragen an die Rechtsabteilung im MSIM-Arbeitsbereich und seine Fähigkeiten verwenden können.

Vorbereitungen
Erforderliche Rolle: sn_msi.Workspace_Manager.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie im MSIM-Arbeitsbereich einen schwerwiegenden Security Incident.
2. Wählen Sie die Registerkarte **Playbook** aus.

   Sie können die Playbooks anzeigen, die für den schwerwiegenden Security Incident aktiviert wurden.

   Hinweis:
   Wenn Sie die Playbooks nicht aufgelistet sehen, müssen Sie zum PAD wechseln und zulassen, dass sie es im anzeigen können **Playbook** Registerkarte.

3. Wählen Sie aus **Playbook Für Anforderung An Die Rechtsabteilung** .
4. Klicken Sie auf jede Spalte, um zu erfahren, welche Aufgaben von diesem Playbook ausgeführt wurden.
5. Klicken Sie Auf **Analyse** Um die Liste der in der Analysephase durchgeführten Aktivitäten anzuzeigen. Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern.
6. Ebenso können Sie auf Eindämmen, Löschen und Überprüfen klicken, um die Liste der Aktivitäten anzuzeigen, die in der jeweiligen Phase ausgeführt wurden.
   Sie haben die Möglichkeit, sie entsprechend Ihren Anforderungen zu ändern. Wenn noch eine Aktivität oder Anwenderaktion vorhanden ist, die Sie ausführen müssen, wird sie in der jeweiligen Phase angezeigt.
7. Wenn in einer der Phasen noch eine Aktivität oder Anwenderaktion erforderlich ist, klicken Sie auf die entsprechende Phase, und führen Sie die Aktion aus, um die Aktivität abzuschließen.

Rollup-Framework für MSIM

Erweitert die Fähigkeit, die Quelldatensätze von zu verknüpfen Management schwerwiegender Sicherheits-Incidents Arbeitsbereich.

Übersicht

Rollup-Framework macht den Rollup-Flow konfigurierbar und erweiterbar. Verwenden Sie dieses Framework-Modell, um die Informationen zu konfigurieren, die zu einem schwerwiegenden Security Incident zusammengefasst werden können.

Zuvor konnte sn_msi.Workspace_Manager Security Incidents und angreifbare Elemente verknüpfen, die als vorgeschlagen oder heraufgestuft wurden MSI. Nach dem Verknüpfen des Security Incidents oder angreifbaren Elements wurden die Informationen zu einem schwerwiegenden Security Incident zusammengefasst. Die Art der Informationen, die für das Rollup erforderlich sind, wurde in den Skripts hartcodiert.

Sie können das Framework-Modell verwenden, um den Rollup-Flow zu konfigurieren, der die folgenden Funktionen unterstützt und auch die vorhandenen Probleme in der Anwendung behebt:

Das Rollup-Framework-Modell ermöglicht dem sn_msi.Workspace_Manager die folgenden Vorteile:

- Fügen Sie die Verknüpfung hinzu, schlagen Sie vor oder heraufstufen MSI Datensatzfähigkeiten in einer beliebigen Tabelle, wodurch die Aufgabentabelle erweitert wird.
- Steuern Sie die Art der Informationen, zu denen ein Rollup durchgeführt werden soll MSI Beim Ausführen von Aktionen wie Verknüpfen/Vorschlagen/Heraufstufen für die Incident-Datensätze.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Unterstützen Sie das Verknüpfen, Vorschlagen oder Heraufstufen für Security Incidents, Korrekturaufgaben und Security Cases Out of the Box (OOTB) sowohl aus der klassischen Umgebung als auch aus Management schwerwiegender Sicherheits-Incidents Arbeitsbereich.

Rollup-Framework zeigt die Konfigurationen wie in der folgenden Tabelle erläutert.

Rollup-Framework-Konfigurationen

Name	Beschreibung
Konfiguration verknüpfter Datensätze	Speichert die Informationen von Aufgabentabellen, die zum Verknüpfen/Heraufstufen/Vorschlagen von verwendet werden können Major Security Incident.
Konfiguration von Rollup-Datensätzen	Erfasst die Informationen, die aus der Aufgabentabelle zusammengefasst werden können, wenn Aktionen zum Verknüpfen/Heraufstufen/ Vorschlagen ausgeführt werden.
Listenlayoutkonfiguration	Steuert die Bezeichnungen und das Listenlayout für verschiedene Tabellen, wie in angezeigt Management schwerwiegender Sicherheits-Incidents Arbeitsbereichsregisterkarten wie Incident-Auswirkung, verknüpfte Datensätze und Threat Intelligence.

Konfigurieren Sie verknüpfte Datensätze in Management schwerwiegender Sicherheits-Incidents

Verwenden Sie die Konfiguration der verknüpften Datensätze, um die Informationen von Aufgabentabellen zu speichern, die zum Verknüpfen/Heraufstufen/Vorschlagen von verwendet werden können Major Security Incident.

Erforderliche Rolle: admin und sn_msi.Workspace_admin.

Hinweis:
Der Administrator kann den Datensatz und erstellen MSIM Der Arbeitsbereich-Administrator kann den Datensatz aktualisieren.

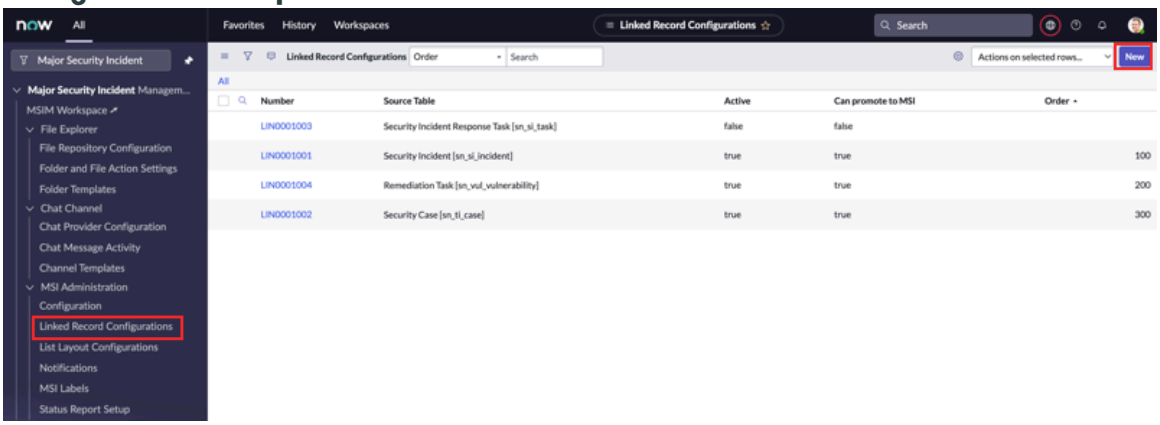
Prozedur

1. Navigieren zu **Management schwerwiegender Sicherheits-Incidents** > **Konfigurationen verknüpfter Datensätze**an.

   Die Seite Konfiguration des verknüpften Datensatzes wird angezeigt.

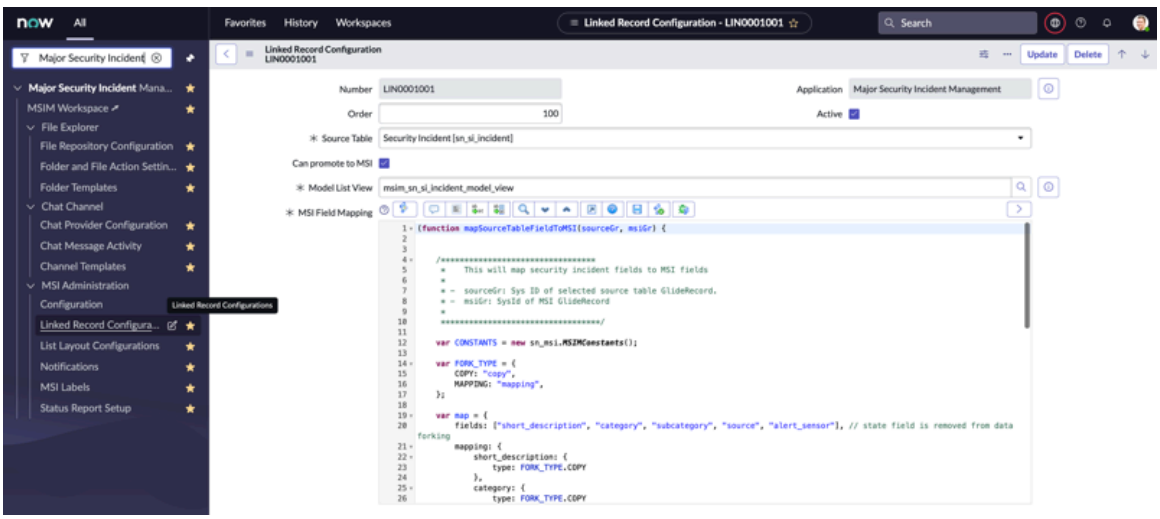
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration verknüpfter Datensätze



2. Klicken Sie auf der Seite Konfiguration des verknüpften Datensatzes auf **Neu**

Hinweis:
Stellen Sie sicher, dass sich die Anwendung in befindet Management schwerwiegender Sicherheits-Incidents Umfang.



3. Füllen Sie die Felder im Formular „Datensatzkonfiguration“ aus.

Feldbeschreibungen Für Verknüpfte Datensätze

Feld	Beschreibung
Quelltabelle	Gibt die Aufgabentabelle an, zu der ein Rollup durchgeführt werden muss Major Security Incident.
Reihenfolge	Ermöglicht Ihnen, die Reihenfolge der aktuellen Quelltabelle in der Dropdown-Liste des MSIM-Arbeitsbereichs zu steuern. Nachfolgend finden Sie ein Beispiel für **Reihenfolge** . Siehe Abbildung 1 unten, die nach dieser Tabelle bereitgestellt wird.
Modell ListView	Wählen Sie eine Ansicht aus, die das Listenlayout steuern kann, das in der modalen Liste der verknüpften Datensätze angezeigt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Kann zu heraufgestuft werden MSI	Aktivieren Sie dieses Kontrollkästchen, um zu bestätigen, ob der Datensatz ein primärer Datensatz ist. Nachfolgend finden Sie ein Beispiel für **Kann zu MSI heraufgestuft werden** Optionsauswahl. Beachten Sie die folgende Abbildung 2, die nach dieser Tabelle bereitgestellt wird. Wenn dieses Kontrollkästchen aktiviert ist und der Wert lautet Wahr , Dann: ○ Sie können einen Quelldatensatz direkt vorschlagen und zu heraufstufen Major Security Incident Verwenden der klassischen Umgebungsaktionen mit zusätzlichen Konfigurationen. ○ Sie können Quelldatensätze mit schwerwiegenden Security Incidents sowohl aus der klassischen Umgebung als auch aus verknüpfen MSIM Arbeitsbereich. ○ Management schwerwiegender Sicherheits-Incidents Mit Arbeitsbereich verknüpfter Datensatzseite werden die verknüpften Quelltabellendatensätze angezeigt. **Hinweis:** Ob ein Datensatz direkt als vorgeschlagen/ heraufgestuft werden kann Major Security Incident, Dann ist dieser Datensatz ein primärer Datensatz. Beispiel: In der Konfiguration der Tabelle „Sicherheitsantwortaufgabe“ der Wert von **Kann zu MSI heraufgestuft werden** Ist „falsch“, da Sie die Sicherheitsantwortaufgabe nicht direkt zu heraufstufen können Major Security Incident. Daher wird sie nicht in angezeigt MSIM Dropdown-Liste der Registerkarte mit verknüpftem Datensatz des Arbeitsbereichs.
MSI Feldzuordnung	Schreiben Sie ein Skript, um die Quelldatensatzfelder einem neu erstellten schwerwiegenden Security Incident zuzuordnen, wenn der Quelltabellendatensatz vorgeschlagen oder heraufgestuft wird. Dieses Skript wird nur ausgeführt, wenn **Kann zu MSI heraufgestuft werden** Wert ist „wahr“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bild 1: Listenansichtsreihenfolge der verknüpften Datensätze

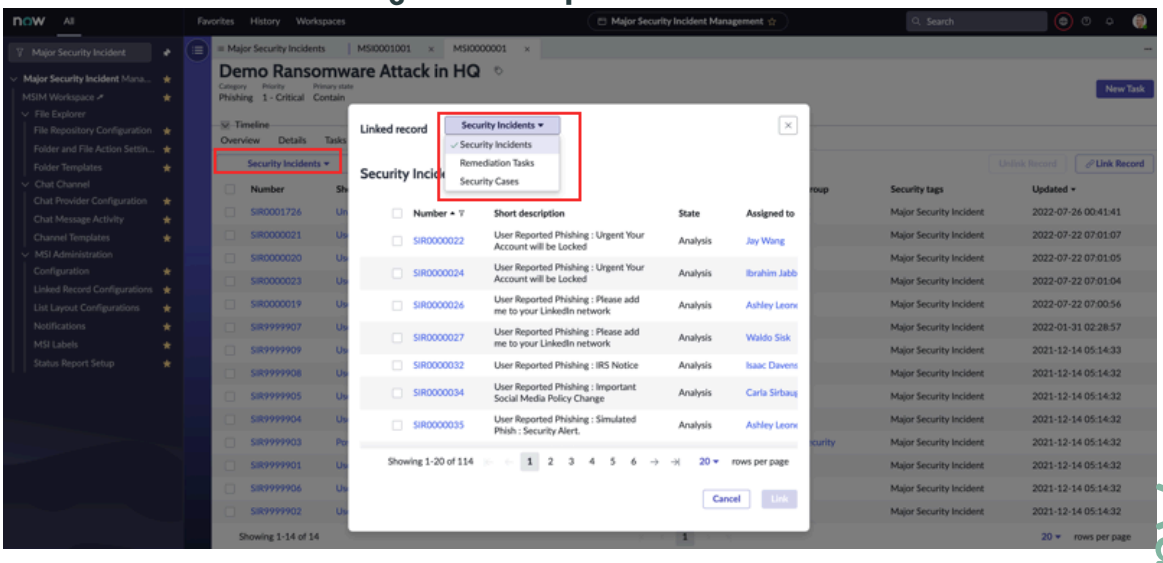
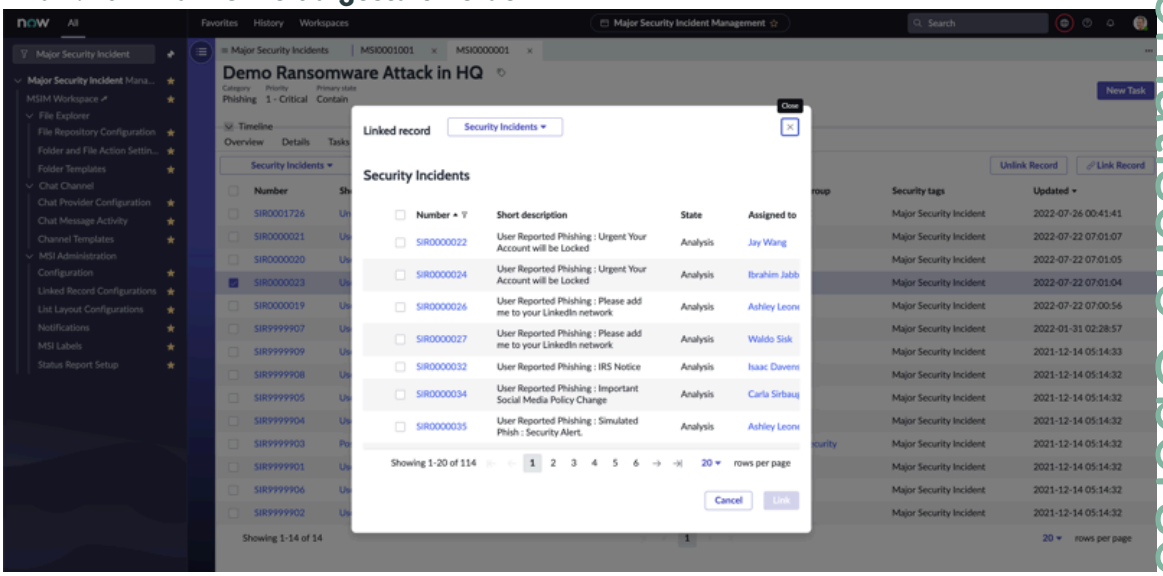


Bild 2: Kann zu MSI heraufgestuft werden



Automatische Übersetzung

Konfigurieren Sie Rollup-Datensätze in Management schwerwiegender Sicherheits-Incidents

Konfigurieren Sie Rollup-Datensätze in Management schwerwiegender Sicherheits-Incidents Zur Steuerung der Informationen, die zusammengefasst werden, wenn der Quelldatensatz als schwerwiegende Security Incidents verknüpft/vorgeschlagen/heraufgestuft wird.

Erforderliche Rolle: admin und sn_msi.Workspace_admin.

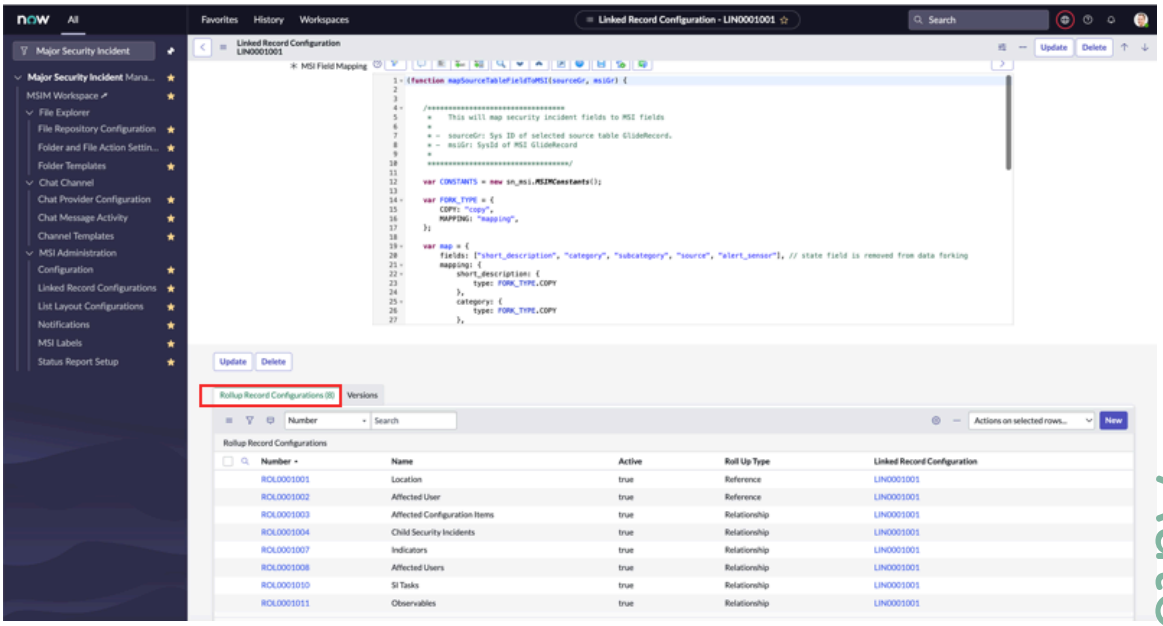
Hinweis:
Der Systemadministrator kann den Datensatz erstellen, und der MSI-Arbeitsbereich-Administrator kann ihn aktualisieren.

Prozedur

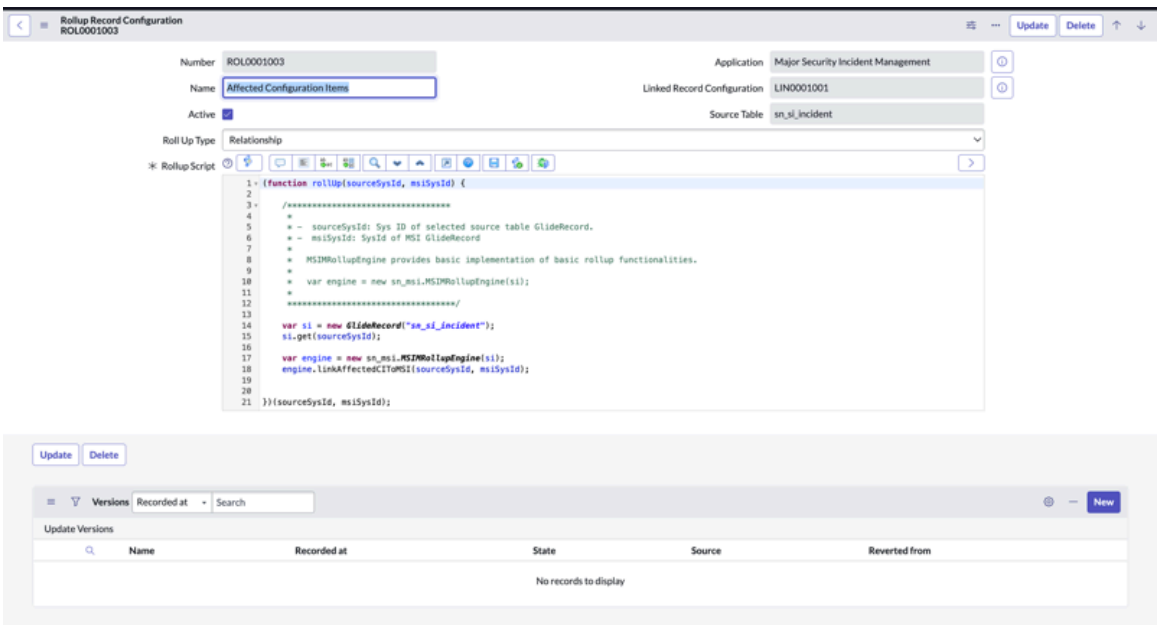
1. Navigieren zu **Antwort Auf Schwerwiegende Security Incidents** > **Konfiguration Der Verknüpften Datensätze**an. Die Seite Konfigurationen verknüpfter Datensätze wird angezeigt.
2. Wählen Sie einen neuen verknüpften Datensatz aus, oder erstellen Sie ihn, und navigieren Sie zu **Rollup-Datensatzkonfiguration** Abschnitt auf derselben Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt „Rollup-Datensatzkonfiguration“



3. Klicken Sie auf **Neu**.



4. Geben Sie auf der Konfigurationsseite die Details ein.

Konfiguration von Rollup-Datensätzen

Feldname	Feldbeschreibung
Name	Gibt den Namen des Rollup-Datensatzes an.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die aktuelle Konfiguration zu implementieren, wenn ein Rollup des Quelldatensatzes stattfindet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldname	Feldbeschreibung
Konfiguration verknüpfter Datensätze	Gibt eine eindeutige Zahl an, die sich auf die Konfiguration Ihrer übergeordneten verknüpften Datensätze bezieht und schreibgeschützt ist.
Quelltabelle	Der Name der Quelltabelle, der in der Konfiguration des verknüpften Datensatzes verwendet wird und schreibgeschützt ist.
Rollup-Typ	Beschreibt die Art der Informationen, die zusammengefasst werden sollen. ○ **Beziehung** : Wählen Sie diese Option aus, wenn die Daten als zugehörige Liste vorhanden sein müssen. ○ **Referenz** : Wählen Sie diese Option aus, wenn die Daten als Referenzfeld im Quelltabellenformular vorhanden sind.
Rollup-Skript	Wenn der Rollup-Typ: **Beziehung** , Dann **Rollup-Skript** Das Feld ist aktiviert, sodass Sie ein Skript schreiben können. Es kann zum Rollup von Informationen verwendet werden. Hier erhält das Skript die Eingaben, die Informationen zum Quelldatensatz und zum schwerwiegenden Security Incident enthalten. Das Skript muss die Informationen aus den Beziehungstabellen finden und ein Rollup zur Tabelle „Verknüpfter Datensatz“ (sn_msi_m2m_Child) durchführen können.
Quellfeld	Wenn der Rollup-Typ: **Referenz** , Dann **Quellfeld** Ist verfügbar. Auf diese Weise können Sie das Referenzfeld Quelltabelle auswählen, das die Informationen enthält, die für das Rollup erforderlich sind.
Zielfeld	Wenn der Rollup-Typ: **Referenz** , Dann **Zielfeld** Ist verfügbar. Dadurch können Sie ein Feld aus der Tabelle „Verknüpfter Datensatz“ (sn_msi_m2m_Child) referenzieren und die Daten speichern, die im ausgewählten Quellfeld und im Quelltabellendatensatz vorhanden sind.

Skript für Rollup wird geschrieben

Name	Beschreibung
Eingaben	• SourceSysId: SYS-ID des Quelltabellendatensatzes, der entweder verknüpft/vorgeschlagen/heraufgestuft wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

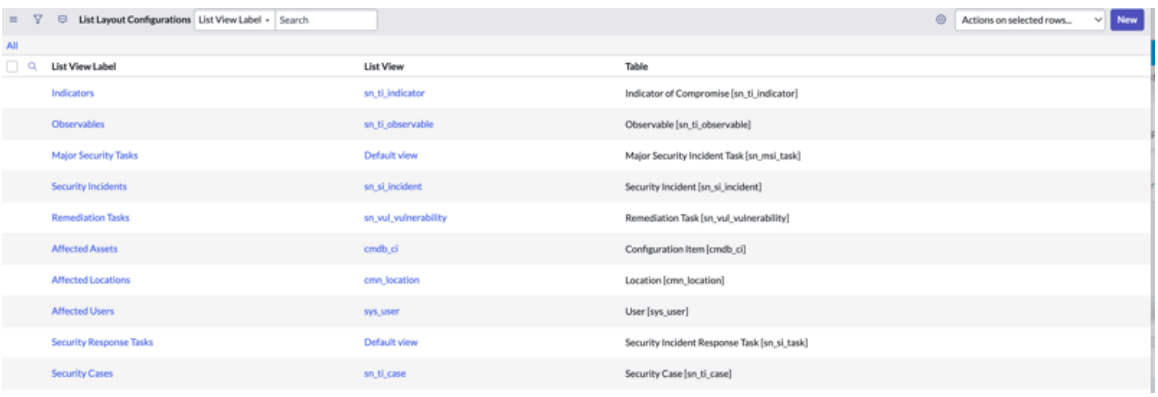
Name	Beschreibung
	• MsiSysId: SYS-ID des schwerwiegenden Security Incidents, mit dem der Quelldatensatz verknüpft/vorgeschlagen/ heraufgestuft wird.
Ausgabe	Kein Ausgaberückgabewert.
Verantwortlichkeit	Das Skript sollte Informationen in die Tabelle „Verknüpfter Datensatz“ (sn_msi_m2m_Child) Rollup ausführen. • Verwenden SourceSysID Zum Abfragen von Daten aus ServiceNow Beziehungstabellen. • Nachdem die Daten abgerufen wurden, führen Sie mit ein Rollup der Daten zu einem verknüpften Datensatz (sn_msi_m2m_Child) durch MSIRollupEngine Dienstprogramm zum Rollup von Daten.

Konfigurieren Sie das Listenlayout in Management schwerwiegender Sicherheits-Incidents

Konfigurieren Sie das Listenlayout, um das in verwendete Layout und die in verwendeten Bezeichnungen anzupassen Management schwerwiegender Sicherheits-Incidents Arbeitsbereich, z. B. Incident-Auswirkung, verknüpfte Datensätze und Threat Intelligence-Registerkarten.

Erforderliche Rolle: admin und sn_msi.Workspace_admin.

Hinweis:
Der Systemadministrator kann den Datensatz erstellen, und der MSI-Arbeitsbereich-Administrator kann ihn aktualisieren.

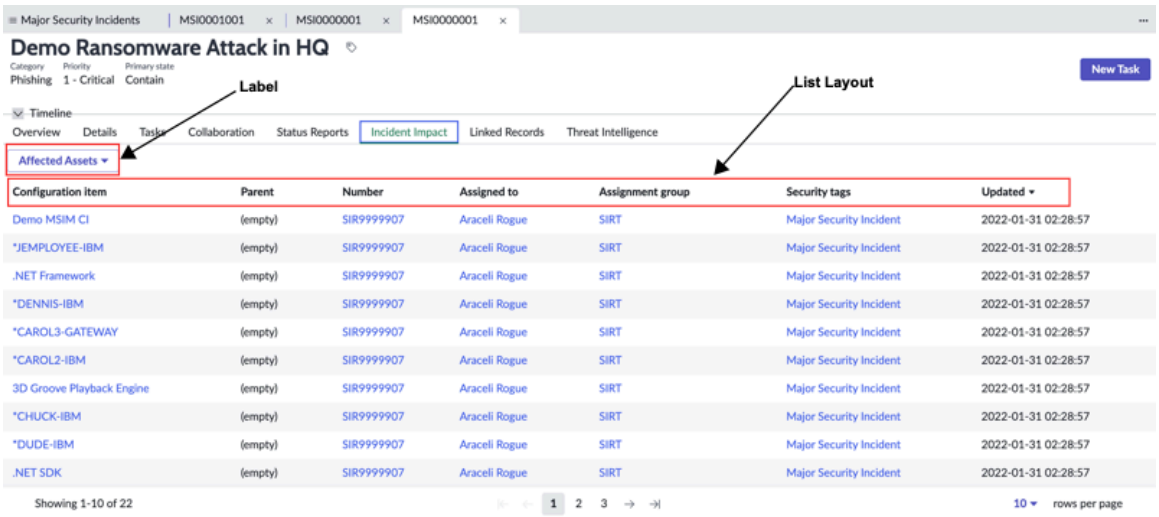


Die Listenlayoutkonfigurationen wurden bereits für vorhandene bekannte Tabellen geliefert, die in angezeigt werden Management schwerwiegender Sicherheits-Incidents Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn Sie die anwenderdefinierte Ansicht für die vorhandenen Tabellen rendern möchten, können Sie den entsprechenden Tabellendatensatz in der Listenlayoutkonfiguration mit der anwenderdefinierten Listenansicht aktualisieren.
- Für neue Aufgabentabellen können Sie eine neue Listenlayoutkonfiguration erstellen, um die anwenderdefinierte Listenansicht und Bezeichnungen zu rendern. Weitere Informationen zum detaillierteren Verfahren finden Sie unter Anleitungen Schritt 4. Erstellen Sie eine Ansicht für eine neue Registerkarte mit verknüpftem Datensatz für einen Sicherheitsfall



Rollup-Beispiel-Anwendungsfallimplementierung für einen Sicherheitsfall

Die folgenden Schritte erklären einen Beispielanwendungsfall zum Hinzufügen von Support zum Verknüpfen/Vorschlagen/Heraufstufen zu schwerwiegendem Security Incident für eine Sicherheitsfalltabelle.

- Schritt 1. Erstellen Sie eine verknüpfte Datensatzkonfiguration für einen Sicherheitsfall
- Schritt 2. Erstellen Sie eine Ansicht für das modale Fenster für einen Sicherheitsfall
- Schritt 3. Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall
- Schritt 4. Erstellen Sie eine Ansicht für eine neue Registerkarte mit verknüpftem Datensatz für einen Sicherheitsfall
- Schritt 5. Fügen Sie Zugriffssteuerungslisten (ACLs) für hinzu Management schwerwiegender Sicherheits-Incidents Arbeitsbereichsanwender
- Schritt 6. Erstellen Sie Geschäftsregeln für einen Sicherheitsfall
- Schritt 7. Erstellen Sie Rollup-Datensatzkonfigurationen

Schritt 1. Erstellen Sie eine verknüpfte Datensatzkonfiguration für einen Sicherheitsfall

Erstellen Sie eine verknüpfte Datensatzkonfiguration für einen Sicherheitsfall.

Vorbereitungen
Erforderliche Rolle: admin und sn_msi.Workspace_admin

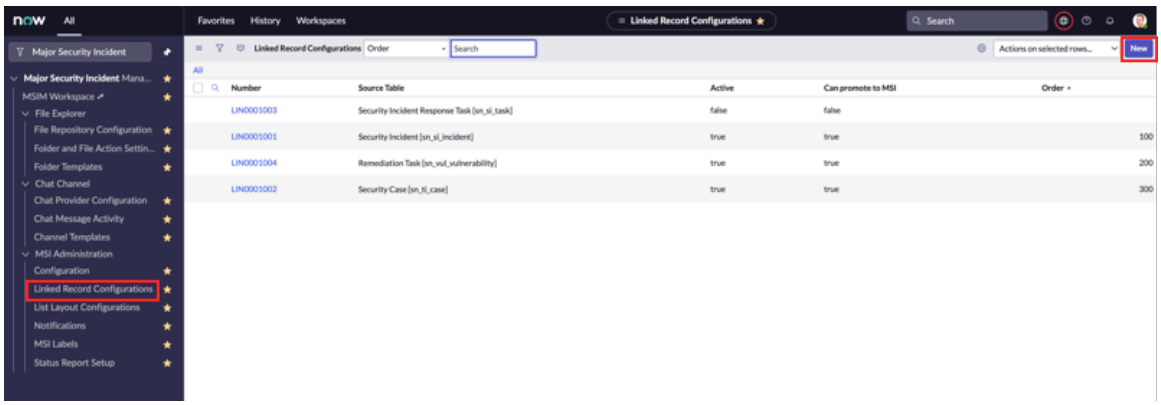
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

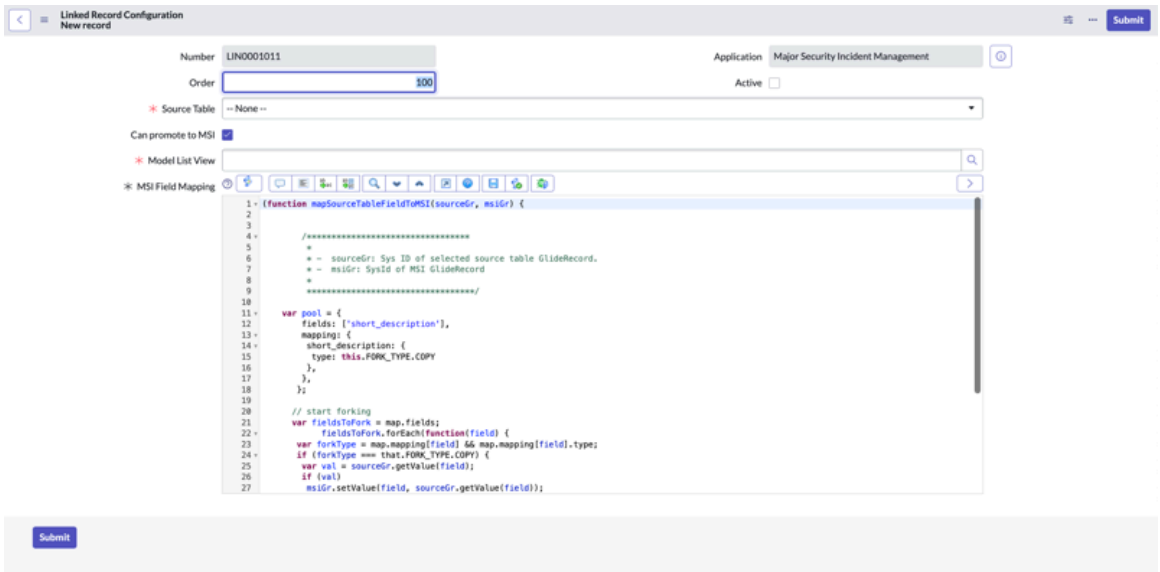
Hinweis:
Der Systemadministrator kann den Datensatz erstellen, und der MSI-Arbeitsbereich-Administrator kann ihn aktualisieren.

Prozedur

1. Suchen Sie in der linken Navigation nach der Konfiguration des verknüpften Datensatzes.
2. Klicken Sie auf **Neu**.



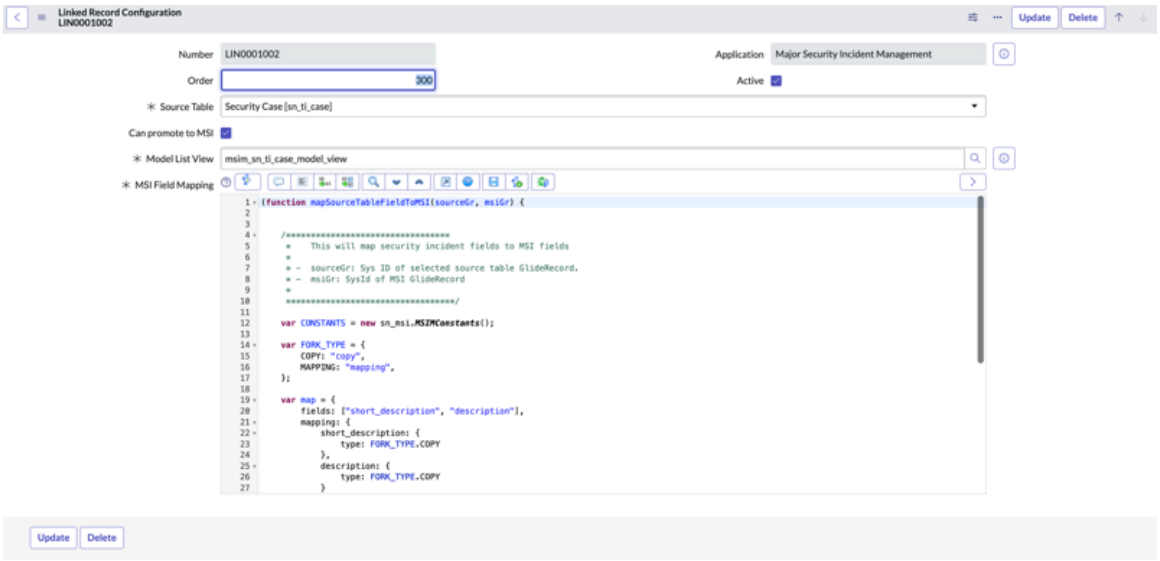
3. Füllen Sie das Formular mit den erforderlichen Spalten aus, und schreiben Sie ein Feldzuordnungsskript.



4. Sie haben jetzt eine verknüpfte Datensatzkonfiguration für den Sicherheitsfall erstellt, indem Sie die Werte wie in der folgenden Tabelle beschrieben hinzugefügt haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Name	Beschreibung
Quelltabelle	Sicherheitsfall (sn_ti_Case). In diesem Beispiel verknüpfen/heraufstufen/schlagen Sie einen Sicherheitsfall als MSI vor.
Reihenfolge	Eingabewert: 300 **Hinweis:** Niedriger die Reihenfolge hat Vorrang vor höheren Ordnungen. Da ein Sicherheitsfall eine höhere Reihenfolge hat als der Security Incident und die Korrekturaufgabe, wird er in der letzten Sequenz angezeigt.
Hochstufen zu MSI möglich	„Wahr“, aktivieren Sie dieses Kontrollkästchen, um den Sicherheitsfall zu „MSI“ hochzustufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Hinweis: ○ Verknüpfen und heben Sie die Verknüpfung von Sicherheitsfalldatensätzen mit schwerwiegenden Security Incidents auf Management schwerwiegender Sicherheits-Incidents Arbeitsbereich. Außerdem ist die Funktion zum Aufheben der Verknüpfung von Datensätzen nur für die verknüpften Datensätze sichtbar. ▪ Dadurch werden die Verknüpfung, das Heraufstufen und das Vorschlagen von Sicherheitsfall zu schwerwiegendem Security Incident mithilfe von klassischen Umgebungsaktionen aktiviert. Diese UI-Aktionen sind jedoch nicht sofort verfügbar. Jede UI-Aktion muss manuell erstellt werden. Weitere Informationen finden Sie unter Schritt 3. Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall. ▪ UI-Aktion „Link/Heraufstufen/ Vorschlagen“ ist für Security Incident, Korrekturaufgabe und Sicherheitsfall sofort einsatzbereit verfügbar. ○ Die Seite mit dem verknüpften Datensatz des MSIM-Arbeitsbereichs zeigt die verknüpften Sicherheitsfalldatensätze an. In der folgenden Abbildung 1 finden Sie die Optionen, die nach dem Aktivieren dieses Kontrollkästchens verfügbar sind.
Modale Listenansicht	msim_sn_ti_case_model_view **Hinweis:** Diese Ansicht enthält Felder und die Reihenfolge der Felder, die in der Listenansicht im Modal „Datensatz verknüpfen“ im MSIM-Arbeitsbereich angezeigt werden. Weitere Informationen finden Sie unter Schritt 2. Erstellen Sie eine Ansicht für das modale Fenster für einen Sicherheitsfall

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Sehen Sie sich die folgende Abbildung 2 an, um sie über anzuzeigen **Verknüpfte Datensätze** Seite.
Feldzuordnungsskript	Dieses Skript beschreibt die Felder aus dem Quelltabellen-Datensatz, der einem neu erstellten schwerwiegenden Security Incident zugeordnet wird, wenn der Quelltabellen-Datensatz vorgeschlagen oder heraufgestuft wird. Welche Eingaben erhalten: ○ SourceGr: Glide-Datensatzobjekt des Sicherheitsfalls ○ MsiGr: Glide-Datensatzobjekt für schwerwiegenden Security Incident Das Skript liest die Kurzbeschreibung des Sicherheitsfalls aus und kopiert sie als Titel in einen schwerwiegenden Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bild 1: Kann zu MSI heraufgestuft werden

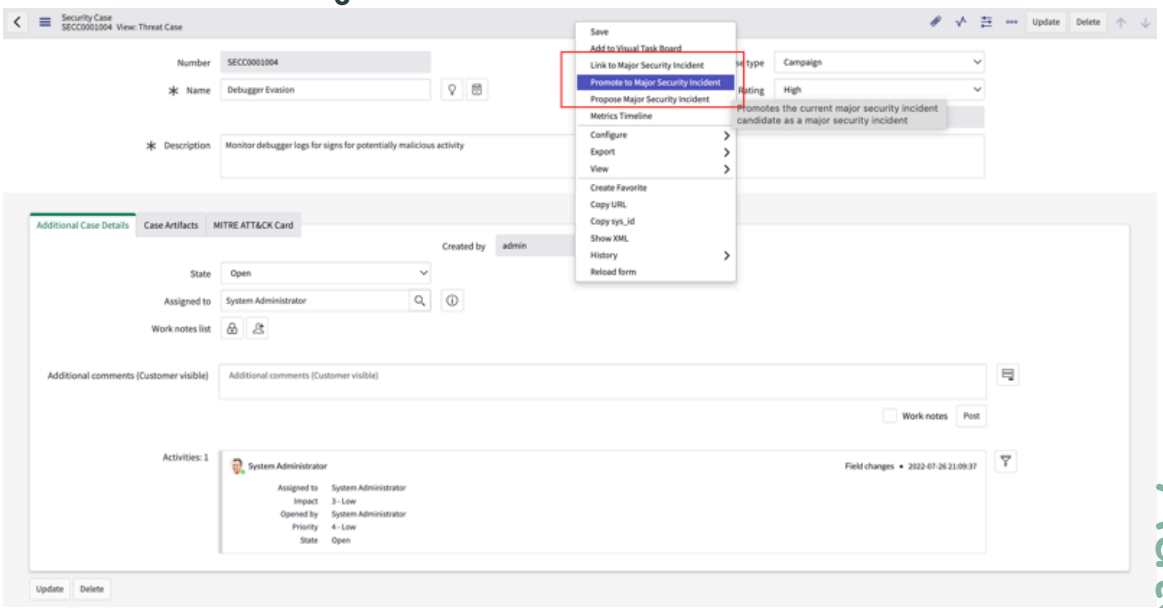
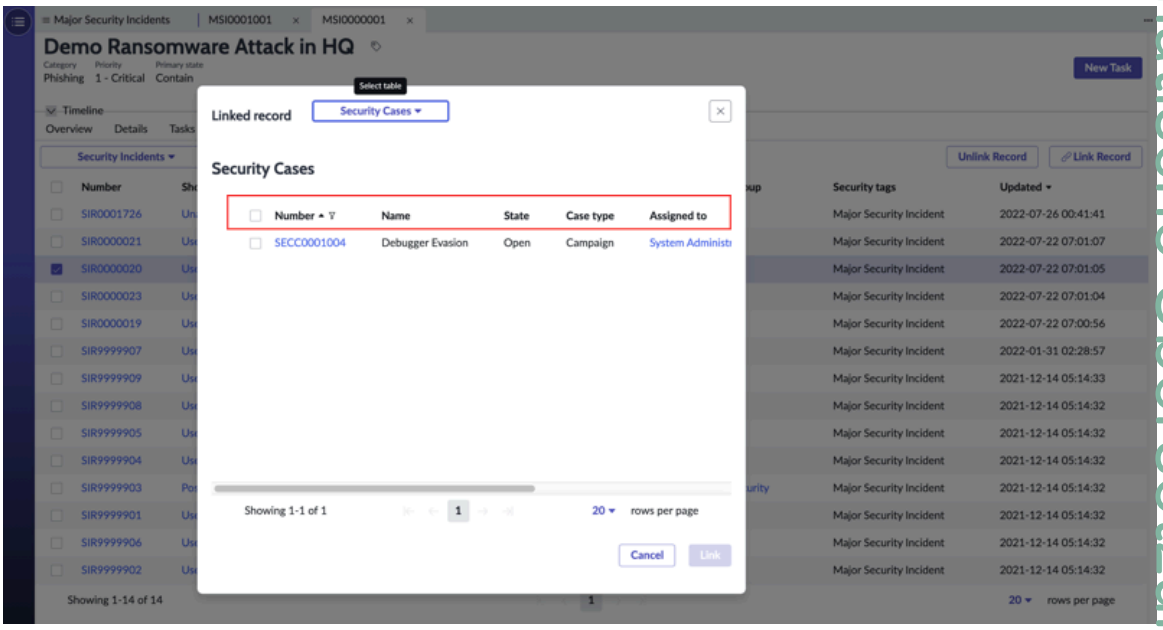


Bild 2. Modale Ansicht



Automatische Übersetzung

Schritt 2. Erstellen Sie eine Ansicht für das modale Fenster für einen Sicherheitsfall

Erstellen Sie eine Ansicht für das modale Fenster für einen Sicherheitsfall.

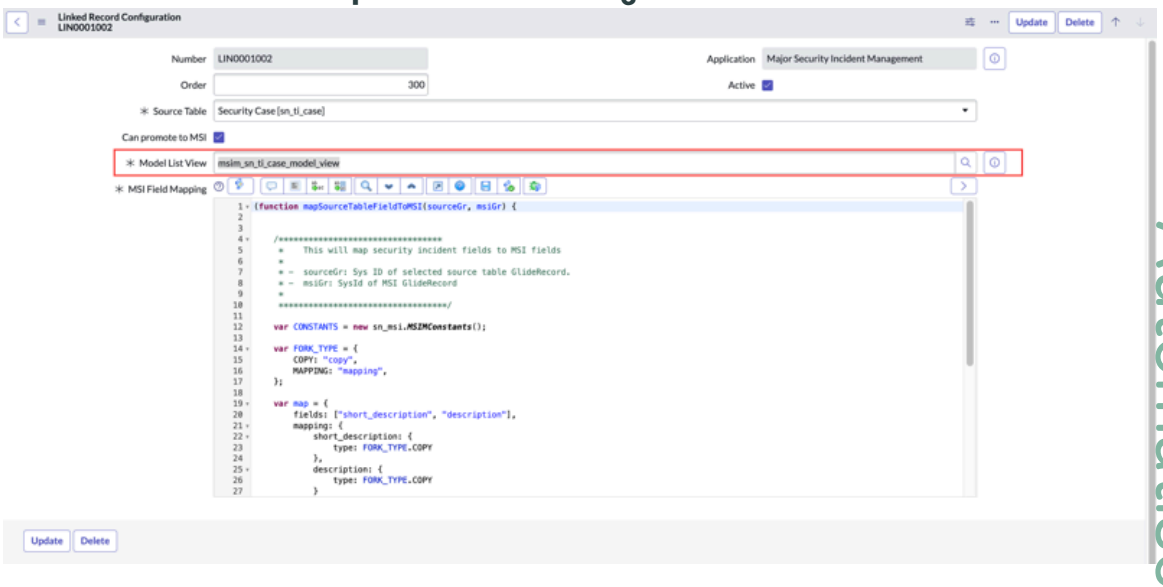
Vorbereitungen

Wichtige Überlegungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Standardmäßig zeigt die modale Liste des verknüpften Datensatzes nur an **Standard** Listenlayout. Wenn Sie das Listenlayout anpassen möchten, können Sie dies mit tun **Anwenderdefinierte Ansicht** In der Quelltabelle.
- Wenn Sie die anwenderdefinierte Ansicht rendern möchten, sollte die anwenderdefinierte Ansicht auch in der Konfiguration des verknüpften Datensatzes für Quelltabelle ausgewählt werden.

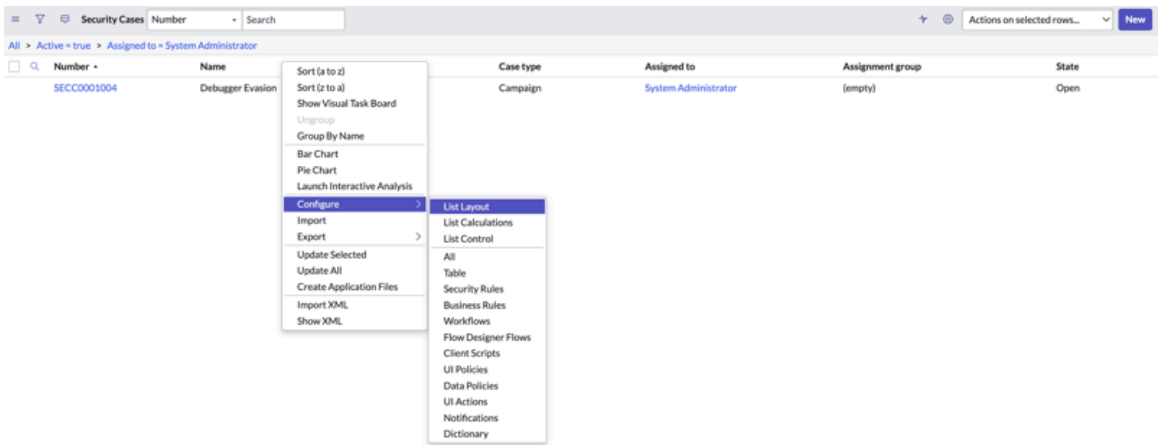
Modale Ansicht der verknüpften Datensatzkonfiguration für Quelltabelle



Erforderliche Rolle: Administrator

Prozedur

1. Wechseln Sie zur Quelltabelle, und klicken Sie auf **Konfigurieren** > **Listenlayout**an.



2. Gehe zu **Listenansicht** > **Namen anzeigen**an.
3. Klicken Sie Auf **Neu** Erstellen Sie in der Dropdown-Liste Ansichtsname eine neue Ansicht, z. B. msim_sn_ti_Case_Modal_View.
4. Wählen Sie die neu erstellte Ansicht aus.
   Nach der Auswahl können Sie die erforderlichen Felder aus der Liste verfügbar auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Speichern**.
6. Navigieren zu **Menü** > **Dashboard-Aufrufe insgesamt** Um zu überprüfen, ob die Ansicht ordnungsgemäß gerendert wurde.

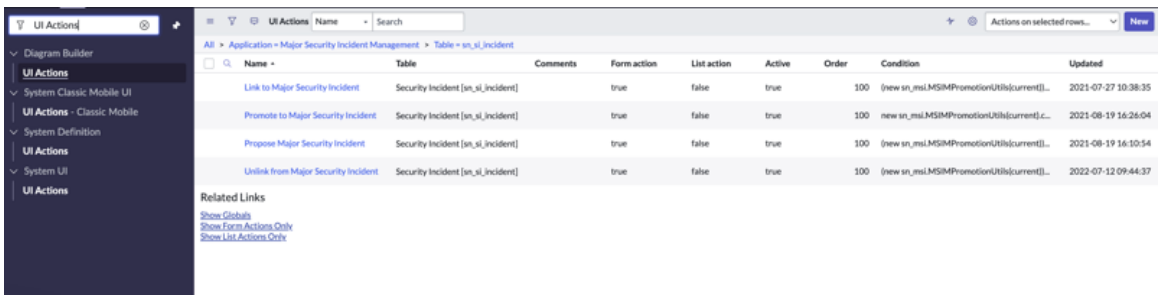
Schritt 3. Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall

Erstellen Sie UI-Aktionen für die Quelltabelle für einen Sicherheitsfall.

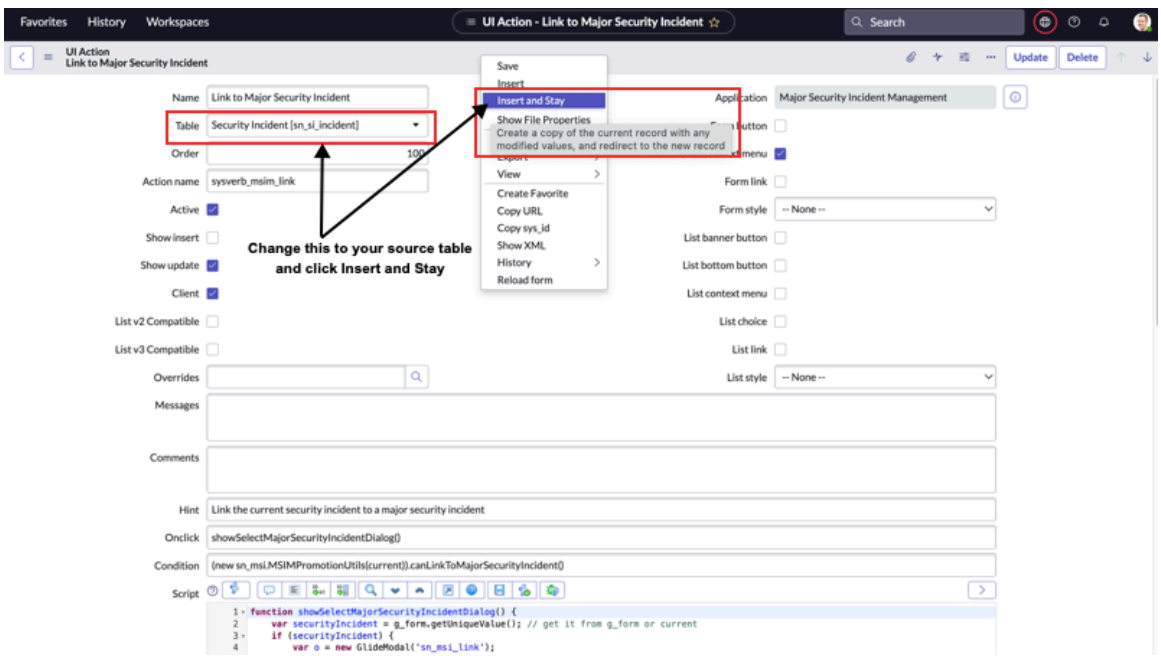
Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Systemdefinition** > **UI-Aktionen**an.
2. Führen Sie die Filteroption aus, um die Liste herauszufiltern **Anwendung** : Management schwerwiegender Security Incidents und **Tabelle** : sn_si_Incident.



3. Wählen Sie jede UI-Aktion einzeln aus, und speichern Sie die Details für die Quelltabelle.



4. Wiederholen Sie die oben genannten Schritte für die folgenden UI-Aktionen:
   - Link zu schwerwiegendem Security Incident
   - Vorgeschlagener Schwerwiegender Security Incident
   - Verknüpfung mit schwerwiegendem Security Incident aufheben
   - Zu schwerwiegendem Security Incident heraufstufen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

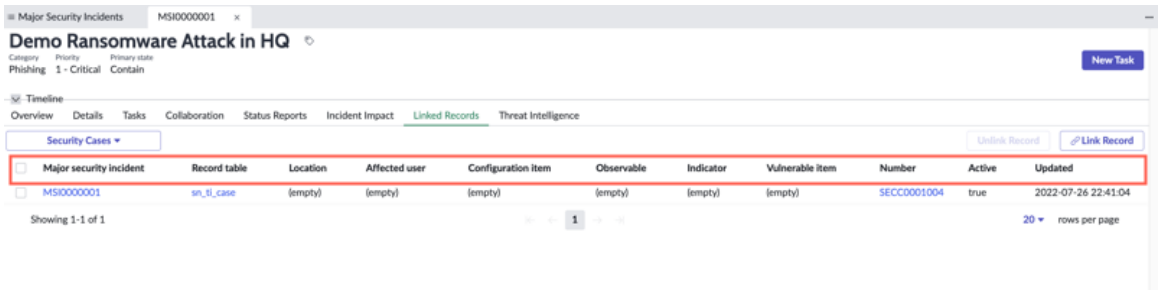
Schritt 4. Erstellen Sie eine Ansicht für eine neue Registerkarte mit verknüpftem Datensatz für einen Sicherheitsfall

Passen Sie das Listenlayout für eine Sicherheitsfalltabelle an, wenn es auf der Seite „Datensätze verknüpfen“ mit angezeigt wird Management schwerwiegender Sicherheits-Incidents Arbeitsbereich.

Vorbereitungen

Voraussetzungen:

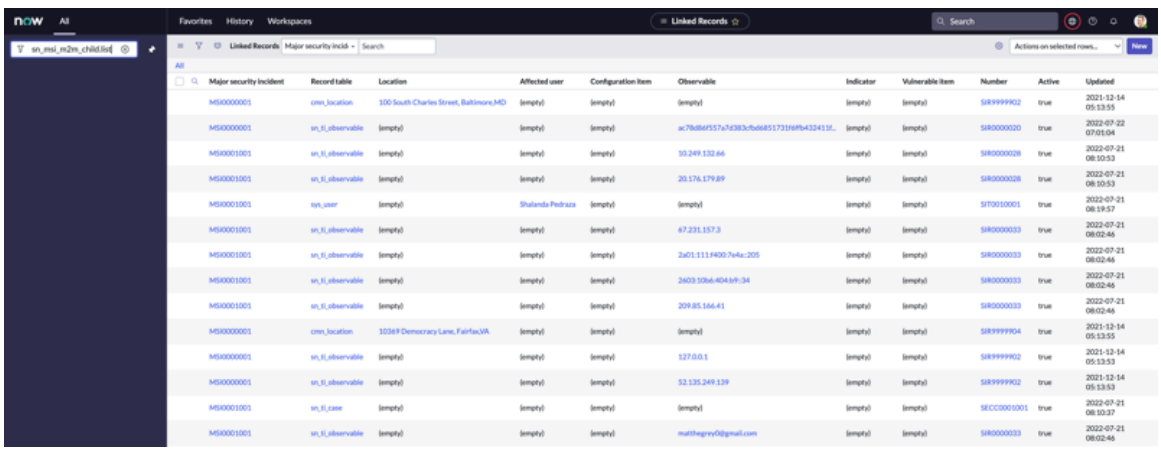
- Wählen Sie die Spalte aus, die sichtbar sein soll, wenn eine Liste für eine Sicherheitsfalltabelle gerendert wird.
- Wählen Sie die Reihenfolge der Felder aus, die in der Dropdown-Liste angezeigt werden sollen.



Erforderliche Rolle: Administrator

Prozedur

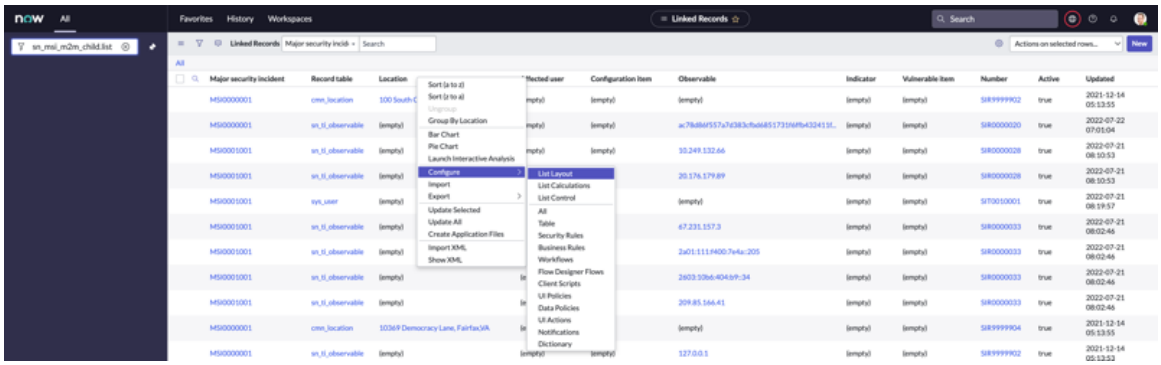
1. Suchen Sie nach **sn_msi_m2m_Child.list** Verwenden Sie die linke Navigation.
   Die Tabelle „Verknüpfte Datensätze“ wird angezeigt.



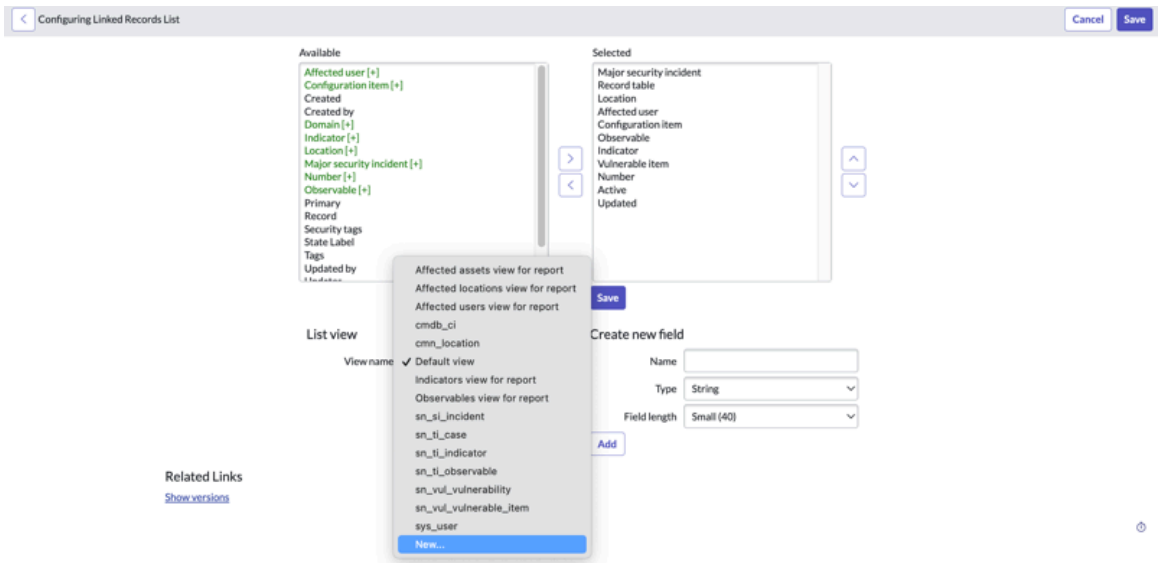
2. Klicken Sie mit der rechten Maustaste auf den Header, und wählen Sie aus **Konfigurieren** > **Listenlayout**an.
   Die Seite Konfigurieren der Liste verknüpfter Datensätze wird angezeigt.

Automatische Übersetzung

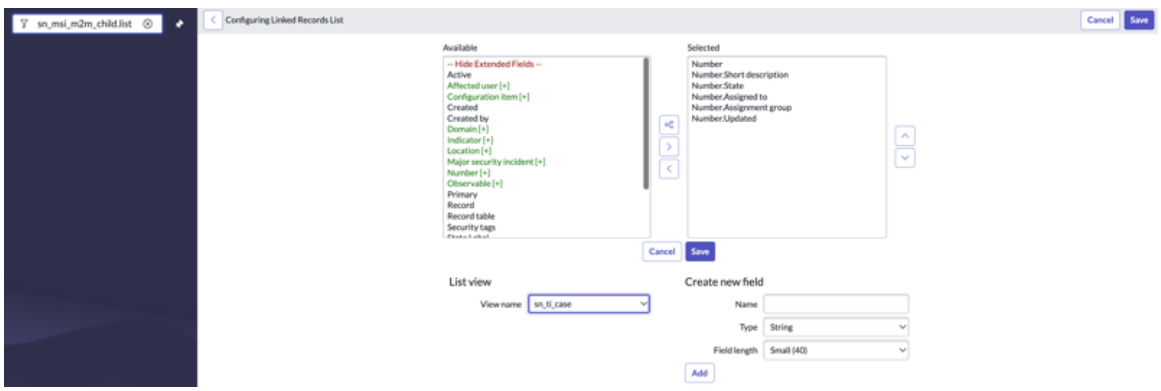
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Gehe zu **Listenansicht** > **Namen anzeigen**an.
4. Wählen Sie Aus **Neu** Aus der Dropdown-Liste Ansichtsname.



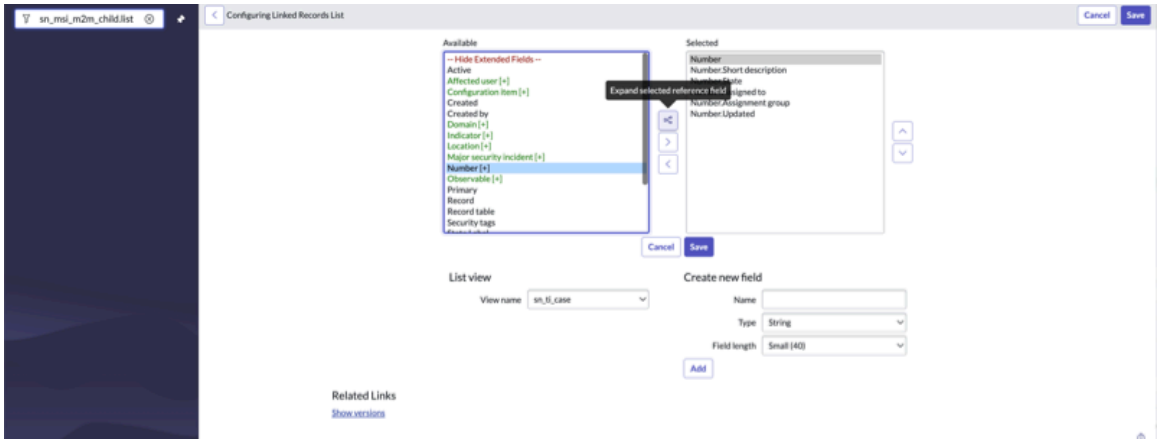
5. Wählen Sie die Spalten aus, die in der Listenansicht des Arbeitsbereichs gerendert werden. Der Sicherheitsfalldatensatz wird in gespeichert **Nummer** Spalte. Um Informationen aus einem Sicherheitsfall zu rendern, müssen Sie DOT-Walk auf dem durchführen **Nummer** Spalte.



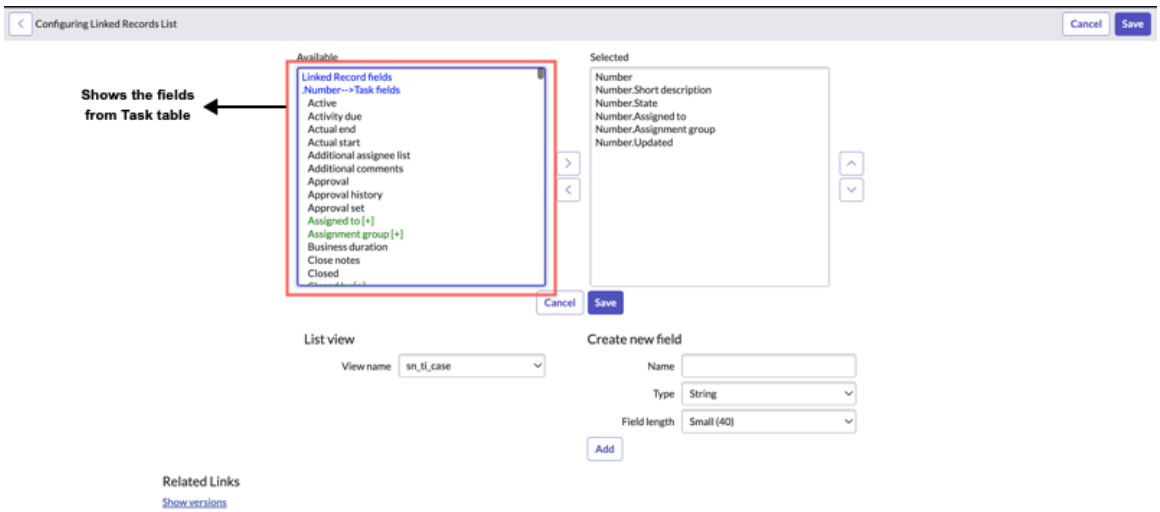
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Um DOT-Walking durchzuführen, wählen Sie zuerst aus **Nummer** Spalte aus der Liste verfügbar, und klicken Sie dann auf **Erweitern Sie Das Ausgewählte Referenzfeld** .



b. Erweitern Sie die Spalten von **Nummer** Um sie auszuwählen und in die Liste ausgewählt zu verschieben.



c. Klicken Sie Auf **Speichern** Zum Speichern und Erstellen einer Ansicht.

6. Der nächste Schritt besteht darin, die erstellte Ansicht in zu rendern Management schwerwiegender Sicherheits-Incidents Arbeitsbereich, müssen Sie einen erstellen **Listenlayoutkonfiguration** .

a. Suchen Sie nach **Listenlayoutkonfiguration** Verwenden Sie die linke Navigation.

b. Klicken **MSI-Administration** > **Listenlayoutkonfigurationen**an.

c. Klicken Sie auf **Neu**, um eine neue Konfiguration zu erstellen.

d. Wählen Sie die Quelltabelle in der Spalte Tabelle aus, und wählen Sie die neu erstellte Ansicht im Feld Listenansicht aus.

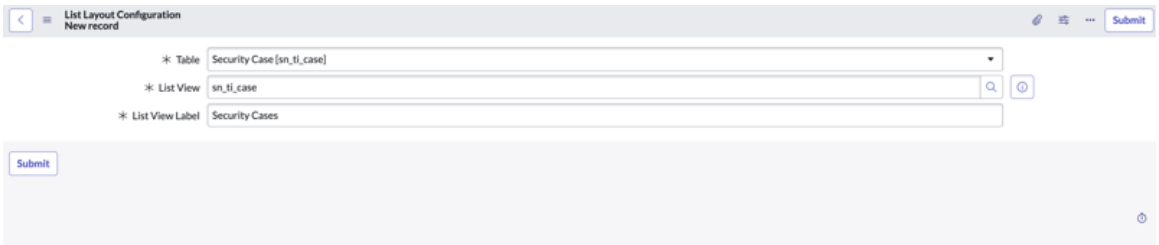
e. Die **Listenansicht** Mit der Bezeichnung können Sie Bezeichnungen steuern, wenn dieselbe Quelltabelle in gerendert wird Management schwerwiegender Sicherheits-Incidents Arbeitsbereich.

f. **Speichern** Der Datensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Navigieren Sie nach dem Speichern des Datensatzes zu Management schwerwiegender Sicherheits-Incidents Arbeitsbereich zum Anzeigen der gerenderten Listenansicht und Bezeichnung im Arbeitsbereich.



Schritt 5. Fügen Sie Zugriffssteuerungslisten (ACLs) für hinzu Management schwerwiegender Sicherheits-Incidents Arbeitsbereichsanwender

Fügen Sie Zugriffssteuerungslisten (ACLs) für hinzu Management schwerwiegender Sicherheits-Incidents Arbeitsbereichsanwender.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis:
Die Berechtigungen, die zum Verknüpfen und Aufheben der Verknüpfung von Funktionen erforderlich sind, werden von gesteuert sn_msi.linkedsivi_read Rolle.

Management schwerwiegender Sicherheits-Incidents Persona enthält die Rolle „sn_msi.linkedsivi_read“.

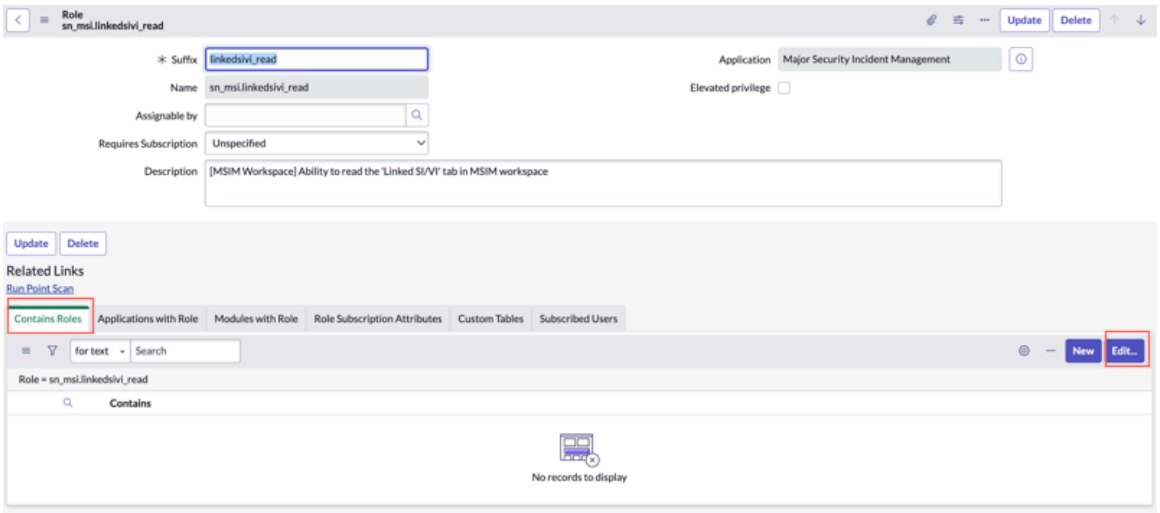
1. sn_msi.Workspace_admin (MSIM-Arbeitsbereich-Administrator)
2. sn_msi.Workspace_Manager (MSIM-Arbeitsbereichsmanager)
3. sn_msi.Workspace_Responder (MSIM Workspace Responder)

Hinweis:
Für jede Quelltabelle müssen Sie sicherstellen, dass die erforderlichen Rollen zu hinzugefügt werden sn_msi.linkedsivi_read Rolle.

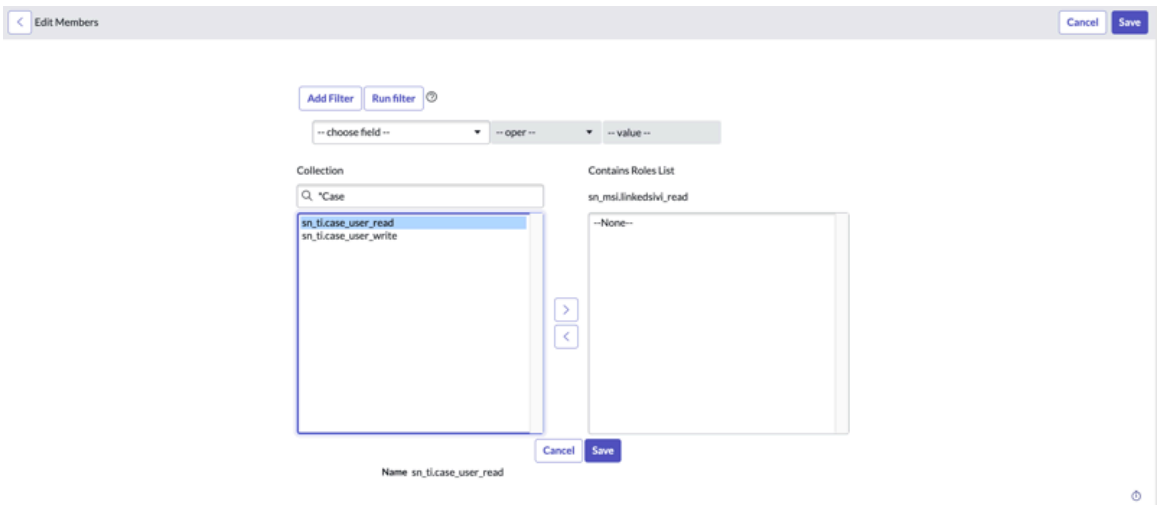
Prozedur

1. Navigieren zu **Anwenderadministration** > **Rollen** Und suchen Sie nach **sn_msi.linkedsivi_read** Rolle.
2. Klicken Sie Auf **Bearbeiten** Im zugehörigen Listenabschnitt enthält Rollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Stellen Sie sicher, dass Ihre Quelltabellenrollen im Abschnitt enthält Rollen hinzugefügt werden.
   Die Seite Mitglieder bearbeiten wird angezeigt, um die für einen Sicherheitsfall erforderlichen Rollen zu konfigurieren.



4. Suchen Sie im Abschnitt Sammlungen nach den Rollen der Quelltabelle.
   Wählen Sie die erforderlichen Rollen aus, die Lese- und Schreibzugriff auf die Quelltabelle für einen Sicherheitsfall zulassen.

Hinweis:

- Für einen Sicherheitsfall sind zwei separate Rollen für Lese- und Schreibvorgänge erforderlich.
- Schreibzugriff auf Tabellen, aus denen der Quelldatensatz ausgewählt werden kann Management schwerwiegender Sicherheits-Incidents Arbeitsbereich – modales Element für verknüpften Datensatz.

5. Klicken Sie Auf **Speichern** Zum Hinzufügen von Rollen.
6. Stellen Sie sicher, dass die Rollen erfolgreich zu hinzugefügt wurden **Enthält Rollen** Abschnitt „zugehörige Liste“.

Schritt 6. Erstellen Sie Geschäftsregeln für einen Sicherheitsfall

Erstellen Sie erforderliche Geschäftsregeln für einen Sicherheitsfall.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Erstellen Sie die drei folgenden Geschäftsregeln für die neue Quelltabelle „Sicherheitsfall“ (sn_ti_Case). Diese Geschäftsregeln sind erforderlich, um die Konsistenz im Verhalten mit der sofort einsatzbereiten Quelltabelle wie Security Incident (sn_si_Incident) zu gewährleisten.

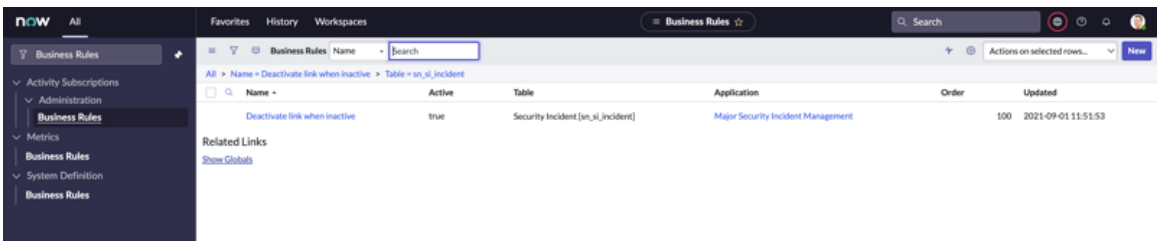
Business-Regeln für die neue Quelltabelle:

1. **Deaktivieren Sie den Link, wenn er inaktiv ist** : Sobald der Sicherheitsfall geschlossen wurde, werden zugehörige Informationen in nicht mehr angezeigt Management schwerwiegender Sicherheits-Incidents Arbeitsbereichsseite.
2. **Synchronisieren Sie Teaminformationen bei der Aktualisierung** : Registerkarte „Details zu schwerwiegenden Security Incidents“ zeigt Informationen zu allen aktiven Teams und Anwendern an, die an verschiedenen Aufgaben arbeiten. Sobald der Anwender „Zugewiesen an“ oder die Zuweisungsgruppe im Sicherheitsfall geändert wurde, müssen wir die Teaminformationen für Sicherheitsfälle im Abschnitt „schwerwiegender Security Incident – aktives Team“ aktualisieren. Diese Business-Regeln aktualisieren den neuen Anwender „Zugewiesen an“ und die Zuweisungsgruppe im Abschnitt „aktives Team“.
3. **Synchronisieren Sie Teaminformationen beim Löschen** : Registerkarte „Details zu schwerwiegenden Security Incidents“ zeigt Informationen zu allen aktiven Teams und Anwendern an, die an verschiedenen Aufgaben arbeiten. Sobald wir den Sicherheitsfall geschlossen haben, müssen wir im Abschnitt „schwerwiegender Security Incident – aktives Team“ keine Teaminformationen mehr anzeigen. Diese Business-Regeln entfernen den Anwender „Zugewiesen an“ und die Zuweisungsgruppe aus dem aktiven Team.

Business-Regeln für neue Quelltabelle erstellen:

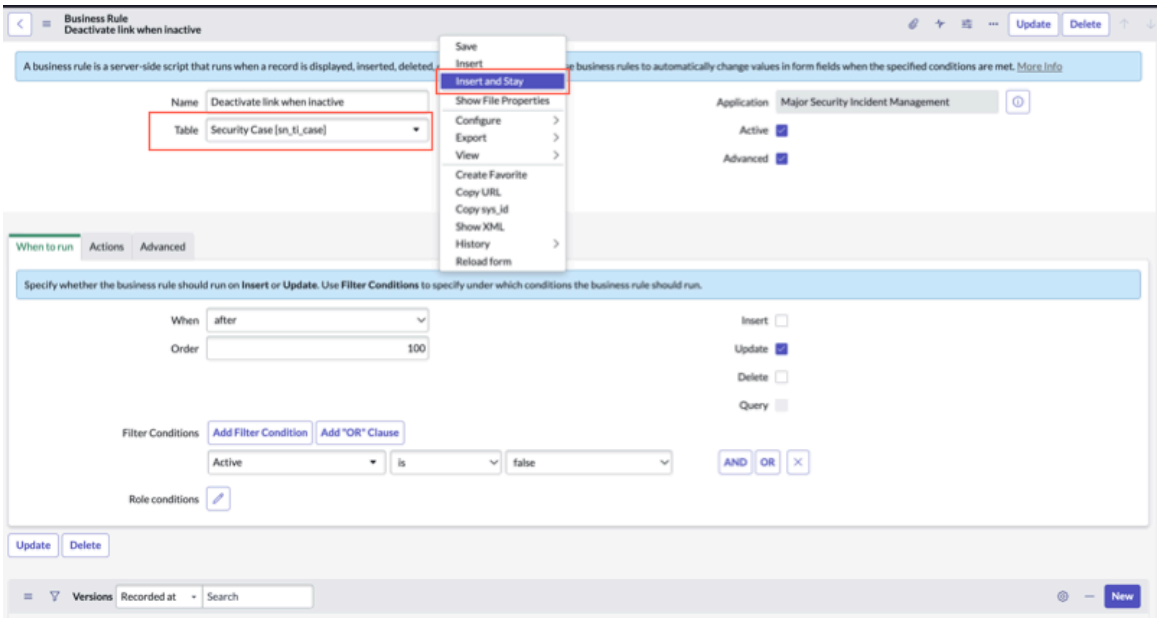
Prozedur

1. Navigieren zu **Systemdefinition** > **Business-Regeln**an.
2. Führen Sie die Filteroption aus, um Business-Regeln-Kriterien mit den folgenden Informationen zu filtern:
   - **Name** : Link deaktivieren, wenn inaktiv
   - **Tabelle** : sn_si_Incident



3. Öffnen Sie den Datensatz, und ändern Sie den Tabellennamen in eine neue Quelltabelle: sn_ti_Case .
4. Klicken Sie mit der rechten Maustaste auf das Menü auf der Seite, und klicken Sie auf **Einfügen und beibehalten** Zum Erstellen des Datensatzes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wiederholen Sie den Vorgang auch für zwei weitere Business-Regeln.
   - Synchronisieren Sie Teaminformationen beim Löschen
   - Synchronisieren Sie Teaminformationen bei der Aktualisierung

Schritt 7. Erstellen Sie Rollup-Datensatzkonfigurationen

Erstellen Sie eine Rollup-Datensatzkonfiguration, um zusätzliche Datensätze mit MSI zu verknüpfen und die Verknüpfung aufzuheben.

Vorbereitungen
Erforderliche Rolle: admin und sn_msi.Workspace_admin

Hinweis:
Der Systemadministrator kann den Datensatz erstellen, und der MSI-Arbeitsbereich-Administrator kann ihn aktualisieren.

Erstellen Sie eine Rollup-Datensatzkonfiguration, um Informationen wie Konfigurationselemente, erkennbare Elemente und Indikatoren der Gefährdung im Zusammenhang mit einem Sicherheitsfall zusammenzufassen.

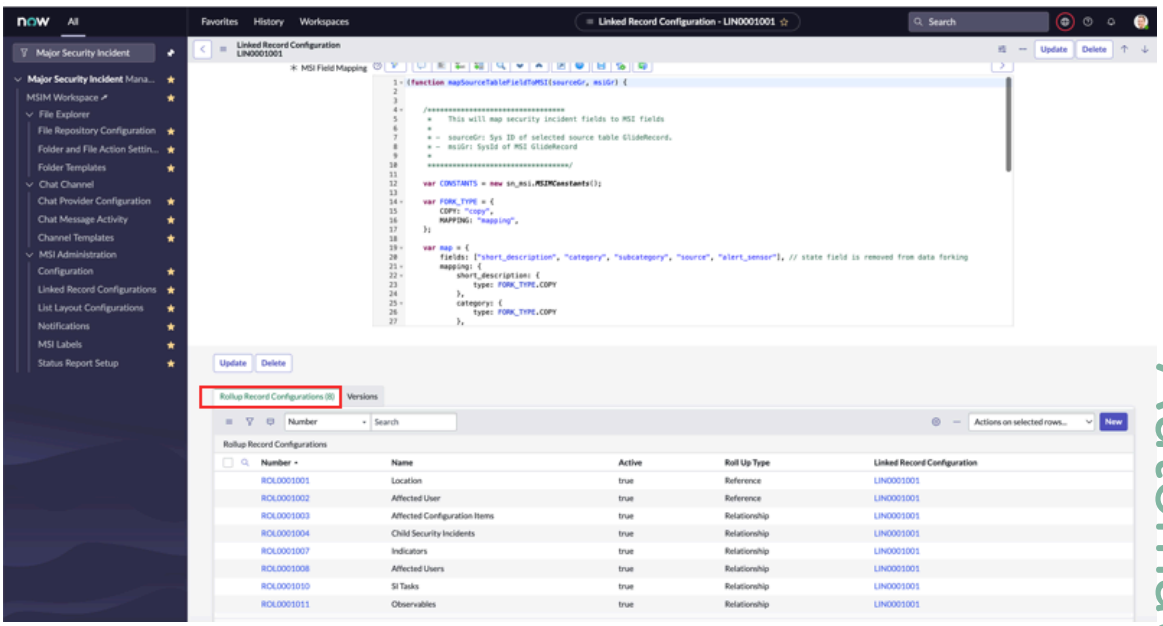
Prozedur

1. Navigieren zu **Antwort Auf Schwerwiegende Security Incidents** > **Konfiguration Der Verknüpften Datensätze**an.
   Die Seite Konfigurationen verknüpfter Datensätze wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen Sie einen neuen verknüpften Datensatz aus, oder erstellen Sie ihn, und navigieren Sie zu **Rollup-Datensatzkonfiguration** Abschnitt auf derselben Seite.

Abschnitt „Rollup-Datensatzkonfiguration“



Nächste Maßnahme

- Weitere Informationen finden Sie unter Konfigurieren Sie Rollup-Datensätze in Management schwerwiegender Sicherheits-Incidents
- Beispielinformationen zu Sicherheitsfällen finden Sie unterSchreiben eines Skripts für einen Sicherheitsfall

Schreiben eines Skripts für einen Sicherheitsfall

Schreiben eines Skripts für einen Sicherheitsfall zur Rollup-Datensatzkonfiguration.

Vorbereitungen

Erforderliche Rolle: admin und sn_msi.Workspace_admin

Hinweis:
Der Systemadministrator kann den Datensatz erstellen, und der MSI-Arbeitsbereich-Administrator kann ihn aktualisieren.

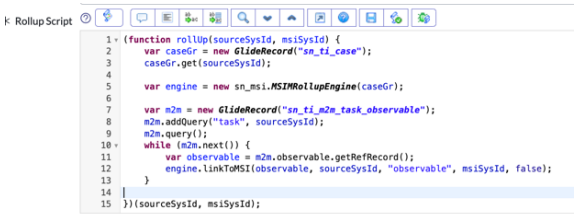
Prozedur

1. Suchen Sie über die linke Navigation nach den Konfigurationen des verknüpften Datensatzes.
2. Navigieren zu **MSI-Administration** > **Konfiguration verknüpfter Datensätze**an.
3. Öffnen Sie den Konfigurationsdatensatz, der für einen Sicherheitsfall erstellt wurde.
4. Die Konfiguration des Rollup-Datensatzes wird im Abschnitt zugehörige Liste angezeigt.
5. Klicken Sie Auf **Neu** Dient zum Erstellen einer neuen Rollup-Datensatzkonfiguration.

   Nachfolgend finden Sie einen Beispieldatensatz, der erstellt wurde, um Daten erkennbarer Elemente im Zusammenhang mit dem Sicherheitsfall Rollup mit den Feldwerten wie folgt durchzuführen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Rollup-Typ	Beziehung **Hinweis:** Die Informationen des erkennbaren Elements sind in einem zugehörigen Listenformat verfügbar.
Rollup-Skript	EingabequelleSysId enthält die SYS-ID des Sicherheitsfalls, und msiSysId enthält die SYS-ID des schwerwiegenden Security Incidents  ○ Line 2: As a first step, query for Glide Record for sourceSysId from **Security Case(sn_ti_case)** table. ○ Line 7: Next, query **sn_ti_m2m_task_observable** table using security case sys ID to figure out all the linked observables to a security case. ○ Line 10: Next, iterate over all the linked observables and link them to a Major Security Incident using the method: `MSIMRollupEngine.linkToMSI(„entityGr“, „sourceSysId“, „fieldNameInLinkedRecordTable“, „msiSysId“, „isPrimaryRecord“)`

Führen Sie einen atomaren Rollup bei Bedarf aus

Rollup-Framework kann keine Updates für die vorhandenen verknüpften Datensätze verarbeiten. In solchen Fällen sollte ein atomarer Rollup bei Bedarf für verknüpfte Datensätze erfolgen, was über Business-Regeln erreicht werden kann.

Um Aktualisierungen der verknüpften Datensätze zu erfassen, müssen Geschäftsregeln in der Quelltabelle erstellt werden.

Diese Business-Regeln funktionieren beim Einfügen, Aktualisieren und Löschen von Vorgängen. Wenn Sie das Einfügen oder Aktualisieren ausführen, müssen Sie Rollup-Informationen zu hinzufügen oder aktualisieren MSI. Wenn Sie löschen, werden die Rollup-Informationen aus entfernt MSI.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Sobald ein Security Incident mit verknüpft ist MSI, Die zugehörigen Informationen werden automatisch zusammengefasst MSI. Aber später, wenn Sie einem ein neues erkennbares Element hinzufügen MSI, Dann wird auch das neu hinzugefügte erkennbare Element zu zusammengefasst MSI. Hier, **Rollup des erkennbaren Elements synchronisieren** Die Business-Regel erfasst das Update und erstellt ein Rollup des aktualisierten Datensatzes MSI. Ebenso verarbeitet dieselbe Business-Regel auch das Entfernen der vorhandenen Rollup-erkennbaren Elemente, wenn sie aus dem Security Incident entfernt wird.

Vordefinierte Business-Regeln

Im Folgenden finden Sie einige vordefinierte Geschäftsregeln, die Ihnen helfen, die Handhabung von atomaren Rollups zu verstehen

Regel	Beschreibung
Rollup-Indikator für Synchronisierung (sn_ti_m2m_Task_indicator)	Verwenden Sie diese Business-Regel, um das Rollup und Entfernen des Indikators der Gefährdung aus Security Incident, Sicherheitsfall und Korrekturaufgabe zu verarbeiten.
Rollup des erkennbaren Elements synchronisieren (sn_ti_m2m_Task_Observable)	Mit dieser Business-Regel wird das Rollup und Entfernen verknüpfter erkennbarer Elemente aus Security Incident, Sicherheitsfall und Korrekturaufgabe verarbeitet.
Rollup betroffener Anwender synchronisieren (sn_si_m2m_Task_affected_user)	Mit dieser Business-Regel wird das Rollup und Entfernen verknüpfter betroffener Anwender aus Security Incident, Sicherheitsfall und Korrekturaufgabe verarbeitet.
Rollup betroffenes CI synchronisieren (Task_ci)	Mit dieser Business-Regel wird das Rollup und Entfernen zugeordneter Konfigurationselemente aus Security Incident, Sicherheitsfall und Korrekturaufgabe verarbeitet.

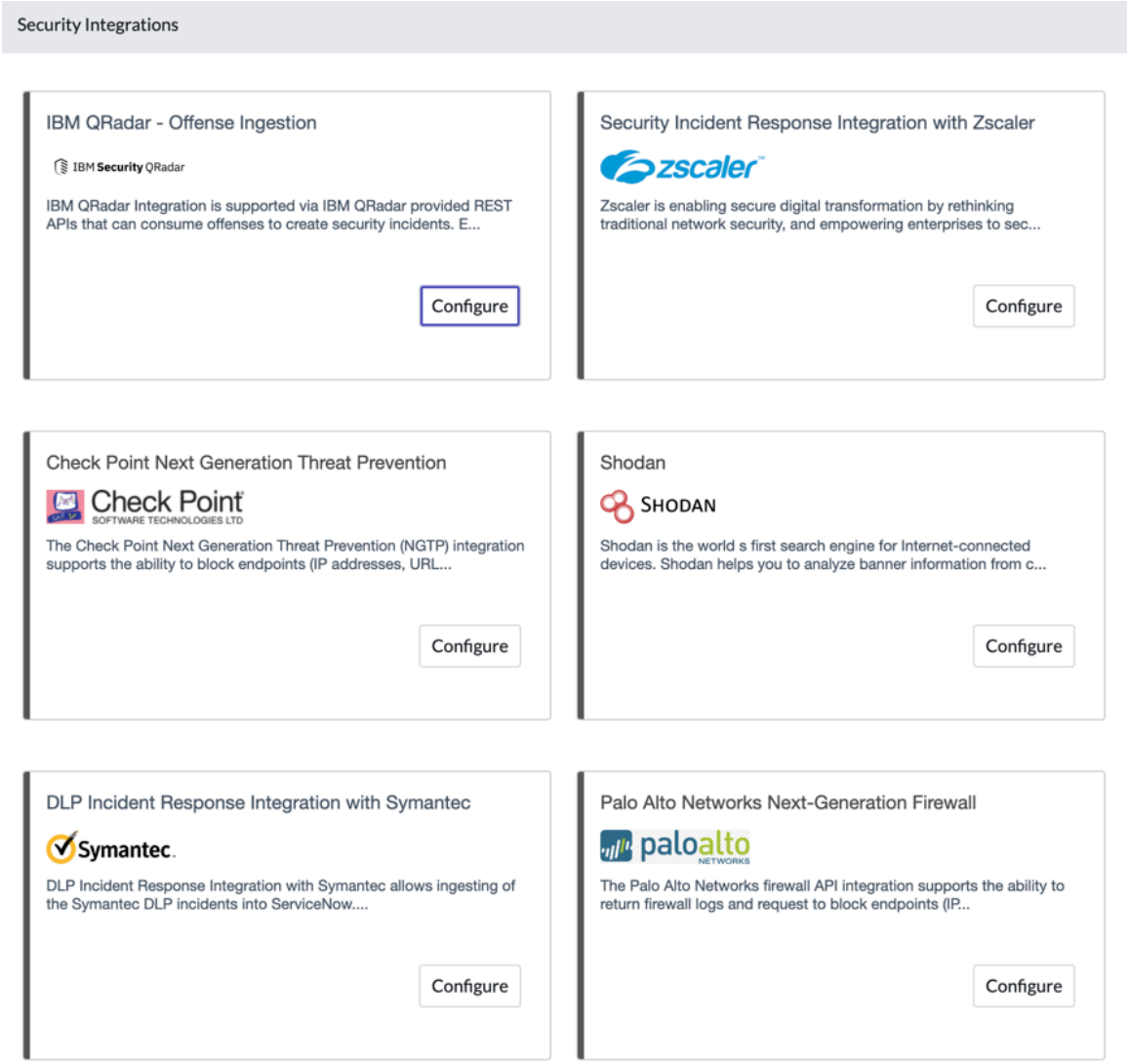
Security Incident Response-Integrationen

Alle Security Operations Kernanwendungen und nicht-Core-Integrationen von Drittparteien sind über verfügbar ServiceNow Store. Dieser Abschnitt enthält Anweisungen zum Aktivieren der Integrationen und zum Konfigurieren beider ServiceNow Und Drittpartei-Integrationen. Ebenfalls enthalten sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten Integrationen, die im Basissystem enthalten sind.

Integrationskonfigurationen

Das Basissystem enthält eine Reihe von „Karten“ für jede der Integrationsimplementierungen, die Sie aktivieren und verwenden können. Außerdem werden Karten für alle im ServiceNow Store veröffentlichten Integrationen angezeigt, die Abhängigkeiten von haben Security Operations Plugins. Die Integrationskarten können angezeigt werden, indem Sie auswählen **Security Operations** > **Integrationskonfigurationen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können die sichtbaren Integrationen mit filtern **Kategorie** Dropdown-Menü. Die **Konfigurationen Anzeigen** Im Dropdown-Menü können Sie mehrere Instanzen von Implementierungen anzeigen, die ihre Erstellung ermöglichen.

Schaltflächen auf Integrationskarten

Integrationskarten zeigen je nach Status der Integration und Quelle der Karte verschiedene Schaltflächen an.

Schaltfläche	Beschreibung
Plugin installieren	Klicken Sie auf diese Schaltfläche, um das entsprechende Plugin zu installieren, um die Integration zu aktivieren. Nachdem das Plugin installiert wurde, ändert sich die Schaltfläche in **Konfigurieren** .
Konfigurieren	Klicken Sie auf diese Schaltfläche, um Informationen zum Konfigurieren der Integration einzugeben. Bei einigen Integrationen müssen Sie möglicherweise API-Schlüssel oder URLs eingeben, die von der Website der Drittpartei-Integration erworben wurden.
Neu	Mit bestimmten Integrationen wie Carbon Black und IBM QRadar können Sie mehrere Implementierungen derselben Integration definieren. Klicken Sie für diese Integrationen auf

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schaltfläche	Beschreibung
	Neu Nachdem das Plugin aktiviert wurde. Mit den Karten können Sie Plugins installieren (falls zutreffend) und die Implementierungen für die Verwendung konfigurieren.
Seite öffnen	Im -Basissystem führt Ihre Instanz eine Abfrage des ServiceNow Store für alle Anwendungen durch, die Abhängigkeiten von haben Security Operations Plugins. Wenn diese Anwendungen gefunden werden und die zugehörigen Anwendungs-Plugins aktiviert sind, werden Integrationskarten für sie mit den anderen Sicherheitsintegrationskarten angezeigt. Klicken Sie Auf **Öffnen Sie Die Seite** Um auf die Website der Drittparteianwendung zuzugreifen, um die Integration zu konfigurieren. Nachdem Sie die Konfiguration abgeschlossen haben, die **Öffnen Sie Die Seite** Schaltfläche ändert sich in **Konfigurieren** .

ArcSight ESM Integration der Ereigniserfassung

Die ArcSight ESM Integration der Ereigniserfassung mit Security Incident Response Mit dem Produkt können Security Incident-Analysten korrelierte Ereignisse erfassen und die Erstellung von Security Incidents mit automatisieren ServiceNow Plattform. Daten werden kontinuierlich basierend auf einem konfigurierten Abfragungsplan erfasst und von Analysten verwendet, um potenzielle Cybersicherheitsbedrohungen zu identifizieren und darauf zu reagieren.

Mit dieser Integration können korrelierte Ereignisse, die Kandidaten für Security Incidents sind, regelmäßig erfasst werden. Sie können Felder in korrelierten Ereignissen Security Incident-Feldern zuordnen, eine Vorschau des Setups eines Ereignisses als Security Incident anzeigen und die geplante Erfassung von Ereignissen einrichten, um Security Incidents automatisch fortlaufend zu erstellen.

Übersicht über ArcSight ESM Integration der Ereigniserfassung

Diese Integration bietet einem Analysten des Security Operations Center (SOC) Transparenz für Korrelationsereignisse in ArcSight ESM. Diese Daten können in integriert werden ServiceNow AI Platform Security Incident Response (SIR) für weitere Untersuchungen und Nachbesserungen. Profile werden in erstellt ServiceNow AI Platform Instanz zur Verarbeitung verschiedener Korrelationsereignistypen, die über Korrelationsabfragebetrachter in erstellt und verfügbar gemacht werden ArcSight ESM. Diese Profile passen den Unterschied an ArcSight ESM Korrelierte Ereignisfelder werden in SIR Security Incidents angezeigt.

Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Erstellen Sie mehrere zu erstellende Ereigniserfassungsprofile SIR Security Incidents für bestimmte Arten von Bedrohungen wie Malware und nicht autorisierte Zugriffsversuche.
- Drag-and-Drop-Zuordnung von ArcSight ESM Korrelationsereignisfeldwerte zu zugeordnet SIR Security Incident-Felder.
- Eine Vorschau von SIR Security Incident-Layout basierend auf Beispielkorrelationsereignissen zur Validierung der Ereigniszuordnungsdetails.
- Erfassen Sie historische Korrelationsereignisse sowie neue wichtige Ereignisse in konfigurierbaren Intervallen.
- Filtern Sie Korrelationsereignisse heraus, die nicht erfüllen SIR Kriterien für die Incident-Generierung, z. B. Ereignisse mit niedriger Priorität

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ereignisse in vorhandenen aggregieren SIR Security Incidents basierend auf übereinstimmenden Feldwerten, um doppelte Security Incidents zu vermeiden.
- Aktualisieren Sie Korrelationsereignisse basierend auf SIR Bedingungen für die Erstellung und/oder den Abschluss von Incidents über eine bidirektionale Schnittstelle.

Unterstützt ServiceNow AI Platform Versionen

Diese Integration unterstützt New York Patch 6 und Orlando ServiceNow AI Platform Releases.

Die folgenden Security Operations-Anwendungen müssen über installiert und aktiviert werden ServiceNow Store. Installieren und aktivieren Sie jeweils eine Anwendung in der unten aufgeführten Reihenfolge, um eine reibungslose Installation sicherzustellen:

1. Sicherheits-Integrations-Framework
2. Security Support Common
3. Security Incident Response
4. Ereignis- und Warnungserfassung für Security Operations
5. Integrations-Hub-Plugins
   a. ServiceNow Integration Hub-Laufzeit
   b. ServiceNow Integration Hub-Aktionsschritt – REST

Weitere Informationen zur Installation von finden Sie Security Operations Kernanwendungen, siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

ArcSight ESM Unterstützte Versionen

Diese Integration wurde mit Version 7.0.0.2436 von getestet ArcSight ESM Manager. Die Integration unterstützt beides ArcSight ESM Lokale und Cloud-/gehostete Serviceumgebungen.

MID-Server

Diese Integration erfordert einen installierten und konfigurierten MID-Server in Ihrem ServiceNow AI Platform® Instanz, die mit verbunden werden soll ArcSight ESM Service, wenn ArcSight ESM Server wird in Ihrem Unternehmensnetzwerk bereitgestellt. Wenn Sie verwenden ArcSight ESM Cloud-Service, ein MID-Server ist nicht erforderlich. Siehe ServiceNow-Produktdokumentationswebsite Weitere Informationen zu MID-Servern.

Referenzen

Referenz	Dokumentbezeichner	Dokumententitel
1	ArcSight ESM Produktdokumentation	ArcSight-Produktdokumentation .
2	ServiceNow Produktdokumentations-Website	ServiceNow-Produktdokumentationswebsite

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie Ihr ein ServiceNow AI Platform® Instanz für ArcSight ESM Integration der Ereigniserfassung

Im folgenden Abschnitt werden die Setup-Aufgaben aufgeführt, die Sie in ausführen müssen ServiceNow AI Platform® Instanz vor der Installation der Anwendung über ServiceNow Store.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Überprüfen Sie anhand der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform® Und Security Incident Response-Rollen (SIR).	Die folgenden Rollen sind für die Installation, das Setup und die Verwendung der Integration in erforderlich ServiceNow AI Platform® Instanz. • Ein Anwender mit ServiceNow AI Platform® Die Administratorrolle (admin) installiert die Anwendung aus dem ServiceNow Store Und weist die Rolle Security Incident-Administrator (sn_si.admin) zu. • Ein Anwender mit der Rolle „sn_si.admin“ überwacht die folgenden Aufgaben in ServiceNow AI Platform®: ◦ Benennt, erstellt und bearbeitet Ereignisprofile. ◦ Wählt Werte aus und ordnet sie zu ArcSight ESM Korrelation von Ereignissen zu Security Incidents. ◦ Zeigt vor dem Abschluss der Konfiguration eine Vorschau der Security Incident-Details auf Richtigkeit an. ◦ Plant die laufende Erfassung korrelierter Ereignisse. ◦ Aktiviert Aktualisierungen korrelierter Ereignisse, wenn ein SIR-Incident erstellt und geschlossen wird. ◦ Weist die Rolle Security Incident Analyst (sn_si.Analyst) zu. ◦ Anwender mit sn_si.Analyst arbeiten mit Security Incidents. Weitere Informationen zu Rollen und dem Zuweisen von Rollen an Anwender finden Sie unter Rollen im ServiceNow-Produktdokumentationswebsite .
Stellen Sie sicher, dass Sie Version 7.0.0.2436 oder höher von verwenden	Wenn Sie Zugriff auf haben ArcSight ESM Abfrage-Viewer haben Sie Zugriff auf die API, die für diese Integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
ArcSight ESM Manager. Frühere Versionen werden nicht unterstützt.	erforderlich ist. Für die API ist kein anderes spezielles Setup erforderlich.
Richten Sie den Abfrage-Viewer in ein ArcSight ESM.	Bevor Sie Korrelationsereignisse erfassen können, müssen Sie den Abfrageanzeige in konfigurieren ArcSight ESM Konsole. Details siehe Richten Sie ein ArcSight ESM Abfrage-Viewer.
Optional Erstellen Sie anwenderdefinierte Phasen in ArcSight ESM Für Aktualisierungen von Korrelationsereignissen.	Ein Korrelationsereignis durchläuft viele Phasen in seinem Lebenszyklus, bevor es geschlossen wird. ArcSight ESM Stellt Standardphasen wie „anfänglich“, „Überwachung“, „in Warteschlange“ und „Geschlossen“ bereit. Einige dieser Phasen erfordern Anwendereingaben, andere Phasen werden jedoch automatisch ohne Anwendereingriff auf das Ereignis angewendet (die **Anwender Erforderlich** Das Feld ist in deaktiviert ArcSight ESM Konsole. Sie können anwenderdefinierte Phasen erstellen, die keine Anwendereingriffe erfordern, und sie in verwenden ServiceNow AI Platform® Instanz. Details siehe Zusätzliche Optionen: Korrelierte Ereignisaktualisierungen und -Abschlüsse basierend auf automatisieren SIR Incident-Status.
Überprüfen Sie, ob Sie eine MID-Serveranwendung installiert und konfiguriert haben.	Konfigurierte MID-Server-Anwendung Ein MID-Server in Ihrem ServiceNow AI Platform® Instanz ist erforderlich, um eine Verbindung mit herzustellen ArcSight ESM Service, wenn ArcSight ESM Server wird in Ihrem Unternehmensnetzwerk bereitgestellt. Siehe Installieren und konfigurieren Sie die ServiceNow-Anwendung für ArcSight ESM Integration der Ereigniserfassung Anweisungen zum Konfigurieren einer MID-Server-Anwendung. Siehe MID-Server Für Informationen zu MID-Servern. Wenn Sie einen gehosteten Service oder einen Cloud-Service verwenden, der über das Internet zugänglich ist, ist kein MID-Server erforderlich.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. **1.** Security Incident Response **2.** Sicherheits-Integrations-Framework **3.** Security Support Common **4.** Ereignis- und Warnungserfassung für Security Operations: Diese Anwendung erfordert:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit ○ Com.Glide.Hub.action_STEP.Rest => ServiceNow IntegrationHub Aktionsschritt – REST **5.** Threat Core Weitere Informationen zur Installation von finden Sie Security Operations Kernanwendungen, siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

Nächste Maßnahme

Sie haben erfolgreich eingerichtet ServiceNow AI Platform® Instanz für die Integration. Der nächste Schritt besteht in der Installation von ArcSight ESM Erfassung von Sicherheitsereignissen für die Anwendung Security Operations aus dem ServiceNow Store Für die Integration.

Richten Sie ein ArcSight ESM Abfrage-Viewer

Erstellen Sie einen Abfragebetrachter, und definieren Sie Filter, die kürzlich erstellte Korrelationsereignisse enthalten, die erfasst werden ServiceNow.

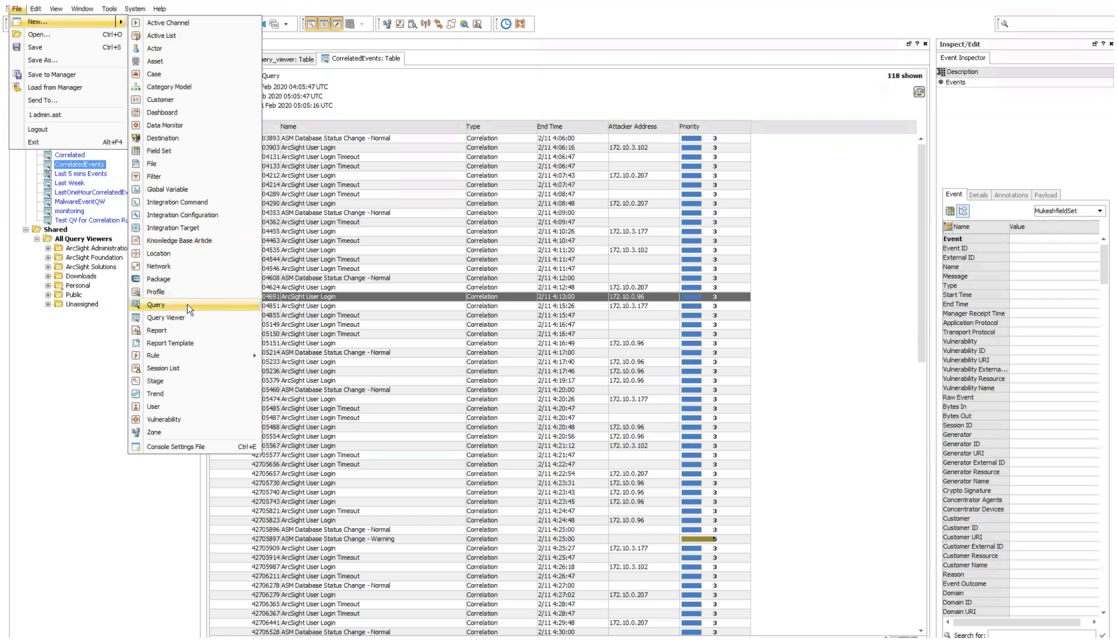
Vorbereitungen

Erforderliche Rolle: ArcSight-Administrator

Prozedur

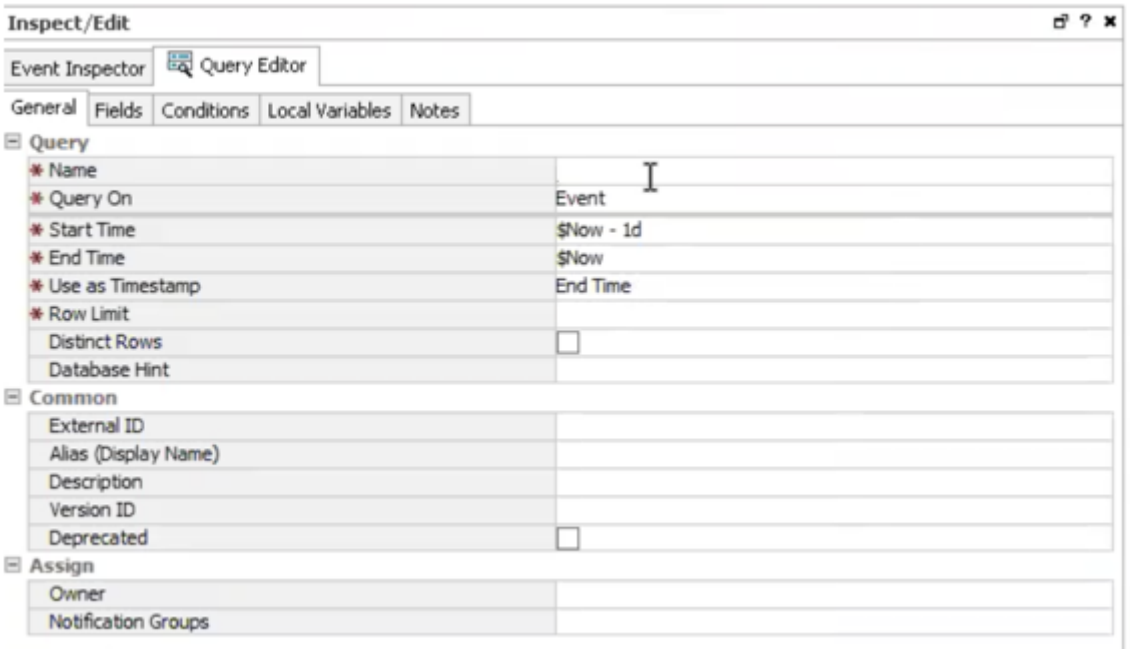
1. Melden Sie sich bei an ArcSight ESM Konsole zum Erstellen eines Abfrage-Viewers.

2. Um eine neue Abfrage zu erstellen, navigieren Sie zu **Datei** > **Neu** > **Abfrage**an.



3. Definieren Sie Bedingungen für die Abfrage-Viewer in **Überprüfen/Bearbeiten** Bereich.

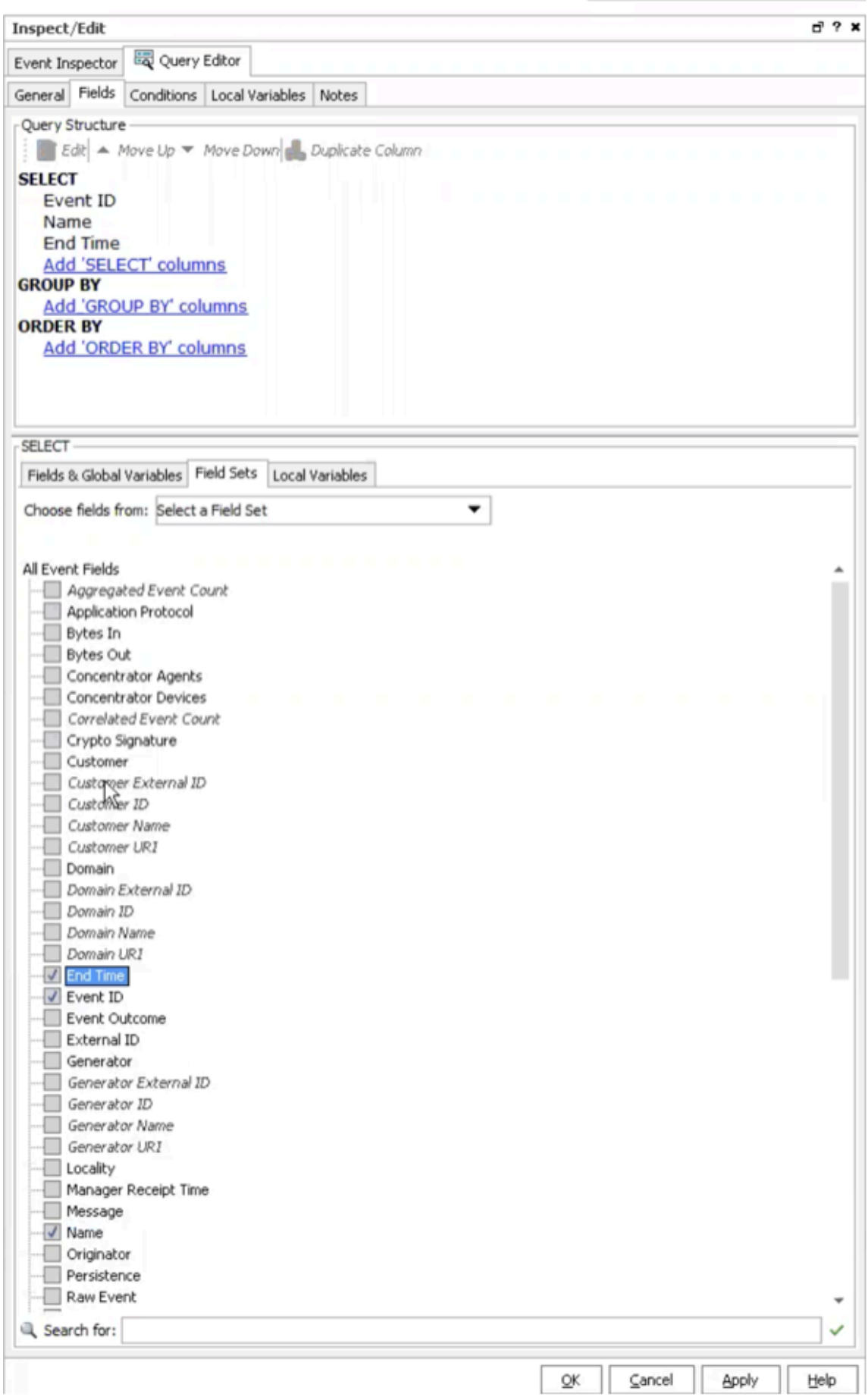
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Felder** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

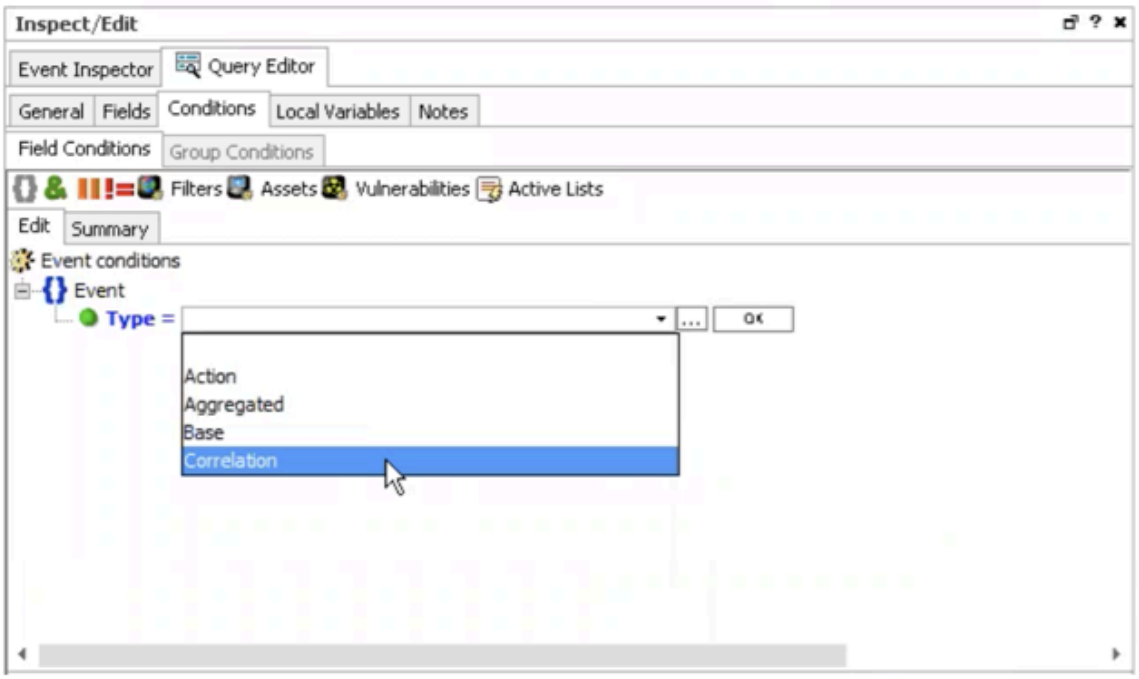


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

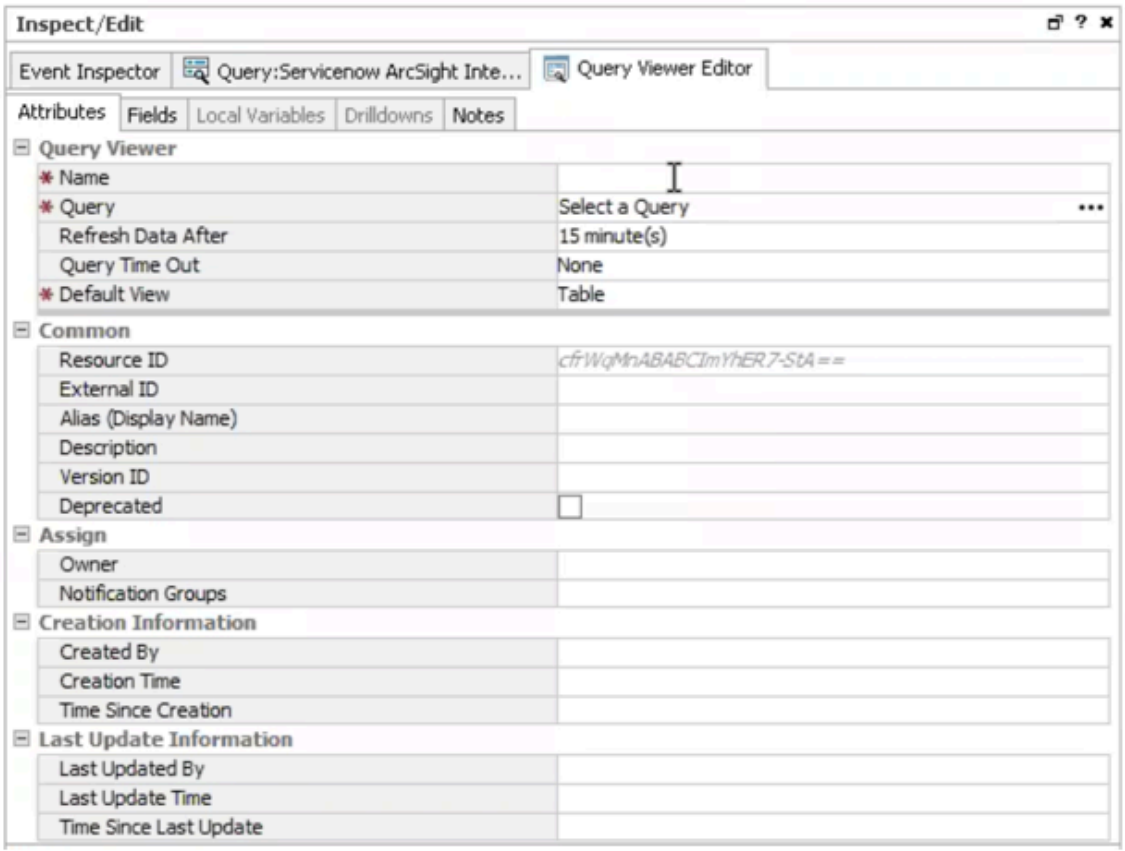
5. Wählen Sie die Felder aus, die bei der Erfassung berücksichtigt werden müssen.
   Sie müssen auswählen `Ereignis-ID` , `Name` , Und `Endzeit` Felder für erfolgreiche Erfassung.
6. Klicken Sie auf **Fügen Sie Spalten „SORTIEREN NACH“ hinzu** Verknüpfen und auswählen **Ereignis-ID** Feld und geben Sie die Sortierreihenfolge als an **Absteigend** Um sicherzustellen, dass die neuesten Ereignisse erfasst werden.
7. Klicken Sie auf **Bedingungen** Registerkarte.
8. Rechtsklick **Ereignis** Unter **Ereignisbedingungen** Unter **Zusammenfassung** Abschnitt.
9. Klicken **Neue Bedingung** > **Stamm** > **Typ** Und wählen Sie den Ereignistyp als aus **Korrelation** .

Wichtig:
Nur Korrelationsereignisse werden abgerufen. Basisereignisse für Korrelationen werden nicht abgerufen.



10. Klicken Sie Auf **OK** Zum Speichern der Abfrage.
    Der nächste Schritt besteht darin, einen Abfrage-Viewer für diese Abfrage zu erstellen.
11. Navigieren zu **Datei** > **Neu** > **Abfrage-Viewer**an.

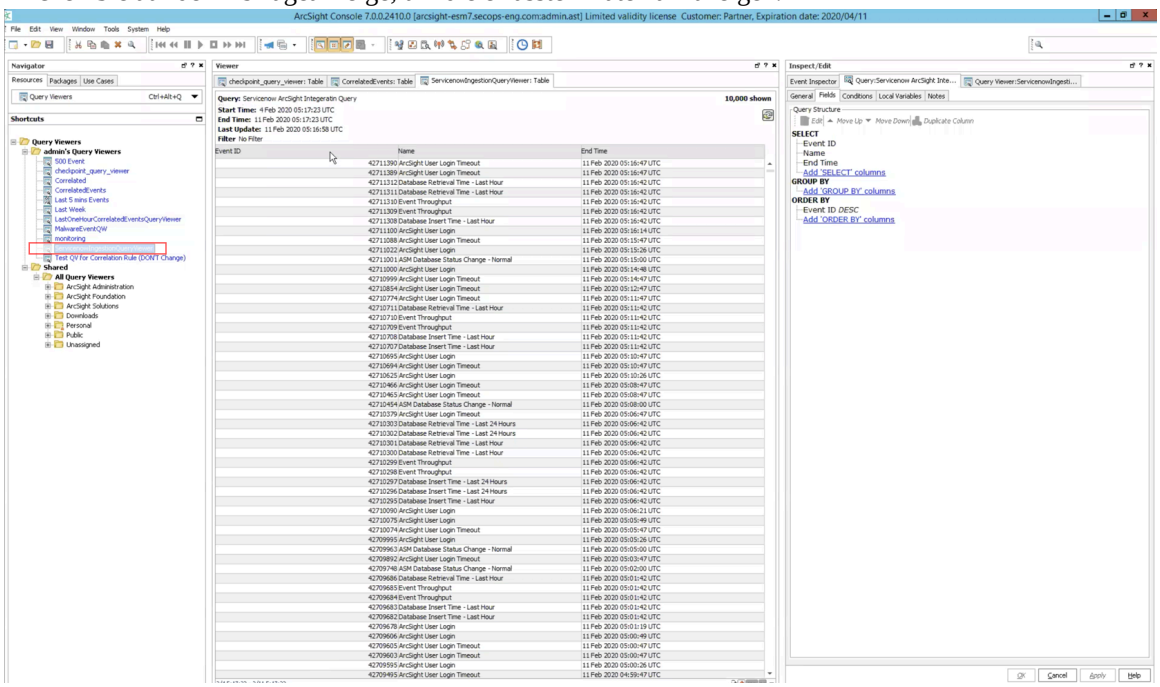
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



12. Klicken Sie auf **Felder** Registerkarte und stellen Sie sicher, dass die Pflichtfelder (*`Ereignis-ID, Name, Endzeit`*), die Sie in Ihrer Abfrage angegeben haben, sind ausgewählt.

13. Klicken Sie Auf **Anwenden** Zum Speichern des Abfrage-Viewers.
Der von Ihnen erstellte neue Abfrage-Viewer wird im Abschnitt Abfrage-Viewer aufgeführt.

14. Klicken Sie auf den Abfrageanzeige, um die erfassten Daten anzuzeigen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie die ServiceNow-Anwendung für ArcSight ESM Integration der Ereigniserfassung

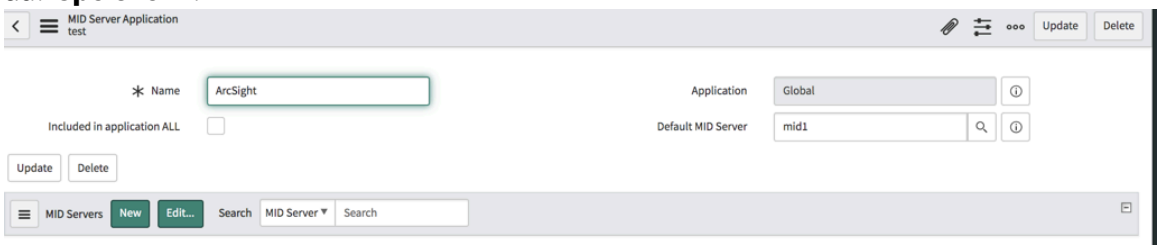
Bevor Sie die Integration für ausführen ServiceNow AI Platform® Führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in integriert wird Security Incident Response Und Security Operations Produkte auf Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn Sie den nicht installiert haben ArcSight ESM Anwendung aus dem ServiceNow Store Informationen zur Integration finden Sie unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie ArcSight ESM Kachel.
3. Klicken Sie auf , um die Anwendung zu konfigurieren **Neu** .
4. Alternativ, wenn ein **Konfigurieren** Die Schaltfläche wird auf einer Kachel angezeigt. Klicken Sie darauf, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie im Formular die Felder aus.
   Gehen Sie wie folgt vor, um eine neue MID-Server-Anwendung zu erstellen:
   a. Navigieren zu **MID-Server** > **Anwendungen** Und klicken Sie auf **Neu** .
   b. Geben Sie einen Namen für die MID-Server-Anwendung ein, und wählen Sie einen MID-Server aus, der als Standard verwendet werden soll.
   c. Deaktivieren Sie das Kontrollkästchen in Anwendung ALLE enthalten, und klicken Sie auf **Speichern** .

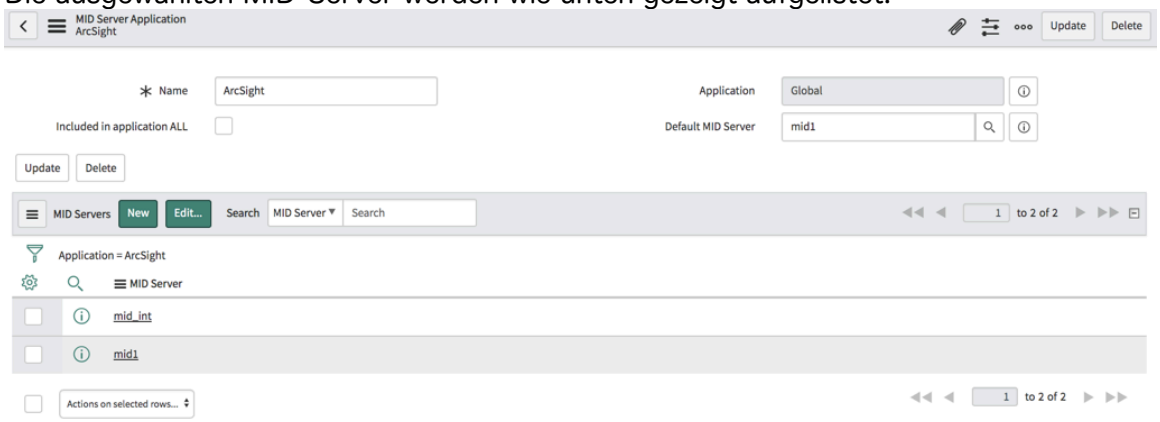


   d. Klicken Sie auf **Bearbeiten**. In **Bearbeiten Sie Mitglieder** Wählen Sie alle verfügbaren MID-Server aus, verschieben Sie sie in die Liste DER MID-Server, und klicken Sie auf **Speichern** .

Automatische Übersetzung

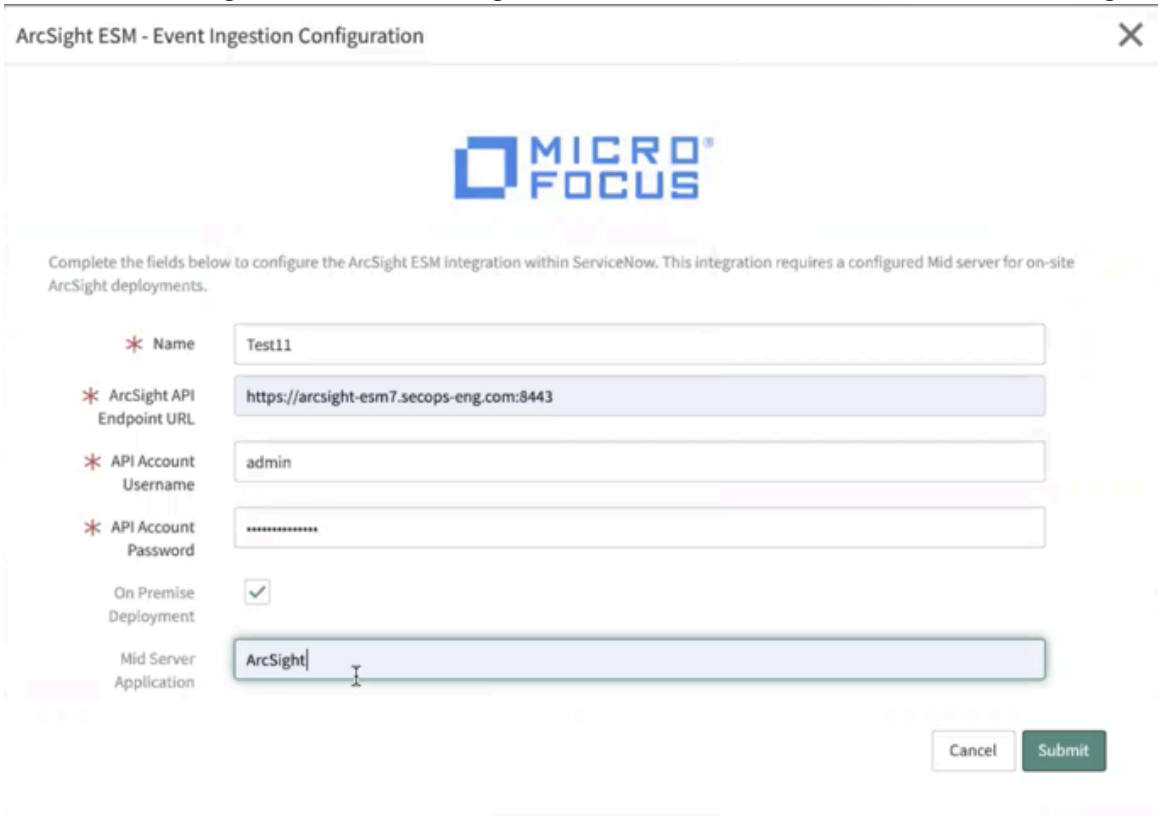
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Die ausgewählten MID-Server werden wie unten gezeigt aufgelistet.



Je nach Verfügbarkeit wird einer der mit der MID-Serveranwendung konfigurierten MID-Server verwendet.

6. Geben Sie die Konfigurationsdetails ein, und geben Sie die von Ihnen erstellte MID-Server-Anwendung an.



Jedes Korrelationsereignis, das Sie von erfassen ArcSight ESM Die Managerkonsole erfordert ein eindeutiges Ereignisprofil in Ihrer Instanz. Jedoch ist ArcSight ESM Die Quelle, die Sie im Formular „Konfiguration der Ereigniserfassung“ konfigurieren, kann für mehrere Profile wiederverwendet werden, solange jedes Profil eindeutige Korrelationsereignistypen erfasst.

7. Klicken Sie auf **Absenden**.
Nachdem sie erfolgreich validiert und übermittelt wurde, jeweils ArcSight ESM Die Serverkonfiguration wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, klicken Sie oben rechts auf der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja** .

Nächste Maßnahme

Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht darin, ein Ereignisprofil zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Profil

Als Anwender mit der Rolle sn_si.admin erstellen Sie ein Profil in Ihrem ServiceNow AI Platform Instanz und bestimmt, welche Korrelationsereignisse Security Incidents erstellen. Vor ServiceNow AI Platform Security Incident Response(SIR) Security Incidents werden aus Korrelationsereignissen erstellt, die Feldwerte aus Ereignissen werden in einem Layout von angezeigt ServiceNow AI Platform Security Incident, damit Sie eine Vorschau anzeigen können, wie der tatsächliche Security Incident erstellt wird.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Korrelationsereignisse werden automatisch in erfasst Security Operations Umgebung von ServiceNow AI Platform Instanz abhängig vom definierten Profiltyp. Ein Profil ist eine Kapselung eines Typs von Korrelationsereignissen, z. B. nicht autorisierte Zugriffsversuche oder Malware.

Nachdem ein Korrelationsereignis erfasst wurde, können Sie einzelne Korrelationsereignisfelder den entsprechenden Feldern im Security Incident zuordnen. Sie können Korrelationsereignisse filtern, um anzugeben, welche Ereignisse Security Incidents erstellen. Sie können beispielsweise Filter bevorzugen, die Security Incidents nur für Korrelationsereignisse erstellen, die als hohes Risiko identifiziert wurden. Sie können auch zusätzliche Ereigniszusammenfassungskriterien definieren, damit eingehende doppelte Korrelationsereignisse zu einem offenen Security Incident zusammengefasst werden. Schließlich können Sie einen Erfassungszeitplan definieren und das Profil aktivieren.

Namen für die Ereignisprofile in Ihrem ServiceNow AI Platform Die Instanz muss eindeutig sein und kann jeweils nur einem aktiven Ereignisprofil zugeordnet werden.

Erstellen und benennen Sie das Profil für ArcSight ESM Integration der Ereigniserfassung

Sie können ein Profil einrichten, um Korrelationsereignisse zu erfassen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

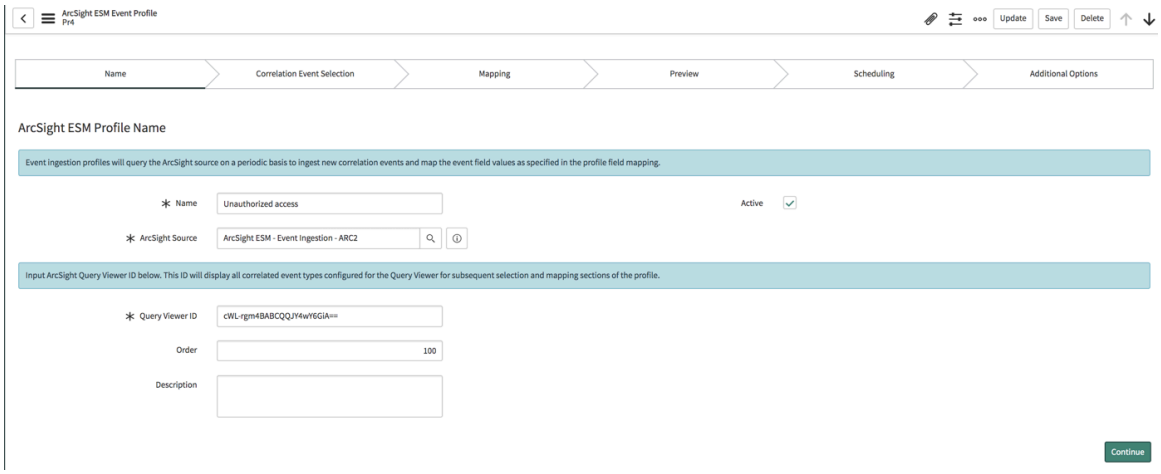
Prozedur

1. Dient zum Erstellen eines Ereignisprofils für ein Korrelationsereignis in ServiceNow AI Platform Instanz, navigieren Sie zu **ArcSight-ESM-Integration** > **ArcSight ESM-Ereignisprofil**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

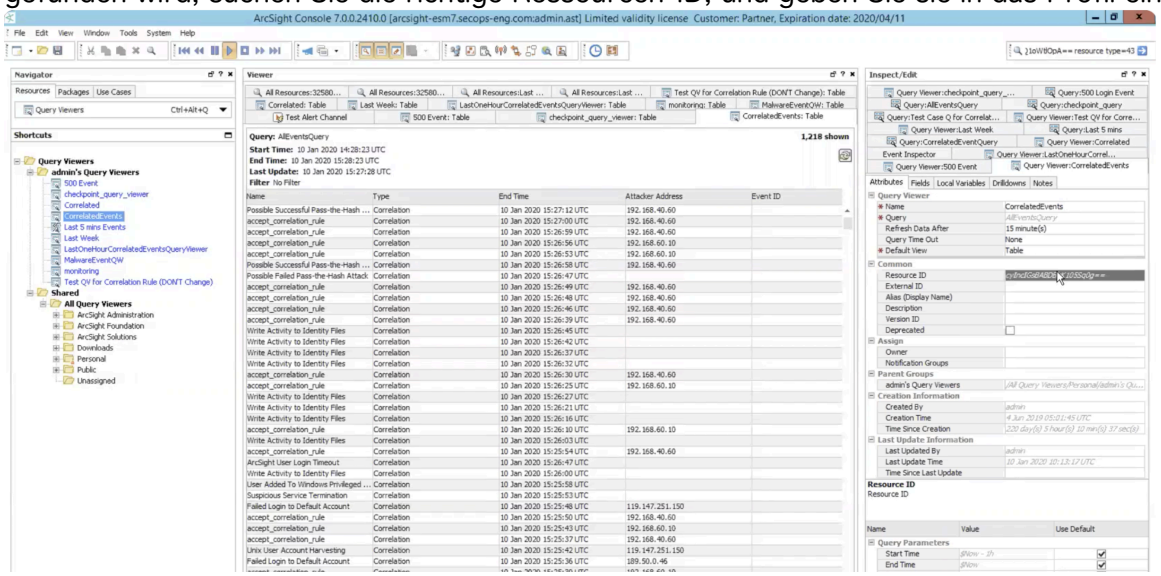
   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nachdem Sie die Profildetails eingegeben haben, klicken Sie auf **Fahren Sie Fort** . Die Abfrage-Viewer-ID wird validiert und ob eine entsprechende Ressourcen-ID in vorhanden ist ArcSight ESM Abfrage-Viewer: Der Name des Abfrage-Viewers wird wie unten dargestellt zurückgegeben. Wenn die Validierung fehlschlägt, überprüfen Sie, ob die Ressourcen-ID in vorhanden ist ArcSight ESM Konsole. Wenn die Ressourcen-ID nicht gefunden wird, suchen Sie die richtige Ressourcen-ID, und geben Sie sie in das Profil ein.



Nächste Maßnahme

Der nächste Schritt besteht darin, die Korrelationsereignistypen für die Erfassung aus der Abfrage-Viewer auszuwählen, die im vorherigen Schritt ausgewählt wurde.

Wählen Sie Korrelationsereignisse für aus ArcSight ESM Integration der Ereigniserfassung

Basierend auf ArcSight ESM Quelle und Abfrageanzeige konfiguriert, wählen Sie eine Korrelationsereignisregel für das Profil aus.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die verfügbaren Korrelationsereignisse an, die in der Korrelationsereignisauswahl in aufgeführt sind ServiceNow AI Platform Instanz, damit Sie bestimmen können, welche Korrelationsereignisse Sie erfassen und Security Incidents erstellen möchten. Sie können für jedes Profil nur einen Korrelationsregeltyp aus der Liste auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Abfrage-Viewer-ID und der Name des Abfrage-Viewers, wie im Formular „Abfrage-Viewer“ angegeben, werden angezeigt. Wählen Sie ein Korrelationsereignis aus der Liste aus, mit dem Sie eine Konfigurationszuordnung für das erfasste korrelierte Ereignis erstellen können.

Klicken Sie im Feld Liste der Korrelationsereignisse auf die Dropdown-Liste. Eine Liste der Korrelationsereignisse, die in vorhanden sind ArcSight ESM Abfrage-Viewer-Konsole wird angezeigt.

Klicken Sie Auf **Fahren Sie Fort** Um mit dem nächsten Schritt im Assistenten fortzufahren.

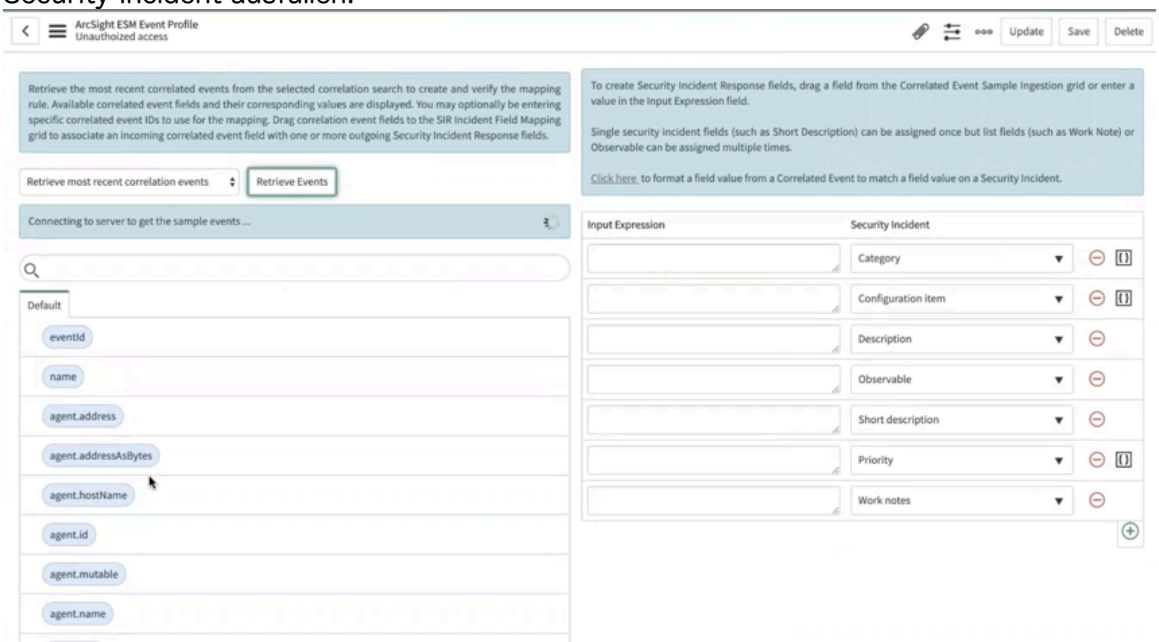
Zuordnungskorrelationsereignisfelder für ArcSight ESM Integration der Ereigniserfassung

Nachdem Sie die spezifische Korrelationsereignisregel aus der Liste identifiziert haben, besteht der nächste Schritt darin, Korrelationsereignisfelder den Feldern im Security Incident-Formular zuzuordnen.

Übersicht über die Zuordnungskorrelationsereignisfelder

Für den Zuordnungsschritt können Sie Beispielkorrelationsereignisse für die ausgewählte Korrelationsregel erfassen. Während dieser Zuordnungsphase können Sie sicherstellen, dass alle relevanten Korrelationsereignisfelddaten dem entsprechenden Ort in zugeordnet werden SIR Incident-Formular und visualisieren Sie dann SIR Incident im Vorschauabschnitt.

Die folgende Abbildung zeigt die Standardzuordnungskonfiguration, die zum Erstellen des Korrelationsereignisprofils bereitgestellt wird. Sie können die Felder anpassen, die den Security Incident ausfüllen.



Wenn Sie auf klicken **Ereignisse Abrufen** , Die Feldnamen des Korrelationsereignisses und die entsprechenden Werte werden auf der linken Seite des Formulars ausgefüllt. Dies sind die ArcSight ESM Korrelationsereignisfelder, die den Security Incident-Feldern zugeordnet werden können.

Möglicherweise möchten Sie einige Beispielkorrelationsereignisse in Ihrer Konsole überprüfen, um sie für den Konfigurationsschritt der Feldzuordnung zu erfassen. Dieser Schritt wird auf der Fortschrittsleiste mit Zuordnung bezeichnet. Wenn diese Seite nicht angezeigt wird, klicken Sie auf **Zuordnung** Auf der Fortschrittsleiste. Sie können bis zu fünf Beispielkorrelationsereignisse aus erfassen ArcSight ESM Manager für die ausgewählte Korrelationsregel zur Unterstützung des Feldzuordnungsprozesses. Es gibt Optionen zum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfassen der fünf neuesten Korrelationsereignisse für das ausgewählte Korrelationsereignis oder zum Erfassen von bis zu fünf spezifischen Korrelationsereignissen basierend auf den Ereignis-IDs.

Nachfolgend finden Sie eine Zusammenfassung der Schritte, die zum Zuordnen von Korrelationsereignissen erforderlich sind:

- Feldzuordnung: Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Korrelationsereignisfelder von der linken Seite ziehen und auf dem ablegen SIR Incident-Zuordnungsabschnitt auf der rechten Seite. Die Zuordnung auf der rechten Seite ordnet das Feld „eingehendes Korrelationsereignis“ einem Feld für ausgehende Security Incidents zu.
- Zuordnungs-Experience: Passen Sie das Zuordnungsraster an, indem Sie Felder mithilfe des +-Symbols unten im SIR-Incident-Feldzuordnungsabschnitt hinzufügen oder entfernen. Verfolgen Sie übersehene oder zuvor zugeordnete Felder mit der bereitgestellten Farbcodierung (zugeordnete Felder sind ausgegraut, blaue Felder sind nicht zugeordnet).
- Bedingungen für die Incident-Generierung: Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen definieren, um zu filtern, welche Korrelationsereignisse Security Incidents erstellen sollen, vs. Korrelationsereignisse, die herausgefiltert werden sollen, z. B. Korrelationsereignisse mit niedriger Priorität. Dies geschieht im Abschnitt „Incident-Generierungsbedingungen“ unter dem Abschnitt „Stichprobenerfassung für Korrelation-Ereignis“.
- Ereigniszusammenfassungskriterien: Definieren Sie zusätzliche Ereigniszusammenfassungskriterien, die ein eingehendes Korrelationsereignis zu einem vorhandenen aggregieren SIR Security Incident anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Mithilfe von Feldübereinstimmungswertkriterien für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen sicherheitsrelevanten Ereignisdaten in einem einzelnen Security Incident platziert werden.
- Formatfeldübersetzung: In bestimmten Fällen Ereignisfeldwerte im ArcSight ESM Das Korrelationsereignis wird möglicherweise nicht direkt in die Felder auf übersetzt SIR Security Incident. Für diese Werte können Sie einen Skripteditor verwenden, um Feldwerte für den Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind.

  Beispielsweise kann ein Kategoriewert „Malware-Warnung“ und „Virusinfektion“ mit dem Skripteditor unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können in eine allgemeine schädliche Code-Aktivität im Feld Kategorie übersetzt werden SIR Security Incident mithilfe der Funktionalität „Formatierungsfeldübersetzung“.

Der nächste Schritt besteht darin, Beispielkorrelationsereignisse zu erfassen und Werte dem zuzuordnen SIR Security Incident-Felder.

Erstellen Sie Zuordnungen für ArcSight ESM Integration der Ereigniserfassung

In diesem Schritt erfassen Sie Beispielkorrelationsereignisse und ordnen den SIR Security Incident-Feldern Werte zu.

Vorbereitungen

Erforderliche Rolle: admin, sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Als Anwender mit der Rolle „sn_si.admin“ können Sie bis zu fünf Beispielkorrelationsereignisse aus der Spalte „Stichprobenerfassung für Korrelationsereignis“ auf der linken Seite des Formulars überprüfen, um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Zuordnung und Übersetzung von Ereignisfeldwerten zu den Security Incident-Feldern in der Spalte „SIR-Incident-Feldzuordnung“ auf der rechten Seite zu unterstützen.
Erstellen Sie anwenderdefinierte Zuordnungen, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Standardmäßig angezeigte Felder sind normalerweise wichtige Felder, die im Antwortformular für Security Incidents ausgefüllt werden müssen. Diese Felder können jedoch entfernt werden, und zusätzliche Felder können mit den Schaltflächen + und - angezeigt werden. Erstellen Sie anwenderdefinierte Karten, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie zuordnen ArcSight ESM Felder, die nicht im Standardzuordnungsraster für den Security Incident angezeigt werden.

Prozedur

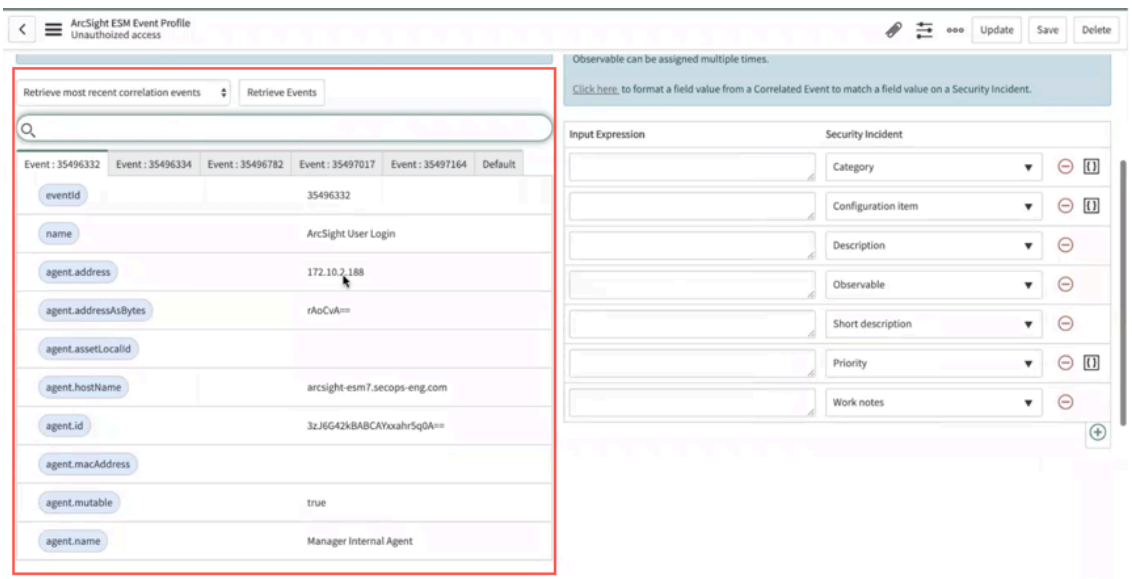
1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie auf **Zuordnung** Auf der Fortschrittsleiste.
2. Sie können entweder die neuesten Beispielkorrelationsereignisse für die ausgewählte Korrelationsregel abrufen oder die eindeutigen Korrelationsereignis-IDs für die spezifischen Korrelationsereignisse angeben, die Sie für Ihre Experience der Korrelationsereigniszuordnung verwenden möchten.
3. Wählen Sie in der Dropdown-Liste eine der folgenden Optionen aus:
   - Neueste Korrelationsereignisse abrufen
   - Korrelationsereignisse basierend auf Ereignis-ID auswählen

   Klicken Sie Auf **Ereignisse Abrufen** Um die neuesten Beispielkorrelationsereignisse aus abzurufen ArcSight ESM Konsole für die ausgewählte Korrelationssuchregel.

   Die Ergebnisse der Korrelationsereignisfelder und -Werte werden als einzelne Registerkarten angezeigt.

   Der Abruf für Beispielkorrelationsereignisse kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt.

   In der folgenden Abbildung werden die Feld-Name-Wert-Paare für das erfasste Korrelationsereignis oder die importierten Beispielereignisse auf der linken Seite dieses Formulars angezeigt, nachdem der Abruf der Erfassung abgeschlossen ist. Diese Werte sind die Werte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.

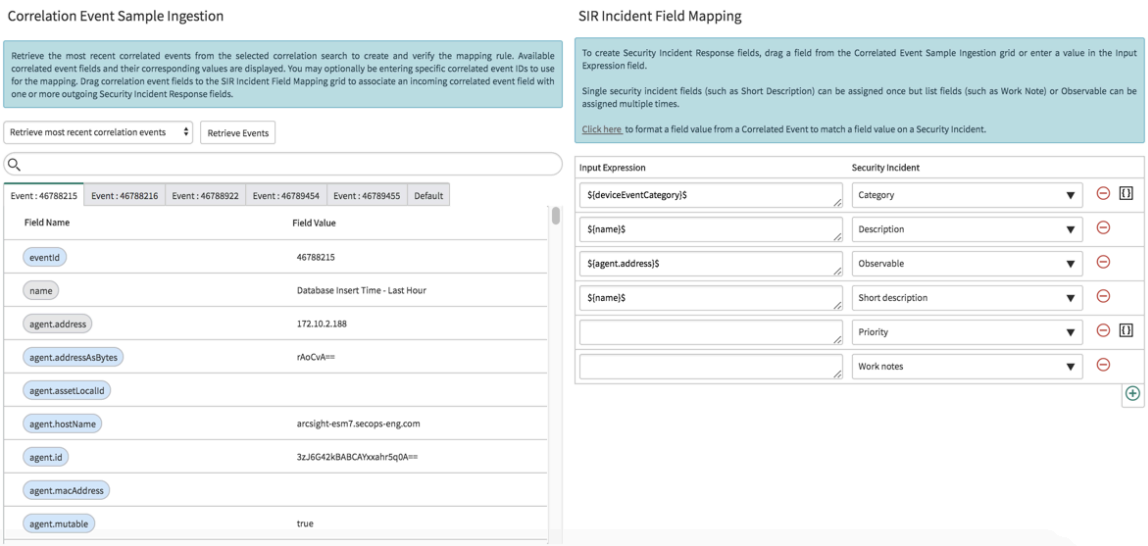


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf der linken Seite des Formulars auf einen blauen Feldnamen.
5. Ziehen Sie den Feldnamen, z. B. Agent.Hostname , Und legen Sie es in einem Feld in der Spalte „Eingabeausdruck“ neben einem Feldnamen in der Spalte „Security Incident“ ab.

   Damit Sie sicherstellen können, dass im Zuordnungsprozess keine Ereignisfelder übersehen oder dupliziert werden, sind Felder farbcodiert. Hellblaue Felder auf der linken Seite zeigen an, dass ein Korrelationsereignisfeld noch nicht ausgewählt und dem Security Incident zugeordnet ist. Möglicherweise möchten Sie ein eingehendes Korrelationsfeld mit mehr als einem Feld in einem Security Incident verknüpfen.

   Ein graues Feld gibt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Mit dieser Farbcodierung können Sie nachverfolgen, welche Ereignisfelder bereits für zukünftige Security Incident-Feldzuordnungen verwendet wurden.



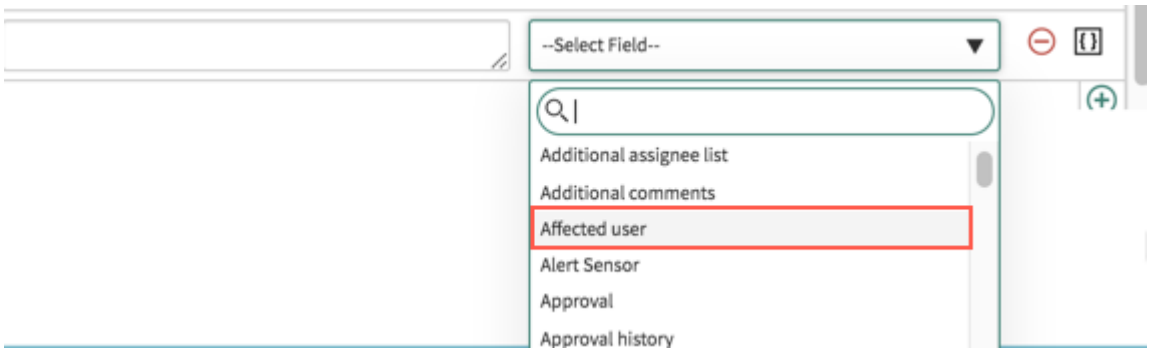
6. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen.

   a. Klicken Sie auf der rechten Seite des Formulars im Abschnitt „SIR-Incident-Feldzuordnung“ unten im Raster auf das Plus-Symbol.
   Ein neues Feld wird angezeigt.

   b. Erweitern Sie in der Spalte Security Incident die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

      In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung: Betroffener Anwender Hat einen grauen Hintergrund, da er im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Korrelationsereignisfelder auf der linken Seite des Formulars hilft diese Farbcodierung für die Security Incident-Felder auf der rechten Seite Ihnen, die bereits zugeordneten SIR-Incident-Felder nachzuverfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Damit mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können Erkennbares Element Das Feld kann mehrmals verschiedenen Werten zugeordnet werden. Ebenso wird Konfigurationselement Und Arbeitsnotizen Felder unterstützen mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

c. Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.

d. Klicken Sie auf der linken Seite des Formulars mit der linken Maustaste, um auszuwählen **Ereignis-ID** Die Sie in wünschen **Eingabeausdruck** Feld.
Ordnen Sie sie mit der Drag-and-Drop-Funktion neben Ihrem neuen Feld zu.

7. Wahlweise: Öffnen Sie den Skripteditor, und fahren Sie mit der Bearbeitung fort.

(Optional) Weitere Informationen zum Skript-Editor finden Sie unter Verwenden Sie den Skript-Editor, um Korrelationsereigniswerte zu formatieren.**Filterbedingungen für die Incident-Generierung**

8. Wahlweise: Nachdem Sie die vorherigen Feldzuordnungsschritte abgeschlossen haben, können Sie dieselben Feldwerte im Generator für Incident-Generierungsbedingungen verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes Korrelationsereignis erfüllen muss, um einen zu erstellen SIR Security Incident.
Um Bedingungen für die Incident-Generierung festzulegen, gehen Sie wie folgt vor.

a. Scrollen Sie im Formular zum Abschnitt Bedingungen für die Incident-Generierung, und wählen Sie aus **Filtern Sie basierend auf Bedingungen** Kontrollkästchen zum Aktivieren der Option.

(Optional) Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den spezifischen Bedingungen entsprechen, die in den Feldern beschrieben werden.

Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen entsprechen den Feldern, die im Abschnitt „Beispielerfassung für Korrelationsereignis“ für die von Ihnen erfassten Ereignisse angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach Korrelationsereignissen, die Sie erfassen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden und müssen genau mit den Werten von übereinstimmen ArcSight ESM Korrelationsereignis.

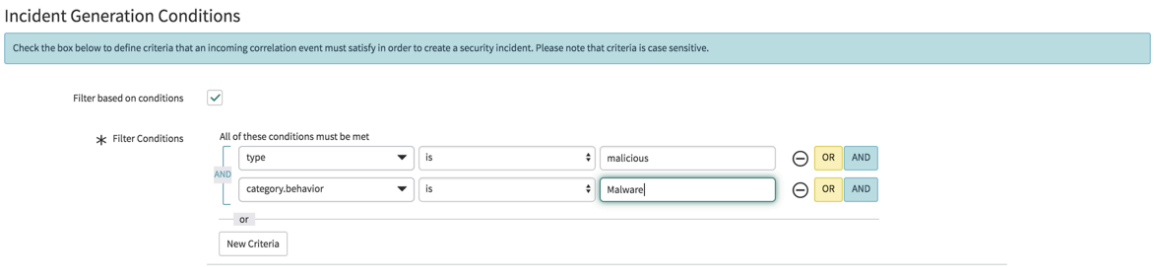
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.

b. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** Oder **ODER** . Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden.

c. Wahlweise: Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

(Optional) Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt werden müssen, bevor Security Incidents erstellt werden.



(Optional) Sie haben die Bedingungen für die Incident-Generierung so festgelegt, dass Security Incidents nur erstellt werden, wenn beide von Ihnen eingegebenen Filterbedingungen erfüllt sind.

Diese Art der Bedingungsfilterung für die Incident-Generierung hilft Ihnen, die Sicherheitsereignisse einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegende Korrelationssuche zu ändern oder Ereignisse in herauszufiltern ArcSight ESM. Wenn zusätzliche Filterkriterien festgelegt sind, werden Incidents nur Korrelationsereignisse zugeordnet, die allen Kriterien entsprechen.

Hinweis:
Wenn einer der Ereignisfeldnamen Sonderzeichen wie Anführungszeichen (“), Bindestriche (‘), Unterstriche (-) oder ampersands (@) enthält, müssen diese Zeichen möglicherweise zu Übersetzungszwecken ersetzt werden und möglicherweise einen doppelten Ereignisnamen erstellen. Die Zuordnung kann entsprechend erfolgen, es wird jedoch ein numerisches Suffix angehängt, um Felder mit doppelten Ereignisnamen zu unterscheiden. Beispiel: Wenn das erste Ereignisfeld lautet `Ereignisse.Ereignis` Und das zweite Ereignisfeld ist `Ereignisse.Ereignis` , Diese Felder können nicht eindeutig identifiziert werden, da die verbleibenden Standardtextzeichen identisch sind. In diesem Fall wird dem zweiten Ereignisfeld ein Suffix hinzugefügt, und das Feld wird in umbenannt `Ereignisse@Ereignis(1)` .

Kriterien für Ereigniszusammenfassung zur Behandlung ähnlicher Korrelationsereignisse und zur Verhinderung doppelter Incidents

9. Wahlweise: Um die Erstellung doppelter Security Incidents zu vermeiden, definieren Sie zusätzliche Ereigniszusammenfassungskriterien, damit eingehende Korrelationsereignisse zu einem offenen Security Incident zusammengefasst werden.
Um die Kriterien festzulegen, führen Sie die folgenden Schritte aus:

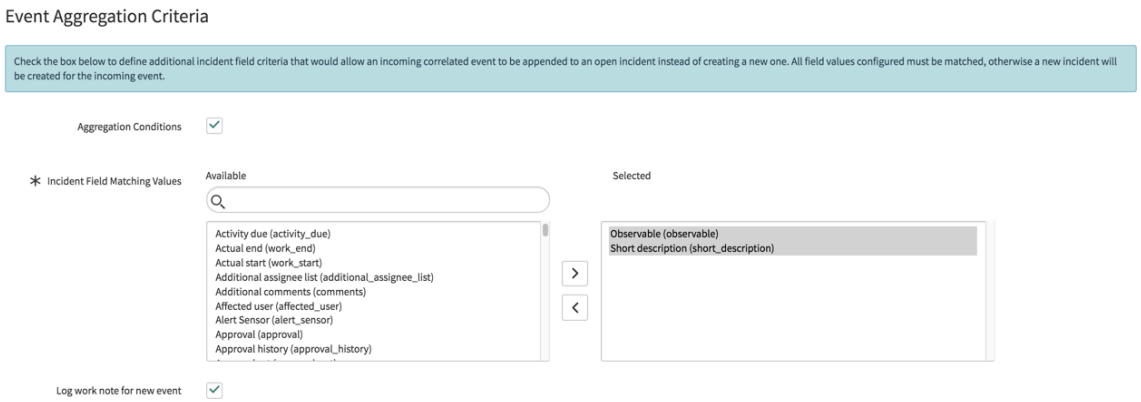
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Scrollen Sie zu **Kriterien Für Ereigniszusammenfassung** Abschnitt im Formular, und aktivieren Sie das Kontrollkästchen Zusammenfassungsbedingungen, um diese Option zu aktivieren.

(Optional) Die Spalten „Incident-Feld-Übereinstimmungswerte“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die in konfiguriert sind SIR Security Incident.

b. Wählen Sie in der Liste verfügbar die Feldwerte aus, die Sie für vorhandene Security Incidents in abgleichen möchten ServiceNow AI Platform Und verschieben Sie sie in die Liste ausgewählt.

(Optional) Alle von Ihnen ausgewählten Feldwerte müssen abgeglichen werden, um dieses eingehende Korrelationsereignis an einen vorhandenen Security Incident anzuhängen. Dies umfasst Felder, z. B. erkennbare Elemente und Konfigurationselemente, denen möglicherweise mehrere Korrelationsereignisfeldwerte zugeordnet sind. Alle Werte müssen übereinstimmen. Wenn nur eine Teilmenge der Werte übereinstimmt, werden die Bedingungen für die Ereigniszusammenfassung nicht erfüllt, und ein neuer Security Incident wird erstellt. Siehe Screenshot unten für die Feldzuordnung mit mehreren Werten.

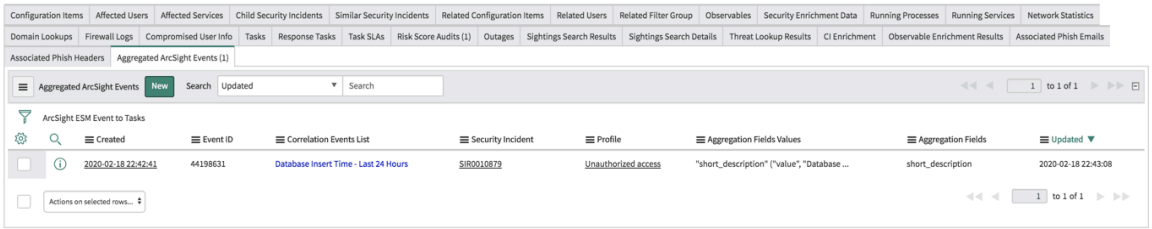


Wenn ein neues Korrelationsereignis allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird das neue Korrelationsereignis automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als SOC-Analyst, der mit Security Incidents arbeitet, können Sie alle hinzugefügten aggregierten Korrelationsereignisse in einer zugehörigen Liste zu einem Security Incident anzeigen. Alle zusammengefassten Korrelationsereignisse für einen Security Incident werden im angezeigt **Zusammengefasste ArcSight-Ereignisse** Zugehörige Liste. Diese Liste enthält Details zu zugehörigen Zeitstempeln und zusammengefassten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum diese Korrelationsereignisse zu vorhandenen Security Incidents aggregiert werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie unter zur linken Seite des Datensatzes **Zugehörige Links** Und klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Link.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn diese zugehörige Liste nicht angezeigt wird, führen Sie die folgenden Schritte aus:

- Klicken Sie mit der rechten Maustaste auf den Header des Security Incident-Formulars, und klicken Sie auf **Konfigurieren** > **Zugehörige Listen**an.
- Wählen Sie Aus **Zusammengefasste ArcSight-Ereignisse** Verschieben Sie sie in der Liste verfügbar in die Liste ausgewählt, und klicken Sie auf **Speichern** .
- Klicken Sie Auf **Zugehörige Listen Anzeigen** . Sie sehen jetzt **Zusammengefasste ArcSight-Ereignisse** Registerkarte im Abschnitt zugehörige Liste.



c. Wahlweise: Um eine Arbeitsnotiz für jedes Mal zu protokollieren, wenn ein Ereignis für den Security Incident aggregiert wird, aktivieren Sie das Kontrollkästchen, um diese Option zu aktivieren.
In der Arbeitsnotiz wird protokolliert, dass ein neues korreliertes Ereignis zusammen mit einem Link zu den korrelierten Ereignisdetails hinzugefügt wurde.

Sie haben Werte aus einem Korrelationsereignis erfolgreich zu Feldern in einem zugeordnet SIR Security Incident. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung einzuschränken. Sie haben auch Korrelationsereignisse zu vorhandenen aggregiert SIR Security Incidents, wenn die Ereignisfeldwerte den konfigurierten Zusammenfassungskriterien entsprechen.

10. Wählen Sie eine Option aus, um mit der Profilkonfiguration fortzufahren.

Vorschau des Security Incidents für anzeigen ArcSight ESM Integration der Ereigniserfassung

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem zugeordnet haben ServiceNow AI Platform Security Incident Response(SIR) Security Incident. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Korrelationsfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin.

Warum und wann dieser Vorgang ausgeführt wird
Als Anwender mit der Rolle „sn_si.admin“ können Sie eine Vorschau eines Security Incidents anzeigen und die Zuordnung nach Bedarf erneut bearbeiten, um Felder mit Fehlern zu beheben oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wurde, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen von Security Incidents werden nicht als tatsächliche Incidents in gespeichert Security Incident Response Produkt.

Prozedur

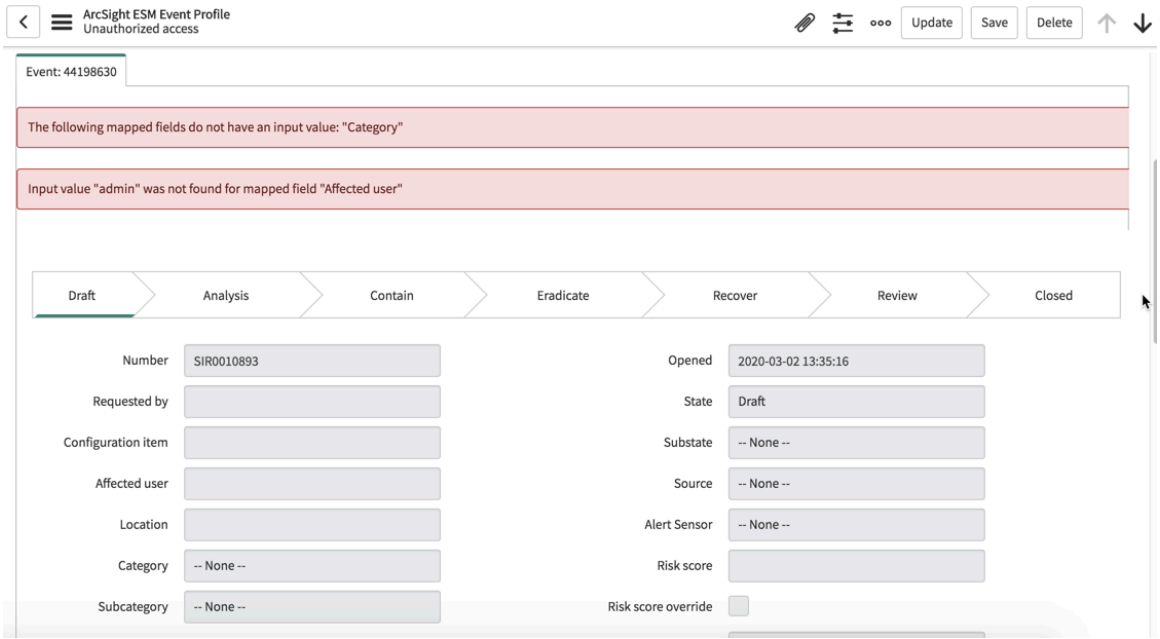
1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie auf **Vorschau** In der Fortschrittsleiste.

2. Wählen Sie in der Auswahlliste Beispiel-Ereignis-IDs ein Element aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Security Incident wird angezeigt. Ändern Sie keine Informationen in den Feldern. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.

3. Überprüfen Sie die Feldzuordnung der Korrelationsereigniswerte für den Security Incident.



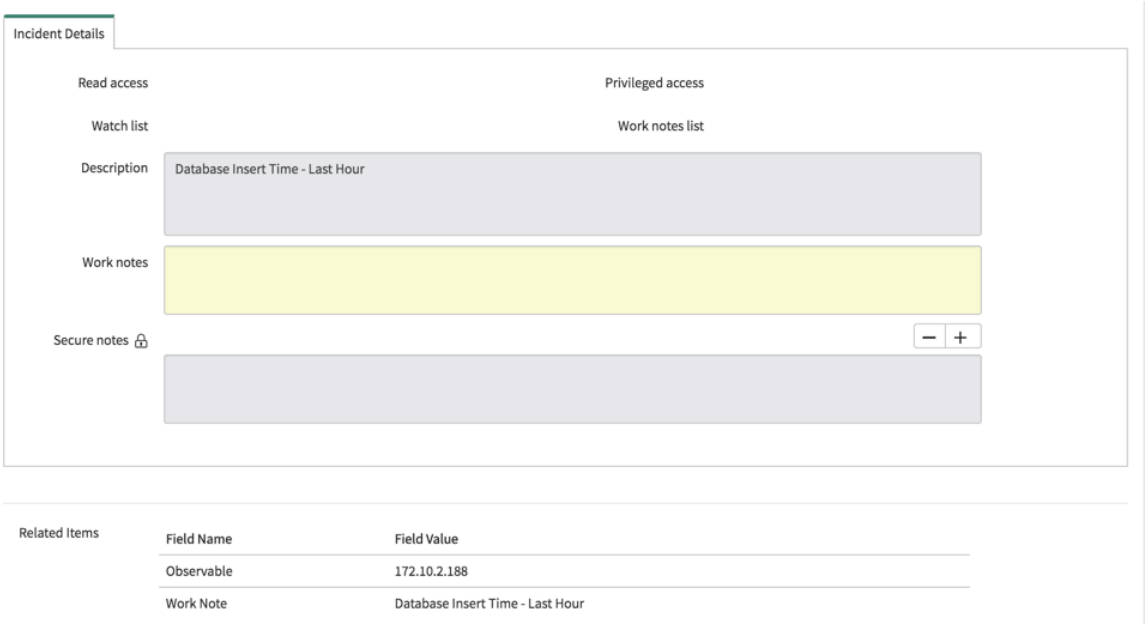
Das vorangegangene Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler. In diesem Beispiel hat ein Feldwert aus dem Korrelationsereignis keinen akzeptablen Wert für das Referenzfeld im SIR-Incident-Formular. Eine Fehlermeldung wird angezeigt, die angibt, dass für keinen Eingabewert gefunden wurde Kategorie Feld, das ein Referenzfeld mit einem bestimmten Satz von Werten ist. Daher wird dieser zugeordnete Feldwert nicht in angezeigt SIR Security Incident-Formular ohne weitere Änderung.

4. Klicken Sie auf, um diesen Fehler zu beheben **Zuordnung** In der Fortschrittsleiste.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie erneut eine Vorschau der Zuordnung an, und beheben Sie alle Fehler, die in Fehlermeldungen beschrieben werden.

Die folgende Abbildung ist ein Beispiel für die Registerkarte Incident-Details in der unteren Hälfte eines Security Incident, nachdem alle Fehlermeldungen gelöst wurden. In diesem Beispiel wurden die Felder Beschreibung und Arbeitsnotizen zugeordnet, und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

diese Felder werden mit den Werten aus den Wertepaaren ausgefüllt, die aus abgerufen wurden ArcSight ESM Beispiele für Korrelationsereignisse.



Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind, besteht der nächste Schritt darin, den Zeitplan zu definieren.

Erstellen Sie einen Zeitplan für ArcSight ESM Ereigniserfassung

Sie können den Abruf- oder Abrufzeitplan für neue korrelierte Ereignisse definieren. Während dieses Schritts können Sie die vorhandenen Einstellungen für den Abruf von Korrelationsereignissen überprüfen oder die Planung nach Bedarf ändern. Mit diesem Schritt können Sie auch historische Korrelationsereignisse mithilfe eines Datumsbereichs abrufen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin.

Warum und wann dieser Vorgang ausgeführt wird

Sie können auswählen, ob Sie während des Planungsschritts historische Korrelationsereignisse erfassen möchten. Sie wählen auch aus, wie oft Sie nach zukünftigen neuen Korrelationsereignissen abfragen, die der Profilkonfiguration entsprechen.

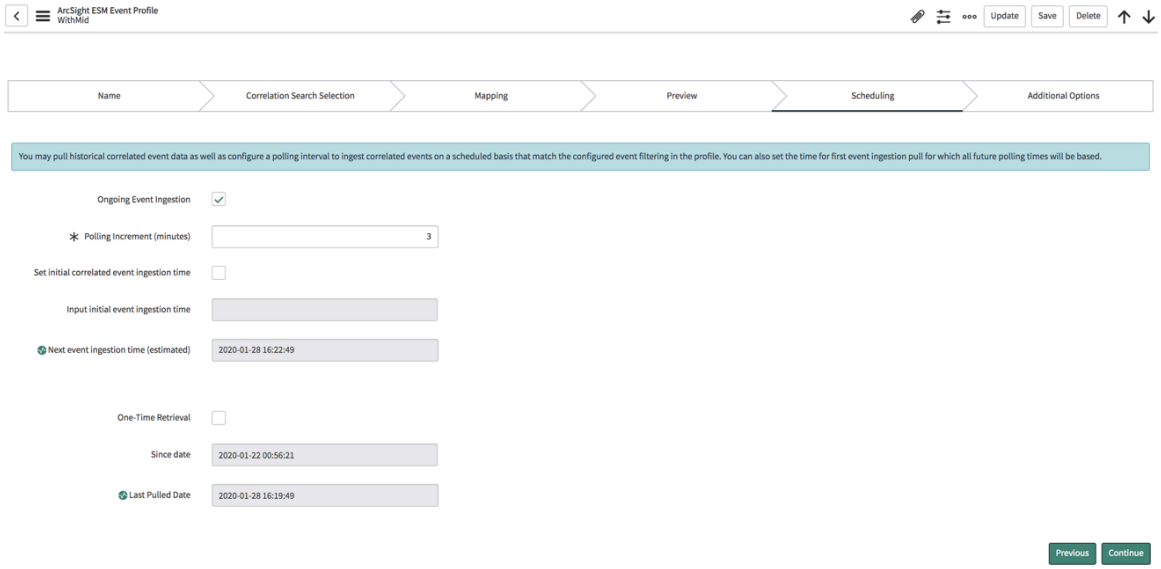
Als Benutzer mit der Rolle sn_si.admin konfigurieren Sie diese Abfrageintervalle pro Profil. Die Leistung von ArcSight ESM Die Integration der Korrelationsereigniserfassung kann von den verschiedenen Abfrageintervallen beeinflusst werden. Bei der Planung möchten Sie möglicherweise die Reduzierung des Abfrageaufwands auf dem abgleichen ArcSight ESM Server gegen den Wunsch, so bald wie möglich benachrichtigt zu werden, wenn ein Ereignis erstellt oder aktualisiert wird. Für jedes Profil ist ein fünf-Minuten-Standardwert festgelegt. Sie können diese Einstellung jedoch bei Bedarf auf eine Minute ändern.

Neue und aktualisierte Korrelationsereignisse werden abgerufen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn die Seite „Zeitplanung“ im Fortschrittsbalken nicht angezeigt wird, wählen Sie aus **Zeitplanung** .
2. Wählen Sie eines aus, um zu planen, wie und wann Korrelationsereignisse aus der <ArcSight>-Konsole abgerufen werden.



Beispiel für die Planung einer ersten Erfassungszeit für Korrelationsereignisse, wenn Sie täglich eine haben ArcSight ESM Sicherheitsprüfung, die einmal täglich um 4 Uhr Ortszeit ausgeführt wird. Sie können das entsprechende Korrelationsereignisprofil in einrichten ServiceNow AI Platform Instanz, die um 4:05 UHR Ortszeit ausgeführt werden soll, um das Security Failure-Ereignis sofort zu erfassen und einen Security Incident zu erstellen. Geben Sie Ein `04 05 00` Im Feld erste Ereigniserfassung. Geben Sie im Feld Schritt (Minuten) den Wert ein `1440` (24 Stunden) zum Planen der nächsten Ereigniserfassung für 24 Stunden ab der ersten Ereigniserfassung. Sowohl die erste Ereigniserfassungszeit als auch die nächste Ereigniserfassungszeit werden in den Feldern angezeigt.

3. Um die Einstellungen für dieses Beispiel zu konfigurieren, führen Sie die folgenden Schritte aus.

   a. Wenn die Seite „Zeitplanung“ angezeigt wird, wählen Sie aus **Laufende Ereigniserfassung** Kontrollkästchen zum Aktivieren dieser Option.

   b. Geben Sie im Feld Schritt (Minuten) den Wert ein `1440` (24 Stunden).

   c. Klicken Sie auf **Legen Sie die Zeit der ersten korrelierten Ereigniserfassung fest** Kontrollkästchen zum Aktivieren der Bearbeitung der Felder „erste Ereigniserfassung“ und „nächste Ereigniserfassung“.

   d. Geben Sie im Feld Zeit der ersten Ereigniserfassung ein `04 05 00` .
   Im Feld nächste Ereigniserfassungszeit (geschätzt) wird die Zeit der nächsten Ereigniserfassung angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie Auf **Fahren Sie Fort** Um zur Seite „zusätzliche Optionen“ zu navigieren.

> **Hinweis:**
> Die Standardanzahl von Security Incidents, die an einem Tag erstellt und zusammengefasst werden können, sowie der Flow-Zeitraum sind in definiert ArcSight ESM Integrationseinstellungen. Sie können diese Einstellungen bei Bedarf ändern. Details siehe ArcSight ESM Integrationseinstellungen für die Integration der Ereigniserfassung.

Zusätzliche Optionen: Korrelierte Ereignisaktualisierungen und -Abschlüsse basierend auf automatisieren SIR Incident-Status

Die ArcSight ESM Die Integration verfügt über eine bidirektionale Schnittstelle, die es ermöglicht, sowohl Korrelationsereignisse Security Incidents zu erstellen, als auch die Möglichkeit, die Korrelationsereignisse zu aktualisieren, sobald der Security Incident erstellt und/oder geschlossen wurde, mit relevanten Incident-Details wie Security Incident-Nummer, Zuweisungsgruppe, SIR Incident-URL usw.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

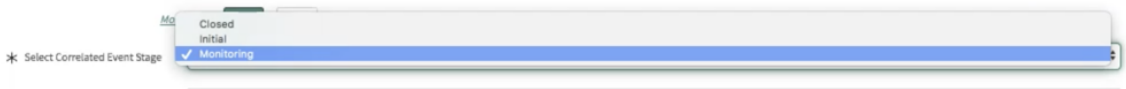
Prozedur

1. Wenn die Seite „zusätzliche Optionen“ im Fortschrittsbalken nicht angezeigt wird, wählen Sie aus **Zusätzliche Optionen** .
2. Befolgen Sie die folgenden Anweisungen, um die Konfiguration für die Aktualisierung korrelierter Ereignisse abzuschließen, wenn der Security Incident erstellt wird.

   Korrelierte Ereignisphase nicht konfiguriert : Wenn Sie keine korrelierten Ereignisphasen in konfiguriert haben ServiceNow AI Platform-Instanz wird nur angezeigt **Phase Zuweisen: Ersteinrichtung** In der Auswahlliste „Aktualisierung korrelierter Ereignisphasen“. Führen Sie die folgenden Schritte aus, um die Phase zu konfigurieren:

   - Geben Sie eine Ressourcen-ID in das Feld Phasenressourcen-ID eingeben ein, und klicken Sie auf **Übermitteln** . Die Ressourcen-ID wird in validiert ArcSight ESM Konsole und der folgende Bildschirm werden angezeigt.

   - Klicken Sie Auf **Speichern** Zum Speichern der neuen Phase (**Überwachung**).
   - Klicken Sie auf die Dropdown-Liste Korrelierte Ereignisphase auswählen.

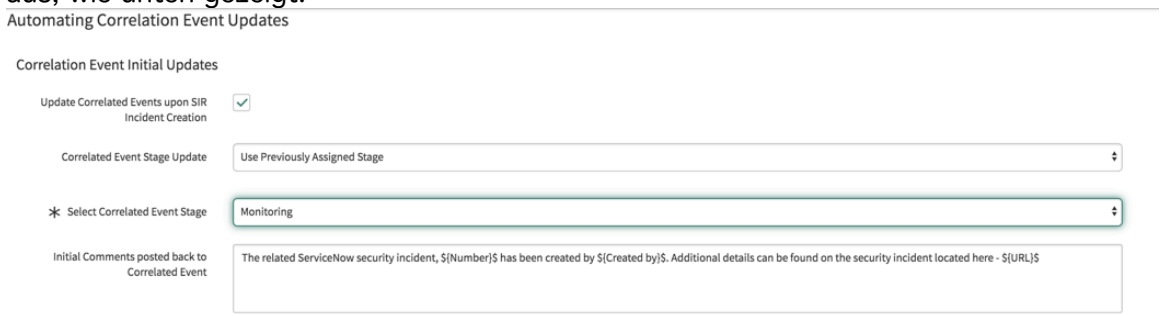


   - Sie können die neu erstellte Phase aus der Liste auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrelierte Ereignisphase ist bereits konfiguriert : Wenn Sie die korrelierte Ereignisphase bereits konfiguriert haben, führen Sie die folgenden Schritte aus:

- Wählen Sie Aus **Zuvor Zugewiesene Phase Verwenden** In der Auswahlliste „Aktualisierung korrelierter Ereignisphasen“.
- Wählen Sie eine vorhandene Phase aus der Auswahlliste korreliertes Ereignis auswählen aus, wie unten gezeigt.

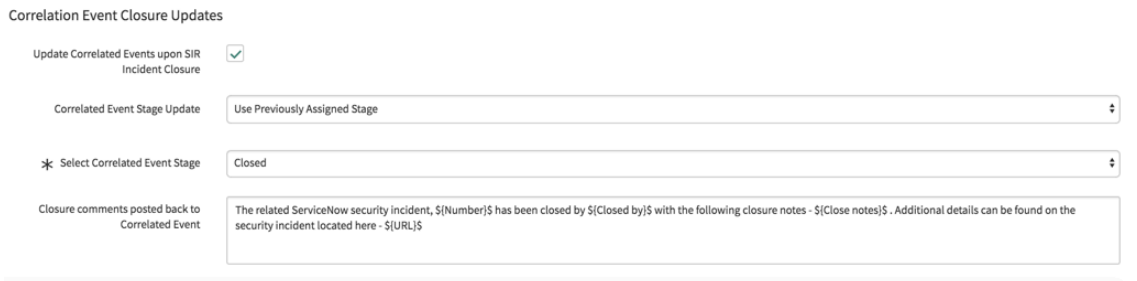


- Anfängliche Kommentare, die an korreliertes Ereignis zurückgesendet werden: Neben dem Aktualisieren des Phasenwerts des Korrelationsereignisses können Sie auch Kommentare zu den Anmerkungen der Korrelationsphase veröffentlichen. Wie in den Anweisungen angegeben, können Sie den Standardtext bearbeiten, der im Abschnitt „Kommentare“ angezeigt wird, einschließlich Hinzufügen oder Ändern der Ersetzungsvariablen im Format ${Feldname}$ für jedes Feld im Formular „Security Incident Response Incident“.

Hinweis:
Sie können entweder die in definierten Standardphasen verwenden ArcSight ESM Konsole oder erstellen Sie eigene anwenderdefinierte Phasen. Führen Sie die folgenden Schritte aus, um eine neue Phase zu erstellen:

- In ArcSight ESM Konsole, wählen Sie aus **Datei** > **Neu** > **Phase**an. Die Registerkarte „Inspect/Edit“ wird angezeigt.
- Definieren Sie die neue Phase, und wählen Sie nicht aus **Anwender Erforderlich** Kontrollkästchen. Stellen Sie sicher, dass die Phase korrekt definiert ist und sich an der richtigen Position im Ereignislebenszyklus befindet.

3. Im Abschnitt Automatisieren des Abschlusses korrelierter Ereignisse können Sie definieren, wie der Security Incident aktualisiert werden soll, wenn er geschlossen wird.
4. Füllen Sie im Formular die Felder aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

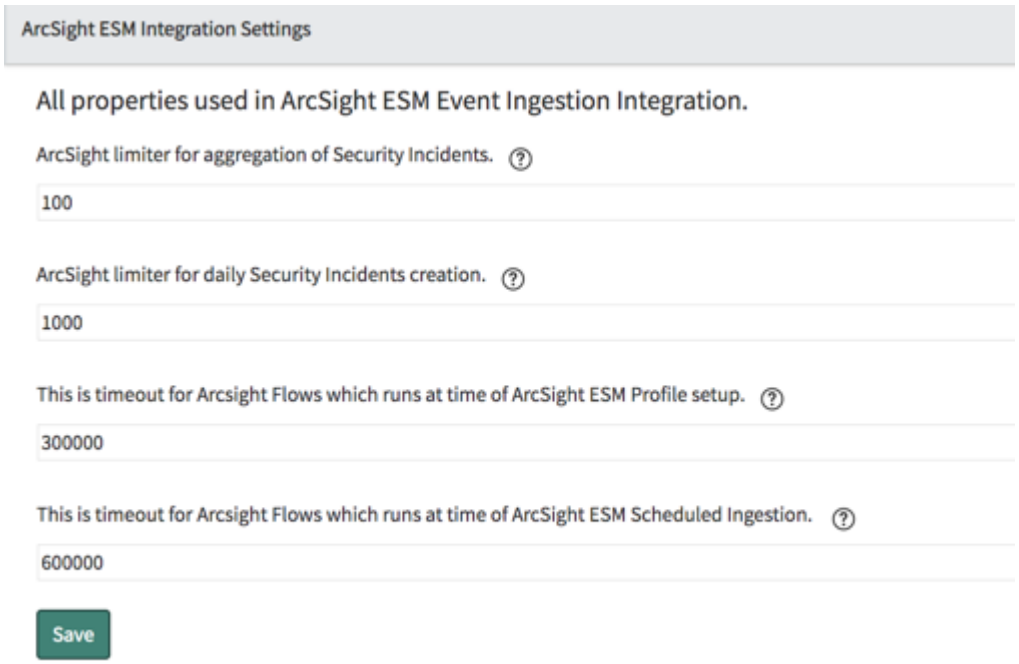
5. Klicken Sie Auf **Beenden** Um die Konfiguration abzuschließen.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um Korrelationsereignisse aus abzurufen ArcSight ESM Konsole basierend auf Ihrer Planung.

ArcSight ESM Integrationseinstellungen für die Integration der Ereigniserfassung

Verwenden Sie diese Option, um zu ändern ArcSight ESM Standarderfassungseinstellungen.

Um die Systemeigenschaften zu ändern, melden Sie sich als Anwender mit an *sn_si.admin* Rolle und navigieren Sie zu **ArcSight-ESM-Integration** > **Einstellungen für ArcSight-ESM-Integration**an.

Die Standardkonfigurationseinstellungen werden angezeigt. Sie können diese Einstellungen bei Bedarf ändern.



Problembehandlung ArcSight ESM Integration der Ereigniserfassung

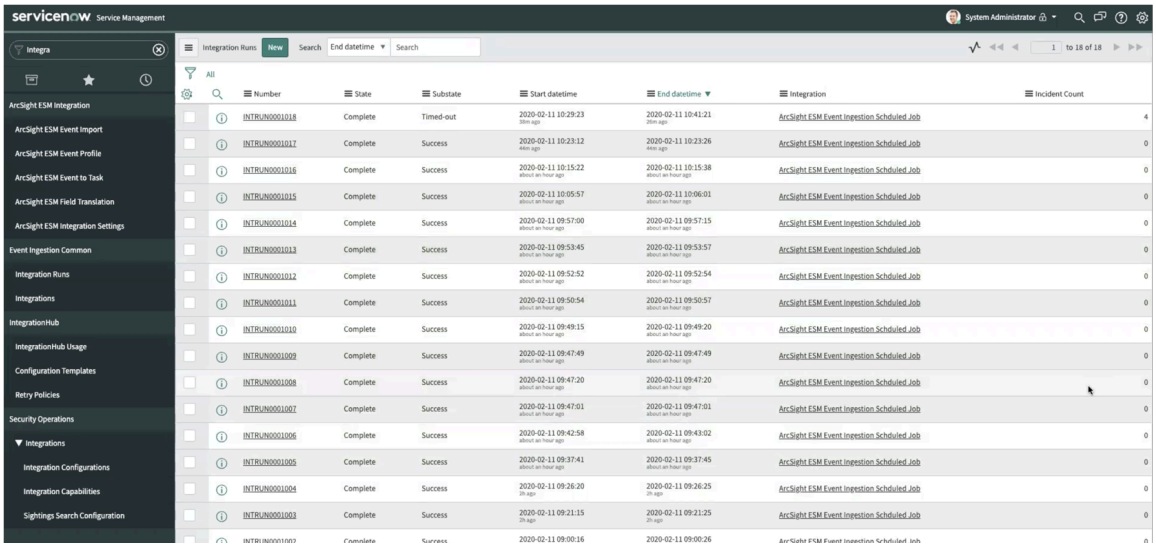
Dieser Abschnitt enthält Informationen zur Behebung von Fehlern, die während der Ereigniserfassung auftreten können.

Integrationsausführungen

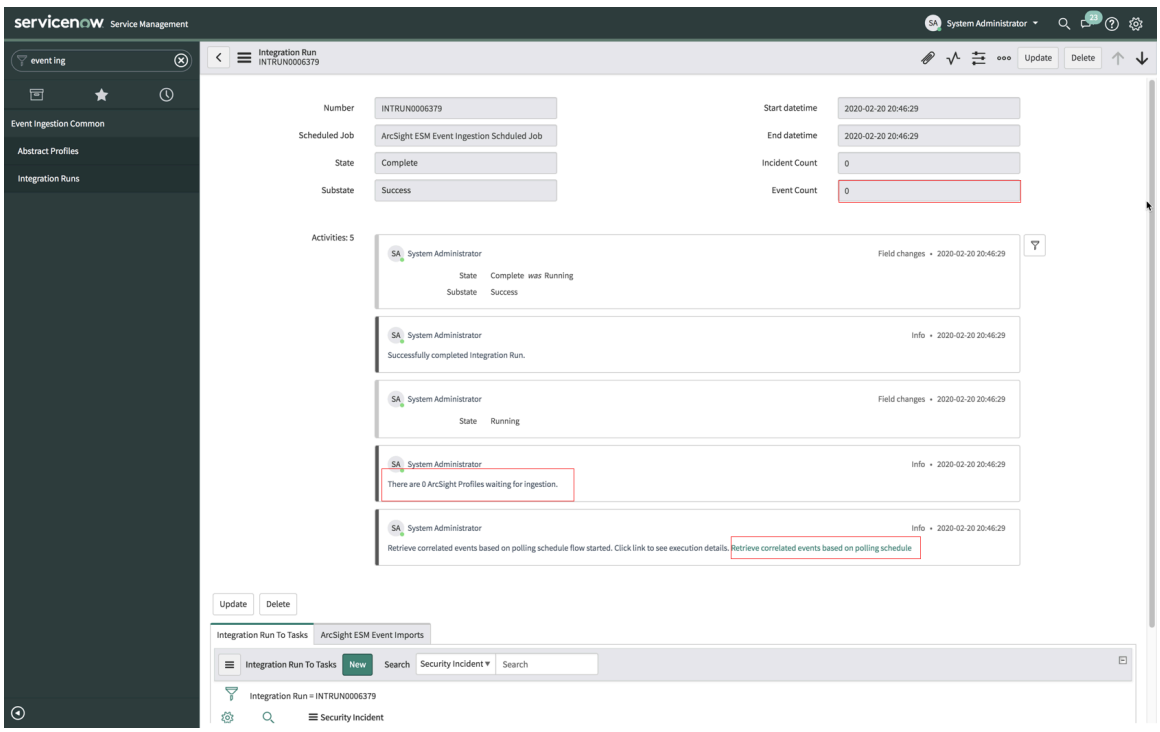
Navigieren zu **Ereigniserfassung Allgemein** > **Integrationsausführungen**an. Eine Integrationsausführung findet jede Minute statt und erfasst Details zu den während der geplanten Aufgabe erfassten Ereignissen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können die Liste der Integrationsausführungen und den Status jeder Ausführung (Erfolg, Zeitüberschreitung, Warten) und die Anzahl der erstellten Security Incidents anzeigen. Klicken Sie auf den Link Nummer, um einen Drilldown zur Seite „detaillierte Integrationsausführung“ durchzuführen.

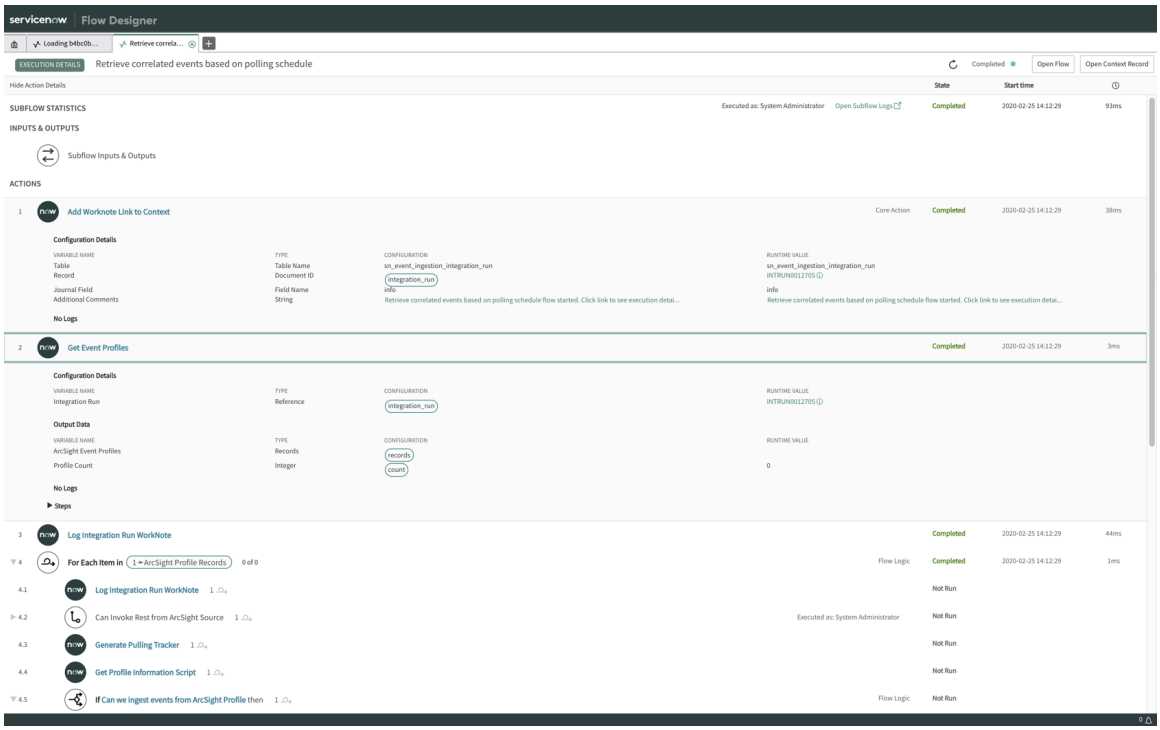


Sie können Details anzeigen, z. B. die Anzahl der Ereignisse, die erfasst wurden, den Status, das Ereignis, das in einen Security Incident umgewandelt wurde, und die verschiedenen Aufgaben, die während der Erfassung ausgeführt wurden. Darüber hinaus können Sie auf den Link klicken, um die Flow-Ausführungsdetails anzuzeigen.

Flow-Ausführungsdetails

Klicken Sie auf den Link Ausführungsdetails, um den Flow anzuzeigen, der der Ereigniserfassung zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können eine schrittweise Ausführung des Flows anzeigen, in der die verschiedenen Aktionen und Subflows beschrieben werden, die als Teil des Flows ausgeführt wurden.

Kopieren ArcSight ESM Profil für die Integration der Ereigniserfassung

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, sollten Sie Profile kopieren, um Zeit zu sparen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

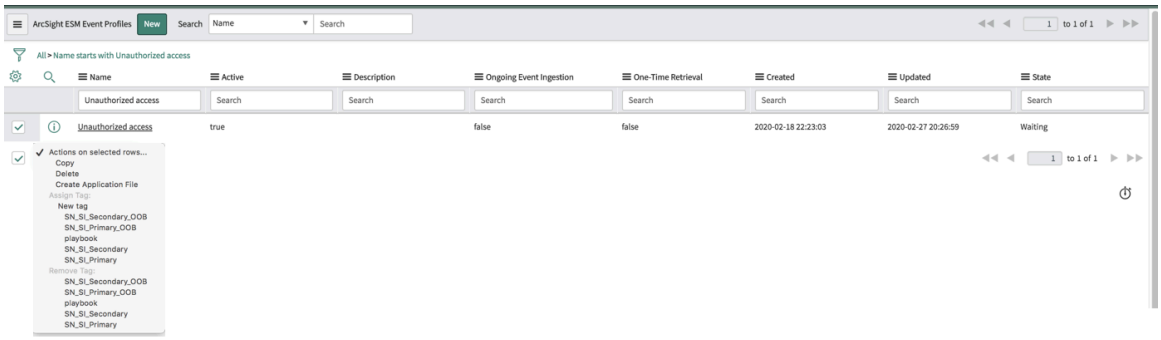
Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie als Anwender mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), sodass es vor Abschluss der Konfiguration nicht versehentlich aktiviert wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und verifiziert haben.

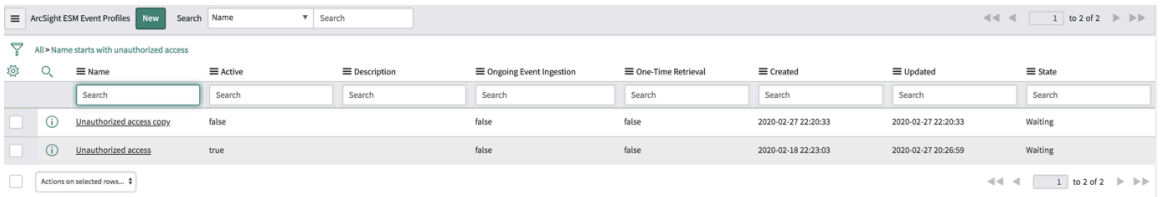
Prozedur

1. Navigieren zu **Alle** > **ArcSight-ESM-Integration** > **ArcSight ESM-Ereignisprofil**an.
2. Wählen Sie in der angezeigten Liste „ArcSight-Profile“ ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Profil wird kopiert und in der Liste angezeigt. Die Kopie verfügt über alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (Wahr), die Kopie ist zu diesem Zeitpunkt deaktiviert (Falsch). Möglicherweise möchten Sie Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf auf das neue Profil angewendet werden.



Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass **Aktiv** Der Spaltenstatus wird auf „falsch“ festgelegt, da das Profil aktiviert werden muss.

Verwenden Sie den Skript-Editor, um Korrelationsereigniswerte zu formatieren

Verwenden Sie zusätzlich zu den direkt zugeordneten Feldern aus den erfassten Korrelationsereigniswerten den Skript-Editor, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Der Skripteditor ändert die Werte von ArcSight ESM Korrelationsereignisfeld, sodass Werte, die von unterstützt werden ServiceNow AI Platform SIR Security Incidents werden den Feldern Kategorie, Konfigurationselement (CI), erkennbares Element und andere Security Incidents zugeordnet.

In bestimmten Fällen ArcSight ESM Korrelationsereigniswerte werden Referenzfeldern wie Kategorie, Konfigurationselement (CI) und erkennbaren Elementen im Security Incident zugeordnet. Als Anwender mit der Rolle „sn_si.admin“ können Sie die zugeordneten Ereignisfeldwerte bearbeiten, um das Format zu übersetzen, oder Datenwerte, die den erwarteten Incident-Feldformaten und -Werten entsprechen. Wenn Sie den Wert von übersetzen möchten ArcSight ESM Korrelationsereignis zu einem Wert, der von diesen Feldern im unterstützt wird SIR Security Incident verwenden Sie den Skript-Editor.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie bei angezeigtem Zuordnungsformular auf den Link, um den Skript-Editor zu öffnen.
2. Wählen Sie in der Auswahlliste ein Zielfeld für den Wert aus, den Sie bearbeiten möchten.
3. Alternativ können Sie im Abschnitt SIR-Incident-Feldzuordnung auf das Klammern-Symbol klicken [{}] Neben einem Feld, um den Skripteditor für dieses Feld zu öffnen.

   In bestimmten Fällen kann eine Skripteinbindung für das Feld Konfigurationselement geeignet sein. Für ein Korrelationsereignis kann beispielsweise kein Wert für das Konfigurationselement übereinstimmen.

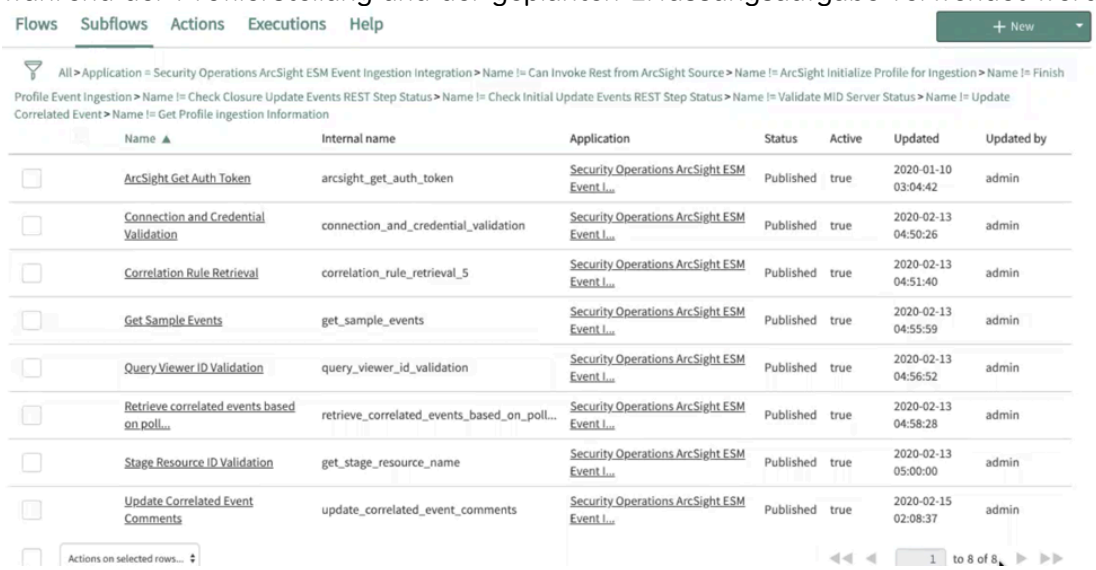
   Wie in der folgenden Abbildung gezeigt, kann eine Übereinstimmung für einen Hostnamen nicht in gefunden werden ServiceNow AI Platform CMDB für das Feld Konfigurationselement können Sie die Regel so bearbeiten, dass, wenn eine IP-Adresse gefunden wird, das Feld Konfigurationselement ausgefüllt wird.

   Der Editor wird geöffnet, wobei das Feld im Zielfeld angezeigt wird.
4. Geben Sie alle Änderungen am Skript ein, und klicken Sie auf **Aktualisieren** Um Ihre Änderungen zu speichern.
   Die ArcSight ESM Die Tabelle „Feldübersetzungen“ wird angezeigt.
5. Schließen Sie die Tabelle, um zum Zuordnungsformular zurückzukehren.

Flow Designer-Nutzung mit ArcSight ESM Integration der Ereigniserfassung

Mit Integration Hub und Flow Designer sind mehrere Flows, Subflows und Aktionen mit verfügbar ArcSight ESM Integration.

Um diese Subflows anzuzeigen, navigieren Sie zu **Flow Designer** > **Designer** Und klicken Sie auf **Subflows** Registerkarte. Die folgende Abbildung zeigt die wichtigen Subflows, die während der Profilerstellung und der geplanten Erfassungsaufgabe verwendet werden.



Diese Subflows werden in der Reihenfolge aufgeführt, in der sie unten ausgeführt werden:

- **Validierung von Verbindungen und Anmeldeinformationen** : Dieser Subflow validiert ServiceNow Konnektivität mit ArcSight ESM Server und die angegebenen Anmeldeinformationen. Dieser Subflow wird verwendet, wenn Sie auf klicken **Konfigurieren** Schaltfläche in **ArcSight ESM: Ereigniserfassung** Kachel in **Security Operations** > **Integrationen** > **Integrationskonfiguration** Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **ArcSight – Authentifizierungstoken abrufen** : Dieser Subflow generiert ArcSight ESM Authentifizierungstoken aus Anwendername und Passwort mit ArcSight ESM Anmeldeservice. Der Anmeldeservice stellt das Authentifizierungstoken bereit, mit dem andere aufgerufen werden können ArcSight ESM Endpunkt. Dieser Subflow wird in allen anderen Subflows verwendet.
- **Validierung der Abfrage-Viewer-ID** : Dieser Subflow überprüft, ob die bei der Profilerstellung angegebene Abfrage-Viewer-ID in vorhanden ist ArcSight ESM Server.
- **Korrelationsregelabruf** : Dieser Subflow ruft die Korrelationsregeln basierend auf der Abfrage-Viewer-ID ab.
- **Beispielereignis Abrufen** : Dieser Subflow ruft die Beispielkorrelationsereignisse aus dem ab ArcSight ESM Server. Diese Beispielereignisse werden dann den Security Incident-Feldern im Abschnitt „Zuordnung“ des Profils zugeordnet.
- **Validierung der Phasenressourcen-ID** : Dieser Subflow validiert die angegebene Phasenressourcen-ID in ArcSight ESM Konsole und ruft den Ressourcennamen ab.
- **Aktualisieren Sie Korrelierte Ereigniskommentare** : Dieser Subflow aktualisiert die korrelierten Ereigniskommentare in den Abschnitten „Initial“ und „Abschluss von Incidents“ auf der Seite „zusätzliche Optionen“ des Profils.
- **Ruft korrelierte Ereignisse basierend auf dem Abrufzeitplan ab** : Dieser Subflow führt die geplante Aufgabe aus, die die korrelierten Ereignisse basierend auf dem Abfrageintervall abruft.

Während der Ausführung lösen die obigen Subflows auch mehrere andere Subflows und Aktionen aus, entweder direkt oder indirekt, wie unten gezeigt.

Flows | Subflows | Actions | Executions | Help — + New

Can Invoke Rest from ArcSight Source	can_invoke_rest_from_arcsight_source	Security Operations ArcSight ESM Event I...	Published	true	2020-01-07 00:46:32	admin
Check Closure Update Events REST Step St...	check_closure_update_events_rest_step_st...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:08	admin
Check Initial Update Events REST Step St...	check_rest_step_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:48:55	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:50:26	admin
Correlation Rule Retrieval	correlation_rule_retrieval_5	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:51:40	admin
Finish Profile Event Ingestion	end_process_run	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:53:48	admin
Get Profile Ingestion Information	get_last_run_date	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:54:31	admin
Get Sample Events	get_sample_events	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:55:59	admin
Query Viewer ID Validation	query_viewer_id_validation	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:56:52	admin
Retrieve correlated events based on poll...	retrieve_correlated_events_based_on_poll...	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 04:58:28	admin
Stage Resource ID Validation	get_stage_resource_name	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:00:00	admin
Update Correlated Event	update_correlated_event	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 23:12:18	admin
Update Correlated Event Comments	update_correlated_event_comments	Security Operations ArcSight ESM Event I...	Published	true	2020-02-15 02:08:37	admin
Validate MID Server Status	validate_mid_server_status	Security Operations ArcSight ESM Event I...	Published	true	2020-02-13 05:03:40	admin

Amazon Web Services(AWS) Security Hub Integration

AWS Security Hub Ist ein Cloud Security Posture Management (CSPM)-Service, der automatisierte und kontinuierliche Sicherheitsprüfungen und Best Practice-Prüfungen für Ihre AWS-Ressourcen bereitstellt.

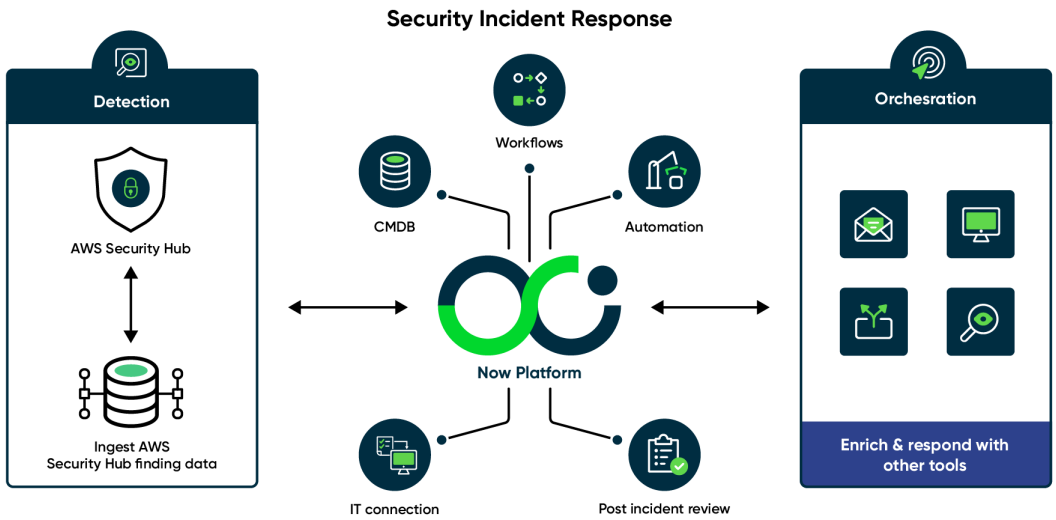
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über AWS Security Hub Integration

AWS Security Hub Ermöglicht Ihnen die Identifizierung von Problemen in Ihren Konfigurationen. Security Hub fasst Ihre Sicherheitswarnungen zusammen, die als Ergebnisse bezeichnet werden. AWS Security Hub Generiert diese Ergebnisse in einem standardisierten Format und priorisiert sie, damit Sie sie einfacher anreichern, untersuchen und korrigieren können. Sie können verwenden AWS Security Hub Integration zum Erfassen von Security Hub-Ergebnissen und zum automatischen Erstellen von Security Incidents in Security Incident Response.

AWS Security Hub Integration in SIR Folgt einer bidirektionalen Architektur. SIR Erfassungen Security Hub Führt Daten durch, um einen Security Incident zu erstellen und gleichzeitig einen zu aktualisieren Security Hub Ergebnis mit Updates im entsprechenden Security Incident.

Im folgenden Diagramm erfahren Sie, wie AWS Security Hub mit integriert wird ServiceNow AI Platform Security Operations Anwendungen.



Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Schlüsselfunktionen

Verwenden Sie die wichtigsten Funktionen dieser Integration, um die folgenden Aktionen auszuführen:

- Erkennen Sie AWS Security Hub-Ergebnisse, die Kandidaten für Security Incidents sind, und automatisieren Sie die Erstellung dieser Security Incidents.
- Ordnen Sie AWS Security Hub-Ergebnisse und Entitätsfelder zu zu SIR Security Incident-Felder.
- Filtern Sie AWS Security Hub-Ergebnisse.
- Fassen Sie Ergebnisse zu vorhandenen offenen Security Incidents zusammen, damit Sie keine doppelten Security Incidents erstellen müssen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Automatisieren Sie Statusaktualisierungen von AWS Security Hub-Ergebnissen für Security Incident Response, damit Sie Security Incidents erstellen und schließen können.

  Hinweis:
  ServiceNow Aktualisiert auch den Status der AWS Security Hub-Ergebnisse basierend auf der Erstellung, dem Fortschritt oder dem Abschluss des Security Incidents. Dieses Update enthält auch Kommentare zu zusammengefassten und neuen Ergebnissen.

- Planen Sie die Ergebniserfassung, um regelmäßig Security Incidents zu erstellen.
- Synchronisieren Sie AWS Security Hub-Ergebniskommentare mit SIR Arbeitsnotizen.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
AWS Security Hub-Produktdokumentationswebsite	AWS Security Hub-Dokumentationswebsite
ServiceNow Produktdokumentations-Website	ServiceNow-Produktdokumentationswebsite

Erste Schritte mit AWS Security Hub Integration

Aktivieren und richten Sie ein AWS Security Hub Ergebnisintegration für das Security Operations-Plugin zur Schnittstelle mit Ihrem ServiceNow® Instanz und Security Incident Response Produkt.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Bevor Sie verwenden können AWS Security Hub Integration müssen Sie sie aus herunterladen ServiceNow Store.

Warum und wann dieser Vorgang ausgeführt wird
Überprüfen Sie die folgende Setup-Prüfliste, und stellen Sie sicher, dass Sie alle Aufgaben für eine reibungslose Integration abgeschlossen haben.

Prüfliste

Weisen Sie die erforderlichen zu, und verifizieren Sie sie ServiceNow® Plattform und Security Incident Response Rollen.	Die folgenden Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich:
	• Die Administratorrolle installiert die Integration aus dem ServiceNow Store Und weist die Rolle sn_si.admin zu.
	• Die Rolle sn_si.admin führt die folgenden Aufgaben aus:
	  ◦ Konfiguriert die Integration.
	  ◦ Erstellt Incident-Profile.
	  ◦ Ordnet zu AWS Security Hub Datenfelder für Security Incident-Felder werden gesucht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

	◦ Plant die laufende Incident-Erfassung. ◦ Aktiviert Incident-Updates, wenn ein Security Incident Response Incident wird erstellt oder geschlossen.
Weisen Sie zu AWS Security Hub Erforderliche Rollen.	Die folgenden Rollen sind in erforderlich AWS Security Hub So registrieren und konfigurieren Sie Ihre Anwendung: • Security HubReadOnlyAccess • Security HubFullAccess
Überprüfen Sie AWS Security Hub Integrationseinstellungen	Navigieren zu **Alle** > **AWS Security Hub-Ergebnisintegration** > **Einstellungen für die Integration von AWS Security Hub-Ergebnissen**an. Überprüfen oder ändern Sie die Eigenschaftseinstellungen entsprechend Ihren Anforderungen.
Konfigurieren Sie Ihre Anwendung in AWS Portal.	Registrieren Sie Ihre Anwendung in AWS Portal und gewähren Sie Ihren Anwendern Lese- und Schreibzugriff auf die Anwendung. Weitere Informationen finden Sie in den folgenden Themen: • Einrichten von AWS Config mit der Konsole • Security Hub-Integrationenan.

Registrieren und konfigurieren Sie AWS Security Hub Portal

Registrieren Sie Ihre Anwendung in AWS Security Hub Portal und gewähren Sie Ihren Anwendern Lese- und Schreibzugriff auf die Anwendung.

Registrieren von ServiceNow® Anwenderprofil auf AWS Portal

Vorbereitungen

Erforderliche Rolle: AWSSecurityHubFullAccess

Prozedur

1. Melden Sie sich beim AWS-Portal an.
2. Navigieren zu **Identitäts- und Zugriffsmanagement (IAM)** > **Anwender** > **Neuen Anwender erstellen**an.
3. In der folgenden Tabelle werden die Felder beschrieben, die Sie zum Erstellen eines Anwenderprofils konfigurieren müssen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Anwenderprofil

Feld	Beschreibung
Geben Sie Anwenderdetails an > **Anwendername**	Name für das Anwenderprofil.
Legen Sie Berechtigungen fest > **Anwender zu Gruppe hinzufügen**	Fügen Sie das Anwenderprofil einer Gruppe mit vordefinierten Berechtigungsrichtlinien hinzu. Sie können eine Gruppe nach Ihren Präferenzen erstellen und der Gruppe Berechtigungsrichtlinien zuweisen. Später können Sie der Gruppe Anwenderprofile hinzufügen, und die der Gruppe zugewiesenen Berechtigungsrichtlinien werden automatisch den Anwenderprofilen zugewiesen.
Berechtigungen kopieren	Kopieren Sie Berechtigungen aus einem Anwenderprofil, und weisen Sie sie dem neuen Anwenderprofil zu.
Richtlinien direkt anhängen	Fügen Sie AWSSecurityHubFullAccess als Berechtigungsrichtlinie für Ihr Anwenderprofil hinzu. Weisen Sie dem Anwenderprofil entsprechend Ihren Einstellungen eine neue Berechtigungsrichtlinie zu.
Überprüfen und erstellen	Überprüfen Sie alle Details, die Sie dem Anwenderprofil hinzugefügt haben.

4. Wählen Sie Aus **Erstellen Sie einen Anwender** .
5. Wählen Sie Aus **Zeigen Sie den Anwender an** Aus dem angezeigten Popup-Fenster.
6. Erstellen Sie einen Zugriffsschlüssel und einen geheimen Zugriffsschlüssel für das Anwenderprofil.
   Sie benötigen diese Schlüssel, um auf zuzugreifen AWS Security Hub Integration von Ihrem ServiceNow® Instanz.
7. Navigieren zu **AWS-Services** > **Suchen** > **AWS Security Hub** > **an.**
8. Wählen Sie Aus **Wechseln Sie zu** *`Security Hub`*.
9. In Aktivieren AWS Security Hub Seite auswählen **Herunterladen** Zum Aktivieren AWS Konfiguration.
   Laden Sie die Dateien herunter, und führen Sie sie in Ihrem Account aus. Dies gewährt Ihnen die Berechtigung, alle Informationen aus verschiedenen AWS-Reporting-Services zu erfassen und in zusammenzufassen AWS Security Hub.
10. Wählen Sie Aus **Aktivieren** *`AWS Security Hub`*Unten auf der Seite.
    Es dauert einige Minuten für *`AWS Security Hub`*Dashboard zum Anzeigen aller Details.
11. Region ändern von **Global** Bis **US-Osten (Ohio)** .
    Der Code für **US-Osten (Ohio)** Ist **USA-Ost-2** . Alle ServiceNow® Diesem Regionscode sind Ressourcen zugewiesen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie AWS Security Hub Integration

Installieren und konfigurieren Sie AWS Security Hub Integration aus dem ServiceNow Store Auf Ihrem ServiceNow AI Platform Instanz, mit der die Erfassung gestartet werden soll AWS Security Hub Ergebnisse.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Laden Sie herunter AWS Security Hub Integration aus dem ServiceNow Store Und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie nach AWS Security Hub Kachel und klicken Sie auf **Konfigurieren** .
4. Füllen Sie im Formular die Felder aus.

AWS Security Hub Konfigurationsformular

Feld	Beschreibung
Name	Name für AWS Security Hub Instanzkonfiguration.
Regionsname	Region, die Sie in zugewiesen haben ServiceNow® Anwenderprofil auf AWS Security Hub Portal.
Geheimer Schlüssel	Geheimer Schlüssel, den Sie für erstellt haben ServiceNow® Anwenderprofil auf AWS Security Hub Portal.
Zugriffsschlüssel	Zugriffsschlüssel, den Sie für erstellt haben ServiceNow® Anwenderprofil auf AWS Security Hub Portal.

5. Klicken Sie auf **Absenden**.

Ergebnisse

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, jeweils Security Hub Die Serverkonfiguration der Ergebniserfassung wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Erstellen Sie ein Profil für AWS Security Hub Integration wird gesucht

Erstellen Sie einen AWS Security Hub Profil in Ihrem ServiceNow AI Platform Instanz, aus der Sie Daten erfassen möchten AWS Security Hub Und erstellen Sie einen entsprechenden Security Incident in Arbeitsbereich für Security Incident Response.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Mit der Integration können Sie Security Incidents für verschiedene Arten von Ergebnissen in erstellen AWS Security Hub Plattform, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese Incidents werden basierend auf den Profilen erstellt, die Sie in konfigurieren ServiceNow AI Platform Instanz. Alle Incidents werden anfänglich für einen konfigurierten Ergebnistyp in einem Profil erstellt. Sie können die von Ihnen erstellten Ergebnisse weiter filtern, um anzugeben, welche Ergebnisse Security Incidents erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Ergebnisse, die die Auswahlkriterien in erfüllen AWS Security Hub Mandanten und sind über verfügbar AWS Security Hub API, werden anfänglich in erfasst ServiceNow AI Platform Instanz.

Prozedur

1. Navigieren zu **Alle** > **AWS Security Hub – Ergebnisintegration** > **AWS Security Hub – Ergebnisprofil**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

AWS Security Hub – Formular „Konfiguration der Ergebniserfassung“

Feld	Beschreibung
Name	Name für das Profil. Dieser Name hilft Ihnen bei der Identifizierung des Profiltyps und ist auch der Standardname für das Sicherheits-Tag, das diesem Profil zugeordnet ist.
Aktiv	Auswählen, um das Profil zu aktivieren. Wenn das Profil aktiv ist, bedeutet dies, dass ServiceNow AI Platform Nimmt aktiv auf AWS Security Hub In werden Ergebnisdaten und entsprechende Security Incidents erstellt SIR Wenn die Filterbedingungen erfüllt sind.
Quelle	Die AWS Security Hub Integrationsmandant, den Sie für die Erfassung von Ergebnissen konfiguriert haben. Wenn Sie mehrere Mandanten konfiguriert haben, wählen Sie den entsprechenden Mandanten für die Ergebnistypen aus, die Sie für das Profil erfassen möchten.
Reihenfolge	Geben Sie einen Wert für dieses Feld ein, der die Reihenfolge angibt, in der Flows ausgeführt werden, wenn zwei oder mehr Profile auslösende Bedingungen teilen. Der Flow mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Beispiel: 100, 200, 300, 400. Der Standardwert ist 100.
Beschreibung	Zusätzlicher Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Ordnen Sie zu AWS Security Hub Ergebnisfelder

Ordnen Sie die Person zu AWS Security Hub Suchfelder für die Felder in SIR Security Incident, damit Sie Incidents mit den zugeordneten Daten erstellen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Auf der Zuordnungsseite in AWS Security Hub Zuordnungsabschnitt wählen Sie eine der Beispielerfassungsmethoden aus.

Beispiel für Erfassungsmethoden

Feld	Beschreibung
Alle standardmäßigen Ergebnisfelder	Verwenden Sie diese Erfassungsmethode, um die statische Liste aller Ergebnisfelder anzuzeigen. Diese Methode enthält nur Standardfeldnamen ohne Werte. Sie können diese Informationen verwenden, um eine Zuordnung zu vorzunehmen SIR Felder.
Aktuelle Abrufen AWS Security Hub Ergebnisse	Verwenden Sie diese Erfassungsmethode, um die neuesten Ergebnisdaten zu importieren. Sie können standardmäßig 5 Beispielergebnisse und maximal 20 Beispielergebnisse erfassen. Die Feldwerte für Beispielergebnisse werden ausgefüllt, wenn das Profil die Beispielergebnisse erfasst. Sie können diese Ergebnisse dem zuordnen **SIR-Incident-Zielfelder** . Die Ergebnisfelder und -Werte werden als einzelne Registerkarten angezeigt.
Importieren Sie Beispieldaten	Wählen Sie Aus **Importieren Sie Beispieldaten** Dient zum Importieren von Beispielergebnissen aus AWS Security Hub. Diese Schaltfläche wird angezeigt, wenn Sie zuletzt abrufen auswählen AWS Security Hub Ergebniserfassungsmethode. Beispielergebnisse werden von abgerufen AWS Security Hub Der Server dauert einige Minuten. Ordnen Sie diese Ergebnisse dem zu **SIR-Incident-Zielfelder** . Die Ergebnisfelder und -Werte werden als einzelne Registerkarten angezeigt.

2. Führen Sie die folgenden Aktionen aus, um den Standardfeldern, die im Security Incident angezeigt werden, Felder hinzuzufügen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie im Abschnitt SIR Incident-Zielfelder die aus

Schaltfläche. Es wird eine Liste von angezeigt SIR Felder, aus denen Sie auswählen können, um ein neues Feld anzuzeigen.

a. Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie dann ein Feld aus.

Hinweis:
Mehrere erkennbare Elemente können für denselben Security Incident angezeigt werden. Zum Beispiel die **Erkennbares Element** Das Feld kann mehrmals verschiedenen Werten zugeordnet werden. Ebenso wird **Konfigurationselement** Und **Felder für Arbeitsnotizen** Unterstützt mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird eine Fehlermeldung angezeigt, dass dieses Feld nicht mehrere Werte unterstützt. Wenn ein Feld in einem Security Incident über eine Liste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

b. Von AWS Security Hub Abschnitt „Quellfelder“ ziehen Sie Ihr Feld, um es Ihrem neuen Feld zuzuordnen.

c. Wenn Sie das Kontrollkästchen aktivieren, das einem Feld entspricht, werden alle neuen oder aktualisierten Änderungen in vorgenommen AWS Security Hub Werden automatisch im jeweiligen SIR mit neuen Incident-Daten aktualisiert.

Hinweis:
Im Basissystem ist die Systemeigenschaft sn_sec_Security.finding_updates standardmäßig auf „wahr“ festgelegt, um zu empfangen AWS Security Hub Updates im Zusammenhang mit neuen Warnungen, die mit SIR verknüpft sind.

- Standardmäßig sind die Felder Betroffene Anwender, Konfigurationselemente und erkennbare Elemente aktiviert. Dies bedeutet, dass immer dann, wenn neue erkennbare Elemente oder zugehörige Konfigurationselemente oder betroffene Anwender dem Incident hinzugefügt werden, diese Informationen während dieses Abfrageintervalls automatisch extrahiert und in die entsprechenden zugehörigen Listen in der Security Incident Response (SIR) eingetragen werden.
- Für alle anderen Felder müssen Sie das Kontrollkästchen aktivieren, das einem Feld für alle neuen oder aktualisierten Änderungen entspricht, die im Ergebnis in vorgenommen wurden AWS Security Hub. Dadurch werden die entsprechenden SIR-Incident-Daten automatisch mit den neuen Incident-Daten aktualisiert.

Wichtig:
Vor der Auswahl dieser Funktionalität muss eine Sorgfaltspflicht durchgeführt werden, da das Überschreiben der vorhandenen Daten zu instabilen Daten führen kann, mit denen der Analyst arbeiten kann, und jede andere Automatisierung, die auch durch die Feldwerte des Security Incident festgelegt wird, kann ebenfalls betroffen sein. Daher ist es wichtig, die Sorgfaltspflicht durchzuführen, bevor Sie eine Überschreibungsfunktion auswählen.

3. Verwenden Sie zum Entfernen eines Felds , (**Element entfernen**) Schaltfläche neben dem Eingabeausdrucksfeld im Abschnitt SIR Incident-Zielfelder.

4. Dient zum Zuordnen eines Feldwerts aus dem AWS Security Hub Abschnitt „Quellfelder“ zu einem Feld im Abschnitt „SIR-Incident-Zielfelder“ verwenden Sie eine der folgenden Aktionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Ziehen Sie den Feldnamen (z. B. ID), und legen Sie ihn neben einem Feldnamen in der Spalte SIR Incident-Zielfelder ab.

Sie können jeden Wert aus dem abgleichen AWS Security Hub Quellfeldabschnitt zu einem Feld im Abschnitt SIR-Incident-Zielfelder. Felder sind farbcodiert, damit Sie Ergebnisfelder im Zuordnungsprozess nicht übersehen oder duplizieren. Hellblaue Felder geben an, dass noch kein Ergebnisfeld ausgewählt und dem Security Incident zugeordnet ist. Möglicherweise möchten Sie ein eingehendes Ergebnisfeld mit mehr als einem Feld in einem Security Incident verknüpfen. Ein graues Feld gibt an, dass ein Ergebnisfeld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Auf diese Weise können Sie visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Ergebnisinformationen nicht zugeordnet sind. Es gibt jedoch einige Felder in AWS Security Hub Abschnitt „Quellfelder“, die nicht mit Feldern im Abschnitt „SIR-Incident-Zielfelder“ kompatibel sind. Wenn Sie solche Werte zuordnen, wird sie beim Erstellen des SIR nicht angezeigt.

b. Sie können eine Kombination aus Text und Feld hinzufügen.
Beispiel: `Ergebnisname ist ${Name}$` . Hier, `Ergebnisname ist` Kann während manuell eingegeben werden `${Name}$` Ist aus zugeordnet AWS Security Hub Abschnitt „Quellfelder“.

c. Sie können ein Quell-Ergebnisfeld manuell eingeben und einem Zielfeld zuordnen.
Verwenden Sie dasFormat $ {field Name}$, um ein Quellergebnisfeld manuell zuzuordnen.
Um beispielsweise einen Schweregrad eines Ergebnisfelds zuzuordnen, lautet das Format `${properties(severity)}$` .

Diese Integration klassifiziert bestimmte Untertypen erkennbarer Elemente. Wenn Sie einen zuordnen AWS Security Hub Suchfeld mit dem SIR-erkennbaren Feld, der ServiceNow AI Platform Klassifiziert das erkennbare Element automatisch. Wenn Sie die eingehenden generischen zuordnen möchten AWS Security Hub Erkennbares Element für den Typ des erkennbaren Elements in SIR, Und ziehen Sie dann per Drag-and-Drop AWS Security Hub Feld im Feld erkennbares Element. Wenn Sie jedoch den erkennbaren Typ für den eingehenden kennen AWS Security Hub Erkennbares Element in SIR, Und ordnen Sie dann speziell dem zu SIR Typfeld des erkennbaren Elements. Einige Beispiele für bestimmte Typen erkennbarer Elemente in SIR Schließen Sie erkennbares Element (Domänenname), erkennbares Element (E-Mail-Adresse), erkennbares Element (IP-Adresse (V4)) und erkennbares Element (Hostname) ein.

Manchmal werden Feldwerte in gesucht AWS Security Hub Kann nicht direkt in die Felder des SIR Security Incident übersetzt werden. Für diese Werte können Sie einen Skripteditor verwenden, um Feldwerte für den Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind.

5. Formatieren einer Feldübersetzung für ein neues Feld aus einem AWS Security Hub Suche um einen Feldwert in einem Security Incident abzugleichen, klicken Sie auf **Klicken Sie hier** Link in **SIR-Incident-Zielfelder** Header.

6. Klicken Sie auf , um die Felder zu ändern, die die Feldübersetzung unterstützen Symbol für Übersetzung des Skriptformatfelds.
Die Felder, die die Feldübersetzung unterstützen, sind **Kategorie** , **Konfigurationselement** , Und **Priorität** . Klicken Sie beispielsweise auf Symbol neben der Kategorie. Die AWS Security Hub Der Editor des Skripts für die Übersetzung des Ergebnisfelds wird geöffnet.

7. Geben Sie alle Änderungen am Skript ein, und klicken Sie auf **Aktualisieren** Um die Änderungen zu speichern und zur Zuordnungsseite zurückzukehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie beispielsweise für Kategorie Folgendes im Skript-Editor:

```
"<Incoming Security Hub finding Field Value>" : "<Category to assign to the Security Incident>".
```

Diese Zuordnung stellt sicher, dass ein Profil nur konfigurierte Kategorien verwendet.

8. Setzen Sie Ihre Zuordnung fort, indem Sie Feldwerte hinzufügen oder entfernen.
   Sie können dieselben Feldwerte im Generator für Incident-Generierungsbedingungen verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes Ergebnis erfüllen muss, um einen Security Incident zu erstellen.
9. Um zum Abschnitt Filtern und Zusammenfassung zu wechseln, klicken Sie auf **Fahren Sie Fort** .

Nächste Maßnahme

Definieren und legen Sie Filterbedingungen fest, damit Sie angeben können, welche Ergebnisse Security Incidents erstellen. Sie können dieselben Feldwerte (definiert im Abschnitt „Zuordnung“) im Generator für Incident-Generierungsbedingungen (im Abschnitt „Filterung und Zusammenfassung“) verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes Ergebnis erfüllen muss, um einen Security Incident zu erstellen.

Definieren Sie Filter- und Zusammenfassungskriterien für AWS Security Hub Ergebniserfassung

Sie können Filterbedingungen definieren und festlegen, um anzugeben, welche eingehenden Ergebnisse Security Incidents erstellen sollen. Sie können auch zusätzliche Incident-Feldkriterien definieren, mit denen eingehende Ergebnisse an einen offenen Security Incident angehängt werden können, anstatt einen weiteren Security Incident für dasselbe Ergebnis zu erstellen.

Legen Sie die Filterbedingungen für fest AWS Security Hub Ergebnisse zum Erstellen von Security Incidents

Legen Sie die Filterbedingungen so fest, dass Security Incidents nur erstellt werden, wenn die Filterbedingungen übereinstimmen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Art der Filterung hilft Ihnen, Security Incidents zu isolieren und die Anzahl der von Ihnen erstellten Security Incidents zu begrenzen. Wenn Sie zusätzliche Filterkriterien festlegen, werden nur die erforderlichen Ergebnisse erfasst, ohne die Abfrage oder die Konfiguration der ausgelösten Incidents ändern zu müssen.

Führen Sie die folgenden Schritte aus, um die Kriterien zu definieren, die eingehend sind AWS Security Hub Das Ergebnis muss erfüllt sein, damit ein Security Incident erstellt wird:

Prozedur

1. Wählen Sie Aus **Vorfilter Anwenden** Im Abschnitt Vorfilterung.

   Sie können diese Option verwenden, um bestimmte Ergebnisse zu filtern und die Belastung der Ergebniserfassung zu reduzieren.

   In **API-Filter** Geben Sie eine JSON-Bedingung gemäß Ihrer Anforderung ein, die bestimmte Ergebnisse basierend auf der Bedingung herausfiltert. Geben Sie beispielsweise den folgenden Wert ein, um Ergebnisse mit dem Workflow-Status „gelöst“ in Security Hub herauszufiltern:

```
{"Filters"{
 "WorkflowStatus":[{
```

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 "Comparison":"NOT_EQUALS",
 "Value": "RESOLVED"}]
 }
}
```

Basierend auf der angegebenen Bedingung, AWS Security Hub Ergebnisse werden erfasst und in angezeigt AWS Security Hub Rohtabelle der Ergebnisse.

Navigieren zu **Alle** > **AWS Security Hub – Ergebnisintegration** > **AWS Security Hub-Ergebnisse – Rohdaten** Zum Anzeigen der Rohergebnisdaten.

2. Wählen Sie im Abschnitt Ergebnisfelder für Filterbedingungen auswählen die Option aus **Verfügbare Ergebnisfelder anzeigen** Dient zum Anzeigen einer Liste aller verfügbaren Felder in einem AWS Security Hub Ergebnis.
   Von **Alle Ergebnisfelder** Wählen Sie die Ergebnisfelder aus, die im Abschnitt „Generierungsbedingungen für Security Incidents“ angezeigt werden sollen.

   Hinweis:
   Ein AWS Security Hub-Ergebnis enthält mehrere Felder und Werte. In **Alle Ergebnisfelder** Liste können Sie gemäß Ihren Anforderungen nach einem Ergebnisfeld suchen und es auswählen.

3. Wählen Sie im Abschnitt Generierungsbedingungen für Security Incidents die Option aus **Filtern Sie basierend auf Bedingungen** Zum Definieren der Kriterien, die ein eingehender AWS Security Hub Das Ergebnis muss erfüllt sein, damit ein Security Incident erstellt wird.

   Das erste Feld in den Filterbedingungen enthält eine Standardliste von zweihundert Feldern, die in einem verfügbar sind AWS Security Hub Ergebnis und die Ergebnisfelder, die Sie im Abschnitt „Ergebnisfelder für Filterbedingungen auswählen“ ausgewählt haben.

   Das zweite Feld in den Filterbedingungen enthält bedingte Operatoren. Die von Ihnen ausgewählte Option bestimmt die Bedingung, die erfüllt sein muss, um ein Ergebnis zu erfassen.

   Das dritte Feld in den Filterbedingungen enthält Werte, die von den verfügbaren Ergebnisfeldern unterstützt werden. Stellen Sie sicher, dass das von Ihnen eingegebene Ergebnisfeld mit den Werten der Ergebnisse übereinstimmt.

   Verwenden Sie beispielsweise die Filterbedingung *`Enthält`* Für die folgenden Felder mit mehreren Werten:

   - Workflow(Status)
   - WorkflowState

4. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter für die erste Zeile fest.
5. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER** .
   - Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden.
6. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien** .

Ergebnisse

Basierend auf den Filterbedingungen AWS Security Hub Ergebnisse werden in importiert SIR. Navigieren zu **Alle** > **AWS Security Hub – Ergebnisintegration** > **AWS Security Hub-Ergebnisse – Import** Zum Anzeigen der importierten Ergebnisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie Bedingungen für die Zusammenfassung AWS Security Hub Ergebnisse zu einem Security Incident

Definieren Sie zusätzliche Incident-Zusammenfassungskriterien, die eingehende aggregieren AWS Security Hub Suche nach einem vorhandenen SIR Security Incident, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Wenn Sie Feldübereinstimmungswertkriterien für jedes Profil verwenden, kann diese zusätzliche Zusammenfassung die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Incident-Daten in einem einzelnen Security Incident platziert werden.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein neuer Incident allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird der Incident automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Anwender mit der Rolle „sn_si.Analyst“, der mit Security Incidents arbeitet, können Sie alle hinzugefügten aggregierten Incidents in einer zugehörigen Liste zu einem Security Incident anzeigen.

Alle aggregiert AWS Security Hub Ergebnisse zu einem Security Incident werden im angezeigt AWS Security Hub Zugehörige Liste. Diese Liste enthält Details zu den zugehörigen Zeitstempeln und aggregierten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum AWS Security Hub Ergebnisse werden den vorhandenen Security Incidents hinzugefügt.

Prozedur

1. Zum Definieren zusätzlicher Incident-Feldkriterien, die eingehende zulassen AWS Security Hub Ergebnis, das an einen offenen Security Incident angehängt werden soll, anstatt einen neuen Incident zu erstellen, wählen Sie aus **Zusammenfassungsbedingungen** Option.
2. In **Incident-Felder mit übereinstimmenden Werten** Geben Sie die Feldwerte ein, die Sie für vorhandene Security Incidents in abgleichen möchten ServiceNow AI Platform Instanz.
   Alle Feldwerte, die Sie im Eingabefeld für die Mehrfachauswahl ausgewählt haben, müssen übereinstimmen, damit die Zusammenfassungskriterien erfüllt sind und dieser eingehende Incident an einen vorhandenen Security Incident angehängt werden kann. Diese Auswahl impliziert, dass es sich um einen handelt *UND* Bedingung, unter der ihnen Felder wie erkennbare Elemente und Konfigurationselemente zugeordnet werden, die mehrere Feldwerte haben können. Wenn nur eine Teilmenge der Werte übereinstimmt, wird die AWS Security Hub Die Bedingungen für die Ergebniszusammenfassung sind nicht erfüllt, und ein neuer Security Incident wird erstellt.
3. Um mehrere übereinstimmende Feldbedingungen hinzuzufügen, klicken Sie auf **Fügen Sie Neue Kriterien Hinzu** .
   Die Zusammenfassung erfolgt, wenn eine der von Ihnen definierten Bedingungen für Mehrfachauswahlfelder erfüllt ist. Diese Auswahl impliziert *ODER* Bedingung.
4. Um die Arbeitsnotiz für ein neues Ergebnis zu aktualisieren, wenn sie einem Security Incident hinzugefügt wird, wählen Sie aus **Arbeitsnotiz für neues Ergebnis protokollieren** .

   Die Arbeitsnotiz protokolliert, dass ein neues Ergebnis hinzugefügt wird, und enthält einen Link zu den Ergebnisdetails. Die Protokoll-Arbeitsnotiz aktualisiert auch weitere Details, die Sie dem Feld Arbeitsnotiz in Ihrem Zuordnungsabschnitt hinzufügen.
5. Klicken Sie auf, um den Zeitplan zu konfigurieren **Fahren Sie Fort** .

Ergebnisse

Basierend auf den Zusammenfassungsbedingungen, AWS Security Hub Ergebnisse werden zusammengefasst, um eine zu erstellen SIR Incident. Navigieren zu **Alle** > **AWS Security Hub**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

– Ergebnisintegration > **AWS Security Hub-Ergebnisse zu Aufgabe** Um die Liste der erstellten Security Incidents anzuzeigen.

Nächste Maßnahme
Legen Sie einen Zeitplan fest, um die Ergebnisdaten und die Ergebnis-Incidents abzurufen, die den Kriterien im Profil entsprechen.

Planen Sie AWS Security Hub Ergebnisabruf

Legen Sie einen Zeitplan fest, um die Ergebnisdaten abzurufen und zu erfassen AWS Security Hub Ergebnisse, die den Kriterien im Profil entsprechen.

Vorbereitungen
Erforderliche Rolle: sn_sni.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können planen, wie oft Sie in der Zukunft abfragen möchten AWS Security Hub Ergebnisse, die mit übereinstimmen AWS Security Hub Profilkonfiguration wird gesucht.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die verschiedenen Abfrageintervalle können sich auf die Leistung von auswirken AWS Security Hub Ergebnisintegration. Planen Sie bei der Planung, dass die Systemlast gegen die Dringlichkeit eines Incident ausgeglichen wird. Für alle Profile ist ein einminütiger Standardwert festgelegt. Sie können diese Einstellung basierend auf der Dringlichkeit des Incident und der erwarteten Belastung Ihres Systems ändern.

Alle Warnungen, die dem Incident in einem bestimmten Abfrageintervall hinzugefügt werden, werden verarbeitet und dann an angehängt AWS Security Hub Zugehörige Listen und Kommentare zu Warnungen.

Prozedur

1. Füllen Sie die Felder im Planungsformular aus.

Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Ergebnisse aus abrufen AWS Security Hub Mandant.

Zeitplanungsformular

Feld	Beschreibung
Laufende Ergebniserfassung	Laufende Ergebniserfassung, die der ServiceNow AI Platform Instanz ruft aus ab AWS Security Hub Mandant für neue Incidents. Security Incidents werden erstellt, wenn ausgelöste Ergebnisse gefunden werden und die Filterkriterien für die Generierung von Security Incidents erfüllt sind.
Geschlossene Ergebnisse abfragen	Abfrage von Ergebnissen, die gelöst wurden. Diese Ergebnisse werden während der laufenden Incident-Erfassung erfasst.
Abfrageschritt (Minuten)	Abfragehäufigkeit, die in Minuten definiert ist.
Legen Sie die Zeit der ersten Ergebniserfassung fest	Ergebniserfassung, die auf dem konfigurierten Datum und der konfigurierten Uhrzeit basiert. Sie können diese Option verwenden, um ein bestimmtes Datum und eine bestimmte Uhrzeit

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	für die anfängliche Erfassung zu definieren. Nachfolgende Erfassungen basieren auf dem Abfrageintervall-Zeitraum.
Geben Sie die Zeit der ersten Ergebniserfassung ein	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben.
Einmaliger Abruf	Aktivieren Sie dieses Kontrollkästchen, um den einmaligen Abruf des Verlaufs zu ermöglichen AWS Security Hub Ergebnisse und führen Sie dann den Abgleich der Daten durch. Wenn Sie dieses Kontrollkästchen aktivieren, ruft die Anwendung alle offenen und geschlossenen ab AWS Security Hub Ergebnisse für den Zeitraum von ungefähr 90 Tagen. Bei der Verarbeitung der Daten werden sowohl laufende Ergebnisse als auch Verlaufsdaten abgerufen, die Verarbeitung der laufenden Ergebnisse hat jedoch Vorrang vor dem historischen Abruf. Andernfalls kann der historische Abruf je nach Dauer und Anzahl der erfassten Ergebnisse einige Zeit dauern. **Hinweis:** Der abgerufene Verlauf AWS Security Hub Ergebnisse werden Deduplizierungsprüfungen unterzogen, um Duplikate innerhalb von zu verhindern Security Incident Response Anwendung.
Seit Datum	Das Datum, ab dem die historischen Ergebnisse erfasst werden AWS Security Hub. **Hinweis:** Die Ergebnisdaten werden ungefähr aus den letzten 90 Tagen abgerufen.

Auf der Planungsseite können Sie definieren, wie und wann Ergebnisse aus abgerufen werden AWS Security Hub Mandant.

2. Um zur Seite „zusätzliche Optionen“ zu navigieren, klicken Sie auf **Fahren Sie Fort** .

Automatisieren Sie AWS Security Hub Aktualisierungen und Abschlüsse durch suchen SIR Incident-Status

Automatisieren Sie die Aktualisierungen und Abschlüsse von Ergebnissen in AWS Security Hub Gemäß SIR Incident-Status. Die AWS Security Hub Die Integration verfügt über eine bidirektionale Schnittstelle, die die Ergebniserfassung ermöglicht, um Security Incidents zu erstellen und den Status der Ergebnisse entsprechend den Änderungen in zu aktualisieren SIR Incident.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Tragen Sie die Details in das Formular ein.
   Befolgen Sie die Anweisungen, um die Konfiguration für die Aktualisierung abzuschließen AWS Security Hub Ergebnisse, wenn Sie einen Security Incident in erstellen oder schließen SIR.

Formular „Automatisieren von Incident-Updates“

Kategorie	Feld	Beschreibung
Status aktualisieren	SIR Incident-Status	Zeigt eine Liste von an SIR Incident-status. Wählen Sie eine Option aus dieser Liste aus, um sie einem zuzuordnen Security Hub Ergebnisstatus.
	Security Hub Ergebnisstatus	Zeigt eine Liste von an Security Hub Workflow-Status. Der Workflow-Status eines Ergebnisses wird am aktualisiert AWS Security Hub Wenn sich der Incident-Status des entsprechenden SIR-Status ändert.
Priorität aktualisieren	SIR Incident-Priorität	Zeigt eine Liste von an SIR Incident-Prioritätsstufen. Wählen Sie eine Option aus dieser Liste aus, um sie einem zuzuordnen Security Hub Prioritätsebene wird gesucht.
	Security Hub Ergebnispriorität	Wählen Sie eine Option aus der Liste von aus Security Hub Schweregradstufen. Der Schweregrad eines Ergebnisses wird auf aktualisiert AWS Security Hub Wenn sich die entsprechende Security Incident-Priorität ändert.
Arbeitsnotizen aktualisieren	Wählen Sie diese Option aus, um den Abschnitt „Notizen“ von zu aktualisieren Security Hub Wenn eine Arbeitsnotiz für den entsprechenden aktualisiert wird SIR Incident. Der Abschnitt „Arbeitsnotizen“ in SIR Hat einen Grenzwert von 512 Zeichen als Hinweisabschnitt von Security Hub Das Ergebnis unterstützt dasselbe.	
Zusätzliche Kommentare aktualisieren	Auswählen, um zu aktualisieren AWS Security Hub Abschnitt „Kommentare suchen“ mit den zusätzlichen Kommentaren, die Sie in angegeben haben SIR Incident.	
Lösungsnotizen aktualisieren	Auswählen, um zu aktualisieren AWS Security Hub Abschnitt „Kommentare schließen“ mit den Lösungshinweisen, die Sie bei angegeben haben SIR Incident wurde gelöst.	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Jede Aktualisierung aus den Arbeitsnotizen überschreibt die letzte Aktualisierung im Abschnitt „Notizen“ von Security Hub Ergebnis. Wir empfehlen Ihnen, relevante Arbeitsnotizen in einem hinzuzufügen SIR Incident.

2. Wählen Sie **Fertigstellen** aus.

Nächste Maßnahme
Das Profil wechselt in den Status „Warten“. Wenn die Bestätigungsnachricht anzeigt, dass das Setup und die Konfiguration abgeschlossen sind, können Sie das Profil aktivieren.

SIR Formular nach einem AWS Security Hub Ergebniserfassung

Nach ServiceNow AI Platform Erfasst AWS Security Hub Ergebnis wird ein Security Incident erstellt, und die Aktualisierungen werden an diesem Security Incident-Datensatz vorgenommen.

Arbeitsnotizen

Eine Arbeitsnotiz wird veröffentlicht, wenn ein Incident aggregiert wird und Sie konfiguriert haben **Arbeitsnotiz für neues Ergebnis protokollieren** Option in Definieren Sie Filter- und Zusammenfassungskriterien für AWS Security Hub Ergebniserfassung.

Sie können auch den internen Ergebnisimport-Datensatz anzeigen, der die Incident-Rohdaten enthält.

Wenn Sie auf klicken **Klicken Sie hier** Link, können Sie den Datensatz in anzeigen AWS Security Hub Umgebung. Das folgende Beispiel zeigt den Datensatz in AWS Security Hub Umgebung.

Aggregiert AWS Security Hub Ergebnisse

Aggregiert Anzeigen AWS Security Hub Ergebnisse: Zeigen Sie die Incidents an, die zum Security Incident aggregiert sind. Navigieren zu **Alle zugehörigen Listen anzeigen** > **Zusammengefasste AWS Security Hub-Ergebnisse**an.

Security Incident erstellen: Wählen Sie einen Incident aus der Liste aus, und klicken Sie auf **Aktionen** Und klicken Sie dann auf **Erstellen Sie einen Security Incident** . Mit dieser Option wird ein neuer Security Incident für den Incident erstellt, und dieser Incident wird vom übergeordneten Security Incident deaggregiert.

Carbon Black: Integration der Incident-Anreicherung

Verwenden Sie die Carbon Black-Integration, um Security Incidents mithilfe von APIs zu untersuchen und darauf zu reagieren, um Endpunkte abzufragen und mit Security Incidents zu interagieren.

Carbon Black – Integrationsressourcen zur Incident-Anreicherung suchen

- Erste Schritte mit der Integration Carbon Black – Incident-Anreicherung
- Security Operations Carbon Black-Integration – Flow Für Laufende Prozesse Abrufen
- Security Operations Carbon Black-Integration – Host-Flow Isolieren
- Security Operations Carbon Black-Integration: Flow Zum Entfernen Der Host-Isolation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verstehen Sie Integrationskonzepte

- Typen von ServiceNow Integrationen bereitgestellt
- Security Operations Workflow-Auslöser

Holen Sie sich Hilfe von ServiceNow-Ressourcen

- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support
- Upgrade auf Madrid

Erste Schritte mit der Integration Carbon Black – Incident-Anreicherung

Die Carbon Black-Incident-Ergänzung erleichtert die Untersuchung eines Security Incidents, indem Protokolle nach potenziell schädlichen Indikatoren abgefragt werden. Bevor Sie die Integration Carbon Black – Incident-Anreicherung verwenden können, müssen Sie sie aus herunterladen ServiceNow Store Und fügen Sie die entsprechende Endpunkt-Basis-URL und DEN MID-Server hinzu.

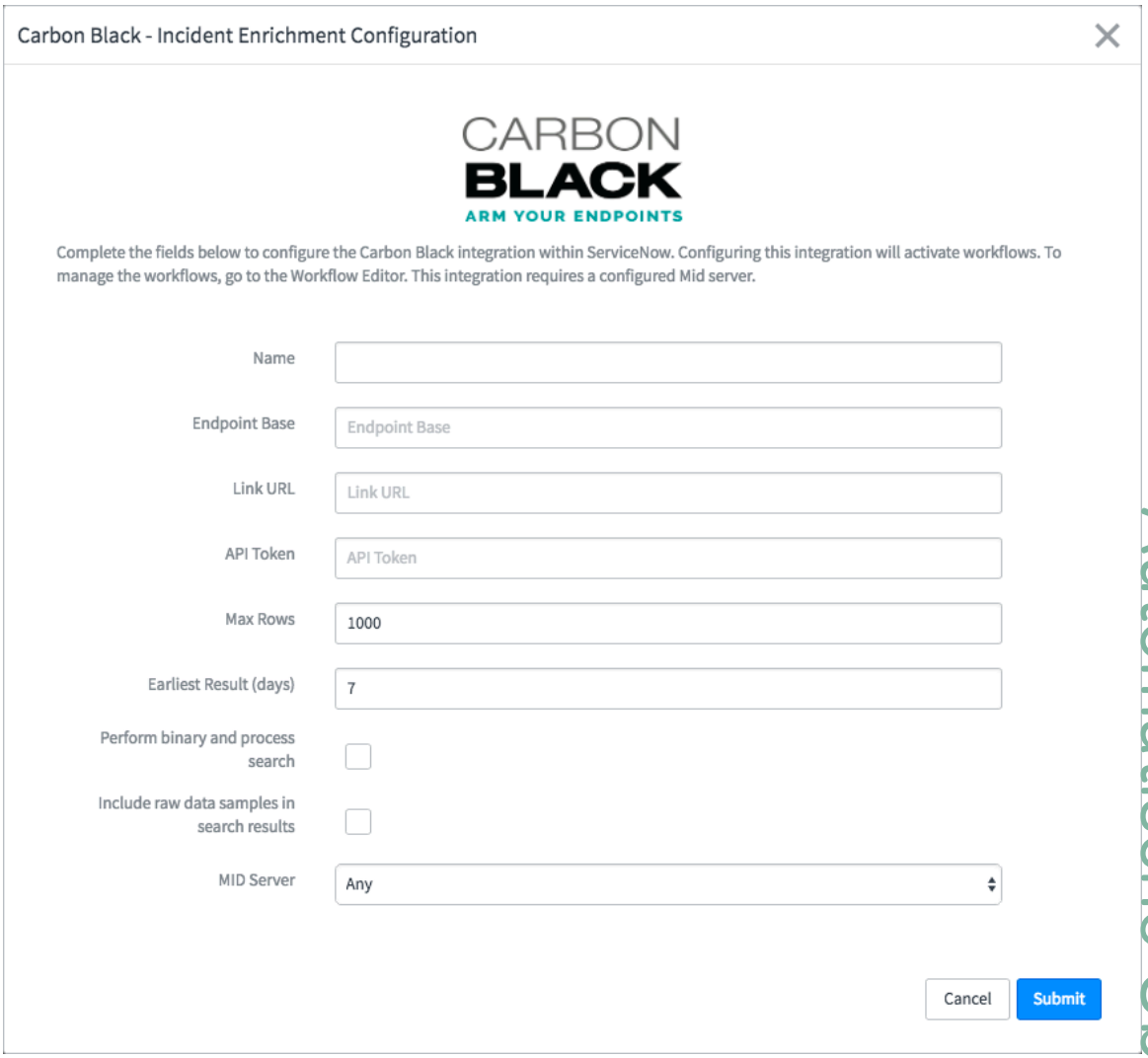
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Wenn der Download abgeschlossen ist, greifen Sie auf zu Carbon Black Website und rufen Sie die Endpunkt-Basis-URL und das API-Token unter Ihrem Profil ab.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**an.
4. Klicken Sie auf der Karte Carbon Black – Incident-Anreicherung auf **Konfigurieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Endpunktbasis	Die Endpunkt-URL, die Sie von der Carbon Black-Website erworben haben.
Link-URL	Die Link-URL, die mit einer Carbon Black-Instanz verknüpft ist, falls verfügbar.
API-Token	Das API-Token, das Sie von der Carbon Black-Website erworben haben.
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten. Der Standardwert ist 1000 Zeilen.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie in Tagen anzeigen möchten.
Binär- und Prozesssuche durchführen	Wählen Sie diese Option aus, um binäre Suchen durchzuführen, um binäre Dateien wie Datei-Hashes zu finden, und um nach .exe-Prozessen zu suchen, die möglicherweise ausgeführt wurden.
Rohdatenmuster in	Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Suchergebnissen berücksichtigen	hängt von Ihrer Einstellung in ab **Anzahl der Zeilen mit Rohdaten** Eigenschaft in Eigenschaften von Security Incident Response .
MID-Server	Wählen Sie Aus **Beliebig** Um einen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Navigieren Sie zum Verwalten der Workflows zu **Workflow-Editor** .

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie aus **Nein** Von **Konfigurationen Anzeigen** Dropdown-Liste.

Integration mit Carbon Black

Mit der Carbon Black-Integration können Sie Security Incidents mithilfe von APIs untersuchen und darauf reagieren, um Endpunkte abzufragen und mit Security Incidents zu interagieren.

Erkunden

- Security Incident Response-Integrationen
- Carbon Black: Integration der Incident-Anreicherung

Einrichten

Erste Schritte mit der Carbon Black-Integration

Verwenden

- Security Operations Workflow-Auslöser
- Zeigen Sie betroffene Elemente für einen Security Incident an
- Security Operations – Flow „Laufende Prozesse Abrufen“
- Security Operations Carbon Black-Integration – Flow Für Laufende Prozesse Abrufen
- Zeigen Sie betroffene Elemente für einen Security Incident an
- Blockierungsanforderung ausführen
- Integration Von Security Operations: Block-Anforderungs-Flow
- Führen Sie „Host Isolieren“ Aus

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie Komponenten, die mit einer Anwendung installiert sind

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Security Operations Carbon Black-Integration – Host-Flow Isolieren
- Security Operations Carbon Black-Integration: Flow Zum Entfernen Der Host-Isolation

---

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Erste Schritte mit der Carbon Black-Integration

Carbon Black ist ein fortschrittliches Sicherheitssystem, das leicht in integriert werden kann Security Operations. Bevor Sie die Carbon Black-Integration verwenden können, müssen Sie die Integration aus herunterladen ServiceNow Store Und fügen Sie die entsprechende Endpunktbasis und das API-Token hinzu.

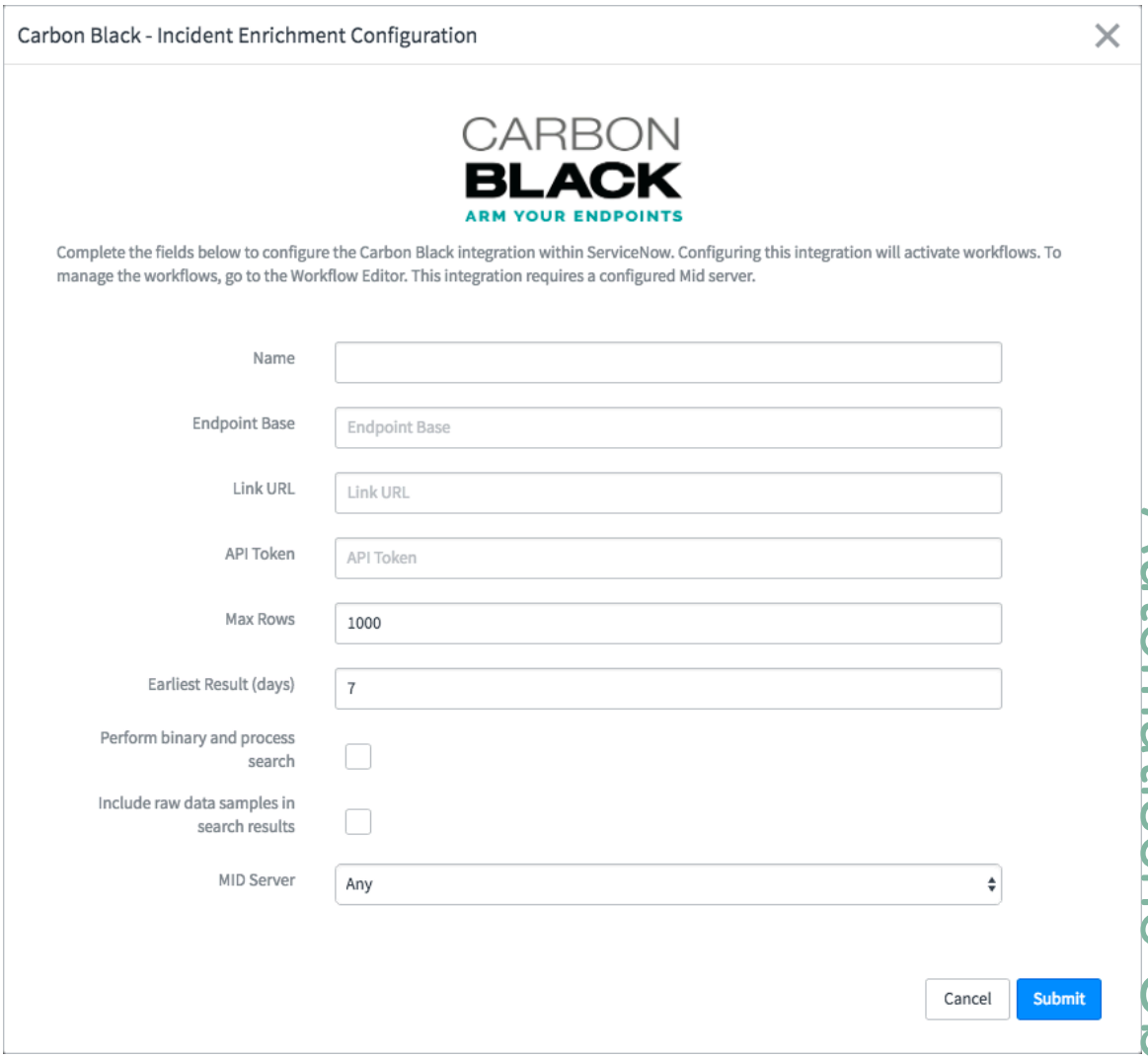
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf zu Carbon Black Website und rufen Sie die Endpunkt-Basis-URL und das API-Token unter Ihrem Profil ab.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. In Carbon Black Karte, klicken Sie auf **Neu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Endpunktbasis	Die Endpunktbasis, die Sie von der Carbon Black-Website erworben haben.
API-Token	Das API-Token, das Sie von der Carbon Black-Website erworben haben.
MID-Server verwenden	Aktivieren Sie dieses Kontrollkästchen, wenn es nicht bereits aktiviert ist.
MID-Server	Wählen Sie Aus **Beliebig** Um einen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.
Hostisolierung aktivieren	Aktivieren Sie dieses Kontrollkästchen, damit ausgewählte Konfigurationselemente von isoliert werden können **Konfigurationselemente** Registerkarte „zugehörige Liste“ in einem Security Incident.

Hinweis:
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Navigieren Sie zum Verwalten der Workflows zu **Workflow-Editor** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie aus **Nein** Von **Konfigurationen Anzeigen** Dropdown-Liste.

Integration mit Check Point Anti-Bot - Email Parser

Die Integration von Check Point Anti-Bot – E-Mail-Parser wird mit einem E-Mail-Parser unterstützt, der E-Mail-Benachrichtigungen vom Check Point Anti-Bot verwendet, um Security Incidents zu erstellen und Ergänzungs- und Antwort-Workflows zu fördern.

Konfigurieren Sie die Integration von Check Point Anti-Bot – E-Mail-Parser

Die Integration von Check Point Anti-Bot – E-Mail-Parser verwendet E-Mail-Benachrichtigungen, um Ergänzungs- und Antwort-Workflows zu fördern.

Vorbereitungen

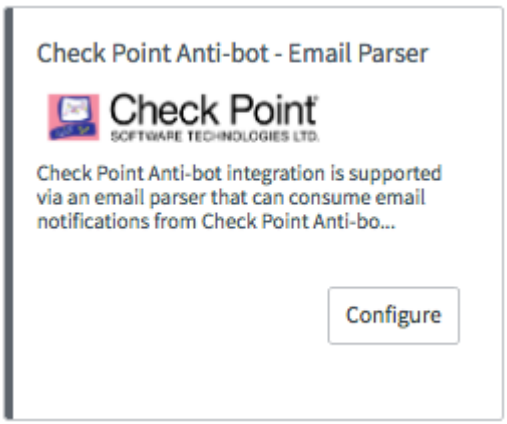
Erforderliche Rolle: sn_si_admin

Warum und wann dieser Vorgang ausgeführt wird

Eine Vorlage für Check Point Anti-Bot-E-Mail-Parser wird zur Verwendung für die Integration bereitgestellt. Sie muss konfiguriert und aktiviert werden, bevor die Integration stattfindet. Durch das Aktualisieren des Parsers wird er aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.



2. Klicken Sie auf der Karte Check Point Anti-Bot – E-Mail-Parser auf **Konfigurieren** .
3. In **Check Point Anti-Bot – E-Mail-Parser-Konfiguration** Klicken Sie auf das Dialogfeld **Konfigurieren Sie Den E-Mail-Parser** Link.
4. Klicken Sie auf **Check Point Anti-Bot** Link zum Bearbeiten der Einstellungen im bereitgestellten Vorlagen-E-Mail-Parser.
   Füllen Sie mindestens aus E-Mail ist von Feld. Informationen zum Erstellen eines E-Mail-Parsers finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
5. Überprüfen Sie **Aktiv** Feld.
6. Klicken Sie Auf **Aktualisieren** In **E-Mail-Parser** Formular.
   Der E-Mail-Parser ist aktiv. Sie müssen nicht zu zurückkehren **Integrationskonfigurationen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Check Point Next Generation Threat Prevention-Integration

In diesem Dokument werden die Schritte beschrieben, die für die Integration von NGTP-Fähigkeiten (Check Point Next Generation Threat Prevention) in erforderlich sind ServiceNow® Security Incident Response(SIR) damit Anwendungen ordnungsgemäß zusammen funktionieren.

Nach der Installation und Konfiguration verwendet der Security Incident-Analyst diese Integration, um schädliche IP-Adressen, URLs und Domänen mithilfe der Funktionen „Liste blockieren“ mit zu blockieren ServiceNow Security Incident Response(SIR) Produkte. Diese Sperranforderungsliste ist in Prüfpunkt-Gateways als anwenderdefinierter Intelligence-Feed konfiguriert. Die Funktion „Anwenderdefinierte Intelligence-Feeds“ bietet die Möglichkeit, anwenderdefinierte Cyber-Intelligence-Feeds der Next Generation Threat Prevention-Engine hinzuzufügen. Ermöglicht das Abrufen von Feeds von einem Drittparteiserver, in diesem Fall von ServiceNow Security Incident Response Anwendung direkt zum Check Point Next Generation Gateway, das von Anti-Virus- und Anti-Bot-Blades erzwungen wird. Der Security Incident Response-Analyst erstellt Einträge für die Checkpoint-Sperrliste aus erkennbaren Elementen, die für schädlich ermittelt wurden ServiceNow SIR Security Incidents.

Bei den meisten Implementierungen ist eine Sperranforderungsliste eine CSV-Datei, die auf einem externen Webserver gehostet wird. Für diese Integration ist dieser Webserver Ihr ServiceNow AI Platform Instanz, die es der Prüfpunkt-Engine der nächsten Generation ermöglicht, die Liste der zu blockierenden IP-Adressen, URLs und Domänen abzurufen.

Um die blockierenden erkennbaren Elemente im Prüfpunkt-Gateway zu erzwingen, stellen Sie sicher, dass die Richtlinie zur Bedrohungsprävention mit aktivierten Anti-Bot- und Anti-Virus-Blades konfiguriert ist. Wenn die Blocklisteneinträge geändert werden, importiert die Threat Prevention-Engine die Liste dynamisch im konfigurierten Intervall und erzwingt die Richtlinie ohne Konfigurationsänderung oder Commit in der Firewall. Für diese Integration ServiceNow AI Platform Hat eine Tabelle erstellt, die Blocklisteneinträge enthält, die von einem autorisierten Prüfpunkt-Gateway der nächsten Generation in den konfigurierten Abrufintervallen abgerufen werden.

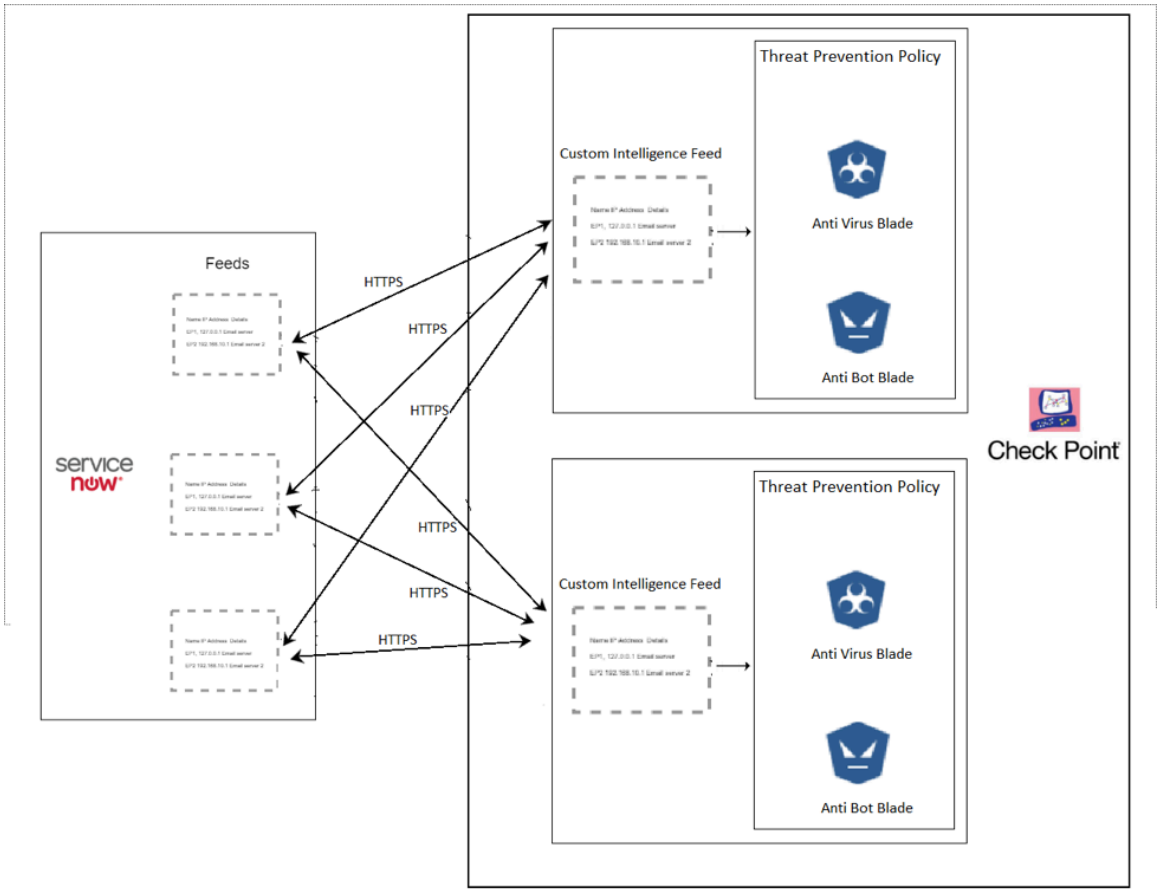
Die Integration umfasst die folgenden Funktionen:

- Flexibilität zum Erstellen mehrerer Blocklisten, die für mehrere Prüfpunkt-Gateways gelten.
- Detaillierte Berichterstellung zu den Arten der blockierten Websites (Phishing, Malware und zulässige Websites).
- Tagging von ServiceNow AI Platform Security Incidents mit Sperrlisteneinträgen nach erkennbarem Typ (URL, Domäne, IP-Adresse).
- Konfigurieren von Ablaufzeiträumen für Sperrlisten, um die Größe der Sperrliste beizubehalten, indem ältere Einträge automatisch ablaufen oder entfernt werden.
- Blocklisteneinträge zwischen verschiedenen Blocklisten werden gesucht.
- Verknüpfen von Blocklisteneinträgen mit Datensätzen erkennbarer Elemente und Security Incidents, die Threat Intelligence-Ergebnisse und Details dazu enthalten, warum ein Eintrag blockiert ist.

Diagramm der Integrationsarchitektur

Unten finden Sie das allgemeine Architekturdiagramm, das die beteiligten Komponenten und Integrationspunkte zwischen NOW Platform und Check Point-Systemen darstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Das Check Point Systems-Logo, das Anti-Virus-Blade-Image und das Anti-Bot-Blade-Image stammen von Check Point Systems ©. Sie sind die Eigenschaft von Prüfpunktsystemen.

Plugins

Die Integration erfordert, dass Security Incident Response(com.snc.security_incident) Plugin aktiviert sein.

Zur Installation Security Incident Response Plugins:

1. Melden Sie sich mit Ihren HI-Anmeldeinformationen bei Ihrer Instanz an.
2. Stellen Sie sicher, dass Sie über die Administratorrolle (Administrator) verfügen.
3. Navigieren Sie in Ihrer Instanz zu Systemdefinition>Plugins.
4. Wählen Sie Security Incident Response aus, und klicken Sie auf Security Incident Response.

Sobald diese Plugins installiert wurden, können Sie das neue Plugin für die Check Point-Integration aus dem ServiceNow Store hochladen und die folgenden Konfigurationsanweisungen befolgen.

Unterstützte Prüfpunkt-BS-Versionen

Diese Integration erfordert den anwenderdefinierten Intelligence-Feed von Check Point- und Anti-Bot- und Anti-Virus-Blades. Diese werden ab R80.20 unterstützt. Installieren Sie den Hotfix der Funktion „Anwenderdefinierte Intelligenz“, bekannt als Prüfpunkt R80.10 Jumbo HF Take 121 und höher. Weitere Informationen zur Produktkompatibilitätsmatrix

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

finden Sie im Abschnitt Installation der Dokumentation zum Prüfpunkt-Feed für anwenderdefinierte Intelligenz.

https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Stellen Sie nach der Installation des Hotfix sicher, dass die folgenden Befehle im Check Point Gateway zugänglich sind. SSH beim Gateway und melden Sie sich im Expertenmodus an.

```
[gw-93440b> expert
[Enter expert password:


Warning! All configurations should be done through clish
You are in expert mode now.

[[Expert@gw-93440b:0]# ioc_feeds --help
External indicators configuration

positional arguments:
  show, add, delete, modify
                        Select an action for the external indicators configurations

optional arguments:
  -h, --help            show this help message and exit
  --feed_name           Set feed name
  --transport           Set feed transport protocol: http, https, local_file, local_directory
  --resource            Set feed resource URL
  --state               Set feed enforcement Active / Inactive
  --feed_action         Set feed action: Prevent, Detect, Ask
  --proxy               Set feed proxy
  --proxy_user_name     Set feed proxy user name
  --user_name           Set user name for remote feed
  --test                Set test as true if feed is for testing purposes only
  --format [ [ ...]]    Enter format in order to fetch custom csv file
  --delimiter           Enter delimiter in order to fetch custom csv file
  --comment [ [ ...]]   Enter comment char in order to fetch custom csv file
Missing a few arguments.
[Expert@gw-93440b:0]#
```

Unterstützte ServiceNow-Versionen

San Diego-Release-Version oder höher wird unterstützt.

Referenzen

Im Folgenden finden Sie einige der Prüfpunktreferenzen, die beim Einrichten der Voraussetzungen nützlich sind.

1. Anwenderdefinierte Intelligence-Feeds-Funktion – https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193
2. Informationen zum Einrichten von Anti-Bot- und Anti-Virus-Blades finden Sie im Prüfpunkt-Benutzerhandbuch. http://downloads.checkpoint.com/dc/download.htm?ID=46534
3. Um die HTTPS-Inspektion am Prüfpunkt einzurichten, folgen Sie dem folgenden Link. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk108202

Berechtigungen und Rollen

Die folgenden ServiceNow-Rollen sind erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Administrator (Administrator) für die Installation des Plugins der Integrationsanwendung
- Security Incident-Administrator (sn_si.admin) zum Erstellen von Blocklisten in ServiceNow und zum Genehmigen von Anforderungen zum Hinzufügen und Deaktivieren von Blocklisteneinträgen.
- Sicherheitsanalyst (hier auch als SOC-Analyst, sn_si.Analyst bezeichnet) für die Erstellung und Verwaltung von Blocklisteneintragsdatensätzen.

Weitere Informationen zum Zuweisen der Sicherheitsanalystenrolle finden Sie im ServiceNow-Dokumentationswebsite , Navigieren Sie zu Security Operations>Security Incident Response> Sicherheitsanalysten zuweisen.

Setup von Check Point NGTP

Bevor Sie verwenden können Check Point NGTP Integration müssen Sie einen API-Account erstellen, Richtlinien einrichten und die Integration aktivieren.

Erstellen Sie einen API-Account für Check Point NGTP Integration

In ist eine API-Account-Rolle erforderlich ServiceNow AI Platform Instanz für diese Integration. Der Anwendername und das Passwort, die diesem Account zugeordnet sind, werden in erstellt ServiceNow AI Platform Und in Prüfpunkt eingegeben, damit sich der Prüfpunkt mit authentifiziert ServiceNow AI Platform Beim Abrufen von Blocklisteneinträgen.

Vorbereitungen

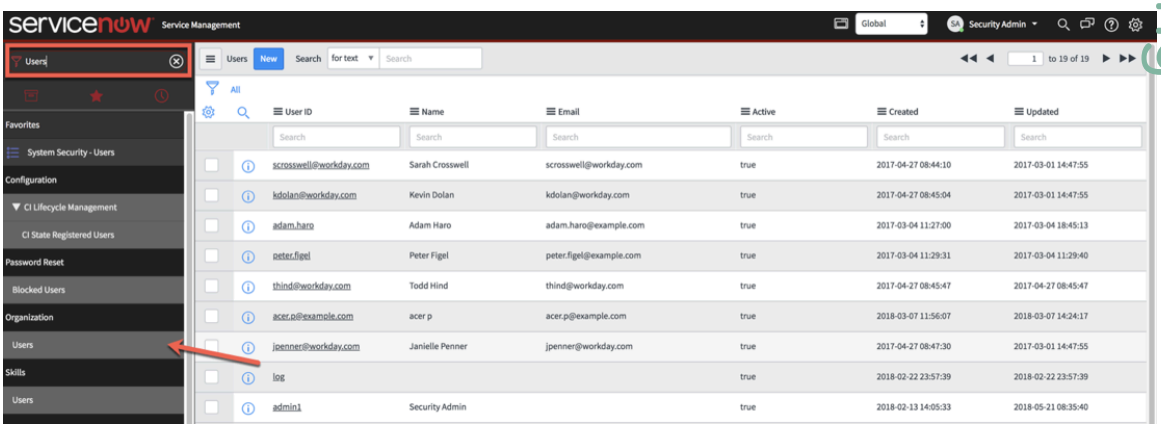
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die ServiceNow AI Platform der administrator erstellt eine API-Account-Rolle (sn_sec_Checkpoint.api_Account_Access). Dieser Account wird ausschließlich für die Eingabe von Anmeldeinformationen verwendet, die für die Authentifizierung am Prüfpunkt erforderlich sind, sodass das Gateway Sperrlisten aus dem abrufen kann ServiceNow AI Platform. Dieser Account ist ein separater, eindeutiger API-Anwenderaccount in ServiceNow AI Platform Instanz und dem Prüfpunkt-Administrator zugewiesen.

Prozedur

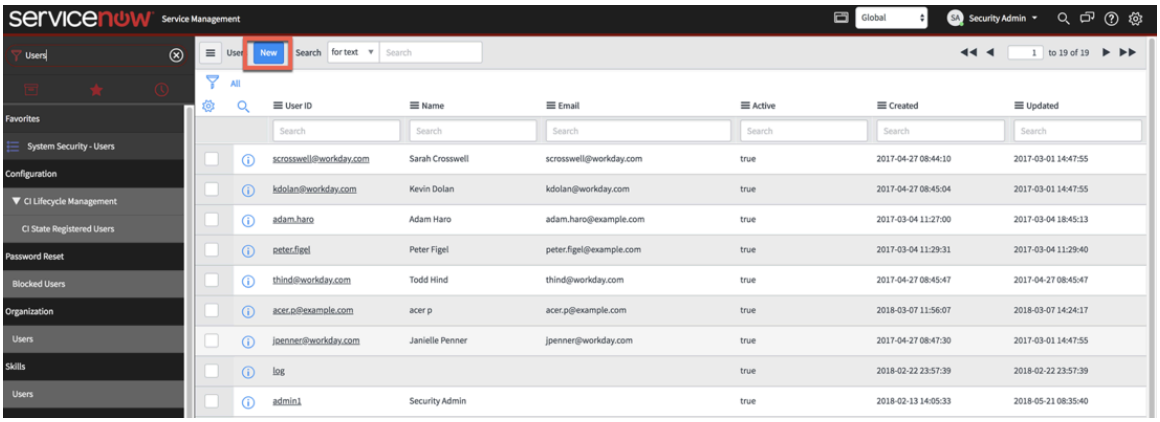
1. Navigieren zu **Alle** > **Organisation** > **Anwender**an.
2. Klicken Sie auf **Anwender** Modul.



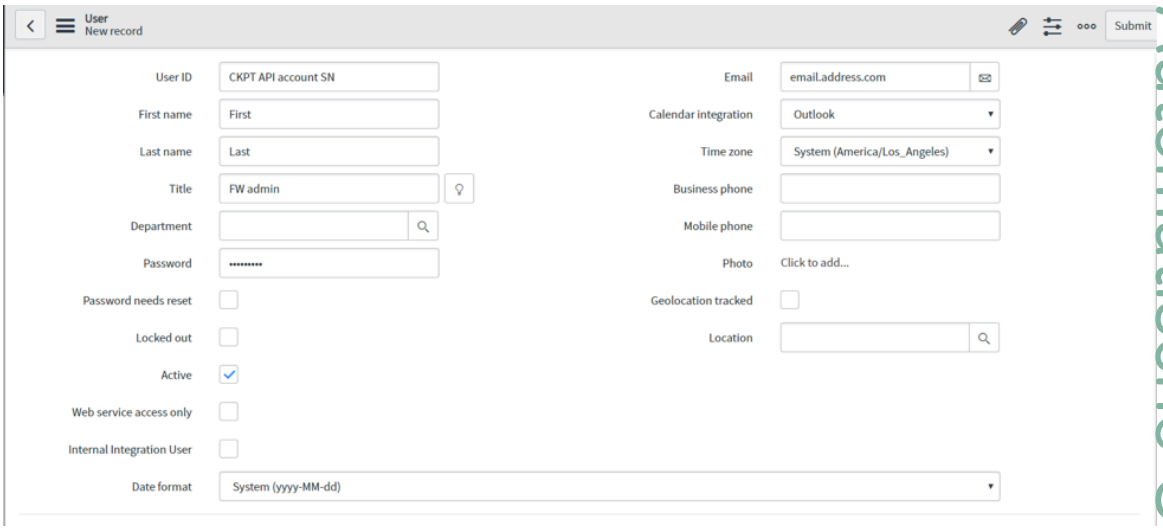
3. Klicken Sie in der angezeigten Liste Anwender auf **Neu** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ein neues Formular wird angezeigt.



4. Füllen Sie das Formular nach Bedarf aus.

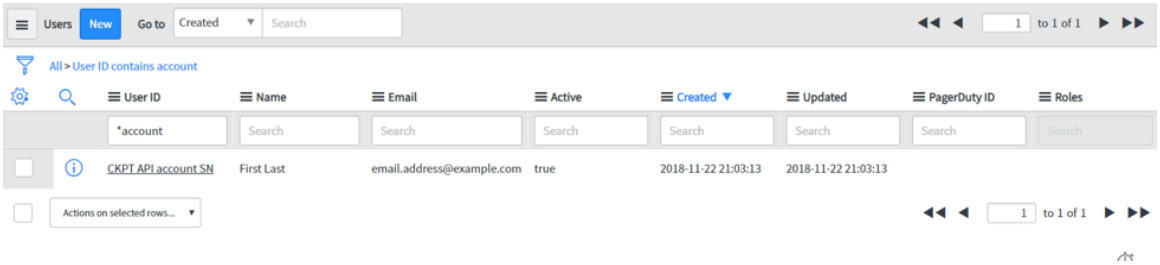
> **Hinweis:**
> Die in der folgenden Tabelle und Abbildung angezeigten Werte für Anwender-ID-Titel und E-Mail-Adresse sind Beispielwerte.

Feld	Beschreibung
Anwender-ID	Eindeutige Anwender-ID für die Rolle in Ihrem ServiceNow AI Platform Instanz. Diese Anwender-ID wird in eingegeben **Anwendername** Feld in **Client-Authentifizierung** Abschnitt des Gateway zum Prüfen des Konfigurationspunkts der Blockliste. Ein Beispiel ist die CKPT-API-Account-SN.
Vorname	Person, die Sie zuweisen
Nachname	Person, die Sie zuweisen
Titel	Stellenbezeichnung, z. B. FW-Administrator.
Passwort	Eindeutiges Passwort, das für diese Rolle erstellt wurde. Dieses Passwort wird in eingegeben **Passwort** Feld in **Client-Authentifizierung** Abschnitt der Blocklistenkonfiguration für Prüfpunkt-Gateway.
E-Mail	Eindeutige E-Mail-Adresse

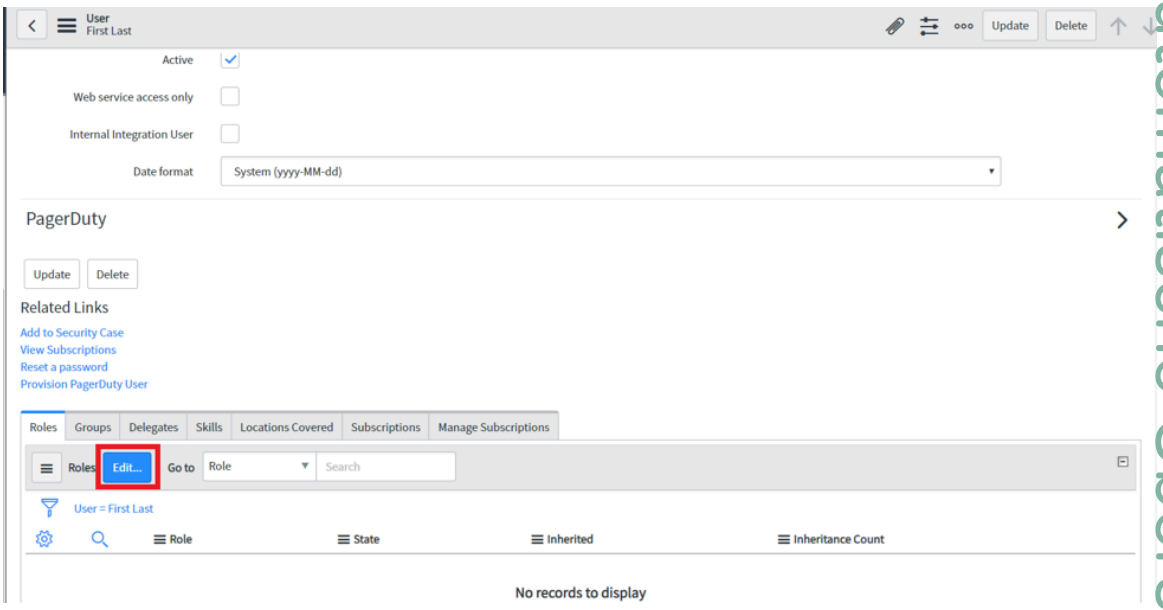
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Absenden**.
   Nach der Übermittlung können Sie die Rolle zuweisen.
6. Klicken Sie in der Liste Anwender in der Spalte Anwender-ID auf den Namen der von Ihnen eingegebenen Anwender-ID, z. B. CKPTAPI-Account-SN.



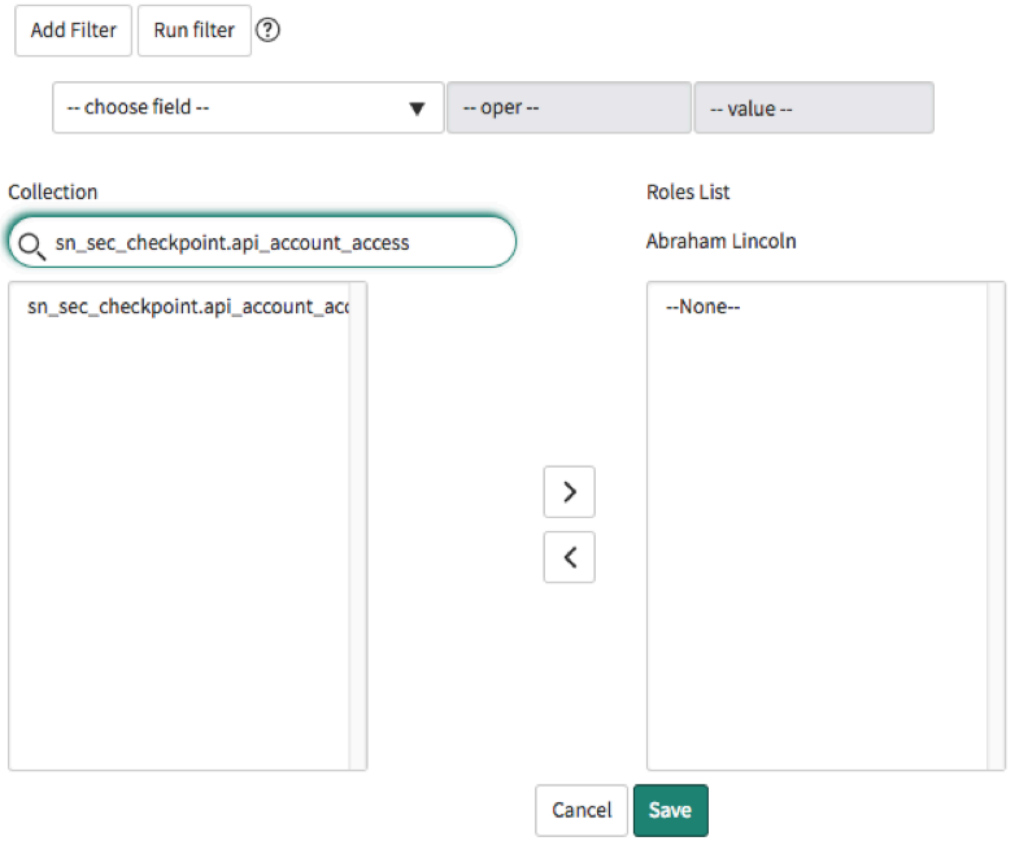
7. Klicken Sie im Abschnitt „Rollen“ im Datensatz öffnen auf **Bearbeiten** .



8. Auf der **Bearbeiten Sie Mitglieder** Formular, das angezeigt wird, geben Sie sn_sec_Checkpoint.api_Account_Access in ein **Sammlung** Feld.

Automatische Übersetzung

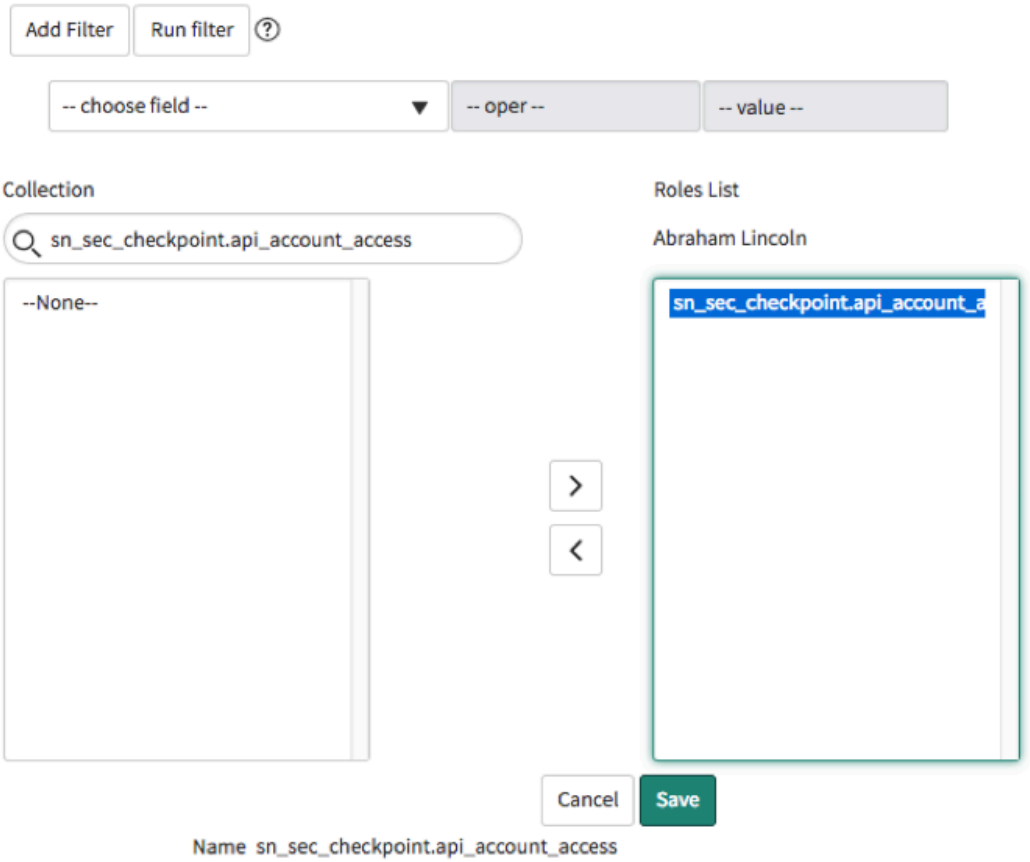
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. In **Sammlung** Wählen Sie die Spalte aus, und verschieben Sie dann sn_sec_Checkpoint.api_Account_Access in **Rollenliste** .
10. Klicken Sie auf **Speichern**.
11. Navigieren Sie zu **Anwender** , Und in **Anwender** Klicken Sie in der Liste auf den ID-Namen, den Sie für die Rolle erstellt haben (CKPT API-Account SN).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



12. Der Anwenderdatensatz wird angezeigt. Dieser Datensatz verifiziert, dass der Anwenderaccount zugewiesen wurde.

Integration mit Check Point NGTP einrichten

Führen Sie die folgenden Schritte aus, um einzurichten Check Point Next Generation Threat Prevention Integration. Dadurch wird sichergestellt, dass die Voraussetzungen für die Integration vorhanden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Überprüfen Sie, ob die Richtlinie zur Bedrohungsvorbeugung mit aktivierten Anti-Bot- und Anti-Virus-Blades konfiguriert ist.
   Ausführliche Informationen zum Einrichten von Anti-Bot- und Anti-Virus-Blades finden Sie im Prüfpunkt-Anwenderhandbuch, das im Abschnitt „Referenz“ erwähnt wird.

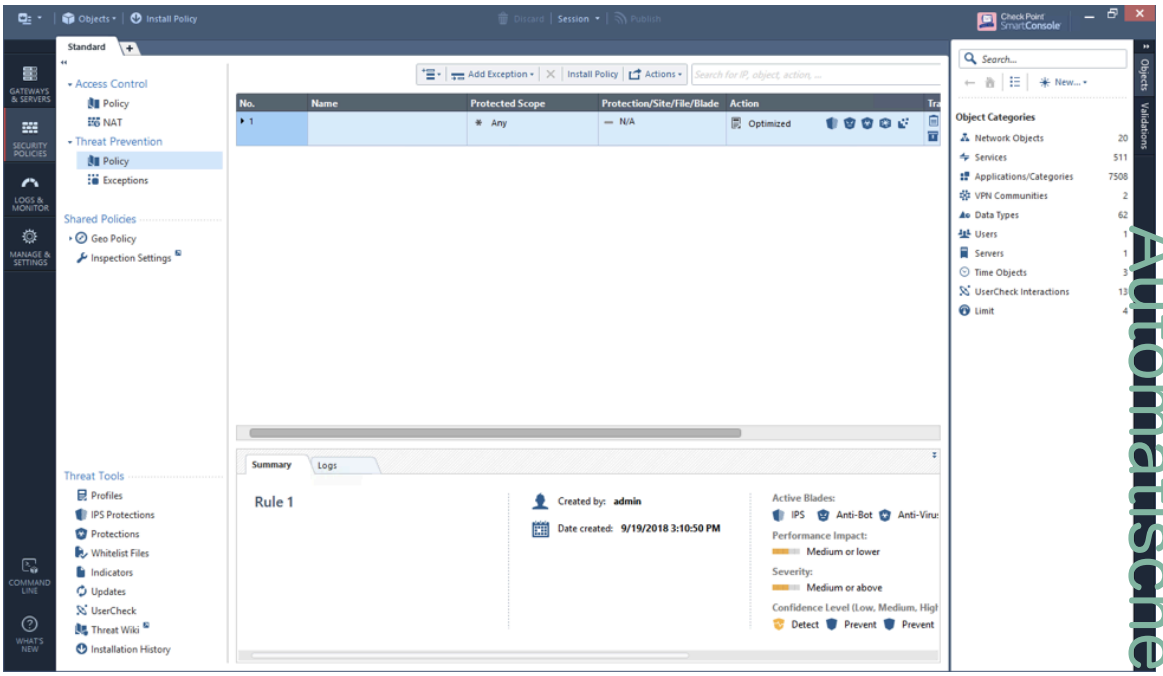
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

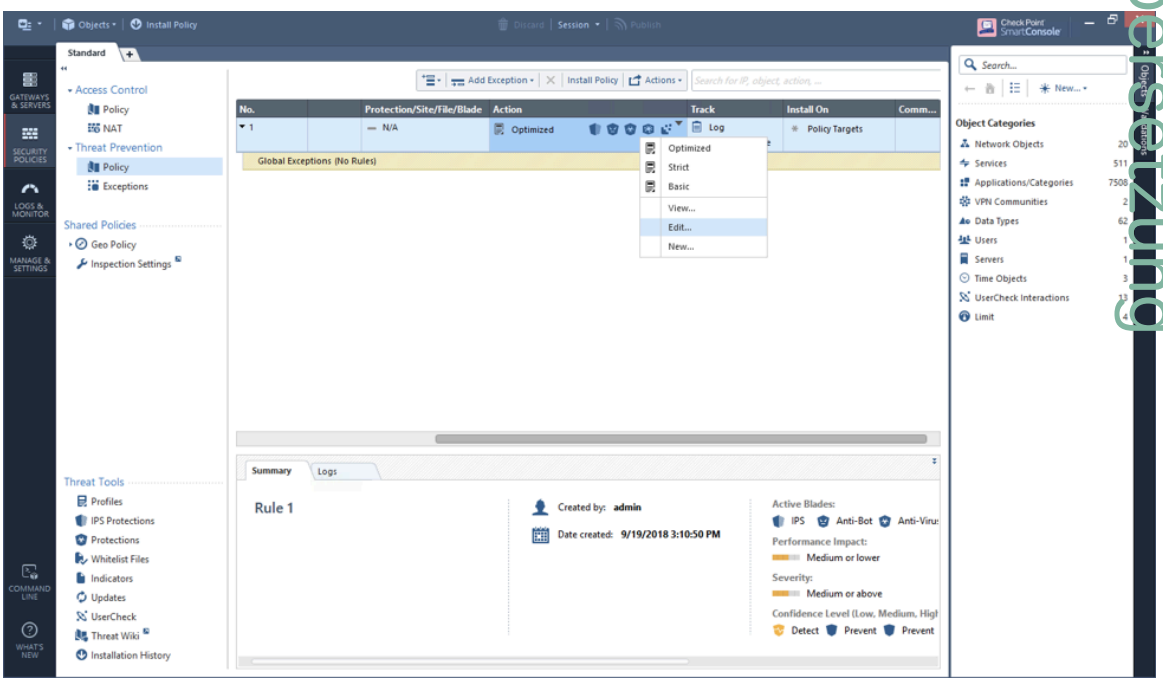
Hinweis:
Die Images in diesem Thema sind privilegiert und proprietär und werden mit der Berechtigung von Check Point Software Technologies, Ltd. Verwendet

a. Melden Sie sich bei an **Intelligente Konsole** .

b. Navigieren zu **Sicherheitsrichtlinien** > **Bedrohungsvorbeugung** > **Richtlinie**an.



c. Öffnen Sie die Richtlinie zur Bedrohungsprävention im Bearbeitungsmodus.



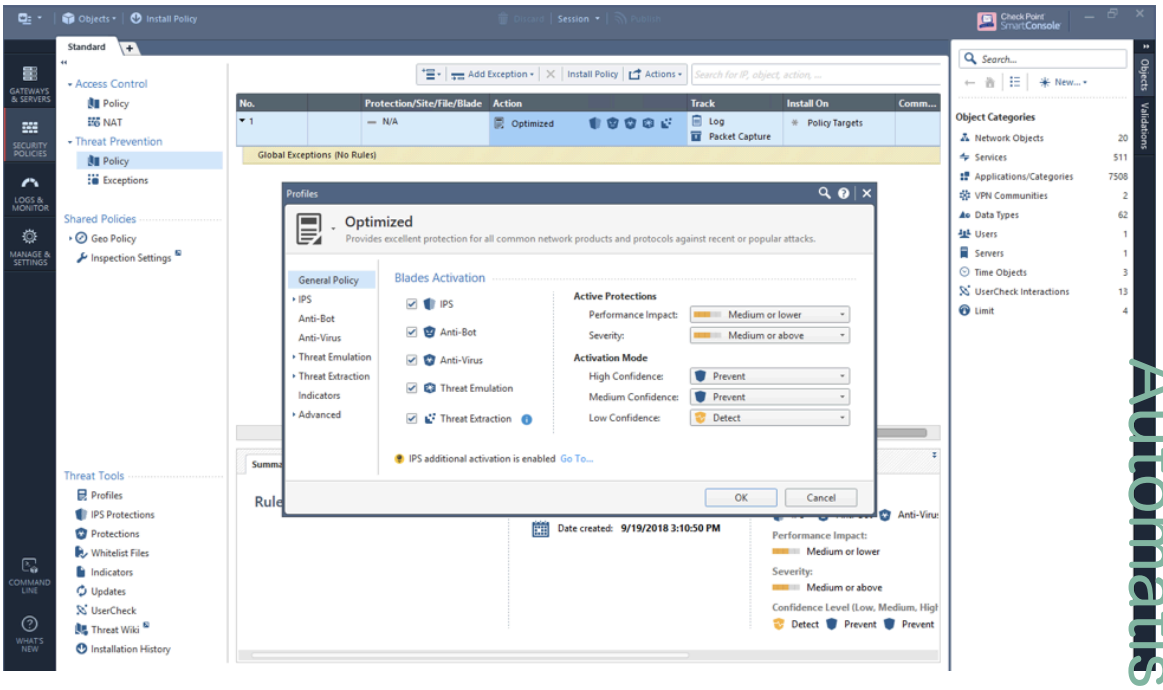
d. Aktiver Schutz # Schweregrad muss „Mittel oder höher“ sein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Aktivierungsmodus # hohe Konfidenz muss „verhindern“ sein.

f. Blades-Aktivierung à Anti-Virus und Anti-Bot müssen ausgewählt werden.



g. Veröffentlichen Sie die Änderungen (falls vorhanden), und installieren Sie die Richtlinie.

2. Wenn nicht bereits konfiguriert, sollten anwenderdefinierte Intelligence-Feeds nach der Aktivierung von Anti-Bot- und Anti-Virus-Blades hinzugefügt werden.
Weitere Informationen finden Sie im Abschnitt „Installation“ der Dokumentation zur anwenderdefinierten Intelligence-Feed-Funktion „Prüfpunkt“. https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

3. Wenn nicht bereits konfiguriert, richten Sie das Prüfpunkt-Gateway ein, um den gesamten Internetverkehr über HTTP-Proxy weiterzuleiten (wenn HTTPS-Inspektion konfiguriert wird).

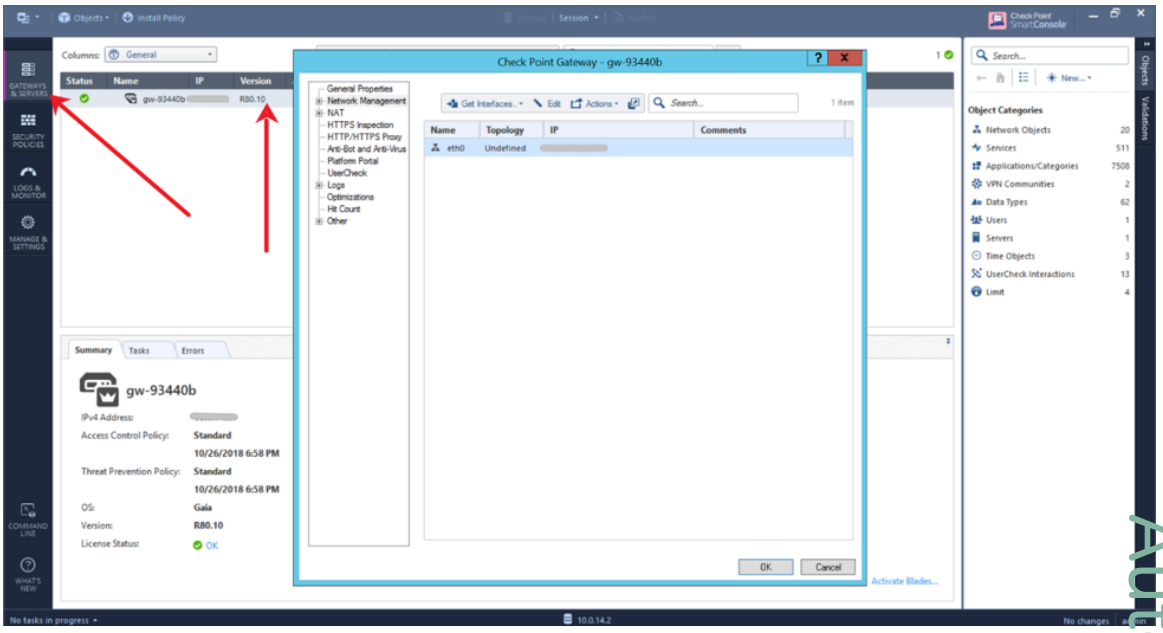
Hinweis:
Für die URL-Blockierung auf Prüfpunkt-NGTP gibt es bestimmte Einstellungen, die sichergestellt werden müssen. HTTPS-Internetverkehr verwendet das SSL-Protokoll (Secure Sockets Layer) und ist verschlüsselt, um Datenschutz zu gewährleisten. HTTPS kann jedoch schädlichen Datenverkehr ausblenden, der hätte blockiert werden sollen. Damit Check Point Gateway Transparenz in HTTPS-Datenverkehr erhält, leiten Sie den Datenverkehr entweder über HTTP-Proxy weiter, oder richten Sie HTTPS-Inspektion (empfohlen) ein. In diesem Abschnitt werden die Schritte zum Einrichten des HTTP-Proxys im Prüfpunkt-Gateway beschrieben.

a. Melden Sie sich bei an **Intelligente Konsole** .

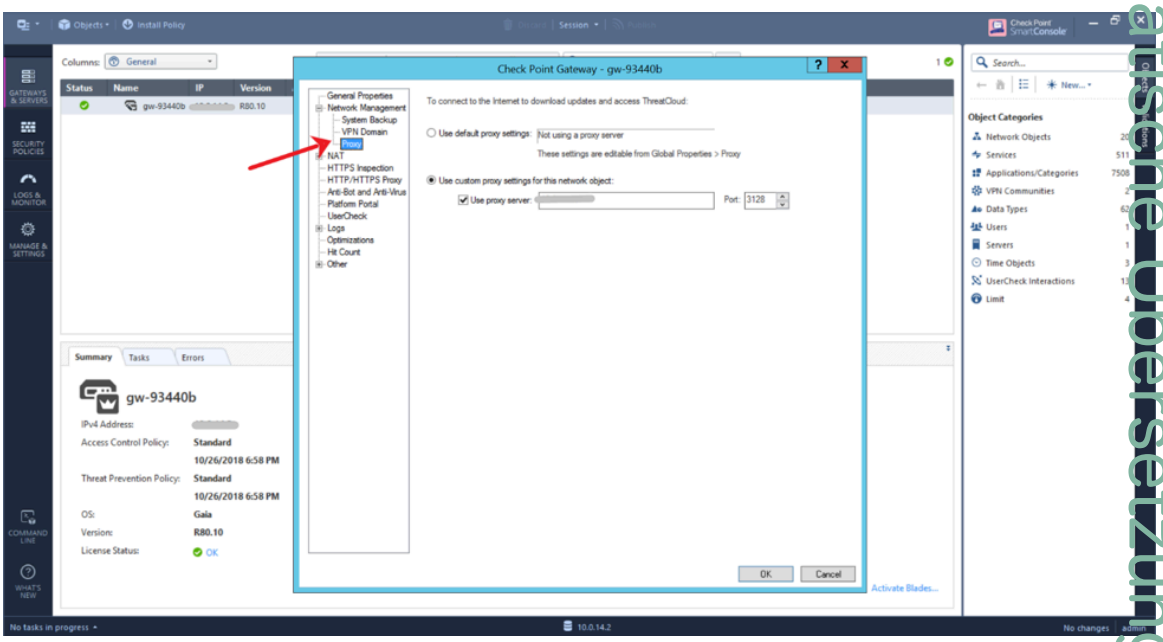
b. Navigieren Sie zu **Server und Gateways** , Und doppelklicken Sie auf den entsprechenden Server.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Navigieren zu **Netzwerkverwaltung** > **Proxy**an.



d. Geben Sie die Proxy-Details an, die für die Weiterleitung des HTTP-Datenverkehrs verwendet werden sollen.

e. Stellen Sie sicher, dass HTTP-Anforderungen vom Clientendpunkt über den HTTP-Proxy erfolgen.

4. Wenn nicht bereits konfiguriert, aktivieren Sie die HTTPS-Inspektion (wenn HTTP-Proxy konfiguriert ist). Wenn der meiste Datenverkehr über SSL erfolgt, wird die Verwendung des HTTPS Inspection Blade empfohlen. Dadurch wird der Datenverkehr für GW transparent. Aktivieren Sie die HTTPS-Inspektion für das Prüfpunkt-Gateway wie folgt.

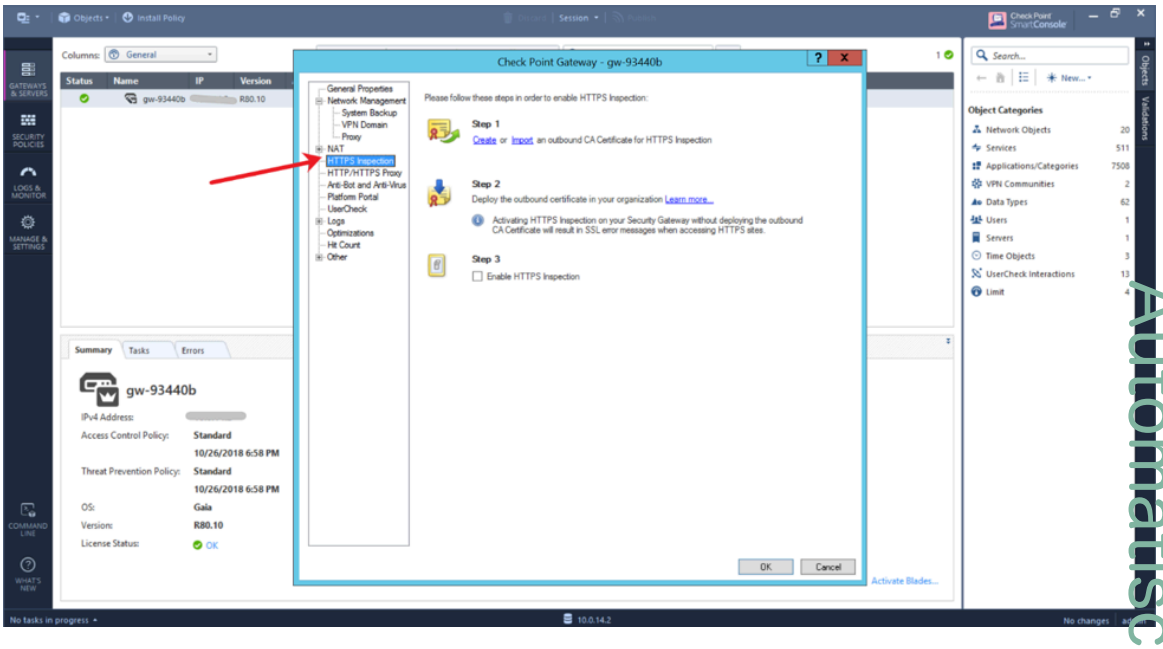
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Melden Sie sich bei an **Intelligente Konsole** .

b. Navigieren Sie zu **Server und Gateways** , Und doppelklicken Sie auf den entsprechenden Server.

c. Navigieren Sie zu **HTTPS-Inspektion** .



d. Folgen Sie dem Schritte zum Konfigurieren der HTTPS-Inspektion Im Prüfpunkt-Anwenderhandbuch.

Aktivieren Sie Check Point NGTP Integration

Wenn Sie die Anwendung nicht installiert haben, befolgen Sie die Anweisungen, um sie zu installieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei der Instanz an, auf der Sie die Anwendung installieren möchten.
2. Navigieren zu **Systemanwendungen** > **Anwendungen**an.
3. Klicken Sie auf **Downloads** Registerkarte.
   Eine Liste der Anwendungen, die für die Installation verfügbar sind, wird angezeigt.
4. Suchen Sie nach Check Point Next Generation Threat Prevention Anwendung, wählen Sie sie aus, und klicken Sie auf **Installieren** .
   Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Arbeiten mit Sperrlisten

Die ServiceNow Check Point Next Generation Threat Prevention Die Integration unterstützt Blocklisten, die erkennbare Elemente für IP, URL und Domäne akzeptieren.

ServiceNow Die konfigurierte Blockliste ist eine CSV-Datei, die auf einem externen Webserver gehostet wird, der für diese Integration der ist ServiceNow AI Platform Instanz. Anwenderdefinierter Intelligence-Feed wird im Prüfpunkt-Gateway konfiguriert, das die IP-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Adressen, URLs und Domänen aus dem abruft ServiceNow AI Platform Im vorkonfigurierten Intervall.

Diese Integration unterstützt drei Arten von Blocklisten:

- IP-Adresse (umfasst eine einzelne IP-Adresse (nur IPv4) für die Sperrliste und CIDR-Blöcke (Adressbereiche) für die Allow-Liste).
- URL
- Domäne

Erkennbare Elemente, die von unterstützt werden Check Point NGTP Integration

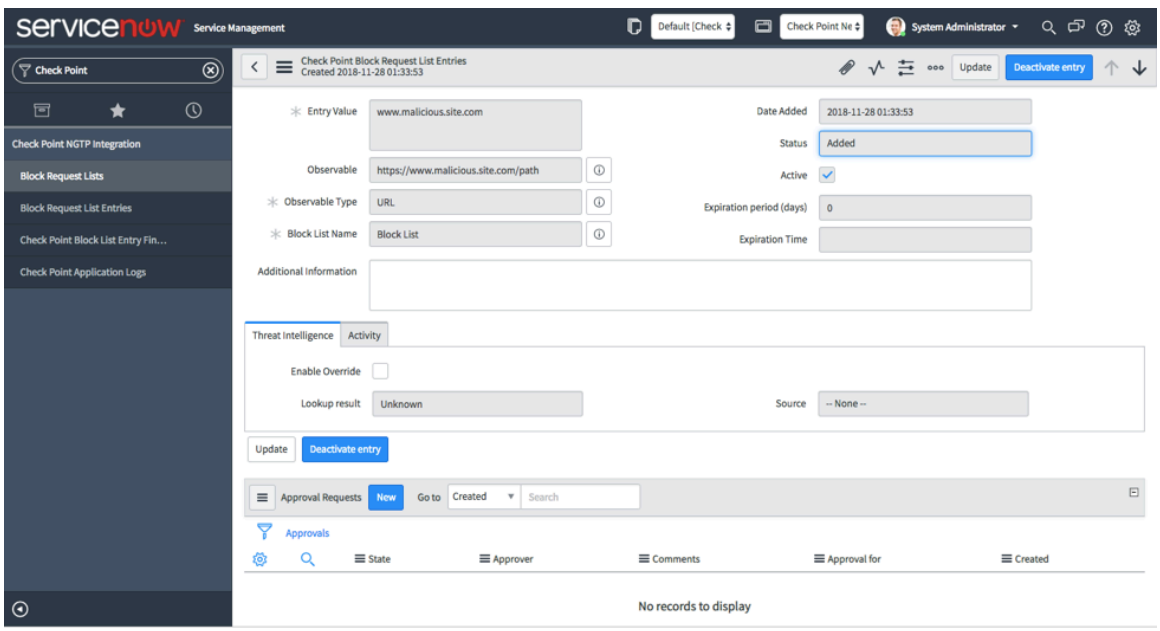
Der Abschnitt listet Beschreibungen der von dieser Integration unterstützten erkennbaren Elemente und Beispielformate für jeden Typ auf.

Erkennbarer Typ	Beispiele	Beschreibung
Domäne	• example.com • mail.example.com	Platzhalter werden nicht unterstützt.
IP-Adresse	95.153.103.54 (IPv4)	Stellt eine einzelne, eindeutige Schnittstellenadresse dar. Die Integration unterstützt nur IPv4- und CIDR-Formate (das CIDR-Format wird nur für die Zulässigkeit der Auflistung unterstützt). Für den Zweck der Allow-Liste bietet die Integration Unterstützung für erkennbare IP-Adressen, einschließlich CIDR-Bereiche (Classless Inter-Domain Routing), z. B. 95.153.100.0/22. **Hinweis:** Eine Fehlermeldung wird angezeigt, wenn Sie versuchen, eine einzelne IP-Adresse an eine Sperrliste anzuhängen, die Sie bereits als Teil eines CIDR-Bereichs aufgeführt haben. Beispielsweise ist die einzelne Adresse 95.153.103.54 Teil des CIDR-Bereichs, der durch 95.153.100.0/22 (95.153.100.0-95.153.103.255) dargestellt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

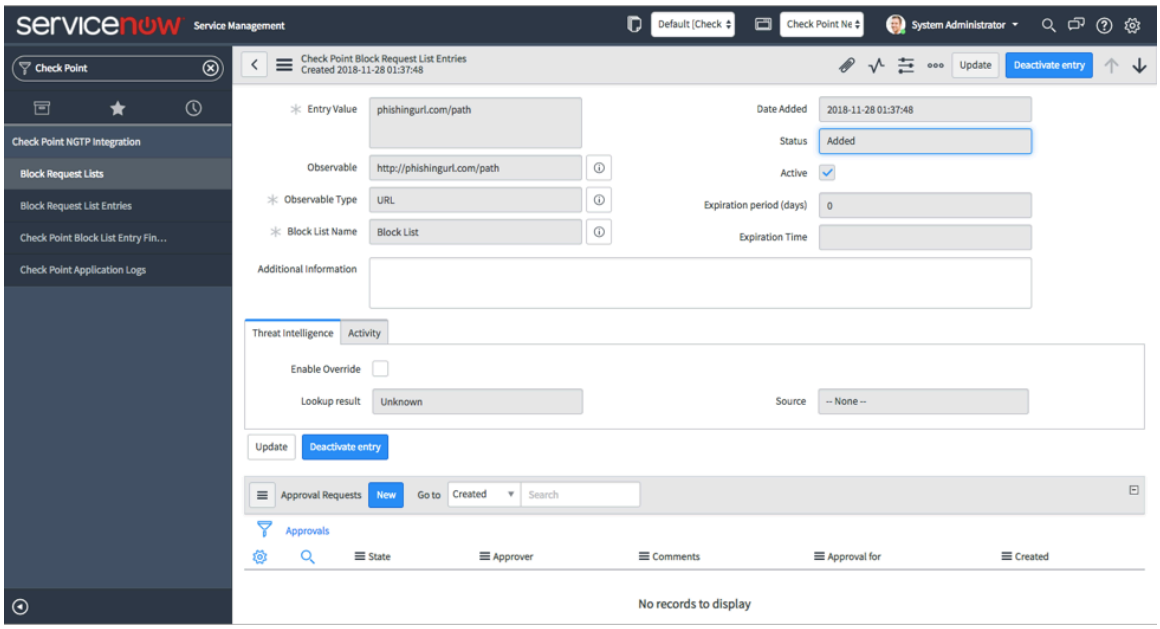
Erkennbarer Typ	Beispiele	Beschreibung
URL	• https://www.example.com • http://www.example.com	Beschreibung: Die HTTPS-URL wird von der Anwendung so formatiert, dass der Pfad von der URL abgeschnitten wird und nur der Domänenname beibehalten wird. Check Point-NGTP basiert auf HTTP-CONNECT-Anforderung, um den Webverkehr zu bewerten und die Blockierung zu erzwingen. Bei der HTTPS-CONNECT-Anforderung ist die gesamte URL in der Anforderung nicht sichtbar, und nur der Domänenname ist sichtbar. Wenn ein Anwender eine HTTPS-URL mit einem bestimmten Pfad blockiert (Beispiel: https://www.example.com/path), kürzt die Anwendung den Pfad automatisch (www.example.com). Die Anwendung behält die Beziehung zwischen dem ursprünglichen erkennbaren Element und der formatierten URL bei. Unten ist der Screenshot des Blocklisteneintrags, der die formatierte URL und das ursprüngliche erkennbare Element anzeigt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei HTTP-URLs mit einem bestimmten Pfad (z. B. http://www.example.com/path) würde der Prüfpunkt die angegebene URL blockieren, da die gesamte URL in der CONNECT-Anforderung sichtbar ist.



Erstellen Sie eine Sperrliste für Check Point NGTP Integration

Erstellen Sie eine Sperrliste in Ihrem ServiceNow AI Platform Instanz. Nach der Genehmigung und Aktivierung können Sie Einträge für diese Sperrlisten aus erkennbaren Elementen erstellen, die für Now Platform Security Incident Response (SIR)-Incidents als schädlich eingestuft wurden, und die Genehmigung zum Blockieren anfordern.

Vorbereitungen

Erforderliche Rolle: Security Incident-Administrator (sn_si.admin)

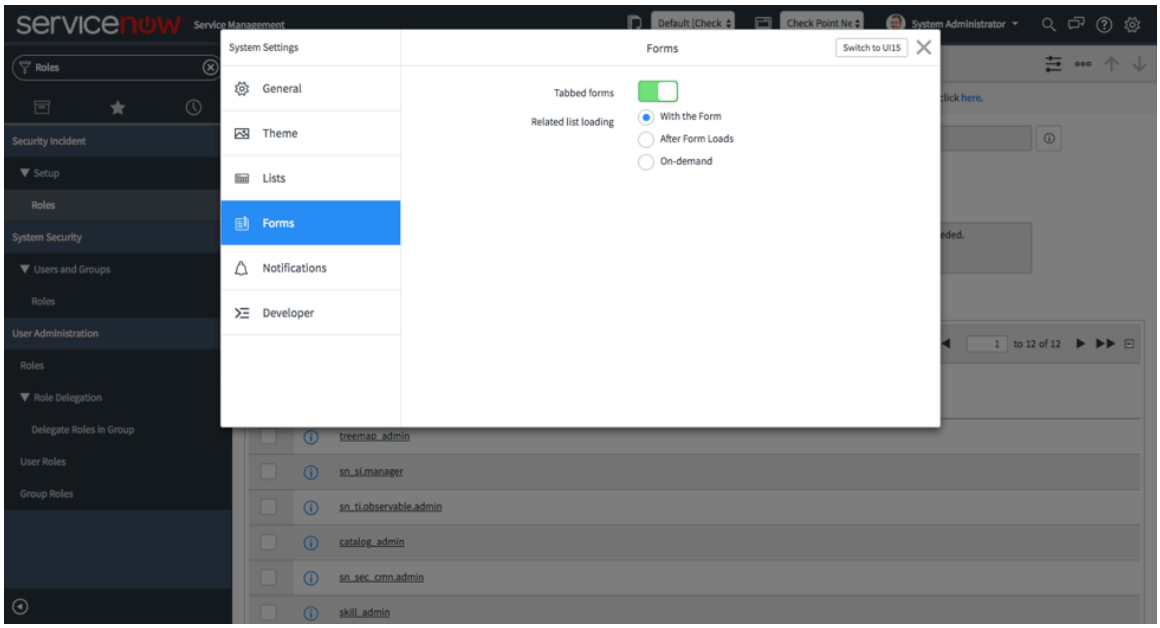
Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie die Sperrliste auf Ihrem ServiceNow AI Platform Instanz, damit der Prüfpunkt in der Liste enthaltene Objekte importieren kann – IP-Adressen, URLs, Domänen. Anwenderdefinierter Intelligence-Feed wird im Prüfpunkt-Gateway konfiguriert, das die IP-Adressen, URLs und Domänen aus der Now-Plattform in vorkonfigurierten Intervallen abruft. Um sicherzustellen, dass die erkennbaren Elemente blockiert werden, sollte die Richtlinie zur Bedrohungsvorbeugung mit aktivierten Anti-Bot- und Anti-Virus-Blades konfiguriert werden.

Hinweis:

Die Zahlen in diesem Thema werden mit angezeigt **Formulare mit Registerkarten** In Systemeinstellungen gelöscht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Prozedur

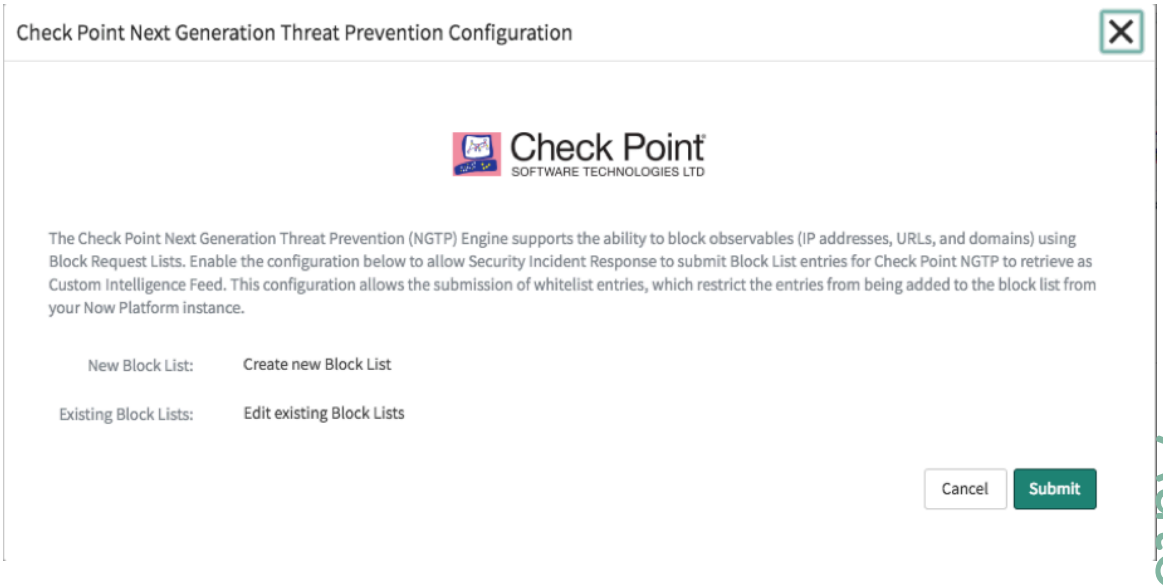
1. Navigieren Sie nach Abschluss der Anwendungsinstallation zu **Integrationen** > **Integrationskonfigurationen**an.
2. Suchen Sie nach **Überprüfen Sie Den Punkt Next Generation Threat Prevention** Karte und klicken Sie auf **Konfigurieren** .

Hinweis:
Privilegierte und proprietäre Inhalte, die mit der Berechtigung von Check Point Software Technologies, Ltd. Verwendet werden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie Auf **Erstellen Sie eine neue Blockliste** .



4. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Name	Name der Sperranforderungsliste des Prüfpunkts. Fügen Sie den Typ des erkennbaren Elements (URL, IP, Domäne) in dieses Feld ein, damit der Sicherheitsanalysten die Absicht der Sperrliste leicht anhand ihres Namens erkennen kann. Der Name sollte auch deutlich angeben, welcher Firewall-Richtlinie diese Blocklistenobjekte zugeordnet sind. Einige Beispiele für Blocklistennamen sind „ausgehende Malware-IP“ oder „ausgehende Phishing-URL“.
Aktiv	Dieses Kontrollkästchen ist standardmäßig deaktiviert, um anzugeben, dass die Sperrliste inaktiv ist. Wenn sie inaktiv ist, kann die Sperrliste keine zusätzlichen Einträge erhalten. Wenn das Kontrollkästchen aktiviert ist (wenn Change-Anforderung geschlossen oder keine Change-Anforderung generiert wird), wird die Sperrliste aktiviert und für Sperrlisteneinträge verfügbar.
Tag anzeigen	Das Kontrollkästchen ist standardmäßig aktiviert, um das erkennbare Element und den zugehörigen Security Incident-Datensatz automatisch zu kennzeichnen, wenn das erkennbare Element in der Sperrliste blockiert ist. Wenn diese Option ausgewählt ist, ist das Feld „Tag für erkennbare Elemente“ im Formular verfügbar. **Hinweis:** Ein Tag-Name wird standardmäßig aus dem Wert erstellt, den Sie im Feld Name mit einem Prüfpunkt-Präfix eingeben, z. B. Prüfpunkt-Malware ausgehende IP. Sie können den Tag-Namen und die Farbe ändern. Der Tag-Name wird im Feld „Tag für erkennbare Elemente“ angezeigt, sobald die Sperrliste gespeichert wurde. Wenn das Kontrollkästchen deaktiviert ist, wird kein Tag erstellt, und das Feld „Tag für erkennbare Elemente“ ist im Formular nicht verfügbar.

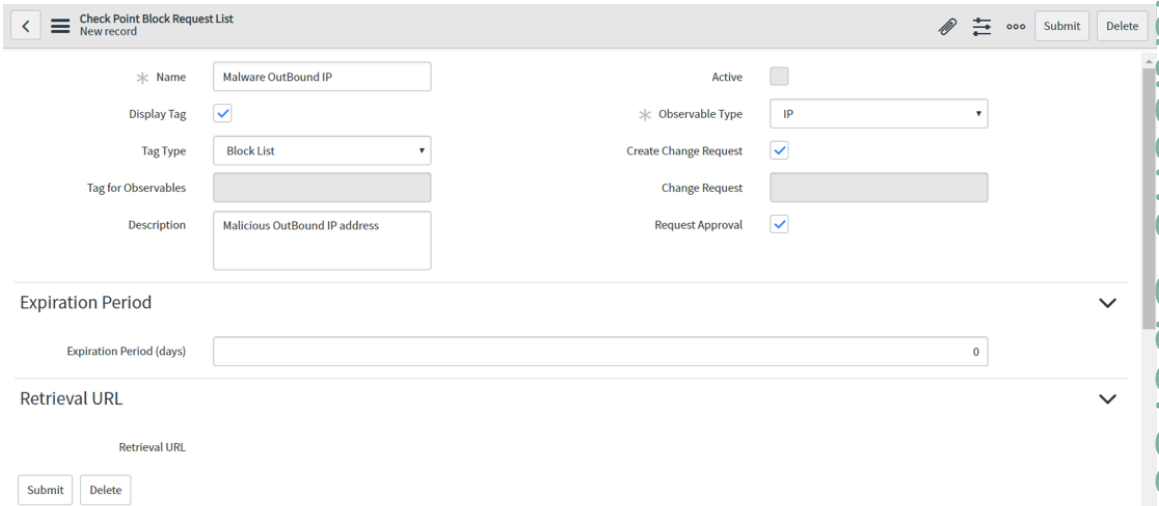
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

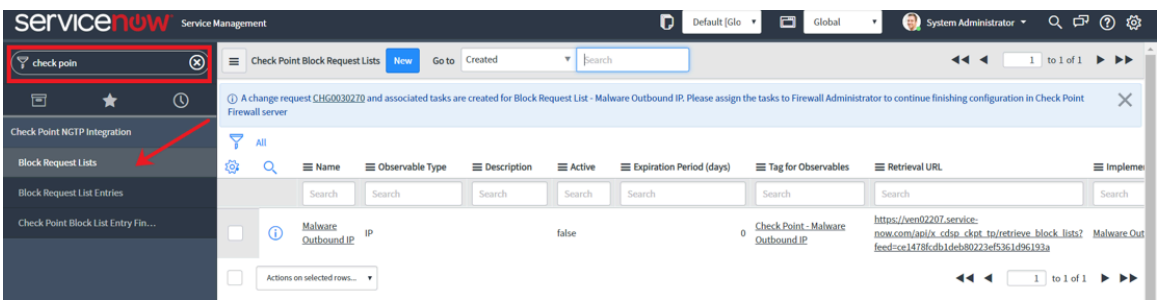
Feld	Beschreibung
Erkennbarer Typ	Wählen Sie einen erkennbaren Typ aus, den diese Blockliste akzeptiert, aus der Liste aus: IP-Adresse (einschließlich CIDR für Allow-Liste), URL oder Domäne.
Tag-Typ	Tags, die in der Liste verfügbar sind. Eine Sperrliste ist eine Liste der erkennbaren Elemente, die der Prüfpunkt Next Generation Threat Prevention blockieren soll. Eine Allow-Liste ist eine Liste von erkennbaren Elementen, die Sie in Check Point Next Generation Threat Prevention in keinem Fall blockieren möchten. Standardmäßig ist die Tag-Farbe „Liste blockieren“ schwarz und die Tag-Farbe „Liste zulassen“ grau. Sie können die Farbe ändern.
Change-Anforderung erstellen	Dieses Kontrollkästchen ist standardmäßig aktiviert, um automatisch eine Change-Anforderung und Change-Aufgaben in zu erstellen ServiceNow AI Platform Instanz, die an den Blocklistendatensatz angehängt sind. Die Change-Anforderung wird verwendet, um die Abruf-URL der Sperrliste im Firewall-Gateway „Check Point Next Generation“ zu konfigurieren. Diese Option wird empfohlen, wenn Ihr Firewall-Administrator auch verwendet ServiceNow AI Platform Für Firewall-Richtlinien- oder -Regeländerungen. Wenn Sie eine Anforderung erstellen, wird die Sperrliste automatisch aktiviert, sobald sie geschlossen wurde. Deaktivieren Sie das Kontrollkästchen, um die Sperrliste manuell zu aktivieren, nachdem der Firewall-Administrator per E-Mail darüber informiert hat, dass der anwenderdefinierte Intelligence-Feed auf allen Prüfpunkt-Gateways konfiguriert wurde. Wenn das Kontrollkästchen Change-Anforderung erstellen deaktiviert ist, ist das Feld Change-Anforderung nicht verfügbar.
Genehmigung anfordern	Dieses Kontrollkästchen ist standardmäßig aktiviert, um Genehmigungen zum Aktivieren/Entfernen von Blocklisteneinträgen aus Sperrlisten anzufordern. Die Genehmigung wird von den Anwendern mit der Rolle „Security Incident-Administrator“ (sn_si.admin) angefordert. Die Genehmigungsanforderung wird per E-Mail an die Genehmiger gesendet. Sobald die Genehmigung akzeptiert wurde, wird der Eintrag in dieser Sperrliste aktiviert. Wenn das Kontrollkästchen nicht aktiviert ist, folgen die Einträge für diese Sperrliste nicht dem Genehmigungs-Workflow und werden direkt in der Sperrliste aktiviert.
Tag für erkennbares Element	Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen Tag anzeigen aktiviert ist. Das Feld wird automatisch ausgefüllt, nachdem die Sperrliste mit einem Standardwert aus dem Feld Name gespeichert wurde. Wenn die Sperrliste mit dem Namen „Malware-URL“ erstellt wird, lautet der abgeleitete Tag-Name „Sperrliste – Malware-URL“
Change-Anforderung	Wenn das Kontrollkästchen Change-Anforderung erstellen aktiviert ist, wird die Change-Anforderungsnummer in der Now Platform-Instanz angezeigt, sobald die Sperrliste gespeichert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn das Kontrollkästchen Change-Anforderung erstellen deaktiviert ist, wird dieses Feld nicht angezeigt.
Beschreibung	Beschreibung der Prüfpunktblockliste. Der Name enthält im Allgemeinen die Typen von Sites und erkennbaren Elementen, die Sie voraussichtlich in dieser Sperrliste befinden, und Sie können dieses Feld für weitere Details verwenden.
Ablaufzeitraum (in Tagen)	Ablaufzeitraum der Sperrliste. 0 (Standard) gibt an, dass der Eintrag „Sperrliste“ nie abläuft. Wenn Sie diesen Wert ändern, ist dieser Eintrag für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben, der 24 Stunden beträgt, und es gibt keinen Höchstwert.
Abruf-URL	Abruf-URL wird automatisch generiert, sobald die Blockliste gespeichert wurde. Um diese Blockliste in Prüfpunkt-Gateways zu konfigurieren, müssen Sie diese URL verwenden. Sobald diese URL konfiguriert ist, ruft der Prüfpunkt erkennbare Elemente ab, die im CSV-Format blockiert werden sollen.



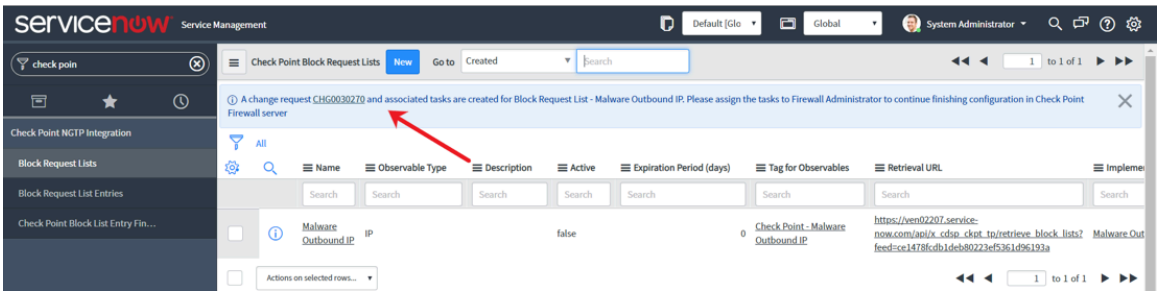
5. Klicken Sie auf **Absenden**.
6. Wenn die Liste der Prüfpunktblockanforderungen nicht angezeigt wird, navigieren Sie zu **Check Point – NGTP-Integration** > **Sperranforderungslisten**an.



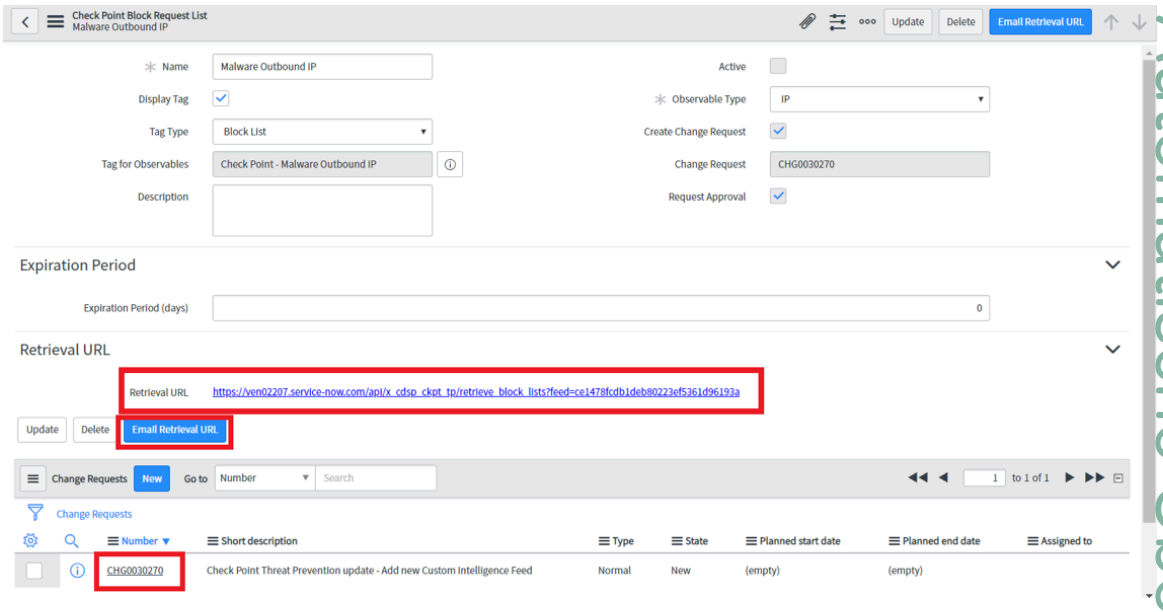
Die neue Blockliste wird angezeigt. Der Sperrlistenstatus ist weiterhin inaktiv (falsch), was bedeutet, dass die Sperrliste nicht zum Akzeptieren von Einträgen verfügbar ist. Wenn „Change-Anforderung erstellen“ konfiguriert wurde, wird eine Meldung angezeigt, die angibt, dass eine Change-Anforderung und Aufgaben in erstellt wurden ServiceNow AI Platform Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. In **Name** Spalte auf ein Element klicken, um den Datensatz zu öffnen.
   Der Datensatz „Sperrliste“ wird angezeigt. Dieses Beispiel zeigt eine ausgehende IP-Blockliste für Malware. Die folgenden Felder, Optionen und Links werden nach der Übermittlung im neuen Datensatz angezeigt und in der folgenden Tabelle beschrieben.



Feld	Beschreibung
E-Mail-Abruf-URL	Sendet eine E-Mail an den Check Point-Firewall-Administrator, dass der Blocklink für die Konfiguration verfügbar ist.
Abruf-URL	Diese URL wird verwendet, um anwenderdefinierten Intelligence-Feed in Prüfpunkt-Gateways zu konfigurieren. **Hinweis:** Wenn Ihre Systemeinstellungen auf Formulare mit Registerkarten festgelegt sind, wird dieser Link auf der Registerkarte „Informationen zum Abruf der Sperrliste“ unten im Datensatz angezeigt.
ServiceNow AI Platform Change-Anforderung	Ein Link zum Change-Anforderungsdatensatz wird im Abschnitt „Change-Anforderungen“ angezeigt, wenn konfiguriert, und die Anforderungsnummer wird im Feld „Change-Anforderung“ angezeigt.
Aktualisieren	Ändern Sie Daten, und aktualisieren Sie die bearbeitbaren Felder.
Löschen	Löschen Sie den Datensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Erstellen und fügen Sie nach Bedarf weitere Blocklisten hinzu.
   Die Sperrlisten werden auf der Seite „Checkpoint-Sperranforderungslisten“ angezeigt.

Nächste Maßnahme

Aktivieren Sie die Sperranforderungsliste manuell oder mit ServiceNow AI Platform Change-Anforderung.

Aktivieren Sie eine Sperrliste für Check Point NGTP Integration

Nachdem die Sperrliste in erstellt wurde ServiceNow AI Platform Und die URL verfügbar ist, konfiguriert der Prüfpunkt-Administrator die Sperrliste als anwenderdefinierter Intelligence-Feed für alle Prüfpunkt-Gateways der nächsten Generation. Bevor Blocklisteneinträge akzeptiert werden können, muss die Blockliste in Prüfpunkt konfiguriert und in aktiviert werden ServiceNow AI Platform.

Vorbereitungen

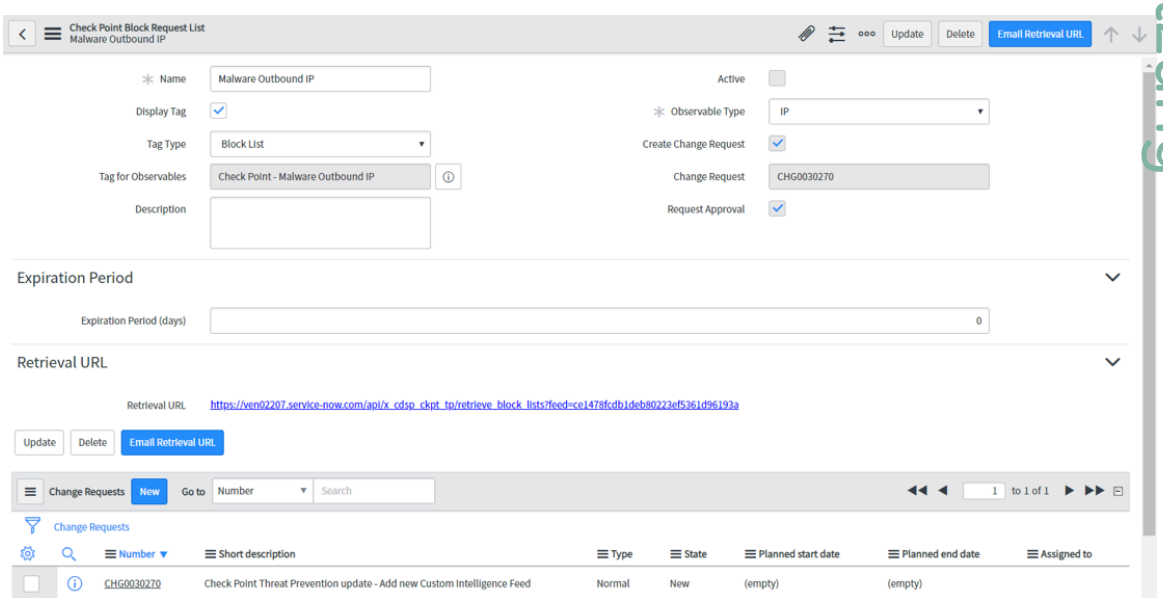
Erforderliche Rolle: Security Incident-Administrator (sn_si.admin)

Warum und wann dieser Vorgang ausgeführt wird

Nachdem die Sperrliste konfiguriert wurde, können Sie als Security Incident-Administrator die Sperrliste manuell aktivieren, oder die Sperrliste wird automatisch nach Abschluss von aktiviert ServiceNow AI Platform Change-Anforderung. Die Change-Anforderung muss genehmigt und vom Status „Inaktiv“ in den Status „aktiv“ verschoben werden, bevor Blocklisteneinträge akzeptiert werden können.

Prozedur

1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Sperranforderungslisten**, Und wählen Sie aus **Sperranforderungslisten** Modul.
2. In **Checkpoint-Sperranforderungslisten** Liste, die angezeigt wird, wählen Sie Ihre neue Blockliste im aus **Name** Spalte.
3. Notieren Sie sich im angezeigten Datensatz **E-Mail-Abruf-URL** Schaltfläche, der aktive Link zum Abrufen der Sperrliste und, falls konfiguriert, die ServiceNow AI Platform Change-Anforderung im Abschnitt Change-Anforderungen.
   Beachten Sie auch, dass das Kontrollkästchen aktiv deaktiviert ist.

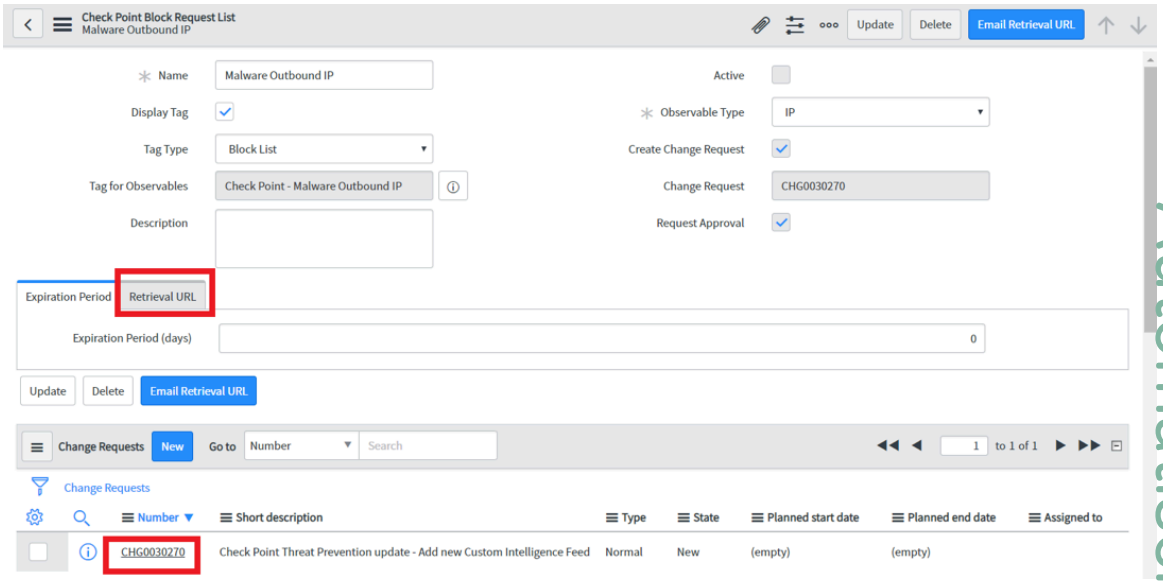


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Formulare mit Registerkarten in Ihren Systemeinstellungen gelöscht sind, wird die URL zum Abrufen der Sperrliste im Abschnitt „Abruf-URL“ angezeigt.

4. Klicken Sie auf **Abruf-URL der Sperrliste** Registerkarte zum Anzeigen der Abruf-URL.
Die folgende Abbildung zeigt die URL zum Abrufen der Sperrliste, die als Registerkarte mit Formularen mit Registerkarten angezeigt wird, die in Ihren Systemeinstellungen ausgewählt sind. Der Link zur Change-Anforderung (CH0030270) wird ebenfalls angezeigt.



5. Um die Konfiguration abzuschließen und die Sperrliste von inaktiv in aktiv zu verschieben, müssen Sie eine der folgenden Optionen auswählen, um den Firewall-Administrator darüber zu informieren, dass die Abruf-URL verfügbar ist.

Option	Beschreibung
Klicken Sie auf E-Mail-Abruf-URL.	Abruf-URL der Sperrliste per E-Mail direkt an den Firewall-Administrator senden. Mit dieser Option kann der Firewall-Administrator die Konfiguration auf der Prüfpunkt-Plattform abschließen. Wählen Sie diese Option aus, wenn der Firewall-Administrator nicht verwendet ServiceNow AI Platform.
Schließen Sie ab ServiceNow AI Platform Change-Anforderung und weisen Sie die Konfigurationsaufgaben dem Firewall-Administrator zu.	Diese Option ist nur verfügbar, wenn der Firewall-Administrator für Check Point auch Now Platform und verwendet ServiceNow AI Platform Change-Management- und Genehmigungsprozesse sind konfiguriert. **Hinweis:** Benutzer mit der Rolle Security Incident-Administrator (sn_si.admin) können genehmigen ServiceNow AI Platform Change-Anforderung. Sobald die Konfigurationsaufgaben abgeschlossen sind und die Change-Anforderung geschlossen wurde, wird die Sperrliste automatisch aktiviert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Nachdem Sie den Firewall-Administrator darüber informiert haben, dass die Abruf-URL verfügbar ist, und Sie bestätigt haben, dass die Sperrliste in Prüfpunkt konfiguriert wurde, als Security Incident-Administrator, besteht Ihr nächster Schritt darin, die Sperrliste zu aktivieren. Sie aktivieren entweder die Sperrliste manuell oder verwenden, falls konfiguriert, die ServiceNow AI Platform Formular „Change-Anforderung“ zum Aktivieren der Sperrliste. Die Sperrliste wird automatisch aktiviert, wenn die Change-Anforderung geschlossen wird.

Konfigurieren Sie eine Blockliste als anwenderdefinierten Intelligence-Feed auf der Check Point NGTP Integration

Der Firewall-Administrator muss den anwenderdefinierten Intelligence-Feed konfigurieren, der der in der NOW-Plattform erstellten Sperrliste entspricht.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Diese Aufgabe muss für jedes der Prüfpunkt-NGTP-Gateway ausgeführt werden. Der Firewall-Administrator benötigt den SSH-Zugriff der Gateway-Server. Wenn Ihre Organisation hat ServiceNow AI Platform Change-Management- und Genehmigungsprozesse; überprüfen Sie, ob die Funktion zum Senden/Empfangen von E-Mails aktiviert ist.

Der Firewall-Administrator benötigt die Abruf-URL der Sperrliste und die ServiceNow-Anwenderanmeldeinformationen mit der Rolle „Check Point API Account Access“ (sn_sec_Checkpoint.api_Account_Access).

Wenn der Firewall-Administrator die NOW-Plattform nicht verwendet, kann der NOW Security Incident-Administrator die erforderlichen Informationen per E-Mail bereitstellen. Wenn der Firewall-Administrator die NOW-Plattform verwendet, kann alternativ die Change-Anforderung, die der Sperrliste zugeordnet ist, dem Firewall-Administrator zugewiesen werden. Diese Change-Anforderung enthält die erforderlichen Informationen zum Konfigurieren des anwenderdefinierten Intelligence-Feeds.

Weitere Informationen zum Einrichten des anwenderdefinierten Intelligence-Feeds in Prüfpunkt-Gateways finden Sie unter: https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk132193

Prozedur

1. Stellen Sie sicher, dass die Funktion zum Senden/Empfangen von E-Mails in Ihrem aktiviert ist ServiceNow AI Platform Instanz, indem Sie zu navigieren **E-Mail-Eigenschaften** > **Administration** > **E-Mail-Eigenschaften**an.
2. Überprüfen Sie dies unter Konfiguration ausgehender E-Mails **E-Mail wird gesendet** Und **E-Mail-Empfang** Sind ausgewählt.
3. Ändern Sie SSH in Prüfpunkt-Gateway mit Expertenmodus.
4. Führen Sie den Befehl aus, um einen anwenderdefinierten Intelligence-Feed hinzuzufügen.
   Die Befehlsausführung ist interaktiv und fordert das Feed-Format und das Passwort auf.
   - Geben Sie bei Aufforderung zum Feed-Format „cp_csv“ ein
   - Bei Aufforderung zur Eingabe DES NOW Platform-Anwenderpassworts mit API-Zugriff.

   Die Befehlsausführung warnt, dass das Serverzertifikat (NOW Platform) vom Computer nicht vertrauenswürdig ist, und fordert Sie auf, das Serversicherheitszertifikat dem vertrauenswürdigen Speicher des Computers hinzuzufügen. Geben Sie Ein **Y** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Meldung „Status:erfolgreich“ wird angezeigt, um zu bestätigen, dass der Feed erfolgreich hinzugefügt wurde.

```
[Expert@gw-93440b:0]# ioc_feeds add --feed_name phishing_url --transport https --resource https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/
retrieve_block_lists?feed=<feed_id> --user_name <now_ckpt_api_user> --feed_action Prevent
Enter feed format. Should be cp_csv/stix_1.x: cp_csv
Only Check Point's csv format files will be loaded
Enter Password
Password: <now_ckpt_api_password>

Default value for active is: true

Feed Name: phishing_url
Feed is Active
File will be fetched via HTTPS
Resource: https://<NOW-INSTANCE>.service-now.com/api/x_cdsp_ckpt_tp/retrieve_block_lists?feed=<feed_id>
Action: Prevent
User Name: admin

[============================================================] 100.0% ...Getting file from the server
The server security certificate is not trusted by your machine.
SHA256 Fingerprint=SHA256 fingerprint of the NOW instance.

Do you want to trust it for this specific feed?  [y/n]: y
Fetching active feeds

Update summary
##############
feed: phishing_url. Status: Succeed
##############
Activating Scheduler

[Expert@gw-93440b:0]#
```

Übermitteln Sie Sperrlisteneinträge aus einem Security Incident für Check Point NGTP Integration

Erkennbare Elemente, die an einen Security Incident-Datensatz angehängt sind, werden zur Genehmigung als Sperrlisteneinträge an verschiedene Sperrlisten übermittelt. Ein optionaler Genehmigungsprozess für Blocklisteneinträge ist Teil des vorkonfigurierten Workflows. Das Gateway importiert Blocklisteneinträge – IP-Adressen, URLs, Domänen –, die in Blocklisten enthalten sind.

Vorbereitungen

Erforderliche Rolle:

- Security Incident-Analyst (sn_si.Analyst), um Blocklisteneinträge zu übermitteln.
- Security Incident-Administrator (sn_si.admin) zum Genehmigen von Blocklisteneinträgen. Diese Berechtigung kann nach Bedarf von Ihrer Organisation zugewiesen werden.

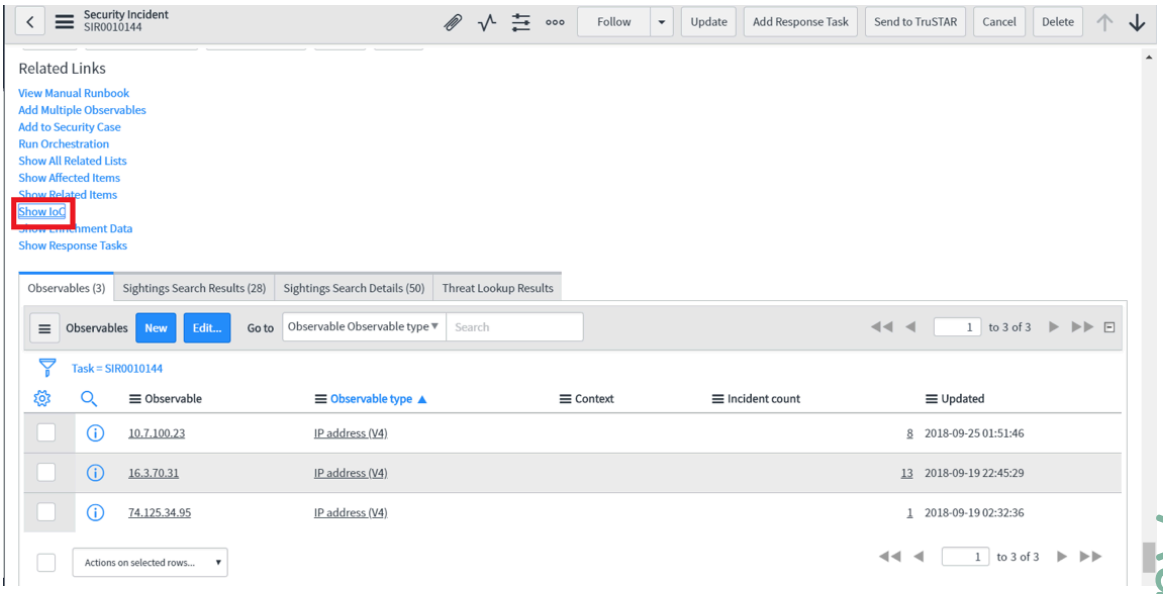
Warum und wann dieser Vorgang ausgeführt wird

Benutzer mit der Rolle „sn_si.Analyst“ übermitteln Blockeinträge, indem sie einen Block für erkennbare Elemente anfordern, die an einen Security Incident-Datensatz angehängt sind. Nach der Übermittlung wird ein Sperrlisteneintrag mit dem Status Ausstehend generiert und zur Genehmigung gesendet. Das folgende Beispiel zeigt eine Blockanforderung für ein erkennbares URL-Element.

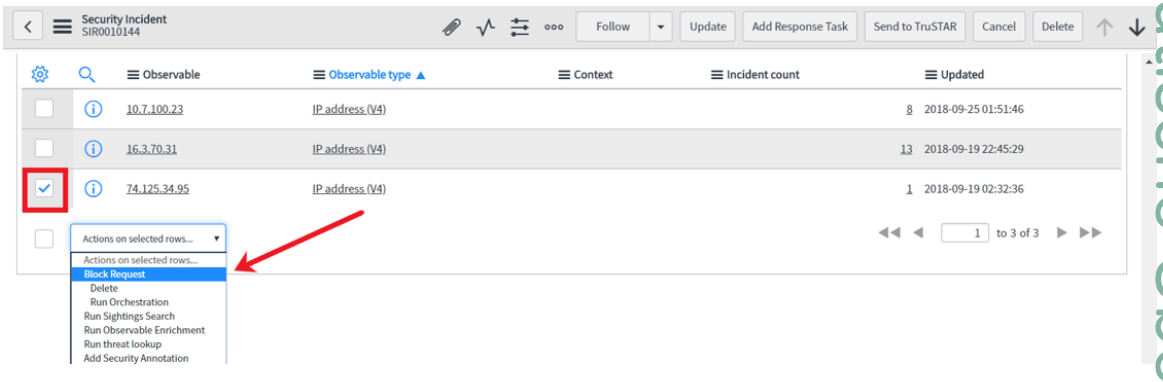
Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**, Und klicken Sie auf einen Security Incident-Datensatz, um ihn zu öffnen.
2. Klicken Sie auf **IOC anzeigen** Zugehöriger Link.

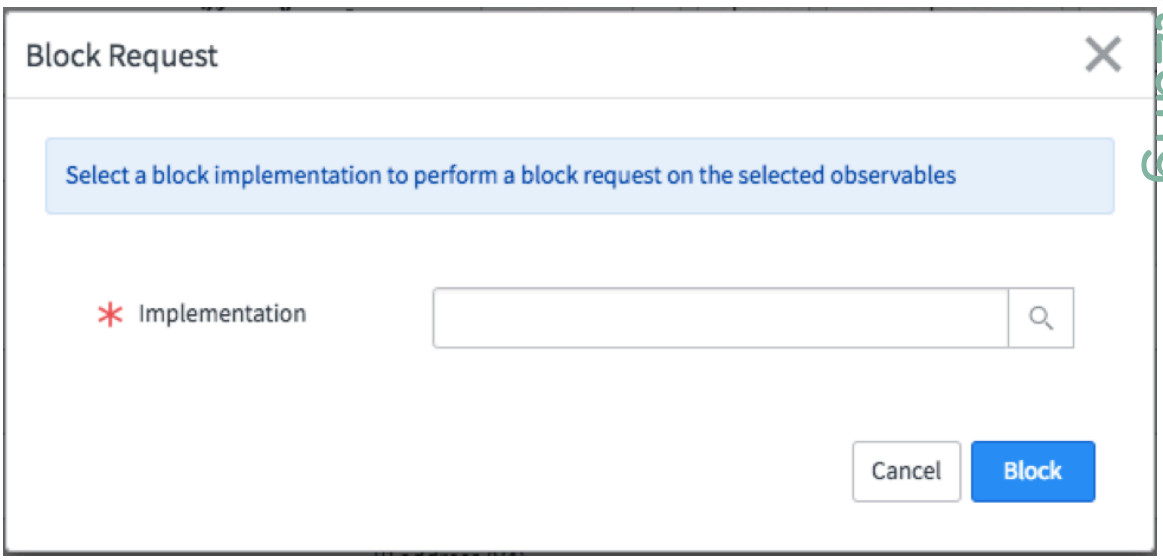
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie in der zugehörigen Liste erkennbare Elemente die erkennbaren Elemente aus, die Sie blockieren möchten, und aus **Aktionen für ausgewählte Zeilen** Liste, wählen Sie aus **Anforderung Blockieren** .



4. Klicken Sie im angezeigten Dialogfeld auf das Suchsymbol ( )

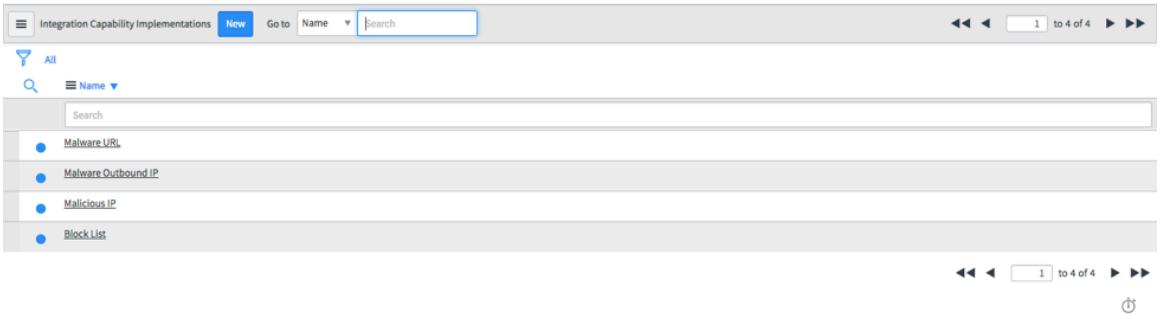


5. Wählen Sie in der Liste die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten.

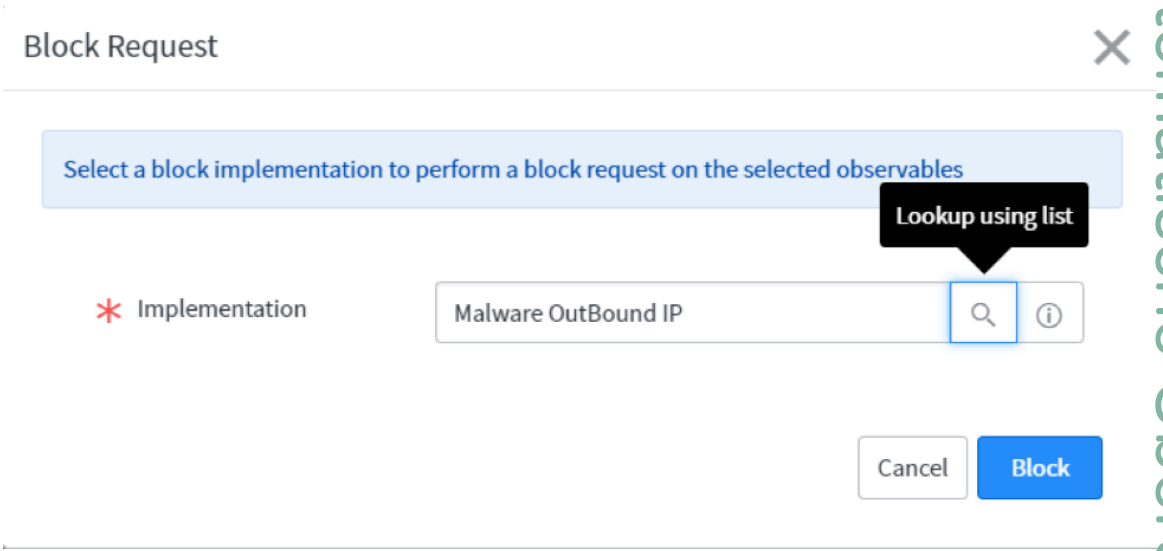
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
In diesem Beispiel muss der Eintrag erkennbares Element Typ (IP) mit dem Typ des erkennbaren Elements der Blockliste (IP) übereinstimmen.

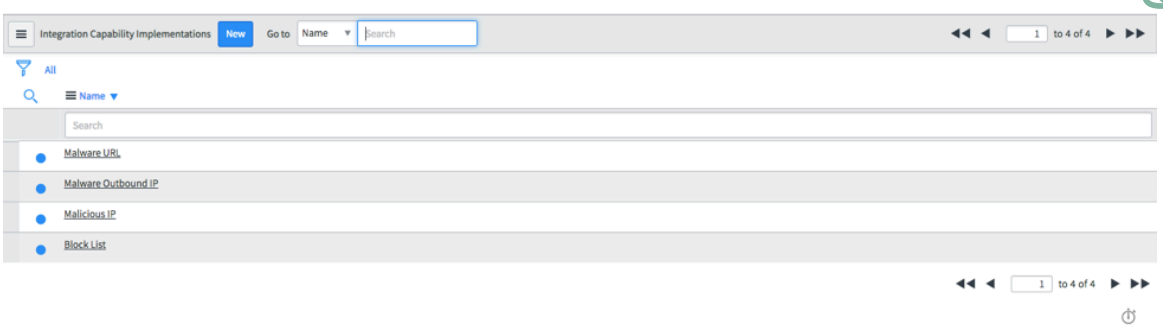


6. Klicken Sie im Dialogfeld „Blockierungsanforderung“ mit dem Namen der Blockliste, der im Feld Implementierung angezeigt wird, auf **Blockieren** .



7. Wählen Sie in der angezeigten Liste die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten.

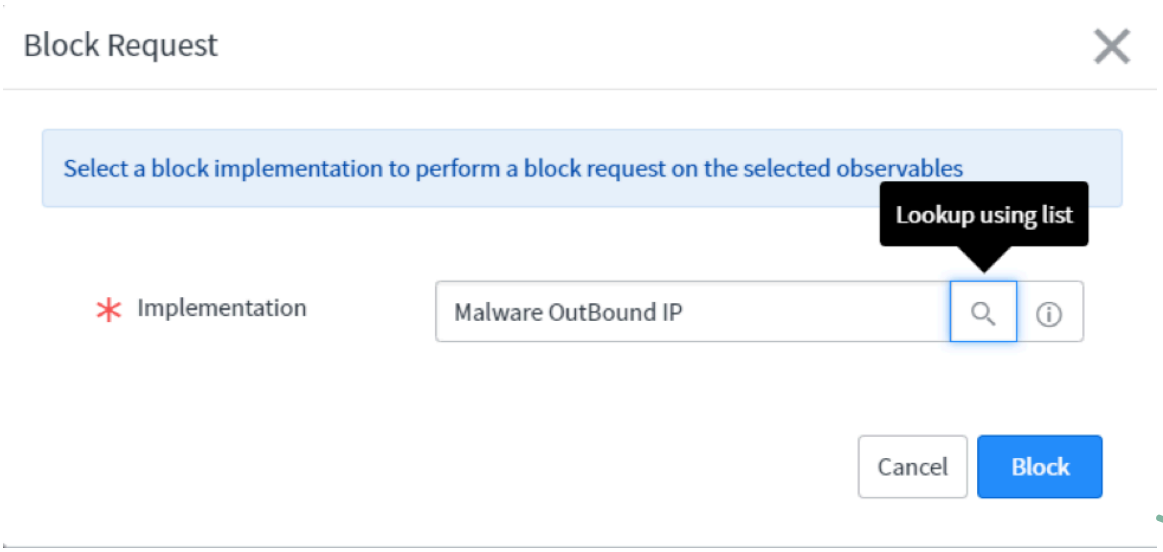
Hinweis:
In diesem Beispiel muss der Eintrag erkennbares Element Typ (IP) mit dem Typ des erkennbaren Elements der Blockliste (IP) übereinstimmen.



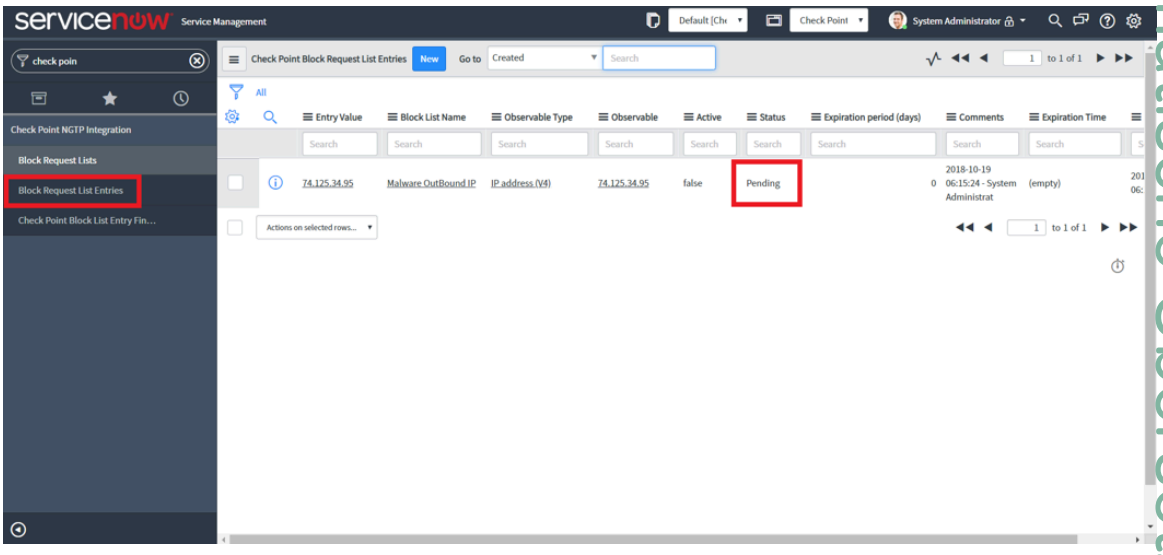
8. Im Dialogfeld „Blockieranforderung“ mit dem Namen der Blockliste, der in angezeigt wird **Implementierung** Feld klicken Sie auf **Blockieren** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



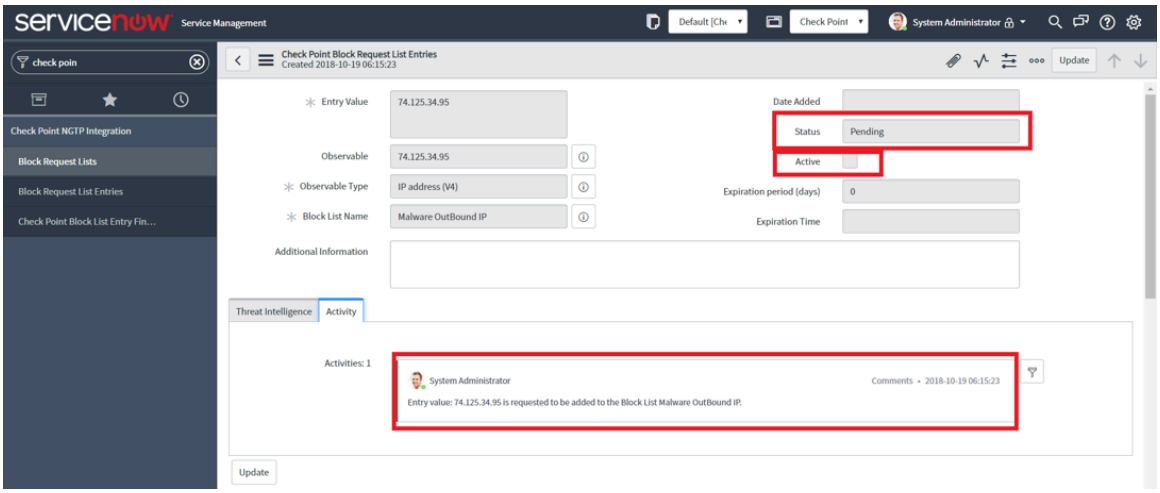
9. Navigieren zu **Check Point – NGTP-Integration** > **Einträge der Sperranforderungsliste**, Und klicken Sie auf **Listeneinträge Für Blockanforderung** .



10. Klicken Sie in der Liste Einträge der Sperranforderungsliste für Prüfpunkte auf Ihr erkennbares Element im **Eingabewert** Spalte zum Öffnen des Datensatzes.
In diesem Beispiel der Datensatz für **74.125.34.95** Wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Status ist Ausstehend, das Kontrollkästchen aktiv ist deaktiviert, und die Arbeitsnotizen zeigen an, dass eine Anforderung zum Hinzufügen des erkennbaren Elements vorhanden ist. Diese Sperrlisteneintragsanforderung ist bereit zur Genehmigung.

Das Symbol neben dem Feld „erkennbares Element“ ist ein Link zu ServiceNow AI Platform Tabelle des erkennbaren Elements.

Der Wert im Feld „erkennbares Element“ (74.125.34.95) verknüpft mit der Tabelle „erkennbares Element“ und entspricht dem Format, das aus dem Ereignis „auslösende Incidents für Security Incidents Response“ übernommen wurde.

Übermitteln Sie Blocklisteneinträge direkt aus der Blocklisteneintragstabelle

Für erkennbare Elemente, die als schädlich eingestuft und keinem bestimmten Now Platform Security Incident zugeordnet sind, übermitteln Sie Sperrlisteneinträge aus der Sperrliste.

Vorbereitungen
Erforderliche Rolle: Security Incident-Administrator (sn_si.Analyst)

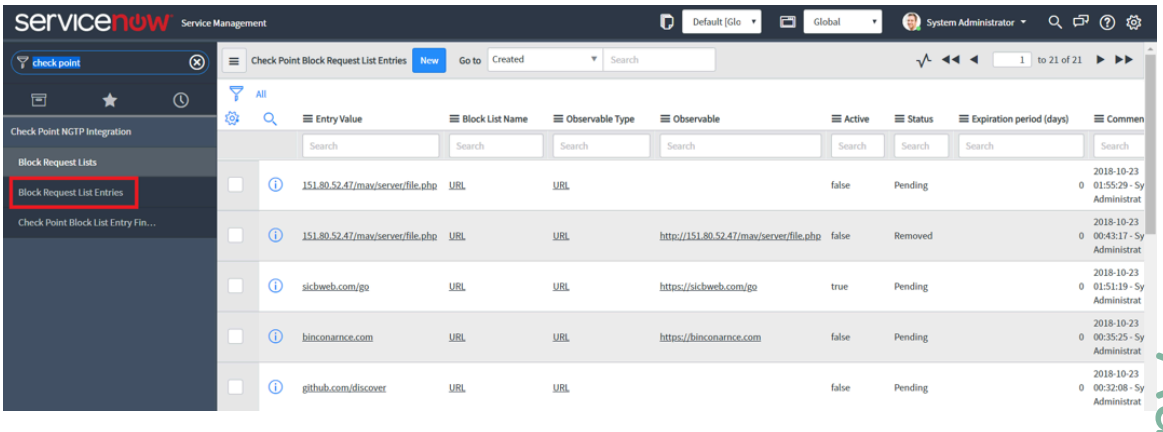
Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie ein erkennbares Element blockieren möchten, das Sie als böswillig eingestuft haben, oder zulassen möchten, dass ein erkennbares Element nicht böswillig ist und das erkennbare Element keinem bestimmten zugeordnet ist ServiceNow AI Platform Security Incident-Datensatz übermitteln Sie Sperrlisteneinträge direkt aus der Sperrliste. Beispiele für diese Arten von Blocklisteneinträgen können URLs oder Domänen für bestimmte Sites sein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

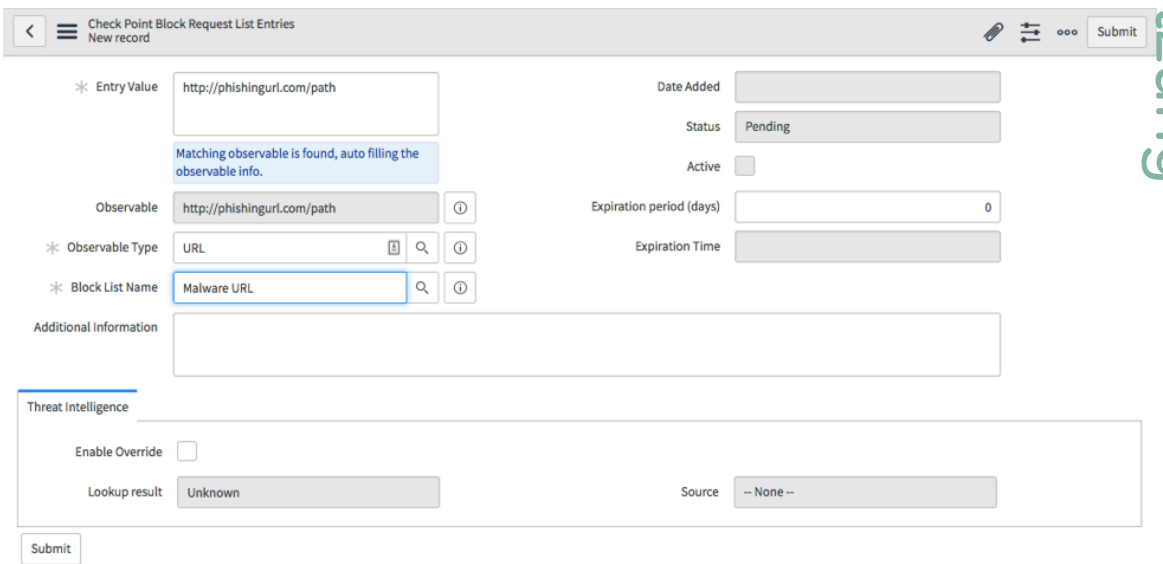
Prozedur

1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Blockieren Sie Anforderungseinträge**an.



2. Klicken Sie auf **Sperranforderungslisten** Modul.
3. Klicken Sie in der Liste Einträge der Sperranforderungsliste für Prüfpunkte auf **Neu** .
4. In **Eingabewert** Geben Sie einen Wert für Ihr erkennbares Element ein.
   Die beiden möglichen Ergebnisse dieses Eintrags:
   - Die verbleibenden Felder im Formular werden automatisch ausgefüllt.
   - Ein übereinstimmendes erkennbares Element wurde gefunden, und es wird eine Meldung angezeigt, dass ein übereinstimmendes erkennbares Element vorhanden ist. Wählen Sie die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten, und klicken Sie auf Absenden. Wählen Sie die Sperrliste aus, an die Sie diesen Eintrag anhängen möchten, bevor Sie den Ablaufzeitraum festlegen.

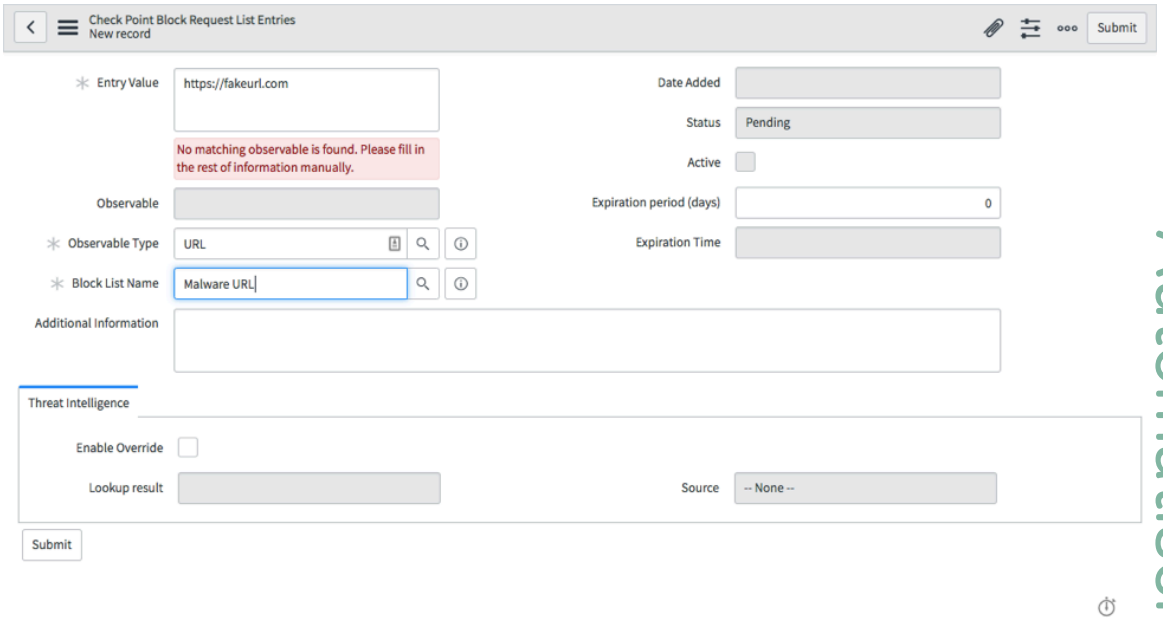
   Es wird eine Nachricht angezeigt, die Sie anweist, das Formular auszufüllen. Es wurde kein übereinstimmendes erkennbares Element gefunden, und Sie müssen das Formular ausfüllen. Wählen Sie nach Abschluss die Sperrliste aus, an die Sie das erkennbare Element anhängen möchten, und klicken Sie auf Absenden. Ein Datensatz eines erkennbaren Elements wird erstellt. Die folgende Abbildung zeigt ein Beispiel für ein vorhandenes erkennbares Domänenelement und wie die Felder automatisch ausgefüllt werden.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf das Suchsymbol, um die Sperrliste auszuwählen, an die Sie den Eintrag anhängen möchten.
6. Klicken Sie auf **Absenden**.
7. Wenn Sie in Ihrem Workflow eine E-Mail-Genehmigung konfiguriert haben, wird eine Genehmigungs-E-Mail-Anforderung gesendet.
   Wenn eine Nachricht angezeigt wird, in der Sie aufgefordert werden, den Rest der Informationen manuell auszufüllen, füllen Sie die Felder aus.



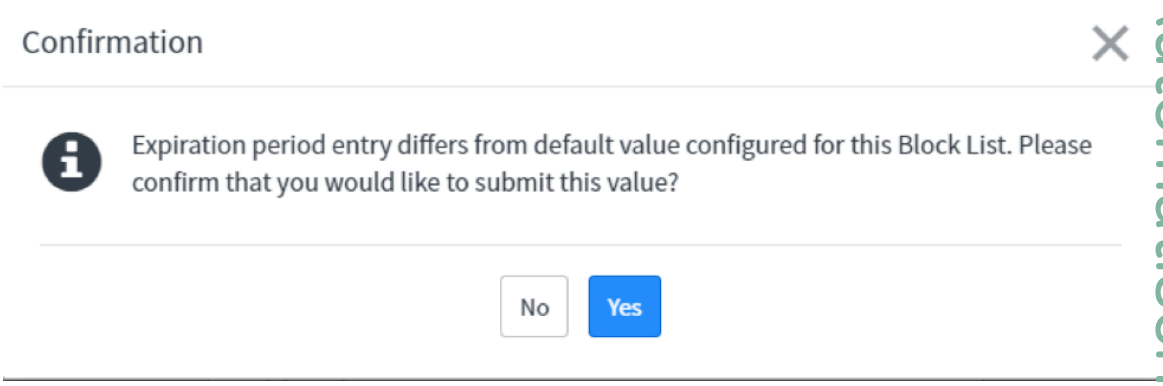
Feld	Beschreibung
Typ des erkennbaren Elements	Typ des erkennbaren Elements, der vom Dialogfeld unterstützt wird.
Name der Sperrliste	Sperrliste, in die Sie den Eintrag aufnehmen möchten. **Hinweis:** Wählen Sie die Sperrliste aus, an die Sie den Eintrag anhängen möchten, bevor Sie den Ablaufzeitraum festlegen.
Überschreibung aktivieren (Standard ist ausgewählt)	Suchergebnis oder Quelle. Wenn konfiguriert, können Sie ein Suchergebnis und die Quelle eingeben, die zum Suchen der Ergebnisse verwendet wird. Diese Felder werden normalerweise ausgefüllt, wenn ein Security Incident-Datensatz erstellt wird. In diesem Fall gibt es kein Suchergebnis oder keine Quelle, und Sie füllen diese Felder manuell aus.
Suchergebnis	Wählen Sie Aus **Unbekannt** Oder **Böswillig** .
Quelle	Quelle, die eine Bedrohungssuche für den Block-Listeneintrag durchführt, z. B. ThreatCrowd usw.
Ablaufzeitraum	Der Ablaufzeitraum, der standardmäßig aus der Sperrliste geerbt wird. Sie können diesen Wert überschreiben, aber nur während der Erstellung des Eintrags. 0 gibt an, dass der Sperrlisteneintrag nie abläuft.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn Sie diesen Wert ändern, ist dieser Eintrag für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben, und es gibt keinen Höchstwert. Wenn Sie beispielsweise am 1. Mai 30 Tage um 14:01 Uhr eingeben, läuft der Eintrag „Sperrliste“ am 31. Mai um 14:01 Uhr ab. Der Zeitplaner prüft jedoch jeden Tag um 00:00 Uhr auf abgelaufene Einträge und ändert den Status des Eintrags am 1. Juni um 00:00 Uhr in „abgelaufen“.

8. Klicken Sie auf **Absenden**.
Wenn Sie den standardmäßigen Ablaufzeitraum des Eintrags „Sperrliste“ geändert haben, wird ein Bestätigungsdialogfeld angezeigt, das angibt, dass sich der Zeitraum von der ausgewählten Sperrliste unterscheidet.

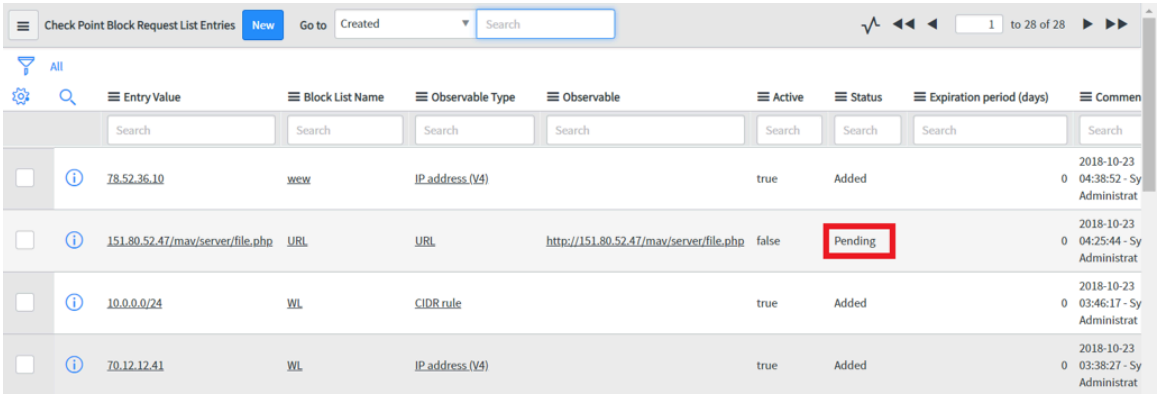


Option	Beschreibung
Ja	Bestätigt die Ablaufüberschreibung, speichert den Datensatz und kehrt zu den Prüfpunktblocklisteneinträgen zurück. Wenn Sie in Ihrem Workflow eine E-Mail-Genehmigung konfiguriert haben, wird eine Genehmigungs-E-Mail-Anforderung gesendet.
Nein	Bricht die Überschreibung ab. Jetzt können Sie den Wert für ändern **Ablaufzeitraum** . Nachdem Sie den Wert geändert haben, klicken Sie auf Absenden, um zur Liste „Prüfpunktblockeinträge“ zurückzukehren.

9. Wenn nicht angezeigt, navigieren Sie zu **Listeneinträge Der Sperranforderung Für Prüfpunkt** , Und beachten Sie, dass der Status für den Eintrag lautet **Ausstehend** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Eintrag ist jetzt zur Genehmigung bereit.

Genehmigen Sie Blocklisteneinträge für Check Point NGTP Integration

Ein Genehmigungsprozess für Blocklisteneinträge ist Teil des vorkonfigurierten Workflows. Sie genehmigen Sperrlisteneinträge, bevor die Einträge in Sperrlisten aktiviert werden. Nachdem Sie den Sperrlisteneintrag genehmigt haben, ruft das Gateway den Eintrag ab, und Ihr erkennbares Element wird von diesem Punkt an blockiert.

Vorbereitungen

- Die Genehmigung für Blocklisteneinträge wird standardmäßig dem Security Incident-Administrator (sn_si.admin) zugewiesen, diese Berechtigung kann jedoch nach Bedarf von Ihrer Organisation zugewiesen werden. Im folgenden Beispiel ServiceNow AI Platform administrator hat Genehmigungsberechtigung.

Erforderliche Rolle: sn.si.admin

Warum und wann dieser Vorgang ausgeführt wird

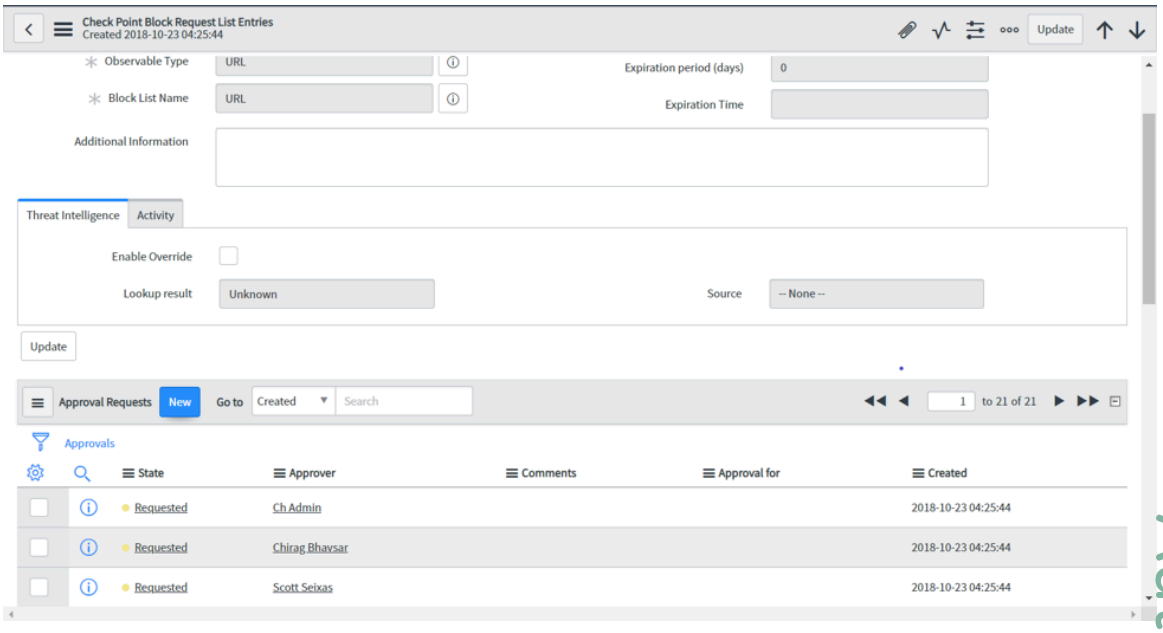
Wenn der Genehmigungsprozess aktiviert ist, wird ein Sperrlisteneintrag erst dann in der Sperrliste aktiviert oder deaktiviert, wenn er genehmigt wurde.

Prozedur

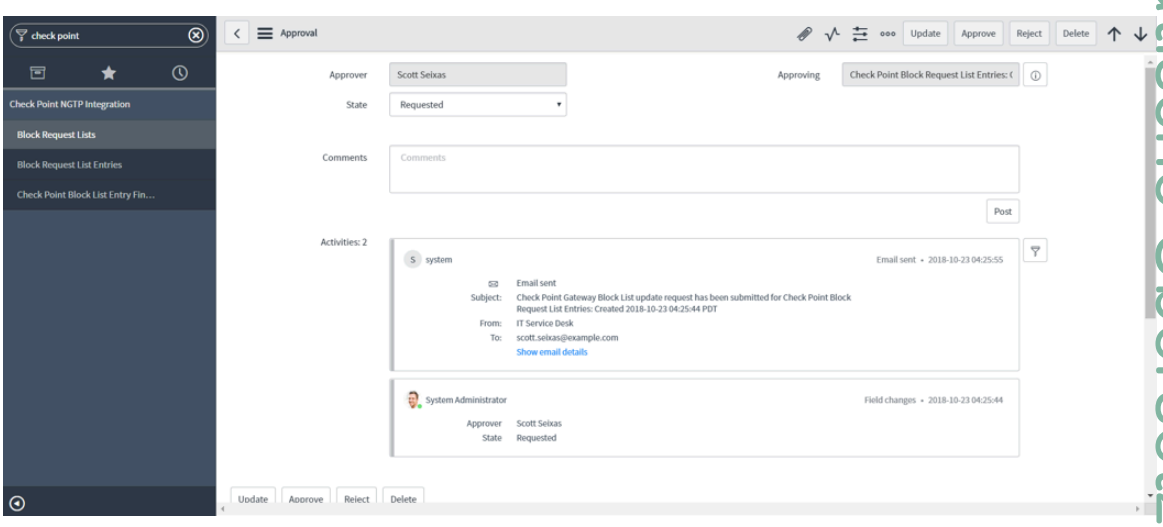
1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Einträge der Sperranforderungsliste**, Und öffnen Sie den Datensatz „Listeneintrag blockieren“.
2. Scrollen Sie im Datensatz „Listeneintrag blockieren“ zu **Genehmigungsanforderungen** Abschnitt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie unter Genehmigungsanforderungen auf ein Element in der **Status** Spalte zum Öffnen.
Der Genehmigungsdatensatz wird angezeigt.



4. Wählen Sie eine Option zum Genehmigen des Blocklisteneintrags aus.

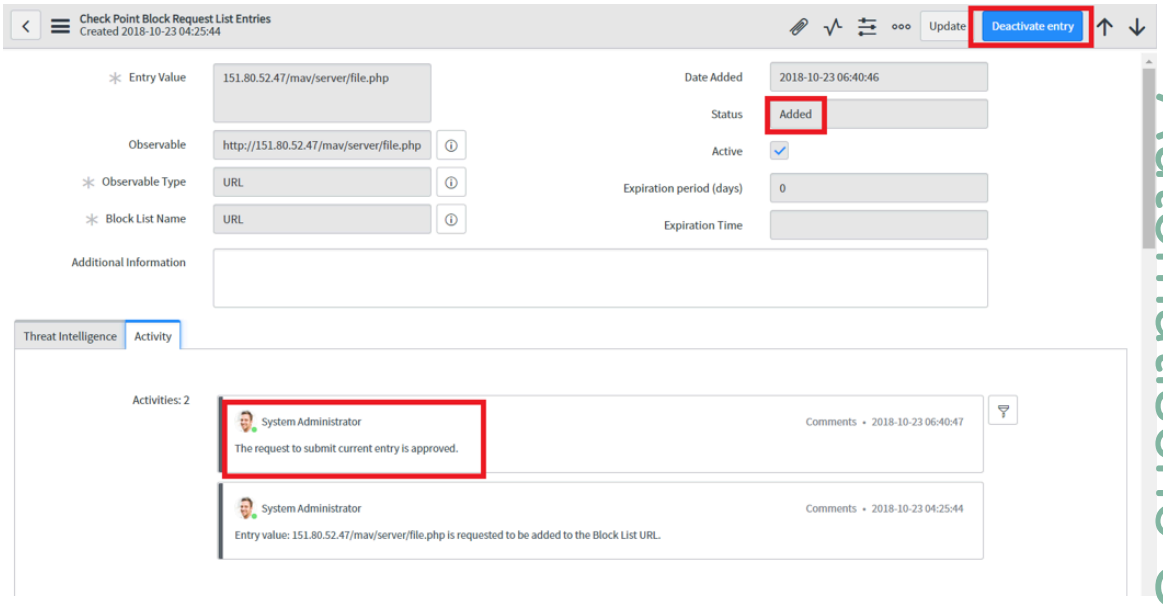
Option	Beschreibung
Genehmigen	Im Eintragsdatensatz ändert sich das Feld Status in hinzugefügt, und das Kontrollkästchen aktiv ist aktiviert. Die Schaltfläche Deaktivieren wird angezeigt und ist aktiv. Arbeitsnotizen zeigen, dass die Anforderung für den Sperrlisteneintrag genehmigt wurde.
Ablehnen	Im Eintragsdatensatz ändert sich das Feld Status in abgelehnt, und das Kontrollkästchen aktiv wird deaktiviert, um anzuzeigen, dass der Eintrag im Gateway nicht blockiert ist.

Automatische Übersetzung

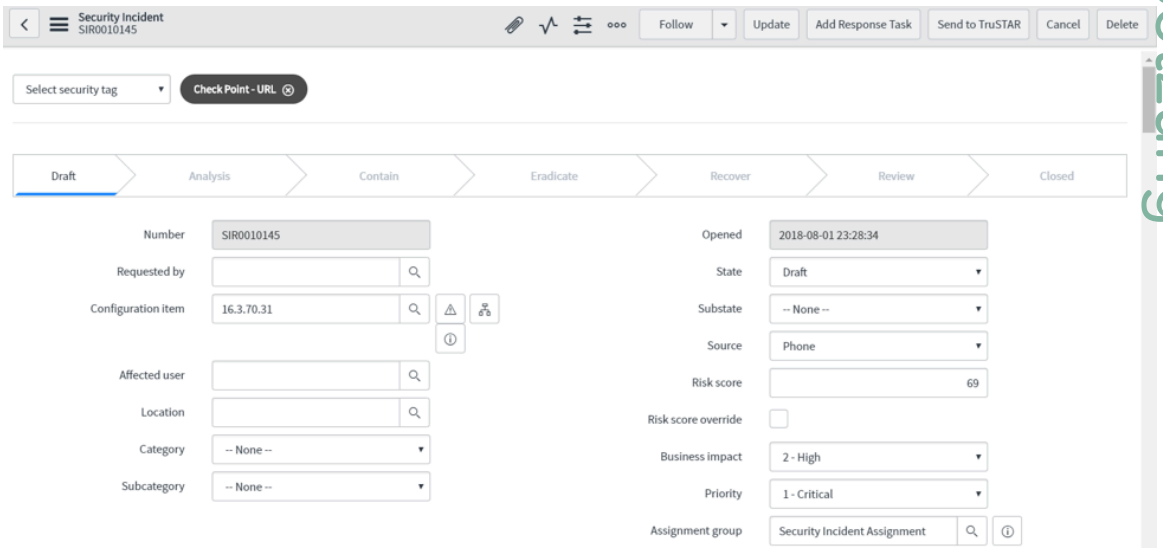
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Arbeitsnotizen zeigen, dass die Anforderung für den Sperrlisteneintrag abgelehnt wurde.

Nachdem Sie den Sperrlisteneintrag genehmigt und aktiviert haben, ruft die Prüfpunkt-Firewall der nächsten Generation den Sperrlisteneintrag nach dem nächsten Abrufintervall ab. Nachdem der Eintrag abgerufen wurde, wird das erkennbare Element von diesem Punkt an blockiert. Beachten Sie in der folgenden Abbildung, dass das Kontrollkästchen aktiv aktiviert ist, der Status hinzugefügt wird und die Arbeitsnotizen anzeigen, dass die Anforderung genehmigt wurde.



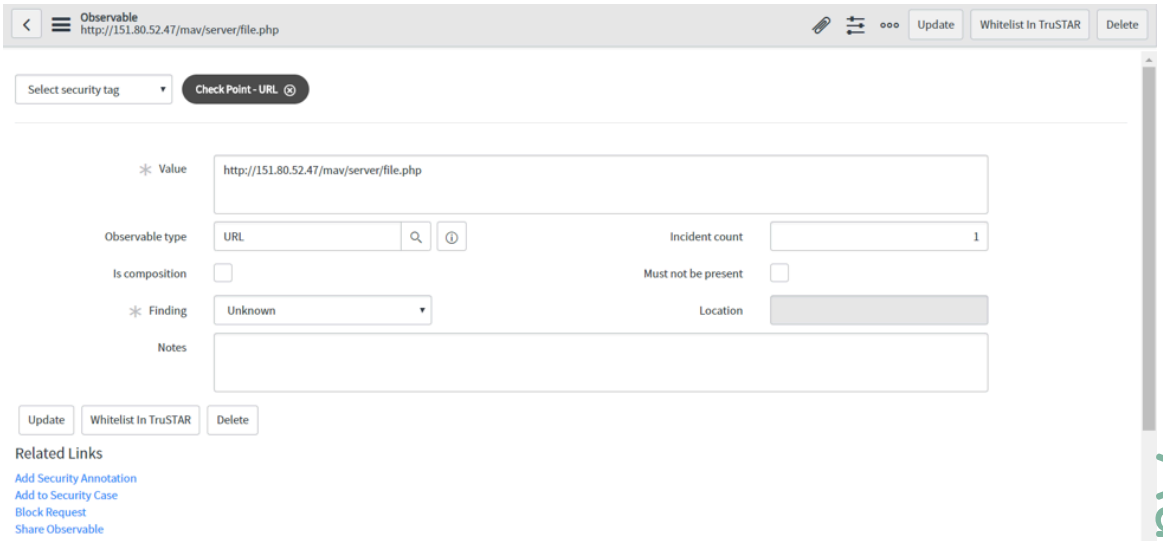
Nachdem der Eintrag „Sperrliste“ genehmigt und aktiviert wurde, wird der Security Incident-Datensatz mit einem Sicherheits-Tag markiert. Das Tag wird oben im Datensatz angezeigt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Sicherheits-Tag wird auch im Datensatz des erkennbaren Elements angezeigt.



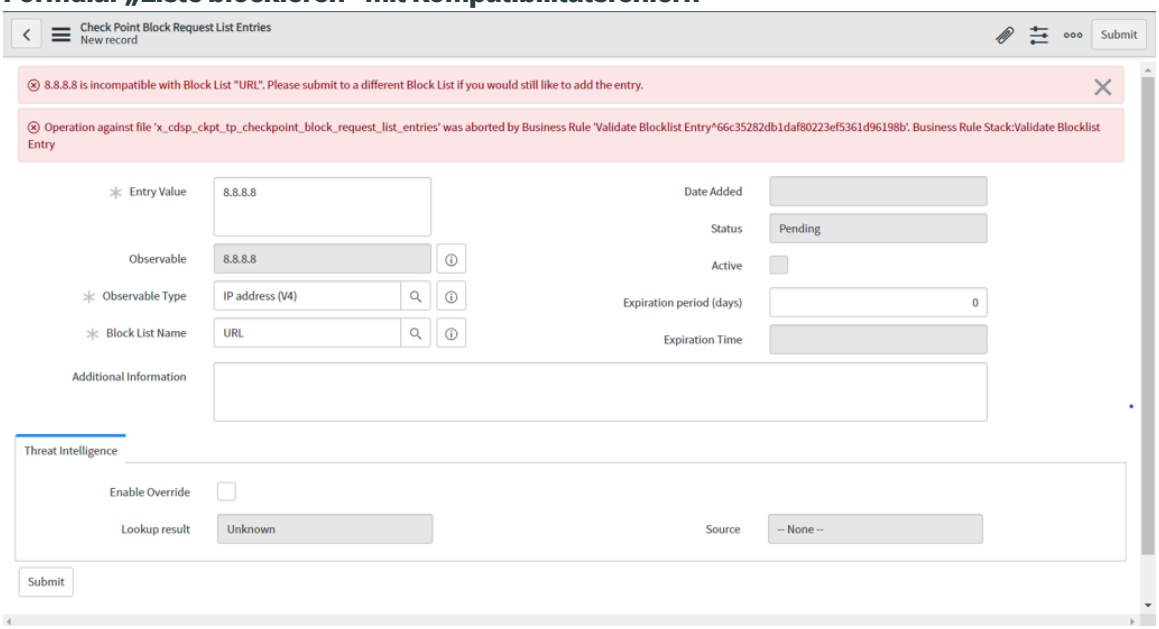
Listeneintragsausnahmen für sperren Check Point NGTP Integration

Es gibt Einschränkungen für das Hinzufügen von Sperrlisteneinträgen zu Sperrlisten. Wenn beim Versuch, Blocklisteneinträge zu Blocklisten hinzuzufügen, Duplikat-, Kompatibilitäts- oder CIDR-Konflikte (Classless Inter-Domain Routing) vorhanden sind, werden Fehlermeldungen angezeigt, die Ihnen helfen, diese Fehler zu beheben.

Kompatibilitätsausnahme

Jede Blockliste akzeptiert nur Einträge, die mit dem Typ des erkennbaren Elements kompatibel sind. Wenn Sie eine Domänenblockliste erstellen und versuchen, eine erkennbare IP-Adresse anzuhängen, wird eine inkompatible Fehlermeldung angezeigt. Beispielsweise kann eine Domänenblockliste nur erkennbare Domänenelemente akzeptieren, wie in der folgenden Abbildung dargestellt.

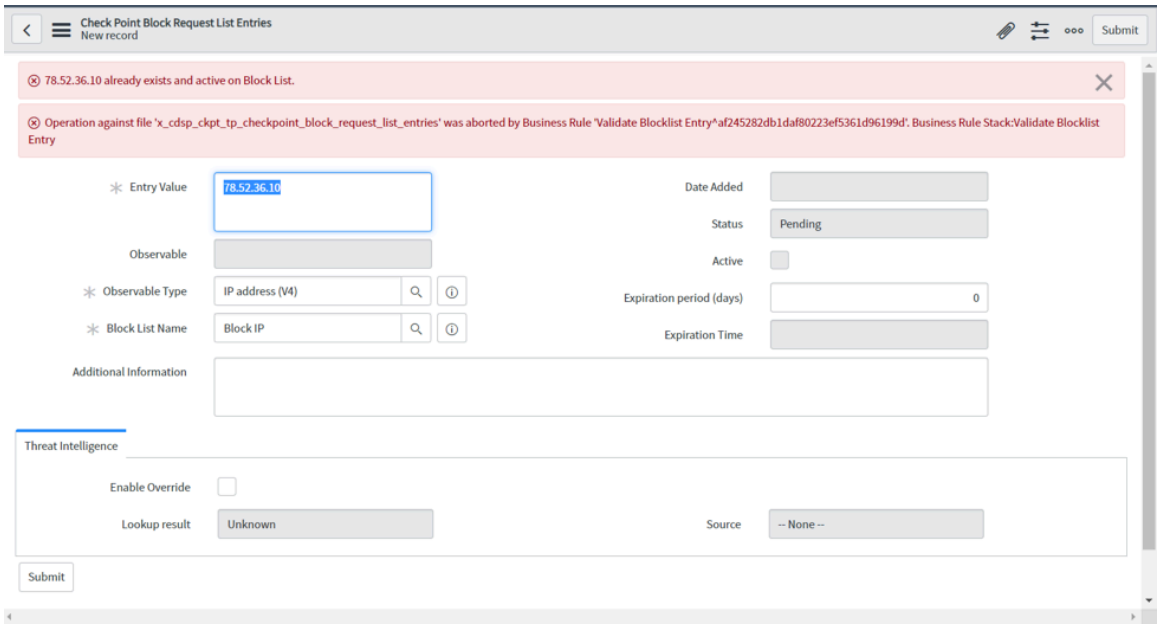
Formular „Liste blockieren“ mit Kompatibilitätsfehlern



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

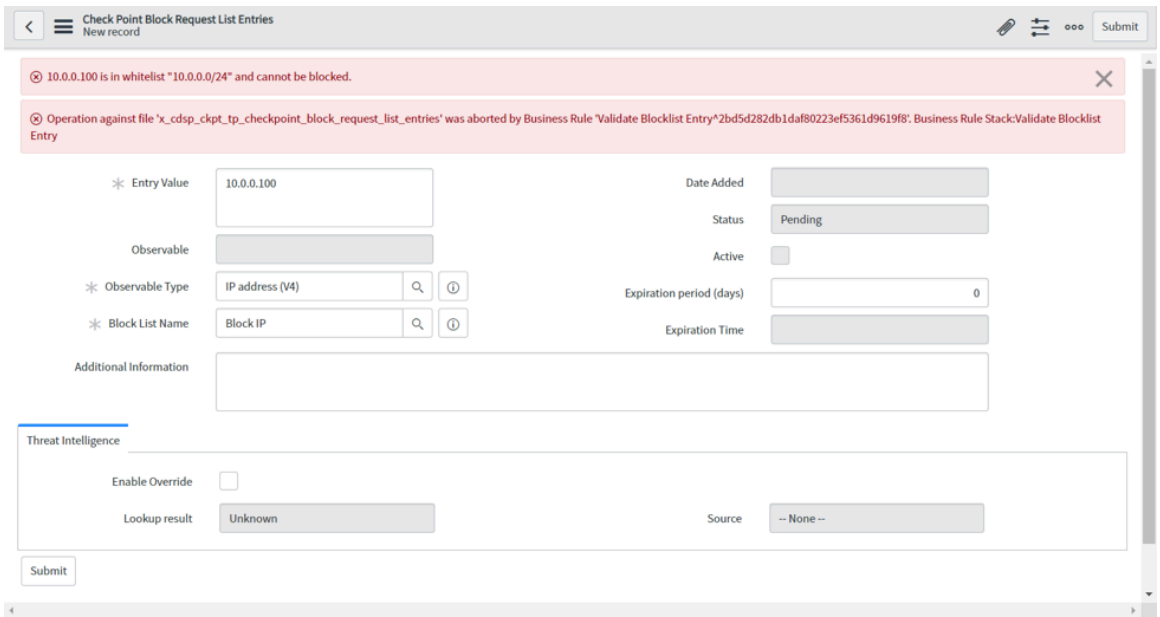
Duplizierungsausnahme

Ein erkennbares Element kann nicht in mehreren Blocklisten desselben erkennbaren Elements-Typs aktiviert werden. Wenn ein erkennbares URL-Element bereits in einer URL-Blockliste aktiviert ist und Sie versuchen, dasselbe erkennbare Element in einer Phishing-URL-Blockliste zu aktivieren, wird eine Duplikationsfehlermeldung angezeigt.



CIDR-Ausnahme (Classless Inter-Domain Routing)

Wenn Sie versuchen, eine einzelne IP-Adresse an eine Allow-Liste anzuhängen und diese IP-Adresse Teil eines erkennbaren CIDR-Elements ist, das sich bereits in einer Block-Liste/Allow-Liste befindet, wird ein CIDR-Konfliktfehler angezeigt. Dieser Fehler gibt an, dass die einzelne IP-Adresse bereits als Teil des erkennbaren CIDR-Elements in der Sperrliste oder der Allow-Liste enthalten ist. Beispielsweise ist 192.168.24.25 Teil des CIDR-Blocks 192.168.0,0/22.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bearbeiten Sie den Sicherheits-Tag-Namen für Check Point NGTP Integration

Wenn das Kontrollkästchen Tag anzeigen beim Erstellen des Blocklistendatensatzes aktiviert ist, können Sie die Tag-Namen und Farben der Sicherheits-Tags bearbeiten. Sicherheits-Tags helfen Ihnen, erkennbare Elemente nachzuverfolgen, die bereits blockiert sind.

Vorbereitungen

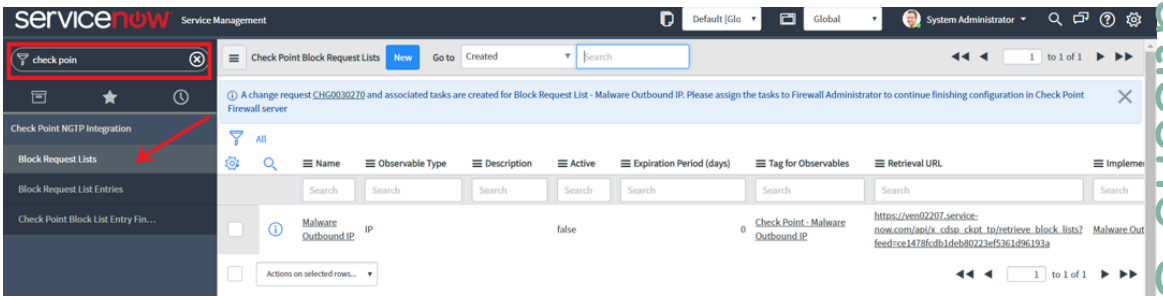
Erforderliche Rolle: sn.si.admin

Warum und wann dieser Vorgang ausgeführt wird

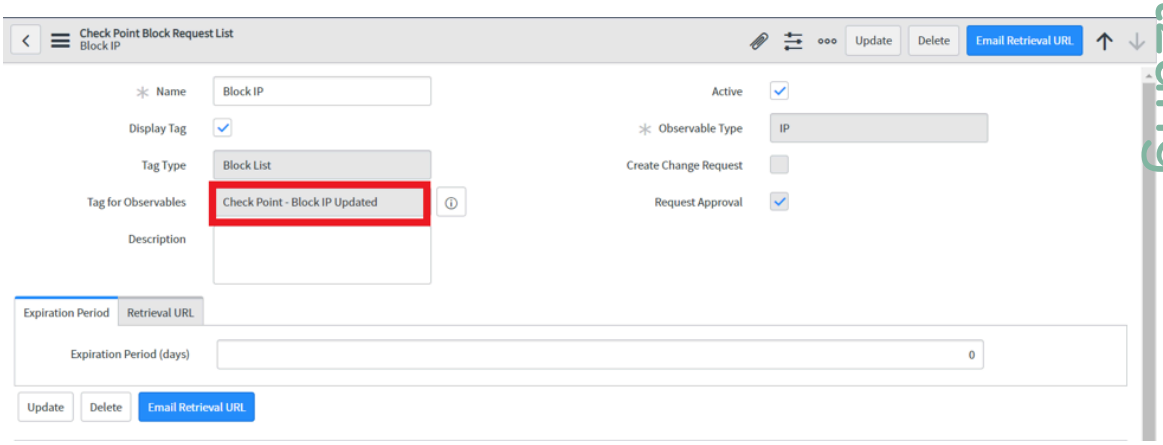
Sicherheits-Tags helfen Ihnen, schnell zu identifizieren, welche Security Incidents erkennbare Elemente auf einer Sperrliste enthalten. Tags helfen Ihnen auch zu identifizieren, ob ein erkennbares Element bereits blockiert ist oder ob es aus einer Sperrliste entfernt wurde. Standardmäßig ist die Farbe des Sicherheits-Tags für Blocklisteneinträge schwarz und für Allow-Listeneinträge grau. Sie können die Namen und Farben der Tags ändern, damit Sie bestimmte Tags leichter erkennen können.

Prozedur

1. Navigieren zu **Alle** > **Check Point – NGTP-Integration** > **Konfiguration Der Sperranforderungsliste**an.



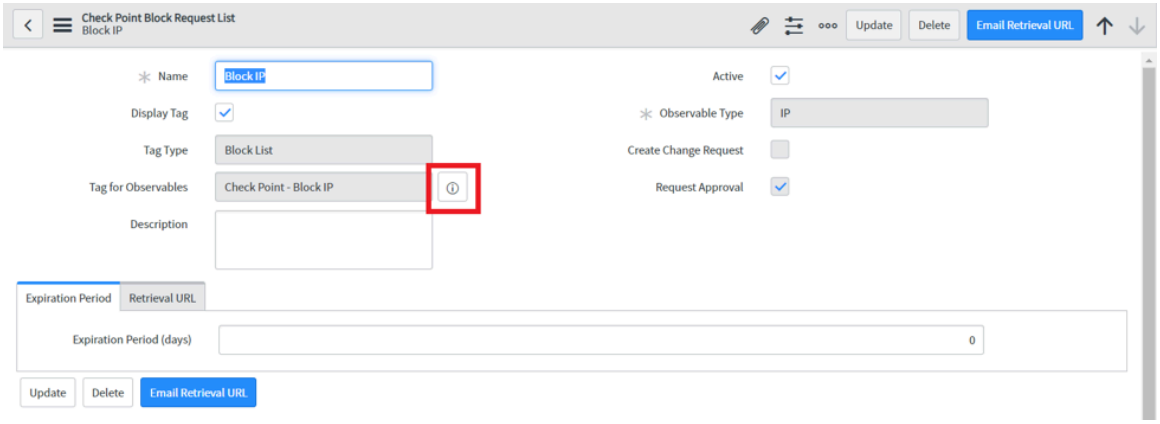
2. Klicken Sie auf ein Element im **Name** Spalte zum Öffnen.
   Der Datensatz „Sperrliste“ wird angezeigt. Standardmäßig ist der Sicherheits-Tag-Name derselbe Wert, den Sie beim Erstellen im Feld Name der Sperrliste eingegeben haben. Standardmäßig enthält der Name auch das Präfix „Sperrliste“, z. B. „Sperrliste – schädliche Malware-URLs“.



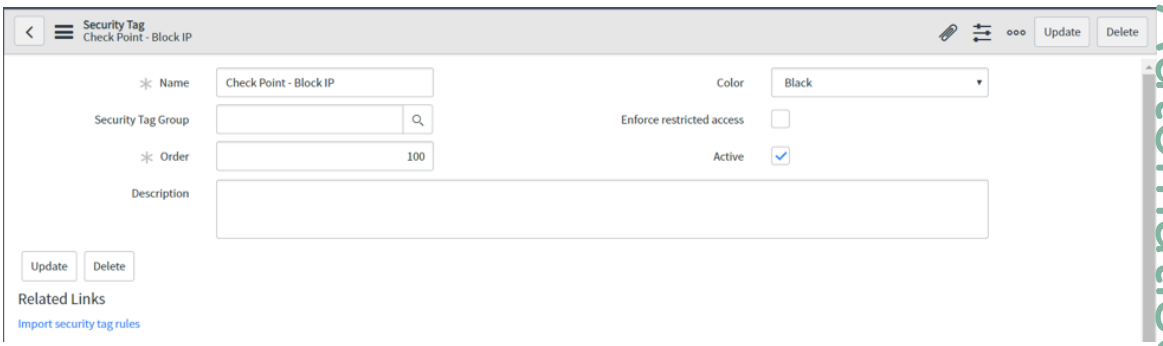
3. Klicken Sie auf das Informationssymbol neben dem Tag für erkennbare Elemente und dann auf Datensatz öffnen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

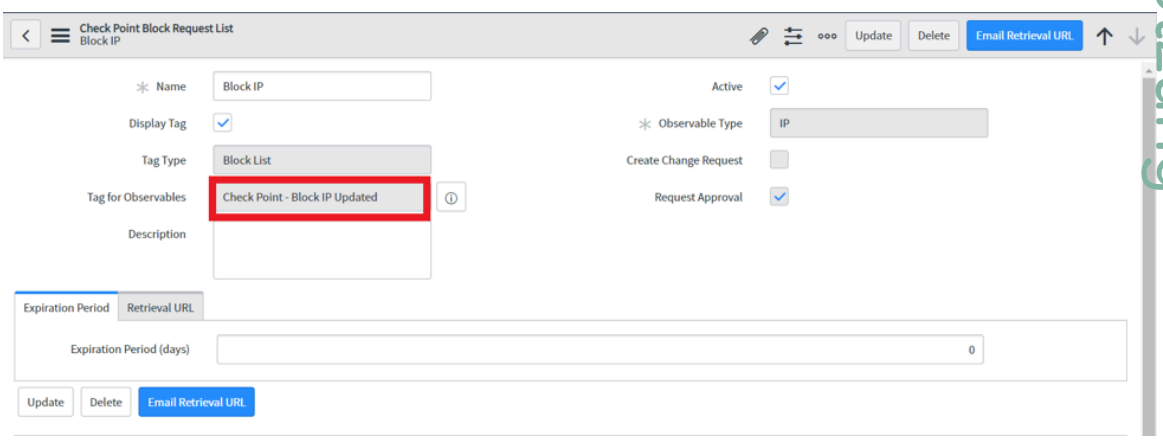


Das Sicherheits-Tag-Formular wird angezeigt.



4. In **Name** Feld ändern Sie den Sicherheits-Tag-Namen.
5. Klicken Sie auf **Aktualisieren**.
   Der aktualisierte Blocklistendatensatz wird mit dem geänderten Tag-Namen angezeigt.

Hinweis:
Im folgenden Beispiel wurde dem Tag-Namen ausgehend hinzugefügt. Behalten Sie das Präfix „Prüfpunkt“ in Ihrem neuen Tag-Namen bei, damit Sie identifizieren können, dass das Tag der Firewall-Integration „Prüfpunkt der nächsten Generation“ zugeordnet ist.

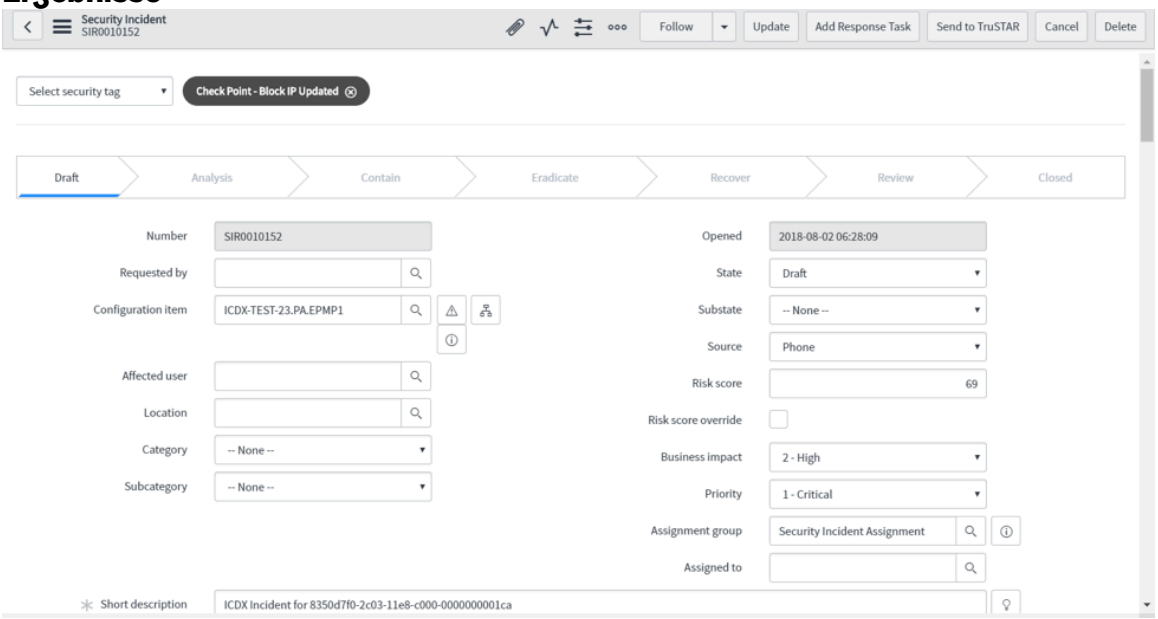


Die Sicherheits-Tags werden für jeden erkennbaren Typ (IP, URL, Domäne) im Security Incident-Datensatz und im Datensatz des erkennbaren Elements jedes Mal angezeigt, wenn das erkennbare Element der Sperrliste hinzugefügt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse



Wenn ein erkennbares Element bereits einer Sperrliste hinzugefügt wurde und ein Sicherheits-Tag für einen Security Incident für dieses erkennbare Element angezeigt wird, wird das Sicherheits-Tag der Sperrliste auch automatisch in allen nachfolgenden Security Incident-Datensätzen angezeigt, die erstellt werden. Diese Duplizierung teilt Ihnen mit, dass sich das erkennbare Element bereits in einer Blockliste befindet. Sie müssen dieses erkennbare Element nicht hinzufügen und erneut blockieren.

Wenn ein erkennbares Element nicht mehr blockiert ist, wird im Security Incident-Datensatz oder im Datensatz des erkennbaren Elements kein Sicherheits-Tag angezeigt. In dieser Instanz gibt kein Sicherheits-Tag an, dass das Ablaufdatum des erkennbaren Elements überschritten ist oder das erkennbare Element in einer Sperrliste deaktiviert wurde.

Deinstallieren Sie Check Point NGTP Integration

Wenn Sie deinstallieren möchten Check Point NGTP Integration von Ihrem ServiceNow AI Platform Instanzen und entfernen Sie alle Reste aus der Integration. Anweisungen zum Deinstallieren von Anwendungen finden Sie auf der ServiceNow-Dokumentationswebsite.

Erforderliche Rolle: admin

Integration mit CrowdStrike Falcon Host

Die CrowdStrike Falcon Host Mit der Integration können Sie erkennbare Elemente in einem Security Incident in eine Beobachtungsliste verschieben, sodass sie zusätzliche Warnungen generieren können. Diese Integration ist eine Implementierung des Workflows CrowdStrike Falcon Host – in Beobachtungsliste veröffentlichen.

Erkunden	Einrichten
Security Incident Response-Integrationen	Beginnen Sie mit dem CrowdStrike Falcon Host Integration

---

Verwenden	Entwickeln

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie Suchen nach erkennbaren Elementen durch	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie Komponenten, die mit einer Anwendung installiert sind

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

CrowdStrike Falcon-Host für Security Operations – Flow „in Beobachtungsliste veröffentlichen“

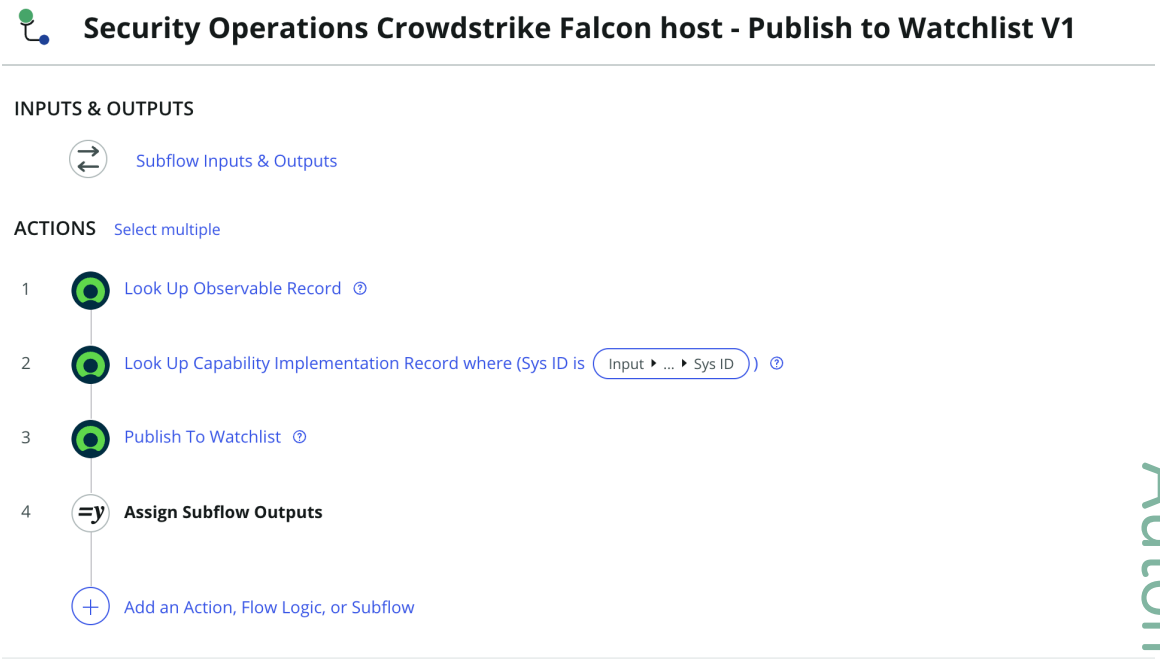
Die **CrowdStrike Falcon-Host für Security Operations: In Beobachtungsliste veröffentlichen** Flow Designer wird verwendet, um die Beobachtungsliste zum Generieren von Warnungen oder Ereignissen anzugeben. Die Warnungen und Ereignisse werden im CrowdStrike Falcon Host-System je nach Konfiguration angezeigt.

Flow „in Beobachtungsliste veröffentlichen“

Dieser Flow Designer wird durch ausgelöst Integration von Security Operations: Funktion „in Beobachtungsliste veröffentlichen“ Wenn Sie ein oder mehrere erkennbare Elemente auswählen, die einem Security Incident zugeordnet sind, und die UI-Aktion in Beobachtungsliste veröffentlichen verwenden, um die erkennbaren Elemente in eine Beobachtungsliste zu verschieben. Die erkennbaren Elemente können dann verwendet werden, um zusätzliche Warnungen zu generieren. Weitere Informationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

finden Sie unter Veröffentlichen Sie erkennbare Elemente in einer Beobachtungsliste einer



Drittpartei.

Beginnen Sie mit dem CrowdStrike Falcon Host Integration

Mit der Integrationskonfigurationsfunktion können Sie Sicherheitsintegrationen von Drittparteien, einschließlich, schnell aktivieren und einrichten CrowdStrike Falcon Host Integration. Bevor Sie verwenden können CrowdStrike Falcon Host Integration müssen Sie sie aus herunterladen ServiceNow Store Und fügen Sie dann einen Anwendernamen und ein Passwort hinzu.

Vorbereitungen

- Wenn Sie ein Upgrade durchführen CrowdStrike Falcon Host Integration aus einer vorherigen Version, dann müssen Sie die vorhandene Konfiguration löschen und eine neue Konfiguration einrichten. Die neue Integration unterstützt die OAUTH2-Authentifizierung. Für dieses Update müssen Sie eingeben **API-Client-ID** Und **API-Client-Geheimnis** Dient zum Authentifizieren und Abschließen der Konfiguration.
- In CrowdStrike Falcon Host Portal **API-Umfänge** , Aktivieren Sie **Lesen** Und **Schreiben** Einstellung für **IOCs (Indikatoren der Gefährdung)** .

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. Klicken Sie auf der Karte CrowdStrike Falcon Host auf **Konfigurieren** .
4. Füllen Sie im Formular die Felder aus, um die Konfiguration abzuschließen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CrowdStrike Falcon-Hostkonfiguration

Feld	Beschreibung
Name	Name der Integration, z. B. `Demo-1` .
API-Client-ID	Die Client-ID, die Sie aus dem Abschnitt „Einstellungen“ Ihres Account-Profils in abrufen CrowdStrike Falcon Host Portal.
API-Client-Geheimnis	Der geheime Clientschlüssel, den Sie im Abschnitt „Einstellungen“ Ihres Account-Profils in abrufen CrowdStrike Falcon Host Portal.

5. Klicken Sie auf **Absenden**.

Ergebnisse

Nachdem konfiguriert wurde, wird CrowdStrike Falcon Host Die Integration kann für die Veröffentlichung erkennbarer Elemente in Beobachtungslisten in ausgewählt werden Security Incident Response.

CrowdStrike Falcon Insight-Integration

Mit CrowdStrike Falcon Insight Für Security Operations Durch die Integration können Sie Korrekturaktionen für die Endpunkte in Echtzeit durchführen, mithilfe von Profilen Details zum Host sammeln und mithilfe von bestimmte Abfragen oder Aktionen für den Endpunkt durchführen ServiceNow AI Platform Security Incident Response Produkt.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Die CrowdStrike Falcon Insight Für Security Operations Die Integration funktioniert mit ServiceNow AI Platform Damit Sie zusätzliche Einblicke in den Umfang eines Incident erhalten können. Die CrowdStrike Falcon Insight Erfasst alle relevanten Endpunkt-Ereignisaktivitäten. Sie können verwenden ServiceNow AI Platform Um sich auf Untersuchungen und Korrekturaktionen zu konzentrieren.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
ServiceNow Produktdokumentations-Website	ServiceNow-Produktdokumentationswebsite
CrowdStrike Falcon Insight für Security Operations	Erste Schritte mit CrowdStrike Falcon Insight Integration

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte mit CrowdStrike Falcon Insight Integration

Sie können aktivieren und einrichten CrowdStrike Falcon Insight Um eine Schnittstelle mit herzustellen ServiceNow AI Platform Instanz und Security Incident Response Produkt.

Erforderliche Rolle: Administrator

Bevor Sie verwenden können CrowdStrike Falcon Insight Für Security Operations Integration müssen Sie sie aus herunterladen ServiceNow Store.

Prüfliste

Setupaufgabe	Beschreibung
Weisen Sie die erforderlichen zu, und verifizieren Sie sie ServiceNow AI Platform Und Security Incident Response Rollen.	Diese Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Die Administratorrolle installiert die Integration aus dem ServiceNow Store Und weist die Rolle sn_si.admin zu. • Die Rolle „sn_si.admin“ konfiguriert die Integration, erstellt und aktiviert Profile und weist dann die Rolle „sn_si.Analyst“ zu. • Die Rolle „sn_si.Analyst“ reagiert auf Security Incidents, startet Profile manuell und kann Anforderungen für Aktionen wie die Isolierung des Hosts und das Entfernen der Host-Isolierung für eine genehmigte Gruppe übermitteln.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie diese Integration konfigurieren.	Die ServiceNow IntegrationHub Enterprise-Paket-Installationsprogramm [Plugin com.glide.hub.integrations.enterprise] ist erforderlich. Dieses Plugin ermöglicht die Ausführung von IntegrationHub-Aktionen und -Flows: Die Security Incident Response Plugin (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Anwendungen, die für die Integration erforderlich sind. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn diese Anwendungen noch nicht installiert sind, müssen Sie jede Anwendung einzeln in der folgenden Reihenfolge installieren und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	aktivieren, um eine reibungslose Installation sicherzustellen: **1.** Security Incident Response Abhängigkeit (com.snc.si_dep) **2.** Sicherheits-Integrations-Framework **3.** Security Support Common **4.** Orchestration Des Sicherheitssupports **5.** Threat Intelligence Support Allgemein **6.** Trusted Security Circles **7.** Security Operations Setup-Assistent **8.** Security Incident Response
Richten Sie eine Genehmigungsgruppe ein.	Eine optionale Genehmigungsfunktion ist verfügbar, um Hostcomputer zu isolieren, im Netzwerk wiederherzustellen und Sichtungssuchen zu initiieren. Zum Aktivieren dieser Option benötigen Sie eine vorherige Genehmigung durch die Rolle „sn_si.admin“, bevor Hostcomputer isoliert und in Ihrem Netzwerk wiederhergestellt werden oder wenn Sichtungssuchen durchgeführt werden. Wenn Sie eine zusätzliche Kontrolle über diese Aktionen benötigen, aktivieren Sie **Genehmigung erforderlich** Option beim Konfigurieren des Profils. Die Genehmigungsbehörde wird dem Anwender mit der Rolle sn_si.admin zugewiesen. Sie können diese Genehmigungsberechtigung auch einer Genehmigungsgruppe zuweisen.
Weisen Sie die Rollen der CrowdStrike Falcon Platform zu, und überprüfen Sie sie.	Die folgenden Rollen sind auf der CrowdStrike Falcon Platform für die Integrationskonfiguration erforderlich: • Die Falcon-Administratorrolle ist erforderlich, um API-Clients oder -Schlüssel anzuzeigen, zu erstellen oder zu ändern. • Die Rolle „Echtzeit-Responder – Administrator“ ist zum Erstellen und Ausführen anwenderdefinierter Skripts erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	• Die Rolle „Echtzeit-Responder – aktiver Responder“ ist zum Erstellen und Ausführen anwenderdefinierter Skripts erforderlich.
Überprüfen Sie, ob die Rollen und Berechtigungen anwenderdefinierter Skripts in der CrowdStrike Falcon Platform aktiviert sind.	Diese Integration verwendet anwenderdefinierte CrowdStrike-Skripts für einige der Ergänzungsfunktionen. • Überprüfen Sie, ob die Rollen „Echtzeit-Beantworter – Administrator“ und „Echtzeit-Beantworter – aktiver Beantworter“ verfügbar sind. • Überprüfen Sie, ob **Standard-Richtlinie (Windows)** Die Option ist in Konfiguration > Antwortrichtlinien in der CrowdStrike Falcon-UI aktiviert. • Überprüfen Sie, ob **Echtzeitantwort** Und **Anwenderdefinierte Skripts** Unter Echtzeitfunktion ist in der CrowdStrike Falcon-UI aktiviert.
Generieren Sie API-Clients und -Schlüssel in der CrowdStrike Falcon Platform.	Erstellen Sie die CrowdStrike-API-Clients oder -Schlüssel in der CrowdStrike Falcon Platform, um sie in zu verwenden ServiceNow AI Platform Integrationskonfiguration.

Erstellen Sie den CrowdStrike-API-Client, und generieren Sie Schlüssel

Erstellen Sie den CrowdStrike-API-Client, und generieren Sie die Client-ID und den Schlüssel, die Sie zum Konfigurieren von verwenden CrowdStrike Falcon Insight Integration.

Vorbereitungen

Erforderliche Rolle: CrowdStrike Falcon-Administrator

Prozedur

1. Navigieren Sie auf der CrowdStrike Falcon Platform zu **API-Clients und Schlüssel** .
2. Klicken Sie in der Tabelle „OAuth2 API-Clients“ auf **Fügen Sie einen neuen API-Client hinzu** .
3. Geben Sie die folgenden Details ein, um Ihren API-Client zu definieren:

Feld	Beschreibung
Client-Name	Geben Sie den Clientnamen ein. Dies ist ein Pflichtfeld.
Beschreibung	Geben Sie die Beschreibung für den Client-Namen ein.
API-Umfänge	Das Definieren der Umfänge ist erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wichtig: Stellen Sie sicher, dass Sie den API-Account aktivieren, und stellen Sie sicher, dass die folgenden Bereiche für den API-Account aktiviert sind: ○ Aktivieren Sie Lese- und Schreibbereiche für die Host-API ○ Aktivieren Sie den Lesebereich für die Indikatoren-API

4. Klicken Sie Auf **Hinzufügen** Um den API-Client zu speichern und die Client-ID und den geheimen Schlüssel zu generieren.

CrowdStrike Falcon Insight installieren und konfigurieren

Installieren und konfigurieren Sie CrowdStrike Falcon Insight Für Security Operations Anwendung aus dem ServiceNow Store Auf Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis:
Sie können eine Fähigkeit nur einem Profil zuordnen. Sie können eine Fähigkeit nicht mehreren Profilen zuordnen. Wenn Sie CrowdStrike-Server konfigurieren, können Sie eine CrowdStrike-Fähigkeit nicht mit mehreren Profilen wiederverwenden, die den CrowdStrike-Server teilen. Ihre Profile können dieselbe CrowdStrike-Fähigkeit haben. Jedes Profil sollte seinen eigenen CrowdStrike-Server verwenden.

Prozedur

1. Laden Sie herunter CrowdStrike Falcon Insight Für die Integration von Security Operations aus dem ServiceNow Store Und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie nach CrowdStrike Falcon Insight Für Security Operations Integrationskachel und klicken Sie auf **Konfigurieren** .
4. Füllen Sie im Formular die Felder aus, um die Konfiguration abzuschließen:

CrowdStrike Falcon Insight-Konfiguration

Feld	Beschreibung
Name	Name der Integration, z. B. `Demo-1` .
CrowdStrike Falcon Insight-API-URL	Basis-URL, die die CrowdStrike-API hostet. Geben Sie die URL mit dem HTTPS-Protokoll ein. Beispiel: https://api.crowdstrike.com.
Client-ID	Die Client-ID, die Sie aus dem Abschnitt „Einstellungen“ Ihres Account-Profils in abrufen CrowdStrike Falcon Insight Portal.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Geheimer Clientschlüssel	Der geheime Clientschlüssel, den Sie im Abschnitt „Einstellungen“ Ihres Account-Profils abrufen CrowdStrike Falcon Insight Portal.

5. Klicken Sie auf **Absenden**.

Ergebnisse

Nachdem die Integration erfolgreich validiert und übermittelt wurde, wird sie auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Sie können anzeigen CrowdStrike Falcon Insight Modul im Anwendungsnavigator.

Erstellen Sie eine Genehmigungsgruppe

Erstellen Sie eine Genehmigungsgruppe für CrowdStrike Falcon Insight Für Security Operations Integration, die Anforderungen zum Isolieren von Hostcomputern, zum Wiederherstellen im Netzwerk und zum Initiieren von Sichtungssuchen genehmigen kann.

Vorbereitungen

Sie können die Genehmigungsberechtigung nicht einer Gruppe neu zuweisen, es sei denn, in Ihrer Instanz ist eine Genehmigungsgruppe verfügbar.

Hinweis:
Die Option „Genehmigungen“ in Profilkonfiguration Wird nur für die Funktionen „Host isolieren“ und „Host-Isolierung entfernen“ angezeigt.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**an.
2. Klicken Sie in der Gruppenliste auf **Neu** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie im Formular die Felder aus.

Genehmigungsgruppenformular

Feld	Beschreibung
Name	Name der Gruppe, die angezeigt wird, wenn Sie eine Genehmigungsanforderung übermitteln.
Gruppen-E-Mail	Gruppen-E-Mail-Verteilerliste oder E-Mail-Adresse des Ansprechpartners, z. B. des Gruppenmanagers
Manager	Name des Gruppenmanagers. Klicken Sie auf das Suchsymbol, um die Liste anzuzeigen.
Übergeordnet	Name der übergeordneten Gruppe, wenn sie einem übergeordneten Element zugeordnet ist.
Typ	Kategorien von Gruppen.
Lieferanten	Vendor_Manager-Rolle, die Sie Anwendern im Lieferantenverwaltungsprozess Ihrer Organisation zuweisen.
Beschreibung	Zusätzliche Informationen zur Gruppe.

4. Klicken Sie auf **Absenden**.
Die neue Gruppe wird in der Gruppenliste angezeigt.

Diese Gruppe ist verfügbar, um Anforderungen zu verarbeiten, wenn Sie aktivieren **Genehmigung erforderlich** Option während der Konfiguration dieses Profils.

Um Anforderungen zu überwachen und zu verarbeiten, die von Anwendern mit der Rolle „sn_si.Analyst“ übermittelt wurden, navigiert jedes Mitglied der Genehmigungsgruppe zu **Meine Genehmigungen** Registerkarte in ServiceNow AI Platform.

Nächste Maßnahme
Der nächste Schritt ist bis Installieren und konfigurieren Die CrowdStrike Falcon Insight Anwendung aus dem ServiceNow Store.

Erstellen Sie ein Fähigkeitsprofil für CrowdStrike Falcon Insight Integration

Erstellen Sie ein Profil, und wählen Sie aus CrowdStrike Falcon Insight Fähigkeiten, die das Profil ausführen soll.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Überlegen Sie, warum Sie ein Profil erstellen möchten, bevor Sie hinzufügen CrowdStrike Falcon Insight Fähigkeiten für IT. In der folgenden Tabelle sind die Fähigkeiten aufgeführt, die Sie einem Profil hinzufügen müssen, wenn das Profil bestimmte Abfragen oder Aktionen ausführen soll.

Sie können ein einzelnes Profil erstellen, das Abfragen nach Systemdetails ausführt, angemeldete Anwender auflistet, laufende Services abruft, laufende Prozesse abruft, Netzwerkstatistiken abruft, isoliert den Host und entfernt den isolierten Host. Alternativ können Sie mehrere Profile erstellen, die jeweils über eine eigene einzelne Fähigkeit verfügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Funktionen zum Isolieren des Hosts, Entfernen der Isolierung und zum Abrufen von Dateien können beim Erstellen eines Profils nicht mit anderen Funktionen zusammengeführt werden.

Profiltypen und erforderliche CrowdStrike Falcon Insight-Fähigkeiten

Zweck des Profils	CrowdStrike-Fähigkeiten
Sammeln Sie Hostdetails und angemeldete Anwender	• **Hostdetails abrufen** • **Angemeldete Anwender abrufen**
Ruft die Netzwerkstatistiken, Prozesse und Services ab, die für einen Host ausgeführt werden	• **Netzwerkstatistiken abrufen** • **Laufende Prozesse Abrufen** • **Laufende Services abrufen**
Isolieren Sie einen Host	**Host isolieren**
Entfernen Sie die Isolierung für einen Host	**Isolation entfernen**
Rufen Sie eine Datei von einem Host-Endpunkt ab	**Datei Abrufen**

Prozedur

1. Navigieren zu **Alle** > **CrowdStrike Falcon Insight-Integration** > **CrowdStrike-Fähigkeitenprofile**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

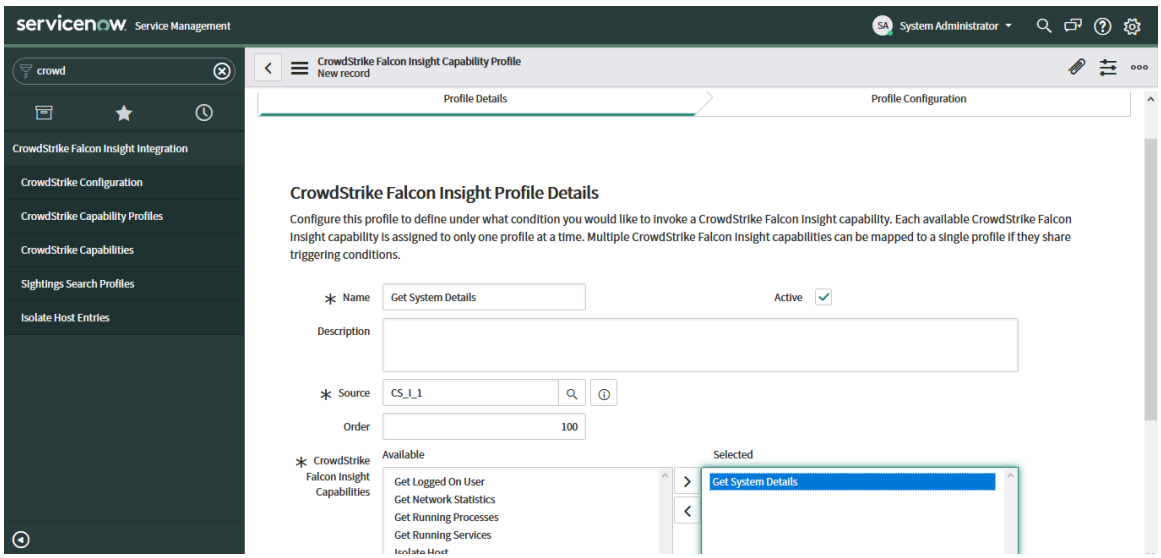
Feld	Beschreibung
Name	Name für das neue Fähigkeitsprofil. Dieser Name hilft Ihnen bei der Identifizierung des Profiltyps und ist auch der Standardname für das Sicherheits-Tag, das diesem Profil zugeordnet ist.
Aktiv	Gibt an, ob das Profil aktiv ist oder nicht. Wenn das Profil aktiv ist, wird es automatisch ausgelöst, wenn ein Security Incident erstellt wird, der den von Ihnen in der Konfiguration angegebenen Filterbedingungen entspricht.
Beschreibung	Eindeutige Beschreibung für das Fähigkeitsprofil.
Quelle	Name des Servers. Sie können zuvor konfigurierte Server nur aus der Liste anzeigen.
Reihenfolge	Flow-Priorität. Der Wert für dieses Feld gibt die Reihenfolge an, in der Flows

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen teilen. Der Flow mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Beispiel: 100, 200, 300, 400. Standard: 100
CrowdStrike Falcon Insight-Fähigkeiten	Fähigkeiten des CrowdStrike Falcon Insight-Profils. Wählen Sie die Fähigkeiten aus, die Sie für dieses Profil wünschen **Verfügbar** Zu **Ausgewählt** Spalte.

Das folgende Beispiel zeigt ein vollständiges Formular für ein Profil mit der Fähigkeit „Systemdetails abrufen“.



4. Klicken Sie auf **Next (Weiter)**.

Nächste Maßnahme

Jetzt können Sie es Konfigurieren Sie Ihr Profil . Stellen Sie sicher, dass Sie haben Hat die Konzepte für die Konfiguration von Profilen und Auslöserbedingungen überprüft Bevor Sie das Profil konfigurieren.

Konfigurieren Sie Profile und Security Incidents für CrowdStrike Falcon Insight Integration

Konfigurieren Sie Ihre Profileinstellungen so, dass das Profil nur unter den von Ihnen festgelegten Bedingungen ausgelöst wird.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Definieren Sie die Bedingungen, die automatisch auslösen CrowdStrike Falcon Insight Fähigkeiten, die Sie für das Profil ausgewählt haben. Sie können auch ein alternatives Eingabefeld für das Feld Configuration Item (CI) auswählen. In diesem alternativen Feld

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können Sie Filterbedingungen festlegen, damit nur die Security Incidents, die sich auf Ihr auslösendes Ereignis beziehen, das Profil automatisch auslösen.

Hinweis:
Navigieren Sie erst zur Seite „Profilkonfiguration“, nachdem Sie die Profildetails eingegeben haben. Weitere Informationen finden Sie unter Erstellen Sie ein Fähigkeitsprofil für die CrowdStrike Falcon Insight-Integration .

Prozedur

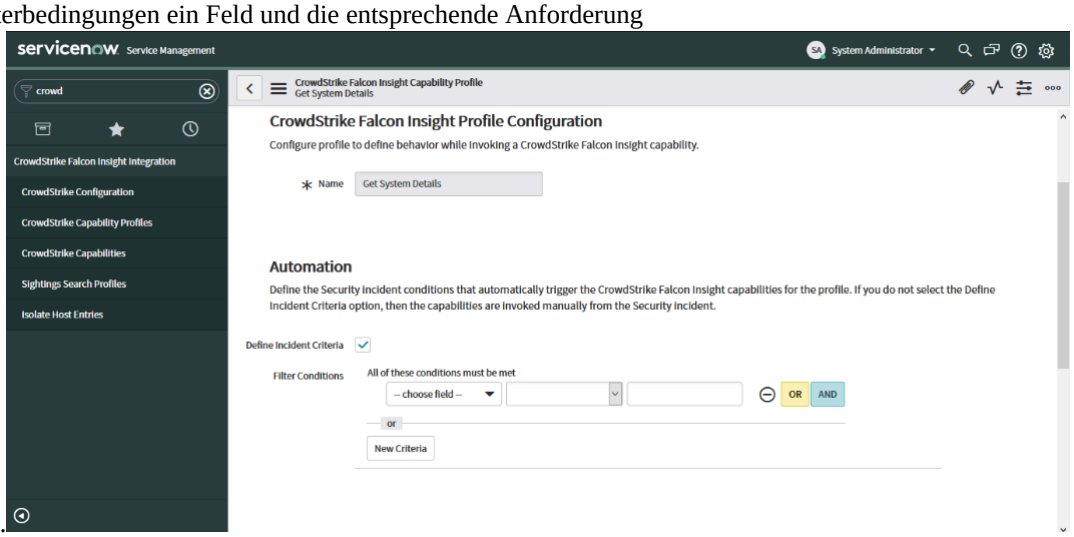
1. Überprüfen und konfigurieren Sie auf der Seite „Profilkonfiguration“ die folgenden Abschnitte:

Incident-Kriterien Definieren (Automatisierung)

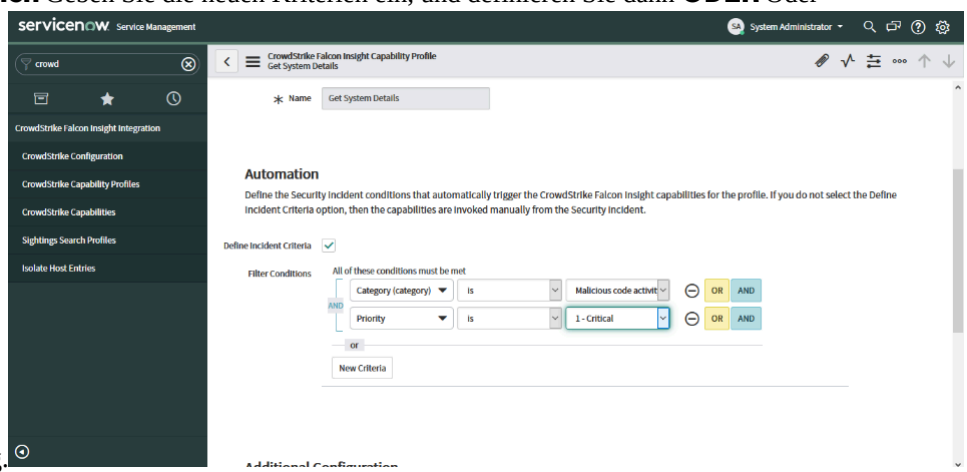
Definieren Sie die Security Incident-Bedingungen, die automatisch auslösen CrowdStrike Falcon Insight Fähigkeiten für das Profil. Wenn Sie nicht auswählen **Definieren Sie Incident-Kriterien** Option werden die Fähigkeiten manuell aus dem Security Incident aufgerufen.

a. Wählen Sie aus **Definieren Sie Incident-Kriterien** Option.

b. Um die Bedingungen zu definieren, wählen Sie im Abschnitt Filterbedingungen ein Feld und die entsprechende Anforderung aus.



c. In **Neue Kriterien** Geben Sie die neuen Kriterien ein, und definieren Sie dann **ODER** Oder **UND**Bedingung.



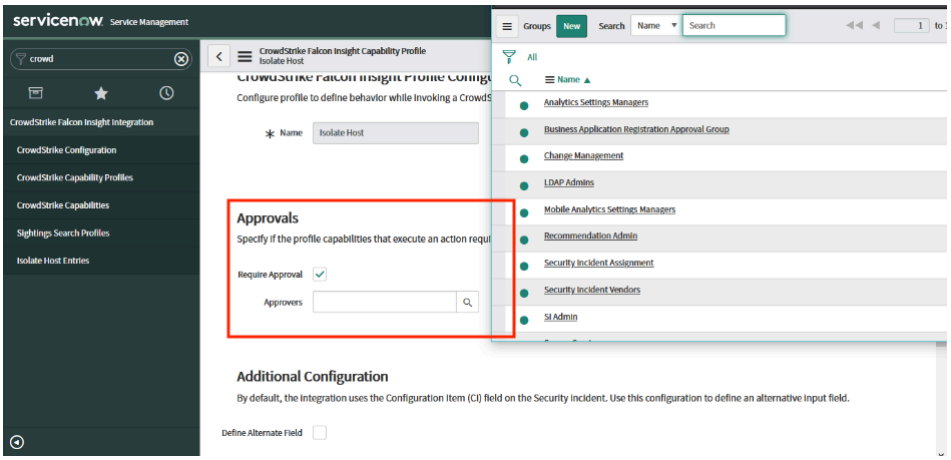
Genehmigungen

Um bei der Verwendung der CrowdStrike Falcon Insight-Funktionen eine zusätzliche Steuerungsstufe zu bieten, wählen Sie aus **Genehmigung Erforderlich** Option. Die Option

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigungen in der Profilkonfiguration wird nur für die Funktionen Host isolieren und Host-Isolation entfernen angezeigt.

Hinweis:
Die Genehmigungsbehörde wird dem Anwender mit der Rolle sn_si.admin zugewiesen. Sie können diese Genehmigungsberechtigung auch einer Genehmigungsgruppe zuweisen. Weitere Informationen finden Sie unter Richten Sie eine Genehmigungsgruppe ein .



Zusätzliche Konfiguration

Wählen Sie ein alternatives Feld im Security Incident aus, um alle übereinstimmenden CI-Daten anzuzeigen, die Sie beim Scannen Ihrer Assets finden. Standardmäßig verwendet die Integration das Feld Configuration Item (CI) für den Security Incident.

a. Wählen Sie aus **Definieren Sie Ein Alternatives Feld** Option.

b. In **Alternatives CI-Auslöserfeld** , Wählen Sie ein Eingabefeld aus.

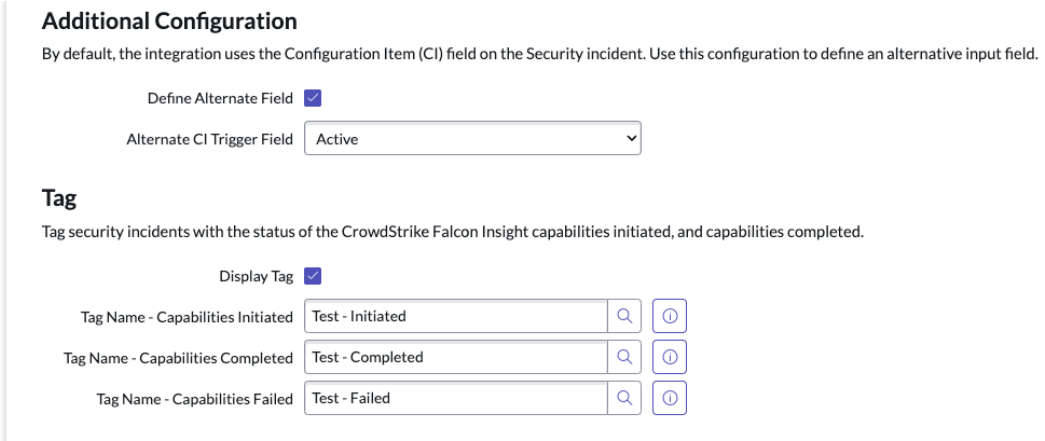
Hinweis:
Weitere Informationen finden Sie unter Verstehen Sie, wie Auslöserbedingungen mit einem Konfigurationselement für ein Profil funktionieren .

Tags

Dient zum Taggen von Security Incidents mit CrowdStrike Falcon Insight Tags „Fähigkeiten – initiiert“ und „Fähigkeiten – abgeschlossen“ und „Fähigkeiten – Fehlgeschlagen“ wählen Sie aus **Tags Anzeigen** Option. Standardmäßig ist diese Option für alle Profile deaktiviert.

Hinweis:
Diese Tags werden mit dem Basissystem bereitgestellt. Sie können bei Bedarf eigene Tags erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Klicken Sie auf **Erledigt**.

Wie Auslöserbedingungen mit einem Konfigurationselement für ein Profil funktionieren

Sie können die Profileinstellungen so konfigurieren, dass ein Profil nur ausgeführt wird, wenn eine Reihe bestimmter Bedingungen erfüllt ist, oder Sie können ein Profil einrichten, um nach bestimmten Feldwerten für einen Security Incident zu suchen.

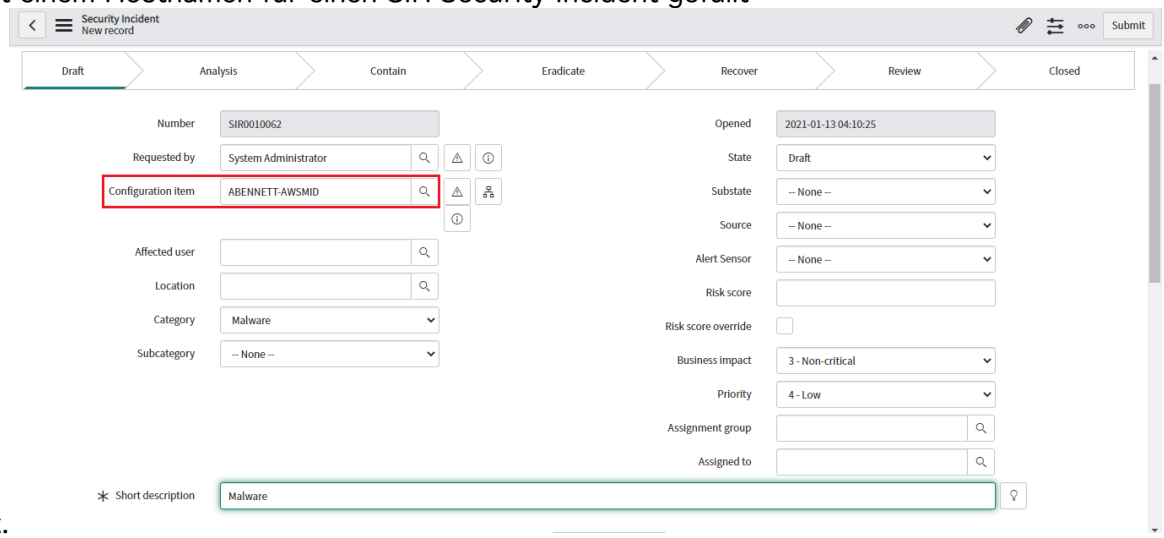
Nachdem Sie ein Profil erstellt und ausgewählt haben CrowdStrike Falcon Insight Fähigkeiten, auf denen das Profil ausgeführt werden soll. Sie können Auslöserbedingungen festlegen, damit Ihr Profil automatisch ausgeführt wird, wenn die Standardfeldwerte mit übereinstimmen ServiceNow AI Platform Security Incident.

Standardmäßig verwendet die -Integration **Konfigurationselement** (CI) Feld in einem Security Incident. Dieses Feld wird verwendet, um Ihre Asset-IDs mit den Informationen abzugleichen, die in gespeichert sind ServiceNow AI Platform Datenbank. Wenn ein SIR Security Incident durch ein Sicherheitsereignis erstellt und ein Profil aktiviert wird, werden Ihre Assets nach einem übereinstimmenden Wert im Hostnamen oder einer IP-Adresse gescannt.

Wenn ein übereinstimmender Wert in der Datenbank gefunden wird, werden diese Daten aus dem gesammelt CrowdStrike Falcon Insight-Konsole und wird in abgerufen ServiceNow AI Platform Instanz, in der sie in den zugehörigen Listen eines Security Incidents angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beispiel zeigt ein Konfigurationselement-Feld, das mit einem Hostnamen für einen SIR Security Incident gefüllt

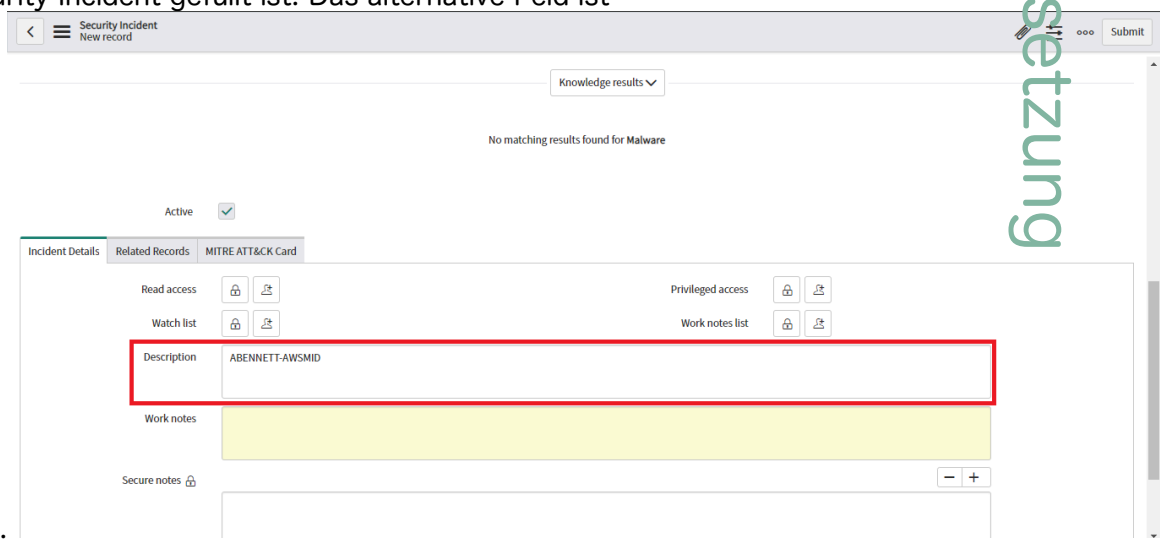


ist.

Wenn **Konfigurationselement** Das Feld (CI) ist nicht mit einem Hostnamen oder einer IP-Adresse gefüllt, die der Datenbank entspricht. Sie können ein anderes Feld im Security Incident auswählen, um alle übereinstimmenden CI-Daten anzuzeigen, die Sie beim Scannen Ihrer Assets finden.

Wenn Sie das Profil-Setup konfigurieren, können Sie eine Alternative auswählen **CI-Auslöser** Feld für die Endpunktidentifizierung, um sicherzustellen, dass die CI-Daten aus dem CrowdStrike Falcon Insight Die Suche wird für den zugehörigen Security Incident ausgefüllt. Sie können jedes Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich anwenderdefinierter Felder, die Sie erstellen. Wenn das Feld CI beim Erstellen des Incident nicht für den zugehörigen Security Incident ausgefüllt ist, wählen Sie das Feld alternatives CI aus, um sicherzustellen, dass Ihre Profile ausgelöst werden.

Das folgende Beispiel zeigt ein alternatives Feld, das mit einem Hostnamen für einen SIR Security Incident gefüllt ist. Das alternative Feld ist



BeschreibungFeld.

Verifizieren CrowdStrike Falcon Insight Auslöserbedingungen für Profil

Testen Sie das Profil, und überprüfen Sie, ob die Auslöserbedingungsfilter, die Sie konfiguriert haben, wie erwartet funktionieren.

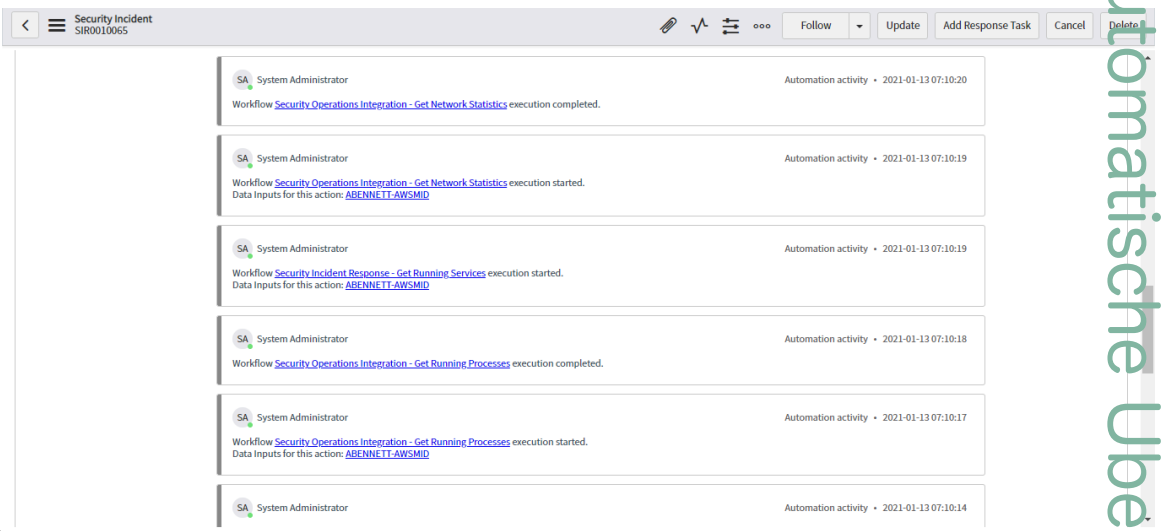
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

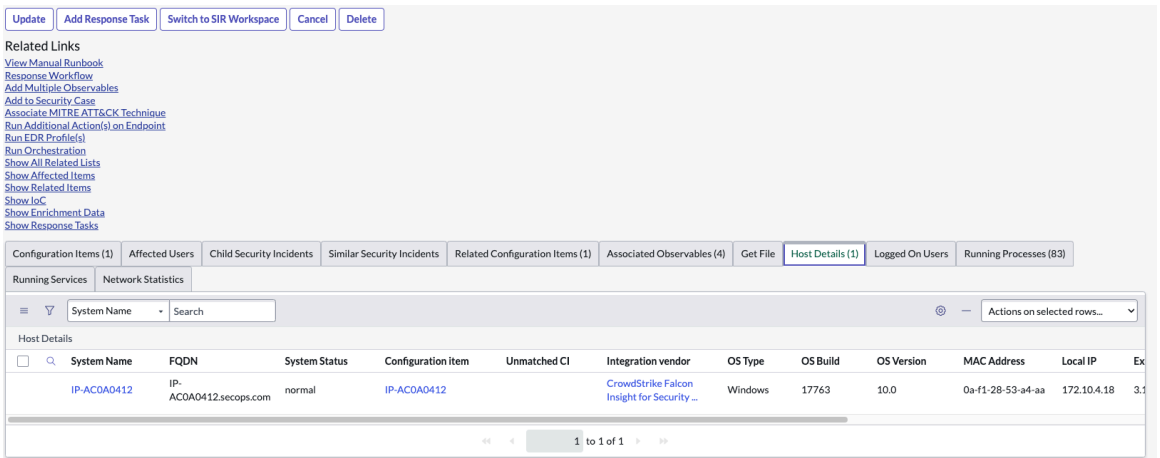
Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Aktivieren Sie das Profil, das auf den von Ihnen angegebenen konfigurierten Auslöserbedingungen basiert, damit Sie die Abfrageergebnisse in anzeigen können ServiceNow AI Platform Security Incidents.

Prozedur
1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie Aus **Neu** Dient zum Erstellen eines Security Incidents.
3. Um einen Security Incident zu erstellen, geben Sie die erforderlichen Informationen ein, und klicken Sie auf **Speichern** .
4. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“, um die Tags „Profil initiiert“ und „Profil abgeschlossen“ anzuzeigen.



5. Überprüfen Sie die Details in CrowdStrike Falcon Insight Details zu zugehörigen Listen wie „Datei abrufen“, „Hostdetails“, „angemeldete Anwender“, „laufende Prozesse“, „ausgeführte Services“, Netzwerkstatistiken usw.



Lösen Sie einen aus CrowdStrike Falcon Insight Profil manuell aus einem Security Incident
Lösen Sie ein Profil manuell aus, nachdem Sie einen Security Incident überprüft haben.

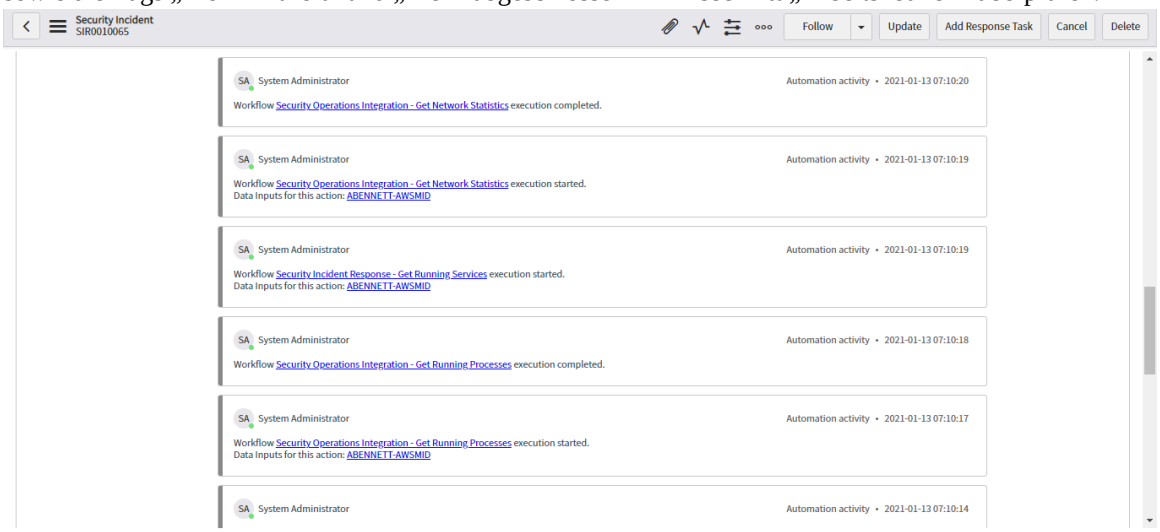
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

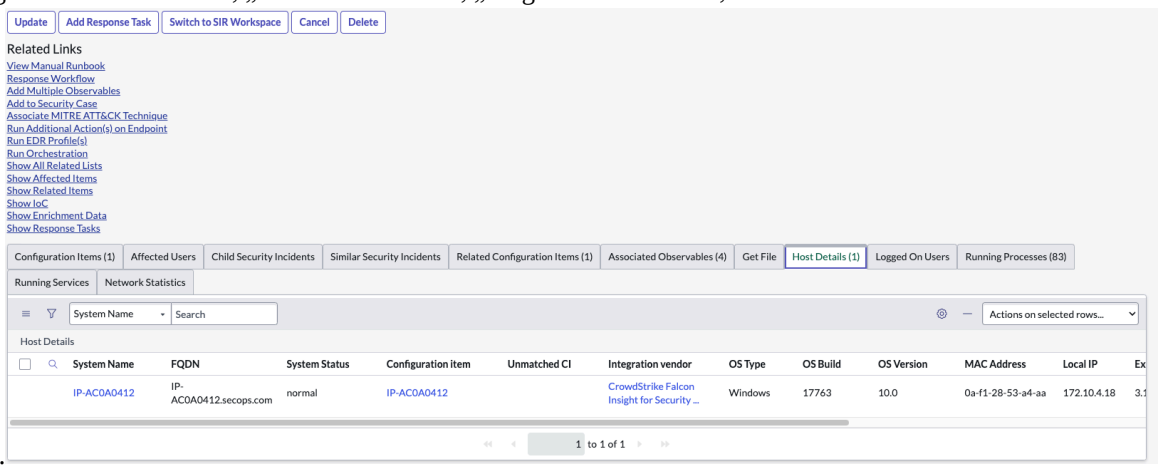
Warum und wann dieser Vorgang ausgeführt wird
Sobald Sie das Profil basierend auf den konfigurierten Auslöserbedingungen aktiviert haben, können Sie die Abfrageergebnisse in anzeigen ServiceNow AI Platform Security Incidents. CrowdStrike Falcon Insight Ermöglicht Ihnen auch die Ausführung einzelner Fähigkeiten für Konfigurationselemente (Configuration Items, CIs) ohne Verwendung eines Profils.

Prozedur
1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit überprüfen möchten CrowdStrike Falcon Insight Informationen.
3. Wählen Sie im Abschnitt zugehörige Listen die Option aus **EDR-Profil(e) ausführen** .
4. Durchsuchen und wählen Sie ein Profil aus der Liste der verfügbaren Profile aus.
5. Wählen Sie Aus **Zugehöriges CI einschließen** Um dieses Profil für alle zugehörigen CIs des Profils auszuführen.
   Wenn dem Security Incident beispielsweise fünf CIs zugeordnet sind, wird das ausgewählte Profil für alle fünf CIs ausgeführt.
6. Klicken Sie auf **Absenden**.
   Das ausgewählte Profil wird manuell ausgelöst. Sie können den Abschnitt „Arbeitsnotizen und Aktivitäten“ sowie die Tags „Profil initiiert“ und „Profil abgeschlossen“ im Abschnitt „Arbeitsnotizen“ überprüfen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Die Ergebnisse werden in Form von zugehörigen Listen angezeigt, z. B. „Datei abrufen“, „Hostdetails“, „angemeldete Anwender“, „laufende Prozesse“, „ausgeführte Services“, Netzwerkstatistiken usw.



8. Führen Sie die folgenden Schritte aus, um einzelne Fähigkeiten für ein CI auszuführen:

   a. Wählen Sie in der zugehörigen Liste Konfigurationselemente das erforderliche CI aus.

   b. Klicken Sie auf **Aktionen für ausgewählte Zeilen...** Dropdown-Liste, und wählen Sie die erforderliche Fähigkeit aus, die Sie für das ausgewählte CI ausführen möchten.
   Beispiel: Host isolieren.

   c. Suchen Sie mithilfe der Suchoption nach der erforderlichen Fähigkeitsimplementierung für das CI, und wählen Sie aus **CrowdStrike Falcon Insight – Host isolieren** .

   d. Klicken Sie Auf **Host Isolieren** Um sie für das ausgewählte CI auszuführen.

Erstellen und konfigurieren Sie ein Profil für die Sichtungssuche

Sichtungssuchen für verwenden CrowdStrike Falcon Insight Um infizierte Computer im Netzwerk Ihrer Organisation zu lokalisieren und Security Incident Response-Fälle zu behandeln.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Sichtungssuche in durch CrowdStrike Falcon Insight Dient zur Bestimmung der Verbreitung einer Bedrohung im Zeitverlauf.

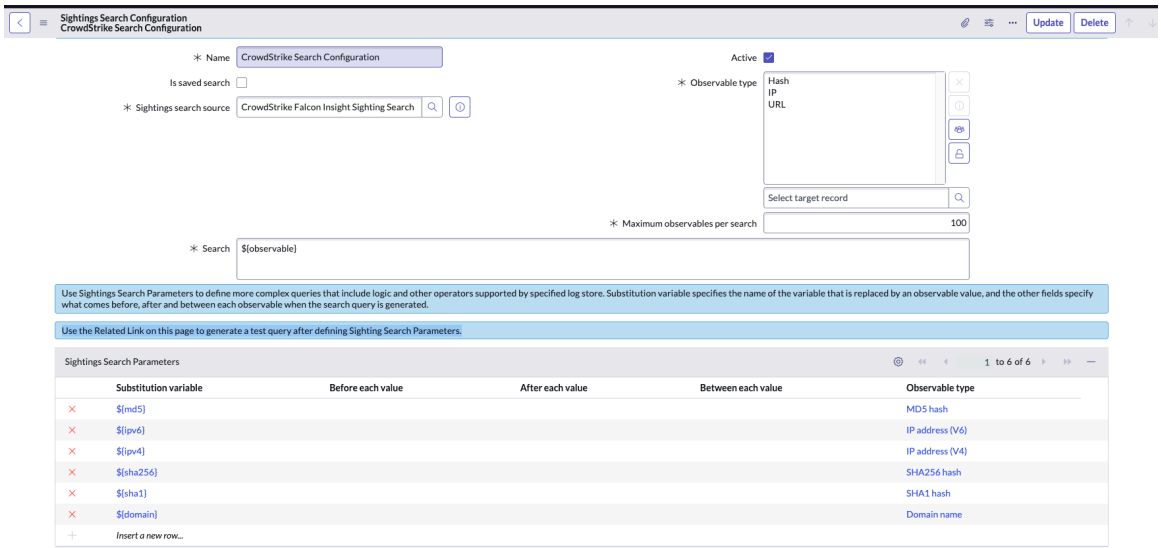
Prozedur

1. Navigieren zu **Alle** > **CrowdStrike Falcon Insight-Integration** > **Sichtungssuchprofile**an.
2. Klicken Sie auf **Neu**.
3. Konfigurieren Sie dieses Profil, um zu bestimmen, welche Server nach einer bestimmten CrowdStrike Falcon Insight-Suchfunktion gesucht werden sollen.
4. Füllen Sie im Formular die folgenden Felder aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name für das Sichtungssuchprofil.
Ist gespeicherte Suche	Wenn Sie diese Option auswählen, wird eine gespeicherte Suchkonfiguration erstellt.
Sichtungssuchquelle	Die Quelle für die Sichtungssuche. Wählen Sie aus **CrowdStrike Falcon Insight-Sichtungssuche** Als Quelle.
Aktiv	Option, um anzugeben, ob zusätzliche aktiv ist oder nicht.
Typ des erkennbaren Elements	Die CrowdStrike Falcon Insight-Integration unterstützt die folgenden Typen erkennbarer Elemente: ○ Hash ○ IP ○ URL Die Sichtungssuche wird für die folgenden erkennbaren Elemente unterstützt: ○ Domänenname ○ IP-Adresse (v4) ○ IP-Adresse (V6) ○ MD5-Hash ○ SHA1-Hash ○ SHA256-Hash
Maximale erkennbare Elemente pro Suche	Maximale Anzahl erkennbarer Elemente, die Sie in einer Suchabfrage anzeigen können.
Suchen	Die Standardsuchzeichenfolge ist `$(erkennbares Element)` , Sie können jedoch Ihre eigene Suchabfrage definieren, indem Sie Parameter angeben, die von unterstützt werden CrowdStrike Falcon Insight Integration.
Sichtungssuchparameter	Parameter zum Definieren komplexerer Abfragen, die Logik und andere Operatoren enthalten, die vom angegebenen Protokollspeicher unterstützt werden Sie können die zugehörigen Links unten auf der Seite verwenden, um eine Testabfrage zu generieren, nachdem Sie Sichtungssuchparameter definiert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Absenden**.
   Die Konfiguration ist abgeschlossen, und Sie können die Sichtungssuche über aufrufen ServiceNow AI Platform Security Incident.
6. Führen Sie die folgenden Schritte aus, um die Konfiguration zu überprüfen und eine Sichtungssuche auszuführen:

   a. Öffnen Sie einen Security Incident, scrollen Sie zum Ende des Security Incident, und klicken Sie auf **Alle zugehörigen Listen anzeigen** .

   b. Wenn Sie ein oder mehrere Konfigurationselemente (Configuration Items, CI) aus auswählen **Laufende Prozesse** Zugehörige Listen.

   > **Hinweis:**
   > Wenn Sie eine Sichtungssuche nach einem CI aus der zugehörigen Liste laufende Prozesse ausführen, ist es nur eine Prozess-Hash-Sichtungssuche.

   c. Klicken Sie auf **Aktionen für ausgewählte Zeilen...** Dropdown-Liste, und wählen Sie aus **Führen Sie die CrowdStrike-Sichtungssuche aus** .

   d. Suchen Sie mithilfe der Suchoption nach dem erforderlichen Sichtungssuchprofil.

   e. Wählen Sie das erforderliche Sichtungssuchprofil aus, und klicken Sie auf **Übermitteln** .

   f. Wenn Sie ein oder mehrere erkennbare Elemente aus auswählen **Zugeordnete Erkennbare Elemente** Zugehörige Listen.

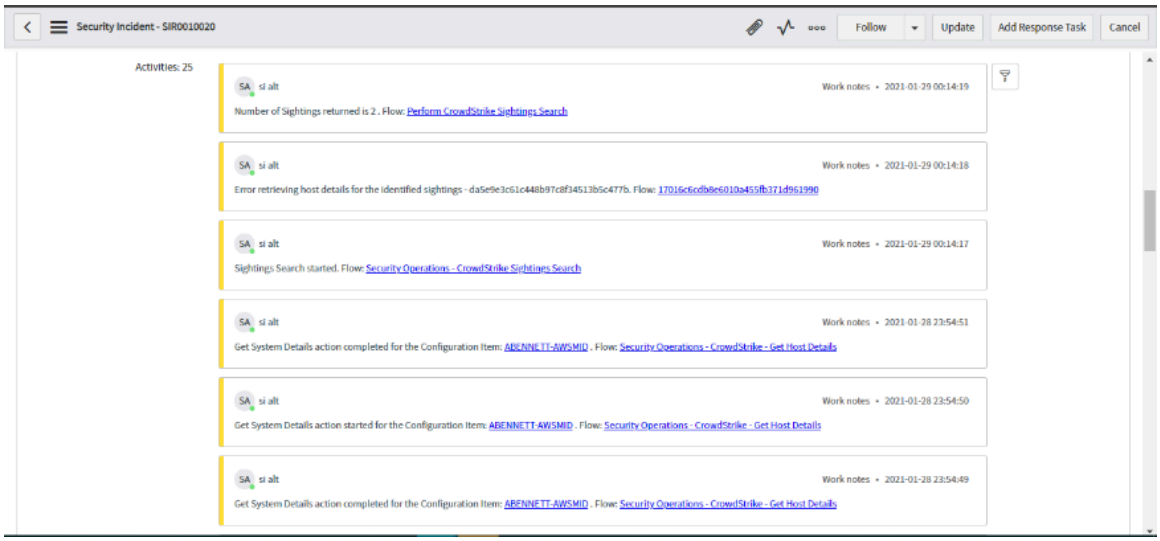
   g. Klicken Sie auf **Aktionen für ausgewählte Zeilen...** Dropdown-Liste, und wählen Sie aus **Sichtungssuche Ausführen** .

   h. Wählen Sie im Popup-Fenster „Zeitrahmen“ einen beliebigen zufälligen Wert aus, und klicken Sie auf **Suchen** .

   i. Validieren Sie nach Abschluss der Suche die Ergebnisse und Details in den Arbeitsnotizen und zugehörigen Listen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



j. Wählen Sie aus **Sichtungen** Registerkarte zum Anzeigen der Sichtungsdetails.

k. Klicken Sie auf **Vorschau** Symbol neben dem CI, um weitere Informationen zu CrowdStrike-Sichtungsdetails anzuzeigen.

l. Klicken Sie auf **Sichtungssuchdetails** Um die Sichtungssuchdetails anzuzeigen, klicken Sie auf **Sichtungssuchergebnisse** Registerkarte für Suchergebnisse.

Konfigurieren und lösen Sie zusätzliche Aktionen in aus CrowdStrike Falcon Insight

Die CrowdStrike Falcon Insight Die Integration unterstützt die Ausführung zusätzlicher Aktionen wie regulärer Ausdruck (regulärer Ausdruck). Die CrowdStrike Falcon Insight Die Integration bietet 40 zusätzliche Aktionen mit dem Basissystem.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

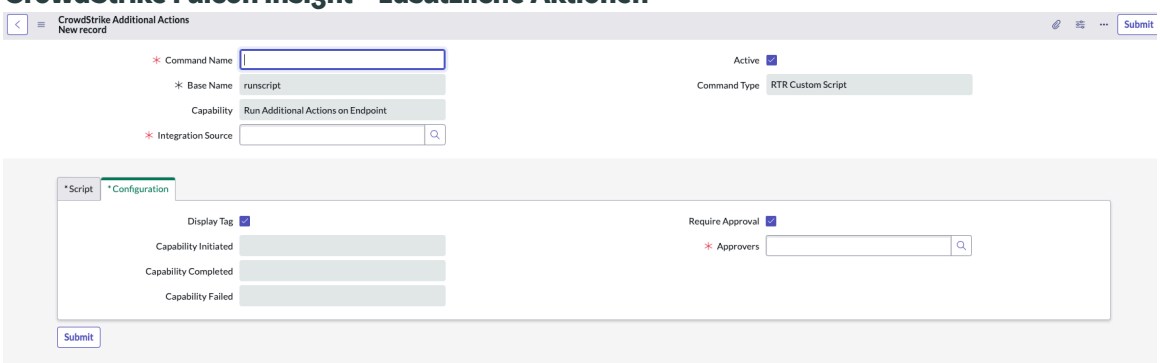
1. Navigieren zu **Alle** > **CrowdStrike Falcon Insight-Integration** > **CrowdStrike: zusätzliche Aktionen**an.
2. Klicken Sie Auf **Neu** Um eine eigene zusätzliche Aktion zu erstellen oder eine vorhandene Aktion auszuwählen, die im Basissystem enthalten ist.
   Erstellen wir beispielsweise eine neue zusätzliche Aktion.
3. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Befehlsname	Befehlsname für die zusätzliche Aktion. Beispiel: „Registrierungssatz“.
Basisname	Basisname für die zusätzliche Aktion. Dieses Feld ist standardmäßig festgelegt. Beispiel: „Reg.“
Fähigkeit	Fähigkeitsname für die zusätzliche Aktion. Dieses Feld ist standardmäßig festgelegt. Beispiel: Zusätzliche Aktionen für Endpunkt ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Integrationsquelle	Die Quelle für die zusätzliche Aktion. Beispiel: CrowdStrike Falcon Insight-Integration.
Aktiv	Option, um anzugeben, ob zusätzliche aktiv ist oder nicht.
Befehlstyp	Befehlstyp für die zusätzliche Aktion. Dieses Feld ist standardmäßig festgelegt. Beispiel: Anwenderdefiniertes RTR-Skript.
Skript	○ **BS-Typ** : Option zum Auswählen des Betriebssystemtyps für Ihr Skript. Wählen Sie eine der folgenden Optionen aus: ▪ **Windows** ▪ **Mac OS X** ▪ **Linux** ▪ **Keine** ○ **Skript** : Option zum Eingeben Ihres Skripts, wenn Sie eines der folgenden Betriebssysteme ausgewählt haben, mit Ausnahme der Option „keine“.
Konfiguration	○ **Tag Anzeigen** : Option zum Anzeigen des Tags für die Konfiguration. Sie können das Tag für die folgenden Felder auswählen: ▪ Fähigkeit: Initiiert. Beispiel: Registrierungssatz – initiiert. ▪ Fähigkeit: Abgeschlossen. Beispiel: Registrierungssatz – Abgeschlossen. ▪ Fähigkeit: Fehlgeschlagen. Beispiel: Registrierungssatz – Fehlgeschlagen. ○ **Genehmigung Erforderlich** : Option zum Auswählen eines Genehmigers oder einer Gruppe, der die Konfiguration genehmigen muss.

CrowdStrike Falcon Insight – zusätzliche Aktionen

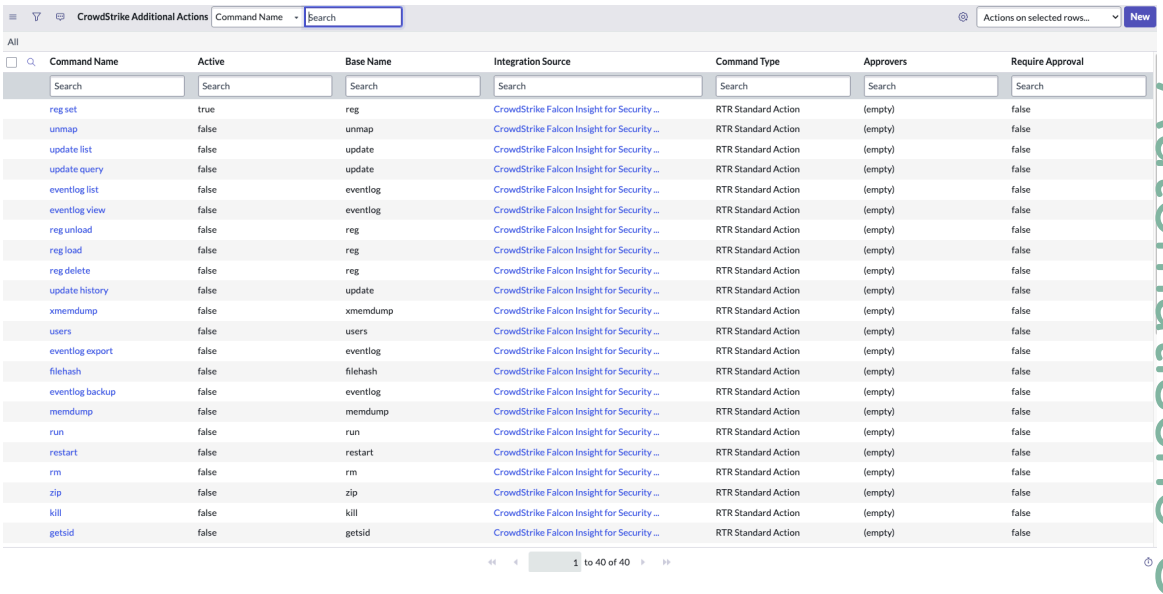


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.
5. Sie können auch aus den folgenden vorhandenen zusätzlichen Aktionen auswählen.
   Das Basissystem enthält 40 zusätzliche Aktionen, mit denen Sie zusätzliche Konfigurationen ausführen können.

Hinweis:
Stellen Sie sicher, dass Sie die Liste „zusätzliche CrowdStrike-Aktionen“ öffnen und die erforderliche zusätzliche Aktion auf festlegen **Wahr** , Andernfalls ist die zusätzliche Aktion im Arbeitsbereich nicht verfügbar.

Liste der zusätzlichen Aktionen, die im Lieferumfang des Basissystems enthalten sind



CrowdStrike Additional Actions | Command Name | Search | Actions on selected rows... | New

All

Command Name	Active	Base Name	Integration Source	Command Type	Approvers	Require Approval
reg set	true	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
unmap	false	unmap	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update list	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update query	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog list	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog view	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg unload	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg load	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
reg delete	false	reg	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
update history	false	update	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
xmemdump	false	xmemdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
users	false	users	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog export	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
filehash	false	filehash	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
eventlog backup	false	eventlog	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
memdump	false	memdump	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
run	false	run	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
restart	false	restart	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
rm	false	rm	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
zip	false	zip	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
kill	false	kill	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false
getsid	false	getsid	CrowdStrike Falcon Insight for Security ...	RTR Standard Action	(empty)	false

1 to 40 of 40

6. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
7. Wählen Sie den Security Incident aus, den Sie mit dem Ausführen zusätzlicher Aktionen für Endpunkt überprüfen möchten.
   a. Klicken Sie im Abschnitt „zugehörige Links“ auf **Führen Sie zusätzliche Aktionen für Endpunkt aus**an.
   b. Durchsuchen und wählen Sie die erforderliche Fähigkeit aus.
      Klicken Sie beispielsweise auf **regelungssatz** Fähigkeit.
   c. Wählen Sie Aus **Zugehöriges CI einschließen** Zum Ausführen der zusätzlichen Aktionen für alle zugehörigen CIs des Endpunkts.
   d. Sie können definieren **Unterschlüssel** Führen Sie für die zusätzliche Aktionen für Endpunkt aus. Dieser Unterschlüssel kann ein HKLM/Software/neuer Schlüssel sein.
8. Klicken Sie auf, um die Ausführung zusätzlicher Aktionen für den Endpunkt zu initiieren **Zusätzliche Aktion Ausführen** .
9. Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.
10. Validiert den Status der Aktion in den zugehörigen Listen „zusätzliche Aktionen in Endpunktlisten“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden CrowdStrike Falcon Insight Integration in Analysten-Arbeitsbereich

Verwenden Sie CrowdStrike Falcon Insight Integration zur Nutzung von CrowdStrike Falcon Insight Fähigkeiten im SIR Analyst-Arbeitsbereich.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Bevor Sie verwenden CrowdStrike Falcon Insight Integration im Security Incident Response-Arbeitsbereich müssen Sie sie aus herunterladen ServiceNow Store Und konfigurieren Sie es. Weitere Informationen finden Sie unter Erste Schritte mit CrowdStrike Falcon Insight Integration.

Warum und wann dieser Vorgang ausgeführt wird

Sie können verwenden CrowdStrike Falcon Insight Integration, um Korrekturaktionen für die Endpunkte in Echtzeit durchzuführen, mithilfe von Profilen Details zum Host zu erfassen und mithilfe von bestimmte Abfragen oder Aktionen für den Endpunkt durchzuführen Security Incident Response Arbeitsbereich.

Die CrowdStrike Falcon Insight Durch die Integration können Analysten Folgendes verwenden CrowdStrike Falcon Insight-Fähigkeiten in Security Incident Response Arbeitsbereich für Analysten:

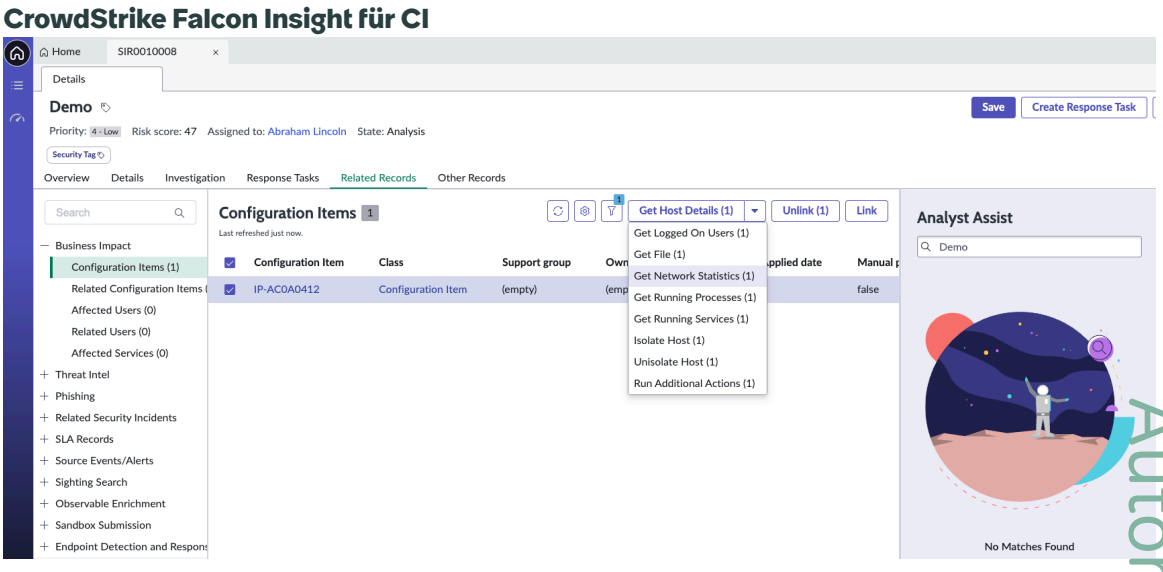
- **Hostdetails abrufen**
- **Angemeldete Anwender abrufen**
- **Netzwerkstatistiken abrufen**
- **Laufende Prozesse Abrufen**
- **Laufende Services abrufen**
- **Host isolieren**
- **Isolation entfernen**
- **Datei Abrufen**

Prozedur

1. Öffnen Sie im SIR-Arbeitsbereich den erforderlichen Security Incident, und wählen Sie aus **Zugehörige Datensätze** Registerkarte.
2. Sie können die CrowdStrike Falcon Insight-Fähigkeiten in der zugehörigen Liste „Geschäftsauswirkung“ für Analysen verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie ein aus **Konfigurationselement** , Und wählen Sie eine Fähigkeit aus der Dropdown-Liste aus.



b. Wählen Sie aus **CrowdStrike Falcon Insight** Implementierung, und klicken Sie auf **Übermitteln** . Die Funktion „Netzwerkstatistiken abrufen“ wird für das CI aufgerufen. Sie können die Arbeitsnotizen für die Ergebnisse und Ergebnisse anzeigen.

3. Sie können die CrowdStrike Falcon Insight-Fähigkeiten im verwenden **Endpunkterkennung und -Antwort (EDR)** Zugehörige Liste für Analyse.

a. Wählen Sie in der zugehörigen Liste Endpunkterkennung und -Antwort (EDR) einen EDR aus der Liste aus.

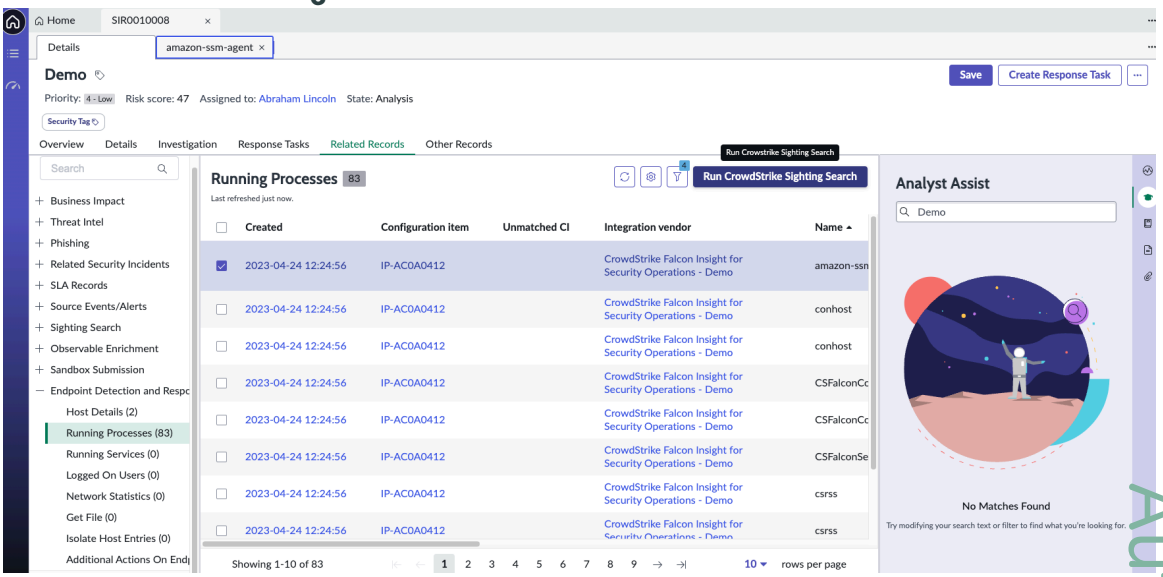
b. Klicken Sie auf einen bestimmten laufenden Prozess, um die Details des laufenden CrowdStrike Falcon Insight-Prozesses anzuzeigen.

c. Um eine CrowdStrike Falcon-Sichtungssuche für einen bestimmten laufenden Prozess auszuführen, wählen Sie den laufenden Prozess aus, und klicken Sie auf **CrowdStrike-Sichtung ausführen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CrowdStrike Falcon Insight für EDR



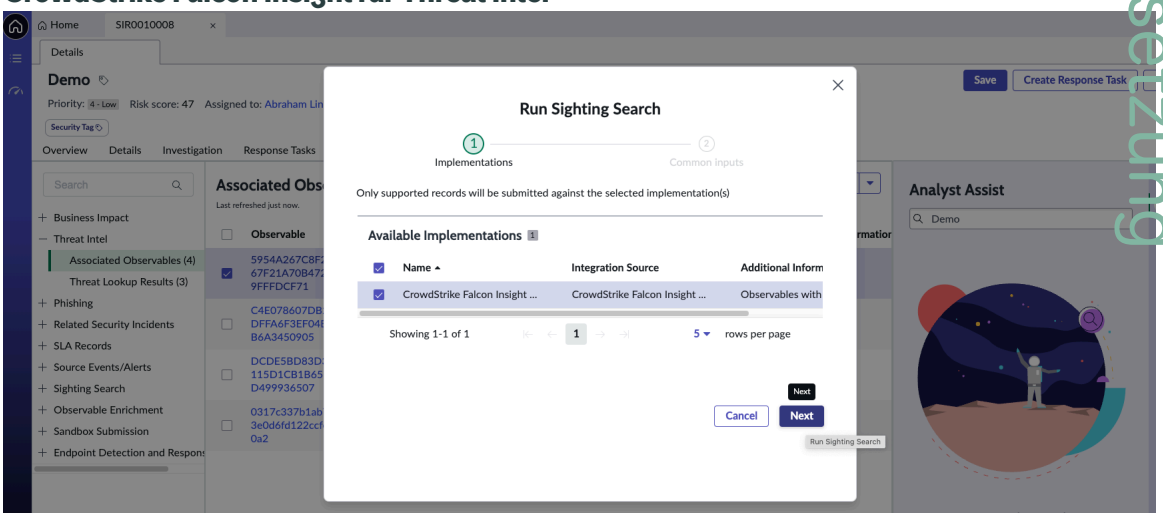
d. Wählen Sie aus **CrowdStrike Falcon Insight** Implementierung, und klicken Sie auf **Führen Sie Die Suche Aus** .
Dann wird eine Hash-Sichtungssuche für den ausgewählten laufenden Prozess ausgeführt. Sie können die Arbeitsnotizen für die Ergebnisse und Ergebnisse anzeigen.

4. Sie können die CrowdStrike Falcon Insight-Fähigkeiten im verwenden **Bedrohungsinformationen** Zur Analyse.

a. Wählen Sie in der Gruppe Threat Intel (Bedrohungsinformationen) eine aus **Erkennbares Element** , Und wählen Sie eine aus CrowdStrike Falcon Insight Fähigkeit aus der Dropdown-Liste.

b. Wählen Sie aus **CrowdStrike Falcon Insight** Implementierung, und klicken Sie auf **Als Nächstes** .

CrowdStrike Falcon Insight für Threat Intel



c. Wählen Sie im Popup-Fenster Datum/Uhrzeit auswählen einen zufälligen Wert aus, und klicken Sie auf **Übermitteln** .
Dann wird eine Sichtungssuche für das ausgewählte erkennbare Element ausgeführt. Sie können die Arbeitsnotizen für die Ergebnisse und Ergebnisse anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CrowdStrike Next-Gen SIEM-Integration

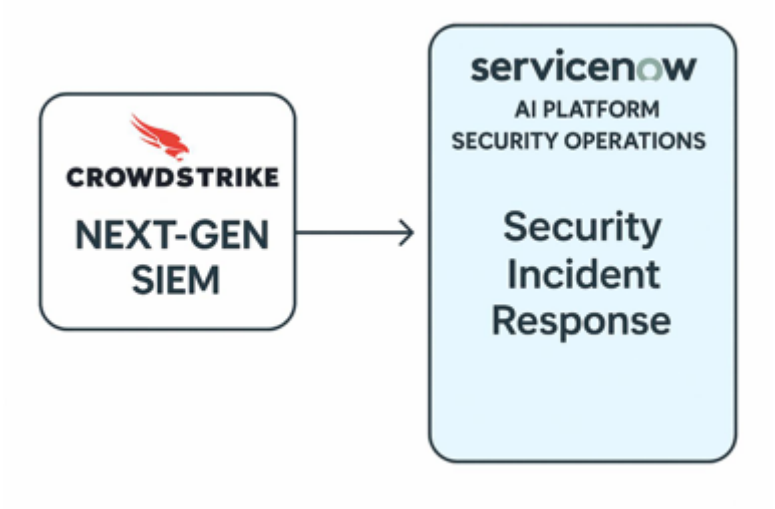
Die CrowdStrike Next-Gen SIEM Die Integration erfasst automatisch Erkennungsdaten, die auf potenzielle Security Incidents hinweisen können, und optimiert die Erstellung von Security Incidents in der ServiceNow® Security Incident Response (SIR), um eine rechtzeitige und effektive Reaktion sicherzustellen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht über CrowdStrike Next-Gen SIEM Integration

In der folgenden Grafik erfahren Sie, wie es geht CrowdStrike Next-Gen SIEM Ist in integriert ServiceNow AI Platform Security Operations Anwendungen.



Schlüsselfunktionen

Verwenden Sie die wichtigsten Funktionen dieser Integration, um die folgenden Aktionen auszuführen:

- Erkennen CrowdStrike Next-Gen SIEM Erkennungen, die Kandidaten für Security Incidents sind und die Erstellung dieser Security Incidents automatisieren.
- Zuordnung CrowdStrike Next-Gen SIEM Fehler- und Entitätsfelder bis SIR Security Incident-Felder.
- Filter CrowdStrike Next-Gen SIEM Fehler.
- Aggregieren Sie Incidents mit vorhandenen offenen Security Incidents, damit Sie keine doppelten Security Incidents erstellen müssen.
- Automatisieren CrowdStrike Next-Gen SIEM Erkennungsstatus-Updates für Security Incident Response, damit Sie Security Incidents erstellen und schließen können.

Hinweis:
ServiceNow Aktualisiert den Status von CrowdStrike Next-Gen SIEM Erkennungen basierend auf der Erstellung oder dem Abschluss von Security Incidents. Dieses Update enthält auch Kommentare zu aggregierten Erkennungen und neuen Erkennungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Planen Sie die Erkennungserfassung, um regelmäßig Security Incidents zu erstellen.
- Synchronisieren CrowdStrike Next-Gen SIEM Erkennungskommentare mit SIR Arbeitsnotizen.

Erste Schritte mit CrowdStrike Next-Gen SIEM Integration

Aktivieren und richten Sie ein CrowdStrike Next-Gen SIEM Integration für Security Operations-Plugin zur Schnittstelle mit Ihrem ServiceNow AI Platform Instanz und Security Incident Response Produkt.

Bevor Sie verwenden können CrowdStrike Next-Gen SIEM Integration müssen Sie sie aus herunterladen ServiceNow Store.

Überprüfen Sie die folgende Setup-Prüfliste, und stellen Sie sicher, dass Sie alle Aufgaben für eine reibungslose Integration abgeschlossen haben.

Prüfliste

Setupaufgabe	Beschreibung
Weisen Sie die erforderlichen zu, und verifizieren Sie sie ServiceNow AI Platform Und Security Incident Response Rollen.	Die folgenden Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Die Administratorrolle installiert die Integration aus dem ServiceNow Store Und weist die Rollen sn_si.ingestion_profile_admin und sn_si.Analyst zu. • Die Rolle sn_si.ingestion_profile_admin führt die folgenden Aufgaben aus: ◦ Konfiguriert die Integration. ◦ Erstellt Erkennungsprofile. ◦ Ordnet zu CrowdStrike Next-Gen SIEM Erkennungsdatenfelder für die Security Incident-Felder. ◦ Plant die laufende Erkennungserfassung. ◦ Aktiviert Erkennungsaktualisierungen, wenn ein Security Incident Response Erkennung wird erstellt oder geschlossen.
Weisen Sie die erforderlichen CrowdStrike-Rollen zu.	Die folgenden Rollen sind in CrowdStrike erforderlich, um Ihre Anwendung zu registrieren und zu konfigurieren: • Anwendungsentwickler für die Registrierung der Anwendung. • Mandantenadministrator für die Erteilung von Berechtigungen für die Anwendung durch Aufruf des Endpunkts der Administratoreinwilligung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie diese Integration konfigurieren.	Die Security Incident Response Plugin (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Anwendungen, die für die Integration erforderlich sind.
Installieren und konfigurieren	Installieren und konfigurieren Sie CrowdStrike Next-Gen SIEM Integration für Security Operations Anwendung aus dem ServiceNow Store Auf Ihrer ServiceNow KI-Plattform-Instanz.

Installieren und konfigurieren

Installieren und konfigurieren Sie CrowdStrike Next-Gen SIEM Integration für Security Operations Anwendung aus dem ServiceNow Store Auf Ihrer ServiceNow KI-Plattform-Instanz.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Anwender mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da diese Rolle standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Laden Sie herunter CrowdStrike Next-Gen SIEM Integration aus dem ServiceNow Store Und installieren Sie es.
   Weitere Informationen finden Sie unter Laden Sie eine Anwendung aus dem herunter ServiceNow Store Zum ersten Mal
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie nach CrowdStrike Next-Gen SIEM Integrationskachel und wählen Sie aus **Konfigurieren** .
4. Füllen Sie im Formular die Felder aus.

CrowdStrike – SIEM-Integrationsformular der nächsten Generation

Feld	Beschreibung
Name	Name des CrowdStrike Next-Gen SIEM Integration.
Client-ID	Die Client-ID, die Sie aus dem Abschnitt „Einstellungen“ Ihres Accountprofils im CrowdStrike-Portal abrufen.
Geheimer Clientschlüssel	Der geheime Clientschlüssel, den Sie im Abschnitt „Einstellungen“ Ihres

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Accountprofils im CrowdStrike-Portal abrufen.
Region	Rechenzentrum, aus dem Daten abgerufen werden sollen. Geben Sie die Region an: US-1, US-2, EU-1, US-GOV-1, US-GOV-2 Standardmäßig ist das Feld auf US-1 festgelegt

5. Wählen Sie **Absenden**.
   Die konfigurierte Integrationskachel wird angezeigt.

Nächste Maßnahme

Erstellen Sie ein Erkennungsprofil

Erstellen Sie ein Erkennungsprofil

Bestimmen Sie CrowdStrike Next-Gen SIEM Erkennungen, die für die Erstellung von Security Incidents geeignet sind, indem ein Erkennungsprofil in erstellt wird ServiceNow AI Platform Instanz.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Navigieren zu **Alle** > *CrowdStrike Next-Gen SIEM* > **Erkennungsprofil**an.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular die Felder aus.

CrowdStrike Next-Gen SIEM – Formular „Konfiguration der Erkennungserfassung“

Feld	Beschreibung
Name	Name des Profils. Dieser Name ist auch der Standardname für das diesem Profil zugeordnete Sicherheits-Tag.
Aktiv	Option zum Aktivieren des Profils. Wenn ein Profil aktiv ist, wird ServiceNow AI Platform Ruft aktiv ab CrowdStrike Next-Gen SIEM Erkennungen und entsprechende Sicherheitserkennungen werden in erstellt Security Incident Response Wenn die Filterbedingungen erfüllt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quelle	CrowdStrike Mandant, den Sie zum Erfassen von Erkennungen konfiguriert haben. Wenn Sie mehrere Mandanten konfiguriert haben, wählen Sie den entsprechenden Mandanten für die Erkennungstypen aus, die Sie für das Profil erfassen möchten.
Reihenfolge	Priorität, in der die Profile ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam haben. Prioritätswerte werden normalerweise als 100 (der Standardwert), 200, 300 usw. angegeben. Das Profil mit der niedrigsten Zahl hat die höchste Priorität.
Beschreibung	Optionale Beschreibung des Profils.

4. Wählen Sie Aus **Aktualisieren** .

   Das anfängliche Erkennungsprofil wird mit grundlegenden Informationen erstellt. Wenn Sie das Profil zu diesem Zeitpunkt speichern, können Sie mit der Definition des Profils fortfahren, falls Sie unterbrochen werden.

5. **Wahlweise:** Fahren Sie sofort mit dem Profildefinitionsprozess fort.

   a. Wählen Sie auf der Seite „CrowdStrike-NextGen-Erkennungsprofile“ das Profil aus, das Sie gerade erstellt haben.

   b. Wählen Sie im Fortschrittsbalken die Option aus **Korrelationsregeln** .

Nächste Maßnahme

Legen Sie Korrelationsregeln fest

Legen Sie Korrelationsregeln fest

Nach dem Erstellen von CrowdStrike Next-Gen SIEM Erkennungsprofil: Wählen Sie Korrelationsregeln aus, um die entsprechenden Erkennungen einem Security Incident zuzuordnen. Korrelationsregeln werden jedes Mal aktualisiert, wenn ein Profil geöffnet wird, und neue Regeln stehen zur Auswahl. Die CrowdStrike Next-Gen SIEM Die Integration unterstützt mehrere Profile.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Wenn Sie nicht mit dem vorherigen Abschnitt des Erkennungsprofildefinitionsprozesses fortfahren, greifen Sie auf das Profil zu, das Sie definieren.

   a. Navigieren zu **Alle** > *CrowdStrike Next-Gen SIEM* > **Erkennungsprofil**an.

   b. Wählen Sie das Profil aus, das Sie mit der Definition fortfahren.

   c. Wählen Sie Aus **Korrelationsregeln** In der Fortschrittsleiste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Löschen Sie **Alle Korrelationsregeln ausgewählt** Kontrollkästchen.
3. Geben Sie im Suchfeld Korrelationsregelliste den Namen der Korrelationsregel ein, der in erstellt wurde CrowdStrike Portal.
4. Wählen Sie die Korrelationsregel aus.
5. Verwenden Sie den Rechtspfeil, um die Regel aus zu verschieben **Verfügbar** Zu **Ausgewählt** Spalte.
6. Schließen Sie diesen Abschnitt des Erkennungsprofildefinitionsprozesses ab, indem Sie auswählen **Fahren Sie Fort** .

Nächste Maßnahme

Einzelperson zuordnen CrowdStrike Next-Gen SIEM Erkennungsfelder für die Felder im ServiceNow AI Platform Security Incident Response Security Incident. Weitere Informationen finden Sie unter Ordnen Sie Erkennungsfelder zu.

Ordnen Sie Erkennungsfelder zu

Ordnen Sie die einzelnen CrowdStrike Next-Gen-Erkennungsfelder den Feldern im zu SIR Security Incident, damit Sie Erkennungen mit den zugeordneten Daten erstellen können.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Wählen Sie auf der Zuordnungsseite im Abschnitt CrowdStrike Next-Gen-Feldzuordnung eine der Beispielerfassungsmethoden aus.

Beispiel für Erfassungsmethoden

Feld	Beschreibung
Alle standardmäßigen Erkennungs- und Ereignisfelder	Verwenden Sie diese Erfassungsmethode, um die statische Liste aller Erkennungen und Ereignisfelder anzuzeigen. Diese Methode enthält nur Standardfeldnamen ohne Werte. Sie können diese Informationen verwenden, um eine Zuordnung zu vorzunehmen SIR Felder.
Ruft Aktuelle Erkennungen Ab	Verwenden Sie diese Erfassungsmethode, um die neuesten Erkennungs- und Entitätsdaten zu importieren. Wenn die CrowdStrike Next-Gen-Erkennung mehrere Warnungen enthält, wird die früheste Warnung, die Teil der Erkennung ist, im Zuordnungsabschnitt angezeigt. Auch während der Erfassung werden die frühesten Feldwerte für Sicherheitswarnungen verwendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie können 5 Beispielerkennungen erfassen. Die Werte des Beispielerkennungsfelds werden ausgefüllt, wenn das Profil die Beispielerkennungen erfasst. Sie können diese Erkennungen dem zuordnen **SIR-Incident-Zielfelder** . Die Erkennungsfelder und -Werte werden als einzelne Registerkarten angezeigt.

2. Führen Sie die folgenden Aktionen aus, um den Standardfeldern, die im Security Incident angezeigt werden, Felder hinzuzufügen:

a. Wählen Sie im Abschnitt SIR Incident-Zielfelder die aus

Schaltfläche „weiteres Feld zuordnen“.
Es wird eine Liste von angezeigt SIR Felder, aus denen Sie ein Feld auswählen können, aus dem ein neues Feld angezeigt werden soll.

b. Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie dann ein Feld aus.

Hinweis:
Mehrere erkennbare Elemente können für denselben Security Incident angezeigt werden. Zum Beispiel die **Erkennbares Element** Das Feld kann mehrmals verschiedenen Werten zugeordnet werden. Ebenso wird **Konfigurationselement** Und **Felder für Arbeitsnotizen** Unterstützt mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird eine Fehlermeldung angezeigt, dass dieses Feld nicht mehrere Werte unterstützt. Wenn ein Feld in einem Security Incident über eine Liste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

c. Ziehen Sie Ihr Feld im Abschnitt „Erkennungs- und Ereignisfelder“ per Drag-and-Drop, um es Ihrem neuen Feld zuzuordnen.

d. Wenn Sie das Kontrollkästchen aktivieren, das einem Feld entspricht, werden bei allen neuen oder aktualisierten Änderungen, die in CrowdStrike vorgenommen werden, die entsprechenden SIR-Incident-Daten automatisch mit den neuen Incident-Daten aktualisiert.

Hinweis:
Im Basissystem ist die Systemeigenschaft sn_sec_cs_ngsiem.detection_updates standardmäßig auf falsch festgelegt, um die CrowdStrike Next Gen-Updates im Zusammenhang mit neuen Warnungen zu erhalten, die mit SIR verknüpft sind.

- Standardmäßig sind die Felder Betroffene Anwender, Konfigurationselemente und erkennbare Elemente aktiviert. Dies bedeutet, dass immer dann, wenn neue erkennbare Elemente oder zugehörige Konfigurationselemente oder betroffene Anwender dem Incident hinzugefügt werden, diese Informationen während dieses Abfrageintervalls automatisch extrahiert und in den entsprechenden zugehörigen Listen in der Security Incident Response (SIR) ausgefüllt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für alle anderen Felder müssen Sie das Kontrollkästchen aktivieren, das einem Feld für alle neuen oder aktualisierten Änderungen entspricht, die im CrowdStrike-Erkennungsdatensatz in CrowdStrike vorgenommen wurden. Dadurch werden die entsprechenden SIR-Incident-Daten automatisch mit den neuen Erkennungsdaten aktualisiert.

Wichtig:
Vor der Auswahl dieser Funktionalität muss eine Sorgfaltspflicht durchgeführt werden, da das Überschreiben der vorhandenen Daten zu instabilen Daten führen kann, mit denen der Analyst arbeiten kann, und jede andere Automatisierung, die auch durch die Feldwerte des Security Incident festgelegt wird, kann ebenfalls betroffen sein. Daher ist es sehr wichtig, die Sorgfaltspflicht durchzuführen, bevor Sie eine Überschreibungsfunktion auswählen.

3. Verwenden Sie zum Entfernen eines Felds Schaltfläche „Element entfernen“ neben dem Eingabeausdrucksfeld im Abschnitt „SIR-Incident-Zielfelder“.
4. Um einen Feldwert aus dem Abschnitt „Erkennungs- und Ereignisfelder“ einem Feld im Abschnitt „SIR-Incident-Zielfelder“ zuzuordnen, verwenden Sie eine der folgenden Aktionen:

   a. Ziehen Sie den Erkennungsfeldnamen (z. B. ID), und legen Sie ihn neben einem Feldnamen in der Spalte SIR-Incident-Zielfelder ab.

   Sie können einen beliebigen Wert aus dem Abschnitt „Erkennungs- und Ereignisfelder“ mit einem Feld im Abschnitt „SIR-Incident-Zielfelder“ abgleichen. Felder sind farbcodiert, damit Sie Erkennungsfelder im Zuordnungsprozess nicht übersehen oder duplizieren. Hellblaue Felder geben an, dass noch kein Erkennungsfeld ausgewählt und dem Security Incident zugeordnet ist. Möglicherweise möchten Sie eingehende Erkennungsfelder mit mehr als einem Feld in einem Security Incident verknüpfen. Ein graues Feld gibt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Auf diese Weise können Sie visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Incident-Informationen nicht zugeordnet sind.

   b. Sie können eine Kombination aus Text und Feld hinzufügen.
   Beispiel: `Erkennungsname ist ${Erkennungen: Name}$` . Hier `Erkennungsname ist` Kann während manuell eingegeben werden `${Erkennungen: Name}$` Wird im Abschnitt „Erkennungs- und Ereignisfelder“ zugeordnet.

   c. Sie können Quellerkennungs- oder Ereignisfelder direkt manuell eingeben und einem Zielfeld zuordnen.

   - Um ein Quellenerkennungsfeld manuell zuzuordnen, verwenden Sie dasFormat $ {field Name}$. Um beispielsweise einen Schweregrad eines Erkennungsfelds zuzuordnen, lautet das Format `${Erkennungen: Schweregrad}$` .
   - Verwenden Sie zum manuellen Hinzufügen von Quellereignisfeldern `${Ereignisnamen: Ereignisfelder}$` Format. Zum Zuordnen von Ereignisfeldern Beschreibung von Ereignissen Sicherheitswarnung lautet das Format `${Events: Description}$` .

Diese Integration klassifiziert bestimmte Untertypen erkennbarer Elemente. Wenn Sie ein CrowdStrike Next-Gen-Feld dem SIR-erkennbaren Feld zuordnen, der ServiceNow AI Platform Klassifiziert das erkennbare Element automatisch. Wenn Sie das eingehende erkennbare CrowdStrike Next- Gen-Element generisch dem erkennbaren Element zuordnen möchten, geben Sie in ein SIR, Ziehen Sie dann das Feld Erkennung und Ereignis per Drag-and-Drop in das Feld erkennbares Element. Wenn Ihnen jedoch der Typ des erkennbaren Elements für das eingehende erkennbare CrowdStrike Next- Gen-Element in bekannt ist SIR, Und ordnen Sie dann speziell dem zu SIR Typfeld des erkennbaren Elements. Einige Beispiele für bestimmte Typen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erkennbarer Elemente in SIR Schließen Sie erkennbares Element (Domänenname), erkennbares Element (E-Mail-Adresse), erkennbares Element (IP-Adresse (V4)) und erkennbares Element (Hostname) ein.

Wenn Ihre eingehenden CrowdStrike Next-Gen-Felder irgendwelche enthalten MITRE-ATT&CK Informationen, ordnen Sie sie dann zu MITRE-ATT&CK Technikfeld. Stellen Sie sicher, dass das Feld Incoming CrowdStrike Next- Gen. enthält MITRE-ATT&CK Technik-ID oder Technikname.

Manchmal werden Erkennungsfeldwerte in CrowdStrike Next- Gen möglicherweise nicht direkt in die Felder im SIR Security Incident übersetzt. Für diese Werte können Sie einen Skripteditor verwenden, um Feldwerte für den Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind.

5. Um eine Feldübersetzung für ein neues Feld aus einer CrowdStrike Next Gen-Erkennung so zu formatieren, dass sie einem Feldwert in einem Security Incident entspricht, wählen Sie aus **Klicken Sie hier** Link in **SIR-Incident-Zielfelder** Header.

6. Um die Felder zu ändern, die die Feldübersetzung unterstützen, wählen Sie aus Symbol für Übersetzung des Skriptformatfelds.
Die Felder, die die Feldübersetzung unterstützen, sind **Betroffener Anwender** , **Konfigurationselement** , Und **Priorität** . Klicken Sie beispielsweise auf Symbol neben der Kategorie. Der Skripteditor CrowdStrike Next- Gen Field Translation wird geöffnet.

7. Geben Sie alle Änderungen am Skript ein, und wählen Sie aus **Aktualisieren** Um die Änderungen zu speichern und zur Zuordnungsseite zurückzukehren.
Definieren Sie beispielsweise für Kategorie Folgendes im Skript-Editor:

```
"<Incoming CrowdStrike Detection Field Value>" : "<Category to assign to the Security Incident>".
```

Diese Zuordnung stellt sicher, dass ein Profil nur konfigurierte Kategorien verwendet.

8. Setzen Sie Ihre Zuordnung fort, indem Sie Feldwerte hinzufügen oder entfernen.
Sie können dieselben Feldwerte im Generator für Erkennungsgenerierungsbedingungen verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Erkennung erfüllen muss, um einen Security Incident zu erstellen.

9. Um zum Abschnitt Filtern und Zusammenfassung zu wechseln, wählen Sie aus **Fahren Sie Fort** .

Nächste Maßnahme

Definieren und legen Sie Filterbedingungen fest, damit Sie angeben können, welche Erkennungen Security Incidents erstellen sollen. Sie können dieselben Feldwerte (definiert im Abschnitt „Zuordnung“) im Generator für Erkennungsgenerierungsbedingungen (im Abschnitt „Filterung und Zusammenfassung“) verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Erkennung erfüllen muss, um einen Security Incident zu erstellen.

Definieren Sie Filter- und Zusammenfassungskriterien

Definieren und legen Sie Filterbedingungen fest, um anzugeben, welche eingehend sind CrowdStrike Next-Gen SIEM Erkennungen sollten Security Incidents erstellen. Sie können auch zusätzliche Erkennungsfeldkriterien definieren, mit denen eine eingehende Erkennung an einen offenen Security Incident angehängt werden kann, anstatt einen Incident zu erstellen.

Legen Sie Filterbedingungen fest

Legen Sie die Filterbedingungen so fest, dass Security Incidents nur erstellt werden, wenn die Filterbedingungen übereinstimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird
Diese Art der Filterung hilft Ihnen, Security Incidents zu isolieren und die Anzahl der von Ihnen erstellten Security Incidents zu begrenzen. Wenn Sie zusätzliche Filterkriterien festlegen, werden nur die erforderlichen Erkennungen erfasst, ohne die Abfrage oder die Konfiguration der ausgelösten Erkennung ändern zu müssen.

Prozedur

1. Um die Kriterien zu definieren, die eine eingehende CrowdStrike Next-Gen-Erkennung erfüllen muss, damit ein Security Incident erstellt wird, wählen Sie aus **Filtern Sie basierend auf Bedingungen** .

   Die Optionen im ersten Feld in den Filterbedingungen entsprechen den Feldern, die im Abschnitt „CrowdStrike Next-Gen-Beispielerkennungserfassung“ für die von Ihnen erfasste Erkennung angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach Erkennung, die Sie erfassen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Stellen Sie sicher, dass die von Ihnen definierten Kriterien mit den Werten der Erkennung übereinstimmen.

   Verwenden Sie die Filterbedingung *`Erkennungs-ID`* Für die folgenden Felder mit mehreren Werten:

   - Composite_ID
   - Host_names
   - Sekunden_zu_gelöst
   - Seconds_to_triaged

   Da die Filterbedingung nur Zeichenfolgen abrufen kann, müssen Sie verwenden *`Erkennungs-ID`* Filterbedingung für die obigen Felder, um sicherzustellen, dass die Daten korrekt gefiltert werden.

2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER** .
   - Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden.
4. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien** .

Definieren Sie Zusammenfassungsbedingungen

Definieren Sie zusätzliche Incident-Zusammenfassungskriterien, die eine eingehende Erkennung zu einem vorhandenen SIR Security Incident aggregieren, anstatt ähnliche, potenziell doppelte Erkennungen zu erstellen. Wenn Sie Feldübereinstimmungswertkriterien für jedes Profil verwenden, kann diese zusätzliche Zusammenfassung die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Erkennungsdaten in einem einzelnen Security Incident platziert werden.

Vorbereitungen
Erforderliche Rolle: sn_si.ingestion_profile_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein neuer Incident allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird der Incident automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Benutzer mit der Rolle sn_si.ingestion_profile_admin, der mit Security Incidents arbeitet, können Sie alle hinzugefügten aggregierten Incidents in einer zugehörigen Liste zu einem Security Incident anzeigen.
Alle aggregierten Incidents für einen Security Incident werden im angezeigt CrowdStrike Next-Gen SIEM Zugehörige Liste „zusammengefasste Incidents“. Diese Liste enthält Details zu den zugehörigen Zeitstempeln und aggregierten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum Incidents zu den vorhandenen Security Incidents hinzugefügt werden.

Prozedur

1. Zum Definieren zusätzlicher Incident-Feldkriterien, die eingehende zulassen CrowdStrike Next-Gen SIEM Erkennung, die an einen offenen Security Incident angehängt werden soll, anstatt einen neuen Incident zu erstellen, wählen Sie aus **Zusammenfassungsbedingungen** Option wie in der folgenden Abbildung gezeigt.
2. In **Incident-Felder mit übereinstimmenden Werten** Geben Sie die Feldwerte ein, die Sie für vorhandene Security Incidents in abgleichen möchten ServiceNow AI Platform Instanz.
   Alle Feldwerte, die Sie im Eingabefeld für die Mehrfachauswahl ausgewählt haben, müssen übereinstimmen, damit die Zusammenfassungskriterien erfüllt sind und dieser eingehende Incident an einen vorhandenen Security Incident angehängt werden kann. Diese Auswahl impliziert, dass es sich um einen handelt *UND* Bedingung, unter der ihnen Felder wie erkennbare Elemente und Konfigurationselemente zugeordnet werden, die mehrere Feldwerte haben können. Wenn nur eine Teilmenge der Werte übereinstimmt, wird die CrowdStrike Next-Gen SIEM Die Bedingungen für die Incident-Zusammenfassung sind nicht erfüllt, und ein neuer Security Incident wird erstellt.
3. Um mehrere übereinstimmende Feldbedingungen hinzuzufügen, klicken Sie auf **Fügen Sie Neue Kriterien Hinzu**
   Die Zusammenfassung erfolgt, wenn eine der von Ihnen definierten Bedingungen für Mehrfachauswahlfelder erfüllt ist. Diese Auswahl impliziert *ODER* Bedingung.
4. Um die Arbeitsnotiz für einen neuen Incident zu aktualisieren, wenn er einem Security Incident hinzugefügt wird, wählen Sie aus **Arbeitsnotiz für neuen Incident protokollieren** .

   Die Arbeitsnotiz protokolliert, dass ein neuer Incident hinzugefügt wird, und enthält einen Link zu den Incident-Details. Die Protokoll-Arbeitsnotiz aktualisiert auch weitere Details, die Sie dem Feld Arbeitsnotiz in Ihrem Zuordnungsabschnitt hinzufügen.
5. Klicken Sie auf, um den Zeitplan zu konfigurieren **Fahren Sie Fort** .

Nächste Maßnahme

Legen Sie einen Zeitplan fest, um die Incident-Daten und erfassten Incidents abzurufen, die den Kriterien im Profil entsprechen.

Planen Sie den Erkennungsabruf

Konfigurieren Sie einen Zeitplan, um zu definieren, wie und wann Sie Erkennungen aus abrufen CrowdStrike Next-Gen SIEM Mandant.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Wenn Sie nicht mit dem vorherigen Abschnitt der Filter- und Zusammenfassungskriterien fortfahren, greifen Sie auf das Profil zu, das Sie definieren.
   a. Navigieren zu **Alle** > *CrowdStrike Next-Gen SIEM* > **Erkennungsprofil**an.
   b. Wählen Sie das Profil aus, das Sie mit der Definition fortfahren.
   c. Wählen Sie Aus **Zeitplanung** In der Fortschrittsleiste.
2. Füllen Sie die Felder im Planungsformular aus.

CrowdStrike Next-Gen SIEM Zeitplanungsformular

Feld	Beschreibung
Laufende Erkennungserfassung	Option zum Festlegen der laufenden Erkennungserfassung, die für festgelegt wird ServiceNow AI Platform Instanz ruft aus ab CrowdStrike Next-Gen SIEM Mandant für neue Erkennungen. Security Incidents werden erstellt, wenn ausgelöste Erkennungen gefunden werden und die Filterkriterien für die Erkennungsgenerierung erfüllt sind.
Abfrageschritt (Minuten)	Abfragehäufigkeit in Minuten definiert.
Legen Sie die Erkennungserfassungszeit fest	Option zum Hinzufügen von Datum und Uhrzeit für die anfängliche Erfassung.
Zeit der ersten Erkennungserfassung	Datum und Uhrzeit, die Sie für die Erkennungserfassung angeben.
Einmaliger Abruf	Option zum Aktivieren des einmaligen Abrufs von Verläufen CrowdStrike Next-Gen SIEM Erkennungen und gefolgt vom Abgleich der Daten. Bei der Verarbeitung der Daten werden sowohl laufende Erkennungen als auch Verlaufsdaten abgerufen. **Hinweis:** Der abgerufene Verlauf CrowdStrike Next-Gen SIEM Erkennungen werden Deduplizierungsprüfungen unterzogen, um Duplikate innerhalb von zu vermeiden Security Incident Response Anwendung.
Seit Datum	Das Datum, ab dem historische Erkennungen erfasst wurden CrowdStrike Next-Gen SIEM.

3. Füllen Sie diesen Abschnitt des Profils aus, indem Sie auswählen **Fahren Sie Fort** .

Nächste Maßnahme

Automatisieren Sie Erkennungs-Updates und -Abschlüsse

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatisieren Sie Erkennungs-Updates und -Abschlüsse

Automatisieren Sie Erkennungs-Updates und -Abschlüsse basierend auf Security Incident Response Incident-Status. Die CrowdStrike Next-Gen SIEM Durch die Integration können Erkennungen Security Incidents erstellen und die Incidents auch aktualisieren, nachdem sie erstellt oder geschlossen wurden.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Wenn Sie nicht mit dem vorherigen Abschnitt des Zeitplanungsprozesses fortfahren, greifen Sie auf das Profil zu, das Sie definieren.
   a. Navigieren zu **Alle** > *CrowdStrike Next-Gen SIEM* > **Erkennungsprofil**an.
   b. Wählen Sie das Profil aus, das Sie mit der Definition fortfahren.
   c. Wählen Sie Aus **Zusätzliche Optionen** In der Fortschrittsleiste.
2. Füllen Sie im Formular die Felder aus.

Formular „Automatisieren von Erkennungsaktualisierungen“

Kategorie	Feld	Beschreibung
Updates Zur Erstellung Von Security Incidents	Aktualisieren Sie den Erkennungsstatus der nächsten CrowdStrike-Generation bei der SIR-Incident-Erstellung	Option zur Verwendung der automatisierten Erkennungs-Update-Funktionalität. Die CrowdStrike Next-Gen SIEM Erkennungsstatus wird in aktualisiert CrowdStrike Next-Gen SIEM Erkennung mit den Kommentaren nach SIR Incident wird in erstellt ServiceNow AI Platform.
	Aktualisierung des anfänglichen Erkennungsstatus	Anfänglicher Erkennungsstatus, der in aktualisiert wird CrowdStrike Next-Gen SIEM Umgebung, entweder „Neu“ oder „in Bearbeitung“.
	Erste Kommentare, die zur Erkennung zurückgesendet werden	Erste Kommentare, die in der -Erkennung veröffentlicht werden CrowdStrike Next-Gen SIEM Umgebung.
Aktualisierungen Des Erkennungsabschlusses	Schließen Sie die CrowdStrike Next-Gen-Erkennung nach SIR-Incident-Abschluss	Option zur Verwendung der automatisierten Erkennungsstatusaktualisierungsfunktion. CrowdStrike Next-Gen SIEM Erkennungen werden in geschlossen CrowdStrike Next-Gen SIEM Portal mit den Kommentaren nach dem SIR Incident wird in geschlossen ServiceNow AI Platform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Feld	Beschreibung
	Aktualisierung des Abschlusserkennungsstatus	Statusaktualisierung in CrowdStrike Next-Gen SIEM Erkennung, wenn der Security Incident in geschlossen wird SIR.
	Abschlusskommentare, die zurück zur Erkennung veröffentlicht wurden	Kommentare, die an die Erkennung in gepostet wurden CrowdStrike Next-Gen SIEM Erkennung, wenn der Security Incident in geschlossen wird SIR.
Geschlossene Erkennungen abrufen	Geschlossene Erkennungen abrufen	Option zum Abrufen geschlossener Erkennungen während der laufenden Erfassung und des einmaligen Abrufs. Geschlossen SIR Incidents werden nicht mit neuen Daten aus aktualisiert CrowdStrike Next-Gen SIEM
Synchronisierung von Erkennungskommentaren und SIR-Arbeitsnotizen	Aktualisieren Sie die SIR-Automatisierungsaktivität mit CrowdStrike Next-Gen-Erkennungskommentaren	Option zum Aktualisieren von CrowdStrike Next-Gen SIEM Kommentare in SIR Automatisierungsaktivität. Der Kommentar in SIR Die Automatisierungsaktivität wird mit dem Präfix angezeigt *`Kommentar aus CrowdStrike .`*
	Aktualisieren CrowdStrike Next-Gen SIEM Erkennungskommentare mit SIR-Arbeitsnotizen	Option zum Aktualisieren von SIR Arbeitsnotizen in CrowdStrike Next-Gen SIEM Erkennungskommentare. Der Kommentar in CrowdStrike Next-Gen SIEM Wird mit dem Präfix angezeigt *`Kommentar von ServiceNow .`*

3. Wählen Sie **Fertigstellen** aus.
4. Aktivieren Sie das Profil.
   a. Wählen Sie aus **Name** Abschnitt des Fortschrittsbalkens.
   b. Aktivieren Sie die Checkbox **Aktiv**.
   c. Wählen Sie **Fortsetzen**.

Integration von CrowdStrike Falcon X Sandbox für Security Operations

Mit CrowdStrike Falcon X Sandbox Für Security Operations Integration können Sie Dateien und URLs als Teil des Security Incident Response-Prozesses an übermitteln CrowdStrike Falcon X Sandbox Dient zum Durchführen einer detaillierten Malware- und Bedrohungsanalyse.

Die CrowdStrike Falcon X Sandbox Die Integration bietet Ihnen eine isolierte virtuelle Umgebung bei Bedarf, in der Sie die Malware-Analyse durchführen und Ergebnisse für bereitstellen können ServiceNow Security Incident durch die Integration.

Wenn Sie Ihre Malware-Incidents übermitteln, werden sie als Teil des Security Incident-Datensatzes aufbewahrt. Sie können diese Datensätze f verwenden Oder weitere Incident-Lösung und automatisieren die Übermittlung von Dateien und URLs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Integration unterstützt die Automatisierung von Phishing- und Malware-Antwort-Playbooks Was ermöglicht Security Operations Zentrieren Sie Mitarbeiter, um produktiver und effizienter auf Security Incidents zu reagieren.

Hauptvorteile

Mit t Seine Integration , Sie können tun Folgen :

- Automatisieren Sie die Übermittlung von Dateien und URLs vom Anwender – Gemeldetes Phishing (URP), E-Mail-Nachrichten, Anhänge und andere Security Incidents.
- Senden Sie zuvor analysierte Dateien und URLs manuell, oder übermitteln Sie sie erneut für die aktualisierte Analyse.
- Erstellen Sie mehrere Übermittlungskonfigurationen, die automatisch angewendet werden CrowdStrike Falcon X SandboxÜbermittlungsparameter wie Betriebssystem, Scan-Typ und Laufzeitoptionen.
- Analysieren Sie Malware Und Bedrohungsergebnisse In einem HTML-formatierten Bericht innerhalb von SIR Incident. Sie können anzeigen t Hreat-Suchergebnisse und Indikatorverlauf für Dateien und URLs, die mehrfach analysiert wurden.
- Tag ServiceNow Incidents mit dem Verarbeitungsstatus der Übermittlung sowie Bedrohungsergebnisergebnisse.

Siehe auch

Dokumentbezeichner	Dokumententitel
CrowdStrike Falcon X Sandbox	Häufig gestellte Fragen zu CrowdStrike Falcon Sandbox
ServiceNow Produktdokumentations-Website	ServiceNow-Produktdokumentationswebsite

Beginnen Sie mit dem CrowdStrike Falcon X Sandbox Integration

Aktivieren und richten Sie ein CrowdStrike Falcon X Sandbox Um eine Schnittstelle mit herzustellen ServiceNow Instanz und Security Incident Response Produkt.

Vorbereitungen

- Bevor Sie verwenden können CrowdStrike Falcon X Sandbox Für die Integration von Security Operations müssen Sie sie aus dem herunterladen ServiceNow Store .
- Überprüfen Sie die folgende Setup-Prüfliste, und stellen Sie sicher, dass Sie alle Aufgaben für einen reibungslosen Abschluss abgeschlossen haben CrowdStrike Falcon X Sandbox Integration.

Erforderliche Rolle: admin, sn_si.admin

Prüfliste

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform Und Security Incident Response Rollen.	Die folgenden Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	• Der Administrator (Administrator) installiert S Andbox-Integration aus dem ServiceNow App Store und weist die Rolle Security Incident-Administrator (sn_si.admin) zu. • sn_si.admin erstellt und bearbeitet Die Konfiguration Und Globale Einstellungen und Dann Weist die Rolle Security Incident Analyst (sn_si.Analyst) zu. • Der Security Incident-Analyst (sn_si.Analyst) reagiert auf Security Incidents , Z. B. Dateien und URLs werden an übermittelt Die S Andbox und Analyse der Übermittlungsergebnisse.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie diese Integration konfigurieren.	Diese Integration wird in unterstützt Paris Und Orlando Releases. Stellen Sie sicher, dass diese abhängigen Plugins installiert sind . Diese Plugins Aktivieren Die Ausführung von IntegrationHub Aktionen und Flows: • ServiceNow IntegrationHub-Aktionsschritt – REST (com.Glide.Hub.action_STEP.Rest) • ServiceNow IntegrationHub-Laufzeit (com.glide.hub.integration.runtime) **Hinweis:** Wenn möglich „t Suchen Sie ein Plugin, das Sie möglicherweise von anfordern müssen ServiceNow Personal. Um ein Plugin anzufordern, befolgen Sie die in Plugin anfordern erläuterten Schritte. Die Security Incident Response Plugin (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Anwendungen Das sind Erforderlich für die Integration. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

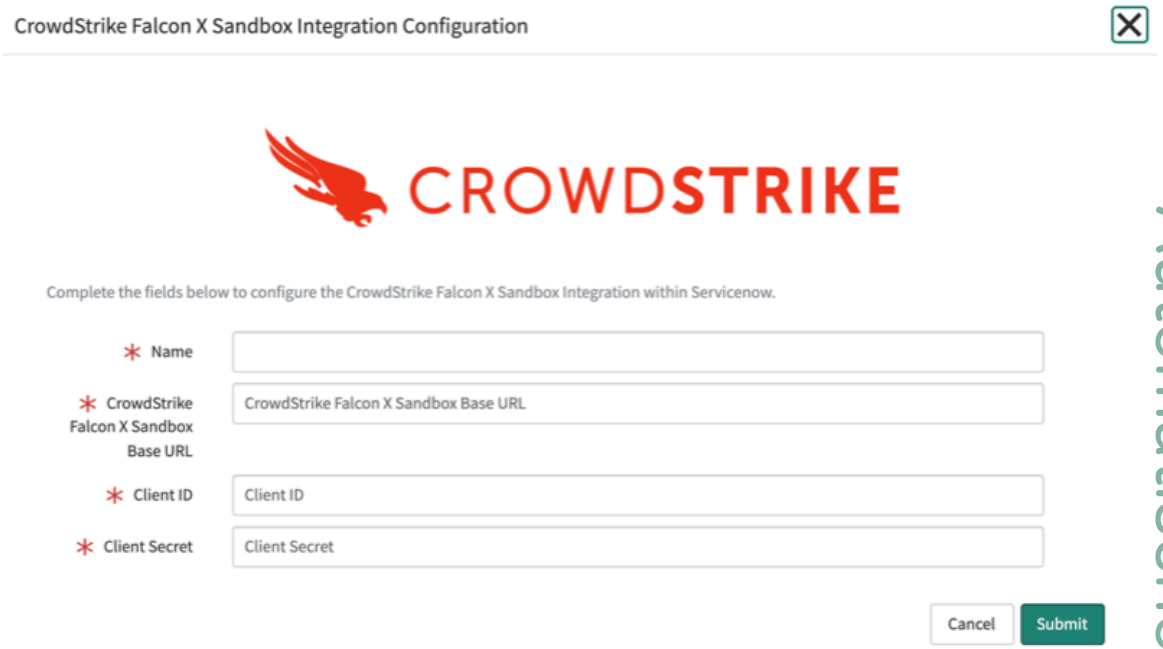
Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. **1.** Security Incident Response Abhängigkeit (com.snc.si_dep) **2.** Sicherheits-Integrations-Framework **3.** Security Support Common **4.** Orchestration Des Sicherheitssupports **5.** Threat Intelligence Allgemeiner Support (erforderlich für u SE Die Sandbox-Integrationsfähigkeiten) **6.** Trusted Security Circles **7.** Security Operations Setup-Assistent **8.** Security Incident Response Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz für die Integration finden Sie unter Ruft die Berechtigung für ein Security Operations-Produkt ab Oder Anwendung und Aktivieren Sie eine ServiceNow Store-Anwendung .
Stellen Sie sicher, dass Sie für den privaten Falcon Sandbox-API-Schlüssel und lizenziert sind o Behalten Sie den bei CrowdStrike Falcon X Sandbox Vollständiger API-Schlüssel.	Diese Integration unterstützt nur die Falcon Sandbox Private Cloud. **Hinweis:** Dieses Release unterstützt die Falcon X-Integration nicht. CrowdStrike Falcon X Sandbox Bietet einen selbst signierten eingeschränkten API-Schlüssel und einen aktualisierten vollständigen API-Schlüssel. Verwenden Sie den vollständigen API-Schlüssel für diese Integration Weil Ermöglicht uneingeschränkten Zugriff für automatisierte Übermittlungen. Weitere Informationen finden Sie unter CrowdStrike Falcon Sandbox Knowledge Base .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Laden Sie die CrowdStrike Falcon Sandbox for Security Operations-Integration aus dem ServiceNow Store herunter .
2. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen** .
3. Suchen Sie nach CrowdStrike Falcon X Sandbox Integrationskachel und klicken Sie auf **Konfigurieren** .



4. Geben Sie die folgenden Details ein, um die Konfiguration abzuschließen:

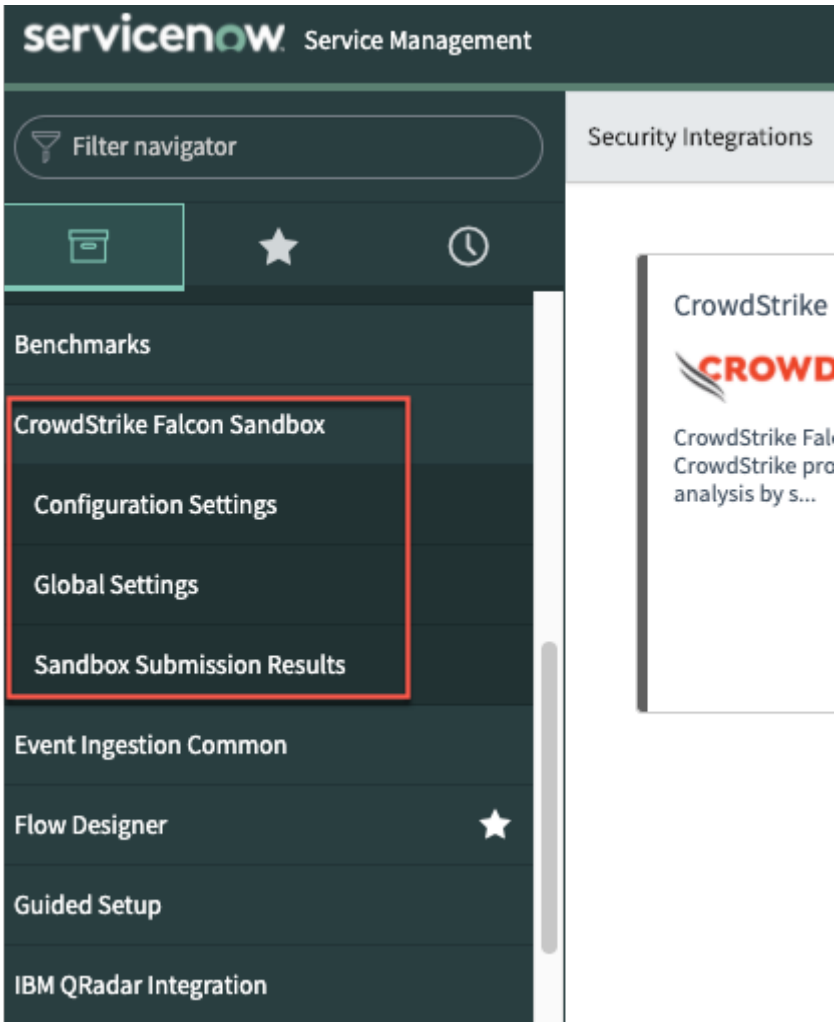
Feld	Beschreibung
Name	Name dieser Integration, z. B. `Demo-1` . Dies ist ein eindeutiger Name zur Identifizierung von S Andbox-Konfiguration können Sie nur eine Integration pro ServiceNow-Instanz konfigurieren.
CrowdStrike Falcon Sandbox-Basis-URL	S Andbox-Basis-URL. Dies URL Ist verfügbar Nach Sie konfigurieren Die S Andbox.Beispiel: `https://servicenow .falcon-sandbox.com` Ist eine Basis-URL .
Client-ID	OAuth2-API-Client-ID. Weitere Informationen finden Sie unter . API-Clients und Schlüssel .
Geheimer Clientschlüssel	Geheimer Schlüssel des OAuth2-API-Clients. Weitere Informationen finden Sie unter . API-Clients und Schlüssel .

5. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach Die Sandbox Wurde erfolgreich validiert und übermittelt, IT Wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Sie können jetzt das Sandbox-Modul in anzeigen Anwendung navigator.



Nächste Maßnahme

Nachdem Sie die Integration erfolgreich abgeschlossen haben, besteht der nächste Schritt in der Einrichtung Sandbox-Übermittlungskonfigurationen .

Richten Sie Sandbox-Übermittlungskonfigurationen ein

Richten Sie die Sandbox-Konfiguration ein, um die Analyseumgebung und Laufzeitoptionen für die Übermittlung von Security Incident-Datensätzen für die Malware-Analyse zu definieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

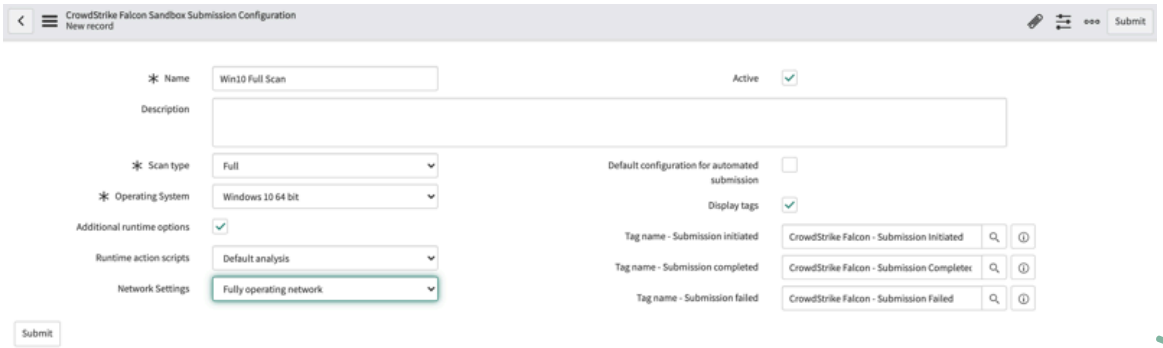
Warum und wann dieser Vorgang ausgeführt wird

Bevor Sie Dateien oder URLs an übermitteln können CrowdStrike Falcon X Sandbox Mit der -Integration müssen Sie mindestens eine Übermittlungskonfiguration konfigurieren. Die Übermittlungskonfiguration definiert das Sandbox-Betriebssystem, den Scan-Typ, die Laufzeitoptionen und andere Merkmale der Incident-Behandlung. Sie können mehrere Konfigurationen für erstellen Verwenden Die verschiedenen Optionen Das Verfügbar in CrowdStrike Falcon X Sandbox Umgebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **CrowdStrike Falcon X Sandbox** > **Konfigurationseinstellungen**an.
2. Klicken Sie auf **Neu**.



3. Füllen Sie die folgenden Felder aus, um eine Konfiguration für zu erstellen Voll **Scan-Typ** .

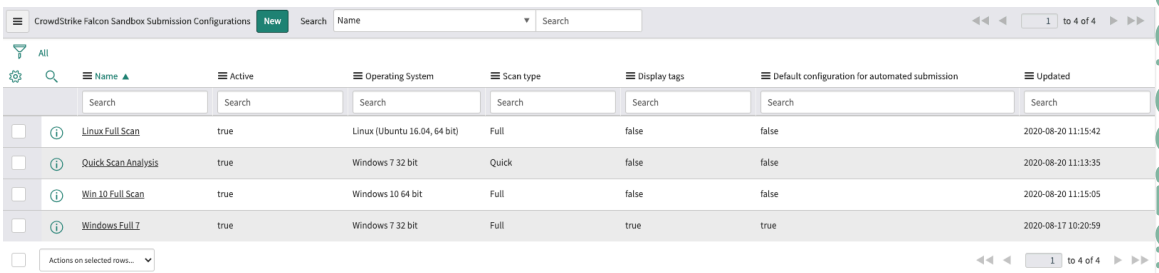
Feld	Beschreibung
Name	Eindeutiger Name für die Übermittlungskonfiguration. Dieser Name wird Analysten angezeigt, wenn sie eine Datei übermitteln. Es ist wichtig, sicherzustellen, dass der Name beschreibend und leicht von den anderen Konfigurationen zu unterscheiden ist (Beispiel: Win 10 Full Scan). Wenn der Name nicht eindeutig ist, wird ein Fehler angezeigt, und doppelte Konfigurationsdatensatznamen werden nicht gespeichert.
Überprüfungstyp	S Kann als eingeben **Voll** . A **Schnell** Der Scan-Typ bietet eine eingeschränkte Bedrohungsanalyse.
Betriebssystem	A Nalysieren Sie die VM-Umgebung, die Die s Andbox scannt die Datei oder URL in.
Aktiv	O PSP Die Sie auswählen Beim manuellen Senden von Dateien oder URLs.
Standardkonfiguration für automatisierte Übermittlung	O PSP Das Ist standardmäßig gelöscht. Wenn Sie diese Option auswählen, kann diese Konfiguration für die Automatisierung der Übermittlung von Malware-Analysen verfügbar sein. **Hinweis:** Sie können nur eine aktive Übermittlungskonfiguration als Standardkonfiguration für automatisierte Übermittlungen haben.
Tags anzeigen	O PSP Das Ist standardmäßig gelöscht. Wenn Sie diese Option auswählen, werden Tags angezeigt, um den Status einer Datei oder URL-Übermittlung anzugeben. Die Verarbeitung der Analyse kann

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	einige Minuten dauern. Die Anzeige-Tags sind Übermittlung initiiert, Übermittlung abgeschlossen, Oder Übermittlung fehlgeschlagen.
Weitere Laufzeitoptionen	O PSP Das Ist standardmäßig gelöscht. Wenn Sie diese Option auswählen, sind zusätzliche Laufzeitparameter verfügbar, die von Sandbox unterstützt werden.
Laufzeit-Aktionsskripts	Option, mit der Sie eine verwenden können A Aktionsskript Die simulieren S Menschliches Verhalten und Interaktion S Mit der Datei oder URL während der Analyse. https://www.crowdstrike.com/endpoint-security-products/falcon-sandbox-malware-analysis/ Siehe CrowdStrike Falcon X Sandbox Dokumentation für weitere Details.
Netzwerkeinstellungen	Option, mit der Sie den Typ der Netzwerkeinstellungen auswählen können, die beim Senden einer URL oder Datei an Sandbox verwendet werden.

4. Klicken Sie auf **Absenden**.
   Nachdem Sie die Konfiguration übermittelt haben, wird sie auf der Seite „Konfigurationseinstellungen“ als Datensatz gespeichert. Die Konfiguration Muss Be **Aktiv** Zur Verwendung in S Andbox-Übermittlungen.



Nächste Maßnahme

Nachdem Sie konfiguriert haben S Andbox-Übermittlungen, der nächste Schritt ist bis Übermitteln Sie Dateien oder ULRs manuell an Sandbox

an.

Übermitteln Sie Dateien oder URLs manuell an Sandbox

Sie können eine Datei oder URL manuell an eine Sandbox senden, wenn bestimmte Incident-Kriterien wie „Kategorie“ „Phishing“ erfüllt sind.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

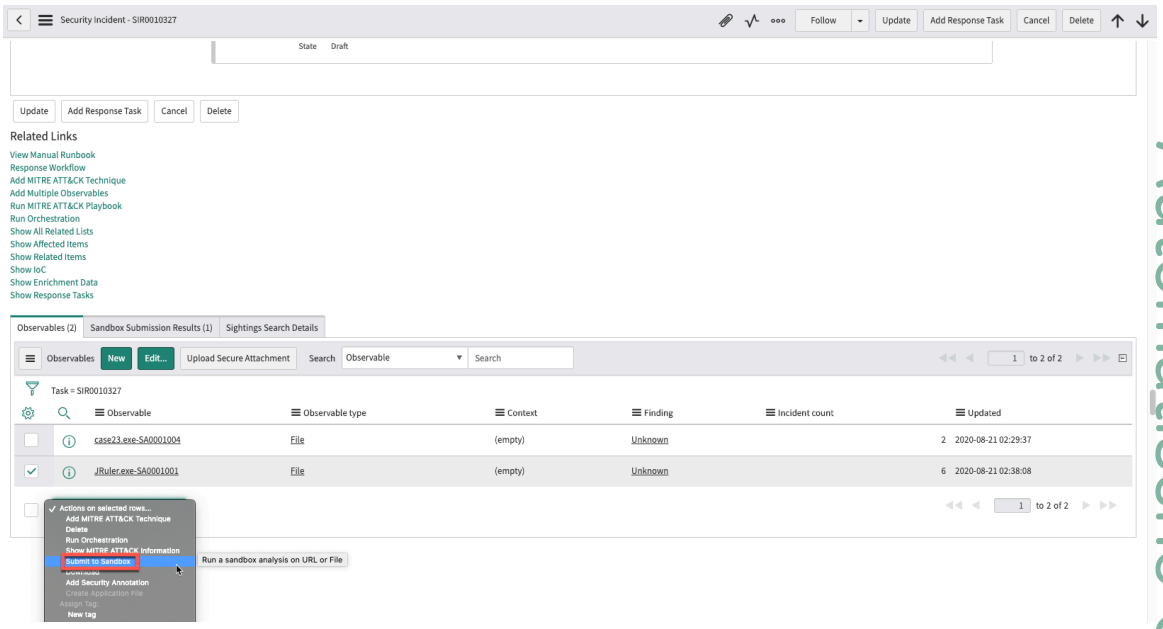
Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie den Security Incident und die Datei oder URL überprüft haben, können Sie auswählen **An Sandbox senden** Option zum Durchführen einer Malware-Analyse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

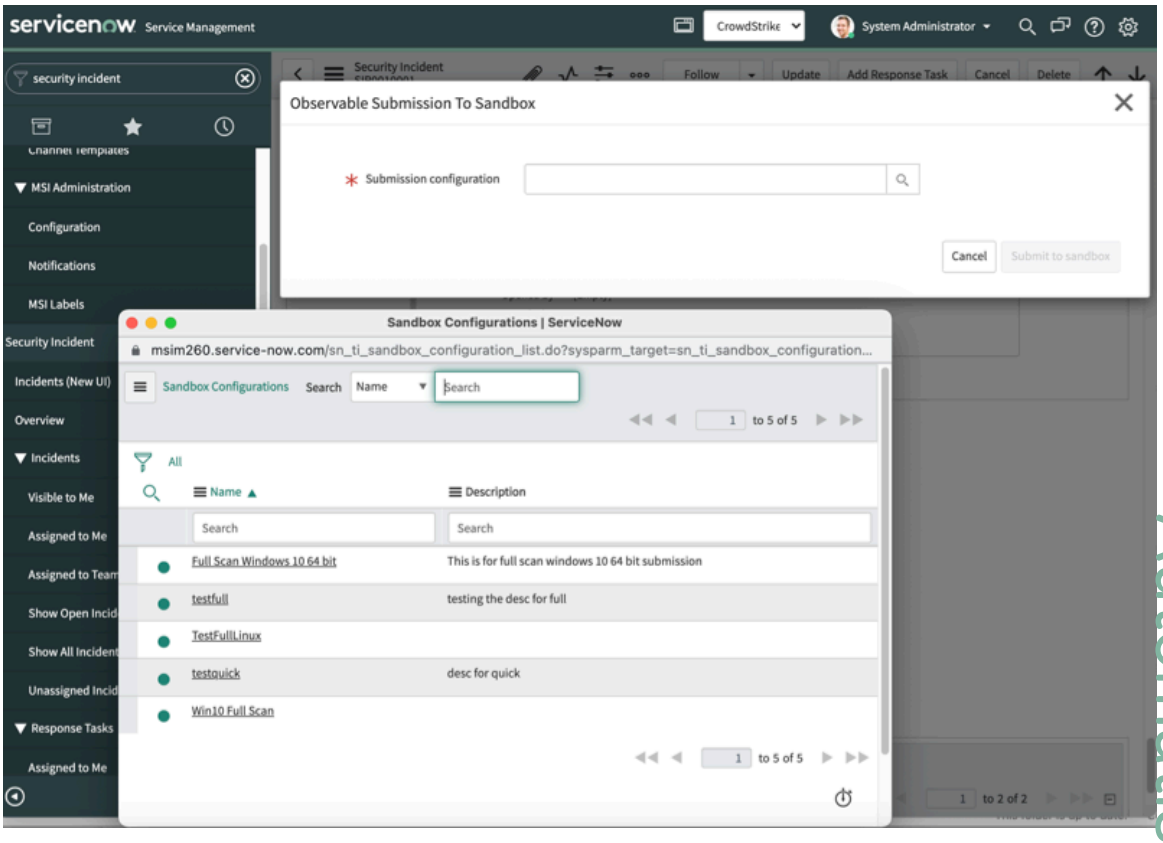
1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen** Und öffnen Sie einen Security Incident, an den Sie einen Datensatz vom Typ Datei oder URL eines erkennbaren Elements übermitteln möchten.
2. Klicken Sie auf **IOC anzeigen** Zugehöriger Link.
3. Auf der **Erkennbare Elemente** Wählen Sie auf der Registerkarte einen oder mehrere Datensätze aus, für die Sie eine Malware- oder Bedrohungsanalyse durchführen möchten, und klicken Sie auf **An Sandbox senden** .



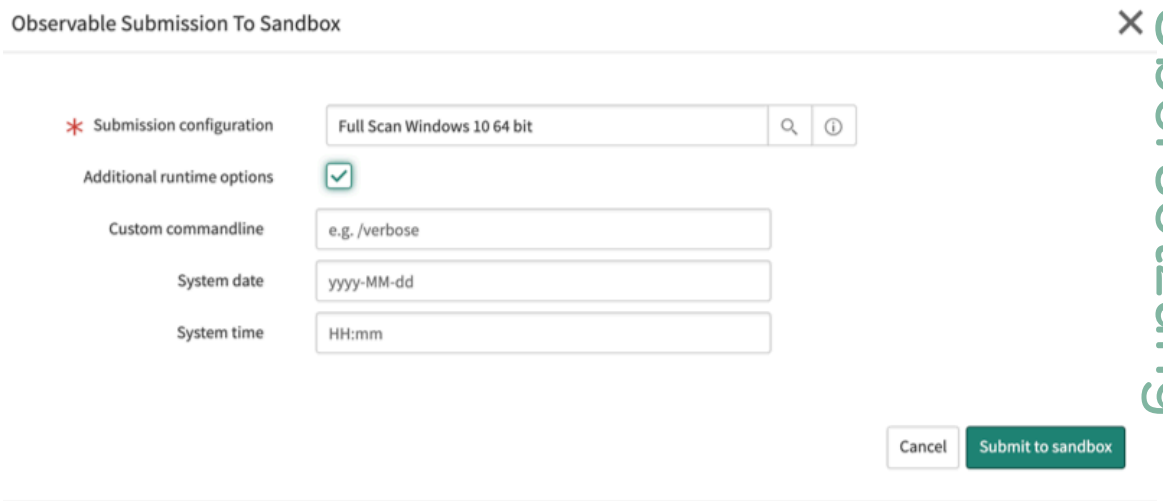
4. Wenn der Filter Dateiübermittlung angezeigt wird, wählen Sie Ihre bevorzugte Sandbox-Konfiguration in aus **Übermittlungskonfiguration** , Und klicken Sie auf **An Sandbox senden** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. **Wahlweise:** Wählen Sie Aus **Zusätzliche Laufzeitoptionen** Wenn Sie weitere anwenderdefinierte Optionen bereitstellen möchten.



Feld	Beschreibung
Anwenderdefinierte Befehlszeile	Reguläre Anwendungsbefehlszeile oder ein spezieller Vorgang.
Systemdatum	Systemdatum im Format JJJJ-MM-TT.
Systemzeit	Systemzeit im Format HH:mm.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie die Übermittlung initiiert haben, können Sie die Arbeitsnotizen anzeigen, um den Status Ihrer Übermittlung anzuzeigen. Weitere Informationen zum Status der Übermittlung oder zum Analysieren der Ergebnisse finden Sie unter **Sandbox-Übermittlungsergebnisse** .

Hinweis:
In CrowdStrike Falcon X Sandbox wird der Schnellscan für URLs nicht unterstützt. Wenn die Arbeitsnotizen zu viele Informationen enthalten, können Sie die Option Filter verwenden, um einen Drilldown zu den erforderlichen Arbeitsnotizen durchzuführen, die für Sie relevant sind.

Nächste Maßnahme

Wenn Sie die erkennbaren Elemente zur Malware-Analyse an die Sandbox senden, Zeigen Sie die Sandbox-Übermittlungsergebnisse an Um die nächsten Schritte bei potenziellen Bedrohungen auszuführen.

Automatisieren CrowdStrike Falcon Sandbox-Übermittlungen mit Flow Designer

Die CrowdStrike Falcon X Sandbox Die Integration enthält Flow-Vorlagen, die mit erstellt wurden Workflow-Studio Die mit Security Incident-Datensätzen arbeiten.

Vorbereitungen

- Überprüfen Sie, ob Sie einen erstellt haben Sandbox-Übermittlungskonfiguration Und haben eine Konfiguration als aktiviert **Standardkonfiguration für automatisierte Übermittlung** . Wenn der Flow ausgelöst wird, erfolgt die Sandbox-Übermittlung in Ihrer Standardkonfiguration.

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Diese Flows dienen in erster Linie dazu, Ihnen den Einstieg zu erleichtern, wenn Sie Datei- oder URL-Übermittlungen als Teil Ihres Incident-Response-Workflows automatisieren möchten.
Wenn Sie einen Beispiel-Flow aktivieren, werden Ihre Phishing-Dateianhänge automatisch übermittelt, wenn Sie die Security Incidents in Ihrem Beispiel-Flow als Phishing definieren. Alternativ können Sie alle .exe-Dateien übermitteln, wenn dieser Dateityp an einen Datensatz eines erkennbaren Elements angehängt ist.

Sie können diese Beispiel-Flows ändern, um eine automatisierte Übermittlung unter verschiedenen Bedingungen, Kategorien, zusammengesetzten Bedingungen usw. auszulösen.

Die Sandbox-Integration besteht aus zwei Basissystem-Flows, die standardmäßig deaktiviert sind.

- **Datei senden, wenn die Kategorie Phishing ist** : Dieser Flow sendet eine Datei zur Malware-Analyse an die Sandbox, wenn die Kategorie des Security Incidents als Phishing definiert ist. Sie müssen eine Datei an den Datensatz des erkennbaren Elements für den Security Incident anhängen. Wenn Sie die URP-Funktionalität (User gemeldetes Phishing) verwenden, werden alle E-Mail-Anhänge automatisch analysiert und dem SIR-Incident-Datensatz als Datensatz erkennbarer Elemente hinzugefügt. Zum Automatisieren der Übermittlung ist keine weitere Aktion erforderlich.
- **Übermitteln, wenn der Dateityp für das erkennbare Element „exe“ ist** : Dieser Flow sendet eine Datei zur Malware-Analyse an die Sandbox, wenn das erkennbare Security Incident eine exe ist. Ähnlich wie beim Phishing-Kategorie-Flow müssen Sie eine Datei an einen Datensatz eines erkennbaren Elements für den Security Incident anhängen. Sie können dies manuell tun, indem Sie die Datei hochladen oder automatisch, wenn den Datensätzen erkennbarer Elemente ein Phishing-E-Mail-Anhang oder ein anderer Mechanismus zugeordnet ist, der den Incident erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Flows konfiguriert sind und die Incident-Bedingungen die Parameter erfüllen, werden die Sandbox-Übermittlungen automatisch ausgelöst, wenn Sie den Security Incident überprüfen. Überprüfen Sie die Arbeitsnotiz, die angibt, dass eine Übermittlung initiiert wurde, ein Tag angezeigt wird, wenn in der Konfiguration aktiviert, und einen Datensatz mit den Ergebnissen der ausstehenden Übermittlung.

Die Sandbox-Integration enthält auch mehrere Subflows. Die Subflows sind interne Komponenten der allgemeinen Integrationsübermittlungsfunktionen. Sie können die Subflows an Ihre Sicherheitskriterien anpassen und bearbeiten.

Sie können auf die Subflows verweisen, um Probleme mit Sandbox-Übermittlungen zu beheben. Jedes Mal, wenn Sie einen Subflow aufrufen, wird ein Ausführungsdatensatz erstellt. Dieser Datensatz gibt an, wo im Flow ein bestimmter Fehler aufgetreten ist, und ermöglicht es Ihnen, das Problem zu beheben.

Sandbox-Integration: Mehrere Workflows

Flows | Subflows | Executions | Help

+ New

All > Application Name contains Sandbox

Name ▲	Internal name	Application	Status	Active	Updated	Updated by
Search	Search	*Sandbox	Search	Search	Search	Search
Add submission status tag on SIR	add_submission_status_tag_on_sir	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 12:33:57	admin
Aggregate Additional Runtime Options	aggregate_additional_runtime_options	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-16 08:47:54	admin
Connection and Credential Validation	connection_and_credential_validation	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-18 02:52:33	admin
CrowdStrike Falcon Sandbox Poll Submission	crowdstrike_falcon_sandbox_polling	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-02 05:11:53	admin
CrowdStrike Falcon Sandbox Submission	submit_file_to_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:17:57	admin
CrowdStrike Falcon Submission Results	crowdstrike_falcon_submission_results	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-13 06:30:16	admin
CrowdStrike Polling Quick/Full Scan	crowdstrike_polling_quickfull_scan	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 20:23:07	admin
Fetch Environment Ids from Sandbox	fetch_environment_ids_from_sandbox	Security Operations CrowdStrike Falcon S...	Published	true	2020-05-25 07:45:54	admin
Submit File or URL to CrowdStrike Quick ...	submit_fileurl_to_crowdstrike	Security Operations CrowdStrike Falcon S...	Published	true	2020-07-20 19:04:42	admin
Submit File/URL to Sandbox	submit_fileurl_to_sandbox	Security Operations CrowdStrike Falcon S...	Draft	true	2020-05-25 07:50:18	admin
Submit Observable for Automated submission	submit_observable_for_automated_submission	Security Operations CrowdStrike Falcon S...	Published	true	2020-08-06 06:15:35	admin

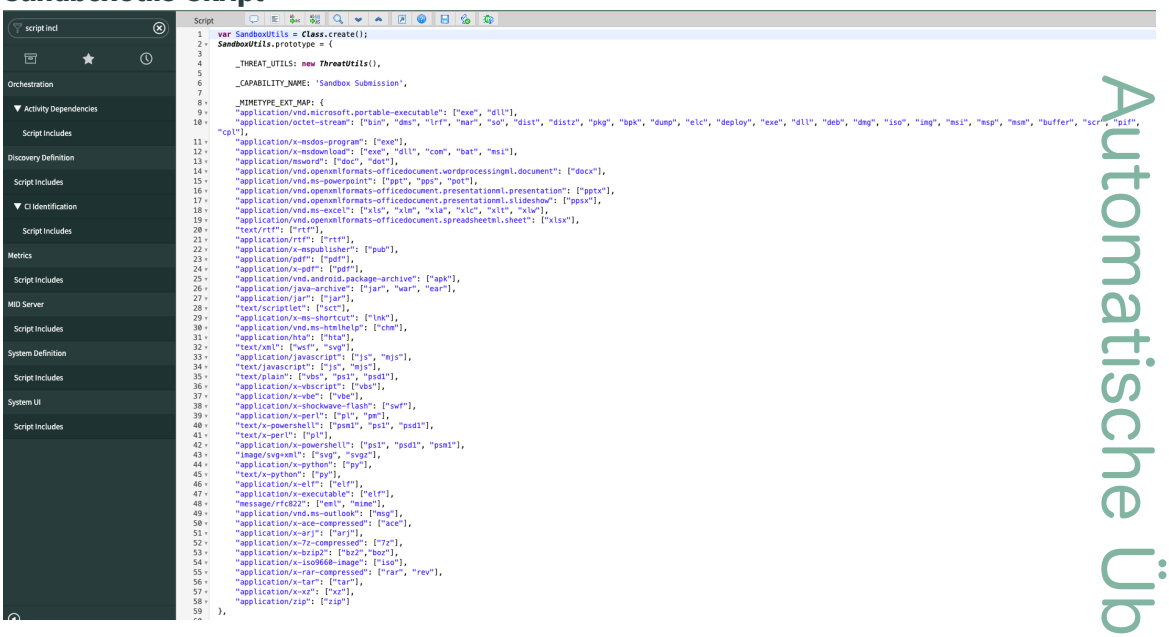
Actions on selected rows... 1 to 11 of 11

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

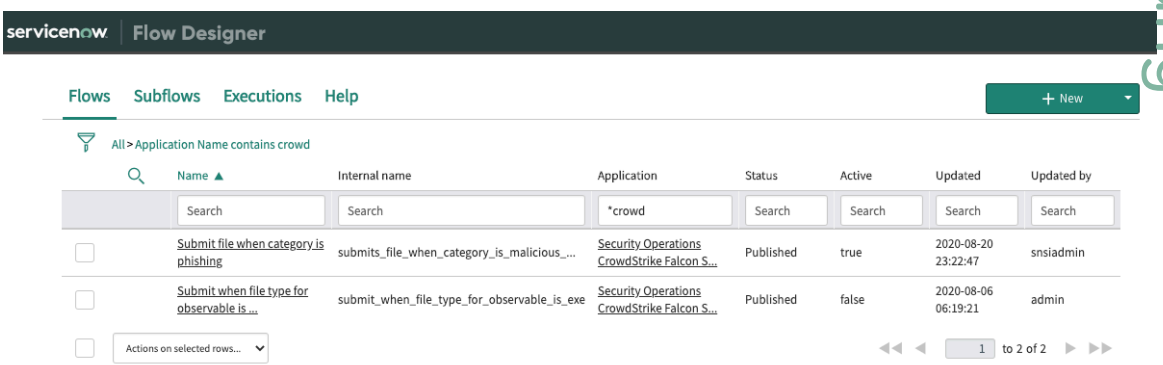
- Wenn Sie die Standard-Flows anpassen möchten, sollten Sie sicherstellen, dass der Subflow „erkennbares Element für automatisierte Übermittlung übermitteln“ in Ihrem Flow enthalten ist, um automatische Übermittlungen auszulösen.
- Sie können Ihre Dateierweiterungen für eine exe anpassen und definieren. Erstellen Sie eine Kopie des Flows **Übermitteln, wenn der Dateityp für das erkennbare Element „exe“ ist** , Und nehmen Sie Änderungen an der Kopie vor. Der Inhaltstyp und die Dateierweiterungen werden in zugeordnet SandboxUtils Skript. Um auf Skripteinbindungen zuzugreifen, navigieren Sie zu **Systemdefinitionen > Skripteinbindungen** Und suchen Sie nach SandboxUtils.

SandboxUtils-Skript



Prozedur

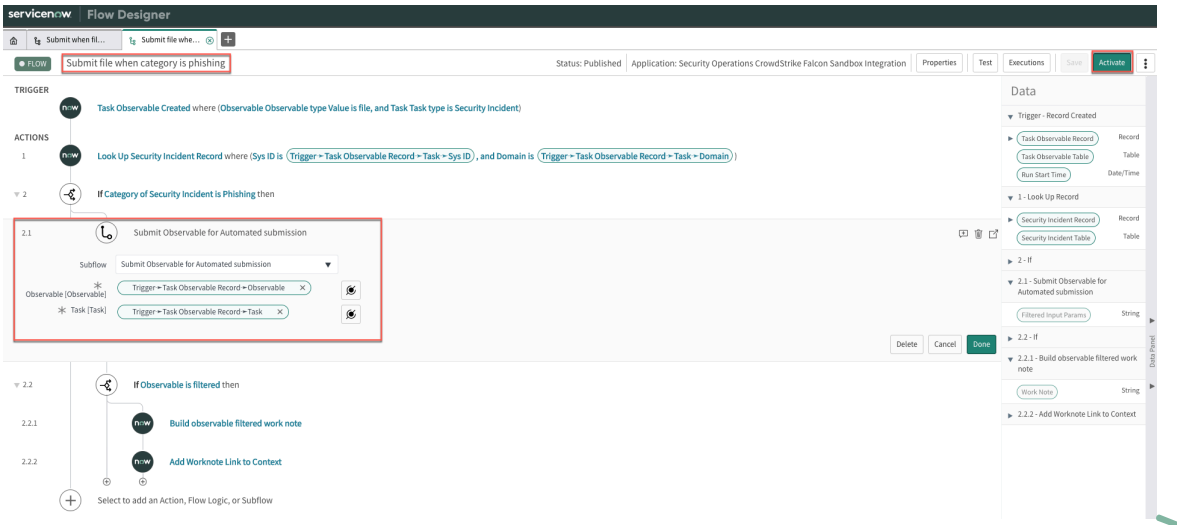
1. Navigieren zu **Alle** > **Flow Designer** > **Designer** > **Flows**an.
2. Filtern Sie die Flows nach **Anwendung** Typ.
   Beispiel: *Crowd filtert die beiden CrowdStrike Falcon X Sandbox Flows.



3. Wählen Sie einen Flow aus, um die Details anzuzeigen.
   Das folgende Beispiel zeigt den Flow „Datei senden, wenn Kategorie Phishing ist“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie Auf **Aktivieren** Und klicken Sie dann auf **OK** Wenn die Bestätigungsnachricht angezeigt wird.

Nächste Maßnahme

Nachdem Sie automatisierte Übermittlungs-Flows konfiguriert haben, können Sie Zeigen Sie die Sandbox-Übermittlungsergebnisse an Um Bedrohungen zu analysieren.

Überwachen Sie Übermittlungsergebnisse In der Sandbox

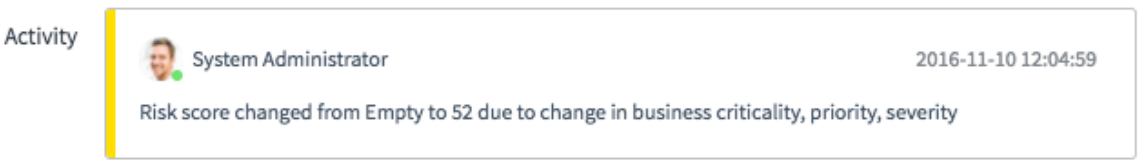
Ergebnisse für alle Sandbox-Übermittlungen werden in angezeigt **Sandbox-Übermittlungsergebnisse** Registerkarte für jeden Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

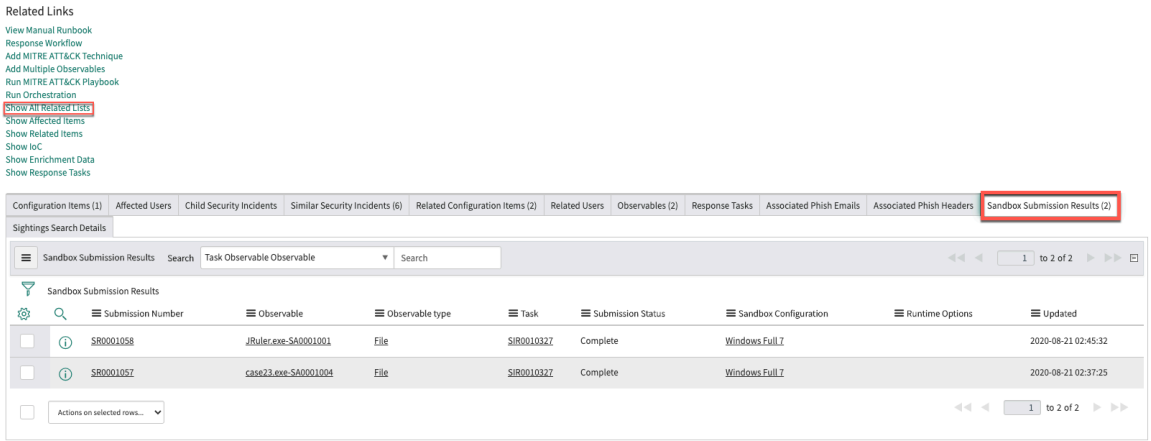
1. Öffnen Sie den Security Incident Das Sie arbeiten mit und überprüfen, ob S Andbox-Übermittlung ist erfolgreich.



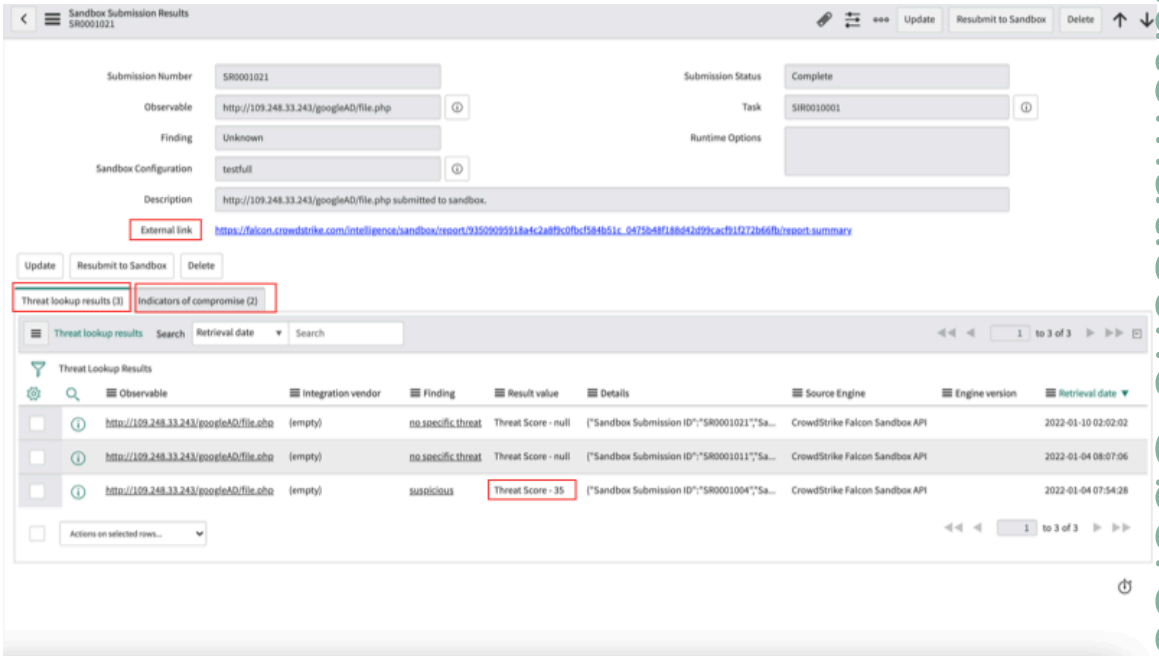
2. Überprüfen Sie W Ork-Notizen für weitere Informationen und Lernen Vorgehensweise, wenn möglich „t Überprüfen Sie, ob der Scan erfolgreich ist.
3. Klicken Sie entweder auf den Link Ergebnisse abschließen In W Ork-Hinweis S Oder Um Der untere Teil des Security Incidents , Navigieren Sie zu **Alle Zugehörigen Listen Anzeigen** > **Sandbox-Übermittlungsergebnisse** .
   Ergebnisse werden auf der Registerkarte Sandbox-Übermittlungsergebnisse angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf „beliebigen Datensatz öffnen“, um den vollständigen anzuzeigen S Andbox-Analyse.



5. **Wahlweise:** Klicken Sie Auf **Erneut an Sandbox übermitteln** Um das erkennbare Element erneut zu verarbeiten.

Ergebnisse

- Die **Ergebnisse der Bedrohungssuche** Die Registerkarte bietet die Bedrohungsbewertung, einschließlich böswilliger Ergebnisse, Bedrohungsbewertungen und zusätzlicher Details. Th Ese-Details Sind Wird in der Standardformatstruktur für die Bedrohungssuche für alle bereitgestellt ServiceNow Integrationen der Bedrohungssuche.
- Die **Kompromittierungsindikatoren** Registerkarte Stellt bereit Die Böswillig oder verdächtig S Andbox-Ergebnisse Mit den Konfidenzpunktzahlen. Die Konfidenzpunktzahlen ähneln anderen Indikatorinformationen, die in gespeichert sind ServiceNow Plattform. Indikatoren, die als informativ klassifiziert sind, sind nicht in dieser Registerkarte enthalten .

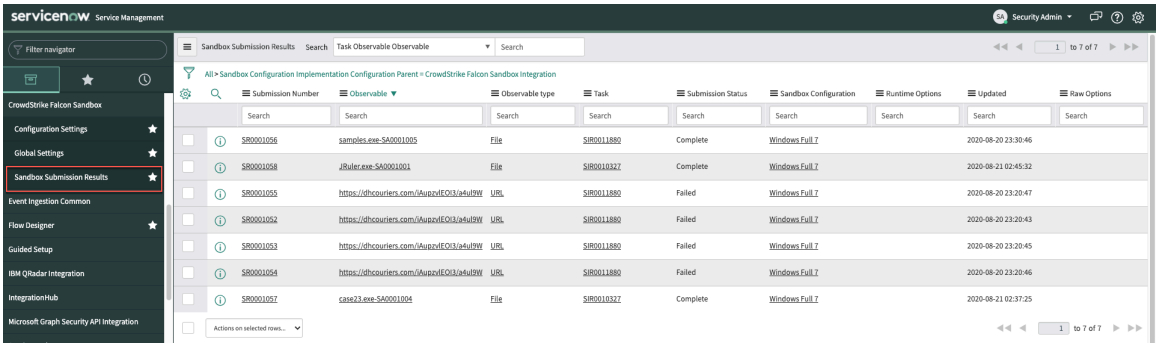
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie Auf **Externer Link** Zum Anzeigen der Sandbox Ergebnisse In CrowdStrike Falcon X Sandbox Portal.

Hinweis:
Diese Option erfordert Das Sie Haben Die CrowdStrike Falcon X Sandbox Rolle Zum Anzeigen der Ergebnisse.

Sie können Überwachen Sie auch Die S Andbox-Übermittlungsergebnisse für alle Security Incidents, indem Sie zu navigieren **CrowdStrike Falcon Sandbox** > **Sandbox-Übermittlungsergebnisse**an.



Tag für Security Incidents mit dem Sandbox-Übermittlungsstatus

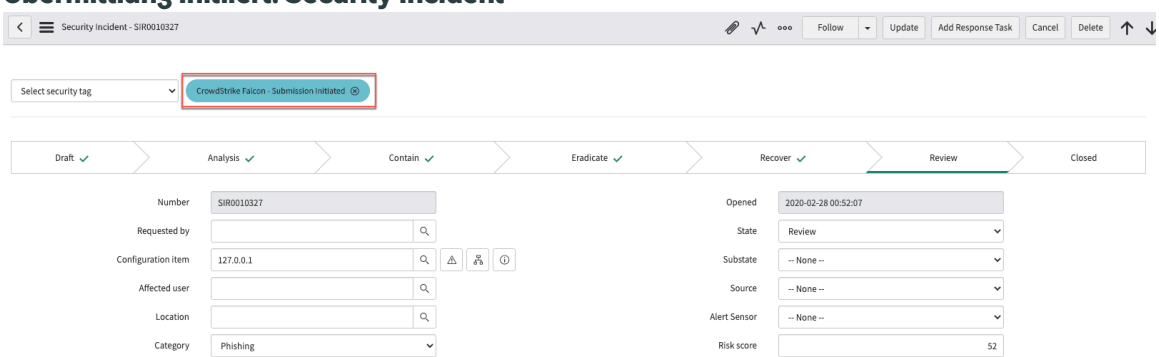
Sie können Security Incidents optional mit den Tags „Übermittlung initiiert“ und „Übermittlung abgeschlossen“ kennzeichnen.

Wenn Sie auswählen **Tags anzeigen** Option in Sandbox-Übermittlungskonfiguration , Tags werden angezeigt, um den Status einer Datei oder URL-Übermittlung anzugeben. Der Status wird auf diese Weise überprüft Nützlich Weil Die S Die Verarbeitung der andbox-Analyse kann einige Minuten dauern.

Die Anzeige-Tags sind Übermittlung aufgerufen Initiiert, Übermittlung abgeschlossen und Übermittlung fehlgeschlagen.

Das folgende Beispiel zeigt einen Security Incident, bei dem die Übermittlung initiiert wurde.

Übermittlung Initiiert: Security Incident

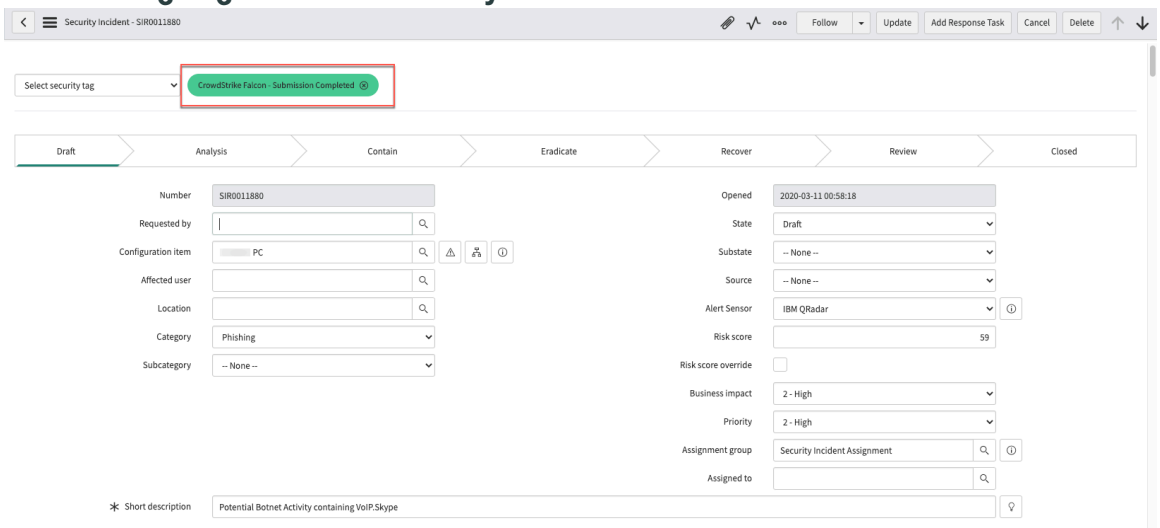


Das folgende Beispiel zeigt einen Security Incident, bei dem die Übermittlung abgeschlossen wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übermittlung Abgeschlossen: Security Incident



Überprüfen Sie die globalen Sandbox-Einstellungen

Überprüfen und ändern Sie die globalen Sandbox-Einstellungen, wenn Probleme mit den Ergebnissen der Datei- oder URL-Übermittlung auftreten.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **CrowdStrike Falcon Sandbox** > **Globale Einstellungen**an.
2. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Dateigrößenbeschränkung (MB)	Größenbeschränkung für Sandbox-Upload-Dateien in Megabyte. **Hinweis:** Die Dateigrößenbeschränkung von 256 MB ist standardmäßig konfiguriert. Erhöhen Sie den Wert nicht über 256 MB. Sie können jedoch die maximale Dateigröße reduzieren, um zu vermeiden, dass große Dateien übermittelt werden.
Maximale Zeitüberschreitung für Übermittlungsergebnisse (Minuten)	Maximale Zeitüberschreitung für Übermittlungsergebnisse aus der Sandbox. **Hinweis:** Die Standardzeitüberschreitung beträgt 30 Minuten. Wenn Ihre Ergebnisse länger als 30 Minuten dauern, können Sie die Zeit erhöhen. Sie können die Ergebnisse auch im Sandbox-Portal anzeigen.

3. Klicken Sie auf **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elasticsearch – Incident-Anreicherung – Integration

Die Elasticsearch– Die Incident-Anreicherungsintegration durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

Erkunden	Einrichten
Security Incident Response-Integrationen	• Beginnen Sie mit dem Elasticsearch– Integration der Incident-Anreicherung • Erstellen Sie Konfigurationsdatensätze für Sichtungssuche
Verwenden	**Entwickeln**
• Führen Sie eine Sichtungssuche aus • Integration Von Security Operations: Sichtungssuche-Flow • Security Operations: Elasticsearch-Sichtungssuche-Flow	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie Komponenten, die mit einer Anwendung installiert sind
Problembehandlung und Hilfe	
• Problembehandlung bei der Integration • Stellen oder beantworten Sie Fragen in der Security Operations-Community • Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen • Kontakt Kundenservice und Support	

Beginnen Sie mit dem Elasticsearch– Integration der Incident-Anreicherung

Elasticsearch Ist eine verteilte, RESTful-Such- und Analytics-Engine, die einfach in integriert werden kann Security Operations. Bevor Sie verwenden können Elasticsearch– Integration der Incident-Anreicherung. Sie müssen sie aus dem herunterladen ServiceNow Store Und fügen Sie die entsprechende API-Basis-URL und Anmeldeinformationen hinzu.

Vorbereitungen

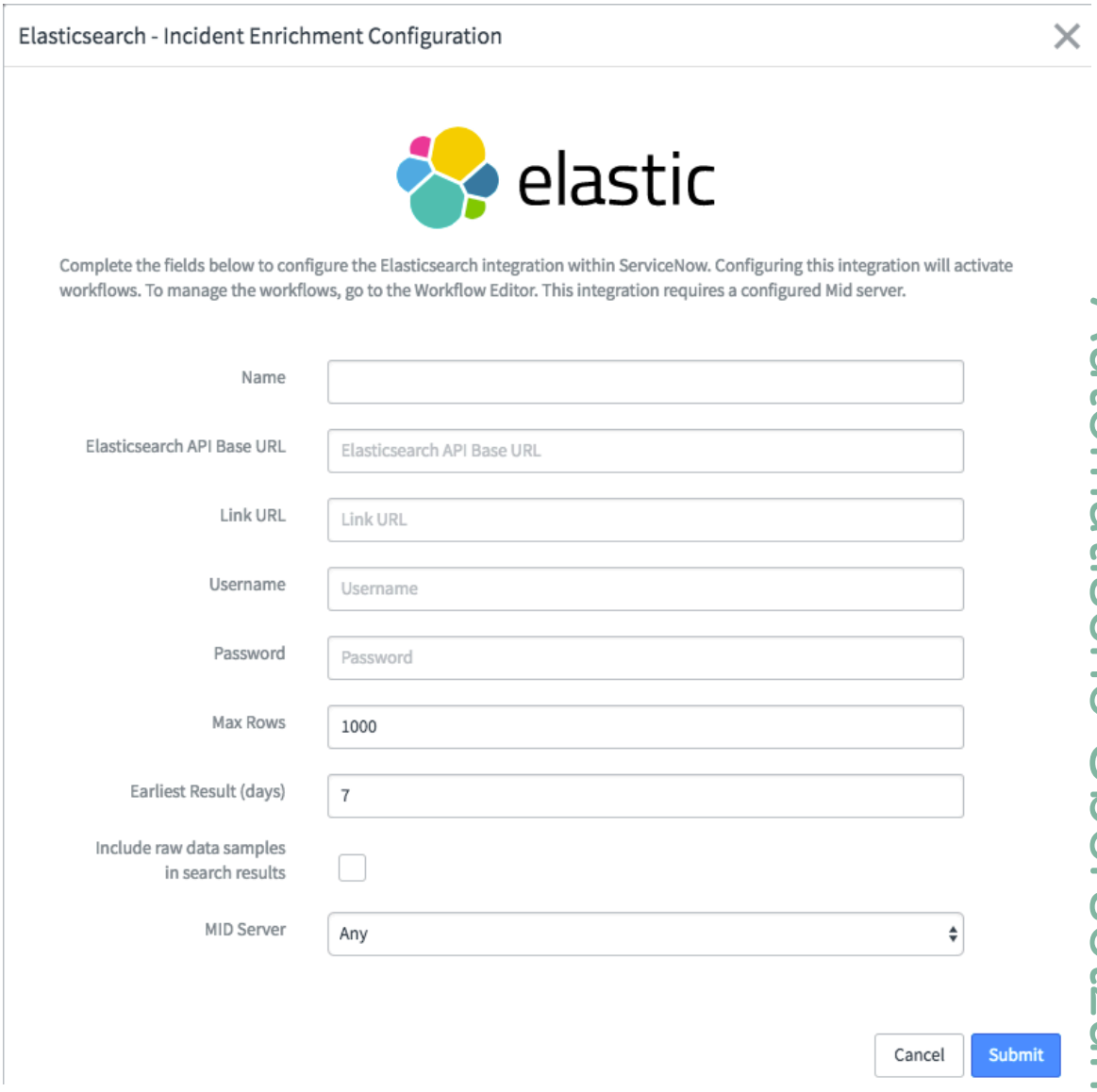
Erforderliche Rolle: sn_si.admin

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf zu Elasticsearch Und rufen Sie die API-Basis-URL unter Ihrem Elasticsearch-Profil ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. In Elasticsearch– Incident-Anreicherungskarte, klicken Sie auf **Neu** .



Automatische Übersetzung

5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Basis-URL der Elasticsearch-API	Die Basis-URL, die Sie von erworben haben Elasticsearch Website.
Link-URL	[Optional] Links zu einer Kibana-Instanz, falls verfügbar
Anwendername	Ihre Informationen Elasticsearch Anwendername.
Passwort	Ihre Informationen Elasticsearch Passwort.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie in Tagen anzeigen möchten.
Rohdatenmuster in Suchergebnissen berücksichtigen	Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in ab **Anzahl der Zeilen mit Rohdaten** Eigenschaft in Eigenschaften von Security Incident Response .
MID-Server	Wählen Sie Aus **Beliebig** Um einen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Navigieren Sie zum Verwalten der Workflows zu **Workflow-Editor** .

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf klicken **Konfigurieren** Oder **Löschen** Zum Ändern oder Löschen der Konfiguration.
8. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie aus **Nein** Von **Konfigurationen Anzeigen** Dropdown-Liste.

Ergebnisse

Nachdem konfiguriert wurde, wird Elasticsearch– Die Incident-Anreicherungsintegration kann ausgewählt werden, um erkennbare Elemente in Beobachtungslisten in Security Incident Response zu veröffentlichen.

FireEye Endpoint Security-Integration

FireEye Endpoint Security (HX-Serie) hilft Organisationen, bekannte und unbekannte Bedrohungen auf einem beliebigen Endpunkt zu untersuchen und zu analysieren.

Qualifizierte Angreifer umgehen heute traditionelle Abwehrmaßnahmen, auf die sich die meisten Sicherheitsteams seit Jahren verlassen, um ihre Endpunkte zu schützen. Selbst wenn eine herkömmliche Verteidigung eine bekannte Bedrohung stoppt, kann sie nicht bestimmen, was diese Bedrohung tun wollte. FireEye HX Endpunktsicherheit hilft Ihrem Sicherheitsteam, bekannte und unbekannte erweiterte Bedrohungen gegen Ihre Endpunkte zu verfolgen und zu stoppen.

Die Integration von Gold Standard Security Incident Response mit FireEye HX, Erleichtert und effizient Sicherheitsanalysten die sofortige Untersuchung und Behebung von Security Incidents, ohne zwischen Tools navigieren zu müssen. Sie können das Netzwerk-Containment verwenden, um Korrekturaktionen für die Endpunkte auszuführen, Profile zu implementieren, um bestimmte Details zum Host zu sammeln, und bestimmte Abfragen oder Aktionen für den Endpunkt auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselfunktionen

- Fähigkeit, Host-Ergänzungsaktionen auszuführen, um weitere Details zum Endpunkt zu erfassen, z. B. Hostdetails, Netzwerkstatistiken, Anwenderdetails, Dateidetails, Prozessdetails und Servicedetails.
- Fähigkeit, die Enterprise-Sicherheitssuche durchzuführen, um potenzielle schädliche erkennbare Elemente auf Endpunkten zu erkennen und Korrekturmaßnahmen zu ergreifen.
- Fähigkeit, Selektierung und Datenerfassung für eine eingehende Endpunktinspektion und -Analyse zu erfassen.

Einschränkungen

Im Folgenden sind die bekannten Einschränkungen dieser Integration aufgeführt:

1. Der Feldwert für die Mid-Anwendung muss manuell eingegeben werden.
2. „Host isolieren“ und „laufende Services abrufen“ können für Linux-Agent nicht ausgeführt werden.
3. „Isolation entfernen“ wird für Linux Agent nicht unterstützt.
4. Die Selektierungsakquisition unterstützt Linux-Agent nicht.
5. Anwender müssen zugehörige Links zum Anzeigen von Ergänzungsdaten konfigurieren. Es ist nicht sofort verfügbar.
6. Für die Sichtungssuche können nur fünf aktive Suchen gleichzeitig vorhanden sein. Verbleibend wird in die Warteschlange gestellt und beginnt nach Abschluss einer der laufenden Sichtungen.
7. Sichtungen sind sofort verfügbar, was standardmäßig als „falsch“ aktiviert ist.
8. Hash wird für GET laufender Prozesse nicht unterstützt.

Richten Sie Ihre NowPlatform-Instanz für die FireEye-Integration ein

Überprüfen und überprüfen Sie das folgende Konfigurationsverfahren, um die NowPlatform-Instanz für die FireEye-Integration einzurichten.

Vorbereitungen
Erforderliche Rolle: ServiceNow AI Platform Administrator (sn_si.admin)

Im folgenden Abschnitt werden die Setup-Aufgaben aufgelistet, die in Ihrer NowPlatform-Instanz vor der Installation der Anwendung für die FireEye-Integration ausgeführt werden müssen.

Vergewissern Sie sich, dass Sie die folgenden Aufgaben abgeschlossen haben, bevor Sie die Anwendung aus dem ServiceNow Store installieren.

Aufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderlichen Rollen NowPlatform und Security Incident Response (SIR) zugewiesen haben.	Die folgenden Rollen sind erforderlich: 1. Anwender mit der Rolle „Systemadministrator“ (Administrator) ist erforderlich, um die Anwendung für die Integration zu installieren. 2. Anwender mit der Rolle „Security Incident-Administrator“ (sn_si.admin)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Beschreibung
	ist erforderlich, um die Integration zu konfigurieren, Profile zu erstellen, zu aktivieren und zu entfernen. 3. Anwender mit der Rolle „Security Incident Analyst“ (sn_si.Analyst) ist erforderlich, um mit Security Incidents zu arbeiten. Ein Anwender mit dieser Rolle kann eine der in der Integration verfügbaren Fähigkeiten initiieren.
Überprüfen Sie, ob Sie einen MID-Server installiert und konfiguriert haben.	MID-Server konfigurieren: Ein MID-Server in Ihrer NowPlatform-Instanz ist erforderlich, um Dateien zu verwalten und eine Verbindung mit dem FireEye-Service herzustellen, der innerhalb Ihres Organisationsnetzwerks bereitgestellt wird. Weitere Informationen zu MID-Servern finden Sie unter https://servicenow.com/docs
Stellen Sie sicher, dass die ServiceNow-Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung installieren.	Die folgenden Anwendungen müssen vor der Installation dieser Anwendung im ServiceNow Store installiert und aktiviert werden. Installieren und aktivieren Sie jeweils eine Anwendung in der unten aufgeführten Reihenfolge, um eine reibungslose Installation sicherzustellen: 1. Security Incident Response-Support 2. Sicherheitssupport Core 3. Security Support Common 4. Security Incident Response 5. Threat Intelligence-Support – Allgemein 6. ServiceNow Integration Hub Enterprise Pack-Installationsprogramm
Bevor Sie die Genehmigungsoption für Profile aktivieren, überprüfen Sie, ob Sie eine Genehmigungsgruppe erstellt haben.	Ein optionaler Genehmigungs-Workflow ist verfügbar, um Hostcomputer zu isolieren, sie wieder im Netzwerk wiederherzustellen, Dateien abzurufen und zusätzliche Aktionen am Endpunkt auszuführen. Wenn Ihre Organisation eine zusätzliche Kontrolle über diese Aktionen wünschen, aktivieren Sie während der Konfiguration der Profile die Option Genehmigung erforderlich. Wenn keine Profile vorhanden sind, wenn eine Fähigkeit direkt aus der zugehörigen Liste aufgerufen wird, können Genehmigungen über das FireEye-Standardeinstellungsmodul bearbeitet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

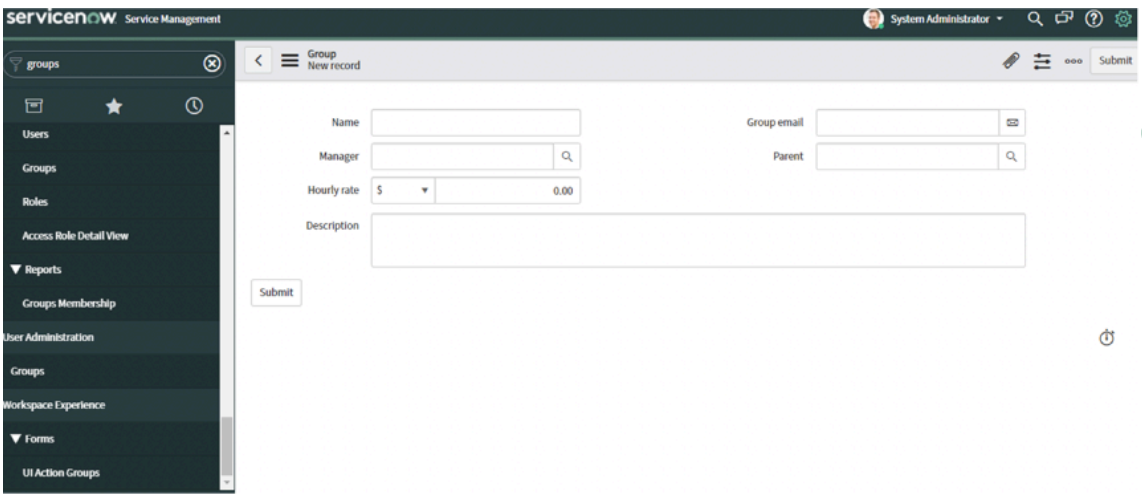
Aufgabe	Beschreibung
	Als Sicherheitsadministrator können Sie Genehmigungen einrichten, während Sie die Profile und Standardeinstellungen konfigurieren. Eine Genehmigungsgruppe muss in Ihrer Instanz in der Gruppenliste verfügbar sein.

Prozedur

1. Navigieren zu **Anwenderadministration** > **Gruppen**an.
2. Klicken **Neu** In der Liste Gruppen.
3. Füllen Sie das Formular mit den folgenden Details aus:

Feld	Beschreibung
Name	Name der Gruppe, die angezeigt wird, wenn eine Genehmigungsanforderung übermittelt wird.
Gruppen-E-Mail	(Optional) Gruppen-E-Mail-Verteilerliste oder die E-Mail-Adresse des Ansprechpartners, z. B. des Gruppenmanagers.
Manager	(Optional) Name des Gruppenmanagers. Klicken Sie auf das Suchsymbol, um die Liste anzuzeigen.
Übergeordnet	(Optional) Name der übergeordneten Gruppe, wenn sie einem übergeordneten Element zugeordnet ist.
Stundensatz	(Optional) der bezahlte Betrag für jede geleistete Stunde.
Beschreibung	(Optional) zusätzliche Informationen zur Gruppe.

4. Klicken **Absenden**an.



Die neue Gruppe wird in der Gruppenliste angezeigt. Sie haben erfolgreich eine Genehmigungsgruppe erstellt. Fügen Sie Ihrer neuen Gruppe nach Bedarf Anwender hinzu, die die vom Sicherheitsanalysten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

übermittelten Anforderungen genehmigen können. Ein Anwender erbt Rollen von allen Gruppen, zu denen der Anwender gehört. Sie können einem Anwender auch Rollen direkt zuweisen.

Um Anforderungen zu überwachen und zu verarbeiten, die von Anwendern mit der Rolle „sn_si.Analyst“ eingereicht wurden, muss jedes Mitglied der Genehmigungsgruppe im zu meine Genehmigungen navigieren ServiceNow AI Platform. Alternativ können die Genehmiger die speziell für die FireEye-Integration übermittelten Anforderungen unter den FireEye-Genehmigungen finden.

Nächste Maßnahme

Der nächste Schritt besteht in der Installation und Konfiguration der Anwendung aus dem ServiceNow Store.

Konfigurieren der Zeitstempeleinstellungen für die Selektierungsakquisition

Konfigurieren und überprüfen Sie die Zeitstempeleinstellungen vor dem Installationsverfahren.

Vorbereitungen

Erforderliche Rolle: NowPlatform Security Incident-Administrator (sn_si.admin)

Vor der Installation der FireEye-Anwendung müssen einige Voraussetzungen für FireEye ausgeführt werden.

Selektierungsakquisition kann mit der Eingabe des Felds „um Zeitstempel“ oder „Standard“ angefordert werden. Um den Zeitstempel werden Informationen angefordert, die während eines bestimmten Zeitraums vor dem Zeitstempel bis zu einem bestimmten Zeitraum nach dem Zeitstempel erfasst wurden. Der Zeitstempel ist der Zeitpunkt, zu dem das Ereignis aufgetreten ist, das die Warnung generiert hat. Wenn Sie Standard auswählen, fordert die Endpoint Security-Appliance Informationen vom Host für alle Daten rund um ein Ereignis an.

Wenn ein Anwender von Endpunktsicherheit eine Selektierungssammlung basierend auf einem bestimmten Datum und einer bestimmten Uhrzeit anfordert, gibt der Service Desk-Mitarbeiter Informationen für ein bestimmtes Zeitfenster vor und nach der Warnung zurück. Die Zeitstempeleinstellungen steuern die Länge des Fensters für die Selektierungssammlung. Zeitstempeleinstellungen gelten nur für Service Desk-Mitarbeiter-URL-Ereignisse (URL-Überwachungsereignisse) und Registrierungsschlüssel-Ereignisse (Registrierungsschlüssel-Ereignisse).

Sie können die Registerkarte Zeitstempeleinstellungen verwenden, um die Dauer vor und nach dem Zeitstempel anzugeben, während der Informationen erfasst werden. Zeitstempeleinstellungen können zwischen 0 und 86400 Sekunden liegen. Der Standardwert für beide Einstellungen ist 600 Sekunden.

Sie können die Registerkarte Zeitstempeleinstellungen auf der Seite „Einstellungen für automatische Selektierung“ verwenden, um die Dauer vor und nach dem Zeitstempel anzugeben, während der Informationen erfasst werden. Der Zeitstempel ist die Zeit, zu der das Ereignis aufgetreten ist, das die Warnung ausgelöst hat.

Prozedur

1. Navigieren zu **Web-UI für Endpunktsicherheit**an.
2. Auswahlvorgang **Administrator** > **Selektierungseinstellungen**an.
3. Klicken **Zeitstempeleinstellungen** Registerkarte im **Einstellungen Für Automatische Selektierung** Seite.
4. Geben Sie die Dauer vor und nach dem Zeitstempel an, für den die Informationen benötigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Geben Sie die Anzahl der Sekunden vor dem angegebenen Zeitstempel ein, für die die Informationen benötigt werden.
6. Geben Sie die Anzahl der Sekunden nach dem Zeitstempel ein, für die die Informationen benötigt werden.
7. Klicken **Speichern**an.

Hinweis:
Sie können alle Werte auf der Seite auf die Standardeinstellungen zurücksetzen, indem Sie auf klicken **Auf Standardwerte zurücksetzen**, Und klicken Sie auf Speichern.

- **Beschaffungsbereich**: Auf der Seite „Übernahmen“ wird angezeigt, wie viel Speicherplatz für Übernahmen verbleibt.
- **Festlegen der Datenträgerauslastungsgrenzen für Akquisitionen:**
  - Selektierungen, Dateiakquisitionen und Datenakquisitionen können sich im Laufe der Zeit ansammeln und eine zunehmende Menge an Speicherplatz belegen. Um dies zu steuern, können Sie eine bestimmte Menge an Speicherplatz für sie zuweisen. Zehn Prozent des von Ihnen angegebenen Datenträgerspeichers sind für automatische Selektierungsakquisitionen reserviert. Wenn der insgesamt zugeteilte Beschaffungsraum überschritten wird, werden die ältesten automatischen Selektierungen gelöscht.
  - Wenn die gesamte Datenträgergröße abgeschlossener Akquisitionen einen angegebenen Grenzwert überschreitet, löscht die Endpoint Security-Appliance die ältesten abgeschlossenen Akquisitionen, bis genügend Speicherplatz gelöscht ist, um die Gesamtzahl unter den angegebenen Grenzwert zu bringen. Akquisitionen, die noch nicht abgeschlossen sind, sind nicht betroffen.
  - Die Endpoint Security-Appliance löscht automatisch Akquisitionen, wenn ein Administrator, Analyst oder Prüfarzt die Endpoint Security Web-UI verwendet, um den zugehörigen Service Desk-Mitarbeiter manuell zu löschen.

  So legen Sie Datenträgerauslastungsgrenzen für vollständige Akquisitionen über die Web-UI fest:
- Navigieren Sie zu **Web-UI für Endpunktsicherheit** .
- Auswahlvorgang **Grenzwerte Für Datenträgerauslastung** Von **Administrator** Menü.
- In **Bereichsbeschränkung für Beschaffung** Bereich: Geben Sie den maximalen Speicherplatz (in GB) an, der zum Speichern von Selektierung, Datei- und Datenerfassungen verwendet werden kann. Gültige Werte und Standardwerte variieren je nach Endpoint Security-Appliance-Modell. Die für Ihr Modell geeigneten Werte werden auf der Seite Datenträgerauslastungslimits angezeigt.
- Klicken **Speichern**an.

Hinweis:
Alle genannten Einstellungen werden eingehalten, und im Falle von Fehlern oder Fehlern ServiceNow AI Platform Gibt nur diese Fehler zurück.

Installieren Sie die Anwendung, und konfigurieren Sie eine Quelle für die Integration

Installieren und konfigurieren Sie die Anwendung aus dem ServiceNow Store auf Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen
Erforderliche Rolle: NowPlatform-Administrator (admin)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

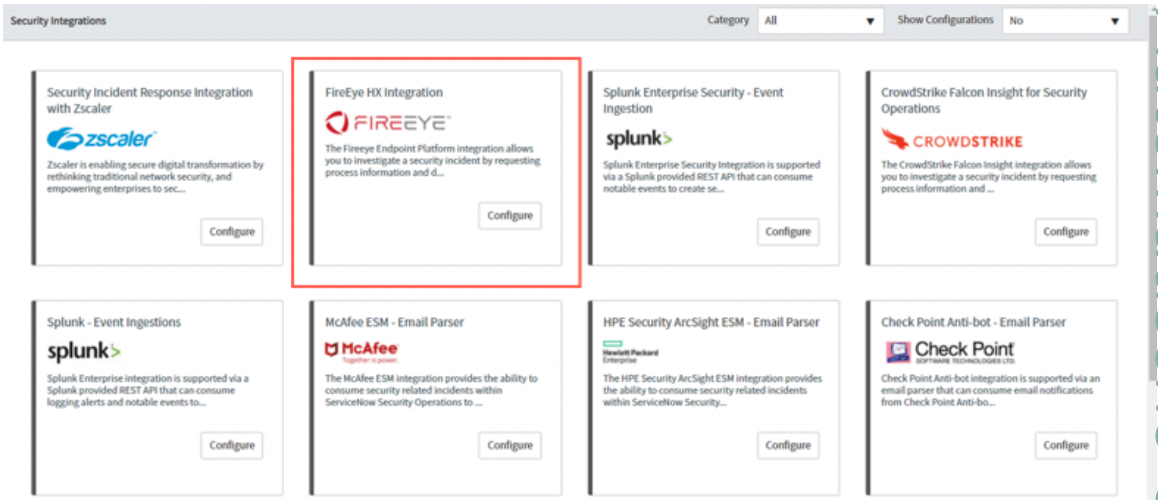
Hinweis:
Ein aktiver MID-Server ist zum Konfigurieren einer Quelle obligatorisch.

Laden Sie die Integration von Security Incident Response mit herunter FireEye HX Anwendung aus dem ServiceNow Store und installieren.

Nachdem Sie die Anwendung erfolgreich installiert haben, führen Sie die folgenden Schritte aus, um sie zu konfigurieren:

Prozedur

1. Navigieren zu **Integrationen** > **Integrationskonfigurationen**an.
2. Rufen Sie die Eigenschaft **Integrationskonfigurationen** Modul zum Anzeigen der verfügbaren Integrationen und zum Auffinden von **FireEye** Kachel.



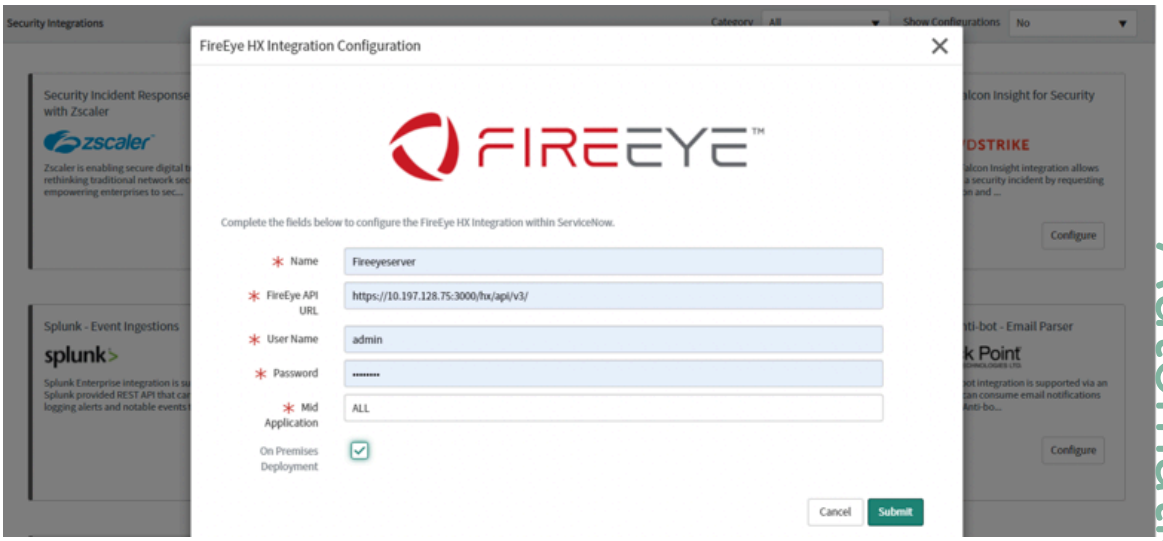
3. Klicken **Konfigurieren** Auf der FireEye-Kachel.
4. Geben Sie die folgenden Details an, um die FireEye-Integration einzurichten:

Feld	Beschreibung
Name	Name der FireEye-Konfiguration. Dieser Name wird verwendet, um die Quelle und die zugehörigen Anmeldeinformationen und Konfigurationen zu identifizieren. Dieser Name hilft Ihnen, die Anmeldeinformationen und Accounts zu unterscheiden und jede Quelle zu identifizieren, um Konflikte mit Profilen zu vermeiden.
API-URL	Basis-URL, die die FireEye-API hostet.
Anwendername	Geben Sie den Anwendernamen des FireEye-Accounts ein.
Passwort	Geben Sie das Passwort des FireEye-Accounts ein.
MID-Anwendung	MID-Anwendung, die in Ihrer Umgebung eingerichtet ist. Mid-Server ist erforderlich, um ZIP-Dateien für einige der Ergänzungsfunktionen zu verarbeiten. Standardmäßig ist es

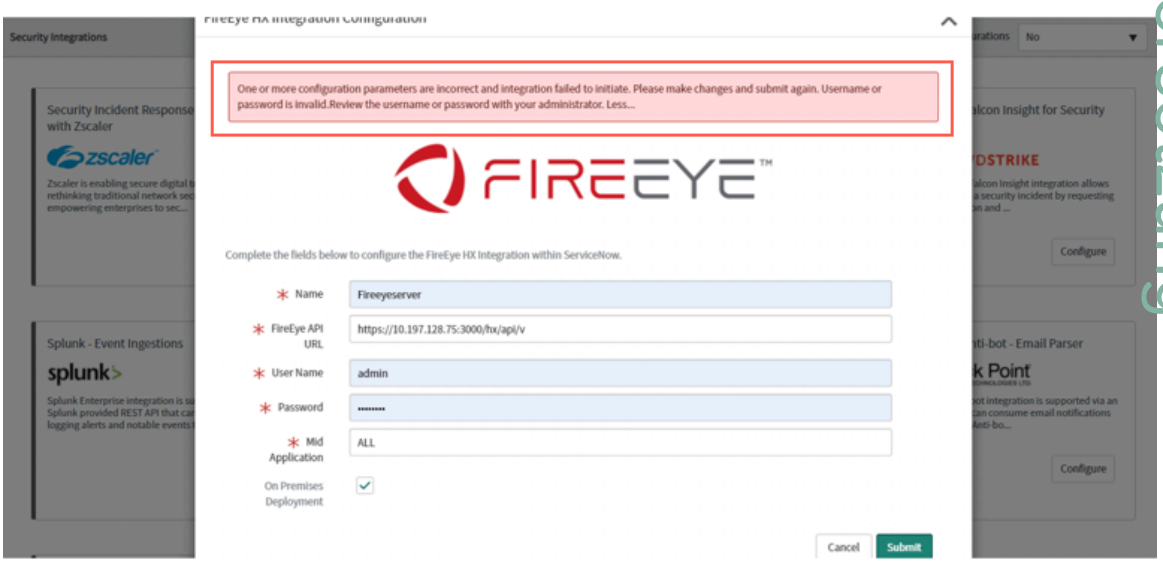
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	„ALLE“. Anwender müssen einen gültigen Anwendungsnamen manuell angeben.
Lokale Bereitstellung	Standard ist deaktiviert. Wenn Sie die cloudbasierte Version von FireEye verwenden, überprüfen Sie, ob das Kontrollkästchen deaktiviert ist.



5. Klicken **Absenden**an.
   Die Liste FireEye-Konfigurationen wird mit Ihrem neuen Konfigurationsdatensatz angezeigt. Sie haben die Konfiguration für einen FireEye-Server abgeschlossen. Wenn Sie keine Verbindung mit FireEye herstellen können oder Ihre Anmeldeinformationen falsch sind, wird eine Validierungsfehlermeldung angezeigt, wie in der folgenden Abbildung dargestellt. Überprüfen Sie, ob Ihre Anmeldeinformationen korrekt sind, und versuchen Sie es erneut.



FireEye: Standardeinstellungen

Im Folgenden finden Sie die zusätzlichen Konfigurationseinstellungen, nachdem Sie die Installation abgeschlossen haben.

Automatische Übersetzung

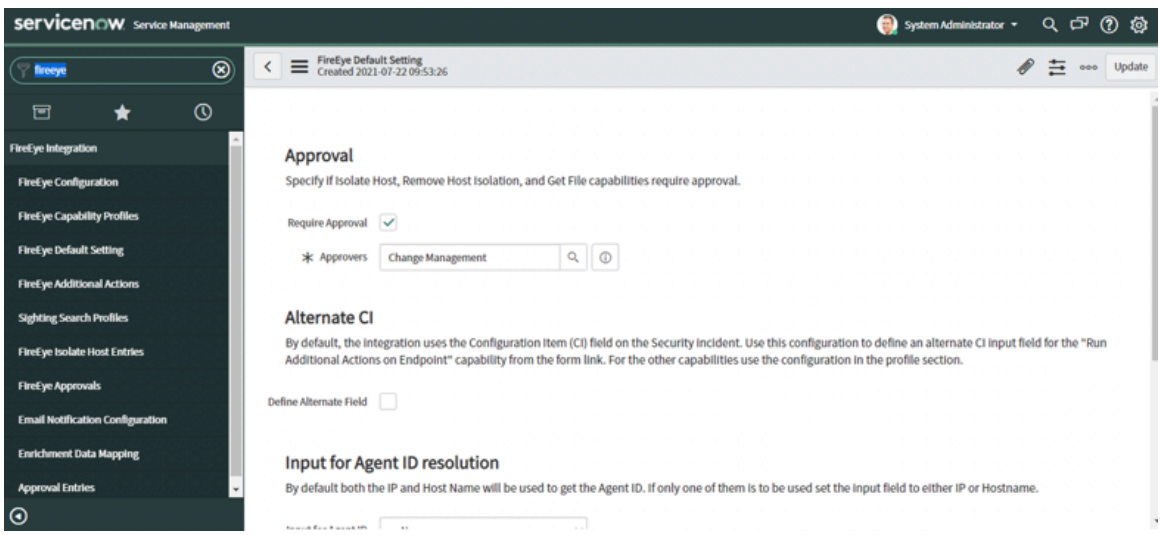
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sobald Sie die Installation abgeschlossen haben, finden Sie in der linken Navigation das Modul „FireEye-Standardeinstellungen“. Enthält Standardeinstellungen für verschiedene FireEye-Funktionen.

Zusätzliche Konfigurationen

Im Folgenden finden Sie die zusätzlichen Konfigurationseinstellungen:

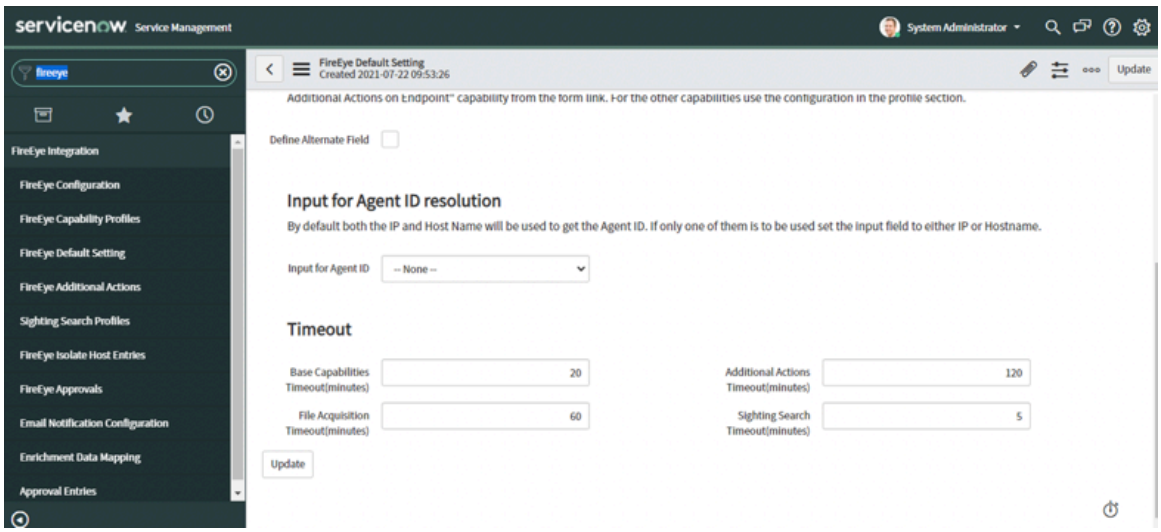
1. **Freigabe**: Diese Genehmigung gilt speziell für die Funktionen „Host isolieren“, „Host-Isolierung entfernen“ und „Datei abrufen“, wenn sie direkt über die zugehörige Liste ausgelöst werden und wenn keine Profile dafür vorhanden sind. Wenn für diese Fähigkeiten/(ein) Profil(e) vorhanden ist(sind), wird die Genehmigungskonfiguration im Profil berücksichtigt.
   - **Genehmigung Erforderlich:** Wenn Sie Genehmigung erforderlich aktivieren, ist das Feld Genehmiger im Formular verfügbar.
   - **Verantwortliche Vertragsgenehmigung**: Liste der Genehmigergruppen. Nachdem Sie eine Anforderung übermittelt haben, ist die Genehmigung der Gruppe erforderlich, um die Anforderung abzuschließen.
2. **Alternatives CI**: Durch Aktivieren dieses Kontrollkästchens wird eine Liste der Felder bereitgestellt, die für die Übergabe eines alternativen CI an die Fähigkeit verfügbar sind. Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Diese Konfiguration gilt nur für die Fähigkeit „zusätzliche Aktionen für Endpunkt ausführen“. Verwenden Sie daher diese Konfiguration, um ein alternatives CI-Eingabefeld nur für die Fähigkeit „zusätzliche Aktionen für Endpunkt ausführen“ zu definieren. Für die anderen Fähigkeiten verwenden Sie die Konfiguration im Profilabschnitt. Wenn die Profile kein alternatives CI definieren, wählen die Fähigkeiten das CI-Feld aus dem Security Incident-Formular aus.
3. **Eingabe für Lösung der Service Desk-Mitarbeiter-ID**: Standardmäßig werden IP und Hostname zum Abrufen der Agent-ID verwendet. Wenn nur eine davon verwendet werden soll, legen Sie das Eingabefeld entweder auf IP oder Hostname fest.



4. **Zeitüberschreitung**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Zeitüberschreitung bei Basisfähigkeiten (Minuten):** Die Funktionen Anreicherung, Host isolieren und Host-Isolierung entfernen schlagen fehl, wenn innerhalb der festgelegten Zeit keine Antwort gerendert wird.
- **Zeitüberschreitung bei zusätzlicher Aktion (Minuten):** Die Fähigkeit „zusätzliche Aktionen für Endpunkt ausführen“ schlägt fehl, wenn innerhalb der festgelegten Zeit keine Antwort gerendert wird.
- **Zeitüberschreitung bei Dateiakquisition (Minuten):** Die Funktion „Datei abrufen“ schlägt fehl, wenn innerhalb der festgelegten Zeit keine Antwort gerendert wird.
- **Zeitüberschreitung bei Sichtungssuche (Minuten):** Die Suche wird nach der festgelegten Zeit beendet.



Erstellen Sie ein Fähigkeitsprofil für die FireEye-Endpunktintegration

Erstellen Sie ein Profil, und wählen Sie aus FireEye HX Fähigkeiten, die das Profil ausführen soll.

Vorbereitungen

Erforderliche Rolle: NowPlatform Security Incident-Administrator (sn_si.admin)

Warum und wann dieser Vorgang ausgeführt wird

Profile werden erstellt, um Fähigkeiten miteinander zu vereinigen, und würden Analysten helfen, die Untersuchung/Korrektur einfach durchzuführen.

Im Folgenden finden Sie die Liste der Fähigkeiten, die Sie Profil(en) hinzufügen können:

1. Hostdetails abrufen
2. Angemeldete Anwender abrufen
3. Netzwerkstatistiken abrufen
4. Laufende Prozesse abrufen
5. Laufende Services abrufen
6. Datei abrufen
7. Host isolieren
8. Isolation entfernen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die Funktionen „Datei abrufen“, „Host isolieren“ und „Host-Isolation entfernen“ beim Erstellen eines Profils nicht mit anderen Funktionen kombinieren. Profile für diese müssen einzeln erstellt werden. Andererseits können Systemdetails abrufen, angemeldete Anwender abrufen, Netzwerkstatistiken abrufen, laufende Prozesse abrufen und laufende Services abrufen zusammengefasst werden. Sie können Profile einzeln erstellen oder sie je nach Bedarf vollständig oder teilweise zusammenfassen. Sobald eine Fähigkeit in einem Profil enthalten ist, kann sie nicht in ein anderes Profil aufgenommen werden.

Führen Sie die folgenden Schritte aus, um ein neues Fähigkeitsprofil zu erstellen:

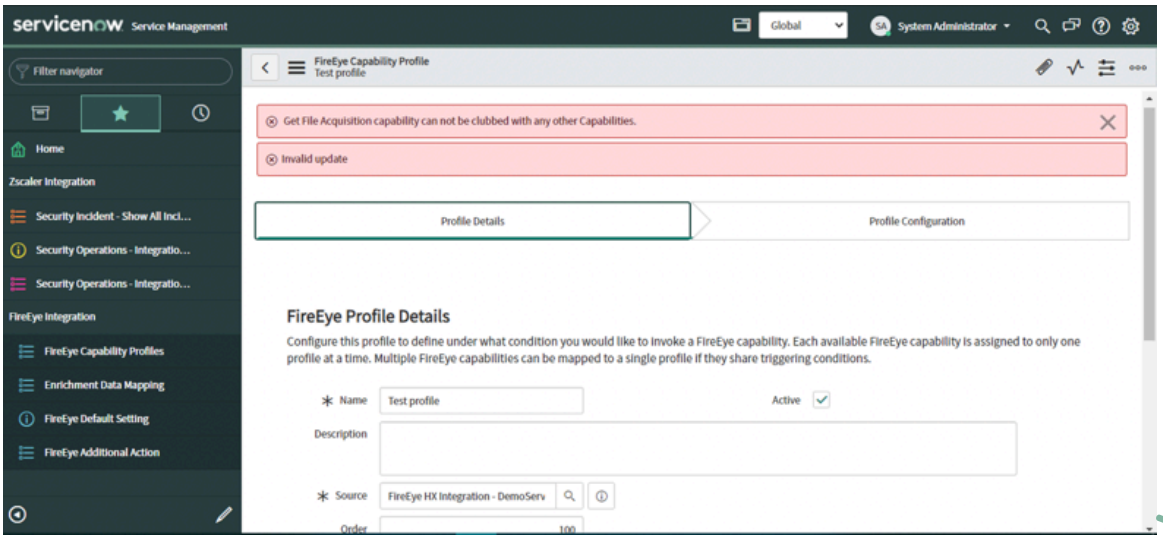
Prozedur

1. Navigieren zu **FireEye-Integration** > **FireEye-Funktionalitätsprofile**an.
   Die Liste der Fähigkeitsprofile wird angezeigt.
2. Klicken **Neu**an.
3. Füllen Sie die Felder im Formular aus.

Name	Name für FireEye HX Fähigkeitsprofil. Dieser Name hilft Ihnen, den Profiltyp zu identifizieren und zu beschreiben.
Beschreibung	Zusätzliche Informationen zum Profil, die das Profil weiter beschreiben.
Quelle	Name des FireEye HX Quelle. In der Auswahlliste sind nur konfigurierte Quellen verfügbar.
FireEye HX-Fähigkeiten	Fähigkeiten von FireEye HX Profil. Wählen Sie die für dieses Profil gewünschten Fähigkeiten aus der Spalte verfügbar aus, und verschieben Sie sie in die Spalte ausgewählt.
Reihenfolge	Flow-Priorität. Der Standardwert ist 100. Der Wert dieses Felds gibt die Reihenfolge an, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen teilen. Der Flow mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Beispiel: 100, 200, 300, 400.
Aktiv	Dies gibt an, dass das Profil aktiv ist. Wenn das Profil aktiv ist, wird es automatisch ausgelöst, wenn ein Security Incident erstellt wird, der den Filterbedingungen entspricht, die Sie in der Konfiguration angegeben haben.

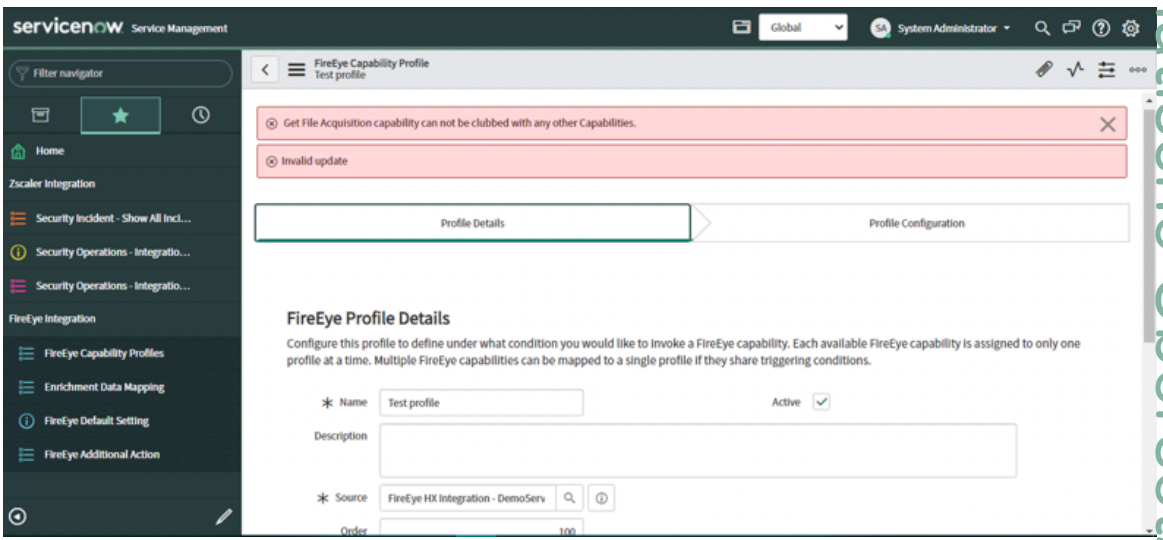
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für Profildetails mit der Fähigkeit „Hostdetails abrufen“.

4. Klicken **Weiter** Um mit der Profilkonfiguration fortzufahren.



Hinweis:
Die Funktionen „Host isolieren“, „Host-Isolierung entfernen“ und „Datei abrufen“ können nicht mit anderen Fähigkeiten kombiniert werden.

Nächste Maßnahme

Der nächste Schritt besteht darin, Ihr Profil zu konfigurieren. Bevor Sie die Einstellungen für das Profil konfigurieren, sollten Sie die Konzepte für die Konfiguration von Profilen und Auslösebedingungen überprüfen. Weitere Informationen finden Sie unter Verstehen, wie Auslöserbedingungen mit einem Konfigurationselement für ein Profil funktionieren.

Verstehen Sie, wie Auslöserbedingungen mit einem Konfigurationselement funktionieren

Nachdem Sie ein Profil erstellt und die FireEye-Fähigkeiten ausgewählt haben, die das Profil ausführen soll, konfigurieren Sie die Profileinstellungen so, dass es nur ausgeführt wird, wenn eine Reihe bestimmter Bedingungen erfüllt sind.

Sie können Auslöserbedingungen festlegen, damit das Profil automatisch ausgeführt wird, wenn ein Security Incident erstellt wird, der der Auslöserbedingung entspricht. Wenn die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

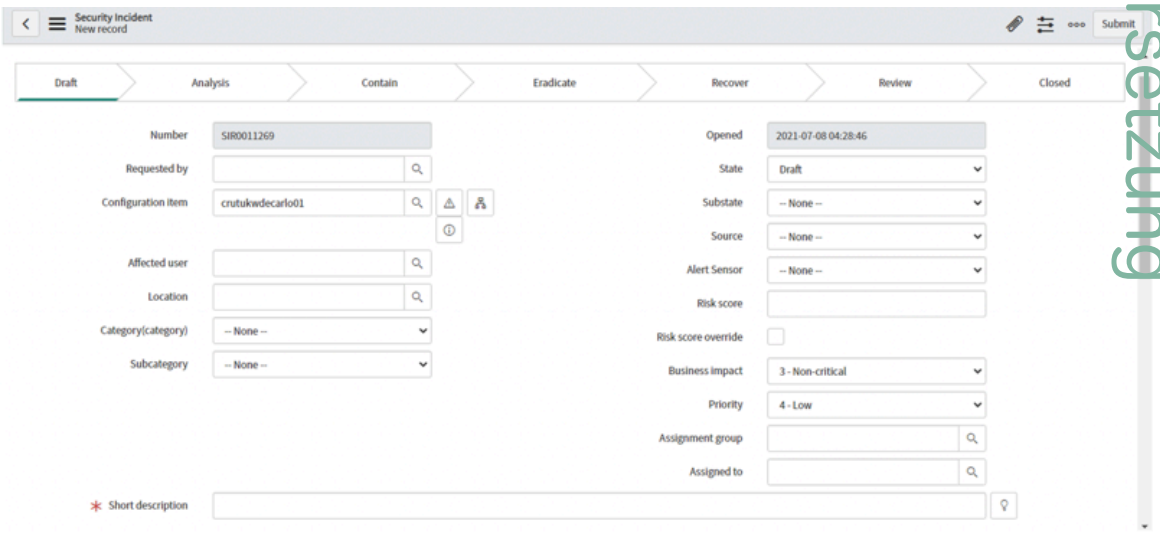
Auslöserbedingung nicht festgelegt ist, können diese Profile manuell ausgeführt werden, indem Sie im Security Incident auf das Formular „EDR-Profil(e) ausführen“ klicken und das Profil auswählen.

Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Dieser Wert wird verwendet, um die IDs Ihrer Assets mit den in der Now Platform CMDB gespeicherten Informationen abzugleichen. Wenn ein Security Incident erstellt wird und ein Profil entweder automatisch oder manuell ausgeführt wird, wird die CMDB durchsucht, um den Hostnamen und/oder die IP-Adresse basierend auf dem Wert des CI-Felds abzurufen. Der Hostname und oder die IP-Adresse werden verwendet, um die Agent-ID in aufzulösen FireEye HX Um den Endpunkt zu identifizieren.

Im Idealfall wird ein übereinstimmender Wert in der Datenbank gefunden, und Daten werden aus gesammelt FireEye HX Konsole für das übereinstimmende Asset. Die Daten für verschiedene Fähigkeiten werden in abgerufen ServiceNow AI Platform Instanz und wird in den zugehörigen Listen eines Security Incidents angezeigt. Wenn das Feld Konfigurationselement (CI) im Security Incident nicht mit einem Hostnamen oder einer IP-Adresse ausgefüllt ist, die der Datenbank entspricht, können Sie ein alternatives Feld im Security Incident auswählen, das entweder den Hostnamen oder die IP-Adresse enthält, um die Lösung der Agent-ID durchzuführen.

Während des Konfigurationsschritts des Profils können Sie ein alternatives CI-Feld für die Endpunktidentifizierung auswählen, um sicherzustellen, dass Sie den Endpunkt identifizieren können FireEye HX. Sie können jedes Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich anwenderdefinierter Felder, die Sie erstellen. Indem Sie dieses alternative CI-Feld als Sicherung auswählen, stellen Sie sicher, dass Ihre Profile auch dann ausgeführt werden, wenn das CI-Feld bei der Incident-Erstellung nicht für den zugehörigen Security Incident ausgefüllt ist.

Hinweis:
Die alternativen CI-Felder werden nur für Fähigkeiten berücksichtigt, die einem Profil hinzugefügt werden können. Für alle zusätzlichen Aktionen wird das alternative CI auf der Seite mit den Standardeinstellungen ausgewählt.



Konfigurieren Sie Profile und Security Incidents für FireEye HX Integration

Nachdem Sie ein Profil erstellt und ausgewählt haben FireEye HX Fähigkeiten, die das Profil ausführen soll, konfigurieren Sie die Einstellungen so, dass das Profil nur unter den definierten Bedingungen aufgerufen werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Konfigurieren Sie das Profil so, dass es nur ausgeführt wird, wenn die von Ihnen angegebenen Bedingungen erfüllt sind. Wählen Sie bei Bedarf ein alternatives Eingabefeld für das Feld Configuration Item (CI) aus, und legen Sie Filterbedingungen fest, damit das Profil automatisch ausgelöst werden kann, wenn ein Security Incident erstellt wird, der die Auslöserbedingungen erfüllt.

Hinweis:
Sie können zu folgendem Ort navigieren: **Profilkonfiguration** Seite erst nach Eingabe von **Profildetails**an.

Prozedur

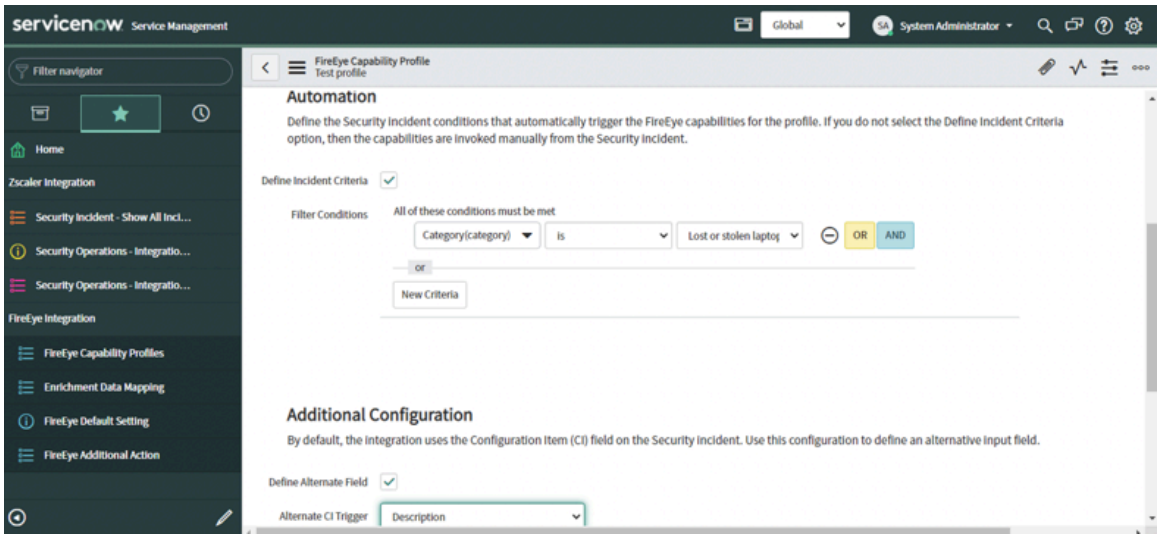
1. Navigieren zu **FireEye-Integration** > **FireEye-Funktionalitätsprofile**an.
2. Klicken **Weiter** Auf der **Profildetails** Seite nach Abschluss des Abschnitts „Profildetails“.
3. Überprüfen und konfigurieren Sie die folgenden Abschnitte:
   - **Incident-Kriterien Definieren (Automatisierung)**: Definieren Sie die Security Incident-Bedingungen, die automatisch ausgelöst werden FireEye HX Fähigkeiten für das Profil. Wenn Sie nicht auswählen **Definiert Incident-Kriterien** Option, dann können das Profil und die zugrunde liegenden Fähigkeiten manuell über den Security Incident aufgerufen werden.
     - Auswahlvorgang **Definiert Incident-Kriterien** Option zum automatischen Auslösen FireEye HX Fähigkeiten im Profil.
     - In **Filterbedingungen**, Wählen Sie das erforderliche Feld aus.
     - Sie können hinzufügen **Neues Kriterium** Und definieren Sie auch die ODER oder die UND-Bedingung.

       Hinweis:
       „Host isolieren“, „Host-Isolierung entfernen“, „Datei abrufen“ kann nicht automatisch ausgelöst werden.

   - **Zusätzliche Konfiguration**: Wenn das Feld Configuration Item (CI) im Security Incident nicht mit einem Hostnamen oder einer IP-Adresse ausgefüllt ist, die der Datenbank entspricht, können Sie ein alternatives Feld im Security Incident auswählen, um abzufragen FireEye HX APIs.
     - Rufen Sie die Eigenschaft **Definieren Sie Ein Alternatives Feld** Option zum Definieren eines alternativen Eingabefelds.
     - Wählen Sie das Eingabefeld aus dem aus **Alternatives CI-Auslöserfeld**an.

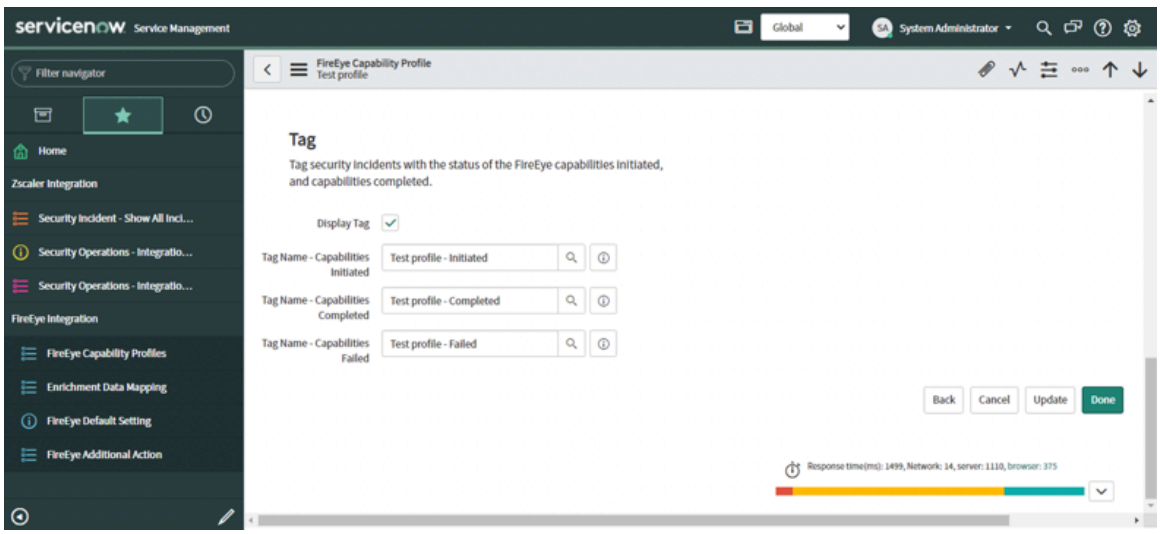
       Hinweis:
       Weitere Informationen finden Sie unter Verstehen Sie, wie Auslöserbedingungen mit einem Konfigurationselement funktionieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- **Tags**: Sie können Security Incidents optional mit dem taggen FireEye HX Tags „Profil initiiert“, „Profil abgeschlossen“ und „Profil fehlgeschlagen“.

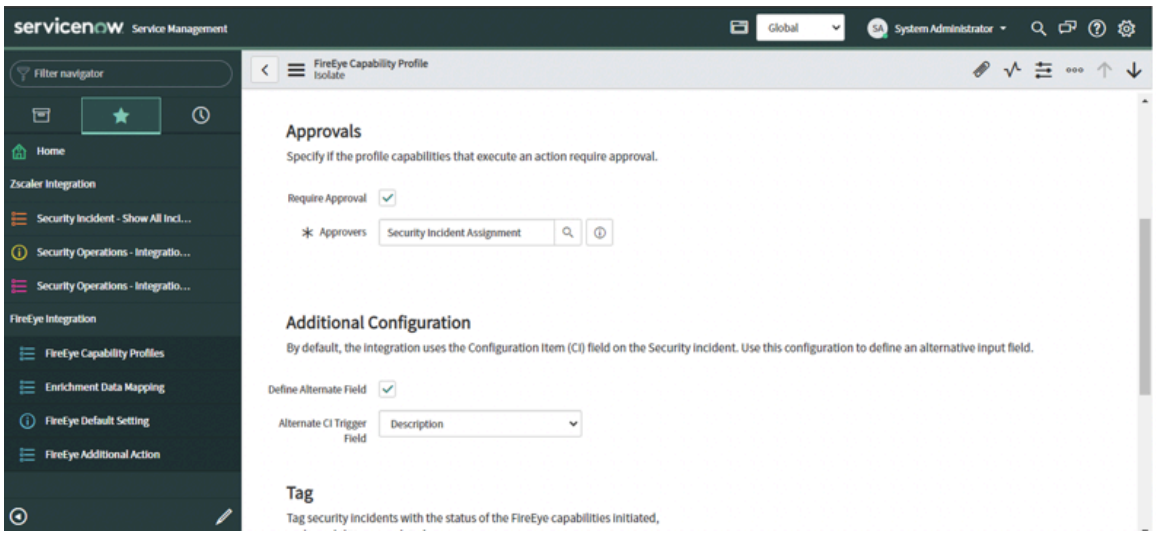
  Rufen Sie die Eigenschaft **Tag anzeigen** Kontrollkästchen zum Aktivieren der Kennzeichnung von Security Incidents. Der Profilname wird beim Aktivieren des Tags vorangestellt. Standardmäßig ist diese Option für alle Profile deaktiviert.



- **Genehmigungen**: Wählen Sie aus **Genehmigung erforderlich** Kontrollkästchen, um bei Verwendung von eine zusätzliche Steuerungsstufe bereitzustellen FireEye HX Fähigkeiten zum Isolieren von Hostcomputern, zum Wiederherstellen im Netzwerk und zum Abrufen der Dateien.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Option Genehmigungen in der Profilkonfiguration wird nur für die Funktionen Host isolieren, Host-Isolierung entfernen und Datei abrufen angezeigt.



4. Klicken Sie auf **Erledigt**.
5. Verifizieren FireEye HX Auslöserbedingungen.

Überprüfen Sie die Auslöserbedingungsfilter

Testen Sie das Profil, und stellen Sie sicher, dass die von Ihnen konfigurierten Auslöserbedingungsfilter wie erwartet funktionieren.

Vorbereitungen
Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

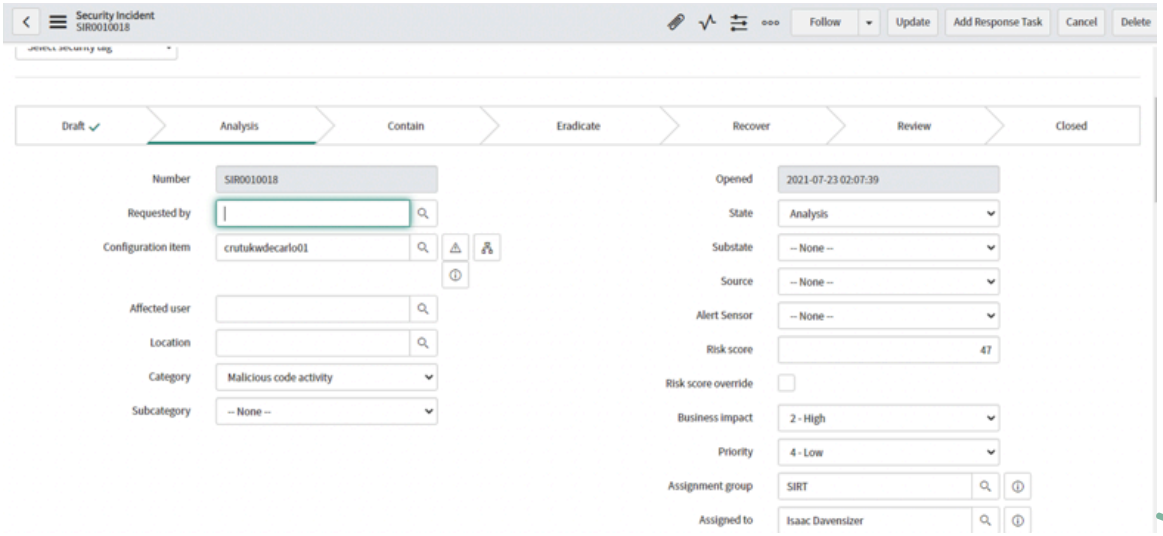
Sobald Sie das Profil aktiviert haben, können Sie basierend auf den konfigurierten Auslöserbedingungen die Abfrageergebnisse in anzeigen ServiceNow AI Platform Security Incidents.

Prozedur

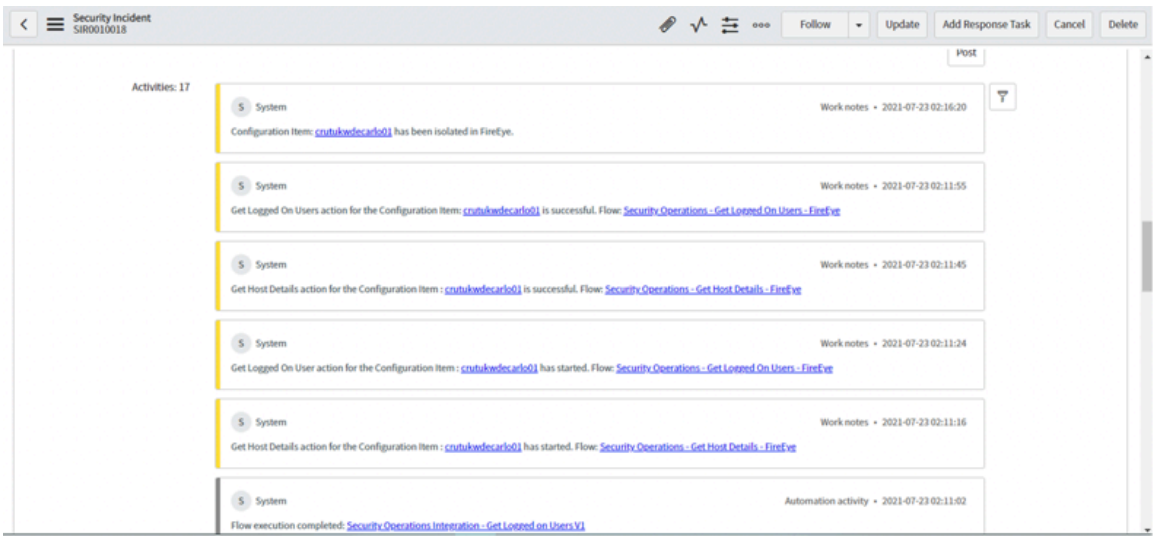
1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Auswahlvorgang **Neu** Um einen neuen Security Incident zu erstellen.
3. Geben Sie die Filterbedingungen wie im Fähigkeitsprofil angegeben an, um das jeweilige Profil auszulösen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken **Speichern**an.



5. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.

6. Zeigen Sie die Tags „Profil initiiert“, „Profil abgeschlossen“ oder „Profil fehlgeschlagen“ an.

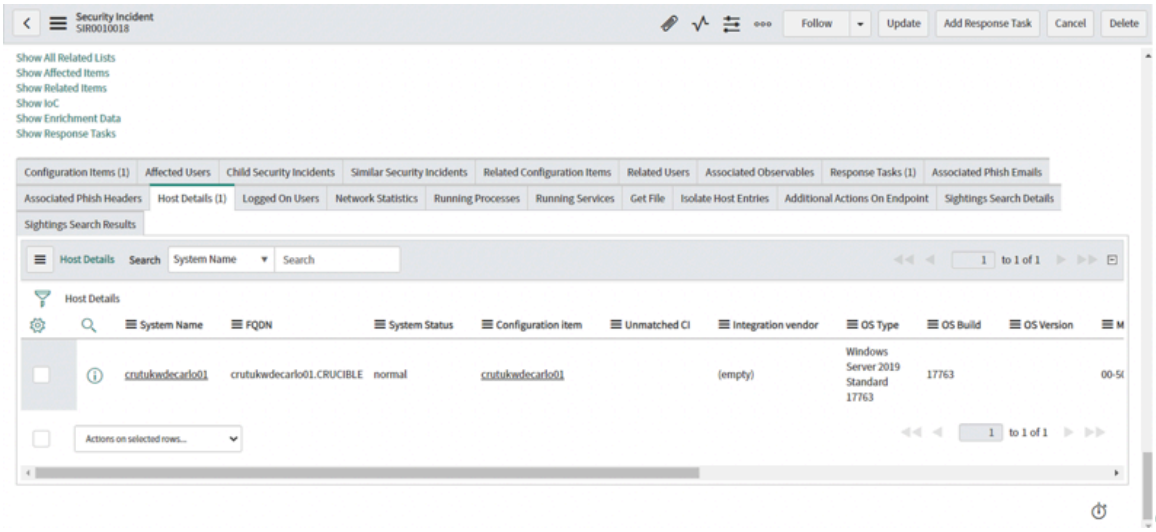
7. Klicken **Alle zugehörigen Listen anzeigen**an.

8. Klicken Sie auf eine zugehörige Liste (Registerkarte).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Hostdetails.



Löst ein FireEye-Fähigkeitsprofil über zugehörige Links aus

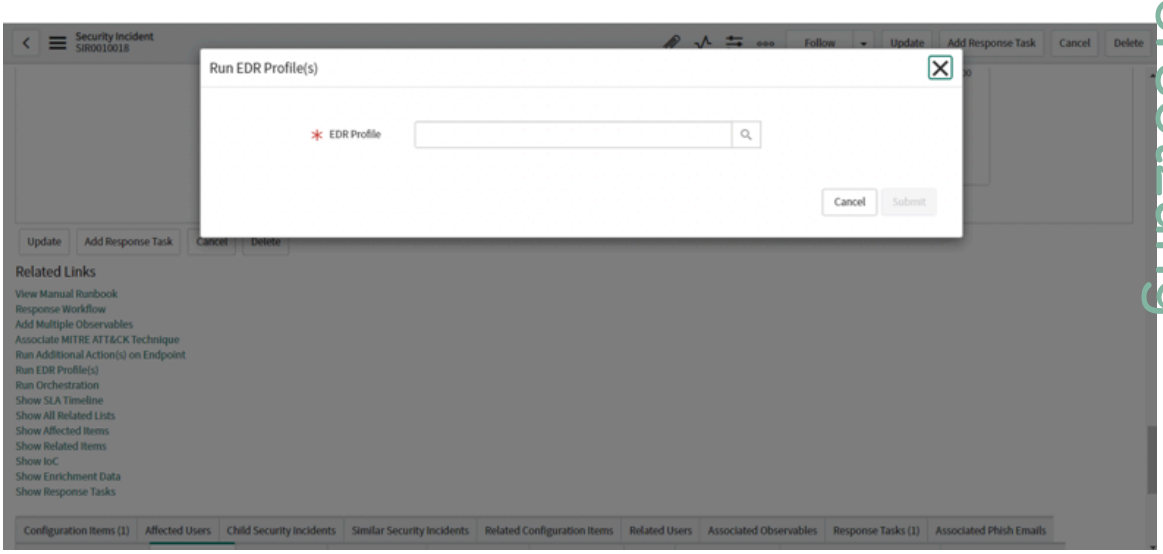
Lösen Sie ein Fähigkeitsprofil manuell aus, nachdem Sie einen Security Incident über zugehörige Links überprüft haben.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

Prozedur

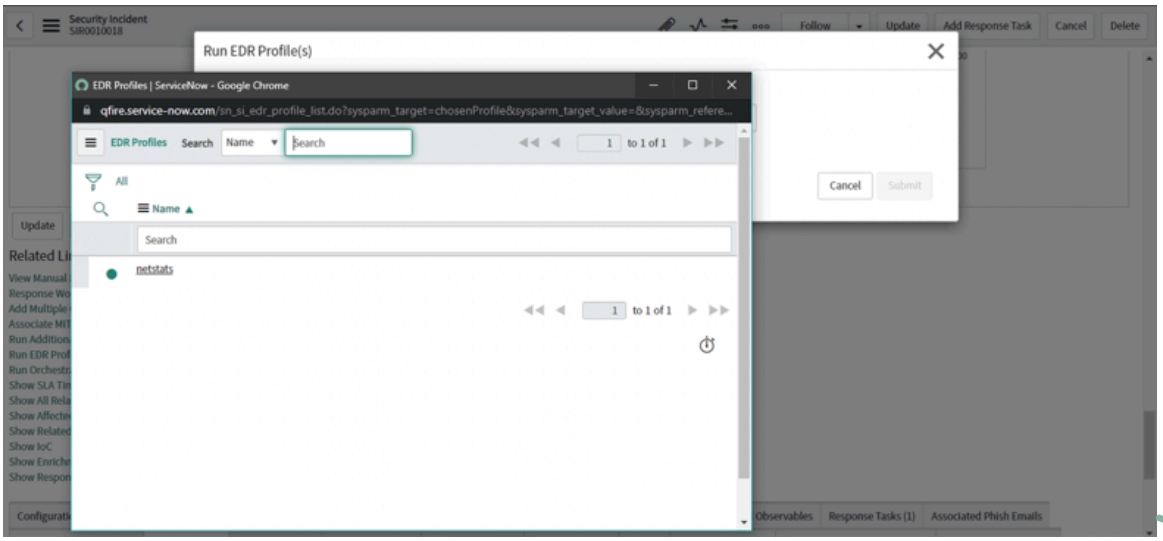
1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie überprüfen möchten.
3. Klicken **EDR-Profil(e) ausführen**Im Abschnitt „zugehörige Links“.

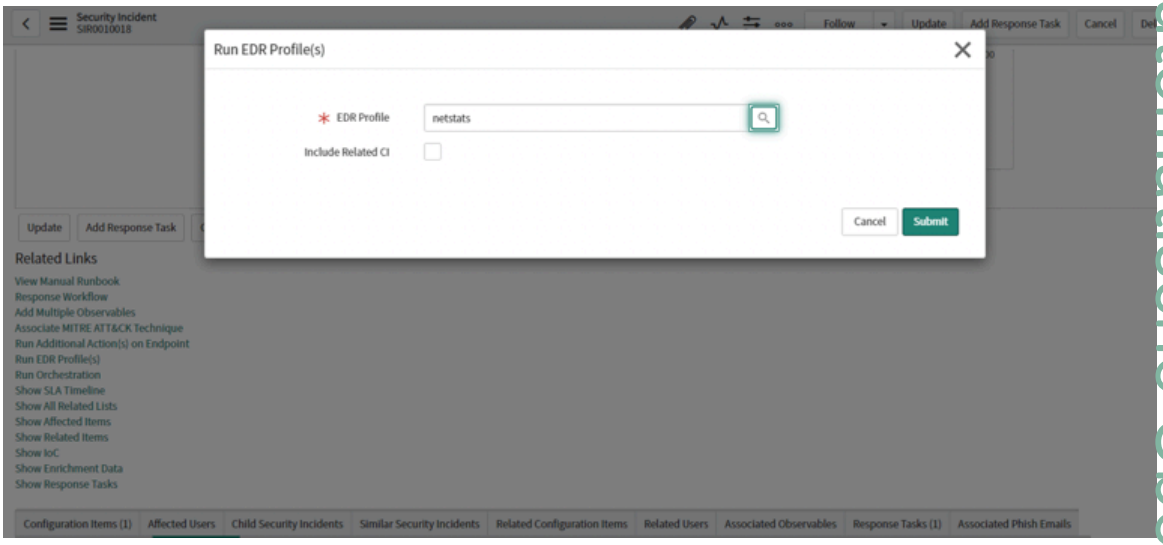


4. Durchsuchen Sie ein Profil, wählen Sie es aus der Liste der verfügbaren Profile aus, und klicken Sie auf **Absenden**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.





5. Das ausgewählte Profil wird manuell ausgelöst.
6. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
7. Zeigen Sie die Tags an, und überprüfen Sie die zugehörigen Listen auf die Daten.

Hinweis:
Zusätzlich zum Ausführen des Profils für das CI oder das alternative CI des Security Incident können Sie das Profil auch für CI-Werte ausführen, die in der zugehörigen Liste „Konfigurationselement“ vorhanden sind, indem Sie im Dialogfeld „Zugehöriges CI einschließen“ aktivieren. Dadurch werden auch Daten für die CI-Werte abgerufen, die in der zugehörigen Liste vorhanden sind. Alternativ können Sie das Profil nur für die in der zugehörigen Liste vorhandenen CI-Werte ausführen.

Löst ein FireEye-Fähigkeitsprofil aus der zugehörigen Liste „Konfigurationselement“ aus

Lösen Sie ein Fähigkeitsprofil manuell aus der zugehörigen Liste des Konfigurationselements aus.

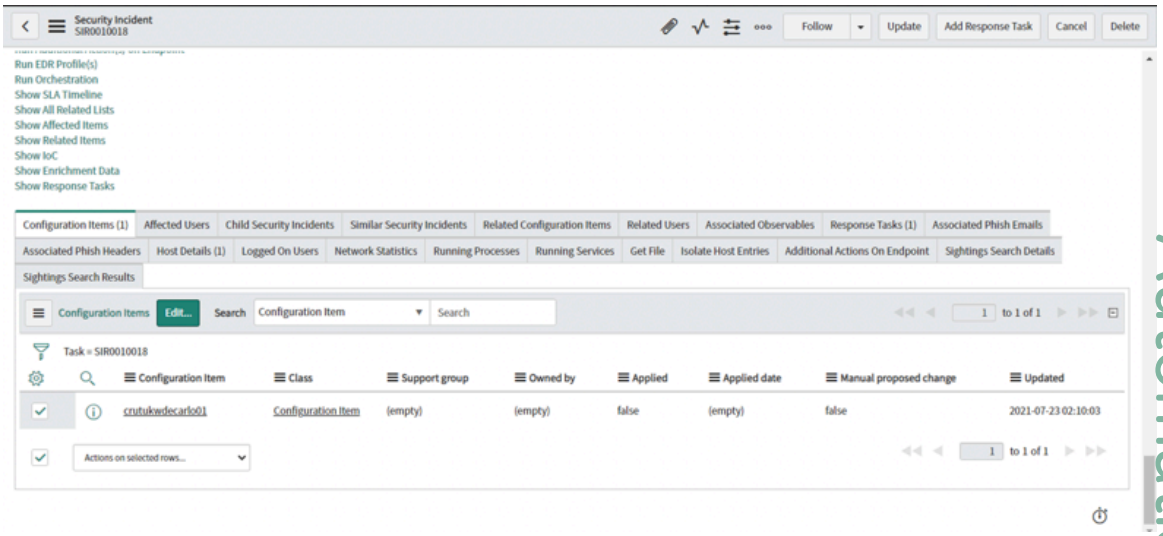
Vorbereitungen
Erforderliche Rolle: sn_si.admin, sn_si.Analyst

Automatische Übersetzung

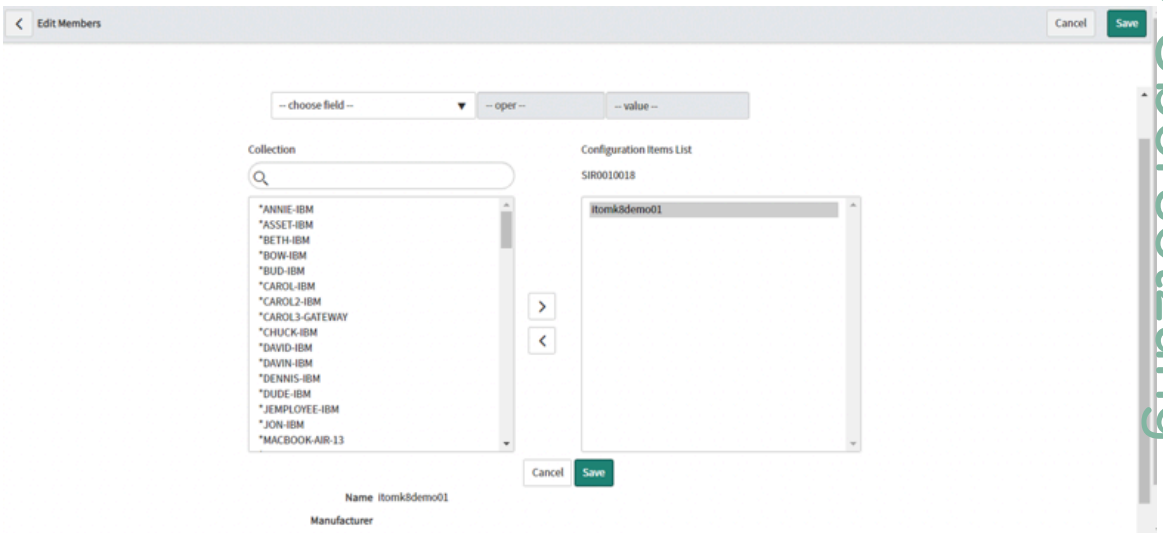
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit überprüfen möchten FireEye HX Informationen.
3. Klicken **Alle zugehörigen Listen anzeigen** Im Abschnitt zugehörige Listen.
4. Klicken Sie auf die Schaltfläche **Konfigurationselement** Zugehörige Liste.



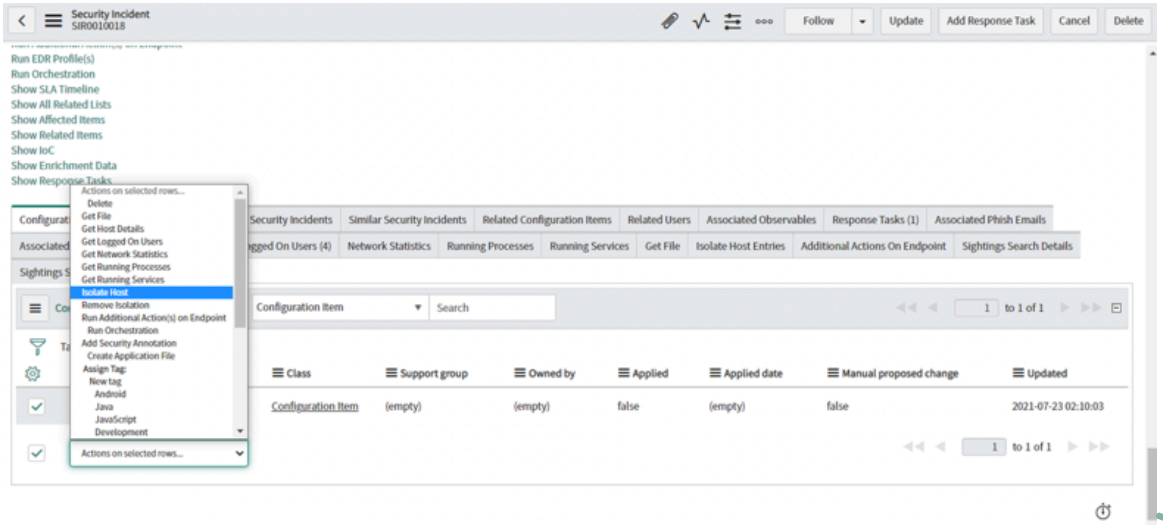
5. Klicken **Bearbeiten** Um die verfügbaren Konfigurationselemente hinzuzufügen, wenn noch keine Werte vorhanden sind, und klicken Sie auf **Speichern**an.



6. Wählen Sie die hinzugefügten Konfigurationselemente aus, und wählen Sie unter Aktionen für ausgewählte Zeilen eine Fähigkeit aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Die ausgewählte Fähigkeit wird manuell ausgelöst.

8. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.

9. Zeigen Sie die Tags an, und überprüfen Sie die Daten in den zugehörigen Listen.

FireEye – Dateifunktion abrufen

Dateibeschaffungsanforderungen weisen einen Endpoint Security Agent an, eine Datei von seinem Host-Endpunkt abzurufen. Dateierfassungen werden für die statische oder dynamische Analyse potenzieller oder verifizierter Gefährdungen sowie zur Nachweisaufbewahrung bei internen Bedrohungsuntersuchungen verwendet. Die Funktion „Datei abrufen“ muss als separates Profil erstellt werden.

Vorbereitungen

Erforderliche Rolle: Administrator

„Dateiprofil abrufen“ wird ausgelöst und erstellt FireEye HX Fähigkeitsprofil mit **Datei abrufen** Fähigkeit.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.

2. Wählen Sie den Security Incident aus, den Sie überprüfen möchten.

3. Klicken **EDR-Profil(e) ausführen**Im Abschnitt „zugehörige Links“.

4. Durchsuchen Sie die Liste der verfügbaren Profile, und wählen Sie Dateiprofil abrufen aus.

5. Geben Sie an **Dateiname** und **Dateipfad**an.

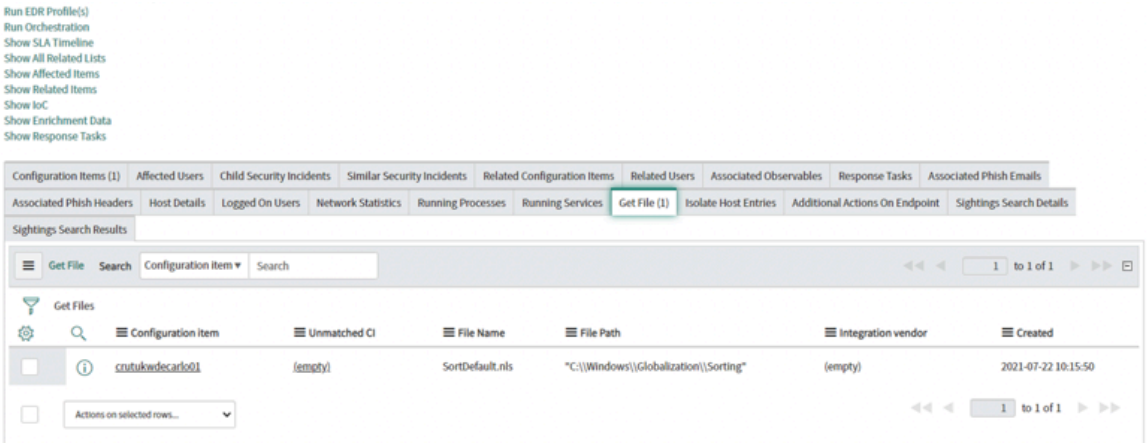
> **Hinweis:**
> Geben Sie den Namen der Datei ein, für die Sie abrufen möchten. Geben Sie einen genauen Pfadnamen oder eine andere geeignete pfadbasierte Windows-Umgebungsvariable an. Sie müssen den Laufwerksbuchstaben oder Pfadnamen angeben. Verschiedene Endpunkte können unterschiedliche Laufwerkszuordnungen haben. Wenn Sie explizit einen Ordnernamen angeben, können Sie den Pfad mit einem umgekehrten Schrägstrich beenden. Der endgültige umgekehrte Schrägstrich ist jedoch nicht obligatorisch.

6. Klicken **Absenden**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Überprüfen Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
8. Zeigen Sie die Tags an, und überprüfen Sie die Ergebnisse in **Datei abrufen** Zugehörige Liste.

Hinweis:
Das Profil „Datei abrufen“ wird jetzt manuell ausgelöst.



So überprüfen Sie eine heruntergeladene Dateibeschaffung:

- Öffnen Sie die ZIP-Datei für die Dateibeschaffung.
- Geben Sie das zum Öffnen der Datei erforderliche Passwort ein. Das Passwort kann angezeigt werden, indem Sie den Mauszeiger über den Download-Link in bewegen FireEye HX Konsole. Führen Sie die folgenden Schritte aus, um das Passwort anzuzeigen:
  - Melden Sie sich bei der FireEye HX-Konsole an.
  - Navigieren zu **Akquisitionen** Und filtern Sie nach Beschaffungstyp – Datei.
  - Wählen Sie den gewünschten Datensatz aus.

    Hinweis:
    Sie können die Details der erworbenen Datei auf der rechten Registerkarte anzeigen.

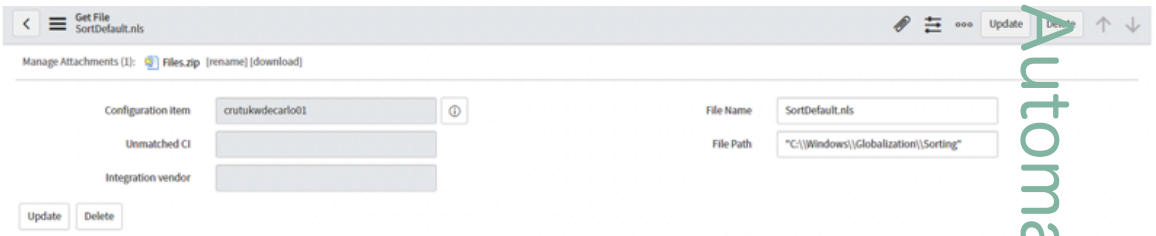
  - Bewegen Sie den Mauszeiger über den **Herunterladen** Link oben verfügbar, um das Passwort zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

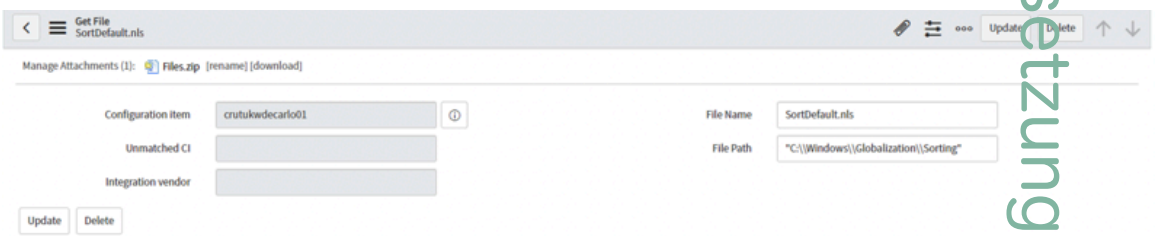
- Öffnen und überprüfen Sie die Dateien in der ZIP-Datei mit einem beliebigen Text- oder XML-Editor.

Hinweis:

- Es wird empfohlen, die abgerufene Datei manuell als erkennbares Element hinzuzufügen, damit sie als Nachweis für den Security Incident nachverfolgt werden kann. Dies hilft auch, die Dateien in Zukunft anzuzeigen, wenn das Passwort vergessen oder geändert wird.
- Die maximale Dateigröße, die für die Aktion „Datei abrufen“ unterstützt wird, beträgt 1024 MB, und dieser Wert kann durch Ändern konfiguriert werden **com.glide.attachment.max_size**, Und die Standardzeitüberschreitung beträgt 60 Minuten, die über konfiguriert werden kann FireEye HX Seite „Standardeinstellungen“.



- „Datei abrufen“ kann auch über die zugehörige Liste des Konfigurationselements ausgelöst werden.



Automatische Übersetzung

FireEye – zusätzliche Aktionen für Endpunkt

Die FireEye-Integration unterstützt die Ausführung zusätzlicher Aktionen, die über die Goldstandardaktionen hinausgehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Aktionen umfassen Selektierungsakquise und Datenakquisitionen. Standardmäßig werden zwei Datenerfassungen unterstützt:

- Umfassendes Skript Für Untersuchungsdetails
- Standardskript Für Untersuchungsdetails

Darüber hinaus wird die Selektierungsakquisition sofort unterstützt. Alle diese drei werden standardmäßig zusammen mit der Quelle erstellt. Die Kunden können auch eigene Aktionen erstellen, d. h. Datenerfassungen aus dem FireEye-Modul „zusätzliche Aktionen“.[1] die maximale Dateigröße, die für zusätzliche FireEye-Aktionen unterstützt wird, beträgt 1024, und dieser Wert kann durch Ändern konfiguriert werden **com.glide.attachment.max_size**, Und die Standardzeitüberschreitung beträgt 120 Minuten, die über die FireEye-Standardeinstellungsseite konfiguriert werden kann.

Umfassendes Skript Für Untersuchungsdetails

Ermöglicht das Sammeln aller forensischen und untersuchenden Artefakte vom Endpunkt, ist jedoch die unerschwinglichste Option. Diese Konfiguration ist ideal für Situationen, in denen es nur ein Fenster zum Sammeln von Daten vom betreffenden Endpunkt gibt und die Möglichkeit, später weitere Daten zu erfassen, nicht garantiert werden kann. Verwenden Sie daher diese Aktion mit Vorsicht.

Standardskript Für Untersuchungsdetails

Aktiviert die gängigsten Optionen für die Erfassung forensischer und untersuchender Artefakte von einem Endpunkt. Soll das primäre Antworttool sein, wenn Sie den Verdacht haben, dass ein Endpunkt gefährdet sein könnte und eine eingehende Analyse dieses Endpunkts durchführen müssen. Ziel ist es, ein Gleichgewicht zwischen der Erfassung der relevantesten und wertvollsten Daten zu finden und gleichzeitig die kostspieligen Optionen zu vermeiden, die später erfasst werden können, sobald eine weitere Untersuchung dies als erforderlich erweist.

Selektierung – Akquisition

Selektierungssammlungen enthalten Informationen aus dem Lookback-Cache sowie zusätzliche forensische Auditinformationen, z. B. URL-Downloadverlauf, Dateidownloadverlauf, Prozess- und Portlisten sowie Standardsysteminformationen. Möglicherweise möchten Sie diese Informationen überprüfen, wenn anomaler Netzwerkverkehr erkannt wird, und Sie möchten mehr Transparenz in Endpunktaktionen haben.

Datenerfassungsskripts auf FireEye verwalten

Datenbeschaffungsanforderungen (manchmal als Live-Antwortanforderungen bezeichnet) ermöglichen es Ihnen, alle benötigten Daten von einem einzigen ausgeführten Endpunkt zu erfassen. Auf der Seite „Datenerfassungsskripts“ in FireEye können Sie die Datenerfassungsskripts erstellen, bearbeiten, kopieren und löschen, die für Datenerfassungsanforderungen verwendet werden.

Zugriff auf die Seite „Datenerfassungsskripts“ in FireEye

So greifen Sie auf die Seite „Datenerfassungsskripts“ zu:

1. Navigieren Sie zu Endpunktsicherheit Web-Anwenderoberfläche.
2. Wählen Sie im Menü Administrator die Option Datenerfassungsskripts aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen eines Skripts auf FireEye

So erstellen Sie ein Datenbeschaffungsskript:

1. Auswahlvorgang **Datenerfassungsskripts** > **Administrator** Menü der Webanwenderoberfläche „Endpunktsicherheit“.
2. Klicken **Skript erstellen**an.
3. Geben Sie einen Namen für das neue Skript in ein **Skriptname** an.
4. Geben Sie optional eine Beschreibung des Skripts ein.
5. Wählen Sie das Betriebssystem aus, für das das Skript gilt. Sie können im Dialogfeld „Skript erstellen“ nur ein einzelnes Betriebssystem auswählen.
6. Klicken **Erstellen** Um die Skriptdefinition zu starten.
7. Wählen Sie im einen Beschaffungsdatentyp aus **Fügen Sie einen Beschaffungstyp hinzu**Dropdown-Feld, und klicken Sie auf **Hinzufügen**an. Optionen für den angeforderten Beschaffungstyp werden rechts neben der Skriptliste angezeigt.
8. Geben Sie Werte für die Beschaffungstypoptionen an, oder verwenden Sie die bereits ausgewählten Standardwerte. Die Web-UI warnt Sie nicht und entfernt keine Registerkarten, Leerzeichen oder unerwünschten Zeichen (z. B. \n) in Ihren Spezifikationen.
9. Wiederholen Sie die vorherigen 2 Schritte, um zusätzliche Daten für das Datenbeschaffungsskript anzufordern. Einige Beschaffungsdatentypen sind nur einmal für ein Skript verfügbar, während andere mehrmals angegeben werden können. Nach dem Hinzufügen eines Beschaffungstyps zu einem Skript die Liste der Beschaffungstypen, die in verfügbar sind **Fügen Sie einen Beschaffungstyp hinzu**Das Dropdown-Feld passt sich entsprechend an.
10. Um einen Beschaffungsdatentyp aus dem Skript zu entfernen, klicken Sie auf das x-Symbol ( ) auf der Registerkarte „Beschaffung“ auf der linken Seite der Seite.

Hinweis:
Diese Integration unterstützt nicht **Bearbeitungen vor dem Erwerb zulassen** Option beim Erstellen von Skripts. Stellen Sie daher sicher, dass das Kontrollkästchen deaktiviert ist.

Exportieren eines Skripts aus FireEye

Sie können ein Datenbeschaffungsskript in eine JSON-Datei exportieren. So exportieren Sie ein Datenbeschaffungsskript:

1. Auswahlvorgang **Datenerfassungsskripts** > **Administrator** Der Webanwenderoberfläche „Endpunktsicherheit“.
2. Wählen Sie im Menü Administrator die Option Datenerfassungsskripts aus.
3. Wählen Sie auf der linken Seite der Seite das Skript aus, das Sie exportieren möchten.
4. auswählen **Aktionen** > **Skript Exportieren**an.
5. Eine JSON-Datei wird auf Ihren Computer heruntergeladen. Der JSON-Dateiname enthält das Betriebssystem, sodass Sie einfach bestimmen können, welche Skripts für welches Betriebssystem gelten.

Erstellen einer neuen Datenerfassungsaktion in ServiceNow AI Platform

Führen Sie die folgenden Schritte aus, um eine neue Aktion zu erstellen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **FireEye-Integration** > **FireEye: zusätzliche Aktionen**an. Die Liste zusätzliche FireEye-Aktionen wird angezeigt.
2. Klicken **Neu**an. Das Formular für die neue Aktion wird angezeigt.
3. Füllen Sie das Formular aus.

Aktionsname	Name der ausgeführten FireEye-Aktion. Dieser Name hilft Ihnen, den Aktionstyp zu identifizieren und zu beschreiben.
Akquisition	Eine Beschaffung ruft die zu analysierenden Daten ab. Dies ist ein schreibgeschütztes Feld und standardmäßig auf Datenerfassung festgelegt.
Quelle	Name der FireEye-Quelle. In der Auswahlliste sind nur konfigurierte Quellen verfügbar.
Fähigkeit	Dies ist ein schreibgeschütztes Feld und wird mit der Fähigkeit „zusätzliche Aktion(en) ausführen“ ausgefüllt
Akquisitionstyp	Typ der Beschaffungsaktion, die abgerufen und analysiert werden muss.
Aktiv	Dies gibt an, dass die Aktion aktiv ist.
Genehmigung erforderlich	Wenn Sie die Option Genehmigung erforderlich aktivieren, ist das Feld Genehmiger im Formular verfügbar. Nachdem Sie eine Anforderung übermittelt haben, ist die Genehmigung der Gruppe erforderlich, um die Anforderung abzuschließen.
Tag anzeigen	Typ des Betriebssystems, z. B. Windows, Mac, Linux zum Hinzufügen von Skripts. **Hinweis:** Derzeit wird nur ein Typ von Betriebssystem unterstützt. Sie können eine Aktion pro Betriebssystem erstellen. Erstellen Sie für andere Betriebssysteme nach Bedarf neue Aktionen.
Skripte	Importiertes Skript aus FireEye muss für den ausgewählten BS-Typ angegeben werden. Jedem BS-Typ kann nur ein Skript hinzugefügt werden.

4. Klicken **Absenden**an.

Datenakquisitionen aus Security Incident werden ausgelöst

Die zusätzlichen erstellten Aktionen können über den zugehörigen Link ausgeführt werden **Zusätzliche Aktion(en) für Endpunkt ausführen** Für den Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Bearbeitungen vor dem Erwerb zulassen Die FireEye-Funktionalität wird für die zusätzlichen Aktionen auf dem Endpunkt nicht unterstützt.

Konfigurieren Sie ein Profil für die Sichtungssuche mit der FireEye-Integration

Konfigurieren Sie das Sichtungssuchprofil mit dem folgenden Verfahren.

Vorbereitungen

Erforderliche Rolle: NowPlatform Security Incident-Administrator (sn_si.admin)

Immer wenn eine Quelle erstellt wird, werden einzelne Sichtungssuchkonfigurationen für fünf Typen (Datei, IPs(v4), MD5, SHA1 und SHA256) erstellt und standardmäßig deaktiviert. Sie sollten sie aktivieren, bevor Sie die Sichtungssuche verwenden. Jeder Typ des erkennbaren Elements verfügt über eine andere Suchabfrage, um Sichtungen abzurufen. Wir initiieren eine andere Suche für jeden erkennbaren Typ. Die Suche mehrerer erkennbarer Elemente nach einer Sichtungssuche ist in FireEye nicht möglich, da dies einen UND-Vorgang für die erkennbaren Elemente ausführt und das Ergebnis möglicherweise ungenau ist.

Hinweis:
Für die Sichtungssuche können nur fünf aktive Suchen gleichzeitig vorhanden sein. Verbleibend wird in die Warteschlange gestellt und beginnt nach Abschluss einer der laufenden Sichtungen.

Wenn Sie ein neues Sichtungssuchprofil erstellen möchten, führen Sie die folgenden Schritte aus, um eines zu erstellen:

Prozedur

1. Navigieren zu **Integrationen** > **Sichtungssuche – Konfiguration**an.
2. Klicken **Neu**an.
3. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Name für das Fähigkeitsprofil.
Ist gespeicherte Suche	Dadurch wird eine gespeicherte Suche ausgeführt, d. h. das Feld „Name“ muss mit dem Namen der gespeicherten Suche übereinstimmen.
Sichtungssuchquelle	Definiert die für die Integration konfigurierte Quelle.
Suchen	Fügen Sie eine native Suchzeichenfolge hinzu, um eine Abfrage zu erstellen.
Aktiv	Abfrage wird nur ausgeführt, wenn sie aktiv ist.
Typ des erkennbaren Elements	Definiert den Typ der Kategorie erkennbarer Elemente.
Maximale erkennbare Elemente pro Suche	Die Anzahl der erkennbaren Elemente bevor die Suchabfrage in mehrere Abfragen aufgeteilt wird. Legen Sie diesen Wert für diese Integration auf 1 fest.
Sichtungssuchparameter	Verwenden Sie Sichtungssuchparameter, um komplexere Abfragen zu definieren, die Logik und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	andere Operatoren enthalten, die vom angegebenen Protokollspeicher unterstützt werden.

4. Klicken **Absenden** Um die Konfiguration abzuschließen.

Rufen Sie die Sichtungssuche aus einem Security Incident auf

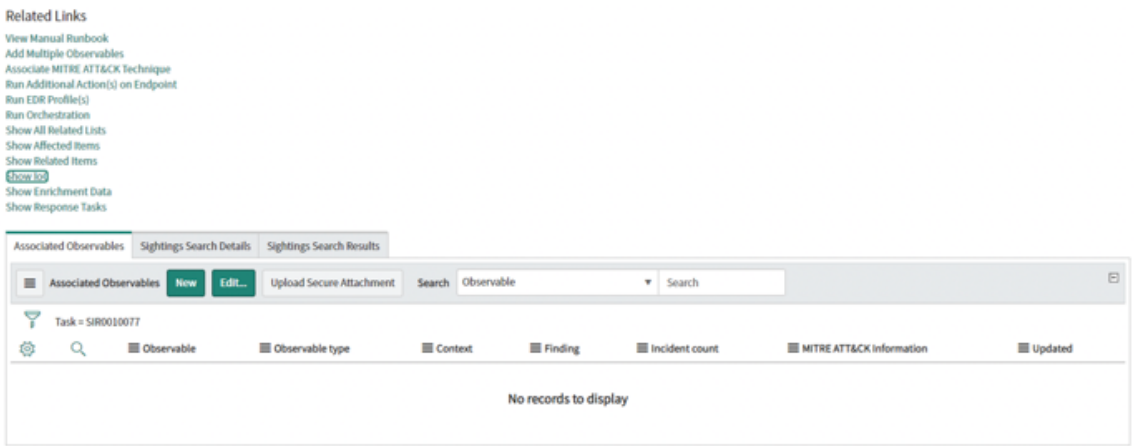
Rufen Sie die Sichtungssuche von einem SIR Security Incident auf, indem Sie das folgende Verfahren befolgen.

Vorbereitungen

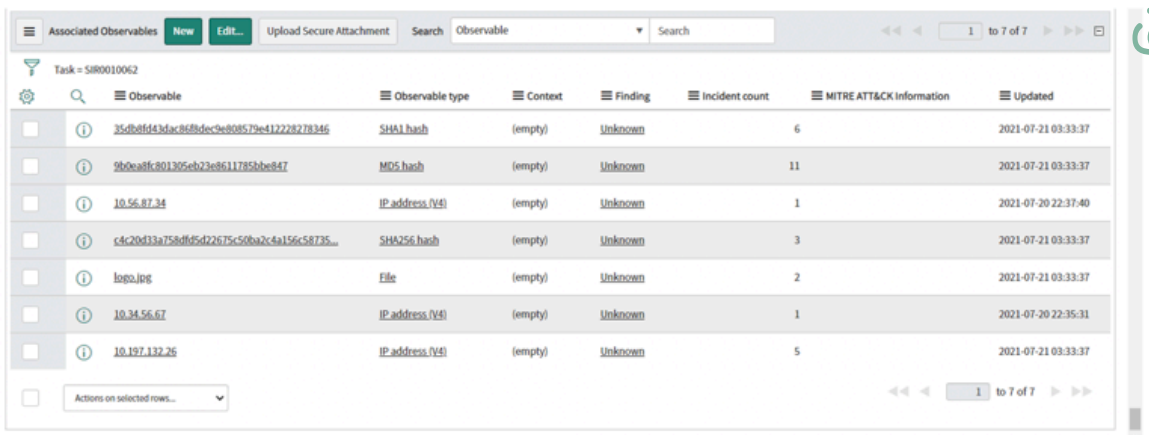
Erforderliche Rolle: ServiceNow AI Platform Administrator (sn_si.admin)

Prozedur

1. Navigieren Sie zu Security Incidents.
2. Öffnen Sie einen vorhandenen SIR, oder erstellen Sie einen neuen SIR.
3. Klicken Sie auf IOC in zugehörigen Links anzeigen.
4. Klicken **Zugehörige erkennbare Elemente** Zugehörige Listen.



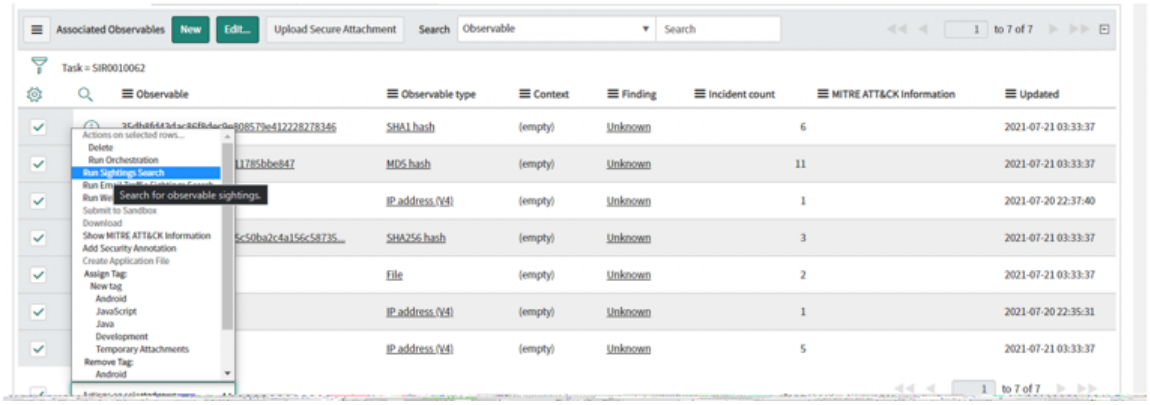
5. Fügen Sie vorhandene erkennbare Elemente hinzu, oder erstellen Sie ein neues erkennbares Element.



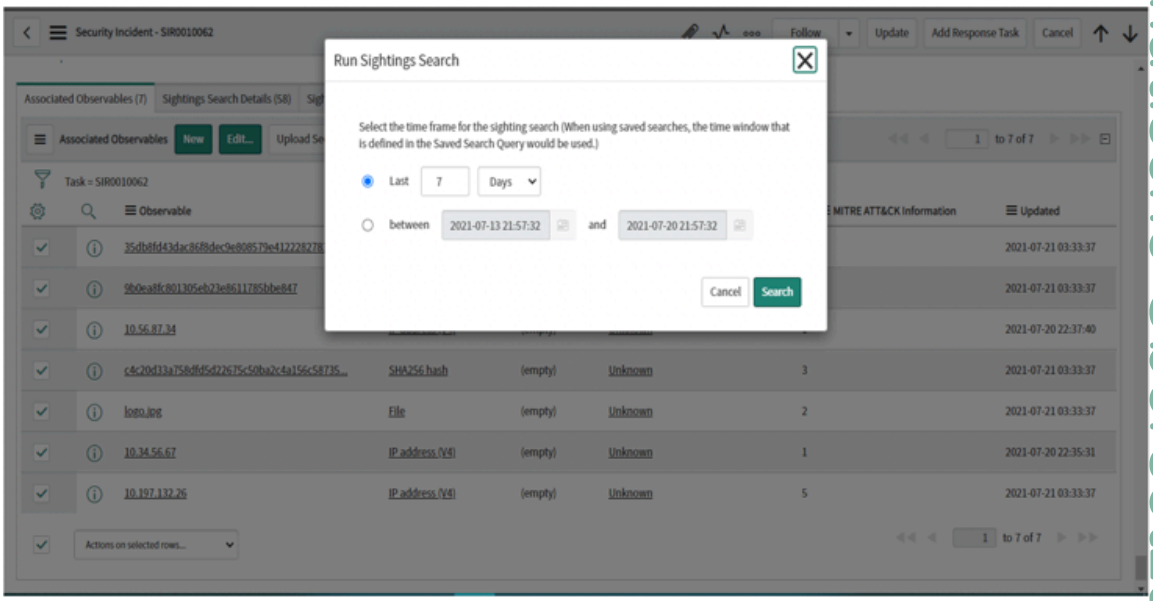
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie die erkennbaren Elemente aus, und klicken Sie unter Aktionen für ausgewählte Zeilen auf **Sichtungssuche ausführen**an.



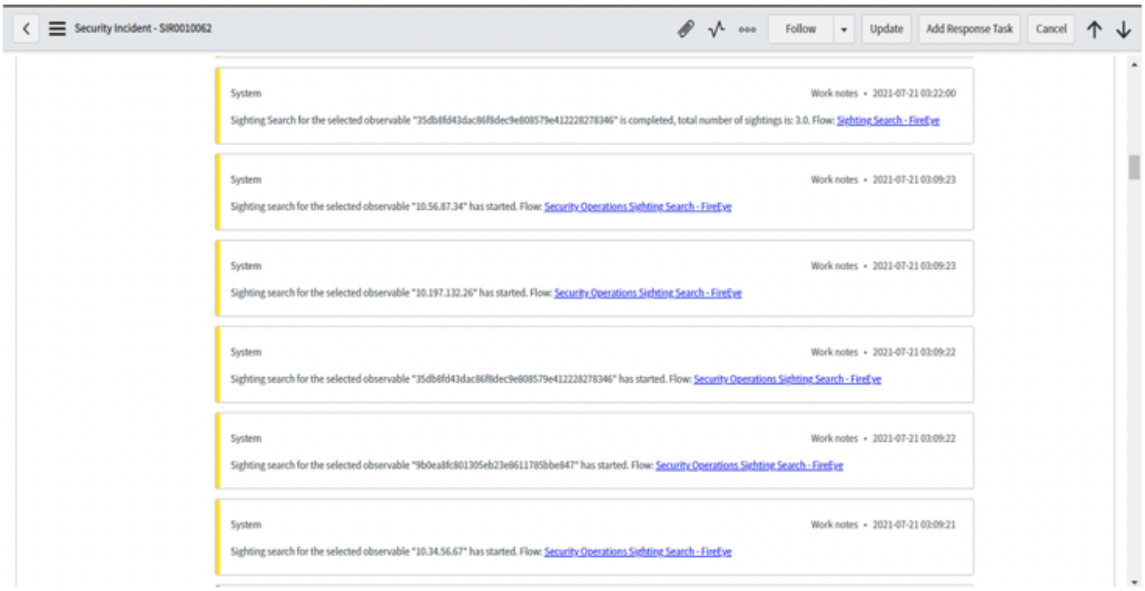
7. Ignorieren Sie die Eingaben im nächsten Dialogfeld, das nach Zeitdaten fragt.
Es sind Standardwerte ausgefüllt. Die Suche wird jedoch in Echtzeit durchgeführt, und die Zeitwerte werden für diese Integration ignoriert.



8. Überprüfen Sie den Status der Arbeitsnotizen.

Automatische Übersetzung

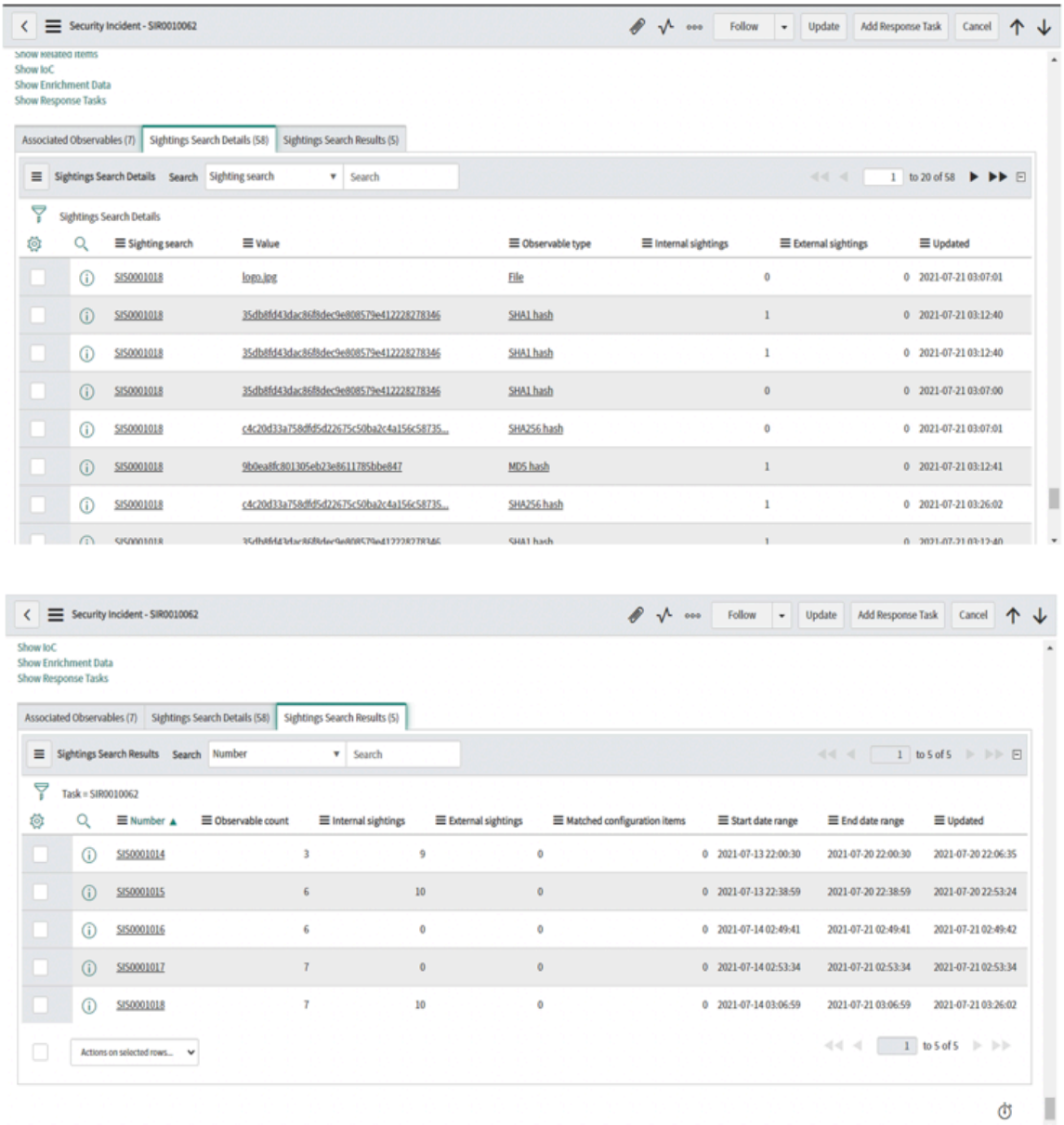
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Überprüfen Sie nach Abschluss der Suche die Ergebnisse und Details in den zugehörigen Listen.
10. Klicken Sie auf **Details einer Sichtungssuche** Registerkarte für Details und **Ergebnisse der Sichtungssuche** Registerkarte für Suchergebnisse.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Have I Been Pwned?-Integration

Die Security Operations Have I Been Pwned? Mit der Integration können Sie Suchen nach Domänennamen und E-Mail-Adressen übermitteln, um festzustellen, ob personenbezogene Daten des Anwenders durch Datenschutzverletzungen gefährdet wurden.

Erkunden

Security Incident Response-Integrationen

Einrichten

- Have I Been Pwned? Integrationen-Setup
- Aktivieren

Verwenden

Entwickeln

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Führen Sie Suchen nach erkennbaren Elementen durch Bedrohungssuche – Have I Been Pwned? Flow

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie Komponenten, die mit einer Anwendung installiert sind

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Have I Been Pwned? Integrationen-Setup

Have I Been Pwned? Ist eine kostenlose Ressource, die verwendet wird, um zu bewerten, ob jemand möglicherweise gefährdet wurde, da sein Online-Account bei einer Datenschutzverletzung gefährdet oder „pwned“ wurde. Es lässt sich problemlos in integrieren Security Operations.

Bevor Sie verwenden können Have I Been Pwned? Integration müssen Sie das Plugin aktivieren. Bei Bedarf können Sie auch Ihre X509-SSL-Zertifizierung aktualisieren.

Die Security Incident Response, Threat Intelligence, Und Security Operations Have I Been Pwned? Plugins sind erforderlich, um zu implementieren Security Operations Have I Been Pwned? Integration.

Bedrohungssuche – Have I Been Pwned? Flow

Die Bedrohungssuche – Have I Been Pwned? Flow führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn die erkennbaren Elemente von einem Typ sind, der von erkannt wurde Have I Been Pwned?, Die erkennbaren Elemente werden auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

Erforderliche Rolle: sn_si_admin

Dieser Flow wird durch ausgelöst Integration von Security Operations: Fähigkeit zur Bedrohungssuche Wenn Sie eine Bedrohungssuche für ein oder mehrere erkennbare Elemente durchführen, und Have I Been Pwned? Implementierung ist ausgewählt. Weitere Informationen finden Sie unter Führen Sie Suchen nach erkennbaren Elementen durch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wurde ich in Flow verschoben

Informationen zu den von diesem Flow verwendeten Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Aktivieren

Mit der Integrationskonfigurationsfunktion können Sie Sicherheitsintegrationen von Drittparteien, einschließlich, schnell aktivieren und einrichten Security Operations Have I Been Pwned? Integration. Bevor Sie verwenden können Have I Been Pwned? Integration müssen Sie sie aus herunterladen ServiceNow Store.

Vorbereitungen

- Die Threat Intelligence Das Plugin muss installiert und aktiviert werden, bevor Sie verwenden können Security Operations Have I Been Pwned? Integration.

Erforderliche Rolle: sn_si_admin

Prozedur

Laden Sie die Integration aus dem herunter ServiceNow Storean.
Diese Integration unterstützt eine offene API und erfordert keine weitere Konfiguration. Have I Been Pwned? Kann jetzt zum Durchführen von Suchen nach erkennbaren Elementen in ausgewählt werden Threat Intelligence Und für erkennbare Elemente in Security Incidents.

Zugehörige Informationen

Führen Sie Suchen nach erkennbaren Elementen durch

Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie eine SSL-Verbindung für die Integration benötigen, gibt es Umstände, in denen das vom Drittanbieter bereitgestellte Zertifikat entweder noch nicht vertrauenswürdig ist ServiceNow Oder ist abgelaufen. Diese Aufgabe ist optional.

Vorbereitungen

Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erwerben Sie das SSL-Zertifikat vom Drittanbieter.
   Sie können beispielsweise ein X.509-Zertifikat (PEM) von einem SSL-Endpunkt im Firefox-Browser wie folgt importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/` .

   b. Klicken Sie auf das Schlosssymbol in der Adresszeile.

   c. Klicken Sie Auf **Weitere Informationen** Und klicken Sie auf **Sicherheit** Registerkarte.

   d. Klicken Sie Auf **Zeigen Sie Das Zertifikat An** Und klicken Sie auf **Detail** Registerkarte.

   e. Klicken Sie Auf **Exportieren** Um das PEM in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor-Tool, und kopieren Sie den Inhalt in die Zwischenablage.
   Sie muss mit beginnen `----- ZERTIFIKAT BEGINNEN------` Und enden mit `----- ENDZERTIFIKAT-----` .

2. Navigieren zu **Systemdefinition** > **Zertifikate**an.
3. Klicken Sie Auf **Neu** Und Erstellen Sie einen neuen Datensatz Für die Integration.
4. In **PEM-Zertifikat** , Fügen Sie das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.
   a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an.
   b. Wählen Sie den aktiven Standard-Identitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.
   c. Scrollen Sie nach unten zu **X.509-Zertifikate** Zugehörige Liste, und klicken Sie auf **Bearbeiten** .
   d. Verschieben Sie das neu erstellte Zertifikat in **Ausgewählt** Spalte.
6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

Hinweis:
Wenn Sie ein abgelaufenes Zertifikat haben, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 ersetzt ein ablaufendes SAML-Zertifikat .

HPE Security ArcSight ESM – E-Mail-Parser-Integration

Die Integration von HPE Security ArcSight ESM – E-Mail-Parser wird mit einem E-Mail-Parser unterstützt, der E-Mail-Benachrichtigungen von ESM verwendet, um Security Incidents zu erstellen.

Konfigurieren Sie die Integration von HPE Security ArcSight ESM – E-Mail-Parser

Die Integration von HPE Security ArcSight ESM – E-Mail-Parser verwendet E-Mail-Benachrichtigungen von ESM, um Ergänzungs- und Antwort-Workflows zu fördern.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

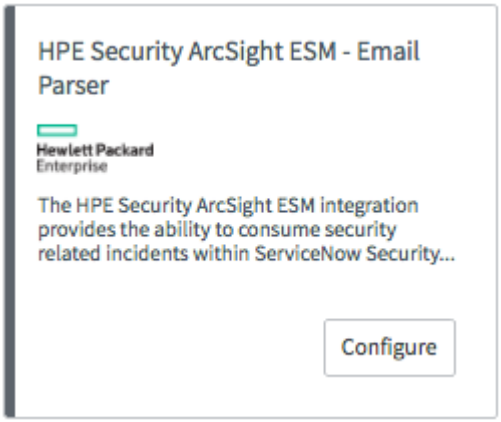
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Eine HPE Security ArcSight ESM – E-Mail-Parser-Vorlage wird zur Verwendung für die Integration bereitgestellt. Sie muss konfiguriert und aktiviert werden, bevor die Integration stattfindet. Durch das Aktualisieren des Parsers wird er aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.



2. Klicken Sie auf der Karte HPE Security ArcSight ESM – E-Mail-Parser auf **Konfigurieren** .
3. In **HPE Security ArcSight ESM – E-Mail-Parser-Konfiguration** Klicken Sie auf das Dialogfeld **Konfigurieren Sie Den E-Mail-Parser** Link.
4. Klicken Sie auf **ArcSight ESM** Link zum Bearbeiten der Einstellungen im bereitgestellten Vorlagen-E-Mail-Parser.
   Füllen Sie mindestens aus E-Mail ist von Feld. Informationen zum Erstellen eines eigenen E-Mail-Parsers finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
5. Überprüfen Sie **Aktiv** Feld.
6. Klicken Sie Auf **Aktualisieren** In **E-Mail-Parser** Formular.
   Der E-Mail-Parser ist aktiv. Sie müssen nicht zu zurückkehren **Integrationskonfigurationen** .

HPE ArcSight Logger – Integration der Incident-Anreicherung

Die HPE ArcSight Logger– Die Incident-Anreicherungsintegration durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

Erkunden

Security Incident Response-Integrationen

Einrichten

- Beginnen Sie mit dem HPE ArcSight Logger
- Erstellen Sie Konfigurationsdatensätze für Sichtungssuche

Verwenden

Entwickeln

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Führen Sie eine Sichtungssuche aus
- Integration Von Security Operations: Sichtungssuche-Flow
- Security Operations – Suchflow Für Arcsight Logger-Sichtungen
- Sichtungssuchdetails Anzeigen
- Zeigen Sie Die Ergebnisse Der Sichtungssuche An
- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie Komponenten, die mit einer Anwendung installiert sind

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Beginnen Sie mit dem HPE ArcSight Logger

HPE ArcSight Logger Streamt Echtzeitdaten, kategorisiert sie in bestimmte Protokolle und lässt sich problemlos in integrieren Security Operations. Bevor Sie verwenden können HPE ArcSight Logger– Integration der Incident-Anreicherung. Sie müssen sie aus dem herunterladen ServiceNow Store Und fügen Sie API-URL und Anmeldeinformationen hinzu.

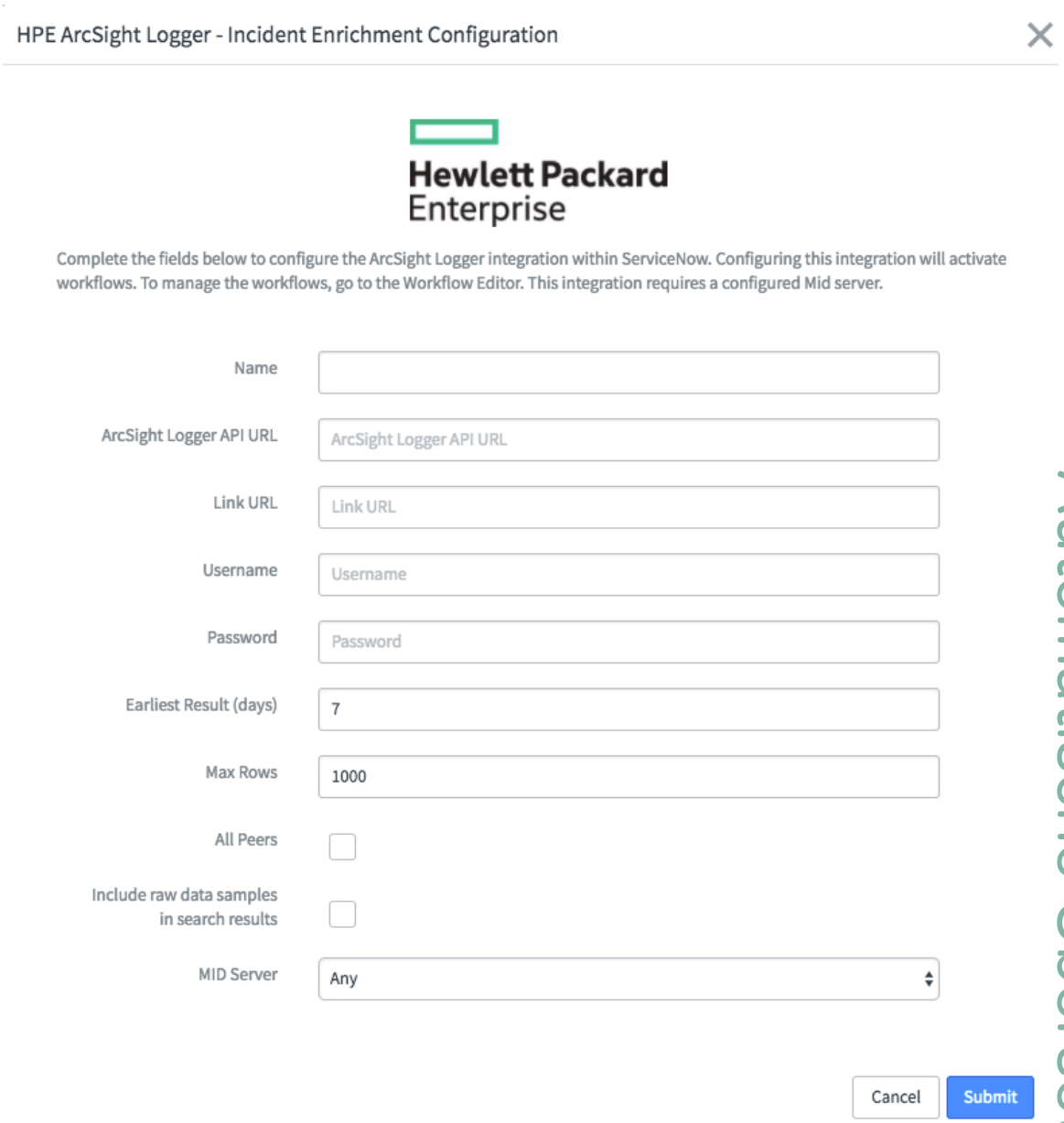
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. In HPE ArcSight Logger– Incident-Anreicherungskarte, klicken Sie auf **Neu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

4. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Basis-URL der ArcSight Logger-API	Die Basis-URL, die Sie von der HPE Security ArcSight Logger-Website erworben haben.
Link-URL	[Optional] die Link-URL, die mit einer HPE Security ArcSight Logger-Instanz verknüpft ist, falls verfügbar.
Anwendername	Ihre Informationen HPE ArcSight Logger Anwendername.
Passwort	Ihre Informationen HPE ArcSight Logger Passwort.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie in Tagen anzeigen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Alle Peers	Die Standardeinstellung ist deaktiviert und durchsucht nur den lokalen Protokollierer, mit dem Sie verbunden sind. Wenn diese Option aktiviert ist, werden alle Protokollierer durchsucht, die miteinander verbunden sind.
Rohdatenmuster in Suchergebnissen berücksichtigen	Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in ab **Anzahl der Zeilen mit Rohdaten** Eigenschaft in Eigenschaften von Security Incident Response .
MID-Server	Wählen Sie Aus **Beliebig** Um einen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Navigieren Sie zum Verwalten der Workflows zu **Workflow-Editor** .

5. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
6. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf klicken **Konfigurieren** Oder **Löschen** Zum Ändern oder Löschen der Konfiguration.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie aus **Nein** Von **Konfigurationen Anzeigen** Dropdown-Liste.

Hybrid-Analyse-Integration

Die Hybrid-Analyse Die Anwendung ist Teil einer offenen Online-Community, in der Anwender Dateien und URLs auf Bedrohungen analysieren. Sie teilen Ergebnisse und nutzen Forschung aus der Community, um effektivere Antworten auf Incidents zu erhalten. Bei Integration mit ServiceNow AI Platform Security Operations Produkt bietet Ihnen die gemeinsam genutzte Threat Intelligence zusätzliche Einblicke in den Schweregrad bestimmter erkennbarer Elemente.

Die Hybrid-Analyse Die Integration führt Bedrohungssuchen für die folgenden erkennbaren Elemente durch:

- Datei-Hashes
- IP-Adressen
- URLs

Der Flow überprüft nach neuen erkennbaren Elementen, wenn sie in Security Incidents ankommen. Wenn die erkennbaren Elemente von einem Typ sind, der von der API-Integration erkannt wird, werden die erkennbaren Elemente ausgewertet. Erkennbare Elemente, die als schädlich eingestuft werden, werden gekennzeichnet.

Installieren und konfigurieren

Bevor Sie die Integration auf Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte so aus Hybrid-Analyse Die Anwendung ist ordnungsgemäß in integriert ServiceNow AI Platform Security Operations.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform Und Security Incident Response Rollen.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Der Administrator (Administrator) installiert die App und weist die Rolle Security Incident-Administrator (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf Security Operations Modul und weist die Rolle „sn_si.Analyst“ zu.
Rufen Sie einen API-Schlüssel ab.	Besuchen Sie Hybridanalyse Website für Informationen zu API-Schlüsseln und zum Erstellen eines Accounts: Hybridanalyse-Website . Die Konfiguration erfordert, dass Sie die API-Schlüssel eingeben.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	Für das Madrid-Release und spätere Familienveröffentlichungen ist das Plugin com.snc.si_dep erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Anwendungen. Folgendes Security Operations Anwendungen müssen über installiert und aktiviert werden ServiceNow Store. Installieren und aktivieren Sie jeweils eine Anwendung in der unten aufgeführten Reihenfolge, um eine reibungslose Installation sicherzustellen: **1.** Sicherheits-Integrations-Framework **2.** Security Support Common **3.** Orchestration Des Sicherheitssupports **4.** Security Incident Response Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz für die Integration finden Sie unter Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

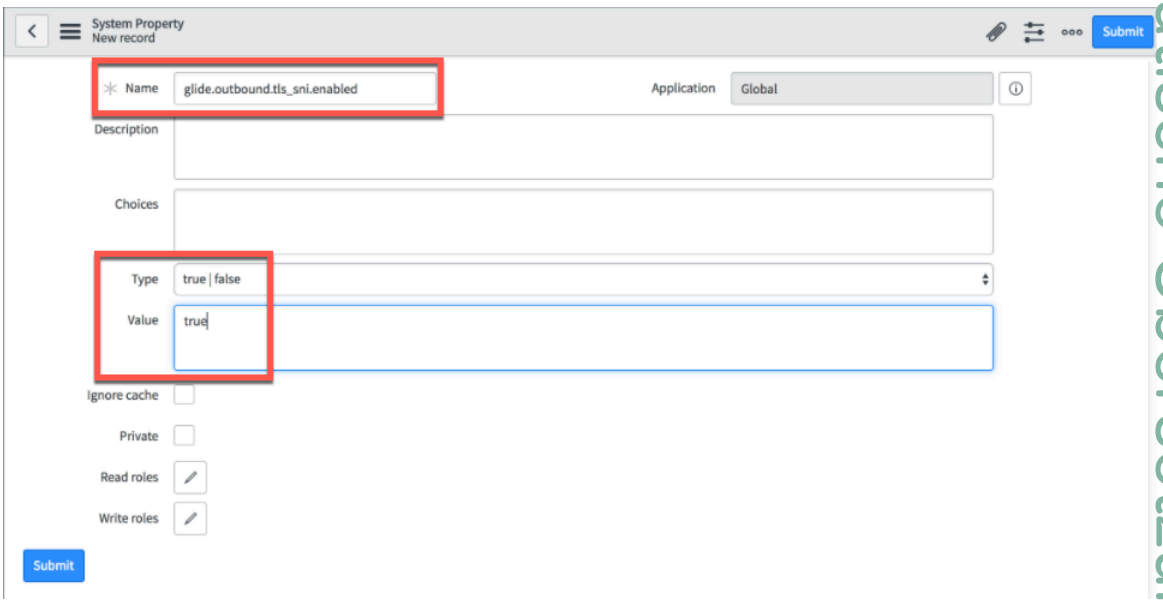
Warum und wann dieser Vorgang ausgeführt wird

Führen Sie die folgenden Schritte aus, um Systemeigenschaften zu aktualisieren und die Integration zu installieren und zu konfigurieren.

Prozedur

1. Geben Sie im Navigationsfilter `sys_properties.list` ein, und drücken Sie die **Eingabetaste**.
   Die **Systemeigenschaften** Liste wird angezeigt.
2. Klicken Sie auf **Neu**.
   Ein neuer Datensatz wird angezeigt.
3. Füllen Sie die Felder aus, oder wählen Sie die in der folgenden Tabelle aufgeführten Werte aus, und klicken Sie auf **Übermitteln** .

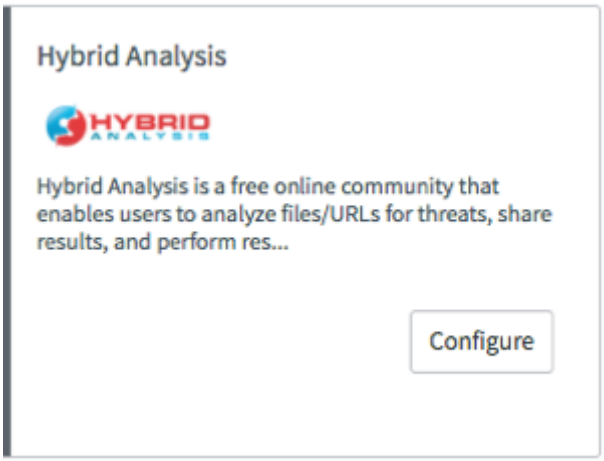
Feldname	Wert
Name	Glide.Outbound.tls_sni.enabled
Typ	Wählen Sie Aus **Wahr I falsch**
Wert	true



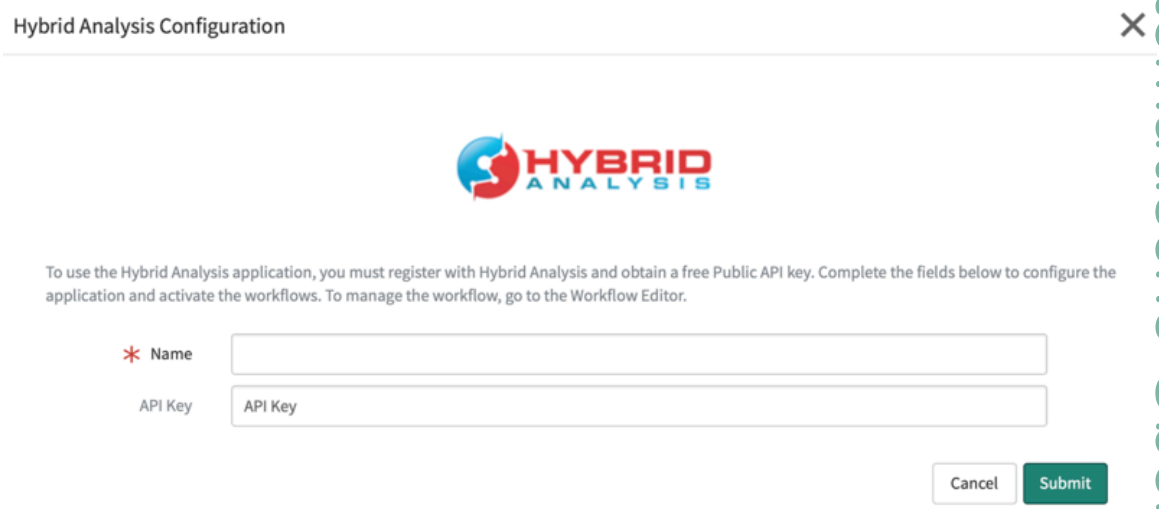
4. Wenn Sie die Anwendung für die Integration nicht installiert haben, finden Sie weitere Informationen unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
5. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie Hybrid-Analyse Kachel.
6. Klicken Sie auf **Konfigurieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. In **Hybridanalysekonfiguration** Geben Sie den API-Schlüssel ein, den Sie aus dem erhalten haben Hybrid-Analyse Website und klicken Sie auf **Übermitteln** .



8. Überprüfen Sie die erfolgreiche Konfiguration.
   Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, eine Fehlermeldung wird angezeigt.

   Trouble?

   Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, wird Hybrid-Analyse API-Schlüssel ist möglicherweise ungültig.

Überprüfen Sie die erwarteten Ergebnisse

Erkennbare Elemente werden automatisch von einem Security Incident generiert und von der Anwendung gescannt. Suchen Sie die Suchergebnisse im Security Incident, um sicherzustellen, dass die Bedrohungssuche erfolgreich ausgeführt wurde. Zeigen Sie auch Rohdaten an, und führen Sie Bedrohungssuchen für untergeordnete erkennbare Elemente aus.

Vorbereitungen

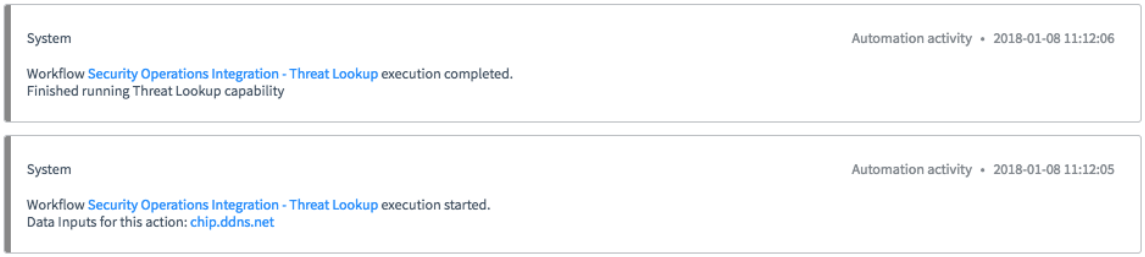
Erforderliche Rolle: sn_si.Analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie den Security Incident-Datensatz, mit dem Sie arbeiten, und überprüfen Sie, ob die Suche erfolgreich ausgeführt wurde.

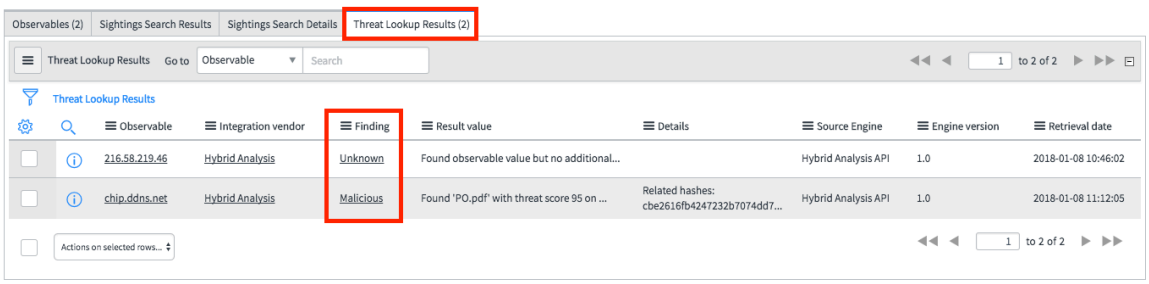


   Nachdem die Anwendung konfiguriert wurde, wird der Flow bei der Incident-Erstellung automatisch gestartet. Der Ausführungs- und Abschlussstatus der Suche wird dann in den Arbeitsnotizen im Security Incident angezeigt.

2. Überprüfen Sie die Arbeitsnotizen, um weitere Informationen zum Fortfahren zu erhalten, wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde.

3. Navigieren Sie zum Ende des Security Incident-Datensatzes, und klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Zugehöriger Link zum Anzeigen von Ergebnissen.

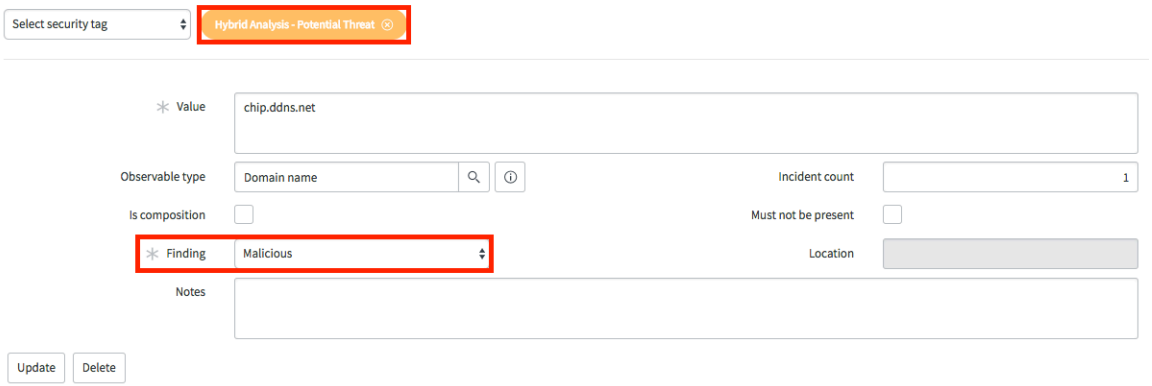
   Hinweis:
   Die Zahlen in den folgenden Schritten werden mit angezeigt **Formulare mit Registerkarten** Einstellung in den Systemeinstellungen aktiv. Klicken Sie in der oberen rechten Ecke des Bannerrahmens auf das Zahnradsymbol Einstellungen. In **Systemeinstellungen** Klicken Sie auf das Dialogfeld, das angezeigt wird **Formulare** Und verifizieren Sie das **Formulare mit Registerkarten** Und **Mit dem Formular** Sind ausgewählt.



   Die **Ergebnisse Der Bedrohungssuche** Auf der Registerkarte werden die Suchergebnisse am unteren Rand des Security Incident-Datensatzes angezeigt. Beachten Sie **Ergebnis** Spaltenanzeigen Unbekannt Für Datensätze, die nicht als schädlich eingestuft wurden. Für Ergebnisse, die mit böswilligen Ergebnissen übereinstimmen, die **Ergebnis** Spaltenanzeigen Böswillig .

4. In **Erkennbares Element** Spalte auf ein erkennbares Element klicken, um den Datensatz zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

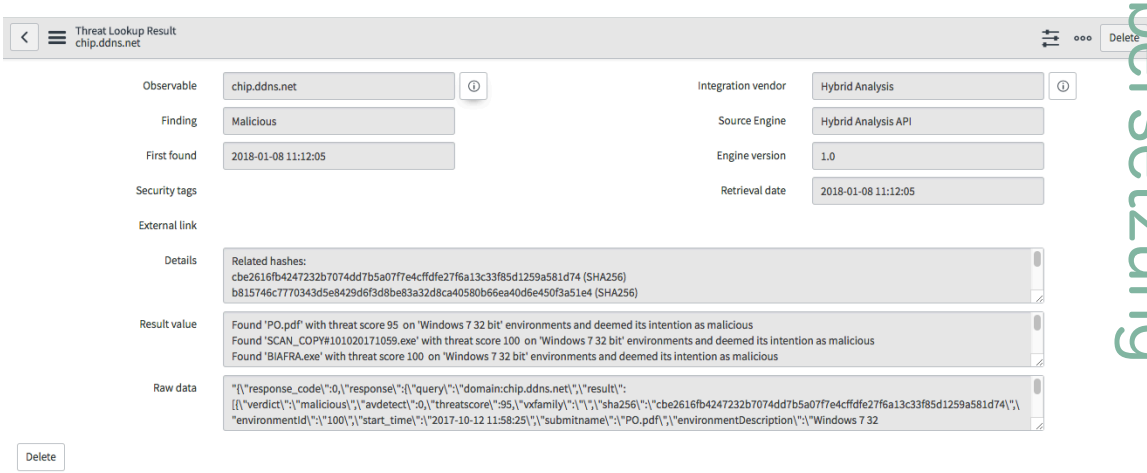


Für Suchvorgänge, die schädlich sind, die **Ergebnis** Feld wird angezeigt Böswillig , Und das erkennbare Element ist mit gekennzeichnet Threat Intelligence Quelle, die festgestellt hat, dass es böswillig ist, in diesem Fall die Hybrid-Analyse Integration.

5. **Wahlweise:** Führen Sie die Schritte aus, um Rohdaten anzuzeigen, eine Liste untergeordneter erkennbarer Elemente anzuzeigen und eine Bedrohungssuche für ausgewählte untergeordnete erkennbare Elemente auszuführen.

   a. Navigieren Sie zurück zum Security Incident und auf der **Ergebnisse Der Bedrohungssuche** Klicken Sie auf das blaue Informationssymbol neben einem erkennbaren Element.

   b. Klicken Sie im angezeigten Fenster auf **Öffnen Sie Den Datensatz** Zum Anzeigen der Daten. Von allen erkennbaren Elementen, die in den Rohdaten angezeigt werden, die in der Suche angezeigt werden, aus Hybrid-Analyse Durch die Integration werden auch untergeordnete oder zugehörige erkennbare Elemente erstellt.

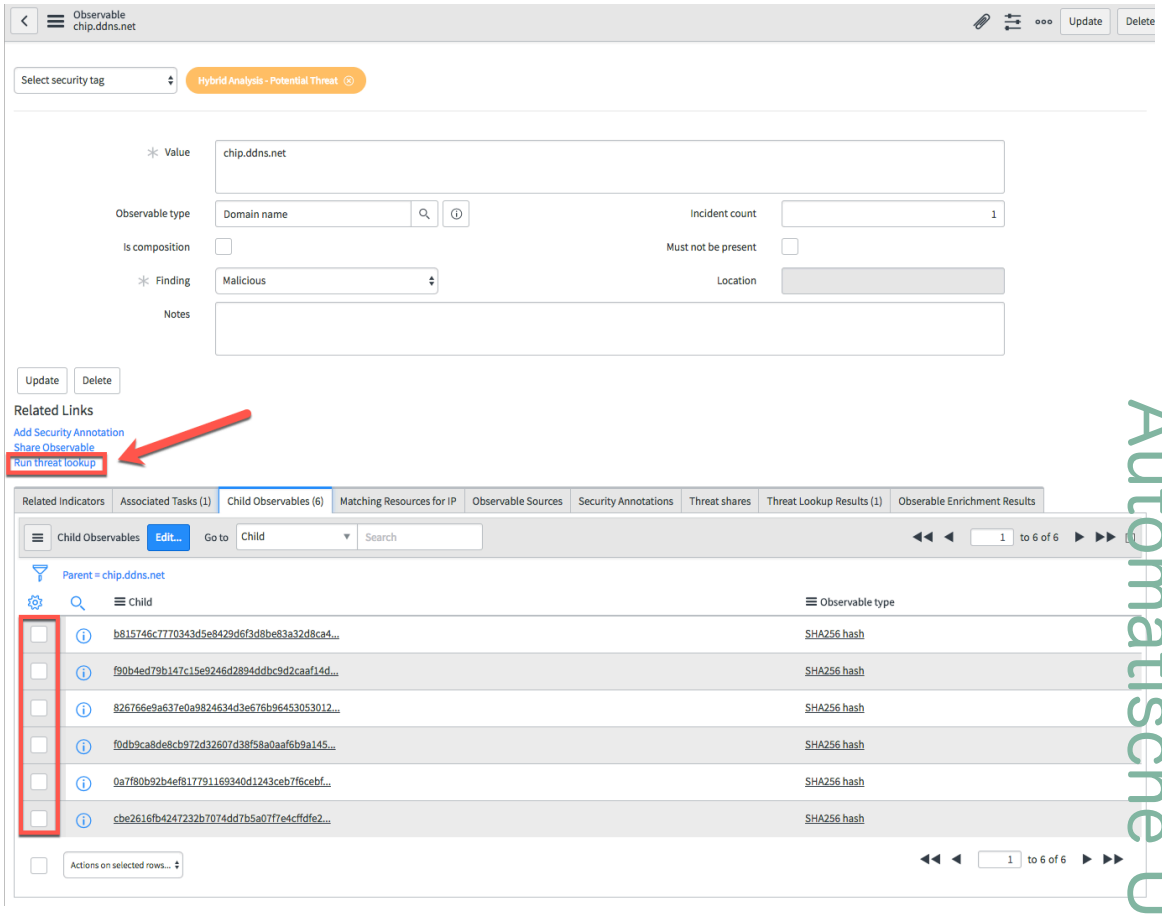
   Der von der API erstellte Link, die Rohdaten und andere Informationen werden angezeigt.

   c. Navigieren Sie zurück zum Security Incident, und klicken Sie auf **IOC anzeigen** Zugehöriger Link. Die untergeordneten erkennbaren Elemente werden im angezeigt **Untergeordnete Erkennbare Elemente** Registerkarte im Security Incident, da bei der Suche eine vorhandene Verbindung zwischen diesen zugehörigen erkennbaren Elementen und dem ursprünglich übermittelten erkennbaren Element gefunden wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Klicken Sie auf das Feld neben einem erkennbaren Element in **Untergeordnet** Spalte zum Auswählen, gefolgt von **Bedrohungssuche ausführen** Zugehöriger Link zum Durchführen einer Suche.



e. Überprüfen Sie im angezeigten Dialogfeld, ob Hybrid-Analyse Integration ist ausgewählt, und klicken Sie auf **Übermitteln** .

f. Überprüfen Sie in den Arbeitsnotizen, ob die Suche erfolgreich ausgeführt wurde, und auf dem **Ergebnisse Der Bedrohungssuche** Suchen Sie auf der Registerkarte Security Incident nach Suchergebnissen für die untergeordneten erkennbaren Elemente.

Trouble?

Wenn unter keine Ergebnisse angezeigt werden **Ergebnisse Der Bedrohungssuche** Überprüfen Sie, ob das erkennbare Element ein Typ ist, der für die Suche durch die Integration unterstützt wird.

(Optional) Fügen Sie ein erkennbares Element für manuell an Hybrid-Analyse

Sie können erkennbare Elemente manuell anhängen, wenn Sie Bedrohungssuchen für erkennbare Elemente durchführen möchten, die nicht an einen Security Incident im ersten Ereignisauslöser angehängt sind. Sie können diese Aufgabe auch ausführen, wenn Sie weitere Informationen zu einem zugehörigen erkennbaren Element wünschen.

Vorbereitungen

Überprüfen Sie, ob das erkennbare Element von einem Typ ist, der von der Integration unterstützt wird. Die Integration führt Suchen nach den folgenden Arten erkennbarer Elemente durch:

Automatische Übersetzung

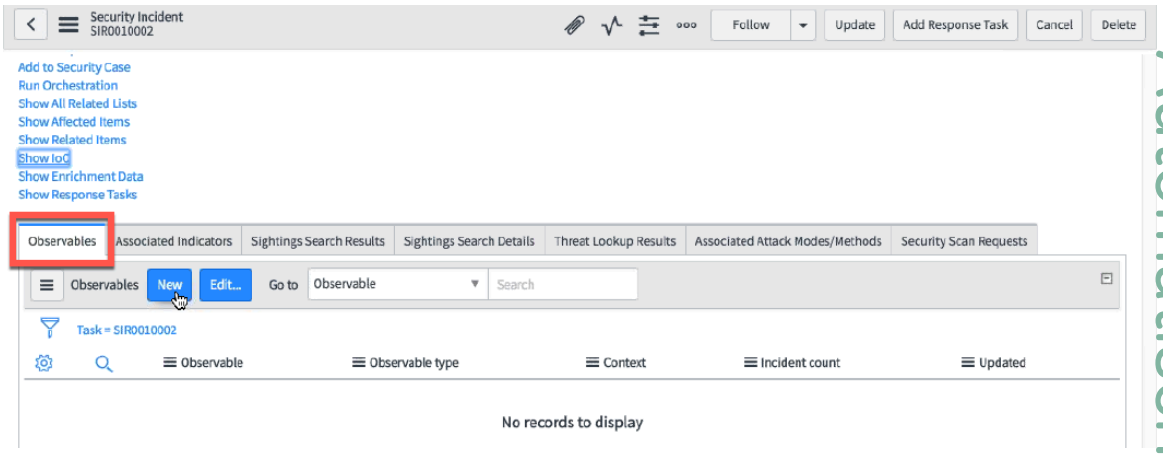
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Datei-Hashes
- IP-Adressen
- URLs

Erforderliche Rolle: sn_si.Analyst

Prozedur

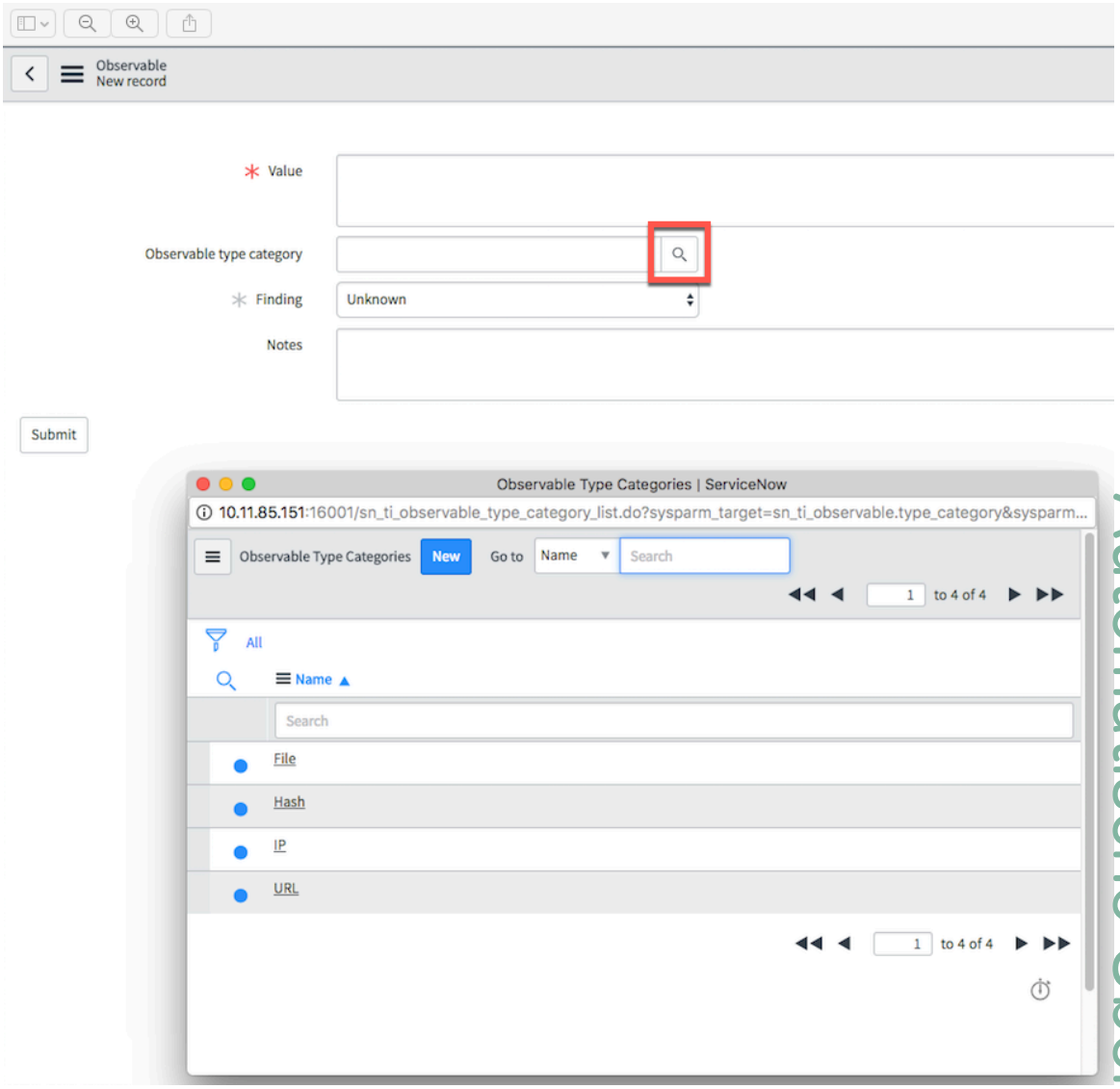
1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen** Und öffnen Sie einen Security Incident, an den Sie das erkennbare Element anhängen möchten.
2. Klicken Sie im offenen Security Incident auf **IOC anzeigen** Link in **Zugehörige Links** .



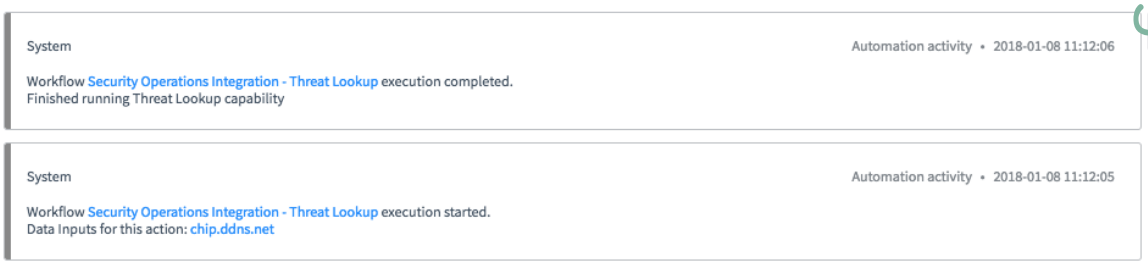
3. Auf der **Erkennbare Elemente** Klicken Sie auf die Registerkarte **Neu** .
   Das Formular „erkennbares Element“ wird angezeigt.
4. In **Wert** Feld ein erkennbares Element (Datei-Hash, IP-Adressen oder URL) eingeben.
5. Klicken Sie auf das Suchsymbol und im **Typkategorien Des Erkennbaren Elements** Dialogfeld auf den gewünschten erkennbaren Typ in der Liste klicken, um das Feld auszufüllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



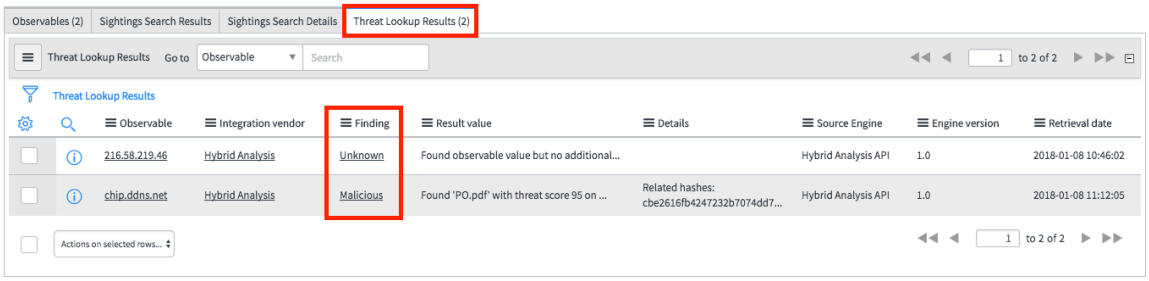
6. Klicken Sie auf **Absenden**.
   Der Flow wird gestartet und überprüft, ob das neue erkennbare Element vorhanden ist. Der Ausführungs- und Abschlussstatus wird im Abschnitt „Arbeitsnotizen“ im Security Incident-Datensatz angezeigt.
7. Navigieren Sie zu Ihrem Security Incident, und überprüfen Sie die Arbeitsnotizen.



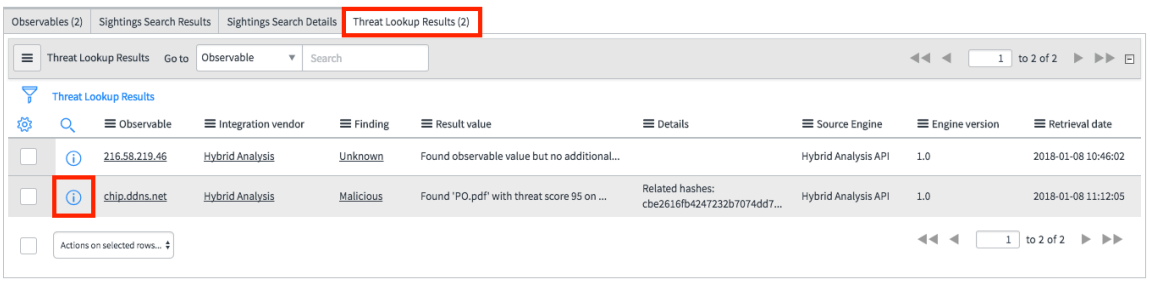
8. Klicken Sie unten im Datensatz auf **Alle Zugehörigen Listen Anzeigen** Zugehöriger Link.
9. Klicken Sie auf **Ergebnisse Der Bedrohungssuche** Registerkarte zum Anzeigen der Ergebnisse.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. In **Erkennbares Element** Klicken Sie auf das blaue Informationssymbol neben einem bestimmten erkennbaren Element, um weitere Informationen und Rohdaten zu erhalten.



11. Klicken Sie im angezeigten Dialogfeld auf **Öffnen Sie Den Datensatz** Zum Anzeigen der Rohdaten und weiterer Details.
    Alternativ können Sie auch ein vorhandenes erkennbares Element an den Security Incident-Datensatz anhängen.
12. **Wahlweise:** Mit **Erkennbare Elemente** Registerkarte ausgewählt, klicken Sie auf **Bearbeiten** .
13. **Wahlweise:** In **Bearbeiten Sie Mitglieder** Formular, das angezeigt wird, verschieben Sie ein vorhandenes erkennbares Element aus **Sammlung** Bis **Liste Erkennbarer Elemente** Und klicken Sie auf **Speichern** .
    Sie kehren zum Security Incident zurück.
14. Wählen Sie in der Spalte ganz links die erkennbaren Elemente aus, für die Sie die Suche ausführen möchten, und aus **Aktionen für ausgewählte Zeilen...** Auswahlliste auswählen **Bedrohungssuche ausführen** .
    Oben im Datensatz wird eine Nachricht angezeigt, dass die Anforderung verarbeitet wird. Überprüfen Sie, ob die Suche erfolgreich ausgeführt wurde.

Trouble?
Überprüfen Sie die Arbeitsnotizen, um weitere Informationen zu erhalten und zu erfahren, wie Sie fortfahren können, wenn Sie nicht verifizieren können, dass die Suche erfolgreich ausgeführt wurde.

IBM QRadar Offense Ingestion Integration

Die IBM QRadar Offense Ingestion Mit der Integration können Sie automatisch abrufen IBM QRadar Vergehen und konvertieren Sie sie in Security Incidents, und ermöglichen Sie automatisierte Antwortaktionen.

Diese Integration unterstützt Folgendes:

- Discovery von IBM QRadar Vergehen, die Kandidaten für Security Incidents sind.
- Letzte Ereignisse oder Flows, die einer Straftat zugeordnet sind, werden abgerufen.
- Verfolgen Sie regelmäßig wichtige Updates zu Vergehen nach.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zuordnung von Vergehen-, Ereignis- und Flow-Feldern zu Security Incident-Feldern.
- Vorläufige Ansicht der zugeordneten Felder.
- Richten Sie geplante Erfassungen von Straftaten ein, um regelmäßig Security Incidents zu erstellen.
- Schließen Sie die Verstöße, wenn die Security Incidents geschlossen werden.

Installieren und konfigurieren Sie ServiceNow Anwendung für IBM QRadar Integration der Verstoßerfassung

Bevor Sie die Integration für ausführen ServiceNow AI Platform® Führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in integriert wird Security Incident Response Und Security Operations Produkte auf Ihrem ServiceNow AI Platform Instanz.

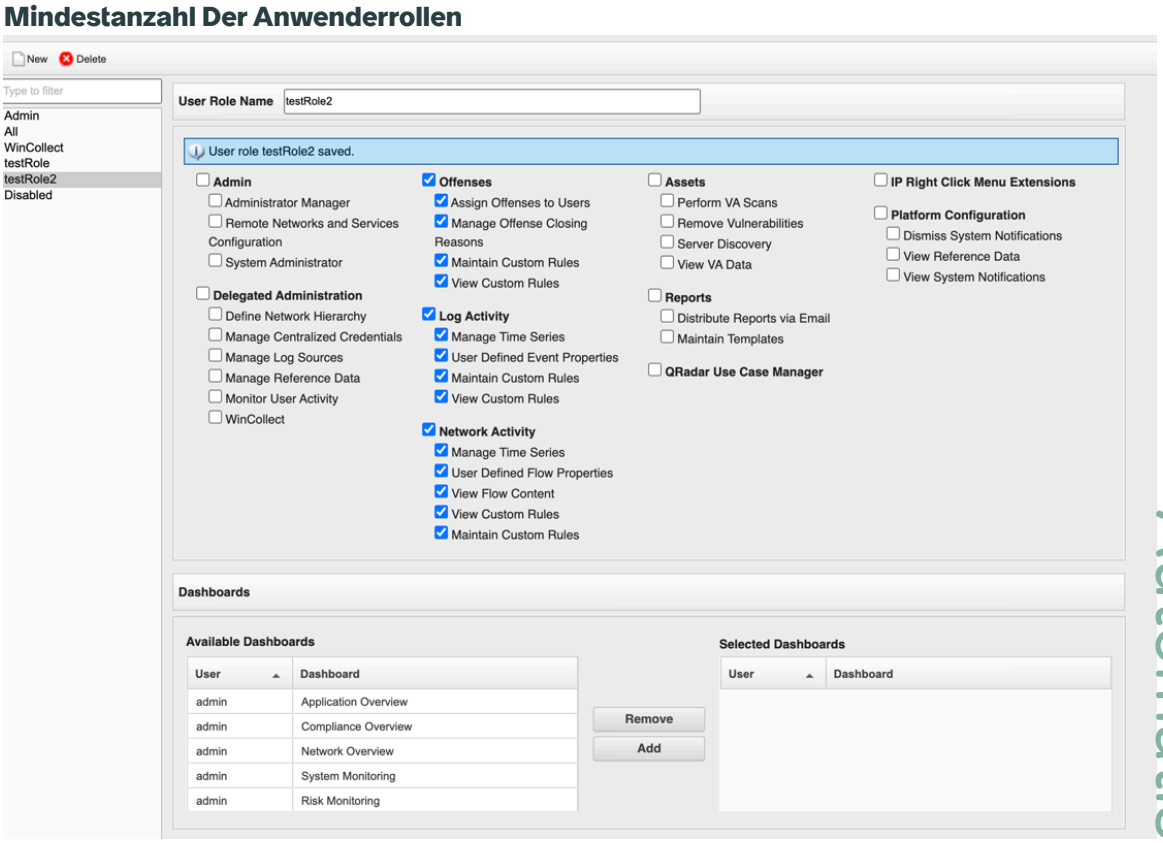
Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

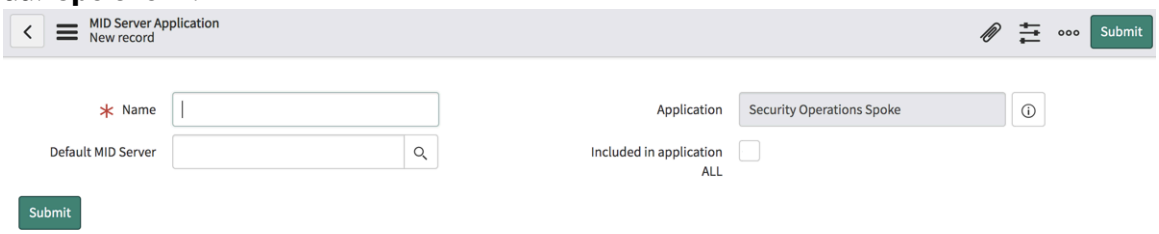
1. Wenn Sie den nicht installiert haben IBM QRadar Anwendung aus dem ServiceNow Store Informationen zur Integration finden Sie unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie IBM QRadar Kachel.
3. Klicken Sie auf , um die Anwendung zu konfigurieren **Neu** .
4. Alternativ, wenn ein **Konfigurieren** Die Schaltfläche wird auf einer Kachel angezeigt. Klicken Sie darauf, um eine vorhandene Konfiguration zu bearbeiten.
5. In **Konfiguration Der Verstoßerfassungen** Füllen Sie die Felder aus, das angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Gehen Sie wie folgt vor, um eine neue MID-Server-Anwendung zu erstellen:

- Navigieren zu **MID-Server** > **Anwendungen** Und klicken Sie auf **Neu** .
- Geben Sie einen Namen für die MID-Server-Anwendung ein, und wählen Sie einen MID-Server aus, der als Standard verwendet werden soll.
- Deaktivieren Sie das Kontrollkästchen in Anwendung ALLE enthalten, und klicken Sie auf **Speichern** .

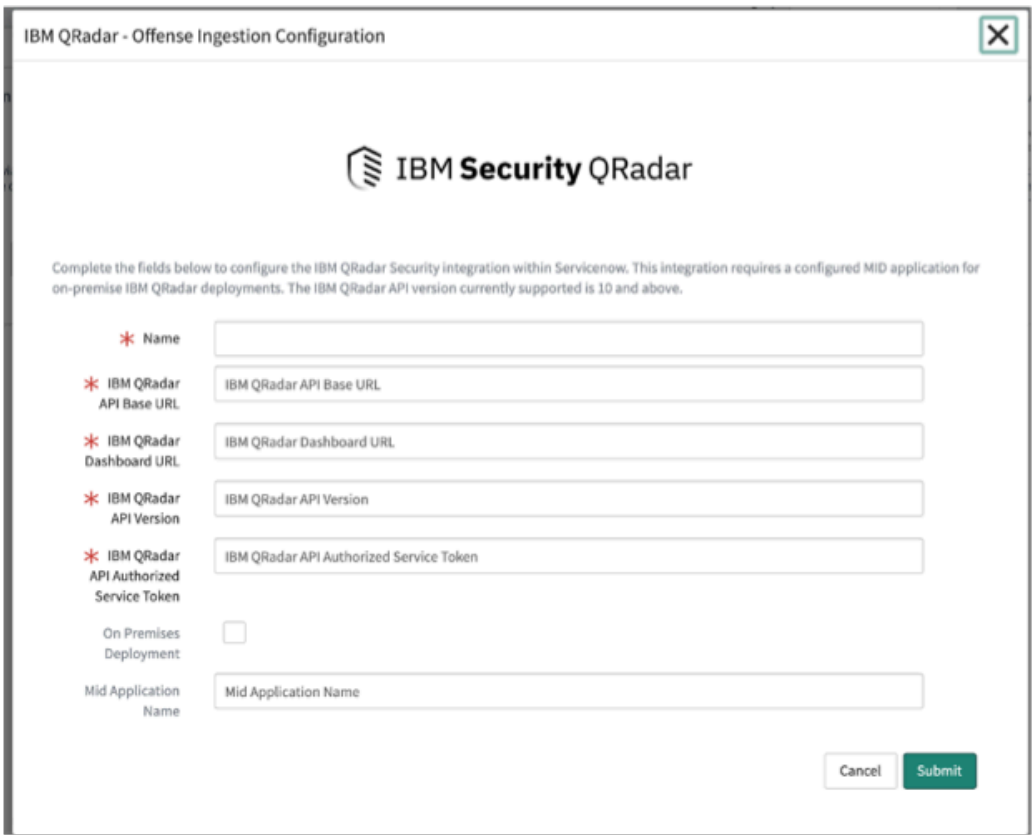


- Klicken Sie auf **Bearbeiten**. In **Bearbeiten Sie Mitglieder** Wählen Sie alle verfügbaren MID-Server aus, verschieben Sie sie in die Liste DER MID-Server, und klicken Sie auf **Speichern** . Je nach Verfügbarkeit wird einer der mit der MID-Serveranwendung konfigurierten MID-Server verwendet.

6. Geben Sie die Konfigurationsdetails ein, und geben Sie die von Ihnen erstellte MID-Server-Anwendung an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Quelle, die Sie in konfigurieren **Konfiguration der Erfassung von IBM QRadar-Vergehen** Formular kann für mehrere wiederverwendet werden ServiceNow AI Platform Profile, solange jedes Profil Verstöße erfasst.

7. Klicken Sie auf **Absenden**.
   Nachdem sie erfolgreich validiert und übermittelt wurde, jeweils IBM QRadar Die Serverkonfiguration wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, klicken Sie oben rechts auf der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja** .

Hinweis:
Wenn Probleme mit auftreten IBM QRadar Domänensegmentierungsfunktion, Kontakt IBM QRadar Kundensupport für Unterstützung.

Nächste Maßnahme
Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht darin, das Profil zu erstellen.

Richten Sie Ihr ein ServiceNow AI Platform® Instanz für IBM QRadar Integration der Verstoßerfassung

Im folgenden Abschnitt werden die Setup-Aufgaben aufgeführt, die Sie in ausführen müssen ServiceNow AI Platform® Instanz vor der Installation der Anwendung über ServiceNow Store.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Überprüfen Sie anhand der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform® Und Security Incident Response-Rollen (SIR).	Die folgenden Rollen sind für die Installation, das Setup und die Verwendung der Integration in erforderlich ServiceNow AI Platform® Instanz. • Ein Anwender mit ServiceNow AI Platform® Die Administratorrolle (admin) installiert die Anwendung aus dem ServiceNow Store Und weist die Rolle Security Incident-Administrator (sn_si.admin) zu. • Ein Anwender mit der Rolle „sn_si.admin“ überwacht die folgenden Aufgaben in ServiceNow AI Platform®: ◦ Namen, Erstellung und Bearbeitung von Verstoßprofilen. ◦ Auswahl und Zuordnung IBM QRadar Datenfelder für Vergehen in die Security Incident-Felder. ◦ Zeigt vor dem Abschluss der Konfiguration eine Vorschau der Security Incident-Details auf Richtigkeit an. ◦ Plant die laufende Erfassung von Straftaten. ◦ Aktiviert Updates für Verstöße, wenn ein SIR-Incident erstellt und geschlossen wird. ◦ Weist die Rolle Security Incident Analyst (sn_si.Analyst) zu. ◦ Anwender mit sn_si.Analyst arbeiten mit Security Incidents. Weitere Informationen zu Rollen und dem Zuweisen von Rollen an Anwender finden Sie unter Rollen im ServiceNow-Produktdokumentationswebsite .
Überprüfen Sie, ob Sie die folgenden Versionen verwenden: • IBM QRadar Version 7.3.2 oder höher. • IBM QRadar API-Version 10 oder höher. Frühere Versionen werden nicht unterstützt.	Wenn Sie Zugriff auf haben IBM QRadar Konsole haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein anderes spezielles Setup erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie eine MID-Serveranwendung installiert und konfiguriert haben.	Konfigurierte MID-Server-Anwendung. Ein MID-Server in Ihrem ServiceNow AI Platform® Instanz ist erforderlich, um eine Verbindung mit herzustellen IBM QRadar Service, wenn IBM QRadar Server wird in Ihrem Unternehmensnetzwerk bereitgestellt. Siehe ServiceNow-Produktdokumentationswebsite Für Informationen zu MID-Servern. Wenn Sie verwenden IBM QRadar Cloud-Service, ein MID-Server ist nicht erforderlich.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. **1.** Security Incident Response **2.** Ereignis- und Warnungserfassung für Security Operations: Diese Anwendung erfordert: ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit ○ Com.Glide.Hub.action_STEP.Rest => ServiceNow IntegrationHub Aktionsschritt – REST **Hinweis:** Die Integration Hub-Komponenten werden zusammen mit dem Plugin „Ereignis- und Warnungserfassung“ installiert. Wenn diese nicht installiert sind, wenden Sie sich an den Kundensupport, um Unterstützung zu erhalten. Weitere Informationen zur Installation von finden Sie Security Operations Kernanwendungen, siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

Nächste Maßnahme

Sie haben erfolgreich eingerichtet ServiceNow AI Platform® Instanz für die Integration. Der nächste Schritt besteht in der Installation von IBM QRadar Anwendung aus dem ServiceNow Store Für die Integration.

Erstellen Sie ein Profil für IBM QRadar Integration der Verstoßerfassung

Als Anwender mit der Rolle sn_si.admin erstellen Sie in ein Verstoßprofil ServiceNow AI Platform Instanz instand setzen und bestimmen, welche Vergehen Security Incidents erstellen. Vor ServiceNow AI Platform Security Incident Response(SIR) Security Incidents werden aus Vergehen erstellt, die Feldwerte aus Vergehen werden in einem Layout von angezeigt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow AI Platform Security Incident, damit Sie eine Vorschau anzeigen können, wie der tatsächliche Security Incident erstellt wird.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Aus Integrationsperspektive mithilfe verfügbarer APIs: IBM QRadar Straftaten werden automatisch in erfasst Security Operations Umgebung von ServiceNow AI Platform Instanz abhängig vom definierten Profiltyp. Die Integrations-Workflows erfassen verschiedene Arten von Straftaten, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese Straftaten werden basierend auf den Profilen erfasst, die Sie in konfigurieren Security Operations Umgebung Ihrer Instanz. Alle Vergehen werden anfänglich für einen konfigurierten Verstoßtyp in einem Profil erfasst. Erfasste Straftaten können dann weiter gefiltert werden, um anzugeben, welche Straftaten Security Incidents verursachen. Sie können beispielsweise Filter bevorzugen, die Security Incidents nur für Straftaten erstellen, die als hohes Risiko identifiziert werden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Vergehen erstellt, werden einzelne Feldwerte zu den Vergehen den entsprechenden Feldern in einem Layout von Security Incidents für eine Vorschau zugeordnet.

Namen für die Verstoßprofile in Ihrem ServiceNow AI Platform Instanz muss eindeutig sein. Sie können mehrere Konfigurationen für mehrere Quellen erstellen und auch mehrere Profile für eine einzelne Quelle erstellen.

Erstellen Sie Profile für die Erfassung IBM QRadar Vergehen

Sie können ein Profil einrichten, um Verstöße zu erfassen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Um ein Profil für eine Straftat in zu erstellen ServiceNow AI Platform Instanz, navigieren Sie zu **Integration mit IBM QRadar** > **IBM QRadar-Profil**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

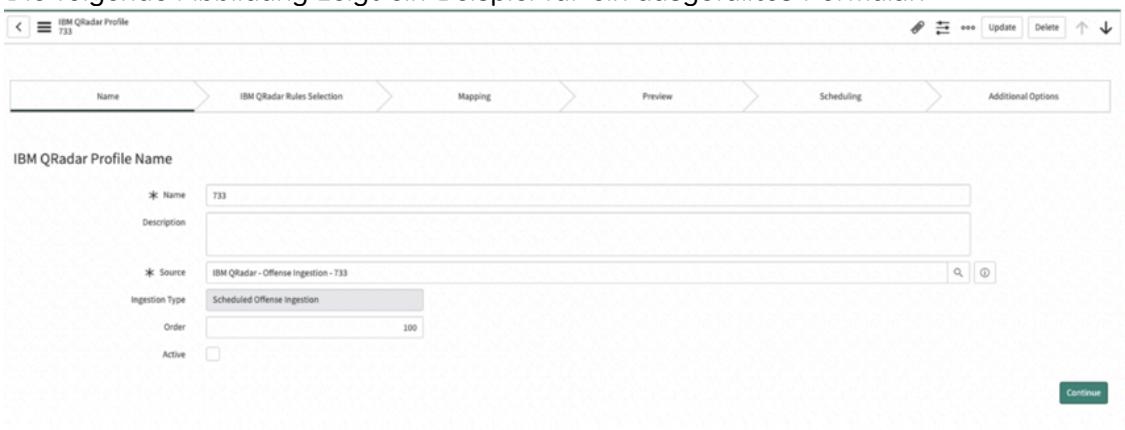
   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

Feld	Beschreibung
Name	Eindeutiger Name für das Profil. Wenn Namen nicht eindeutig sind, wird ein Fehler angezeigt, und doppelte Profilnamen werden nicht gespeichert. Profilnamen in Ihrem ServiceNow AI Platform Instanz muss eindeutig sein.
Aktiv	Das Kontrollkästchen ist standardmäßig deaktiviert. Wenn diese Option deaktiviert ist, ist das Profil nicht aktiv, und die Erfassung findet nicht statt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Sie sollten alle Abschnitte im Profil abschließen, bevor Sie es aktivieren.
Quelle	Die IBM QRadar Server, den Sie für die Erfassung von Straftaten konfiguriert haben. Wenn Sie mehrere haben IBM QRadar Server konfiguriert. Wählen Sie den entsprechenden Server für die Verstoßtypen aus, die für das Profil erfasst werden. Sie müssen einen Wert eingeben.
Reihenfolge	Der Standardwert ist 100. Wenn Sie mehrere Profile erstellt haben, gibt dieser Wert eine Laufzeitausführungspriorität an, wenn zwei oder mehr Profile dieselben Auslösebedingungen haben. Der Workflow im Profil mit der niedrigsten Zahl hat die höchste Priorität.
(Optional) Beschreibung	Zusätzlicher Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.



Nächste Maßnahme

Der nächste Schritt besteht darin, die Vergehen für die Erfassung auszuwählen.

Wählen Sie Aus IBM QRadar Regeln

Basierend auf IBM QRadar Quelle: Wählen Sie eine oder mehrere aus IBM QRadar Regeln für das Profil.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die verfügbaren an IBM QRadar Regeln in Ihrem ServiceNow AI Platform Instanz, damit Sie die aktiven kennen IBM QRadar Regeln, für die Sie Security Incidents erfassen und erstellen möchten.

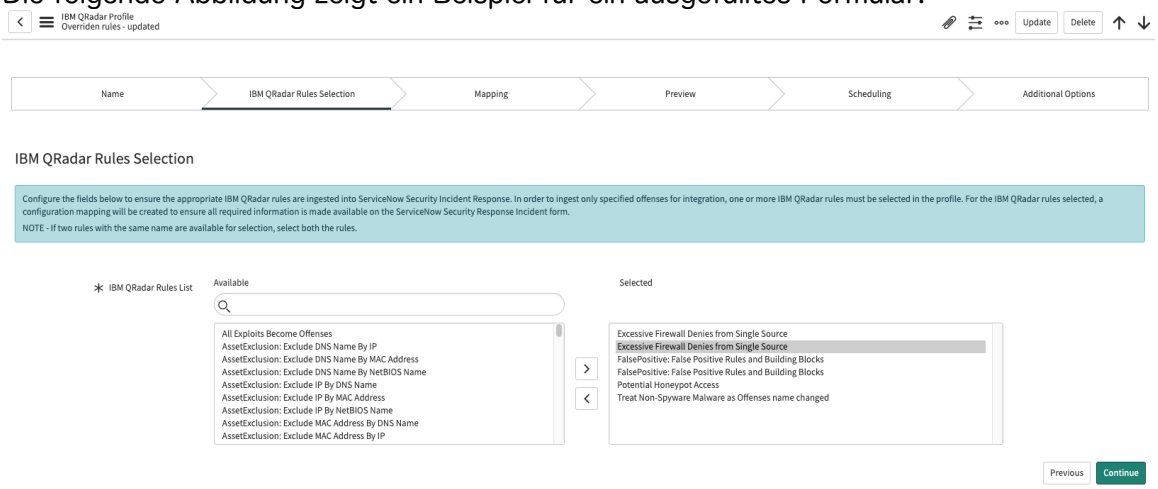
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In IBM QRadar, Sie können Regeln anhand ihrer Herkunft als System-, Überschreibungsregeln und Anwenderregeln identifizieren. Standardmäßig ist der Ursprung einer Regel mit einer Systemregel verknüpft. Wenn Sie eine Systemregel in ändern IBM QRadar, Der Ursprung ist auf Überschreiben festgelegt.

Klicken Sie auf die Liste im IBM QRadar Regellistenfeld. Eine Liste der aktiven IBM QRadar Regeln, die in vorhanden sind IBM QRadar Konsole wird angezeigt. Wählen Sie eine oder mehrere Regeln aus der Liste aus, und verschieben Sie sie in **Ausgewählt** Spalte. Von mindestens einem der ausgelösten Vergehen IBM QRadar Ausgewählte Regeln werden in diesem Profil erfasst.

Regeln mit demselben Namen : In ServiceNow AI Platform Instanz wird eine Liste aktiver oder aktivierter Regeln angezeigt. Wenn Sie eine aktive oder aktivierte Systemregel in ändern IBM QRadar, Eine neue Überschreibungsregel wird erstellt. Dies führt dazu, dass zwei Regeln mit demselben Namen in angezeigt werden ServiceNow AI Platform. Wenn dieses Szenario auftritt, wählen Sie beide Regeln aus, um Security Incidents zu erfassen und zu erstellen.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular:



Klicken Sie Auf **Fahren Sie Fort** Um mit dem nächsten Schritt im Assistenten fortzufahren.

Zuordnung von Verstoßfeldern für IBM QRadar Integration

Nachdem Sie die Regeln ausgewählt haben, besteht der nächste Schritt darin, den Feldern im Security Incident-Formular Vergehen, Ereignis oder Flow zuzuordnen.

Übersicht

Für den Zuordnungsschritt müssen Sie zuerst Beispielvergehen für mindestens ein ausgewähltes Element erfassen IBM QRadar Regeln. Dann müssen Sie sicherstellen, dass alle relevanten Felddaten zu Straftaten dem entsprechenden Ort in zugeordnet sind SIR Incident-Formular und visualisieren Sie dann SIR Incident im Vorschauabschnitt.

Die Zuordnung der Beispielvergehen-Felder umfasst Folgendes:

- Beispieldaten werden abgerufen und ausgefüllt: Siehe Das Beispiel wird erfasst IBM QRadar Vergehen.
- Zuordnung der Verstoßfelder zum Security Incident: Siehe Zuordnung IBM QRadar Verstoßfelder zu Security Incident Response-Feldern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Beispiel wird erfasst IBM QRadar Vergehen

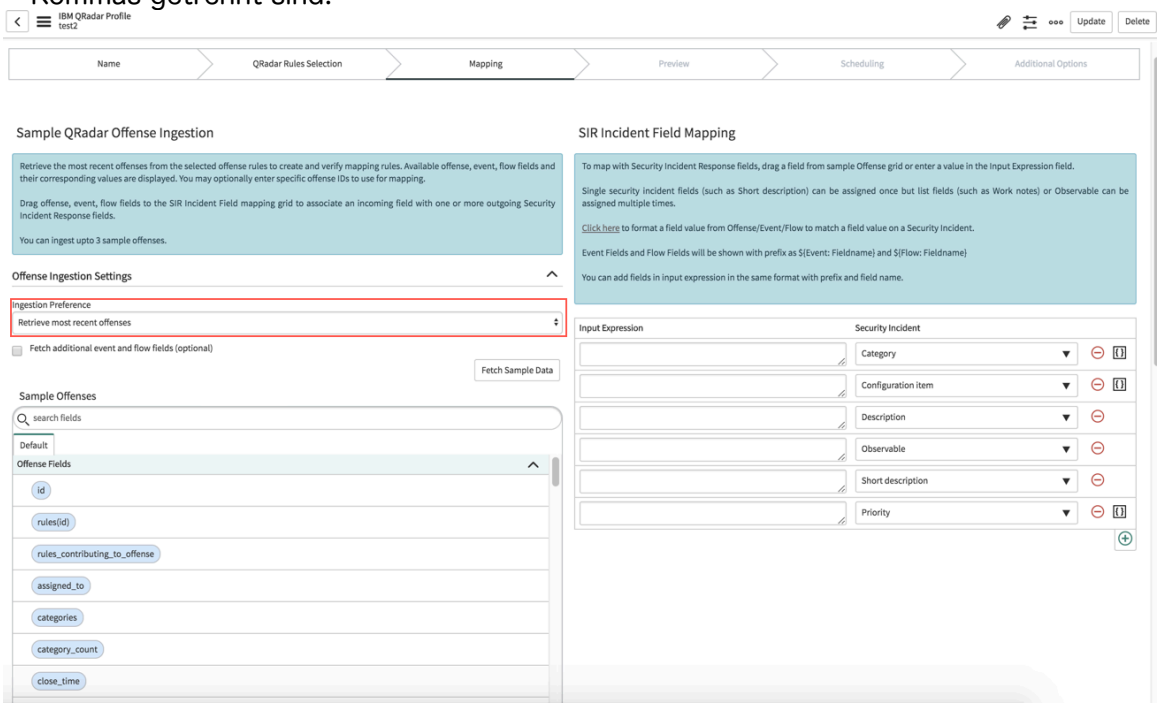
Sie können Beispielvergehen für eine oder mehrere ausgewählte Fälle erfassen IBM QRadar Regeln.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie auf **Zuordnung** Auf der Fortschrittsleiste.
2. Sie können entweder die drei neuesten Beispielvergehen abrufen oder die eindeutigen Vergehen-IDs für die spezifischen Straftaten angeben, die Sie für Ihre Zuordnungs-Experience verwenden möchten.
   Von **Erfassungseinstellung** Auswahlliste wählen Sie eine der folgenden Optionen aus:
   - Letzte Vergehen abrufen: Die drei letzten Vergehen für die ausgewählten Regeln werden abgerufen.
   - Straftaten basierend auf Straftaten-ID auswählen: Geben Sie die Straftat-ID für die abzurufenden Straftaten an. Sie können maximal 3 Vergehen-IDs angeben, die durch Kommas getrennt sind.



3. Klicken Sie Auf **Rufen Sie Beispieldaten Ab** Dient zum Abrufen der neuesten Beispielvergehen-Daten aus dem IBM QRadar Konsole für die ausgewählten Verstoßregeln.

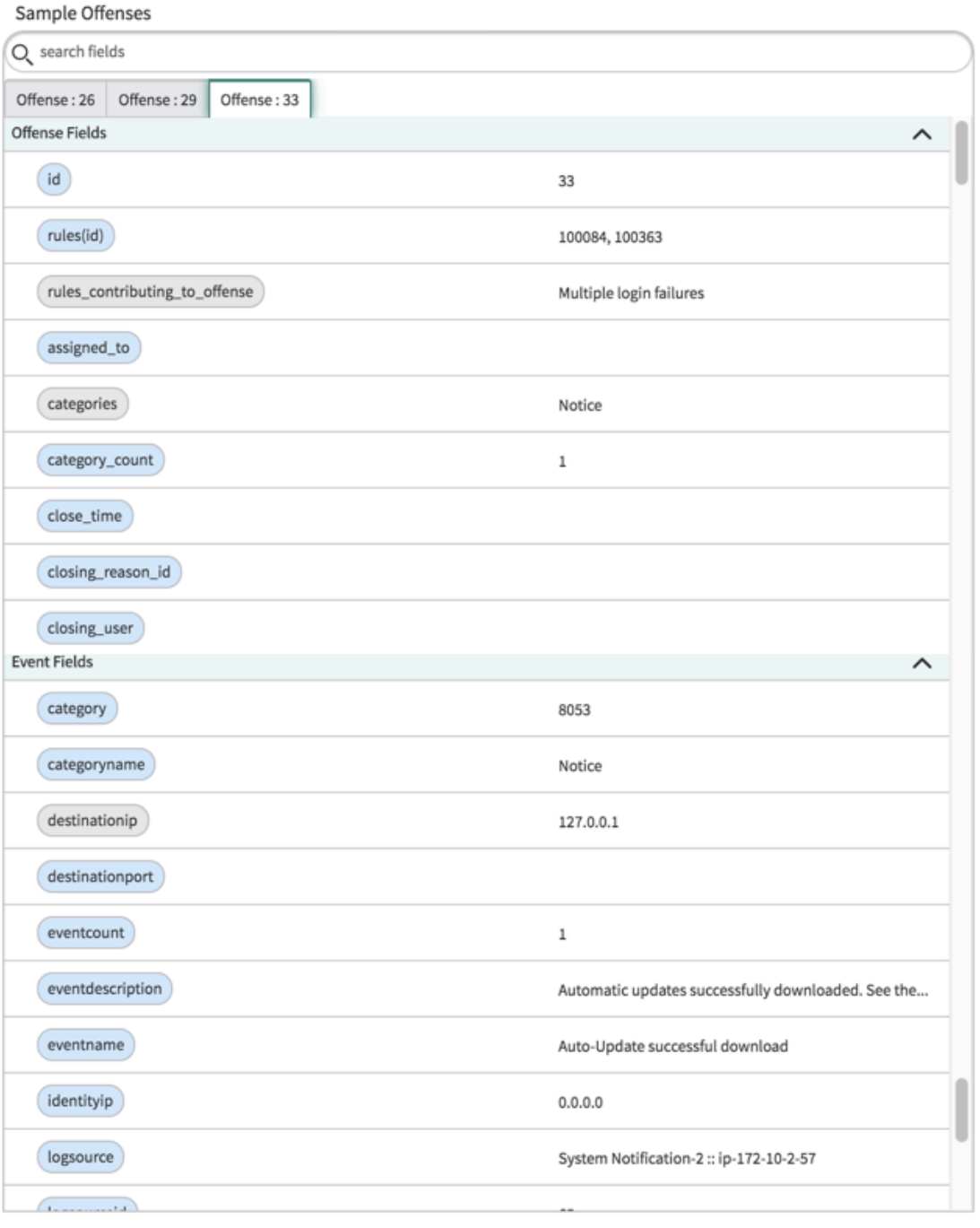
   Die Ergebnisse der Verstoßfelder und Werte werden als einzelne Registerkarten angezeigt. Eine Straftat kann durch drei Arten von Regeln ausgelöst werden:
   - Ereignis: In dieser Regel werden Ereignisprotokolle überprüft, und wenn die angegebenen Kriterien erfüllt sind, wird ein Verstoß erstellt.
   - Flow: Netzwerkdaten und -Datenverkehr werden überprüft, und wenn bestimmte Bedingungen erfüllt sind, wird eine Straftat erstellt.
   - Allgemein: In diesem Fall können Sie Bedingungen für Ereignisse oder Flows angeben, wobei entweder oder beide Bedingungen erfüllt sind, wird eine Straftat erstellt.

   Der Abruf für Beispielvergehen kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt. Abhängig von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Regel oder den Regeln, die den Verstoß ausgelöst haben, werden die Ereignis- oder Flow-Felder zusammen mit den Verstoßfeldern wie in der folgenden Abbildung dargestellt ausgefüllt:



Hinweis:
Die angezeigten Ereignis- oder Flow-Felder gehören zum ersten Ereignis- oder Flow-Feld, das den Verstoß basierend auf dem entsprechenden Ereignis oder Flow-Regel ausgelöst hat.

4. Im Folgenden sind anwenderdefinierte Vergehen-Felder aufgeführt, die für diese Integration erstellt wurden. Neben diesen anwenderdefinierten Feldern sind Felder für Standardvergehen für die Zuordnung verfügbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

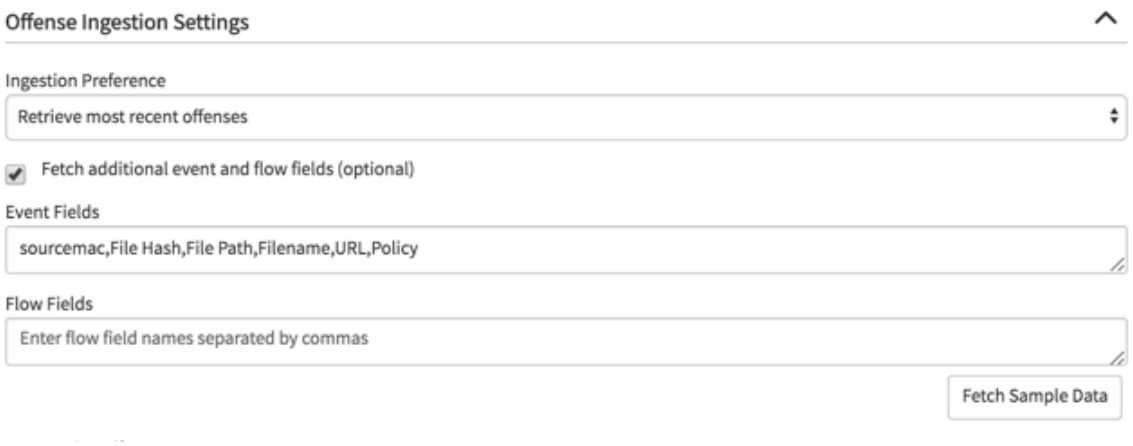
- Rules_Contributing_to_offense: IBM QRadar Regeln, die basierend auf der Regel-ID zur Vergehen beigetragen haben.
- Anwender: Anwendernamen für die Straftat
- Remote_destination_ip: Die Remote-Ziel-IPs für die Straftat.

  Basierend auf den lokalen Ziel-IDs für die Straftat sind die folgenden anwenderdefinierten lokalen Zieladressfelder verfügbar:
  - Local_destination_address (Domain_ID)
  - Local_destination_address (event_Flow_count)
  - Local_destination_address (first_event_Flow_seen)
  - Local_destination_address (ID)
  - LOCAL_destination_address (Last_event_Flow_seen)
  - Local_destination_address (local_destination_address_IDs)
  - Local_destination_address (Größe)
  - Local_destination_address (Netzwerk)
  - Local_destination_address (offense_IDs)
  - Local_destination_address (local_destination_ip)

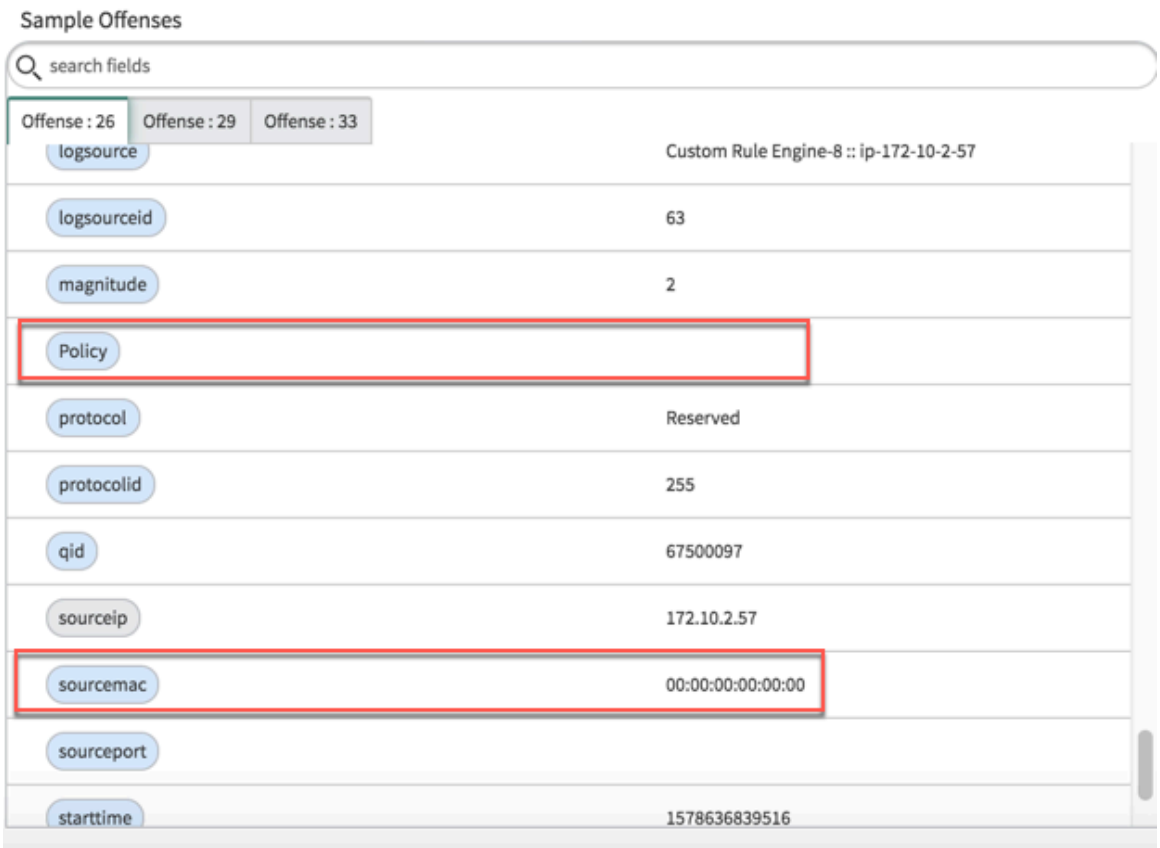
- Die folgenden Quelladressen sind basierend auf den Quell-IDs der Straftat verfügbar:
  - Source_ADDRESS (Domain_ID)
  - Source_ADDRESS (event_Flow_count)
  - Source_ADDRESS (first_event_Flow_seen)
  - Source_ADDRESS (ID)
  - Source_ADDRESS (Last_event_Flow_seen)
  - Source_ADDRESS (Source_address_IDs)
  - Source_address (Größe)
  - Source_address (Netzwerk)
  - Source_ADDRESS (offense_IDs)
  - Source_ADDRESS (Source_ip)

Wählen Sie aus **Zusätzliche Ereignis- und Flow-Felder abrufen (optional)** Kontrollkästchen. Sie können Beispielereignis- und Flow-Daten aus allen aktiven, gültigen anwenderdefinierten Ereignis- und Flow-Feldern abrufen. Geben Sie die anwenderdefinierten Felder durch Kommas getrennt an, wie unten gezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

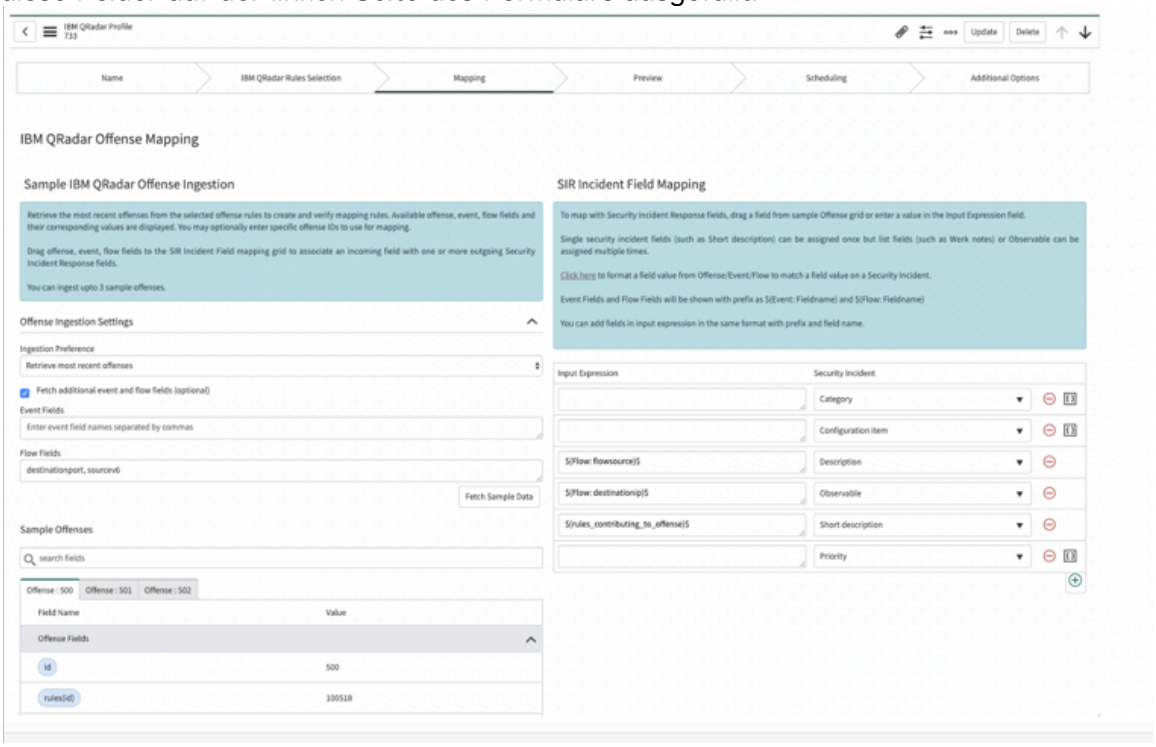


Klicken Sie Auf **Rufen Sie Beispieldaten Ab** . Die angegebenen Ereignis- oder Flow-Felder werden zusammen mit ihren Werten (falls verfügbar) wie unten gezeigt an den Abschnitt „Ereignis“ oder „Flow“ angehängt:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie die Beispieldaten abgerufen haben, werden die entsprechenden Werte für diese Felder auf der linken Seite des Formulars ausgefüllt.



Nächste Maßnahme
Nachdem Sie die Beispieldaten abgerufen haben, ordnen Sie die Verstoßfelder dem Security Incident zu.

Zuordnung IBM QRadar Verstoßfelder zu Security Incident Response-Feldern

Ordnen Sie einzelne Vergehen-, Ereignis- und Flow-Felder Feldern Feldern in einem zu ServiceNow AI Platform SIR Security Incident.

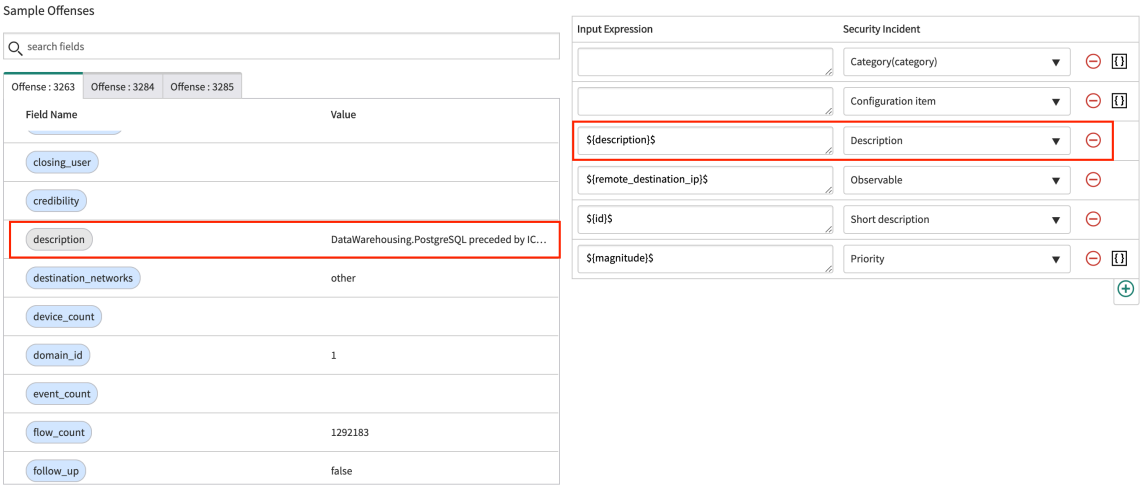
Zuordnung des Verstoßfelds

Verwenden Sie als Anwender mit der Rolle „sn_si.admin“ die Felder aus dem Abschnitt „Beispielvergehen“ auf der linken Seite, und ordnen Sie sie den Security Incident-Feldern in der Spalte „SIR-Incident-Feldzuordnung“ zu. Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Vergehen-, Ereignis- oder Flow-Felder von der linken Seite ziehen und auf dem ablegen ServiceNow SIR Incident-Zuordnungsabschnitt auf der rechten Seite. Die Zuordnung auf der rechten Seite ordnet das Feld „eingehender Verstoß“ einem Feld „ausgehender Security Incident“ zu.

1. Nachdem Sie die Beispieldaten abgerufen haben, ordnen Sie die Felder „Verstoß“, „Ereignis“ oder „Flow“ dem Security Incident zu. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf der linken Seite des Formulars auf einen blauen Feldnamen.
2. Ziehen Sie den Feldnamen, z. B. Beschreibung , Und legen Sie es in einem Feld in der Spalte „Eingabeausdruck“ neben einem Feldnamen in der Spalte „Security Incident“ ab.

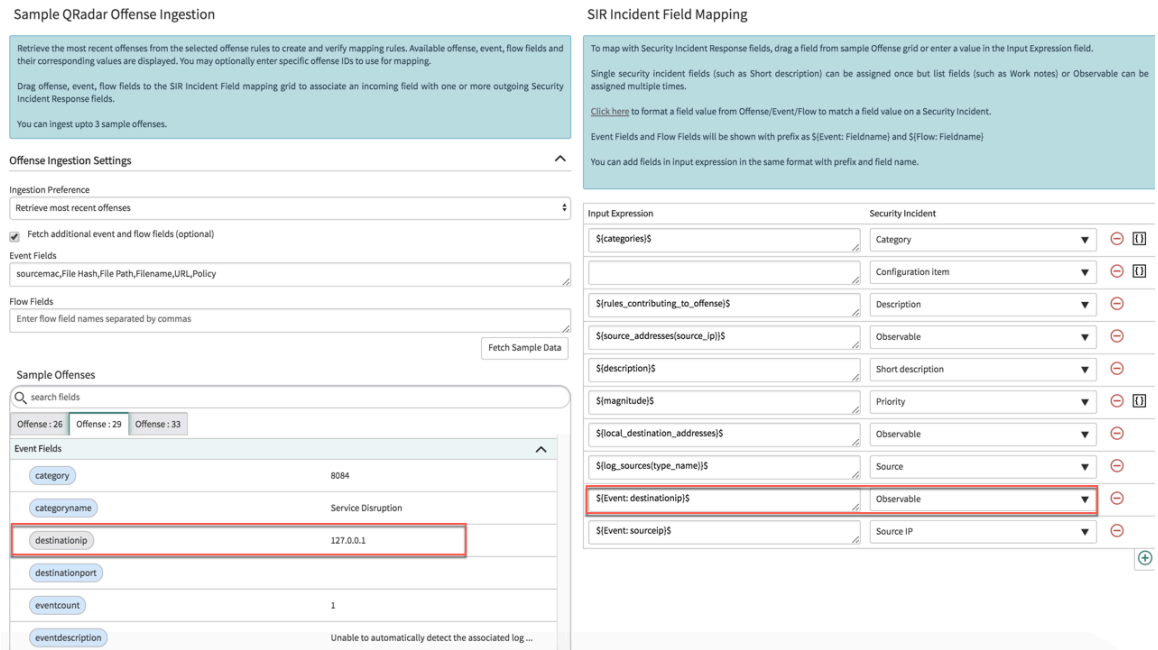
   Der Feldwert wird in der Spalte „Eingabeausdruck“ angezeigt. In der folgenden Abbildung: Beschreibung Ist dem zugeordnet Beschreibung Feld im Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:

Wenn Sie den Namen des Ereignis- oder Flow-Felds im Abschnitt „Eingabeausdruck“ manuell eingeben, müssen Sie ein Präfix als hinzufügen `${Event:eventfield}$` Oder `${Flow:Flowfield}$` Vor dem Namen des zugeordneten Felds.



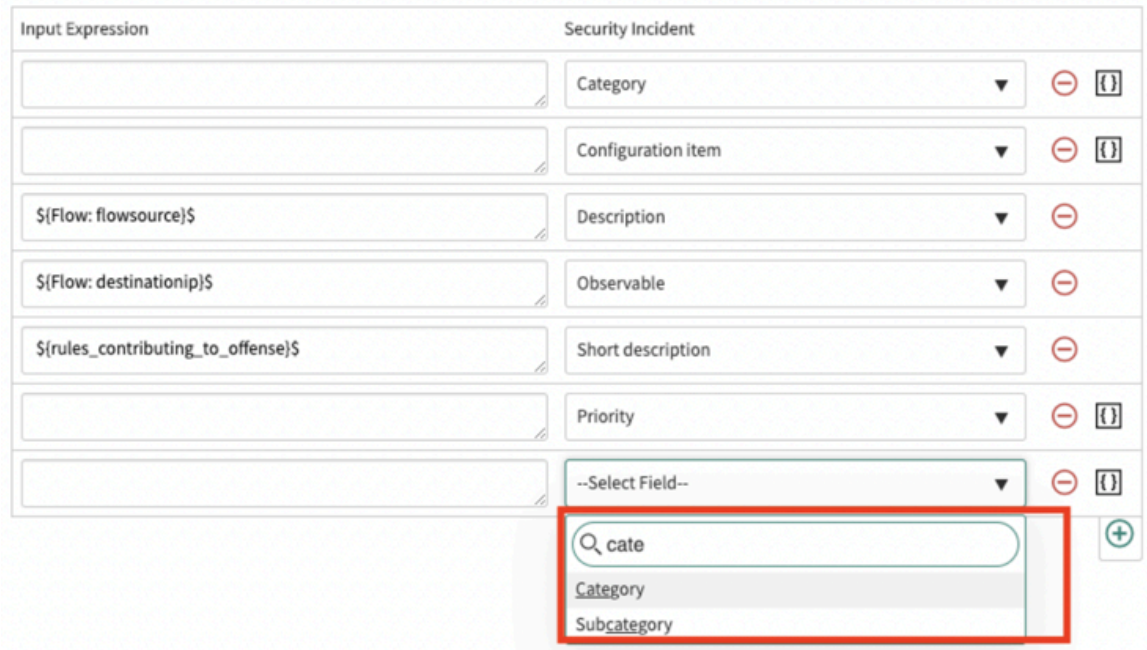
Damit Sie sicherstellen können, dass im Zuordnungsprozess keine Vergehen-, Ereignis- oder Flow-Felder übersehen oder dupliziert werden, sind Felder farbcodiert. Die Farbcodierung der Verstoßfelder hilft Ihnen, die Verstoßwerte nachzuverfolgen, die Sie bereits zugeordnet haben, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder blau angezeigt werden. Dies hilft Ihnen, besser zu visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Verstoßinformationen nicht zugeordnet sind.

Hellblaue Felder auf der linken Seite zeigen an, dass ein Verstoßfeld noch nicht ausgewählt und dem Security Incident zugeordnet ist. Möglicherweise möchten Sie ein eingehendes Vergehen-, Ereignis- oder Flow-Feld mit mehr als einem Feld in einem Security Incident verknüpfen. Ein graues Feld gibt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen:
   a. Klicken Sie auf der rechten Seite des Formulars im Abschnitt „SIR-Incident-Feldzuordnung“ unten im Raster auf das Plus-Symbol (+). Ein neues Feld wird angezeigt.
   b. Erweitern Sie in der Spalte Security Incident die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

      In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung hat Kategorie einen grauen Hintergrund, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Verstoßfelder auf der linken Seite des Formulars hilft diese Farbcodierung für die Security Incident-Felder auf der rechten Seite Ihnen, die bereits zugeordneten SIR-Incident-Felder nachzuverfolgen.



Hinweis:
Da mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „erkennbares Element“ mehrmals verschiedenen Werten zugeordnet werden. Ebenso unterstützen die Felder „Konfigurationselement“ und „Arbeitsnotizen“ mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

   c. Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.
   d. Wählen Sie auf der linken Seite des Formulars das Feld Verstoß aus, und ziehen Sie es per Drag-and-Drop in ein entsprechendes Security Incident-Feld auf der rechten Seite.
4. Entfernen Sie Felder, indem Sie das Symbol „ –“ neben dem Feldnamen im Abschnitt „SIR-Incident-Feldzuordnung“ verwenden.
5. Fahren Sie mit der Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder entfernen.

Verstoßfelder mit mehreren Werten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Security Incident-Felder wie **Kategorie** Und **Anwender** Felder (z. B. Betroffener Anwender, Zugewiesen an), die mit dem Basisprodukt verfügbar sind, unterstützen nicht mehrere Werte.
- Folgendes IBM QRadar Felder unterstützen mehrere Werte:
  - *Kategorien*
  - *Target_Networks*
  - *Source_address_IDs*
  - *LOCAL_destination_address_IDs*
  - *Remote_destination_ips*
  - *Rules_Contributing_to_offense*
  - *Anwender*

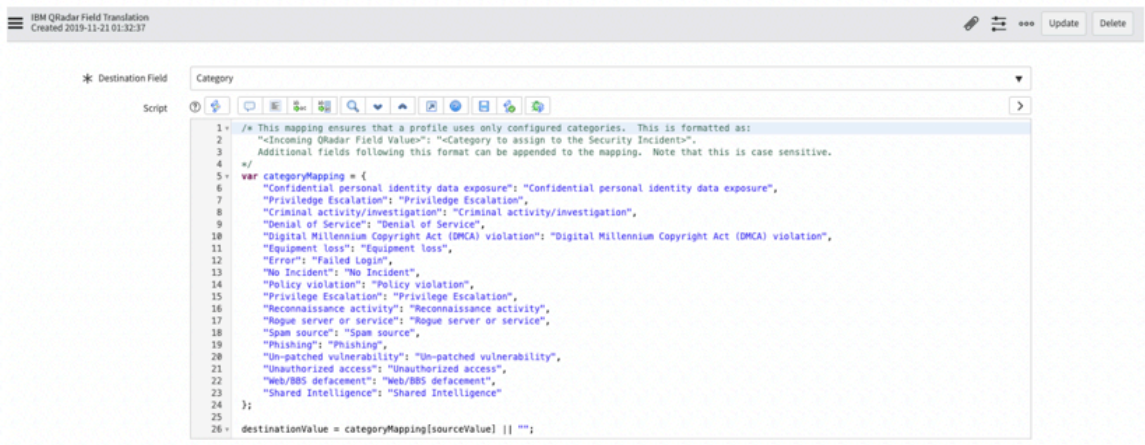
  Wenn Sie die obigen Felder einem zuordnen müssen Security Incident Response Neben CI- und erkennbaren Feldern müssen Sie neue Felder erstellen Security Incident Response Felder vom Typ **Liste** Und verwenden Sie sie für die Zuordnung.

Hinweis:
Standardmäßig nur nicht-Referenz **Liste** Typfelder werden unterstützt.

Formatierungsfeldübersetzung

In bestimmten Fällen werden Feldwerte für Verstoß in angegeben IBM QRadar Kann nicht direkt in die Felder des SIR Security Incident übersetzt werden. Für diese Werte können Sie einen Skripteditor verwenden, um Feldwerte für den Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind. Beispielsweise kann ein Kategoriewert von Malware-Warnung und Virusinfektion mit dem Skript-Editor verschiedene Feldwerte für die Quellkategorie haben, aber beide Werte können mithilfe der Funktionalität Formatierungsfeldübersetzung in eine allgemeine schädliche Code-Aktivität im Feld Kategorie des SIR Security Incident übersetzt werden.

Um den Skript-Editor zu verwenden, klicken Sie auf {{}}. Der Skripteditor wird angezeigt.



Geben Sie alle Änderungen am Skript ein, und klicken Sie auf **Aktualisieren** Um die Änderungen zu speichern und zur Zuordnungsseite zurückzukehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingungen für die Incident-Generierung

Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, damit Sie angeben können, welche Verstöße Security Incidents erstellen sollen und welche Verstöße herausgefiltert werden sollen, z. B. Verstöße mit niedriger Priorität. Sie können dieselben Feldwerte im Generator für Incident-Generierungsbedingungen verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Straftat erfüllen muss, um einen Security Incident zu erstellen. Um Bedingungen für die Incident-Generierung festzulegen, gehen Sie wie folgt vor.

1. Scrollen Sie zu **Bedingungen Für Die Incident-Generierung** Abschnitt im Formular, und wählen Sie aus **Filtern Sie basierend auf Bedingungen** Kontrollkästchen zum Aktivieren der Option.

   Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den spezifischen Bedingungen entsprechen, die in den Feldern beschrieben werden.

   Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen stimmen mit den Feldern überein, die im Abschnitt „QRadar-Vergehen-Erfassung“ für die von Ihnen erfassten Vergehen angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach den Vergehen, die Sie erfassen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden und müssen genau mit den Werten von übereinstimmen IBM QRadar Vergehen. Wenn Sie sich nicht sicher sind, welche Werte in die Filterfelder eingegeben werden sollen, kehren Sie möglicherweise zu zurück IBM QRadar Konsole und überprüfen Sie Ihre Verstöße auf die Stichwörter.

   Hinweis:
   Die `Kategorien` , `Target_Networks` , `Source_address_IDs` , `LOCAL_destination_address_IDs` , `Remote_destination_ips` , `Rules_Contributing_to_offense` , Und `Anwender` Verstoßfelder können mehrere Werte haben (da die Werte in Arrays gespeichert werden). Da die Filterbedingung nur Zeichenfolgen abrufen kann, müssen Sie verwenden `Enthält` Filterbedingung für diese Felder, um sicherzustellen, dass die Daten korrekt gefiltert werden.

2. Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** Oder **ODER** .
   - Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden.
4. (Optional) Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

   Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt werden müssen, bevor Security Incidents erstellt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die Bedingungen für die Incident-Generierung so festgelegt, dass Security Incidents nur erstellt werden, wenn beide von Ihnen eingegebenen Filterbedingungen erfüllt sind.

Diese Art der Bedingungsfilterung für die Incident-Generierung hilft Ihnen, die Verstöße einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegende Regel oder Filter in zu ändern IBM QRadar. Wenn zusätzliche Filterkriterien festgelegt sind, werden Incidents nur Vergehen zugeordnet, die allen Kriterien entsprechen.

Hinweis:
Wenn eines der Verstoßfeldnamen Sonderzeichen wie Anführungszeichen (“), Bindestriche (‘), Unterstriche (-) oder Ampersand (@) enthält, müssen diese Zeichen möglicherweise zu Filterzwecken ersetzt werden, es wird jedoch ein numerisches Suffix angehängt, um Felder mit doppelten Verstoßnamen zu unterscheiden. Beispiel: Wenn das Feld erster Verstoß lautet `Warnungen.Warnung` Und das zweite Vergehen-Feld ist `Warnungen@Warnungen` , Diese Felder können nicht eindeutig identifiziert werden, da die verbleibenden Standardtextzeichen identisch sind. In diesem Fall wird dem zweiten Verstoßfeld ein Suffix hinzugefügt, und das Feld wird in umbenannt `Warnungen@Alert(1)` Wenn in der Liste Filterbedingungen angezeigt.

Zusammenfassungskriterien für Straftaten, um ähnliche Straftaten zu behandeln und doppelte Incidents zu verhindern

Definieren Sie zusätzliche Zusammenfassungskriterien für Straftaten, die eine eingehende Straftat zu einem vorhandenen SIR Security Incident aggregieren, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Mithilfe von Feldübereinstimmungswertkriterien für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl aktiver, sich überschneidender Security Incidents reduzieren, indem alle zugehörigen Verstoßdaten in einem einzelnen Security Incident platziert werden. Um die Kriterien festzulegen, führen Sie die folgenden Schritte aus:

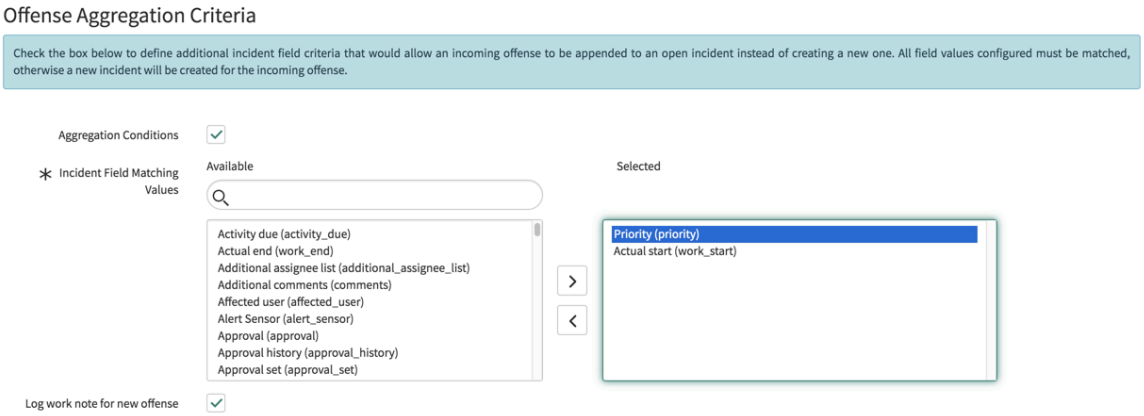
1. Scrollen Sie im Formular zum Abschnitt „Aggregationskriterien für Straftaten“, und wählen Sie aus **Zusammenfassungsbedingungen** Kontrollkästchen zum Aktivieren dieser Option.

   Die Spalten „Incident-Feld-Übereinstimmungswerte“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die in konfiguriert sind SIR Security Incident.

2. Wählen Sie in der Liste verfügbar die Feldwerte aus, die Sie für vorhandene Security Incidents in abgleichen möchten ServiceNow AI Platform Und verschieben Sie sie in die Liste ausgewählt.

   Alle von Ihnen ausgewählten Feldwerte müssen abgeglichen werden, um diese eingehende Warnung an einen vorhandenen Security Incident anzuhängen. Dies umfasst Felder, z. B. erkennbare Elemente und Konfigurationselemente, denen mehrere Vergehen-Feldwerte zugeordnet sein können. Alle Werte müssen übereinstimmen. Wenn nur eine Teilmenge der Werte übereinstimmt, werden die Aggregationsbedingungen für Straftaten nicht erfüllt, und ein neuer Security Incident wird erstellt. Siehe Screenshot unten für die Feldzuordnung mit mehreren Werten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn eine neue Straftat allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird die neue Straftat automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Anwender mit der Rolle „sn_si.Analyst“, der mit Security Incidents arbeitet, können Sie alle hinzugefügten aggregierten Verstöße in einer zugehörigen Liste zu einem Security Incident anzeigen. Diese Liste enthält Details zu zugehörigen Zeitstempeln und zusammengefassten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum diese Verstöße zu vorhandenen Security Incidents zusammengefasst werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie unter zugehörige Links zur linken Seite des Datensatzes, und klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Link.

3. (Optional) um eine Arbeitsnotiz für eine neue Straftat zu protokollieren, die kürzlich zum Security Incident hinzugefügt wurde, aktivieren Sie das Kontrollkästchen, um diese Option zu aktivieren. In der Arbeitsnotiz wird protokolliert, dass eine neue Straftat hinzugefügt wurde, zusammen mit einem Link zu den Verstoßdetails und allen anderen Details, die dem Feld „Arbeitsnotiz“ in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

   Sie haben erfolgreich Werte aus einem zugeordnet IBM QRadar Verstoß gegen Felder in einem Security Incident. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung einzuschränken. Sie haben auch Vergehen an vorhandene Security Incidents angehängt, wenn die Feldwerte des Verstoßes den konfigurierten Zusammenfassungskriterien entsprechen.

4. Klicken Sie Auf **Fahren Sie Fort** Um mit der Profilkonfiguration fortzufahren. Der nächste Schritt besteht darin, eine Vorschau der Felder anzuzeigen, die Sie einem zugeordnet haben SIR Security Incident

Vorschau des Security Incidents anzeigen

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem zugeordnet haben SIR Security Incident. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Verstoßfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

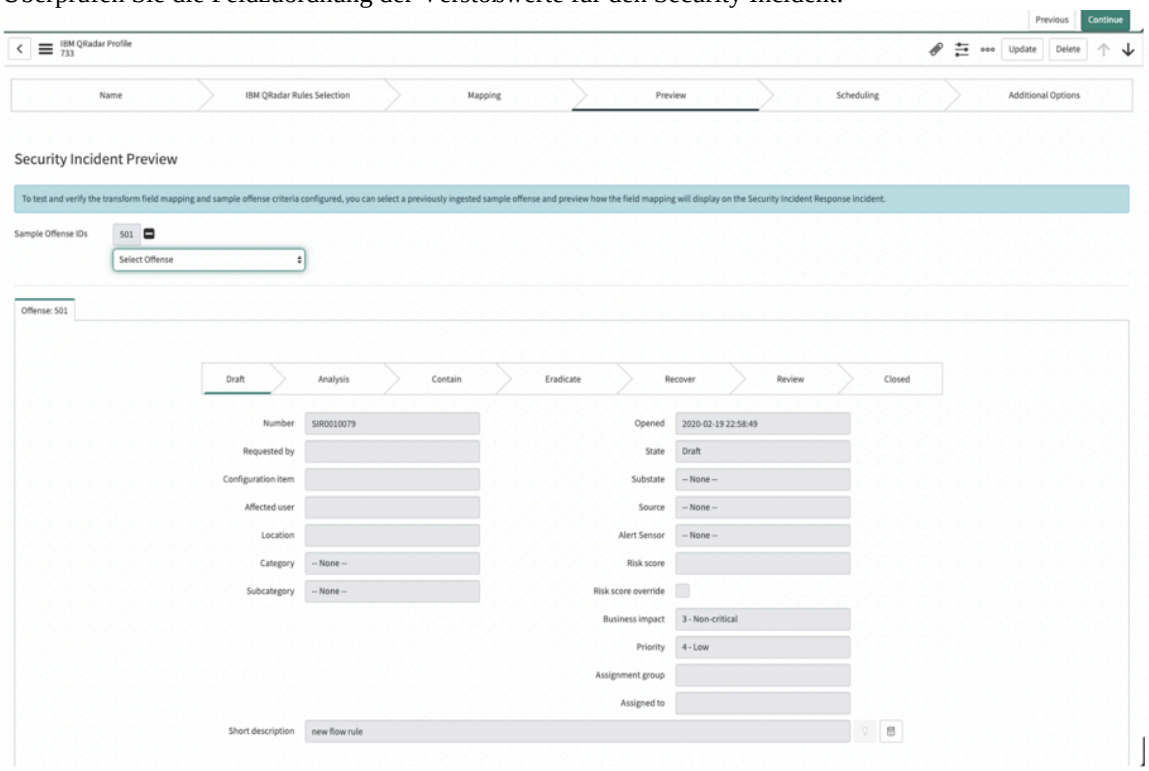
Als Anwender mit der Rolle „sn_si.admin“ können Sie eine Vorschau eines Security Incidents anzeigen und die Zuordnung nach Bedarf erneut bearbeiten, um Felder mit Fehlern zu beheben oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

abgeschlossen wurde, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen von SIR Security Incidents werden nicht als tatsächliche Incidents in gespeichert Security Incident Response Produkt.

Prozedur

1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie auf **Vorschau** In der Fortschrittsleiste.
2. Wählen Sie in der Auswahlliste Beispiel-IDs für Straftaten ein Element aus.
   Der Security Incident wird angezeigt. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.
3. Überprüfen Sie die Feldzuordnung der Verstoßwerte für den Security Incident.



Das vorherige Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler der erfassten Beispiele.

4. Klicken Sie auf, um diesen Fehler zu beheben **Zuordnung** In der Fortschrittsleiste.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie erneut eine Vorschau der Zuordnung an, und beheben Sie alle Fehler, die in Fehlermeldungen beschrieben werden.

Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind, besteht der nächste Schritt darin, den Zeitplan zu definieren.

Zeitplan definieren

Sie können den Zeitplan für die Erfassung von Straftaten definieren. Während dieses Schritts können Sie die Standardeinstellungen für den Abruf von Straftaten überprüfen oder die Planung nach Bedarf ändern. Mit diesem Schritt können Sie auch historische Straftaten mithilfe eines Datumsbereichs abrufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können auswählen, ob Sie während des Planungsschritts historische Verstöße erfassen möchten. Sie wählen auch aus, wie oft Sie nach zukünftigen neuen Vergehen und aktualisierten Vergehen abfragen, die der Profilkonfiguration entsprechen.

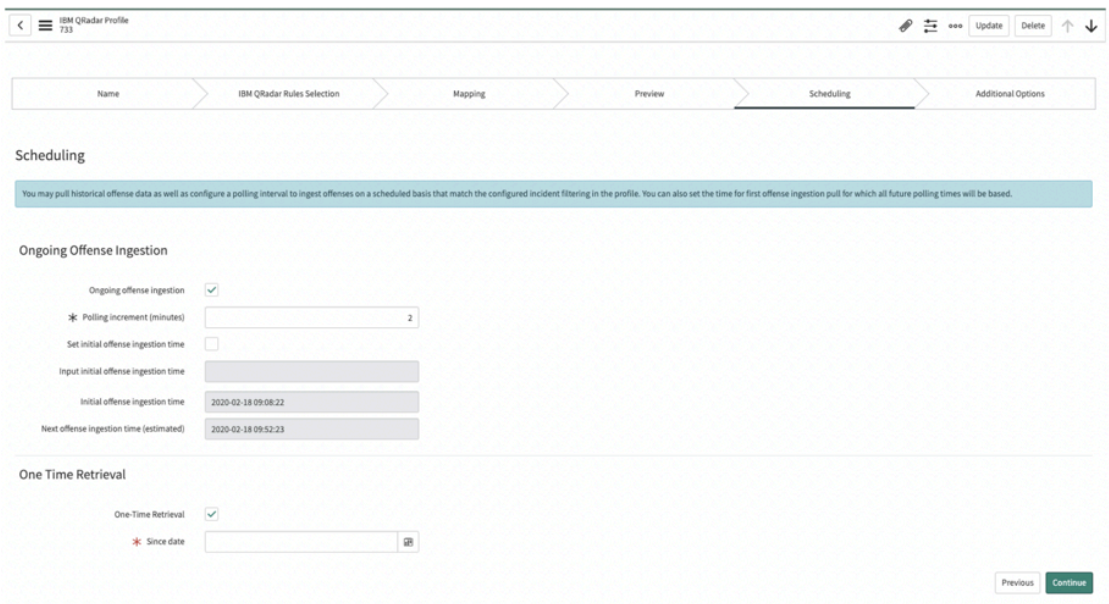
Als Benutzer mit der Rolle sn_si.admin konfigurieren Sie diese Abfrageintervalle pro Profil. Die Leistung von IBM QRadar Die Integration der Verstoßerfassung kann durch die verschiedenen Abfrageintervalle beeinträchtigt werden. Bei der Planung möchten Sie möglicherweise die Reduzierung des Abfrageaufwands auf dem abgleichen IBM QRadar Server gegen den Wunsch, so bald wie möglich benachrichtigt zu werden, wenn eine Straftat erstellt oder aktualisiert wird. Für jedes Profil ist ein fünf-Minuten-Standardwert festgelegt. Sie können diese Einstellung jedoch bei Bedarf auf eine Minute ändern.

Neue und aktualisierte Verstöße werden abgerufen

Wenn der Abfragezeitplan festgelegt ist, ruft die geplante Aufgabe sowohl neue als auch aktualisierte Verstöße ab, die zuvor abgerufen wurden, aber die Incident-Filterkriterien nicht erfüllten. Dies bietet Ihnen die Flexibilität, Incidents basierend auf Kriterien zu erstellen, die möglicherweise nicht vorhanden sind, wenn eine Straftat erstmals erstellt wird, aber verfügbar werden, nachdem ein Update erfolgt ist, z. B. während der Untersuchungsphase. Sobald ein Incident für eine bestimmte Straftat erstellt wurde, werden die nachfolgenden Aktualisierungen ignoriert, da erwartet wird, dass die Straftat jetzt als aktiv behandelt wird ServiceNow Security Incident. Alle anderen Straftaten, die zuvor erfasst wurden, aber die Kriterien für die Incident-Generierung nicht erfüllen, werden weiterhin abgerufen und anhand der Incident-Generierungskriterien überprüft, bis sie Teil eines aktiven Incident werden.

Prozedur

1. Wenn die Seite „Zeitplanung“ im Fortschrittsbalken nicht angezeigt wird, wählen Sie aus **Zeitplanung** .
2. Wählen Sie eine aus, um zu planen, wie und wann Straftaten aus abgerufen werden IBM QRadar Konsole.



3. Klicken Sie Auf **Fahren Sie Fort** Um zur Seite „zusätzliche Optionen“ zu navigieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatisieren Sie die Aktualisierung und den Abschluss von Verstößen basierend auf dem SIR-Incident-Status

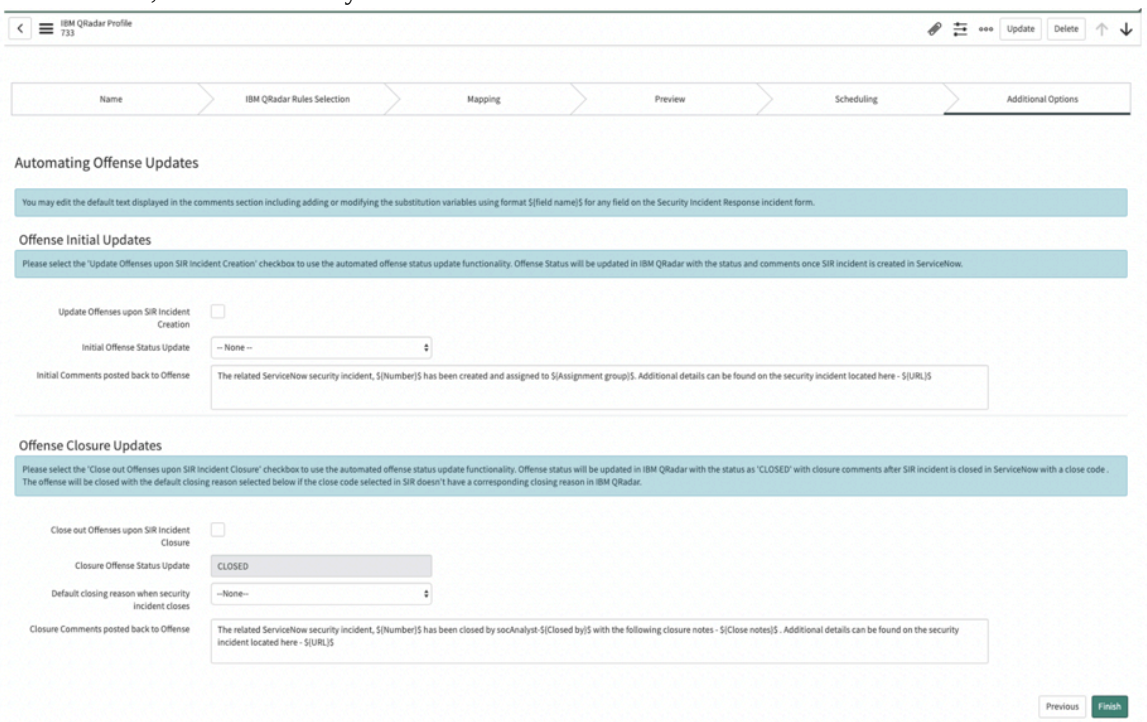
Die IBM QRadar Die Integration verfügt über eine bidirektionale Schnittstelle, mit der sowohl Verstöße Security Incidents erstellen als auch die Möglichkeit haben, die Verstöße zu aktualisieren, sobald der Security Incident erstellt und/oder geschlossen wurde, mit relevanten Incident-Details wie Security Incident-Nummer, Zuweisungsgruppe, Security Incident-URL usw.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn die Seite „zusätzliche Optionen“ im Fortschrittsbalken nicht angezeigt wird, wählen Sie aus **Zusätzliche Optionen** .
2. Befolgen Sie die folgenden Anweisungen, um die Konfiguration für die Aktualisierung von Straftaten abzuschließen, wenn der Security Incident erstellt wird.



3. Klicken Sie Auf **Beenden** Um die Konfiguration abzuschließen und das Profil in zu verschieben **Warten** status.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um Straftaten aus dem abzurufen IBM QRadar Konsole basierend auf Ihrer Planung.

Konfigurationseinstellungen

Verwenden Sie diese Option, um zu ändern IBM QRadar Standardsystemeigenschaften der Erfassungsintegration.

Um die Systemeigenschaften zu ändern, melden Sie sich als Anwender mit an *sn_si.admin* Rolle und navigieren Sie zu **Integration mit IBM QRadar** > **IBM QRadar-Integrationseinstellungen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM QRadar-Integrationseinstellungen

Eigenschaftsname	Beschreibung
Grenzwert für die Anzahl von Security Incidents erzwingen, die innerhalb von 24 Stunden erstellt werden können. sn_sec_qradar.max_si_per_day	Gibt die maximale Anzahl von Security Incidents an, die in 24 Stunden erstellt werden können. • Typ: Ganzzahl • Standardwert: 1000
Erzwingen Sie eine Beschränkung der Anzahl von Straftaten, die zu einem einzelnen Incident zusammengefasst werden können. sn_sec_qradar.max_Aggregation_per_si	Das Aggregationslimit für Verstöße für einen Security Incident. Wenn beispielsweise 102 Verstöße vorliegen, werden die ersten 100 Verstöße zu zusammengefasst Security Incident_1 Und die verbleibenden 2 bis Security Incident_2 . • Typ: Ganzzahl • Standardwert: 100
Diese Eigenschaft legt den Zeitraum von AQL fest, um aktuelle Ereignisse/Flows für eine bestimmte Straftat abzurufen. sn_sec_qradar.on_Demand_recent_days_limit	Gibt die Anzahl der Tage an, um aktuelle Ereignisse oder Flows für eine bestimmte Straftat abzurufen. • Typ: Ganzzahl • Standardwert: 7
Diese Eigenschaft begrenzt die Anzahl der letzten Ereignisse, die für eine bestimmte Straftat abgerufen wurden. sn_sec_qradar.on_Demand_event_limit	Gibt die Anzahl der Ereignisse an, die für eine Straftat abgerufen werden. Die neuesten Ereignisse werden zuerst basierend auf dem Ereigniszeitstempel abgerufen. • Typ: Ganzzahl • Standardwert: 100
Diese Eigenschaft begrenzt die Anzahl der letzten Flows, die für eine bestimmte Straftat abgerufen wurden. sn_sec_qradar.on_Demand_Flow_limit	Gibt die Anzahl der Flows an, die für eine Straftat abgerufen werden. Die neuesten Flows werden zuerst basierend auf dem Flow-Zeitstempel abgerufen. • Typ: Ganzzahl • Standardwert: 100
Diese Eigenschaft legt den Zeitüberschreitungswert (Sekunden) für die AQL fest, die letzte Flows/ Ereignisse für eine bestimmte Straftat abruft. sn_sec_qradar.on_Demand_timeout	• Typ: Ganzzahl • Standardwert: 300
Zeitüberschreitung bei Such-IDs (Sekunden) für Datensätze in der Warteschlange zur Abfrage von AQLs einer Straftat.	Die Zeitüberschreitung der AQL für eine Straftat in der Warteschlange, bevor ein Security Incident erstellt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM QRadar-Integrationseinstellungen (Fortsetzung)

Eigenschaftsname	Beschreibung
sn_sec_qradar.sid_ttl	wird. Wenn beispielsweise 90 Verstöße vorliegen, werden die ersten 50 Verstöße für AQL-Daten im ersten Batch und die verbleibenden 40 Verstöße im nachfolgenden Batch im selben Abfrageintervall verarbeitet. • Typ: Ganzzahl • Standardwert: 300
Schwellenwert zur Steuerung der Anzahl der Suchvorgänge, die in ausgeführt werden können IBM QRadar Zu einem Zeitpunkt, der durch die geplante Integration ausgelöst wird Job.sn_sec_qradar.Records_threshold_in_que_for_aql	Gibt die Anzahl der Verstöße an, die Sie in einem einzelnen Batch in einem Abfrageintervall abrufen. • Typ: Ganzzahl • Standardwert: 50
Dies ist die Anzahl der Tage für die Bereinigung von Integrationstabellen. sn_sec_qradar.Queue_item_expire	Im Folgenden finden Sie die Integrationstabellen: • sn_sec_qradar_Events: IBM QRadar-Ereignisse • sn_sec_qradar_Flows: IBM QRadar-Flows • sn_sec_qradar_offense_Updates: Updates für IBM QRadar-Verstöße • sn_sec_qradar_offense_to_Task: IBM QRadar-Verstoß gegen Aufgabe • Typ: Ganzzahl • Standardwert: 30
Verstoßgrenze pro geplanter Aufgabe, die pro Profil ausgeführt wird, entweder beim einmaligen Abruf oder bei laufender Erfassung. sn_sec_qradar.max_offense_limit_per_Run	Gibt die Anzahl der Straftaten an, die Sie in abrufen ServiceNow AI Platform In einem einzelnen Abruf. • Typ: Ganzzahl • Standardwert: 1000
Legen Sie diese Eigenschaft fest, um die Funktion „Verstöße aktualisieren“ zu aktivieren. sn_sec_qradar.get_offense_updates	**Hinweis:** Das Aktivieren dieser Einstellung kann zu einer Verzögerung beim Erstellen eines Security Incidents führen. • Typ: Wahr| falsch • Standardwert: falsch

Alle geänderten Integrationseinstellungen werden während des nächsten Abfrageintervalls angewendet, wie im Profil definiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optional: Kopieren Sie eine IBM QRadar Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, sollten Sie Profile kopieren, um Zeit zu sparen.

Vorbereitungen

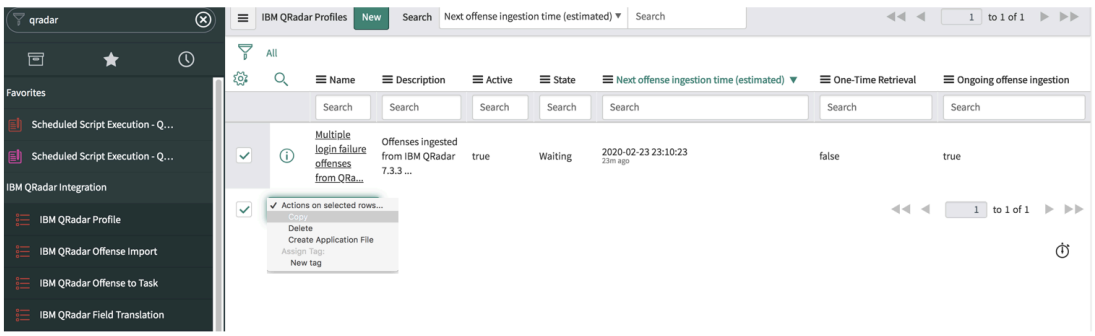
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie als Anwender mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), sodass es vor Abschluss der Konfiguration nicht versehentlich aktiviert wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und verifiziert haben.

Prozedur

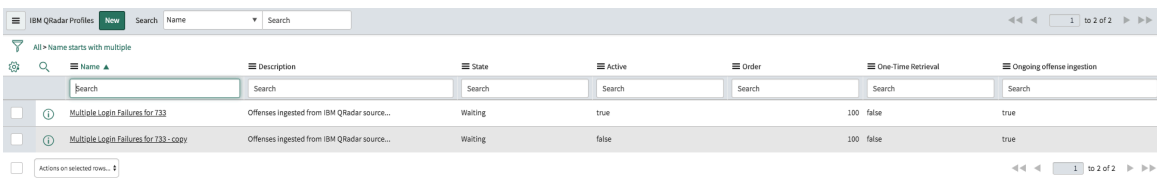
1. Navigieren zu **Alle** > **Integration mit IBM QRadar** > **IBM QRadar-Profil**an.
2. Wählen Sie in der angezeigten Liste IBM QRadar-Profile ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren** .



Das Profil wird kopiert und in der Liste angezeigt. Die Kopie verfügt über alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält Kopieren . Obwohl das ursprüngliche Profil aktiviert ist (Wahr), die Kopie ist zu diesem Zeitpunkt deaktiviert (Falsch). Möglicherweise möchten Sie Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf auf das neue Profil angewendet werden.

Hinweis:

Wenn Sie eine andere Quelle für das Profil auswählen, müssen Sie neue Regeln auswählen (Wählen Sie Aus IBM QRadar Regeln) Für das Profil. Wenn Sie jedoch dieselbe Quelle verwenden und neue Regeln auswählen, werden die Beispielvergehen gelöscht.



Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass **Aktiv** Der Spaltenstatus wird auf „falsch“ festgelegt, da das Profil aktiviert werden muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Sie werden aufgefordert, das neue Profil zu aktivieren (zu aktivieren), nachdem Sie die Konfigurationsschritte abgeschlossen haben.

Domänentrennung Und IBM QRadar Verstoßerfassung

Domänentrennung Wird in unterstützt IBM QRadar Verstoßerfassung. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Funktionsweise der Domänentrennung in IBM QRadar Verstoßerfassung

Führen Sie die folgenden Schritte aus, um die Domänentrennung zu erreichen:

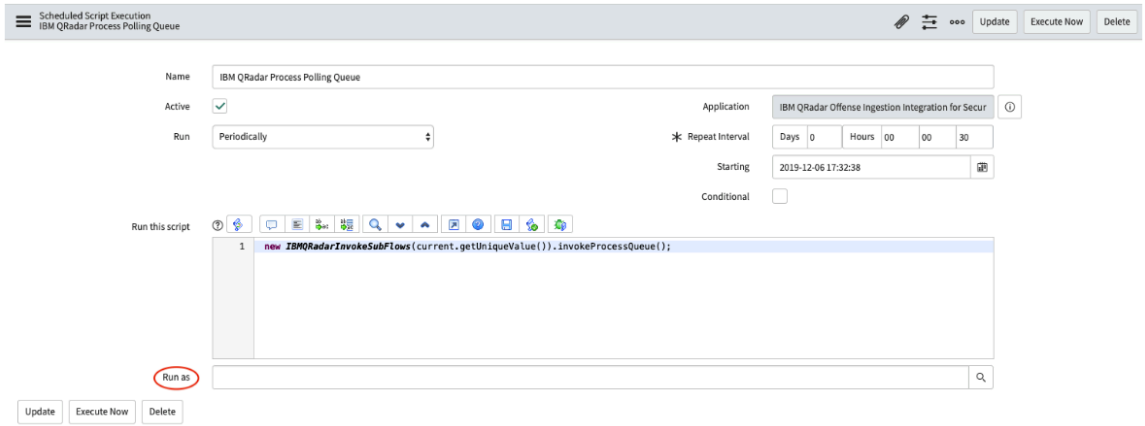
- Erstellen Sie einen Anwender mit `sn_si.admin` Rolle in der jeweiligen Domäne.

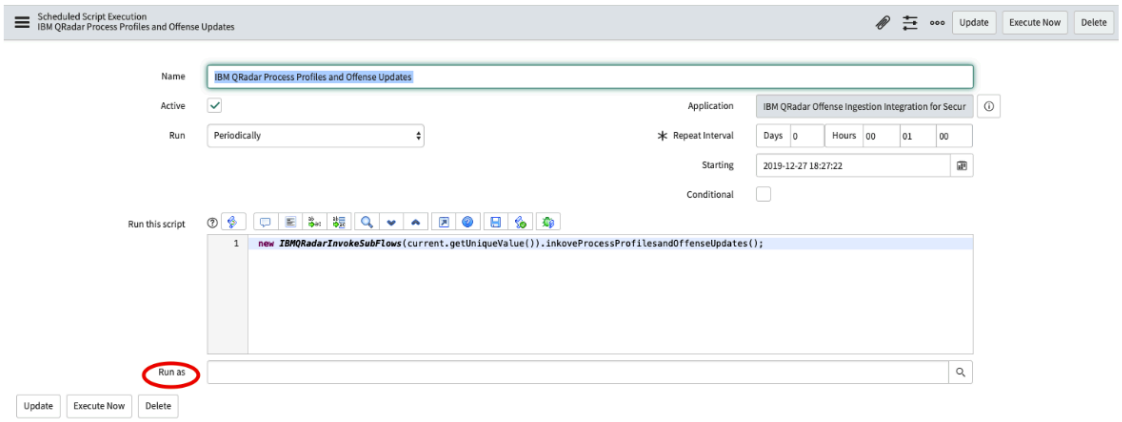
> **Hinweis:**
> Wenn Sie das Profil erstellen, verwenden Sie die Domänenauswahl, um die bestimmte Domäne auszuwählen. Erstellen Sie den Anwender nicht in der übergeordneten Domäne, und ändern Sie später die Domäne des Profils. Sie sollten für jede Domäne einen bestimmten Anwender für Ihr Profil mit haben `sn_si.admin` Rolle. Verwenden Sie diesen Anwender, um Einstellungen im Profil zu erstellen oder zu ändern.

- Deaktivieren Sie vorhandene geplante Aufgaben.
- Replizieren Sie IBM QRadar Warteschlange für Prozessabfrage, die IBM QRadar Prozessprofile und die Offense aktualisiert geplante Aufgaben für jede Domäne.
- Ändern Sie **Ausführen als** Vom Systemanwender zum Anwender mit `sn_si.admin` Rolle in der jeweiligen Domäne und führt die geplante Aufgabe aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.





Zugehörige Informationen

Domänentrennung für Service Provider

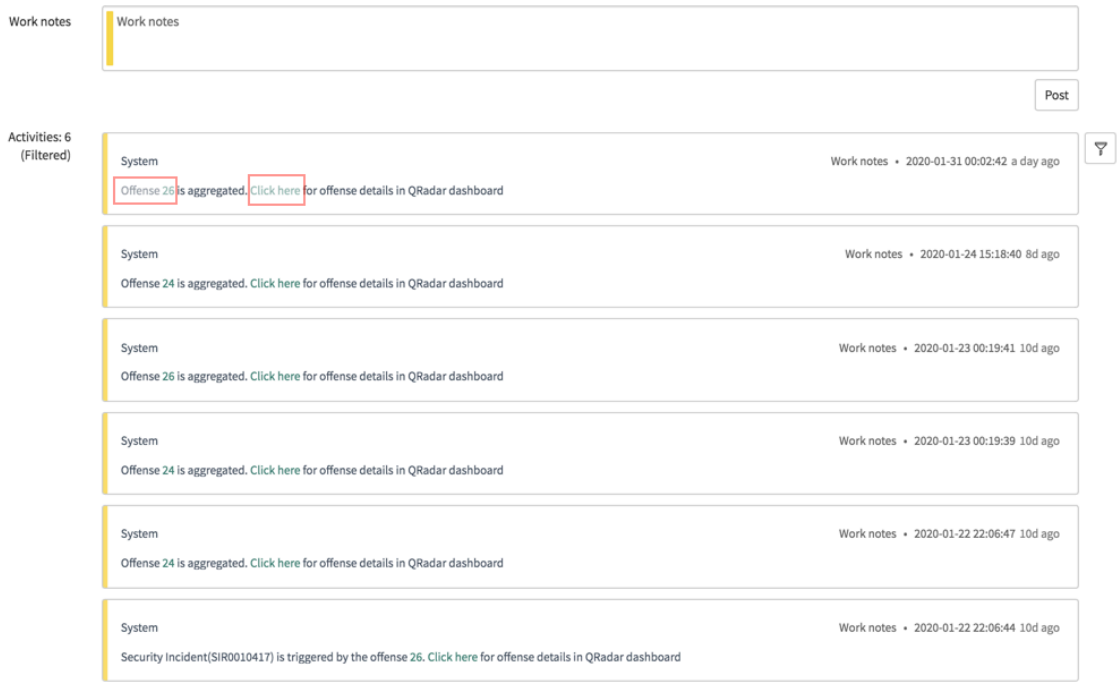
Formular „Security Incident Response“ nach Erfassung des Verstoßes

Nach einem IBM QRadar Verstoß wurde erfasst, ein Security Incident wird erstellt, und die entsprechenden Aktualisierungen werden am Security Incident-Datensatz vorgenommen.

Arbeitsnotiz

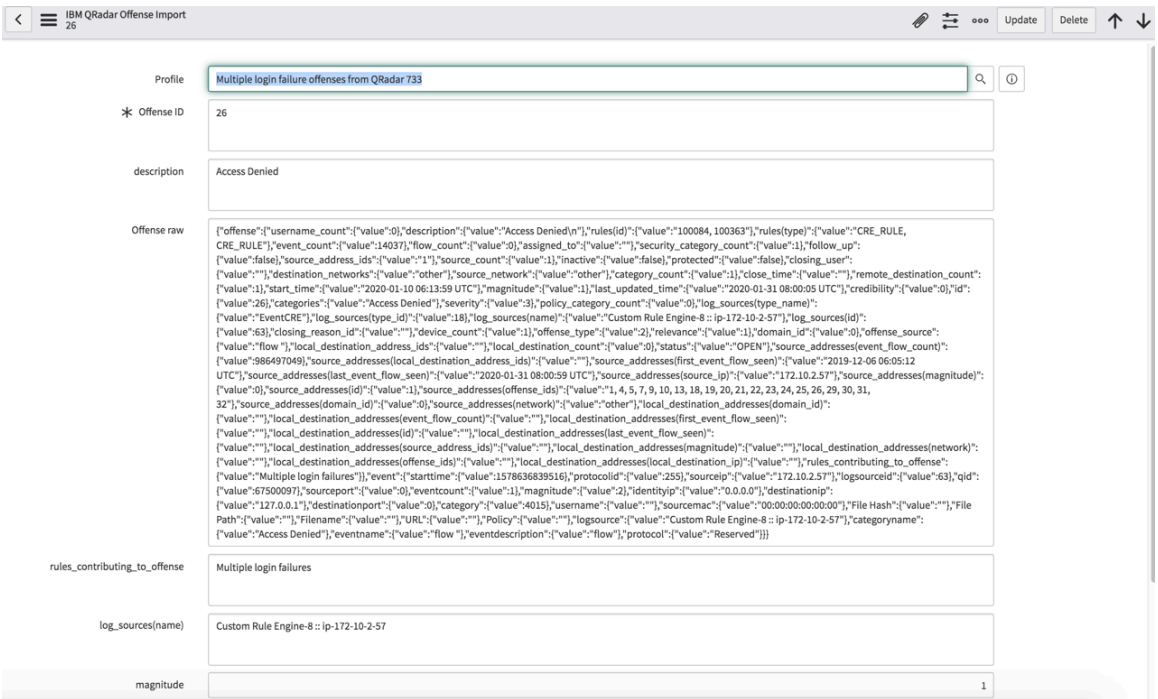
Eine Arbeitsnotiz wird mit Details zur Straftat veröffentlicht, die den Security Incident ausgelöst hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Klicken Sie auf den Link Verstoß, um zum internen Security Incident-Datensatz zu navigieren. Die **Klicken Sie hier** Hyperlink führt Sie zu IBM QRadar Dashboard, in dem Sie die Verstoßdetails anzeigen können.

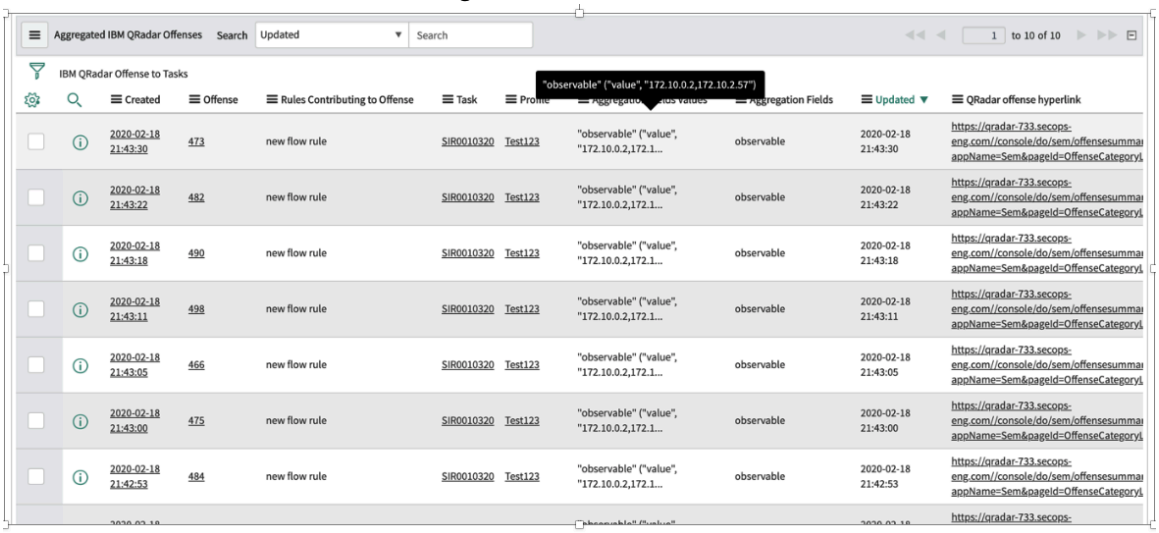
Wenn Sie ausgewählt haben **Arbeitsnotiz für neuen Verstoß protokollieren** Option in den Verstoßzusammenfassungskriterien wie in beschrieben Zuordnung IBM QRadar Verstoßfelder zu Security Incident Response-Feldern, Eine Arbeitsnotiz wird veröffentlicht, wenn die Straftat aggregiert wird.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

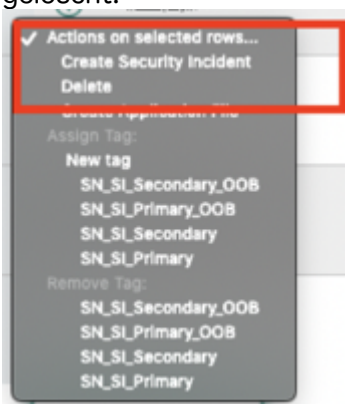
Zusammengefasste Straftaten

Klicken **Zugehörige Listen** > **Aggregierte IBM QRadar-Verstöße** Dient zum Anzeigen der mit dem Security Incident zusammengefassten Verstöße. Klicken Sie auf den Hyperlink QRadar-Verstoß, um die Straftat in anzuzeigen IBM QRadar Dashboard.



Security Incident erstellen: Wählen Sie eine Straftat aus der Liste aus, und klicken Sie auf **Aktionen** Und klicken Sie auf **Erstellen Sie einen Security Incident** . Diese Option erstellt einen Security Incident für die Straftat, und diese Straftat wird vom übergeordneten Security Incident getrennt.

Verstoßdatensatz löschen: Wählen Sie eine Vergehen aus der Liste aus, und klicken Sie auf **Aktionen** Und klicken Sie auf **Löschen** . Mit dieser Option wird der Verstoßdatensatz gelöscht.

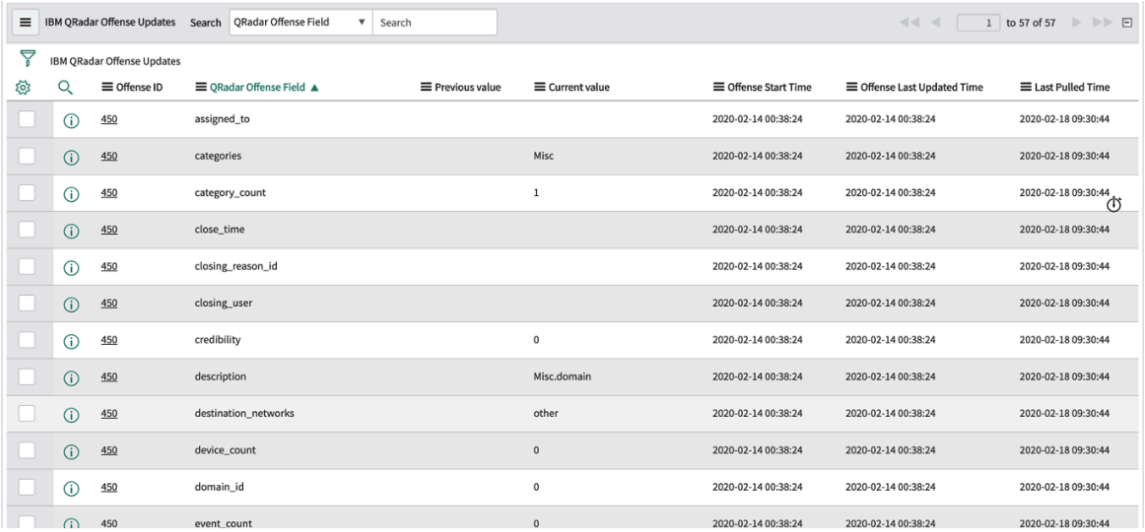


Updates für IBM QRadar-Verstoß

Dies zeigt die Felder „Standard“ und „anwenderdefinierte Straftat“ an und verfolgt Änderungen an der Straftat während jedes Abfrageintervalls. Dies ist hilfreich, da Sie Aktualisierungen von Straftaten direkt anzeigen können, ohne zu navigieren IBM QRadar Dashboard. Alle Änderungen an den Werten werden in den Feldern „vorheriger Wert“ und „Aktueller Wert“ angezeigt.

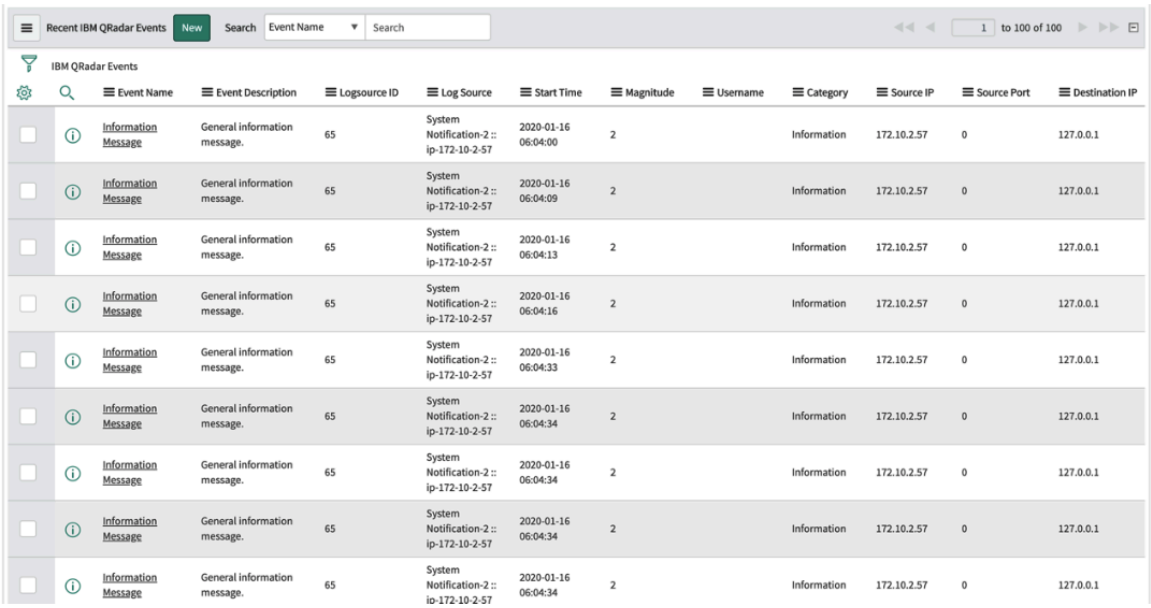
Um die Funktion „Verstöße aktualisieren“ zu aktivieren, navigieren Sie zu **Integration mit IBM QRadar** > **IBM QRadar-Integrationseinstellungen** Und aktivieren **Legen Sie diese Eigenschaft fest, um die Funktion „Verstöße aktualisieren“ zu aktivieren** . Standardmäßig ist diese Einstellung deaktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Letzte IBM QRadar-Ereignisse

Klicken Sie auf **Ruft die letzten IBM QRadar-Ereignisse ab** Option unter **Zugehörige Links** Um die neuesten anzuzeigen IBM QRadar Ereignisse.

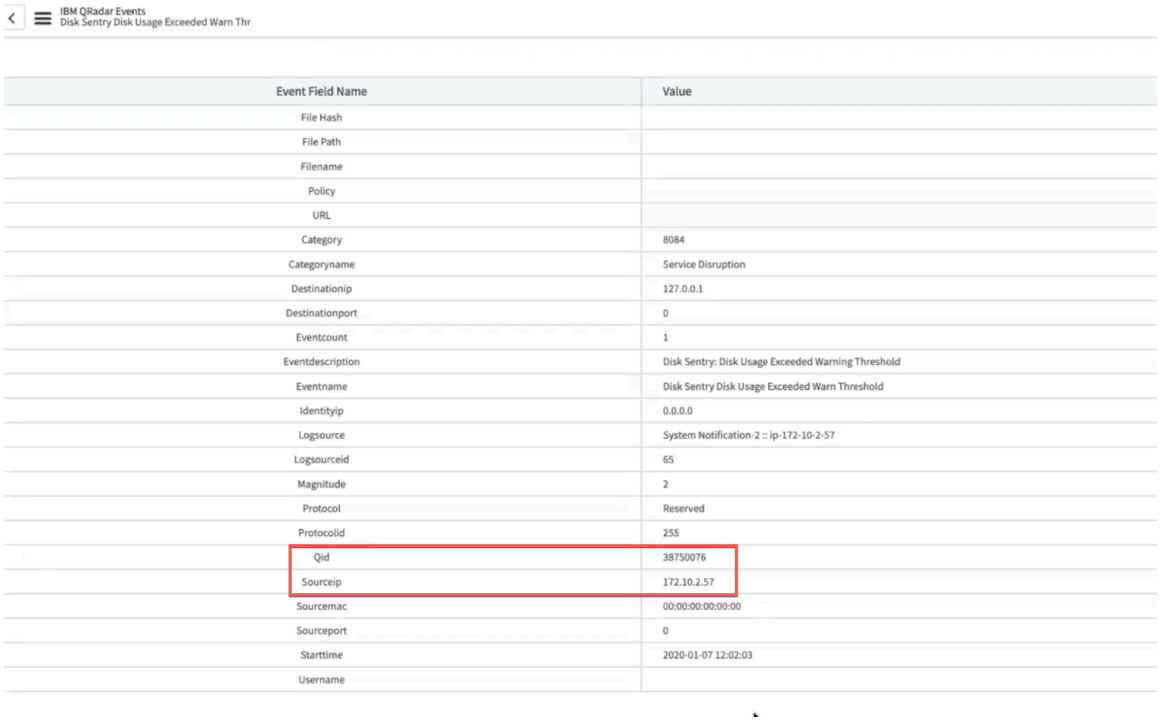


Standardmäßig wird eine maximale Anzahl von 100 Ereignissen angezeigt. Sie können diese Standardeinstellung in ändern Konfigurationseinstellungen.

Hinweis:

Die obige Abbildung zeigt die Standard-Ereignisfelder, die der Straftat zugeordnet sind. Wenn Sie anwenderdefinierte Ereignisfelder konfiguriert und zugeordnet haben (siehe Zuordnung IBM QRadar Verstoßfelder zu Security Incident Response-Feldern), können Sie sie in der Listenansicht anzeigen, indem Sie auf den Link Ereignisname klicken.

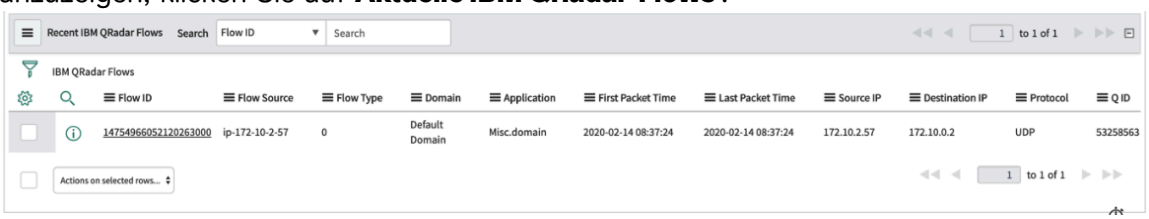
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Event Field Name	Value
File Hash	
File Path	
Filename	
Policy	
URL	
Category	8084
Categoryname	Service Disruption
Destinationip	127.0.0.1
Destinationport	0
Eventcount	1
Eventdescription	Disk Sentry: Disk Usage Exceeded Warning Threshold
Eventname	Disk Sentry Disk Usage Exceeded Warn Threshold
Identityip	0.0.0.0
Logsource	System Notification-2 :: ip-172-10-2-57
Logsourceid	65
Magnitude	2
Protocol	Reserved
Protocolid	255
Qid	38750076
Sourceip	172.10.2.57
Sourcemac	00:00:00:00:00:00
Sourceport	0
Starttime	2020-01-07 12:02:03
Username	

Aktuelle IBM QRadar-Flows

Mit Integration Hub und Flow Designer sind mehrere Flows, Subflows und Aktionen mit verfügbar IBM QRadar Integration. Wenn Sie auf klicken **Ruft die letzten IBM QRadar-Flows ab** Option unter „zugehörige Links“ werden die neuesten Flows abgerufen. Um diese Flows anzuzeigen, klicken Sie auf **Aktuelle IBM QRadar-Flows** .



Standardmäßig wird eine maximale Anzahl von 100 Flows angezeigt. Sie können diese Standardeinstellung in ändern Konfigurationseinstellungen.

Hinweis:
Die obige Abbildung zeigt die Standard-Flow-Felder, die der Straftat zugeordnet sind. Wenn Sie anwenderdefinierte Flow-Felder konfiguriert und zugeordnet haben (siehe Zuordnung IBM QRadar Verstoßfelder zu Security Incident Response-Feldern), können Sie sie in der Listenansicht anzeigen, indem Sie auf den Link Flow-ID klicken.

Nutzung von Flow Designer und Integration Hub mit Integration von IBM QRadar Offense Insertion

Mit der Flow Designer- und Integration Hub-Funktionalität wurden mehrere Subflows und Aktionen als Teil von erstellt IBM QRadar Integration der Verstoßerfassung.

Folgendes IBM QRadar Subflows sind verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Validierung von Verbindungen und Anmeldeinformationen : Dies wird in der Konfigurationskachel zum Validieren des Hosts und der Anmeldeinformationen beim ersten Setup verwendet.
- IBM QRadar-Regelabruf : Dies wird im Abschnitt „Regeln“ des Profil-Setups verwendet, um alle aktiven Regeln in abzurufen IBM QRadar. Dieser Subflow wird asynchron ausgelöst.
- Ruft Beispielvergehen-Daten aus IBM QRadar ab : Dies wird im Abschnitt „Zuordnung“ des Profil-Setups verwendet, um Beispieldaten abzurufen. Dieser Subflow wird asynchron ausgelöst.
- Statusaktualisierungen für IBM QRadar-Verstoß : Dies wird jede Minute durch eine geplante Aufgabe ausgelöst und aktualisiert die Straftat in IBM QRadar Wenn der Security Incident erstellt oder geschlossen wird.
- Prozessprofile aus Vergehen für geplante Aufgaben und Warteschlangen : Dies wird jede Minute durch eine geplante Aufgabe ausgelöst, um Verstöße pro Profil basierend auf dem Abfrageintervall abzurufen. Dadurch werden Verstöße abgerufen und zur weiteren Verarbeitung in die Warteschlange der Abfragetabelle gestellt.
- Verarbeiten Sie die Abrufwarteschlange und die Abfrage in Batches : Dies wird alle 30 Sekunden durch eine geplante Aufgabe ausgelöst, um die Warteschlange der Abruftabelle zu verarbeiten.
- Ruft die letzten IBM QRadar-Flows ab : Dies wird über den Security Incident-Formularlink ausgelöst, um die neuesten Flows von Straftaten abzurufen.
- Ruft die letzten IBM QRadar-Ereignisse ab : Dies wird über den Link des Security Incident-Formulars ausgelöst, um die neuesten Verstoßereignisse abzurufen.

Um diese Subflows anzuzeigen, melden Sie sich als Anwender mit an `sn_si.admin` Rolle und navigieren Sie zu **Flow Designer** > **Designer**an. Klicken Sie auf den Namenslink eines der oben aufgeführten Subflows, um den Subflow im Detail anzuzeigen.

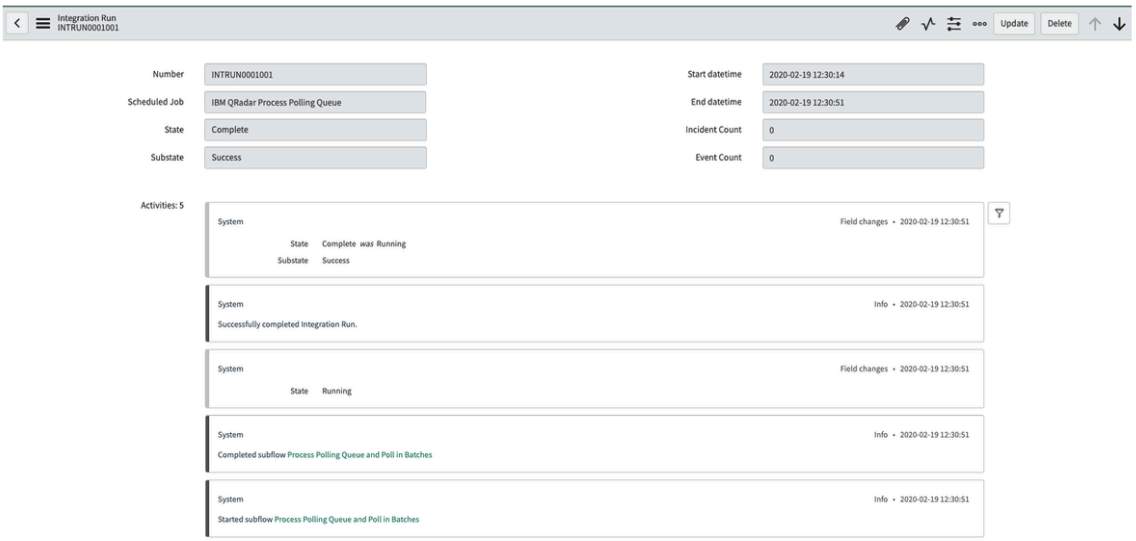
Problembehandlung IBM QRadar Integration der Verstoßerfassung

Dieser Abschnitt behandelt wichtige Tipps zur Fehlerbehebung und häufig gestellte Fragen im Zusammenhang mit IBM QRadar Verstoßerfassung.

- Integrationsausführung: Wenn die Ausführung einer geplanten Aufgabe beginnt, wird ein Datensatz der Integrationsausführung mit Protokollen, Fehlern und Warnungen angezeigt. Die Anzahl der abgerufenen Verstöße und die Anzahl der Incidents, die in einer geplanten Aufgabenausführung erstellt wurden, werden ebenfalls angezeigt. Anwender mit der Rolle „sn_si.Analyst“ können sehen, ob Fehler/Profile beim Abrufen während der Integrationsausführung fehlgeschlagen sind.

  Arbeitsnotizen in der Integrationsausführung bieten Links zu den ausgeführten Subflows. Benutzer mit der Rolle „sn_si.Analyst“ können überprüfen `sn_event_ingestion_Integration_Run` Tabelle für alle aufgetretenen Fehler. Um Integrationsprobleme zu beheben, müssen Sie zuerst die Integrationsausführung überprüfen. Fehler werden als Arbeitsnotizen in den Datensätzen der Integrationsausführung für jede geplante Aufgabenausführung protokolliert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- SSL-Probleme: Beim Herstellen einer Verbindung mit IBM QRadar Cloud-Instanzen: Stellen Sie sicher, dass die Instanz über ein gültiges CA-Zertifikat verfügt, das noch nicht abgelaufen ist. Sie können RSA- oder eigene Zertifikate in die Plattform importieren und sicherstellen, dass der allgemeine Name des Zertifikats mit dem Hostnamen übereinstimmt. Details siehe https://support.servicenow.com/nav_to.do?uri=%2Fkb_view.do%3Fsys_kb_id%3D55ecefd61bf3774cada243f6fe4bcb44 .
- Unvollständiges Profil: Beim Konfigurieren des Profils in den zusätzlichen Optionen (Automatisieren Sie die Aktualisierung und den Abschluss von Verstößen basierend auf dem SIR-Incident-Status) Abschnitt müssen Sie auf klicken **Beenden** Schaltfläche, um sicherzustellen, dass das Profil in den Status „Warten“ verschoben wird, um anzuzeigen, dass es auf die Erfassung wartet.
- Profil validieren: Um zu validieren, ob die Integration ordnungsgemäß funktioniert, überprüfen Sie die profilstatus, das Datum des letzten Abrufs des Profils, die Tabelle des Verstoßimports und die Datensätze der Aufgabentabelle.
- MID-Server-Konfiguration: Wenn Sie installieren IBM QRadar Anwendung lokal: Nach der Konfiguration des MID-Servers müssen Sie eine MID-Server-Anwendung erstellen. Der Name der MID-Server-Anwendung sollte in der Kachel für Integrationskonfigurationen anstelle des MID-Server-Namens verwendet werden.

Hinweis:
Die Standardzeitüberschreitung für MID-Service beträgt 30 Sekunden. Anweisungen zum Deaktivieren des Zeitüberschreitungszeitraums finden Sie unter <link>. Beachten Sie, dass dies ein systemweiter Change ist und sich auf andere Integrationen auswirken kann.

- Verstöße-Updates: Wenn Sie aktiviert haben `sn_sec_qradar.get_offense_updates` Eigenschaft, und Sie bemerken eine Verzögerung bei der Erstellung von Security Incidents, und deaktivieren Sie dann die Eigenschaft. Aktivieren Sie diese Eigenschaft nicht, wenn das Abfrageintervall niedrig und die Last der Vergehen in QRadar hoch ist, da dies die Warteschlangenlast erhöht.
- Fehlende Ereignis-, Flow-Daten, Remote_ip- oder Anwenderdaten in einem Security Incident: Wenn Sie feststellen, dass Ereignis, Flow-Daten, Remote_ip oder Anwenderdaten in einem Security Incident fehlen, erhöhen Sie die Zeitüberschreitung (Sekunden) für `sn_sec_qradar.sid_ttl` Parameter. Wenn Sie die Dauer erhöhen, wird die Erstellung des Security Incidents verzögert, bis die AQLs die Analyse jedes Verstoßes abgeschlossen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeitüberschreitungen: Wenn Sie Zeitüberschreitungsfehler in den Anwendungsprotokollen anzeigen, überprüfen und ändern Sie die folgenden Flow Designer-Aktionen:

Flow Designer-Aktionen

Parameter	Aktion
Beispielvergehen Abrufen `VAR Flow_output = sn_fd.FlowAPI.ExecuteAction('sn_sec_qradar.Fire_Rest_for_offenses', Flow_input, 60000);`	Überprüfen und aktualisieren Sie die Dauer in Millisekunden.
Beispielvergehen Abrufen `VAR Flow_output = sn_fd.FlowAPI.ExecuteAction('sn_sec_qradar.Fire_Rest_for_offenses', Flow_input);`	Fügen Sie einen Parameter für hinzu `ExecuteAction` Und geben Sie die Dauer in Millisekunden ein.
Vergehen für Profil- und Warteschlangendatensätze in der Abfragetabelle abrufen `VAR Flow_output = sn_fd.FlowAPI.ExecuteAction('sn_sec_qradar.Fire_Rest_for_offenses', Flow_input, 180000);`	Überprüfen und aktualisieren Sie die Dauer in Millisekunden.
Wrapper zum Testen der Verbindungs-REST `VAR Rest_output = sn_fd.FlowAPI.ExecuteAction('sn_sec_qradar.Test_connection_Rest', Rest_input);`	Fügen Sie einen Parameter für hinzu `ExecuteAction` Und geben Sie die Dauer in Millisekunden ein.
Wrapper zum Validieren der REST-API-Anmeldeinformationen `VAR Rest_output = sn_fd.FlowAPI.ExecuteAction('sn_sec_qradar.validate_credentials_Rest', Rest_input);`	Fügen Sie einen Parameter für hinzu `ExecuteAction` Und geben Sie die Dauer in Millisekunden ein.
REST-Schritt für Updates von IBM QRadar-Vergehen `VAR-Ergebnis = sn_fd.FlowAPI.ExecuteAction('sn_sec_qradar.'+restStep, Eingaben,60000);`	Überprüfen und aktualisieren Sie die Dauer in Millisekunden.

IBM QRadar – Integration der Incident-Anreicherung

Die IBM QRadar– Die Incident-Anreicherungsintegration durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

Erkunden **Einrichten**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response-Integrationen

- Beginnen Sie mit dem IBM QRadar– Integration der Incident-Anreicherung
- Erstellen Sie Konfigurationsdatensätze für Sichtungssuche

Verwenden

- Führen Sie eine Sichtungssuche aus
- Integration Von Security Operations: Sichtungssuche-Flow
- Security Operations – QRadar-Sichtungssuche-Flow
- Sichtungssuchdetails Anzeigen
- Zeigen Sie Die Ergebnisse Der Sichtungssuche An

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Beginnen Sie mit dem IBM QRadar– Integration der Incident-Anreicherung

IBM QRadar Ist ein SIEM-Produkt (Enterprise Security Information and Event Management), das leicht in integriert werden kann Security Operations. Bevor Sie verwenden können IBM QRadar– Integration der Incident-Anreicherung. Sie müssen sie aus dem herunterladen ServiceNow Store Und fügen Sie die entsprechende API-Basis-URL und den API-Schlüssel hinzu.

Vorbereitungen

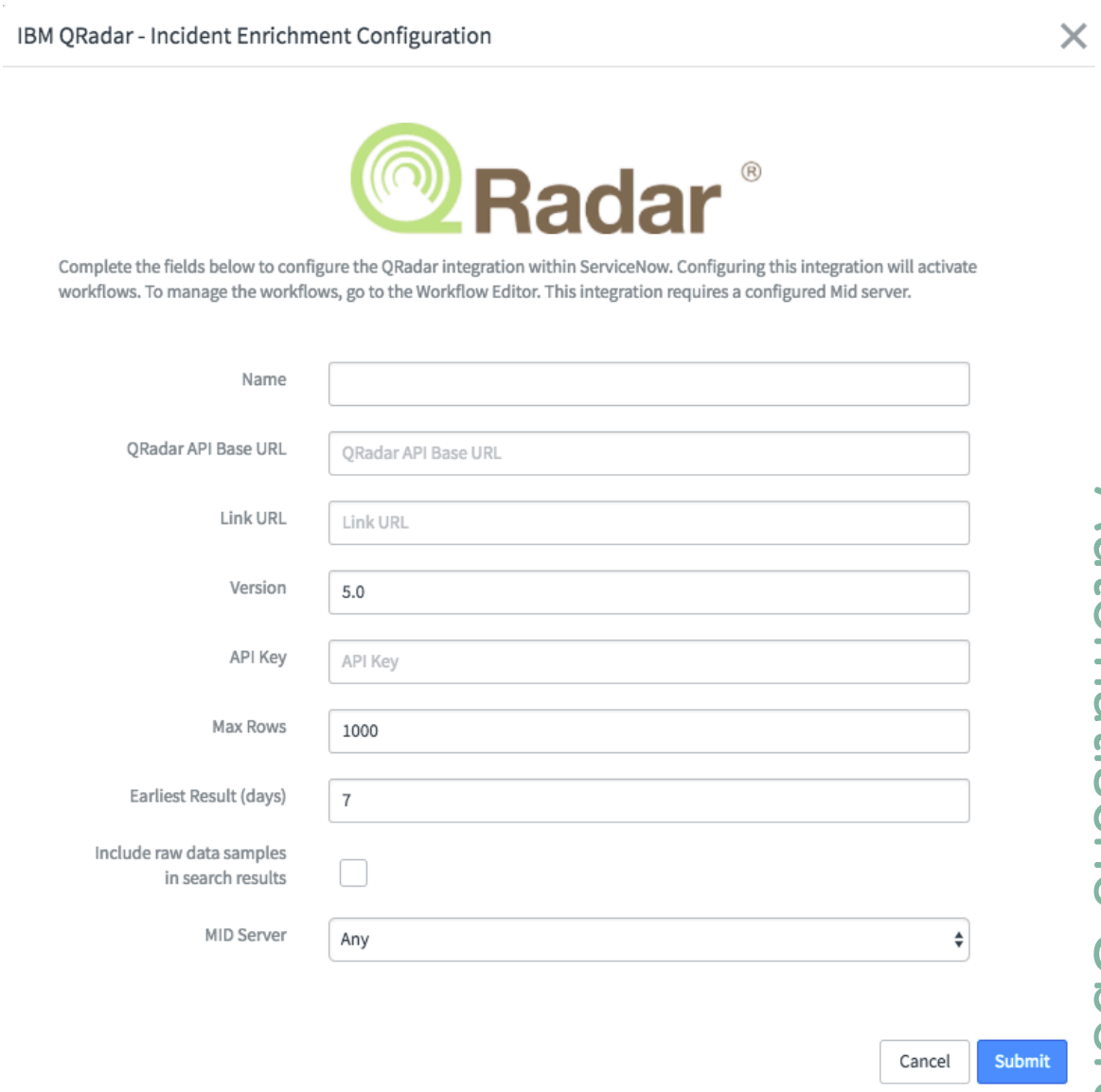
Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf zu IBM QRadar Und erhalten Sie die API-Basis-URL und den API-Schlüssel unter Ihrem IBM QRadar Profil.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. In IBM QRadar– Incident-Anreicherungskarte, klicken Sie auf **Neu** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Basis-URL der QRadar-API	Die Basis-URL, die Sie von erworben haben IBM QRadar Website.
Link-URL	[Optional] die Link-URL, die mit einem verknüpft ist IBM QRadar Instanz, falls verfügbar.
Version	Die IBM QRadar Version; 5,0 ist der Standard.
API-Schlüssel	Der API-Schlüssel, den Sie vom erhalten haben IBM QRadar Website.
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie in Tagen anzeigen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Rohdatenmuster in Suchergebnissen berücksichtigen	Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung in ab **Anzahl der Zeilen mit Rohdaten** Eigenschaft in Eigenschaften von Security Incident Response .
MID-Server	Wählen Sie Aus **Beliebig** Um einen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Navigieren Sie zum Verwalten der Workflows zu **Workflow-Editor** .

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf klicken **Konfigurieren** Oder **Löschen** Zum Ändern oder Löschen der Konfiguration.
8. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie aus **Nein** Von **Konfigurationen Anzeigen** Dropdown-Liste.

LogRhythm Übersicht

Die Zuordnungsflexibilität dieser Integration bietet Analysten Transparenz für Ereignisse und zugehörige Alarmdaten, die in integriert werden können ServiceNow AI Platform Security Incidents für weitere Untersuchungen und Nachbesserungen.

Alarmprofile werden in erstellt ServiceNow AI Platform Instanz zum Anpassen der Unterschiede LogRhythm Alarmfelder werden auf einem angezeigt ServiceNow AI Platform Security Incident. Eine Standardzuordnung von Alarmfeldern wird bereitgestellt, die bearbeitet werden kann, um kundenspezifische Anforderungen zu erfüllen.

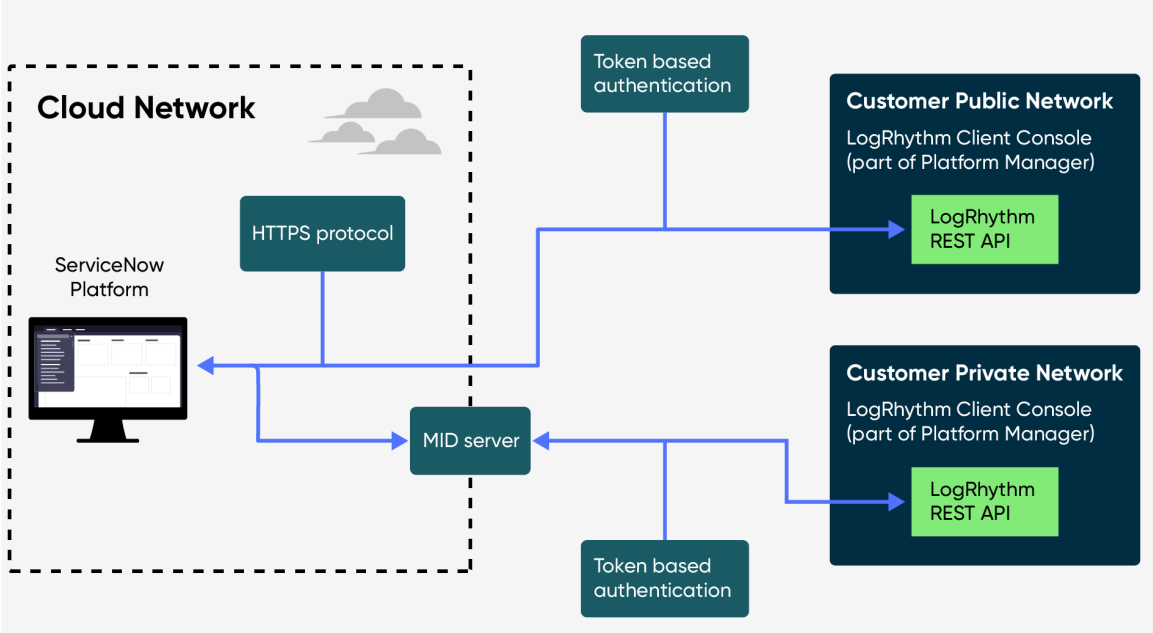
Die folgende Abbildung zeigt ein Beispiel für eine Kundenumgebung. Wenn ein Ereignis die Erstellung eines Security Incidents in auslöst ServiceNow AI Platform® Instanz wird eine Anforderung von gesendet ServiceNow AI Platform® Instanz zum Abrufen von Alarmen aus LogRhythm Client-Konsole entweder über einen MID-Server oder sogar ohne ihn.

Der REST API-Schlüssel wird von verwendet ServiceNow AI Platform® Dient zur Authentifizierung bei LogRhythm Client-Konsole. Diese Verbindung ermöglicht Ihren ServiceNow AI Platform Instanz zum Abrufen einer Einzelperson LogRhythm Alarme basierend auf konfigurierten Profilen.

Die REST-API wird verwendet, um Nachrichtendetails zu erfassen, auf die die REST-API nicht zugreift.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LogRhythm-Integration



Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Flexibilität, mehrere Alarmprofile für verschiedene Alarmtypen zu erstellen, z. B. Phishing Und Malware .
- Drag-and-Drop-Zuordnung von LogRhythm Zuzuordnende Alarmfeldwerte SIR Security Incident-Felder.
- Eine Vorschau von SIR Security Incident-Layout basierend auf LogRhythm Beispielalarme.
- Erfassen Sie historische Alarme sowie laufende zukünftige Alarme in konfigurierbaren Intervallen.
- Automatisiert LogRhythm Alarmabschluss am SIR Incident-Abschluss. Eine URL zu SIR Incident sowie eine Incident-ID werden zur einfachen Referenz bereitgestellt.

Unterstützte Releases von ServiceNow AI Platform

Diese Integration ist mit den Releases Quebec oder höher von kompatibel ServiceNow AI Platform®.

Unterstützte Versionen von LogRhythm

Diese Integration ist kompatibel mit LogRhythm7,8 oder höher. Die früheren Versionen werden aufgrund von API-Einschränkungen nicht unterstützt.

Hinweis:
Die folgenden Themen sind nummeriert. Um eine reibungslose Installation zu gewährleisten und die erwarteten Ergebnisse zu verifizieren, befolgen Sie die Themen in der Reihenfolge, in der sie angezeigt werden.

Richten Sie die REST-API für ein LogRhythm

Sie verwenden LogRhythm REST-API-Schlüssel zum Sammeln zusätzlicher Ereignisdetails für einzelne Alarmfelder. Der API-Schlüssel stellt Details bereit, die mit nicht verfügbar sind LogRhythm REST-API.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

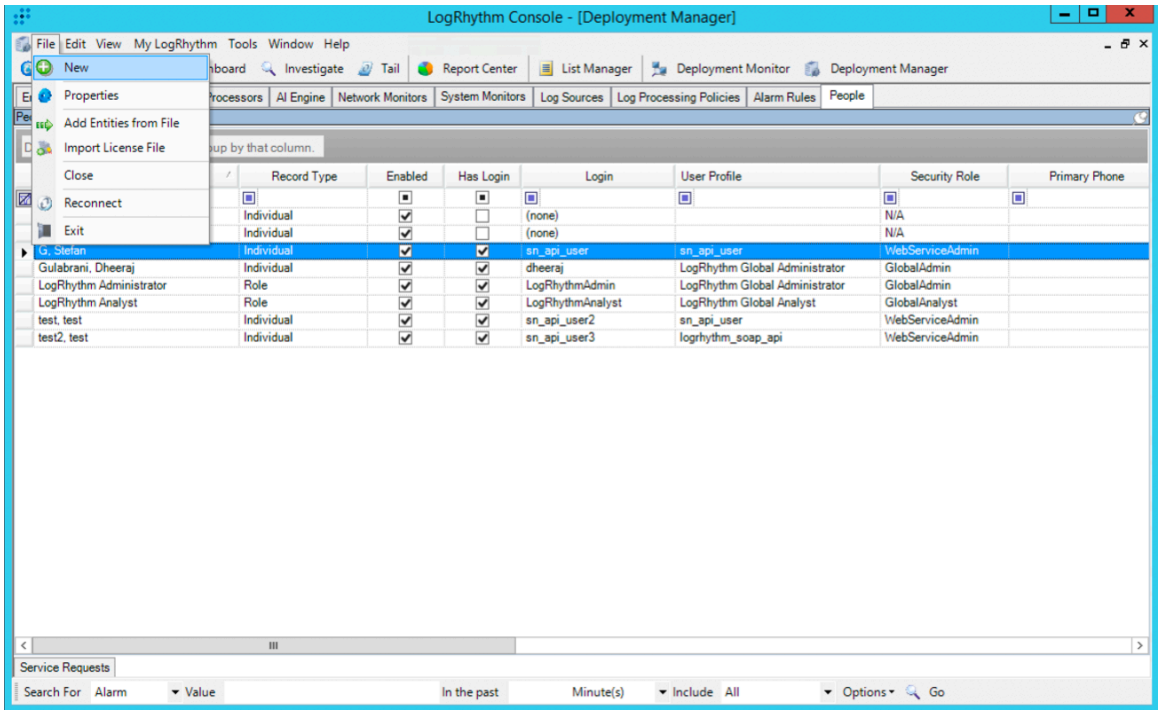
Erforderliche Rolle: LogRhythm Client-Konsole/Plattformmanager-Administrator

Warum und wann dieser Vorgang ausgeführt wird

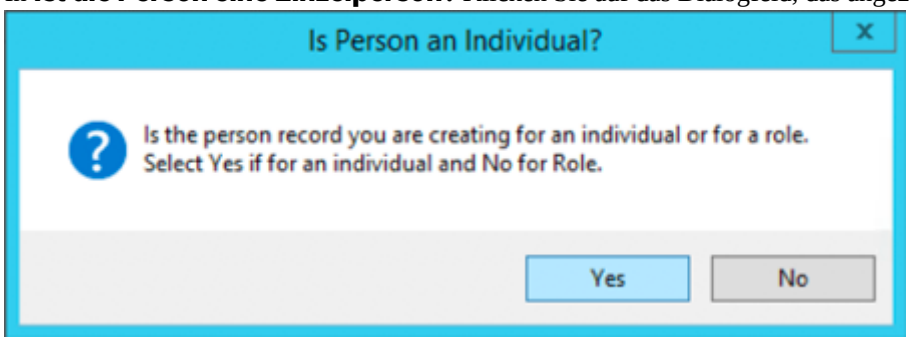
Diese Aufgabe wird für ausgeführt LogRhythm Client-Konsole. Richten Sie ein LogRhythm REST-API vor der Installation des Plugins aus dem ServiceNow Store.

Prozedur

1. Navigieren Sie zu LogRhythm Client-Konsole und wählen Sie aus **Datei** Menü.
2. Klicken Sie Auf **Neu** Um einen neuen Anwender zu erstellen.



3. In **Ist die Person eine Einzelperson?** Klicken Sie auf das Dialogfeld, das angezeigt wird **Ja** .

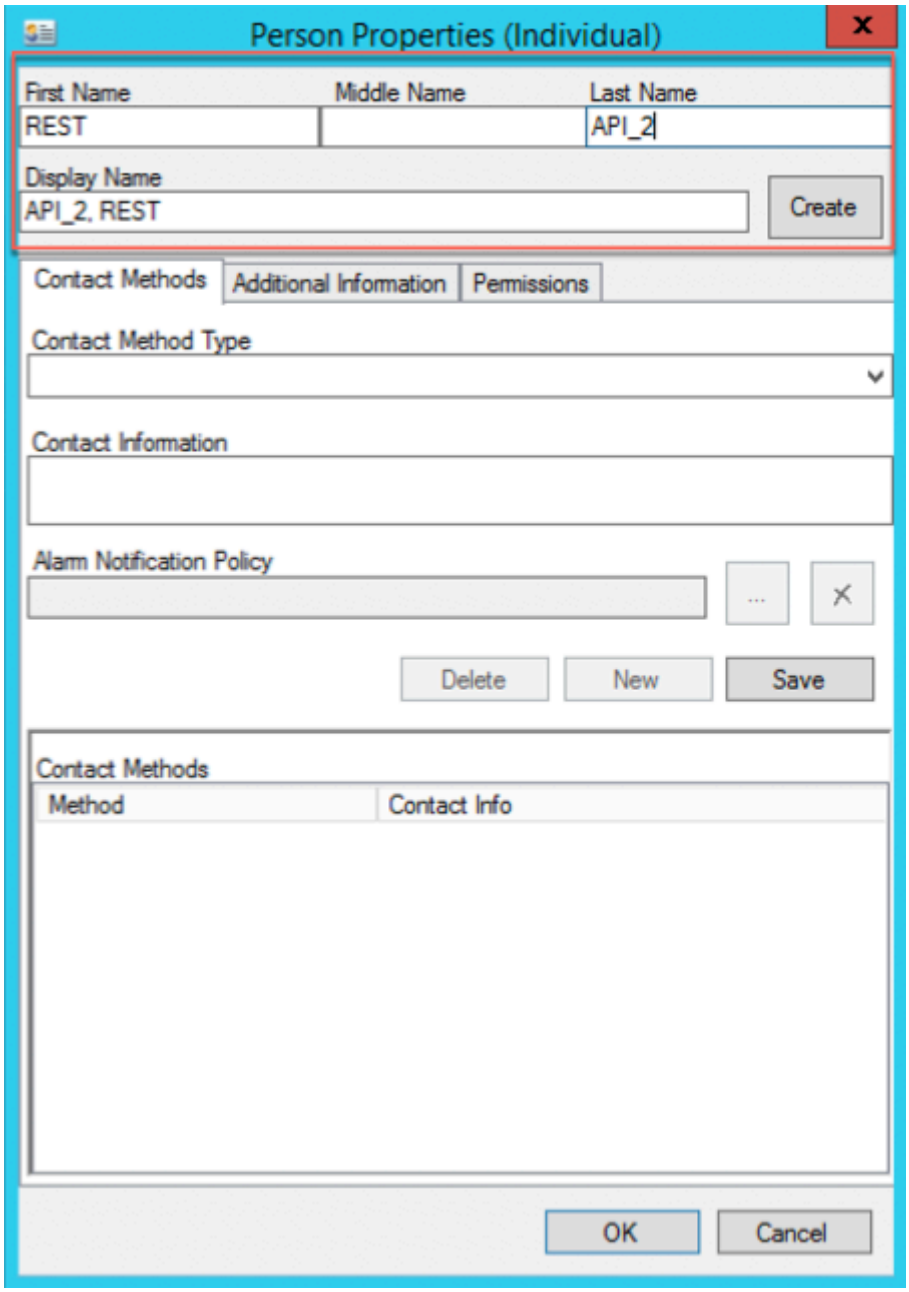


4. Füllen Sie im angezeigten Dialogfeld „Personeneigenschaften“ die Namensfelder aus.

   Verwenden Sie einen anderen Namen für LogRhythm REST API als die, die Sie zum Erstellen der REST API verwendet haben, z. B. `REST API_2` .

Automatische Übersetzung

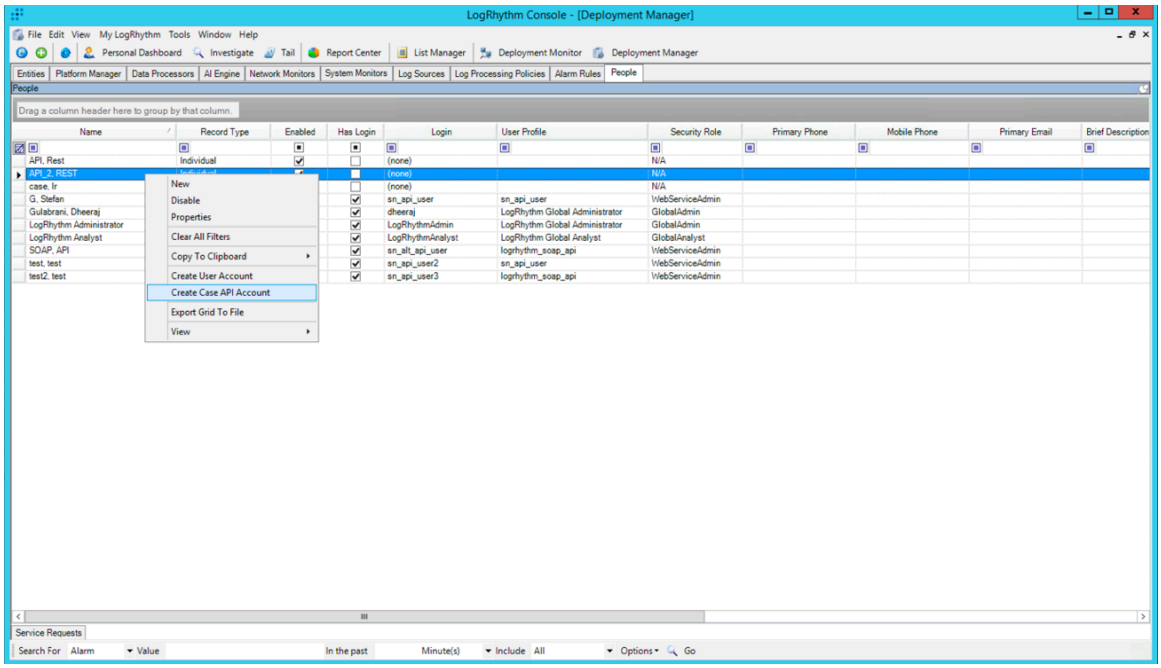
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **OK**.
6. Klicken Sie mit der rechten Maustaste auf die neue Liste in der Spalte Name (**API_2_REST**) Und wählen Sie in der Auswahlliste aus **Erstellen Sie einen Fall-API-Account** .

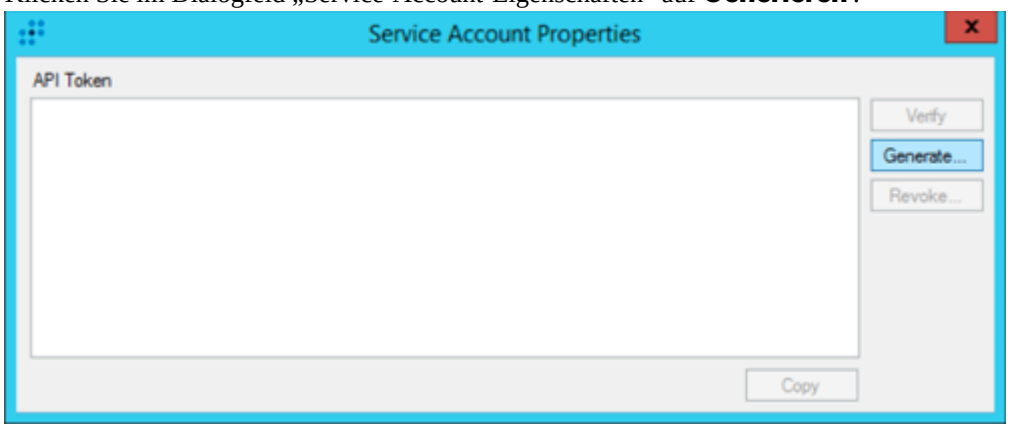
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

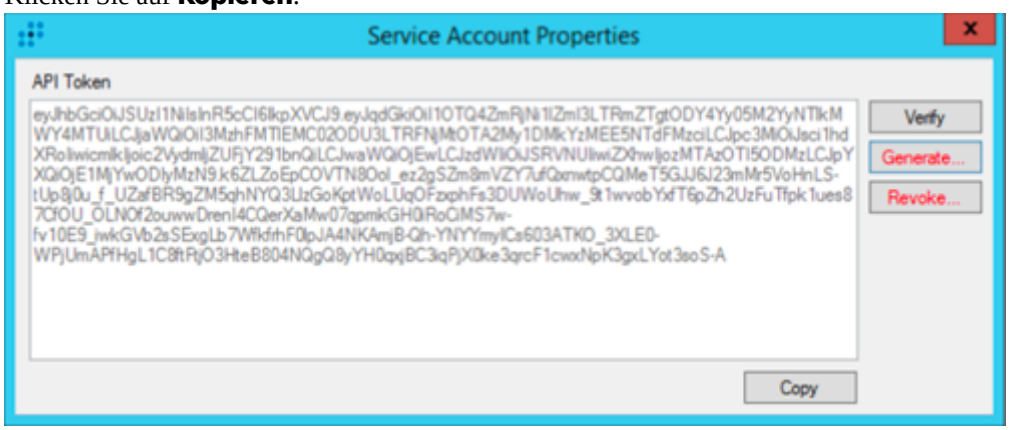


Hinweis:
Die Fall-API wird nicht verwendet, aber die Anmeldeinformationen für den Fall-API-Account und den LogRhythm REST API sind identisch.

7. Klicken Sie im Dialogfeld „Service-Account-Eigenschaften“ auf **Generieren** .



8. Klicken Sie auf **Kopieren**.



Sie haben jetzt eingerichtet LogRhythm REST-API. Sie fügen die im vorherigen Schritt kopierte Zeichenfolge in ein ServiceNow AI Platform Instanz in LogRhythm REST API-Token-Feld während der in aufgeführten Konfigurationsschritte Installieren Sie das Plugin, und konfigurieren Sie LogRhythm.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Sie sind jetzt bereit für Installieren Sie das Plugin, und konfigurieren Sie LogRhythm.

Installieren Sie das Plugin, und konfigurieren Sie LogRhythm

Bevor Sie die Integration in Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in integriert wird Security Operations Auf der ServiceNow AI Platform®.

Vorbereitungen

Erforderliche Rolle: Administrator

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich. Die neueste LogRhythm Version ist 7,8 oder höher.

Hinweis:
Ihre vorhandenen Alarmprofile werden am nicht mehr unterstützt LogRhythm Version, daher müssen Sie neue Alarmprofile erstellen und die erforderlichen Konfigurationen durchführen.

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform® Und Security Incident Response-Rollen (SIR).	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Der Systemadministrator (Administrator) installiert das Anwendungs-Plugin und weist die Rolle Security Incident-Administrator (sn_si.admin) zu. • Die (sn_si.admin) überwacht die folgenden Aufgaben: ◦ Benennt, erstellt und bearbeitet Alarmprofile. ◦ Ordnet Alarme zu und filtert sie – identifiziert bestimmte LogRhythm Alarme, die Security Incidents erstellen und konfigurieren, wie diese Alarmfelder einem zugeordnet werden ServiceNow AI Platform® Security Incident. ◦ Zeigt vor dem Abschluss der Konfiguration eine Vorschau der Security Incident-Details auf Richtigkeit an. ◦ Erfasst historische Alarme und Zeitpläne, die abgerufene Alarme haben. ◦ Weist die Rolle Security Incident Analyst (sn_si.Analyst) zu. ◦ Diese Rolle hat auch Zugriff auf Security Operations Modul.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	• Der Security Incident-Analyst (sn_si.Analyst) reagiert auf Security Incidents, die basierend auf den Alarmprofileinstellungen erstellt werden.
Besorgen Sie sich einen LogRhythm API-Anwendernamen und Passwort und verifizieren, dass Sie Version verwenden LogRhythm7,8 oder höher.	Besuchen Sie die Produktwebsite, um Informationen zu API-Schlüsseln zu erhalten und einen Account zu erstellen: LogRhythm Enterprise-Website . Die Anwenderaccounts, Anmeldeinformationen und Zertifikate müssen vor der Installation der Anwendung ordnungsgemäß konfiguriert werden. Die Integration erfordert LogRhythm Version 7,8 oder höher und LogRhythm REST-APIs. Weitere Informationen finden Sie unter Richten Sie die REST-API für ein LogRhythm.
Überprüfen Sie, ob Sie einen MID-Server installiert und konfiguriert haben.	Ein MID-Server ist in erforderlich ServiceNow AI Platform Umgebung. Siehe ServiceNow-Produktdokumentationswebsite Informationen zum Einrichten und Konfigurieren VON MID-Servern.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	Für das Rome-Release und spätere Familienveröffentlichungen Security Incident Response Abhängigkeits-Plugin (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Für die Integration erforderliche Anwendungen. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. **1.** Security Incident Response **2.** Sicherheits-Integrations-Framework **3.** Security Support Common **4.** Orchestration Des Sicherheitssupports

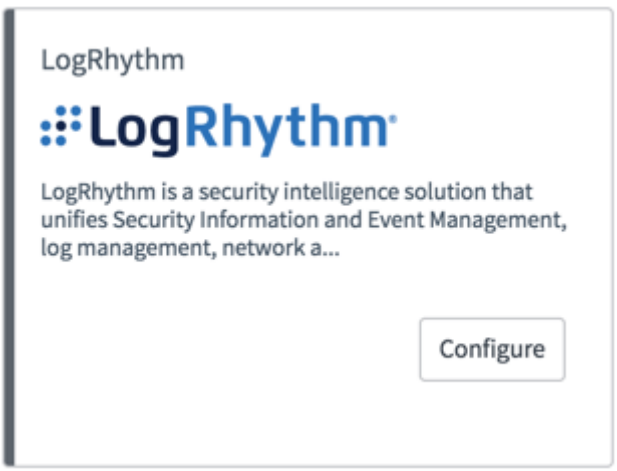
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz für die Integration finden Sie unter Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

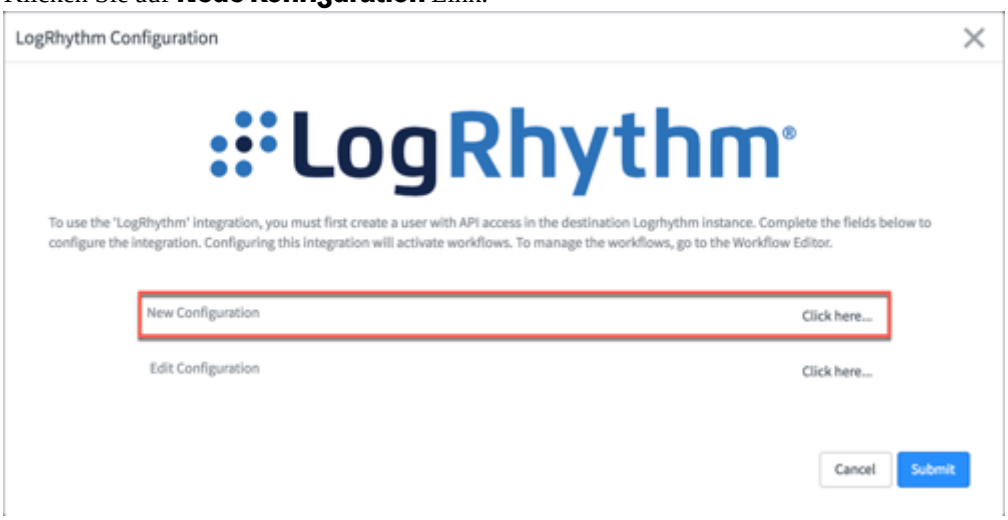
Wichtig:
Wenn Sie Verbindungsprobleme mit haben LogRhythm Clientkonsole, siehe Überprüfen Sie die Konnektivität für LogRhythm.

Prozedur

1. Wenn Sie die Anwendung für die Integration nicht installiert haben, finden Sie weitere Informationen unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Sobald die Installation abgeschlossen ist, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie LogRhythm Kachel.
3. Klicken Sie auf **Konfigurieren**.



4. Klicken Sie auf **Neue Konfiguration** Link.



5. Füllen Sie die Felder des Formulars aus.

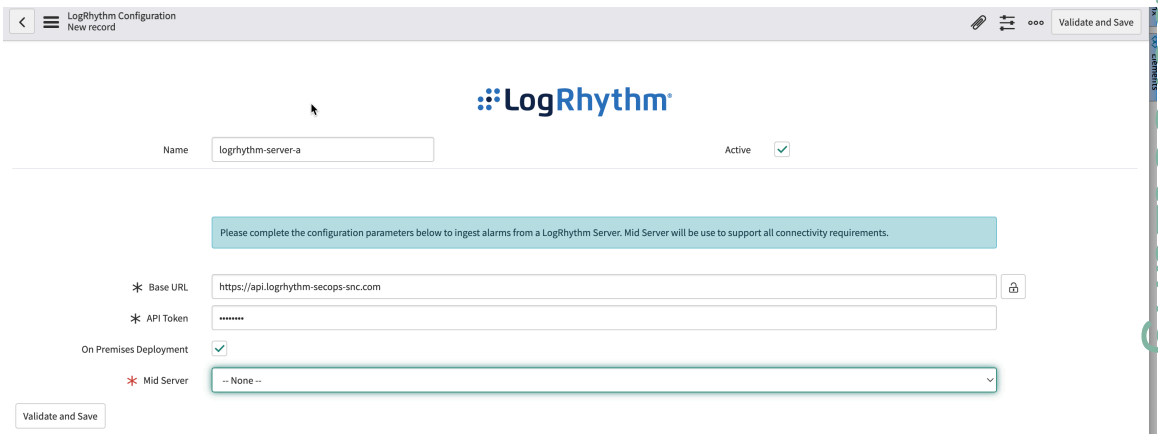
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LogRhythm-Konfiguration

Feld	Beschreibung
Name	LogRhythm Servername, z. B. `logrhythm-Server-A` .
Basis-URL	Basis-URL, die hostet LogRhythm REST-API. Der MID-Server ermöglicht den Zugriff auf das Netzwerk, in dem die LogRhythm-Client-Konsole gehostet wird. Diese URL ist, wo der LogRhythm Server wird in diesem Netzwerk gehostet. Klicken Sie auf das Schlosssymbol am rechten Ende, um das Feld zu bearbeiten und Text für eine URL einzugeben, z. B. `https://logrhythm.secops-eng.com:8501/` .
API-Token	Geben Sie das Token ein, das Ihrer REST-API zugeordnet ist, die Sie auf der erstellt haben LogRhythm Client-Konsole.
Lokale Bereitstellung	Option zur Auswahl, ob es sich um einen handelt LogRhythm Lokale Bereitstellung.
MID-Server	Bestimmter MID-Server, der in Ihrer Umgebung eingerichtet ist. Nur die aktiven MID-Server, die validiert wurden, sind in dieser Auswahlliste verfügbar.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.



6. Klicken Sie Auf **Validieren und speichern** .
   Nachdem die Validierung erfolgreich abgeschlossen wurde, werden eine Meldung und die angezeigt LogRhythm Konfigurationsseite wird neu geladen. Der nächste Schritt besteht darin, ein Alarmprofil zu erstellen.

Nächste Maßnahme

Nachdem Sie die Validierung erfolgreich abgeschlossen haben, ist der nächste Schritt bis Erstellen eines Alarmprofils für LogRhythm.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen eines Alarmprofils für LogRhythm

In einem Alarmprofil, das Sie erstellen und benennen, geben Sie an, welche Alarme Sie aus abrufen möchten LogRhythm Client-Konsole. Sie definieren auch, wie sie Feldern in einem zugeordnet werden ServiceNow AI Platform Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

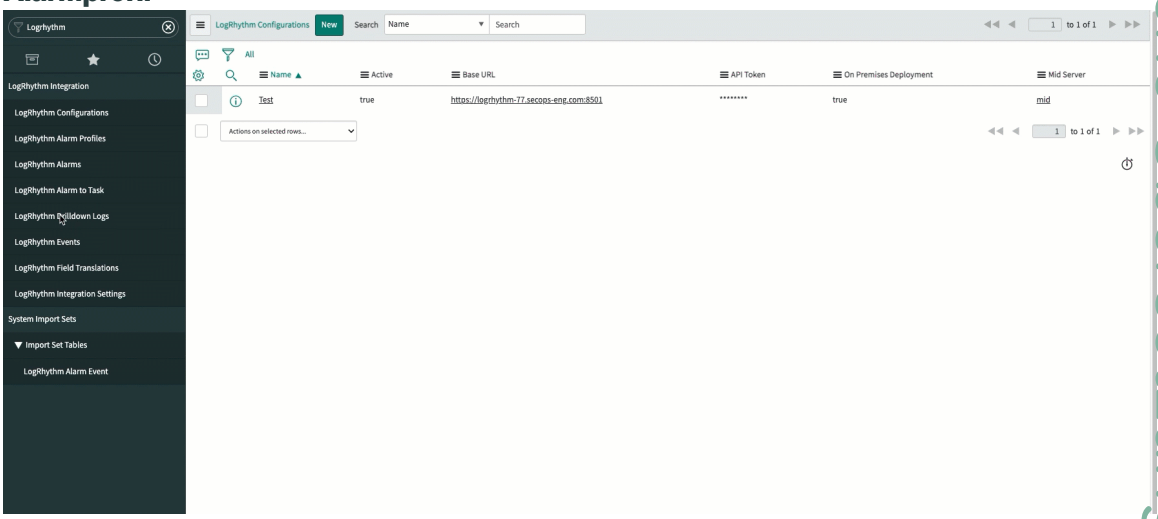
Warum und wann dieser Vorgang ausgeführt wird

Basierend auf dem konfigurierten Alarmprofil kann ein Alarmprofil alle Arten von Alarmen sofort erfassen, Sie können jedoch Filterkriterien verwenden, um bestimmte Arten von Alarmen zu erfassen. Wird verwendet ServiceNow AI Platform Integration werden alle konfigurierten Alarmregeln oder bestimmte basierend auf dem erstellten Profil erfasst. Alarmregeln wie nur Alarme mit hohem Risiko können dann gefiltert werden, um anzugeben, welche Alarme Security Incidents erstellen sollen. Bevor Security Incidents erstellt werden, werden einzelne Feldwerte in den gefilterten Alarmen den entsprechenden Feldern in zugeordnet ServiceNow AI Platform Security Incident. Diese Konfiguration erfolgt über ein Alarmprofil in Ihrem ServiceNow AI Platform Instanz.

Prozedur

1. Navigieren zu **Alle** > **LogRhythm-Integration**an.
2. Wählen Sie aus **LogRhythm-Alarmprofile** Modul zum Anzeigen von **Alarmprofile** Liste.

Alarmprofil



3. Klicken Sie auf, um ein neues Alarmprofil zu erstellen **Neu** .
   Ein neues Alarmprofilformular wird angezeigt. Oben auf der Seite in der Fortschrittsleiste **Name** Ist ausgewählt. Diese Leiste verfolgt Ihren Fortschritt während der Konfiguration.
4. Füllen Sie die Felder im Formular aus.

Alarmprofil

Feld	Beschreibung
Name	Name für das Alarmprofil. Dieser Name hilft Ihnen, die Alarmtypen zu identifizieren, z. B. *Nicht autorisierter Zugriff* (*VPN*), *Malware* , Oder *Phishing* .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Kurzbeschreibung	Kurztext für zusätzliche Informationen zum Alarmprofil, das den Typ der Alarme oder eine Alarmkategorie enthalten kann. Eine Beispielbeschreibung: Alle Alarme, die nicht autorisierten Powershell- und Sudo-Zugriffsversuchen zugeordnet sind.
Quelle	Quellserver aus der Auswahlliste. Die Liste besteht aus LogRhythm Konfigurationen, die Sie bereits eingerichtet haben, z. B. `logrhythm-Server-A` . Weitere Informationen finden Sie unter Installieren Sie das Plugin, und konfigurieren Sie LogRhythm.
Reihenfolge	Alarmprofilpriorität. Dieses Feld gibt die Reihenfolge an, in der die Alarmprofile ausgeführt werden, wenn mindestens zwei Alarmprofile die auslösenden Bedingungen gemeinsam haben.
Aktiv	Standardmäßig ist diese Option nicht ausgewählt. Nachdem Sie alle Schritte zur Einrichtung des Alarmprofils abgeschlossen haben, und klicken Sie auf **Beenden** , Sie werden aufgefordert, dieses Kontrollkästchen zu aktivieren, um das Alarmprofil zu aktivieren. Wenn das Alarmprofil aktiv ist, werden Alarme aus dem abgerufen LogRhythm Clientkonsole automatisch.

5. Klicken Sie Auf **Fahren Sie Fort** Um Ihre Daten zu speichern und mit dem Zuordnungsformular fortzufahren.

   Wenn die Validierung erfolgreich ist, werden die Seite und neu geladen **Zuordnung** Formular wird angezeigt. Sie können mit der Konfiguration erst fortfahren, wenn Sie Ihre Verbindung und Ihre Anmeldeinformationen erfolgreich validiert haben.

Zugehörige Informationen

Zuordnung

Zuordnung

Nachdem Sie ausgewählt haben LogRhythm Quelle, die Sie erfassen möchten. Sie müssen einzelne zuordnen LogRhythm Alarmfelder für ServiceNow AI Platform Security Incident-Felder.

Die Zuordnung von Alarmen umfasst die folgenden Aufgaben:

- Zuordnung LogRhythm Alarme. Für diese Aufgabe Listen Sie Beispielalarme auf, und erfassen (abrufen) Sie sie mithilfe der Alarm-IDs oder der neuesten Alarme aus dem LogRhythm Client-Konsole.
- Die Beispielalarmfelder sind in drei Gruppen kategorisiert:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Alarmfelder : Die verfügbaren Alarmfelder und die entsprechenden Werte werden angezeigt.
- Ereignisfelder : Die verfügbaren Ereignisfelder und die entsprechenden Werte werden angezeigt.
- DrillDownLog-Felder : Die verfügbaren Drilldown-Protokollfelder und die entsprechenden Werte werden angezeigt.

- Jede von Ihnen abgerufene Alarm-ID wird als Registerkarte angezeigt. Überprüfen Sie auf den Registerkarten „Alarm-ID“, ob alle Felder für kritische Alarme aus dem vorhanden sind Alarmbeispielerfassung Abschnitt auf der linken Seite des Formulars sind dem zugeordnet SIR-Incident-Feldzuordnung Abschnitt auf der rechten Seite des Formulars.
- Nachdem Sie die Alarme dem zugeordnet haben SIR-Incident-Feldzuordnung Feld können Sie sehen, dass die Alarmkategorie auch in angezeigt wird Eingabeausdruck Feld. Beispiel: ${Alarm: Alarmid}$.
- Sie können die Konfiguration ändern, indem Sie dem Security Incident Felder hinzufügen oder entfernen. Verfolgen Sie übersehene oder duplizierte Felder mit der bereitgestellten Farbcodierung nach.
- Sie können Alarme filtern, um anzugeben, welche Alarme in die SIR-Anwendung aufgenommen werden. Sie können die Alarme entweder direkt filtern oder die Alarmkategorien verwenden, um Ihre Suche basierend auf Alarmen, Ereignissen oder DrillDownLogs aufzurufen.
- Verwenden Sie den Skripteditor, wenn Sie Werte für die Felder Priorität und Kategorie im Security Incident formatieren möchten.

Der nächste Schritt ist bis Zuordnung LogRhythm Alarmfelder zu Security Incident-Feldern.

Zugehörige Informationen

Zuordnung LogRhythm Alarmfelder zu Security Incident-Feldern

Verwenden Sie zum Formatieren den Skripteditor LogRhythm Werte

Alarme für filtern LogRhythm

Zuordnung LogRhythm Alarmfelder zu Security Incident-Feldern

Sie ordnen den Security Incident-Feldern einzelne Alarmfelder zu. Die vorkonfigurierte Zuordnung kann bearbeitet werden, und die Farbcodierung für die Felder hilft Ihnen, Alarme zu überwachen, die Sie bereits zugeordnet haben. Mit diesem Schritt können Sie visualisieren, wie sich Ihre Änderungen auf die Felder für den Security Incident auswirken.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Wenn Sie mit nicht vertraut sind LogRhythm Alarme, navigieren Sie zu LogRhythm Client-Konsole und überprüfen Sie einige Beispiele für Alarm-IDs. Für das folgende Beispiel: LogRhythm Alarme 9468 Und 9474 Wurden verwendet, um die Alarme dem Security Incident zuzuordnen.

Warum und wann dieser Vorgang ausgeführt wird

Mit diesem Formular ordnen Sie zu LogRhythm Alarmregeln auf der linken Seite zu den Security Incident-Feldern auf der rechten Seite.

Die folgende Abbildung zeigt die Standardzuordnung von Alarmen, die für jedes Alarmprofil vorkonfiguriert ist. Diese Standardzuordnung kann bearbeitet werden, und mit diesem Formular passen Sie die Felder an, die den Security Incident ausfüllen. Nachdem Sie

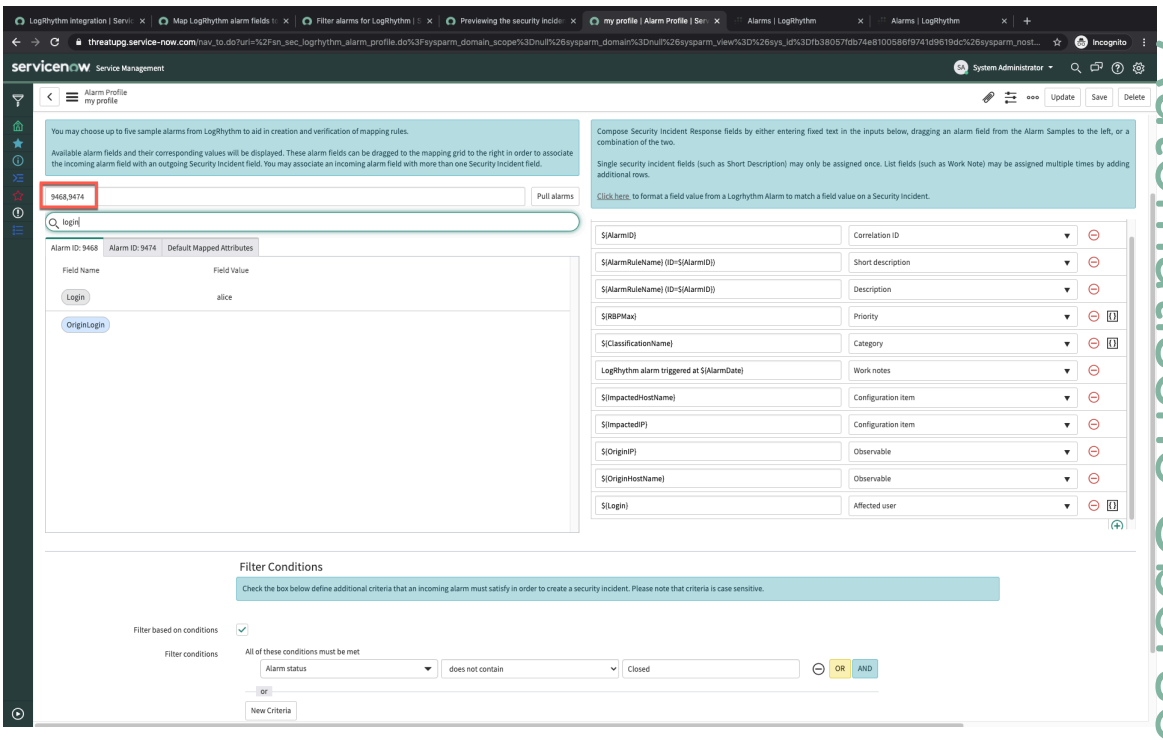
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

diese Zuordnung abgeschlossen haben, können Sie sehen, wie sich das Hinzufügen oder Entfernen von Alarmfeldern potenziell auf die Feldwerte für den Security Incident auswirkt.

Auf der linken Seite dieses Formulars in der folgenden Abbildung LogRhythm Alarmregeln sind umrissen. Die Werte dieser Alarmregeln werden den Security Incident-Feldern auf der rechten Seite des Formulars zugeordnet.

Prozedur

1. Klicken Sie nach dem Erstellen eines Alarmprofils für LogRhythm auf **Zuordnung** Auf der Fortschrittsleiste.
2. In **Alarmbeispielerfassung** Geben Sie bis zu fünf Beispiele ein LogRhythm Alarm-IDs durch Kommas getrennt (9468,9474).



3. Klicken Sie neben dem Alarmfeld auf **Alarme Abrufen** .

   Der Abruf für Beispielalarme kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt.

   Nachdem die Beispielalarm-IDs übermittelt und erfolgreich aus abgerufen wurden LogRhythm Server, die Alarmfelder und die entsprechenden Werte werden auf Registerkarten angezeigt.

Hinweis:

Nachdem eine Alarm-ID erfolgreich abgerufen wurde, wird ServiceNow AI Platform Kann die folgende Nachricht zurückgeben: Die folgenden neuen Felder sind in Kürze zum Filtern verfügbar. Laden Sie dieses Profil in einigen Minuten neu, wenn eine Filterung basierend auf diesen Feldern erforderlich ist. Itemspacketsin, itemspacketsout .

Diese Meldung tritt auf, wenn der einzelne Alarm, der abgerufen wurde, Feldnamen enthält, die zuvor nicht von verarbeitet wurden ServiceNow AI Platform. Diese Felder sind für die Zuordnung verfügbar. Wenn diese Nachricht angezeigt wird, laden Sie das Formular neu, damit diese Felder in den Filterauswahllisten des Bedingungsgenerators angezeigt und verfügbar sind, wenn Sie bereit sind, Filterbedingungen festzulegen.

Automatische Übersetzung

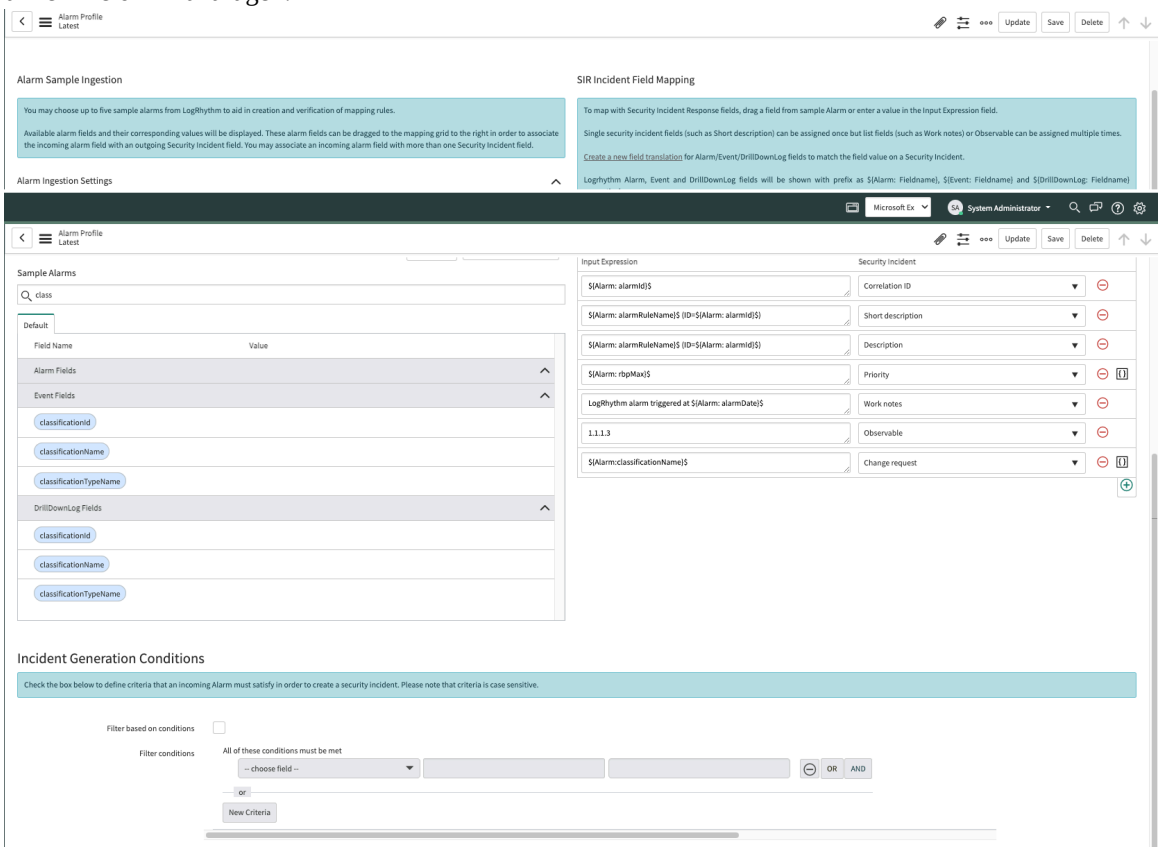
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch die Erfassung dieser Beispielalarme in der Alarmprofilkonfiguration können Sie verhindern, dass Alarmfelder dem Security Incident zugeordnet werden, die keine Werte enthalten. Außerdem werden Alarmfelder mit Werten an den entsprechenden Feldern im Security Incident ausgerichtet. Dieser Schritt stellt sicher, dass alle Felder für kritische Alarme zugeordnet sind und keine fehlenden Feldwerte für den Security Incident vorhanden sind.

Damit Sie sicherstellen können, dass im Zuordnungsprozess keine Alarme übersehen oder dupliziert werden, sind Alarmfelder farbcodiert. Ein hellblaues Alarmfeld (Account , AlarmRuleID , Alarmstatus , Usw.) gibt an, dass noch kein Feld für die Zuordnung zu einem Security Incident ausgewählt ist.

Ein graues Feld (Alarmdatum , AlarmID , Und Alarmregelname) Gibt an, dass bereits ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen, da in bestimmten Fällen ein Alarmfeld mehreren Feldern in einem Security Incident zugeordnet werden kann. Zum Beispiel die Erkennbare Elemente Und Arbeitsnotiz Felder können mehr als einen Wert haben.

4. Klicken Sie auf, um die Beispielalarmdaten zu löschen **Löschen Sie Beispielalarmdaten** .
5. Um die Standardkonfiguration für den Security Incident zu bearbeiten, führen Sie die folgenden Schritte aus, um ein Feld hinzuzufügen:



   a. Klicken Sie unten rechts im Formular auf das Plus-Symbol.
   Ein neues Feld wird angezeigt.

   b. Wählen Sie in der Spalte Security Incident ein verfügbares Feld aus der Auswahlliste aus.

   In der erweiterten Auswahlliste sind einige der Felder schattiert. Beispiel: Kategorie Hat einen grauen Hintergrund, was darauf hinweist, dass er im Security Incident zugeordnet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wurde. Ähnlich der Farbcodierung für LogRhythm Alarmfelder. Diese Farbcodierung für die Security Incident-Felder stellt sicher, dass Werte aus den Alarmfeldern nicht versehentlich demselben Security Incident-Feld zugeordnet werden.

In der Abbildung oben die Alarmregel ${Alarm:classificationName}$ Ist bereits zugeordnet Kategorie Feld im Security Incident in diesem Profil.

Hinweis:
Das Feld „erkennbares Element“ kann mehr als dem Feld desselben Security Incidents zugeordnet werden, sodass mehrere erkennbare Elemente angezeigt werden können. Ebenso wird Konfigurationselement Und Arbeitsnotizen Felder können zugeordnet werden, um mehrere Werte anzuzeigen.

Auf der Seite „Alarmbeispielerfassung“ des Formulars gibt Blau an, dass kein Alarmregelfeld zugeordnet wurde. Grau gibt an, dass es zugeordnet wurde. In der Auswahlliste auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars gibt weiß an, dass ein Feld nicht zugeordnet wurde. Grau gibt an, dass ein Feld zugeordnet wurde. Verwenden Sie diese Farbcodierung, um Ihre Feldzuordnung nachzuverfolgen.

In der obigen Abbildung Betroffener Anwender Wurde aus der Auswahlliste als neues Feld im Security Incident ausgewählt.

c. Klicken Sie im Abschnitt „Alarmbeispielerfassung“ auf der linken Seite des Formulars mit der linken Maustaste, um die gewünschte Alarm-ID im Feld „Eingabeausdruck“ auszuwählen.

In der obigen Abbildung Melden Sie Sich An Wurde ausgewählt.

d. Ziehen Sie es in das gelöschte Feld, und geben Sie es frei.
In der linken Spalte im Abschnitt SIR-Incident-Feldzuordnung der neue Wert für Betroffener Anwender Feld wird angezeigt. In diesem Fall wird Melden Sie Sich An Wert aus LogRhythm Alarm wird in angezeigt Betroffener Anwender Feld im Security Incident.

6. Alternativ können Sie zum manuellen Eingeben eines Werts für Felder in der Spalte „Eingabeausdruck“ Ihren Cursor in das Feld „Eingabeausdruck“ setzen und einen gewünschten Alarmwert eingeben.

Beispiel: In der obigen Abbildung wurde ein anderes Feld hinzugefügt (Zuweisungsgruppe) Zum Security Incident-Formular, und Security Incident-Zuweisung Wurde manuell in das Feld eingegeben.

7. Fahren Sie mit der Bearbeitung der vorkonfigurierten Zuordnung nach Bedarf fort.
Wenn Sie Werte aus übersetzen müssen LogRhythm Alarmfelder mit Werten, die von den Feldern im Security Incident unterstützt werden, können Sie den Skript-Editor verwenden. Weitere Informationen finden Sie unter Verwenden Sie zum Formatieren den Skripteditor LogRhythm Werte.

Nächste Maßnahme

Nachdem Sie die Feldzuordnung abgeschlossen haben, ist der nächste Schritt bis Alarme für filtern LogRhythm.

Alarme für filtern LogRhythm

Durch das Festlegen von Filterkriterien für Alarme, nachdem Sie Felder zugeordnet haben, können Sie bestimmen, welche Alarme in die SIR-Anwendung aufgenommen werden sollen. Durch das Filtern von Alarmen können Sie die Anzahl der Alarme, die Sie erfassen, erheblich reduzieren, wenn das Alarmprofil aktiviert ist.

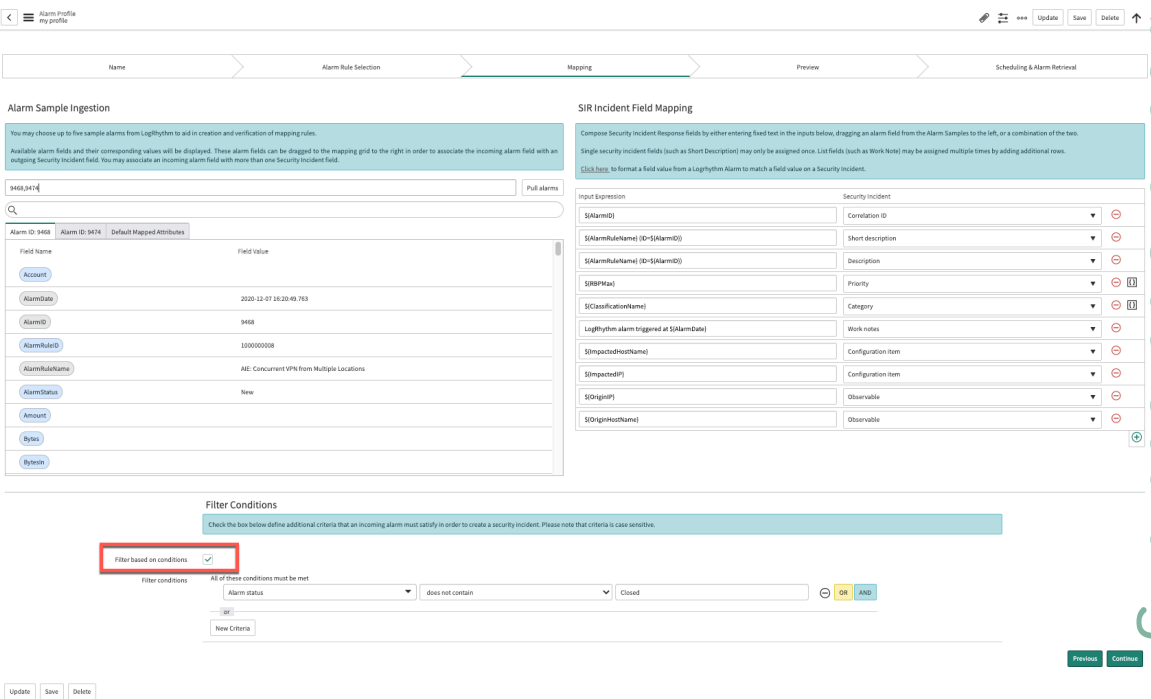
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie die Filterbedingungen unten im Zuordnungsformular, um bestimmte Alarme herauszufiltern oder die Erfassung auf Alarme zu beschränken, die bestimmte Kriterien auf Feldebene erfüllen. Durch das Filtern wird die Anzahl der Alarme, die Sie erfassen, erheblich reduziert, sobald das Alarmprofil aktiviert ist. Verwenden Sie die Filterung, um eine verwaltbare Menge von Alarmen zu erfassen, die Ihre Security Operations Center (SOC)-Mitarbeiter unterstützen können.

Hinweis:
Das folgende Beispiel zeigt eine Standardfiltereinstellung, in der Alarmstatus-hat-nicht-enthält-geschlossen Ist die Standardeinstellung. Dieser Filter ruft nur aktive Alarme ab, und diese Einstellung reduziert die Anzahl der abgerufenen Alarme. Die folgenden Schritte veranschaulichen, wie Sie einen weiteren nützlichen Filter hinzufügen, der nur Alarme mit den höchsten Schweregrad- oder Prioritätswerten enthält.

Prozedur
1. Um die Filterkriterien zu bearbeiten, wählen Sie aus **Filtern Sie basierend auf Bedingungen** Kontrollkästchen.

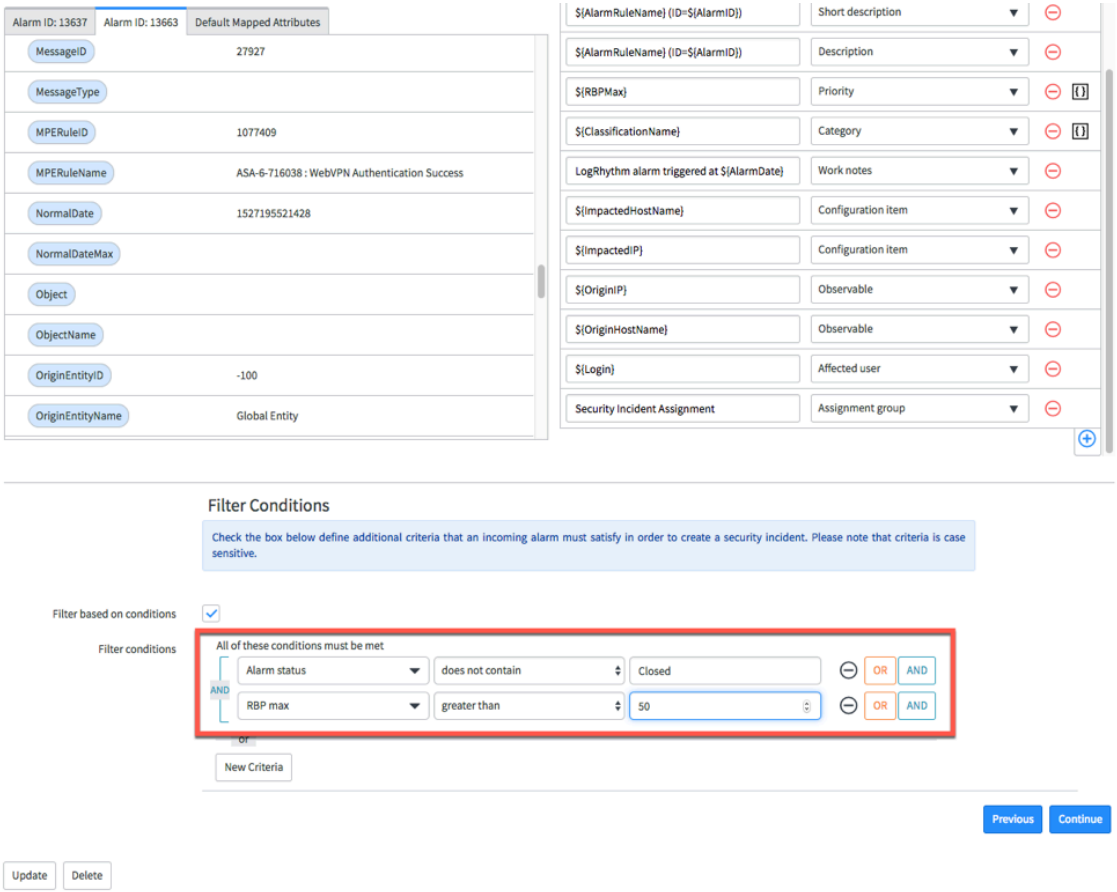


2. Rechts von **Filterbedingungen** Feld klicken Sie auf **ODER** Oder **UND** .
3. Wählen Sie in der neuen Zeile, die angezeigt wird, die Filterbedingungen aus den Auswahllisten aus.

Die folgende Abbildung zeigt einen zusätzlichen Filter, der den Kriterien hinzugefügt wurde, in der risikobasierte Priorität (RBP max) Ist größer als 50 . Nur mit dieser Filtereinstellung LogRhythm Alarme mit einem risikobasierten Prioritätswert, der größer als 50 ist, werden abgerufen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Nachdem Sie überprüft haben, dass alle kritisch sind LogRhythm Alarmfelder werden dem zugeordnet ServiceNow AI Platform Security Incident und Sie haben Filterkriterien festgelegt, um die Alarmerfassung zu beschränken. Wählen Sie eines aus, um die Konfiguration fortzusetzen.

Nächste Maßnahme

Der nächste Schritt besteht darin, eine Vorschau Ihrer zugeordneten Felder für den Security Incident anzuzeigen. Weitere Informationen finden Sie unter Vorschau des Security Incidents mit zugeordnet anzeigen LogRhythm Alarmwerte.

Vorschau des Security Incidents mit zugeordnet anzeigen LogRhythm Alarmwerte

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie den Feldern im Security Incident zugeordnet haben. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle kritischen zugeordnet haben LogRhythm Alarmfelder, die im Security Incident angezeigt werden sollen.

Erforderliche Rolle: sn_si.admin.

Security Incident

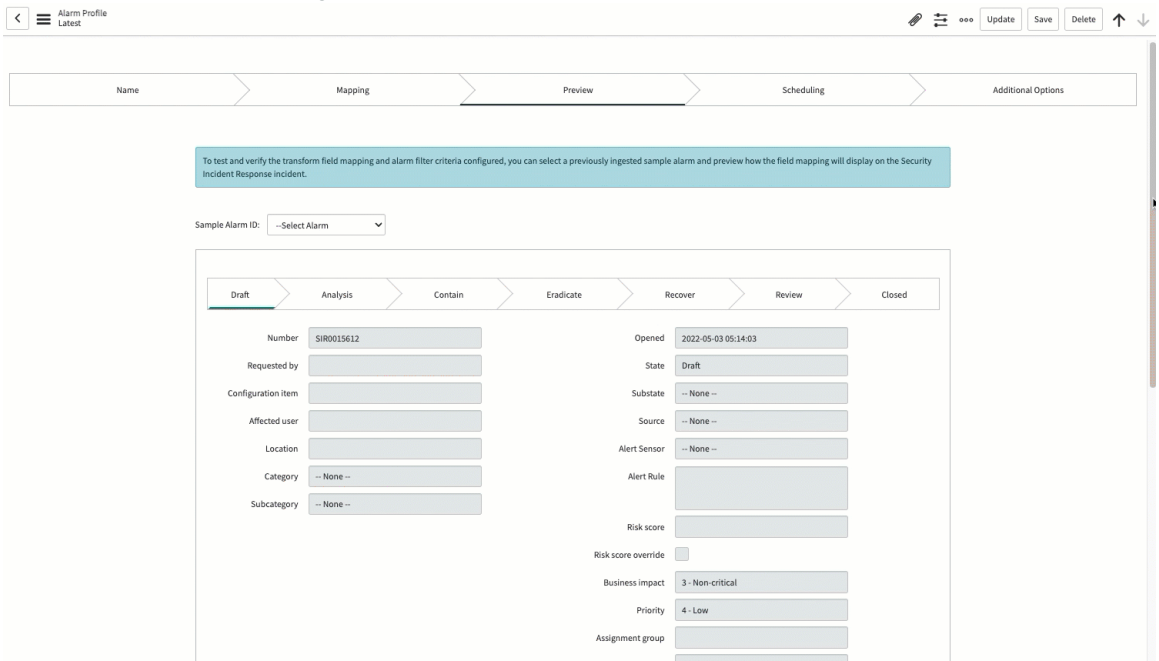
Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie auf **Vorschau** In der Fortschrittsleiste.

Ein Beispiel für die Vorschau für das gesamte ServiceNow AI Platform Security Incident wird in den beiden folgenden Abbildungen angezeigt. Dieses Beispiel der Vorschau des Security Incidents wird mit ausgefüllt LogRhythm Alarmfelder, die dem Beispielalarm zugeordnet sind 13663 .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung ist Konfigurationselement , Betroffener Anwender , Priorität , Zuweisungsgruppe , Und Kurzbeschreibung Felder des Security Incidents werden ausgefüllt.

Obere Hälfte des Security Incidents



In der unteren Hälfte des Security Incident-Formulars die Beschreibung Feld ist ausgefüllt. Im Abschnitt zugehörige Elemente wird die Konfigurationselement , Erkennbares Element , Und Arbeitsnotiz Felder werden mit Werten ausgefüllt. Wenn mehrere Werte für diese Felder zugeordnet sind, wird jeder Wert im Security Incident angezeigt, da jedes dieser Felder mehr als einen Wert akzeptieren kann.

Fehlerbedingungen in der Vorschau

Die folgenden Warnmeldungen können bei der Vorschau des Security Incident angezeigt werden. Wenn ein Beispielalarm die Filterkriterien nicht erfüllt, wird der gesamte Security Incident nicht ausgefüllt.

Eingabewert nicht gefunden

Wenn die Alarm-ID in den Filterbedingungen enthalten ist, kann dennoch eine Warnmeldung angezeigt werden, wenn für bestimmte zugeordnete Felder keine spezifischen Eingabewerte gefunden werden. Im folgenden Beispiel wird in der Vorschau des Datensatzes davon ausgegangen, dass kein Wert in vorhanden ist Zugewiesen an Feld, obwohl es zugeordnet wurde.

Überprüfen Sie für diesen Nachrichtentyp im Zuordnungsdatensatz, ob der Eingabewert korrekt ist. In diesem Fall die Person in Zugewiesen an Das Feld in Security Incident ist in falsch ServiceNow AI Platform Instanz. Wenn dieser Alarm erfasst wird und ein Security Incident mit dieser Bedingung erstellt wird, werden Felder mit diesem Eingabewert (Abel Tuter) Werden im Security Incident leer gelassen.

Die verbleibenden blauen Nachrichten sind informativ und zeigen an, dass diese Felder keinen Wert zum Anzeigen in der Vorschau haben. Diese Vorschau ermöglicht es dem Security Incident-Administrator, das Alarmprofil zu konfigurieren, um sicherzustellen, dass diese Felder in der Anfangsphase keinen Wert haben, da in bestimmten Fällen Security Incident-Felder später automatisch ausgefüllt werden können. Andere Zuordnungsfehler werden ebenfalls angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie mit der Zuordnung und der Security Incident-Vorschau zufrieden sind, wählen Sie eine aus, um mit der Konfiguration fortzufahren.

Option	Beschreibung
Klicken Sie Auf **Fahren Sie Fort** Oder **Zeitplanung** In der Fortschrittsleiste.	Wechseln Sie zu **Planung Und Alarmabruf** Formular. **Planung Und Alarmabruf** Ist im Fortschrittsbalken ausgewählt. Der nächste Schritt besteht darin, den Alarmabruf zu planen.
Klicken Sie Auf **Zurück** .	Kehren Sie zum Alarmprofil zurück, und fahren Sie mit der Zuordnung fort.
Geben Sie eine andere Alarm-ID in ein **Beispiel für Alarm-ID** Auswahlliste oben im Vorschauformular.	Die **Beispiel für Alarm-ID** Die Auswahlliste wird für jede von Ihnen eingegebene Alarm-ID angezeigt. Sie können bis zu fünf Alarme auswählen. Mit dieser Option können Sie eine weitere Vorschau anzeigen LogRhythm Alarm-ID für einen Security Incident.

Nachdem Sie die Vorschau des Security Incidents angezeigt haben und mit den Ergebnissen zufrieden sind, ist der nächste Schritt bis Planen und abrufen LogRhythm Alarme.

Planen und abrufen LogRhythm Alarme

Nachdem Sie eine Vorschau des Security Incidents mit anzeigen LogRhythm Alarme, die Sie ausgewählt und zugeordnet haben, sind Sie bereit, den Alarmabruf zu planen. Nachdem Sie diesen Schritt abgeschlossen haben, kann das Alarmprofil aktiviert werden.

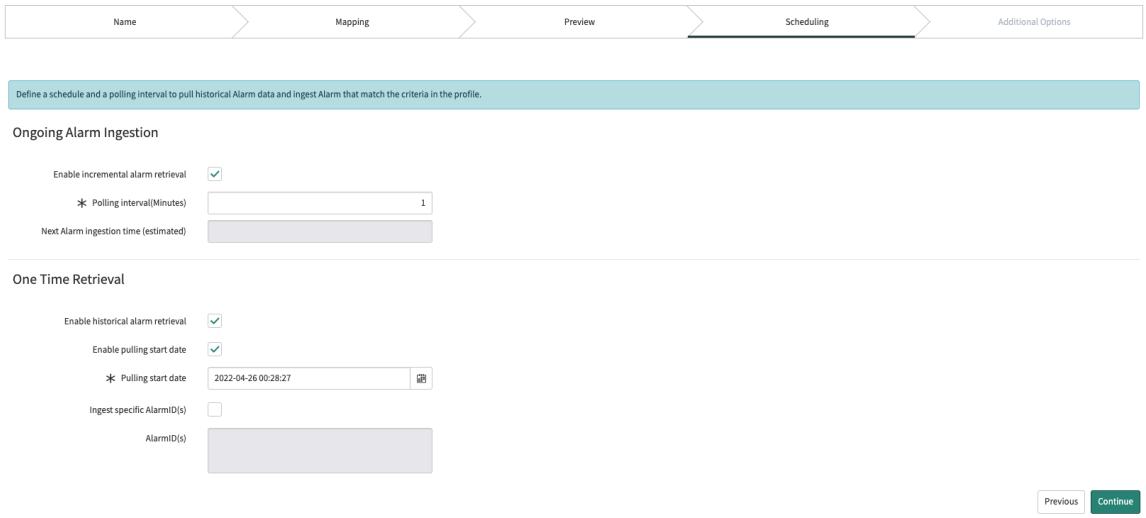
Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Mit der Zeitplanung können Sie die Zeitplanung und die Typen der zum Abruf ausgewählten Alarme ändern. Sie filtern die Alarme, die Sie erfassen, basierend auf einem Datumsbereich oder bestimmten Alarm-IDs. Mit diesem Schritt legen Sie fest, ob Sie historische Alarme erfassen möchten und wie oft Sie zukünftige Alarme abrufen, die der Alarmprofilkonfiguration entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie auf **Zeitplanung** Gehen Sie auf den Fortschrittsbalken.

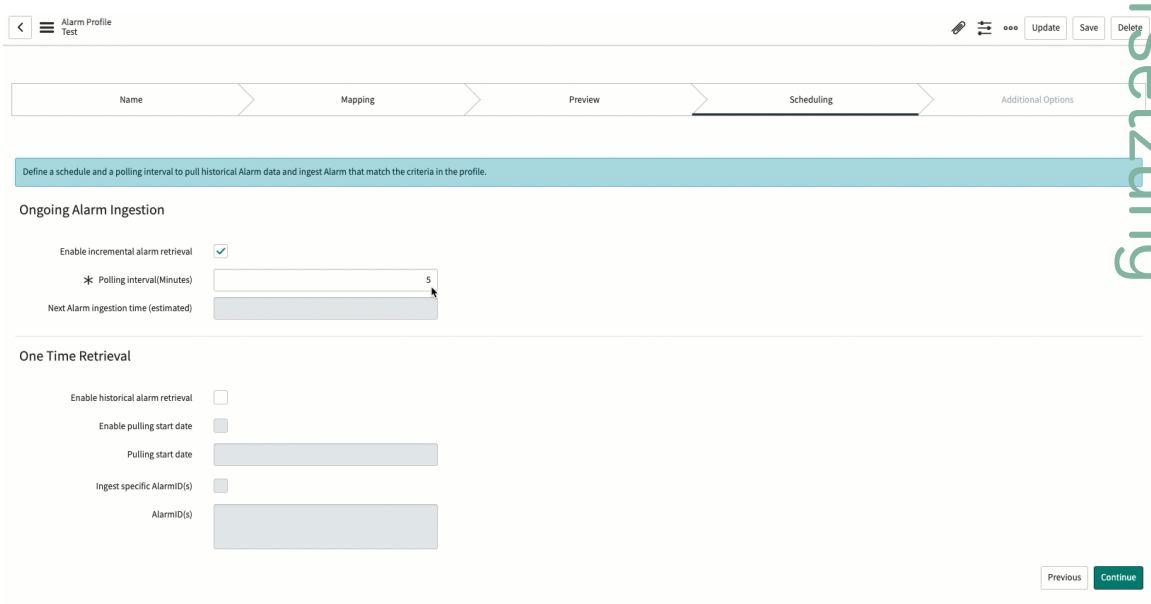


2. Wählen Sie aus den folgenden Optionen aus, um Ihren Alarmabruf zu konfigurieren.

3. Um den historischen Alarmabruf zu bearbeiten, führen Sie die folgenden Schritte aus, um ein Datum für den Alarmabruf oder eine bestimmte Alarm-ID einzugeben.

   a. Wählen Sie Aus **Aktivieren Sie das Abrufen des Startdatums** , Und wählen Sie dann aus **Startdatum wird abgerufen** .

   b. In **Startdatum wird abgerufen** Klicken Sie auf den angezeigten Kalender, und wählen Sie das Datum gefolgt vom grünen Häkchen aus, um Ihren Eintrag zu speichern.



   Das Datum wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Alternativ wählen Sie aus **Spezifische Alarm-ID(s) erfassen** Option, und in der **Alarm-ID(s)** Geben Sie die spezifischen Alarm-IDs für die Verlaufsdaten ein, um bestimmte Alarm-IDs abzurufen.

   Sie können bis zu fünf durch Kommas getrennte Alarme eingeben.

d. Klicken Sie auf **Aktualisieren**.

4. Wählen Sie eine der folgenden Optionen aus, um mit der Bearbeitung fortzufahren oder die Konfiguration abzuschließen.

Nächste Maßnahme

Nachdem Sie die Details zur laufenden Alarmerfassung und zum einmaligen Abruf konfiguriert haben, ist der nächste Schritt bis Zusätzliche Optionen für LogRhythm Alarme.

Zusätzliche Optionen für LogRhythm Alarme

Die LogRhythm Die Enterprise-Integration bietet Ihnen die Möglichkeit, automatisch zu aktualisieren oder zu schließen LogRhythm Alarme basierend auf den Security Incidents.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie die Option Alarm-Erstaktualisierungen aktivieren, werden die Alarme automatisch in den LogRhythm-Kommentaren mit den ersten Alarmaktualisierungen aktualisiert.
Wenn Sie die Option Alarm-Abschlussaktualisierungen aktivieren, werden die Alarme in LogRhythm zusammen mit dem SIR-Abschlusscode und und den Abschlusskommentaren automatisch geschlossen.

Die LogRhythm Alarm-ID ist mit verbunden ServiceNow AI Platform Security Incident-ID während des gesamten Lebenszyklus des Incident. Diese Korrelation ermöglicht das gleichzeitige und automatisierte Schließen von Security Incidents/Alarmen. Wenn Security Incident Response(SIR) Der Security Incident-Datensatz ist geschlossen. Im Alarm auf wird ein Kommentar veröffentlicht LogRhythm Webkonsole. Dieser Kommentar gibt an, dass der Alarm basierend auf dem Schließen von geschlossen wurde ServiceNow AI Platform Security Incident. Die Incident-Nummer und eine URL, die zur Referenz auf den Security Incident zurückgreift, sind auch im Kommentarabschnitt in enthalten LogRhythm Alarm.

Prozedur

1. Klicken Sie auf **Zusätzliche Optionen** Gehen Sie auf den Fortschrittsbalken.
2. Um die automatisierte Alarmaktualisierung für die SIR-Incident-Erstellung zu verwenden, wählen Sie aus den folgenden Optionen aus, um Ihren Alarmabruf zu konfigurieren.
3. Um die automatisierte Alarmaktualisierung für den SIR-Incident-Abschluss zu verwenden, wählen Sie aus den folgenden Optionen aus, um Ihren Alarmabruf zu konfigurieren.
4. Klicken Sie Auf **Beenden** Zum Speichern des Alarmprofils.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trouble?
Wenn Sie keine Notizen sehen, die darauf hinweisen, dass der Alarm im Security Incident erfolgreich geschlossen wurde, lesen Sie die Arbeitsnotizen, um weitere Informationen darüber zu erhalten, wie Sie das Problem beheben können. Überprüfen Sie auch Ihre Serververbindung. Wenn Sie bestätigen ServiceNow AI Platform Security Incident wurde geschlossen, und der Server ist nicht abgelaufen. Möglicherweise müssen Sie den Alarm auf manuell schließen LogRhythm Webkonsole.

Zusätzliche Konfigurationen für LogRhythm Integration

Verwenden Sie LogRhythm Integrationseinstellungen zum Ändern der voreingestellten System- und Problembehandlungseigenschaften gemäß Ihren Anforderungen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **LogRhythm-Integration** > **LogRhythm-Integrationseinstellungen**an.
2. Konfigurieren Sie die Systemeigenschaften entsprechend Ihren Anforderungen.
3. Füllen Sie die Felder im Formular aus.

LogRhythm Eigenschaften Des Integrationssystems

Feld	Beschreibung
Dadurch wird der Filter angewendet, bevor die Daten in ServiceNow-Tabellen gespeichert werden.	Option, um zu bestimmen, ob Sie den Filter anwenden möchten, bevor die Daten in den ServiceNow-Tabellen gespeichert werden. Standardmäßig ist der Wert auf „Ja“ festgelegt.
Max. Security Incident kann an einem Tag erstellt werden	Option zum Definieren der maximalen Anzahl von Security Incidents, die an einem Tag erstellt werden können. Standardmäßig ist der Wert auf 2000 festgelegt.
LogRhythm Die regelmäßige Erfassung kann 1000+ Alarme sein, daher wird Paginierung zum Erfassen der Alarme verwendet. Grenzwert pro Seite zum Abrufen der Anzahl von Alarmen pro Seite.	Option zum Definieren der maximalen Anzahl von Alarmen, die auf einer einzelnen Seite abgerufen werden sollen. Standardmäßig ist der Wert auf 100 festgelegt.
Löschen Sie Datensätze der Tabelle „Quelle zu Aufgabe“, die älter als die angegebene Anzahl von Tagen sind.	Option zum Löschen von Datensätzen der Quelle-zu-Aufgabe-Tabelle, wenn die angegebene Anzahl von Tagen überschritten wurde. Standardmäßig ist der Wert auf 30 festgelegt.

4. Konfigurieren Sie die Fehlerbehebungseigenschaften entsprechend Ihren Anforderungen.
5. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften der LogRhythm-Integration zur Problembehandlung

Feld	Beschreibung
Geplante Erfassung debuggen: Aktiviert Systemprotokolle auf Debug-Ebene für die Erfassung durch eine geplante Aufgabe. Dadurch werden alle Nachrichten/Ausnahmen protokolliert, die von der geplanten Erfassung beim Abrufen von Alarmen/Drilldownlogs/Ereignissen aus generiert werden LogRhythm.	Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Erfassung durch die geplante Aufgabe. Standardmäßig ist der Wert auf Nein festgelegt
Transformationszuordnung debuggen: Aktiviert Systemprotokolle auf Debug-Ebene für Transformationszuordnung. Dadurch werden alle Nachrichten protokolliert, die von Transformationszuordnungen beim Erstellen eines Security Incidents aus dem Alarmimport generiert werden. Dadurch wurde auch die UI-Aktion in der Alarmimporttabelle aktiviert, um die Transformationszuordnung erneut auszuführen.	Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Transformationszuordnung. Standardmäßig ist der Wert auf Nein festgelegt
Beispielerfassung in Alarmprofil debuggen: Dies aktiviert Systemprotokolle auf Debug-Ebene für die Beispielerfassung. Dadurch werden alle Nachrichten protokolliert, die während der Erfassung von Beispielen generiert werden.	Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Beispielerfassung. Standardmäßig ist der Wert auf Nein festgelegt
Debug-Vorschau in Alarmprofil: Aktiviert Systemprotokolle auf Debug-Ebene für die Alarmprofilvorschau. Dadurch werden alle Nachrichten protokolliert, die generiert werden, während die Vorschau für einen Beispielalarm gerendert wird.	Option zum Aktivieren von Systemprotokollen auf Debug-Ebene für die Alarmprofilvorschau. Standardmäßig ist der Wert auf Nein festgelegt
Ausgehende REST-Aufrufe debuggen: Durch Aktivieren dieser Eigenschaft wird die Protokollierung auf Debug-Ebene in der Tabelle „Systemprotokolle“ für alle REST-Aufrufe (Anforderung und Antwort) mit oder ohne MID-Server von ermöglicht LogRhythm.	Option zum Aktivieren der Protokollierung auf Debug-Ebene in der Tabelle „Systemprotokolle“ für alle REST-Aufrufe, die mit oder ohne MID-Server von ausgeführt werden LogRhythm. Standardmäßig ist der Wert auf Nein festgelegt

6. Klicken Sie auf **Speichern**.

Verwenden Sie zum Formatieren den Skripteditor LogRhythm Werte

Zusätzlich zu den direkt zugeordneten Feldern aus den abgerufenen Alarmwerten und den manuell eingegebenen Alarmwerten können Sie den Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Dies ist optional.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Der Skripteditor ändert die Werte von LogRhythm Alarm, also die Werte, die dem zugeordnet sind Priorität Und Kategorie Felder im Security Incident werden unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

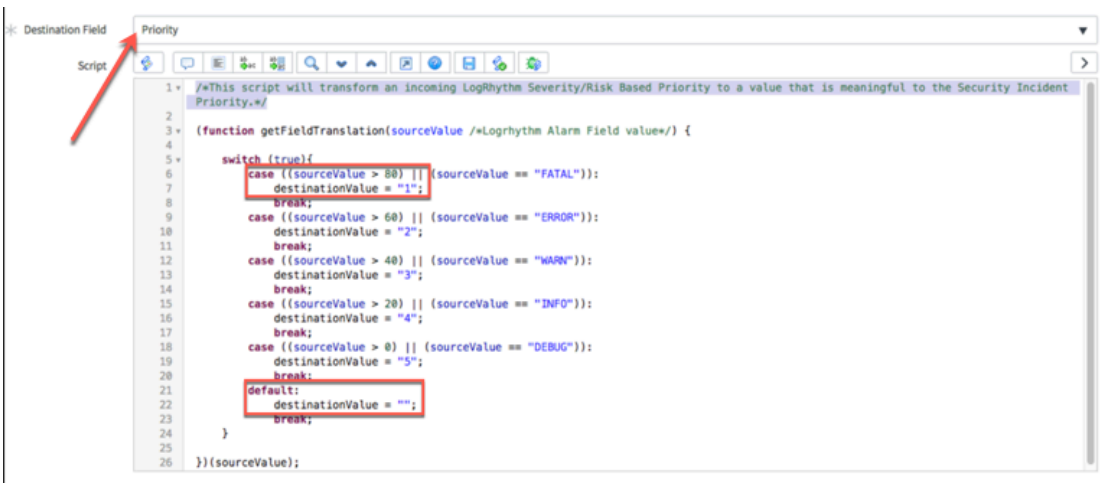
In bestimmten Fällen: Wenn LogRhythm Alarmwerte werden dem zugeordnet Priorität Und Kategorie Felder im Security Incident. Möglicherweise möchten Sie die zugeordneten Werte bearbeiten. Wenn Sie den Wert von übersetzen möchten LogRhythm Alarm auf einen Wert, der von unterstützt wird Priorität Oder Kategorie Felder im Security Incident verwenden Sie den Skript-Editor.

Prozedur

1. Wenn das Zuordnungsformular angezeigt wird, klicken Sie im Abschnitt SIR-Incident-Feldzuordnung auf das Klammern-Symbol [{}] Zum Öffnen des Skripteditors.

   Die Standardwerte sind für enthalten Priorität Und Kategorie Felder im Security Incident. Sie können diese Werte bearbeiten.

   Überprüfen Sie in diesem Beispiel im Editor öffnen das **Priorität** Wird in angezeigt **Zielfeld** Auswahlliste, wie in der folgenden Abbildung dargestellt. Beachten Sie, dass dieses Feld der Security Incident ist *Priorität* , Nicht der LogRhythm Risikobasiert *Priorität* .

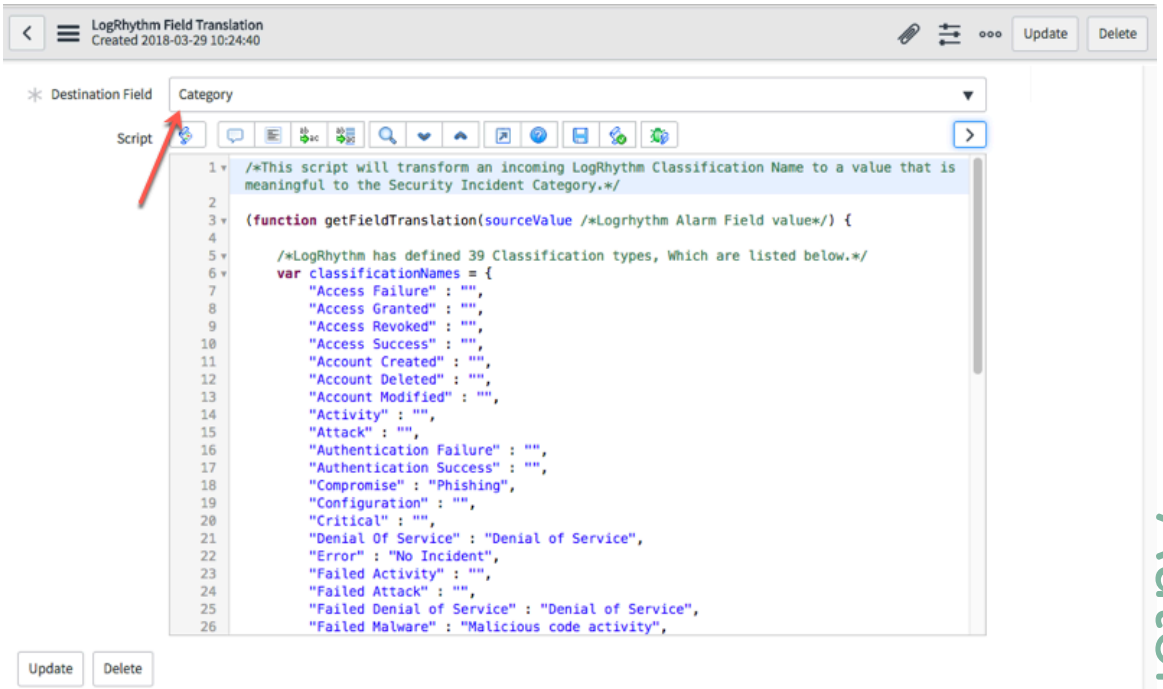
   In bestimmten Fällen kann eine Skripteinbindung für geeignet sein Priorität Feld. Für ein LogRhythm Alarm wird beispielsweise einer risikobasierten Prioritätspunktzahl ein Wert zwischen 0 und 100 zugewiesen. Jedoch in ServiceNow AI Platform, Das Prioritätsfeld für einen Security Incident unterstützt Werte zwischen 1 und 5. Wie in der vorherigen Abbildung dargestellt, übersetzt eine Skripteinbindung LogRhythm Alarmfeldwerte auf die entsprechenden Werte, die vom Feld im Security Incident in unterstützt werden ServiceNow AI Platform.

   In diesem Beispiel für Priorität Feld, wenn LogRhythm Alarmwert ist 80 Oder größer, 1 Wird im Feld Security Incident angezeigt (Priorität). Dieser Wert wird in einen übersetzt Kritisch Priorität im Security Incident. Wenn für den Alarm kein Wert vorhanden ist, wird das Feld im Security Incident auf null festgelegt.

2. Geben Sie alle Änderungen ein, und klicken Sie auf **Aktualisieren** Um Ihre Änderungen zu speichern. Die LogRhythm Die Tabelle „Feldübersetzungen“ wird angezeigt.
3. Schließen Sie die Tabelle, um zum Zuordnungsformular zurückzukehren.

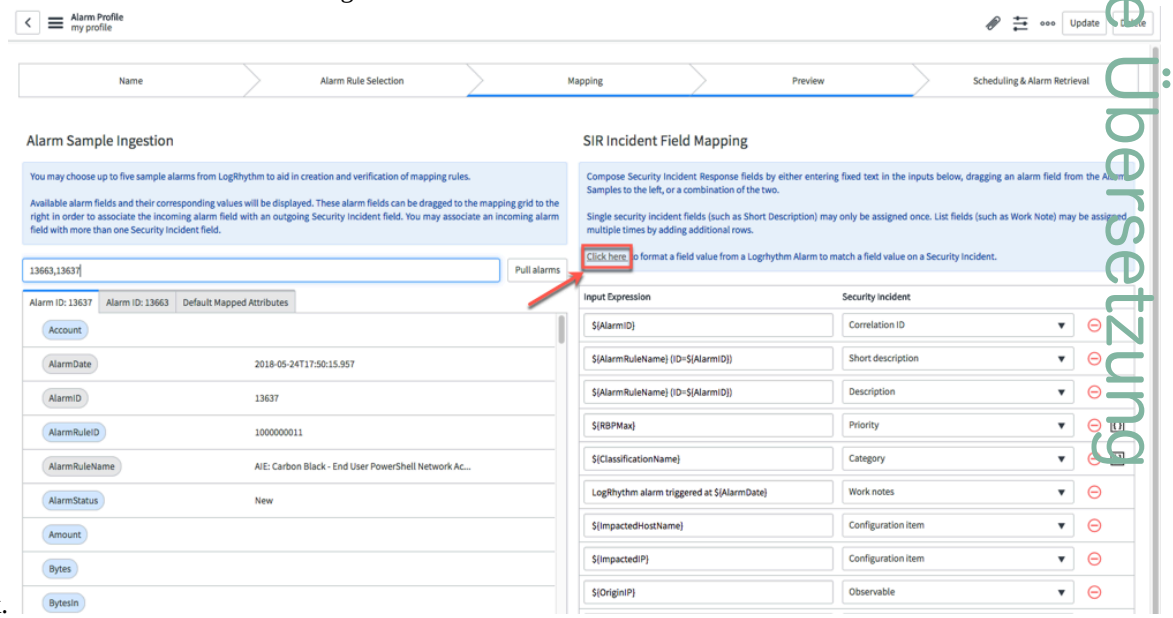
   Die folgende Abbildung zeigt den Skripteditor mit Kategorie In der Auswahlliste Zielfeld ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wenn Sie der Liste „Feldübersetzungen“ ein neues Feld hinzufügen möchten, führen Sie die folgenden Schritte aus, um einen neuen Datensatz hinzuzufügen.

a. Wenn das Zuordnungsformular angezeigt wird, klicken Sie im Abschnitt SIR-Incident-Feldzuordnung auf **Klicken Sie hier**Link.

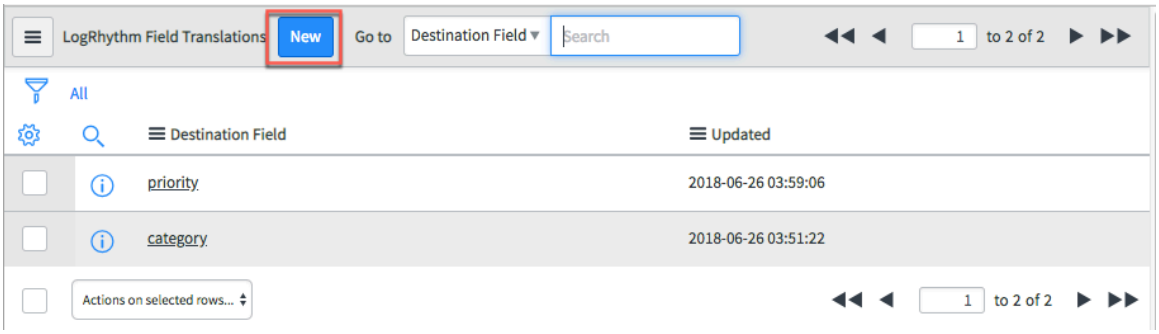


Die LogRhythm Feldübersetzungsliste mit Priorität Und Kategorie Zielfelder werden angezeigt.

b. Klicken Sie auf „Neu“.

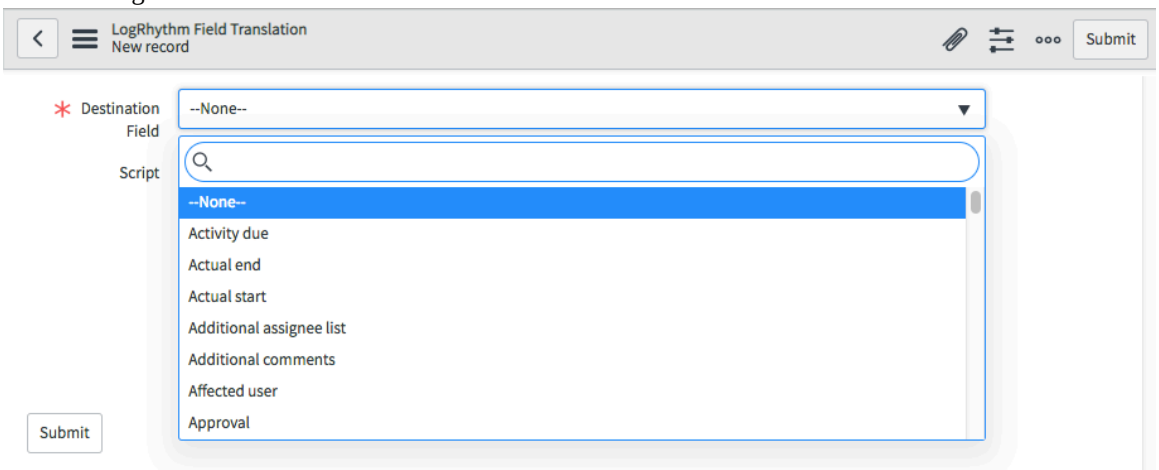
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ein neuer Datensatz wird angezeigt.

c. Wählen Sie in der Auswahlliste Zielfeld ein Zielfeld im Security Incident aus, in dem Sie Ihre geskripteten Werte anzeigen möchten.



d. Klicken Sie auf **Absenden**.
Der Skripteditor wird angezeigt.

e. Geben Sie alle Änderungen in den Editor ein, und klicken Sie auf **Übermitteln** Um Ihre Änderungen zu speichern.
Die LogRhythm Die Tabelle „Feldübersetzungen“ mit Ihrem neuen Datensatz wird angezeigt.

5. Schließen Sie die Tabelle, um zum Zuordnungsformular zurückzukehren.

Kopieren Sie ein Alarmprofil für LogRhythm

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt ein neues Alarmprofil zu erstellen. Wenn Sie mehrere Alarmprofile für verschiedene Arten von Alarmen erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, können Sie Alarmprofile kopieren, um Zeit zu sparen. Dieser Prozess ist optional.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

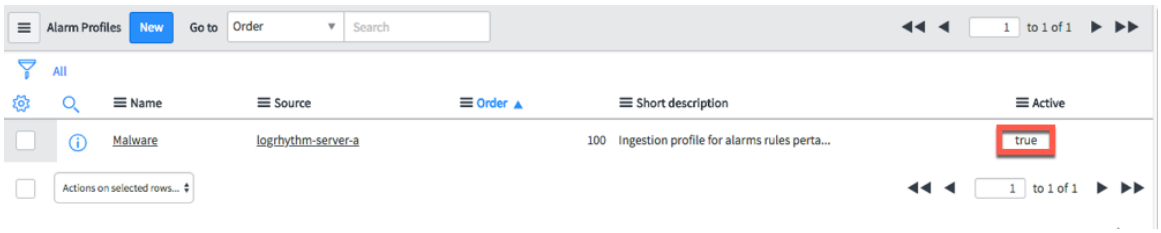
Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus wird das kopierte Profil auf „inaktiv“ gesetzt, sodass es vor Abschluss der Konfiguration nicht versehentlich aktiviert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

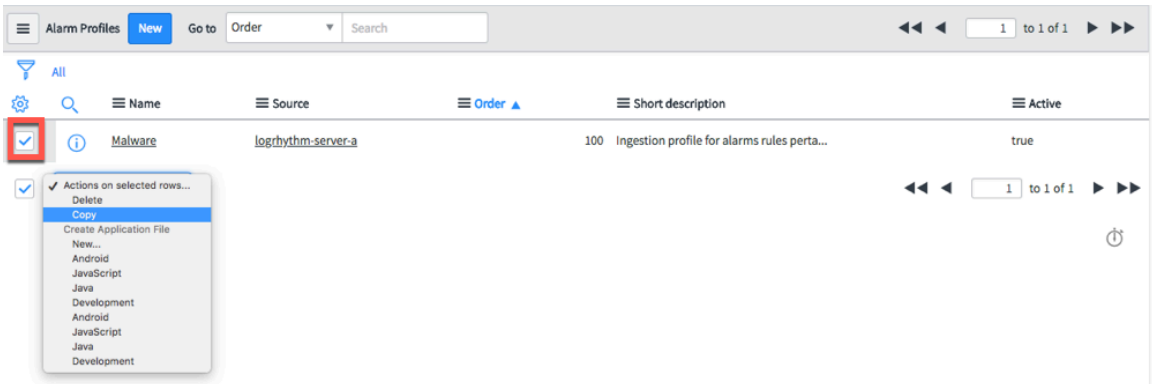
Prozedur

1. Navigieren zu **Alle** > **LogRhythm-Integration** > **LogRhythm-Alarmprofile**an.

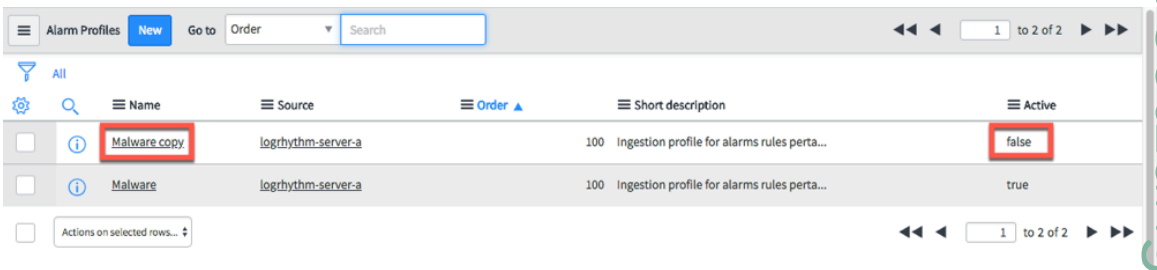
   Beachten Sie in der angezeigten Liste die Aktiv Spalte gibt an, ob das Profil aktiv ist (Wahr).



2. Im Feld links von **Name** Wählen Sie den Namen des Datensatzes aus.
3. Von **Aktionen für ausgewählte Zeilen** Auswahlliste auswählen **Kopieren** .



In **Alarmprofile** Liste, sowohl die Kopie als auch das ursprüngliche Profil werden angezeigt. Obwohl der ursprüngliche Datensatz aktiv ist, ist die Kopie zu diesem Zeitpunkt inaktiv (Falsch). Nachdem Sie es konfiguriert haben, aktivieren Sie dieses kopierte Profil.



Sie können Werte des kopierten Profils bearbeiten und umbenennen, damit von Ihnen abgerufene Alarmregeln auf das neue Profil angewendet werden. Sie werden aufgefordert, das neue Profil zu aktivieren, sobald die Konfigurationsschritte abgeschlossen sind.

Automatische Übersetzung

Automatisierten Alarmabschluss für deaktivieren LogRhythm

Deaktivieren Sie die automatisierte Alarmschließungsfunktion, wenn Sie die Informationen zum Abschluss von Security Incidents nicht mehr im anzeigen möchten LogRhythm Webkonsole. Nach der Deaktivierung wird ServiceNow AI Platform Schließt Alarme innerhalb von nicht mehr LogRhythm Webkonsole. Dieser Prozess ist optional.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

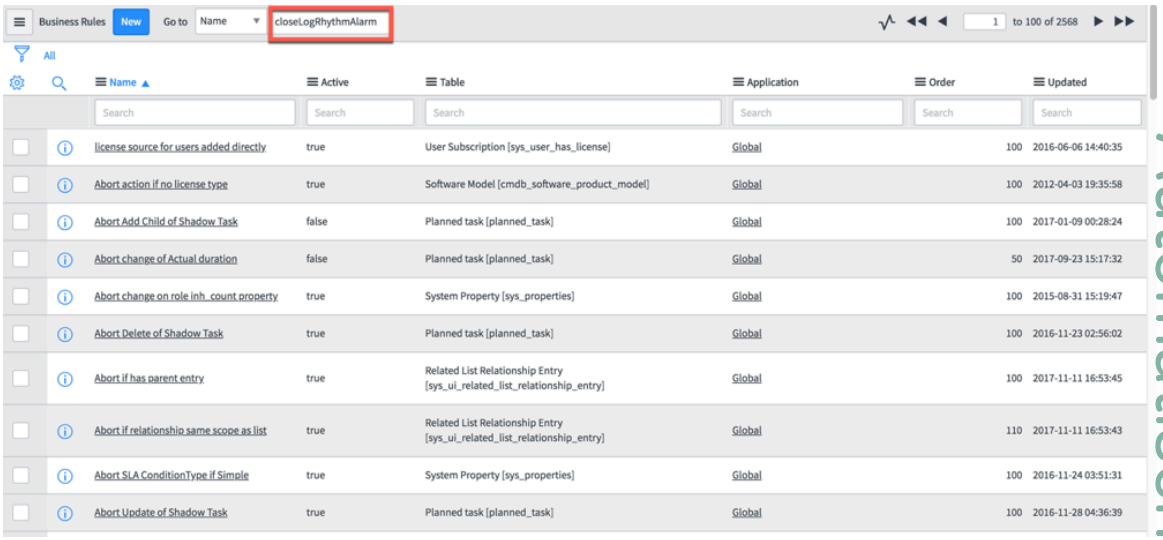
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Nach der Deaktivierung werden die Statusnotizen und andere Abschlussinformationen zum Security Incident nicht mehr im angezeigt LogRhythm Webkonsole.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Business-Regeln** Und wählen Sie aus **Business-Regeln** Modul.
2. Wenn nicht in angezeigt **Business-Regeln** Liste, geben Sie ein **LogRhythm – Alarm bei SI-Abschluss schließen** Drücken Sie im Suchfeld **Geben Sie Ein** .



3. In **Name** Klicken Sie auf die Spalte **LogRhythm – Alarm bei SI-Abschluss schließen** Link zum Öffnen des Datensatzes.
4. Löschen Sie im angezeigten Datensatz **Aktiv** Kontrollkästchen.
5. Klicken Sie auf **Aktualisieren**.
   Die automatisierte Alarmschließungsfunktion ist jetzt deaktiviert.

Anzeigen LogRhythm Drilldown-Ereignisse

Zeigen Sie die zugehörigen Roh- oder Basisereignisse für an LogRhythm Alarm im Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Als Sicherheitsanalyst können Sie die zugehörigen Roh- oder Basisereignisse für anzeigen LogRhythm Alarm, ohne zu wechseln LogRhythm Konsole. Sie können dies tun, indem Sie zu einer zugehörigen Liste wechseln, die alle Drilldown-Ereignisse in enthält SIR Incident.

Prozedur

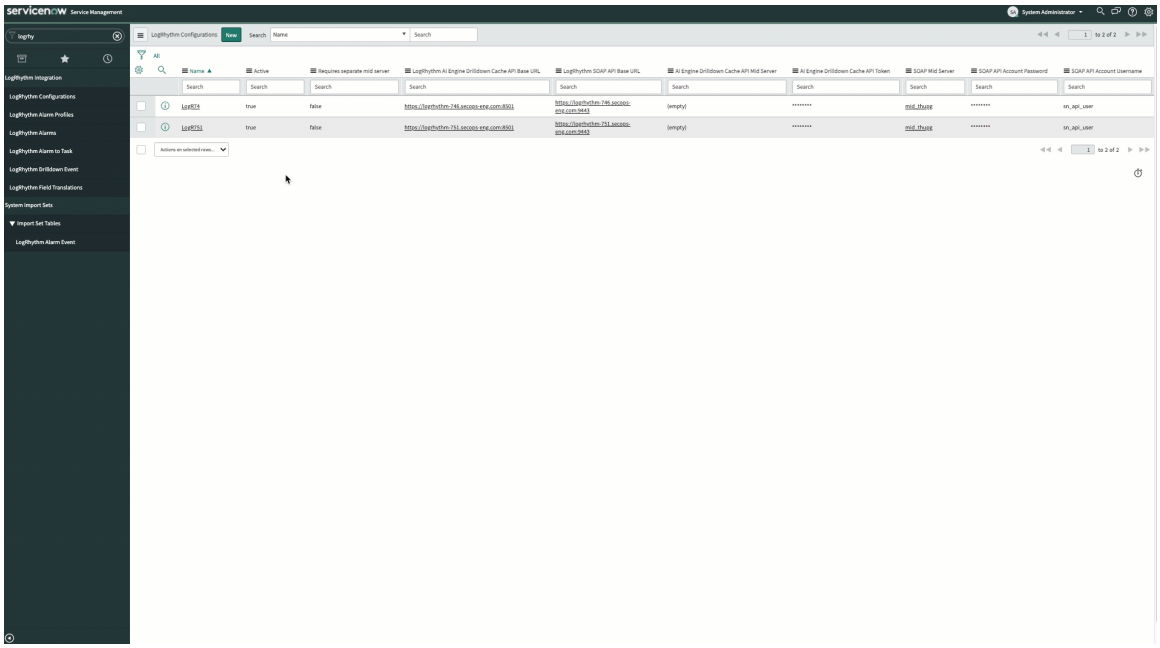
Navigieren zu **Alle** > **LogRhythm-Integration** > **LogRhythm-Drilldown-Ereignisse**an.

Die folgende Abbildung zeigt, wie Sie zu navigieren **LogRhythm-Drilldown-Ereignisse** Modul, sortieren Sie die Liste der Ereignisse nach **Nach Alarm-ID gruppieren** , Und klicken Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auf den zugehörigen Security Incident. Im Security Incident finden Sie den **LogRhythm-Drilldown-Ereignisse** Registerkarte in den zugehörigen Links.



Fehlerbehebung bei der LogRhythm-Integration

Beheben Sie Konnektivitäts- und Alarmerfassungsprobleme.

Informationen zur Fehlerbehebung finden Sie in den folgenden Themen:

- Überprüfen Sie die Konnektivität für LogRhythm
- Skriptausführung und Systemprotokoll für LogRhythm

Überprüfen Sie die Konnektivität für LogRhythm

Überprüfen Sie Ihre Verbindung mit LogRhythm Clientkonsole durch Senden von Curl-Anforderungen zum Testen von LogRhythm REST-API. Der Verifizierungsprozess ist optional.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Dient zum Überprüfen der Verbindung mit LogRhythm Client-Konsole funktioniert ordnungsgemäß, nachdem Sie eingerichtet haben LogRhythm REST APIs: Senden Sie zwei Curl-Anforderungen vom Computer, der den in konfigurierten MID-Server hostet Installieren Sie das Plugin, und konfigurieren Sie LogRhythm.

Die LogRhythm DIE REST-API verwendet WSSE für die Authentifizierung, die einige externe Skriptfunktionen erfordert, um mit Curl und Postman zu arbeiten.

Die LogRhythm DIE REST-API verwendet ein Token für die Authentifizierung, damit Sie den tatsächlichen Validierungsaufruf durchführen können, den die Integration verwendet. Die „0“ am Ende der URL ist ein LogRhythm Alarm-ID. Die LogRhythm REST API mit einer Standardkonfiguration erfordert Port 8501. Diese Portnummer muss in der URL enthalten sein, die Sie für den Test verwenden möchten.

Prozedur

Aktualisieren Sie die URL **<LogRhythm-REST-url>** Und-Token **<api token>** In der folgenden Curl-Anforderung und senden Sie sie, um zu validieren LogRhythm REST-API: `Curl -k -i -V --Trace-time -o /`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dev/null -H „Inhaltstyp: Text/JSON“ -H „Autorisierung: Bearer-<api token>“ „https://<cache Drilldown-url>/lr-Drilldown-Cache-api/Drilldown/0“
Für eine erfolgreiche Verbindung mit LogRhythm REST API, Sie sollten HTTP 404 erhalten, aber der Antworttext enthält Alarm-ID: 0 nicht gefunden .

Skriptausführung und Systemprotokoll

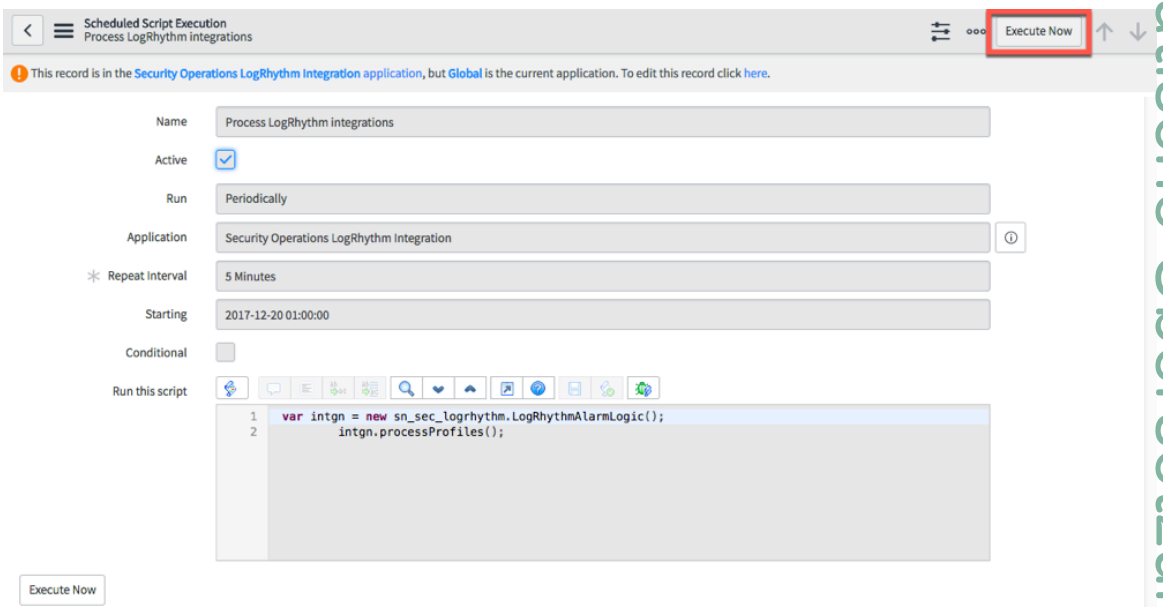
Wenn Sie ein Problem mit der Alarmerfassung beheben, können Sie das standardmäßige fünfminütige Abfrageintervall überschreiben, um die Ergebnisse sofort anzuzeigen. Rufen Sie in diesem Szenario die Skriptausführung manuell auf, um die Abfrage auszuführen. Diese Ausführung ist optional.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Geplante Aufgabe** > **Geplante Aufgaben** Und wählen Sie aus **Geplante Aufgaben** Modul.
2. Klicken Sie auf Prozess LogRhythm Integrationsauftragsdatensatz.
3. Klicken Sie im angezeigten Datensatz „geplante Skriptausführung“ auf **Jetzt Ausführen** .



Wenn Sie weitere Hilfe bei der Fehlerbehebung benötigen, können Sie auf das Systemprotokoll für zugreifen LogRhythm Abfragen.

4. Führen Sie bei anderen allgemeinen Problembehebungsproblemen die folgenden Schritte aus, um auf die Systemprotokolle zuzugreifen.

   a. Navigieren zu **Systemprotokoll** > **Alle** Und wählen Sie aus **Alle** .

   b. Legen Sie den Filter fest (Wechseln Sie zu) Bis **Quelle** Und geben Sie ein sn_sec_logrhythm .

   c. Drücken Sie die **Eingabetaste**.
   Alle von der Integration generierten Nachrichten werden in dieser Tabelle angezeigt. Die aufgeführten Nachrichten können Einblicke in die laufenden Prozesse der Integration geben und Sie bei der weiteren Fehlerbehebung unterstützen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

McAfee ePO-Integration

Die McAfee ePO EDR-Fähigkeit (Integration Endpoint Detection and Response), mit der Analysten des Security Operations Center (SOC) Cyberbedrohungen erkennen und Schäden beheben können, die durch schädliche Dateien verursacht wurden.

Übersicht

Es gibt zwei Sätze von McAfee ePO In dieser Integration verwendete Fähigkeiten, die Fähigkeiten, die Aktionen aufrufen, z. B. das Isolieren eines Hosts und das Initiieren eines Malware-Scans, und die Fähigkeiten, die Abfragen ausführen, um Systemdetails und Bedrohungsereignisse zu erfassen. Beide Arten von Fähigkeiten, die Aktionen und die Abfragen, werden von aufgerufen ServiceNow AI Platform® Instanz. Sie können diese Fähigkeiten gruppieren, sodass sie automatisch ausgeführt werden, wenn ein bestimmter Typ von Sicherheitsereignissen auftritt, oder Sie können sie manuell aus aufrufen ServiceNow AI Platform® Security Incident.

Folgendes McAfee ePO Für diese Integration sind Fähigkeiten verfügbar.

Rufen Sie Systemdetails ab

Erfassen Sie Systemdetails, die Betriebssystemdetails enthalten.

Initiieren Sie einen Malware-Scan

Initiieren Sie basierend auf der Scankonfiguration und der Planung einen Scan eines betroffenen Endpunkts.

Host isolieren/Isolierung aufheben

Entfernen Sie ein System für Untersuchungen vom Netzwerkzugriff, und stellen Sie den Zugriff auf das Netzwerk wieder her.

Listen Sie Bedrohungsereignisse auf

Erfassen Sie den Compliance-Status und die neuesten Bedrohungsereignisse.

Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen.

- Unterstützt die automatisierte Auslösung von McAfee ePO Abfragen, die auf Incident-Bedingungen basieren.
- Unterstützt das Starten McAfee ePO Fähigkeiten manuell von ServiceNow AI Platform® Security Incident Response(SIR) Security Incidents, die Aktionen bei Bedarf ausführen.
- Die Flexibilität, mehrere Profile zum Auslösen verschiedener Typen von zu erstellen McAfee ePO Und ServiceNow AI Platform® Security Operations Fähigkeiten. Diese Profile erfassen Bedrohungsereignisinformationen oder führen Aktionen basierend auf den Bedingungen bestimmter Incident-Kategorien wie Malware aus.
- Validieren Sie Ihre Profilkonfiguration mit einer Vorschau von McAfee ePO Ergebnisse für SIR Security Incidents.
- Wenn Tagging aktiviert ist, identifizieren Sicherheits-Tags welche McAfee ePO Fähigkeiten werden anfänglich von einem Workflow gestartet und wenn die Abfragen oder Aktionen erfolgreich abgeschlossen wurden.
- Ein vollständiger Audit-Pfad von McAfee ePO Abfragen und Aktionen werden in den Arbeitsnotizen auf veröffentlicht SIR Security Incidents und Befehle aus der ServiceNow AI Platform® Sind in angemeldet McAfee ePO Konsole.
- Unterstützt mehrere McAfee ePO Konsolen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Plugins

Das Plugin „com.snc.si_dep“ ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Anwendungen.

Folgendes Security Operations Anwendungen müssen über installiert und aktiviert werden ServiceNow Store. Installieren und aktivieren Sie jeweils eine Anwendung in der unten aufgeführten Reihenfolge, um eine reibungslose Installation sicherzustellen:

1. Sicherheits-Integrations-Framework
2. Security Support Common
3. Orchestration Des Sicherheitssupports
4. Security Incident Response
5. Arbeitsbereich für Security Incident Response

Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz für die Integration finden Sie unter Richten Sie Ihr ein ServiceNow AI Platform Instanz für McAfee ePO Integration.

Die ServiceNow Erweiterungs-Plugin

Die ServiceNow Security Operations-Erweiterung für McAfee ePO #Das Erweiterungs-Plugin ist für diese Integration erforderlich. Installieren Sie diese ServiceNow Plugin in Ihrem McAfee ePO Konsole. Weitere Informationen finden Sie unter Richten Sie Ihr ein ServiceNow AI Platform Instanz für McAfee ePO Integration.

MID-Server

Diese Integration erfordert einen installierten und konfigurierten MID-Server in Ihrem ServiceNow AI Platform® Instanz, die mit verbunden werden soll McAfee ePO Server (Konsole). Siehe ServiceNow-Produktdokumentationswebsite Weitere Informationen zu MID-Servern.

Unterstützte Versionen von McAfee

Die Integration unterstützt die Versionen 5.9.1 und 5,10 von McAfee ePO. Unterstützt McAfee Agent: MA 5.5.1.388 weitere Informationen zu McAfee-Produkten und dem ePolicy Orchestrator finden Sie unter McAfee-Produkt-Website .

Die Integration unterstützt die Version 10,5 des McAfee Endpoint Security Threat Prevention-Produkts. Wenn Sie Version 10.5 nicht ausführen, wenden Sie sich an Ihren McAfee ePO Administrator, um zu sehen, ob Ihre Version Scans bei Bedarf über Tag-Aktionen unterstützen kann.

McAfee ePO In dieser Integration werden Sicherheits-Tags verwendet. Sie müssen diese Tags in erstellen McAfee ePO Konsole. Weitere Informationen zu diesen Tags finden Sie unter Richten Sie Ihr ein McAfee ePO Konsole, in die integriert werden soll Security Incident Response(SIR).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenzen

Referenz	Dokumentbezeichner	Dokumententitel
1	McAfee-Produkt-Website	McAfee-Produkt-Website
2	McAfee-Geschäftsproduktdokumentation für ePolicy Orchestrator Cloud	McAfee-Produktdokumentation
3	ServiceNow Produktdokumentations-Website	ServiceNow-Produktdokumentationswebsite

Eine Prüfliste zum Nachverfolgen Ihres Fortschritts beim Einrichten, Installieren und Überprüfen der Ergebnisse für die Integration finden Sie unter Prüfliste für McAfee ePO Integration.

Um eine reibungslose Installation der Anwendung zu gewährleisten und die erwarteten Ergebnisse zu überprüfen, befolgen Sie die Themen in der Reihenfolge, in der sie angezeigt werden.

Zugehörige Informationen

Integrationsarchitektur für McAfee ePO

Integrationsarchitektur für McAfee ePO

Das folgende Thema bietet einen Überblick über die Systemarchitektur und listet die wichtigsten Funktionen der Integration auf. Dieser Abschnitt enthält auch Informationen zu den Setup-Schritten, die Sie in ausführen müssen ServiceNow AI Platform Instanz und im McAfee ePolicy Orchestrator (McAfee ePO) -Konsole vor der Installation der Anwendung über ServiceNow Store.

Schlüsselbegriffe für McAfee ePO Integration

Die folgenden Begriffe werden in der Installations- und Konfigurationsdokumentation für die Integration verwendet.

ServiceNow AI Platform

Ein Unternehmen ServiceNow Produkt. Die ServiceNow AI Platform Ist die Basis, auf der einzelne Komponenten basieren, z. B. Security Incident Response(SIR), IT Service Management, (ITSM) und andere Produkte werden erstellt.

Security Incident Response (SIR)

A ServiceNow AI Platform Anwendung, die den Fortschritt von Security Incidents von der Erkennung und ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur endgültigen Überprüfung und Schließung von Security Incidents nachverfolgt.

Plugin

Plugins sind Softwarekomponenten, die bestimmte Funktionen in Ihrem bereitstellen ServiceNow AI Platform Instanz. Weitere Informationen zur Installation und Konfiguration der Integrations-Plugins finden Sie unter Installieren Sie die Anwendung, und konfigurieren Sie einen Server für McAfee ePO Integration.

EPolicy Orchestrator (McAfee ePO)

Die Anwenderkonsole, in der Sie die McAfee-Services, -Produkte und -Einstellungen verwalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

McAfee-Erweiterungs-Plugin

Dies ServiceNow Das Erweiterungs-Plugin ist für diese Integration erforderlich. Dieses Plugin befindet sich auf Ihrem McAfee ePO Konsole und verbindet mit McAfee ePO-Konsole zu Ihrem ServiceNow AI Platform Instanz.

Fähigkeit

Eine automatische Aktivität, die von Ihrem initiiert wurde ServiceNow AI Platform Instanz, die in ausgeführt wird McAfee ePO Konsole zum Durchführen von Ergänzungsabfragen und Ausführen von Aktionen für Ihre Assets.

Profil

Einstellungen für McAfee ePO Fähigkeiten, die Sie konfigurieren, um anzugeben, wann und unter welchen Bedingungen Fähigkeiten Ergänzungsabfragen durchführen und Aktionen für Ihre Assets ausführen.

MID-Server verwenden

Eine Anwendung, die die Kommunikation und den Datenverkehr zwischen erleichtert ServiceNow AI Platform Und externe Anwendungen, Datenquellen und Services.

ServiceNow Administrator (Administrator)

Ein Anwender mit dieser Rolle lädt herunter und installiert SIR Und McAfee ePO Plugins für Ihren ServiceNow AI Platform Instanz. Ein Benutzer mit dieser Rolle weist bei Bedarf auch die Rolle Security Incident-Administrator zu.

ServiceNow Security Incident-Administrator (sn_si.admin)

Ein Anwender mit dieser Rolle führt die Konfiguration von durch McAfee ePO Integration mit Security Incident Response(SIR) Produkt in Ihrem ServiceNow AI Platform Instanz nach Bedarf. Ein Anwender mit dieser Rolle weist bei Bedarf auch die Rolle Security Incident Analyst zu.

ServiceNow Security Incident-Analyst (sn_si.Analyst)

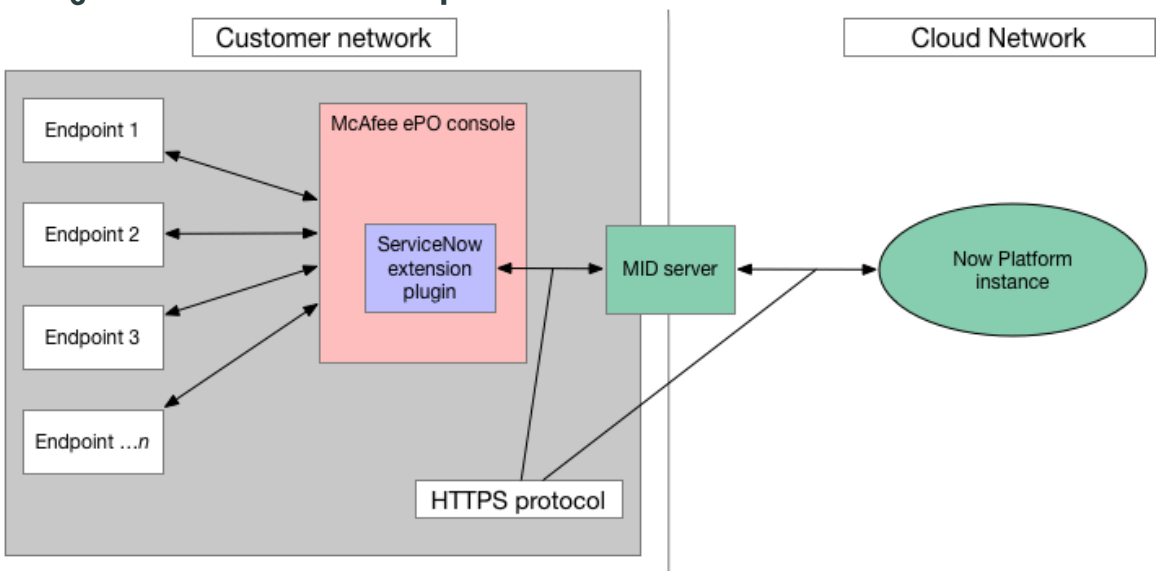
Ein Anwender mit dieser Rolle interagiert mit Security Incidents im SIR-Produkt und analysiert sie.

Systemverbindung und Daten-Flow

Die folgende Abbildung zeigt ein Beispiel für eine Kundenumgebung. A ServiceNow AI Platform MID-Server ist erforderlich, damit Ihr ServiceNow AI Platform Instanz kann eine Verbindung zu herstellen McAfee ePO Server (Konsole) über ein ServiceNow Erweiterungs-Plugin. Nachdem Sie verbunden sind, rufen Sie Fähigkeiten von auf ServiceNow AI Platform Um Malware-Scans zu initiieren, isolieren Sie Hostcomputer, und stellen Sie sie in Ihrem Netzwerk wieder her, rufen Sie die letzten Scan-Ergebnisse ab, und sammeln Sie Systemdetails zu Ihren Assets. Wenn diese Fähigkeiten Ergebnisse aus Ihren Assets zurückgeben, die Ihren Suchkriterien entsprechen, werden Daten über den MID-Server in abgerufen ServiceNow AI Platform Instanz. Daten werden in den zugehörigen Listen von angezeigt ServiceNow AI Platform Security Incident Response(SIR) Security Incident. Die folgende Abbildung zeigt den Daten-Flow für eine Gruppe von Endpunkten, die von einem verwaltet werden McAfee ePO Konsole.

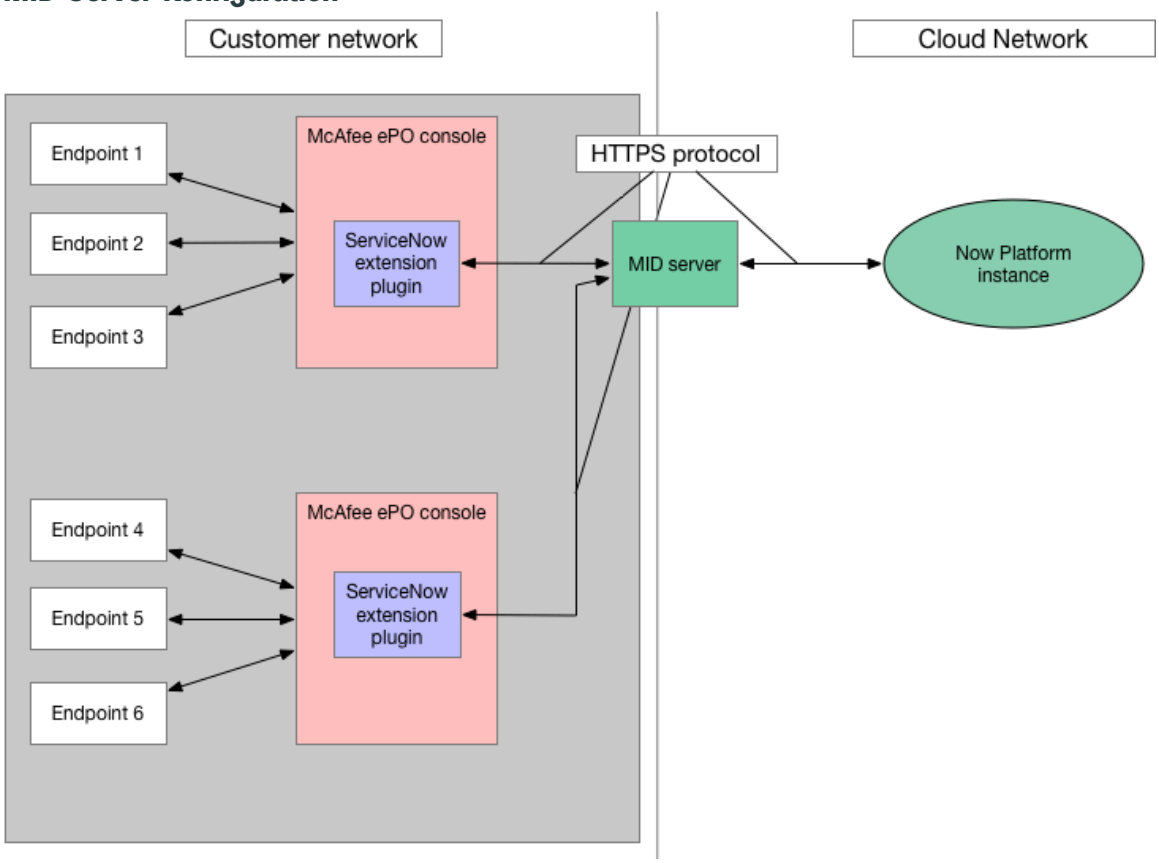
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration eines einzelnen Endpunkts



Wie in der folgenden Abbildung gezeigt, kann diese Integration mehr als einen unterstützen McAfee ePO Konsole. Sie können eine Gruppe von Endpunkten von einem verwalten lassen McAfee ePO Konsole und eine andere Gruppe von Endpunkten, die von einer anderen verwaltet werden McAfee ePO Konsole. Daten aus mehreren McAfee ePO Konsolen werden über einen einzelnen MID-Server abgerufen. Sie können jedoch auch mehrere MID-Server konfigurieren, wenn dies von Ihrer Organisation erforderlich ist.

MID-Server-Konfiguration



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

-Workflows für McAfee ePO Integration

Diese Integration umfasst die folgenden Workflows. Diese Workflows sind vorkonfiguriert und speziell für diese Integration konzipiert. Sie können diese Workflows nach Bedarf bearbeiten, um die Anforderungen Ihrer Organisation zu erfüllen. Weitere allgemeine Informationen zu Workflows und zur Verwendung des Workflow-Editors finden Sie unter Erste Schritte mit Workflows .

- Integration von Security Operations McAfee EPO – Hostdetails abrufen
- Integration von Security Operations McAfee EPO – Malware-Scan initiieren
- Security Operations McAfee EPO-Integration – Host isolieren
- Integration von Security Operations McAfee EPO: Listen Sie Bedrohungsereignisse auf
- Security Operations McAfee EPO-Integration – Isolierung entfernen

Externe Systemverbindung

Die Integration erfordert, dass der MID-Server über eine HTTPS-Protokollverbindung mit dem kommuniziert McAfee ePO Konsole.

Prüfliste für McAfee ePO Integration

Verwenden Sie diese Prüfliste, um Sie durch alle Aufgaben der Integration zu führen. Die folgende Prüfliste enthält Setup- und Installationsaufgaben sowie Beispiele für Anwendungsfälle, die die erwarteten Ergebnisse für die Integration enthalten.

Vorbereitungen
Erforderliche Rolle: Für jeden Schritt werden Rollen aufgelistet.

Warum und wann dieser Vorgang ausgeführt wird
Verfolgen Sie Ihren Fortschritt beim Setup, der Installation und der Konfiguration der Integration mit der folgenden Tabelle. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren. Jede Zeile der Tabelle listet Aufgaben auf und gibt die Rollen an, die zur Ausführung der Aufgaben erforderlich sind. Nummerierte Themen des Installations- und Konfigurationsleitfadens werden ebenfalls referenziert.

Prozedur

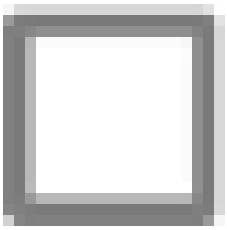
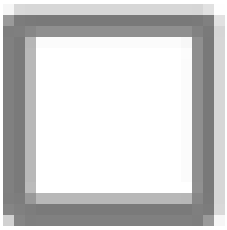
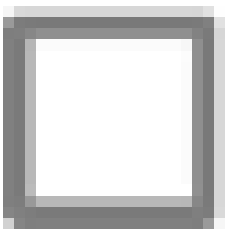
Führen Sie die Schritte in der Tabelle in der Reihenfolge aus, in der sie angezeigt werden.

Prüfliste

Element	Beschreibung
☐	Als Anwender mit ServiceNow AI Platform® Administratorrolle, richten Sie Ihr ein ServiceNow AI Platform® Instanz. **a.** Zuweisen ServiceNow AI Platform® Und Security Incident Response Rollen. **b.** Überprüfen Sie, ob vorhanden ist ServiceNow Security Incident Response Und andere Plugins, die die Integration unterstützen, werden für Ihr Release von installiert und aktiviert ServiceNow AI Platform. **c.** Installieren und konfigurieren Sie einen MID-Server in Ihrem ServiceNow AI Platform® Instanz.

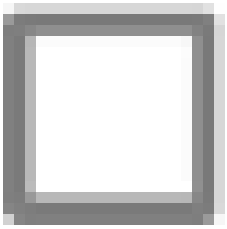
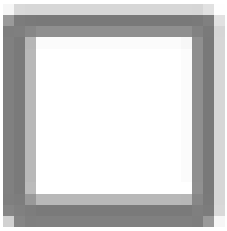
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Beschreibung
	d. Erstellen Sie eine Genehmigungsgruppe, wenn Sie Anforderungen verarbeiten möchten, die vom Security Incident-Analysten für den isolierten Host übermittelt wurden, und Aktionen für Malware-Scans initiieren möchten. Weitere Informationen finden Sie unter Richten Sie Ihr ein ServiceNow AI Platform Instanz für McAfee ePO Integration.
	Als McAfee ePO Administrator, richten Sie Ihr ein McAfee ePO Konsole. **a.** Stellen Sie sicher, dass Sie Version 5,9 von verwenden McAfee ePO. **b.** Installieren Sie ServiceNow Erweiterungs-Plugin in Ihrem McAfee ePO Konsole. **c.** Stellen Sie sicher, dass Sie Sicherheits-Tags in erstellt haben McAfee ePO Konsole für die Isolierung des Hosts und die Initiierung von Malware-Scan-Aktionen. Weitere Informationen finden Sie unter Richten Sie Ihr ein McAfee ePO Konsole, in die integriert werden soll Security Incident Response(SIR). Um weitere Informationen zu erhalten und die Plugin-Datei für die Erweiterung zu erhalten, finden Sie in ServiceNow AI Platform Instanz, navigieren Sie zu **Wissen** > **Artikel** > **Alle** Und geben Sie im Feld Suche Folgendes ein: ServiceNow Security Operations-Erweiterung für McAfee ePO .
	Als Anwender mit ServiceNow AI Platform Administratorrolle installieren McAfee ePO Anwendung aus dem ServiceNow Store, Konfigurieren Sie einen Server, und stellen Sie eine Verbindung mit her McAfee ePO Konsole. Weitere Informationen finden Sie unter Installieren Sie die Anwendung, und konfigurieren Sie einen Server für McAfee ePO Integration.
	Als Anwender mit ServiceNow AI Platform Security Incident-Administratorrolle. Bearbeiten Sie die Sicherheits-Tag-Namen in Ihrem ServiceNow AI Platform® Instanz so, dass sie mit den Tag-Namen übereinstimmen, die Sie in erstellt haben McAfee ePO Konsole. Weitere Informationen finden Sie unter Bearbeiten Sie Sicherheits-Tags in ServiceNow AI Platform Für McAfee ePO Integration.
	Erstellen Sie als Benutzer mit der Rolle „Security Incident-Administrator“ ein Profil für McAfee ePO Fähigkeiten. Informationen zu Profilen finden Sie unter McAfee ePO Integrationsfähigkeitsprofile. Informationen zu den zum Erstellen eines Profils erforderlichen Schritten finden Sie unter Erstellen Sie ein Fähigkeitsprofil.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Beschreibung
	Konfigurieren Sie als Benutzer mit der Rolle „Security Incident-Administrator“ ein Profil, und testen Sie Security Incidents. **a.** Überprüfen Sie die Informationen zu Auslösebedingungen und Einstellungen. **b.** Konfigurieren Sie ein Profil. **c.** Security Incidents testen und in der Vorschau anzeigen. **d.** Suchen Sie Suchergebnisse und andere Details in den zugehörigen Listen des Security Incident. **e.** Erstellen und konfigurieren Sie verschiedene Arten von Profilen und testen Sie Security Incidents für jeden Typ. Informationen zu Auslösebedingungen und dem Feld „alternatives CI“ finden Sie unter Definieren von Auslösebedingungen mit einem CI-Feld (Configuration Item). Die Schritte, die zum Konfigurieren eines Profils, Testen und Vorschauen von Security Incidents und Beispiele für Profiltypen erforderlich sind, finden Sie in den folgenden Beispielen Einstellungen konfigurieren.
	Als Anwender mit ServiceNow AI Platform Rolle des Security Incident-Analysten, zusätzliche Anforderungen für Malware-Scans übermitteln und Bedrohungsereignisse auflisten. Weitere Informationen finden Sie unter Auslöser McAfee ePO Profil manuell aus einem Security Incident In ServiceNow AI Platform, Als Anwender mit einer Genehmigungsrolle oder als Mitglied einer Genehmigungsgruppe genehmigen Sie Anforderungen zum Isolieren der Hostisolierung und Entfernen der Isolierung. Weitere Informationen zur Verarbeitung von Genehmigungsanforderungen finden Sie unter Erstellen Sie eine Genehmigungsgruppe.

Sie haben die Einrichtungsschritte erfolgreich abgeschlossen, die Anwendung installiert und konfiguriert und die erwarteten Ergebnisse für die Integration verifiziert.

Richten Sie Ihr ein ServiceNow AI Platform® Instanz für McAfee ePO Integration

Im folgenden Abschnitt werden die Setup-Aufgaben aufgeführt, die Sie in ausführen müssen ServiceNow AI Platform® Instanz vor der Installation der Anwendung für McAfee ePO Integration.

Richten Sie Anforderungen ein

Erforderliche Rolle: ServiceNow AI Platform Administrator (Administrator). Überprüfen Sie die folgenden Informationen vor Ihrem ServiceNow AI Platform® Instanz für McAfee ePO Integration.

Die folgende Tabelle enthält eine Liste der Setup-Anforderungen für die Anwendung. Vergewissern Sie sich, dass Sie diese Aufgaben abgeschlossen haben, bevor Sie die Anwendung für die Integration aus installieren ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie die Aufgabe ein	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform® Und Security Incident Response(SIR) Rollen.	Die folgenden Rollen sind erforderlich: • Ein Anwender mit der Rolle „Systemadministrator“ (Administrator), um die Anwendung zu installieren. • Ein Anwender mit der Rolle „Security Incident Administrator“ (sn_si.admin) konfiguriert die Anwendung und erstellt, aktiviert und entfernt Profile. • Ein Anwender mit der Rolle Security Incident Analyst (sn_si.Analyst) arbeitet mit Security Incidents. Aufgaben umfassen das manuelle Starten von Profilen aus Security Incidents. Wenn die Genehmigungsoption während des Konfigurationsschritts in einem Profil ausgewählt ist, übermitteln Anwender mit dieser Rolle auch Anforderungen zum Isolieren von Hosts und zur Rückgabe an das Netzwerk.
Stellen Sie sicher, dass Sie Version 5,9 von verwenden McAfee ePO.	Die Integration unterstützt Version 10.4.3 des McAfee ePolicy Orchestrator.
Überprüfen Sie, ob Sie installiert haben ServiceNow Erweiterungs-Plugin in Ihrem McAfee ePO Konsole.	Installieren Sie ServiceNow Plugin in Ihrem McAfee ePO Konsole. Weitere Informationen und zum Abrufen der Plugin-Datei finden Sie in ServiceNow AI Platform Instanz, navigieren Sie zu **Wissen** > **Artikel** > **Alle** Und geben Sie im Feld Suche ServiceNow Security Operations Extension für McAfee ePO ein.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	Security Incident Response Dependency-Plugin (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Für die Integration erforderliche Anwendungen. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie die Aufgabe ein	Beschreibung
	1. Security Incident Response **2.** Arbeitsbereich für Security Incident Response **3.** Sicherheits-Integrations-Framework **4.** Security Support Common **5.** Orchestration Des Sicherheitssupports Weitere Informationen zum Installieren der Core-Anwendungen für Security Operations finden Sie unter Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.
Überprüfen Sie, ob Sie einen MID-Server installiert und konfiguriert haben.	In ist ein installierter und konfigurierter MID-Server erforderlich ServiceNow AI Platform® Instanz. Siehe ServiceNow-Produktdokumentationswebsite Weitere Informationen zu MID-Servern.
Wenn Sie den Genehmigungsprozess für Profile aktivieren möchten, stellen Sie sicher, dass Sie eine Genehmigungsgruppe zur Verarbeitung von Anforderungen erstellt haben.	Es ist ein optionaler Genehmigungsprozess verfügbar, um Hostcomputer zu isolieren und im Netzwerk wiederherzustellen. Wenn diese Option aktiviert ist, ist eine vorherige Genehmigung erforderlich, bevor Hostcomputer isoliert und in Ihrem Netzwerk wiederhergestellt werden. Wenn Ihre Organisation eine zusätzliche Kontrolle über diese Aktionen haben möchte, aktivieren Sie **Genehmigung erforderlich** Option während des Konfigurationsschritts für ein Profil. Standardmäßig ist der Genehmigungsbehörde zugewiesen ServiceNow AI Platform® Security Incident-Administrator (sn_si.admin). Diese Berechtigung kann einer Genehmigungsgruppe neu zugewiesen werden. Innerhalb der Gruppe hat jedes Mitglied die Berechtigung, Anforderungen zu genehmigen oder abzulehnen. Sie wählen während des Konfigurationsschritts Ihres Profils eine aktive Genehmigungsgruppe aus. Weitere Informationen finden Sie unter Erstellen Sie eine Genehmigungsgruppe.

Richten Sie Ihr ein McAfee ePO Konsole, in die integriert werden soll Security Incident Response(SIR)

Im folgenden Abschnitt werden die Setup-Schritte aufgeführt, die Sie in ausführen müssen McAfee ePO-Konsole vor der Installation der Anwendung über ServiceNow Store Für die Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: McAfee ePO Administrator

Als Anwender mit McAfee ePO Administratorberechtigung. Überprüfen Sie, ob Sie installiert haben Servicenow.zip Erweiterungs-Plugin in Ihrem McAfee ePO Konsole. Dieses Erweiterungs-Plugin ist für die Integration erforderlich. Weitere Informationen und zum Abrufen des Plugins finden Sie in ServiceNow AI Platform Instanz, navigieren Sie zu **Wissen** > **Artikel** > **Alle**an. Geben Sie im Feld Suche ServiceNow Security Operations Extension für McAfee ePO ein.

Warum und wann dieser Vorgang ausgeführt wird

Die ServiceNow Das Erweiterungs-Plugin verbindet mit ServiceNow AI Platform Instanz für Ihren McAfee ePO Konsole. Mit dieser Verbindung können Sie auf die Sicherheits-Tags verweisen, die Sie in erstellen McAfee ePO Konsole für die Isolierung des Hosts und die Initiierung von Malware-Scan-Aktionen für die Fähigkeitsprofile in Ihrem ServiceNow AI Platform Instanz.

Die Sicherheits-Tags in Ihrem McAfee ePO Die Konsole muss mit den Sicherheits-Tags in den Fähigkeitsdatensätzen in übereinstimmen ServiceNow AI Platform Instanz.

Die folgenden Schritte zeigen Ihnen, wie Sie das Erweiterungs-Plugin installieren und ein Sicherheits-Tag in erstellen McAfee ePO Konsole und weisen Sie dem Tag eine Aktion zu. Für weitere Informationen zu den Sicherheits-Tags in McAfee ePO-Konsole, siehe McAfee-Produktdokumentation Website.

Hinweis:
Die Zahlen im folgenden Abschnitt stammen aus dem McAfee ePO Konsole.

Prozedur

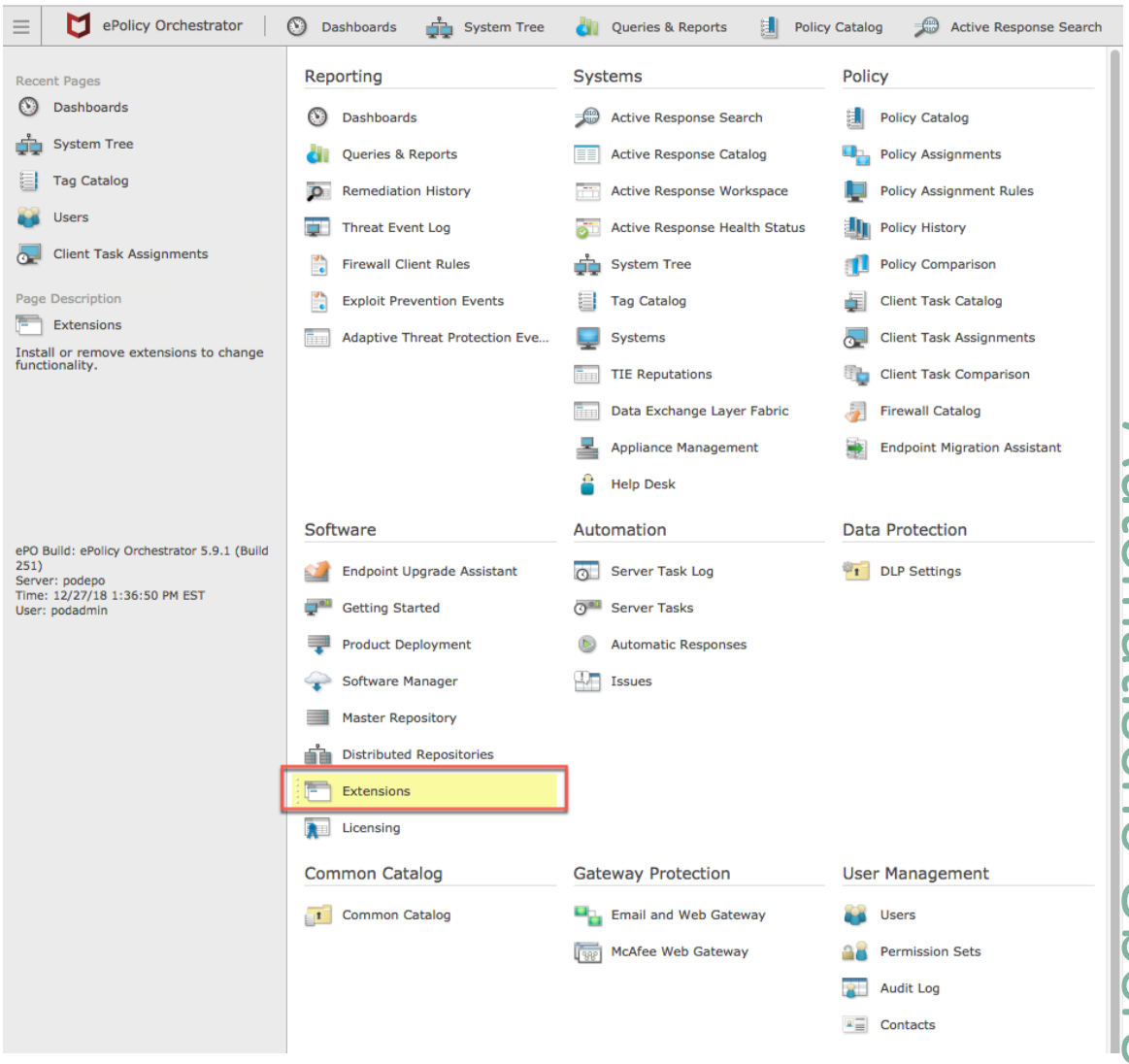
1. Wenn Sie den nicht installiert haben ServiceNow Erweiterungs-Plugin auf Ihrem McAfee ePO Führen Sie die folgenden Schritte aus, um sie zu installieren.

   a. Melden Sie sich bei an McAfee ePO Konsole mit Ihrem McAfee-Anwendernamen und Passwort.

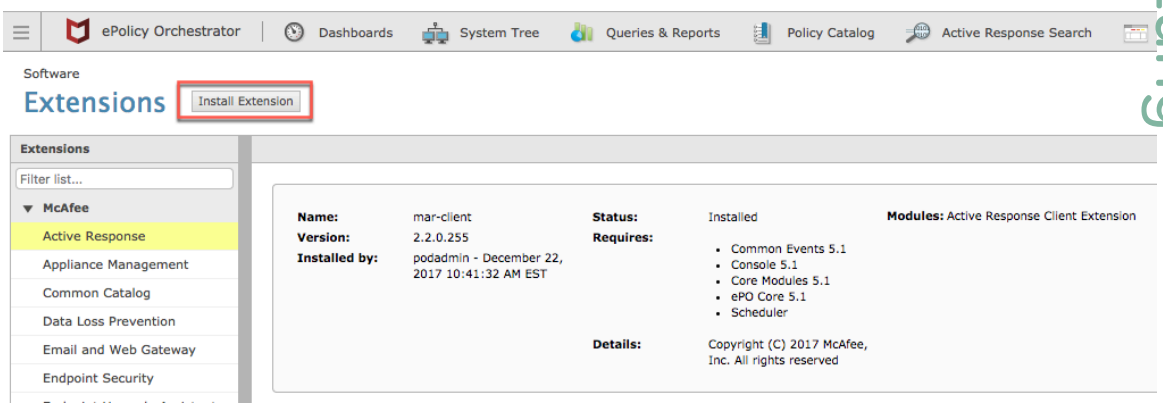
2. Wenn die in der folgenden Abbildung gezeigte Seite nicht angezeigt wird, klicken Sie oben links im Banner der Homepage auf das Menüsymbol, um sie anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie im Abschnitt Software auf **Erweiterungen** Link.



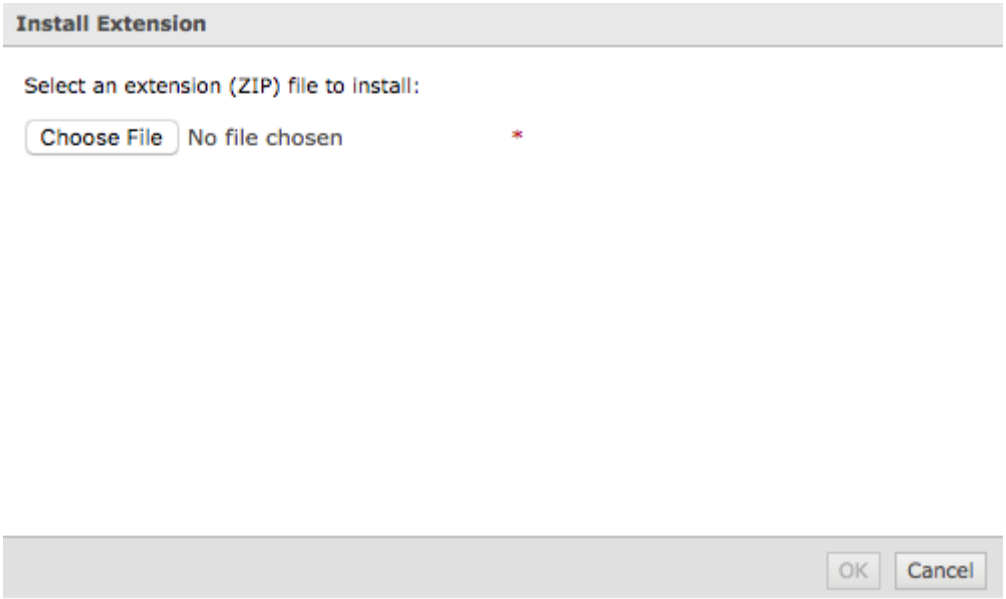
4. Klicken Sie auf der angezeigten Seite „Erweiterungen“ auf **Installieren Sie Die Erweiterung** .



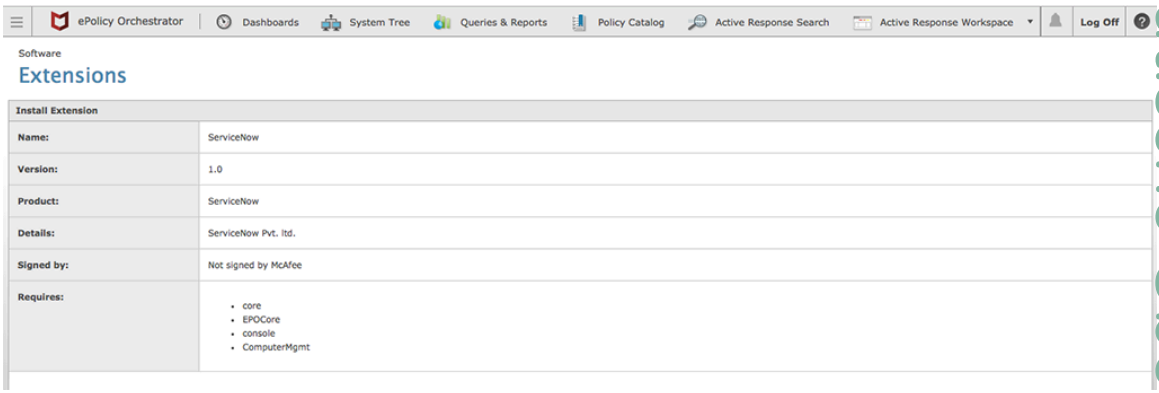
5. Klicken Sie im Dialogfeld „Erweiterung installieren“ auf **Wählen Sie Datei** , Navigieren Sie zu Servicenow.zip Datei auf Ihrem System und klicken Sie auf **OK** Um es herunterzuladen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nachdem der Download abgeschlossen ist, wird die Seite „Softwareerweiterungen“ mit angezeigt ServiceNow Erweiterungs-Plugin aufgeführt.

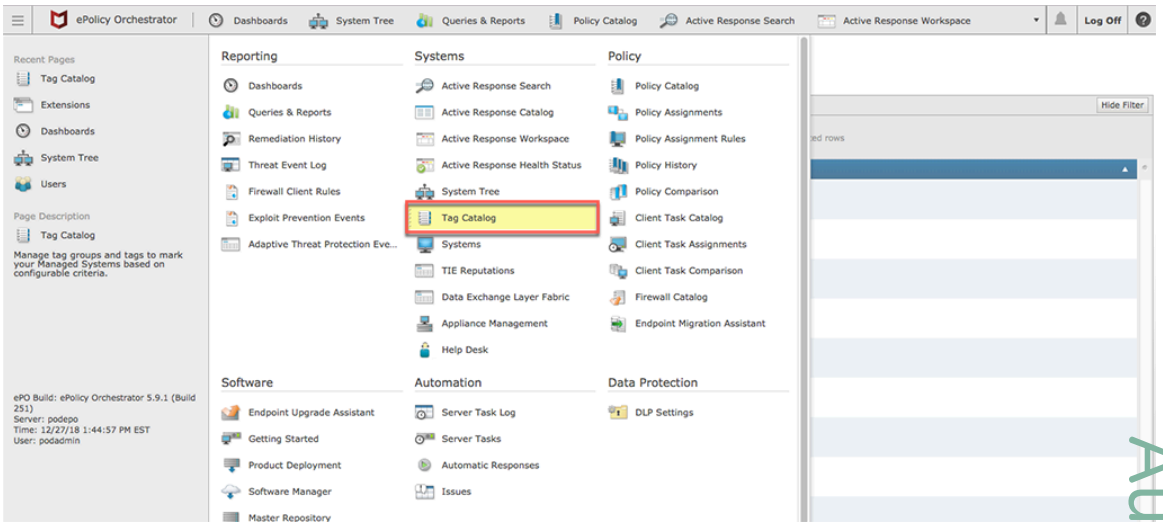


Sie haben erfolgreich installiert ServiceNow Plugin-Erweiterung auf Ihrem McAfee ePO Konsole.

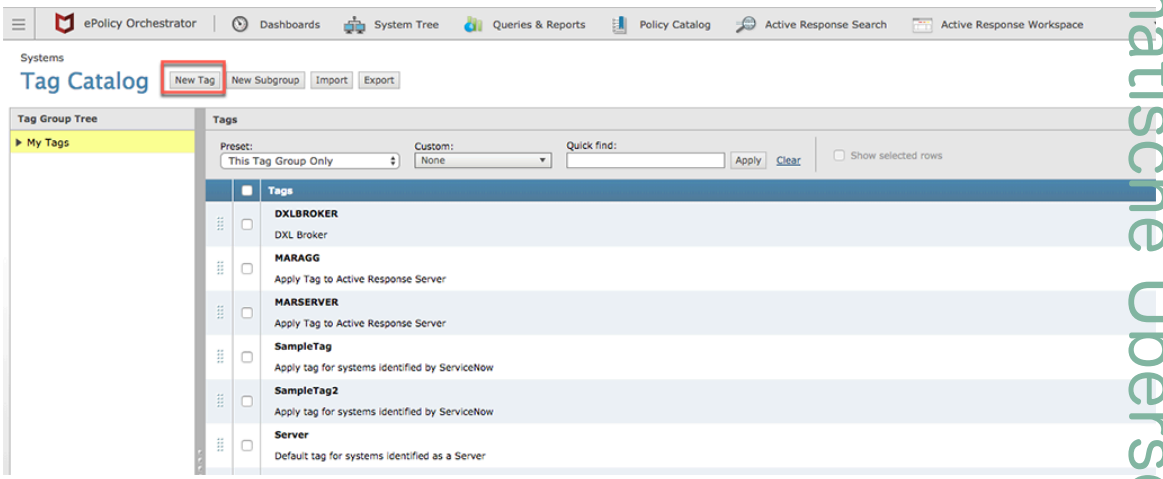
6. Wenn Sie in keine Sicherheits-Tags erstellt haben McAfee ePO Konsole für die Aktionen „Malware-Scan initiieren“ und „Host isolieren“ führen Sie die folgenden Schritte aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren Sie zur Homepage, und klicken Sie auf **Tag-Katalog** Link.

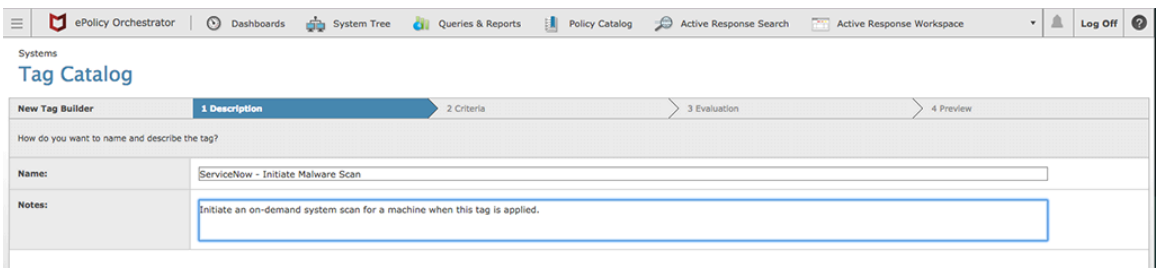


b. Klicken Sie auf der angezeigten Tag-Katalog-Seite auf **Neues Tag** .



c. Wenn der Schritt Beschreibung in der angezeigten Fortschrittsleiste ausgewählt ist, geben Sie einen Namen und eine Beschreibung für das Tag ein.

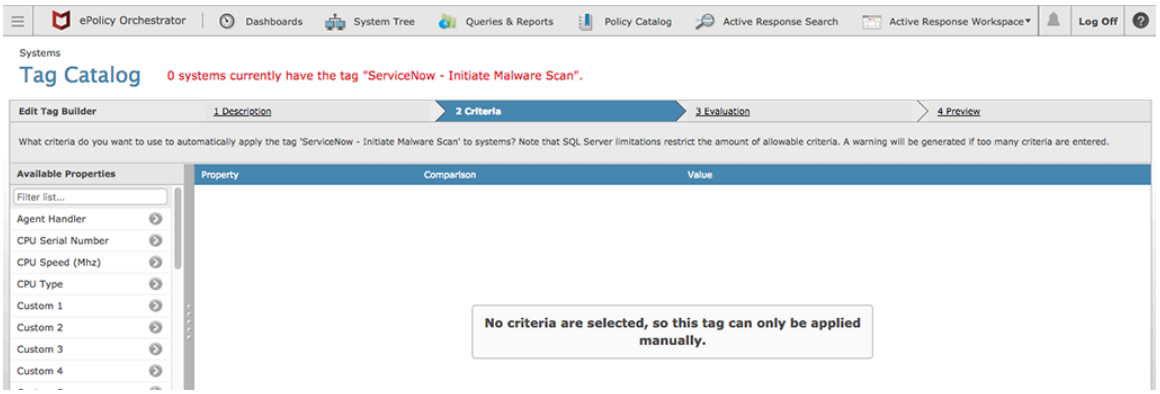
In diesem Beispiel wird ein Tag mit einem Namen und einer Beschreibung für die Fähigkeit „Malware-Scan initiieren“ angezeigt. Dieser Tag-Name ist das, was in Ihrem abgeglichen und referenziert wird ServiceNow AI Platform Instanz.



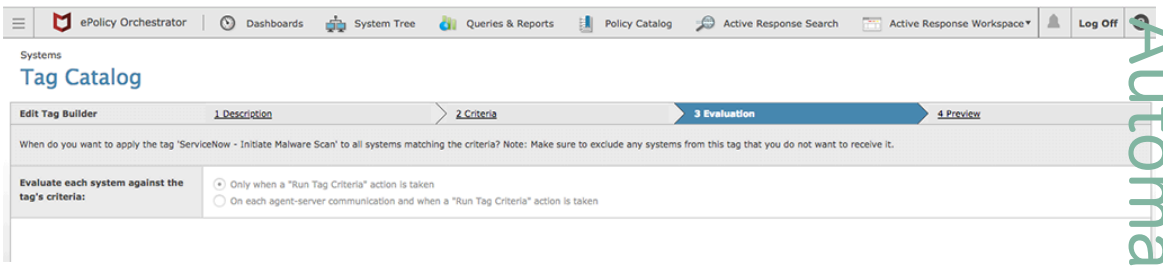
d. Um zum Kriterienschritt zu gelangen, klicken Sie auf **Kriterien** In der Fortschrittsleiste.
Die angezeigten Nachrichten zeigen an, dass diesem Tag derzeit keine Aktionen zugewiesen sind und das Tag nur manuell angewendet werden kann.

Automatische Übersetzung

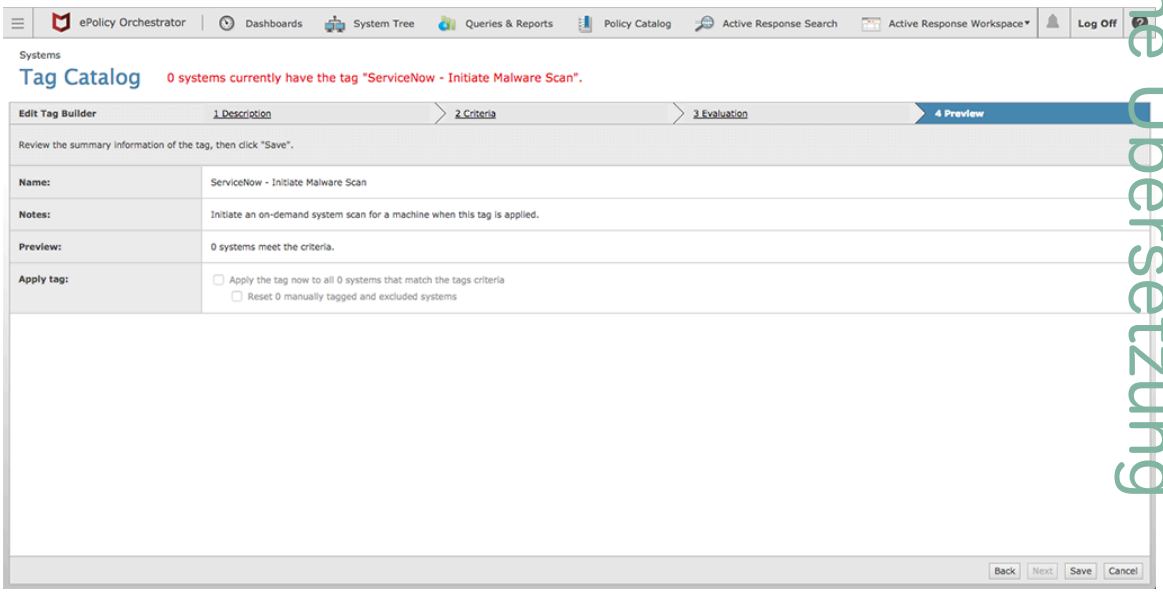
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Klicken Sie Auf **Bewertung** In der Fortschrittsleiste, um fortzufahren.



f. Wenn die Seite „Tag-Katalog“ des Bewertungsschritts angezeigt wird, belassen Sie die Einstellungen auf dieser Seite in ihren Standardeinstellungen, und klicken Sie in der Fortschrittsleiste auf **Vorschau** .

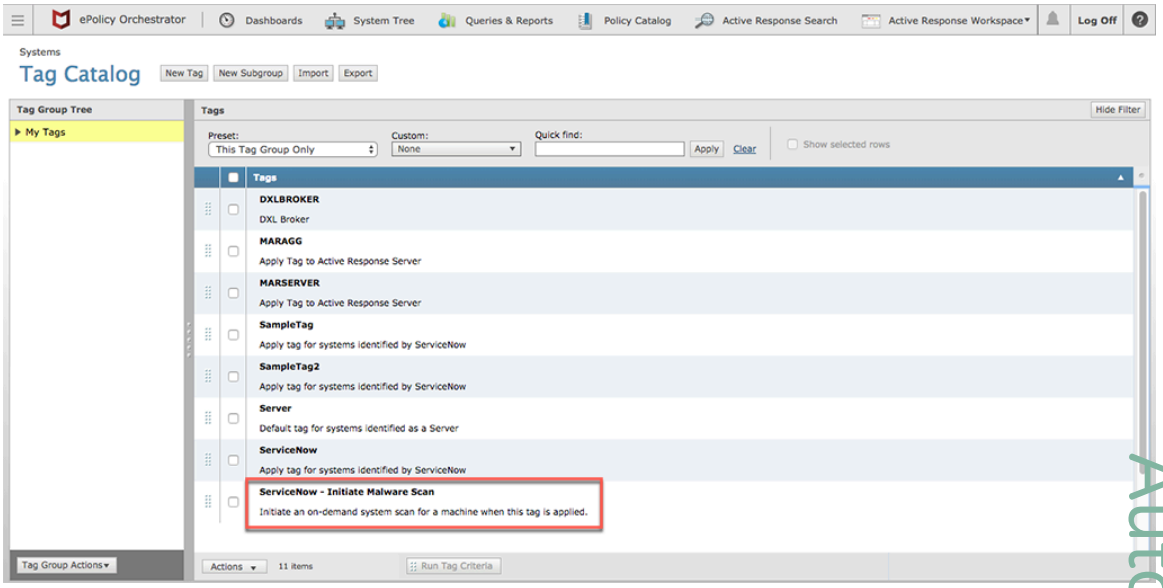


g. Wenn die Vorschauseite angezeigt wird, klicken Sie unten rechts auf der Seite auf **Speichern** Zum Speichern des Datensatzes.

Automatische Übersetzung

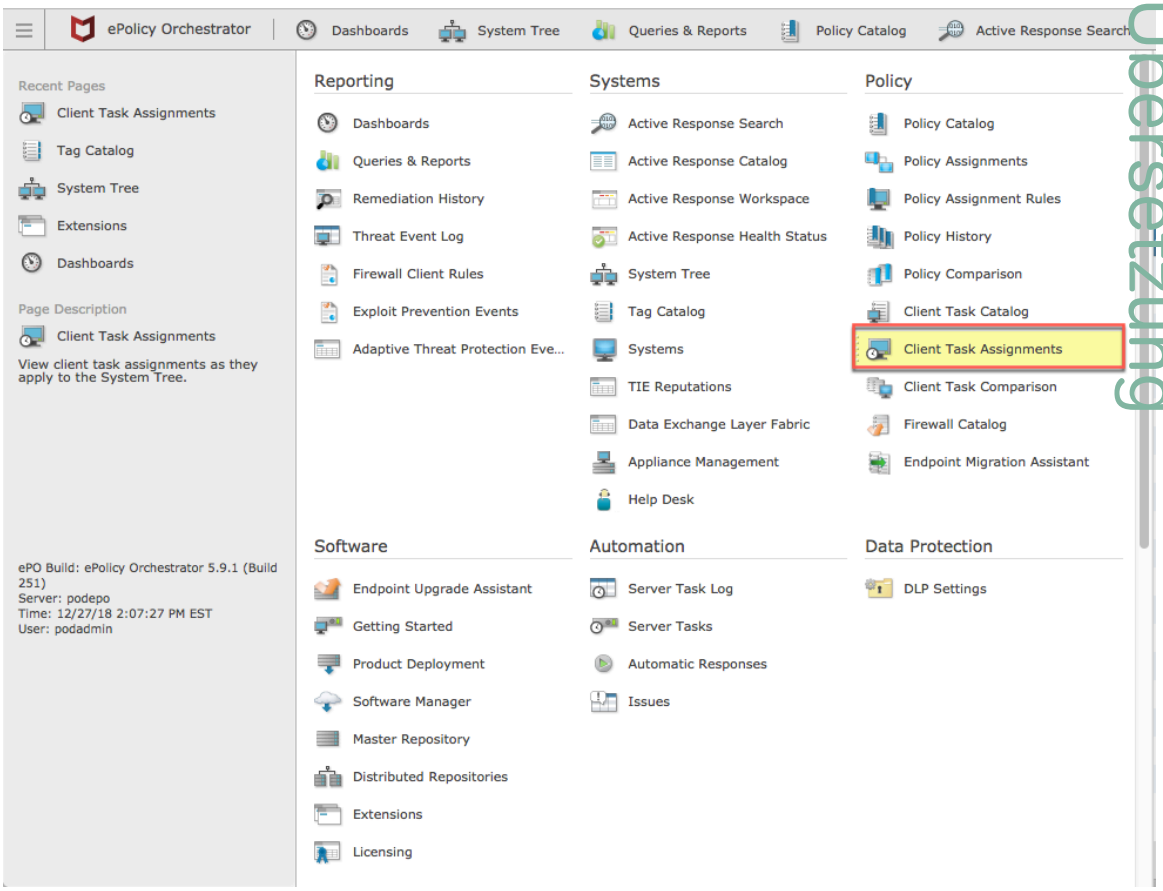
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das neue Tag wird im Tag-Katalog angezeigt, wie in der folgenden Abbildung dargestellt.



7. Erstellen Sie ein Sicherheits-Tag für die Host-Isolierungsaktion, indem Sie die vorherigen Schritte wiederholen.
   Nachdem Sie beide Tags erstellt haben, können Sie den neuen Tags Aktionen zuweisen.
8. Führen Sie die folgenden Schritte aus, um Ihrem neuen Tag eine Aktion hinzuzufügen.

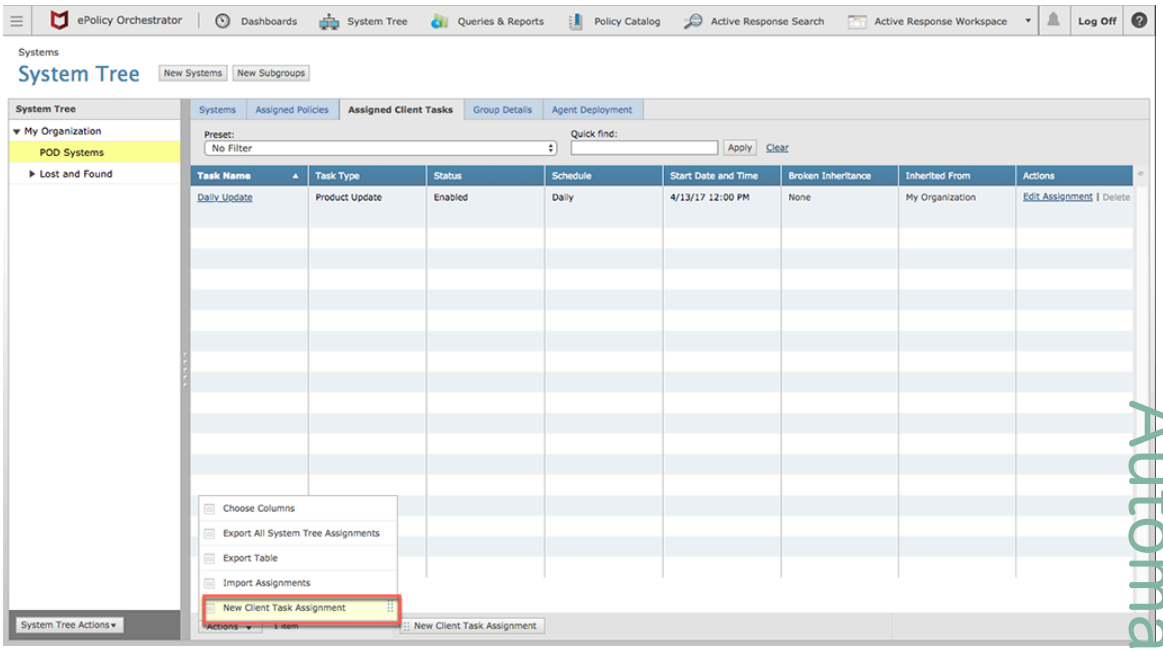
   a. Navigieren Sie zur Homepage, und klicken Sie im Abschnitt Richtlinie auf **Client-Aufgabenzuweisungen** Link.



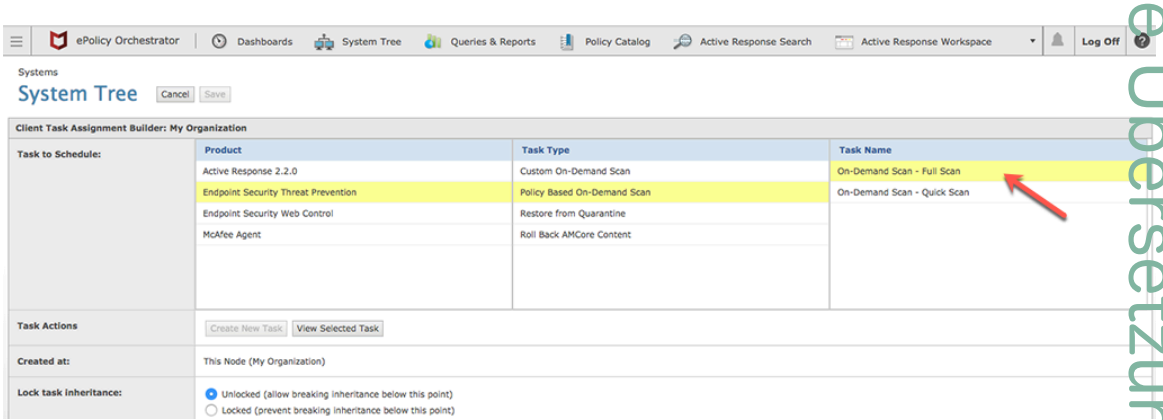
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Erweitern Sie auf der Seite „Systemstruktur“, die unten auf der Seite angezeigt wird **Aktionen** Menü und wählen Sie aus **Neue Client-Aufgabenzuweisung** .



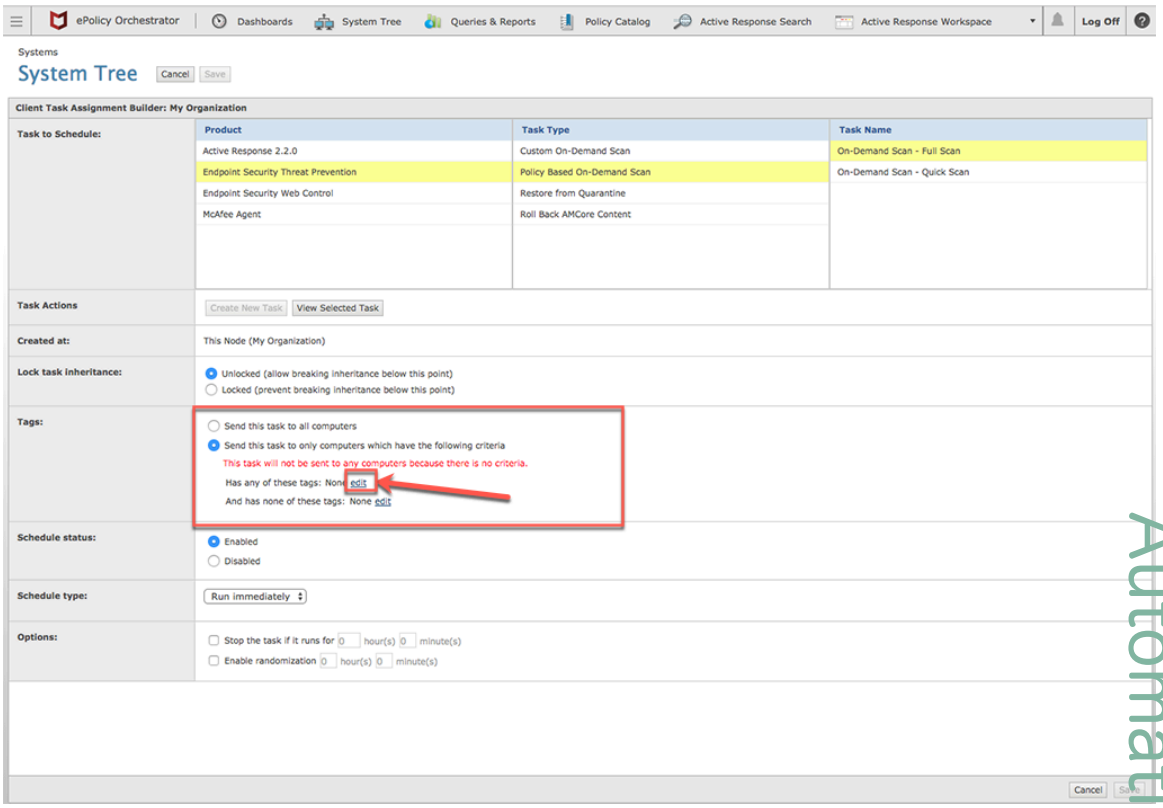
c. Navigieren Sie auf der angezeigten Seite zu **Endpoint Security Threat Prevention** > **Richtlinienbasiert Bei Bedarf-Scan** > **Scan Bei Bedarf: Vollständiger Scan** Indem Sie den Pfad wie in der folgenden Abbildung gezeigt auswählen.



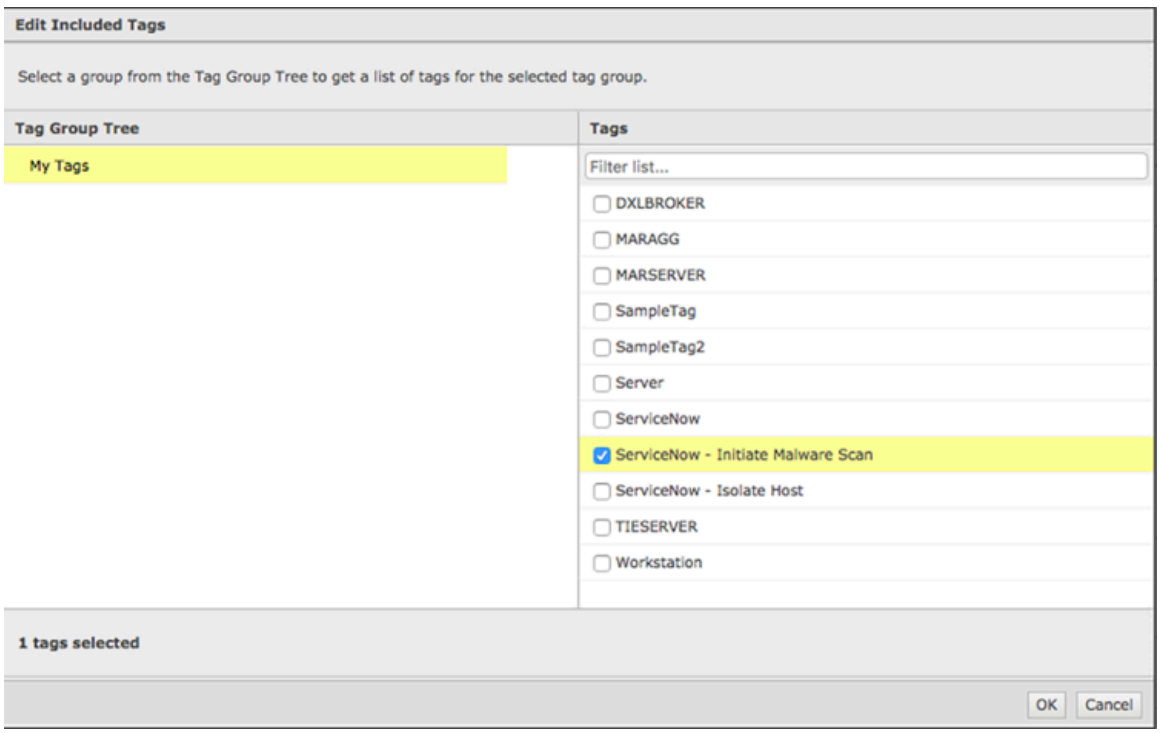
d. Im Abschnitt „Tags“ unter der Optionsschaltfläche und neben Hat eines der folgenden Tags: , Klicken Sie auf **Bearbeiten** Link zum Bearbeiten der Kriterien für das Tag.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Wählen Sie im angezeigten Dialogfeld Malware-Scan initiieren aus ServiceNow Tag, das Sie in den vorherigen Schritten erstellt haben, und klicken Sie auf **OK** .

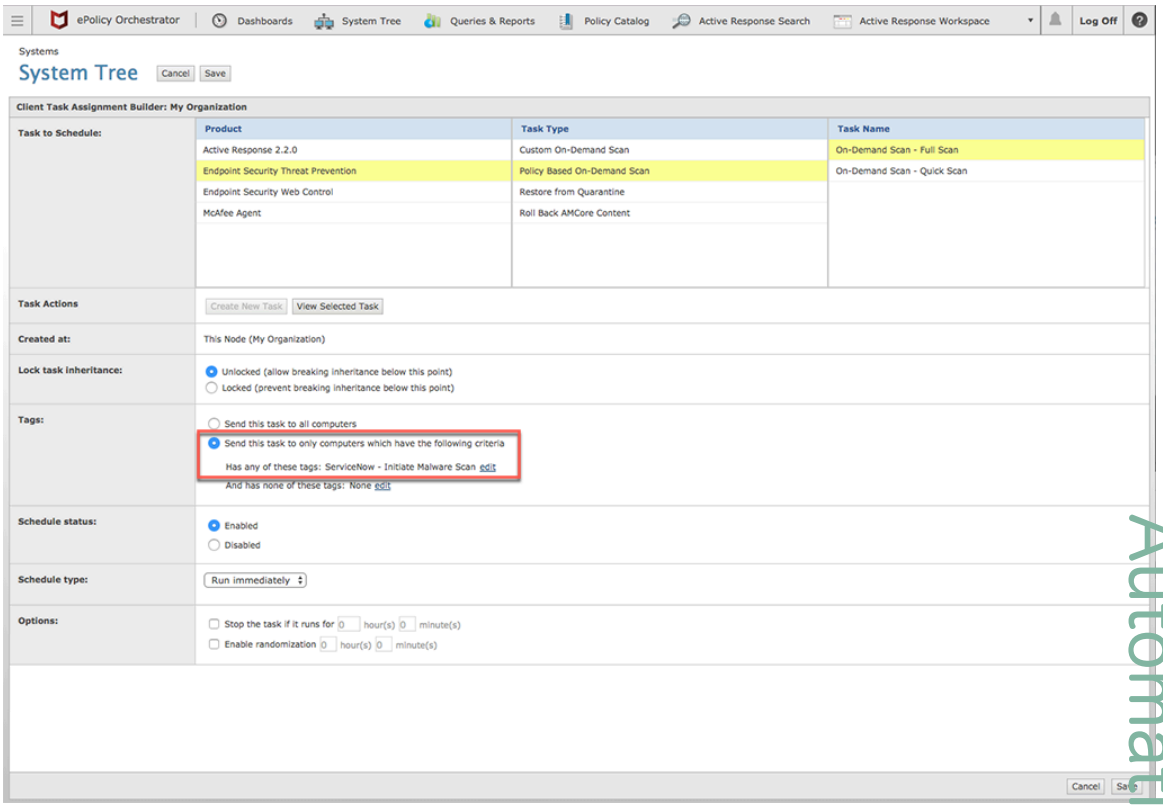


Das von ServiceNow erstellte Tag „Malware-Scan initiieren“ ist der Aktion „Scan bei Bedarf“ zugewiesen.

f. Klicken Sie auf **OK**.
Im Abschnitt „Tags“ unter der Optionsschaltfläche und neben Hat eines der folgenden Tags: , Das Tag Malware-Scan initiieren wird angezeigt.

Automatische Übersetzung

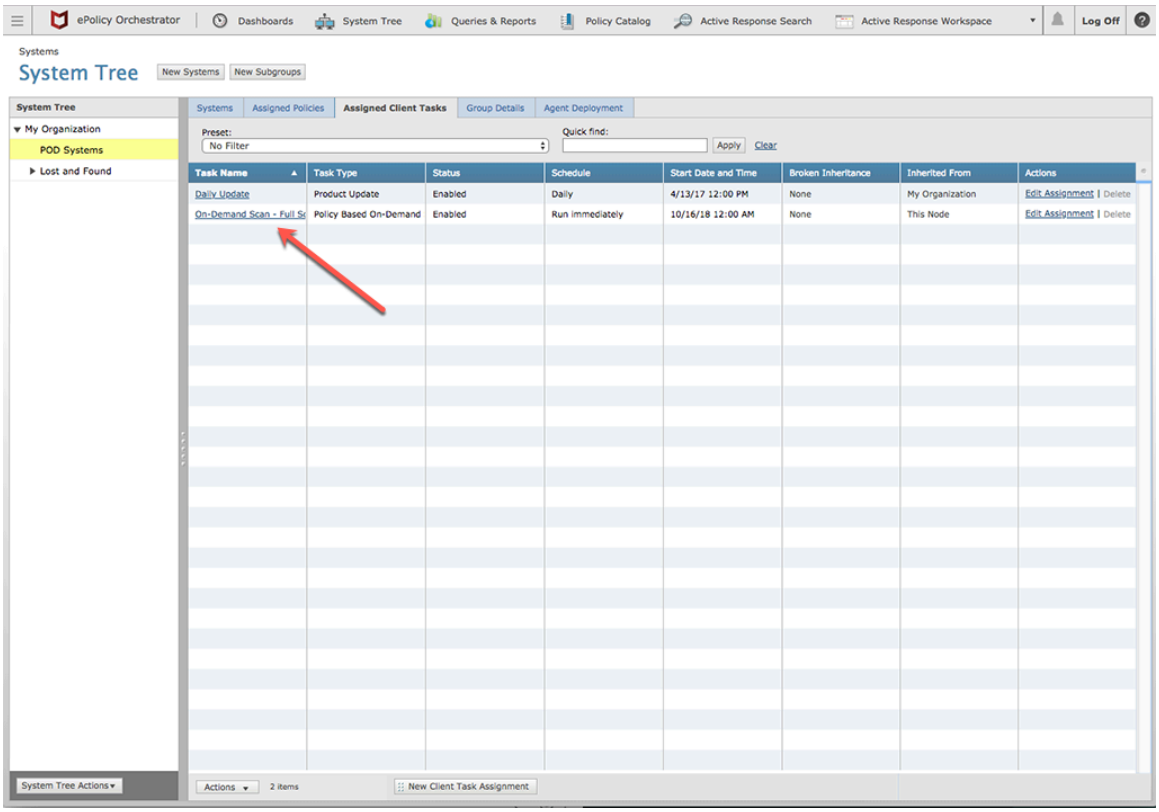
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



g. Klicken Sie auf **Speichern**.
Auf der Seite „Systemstruktur“ wird die Aufgabe in der Liste zugewiesene Client-Aufgaben (Registerkarte) angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



h. Wenn Sie der Aktion Host isolieren keine Aktion zugewiesen haben, wiederholen Sie die vorherigen Schritte, um sie zuzuweisen.

Sie haben das Erweiterungs-Plugin erfolgreich installiert, Sicherheits-Tags erstellt und Ihren Tags Aufgaben zugewiesen. Sie haben das Setup für die Integration in abgeschlossen McAfee ePO Konsole. Der nächste Schritt besteht darin, einen Server in zu konfigurieren ServiceNow AI Platform Instanz.

Installieren Sie die Anwendung, und konfigurieren Sie einen Server für McAfee ePO Integration

Bevor Sie die -Workflows für die -Integration aufrufen, installieren und konfigurieren Sie McAfee ePO Anwendung aus dem ServiceNow Store Auf Ihrem ServiceNow AI Platform Instanz. Die Konfiguration ist erforderlich, um eine Verbindung mit herzustellen McAfee ePO Konsole.

Vorbereitungen

Erforderliche Rolle: ServiceNow AI Platform Administrator (Administrator)

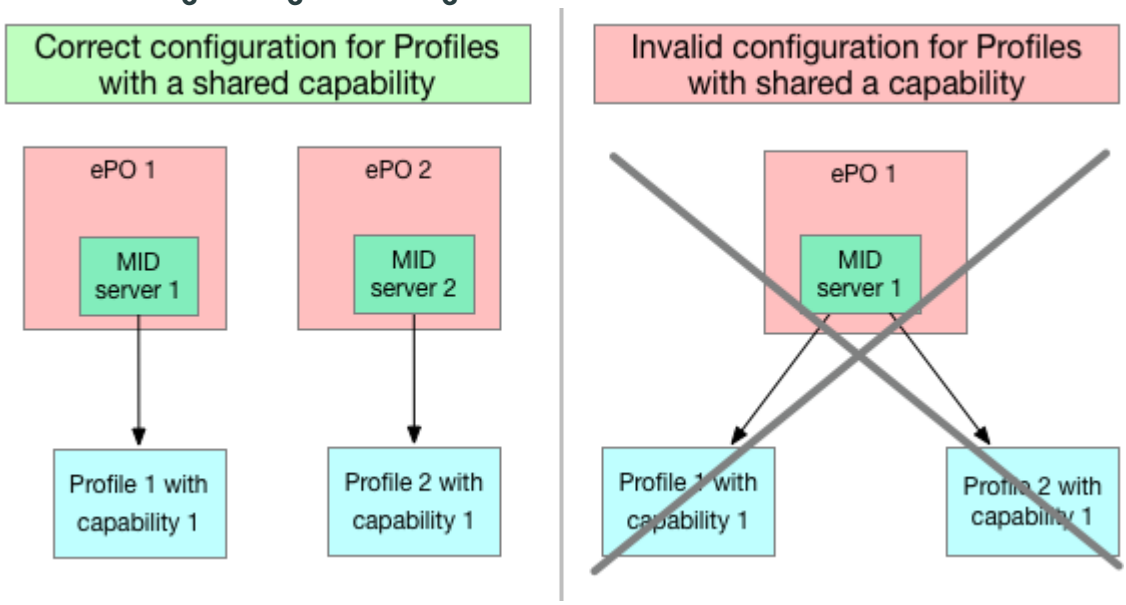
Warum und wann dieser Vorgang ausgeführt wird

Die Integration unterstützt mehrere Server, um jedoch Konflikte in Profilen zu vermeiden, die dieselben Auslösebedingungen haben, können Sie keinen freigeben McAfee ePO Fähigkeit mit mehreren Profilen, die dieselbe verwenden McAfee ePO Server. Wie in der folgenden Abbildung gezeigt, können Sie beispielsweise Fähigkeit 1 in mehr als einem Profil haben, solange jedes Profil so lang ist McAfee ePO Der Server ist einem eindeutigen Profil mit Fähigkeit 1 zugeordnet.

Automatische Übersetzung

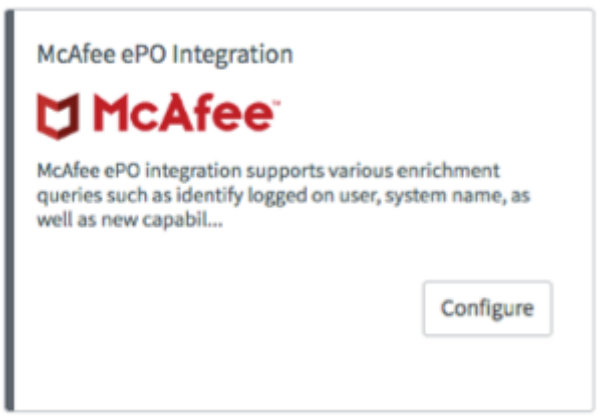
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einschränkungen des gemeinsam genutzten McAfee-Profils



Prozedur

1. Laden Sie herunter McAfee ePO Für Security Operations Von ServiceNow Store Und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie nach McAfee ePO Für Security Operations Integrationskachel und klicken Sie auf **Konfigurieren** .



4. Füllen Sie im Formular die Felder aus.

McAfee ePO-Integrationskonfiguration

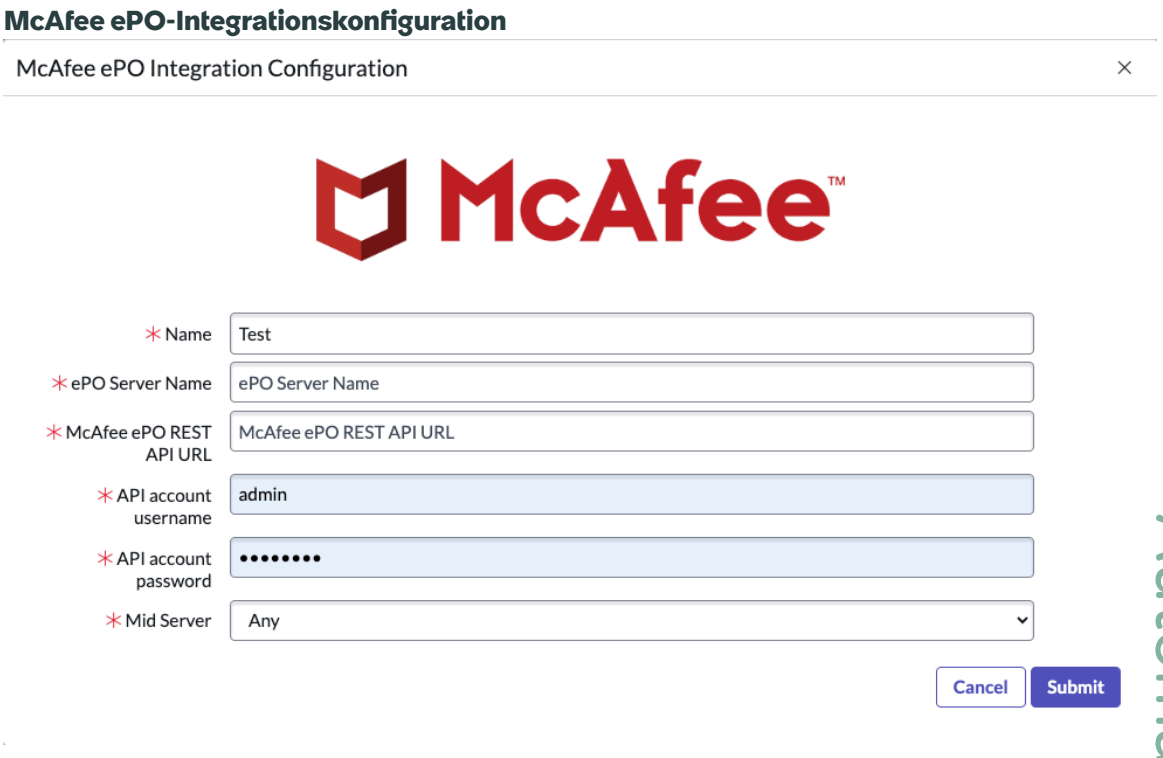
Feld	Beschreibung
Name	Name der Integration, z. B. `Demo-1` .
ePO-Servername	Name für McAfee ePO Server. Wenn Sie einen Server verwenden, ist ein Beispiel: `McAfee-Hauptsitz` (McAfee-Hauptsitz). Mit diesem Namen werden der Server und die zugehörigen Anmeldeinformationen erkannt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn Ihre Organisation Unterstützung für mehrere Server benötigt, geben Sie den Namen für jeden Server ein, und wiederholen Sie den Vorgang.
McAfee ePO-REST-API-URL	Basis-URL, die hostet McAfee ePO REST-API. Geben Sie die URL mit dem Protokoll https:// ein, z. B. `https://corp.epo_server:8443` .
API-Kontoanwendername	Eindeutiger Account-Anwendername, z. B. `ServiceNow-API` .
API-Kontopasswort	Eindeutiges Passwort für den API-Account.
MID-Server	Wählen Sie den Namen des MID-Servers aus, den Sie während des Setups von konfiguriert haben ServiceNow AI Platform Instanz. Sie können einen bestimmten MID-Server aus der Liste auswählen oder auswählen **Beliebig** Um die automatische Auswahl eines gültigen MID-Servers aus der Liste für diese Integration zu aktivieren. **Hinweis:** ○ Der während dieser Konfigurationszeit ausgewählte MID-Server gilt für die gesamte Integration. ○ In dieser Liste werden nur aktive und validierte MID-Server angezeigt. Standardmäßig ist der Wert auf festgelegt **Beliebig** . Ein Beispielname ist, `secops_LOCAL_MID-Server` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Absenden**.
   Die Liste McAfee ePO-Konfigurationen wird mit Ihrem neuen Konfigurationsdatensatz angezeigt. Sie haben die Konfiguration für erfolgreich abgeschlossen McAfee ePO Server.

> **Hinweis:**
> Wenn Ihre Organisation Unterstützung für mehrere Server benötigt, wiederholen Sie die Schritte.

Bearbeiten Sie Sicherheits-Tags in ServiceNow AI Platform Für McAfee ePO Integration

Bearbeiten Sie im Rahmen des Setups für die Integration die Sicherheits-Tag-Namen, die Sie in erstellt haben McAfee ePO-Konsole in Ihrem ServiceNow AI Platform Instanz. Bearbeiten Sie die Tag-Namen in ServiceNow AI Platform Instanz so, dass sie mit den Namen der Tags in übereinstimmen McAfee ePO Konsole.

Vorbereitungen
Erforderliche Rolle: ServiceNow AI Platform Security Incident-Administrator (sn_si.admin)

Warum und wann dieser Vorgang ausgeführt wird
Die Sicherheits-Tag-Namen in Ihrem McAfee ePO Die Konsole für die Aktionen „Malware-Scan initiieren“ und „Host isolieren“ muss mit den Sicherheits-Tag-Namen in den Datensätzen für diese Funktionen von übereinstimmen ServiceNow AI Platform Instanz.

Bevor Sie ein Fähigkeitsprofil zum Ausführen Ihrer Fähigkeiten erstellen, zeigen Sie die Liste der verfügbaren an McAfee ePO-Fähigkeiten und bearbeiten Sie die Sicherheits-Tags in Ihrem ServiceNow AI Platform Instanz so, dass sie mit den Sicherheits-Tag-Namen in übereinstimmen McAfee ePO Konsole.

Weitere Informationen zum Erstellen der Sicherheits-Tag-Namen in finden Sie in McAfee ePO Konsole, siehe Richten Sie Ihr ein McAfee ePO Konsole, in die integriert werden soll Security Incident Response(SIR).

Automatische Übersetzung

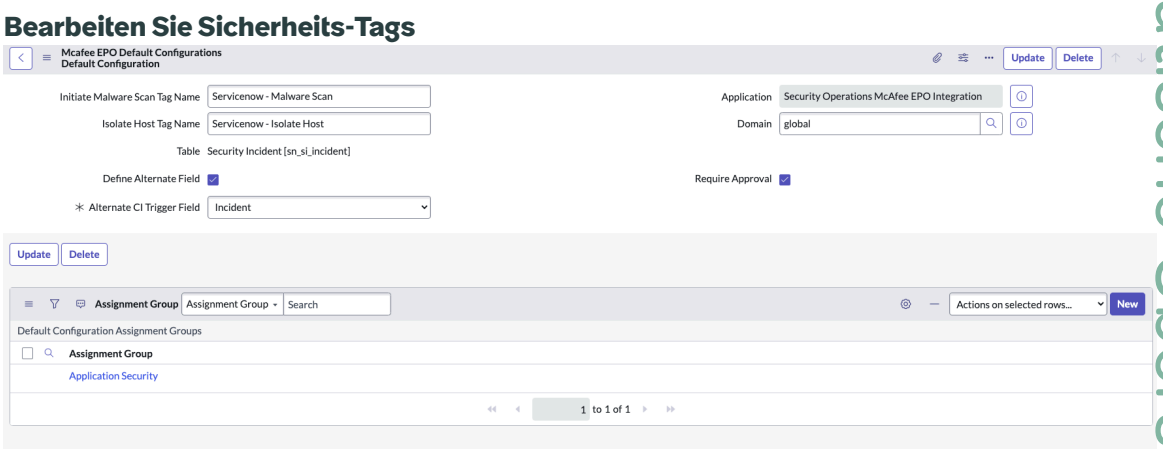
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **McAfee ePO-Integration** > **Standardeinstellungen**an.
2. Dient zum Bearbeiten des Sicherheits-Tag-Namens von McAfee ePO Integration, klicken Sie auf **Standardkonfiguration** .

   Hinweis:
   Stellt sicher, dass Sie diese Konfiguration durchführen, nachdem Sie installiert haben McAfee ePO Integration.

3. Geben Sie im Feld Tag-Name des Malware-Scans initiieren den Namen des Sicherheits-Tags ein, das Sie in erstellt haben McAfee ePO Konsole für die Aktion „Scan initiieren“.
   Beispiel: ServiceNow – Malware-Scan
4. Geben Sie im Feld Host-Tag-Name isolieren den Namen des Sicherheits-Tags ein, das Sie in erstellt haben McAfee ePO Konsole für die Aktion „Host isolieren“.
   Beispiel: ServiceNow – Host isolieren
5. Wenn Sie das Feld „CI-Auslöser“ bei der Incident-Erstellung nicht verwenden möchten, wählen Sie aus **Definieren Sie ein alternatives Feld** Kontrollkästchen.
   Wenn diese Option aktiviert ist, wird die Auswahlliste alternatives CI-Auslöserfeld angezeigt.



6. Wählen Sie ein alternatives Feld aus der Auswahlliste aus, um nach Ihren CI-Suchkriterien zu suchen.
   In diesem Beispiel glauben Sie als Anwender mit der Rolle „sn_si.admin“, dass das CI-Feld bei der Incident-Erstellung nicht im Security Incident ausgefüllt wird. Alternativ denken Sie, dass CI-Informationen für einen FQDN, einen Hostnamen oder eine IP-Adresse in ausgefüllt werden Identifiziertes CI Feld im Security Incident, und Sie wählen das Feld „identifiziertes CI“ als Alternative aus. Das identifizierte CI ist für dieses Beispiel ausgewählt, Sie können jedoch jedes Feld im Security Incident für das alternative CI verwenden.
7. Wählen Sie im Feld Domäne mithilfe der Suchoption eine Domäne oder Gruppe für diese Konfiguration aus.
   Beispiel: Global.
8. Wählen Sie im Feld Genehmigung erforderlich die Option aus **Genehmigung Erforderlich** Aktivieren Sie das Kontrollkästchen, wenn Sie die Funktionen Host isolieren und Isolierung entfernen verwenden.

   Hinweis:
   Die Funktionen „Malware-Scan initiieren“, „Bedrohungsereignisse auflisten“ und „Systemdetails abrufen“ erfordern keine Genehmigung.

9. Klicken Sie auf **Aktualisieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der EPO-Tag-Name wird aktualisiert und in der Liste „McAfee ePO-Standardkonfigurationen“ angezeigt. Der Sicherheits-Tag-Name für die Malware-Scan-Aktion in Ihrem ServiceNow AI Platform Instanz stimmt mit dem Namen für den Scan in überein McAfee ePO Konsole.

Sie haben die EPO-Tag-Namen für den Malware-Scan und die Host-Isolierungsfunktionen in erfolgreich bearbeitet ServiceNow AI Platform Instanz. Der nächste Schritt besteht darin, ein Profil für Ihre Fähigkeiten zu erstellen.

Zugehörige Informationen

McAfee-Produktdokumentation

Erstellen Sie eine Genehmigungsgruppe

Erstellen Sie eine Genehmigungsgruppe für McAfee ePO Für Security Operations Integration, die Anforderungen zum Isolieren von Hostcomputern genehmigen und sie im Netzwerk wiederherstellen kann.

Vorbereitungen

Sie können die Genehmigungsberechtigung nicht einer Gruppe neu zuweisen, es sei denn, in Ihrer Instanz ist eine Genehmigungsgruppe verfügbar.

Hinweis:
Die Option „Genehmigungen“ in Einstellungen konfigurieren Wird nur für die Funktionen „Host isolieren“ und „Host-Isolierung entfernen“ angezeigt.

Erforderliche Rolle: ServiceNow AI Platform® Security Incident-Administrator (sn_si.admin)

Warum und wann dieser Vorgang ausgeführt wird

Genehmigungsanforderungen, die vom Security Incident-Analyst zum Isolieren von Hostcomputern und zum Entfernen der Isolierung übermittelt werden, werden standardmäßig dem Anwender mit der Rolle „sn_si.admin“ zugewiesen. Als Anwender mit dieser Rolle können Sie diese Genehmigungsberechtigung während des Konfigurationsschritts für ein Profil neu zuweisen. Bevor Sie einer Genehmigungsgruppe eine Berechtigung neu zuweisen können, muss eine Genehmigungsgruppe im verfügbar sein Gruppen Liste in Ihrem ServiceNow AI Platform Instanz.

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Gruppen**an.
2. Klicken Sie in der Gruppenliste auf **Neu** .
3. Füllen Sie im Formular die Felder aus.

Genehmigungsgruppenformular

Feld	Beschreibung
Name	Name der Gruppe, die angezeigt wird, wenn eine Genehmigungsanforderung übermittelt wird, z. B. Genehmigt die McAfee-Host-Isolierung .
Gruppen-E-Mail	Gruppen-E-Mail-Verteilerliste oder die E-Mail-Adresse des Ansprechpartners, z. B. des Gruppenmanagers, McAfeeApproval@servicenow .Com
Manager	Name des Gruppenmanagers. Klicken Sie auf das Suchsymbol, um die Liste anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übergeordnet	(Optional) andere Gruppe, der diese Gruppe angehört, wenn diese Gruppe ein übergeordnetes Element hat.
Beschreibung	Zusätzliche Informationen zu dieser Gruppe.
Mitglieder einbeziehen	Option zum Einbeziehen von Mitgliedern in diese Gruppe.
Standard-Beauftragter	Option zum Auswählen eines Anwenders als Standardbeauftragter für diese Gruppe. Verwenden Sie die Suchoption, um die Liste der Anwender zu öffnen.
Rollen	Option zum Auswählen der Rollen für diese Gruppe. Verwenden Sie die Option Hinzufügen und Entfernen, um Rollen hinzuzufügen und zu entfernen.
Typ	Option zum Auswählen einer Kategorie für diese Gruppe. Verwenden Sie die Suchoption, um die Liste der Gruppentypen zu öffnen.
Lieferanten	Option zum Auswählen eines Lieferanten für diese Gruppe. Verwenden Sie die Suchoption, um die Liste der Lieferanten zu öffnen.

4. Klicken Sie auf **Absenden**.
   Die neue Gruppe wird in der Gruppenliste angezeigt.

   Diese Gruppe ist verfügbar, um Anforderungen zu verarbeiten, wenn Sie aktivieren **Genehmigung erforderlich** Option während der Konfiguration dieses Profils.

   Um Anforderungen zu überwachen und zu verarbeiten, die von Anwendern mit der Rolle „sn_si.Analyst“ übermittelt wurden, navigiert jedes Mitglied der Genehmigungsgruppe zu **Meine Genehmigungen** Registerkarte in ServiceNow AI Platform.

McAfee ePO Integrationsfähigkeitsprofile

Als Benutzer mit der Rolle Security Incident-Administrator (sn_si.admin) erstellen Sie Profile für McAfee ePO-Fähigkeiten in Ihrem ServiceNow AI Platform® Instanz. Sie gruppieren Abfragen oder Aktionen in Profilen und bestimmen welche McAfee ePO Fähigkeiten, die Sie ausführen möchten, wenn ein neuer Security Incident erstellt wird.

Fähigkeitsprofile

Sie erstellen Profile ™Damit Sie gruppieren können McAfee ePO-Fähigkeiten und konfigurieren Sie die Einstellungen für diese -Fähigkeiten von Ihrem aus ServiceNow AI Platform® Instanz. Sie haben die Flexibilität, mehrere Profile für diese Fähigkeiten zu erstellen, sodass Sie bestimmen können, welche Aktionen oder Abfragen aufgerufen werden, wenn ein aufgerufen wird Security Incident Response(SIR) Incident wird erstellt. Um die Anforderungen Ihrer Organisation zu erfüllen, können Sie beispielsweise ein einzelnes Profil erstellen, das Abfragen nach Systemdetails ausführt, Malware-Scans initiiert und Hostcomputer isoliert, oder Sie können mehrere Profile erstellen, jedes mit einem eigenen, einzelnen McAfee ePO Fähigkeit.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Profiltypen und erforderlich McAfee ePO Fähigkeiten

Primärer Zweck Ihres Profils	Richten Sie Anforderungen ein	McAfee ePO-Fähigkeiten, die für diesen Profiltyp erforderlich sind
Erfassen Sie Systemdetails	Keine	**Hostdetails abrufen**
Isolieren Sie einen Host	Verifizieren Sie mit Ihrem McAfee ePO Administrator, den Sie die Sicherheits-Tags für die Aktion „Host isolieren“ in erstellt haben McAfee ePO Konsole. Weitere Informationen finden Sie unter Richten Sie Ihr ein McAfee ePO Konsole, in die integriert werden soll Security Incident Response(SIR).	**Host isolieren**
Scannen und suchen Sie nach Bedrohungen auf Ihrem Host	Verifizieren Sie mit Ihrem McAfee ePO Administrator, den Sie die Sicherheits-Tags für die Aktion „Malware-Scan initiieren“ in erstellt haben McAfee ePO Konsole. Weitere Informationen finden Sie unter Richten Sie Ihr ein McAfee ePO Konsole, in die integriert werden soll Security Incident Response(SIR).	**Initiieren Sie Einen Malware-Scan** **Hinweis:** Als Teil von McAfee ePO Malware-Scan, die Funktionalität „Bedrohungsereignisse auflisten“ wird automatisch aufgerufen. Sie müssen jedoch nicht die Fähigkeit „Bedrohungsereignisse auflisten“ zum Profil mit der Malware-Scan-Funktion hinzufügen. Ergebnisse des Malware-Scans werden auf der Registerkarte Details zum Bedrohungsereignis im Security Incident angezeigt.
Entfernen Sie die Isolierung für einen Host	Verifizieren Sie mit Ihrem McAfee ePO Administrator, den Sie die Sicherheits-Tags für die Aktion „Host isolieren“ in erstellt haben McAfee ePO Konsole. Weitere Informationen finden Sie unter Richten Sie Ihr ein McAfee ePO Konsole, in die integriert werden soll Security Incident Response(SIR).	**Isolation entfernen**
Sammeln Sie Bedrohungsanreicherungsdaten.	Keine	**Listen Sie Bedrohungsereignisse Auf**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Fähigkeitsprofil

Erstellen Sie ein Profil, und wählen Sie aus McAfee ePO Fähigkeiten, die das Profil ausführen soll.

Vorbereitungen

Erforderliche Rolle: ServiceNow AI Platform® Security Incident-Administrator (sn_si.admin)

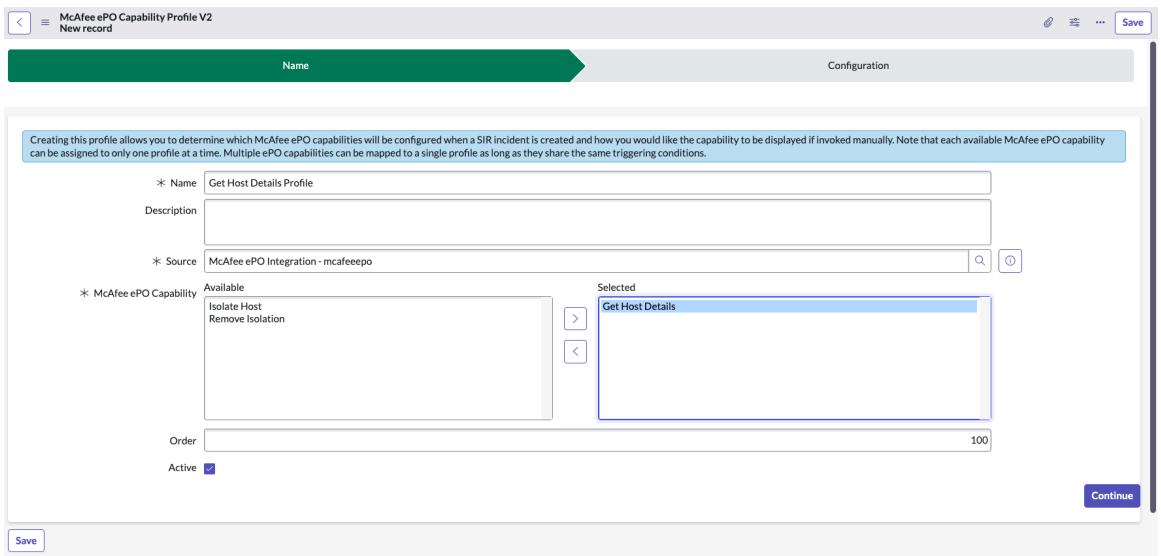
Warum und wann dieser Vorgang ausgeführt wird

Für diesen Schritt der Konfiguration erstellen Sie ein Profil für McAfee ePO Fähigkeiten. Berücksichtigen Sie beim Erstellen von Profilen die Absicht des Profils, bevor Sie hinzufügen McAfee ePO Fähigkeiten für IT. Beachten Sie beim Erstellen von Profilen die folgende Tabelle.

In der folgenden Tabelle sind die Fähigkeiten aufgeführt, die Sie einem Profil hinzufügen müssen, wenn das Profil bestimmte Abfragen oder Aktionen ausführen soll. Erstellen Sie ein einzelnes Profil, das Abfragen nach Hostdetails ausführt, Malware-Scans initiiert, die Isolierung entfernt und Hostcomputer isoliert, oder erstellen Sie mehrere Profile, jeweils mit eigener, einzelner Fähigkeit.

Prozedur

1. Navigieren zu **McAfee ePO-Integration** > **McAfee ePO-Fähigkeitsprofile**an.
   Die McAfee ePO Die Liste Fähigkeitsprofile wird angezeigt.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.



4. Klicken Sie auf, um das Profil zu speichern und zu validieren **Fahren Sie Fort** .
   Wenn die Validierung erfolgreich ist, werden die Seite und neu geladen **Konfiguration** Formular wird angezeigt.

Nächste Maßnahme

Der nächste Schritt besteht darin, Ihr Profil zu konfigurieren. Bevor Sie die Einstellungen für das Profil konfigurieren, sollten Sie die Konzepte für die Konfiguration von Profilen und Auslösebedingungen überprüfen. Siehe Richten Sie Ihr ein McAfee ePO Konsole, in die integriert werden soll Security Incident Response(SIR) und Definieren von Auslösebedingungen mit einem CI-Feld (Configuration Item), um weitere Informationen zu erhalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren von Auslösebedingungen mit einem CI-Feld (Configuration Item)

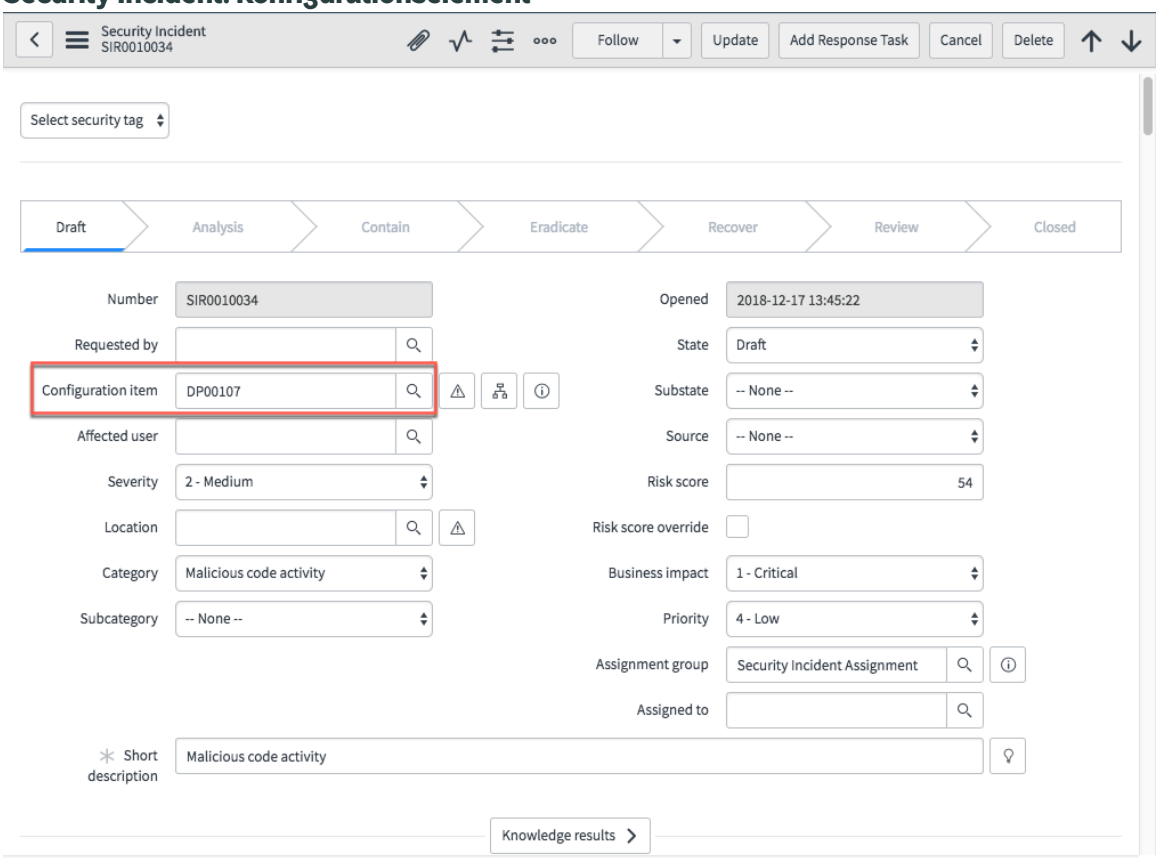
Nachdem Sie ein Profil erstellt und ausgewählt haben McAfee ePO Fähigkeiten, die das Profil ausführen soll, konfigurieren Sie die Einstellungen des Profils so, dass es nur ausgeführt wird, wenn eine Reihe bestimmter Bedingungen erfüllt sind.

Sie haben die Flexibilität, diese Auslösebedingungen festzulegen, damit das Profil automatisch basierend auf den Standardfeldwerten ausgeführt wird, die auf einem abgeglichen werden ServiceNow AI Platform® Security Incident Response Security Incident. Alternativ können Sie ein Profil so einrichten, dass es nach Übereinstimmungen für Feldwerte sucht, die Sie speziell im Security Incident identifizieren.

Einer der Schlüssel für die Funktionalität der Integration und die Funktionsweise eines Profils ist das Feld Konfigurationselement (CI) auf der ServiceNow AI Platform® Security Incident Response(SIR) Security Incident. Der Wert dieses Felds ist der Prinzipalwert für einen Security Incident. Dieser Wert wird verwendet, um die IDs Ihrer Assets mit den in gespeicherten Informationen abzugleichen ServiceNow AI Platform® Datenbank. Wenn ein SIR Security Incident wird durch ein Sicherheitsereignis erstellt, und ein Profil wird aktiviert. Ihre Assets werden basierend auf dem Wert des Felds Konfigurationselement nach einem übereinstimmenden Wert für einen vollqualifizierten Domänennamen (FQDN), einen Hostnamen oder eine IP-Adresse gescannt.

Im Idealfall wird in der Datenbank ein übereinstimmender Wert gefunden, und Daten können aus gesammelt werden McAfee ePO Konsole für das übereinstimmende Asset, abgerufen in Ihr ServiceNow AI Platform® Instanz und wird in den zugehörigen Listen eines Security Incidents angezeigt. Die folgende Abbildung zeigt ein Beispiel für das Feld Konfigurationselement, das mit einem Hostnamen auf einem ausgefüllt wird SIR Security Incident.

Security Incident: Konfigurationselement



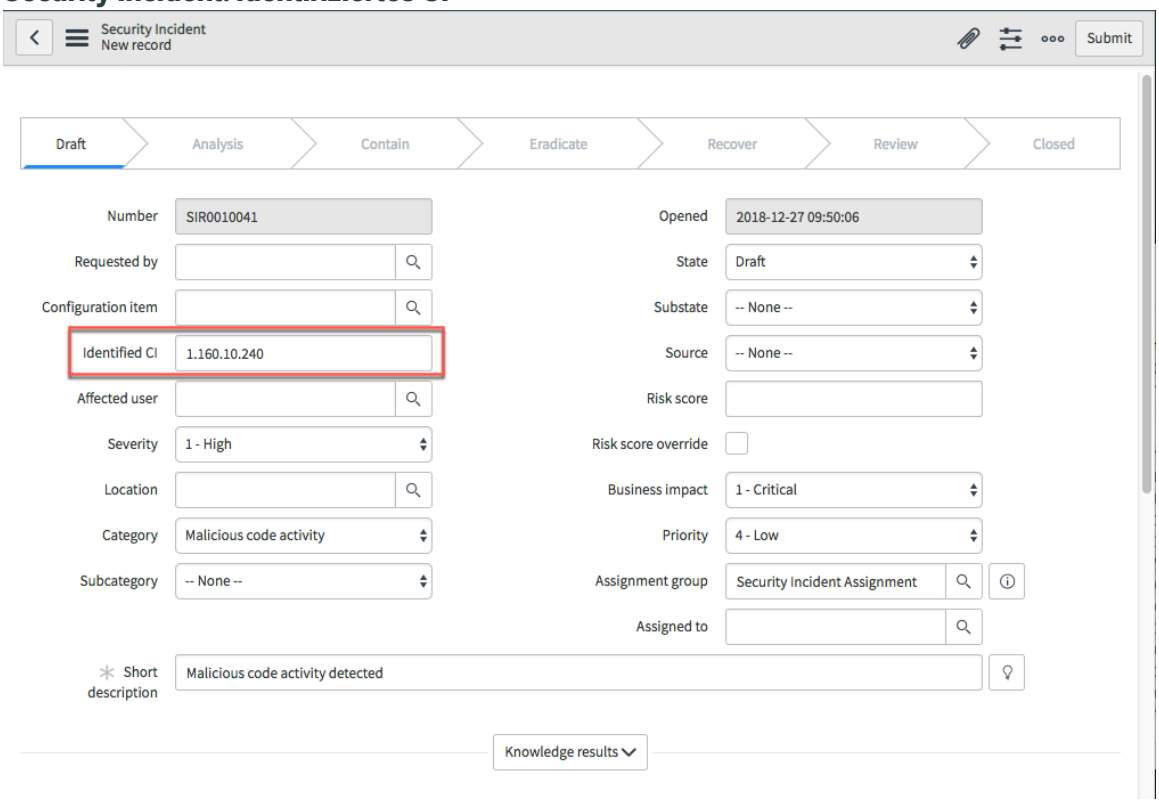
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Feld Configuration Item (CI) im Security Incident nicht ausgefüllt ist oder keine Übereinstimmung für einen FQDN, einen Hostnamen oder eine IP-Adresse gefunden werden kann, die der Datenbank entspricht, können Sie ein alternatives Feld im Security Incident auswählen, um alle übereinstimmenden CI-Ergänzungsdaten anzuzeigen, die während des Scans Ihrer Assets gefunden wurden.

Während des Konfigurationsschritts des Profils können Sie ein alternatives CI-Auslöserfeld für die Endpunktidentifizierung auswählen, um sicherzustellen, dass die CI-Ergänzungsdaten aus dem stammen McAfee ePO Die Suche wird für den zugehörigen Security Incident ausgefüllt. Sie können jedes Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich anwenderdefinierter Felder, die Sie erstellen. Indem Sie dieses alternative CI-Feld als Sicherung auswählen, stellen Sie sicher, dass Ihre Profile auch dann ausgeführt werden, wenn das CI-Feld bei der Incident-Erstellung nicht für den zugehörigen Security Incident ausgefüllt ist.

Als Analyst des Security Operations Center (SOC) erstellen Sie beispielsweise ein anwenderdefiniertes Feld für einen Security Incident mit der Bezeichnung IP-Adresse in meinem Security Incident. Wenn Sie nicht der Meinung sind, dass der Wert dieses anwenderdefinierten Felds bei der Incident-Erstellung im Feld Konfigurationselement im Security Incident angezeigt wird, können Sie das Profil so einrichten, dass es nach dieser IP-Adresse sucht. Bei Übereinstimmung wird die IP-Adresse im Feld Ihrer Wahl im Security Incident angezeigt. In der folgenden Abbildung ist Identifiziertes CI Das Feld ist als alternatives Feld für die IP-Adresse in diesem Beispiel ausgewählt.

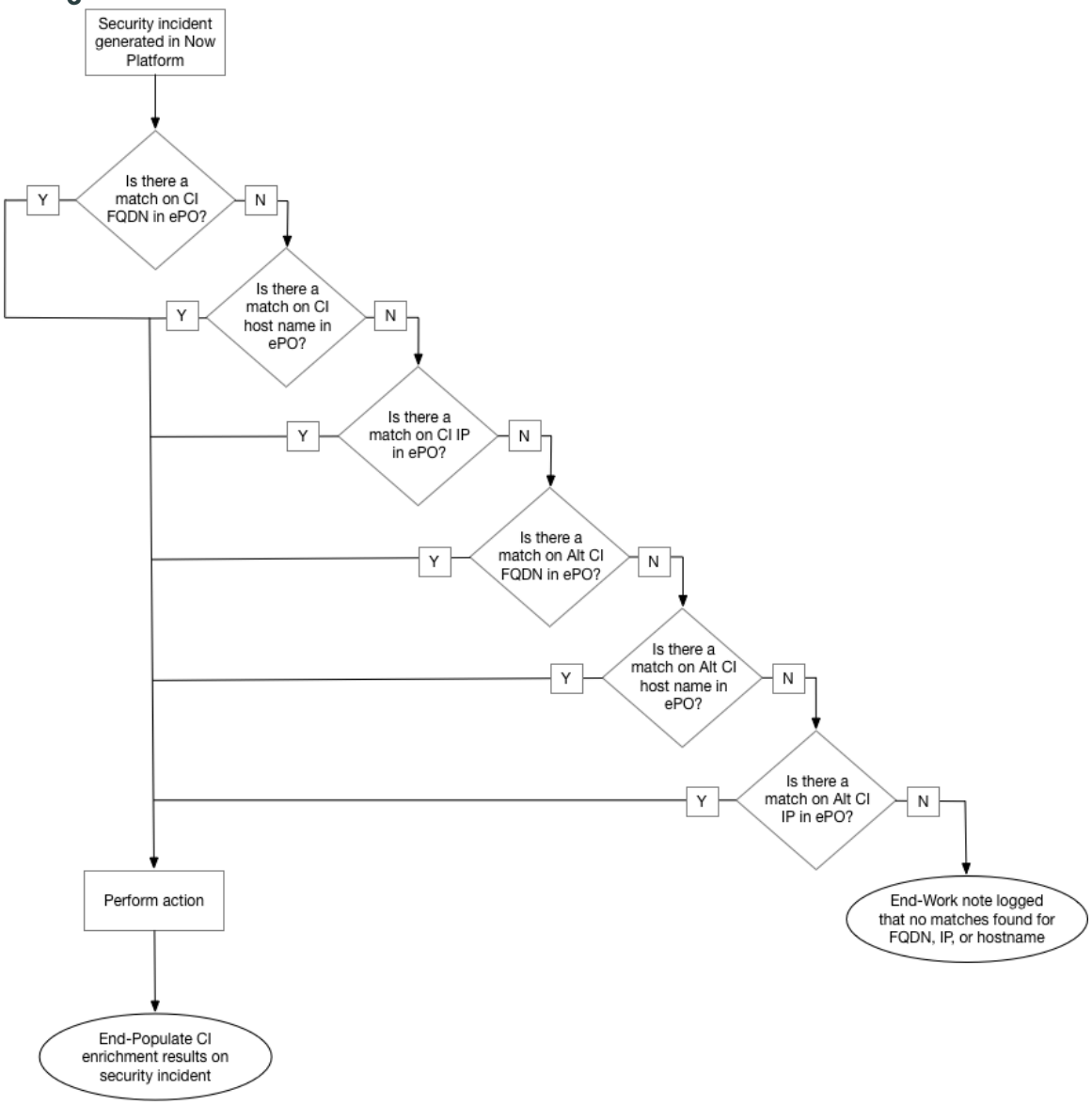
Security Incident: Identifiziertes CI



Die folgende Abbildung zeigt, wie die erste Suche des Workflows nach Übereinstimmungen für Konfigurationselemente scannt. Wenn das Feld Auslöser für alternatives CI aktiviert ist, scannt die zweite Suche nach Übereinstimmungen nach alternativen Werten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationselemente-Workflow



Wenn keine übereinstimmenden IDs für das CI-Feld oder das alternative CI-Feld gefunden werden, wird eine Arbeitsnotiz protokolliert, und eine Meldung wird im Security Incident angezeigt. Wenn keine Übereinstimmungen gefunden werden, werden keine Ergänzungsdaten für die Security Incidents im Zusammenhang mit dem Ereignis ausgefüllt.

Sie aktivieren das alternative CI-Auslöserfeld und wählen das Feld aus, in dem Sie die übereinstimmende ID während des Konfigurationsschritts für ein Profil anzeigen möchten. Dieser Schritt zum Aktivieren des Felds „alternatives CI“ wird zusammen mit den anderen Profilkonfigurationsanforderungen in beschrieben Einstellungen konfigurieren.

Einstellungen konfigurieren

Nachdem Sie ein Profil erstellt und ausgewählt haben McAfee ePO Fähigkeiten, die das Profil ausführen soll, konfigurieren Sie die Einstellungen so, dass das Profil nur unter den von Ihnen definierten spezifischen Bedingungen aufgerufen wird.

Konfigurieren eines Profils

In diesem Schritt konfigurieren Sie ein Fähigkeitsprofil so, dass es nur ausgeführt wird, wenn die von Ihnen angegebenen Bedingungen erfüllt sind. Sie definieren, welche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingungen für Security Incidents automatisch auslösen McAfee ePO Fähigkeiten, die Sie für das Profil ausgewählt haben. Sie haben auch die Möglichkeit, ein alternatives Eingabefeld für das Feld Configuration Item (CI) auszuwählen und Filterbedingungen festzulegen, damit nur die Security Incidents, die sich auf Ihr auslösendes Ereignis beziehen, das Profil automatisch starten. Der Konfigurationsschritt enthält die folgenden Einstellungen im Konfigurationsformular für das Profil.

Auslöserfeld für alternatives Konfigurationselement (CI)

In Fällen, in denen das Feld Configuration Item (CI) auf der angezeigt wird ServiceNow AI Platform® Security Incident Response(SIR) Security Incident ist nicht mit einem Wert ausgefüllt, oder in der Datenbank kann keine Übereinstimmung gefunden werden. Sie können ein alternatives Feld im Security Incident auswählen, um alle übereinstimmenden CI-Ergänzungsdaten anzuzeigen, die während des Scans Ihrer Assets gefunden wurden. Weitere Informationen zu den Feldern Konfigurationselement und Alternatives Konfigurationselement für einen Security Incident finden Sie unter Definieren von Auslösebedingungen mit einem CI-Feld (Configuration Item).

Sicherheits-Tags

Damit Sie den Status isolierter Hostcomputer nachverfolgen können und wann Malware-Scans initiiert werden, ist eine optionale Tagging-Funktion verfügbar. Standardmäßig ist diese Option im Konfigurationsformular für Profile deaktiviert. Wenn diese Option während des Konfigurationsschritts aktiviert ist, werden Sicherheits-Tag-Namen im Konfigurationsformular angezeigt. Dies sind die Namen der Tags, die in zugehörigen Security Incidents angezeigt werden. Diese Tags informieren Sie, wenn eine Host-Isolierungsaktion erfolgreich initiiert und genehmigt wurde. Nachdem ein Host erfolgreich an das Netzwerk zurückgegeben wurde, wird das Sicherheits-Tag automatisch aus dem Security Incident entfernt. Bei Malware-Scans wird im zugehörigen Security Incident ein Tag angezeigt, wenn ein Scan geplant wird. Nach Abschluss des Scans wird das geplante Tag automatisch durch ein Tag ersetzt, das angibt, dass der Scan erfolgreich abgeschlossen wurde.

Automatischer Auslöser basierend auf Incident

Wenn die Option Automatischer Auslöser basierend auf Incident aktiviert ist, ist der Filterbedingungsgenerator verfügbar, und Sie müssen Filterbedingungen festlegen, die angeben, wann das Profil automatisch ausgeführt wird. Ein allgemeiner Filter ist Kategorie ist schädliche Codeaktivität ™Und Geschäftsauswirkung ist 1 – Kritisch ™. Mit diesen Filtern starten nur Security Incidents, die sich auf schädlichen Code beziehen und kritische Geschäftsauswirkungen haben, das Profil. Die Verwendung der Option „Automatischer Auslöser“ kann die Anzahl der Security Incidents reduzieren, die das Profil automatisch aufrufen.

Genehmigungen

Wenn Ihre Organisation ein zusätzliches Maß an Kontrolle über Aktionen wie das Isolieren von Hostcomputern und das Initiieren von Malware-Scans wünscht, können Sie die Option Genehmigung anfordern während des Konfigurationsschritts für ein Profil aktivieren.

Wenn beispielsweise sowohl die Genehmigungs- als auch die Tagging-Funktionen für ein Profil aktiviert sind, wird der zugehörige Security Incident automatisch mit dem Tag versehen, dass die Aktion initiiert wird, nachdem eine Anforderung zum Isolieren eines Hostcomputers oder zur Rückgabe an das Netzwerk zur Genehmigung übermittelt wurde. Anforderungen werden standardmäßig zur Genehmigung an einen Anwender mit der Rolle „sn_si.admin“ gesendet. Diese Genehmigung kann jedoch einer anderen Person oder einer Genehmigungsgruppe entsprechend den Anforderungen Ihrer Organisation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugewiesen werden. Genehmiger verarbeiten Anforderungen in **Meine Genehmigungen** In ihren ServiceNow AI Platform® Instanzen. Sicherheits-Tags werden für zugehörige Security Incidents angezeigt. Alle Workflow-Aktivitäten werden auch in Arbeitsnotizen protokolliert, um einen Audit-Pfad zu erstellen.

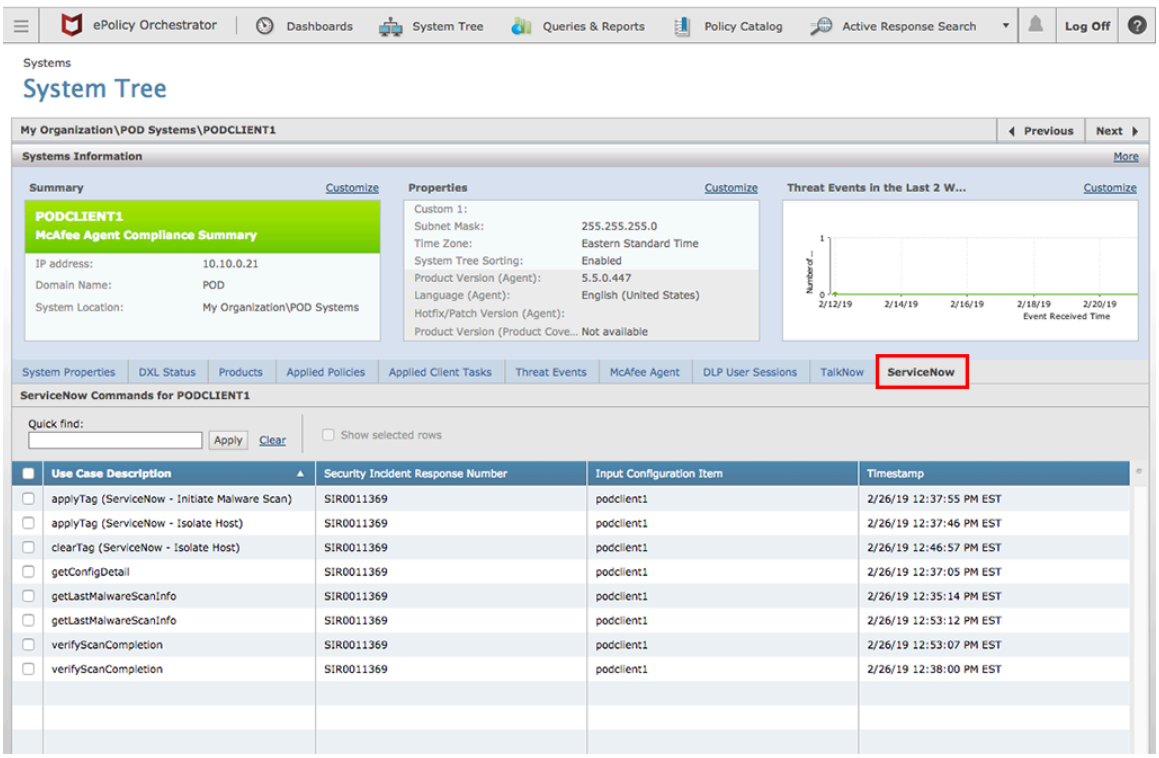
ServiceNow Audit-Protokoll in McAfee ePO Konsole

In Version 5.10.0 von McAfee ePO, A ServiceNow Die Registerkarte wird mit einem Protokoll von Befehlen angezeigt, die von Ihrem initiiert werden ServiceNow AI Platform® Instanz. Nachdem eine Aktion oder Abfrage über ein Profil in aufgerufen wurde ServiceNow AI Platform® Instanz auf einem Hostcomputer (Endpunkt) in McAfee ePO Konsole, ein Audit-Protokoll von ServiceNow Befehle werden in erstellt McAfee ePO Konsole. Dieses Protokoll wird in der Systemstruktur in angezeigt McAfee ePO Konsole und hilft Ihnen, die Zeiten der Befehle zu auditieren, die an bestimmte Endpunkte gesendet werden. Zum Anzeigen protokollierter Elemente ServiceNow Ereignisse auf bestimmten Computern in einem McAfee ePO-Konsole führen Sie die folgenden Schritte aus.

1. Navigieren Sie zur Systemstruktur in McAfee ePO-Konsole und suchen Sie ServiceNow Registerkarte.
2. Klicken Sie auf die Registerkarte, um eine Liste der Hostcomputer zu öffnen.
3. Klicken Sie in der Spalte Name auf einen Hostnamen, um das Audit-Protokoll zu öffnen.

In der folgenden Abbildung ein Beispiel für ein Protokoll für einen Host (PODCLIENT1) Wird angezeigt.

PODClient



Die Ereignisse, die über die Profile in Ihrem initiiert wurden ServiceNow AI Platform® Instanzen werden aufgezeichnet und im Protokoll angezeigt. Überprüfen Sie, indem Sie den Status des Hostcomputers überprüfen, ob die im Protokoll aufgeführten Ereignisse auf dem Host erfolgreich abgeschlossen wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielprofile

Die folgenden Themen enthalten Beispiele für die Konfiguration von Profilen und das Testen von Security Incidents. Diese Beispiele umfassen Profile für alle McAfee ePO Fähigkeiten, die für diese Integration verfügbar sind.

Konfigurieren Sie Profile und Security Incidents für Systemanreicherungsabfragen

Konfigurieren Sie Ihre Profileinstellungen so, dass das Profil nur unter den von Ihnen festgelegten Bedingungen ausgelöst wird.

Vorbereitungen

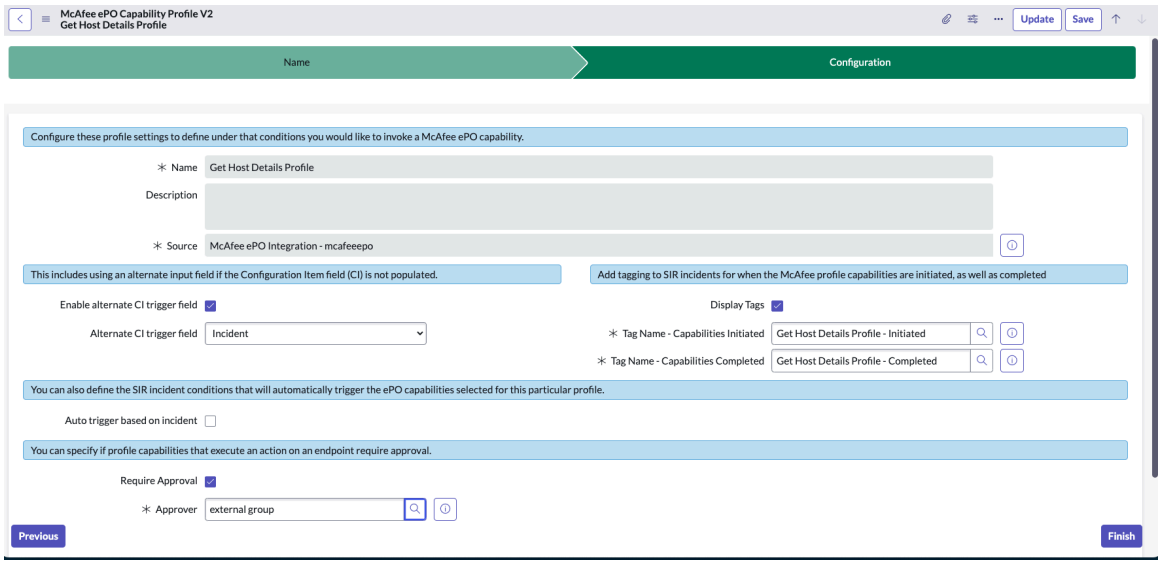
Erforderliche Rolle: ServiceNow AI Platform® Security Incident-Administrator (sn_si.admin)

Warum und wann dieser Vorgang ausgeführt wird

Definieren Sie die Bedingungen, die automatisch auslösen McAfee ePO Fähigkeiten, die Sie für das Profil ausgewählt haben. Sie können auch ein alternatives Eingabefeld für das Feld Configuration Item (CI) auswählen. In diesem alternativen Feld können Sie Filterbedingungen festlegen, damit nur die Security Incidents, die sich auf Ihr auslösendes Ereignis beziehen, das Profil automatisch auslösen.

Prozedur

1. Wenn die Konfigurationsseite nicht angezeigt wird, klicken Sie auf **Konfiguration** Auf der Fortschrittsleiste.
2. Füllen Sie die Felder im Formular aus



3. Um die Option „alternatives CI-Feld“ zu aktivieren und die Filterbedingungen festzulegen, die dieses Profil automatisch aufrufen, führen Sie die folgenden Schritte aus.

   a. Wählen Sie aus **Aktivieren Sie das alternative CI-Auslöserfeld** Kontrollkästchen.
   Das Feld alternativer CI-Auslöser wird angezeigt. In diesem Beispiel glauben Sie als Anwender mit der Rolle „sn_si.admin“, dass das CI-Feld bei der Incident-Erstellung nicht im Security Incident ausgefüllt wird. Alternativ denken Sie, dass CI-Informationen für einen FQDN, einen Hostnamen oder eine IP-Adresse in ausgefüllt werden Identifiziertes CI Feld im Security Incident, und Sie wählen das Feld „identifiziertes CI“ als Alternative aus. Das identifizierte CI ist für dieses Beispiel ausgewählt, Sie können jedoch jedes Feld im Security Incident für das alternative CI verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Von **Alternativer CI-Auslöser** Feldauswahlliste, die angezeigt wird, wählen Sie aus **Identifiziertes CI** Feld.

Alle verfügbaren Felder im Security Incident werden in der Liste angezeigt, einschließlich aller anwenderdefinierten Felder. Im Feld alternativer CI-Auslöser Identifiziertes CI Wird angezeigt.

Wenn dieses Profil aufgerufen wird und das CI-Feld beim ersten Ereignisauslöser nicht im zugehörigen Security Incident ausgefüllt wird, verwendet das Profil alternativ den Wert aus dem Feld „identifiziertes CI“ in der Suche.

c. Wählen Sie aus **Automatischer Auslöser basierend auf Incident** Kontrollkästchen.
Der Generator für Filterbedingungen wird angezeigt. Legen Sie mit dieser Option Filterbedingungen fest, und geben Sie an, wann das Profil bei der Erstellung eines Security Incidents automatisch aufgerufen wird.

d. Definieren Sie die SIR-Incident-Bedingungen, die automatisch die für dieses bestimmte Profil ausgewählten ePO-Fähigkeiten auslösen.

e. Wenn die Profilfunktionen, die eine Aktion für einen Endpunkt ausführen, eine Genehmigung erfordern, wählen Sie aus **Genehmigung Erforderlich** Kontrollkästchen.

f. Wählen Sie über das Suchsymbol eine Genehmigung aus.

4. Klicken Sie auf **Fertigstellen**.
Sie haben das Profil erfolgreich so konfiguriert, dass es bei der Incident-Erstellung automatisch ausgelöst wird und ein alternatives Feld zum Ausfüllen übereinstimmender CI-Ergebnisse verwendet wird.

Konfigurieren Sie ein Profil, um einen Malware-Scan zu initiieren

Nachdem Sie ein Profil mit der Funktion „Malware-Scan initiieren“ und anderen erstellt haben McAfee ePO Fähigkeiten, die das Profil ausführen soll, konfigurieren Sie die Einstellungen des Profils so, dass es unter den von Ihnen definierten spezifischen Bedingungen aufgerufen wird.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

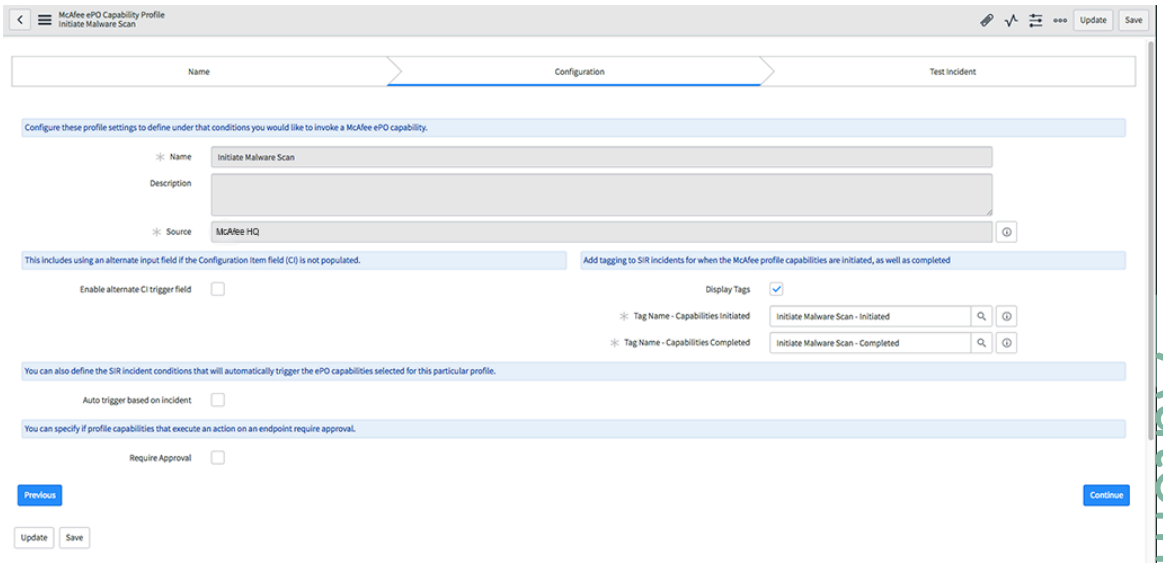
Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie als Anwender mit der Rolle „sn_si.admin“ das Profil so, dass ein Scan nur geplant wird, wenn die von Ihnen angegebenen Bedingungen erfüllt sind ServiceNow AI Platform Security Incident Response(SIR) Security Incidents. Sie definieren, welche Bedingungen für Security Incidents den Scan auslösen. Alle anderen McAfee ePO Fähigkeiten, die Sie für das Profil auswählen, teilen die auslösenden Bedingungen. Die Optionen zum Auswählen eines alternativen Eingabefelds für das Feld Configuration Item (CI) und zum Festlegen von Filterbedingungen sind verfügbar. Möglicherweise ziehen Sie es vor, die Filterung so festzulegen, dass nur diese Filter vorhanden sind SIR Security Incidents, die sich auf Ihr auslösendes Ereignis beziehen, rufen das Profil automatisch auf.

Wie bei der Aktion „Host isolieren“ können Sie einen Scan bei Bedarf direkt von starten SIR Security Incident. Weitere Informationen zum manuellen Starten eines Scans finden Sie unter Auslöser McAfee ePO Profil manuell aus einem Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn die Konfigurationsseite nicht angezeigt wird, klicken Sie auf **Konfiguration** Auf der Fortschrittsleiste.



   Das Formular Konfiguration wird angezeigt.

2. Füllen Sie das Formular aus.

   In diesem Beispiel sind die Genehmigungs- und Tagging-Optionen für das Profil aktiviert. Weitere Informationen zum Konfigurieren von finden Sie Aktivieren Sie das alternative CI-Auslöserfeld Und Automatischer Auslöser basierend auf Incident Optionen, siehe Konfigurieren Sie Profile und Security Incidents für Systemanreicherungsabfragen.

3. Wählen Sie eine Option aus, um fortzufahren.
   Sie haben das Profil erfolgreich konfiguriert, sodass bei der Incident-Erstellung automatisch ein Malware-Scan ausgelöst wird. Ein alternatives CI-Feld wird verwendet, um übereinstimmende CI-Ergebnisse aus dem Scan auszufüllen. Der nächste Schritt besteht in der Vorschau und dem Testen von Security Incidents für dieses Profil.

Auslöser McAfee ePO Profil manuell aus einem Security Incident

Lösen Sie ein Fähigkeitsprofil manuell aus einem aus ServiceNow AI Platform Security Incident Response(SIR) Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Hinweis:
Die Option „Genehmigungen“ in Einstellungen konfigurieren Wird nur für die Funktionen „Host isolieren“ und „Host-Isolierung entfernen“ angezeigt.

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Anforderung zum Abrufen von Hostdetails, zum Isolieren des Hostcomputers oder zum Entfernen der Isolierung eines Computers automatisch aufrufen, wenn die Auslöserbedingungen, die Sie im Profil angeben, den Bedingungen für Security Incidents entsprechen. Wenn Sie eine Anforderung alternativ manuell übermitteln möchten, senden Sie die Anforderung direkt aus einem Security Incident.

Automatische Übersetzung

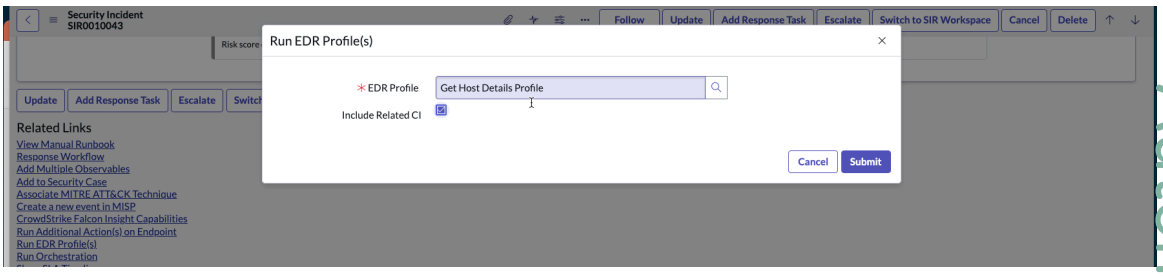
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sobald Sie das Profil basierend auf den konfigurierten Auslöserbedingungen aktiviert haben, können Sie die Abfrageergebnisse in anzeigen ServiceNow AI Platform Security Incidents. McAfee ePO Mit Integrationen können Sie auch einzelne Fähigkeiten für Konfigurationselemente (Configuration Items, CIs) ausführen, ohne ein Profil zu verwenden.

Prozedur

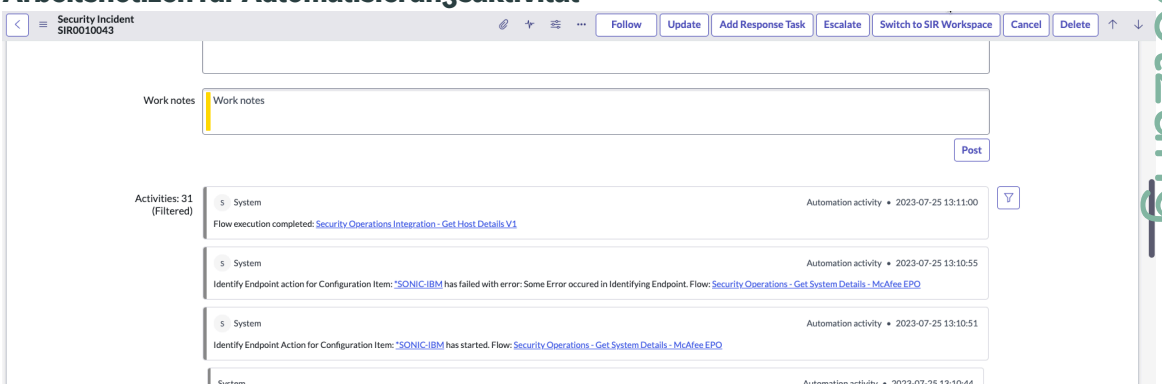
1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit überprüfen möchten McAfee ePO Informationen.
3. Wählen Sie im Abschnitt zugehörige Listen die Option aus **EDR-Profil(e) ausführen** .

McAfee – EDR-Profil ausführen



4. Durchsuchen und wählen Sie ein Profil aus der Liste der verfügbaren Profile aus.
   Die Liste der verfügbaren Profile ist „Hostdetails abrufen“, „Hostcomputer isolieren“ und „Isolierung entfernen“. Wählen Sie beispielsweise Hostdetails abrufen aus.
5. Wählen Sie Aus **Zugehöriges CI einschließen** Um dieses Profil für alle zugehörigen CIs des Profils auszuführen.
   Wenn dem Security Incident beispielsweise fünf CIs zugeordnet sind, wird das ausgewählte Profil für alle fünf CIs ausgeführt.
6. Klicken Sie auf **Absenden**.
   Das ausgewählte Profil wird manuell ausgelöst. Sie können den Abschnitt „Arbeitsnotizen und Aktivitäten“ sowie die Tags „Profil initiiert“ und „Profil abgeschlossen“ im Abschnitt „Arbeitsnotizen“ überprüfen.

Arbeitsnotizen für Automatisierungsaktivität

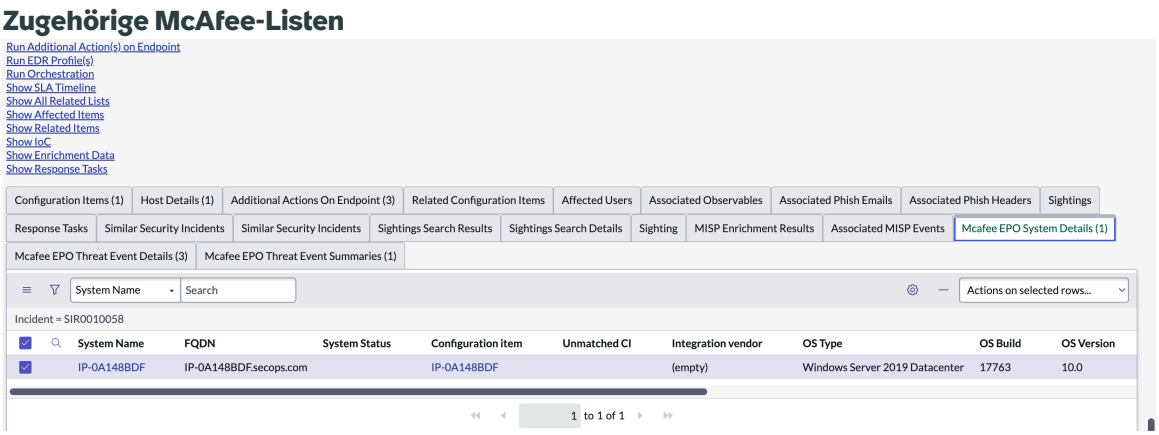


Die Ergebnisse werden in Form von zugehörigen Listen angezeigt, z. B. Hostdetails abrufen, Hostcomputer isolieren oder Isolierung entfernen.

Hinweis:
Alle zugehörigen Listentabellen erweitern die Basistabellen. In diesem Beispiel ist die McAfee EPO-Systemdetails eine erweiterte Tabelle der Basistabelle „Hostdetails“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Führen Sie die folgenden Schritte aus, um einzelne Fähigkeiten für ein Konfigurationselement (Configuration Item, CI) auszuführen:

   a. Wählen Sie in der zugehörigen Liste Konfigurationselemente das erforderliche CI aus.

   b. Klicken Sie auf **Aktionen für ausgewählte Zeilen...** Dropdown-Liste, und wählen Sie die erforderliche Fähigkeit aus, die Sie für das ausgewählte CI ausführen möchten.
   Beispiel: Host isolieren.

   c. Klicken Sie Auf **Host Isolieren** Um sie für das ausgewählte CI auszuführen.
   Das ausgewählte CI wird vom Netzwerk isoliert.

Lösen Sie zusätzliche Aktionen in aus McAfee ePO Integration

Die Funktionen Bedrohungsereignisse auflisten und Malware-Scan initiieren können über zusätzliche Aktionen ausführen ausgelöst werden.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können zusätzliche Aktionen in konfigurieren und auslösen McAfee ePO Integration ermöglicht durch **Führen Sie zusätzliche Aktionen für Endpunkt aus** , Die enthalten McAfee ePO Listen Sie Bedrohungsereignisse und auf McAfee ePO Initiieren Sie Malware-Scan-Fähigkeiten.

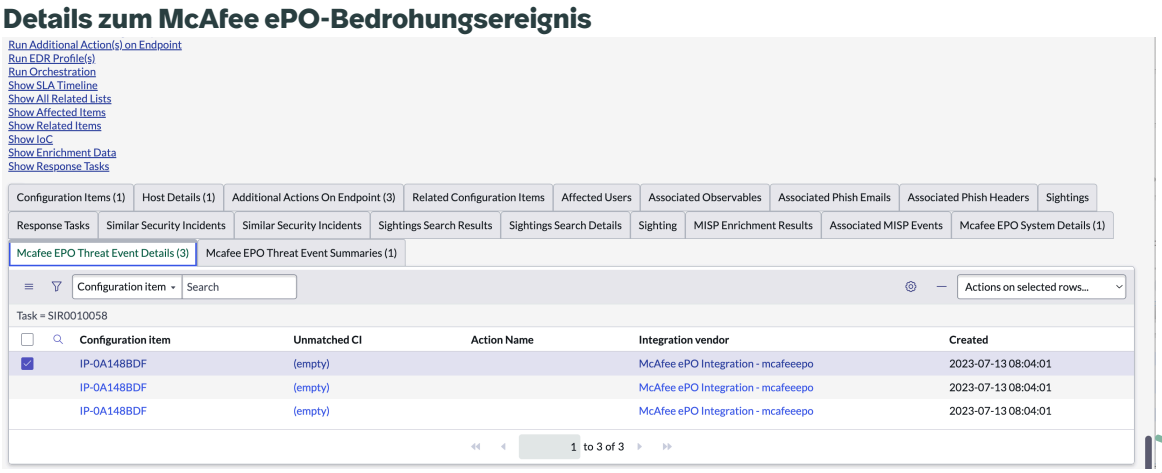
Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, für den Sie die zusätzlichen Aktionen ausführen möchten.
3. Klicken Sie im Abschnitt zugehörige Links auf **Zusätzliche Aktion(en) für Endpunkt ausführen** .
4. Durchsuchen Sie die Fähigkeitsimplementierung, die Sie auslösen möchten, und wählen Sie sie aus der Liste der zusätzlichen Aktionen aus.
   Beispiel: McAfee ePO Listen Sie Bedrohungsereignisse Auf.
5. Wählen Sie Aus **Zugehöriges CI einschließen** Um diese zusätzliche Aktion für alle zugehörigen CIs des Profils auszuführen.
   Wenn dem Security Incident beispielsweise fünf CIs zugeordnet sind, wird das ausgewählte Profil für alle fünf CIs ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie Auf **Führen Sie Zusätzliche Aktionen Aus** .



Hinweis:
Alle zugehörigen Listentabellen erweitern die Basistabellen. In diesem Beispiel ist die Tabelle „Details zu McAfee EPO-Bedrohungsereignissen“ eine erweiterte Tabelle der Basistabelle „zusätzliche Aktionen für Endpunkt“.

7. Zeigen Sie die McAfee ePO-Bedrohungsereignisdetails in den zugehörigen Listen an, und validieren Sie sie.

Verwenden McAfee ePO Integration in Analysten-Arbeitsbereich

Verwenden Sie McAfee ePO Integration zur Nutzung von McAfee ePO Fähigkeiten im SIR Analyst-Arbeitsbereich.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Bevor Sie verwenden McAfee ePO Integration im Security Incident Response-Arbeitsbereich müssen Sie sie aus herunterladen ServiceNow Store Und konfigurieren Sie es. Weitere Informationen finden Sie unter Richten Sie Ihr ein ServiceNow AI Platform Instanz für McAfee ePO Integration.

Warum und wann dieser Vorgang ausgeführt wird

Sie können verwenden McAfee ePO Integration, um Korrekturaktionen für die Endpunkte in Echtzeit durchzuführen, mithilfe von Profilen Details zum Host zu erfassen und mithilfe von bestimmte Abfragen oder Aktionen für den Endpunkt durchzuführen Security Incident Response Arbeitsbereich.

Die McAfee ePO Durch die Integration können Analysten Folgendes verwenden McAfee ePO-Fähigkeiten in Security Incident Response Arbeitsbereich für Analysten:

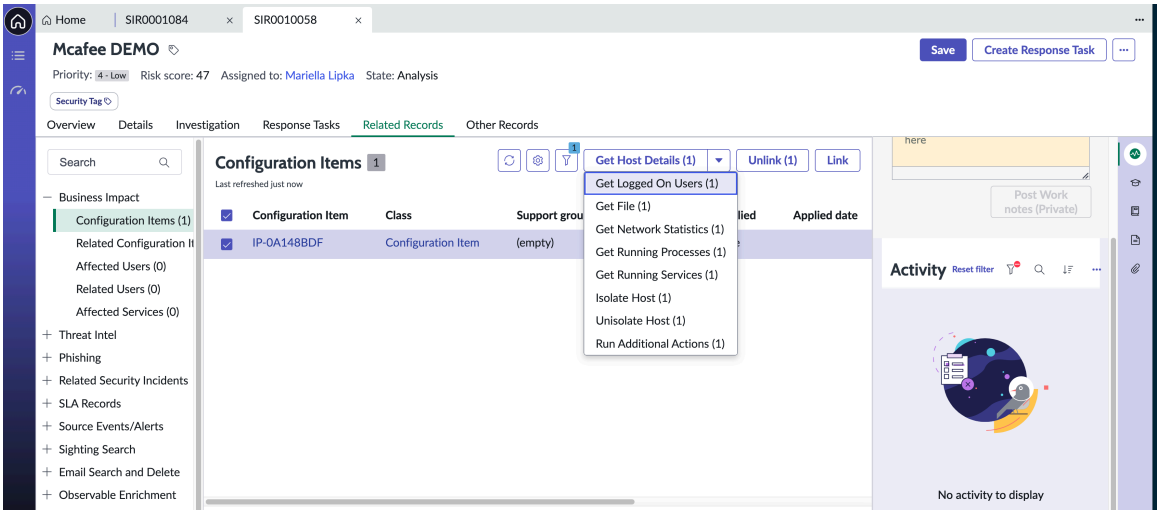
- **Hostdetails abrufen**
- **Host isolieren**
- **Isolation entfernen**
- **Zusätzliche Aktion(en) für Endpunkt ausführen**

Automatische Übersetzung

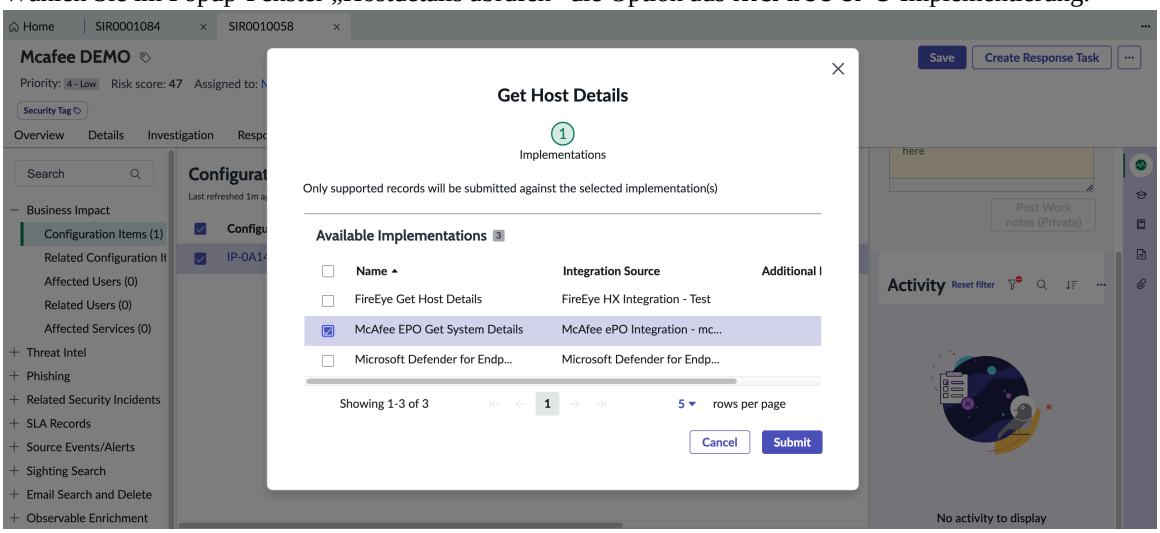
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie auf, um den Security Incident im SIR-Arbeitsbereich zu öffnen **Wechseln Sie zum SIR-Arbeitsbereich** Für den Security Incident.
2. Wählen Sie im SIR-Arbeitsbereich die aus **Zugehörige Datensätze** Registerkarte.
3. Wählen Sie beliebig aus **Konfigurationselement** , Und wählen Sie eine McAfee ePO-Fähigkeit aus, die in der Dropdown-Aktion zugehörige Liste ausgelöst werden soll.
   Beispiel: Hostdetails abrufen.



4. Wählen Sie im Popup-Fenster „Hostdetails abrufen“ die Option aus **McAfee ePO** Implementierung.

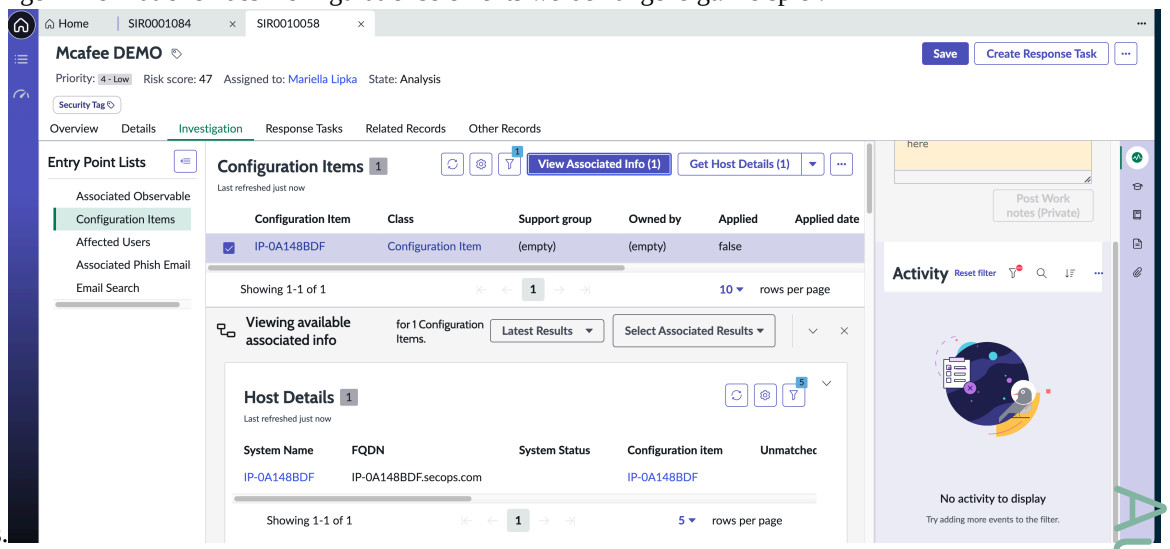


5. Klicken Sie auf **Absenden**.
   Die Fähigkeit „Hostdetails abrufen“ wird für das CI aufgerufen. Sie können die Arbeitsnotizen für die Ergebnisse und Ergebnisse anzeigen.
6. Um die Daten für die ausgelöste Fähigkeit anzuzeigen, wählen Sie aus **Untersuchung** Registerkarte.
7. Wählen Sie aus **Konfigurationselement** , Und klicken Sie auf **Zeigen Sie Zugehörige Informationen An** Aktion.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die zugehörigen Informationen des Konfigurationselements werden angezeigt. Beispiel:



Hostdetails.

8. Klicken Sie auf **Konfigurationselement** Zum Anzeigen der Hostdetails.
   Ebenso können Sie die andere McAfee ePO-Fähigkeit für Ihre Security Incidents im SIR Analyst Workspace verwenden.
9. Sie können die McAfee ePO-Fähigkeiten auf verwenden **Endpunkterkennung und -Antwort (EDR)** Zugehörige Liste für Analyse.
10. Durchsuchen und wählen Sie ein Profil aus der Liste der verfügbaren Profile aus.
    Die Liste der verfügbaren Profile ist „Hostdetails abrufen“, „Hostcomputer isolieren“ und „Isolierung entfernen“. Wählen Sie beispielsweise Hostdetails abrufen aus.
11. Wählen Sie aus **McAfee ePO** Implementierung, und klicken Sie auf **Übermitteln** .

Testen Sie Security Incidents, um Malware-Scans zu initiieren

Nachdem Sie ein Profil für den Malware-Scan konfiguriert haben, testen Sie das Profil, und zeigen Sie die Security Incidents an, die den Einstellungen Ihres Profils entsprechen. Zeigen Sie eine Vorschau der Scan-Ergebnisse in den zugehörigen Listen von an ServiceNow AI Platform Security Incident Response(SIR) Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

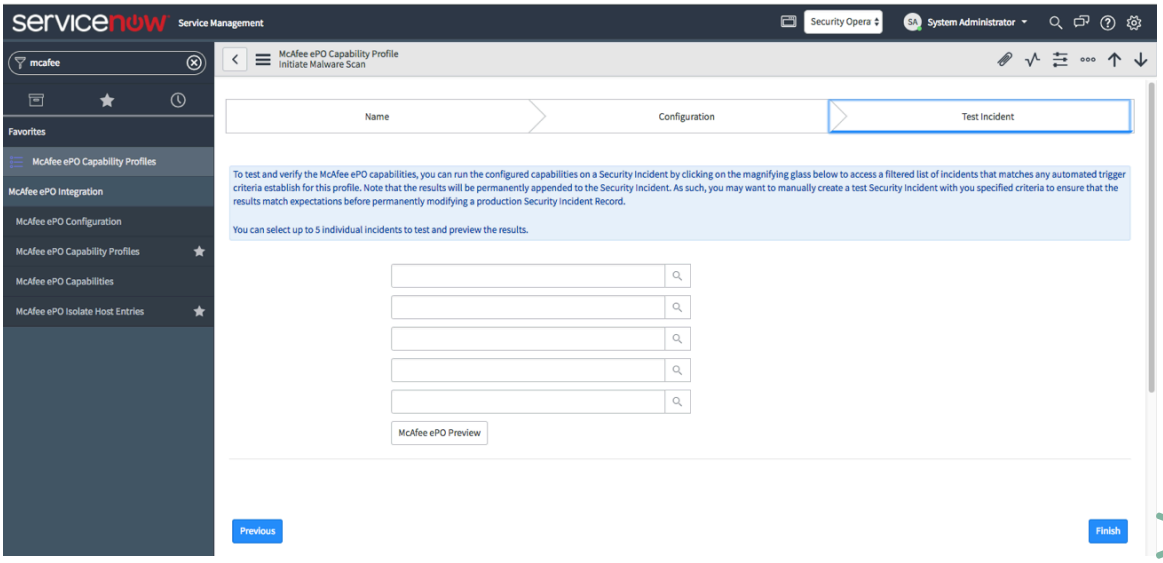
Stellen Sie als Anwender mit der Rolle „sn_si.admin“ sicher, dass das Profil mit der Malware-Scan-Funktion aufgerufen wird und dass die Scan-Suchergebnisse mit den erwarteten Ergebnissen einer Vorschau der zugehörigen Listen auf übereinstimmen ServiceNow AI Platform Security Incident Response(SIR) Security Incident. Mit der Vorschau können Sie überprüfen, ob Scanergebnisse wie erwartet für das Profil zurückgegeben werden.

Prozedur

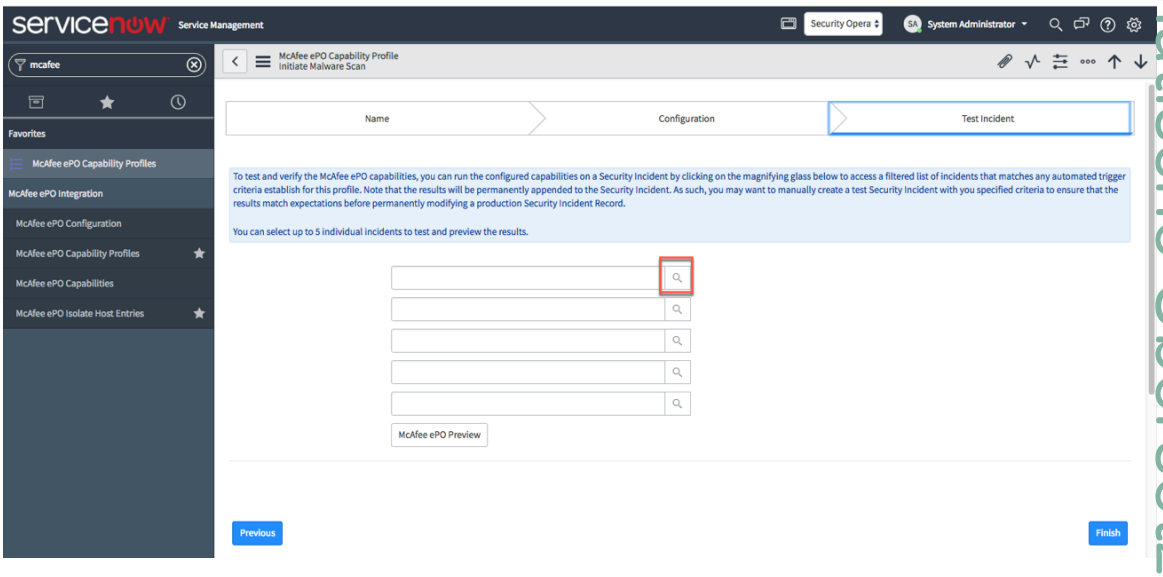
1. Wenn die Seite Incident testen nicht angezeigt wird, klicken Sie auf **Test-Incident** In der Fortschrittsleiste.
   Die Seite Test Incident wird für Ihr Profil angezeigt. In diesem Beispiel wird das Profil „Malware-Scan initiieren“ angezeigt, das Sie in den vorherigen Abschnitten erstellt und konfiguriert haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Klicken Sie rechts neben dem oberen Feld auf das Suchsymbol, um einen Security Incident auszuwählen, der in der Vorschau angezeigt werden soll.

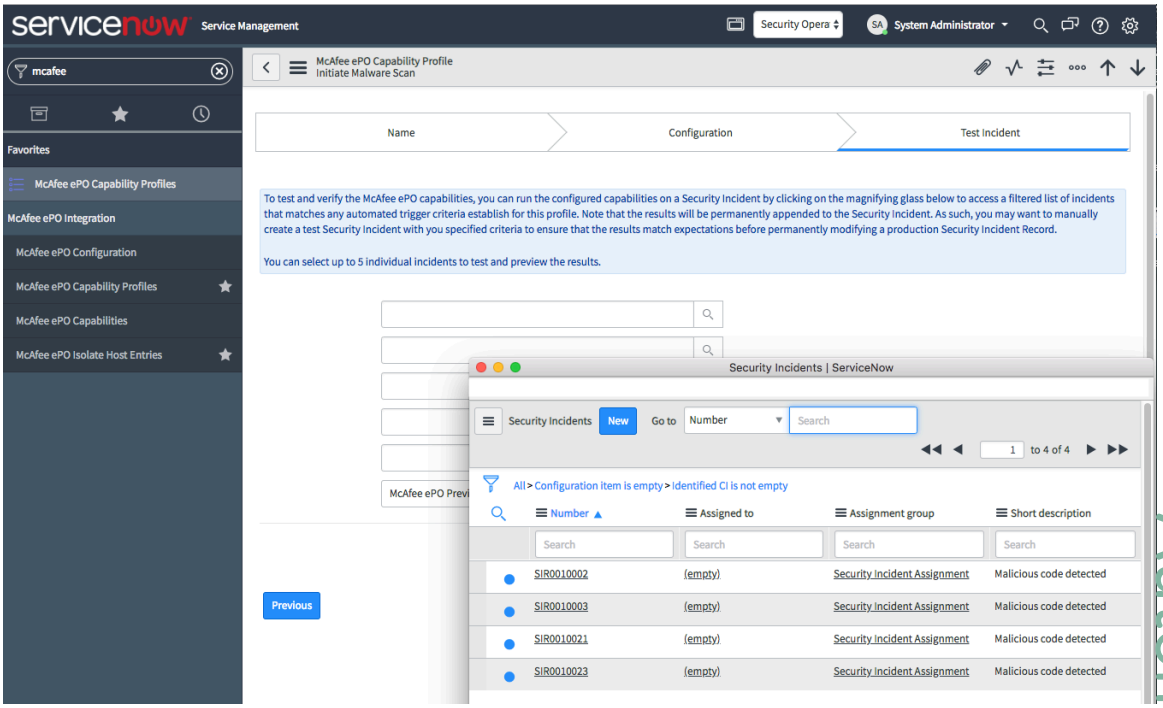


Es werden nur Security Incidents angezeigt, die den Profilkriterien entsprechen.

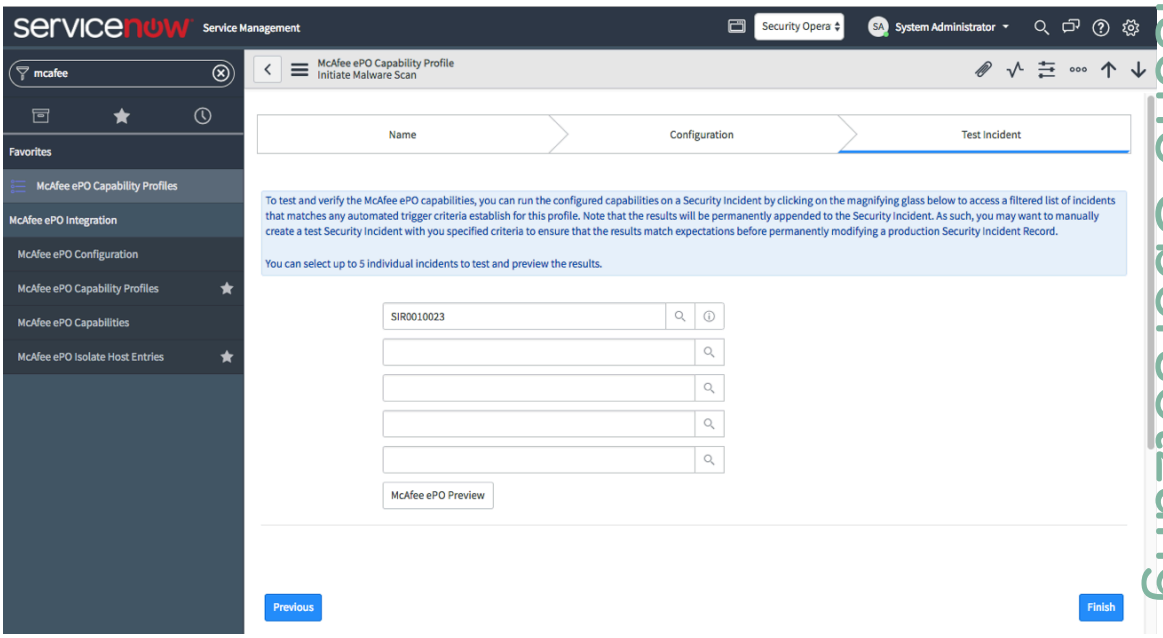
3. Wählen Sie in der Spalte Nummer der angezeigten Liste ein Element aus, das Sie in der Vorschau anzeigen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



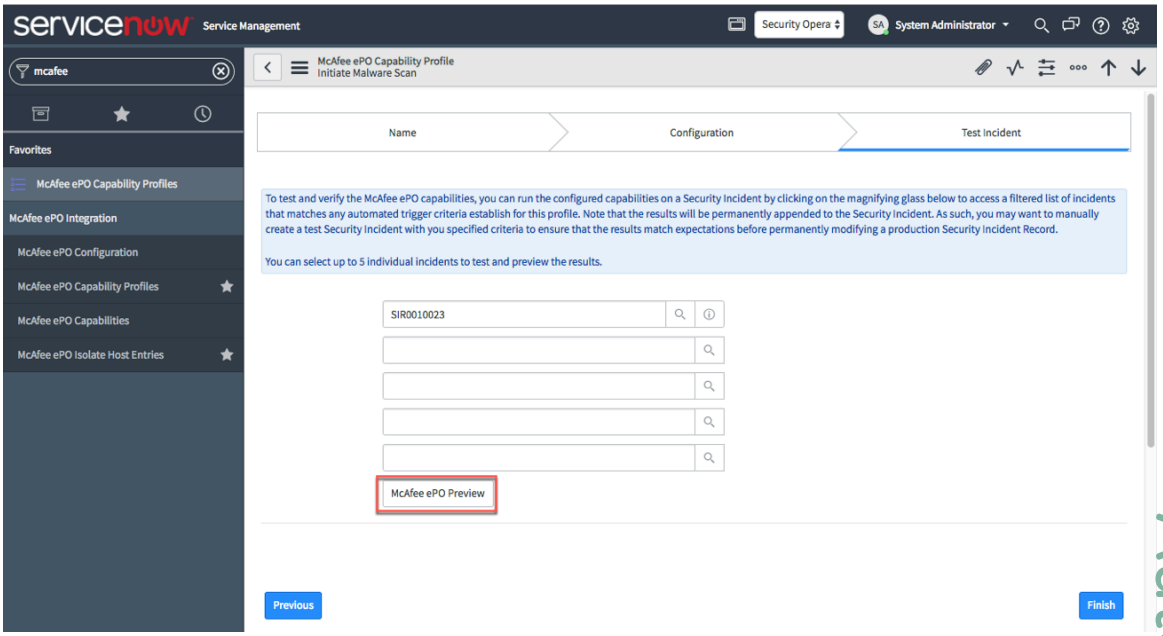
Die Nummer des Security Incidents wird im Feld angezeigt.



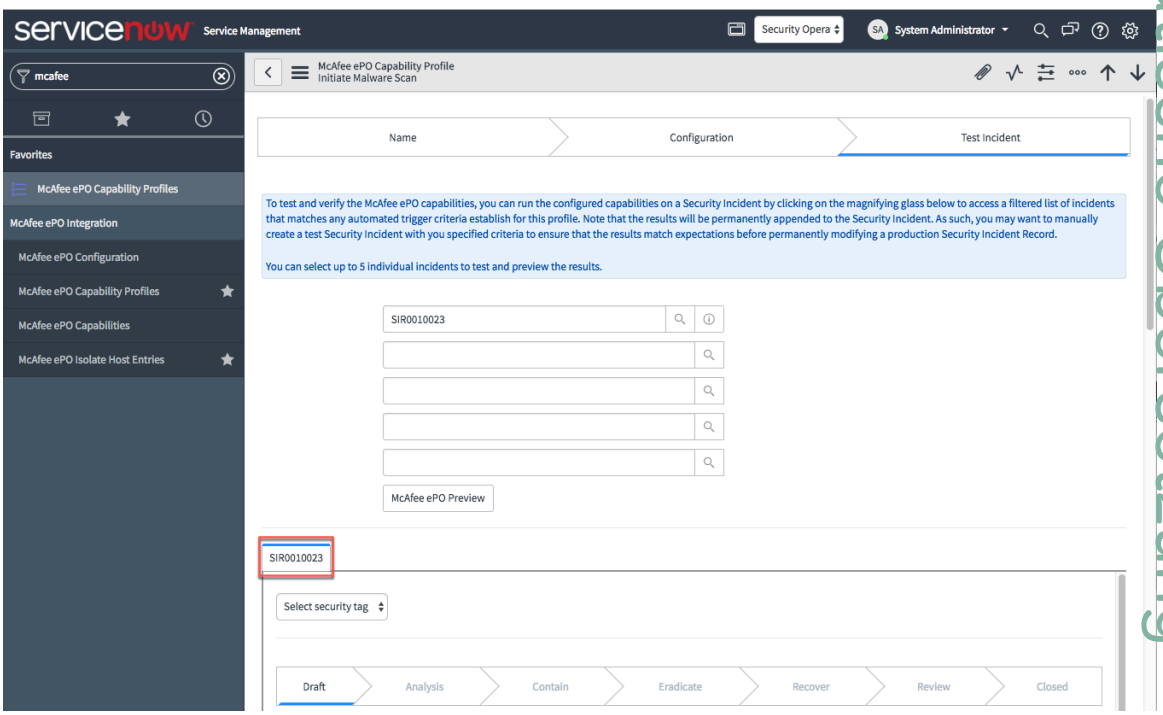
4. Wiederholen Sie die Schritte 2 und 3, bis alle Incidents, die Sie in der Vorschau anzeigen möchten, in den Feldern angezeigt werden.
   Wählen Sie bis zu fünf Security Incidents für die Vorschau aus.
5. Klicken Sie Auf **McAfee ePO-Vorschau** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Security Incidents, die den Ereignisbedingungen Ihres Profils entsprechen, werden angezeigt. Nachdem die Seite geladen wurde, werden unten auf der Seite Registerkarten für jeden Security Incident angezeigt.

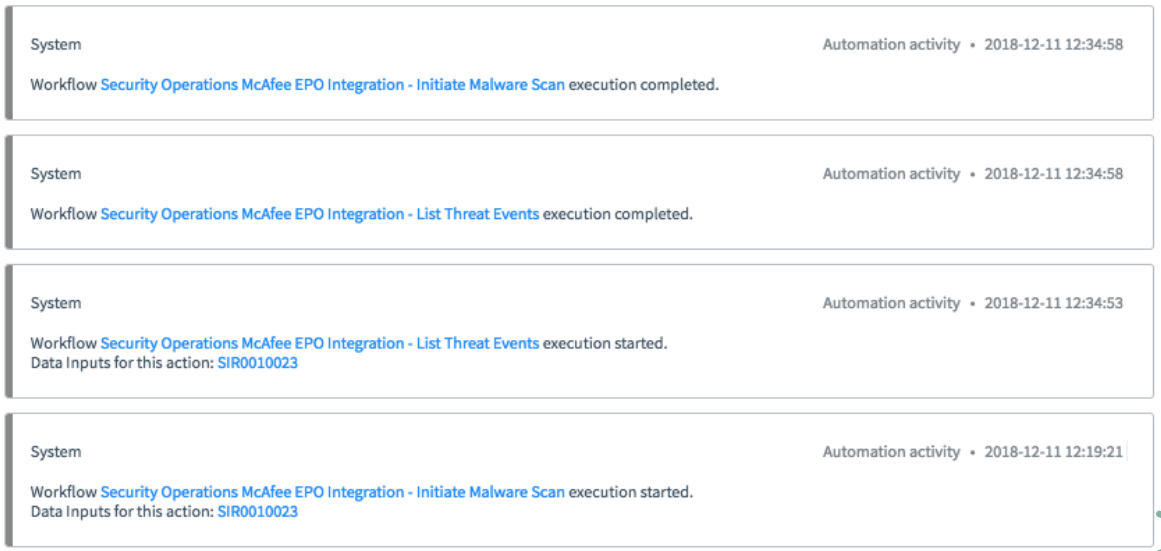


6. Scrollen Sie, um die Arbeitsnotizen anzuzeigen.

Hinweis:
Der Workflow „Bedrohungsereignisse auflisten“ ist Teil des Scans. Weitere Informationen zum Erstellen eines Profils mit der Malware-Scan-Funktion finden Sie unter Erstellen Sie ein Fähigkeitsprofil.

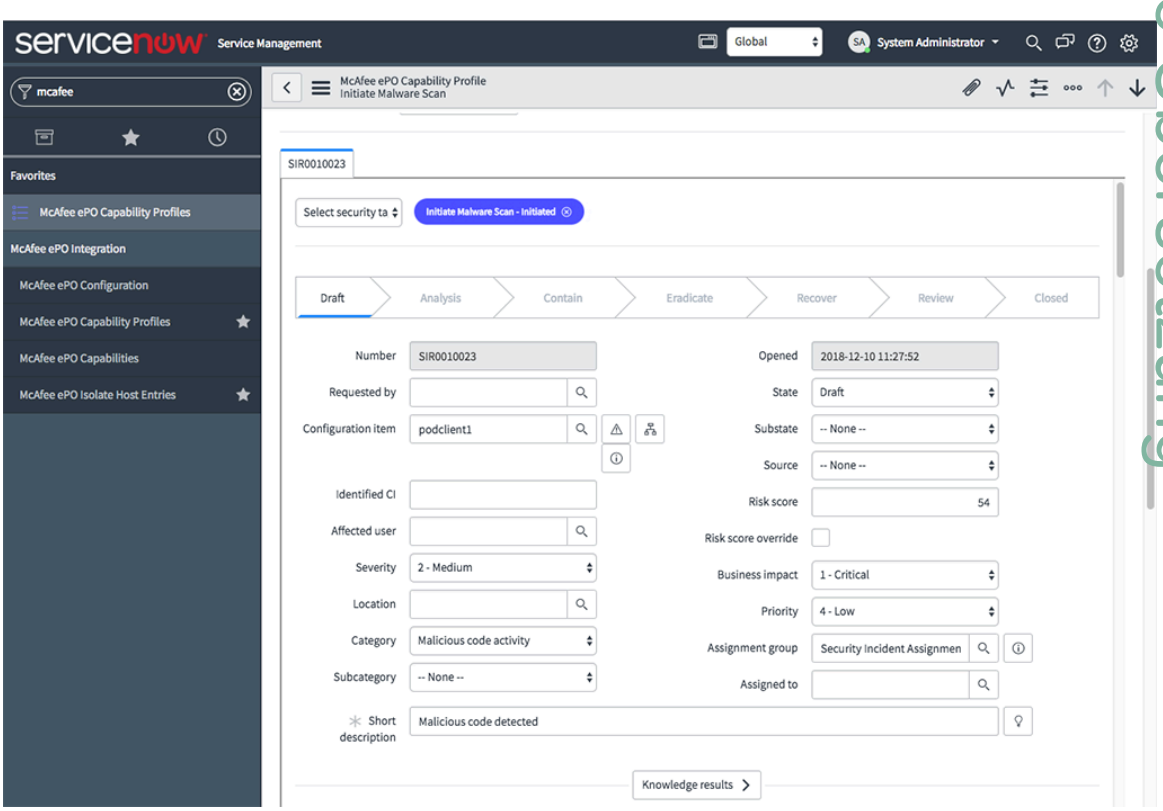
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



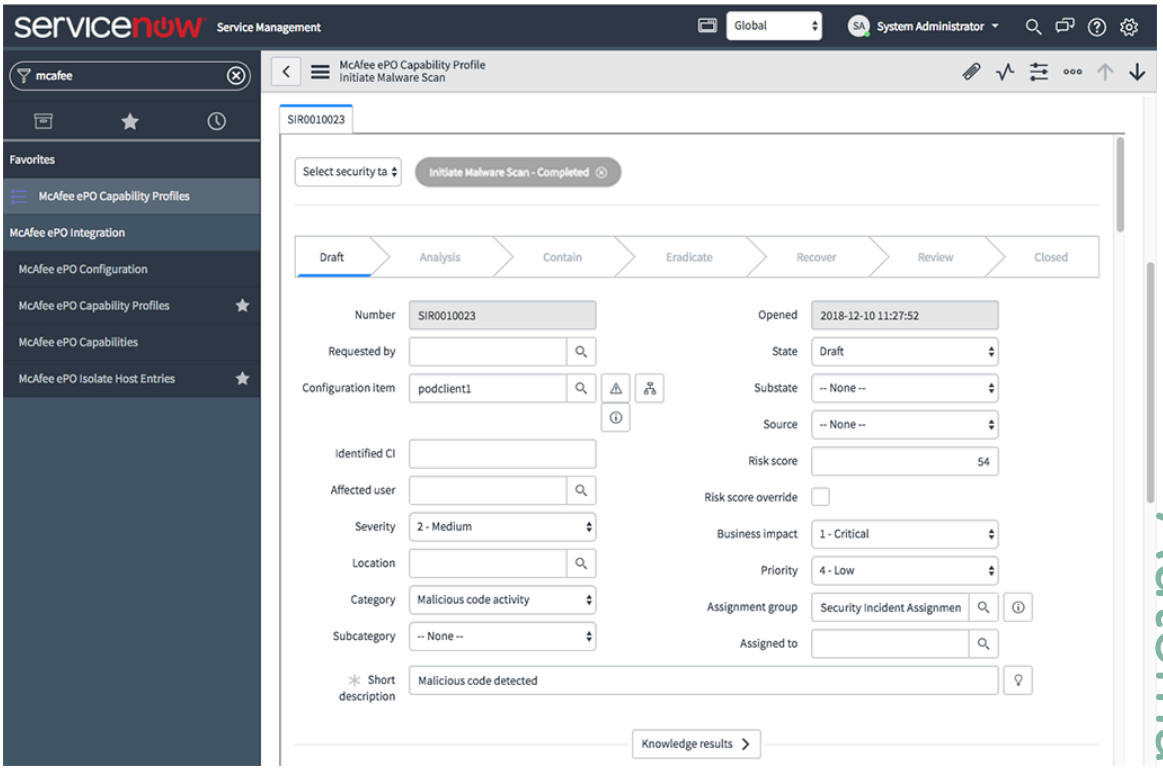
Scans werden manchmal für die Ausführung nach Spitzenarbeitszeiten geplant, um ihre Auswirkungen auf Anwender im Netzwerk zu minimieren. Der Scan wird möglicherweise nicht sofort abgeschlossen. In diesem Fall wird oben im Security Incident ein Sicherheits-Tag angezeigt, das angibt, dass der Scan geplant ist. Den Status des Workflows finden Sie in den Arbeitsnotizen. Die Liste der Arbeitsnotizen, wenn Workflows beginnen und erfolgreich abgeschlossen wurden. In diesem Beispiel zeigen die Arbeitsnotizen in der folgenden Abbildung, dass der Scan gestartet und erfolgreich abgeschlossen wurde. Die Funktion „Bedrohungsereignisse auflisten“ wurde ebenfalls gestartet und als Teil des Scans erfolgreich abgeschlossen.

Die folgende Abbildung zeigt ein Beispiel für ein Sicherheits-Tag für den zugehörigen Security Incident.

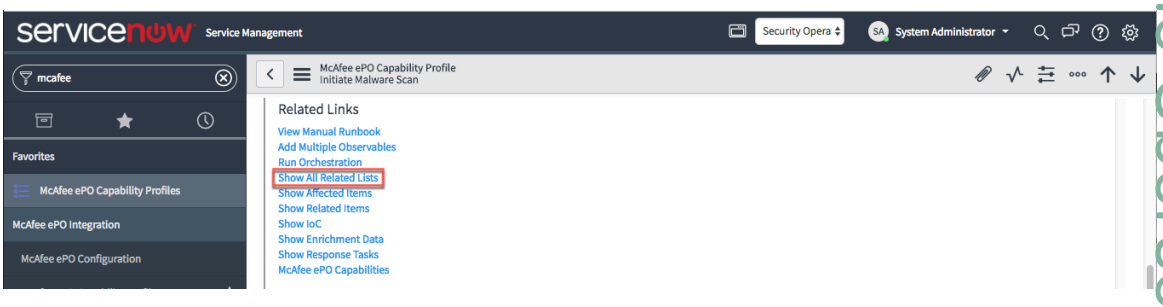


Beim Security Incident wird das geplante Tag nach erfolgreichem Abschluss des Scans automatisch durch das Tag „Abgeschlossen“ ersetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

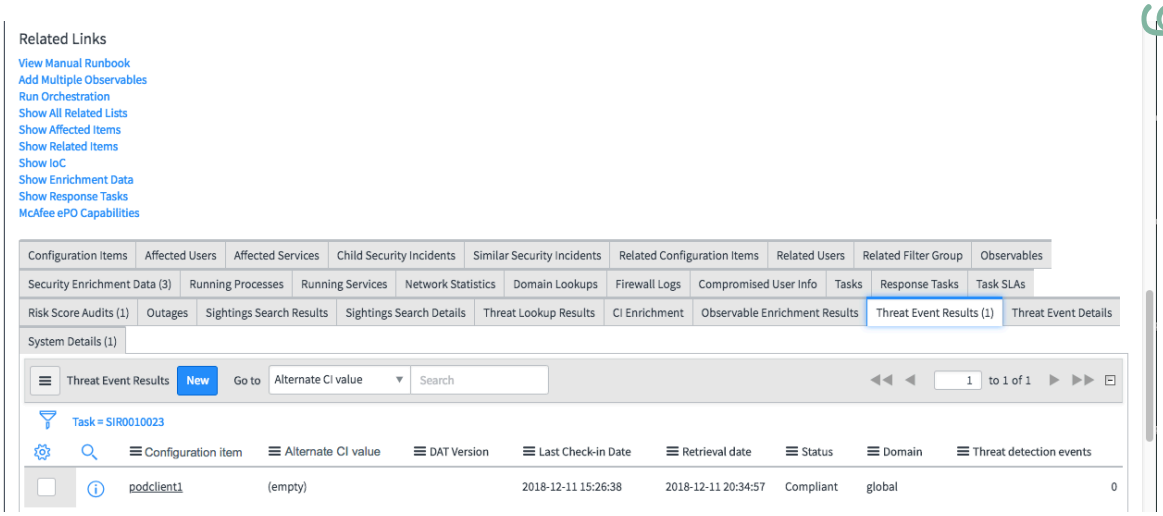


7. Nachdem Sie überprüft haben, dass der Scan erfolgreich abgeschlossen wurde, scrollen Sie im Security Incident, um die zugehörigen Links anzuzeigen, und klicken Sie auf **Alle zugehörigen Listen anzeigen** .



Die Liste Bedrohungsereignisergebnisse und Bedrohungsereignisdetails werden als Registerkarten angezeigt.

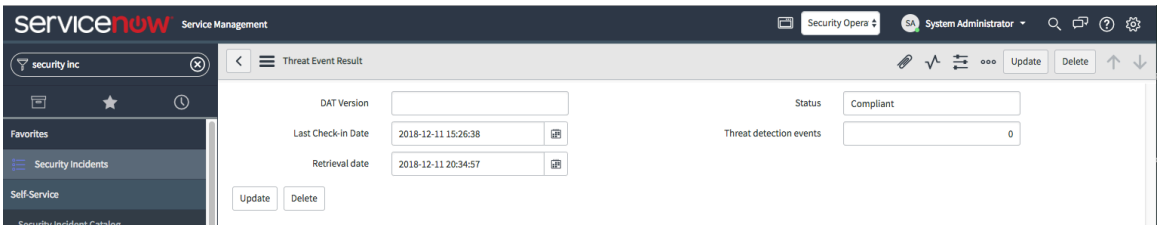
8. Wenn die Liste Details zum Bedrohungsereignis nicht ausgewählt ist, wählen Sie sie aus, um die Ergebnisse anzuzeigen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Klicken Sie auf ein Element in der Spalte Quelle, um einen Datensatz zu öffnen und die Ergänzungsdaten anzuzeigen.



Die Ergänzungsdaten enthalten die folgenden Informationen.

- Der CI-Feldwert, der während des Scans abgeglichen wurde.
- Datum des letzten Check-ins mit Zeitzone. Diese Daten beziehen sich darauf, wann zur Ortszeit die aktuellsten Daten aus abgerufen wurden McAfee ePO Konsole.
- Rohdaten

Sie haben erfolgreich verifiziert, dass der Scan-Workflow für Security Incidents erfolgreich abgeschlossen wurde, die den Kriterien für die automatische Auslösung entsprechen, die Sie für dieses Profil festgelegt haben.

10. Wählen Sie eine, um fortzufahren.

Testen Sie Security Incidents, und genehmigen Sie Anforderungen für den isolierten Host

Mit dem Test- und Vorschauschritt können Sie überprüfen, ob die Ergebnisse des Workflows für die Hostisolierung und das Entfernen der Hostisolierung wie erwartet für das Profil zurückgegeben werden.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

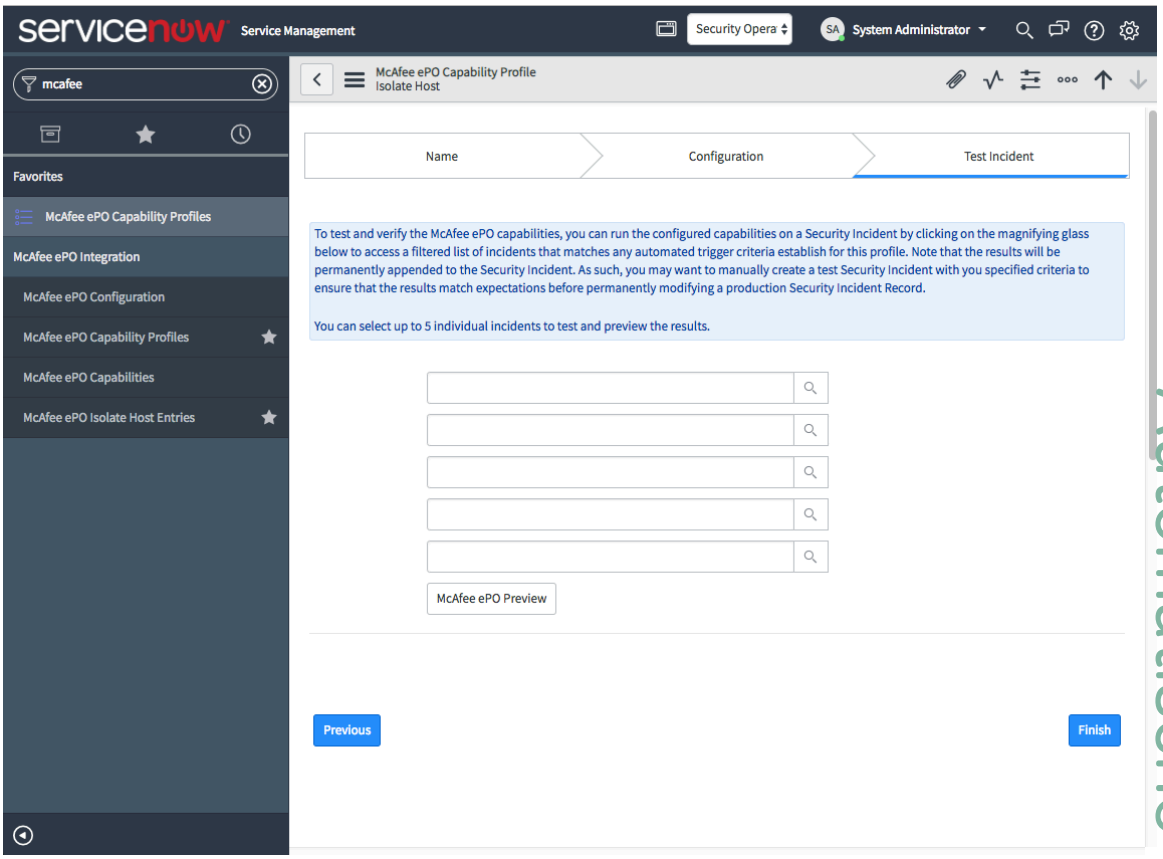
Warum und wann dieser Vorgang ausgeführt wird
Stellen Sie während dieses Schritts der Konfiguration als Anwender mit der Rolle „sn_si.admin“ sicher, dass das Profil, das Sie mit der Funktion „Host isolieren“ konfiguriert haben, Security Incidents und übereinstimmende Asset-IDs wie erwartet zurückgibt. Zeigen Sie den ist-Wert an ServiceNow AI Platform Security Incident Response(SIR) Security Incidents, die erstellt werden, wenn Bedingungen für Sicherheitsereignisse auftreten, die den Einstellungen Ihres Profils entsprechen.

Nachdem eine Anforderung zum Isolieren eines Hostcomputers übermittelt wurde, verarbeiten Sie die Anforderung als Anwender mit einer Genehmigerrolle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn die Seite Incident testen nicht angezeigt wird, klicken Sie auf **Test-Incident** In der Fortschrittsleiste.

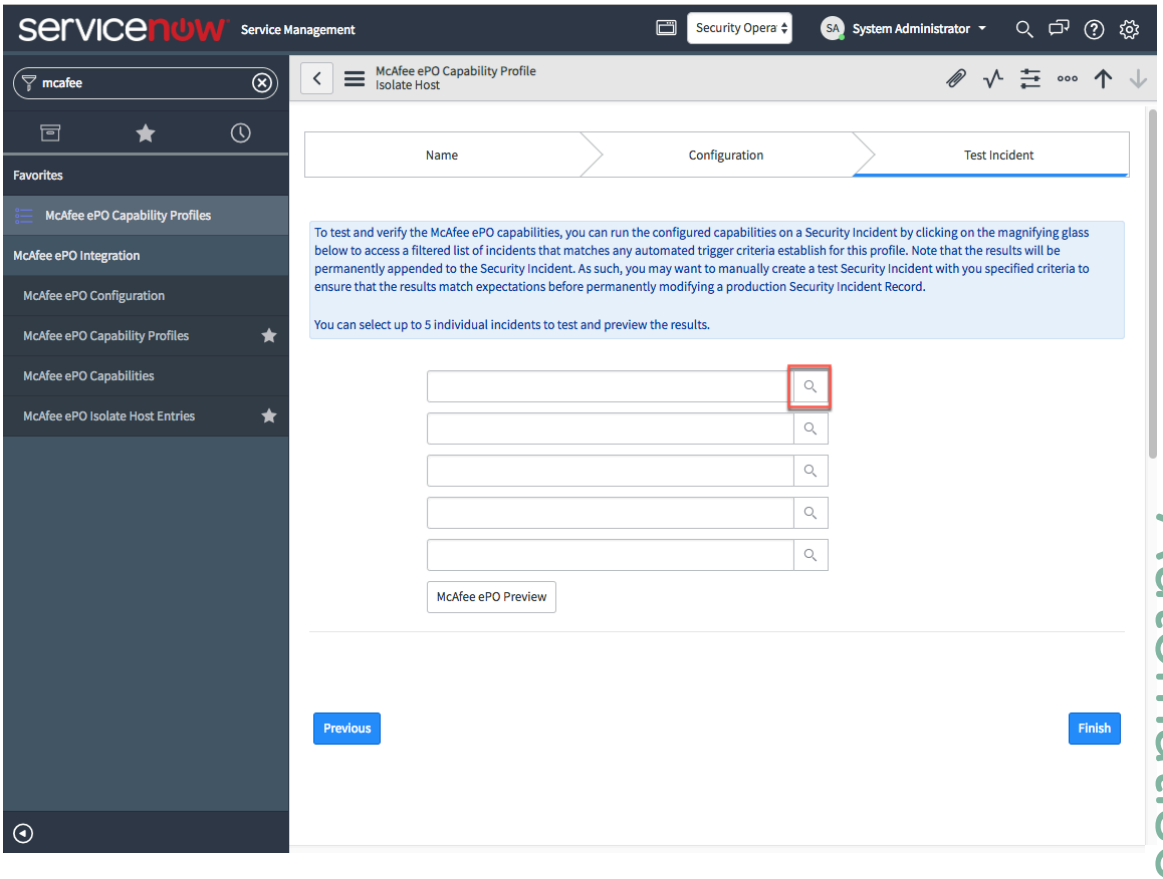


Die Seite Test Incident wird für Ihr Profil angezeigt. Für dieses Beispiel die Host Isolieren ™Das Profil, das Sie in den vorherigen Abschnitten erstellt und konfiguriert haben, wird angezeigt.

2. Klicken Sie rechts neben dem oberen Feld auf das Suchsymbol, um einen Security Incident für die Vorschau auszuwählen.

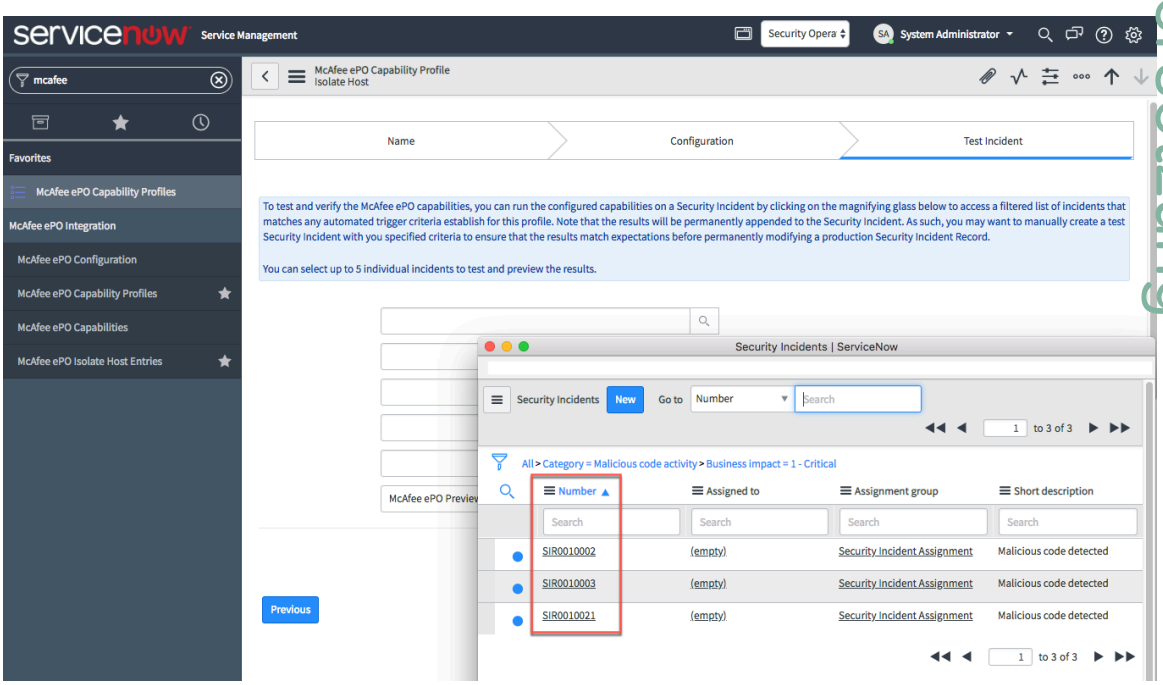
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie in der Spalte Nummer der angezeigten Liste ein Element aus, das Sie in der Vorschau anzeigen möchten.

Es werden nur Security Incidents angezeigt, die den von Ihnen für das Profil festgelegten Kriterien entsprechen.

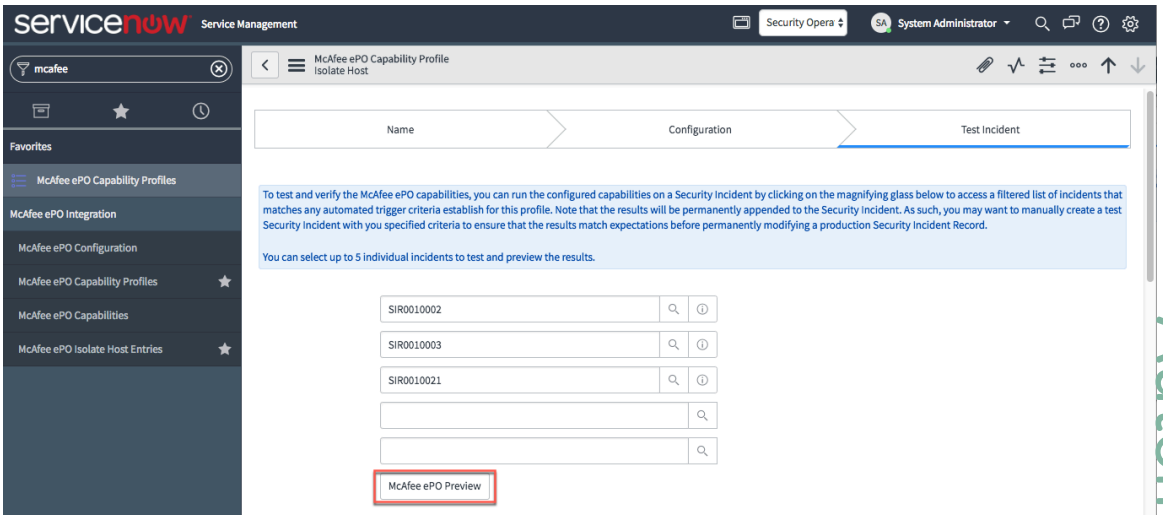


Die Security Incidents werden auf der Seite angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

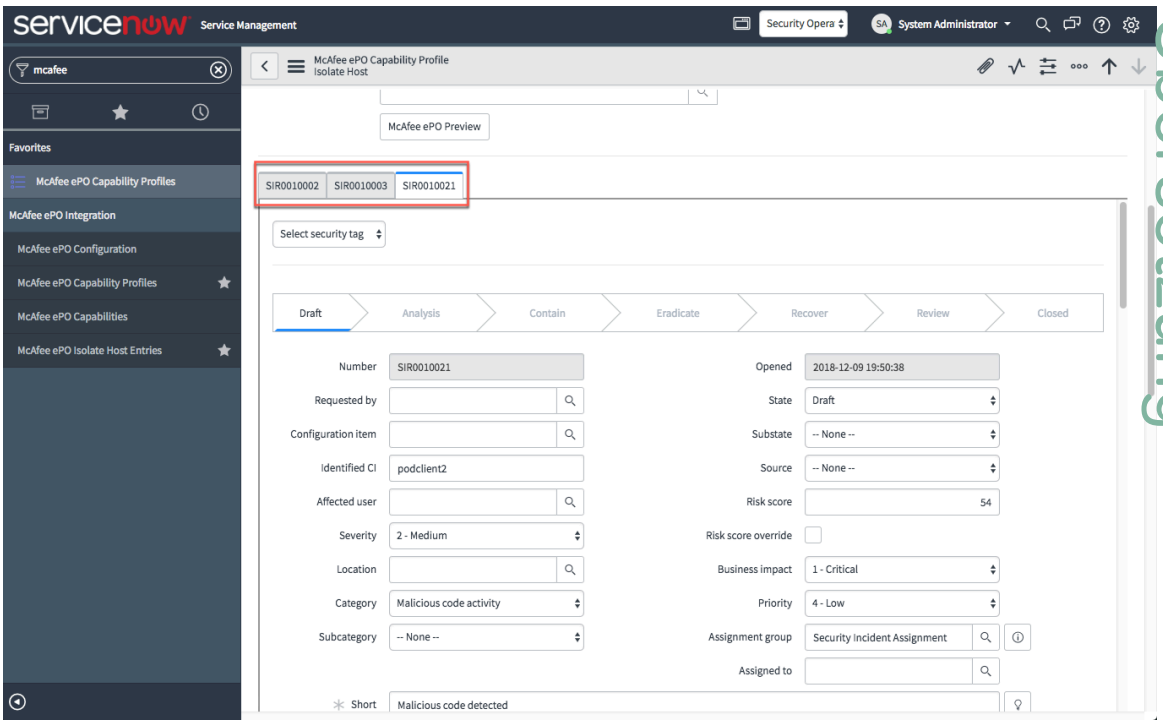
4. Wiederholen Sie die Schritte 2 und 3, bis alle Incidents, die Sie in der Vorschau anzeigen möchten, in den Feldern angezeigt werden.
   Wählen Sie bis zu fünf Security Incidents für die Vorschau aus.
5. Klicken Sie Auf **McAfee ePO-Vorschau** Dient zum Anzeigen der Security Incidents.



Die Incidents, die für die Bedingungen des Sicherheitsereignisses erstellt wurden, die Ihrem Profil entsprechen, werden auf Registerkarten angezeigt.

Hinweis:

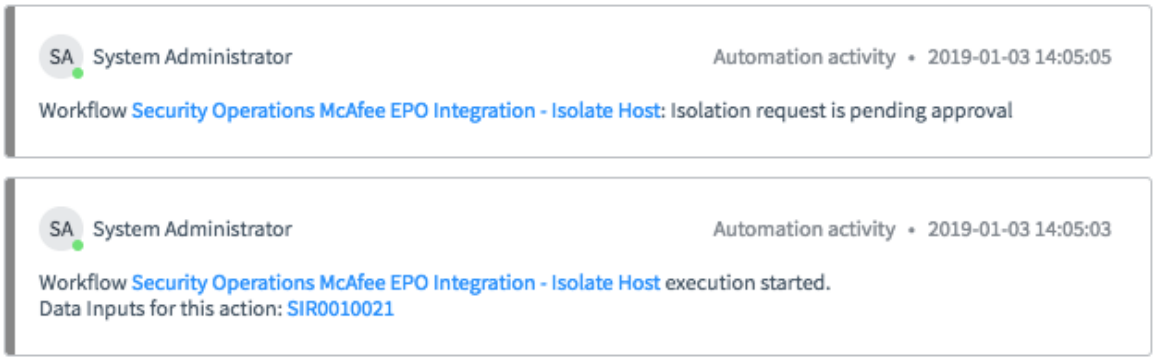
Wenn Sie die Seite „Incident testen“ zu diesem Zeitpunkt verlassen, werden Ihre Security Incidents aus diesen Feldern gelöscht.



6. Wählen Sie eine Registerkarte aus, und scrollen Sie im Security Incident, um die Arbeitsnotizen anzuzeigen.

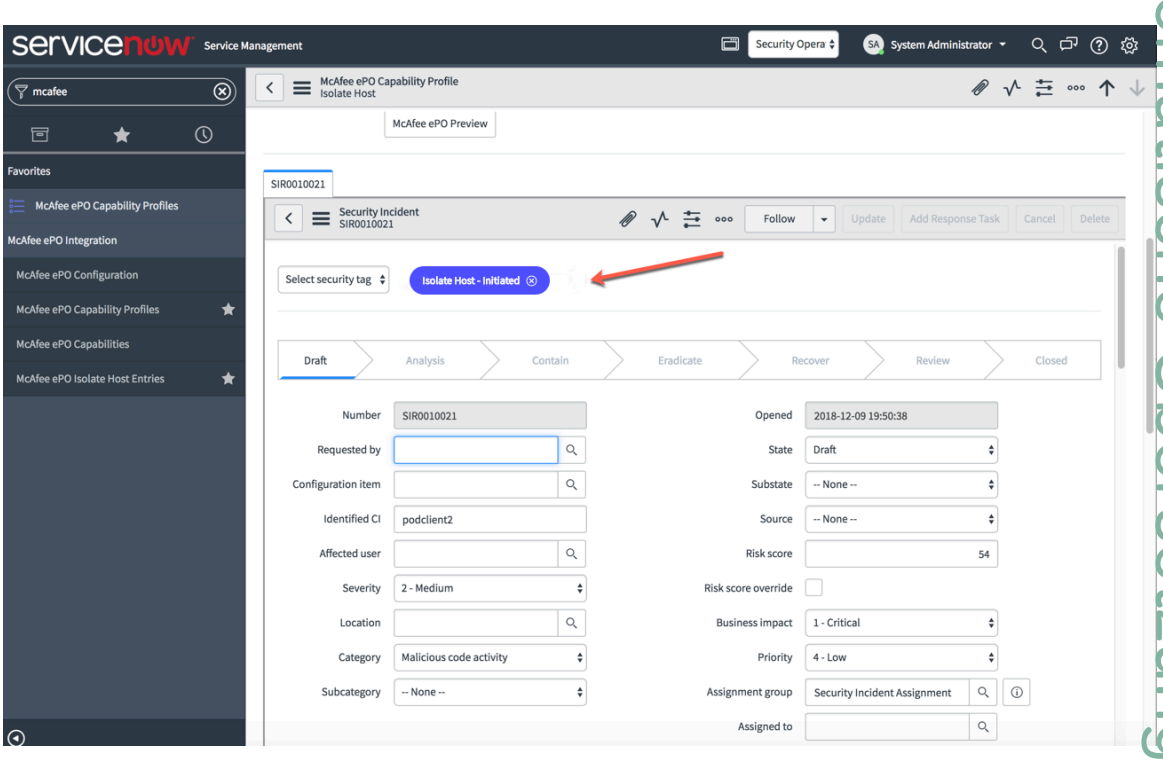
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Für dieses Beispiel wird SIR0010021 aus dem vorherigen Bild ausgewählt. Die Liste der Arbeitsnotizen, in der der Workflow zum Isolieren des Hosts gestartet wird. Weil **Genehmigung Erforderlich** Die Option ist für dieses Profil aktiviert. Die Arbeitsnotizen geben an, dass die Anforderung ist Genehmigung ausstehend .

Oben im Incident wird das Sicherheits-Tag angezeigt, das angibt, dass die Anforderung initiiert wurde (Host Isolieren – Initiiert).



Sie haben erfolgreich Security Incidents gefunden, die Ihrem Profil für die Fähigkeit „Host isolieren“ entsprechen, und einen Security Incident angezeigt.

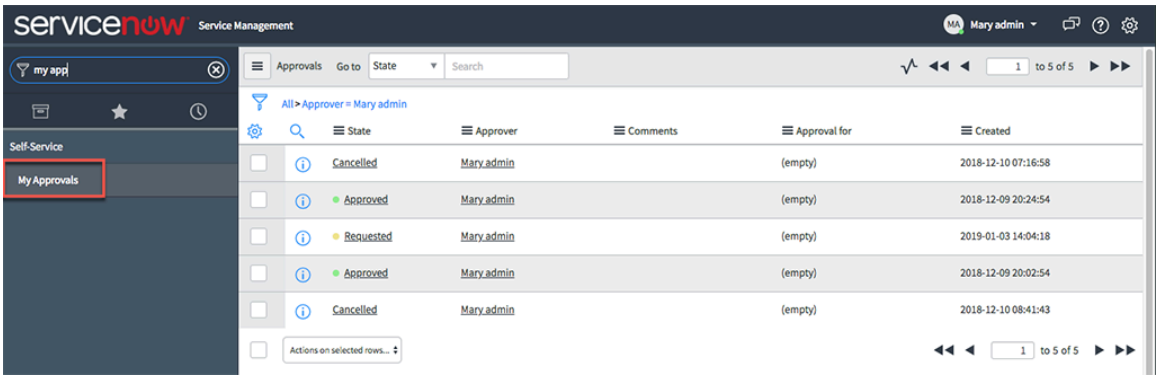
7. Wenn Sie ein Anwender in einer Genehmigungsgruppe sind, führen Sie die folgenden Schritte aus, um eine Anforderung zu verarbeiten.

   a. Navigieren Sie zu **Meine Genehmigungen** In Ihrer Instanz.

      In diesem Beispiel lautet der Anwendername des Genehmigers Mary-Administrator ™.

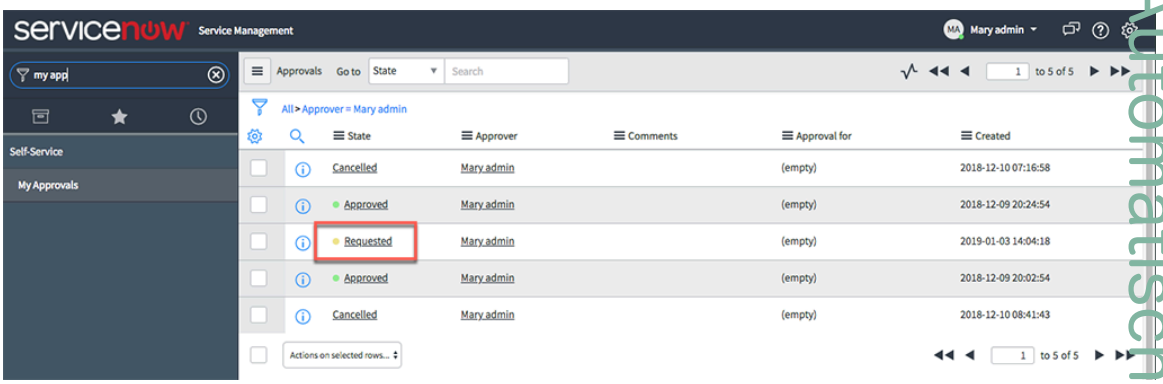
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

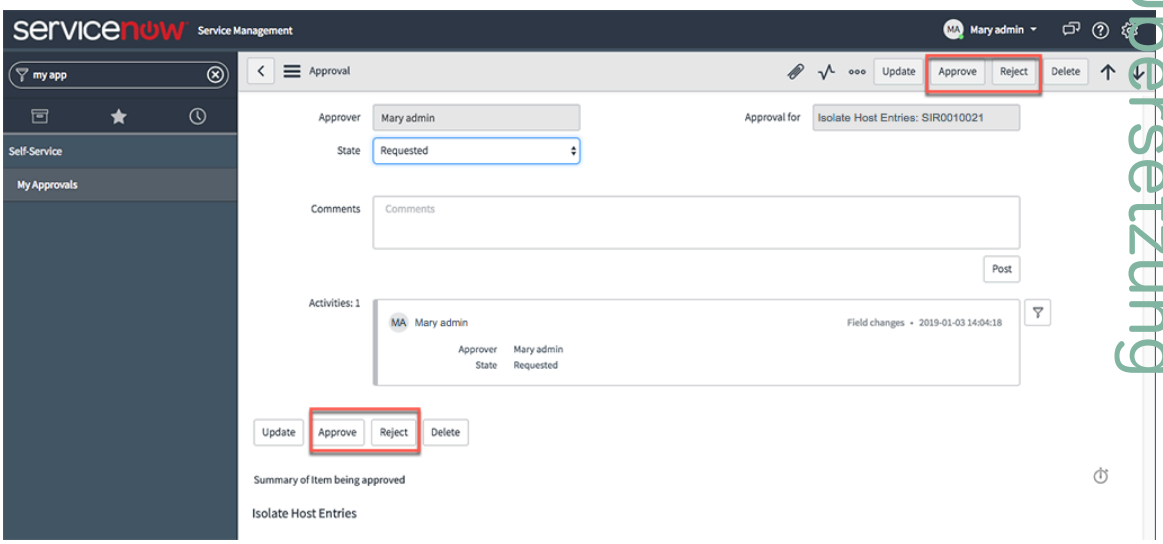


Die Genehmigungsliste wird angezeigt.

b. Klicken Sie in der Spalte Status auf ein Element, um den Genehmigungsdatensatz zu öffnen.



c. Klicken Sie im angezeigten Genehmigungsdatensatz auf **Genehmigen** Oder **Ablehnen** .

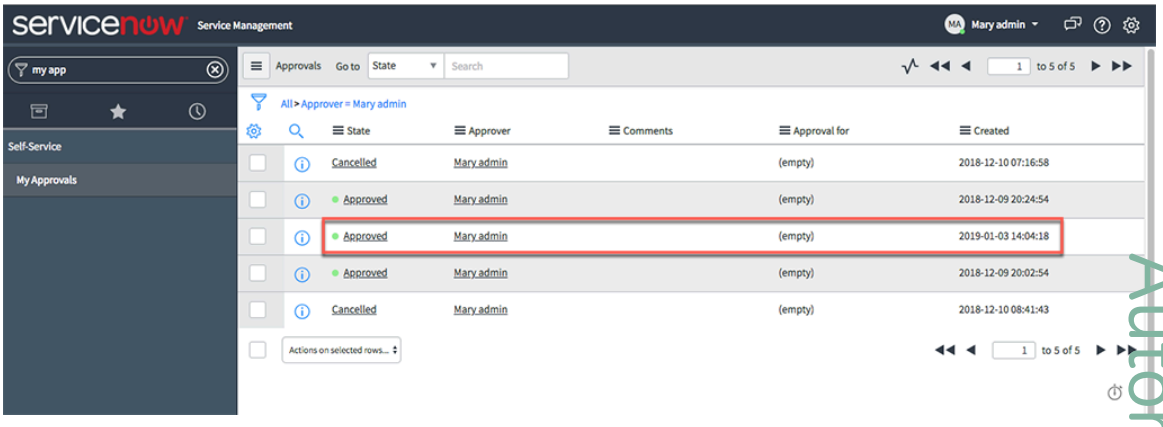


Nachdem Sie die Anforderung verarbeitet haben, kann die Ausführung des Workflows einige Minuten dauern. Im Datensatz oben wird eine Meldung angezeigt, wie in der folgenden Abbildung dargestellt, wenn die Transaktion länger als einige Sekunden dauert.

Automatische Übersetzung

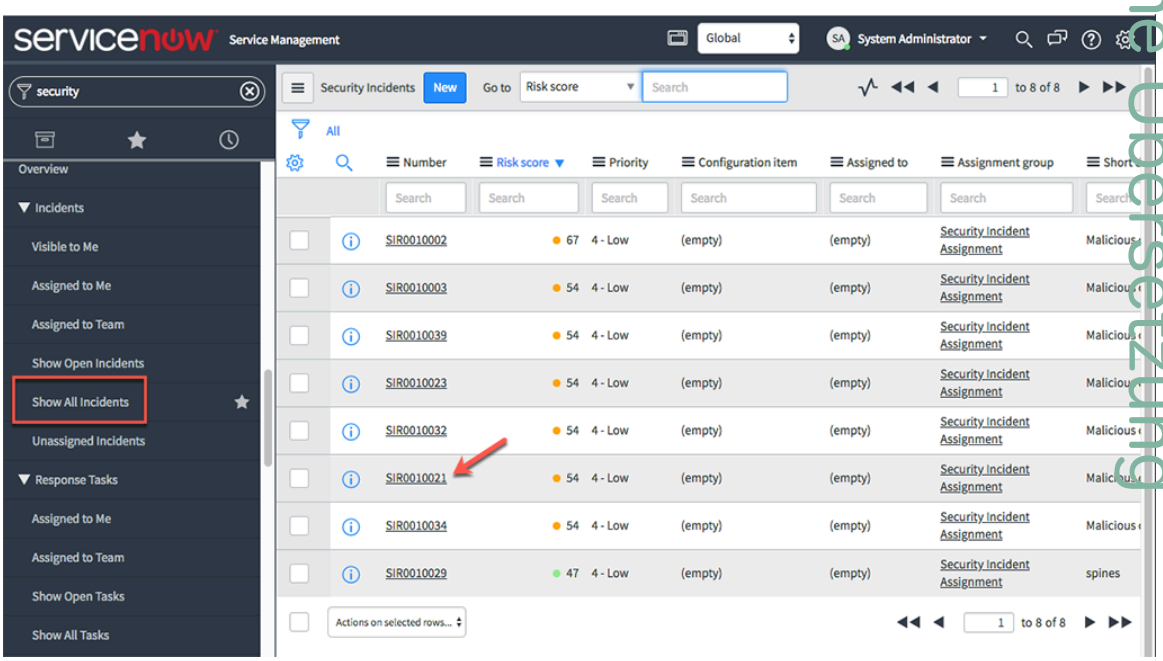
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach einigen Minuten ändert sich im angezeigten Genehmigungsdatensatz die Spalte Status von Angefordert Bis Genehmigt . Es sind keine zusätzlichen Genehmigungen erforderlich, um den Hostcomputer für diese Anforderung zu isolieren. Wenn die Anforderung abgelehnt wird, wird der Host nicht isoliert, und die Anforderung bleibt ausstehend. Wenn die Anforderung abgelehnt wird, müssen Sie als Anwender mit der Rolle „sn_si.Analyst“ eine neue Anforderung übermitteln, wenn Sie den Endpunkt trotzdem isolieren möchten.



Die Anforderung zum Isolieren des Hostcomputers in der obigen Abbildung wird genehmigt.

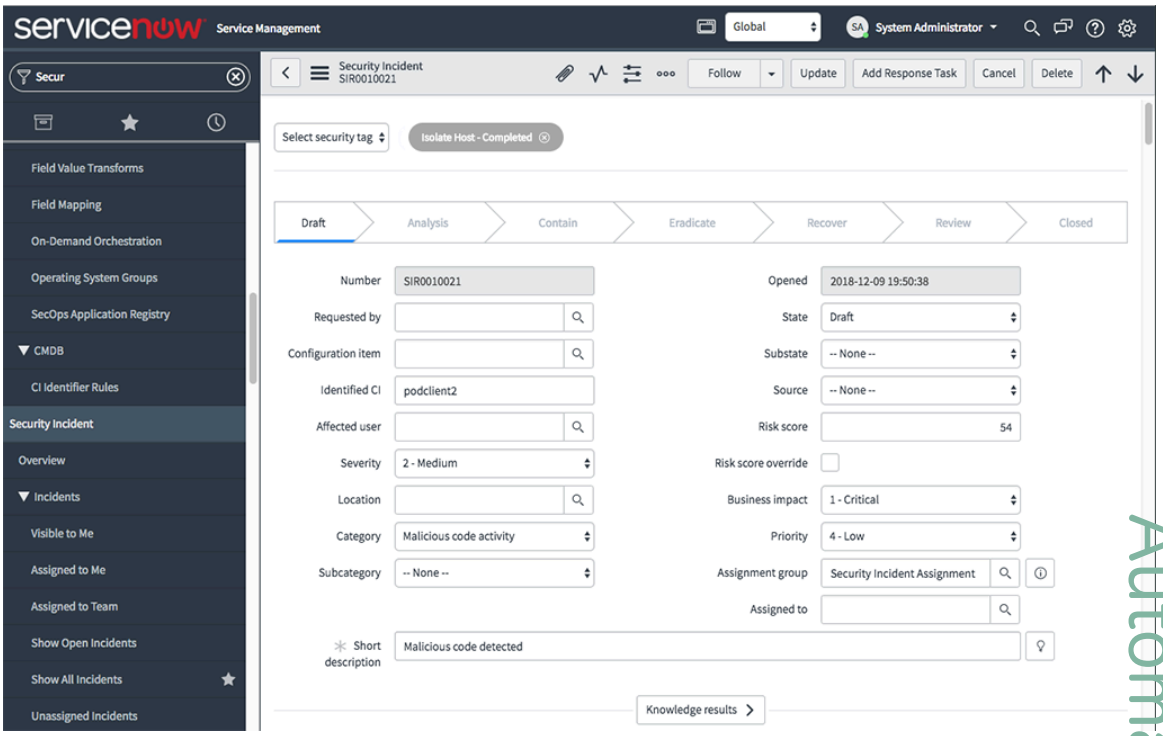
d. Navigieren zu **Security Incident** > **Incidents** > **Alle Incidents anzeigen** Und klicken Sie in der Spalte Nummer auf einen Eintrag, um den Security Incident zu öffnen, mit dem Sie arbeiten.



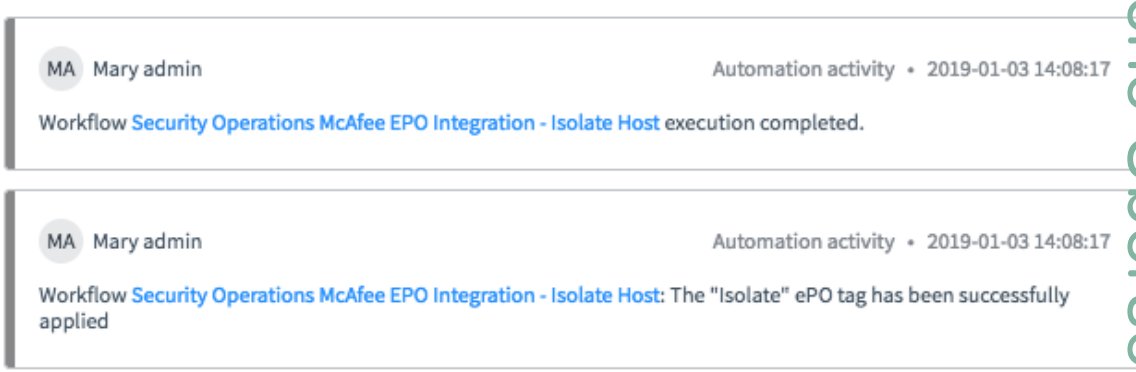
Für den Security Incident, der angezeigt wird, die Host Isolieren – Abgeschlossen ™Tag ersetzt Host Isolieren – Initiiert ™Tag. Der Host-Isolations-Workflow für dieses Beispiel ist erfolgreich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Arbeitsnotizen zum Security Incident zeigen auch an, dass die Host-Isolierung abgeschlossen ist, und der Genehmiger Mary-Administrator™, Ist aufgeführt.



Wichtig:
Obwohl das Sicherheits-Tag und die Arbeitsnotizen zum Security Incident darauf hinweisen, dass ein erfolgreicher Workflow zum Isolieren des Hosts abgeschlossen ist, kehren Sie zu zurück McAfee ePO Konsole und verifizieren Sie, dass der Hostcomputer von Ihrem Netzwerk isoliert ist.

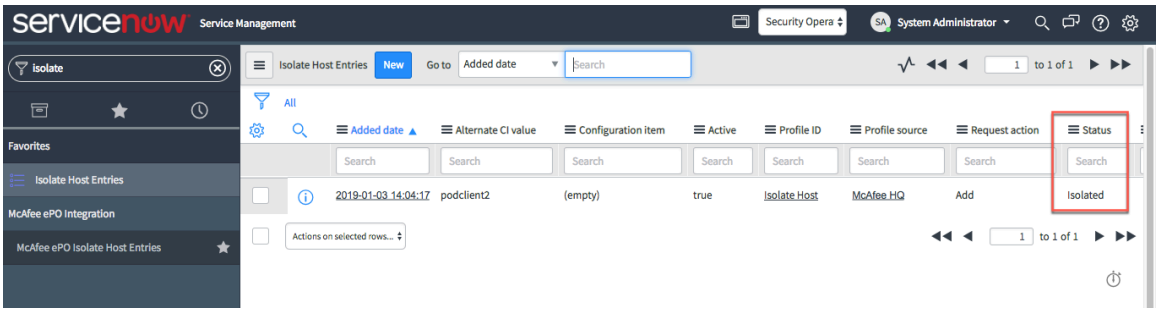
Nachdem Sie Ihre Untersuchung des Assets abgeschlossen haben, starten Sie den Workflow „Isolierung entfernen“ aus der Host-Isolationseinträge™Tabelle in Ihrem ServiceNow AI Platform® Instanz, um den Host an das Netzwerk zurückzugeben.

8. Führen Sie die folgenden Schritte aus, um den Host aus der Quarantäne zu entfernen und an das Netzwerk zurückzugeben.

Automatische Übersetzung

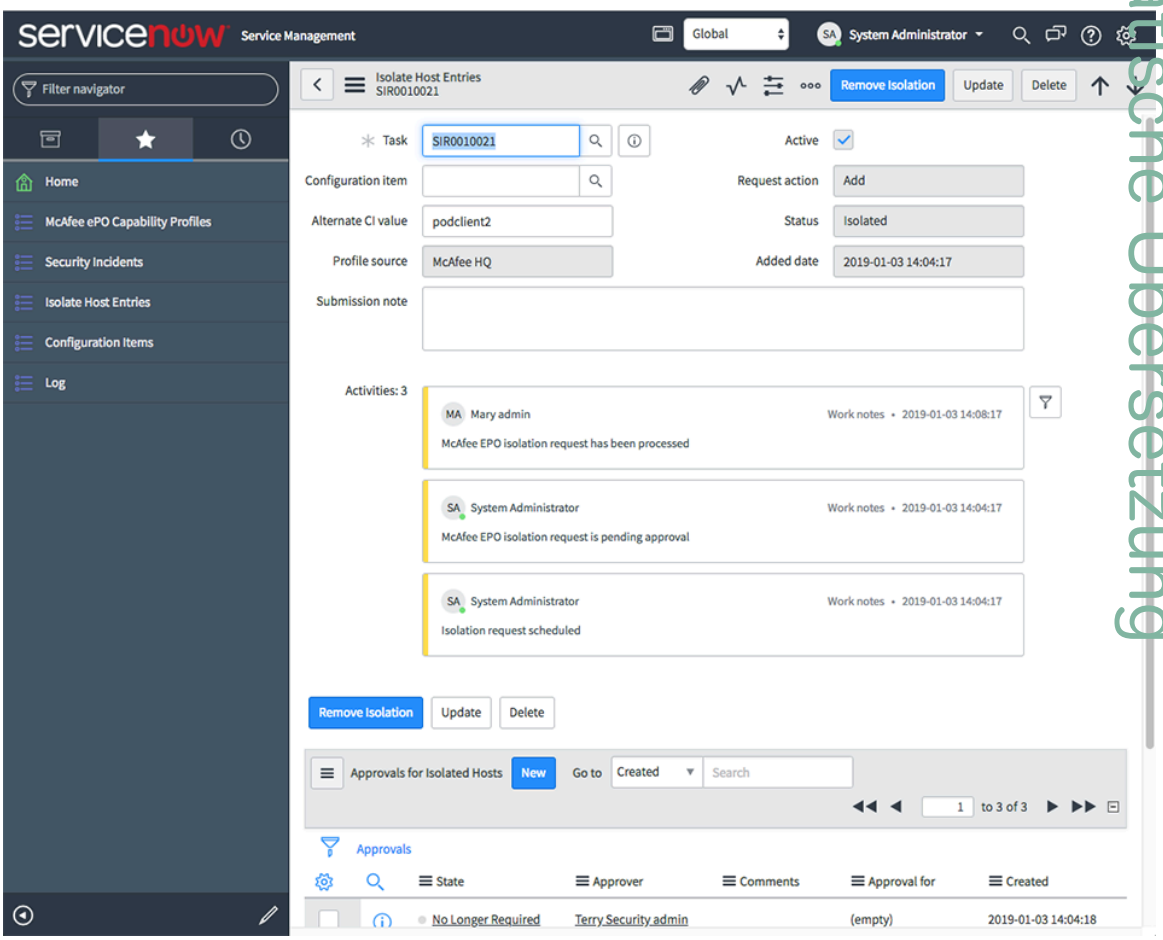
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wenn McAfee ePO Die Tabelle „Hosteinträge isolieren“ wird nicht angezeigt. Navigieren Sie zu **McAfee EPO-Integration** > **McAfee-EPO-Integration – Host-Einträge isolieren**an.



Die Liste Host-Einträge isolieren wird angezeigt. Suchen Sie oben in der Liste in der Spalte Status nach dem Asset, das Sie isoliert haben.

b. Klicken Sie in der Spalte „hinzugefügtes Datum“ auf das Element, um den Datensatz zu öffnen.
Der Datensatz Host-Einträge isolieren wird angezeigt. In den Arbeitsnotizen wird ein Audit-Pfad für alle Aktionen angezeigt, die dem Security Incident zugeordnet sind. In der folgenden Abbildung ist der letzte Eintrag in den Arbeitsnotizen eine erfolgreiche Host-Isolierung. Das Datum, an dem die Quarantäne abgeschlossen wurde, wird im angezeigt **Hinzugefügtes Datum** Feld (2019-01-03 14:04:17).

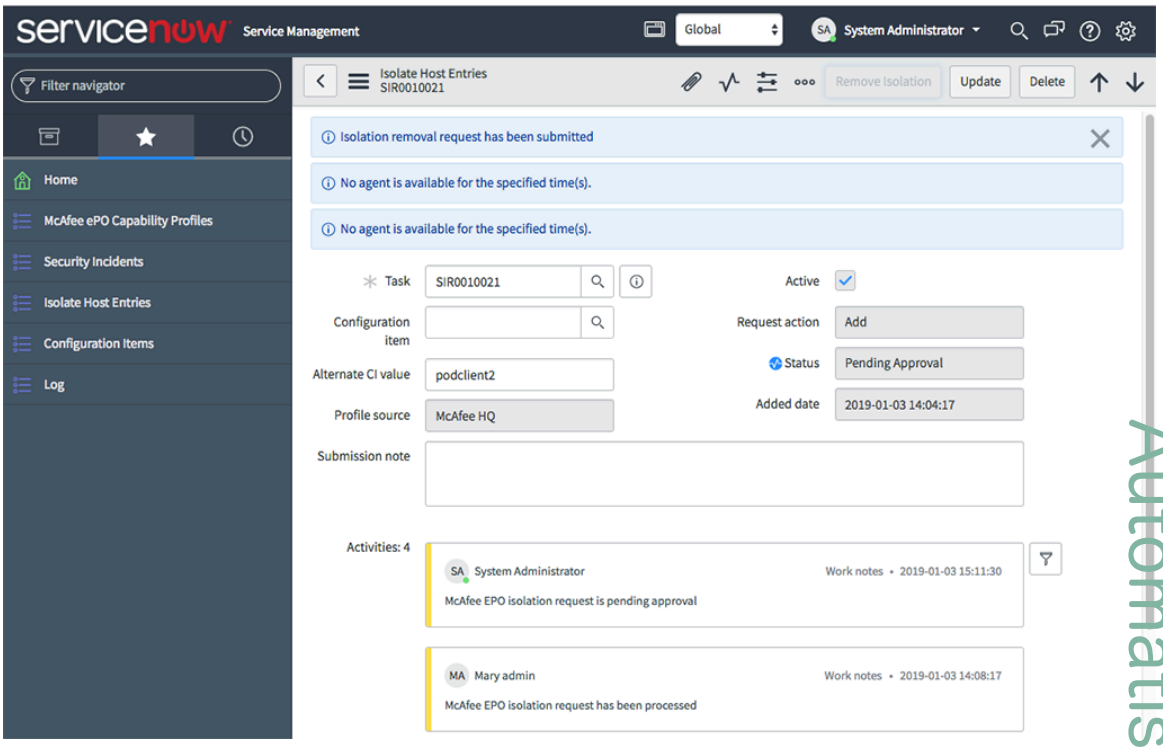


c. Klicken Sie Auf **Entfernen Sie Die Isolierung** Um den Workflow zu starten, um den Computer im Netzwerk wiederherzustellen.
Der Datensatz Host-Eintrag isolieren wird angezeigt. Oben im Datensatz gibt eine Nachricht an, dass die Anforderung übermittelt wurde. Der Status ändert sich von **Isoliert** Bis **Genehmigung Ausstehend** ,

Automatische Übersetzung

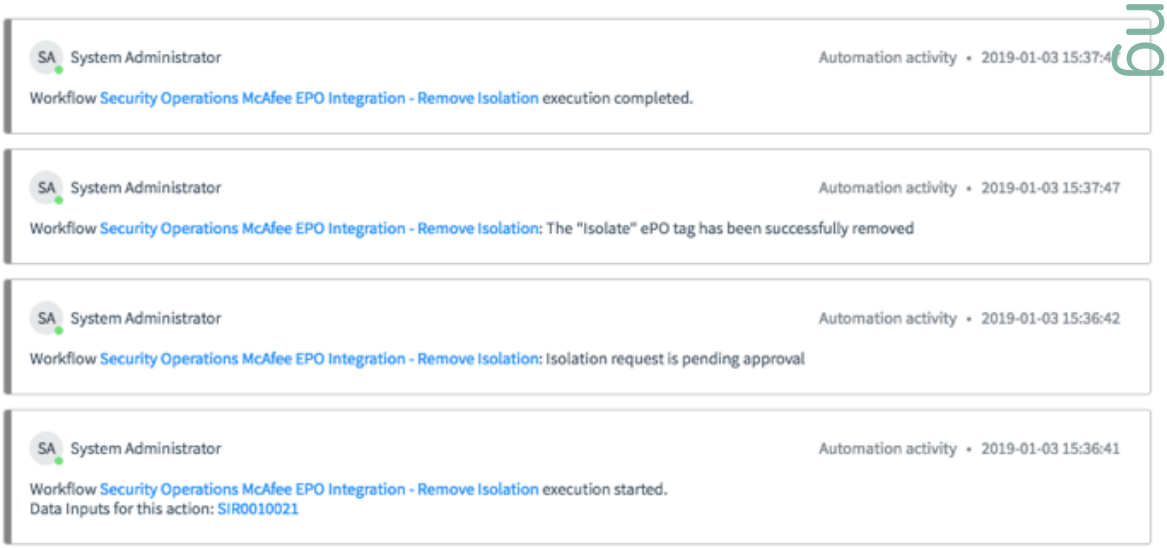
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Und eine Arbeitsnotiz wird protokolliert. In diesem Fall hat der Systemadministrator angefordert, dass der Computer im Netzwerk wiederhergestellt wird.



d. Nachdem Sie über die Anforderung benachrichtigt wurden, navigieren Sie als Anwender mit Genehmigungsberechtigung für die Hostisolierung zu **Meine Genehmigungen** Öffnen Sie in Ihrer Instanz den Datensatz für die Anforderung zum Entfernen der Isolation.

e. Klicken Sie Auf **Genehmigen** Um die Anforderung zu genehmigen und das Asset an das Netzwerk zurückzugeben.
Alternativ können Sie auf klicken **Ablehnen** Um die Anforderung im Status „Genehmigung ausstehend“ zu behalten. Wenn eine Anforderung abgelehnt wird, muss eine neue Anforderung übermittelt werden, um den Host zu isolieren. Nachdem Sie die Anforderung zum Entfernen der Hostisolierung genehmigt haben, wird das Tag im Security Incident entfernt. Arbeitsnotizen erstellen einen Audit-Pfad für die Anforderung zum Entfernen der Isolation. In diesem Beispiel hat der Systemadministrator die Anforderung initiiert und genehmigt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Sicherheits-Tag und die Arbeitsnotizen zum Security Incident zeigen an, dass der Workflow zum Entfernen der Hostisolierung erfolgreich abgeschlossen wurde. Um sicherzustellen, dass sich der Host wieder im Netzwerk befindet, kehren Sie zu zurück McAfee ePO Konsole und verifiziert, dass der Hostcomputer jetzt aktiv ist.

9. Wählen Sie eine, um fortzufahren.

Bearbeiten Sie die Namen und Farben der Start- und Abschluss-Tags

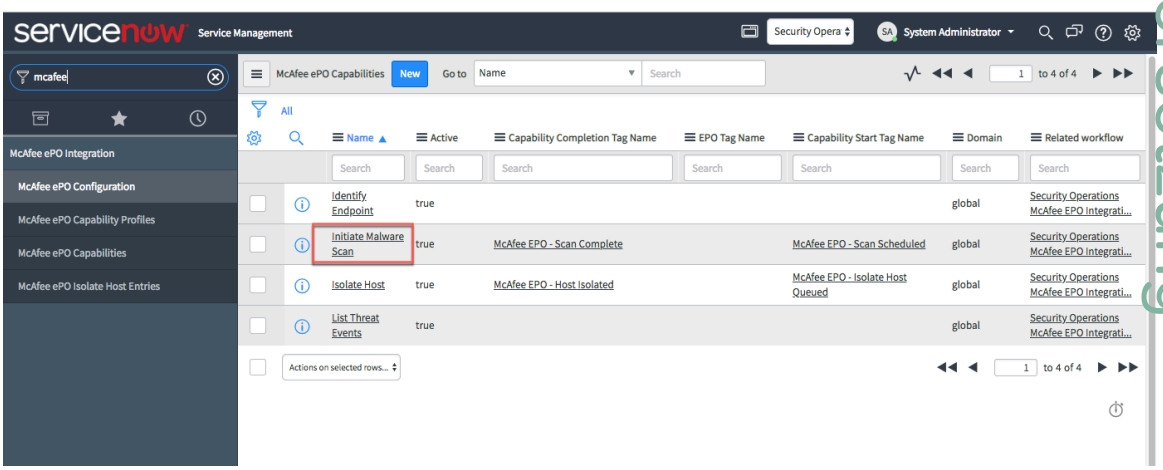
Möglicherweise möchten Sie die Namen und Farben der Start- und Abgeschlossen-Tags für die Funktionen „Malware-Scan initiieren“ und „Host isolieren“ bearbeiten. Die Tags Start und Abgeschlossen helfen Ihnen, schnell zu identifizieren, welche Fähigkeiten von aufgerufen werden ServiceNow AI Platform Security Incident Response(SIR) Security Incidents.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Als Anwender mit der Rolle „sn_si.admin“ können Sie die Farben und Namen der in angezeigten Sicherheits-Tags bearbeiten SIR Security Incidents. Sie können Sicherheits-Tag-Gruppen auch Tags zuweisen, um sie in Ihrem zu organisieren ServiceNow AI Platform® Instanz. Sie können beispielsweise die Farben von Tags ändern, sodass das Start-Tag einer Fähigkeit eine Farbe und das Abschluss-Tag eine andere Farbe hat. Diese verschiedenen Farben können Ihnen helfen, schnell zu erkennen, wann Scans beginnen und erfolgreich abgeschlossen wurden. Weitere Informationen zum Einrichten von Sicherheits-Tag-Gruppen und -Tags finden Sie unter Richten Sie Sicherheits-Tag-Gruppen und -Tags ein .

Prozedur

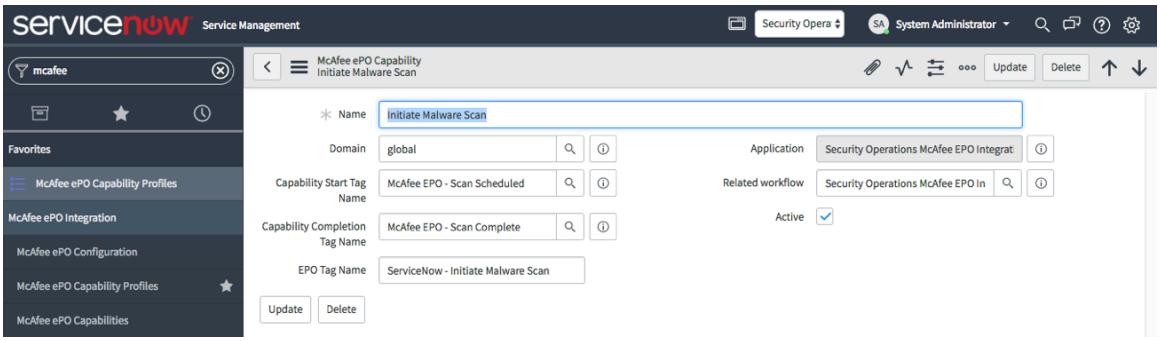
1. Um die Namen und Farben der Sicherheits-Tags zu bearbeiten, navigieren Sie zu **McAfee-EPO-Fähigkeiten** , Und klicken Sie in der Spalte Name auf ein Element in der Liste.



Der Datensatz für die Fähigkeit wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Um ein Tag zu bearbeiten, klicken Sie rechts neben einem Tag-Namen auf das Informationssymbol, und öffnen Sie den Tag-Datensatz.

   Bearbeiten Sie die Felder im angezeigten Datensatz.

3. Wählen Sie eine, um fortzufahren.

McAfee ESM: E-Mail-Parser-Integration

Die ESM – E-Mail-Parser-Integration wird von einem E-Mail-Parser unterstützt, der E-Mail-Benachrichtigungen von ESM verwendet, um Security Incidents zu erstellen.

Konfigurieren Sie die Integration von McAfee ESM – E-Mail-Parser

McAfee ESM – E-Mail-Parser-Integration verwendet E-Mail-Benachrichtigungen von ESM, um Ergänzungs- und Antwort-Workflows zu fördern.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

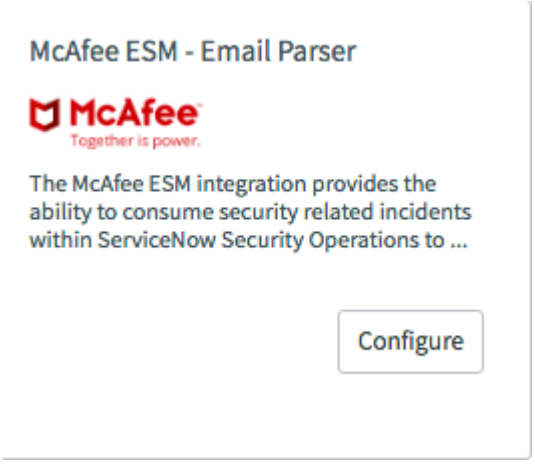
Warum und wann dieser Vorgang ausgeführt wird

Eine McAfee ESM-E-Mail-Parser-Vorlage wird zur Verwendung für die Integration bereitgestellt. Sie muss konfiguriert und aktiviert werden, bevor die Integration stattfindet. Durch das Aktualisieren des Parsers wird er aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Klicken Sie auf der Karte McAfee ESM – E-Mail-Parser auf **Konfigurieren** .
3. In **McAfee ESM: E-Mail-Parser-Konfiguration** Klicken Sie auf das Dialogfeld **Konfigurieren Sie Den E-Mail-Parser** Link.
4. Klicken Sie auf **McAfee ESM** Link zum Bearbeiten der Einstellungen im bereitgestellten Vorlagen-E-Mail-Parser.
   Füllen Sie mindestens aus `E-Mail ist von` Feld. Informationen zum Erstellen eines eigenen E-Mail-Parsers finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
5. Überprüfen Sie **Aktiv** Feld.
6. Klicken Sie Auf **Aktualisieren** In **E-Mail-Parser** Formular.
   Der E-Mail-Parser ist aktiv. Sie müssen nicht zu zurückkehren **Integrationskonfigurationen** .

McAfee ESM: Incident-Anreicherungsintegration

McAfee ESM – Die Incident-Anreicherungsintegration durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

Erkunden

Security Incident Response-Integrationen

Einrichten

- Beginnen Sie mit dem McAfee ESM– Integration der Incident-Anreicherung
- Erstellen Sie Konfigurationsdatensätze für Sichtungssuche

Verwenden

- Führen Sie eine Sichtungssuche aus
- Integration Von Security Operations: Sichtungssuche-Flow
- Security Operations – Suchflow für McAfee ESM-Sichtungen

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

- Sichtungssuchdetails Anzeigen
- Zeigen Sie Die Ergebnisse Der Sichtungssuche An

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Beginnen Sie mit dem McAfee ESM– Integration der Incident-Anreicherung

McAfee ESM Schützt Endpunkte vor Viren, Spyware, Trojanischen Pferden und anderen Malware-Bedrohungen und lässt sich problemlos in integrieren Security Operations. Bevor Sie verwenden können McAfee ESM– Integration der Incident-Anreicherung. Sie müssen sie aus dem herunterladen ServiceNow Store Und fügen Sie die entsprechende API-Basis-URL und Anmeldeinformationen hinzu.

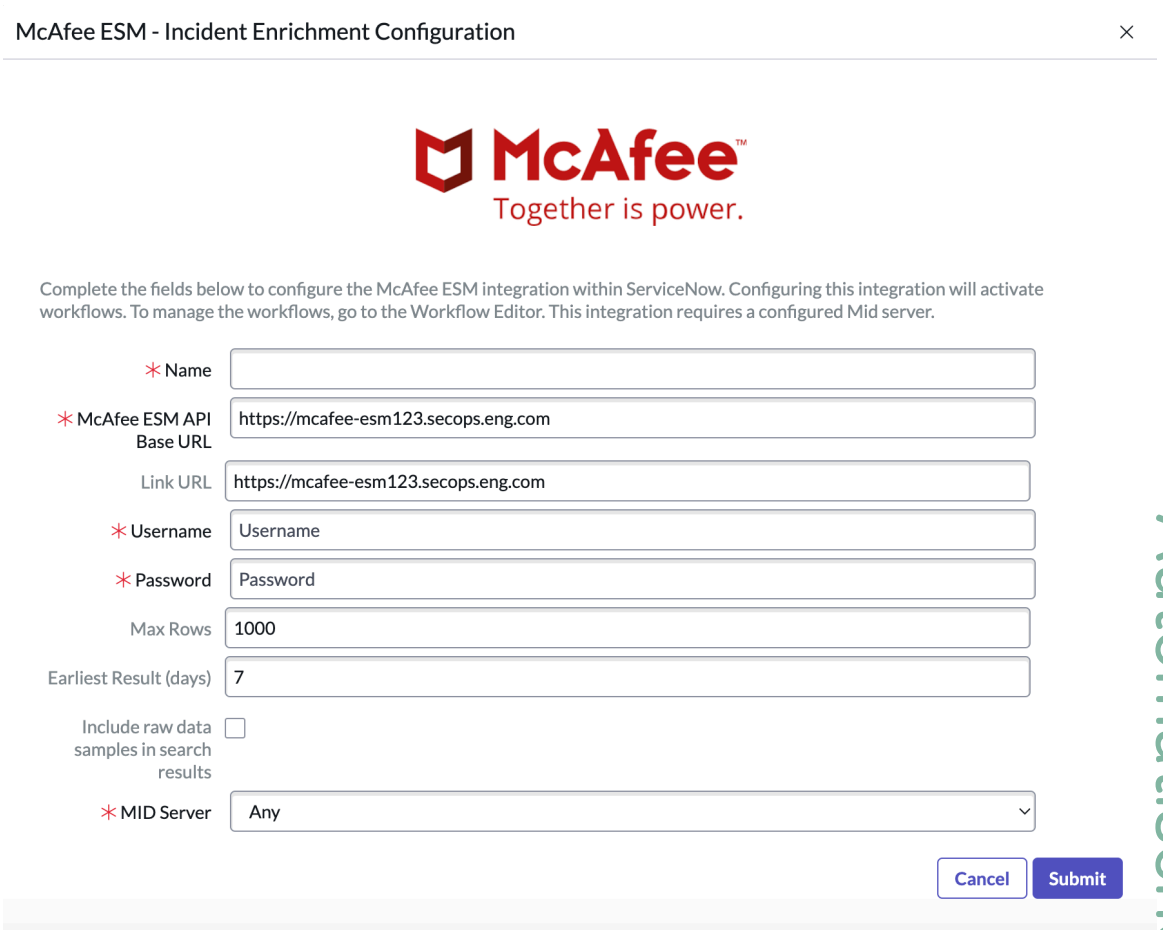
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. In McAfee ESM– Incident-Anreicherungskarte, klicken Sie auf **Neu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Basis-URL der McAfee ESM-API	Die Basis-URL, die Sie von der McAfee ESM-Website erworben haben.
Link-URL	[Optional] die Link-URL, die mit einer McAfee ESM-Instanz verknüpft ist, falls verfügbar. **Hinweis:** Wenn Sie einen Fehler erhalten, verwenden Sie die McAfee ESM API-Basis-URL.
Anwendername	Ihr McAfee ESM-Anwendername.
Passwort	Ihr McAfee ESM-Passwort.
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie in Tagen anzeigen möchten.
Rohdatenmuster in	Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Suchergebnissen berücksichtigen	hängt von Ihrer Einstellung in ab **Anzahl der Zeilen mit Rohdaten** Eigenschaft in Eigenschaften von Security Incident Response .
MID-Server	Wählen Sie Aus **Beliebig** Um einen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Navigieren Sie zum Verwalten der Workflows zu **Workflow-Editor** .

5. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
6. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf klicken **Konfigurieren** Oder **Löschen** Zum Ändern oder Löschen der Konfiguration.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie aus **Nein** Von **Konfigurationen Anzeigen** Dropdown-Liste.

Microsoft Azure Sentinel-Integration

Microsoft Azure Sentinel Ist eine cloudbasierte Lösung für Security Information Event Management (SIEM) und Security Orchestration Automated Response (SOAR). Sie können verwenden Microsoft Azure Sentinel Integration zum Erfassen von Azure Sentinel-Incidents und zum automatischen Erstellen von Security Incidents in Security Incident Response.

Apps im Store anfordern

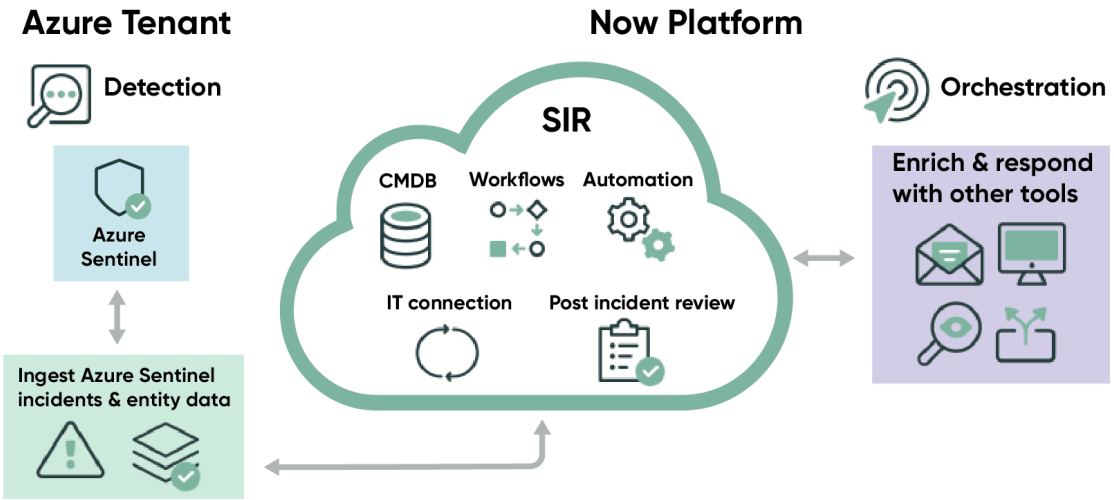
Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht

Im folgenden Diagramm finden Sie weitere Informationen dazu Microsoft Azure Sentinel Ist in integriert ServiceNow AI Platform Security Operations Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Now Platform - Azure Sentinel integration overview



Schlüsselfunktionen

Verwenden Sie die wichtigsten Funktionen dieser Integration, um die folgenden Aktionen auszuführen:

- Erkennen Microsoft Azure Sentinel Incidents, die Kandidaten für Security Incidents sind und die Erstellung dieser Security Incidents automatisieren.
- Zuordnung Microsoft Azure Sentinel Incident- und Entitätsfelder bis SIR Security Incident-Felder.
- Filter Microsoft Azure Sentinel Incidents.
- Aggregieren Sie Incidents mit vorhandenen offenen Security Incidents, damit Sie keine doppelten Security Incidents erstellen müssen.
- Automatisieren Microsoft Azure Sentinel Incident-Statusaktualisierungen für Security Incident Response, damit Sie Security Incidents erstellen und schließen können.

Hinweis:
ServiceNow Aktualisiert den Status von Microsoft Azure Sentinel Incidents basierend auf der Erstellung oder dem Abschluss von Security Incidents. Dieses Update enthält auch Kommentare zu aggregierten Incidents und neuen Incidents.

- Planen Sie die Incident-Erfassung, um regelmäßig Security Incidents zu erstellen.
- Synchronisieren Microsoft Azure Sentinel Incident-Kommentare mit SIR Arbeitsnotizen.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
Microsoft Produktdokumentations-Website	Microsoft-Produktdokumentations-Website
ServiceNow Produktdokumentations-Website	ServiceNow-Produktdokumentationswebsite

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte mit Microsoft Azure Sentinel Integration

Aktivieren und richten Sie ein Microsoft Azure Sentinel – Incident Ingestion Für das Security Operations-Plugin zur Schnittstelle mit Ihrem ServiceNow AI Platform Instanz und Security Incident Response Produkt.

Bevor Sie verwenden können Microsoft Azure Sentinel Integration müssen Sie sie aus herunterladen ServiceNow Store.

Erforderliche Rolle: Microsoft Azure Anwendungsentwickler, Microsoft Azure Mandantenadministrator.

Überprüfen Sie die folgende Setup-Prüfliste, und stellen Sie sicher, dass Sie alle Aufgaben für eine reibungslose Integration abgeschlossen haben.

Prüfliste

Setupaufgabe	Beschreibung
Weisen Sie die erforderlichen zu, und verifizieren Sie sie ServiceNow AI Platform Und Security Incident Response Rollen.	Die folgenden Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Die Administratorrolle installiert die Integration aus dem ServiceNow Store Und weist die Rolle sn_si.ingestion_profile_admin zu. • Die Rolle sn_si.ingestion_profile_admin führt die folgenden Aufgaben aus: ◦ Konfiguriert die Integration. ◦ Erstellt Incident-Profile. ◦ Ordnet zu Microsoft Azure Sentinel Incident-Datenfelder zu Security Incident-Feldern. ◦ Plant die laufende Incident-Erfassung. ◦ Aktiviert Incident-Updates, wenn ein Security Incident Response Incident wird erstellt oder geschlossen. ◦ Weist die Rolle Security Incident Analyst (sn_si.Analyst) zu.
Weisen Sie zu Microsoft Azure Erforderliche Rollen.	Die folgenden Rollen sind in erforderlich Microsoft Azure So registrieren und konfigurieren Sie Ihre Anwendung: • Anwendungsentwickler für die Registrierung der Anwendung. • Mandantenadministrator für die Erteilung von Berechtigungen für die Anwendung durch Aufruf des Endpunkts der Administratoreinwilligung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie diese Integration konfigurieren.	Die ServiceNow IntegrationHub Starterpaket-Installationsprogramm [Plugin com.glide.hub.integrations] ist erforderlich. Die Security Incident Response Plugin (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Anwendungen, die für die Integration erforderlich sind. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn diese Anwendungen noch nicht installiert sind, müssen Sie jede Anwendung einzeln in der folgenden Reihenfolge installieren und aktivieren, um eine reibungslose Installation sicherzustellen: **1.** Security Incident Response **2.** Security Incident Response-Benutzeroberfläche **3.** ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) **4.** ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)
Registrieren und konfigurieren Sie Ihre Anwendung in Microsoft Azure Portal.	Registrieren Sie Ihre Anwendung in Microsoft Azure Portal und gewähren Sie Ihren Anwendern Lese- und Schreibzugriff auf die Anwendung.

Registrieren und konfigurieren Sie Microsoft Azure Portal

Registrieren Sie Ihre Anwendung in Microsoft Azure Portal und gewähren Sie Ihren Anwendern Lese- und Schreibzugriff auf die Anwendung.

Vorbereitungen

Erforderliche Rolle: Microsoft Azure Anwendungsentwickler, Microsoft Azure Mandantenadministrator

Prozedur

1. Melden Sie sich bei an Microsoft Azure Portal.

2. Suchen und wählen Sie aus **App-Registrierungen** .

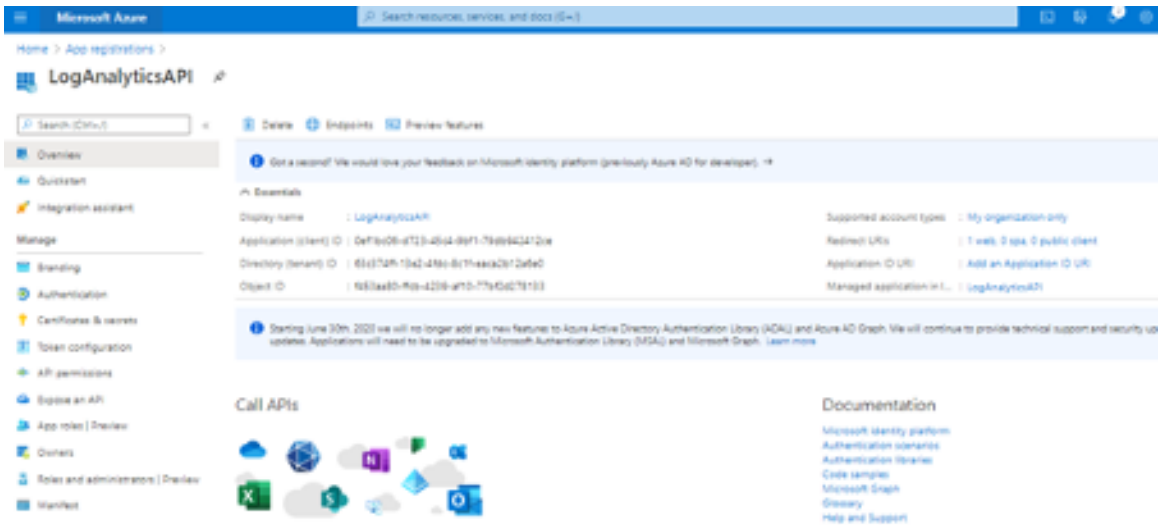
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **New registration (Neue Registrierung)**.
4. Füllen Sie im Formular die Felder aus.

Registrierungsformular für ein Anwendungsformular

Feld	Beschreibung
Name	Anwenderorientierter Anzeigename für die Anwendung. Beispiel: LogAnalyticsAPI.
Unterstützte Account-Typen	Account-Typ, der diese Anwendung verwenden oder auf die API zugreifen kann.
Umleitungs-URI	Umleitungs-URI. Die Authentifizierungsantwort wird nach der erfolgreichen Authentifizierung eines Anwenders an diesen URI weitergeleitet.

5. Klicken Sie auf **registrieren**.
Nachdem Sie die Anwendung erfolgreich registriert haben, wird die Übersichtsseite angezeigt.



6. Navigieren zu **Verwalten** > **Zertifikate und Geheimnisse**an.
7. Klicken Sie im Abschnitt geheime Clientgeheimnisse auf **Neues geheimes Clientgeheimnis** .
Sie können das geheime Clientgeheimnis später nicht anzeigen. Stellen Sie daher sicher, dass Sie das geheime Clientgeheimnis jetzt in diesem Schritt kopieren und speichern. Wenn Sie das geheime Clientgeheimnis vergessen, können Sie ein neues generieren, indem Sie die Anweisungen in den Schritten 4 und 5 befolgen.
8. Navigieren zu **Verwalten** > **API-Berechtigungen**an.
9. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
10. Klicken Sie im Fenster „API-Berechtigungen anfordern“ auf **APIs, die meine Organisation verwendet** Registerkarte.
11. Suchen und auswählen **Log Analytics-API** App-Name.
12. Wählen Sie in den Log Analytics API-Berechtigungen die Option aus **Anwendungsberechtigungen** .
Durch Aktivieren dieser Berechtigung wird sichergestellt, dass die Anwendung als Hintergrundservice oder Daemon ohne angemeldeten Anwender ausgeführt wird.
13. Wählen Sie im Abschnitt Daten die Option aus **Daten.Lesen**
14. Klicken Sie Auf **Fügen Sie Berechtigungen Hinzu** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Berechtigungen werden aktualisiert.

15. Aktivieren Sie **Erteilen Sie die Administratoreinwilligung für das Standardverzeichnis** Option für die Data.Read-API-Berechtigung, die Sie in Schritt 13 aktiviert haben.
16. Suchen und wählen Sie aus **Log Analytics-Arbeitsbereiche** .
17. Wählen Sie Ihren Sentinel Log Analytics-Arbeitsbereich aus.
    Sie sehen jetzt die Übersichtsseite des Sentinel Log Analytics-Arbeitsbereichs.
18. Navigieren zu **Zugriffssteuerung (IAM)** > **Rollenzuweisungen**an.
19. Klicken Sie Auf **Hinzufügen** , Und wählen Sie aus **Fügen Sie Rollenzuweisung hinzu** .
20. Füllen Sie im Formular die Felder aus.

Formular „Rollenzuweisung hinzufügen“

Feld	Beschreibung
Rolle	Account-Typ, der diese Anwendung verwenden kann. Wählen Sie Aus **Azure Sentinel Responder** .
Assign access zu (Zugriff zuweisen an)	Von Ihnen definierter Berechtigungsbereich. Wählen Sie Aus **Anwender** , **Gruppe** , Oder **Service-Prinzipal** .
Auswahlvorgang	Anwendung, die Sie zuvor in Schritt 4 erstellt haben. Beispiel: LogAnalyticsAPI.

21. Klicken Sie auf **Speichern**.

Installieren und konfigurieren Sie Microsoft Azure Sentinel Integration

Installieren und konfigurieren Sie Microsoft Azure Sentinel Integration aus dem ServiceNow Store Auf Ihrem ServiceNow AI Platform Instanz zum Starten der Erfassung von Azure Sentinel-Incidents.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Laden Sie herunter Microsoft Azure Sentinel Integration aus dem ServiceNow Store Und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie nach Microsoft Azure Sentinel Kachel und klicken Sie auf **Konfigurieren** .
4. Füllen Sie im Formular die Felder aus.

Microsoft Azure Sentinel – Formular „Konfiguration der Incident-Erfassung“

Feld	Beschreibung
Name	Name für Microsoft Azure Cloud Instanzkonfiguration.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Identitäts-URL	Identitäts-URL für Microsoft Azure Cloud Mandant. Beispiel: `login.microsoftonline.com` . Weitere Informationen finden Sie unter Microsoft Azure-Dokumentation .
Azure Resource Manager	Azure Resource Manager-Endpunkt für Microsoft Azure Cloud Mandant. Beispiel: `management.azure.com` . Weitere Informationen finden Sie unter Microsoft Azure-Dokumentation .
Mandanten-ID	Microsoft Azure Sentinel Mandanten-ID. Dies ist die Instanz, von der aus alle Incidents in der stammen Microsoft Azure Portal wird abgerufen.
Client-ID	Client-ID für die Anwendung, die Sie in registriert haben Microsoft Azure Portal.
Geheimer Clientschlüssel	Geheimer Clientschlüssel für Ihre registrierte Anwendung.
Abonnement-ID	Abonnement-ID für Ihre registrierte Anwendung.
Ressourcengruppenname	Ressourcengruppenname für Ihre registrierte Anwendung.
Arbeitsbereichsname	Arbeitsbereichsname für Ihre registrierte Anwendung.

5. Klicken Sie auf **Absenden**.

Ergebnisse
Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird jede Konfiguration des Incident-Erfassungsservers auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Erstellen Sie ein Profil für Microsoft Azure Sentinel

Erstellen Sie ein Incident-Profil in Ihrem ServiceNow AI Platform Instanz und bestimmen Sie Microsoft Azure Sentinel Incidents, die zum Erstellen von Security Incidents geeignet sind.

Vorbereitungen
Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird
Mit der Integration können Sie verschiedene Arten von Incidents erstellen, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese Incidents werden basierend auf den Profilen erstellt, die Sie in konfigurieren ServiceNow AI Platform Instanz. Alle Incidents werden anfänglich für einen konfigurierten Incident-Typ in einem Profil erstellt. Erstellte Incidents können dann weiter gefiltert werden, um anzugeben, welche Incidents Security Incidents erstellen.

Alle Incidents, die die Auswahlkriterien in erfüllen Microsoft Azure Mandanten und sind über verfügbar Microsoft Azure Sentinel API, werden anfänglich in erfasst ServiceNow AI Platform Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Microsoft Azure Sentinel-Integration** > **Azure Sentinel-Incident-Profil**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Microsoft Azure Sentinel – Formular „Konfiguration der Incident-Erfassung“

Feld	Beschreibung
Name	Name für das Profil. Dieser Name hilft Ihnen bei der Identifizierung des Profiltyps und ist auch der Standardname für das Sicherheits-Tag, das diesem Profil zugeordnet ist.
Aktiv	Indikator, dass das Profil aktiv ist. Wenn das Profil aktiv ist, bedeutet dies, dass ServiceNow AI Platform Fragt aktiv Azure Sentinel-Incidents ab und stellt fest, dass entsprechende Security Incidents in erstellt werden SIR Wenn die Filterbedingungen erfüllt sind.
Quelle	Microsoft Azure Mandant, den Sie zum Erfassen von Incidents konfiguriert haben. Wenn Sie mehrere Mandanten konfiguriert haben, wählen Sie den entsprechenden Mandanten für die Incident-Typen aus, die Sie für das Profil erfassen möchten.
Reihenfolge	Flow-Priorität. Der Wert für dieses Feld gibt die Reihenfolge an, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen teilen. Der Flow mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Beispiel: 100, 200, 300, 400. Der Standardwert ist 100.
Beschreibung	Zusätzlicher Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

4. Um zum Abschnitt „Zuordnung“ zu wechseln, klicken Sie auf **Fahren Sie Fort** .

Nächste Maßnahme

Einzelperson zuordnen Microsoft Azure Sentinel Incident-Felder zu den Feldern auf der ServiceNow AI Platform SIR Security Incident.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ordnen Sie zu Microsoft Azure Sentinel Incident-Felder

Ordnen Sie die Person zu Microsoft Azure Sentinel Incident-Felder zu den Feldern auf der SIR Security Incident, damit Sie Incidents mit den zugeordneten Daten erstellen können.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

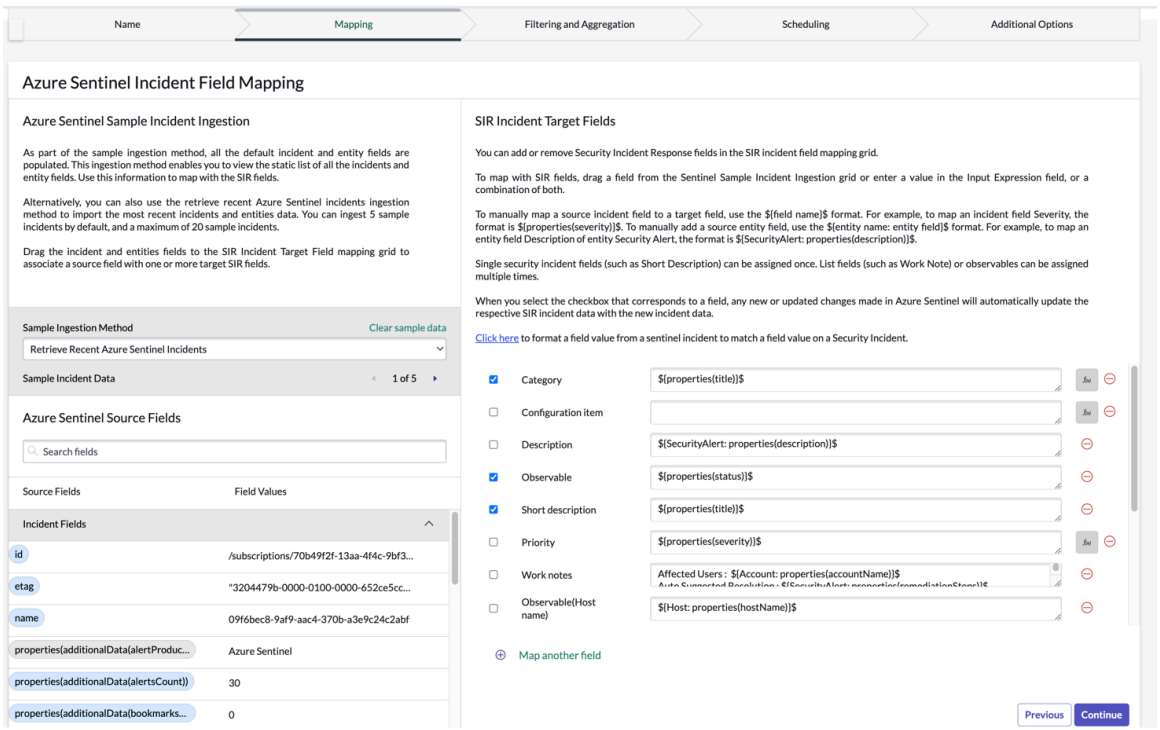
1. Wählen Sie auf der Zuordnungsseite im Abschnitt Azure Sentinel-Feldzuordnung eine der Beispielerfassungsmethoden aus.

Beispiel für Erfassungsmethoden

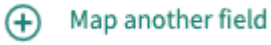
Feld	Beschreibung
Alle Standard-Incident- und Entitätsfelder	Verwenden Sie diese Erfassungsmethode, um die statische Liste aller Incidents und Entitätsfelder anzuzeigen. Diese Methode enthält nur Standardfeldnamen ohne Werte. Sie können diese Informationen verwenden, um eine Zuordnung zu vorzunehmen SIR Felder.
Ruft die letzten Azure Sentinel-Incidents ab	Verwenden Sie diese Erfassungsmethode, um die neuesten Incident- und Entitätsdaten zu importieren. Wenn der Azure Sentinel-Incident die Entitätsdaten enthält, werden die Entitätsdaten abgerufen, und sie sind für die Zuordnung im Abschnitt „Azure Sentinel-Quellfelder“ verfügbar. Manchmal enthält der Azure Sentinel-Incident möglicherweise nicht die Entitätsdaten, daher sind die Entitätsfelder in einem solchen Szenario nicht für die Zuordnung verfügbar. Wenn der Azure Sentinel-Incident mehrere Warnungen enthält, wird die früheste Warnung, die Teil des Incident ist, im Zuordnungsabschnitt angezeigt. Auch während der Erfassung werden die frühesten Feldwerte für Sicherheitswarnungen verwendet. Sie können standardmäßig 5 Beispiel-Incidents und maximal 20 Beispiel-Incidents erfassen. Die Werte des Felds Beispiel-Incident werden ausgefüllt, wenn das Profil die Beispiel-Incidents erfasst. Sie können diese

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Incidents dem zuordnen **SIR-Incident-Zielfelder** . Die Incident-Felder und -Werte werden als einzelne Registerkarten angezeigt.
Importieren Sie Beispieldaten	Klicken Sie Auf **Importieren Sie Beispieldaten** Dient zum Importieren von Beispiel-Incidents aus Azure Sentinel. Diese Schaltfläche wird angezeigt, wenn Sie die Erfassungsmethode Letzte Azure Sentinel-Incidents abrufen auswählen. Beispiel-Incidents werden von abgerufen Microsoft Azure Sentinel Der Server kann einen Moment dauern. Ordnen Sie diese abgerufenen Incidents dem zu **SIR-Incident-Zielfelder** . Die Incident-Felder und -Werte werden als einzelne Registerkarten angezeigt.



2. Führen Sie die folgenden Aktionen aus, um den Standardfeldern, die im Security Incident angezeigt werden, Felder hinzuzufügen:

   a. Klicken Sie im Abschnitt SIR Incident-Zielfelder auf 

   Schaltfläche „weiteres Feld zuordnen“.
   Es wird eine Liste von angezeigt SIR Felder, aus denen Sie ein Feld auswählen können, aus dem ein neues Feld angezeigt werden soll.

   b. Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie dann ein Feld aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Mehrere erkennbare Elemente können für denselben Security Incident angezeigt werden. Zum Beispiel die **Erkennbares Element** Das Feld kann mehrmals verschiedenen Werten zugeordnet werden. Ebenso wird **Konfigurationselement** Und **Felder für Arbeitsnotizen** Unterstützt mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird eine Fehlermeldung angezeigt, dass dieses Feld nicht mehrere Werte unterstützt. Wenn ein Feld in einem Security Incident über eine Liste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

c. Ziehen Sie Ihr Feld im Abschnitt „Azure Sentinel-Quellfelder“ per Drag-and-Drop, um es Ihrem neuen Feld zuzuordnen.

d. Wenn Sie das Kontrollkästchen aktivieren, das einem Feld entspricht, werden bei allen neuen oder aktualisierten Änderungen, die in Azure Sentinel vorgenommen wurden, die entsprechenden SIR-Incident-Daten automatisch mit den neuen Incident-Daten aktualisiert.

Hinweis:
Im Basissystem ist die Systemeigenschaft sn_sec_sentinel.incident_updates standardmäßig auf „wahr“ festgelegt, um zu empfangen Microsoft Azure Sentinel Updates im Zusammenhang mit neuen Warnungen, die mit SIR verknüpft sind.

- Standardmäßig sind die Felder Betroffene Anwender, Konfigurationselemente und erkennbare Elemente aktiviert. Dies bedeutet, dass immer dann, wenn neue erkennbare Elemente oder zugehörige Konfigurationselemente oder betroffene Anwender dem Incident hinzugefügt werden, diese Informationen während dieses Abfrageintervalls automatisch extrahiert und in den entsprechenden zugehörigen Listen in der Security Incident Response (SIR) ausgefüllt werden.
- Für alle anderen Felder müssen Sie das Kontrollkästchen aktivieren, das einem Feld für alle neuen oder aktualisierten Änderungen entspricht, die im Azure Sentinel-Incident-Datensatz in Azure Sentinel vorgenommen wurden. Dadurch werden die entsprechenden SIR-Incident-Daten automatisch mit den neuen Incident-Daten aktualisiert.

Wichtig:
Vor der Auswahl dieser Funktionalität muss eine Sorgfaltspflicht durchgeführt werden, da das Überschreiben der vorhandenen Daten zu instabilen Daten führen kann, mit denen der Analyst arbeiten kann, und jede andere Automatisierung, die auch durch die Feldwerte des Security Incident festgelegt wird, kann ebenfalls betroffen sein. Daher ist es sehr wichtig, die Sorgfaltspflicht durchzuführen, bevor Sie eine Überschreibungsfunktion auswählen.

3. Verwenden Sie zum Entfernen eines Felds Schaltfläche „Element entfernen“ neben dem Eingabeausdrucksfeld im Abschnitt „SIR-Incident-Zielfelder“.

4. Um einen Feldwert aus dem Abschnitt „Azure Sentinel-Quellfelder“ einem Feld im Abschnitt „SIR Incident-Zielfelder“ zuzuordnen, verwenden Sie eine der folgenden Aktionen:

a. Ziehen Sie den Feldnamen (z. B. ID), und legen Sie ihn neben einem Feldnamen in der Spalte SIR Incident-Zielfelder ab.

Sie können einen beliebigen Wert aus dem Abschnitt „Azure Sentinel-Quellfelder“ mit einem Feld im Abschnitt „SIR Incident-Zielfelder“ abgleichen. Felder sind farbcodiert, damit Sie Incident-Felder im Zuordnungsprozess nicht übersehen oder duplizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hellblaue Felder geben an, dass ein Incident-Feld noch nicht ausgewählt und dem Security Incident zugeordnet ist. Möglicherweise möchten Sie ein Feld für eingehende Incidents mehreren Feldern in einem Security Incident zuordnen. Ein graues Feld gibt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Auf diese Weise können Sie visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Incident-Informationen nicht zugeordnet sind.

b. Sie können eine Kombination aus Text und Feld hinzufügen.
Beispiel: `Incident-Name ist ${Name}$` . Hier `Incident-Name ist` Kann während manuell eingegeben werden `${Name}$` Wird aus dem Abschnitt „Azure Sentinel-Quellfelder“ zugeordnet.

c. Sie können ein Quell-Incident- oder Entitätsfeld direkt manuell eingeben und einem Zielfeld zuordnen.

- Um ein Quell-Incident-Feld manuell zuzuordnen, verwenden Sie dasFormat $ {field Name}$. Um beispielsweise ein Incident-Feld mit Schweregrad zuzuordnen, lautet das Format `${properties(severity)}$` .
- Um ein Quellentitätsfeld manuell hinzuzufügen, verwenden Sie `${Entitätsname: Entitätsfeld}$` Format. Um beispielsweise ein Entitätsfeld Beschreibung der Entitätssicherheitswarnung zuzuordnen, lautet das Format `${SecurityAlert: Properties(description)}$` .

Diese Integration klassifiziert bestimmte Untertypen erkennbarer Elemente. Wenn Sie ein Azure Sentinel-Feld dem Feld SIR-erkennbares Element zuordnen, der ServiceNow AI Platform Klassifiziert das erkennbare Element automatisch. Wenn Sie das eingehende erkennbare Azure Sentinel-Element generisch dem erkennbaren Element in zuordnen möchten SIR, Ziehen Sie dann das Feld Azure Sentinel per Drag-and-Drop in das Feld erkennbares Element. Wenn Sie jedoch den Typ des erkennbaren Elements für das eingehende Azure Sentinel-Element in kennen SIR, Und ordnen Sie dann speziell dem zu SIR Typfeld des erkennbaren Elements. Einige Beispiele für bestimmte Typen erkennbarer Elemente in SIR Schließen Sie erkennbares Element (Domänenname), erkennbares Element (E-Mail-Adresse), erkennbares Element (IP-Adresse (V4)) und erkennbares Element (Hostname) ein.

Wenn Ihre eingehenden Azure Sentinel-Felder irgendwelche enthalten MITRE-ATT&CK Informationen, ordnen Sie sie dann zu MITRE-ATT&CK Technikfeld. Stellen Sie sicher, dass das Feld eingehender Azure Sentinel enthält MITRE-ATT&CK Technik-ID oder Technikname.

Manchmal Incident-Feldwerte in Microsoft Azure Sentinel Kann nicht direkt in die Felder des SIR Security Incident übersetzt werden. Für diese Werte können Sie einen Skripteditor verwenden, um Feldwerte für den Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind.

5. Um eine Feldübersetzung für ein neues Feld aus einem Azure-Sentinel-Incident so zu formatieren, dass sie einem Feldwert in einem Security Incident entspricht, klicken Sie auf **Klicken Sie hier** Link in **SIR-Incident-Zielfelder** Header.

6. Klicken Sie auf , um die Felder zu ändern, die die Feldübersetzung unterstützen Symbol für Übersetzung des Skriptformatfelds.
Die Felder, die die Feldübersetzung unterstützen, sind **Kategorie** , **Konfigurationselement** , Und **Priorität** . Klicken Sie beispielsweise auf Symbol neben der Kategorie. Der Skripteditor für Azure Sentinel-Feldübersetzung wird geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Geben Sie alle Änderungen am Skript ein, und klicken Sie auf **Aktualisieren** Um die Änderungen zu speichern und zur Zuordnungsseite zurückzukehren.
   Definieren Sie beispielsweise für Kategorie Folgendes im Skript-Editor:

   ```
   "<Incoming Sentinel Incident Field Value>" : "<Category to assign to the Security Incident>".
   ```

   Diese Zuordnung stellt sicher, dass ein Profil nur konfigurierte Kategorien verwendet.
8. Setzen Sie Ihre Zuordnung fort, indem Sie Feldwerte hinzufügen oder entfernen.
   Sie können dieselben Feldwerte im Generator für Incident-Generierungsbedingungen verwenden, um zusätzliche Kriterien zu definieren, die ein eingehender Incident erfüllen muss, um einen Security Incident zu erstellen.
9. Um zum Abschnitt Filtern und Zusammenfassung zu wechseln, klicken Sie auf **Fahren Sie Fort** .

Nächste Maßnahme

Definieren und legen Sie Filterbedingungen fest, damit Sie angeben können, welche Incidents Security Incidents erstellen sollen. Sie können dieselben Feldwerte (definiert im Abschnitt „Zuordnung“) im Generator für Incident-Generierungsbedingungen (im Abschnitt „Filterung und Zusammenfassung“) verwenden, um zusätzliche Kriterien zu definieren, die ein eingehender Incident erfüllen muss, um einen Security Incident zu erstellen.

Definition von Filter- und Zusammenfassungskriterien

Sie können Filterbedingungen definieren und festlegen, um anzugeben, welche eingehend sind Microsoft Azure Sentinel Incidents müssen Security Incidents erstellen. Sie können auch zusätzliche Incident-Feldkriterien definieren, mit denen ein eingehender Incident an einen offenen Security Incident angehängt werden kann, anstatt einen Incident zu erstellen.

Legen Sie die Filterbedingungen für Security Incidents fest

Legen Sie die Filterbedingungen so fest, dass Security Incidents nur erstellt werden, wenn die Filterbedingungen übereinstimmen.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Diese Art der Filterung hilft Ihnen, Security Incidents zu isolieren und die Anzahl der von Ihnen erstellten Security Incidents zu begrenzen. Wenn Sie zusätzliche Filterkriterien festlegen, werden nur die erforderlichen Incidents erfasst, ohne die Abfrage oder die Konfiguration der ausgelösten Incidents ändern zu müssen.

Prozedur

1. Zum Definieren der Kriterien, die ein eingehender Microsoft Azure Sentinel Incident muss erfüllen, damit ein Security Incident erstellt wird. Wählen Sie aus **Filtern Sie basierend auf Bedingungen** .

   Die Optionen im ersten Feld in den Filterbedingungen entsprechen den Feldern, die im Abschnitt „Azure Sentinel-Incident-Erfassung“ für den von Ihnen erfassten Incident angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach Incident, den Sie erfassen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Überprüfen Sie, ob die von Ihnen definierten Kriterien den Werten des Incident entsprechen.

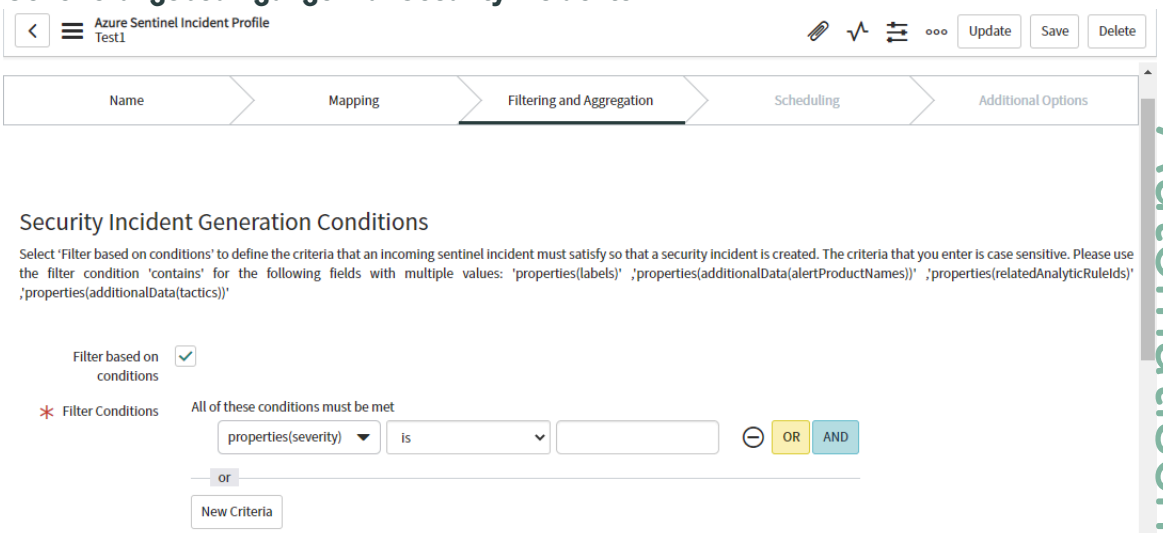
   Verwenden Sie die Filterbedingung *`Enthält`* Für die folgenden Felder mit mehreren Werten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- properties(labels)
- properties(additionalData(alertProductNames))
- properties(relatedAnalyticRuleIds)
- properties(additionalData(tactics))

Da die Filterbedingung nur Zeichenfolgen abrufen kann, müssen Sie verwenden *Enthält* Filterbedingung für die obigen Felder, um sicherzustellen, dass die Daten korrekt gefiltert werden.

Generierungsbedingungen für Security Incidents



2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER** .
   - Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden.
4. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien** .

Definieren Sie Zusammenfassungsbedingungen

Definieren Sie zusätzliche Incident-Zusammenfassungskriterien, die einen eingehenden Incident zu einem vorhandenen SIR Security Incident aggregieren, anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Wenn Sie Feldübereinstimmungswertkriterien für jedes Profil verwenden, kann diese zusätzliche Zusammenfassung die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Incident-Daten in einem einzelnen Security Incident platziert werden.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein neuer Incident allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird der Incident automatisch dem zuletzt geöffneten Security

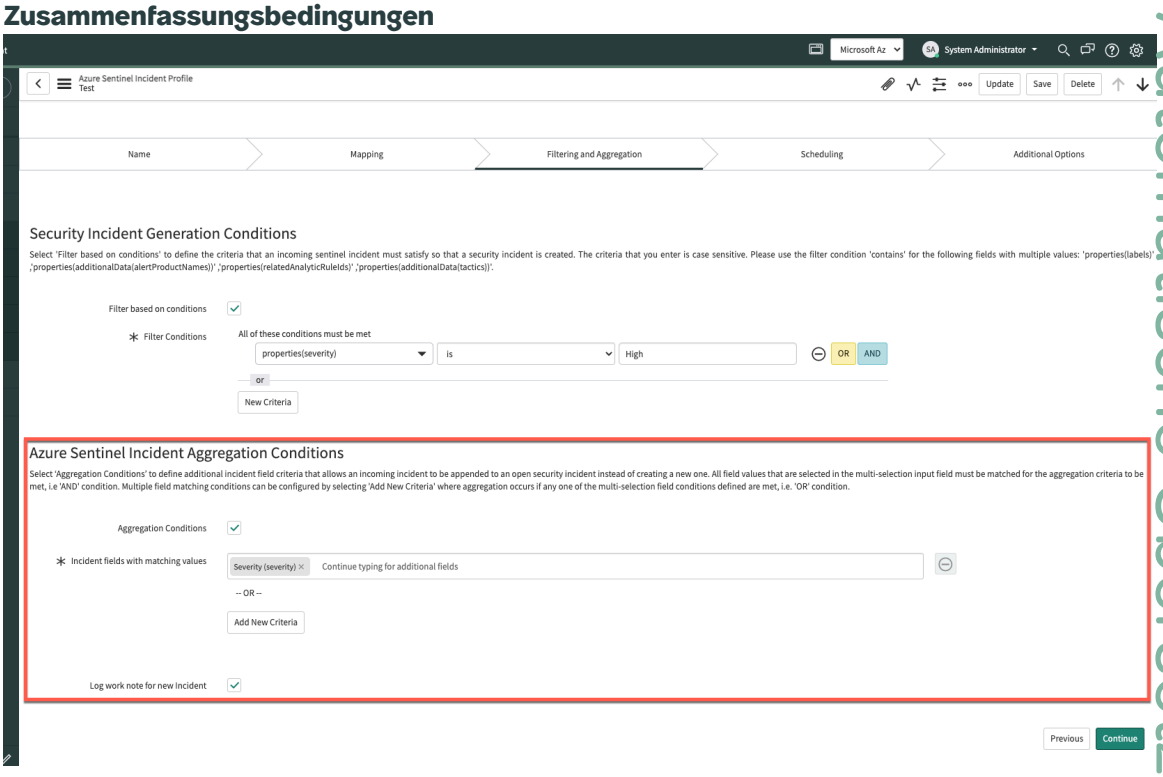
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incident mit denselben Feldwerten hinzugefügt. Als Anwender mit der Rolle „sn_si.Analyst“, der mit Security Incidents arbeitet, können Sie alle hinzugefügten aggregierten Incidents in einer zugehörigen Liste zu einem Security Incident anzeigen.
Alle aggregierten Incidents für einen Security Incident werden in der zugehörigen Liste „aggregierte Incidents“ von Azure Sentinel angezeigt. Diese Liste enthält Details zu den zugehörigen Zeitstempeln und aggregierten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum Incidents zu den vorhandenen Security Incidents hinzugefügt werden.

Prozedur

1. Zum Definieren zusätzlicher Incident-Feldkriterien, die eingehende zulassen Microsoft Azure Sentinel Incident, der an einen offenen Security Incident angehängt werden soll, anstatt einen neuen Incident zu erstellen, wählen Sie aus **Zusammenfassungsbedingungen** Option wie in der folgenden Abbildung gezeigt.



2. In **Incident-Felder mit übereinstimmenden Werten** Geben Sie die Feldwerte ein, die Sie für vorhandene Security Incidents in abgleichen möchten ServiceNow AI Platform Instanz.
Alle Feldwerte, die Sie im Eingabefeld für die Mehrfachauswahl ausgewählt haben, müssen übereinstimmen, damit die Zusammenfassungskriterien erfüllt sind und dieser eingehende Incident an einen vorhandenen Security Incident angehängt werden kann. Diese Auswahl impliziert dass es sich um einen handelt *UND* Bedingung, unter der ihnen Felder wie erkennbare Elemente und Konfigurationselemente zugeordnet werden, die mehrere Feldwerte haben können. Wenn nur eine Teilmenge der Werte übereinstimmt, werden die Zusammenfassungsbedingungen für Azure Sentinel-Incidents nicht erfüllt, und ein neuer Security Incident wird erstellt.
3. Um mehrere übereinstimmende Feldbedingungen hinzuzufügen, klicken Sie auf **Fügen Sie Neue Kriterien Hinzu**
Die Zusammenfassung erfolgt, wenn eine der von Ihnen definierten Bedingungen für Mehrfachauswahlfelder erfüllt ist. Diese Auswahl impliziert *ODER* Bedingung.
4. Um die Arbeitsnotiz für einen neuen Incident zu aktualisieren, wenn er einem Security Incident hinzugefügt wird, wählen Sie aus **Arbeitsnotiz für neuen Incident protokollieren** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Arbeitsnotiz protokolliert, dass ein neuer Incident hinzugefügt wird, und enthält einen Link zu den Incident-Details. Die Protokoll-Arbeitsnotiz aktualisiert auch weitere Details, die Sie dem Feld Arbeitsnotiz in Ihrem Zuordnungsabschnitt hinzufügen.

5. Klicken Sie auf, um den Zeitplan zu konfigurieren **Fahren Sie Fort** .

Nächste Maßnahme
Legen Sie einen Zeitplan fest, um die Incident-Daten und erfassten Incidents abzurufen, die den Kriterien im Profil entsprechen.

Planen Sie Microsoft Azure Sentinel Incident-Abruf

Legen Sie einen Zeitplan fest, um die Incident-Daten abzurufen und zu erfassen Microsoft Azure Sentinel Incidents, die den Kriterien im Profil entsprechen.

Vorbereitungen
Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird
Sie können planen, wie oft Sie in der Zukunft abfragen möchten Microsoft Azure Sentinel Incidents, die der Incident-Profilkonfiguration entsprechen.

Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Planung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Aktivieren Sie , um ein bestimmtes Datum und eine bestimmte Uhrzeit für die anfängliche Erfassung zu definieren **Legen Sie die Incident-Erfassungszeit fest** . Die nachfolgende Erfassung basiert auf dem Abfrageintervall-Zeitraum.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die verschiedenen Abfrageintervalle können sich auf die Leistung von auswirken Microsoft Azure Sentinel Incident-Integration. Planen Sie bei der Planung, dass die Systemlast gegen die Dringlichkeit eines Incident ausgeglichen wird. Für alle Profile ist ein einminütiger Standardwert festgelegt. Sie können diese Einstellung basierend auf der Dringlichkeit des Incident und der erwarteten Belastung Ihres Systems ändern.

Alle Warnungen, die dem Incident in einem bestimmten Abfrageintervall hinzugefügt werden, werden ausgeführt und dann an die zugehörigen Listen mit Azure Sentinel-Warnungen angehängt, und Arbeitsnotizen werden ebenfalls veröffentlicht.

Prozedur

1. Füllen Sie die Felder im Planungsformular aus.

   Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Incidents aus abrufen Microsoft Azure Mandant.

Zeitplanungsformular

Feld	Beschreibung
Fortlaufende Incident-Erfassung	Laufende Incident-Erfassung, die der ServiceNow AI Platform Instanz ruft aus ab Microsoft Azure Mandant für neue Incidents. Security Incidents werden erstellt, wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	ausgelöste Incidents gefunden werden und die Filterkriterien für die Incident-Generierung erfüllt sind.
Abfrageschritt (Minuten)	Abfragehäufigkeit, die in Minuten definiert ist.
Incident-Erfassungszeit festlegen	Incident-Erfassung, die auf dem konfigurierten Datum und der konfigurierten Uhrzeit basiert. Sie können diese Option verwenden, um ein bestimmtes Datum und eine bestimmte Uhrzeit für die anfängliche Erfassung zu definieren. Nachfolgende Erfassungen basieren auf dem Abfrageintervall-Zeitraum.
Eingabe Incident-Erfassungszeit	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben.
Einmaliger Abruf	Aktivieren Sie dieses Kontrollkästchen, um den einmaligen Abruf historischer Azure Sentinel-Incidents zu ermöglichen und dann den Abgleich der Daten durchzuführen. Wenn Sie diesen Checkkox auswählen, ruft die Anwendung alle offenen und geschlossenen Azure Sentinel-Incidents für den Zeitraum von ungefähr 6 Monaten ab. Bei der Verarbeitung der Daten werden sowohl laufende Incidents als auch Verlaufsdaten abgerufen, aber die Verarbeitung der laufenden Incidents hat Vorrang vor dem historischen Abruf, und andernfalls kann der historische Abruf einige Zeit in Anspruch nehmen, je nachdem, wie lange Sie die Incidents erfassen. **Hinweis:** Die abgerufenen historischen Azure Sentinel-Incidents werden Deduplizierungsprüfungen unterzogen, um Duplikate in der Anwendung „Security Incident Response“ zu verhindern.
Seit Datum	Das Datum, seit dem die historischen Incidents aus Azure Sentinel erfasst werden. **Hinweis:** Die Incident-Daten werden ungefähr aus den letzten 6 Monaten abgerufen.

Auf der Planungsseite können Sie definieren, wie und wann Incidents aus abgerufen werden Microsoft Azure Mandant.

2. Um zur Seite „zusätzliche Optionen“ zu navigieren, klicken Sie auf **Fahren Sie Fort** .

Automatisieren Sie die Incident-Updates und -Abschlüsse durch SIR Incident-Status

Automatisieren Sie die Incident-Updates und -Abschlüsse durch SIR Incident-Status. Die Microsoft Azure Sentinel Die Integration verfügt über eine bidirektionale Schnittstelle,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die es beiden Incidents ermöglicht, Security Incidents zu erstellen und die Incidents zu aktualisieren, nachdem der Security Incident erstellt oder geschlossen wurde.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Tragen Sie die Details in das Formular ein.
   Befolgen Sie die Anweisungen, um die Konfiguration zum Aktualisieren von Incidents abzuschließen, wenn Sie einen Security Incident in erstellen oder schließen SIR.

Formular „Automatisieren von Incident-Updates“

Kategorie	Feld	Beschreibung
Aktualisierungen der Incident-Erstellung	Aktualisieren Sie den Status von Azure Sentinel-Incidents bei der SIR-Incident-Erstellung	Option, mit der Sie die automatisierte Incident-Update-Funktionalität verwenden können. Die Microsoft Azure Sentinel Incident-Status wird in aktualisiert Microsoft Azure Incident mit den Kommentaren nach SIR Incident wird in erstellt ServiceNow AI Platform.
	Anfangsstatusaktualisierung für Incident	Anfänglicher Incident-Status, der in aktualisiert wird Microsoft Azure Sentinel Umgebung. Sie können auswählen **Neu** Oder **Aktiv** Als Status.
	Anfangskommentare, die an den Incident zurückgesendet werden	Erste Kommentare, die in dem Incident veröffentlicht werden Microsoft Azure Sentinel Umgebung. Bearbeiten Sie den Standardtext, der im Kommentarabschnitt angezeigt wird, indem Sie die Ersetzungsvariablenim Format $ {field Name}$ für ein beliebiges Feld in hinzufügen oder ändern SIR Incident-Formular.
Updates zum Incident-Abschluss	Schließen Sie Azure Sentinel-Incidents nach SIR-Incident-Abschluss	Option, mit der Sie die automatisierte Funktionalität zur Statusaktualisierung von Incidents verwenden können. Microsoft Azure Sentinel Incidents werden in geschlossen Microsoft Azure Incident mit den Kommentaren nach SIR Incident wird in geschlossen ServiceNow AI Platform.
	Statusaktualisierung für Abschluss-Incident	Statusaktualisierung in Microsoft Azure Sentinel Incident, wenn der Incident in geschlossen wird SIR.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

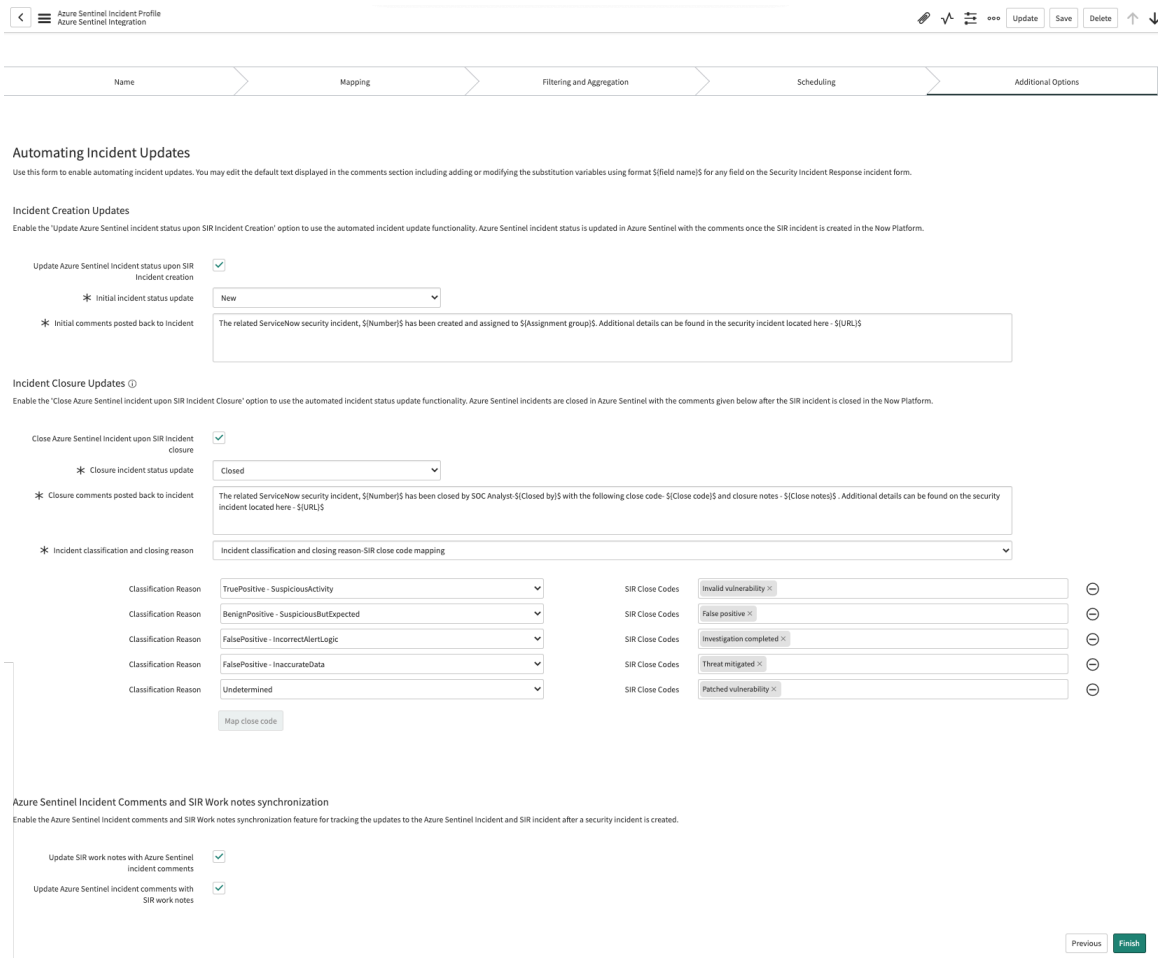
Kategorie	Feld	Beschreibung
	Abschlusskommentare, die an den Incident zurückgesendet wurden	Kommentare, die in dem Incident veröffentlicht werden Microsoft Azure Sentinel Incident, wenn der Incident in geschlossen wird SIR. Bearbeiten Sie den Standardtext, der im Kommentarabschnitt angezeigt wird, indem Sie die Ersetzungsvariablenim Format $ {field Name}$ für ein beliebiges Feld in hinzufügen oder ändern SIR Incident-Formular.
	Incident-Klassifizierung und Abschlussgrund	Methode für die Incident-Klassifizierung und den Abschlussgrund, die zum Schließen des Incident in verwendet wird Microsoft Azure Sentinel Umgebung. Wählen Sie aus **Standardmäßige Incident-Klassifizierung und Abschlussgrund** Methode zum Schließen des Incident in Microsoft Azure Sentinel Umgebung. Wenn Sie diese Methode auswählen, müssen Sie definieren **Standardmäßige Incident-Klassifizierung und Abschlussgrund** . Wenn Sie einen Incident in SIR schließen, wird der Incident-Status in Azure Sentinel auch mit dem angegebenen geschlossen **Standardmäßige Incident-Klassifizierung und Abschlussgrund** . Wählen Sie aus **Incident-Klassifizierung und Abschlussgrund – SIR-Abschlusscodezuordnung** Methode zum Schließen der Incidents und zum Zuordnen der Klassifizierungsgründe zu SIR Abschlusscodes. Sie können mehrere zuordnen SIR Schließen Sie Codes für einen einzelnen Klassifizierungsgrund. Nachdem Sie einen Incident in geschlossen haben SIR Mit dem Abschlusscode wird der Incident-Status in Azure Sentinel auch mit der zugeordneten Incident-Klassifizierung und dem Abschlussgrund geschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Feld	Beschreibung
		Wenn der Klassifizierungsgrund und SIR Abschlusscodes werden nicht zugeordnet, oder es wurde keine Übereinstimmung gefunden. Dann wird der Incident mit dem Standardklassifizierungsgrund „Unbestimmt“ in geschlossen Microsoft Azure Sentinel Umgebung.
Synchronisierung von Azure Sentinel-Incident-Kommentaren und SIR-Arbeitsnotizen	SIR-Arbeitsnotizen mit Azure Sentinel-Incident-Kommentaren aktualisieren	Option, die Sie auswählen können, um Ihren zu aktualisieren Microsoft Azure Sentinel Kommentare in SIR Arbeitsnotizen. Der Kommentar in SIR Arbeitsnotizen werden mit dem Präfix angezeigt *`Kommentar von Sentinel`* . Der Kommentar enthält auch die Sentinel-ID, Analystendetails und den Zeitstempel.
	Azure Sentinel-Incident-Kommentare mit SIR-Arbeitsnotizen aktualisieren	Option, die Sie auswählen können, um Ihren zu aktualisieren SIR Arbeitsnotizen in Microsoft Azure Sentinel Incident-Kommentare. Der Kommentar in Microsoft Azure Sentinel Wird mit dem Präfix angezeigt *`Kommentar von ServiceNow`* .

Das folgende Beispiel zeigt die Konfigurationsoptionen, die für die Automatisierung von Incident-Updates verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Klicken Sie auf **Fertigstellen**.

Nächste Maßnahme

Das Profil wechselt in den Status „Warten“. Wenn die Bestätigungsnachricht anzeigt, dass das Setup und die Konfiguration abgeschlossen sind, können Sie das Profil aktivieren.

Kopieren Sie ein Microsoft Azure Sentinel Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt ein Profil zu erstellen. Wenn Sie mehrere Profile erstellen, können Sie die Einstellungen eines vorhandenen Profils wiederverwenden, indem Sie diese Profile kopieren.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:

Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

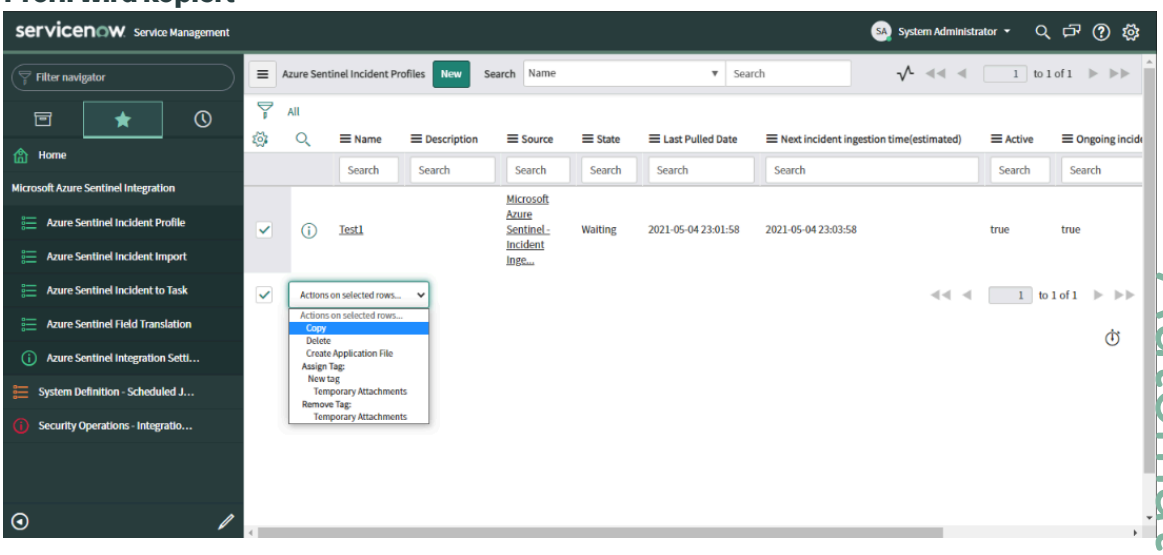
Wenn Sie ein Profil kopieren, wird der Profilname anfänglich geändert, um zu vermeiden, dass doppelte Profile erstellt werden. Das kopierte Profil ist ebenfalls deaktiviert (auf „falsch“ festgelegt), um sicherzustellen, dass Sie es nicht versehentlich aktivieren, bevor Sie die Konfiguration abgeschlossen haben. Sie können die Profile kopieren und vorhandene Zuordnungen für Security Incidents verwenden, die Sie bereits in der Vorschau angezeigt und verifiziert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

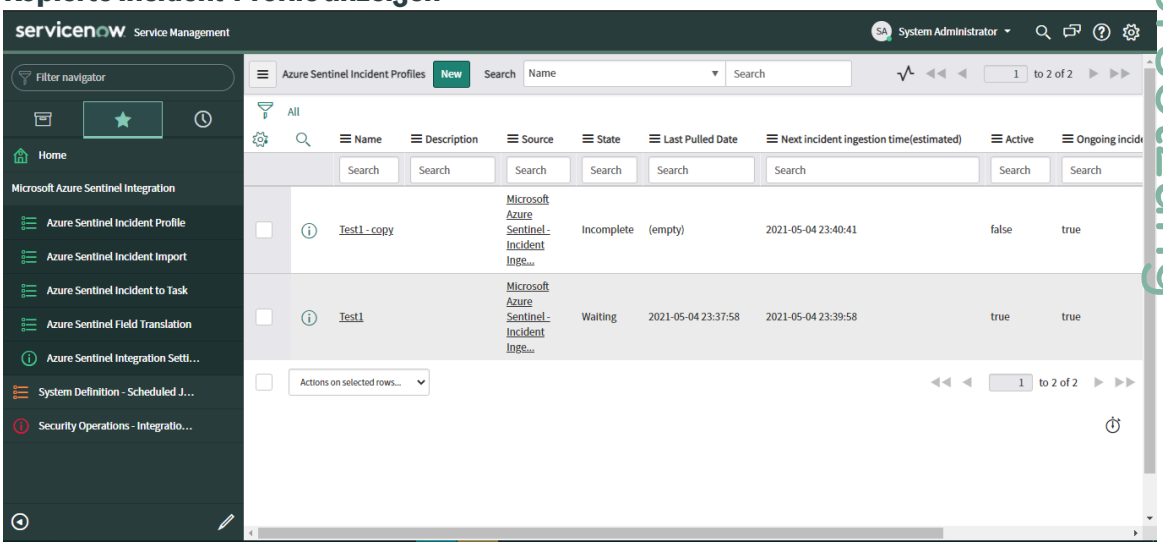
1. Navigieren zu **Alle** > **Microsoft Azure Sentinel-Integration** > **Azure Sentinel-Profil**an.
2. Wählen Sie in der Liste Azure Sentinel-Profile ein Profil aus, das Sie kopieren möchten, und klicken Sie dann in der Liste Aktionen für ausgewählte Zeilen auf **Kopieren** Wie im folgenden Beispiel gezeigt.

Profil wird kopiert



Das Profil wird kopiert und in der Liste angezeigt, wie im folgenden Beispiel gezeigt. Die Kopie verfügt über alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält das Wort „Kopieren“. Obwohl das ursprüngliche Profil aktiviert ist (wahr), wird die Kopie zu diesem Zeitpunkt deaktiviert (falsch). Möglicherweise möchten Sie Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf für das neue Profil gelten.

Kopierte Incident-Profile anzeigen



Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Der Spaltenstatus „aktiv“ wird auf „falsch“ festgelegt, was bedeutet, dass das Profil aktiviert werden muss.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

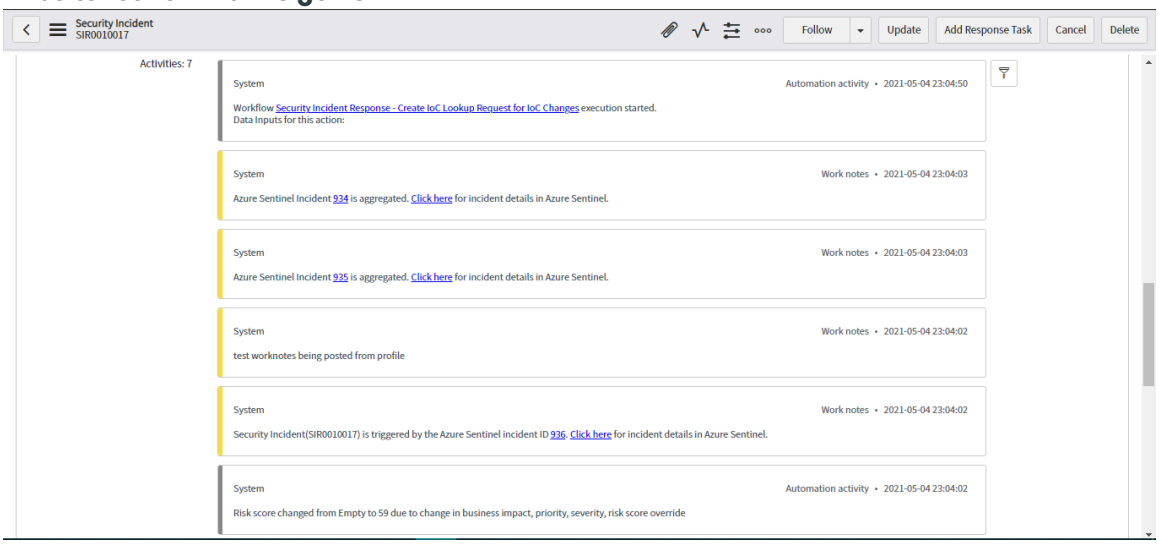
SIR Formular nach der Incident-Erfassung

Nach ServiceNow AI Platform Erfasst Microsoft Azure Sentinel Incident wird ein Security Incident erstellt, und die Aktualisierungen werden an diesem Security Incident-Datensatz vorgenommen.

Arbeitsnotizen

Eine Arbeitsnotiz wird veröffentlicht, wenn ein Incident aggregiert wird und Sie konfiguriert haben **Arbeitsnotiz für neuen Incident protokollieren** Option in Incident-Zusammenfassungskriterien . Das folgende Beispiel zeigt die Arbeitsnotizen in SIR.

Arbeitsnotizen in anzeigen SIR



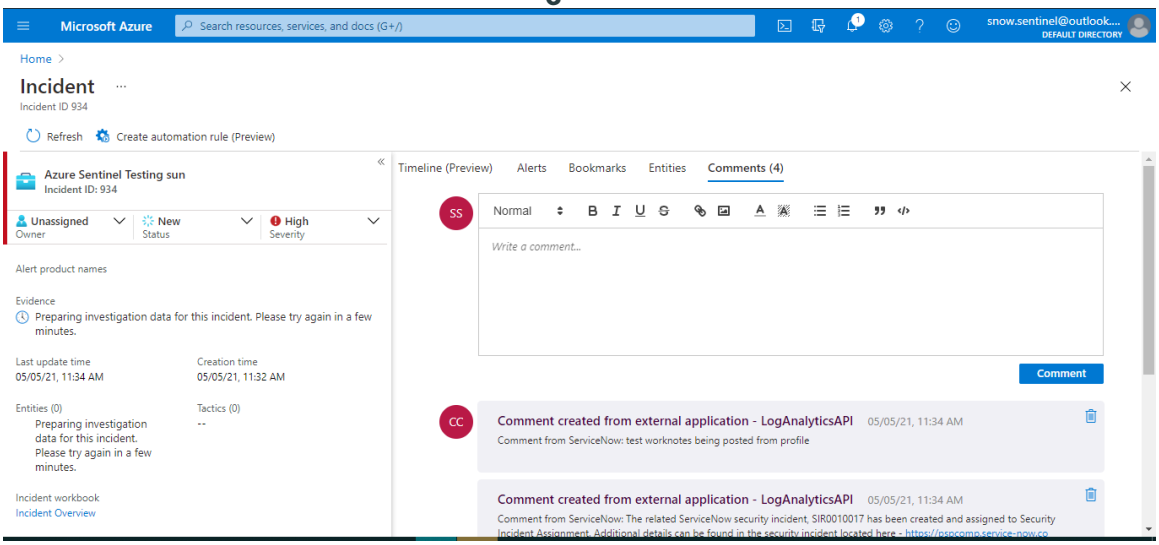
Wenn Sie auf die Incident-Nummer klicken, können Sie den internen Incident-Importdatensatz anzeigen, der die Incident-Rohdaten enthält. Das folgende Beispiel zeigt die Incident-Rohdaten in SIR.

Incident-Rohdaten in anzeigen SIR

Wenn Sie auf klicken **Klicken Sie hier** Link, können Sie den Datensatz in anzeigen Microsoft Azure Sentinel Umgebung. Das folgende Beispiel zeigt den Datensatz in Microsoft Azure Sentinel Umgebung.

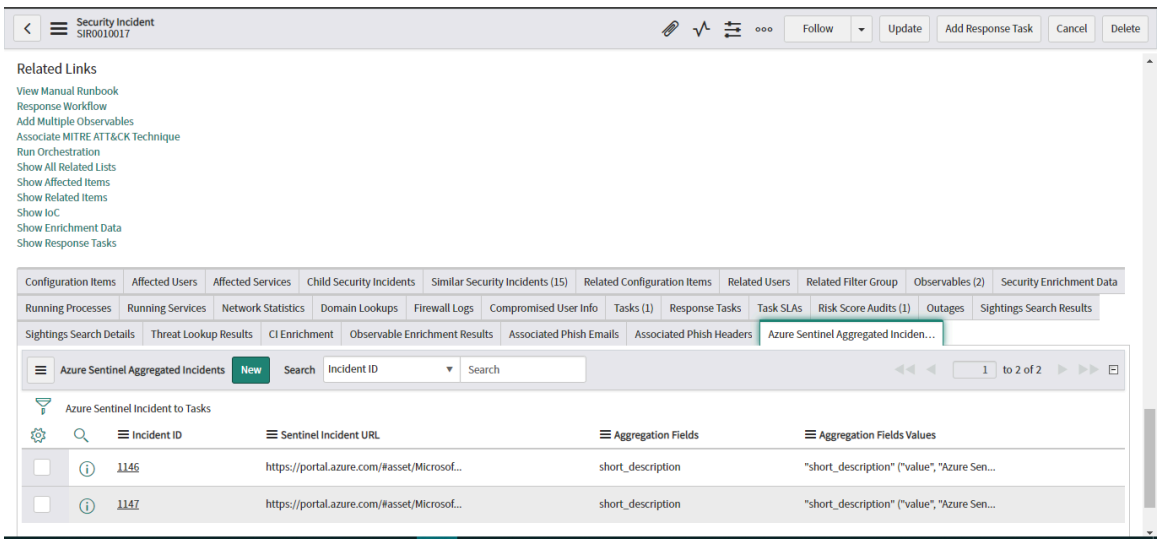
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incident-Datensatz in Azure Sentinel anzeigen



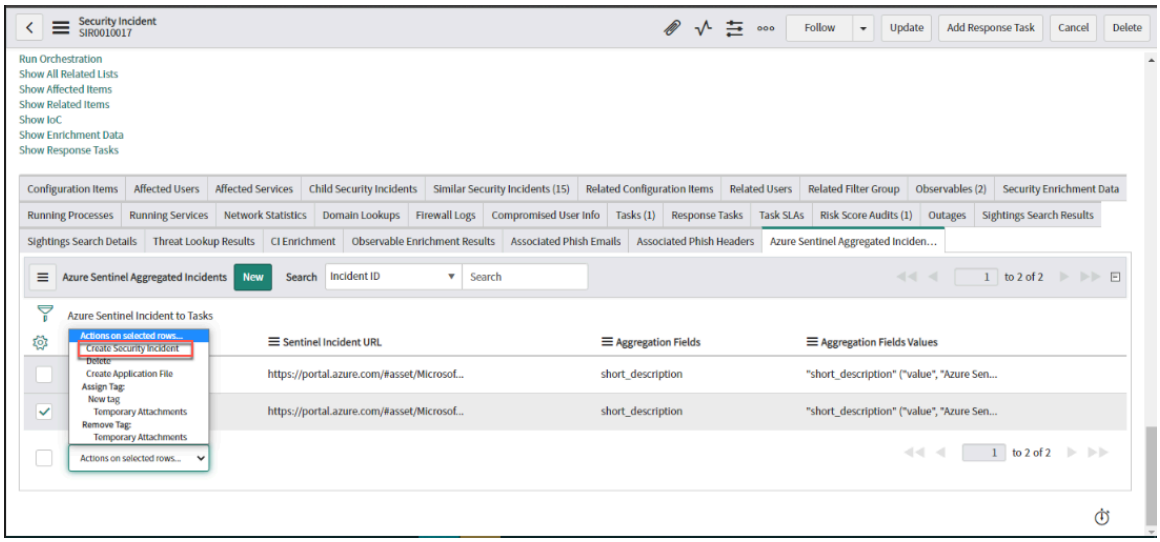
Aggregierte Sentinel-Incidents

Aggregierte Sentinel-Incidents Anzeigen: Zeigen Sie die Incidents an, die zum Security Incident aggregiert sind. Navigieren zu **Alle zugehörigen Listen anzeigen** > **Zusammengefasste Microsoft Azure Sentinel-Incidents**an.



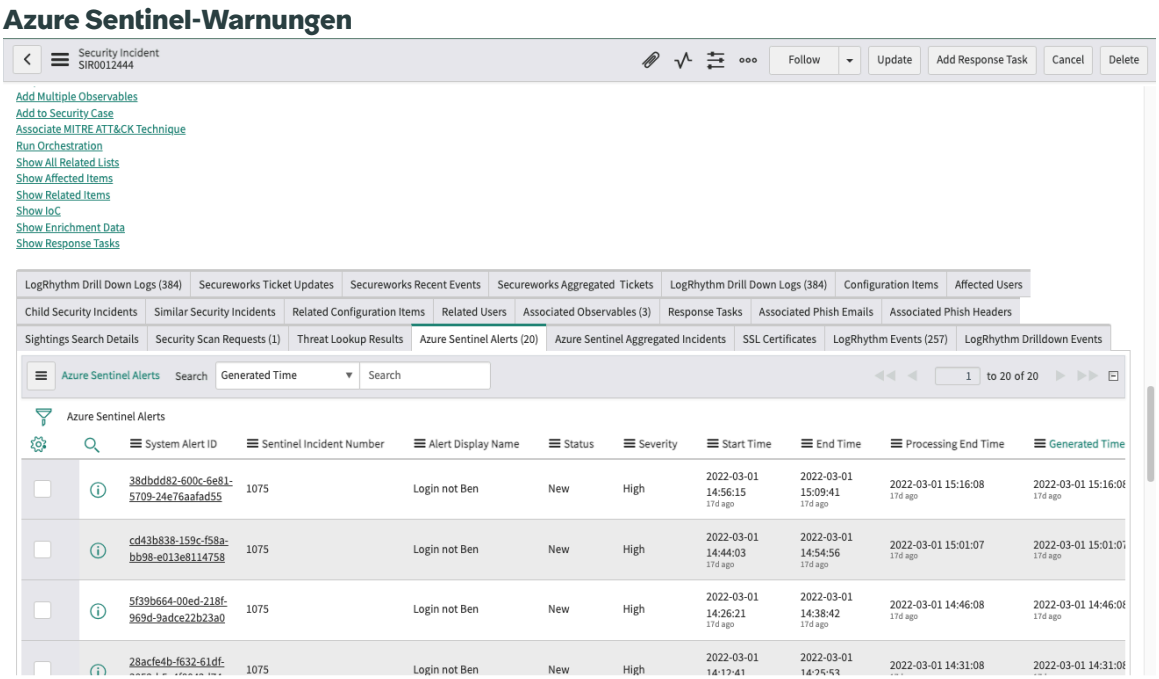
Security Incident erstellen: Wählen Sie einen Incident aus der Liste aus, und klicken Sie auf **Aktionen** Und klicken Sie dann auf **Erstellen Sie einen Security Incident** . Mit dieser Option wird ein neuer Security Incident für den Incident erstellt, und dieser Incident wird vom übergeordneten Security Incident deaggregiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Azure Sentinel-Warnungen

Um die Warnungen anzuzeigen, die dem Sentinel-Incident zugeordnet sind, der den Security Incident ausgelöst hat, navigieren Sie zu **Alle zugehörigen Listen anzeigen** > **Azure Sentinel-Warnungen**an.



Überprüfen Sie Microsoft Azure Sentinel Integrationseinstellungen

Überprüfen Sie Microsoft Azure Sentinel Integrationseinstellungen, damit Sie die Systemeigenschaften an Ihre Umgebung anpassen können.

Vorbereitungen
Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Microsoft Azure Sentinel-Integration** > **Azure Sentinel-Integration: Einstellungen**an.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.

Microsoft Azure Sentinel Integrationseinstellungen

Eigenschaftsname	Beschreibung
Erzwingen Sie einen Grenzwert für die Anzahl der Tage, für die Beispieldaten abgerufen werden können. sn_sec_sentinel.max_num_of_days_for_sample_data	Maximale Anzahl von Tagen, für die Sie Beispieldaten aus abrufen können Microsoft Azure Sentinel Umgebung. Typ: Ganzzahl Standardwert: 7
Erhalten Sie Updates im Zusammenhang mit neuen Warnungen, die mit SIR verknüpft sind. sn_sec_sentinel.incident_updates	Aktivieren Sie die Option, um Incident-Updates zu erhalten. Typ: Boolesch Standardwert: True
Das Trennzeichen, in das die Werte aufgeteilt werden sollen Microsoft Azure Sentinel Feldzuordnungen. sn_sec_sentinel.delimiter	Das Trennzeichen, in das die Werte aufgeteilt werden sollen Microsoft Azure Sentinel Feldzuordnungen. Typ: Zeichenfolge Standardwert: „, “ (Komma mit Leerzeichen)
Erzwingen Sie einen Grenzwert für die Anzahl der Beispielincidents, die abgerufen werden können. sn_sec_sentinel.max_num_of_sample_Incident_per_call	Maximale Anzahl von Beispielincidents, die Sie aus abrufen Microsoft Azure Sentinel Umgebung für Erfassung. Typ: Ganzzahl Standardwert: 5 Beispiel-Höchstwert: 20
Erzwingen Sie einen Grenzwert für die Anzahl der Sentinel-Incidents, die zu einem einzelnen Incident zusammengefasst werden können. sn_sec_sentinel.max_aggregations_per_si	Incident-Zusammenfassungslimit für einen Security Incident. Wenn beispielsweise 102 Incidents vorhanden sind, werden die ersten 100 zu Security Incident_1 und die verbleibenden 2 zu Security Incident_2 aggregiert. Typ: Ganzzahl Standardwert: 100

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftsname	Beschreibung
Erzwingen Sie einen Grenzwert für die Anzahl der Security Incidents, die innerhalb von 24 Stunden erstellt werden können. sn_sec_sentinel.max_si_per_day	Maximale Anzahl von Security Incidents, die innerhalb von 24 Stunden in erstellt werden können ServiceNow AI Platform. Typ: Ganzzahl Standardwert: 1000
Maximaler Paginierungsgrenzwert für das Abrufen der Incident-Daten in einem REST-Aufruf. sn_sec_sentinel.max_page_size	Paginierungsgrenzwert zum Abrufen der Incident-Daten in einem REST-Aufruf von Microsoft Azure Sentinel Umgebung. Typ: Ganzzahl Standardwert: 100
API-Versionswert für Incidents. sn_sec_sentinel.sentinel_security_incident_api_version	Die Microsoft API-Version zum Abrufen von Sentinel-Incidents. Standardwert: 2021-10-01
API-Versionswert für Warnungen. sn_sec_sentinel.sentinel_security_alert_api_version	Die Microsoft API-Version zum Abrufen von Sentinel-Warnungen. Standardwert: 2021-10-01
API-Versionswert für Entitäten. sn_sec_sentinel.sentinel_security_entities_api_version	Die Microsoft API-Version zum Abrufen von Sentinel-Entitäten. Standardwert: 2021-10-01
sn_sec_sentinel.Logging.verbosity	Die Protokollausführlichkeitsstufe der Anwendung, d. h. der Name des Informationstyps. Sie können den Wert auch auf die folgenden Optionen aktualisieren: ○ **Fehler** ○ **warnen** ○ **Info** ○ **debuggen** Standardwert: **Info** .

3. Klicken Sie auf **Speichern**.
   Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

Domänentrennung

Domänentrennung wird für diese Anwendung unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Funktionsweise der Domänentrennung in Microsoft Azure Sentinel Integration

Führen Sie die folgenden Schritte aus, um die Domänentrennung zu erreichen:

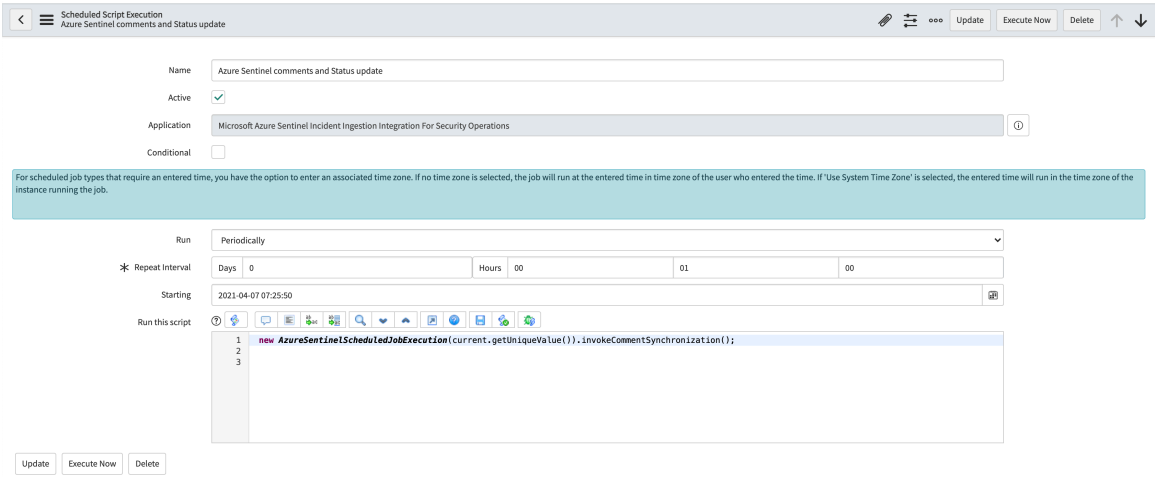
- Erstellen Sie einen Anwender mit der Rolle sn_si.admin in der jeweiligen Domäne.

> **Hinweis:**
> Wenn Sie das Profil erstellen, verwenden Sie die Domänenauswahl, um eine Domäne auszuwählen. Erstellen Sie den Anwender nicht in der übergeordneten Domäne, und ändern Sie später die Domäne des Profils. Sie sollten für jede Domäne für Ihr Profil einen Anwender mit der Rolle „sn_si.admin“ haben. Verwenden Sie diesen Anwender, um Einstellungen im Profil zu erstellen oder zu ändern.

- Deaktivieren Sie vorhandene geplante Aufgaben.
- Replizieren Sie die folgenden geplanten Aufgaben für jede Domäne:
  - Azure Sentinel Ruft Warnungen Und Entitäten Ab
  - Synchronisierung Von Azure Sentinel-Kommentaren
  - Azure Sentinel-Statusaktualisierung
  - Azure Sentinel – Profilprozess
  - Azure Sentinel – Prozessrohdaten
  - Azure Sentinel-Datenbereinigung
  - Azure Sentinel – Verlaufskommentar Abrufen
- Ändern Sie **Ausführen als** Vom Systemanwender zum Anwender mit der Rolle „sn_si.admin“ in der jeweiligen Domäne, und führen Sie dann die geplante Aufgabe aus.

Das folgende Beispiel zeigt, wie Sie den Auftrag „Azure Sentinel-Kommentare und Statusaktualisierung“ replizieren und den Auftrag als Systemanwender ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zugehörige Informationen

Domänentrennung für Service Provider

Wird Verglichen Microsoft Azure Sentinel Und Microsoft Graph-Sicherheits-API Integrationen mit SIR

Sie können die Unterschiede zwischen anzeigen Microsoft Azure Sentinel Und Microsoft Graph-Sicherheits-API Integrationen und wählen Sie die richtige Integration mit aus ServiceNow AI Platform Instanz.

Microsoft Azure Sentinel – Incident Ingestion – Übersicht

Microsoft Azure Sentinel Ist eine cloudbasierte Lösung für Security Information Event Management (SIEM) und Security Orchestration Automated Response (SOAR). Microsoft Azure Sentinel Stellt intelligente Security Analytics und Threat Intelligence im gesamten Unternehmen bereit. Es bietet eine einzige Lösung für die Erkennung von Warnungen, die Sichtbarkeit von Bedrohungen, die proaktive Jagd und die Reaktion auf Bedrohungen.

Microsoft Graph-Sicherheits-API – Übersicht

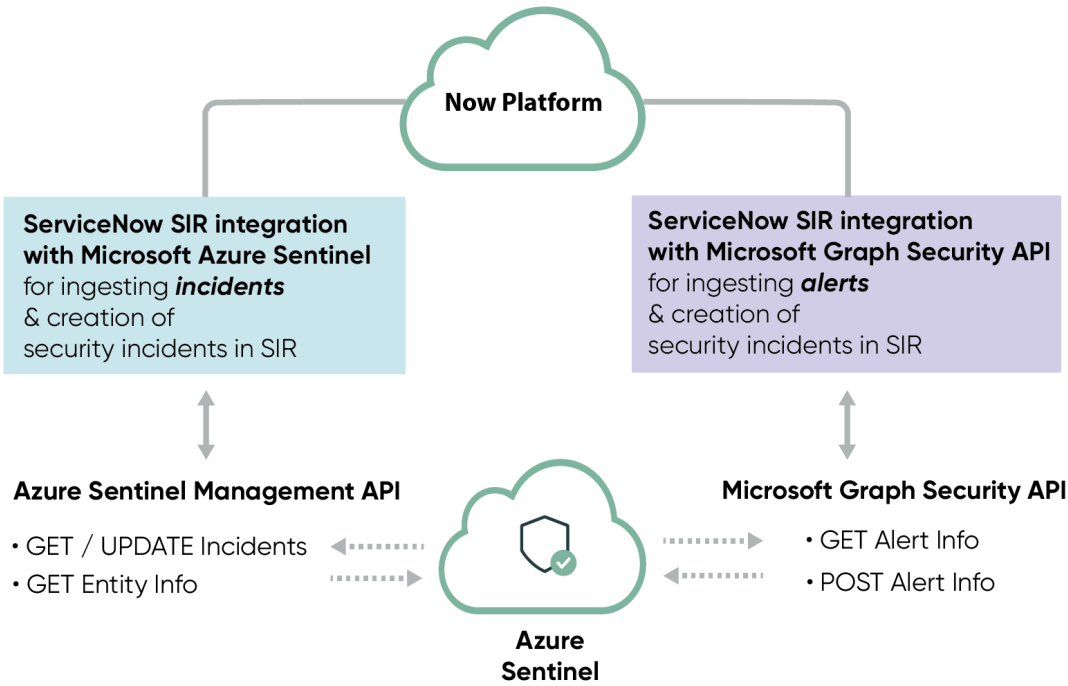
Die Microsoft Graph-Sicherheits-API Ist ein intermediärer Service (oder Broker), der eine einzige programmgesteuerte Schnittstelle zum Verbinden mehrerer Sicherheitsanbieter (nativ zu Microsoft sowie) bietet ServiceNow Partner).

Die Microsoft Graph-Sicherheits-API Die Integration behebt diese Probleme mithilfe von Microsoft Graph-Sicherheits-API Um eine Verbindung mit verschiedenen Microsoft-Sicherheitstechnologien wie Azure Sentinel, Microsoft Defender Advanced Threat Protection und Azure Advanced Threat Protection herzustellen. Warnungen von Microsoft-Sicherheitsanbietern werden erfasst, und Security Incidents werden automatisch in erstellt Security Incident Response.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusammenfassung der Funktionsunterschiede

Azure Sentinel and Graph Security API (Microsoft architecture)



Microsoft Azure Sentinel Vs Microsoft Graph-Sicherheits-API

Microsoft Azure Sentinel	Microsoft Graph-Sicherheits-API
Erfassungen Microsoft Azure Sentinel Incidents zusammen mit Entitätsinformationen (falls verfügbar) und automatisiert die Erstellung von Security Incidents in SIR.	Erfasst Warnungen von mehreren Sicherheitsanbietern (einschließlich Azure Sentinel) in einem Standardschema und automatisiert die Erstellung von Security Incidents in SIR.
Automatisiert Microsoft Azure Sentinel Incident-Statusaktualisierungen für Security Incident Response, damit Sie Security Incidents erstellen und schließen können. **Hinweis:** ServiceNow Aktualisiert den Status von Microsoft Azure Sentinel Incidents basierend auf der Erstellung oder dem Abschluss von Security Incidents.	Unterstützt Warnungsaktualisierungen (Änderung des Warnungsstatus und Abschluss von Warnungen) für ausgewählte Sicherheitsanbieter. **Hinweis:** Weitere Informationen zu finden Microsoft Graph-Sicherheits-API Unterstützte Sicherheitsanbieter, zeigen Sie an Microsoft-Dokumentation .
Verwenden Sie diese Integration, wenn Ihr Szenario die folgenden Bedingungen enthält:	Verwenden Sie diese Integration, wenn Ihr Szenario die folgenden Bedingungen enthält:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Microsoft Azure Sentinel Vs Microsoft Graph-Sicherheits-API (Fortsetzung)

Microsoft Azure Sentinel	Microsoft Graph-Sicherheits-API
• Vorläufige Incident-Untersuchung befindet sich in Microsoft Azure Sentinel Und die nachfolgende Untersuchung befindet sich in SIR • Erfassen Microsoft Azure Sentinel Incidents bis SIR	• Führen Sie eine Incident-Untersuchung in durch SIR. • Erfassen Microsoft Azure Sentinel Warnungen in SIR. • Incidents werden nicht in erstellt Microsoft Azure Sentinel.
Warnung ist eine Entität in Microsoft Azure Sentinel. Sie können keine eigenständigen oder bestimmten Warnungen mit abrufen Microsoft Azure Sentinel Verwaltungs-API. Sie können nur die Warnungsdaten abrufen, die einem Incident zugeordnet sind. Die mit dieser Integration verfügbaren Warnungsdaten sind reicher als die mit verfügbaren Warnungsdaten Microsoft Graph-Sicherheits-API.	Die Microsoft Azure Sentinel Normalisierte Warnungsdaten sind verfügbar. Die Microsoft Azure Sentinel Warnungsfelder, die intern in zugeordnet sind Microsoft Graph-Sicherheits-API, Und sind in verfügbar Microsoft Graph-Sicherheits-API, Sind zur Verwendung in dieser Integration verfügbar.
	Sie können Warnungen in nicht aktualisieren Microsoft Azure Sentinel Diese Integration wird verwendet.

Microsoft Defender for Endpoint-Integration

Die Microsoft Defender for Endpoint Ermöglicht Ihnen die proaktive Untersuchung, Analyse und Eindämmung bekannter und unbekannter Bedrohungen an jedem Endpunkt.

Die Microsoft Defender for Endpoint Die Integration hilft Sicherheitsanalysten, Security Incidents effizient zu untersuchen und zu beheben, ohne zwischen Tools navigieren zu müssen.

Sie können diese Integration verwenden, um Konfigurationen zum Abrufen der Hostdetails, Details der angemeldeten Anwender, Details zu zugehörigen Computern und anderer Ergänzungsfunktionen zu erstellen. Sie können anfordern, jeden Computer vom Zugriff auf Netzwerke zu isolieren oder die Computer aus der Isolierung zu entfernen. Anforderungen können von den Genehmigern akzeptiert oder abgelehnt werden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Schlüsselfunktionen

Microsoft Defender for Endpoint Verfügt über die folgenden wichtigen Funktionen:

- Führen Sie die Enterprise-Sicherheitssuche durch, um potenzielle schädliche erkennbare Elemente auf Endpunkten zu erkennen und Korrekturmaßnahmen zu ergreifen.
- Führen Sie Antwortaktionen aus, z. B. Host isolieren, Isolierung entfernen, App-Ausführung einschränken, Virenschutz-Scan ausführen, App-Einschränkung entfernen, und Datei anhalten und unter Quarantäne stellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen oder aktualisieren Sie Indikatoren.
- Ergänzungen erkennbarer Elemente durchführen und Daten im Zusammenhang mit Indikatoren abrufen.

Microsoft Defender for Endpoint

Untersuchen Erste Schritte mit Microsoft Defender for Endpoint	**Installieren** Installieren Sie die Anwendung, und konfigurieren Sie eine Quelle für die Integration	**Konfigurieren** Konfigurieren Sie Profile und Security Incidents für Microsoft Defender for Endpoint
Fähigkeitsprofil Erstellen Sie ein Fähigkeitsprofil für die Microsoft Defender for Endpoint-Integration.	**Zusätzliche Konfigurationen** Zusätzliche Konfigurationen, die Sie in Microsoft Defender for Endpoint ausführen können	**Verschiedenes** Erstellen und konfigurieren Sie ein Profil für Sichtungssuche und -Indikatoren mit Microsoft Defender for Endpoint.

Registrieren und konfigurieren Sie Microsoft Defender for Endpoint In Microsoft Azure Portal

Registrieren Sie Microsoft Defender for Endpoint Anwendung im Microsoft Azure-Portal und gewähren Lese- und Schreibzugriff auf die Anwendung.

Vorbereitungen

Erforderliche Rolle: Anwendungsentwickler, Mandantenadministrator.

Prozedur

1. Melden Sie sich beim Microsoft Azure-Portal an.
2. Geben Sie Ein App-Registrierungen Klicken Sie im Suchfeld auf **Klicken Sie auf neue Registrierung** .
3. Geben Sie einen Namen für Ihre Anwendung und den Umleitungs-URI ein, und klicken Sie auf **Registrieren** .
   Ein Beispielname ist Microsoft Defender für Endpunkt . Der Umleitungs-URI wird verwendet, wenn der Administrator die Zustimmung für die Anwendung erteilt.
4. In **App-Registrierungen** Wählen Sie die Anwendung aus, die Sie in Schritt 3 registriert haben.
5. Wählen Sie unter Verwalten die Option aus **Zertifikate und Geheimnisse** .
6. Um ein geheimes Clientgeheimnis zu erstellen, wählen Sie aus **Neues geheimes Clientgeheimnis** .
7. Kopieren Sie das geheime Clientgeheimnis, und speichern Sie es.

   Wenn Sie das geheime Clientgeheimnis vergessen haben, können Sie ein neues geheimes Clientgeheimnis generieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

8. Navigieren zu **Verwalten** > **API-Berechtigungen**an.
9. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.
10. Klicken Sie im Fenster „API-Berechtigungen anfordern“ auf **APIs, die meine Organisation verwendet** Registerkarte.
11. Suchen und wählen Sie aus **WindowsDefenderATP** .
12. Wählen Sie in den WindowsDefenderATP-Berechtigungen die Option aus **Anwendungsberechtigungen** .
    Durch Aktivieren dieser Berechtigung wird sichergestellt, dass die Anwendung als Hintergrundservice oder Daemon ohne angemeldeten Anwender ausgeführt wird.
13. Fügen Sie die folgenden Berechtigungen auf Anwendungsebene hinzu, und gewähren Sie dem Administrator die Zustimmung für die neu hinzugefügten API-Berechtigungen.

Berechtigung	Anzeigename Der Berechtigung
Computer.Lesen.Alle	Lesen Sie alle Computerprofile
Anwender.Lesen.Alle	Anwenderprofile lesen
Computer.Isolieren	Computer isolieren
Computer.EinschränkungAusführung	Codeausführung einschränken
Computer.Scan	Computer scannen
Computer.Anhalten AndQuarantäne	Anhalten und Quarantäne stellen
URL.Lesen.alle	URLs lesen
Datei.Lesen.Alle	Lesen Sie Dateiprofile
Ip.Lesen.Alle	Lesen Sie IP-Adressprofile
TI.Lesen.Schreiben.alle	Lese- und Schreibindikatoren

Beginnen Sie mit dem Microsoft Defender for Endpoint Integration

Im folgenden Abschnitt werden die Setup-Aufgaben aufgeführt, die Sie in ausführen müssen ServiceNow AI Platform® Instanz vor der Installation von Microsoft Defender for Endpoint Anwendung aus dem ServiceNow Store.

Vorbereitungen

Erforderliche Rolle: Administrator

Überprüfen Sie anhand der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform Und Security Incident Response-Rollen (SIR).	Die folgenden Rollen sind erforderlich: 1. Sie müssen über die Rolle „Systemadministrator“ (Administrator) verfügen, um die Anwendung für die Integration zu installieren. 2. Sie müssen über die Rolle „Security Incident-Administrator“ (sn_si.admin)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	verfügen, um die Integration zu konfigurieren, Profile zu erstellen, zu aktivieren und zu entfernen. 3. Sie müssen über die Rolle „Security Incident Analyst“ (sn_si.Analyst) verfügen, um mit Security Incidents zu arbeiten. Ein Anwender mit dieser Rolle kann eine der in der Integration verfügbaren Fähigkeiten initiieren.
Stellen Sie sicher, dass die ServiceNow-Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, installiert und aktiviert sind, bevor Sie die Anwendung installieren.	Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn diese Anwendungen noch nicht installiert sind, müssen Sie jede Anwendung einzeln in der folgenden Reihenfolge installieren und aktivieren, um eine reibungslose Installation sicherzustellen: 1. Security Incident Response 2. ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) 3. ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest)
Bevor Sie die Genehmigungsoption für Profile aktivieren, überprüfen Sie, ob Sie eine Genehmigungsgruppe erstellt haben.	Ein optionaler Genehmigungs-Workflow ist verfügbar, um Hostcomputer zu isolieren, sie wieder im Netzwerk wiederherzustellen und zusätzliche Aktionen am Endpunkt auszuführen. Wenn Ihre Organisation eine zusätzliche Kontrolle über diese Aktionen wünschen, aktivieren Sie während der Konfiguration der Profile die Option Genehmigung erforderlich. In einem Szenario, in dem das Profil verfügbar ist, hat die Profilkonfiguration für die Genehmigung Vorrang. In einem Szenario, in dem das Profil nicht verfügbar ist, werden die Genehmigungen basierend auf den Standardeinstellungen verarbeitet. Als Sicherheitsadministrator können Sie Genehmigungen einrichten, während Sie die Profile und Standardeinstellungen konfigurieren. Eine Genehmigungsgruppe muss in Ihrer Instanz in der Gruppenliste verfügbar sein. Um Anforderungen zu überwachen und zu verarbeiten, die von Anwendern mit der Rolle „sn_si.Analyst“ übermittelt werden, muss jedes Mitglied der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	Genehmigungsgruppe im zu meine Genehmigungen navigieren ServiceNow AI Platform®. Alternativ können die Genehmiger die Anforderungen finden, die ausschließlich für übermittelt wurden Microsoft Defender for Endpoint Integration unter dem Modul „Genehmigungen“. Weitere Informationen zum Erstellen einer Anwendergruppe finden Sie unter Erstellen Sie eine Anwendergruppe .

Nächste Maßnahme

Sie haben erfolgreich eingerichtet ServiceNow AI Platform® Instanz für Microsoft Defender for Endpoint Integration. Der nächste Schritt besteht in der Installation von Microsoft Defender for Endpoint Anwendung aus dem ServiceNow Store für die Integration.

Installieren Sie die Anwendung, und konfigurieren Sie Microsoft Defender for Endpoint Integration

Installieren und konfigurieren Sie Microsoft Defender for Endpoint Integration aus dem ServiceNow Store Auf Ihrem ServiceNow AI Platform Instanz. Beginnen Sie mit der Erstellung von Fähigkeitsprofilen mithilfe der Konfigurationen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Laden Sie die Microsoft Defender for Endpoint-Integration aus dem herunter ServiceNow Store Und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie nach der Kachel Microsoft Defender for Endpoint, und klicken Sie auf **Konfigurieren** .
4. Füllen Sie die folgenden Felder des Formulars aus.

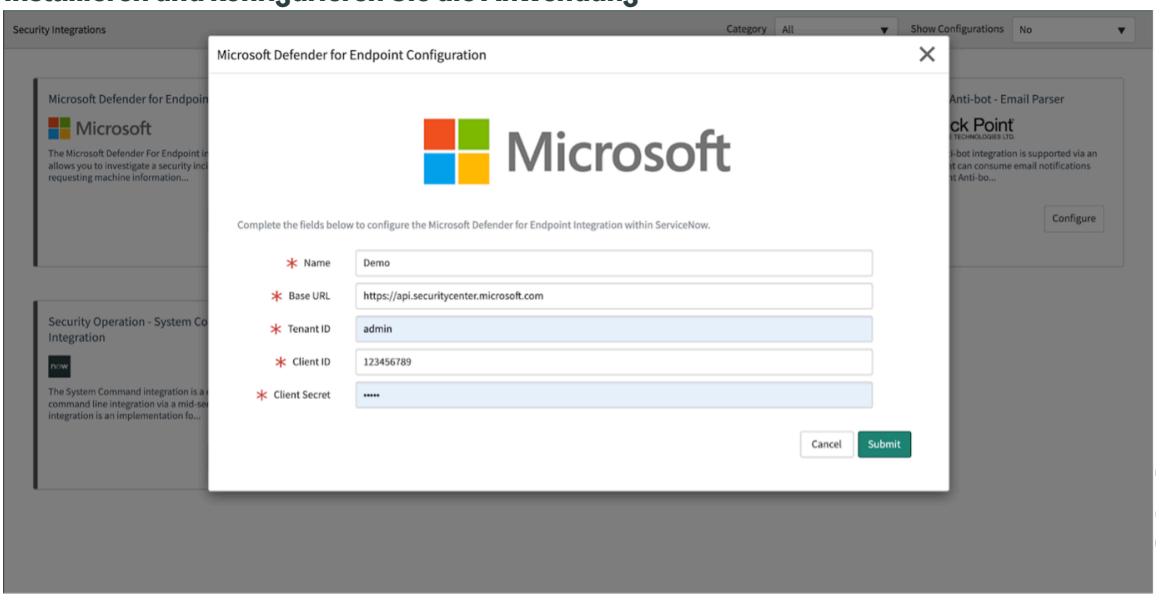
Konfigurieren Sie Microsoft Defender für Endpunkt

Name	Name für Microsoft Defender for Endpoint Instanzkonfiguration.
Basis-URL	Die Servicebasis-URL für Microsoft Defender for Endpoint
Mandanten-ID	Die Microsoft Defender for Endpoint Mandanten-ID. Alle Aktionen werden für diese Instanz ausgeführt.
Client-ID	Client-ID für die Anwendung, die Sie im Microsoft Azure-Portal registriert haben.
Geheimer Clientschlüssel	Geheimer Clientschlüssel für Ihre registrierte Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Absenden**.

Installieren und konfigurieren Sie die Anwendung



Ergebnisse

Die Microsoft Defender for Endpoint Die Konfigurationsliste wird mit Ihrem neuen Konfigurationsdatensatz angezeigt. Sie haben die Konfiguration für abgeschlossen Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint Standardeinstellungen

Es gibt zusätzliche Konfigurationseinstellungen, die Sie nach Abschluss der Installation ausführen müssen.

Nach Abschluss der Installation finden Sie das Modul „Standardeinstellungen“ unter Microsoft Defender for Endpoint Anwendung im linken Navigationsbereich. Enthält die Standardeinstellungen für verschiedene Microsoft Defender for Endpoint Funktionalitäten.

Erforderliche Rollen: sn_si.admin, sn_si.Analyst (schreibgeschützt).

Zusätzliche Konfigurationen

Im Folgenden finden Sie zusätzliche Konfigurationseinstellungen:

- **Genehmigung** : Diese Genehmigung gilt speziell für die Aktion „Host isolieren“, die Aktion „Host-Isolierung entfernen“ und zusätzliche Aktionen wie „App-Ausführung einschränken“, „App-Einschränkung entfernen“ und „Antivirus-Scan ausführen“. Sie können diese Genehmigung nur verwenden, wenn Aktionen direkt über die zugehörige Liste ausgelöst werden und wenn keine Profile vorhanden sind. Wenn Profile für diese Fähigkeiten vorhanden sind, hat die Genehmigungskonfiguration im Profil Vorrang.
  - **Genehmigung Erforderlich** : Wenn Sie aktivieren **Genehmigung Erforderlich** , Das Feld Genehmiger ist im Formular verfügbar.
  - **Genehmiger** : Liste der Genehmigergruppen. Nachdem Sie eine Anforderung übermittelt haben, ist die Genehmigung der Gruppe erforderlich, um die Anforderung abzuschließen.
- **Alternatives CI** : Durch Aktivieren dieses Kontrollkästchens wird die Liste der Felder bereitgestellt, die zum Übergeben eines alternativen CI an die Fähigkeit verfügbar sind. Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Diese Konfiguration gilt nur für die Fähigkeit „zusätzliche Aktionen für Endpunkt

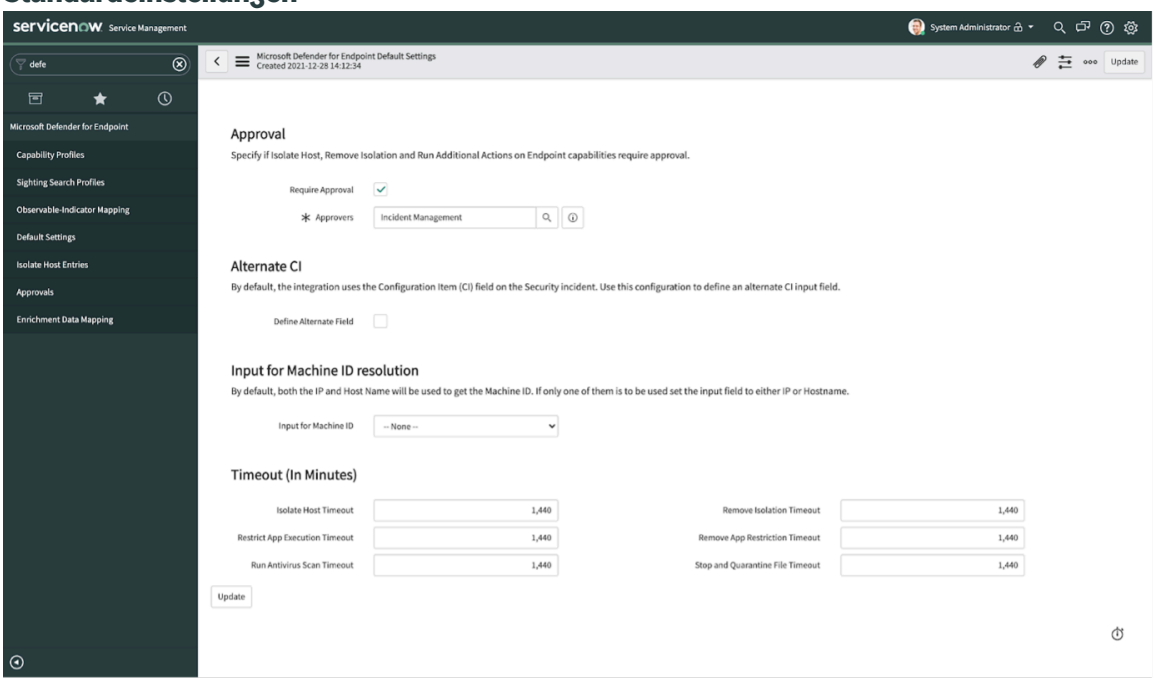
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ausführen“. Verwenden Sie diese Konfiguration, um ein alternatives CI-Eingabefeld für die Funktionalität „nur zusätzliche Aktionen für Endpunkt ausführen“ zu definieren. Verwenden Sie für die anderen Fähigkeiten die Konfiguration im Profilabschnitt. Wenn die Profile kein alternatives CI definieren, übernehmen die Fähigkeiten das CI-Feld aus dem Security Incident-Formular.

- **Eingabe für Lösung der Service Desk-Mitarbeiter-ID** : Standardmäßig werden IP und Hostname zum Abrufen der Agent-ID verwendet. Wenn Sie nur eine davon verwenden, legen Sie das Eingabefeld entweder auf IP oder Hostname fest.
- **Zeitüberschreitung** :
  - **Host-Zeitüberschreitung isolieren (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeiten „Host isolieren“ an.
  - **Zeitüberschreitung beim Entfernen der Isolierung (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeit „Isolierungszeitüberschreitung entfernen“ an.
  - **Zeitüberschreitung bei App-Ausführung beschränken (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeit „App-Ausführung einschränken“ an.
  - **Zeitüberschreitung beim Entfernen der App-Einschränkung (in Minuten):** Gibt den Ausführungsschwellenwert für die Fähigkeit „App-Einschränkung entfernen“ an.
  - **Zeitüberschreitung beim Ausführen von Antivirus-Scans (in Minuten):** Gibt den Ausführungsschwellenwert für die Funktionalität „Antivirus-Scan ausführen“ an.
  - **Zeitüberschreitung bei Stopp und Quarantäne der Datei (in Minuten):** Gibt den Ausführungsschwellenwert für die Funktion „Datei stoppen und in Quarantäne stellen“ an.

Standardeinstellungen



Ordnen Sie zu Microsoft Defender for Endpoint Indikatortypen

Ordnen Sie den Typ des erkennbaren ServiceNow-Elements zu Microsoft Defender for Endpoint Indikatortyp. Diese Zuordnung wird in den Aktionen „Anreicherung erkennbarer Elemente“ und „Indikator erstellen“ in Microsoft Defender verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

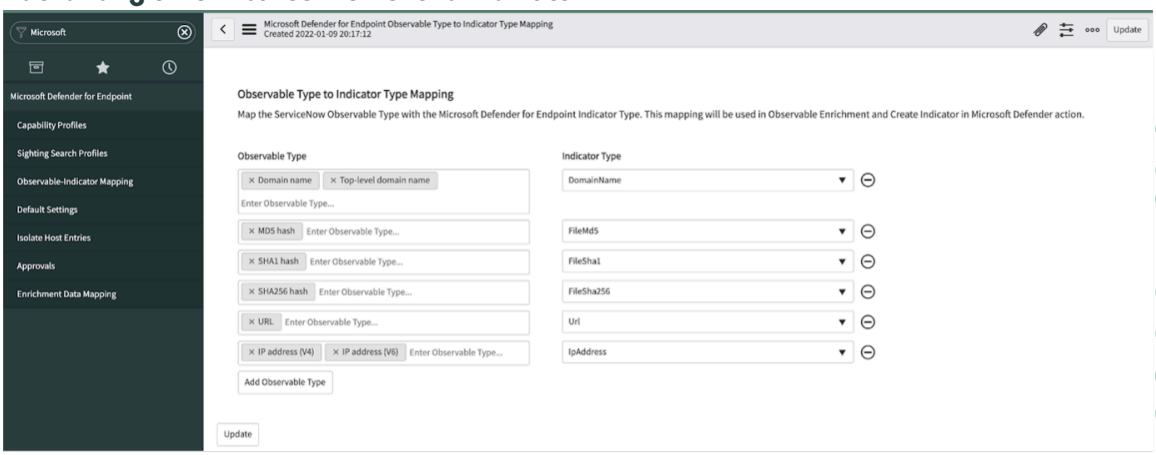
Vorbereitungen
Erforderliche Rolle: sn_si.admin oder sn_si.Analyst (schreibgeschützt)

Warum und wann dieser Vorgang ausgeführt wird
In einem Szenario, in dem der Typ des erkennbaren Elements keinem Indikatortyp zugeordnet ist, sind solche erkennbaren Elemente nicht für die Ergänzung erkennbarer Elemente und die Indikatorerstellung in Microsoft Defender for Endpoint geeignet.

Prozedur

1. Navigieren zu **Microsoft Defender für Endpunkt** > **Zuordnung erkennbares Element zu Indikator**an.

Zuordnung erkennbares Element zu Indikator



2. Fügen Sie einen erkennbaren Typ auf eine der folgenden Arten hinzu oder aktualisieren Sie ihn:
   - Um eine neue Zuordnung hinzuzufügen, klicken Sie auf **Fügen Sie Den Typ Des Erkennbaren Elements Hinzu** .
   - Um das erkennbare Element auf die Zuordnung des Indikatortyps zu aktualisieren, klicken Sie auf eine beliebige vorhandene Zeile.
3. Klicken Sie auf, um die Zuordnung zu speichern **Aktualisieren** .

Erstellen Sie ein Fähigkeitsprofil für Microsoft Defender for Endpoint Integration

Erstellen Sie ein Profil, und wählen Sie aus Microsoft Defender for Endpoint Fähigkeiten, die das Profil ausführen soll.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Profile werden erstellt, um die Fähigkeiten zu vereinigen oder zu gruppieren, was Analysten helfen würde, die Untersuchung oder Korrektur einfach durchzuführen. Sie können dem Profil die folgenden Fähigkeiten hinzufügen:

- Hostdetails abrufen
- Angemeldete Anwender abrufen
- Host isolieren
- Isolation entfernen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können beim Erstellen eines Profils die Funktionen „Host isolieren“ und „Host-Isolation entfernen“ nicht mit anderen Funktionen kombinieren. Profile für diese Fähigkeiten müssen einzeln erstellt werden. Andererseits können die Funktionen Hostdetails abrufen und angemeldete Anwender abrufen zusammen zusammengefasst werden. Sie können Profile einzeln erstellen oder sie gemäß Ihren Anforderungen vollständig oder teilweise gruppieren.

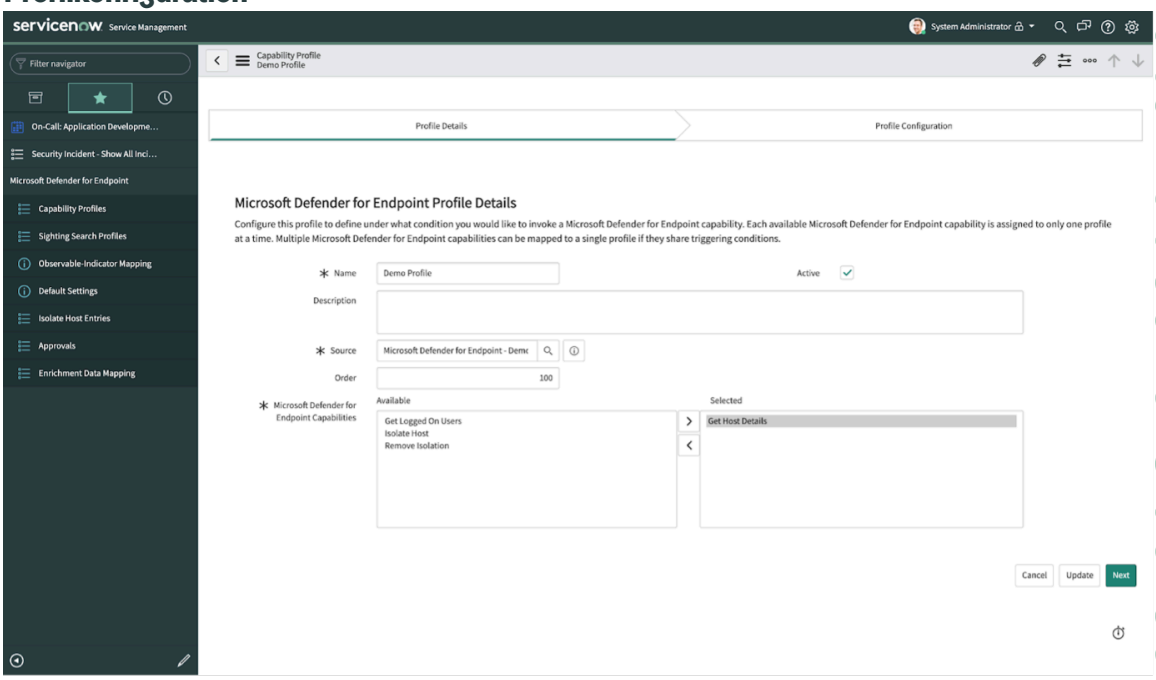
Hinweis:
Nachdem eine Fähigkeit in einem Profil enthalten ist, kann sie nicht in ein anderes Profil derselben Quelle aufgenommen werden.

Prozedur

1. Navigieren zu **Microsoft Defender für Endpunkt** > **Fähigkeitsprofile**an.

   Die Liste Microsoft Defender für Endpunktfähigkeitsprofile wird angezeigt.

Profilkonfiguration



2. Klicken **Neu**an.
3. Füllen Sie im Formular die Felder aus.

Formular „Fähigkeitsprofil“

Feld	Beschreibung
Name	Name für Microsoft Defender for Endpoint Fähigkeitsprofil. Dieser Name hilft Ihnen, den Profiltyp zu identifizieren und zu beschreiben.
Beschreibung	Zusätzliche Informationen zum Profil, die das Profil weiter beschreiben.
Quelle	Name des Microsoft Defender for Endpoint Quelle. Nur konfigurierte Quellen sind aus der Liste verfügbar.
Microsoft Defender for Endpoint-Fähigkeiten	Fähigkeiten von Microsoft Defender for Endpoint Profil. Wählen Sie in der Spalte verfügbar die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	gewünschten Fähigkeiten für dieses Profil aus, und verschieben Sie sie in die Spalte ausgewählt.
Reihenfolge	Flow-Priorität. Der Standardwert ist 100. Der Wert dieses Felds gibt die Reihenfolge an, in der Flows ausgeführt werden, wenn zwei oder mehr Profile Auslösebedingungen teilen. Der Flow mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Beispiel: 100, 200, 300, 400.
Aktiv	Option, um anzugeben, dass das Profil aktiv ist. Nach Das Profil ist aktiv. Das Profil wird automatisch ausgelöst, wenn ein Security Incident erstellt wird, der den Filterbedingungen entspricht, die Sie in der Konfiguration angegeben haben.

4. Um mit der Profilkonfiguration fortzufahren, klicken Sie auf **Weiter**an.

Nächste Maßnahme

Der nächste Schritt besteht darin, Ihr Profil zu konfigurieren. Bevor Sie die Einstellungen für das Profil konfigurieren, sollten Sie möglicherweise überprüfen, wie Profile und Konfigurations- und Auslösebedingungen konfiguriert werden. Weitere Informationen finden Sie unter Auslöserbedingungen in einem Konfigurationselement.

Auslöserbedingungen in einem Konfigurationselement

Nachdem Sie ein Profil erstellt und ausgewählt haben Microsoft Defender for Endpoint Fähigkeiten, die das Profil ausführen soll, konfigurieren Sie die Profileinstellungen so, dass das Profil nur ausgeführt wird, wenn eine Reihe bestimmter Bedingungen erfüllt ist.

So lösen Sie Bedingungen in einem Konfigurationselement aus

Sie können Auslöserbedingungen festlegen, damit das Profil automatisch ausgeführt wird, wenn ein Security Incident erstellt wird, der der Auslöserbedingung entspricht. Wenn die Auslöserbedingung nicht festgelegt ist, können diese Profile manuell ausgeführt werden, indem Sie im Security Incident auf das Formular „EDR-Profil(e) ausführen“ klicken und das Profil auswählen.

Standardmäßig verwendet die Integration das Feld Configuration Item (CI) im Security Incident. Dieser Wert wird verwendet, um die IDs Ihrer Assets mit den in gespeicherten Informationen abzugleichen ServiceNow AI Platform Configuration Management Database (CMDB). Wenn ein Security Incident erstellt wird und ein Profil entweder automatisch oder manuell ausgeführt wird, wird der verwendet CMDB Wird gesucht, um den Hostnamen oder die IP-Adresse basierend auf dem Wert des CI-Felds abzurufen. Der Hostname oder die IP-Adresse wird verwendet, um die Agent-ID in aufzulösen Microsoft Defender for Endpoint Um den Endpunkt zu identifizieren.

In einem idealen Szenario wird ein übereinstimmender Wert in der Datenbank gefunden, und Daten werden aus dem gesammelt Microsoft Defender for Endpoint Konsole für das übereinstimmende Asset. Die Daten für verschiedene Fähigkeiten werden in abgerufen ServiceNow AI Platform Configuration Management Database (CMDB) Instanz und wird in den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugehörigen Listen eines Security Incidents angezeigt. Wenn das Feld Configuration Item (CI) im Security Incident nicht mit einem Hostnamen mit oder einer IP-Adresse ausgefüllt ist, die der Datenbank entspricht, können Sie ein alternatives Feld im Security Incident auswählen, das entweder den Hostnamen oder die IP-Adresse enthält, um die Lösung der Agent-ID durchzuführen.

Während des Konfigurationsschritts des Profils können Sie ein alternatives CI-Feld für die Endpunktidentifizierung auswählen, um sicherzustellen, dass Sie den Endpunkt auf identifizieren können Microsoft Defender for Endpoint. Sie können jedes Feld im Security Incident als alternatives CI-Auslöserfeld auswählen, einschließlich anwenderdefinierter Felder, die Sie erstellen. Indem Sie dieses alternative CI-Feld als Sicherung auswählen, stellen Sie sicher, dass Ihre Profile auch dann ausgeführt werden, wenn das CI-Feld bei der Incident-Erstellung nicht für den zugehörigen Security Incident ausgefüllt ist.

Hinweis:
Die alternativen CI-Felder werden nur für Fähigkeiten berücksichtigt, die einem Profil hinzugefügt werden können. Diese Fähigkeiten umfassen Hostdetails abrufen, angemeldete Anwender abrufen, Host isolieren und Isolierung entfernen. Für alle zusätzlichen Aktionen muss das alternative CI im Modul „Standardeinstellungen“ konfiguriert werden.

Konfigurieren Sie Profile und Security Incidents für Microsoft Defender for Endpoint Integration

Erstellen Sie ein Profil, und wählen Sie aus Microsoft Defender for Endpoint Fähigkeiten, die das Profil ausführen soll. Sie müssen die Einstellungen so konfigurieren, dass das Profil nur unter den definierten Bedingungen ausgelöst werden kann.

Vorbereitungen
Erforderliche Rolle: sn_si.admin, sn_si.Analyst (schreibgeschützt)

Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie das Profil so, dass es nur ausgeführt wird, wenn die von Ihnen angegebenen Bedingungen erfüllt sind. Bei Bedarf können Sie ein alternatives Eingabefeld für das Feld Configuration Item (CI) auswählen und Filterbedingungen festlegen, damit das Profil automatisch ausgelöst werden kann, wenn ein Security Incident erstellt wird, der die Auslöserbedingungen erfüllt.

Hinweis:
Sie können erst zur Seite „Profilkonfiguration“ navigieren, nachdem Sie die Seite „Profildetails“ aufgerufen haben.

Prozedur

1. Navigieren zu **Microsoft Defender für Endpunkt** > **Fähigkeitsprofile**an.
2. Klicken Sie nach Abschluss des Abschnitts „Profildetails“ auf **Weiter**an.
   Überprüfen und konfigurieren Sie die Abschnitte.
3. Wählen Sie im Abschnitt Incident-Kriterien definieren (Automatisierung) die Option aus **Definieren Sie Incident-Kriterien** Option zum automatischen Auslösen Microsoft Defender for Endpoint Fähigkeiten im Profil.
   Incident-Kriterien Definieren (Automatisierung) : Definieren Sie die Bedingungen für Security Incidents, die die Microsoft Defender for Endpoint-Fähigkeiten für das Profil automatisch auslösen würden. Wenn Sie nicht auswählen **Definieren Sie Incident-Kriterien** Option, dann können das Profil und die zugrunde liegenden Fähigkeiten manuell über den Security Incident aufgerufen werden.

   Hinweis:
   Die Funktionen „Host isolieren“ und „Host-Isolation entfernen“ können nicht automatisch ausgelöst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. In **Filterbedingungen** , Wählen Sie das erforderliche Feld aus.

b. Hinzufügen **Neue Kriterien** Und definieren Sie auch **ODER** Oder **UND** Bedingung.

4. Wählen Sie im Abschnitt Genehmigungen die aus **Genehmigung Erforderlich** Kontrollkästchen, um eine zusätzliche Kontrollstufe bereitzustellen.

   Wenn Sie diese Option auswählen, haben Sie mehr Kontrolle über die Verwendung der Microsoft Defender for Endpoint-Funktionen zum Isolieren von Hostcomputern, Wiederherstellen im Netzwerk und Abrufen von Dateien.

   Die Option Genehmigungen in der Profilkonfiguration wird nur für die Funktionen Host isolieren und Host-Isolation entfernen angezeigt.

5. Wählen Sie im Abschnitt zusätzliche Konfiguration die aus **Definieren Sie Ein Alternatives Feld** Option zum Definieren eines alternativen Eingabefelds.
   Zusätzliche Konfiguration : Wenn das Feld Configuration Item (CI) im Security Incident nicht mit einem Hostnamen oder einer IP-Adresse ausgefüllt ist, die der Datenbank entspricht, können Sie ein alternatives Feld im Security Incident auswählen, um die Microsoft Defender for Endpoint-APIs abzufragen.

   Hinweis:
   Weitere Informationen finden Sie unter Auslöserbedingungen in einem Konfigurationselement.

   a. Wählen Sie aus **Definieren Sie Ein Alternatives Feld** Option.

   b. Wählen Sie das Eingabefeld aus dem aus **Alternatives CI-Auslöserfeld**an.

6. Wählen Sie im Abschnitt Tags die Option aus **Tag Anzeigen** Kontrollkästchen zum Aktivieren der Kennzeichnung von Security Incidents. Der Profilname wird beim Aktivieren des Tags vorangestellt.

   Sie können Security Incidents optional mit Tags für die Tags „Profil initiiert“, „Profil abgeschlossen“ und „Profil fehlgeschlagen“ kennzeichnen. Standardmäßig ist diese Option für alle Profile deaktiviert.

7. Klicken **Fertig**an.

Überprüfen Sie die Auslöserbedingungsfilter

Validieren Sie das Profil, und überprüfen Sie, ob die von Ihnen konfigurierten Auslöserbedingungsfilter wie erwartet funktionieren.

Vorbereitungen
Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

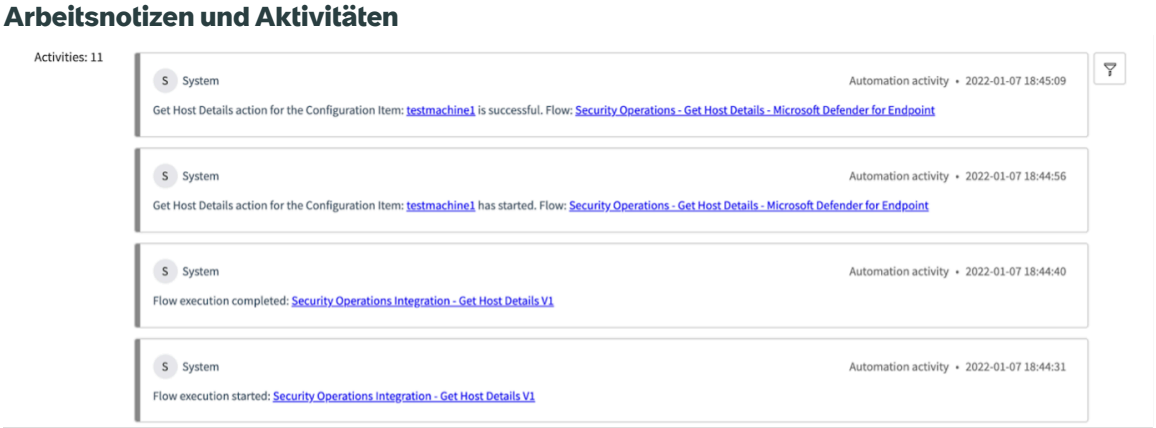
Warum und wann dieser Vorgang ausgeführt wird
Nachdem Sie das Profil aktiviert haben, können Sie basierend auf den konfigurierten Auslöserbedingungen die Abfrageergebnisse in anzeigen ServiceNow AI Platform® Security Incidents.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Um einen neuen Security Incident zu erstellen, wählen Sie aus **Neu**an.
3. Um das jeweilige Profil auszulösen, geben Sie die Filterbedingungen wie im Fähigkeitsprofil angegeben an.
4. Klicken **Speichern**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Um den Abschnitt „Arbeitsnotizen und Aktivitäten“ zu validieren, zeigen Sie die Datensätze an, die mit den Tags „Profil initiiert“, „Profil abgeschlossen“ oder „Profil fehlgeschlagen“ gekennzeichnet sind.



6. Klicken Sie auf, um alle Daten in den zugehörigen Listen zu validieren **Alle Zugehörigen Listen Anzeigen** .
7. Klicken Sie auf beliebig **Zugehörige Liste** Registerkarte zum Validieren der Details. Beispiel: Hostdetails.

Lösen Sie aus Microsoft Defender for Endpoint Fähigkeiten aus zugehörigen Links

Lösen Sie ein Fähigkeitsprofil manuell aus, nachdem Sie einen Security Incident über zugehörige Links überprüft haben.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Zusätzlich zum Ausführen des Profils für das CI oder das alternative CI des Security Incident können Sie das Profil auch für CI-Werte ausführen, die in der zugehörigen Liste „Konfigurationselement“ vorhanden sind, indem Sie auswählen **Zugehöriges CI einschließen** Im Dialogfeld. Dadurch werden auch die Daten für die in der zugehörigen Liste vorhandenen CI-Werte abgerufen. Alternativ können Sie das Profil nur für die in der zugehörigen Liste vorhandenen CI-Werte ausführen.

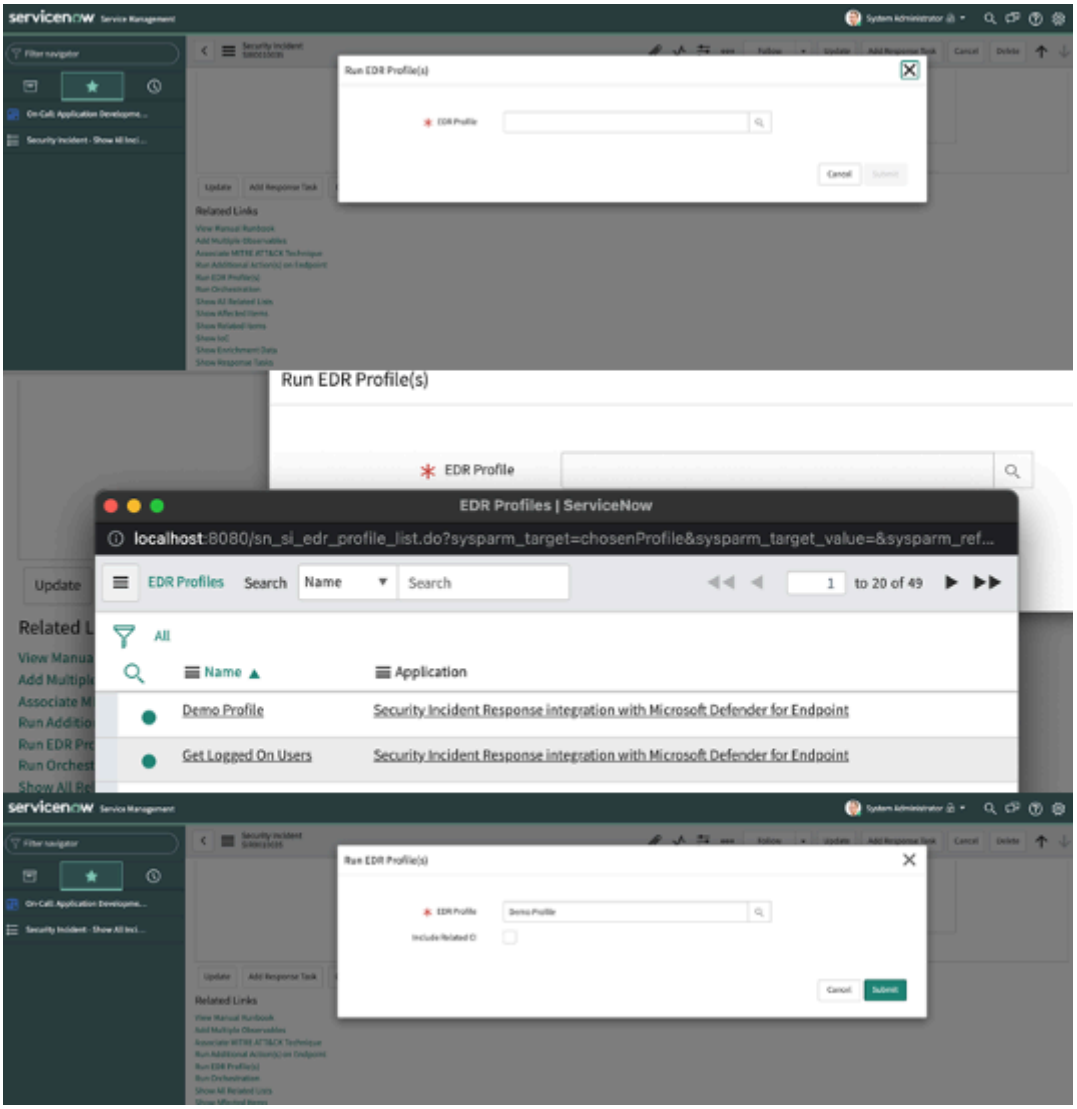
Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit überprüfen möchten Microsoft Defender for Endpoint Informationen.
3. Klicken Sie im Abschnitt zugehörige Links auf **EDR-Profil(e) ausführen** .
4. Durchsuchen Sie ein Profil, wählen Sie es aus der Liste der verfügbaren Profile aus, und klicken Sie auf **Übermitteln** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Profil auswählen



Das ausgewählte Profil wird manuell ausgelöst.

5. Validieren Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
6. Zeigen Sie die Tags an, und validieren Sie die Daten in den zugehörigen Listen.

Lösen Sie aus Microsoft Defender for Endpoint Aus der zugehörigen Liste „Konfigurationselement“

Lösen Sie ein Fähigkeitsprofil manuell aus der zugehörigen Liste des Konfigurationselements aus.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit überprüfen möchten Microsoft Defender for Endpoint Informationen.
3. Klicken **Alle zugehörigen Listen anzeigen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die zugehörige Liste Konfigurationselement.
5. Wählen Sie die hinzugefügten Konfigurationselemente aus.
6. Von **Aktionen** Wählen Sie in ausgewählten Zeilen eine Fähigkeit aus.
   Die ausgewählte Fähigkeit wird manuell ausgelöst.
7. Validieren Sie den Abschnitt „Arbeitsnotizen und Aktivitäten“.
8. Zeigen Sie die Tags an, und validieren Sie die Daten in den zugehörigen Listen.

Zusätzliche Konfigurationen in Microsoft Defender for Endpoint

Die Microsoft Defender for Endpoint Die Integration unterstützt die Ausführung zusätzlicher Aktionen, die über die Standardaktionen hinausgehen.

Die Microsoft Defender for Endpoint Unterstützt die folgenden zusätzlichen Konfigurationen:

Konfigurieren Sie die Fähigkeit „Host isolieren“ in Microsoft Defender for Endpoint

Isolieren Sie den Host vom Zugriff auf das Netzwerk in Microsoft Defender for Endpoint Basierend auf dem Schweregrad des Angriffs. Durch die Isolierung des Hosts vom Netzwerk können Sie andere schädliche Aktivitäten oder potenzielle Angriffe auf andere Hosts verhindern.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

Anforderungen für die Fähigkeit „Host isolieren“

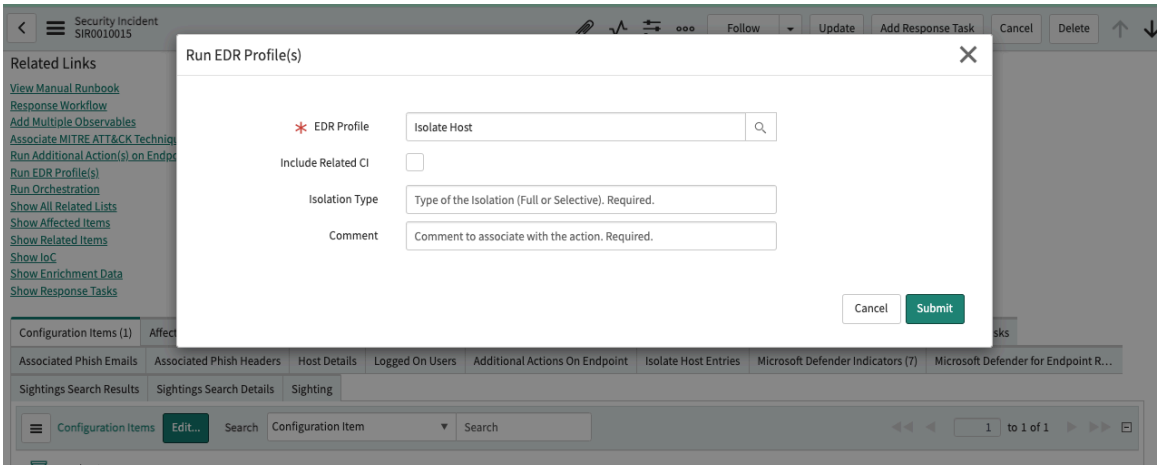
Fähigkeit	Erforderlich	Beschreibung
Host isolieren	Isolationstyp	(Erforderlich) Typ der Isolierung (vollständig oder selektiv).
	Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit den Informationen zu Microsoft Defender for Endpoint überprüfen möchten.
3. Klicken Sie im Abschnitt zugehörige Links auf **EDR-Profil(e) ausführen** .
4. Durchsuchen und wählen Sie ein Profil mit aus **Host-Fähigkeit isolieren** Aus der Liste der verfügbaren Profile ausgewählt, und klicken Sie auf **Übermitteln** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Host isolieren



Alternativ können Sie die folgenden Schritte ausführen:

a. Klicken Sie im Abschnitt zugehörige Listen auf **Alle Zugehörigen Listen Anzeigen** .

b. Klicken Sie auf **Konfigurationselement** Zugehörige Liste.

c. Wählen Sie Aus **Host Isolieren** Und wählen Sie die entsprechenden Fähigkeiten aus.

5. Validieren Sie den Abschnitt Automatisierungsaktivität und -Aktivitäten, und stellen Sie sicher, dass die Daten den Erwartungen entsprechen.
6. Zeigen Sie die Daten an, und validieren Sie die Details zum Isolieren des Hosts in den zugehörigen Listen.

Konfigurieren Sie die Funktion „Host-Isolation entfernen“ in Microsoft Defender for Endpoint

Entfernen Sie bei Bedarf die Isolierung eines Hosts, der zuvor vom Netzwerk in isoliert wurde Microsoft Defender for Endpoint. Sie können andere schädliche Aktivitäten oder potenzielle Angriffe auf andere Hosts verhindern.

Vorbereitungen

Anforderungen für die Fähigkeit „Isolation entfernen“

Fähigkeit	Erforderliche Eingabe	Beschreibung
Isolation entfernen	Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll.

Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

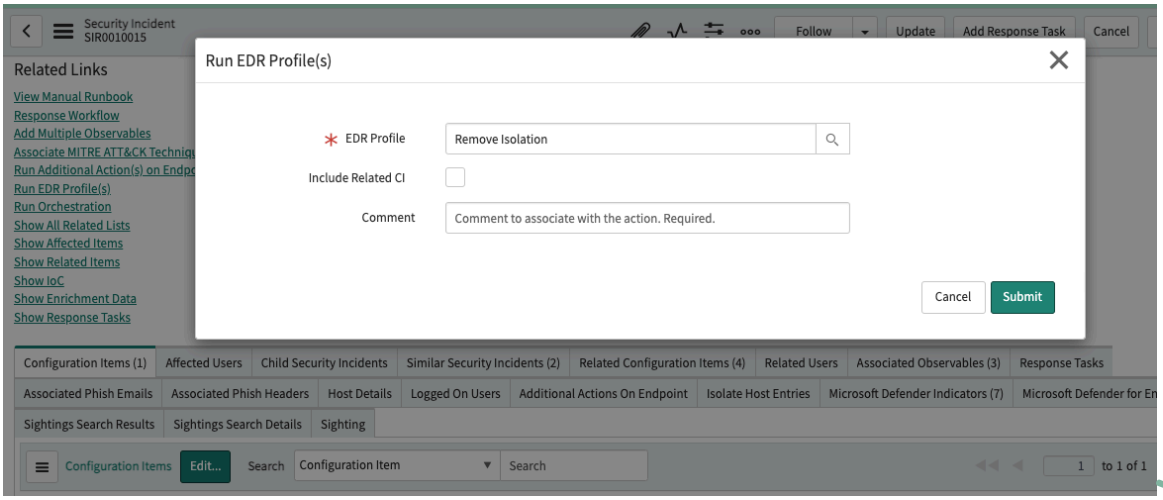
Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit den Informationen zu Microsoft Defender for Endpoint überprüfen möchten.
3. Klicken Sie im Abschnitt zugehörige Links auf **EDR-Profil(e) ausführen** .
4. Durchsuchen und wählen Sie ein Profil mit aus **Entfernen Sie die Isolationsfähigkeit** Aus der Liste der verfügbaren Profile ausgewählt, und klicken Sie auf **Übermitteln** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Isolation entfernen



Alternativ können Sie die folgenden Schritte ausführen:

a. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Im Abschnitt zugehörige Listen.

b. Klicken Sie auf **Konfigurationselement** Zugehörige Liste.

c. Wählen Sie Aus **Entfernen Sie Die Isolierung** Und wählen Sie die entsprechenden Fähigkeiten aus.

5. Validieren Sie den Abschnitt Automatisierungsaktivität und -Aktivitäten.
6. Zeigen Sie die Daten an, und validieren Sie die Details zum Isolieren des Hosts in den zugehörigen Listen.
7. Validiert die Automatisierungsaktivitäten der Ausführung.

Konfigurieren Sie die Funktion „Antivirus-Scan ausführen“ in Microsoft Defender for Endpoint

Initiieren Sie Remote einen Virenschutz-Scan, um Malware zu identifizieren und zu beheben, die auf einem gefährdeten Gerät vorhanden sein könnte. Führen Sie den Scan als Teil des Untersuchungs- oder Antwortprozesses aus.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

Anforderungen für die Fähigkeit „Antivirus-Scan ausführen“

Eingabe	Beschreibung
Scantyp	(Erforderlich) Typ des Scans (vollständig oder schnell).
Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit den Informationen zu Microsoft Defender for Endpoint überprüfen möchten.

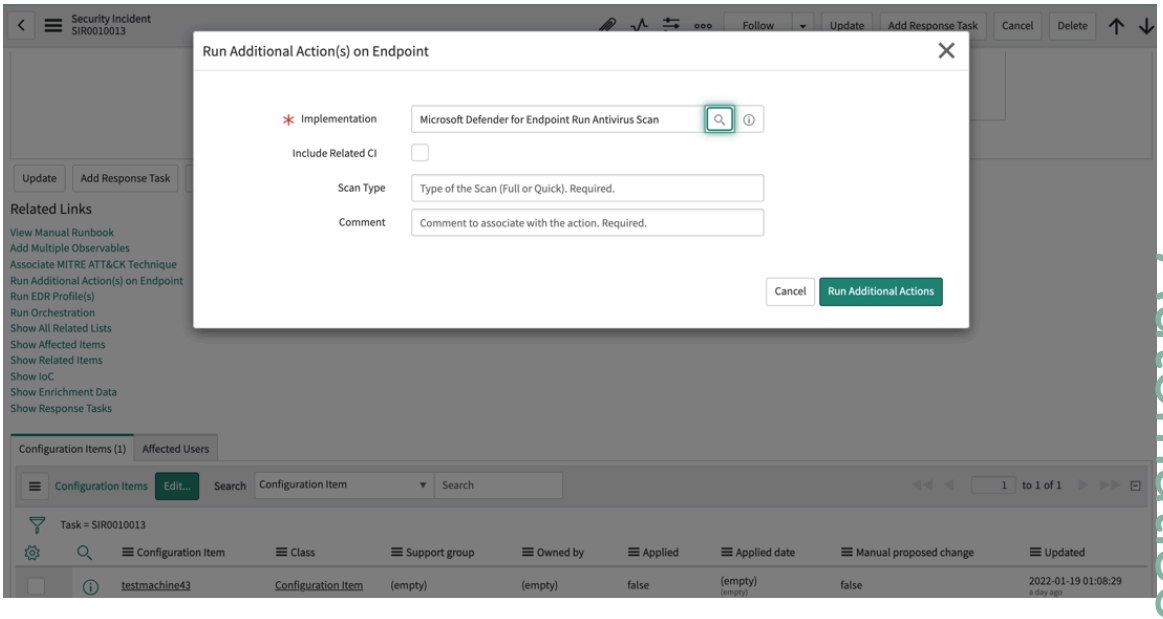
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie im Abschnitt „zugehörige Links“ auf **Führen Sie zusätzliche Aktionen für Endpunkt aus**an.

b. Durchsuchen und wählen Sie die erforderliche Fähigkeit aus.
Klicken Sie beispielsweise auf **Führen Sie Einen Virenschutz-Scan Aus** Fähigkeit.

Virenschutz-Scan ausführen



Alternativ können Sie die folgenden Schritte ausführen:

a. Klicken Sie im Abschnitt zugehörige Listen auf **Alle Zugehörigen Listen Anzeigen** .

b. Klicken Sie auf **Konfigurationselement** Zugehörige Liste.

c. Wählen Sie die hinzugefügten Konfigurationselemente aus, und wählen Sie unter Aktionen für ausgewählte Zeilen die Option aus **Führen Sie zusätzliche Aktionen für Endpunkt aus** .

Nachdem Sie ausgewählt haben **Führen Sie Einen Virenschutz-Scan Aus** Fähigkeitsimplementierung, die **Zusätzlicher Scan-Typ** Und **Kommentareingabe** Felder werden angezeigt.

3. Wählen Sie aus **Scan-Typ** Die Sie ausführen möchten (schnell oder vollständig), und fügen Sie vor dem Ausführen des Scans einen Kommentar hinzu.

4. Klicken Sie auf, um den Virenschutz-Scan zu initiieren **Zusätzliche Aktion Ausführen** .

5. Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.

6. Validiert den Status der Aktion in den zugehörigen Listen „zusätzliche Aktionen in Endpunktlisten“.

Konfigurieren Sie die Fähigkeit „App-Ausführung einschränken“ in Microsoft Defender for Endpoint

Um einen Angriff einzudämmen, beschränken oder sperren Sie ein Gerät, und verhindern Sie die Ausführung nachfolgender Versuche potenziell schädlicher Programme.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Anforderungen für die Fähigkeit „App-Ausführung einschränken“

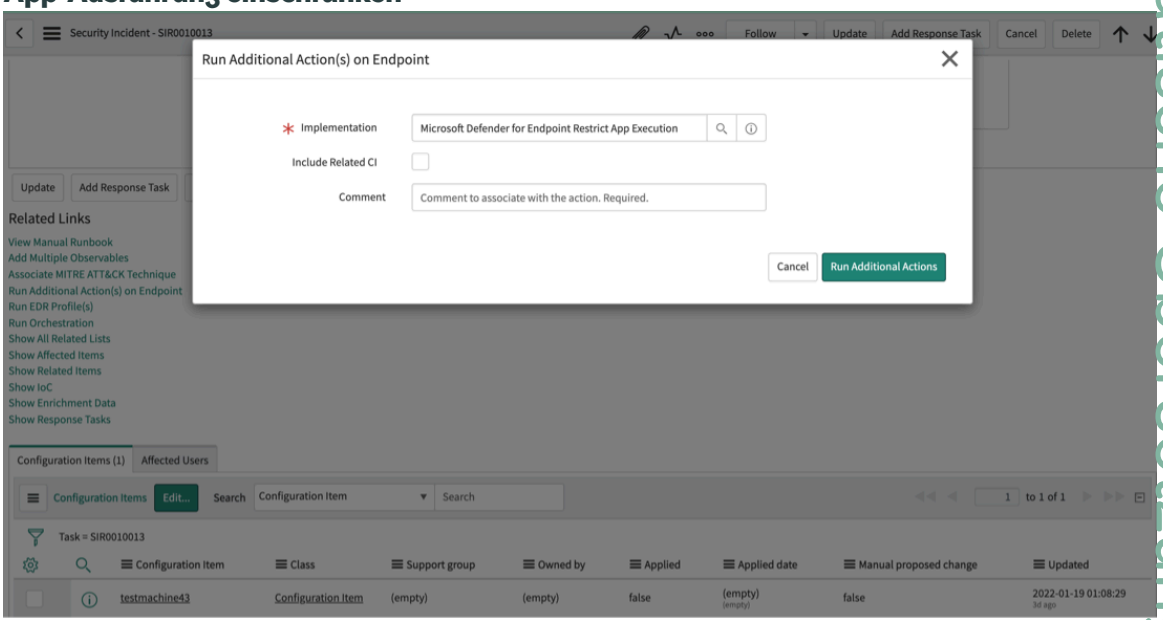
Eingabe	Beschreibung
Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll)

Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit den Informationen zu Microsoft Defender for Endpoint überprüfen möchten.
   a. Klicken Sie im Abschnitt „zugehörige Links“ auf **Führen Sie zusätzliche Aktionen für Endpunkt aus**an.
   b. Durchsuchen und auswählen **App-Ausführung Einschränken** Fähigkeit.

App-Ausführung einschränken



Alternativ können Sie die folgenden Schritte ausführen:

a. Klicken Sie im Abschnitt zugehörige Listen auf **Alle Zugehörigen Listen Anzeigen** .
b. Klicken Sie auf **Konfigurationselement** Zugehörige Liste.
c. Wählen Sie die hinzugefügten Konfigurationselemente aus.
d. Wählen Sie unter Aktionen für ausgewählte Zeilen die Option aus **Führen Sie zusätzliche Aktionen für Endpunkt aus** .

3. Um die App-Ausführung auf dem Computer beschränken zu aktivieren, klicken Sie auf **Zusätzliche Aktion Ausführen** .
4. Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.
5. Validiert den Status der Aktion in den zugehörigen Listen „zusätzliche Aktionen in Endpunktlisten“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Funktion „App-Einschränkung entfernen“ in Microsoft Defender for Endpoint

Entfernen Sie bei Bedarf die Einschränkungen aller Anwendungen auf dem Gerät.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

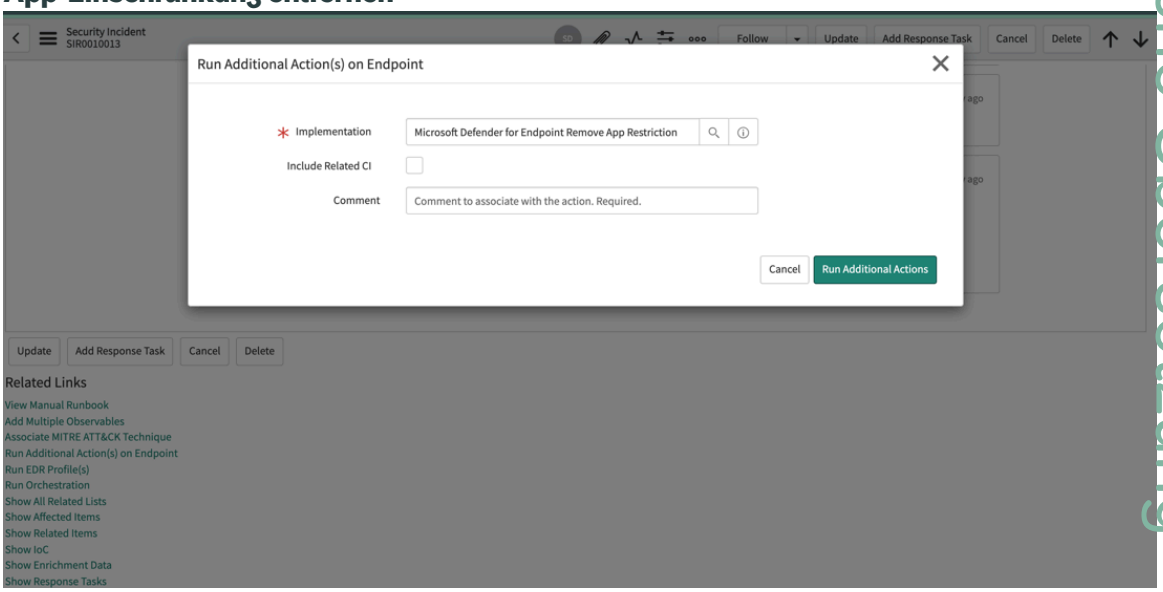
Anforderungen für die Fähigkeit „App-Einschränkung entfernen“

Eingabe	Beschreibung
Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll)

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit den Informationen zu Microsoft Defender for Endpoint überprüfen möchten.
   a. Klicken Sie im Abschnitt „zugehörige Links“ auf **Führen Sie zusätzliche Aktionen für Endpunkt aus**an.
   b. Durchsuchen und auswählen **Entfernen Sie Die App-Einschränkung** Fähigkeit.

App-Einschränkung entfernen



Alternativ können Sie die folgenden Schritte ausführen:

a. Klicken Sie im Abschnitt zugehörige Listen auf **Alle Zugehörigen Listen Anzeigen** .
b. Klicken Sie auf **Konfigurationselement** Zugehörige Liste.
c. Wählen Sie die hinzugefügten Konfigurationselemente aus.
d. Wählen Sie Aus **Führen Sie zusätzliche Aktionen für Endpunkt aus** .
Das Eingabefeld zusätzlicher Kommentar wird angezeigt.

3. Klicken Sie auf, um die App-Einschränkung zu entfernen **Zusätzliche Aktion Ausführen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.
5. Validiert den Status der Aktion in den zugehörigen Listen „zusätzliche Aktionen in Endpunktlisten“.

Konfigurieren Sie das Abrufen zugehöriger Computer aus der Defender-Fähigkeit in Microsoft Defender for Endpoint

Ruft die Liste der zugehörigen Computer bestimmter erkennbarer Elemente ab.

Vorbereitungen

Hinweis:
Unterstützte erkennbare Elemente sind Domänenname, SHA1-Hash und Anwendername.

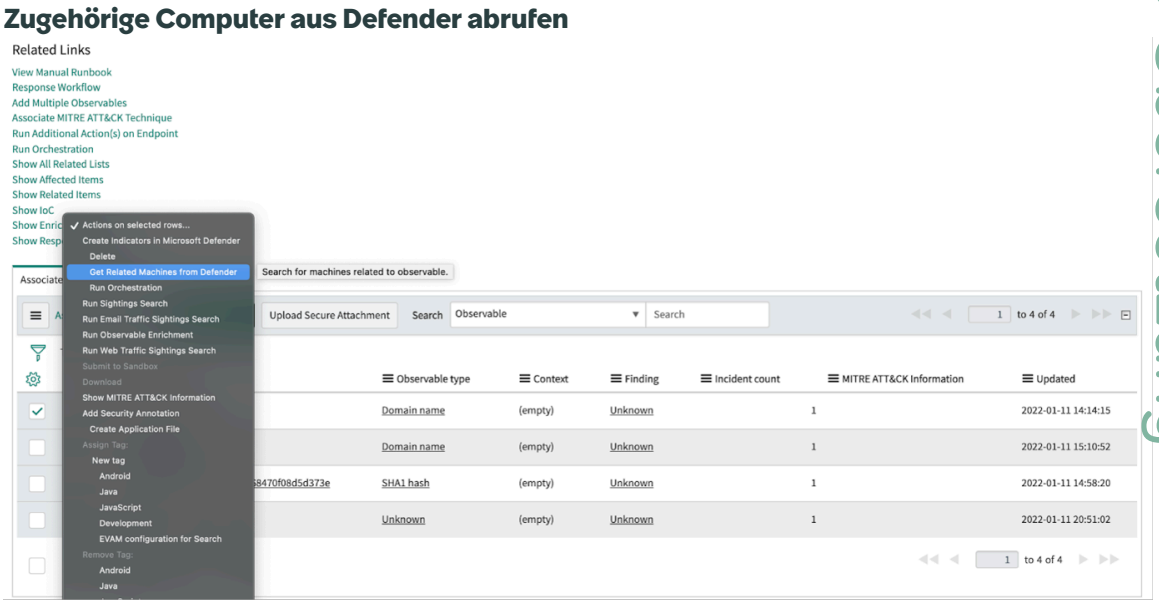
Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Liste der Computer abrufen, die auf die bestimmten erkennbaren Elemente zugegriffen haben. Sie können die Liste in der Tabelle „Details zu Microsoft Defender for Endpoint-bezogenen Computern“ speichern. Sie können die Fähigkeit zugehörige Computer aus Defender abrufen aus der zugehörigen Liste zugeordnete erkennbare Elemente auslösen.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit den Informationen zu Microsoft Defender for Endpoint überprüfen möchten.



3. Klicken Sie im Abschnitt „zugehörige Links“ auf **IOC anzeigen** .
4. Klicken Sie auf die zugehörige Liste zugeordnete erkennbare Elemente.
5. Wählen Sie die zugehörigen erkennbaren Elemente aus.
6. Wählen Sie in der Liste Aktionen die Option aus **Ruft zugehörige Computer aus Defender ab** Fähigkeit.
7. Validieren Sie den Abschnitt Automatisierungsaktivität und -Aktivitäten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Zeigen Sie die Daten an, und validieren Sie die Details zu Microsoft Defender for Endpoint-bezogenen Computern in den zugehörigen Listen.
9. Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.

Konfigurieren Sie die Funktion zum Stoppen und Quarantäne von Dateien in Microsoft Defender for Endpoint

Stoppen und Quarantäne von Dateien auf der Microsoft Defender-Plattform aus.

Vorbereitungen
Unterstützte erkennbare Typen: SHA1-Hash.

Anforderungen für die Fähigkeit zum Stoppen und Quarantäne von Dateien

Eingabe	Beschreibung
Kommentar	(Erforderlich) Kommentar, der der Aktion zugeordnet werden soll)

Erforderliche Rolle: sn_si.admin oder sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Sie können die Aktion Datei stoppen und in Quarantäne stellen nur für bestimmte erkennbare Elemente vom Typ SHA1 ausführen. Speichern Sie die Details in der Tabelle „zusätzliche Aktionen für Endpunkt“. Sie können die Funktion Datei stoppen und in Quarantäne sperren in der zugehörigen Liste Microsoft Defender for Endpoint-Details zu Computern auslösen.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit den Informationen zu Microsoft Defender for Endpoint überprüfen möchten.
3. Klicken Sie im Abschnitt „zugehörige Links“ auf **Alle Zugehörigen Listen Anzeigen** .
4. Klicken Sie auf die zugehörige Liste Microsoft Defender für Endpunktbezogene Computerdetails.
5. Wählen Sie einen oder mehrere Datensätze aus.
6. Von **Aktionen** Wählen Sie in ausgewählten Zeilen die aus **Stoppen und Datei in Quarantäne stellen** Fähigkeit.
7. Validieren Sie den Abschnitt Automatisierungsaktivität und -Aktivitäten.
8. Zeigen Sie die Daten an, und validieren Sie die Daten in den zugehörigen Listen.
9. Zeigen Sie die Automatisierungsaktivitäten der Ausführung an, und validieren Sie sie.

Erstellen und konfigurieren Sie ein Profil für die Sichtungssuche mit Microsoft Defender for Endpoint Integration

Erstellen und konfigurieren Sie das Sichtungssuchprofil automatisch mit Microsoft Defender for Endpoint.

Vorbereitungen
Erforderliche Rolle: sn_si.admin, sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können den Sichtungssuche-Workflow verwenden, um die Sichtungssuchen durchzuführen. Dieser Workflow akzeptiert eine Liste erkennbarer Elemente, findet alle Implementierungsfähigkeiten, erstellt die Abfragen, die auf den Sichtungssuchkonfigurationen basieren, und führt die Suchen aus, die auf dem konfigurierten Workflow basieren.

Die Microsoft Defender for Endpoint Stellt ein Basissystem-Sichtungssuchprofil bereit, mit dem Sie die automatischen Sichtungssuchen konfigurieren können. Mit diesem Profil können Sie auf die zugehörigen Sichtungsinformationen erkennbarer Elemente einer Organisation zugreifen und auch Sichtungen aus anderen Organisationen anzeigen.

Prozedur

1. Navigieren zu **Integrationen** > **Sichtungssuche: Konfiguration**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die folgenden Felder des Formulars aus.

Formular „Konfiguration der Sichtungssuche“

Feld	Beschreibung
Name	Name für das Sichtungssuchprofil.
Ist gespeicherte Suche	Option zum Speichern der Suchkonfiguration. Die gespeicherten Suchkonfigurationsabfragen sind Beispielabfragen. Sie können sie durch die Parameter für Ihre Umgebung ersetzen und nach Bedarf zusätzliche gespeicherte Suchkonfigurationen erstellen.
Sichtungssuchquelle	Die für die Sichtungssuche in konfigurierte Quelle Microsoft Defender for Endpoint Integration.
Suchen	Native Suchzeichenfolge, die eine Abfrage bildet.
Aktiv	Option zum Aktivieren der gespeicherten Suchkonfiguration. Nur aktive Suchkonfigurationen können eine Sichtungssuche durchführen.
Typ des erkennbaren Elements	Typ der Kategorie des erkennbaren Elements. Zum Beispiel IP-Adresse, Hash-Wert, URL und Domänenname.
Maximale Anzahl erkennbarer Elemente pro Suche	Maximale Anzahl erkennbarer Elemente, die Sie in einer Suchabfrage anzeigen können. Legen Sie diesen Wert für diese Integration auf 1 fest.
Sichtungssuchparameter	Parameter zum Definieren komplexerer Abfragen, die Logik und andere Operatoren enthalten, die vom angegebenen Protokollspeicher unterstützt werden.

4. Klicken Sie auf **Absenden**.

Führen Sie eine manuelle Sichtungssuche in durch Microsoft Defender for Endpoint

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Sichtungssuche in durch Microsoft Defender for Endpoint Dient zur Bestimmung der Verbreitung einer Bedrohung im Zeitverlauf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.admin, sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Typen erkennbarer Elemente werden unterstützt:

- Domänenname
- IP-Adresse (v4)
- IP-Adresse (V6)
- MD5-Hash
- SHA1-Hash
- SHA256-Hash

Prozedur

1. Navigieren Sie zu **Security Incidents** .
2. Öffnen Sie einen vorhandenen SIR, oder erstellen Sie einen neuen SIR.
3. Klicken Sie in den zugehörigen Links auf **IOC anzeigen** .
4. Klicken Sie auf die zugehörigen Listen der zugehörigen erkennbaren Elemente.
5. Wählen Sie die erkennbaren Elemente aus.
6. Klicken Sie in der Liste Aktionen auf **Ergänzung Erkennbarer Elemente Ausführen** .
7. Wählen Sie die erkennbaren Elemente unter aus **Aktion** Klicken Sie auf ausgewählte Zeilen, und klicken Sie auf **Sichtungssuche Ausführen** .

   Hinweis:
   Sichtungssuche wird für Domänennamen, IP-Adresse (V4), IP-Adresse (V6), MD5-Hash, SHA1-Hash, erkennbare Elemente vom Typ SHA256 und SHA256.

8. Geben Sie den Zeitrahmen für die Suche an, und klicken Sie auf **Suchen** .

   Hinweis:
   Microsoft Defender for Endpoint unterstützt Sichtungssuche nur für die letzten 30 Tage. Wenn Ihre Bereichsabfrage vor den letzten 30 Tagen liegt, ruft die Sichtungssuche keine Daten ab. Wenn sich Ihre Bereichsabfrage mit den letzten 30 Tagen überschneidet, werden nur Sichtungen aus den letzten 30 Tagen abgerufen, und wenn Ihre Bereichsabfrage innerhalb der letzten 30 Tage liegt, werden die Sichtungen von der definierten Startzeit bis zur aktuellen Uhrzeit abgerufen.

9. Validieren Sie nach Abschluss der Suche die Ergebnisse und Details in den zugehörigen Listen.
10. Klicken Sie Auf **Sichtungssuchdetails** Zum Anzeigen der Sichtungssuchdetails.
11. Klicken Sie auf **Sichtung** Registerkarte für Details und **Sichtungssuchergebnisse** Registerkarte für Suchergebnisse.

    Sie können zusätzliche Informationen zu der jeweiligen Sichtung in anzeigen **Zusammenfassung** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie eine automatische Ergänzung erkennbarer Elemente in durch Microsoft Defender for Endpoint

Führen Sie eine automatische Ergänzung erkennbarer Elemente in durch Microsoft Defender for Endpoint Dient zum Anreichern erkennbarer Elemente mit zusätzlichen Informationen aus verschiedenen Quellen.

Vorbereitungen

Überprüfen Sie, ob Sie aktiviert haben **Security Incident Response** Systemeigenschaft. Diese Option löst die Ergänzungsfunktion für erkennbare Elemente in SIR aus, wenn ein erkennbares Element einem Security Incident zugeordnet ist.

Erforderliche Rolle: sn_si.admin, sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Sie können diese Fähigkeit während Untersuchungen zur Reaktion auf Incidents verwenden, um eine identifizierte Bedrohung einzudämmen. Wenn dem Security Incident neue erkennbare Elemente zugeordnet sind, können Sie die Ergänzung erkennbarer Elemente in der Microsoft Defender for Endpoint-Fähigkeit aktivieren, dass sie automatisch ausgeführt wird.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit den Informationen zu Microsoft Defender for Endpoint überprüfen möchten.
3. Validiert die Automatisierungsaktivität, sobald die neuen erkennbaren Elemente dem Security Incident zugeordnet wurden.
4. Zeigen Sie die Ergebnisse und Ergänzungsergebnisse in der zugehörigen Liste Indikatoren des Security Incidents an.
   In der folgenden Tabelle finden Sie weitere Informationen zur Ergänzung erkennbarer Elemente.

Microsoft Defender-Indikator

Feld	Beschreibung
Indikator-ID	Identität der Indikatorentität. Klicken Sie Auf **Öffnen** Um den Datensatz im Detail anzuzeigen ServiceNow AI Platform Instanz
Erkennbares Element	Das dem Ergebnis zugeordnete erkennbare Element.
Titel	Titel für den Indikator.
Indikatortyp	Typ des Indikators.
Aktion	Vom Indikator ausgeführte Aktion.
Empfohlene Aktion	Empfohlene Aktionen für den Indikator.
Integrationslieferant	Defender-Quellintegration, aus der die Daten abgerufen werden.
Ablaufdatum	Ablaufzeit für den Indikator.
Abrufdatum	Datum, an dem der Ergänzungsdatensatz erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie eine manuelle Ergänzung erkennbarer Elemente in durch Microsoft Defender for Endpoint

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Ergänzung erkennbarer Elemente durch, um erkennbare Elemente mit zusätzlichen Informationen aus zu ergänzen Microsoft Defender for Endpoint.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Die Microsoft Defender for Endpoint Die Integration ermöglicht die Ergänzung erkennbarer Elemente für alle Typen erkennbarer Elemente, die im Modul „Zuordnung erkennbarer Elemente – Indikator“ zugeordnet sind.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit den Informationen zu Microsoft Defender for Endpoint überprüfen möchten.
3. Klicken Sie Auf **Alle zugehörigen Listen anzeigen** .
4. Klicken Sie auf **Zugeordnete Erkennbare Elemente** Registerkarte.
5. Wählen Sie die erkennbaren Elemente aus.
6. Klicken Sie in der Liste Aktionen auf **Ergänzung Erkennbarer Elemente Ausführen** .
7. Wählen Sie einen Microsoft Defender für Endpunkt aus **Quelle** Und verschieben Sie es in **Ausgewählt** Spalte, um anzugeben, welche Implementierung Sie zum Anreichern der ausgewählten erkennbaren Elemente verwenden möchten.
8. Klicken Sie auf **Absenden**.
9. Um den Status der Ausführung zu validieren, zeigen Sie die Arbeitsnotizen an.
10. Um die Ergebnisse anzuzeigen, klicken Sie auf **Microsoft Defender-Indikator** Registerkarte.
    In der folgenden Tabelle finden Sie weitere Informationen zur Ergänzung erkennbarer Elemente.

Microsoft Defender-Indikator

Feld	Beschreibung
Indikator-ID	Identität der Indikatorentität. Klicken Sie Auf **Öffnen** Um den Datensatz im Detail anzuzeigen ServiceNow AI Platform Instanz
Erkennbares Element	Das dem Ergebnis zugeordnete erkennbare Element.
Titel	Titel für den Indikator.
Indikatortyp	Typ des Indikators.
Aktion	Vom Indikator ausgeführte Aktion.
Empfohlene Aktion	Empfohlene Aktionen für den Indikator.
Integrationslieferant	Defender-Quellintegration, aus der die Daten abgerufen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ablaufdatum	Ablaufzeit für den Indikator.
Abrufdatum	Datum, an dem der Ergänzungsdatensatz erstellt wird.

Indikatoren in Microsoft Defender for Endpoint erstellen

Erstellen Sie mithilfe von Indikatoren aus zugeordneten erkennbaren Elementen des Security Incident Microsoft Defender for Endpoint.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.Analyst

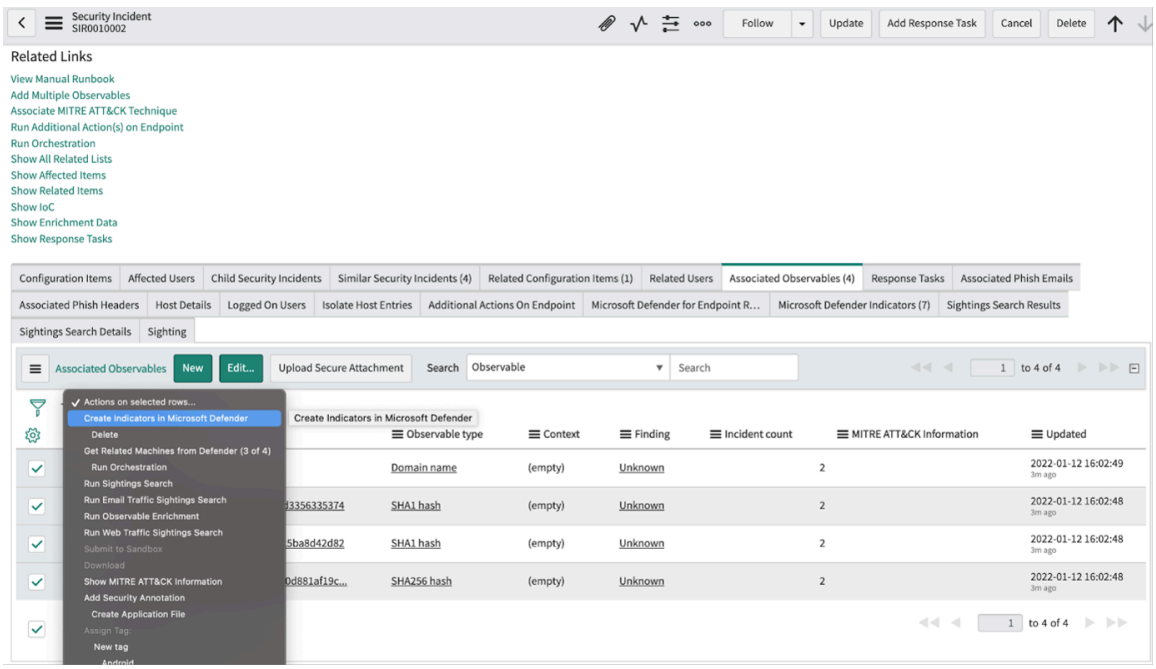
Warum und wann dieser Vorgang ausgeführt wird

Die Microsoft Defender for Endpoint Die Integration ermöglicht die Ergänzung erkennbarer Elemente für alle Typen erkennbarer Elemente, die im Zuordnungsmodul „erkennbares Element – Indikator“ zugeordnet sind.

Mit Indikatoren erstellen können Sie eine Liste von Indikatoren für die Erkennung und das Blockieren von Prävention und Antworten festlegen. Sie können die Indikatoren aus dem zugehörigen erkennbaren Element des Security Incidents erstellen.

Prozedur

1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie Indikatoren in Microsoft Defender for Endpoint erstellen möchten.
3. Klicken Sie auf die zugehörigen Listen der zugehörigen erkennbaren Elemente.
4. Fügen Sie vorhandene erkennbare Elemente hinzu, oder erstellen Sie neue erkennbare Elemente.
5. Wählen Sie die erkennbaren Elemente aus.
6. Von **Aktionen** Klicken Sie in ausgewählten Zeilen auf **Erstellen Sie einen Indikator in Microsoft Defender** .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Ausgewählte Erkennbare Elemente	Betroffene erkennbare Elemente. Diese Aktion kann verwendet werden, um Indikatoren für mehrere erkennbare Elemente zu erstellen. Wenn Sie die Auswahl eines erkennbaren Elements aufheben möchten, können Sie dies tun, indem Sie die Auswahl der erkennbaren Elemente aus der Liste aufheben. **Hinweis:** Wenn die unterstützten Typen erkennbarer Elemente nicht zugeordnet sind, werden die Indikatoren nicht in Microsoft Defender für solche erkennbaren Elemente erstellt.
Titel	Titel für den Indikator.
Beschreibung	Beschreibung für den Indikator.
Ablaufzeit	Ablaufzeit für den Indikator.
Empfohlene Aktionen	Empfohlene Aktionen, die für den Indikator ausgeführt werden müssen.
Quelle	Integrationskonfiguration zum Erstellen des Indikators.
Aktion	Aktionen, die ausgeführt werden, wenn der Indikator in der Organisation erkannt wird. Die möglichen Werte lauten wie folgt: ○ **Warnen** ○ **Blockieren** ○ **Audit** ○ **„BlockAndNachNachbessern** ○ **Zulässig**
Anwendung	Die Microsoft Defender for Endpoint-Anwendung, die dem Indikator zugeordnet ist. Dieses Feld gilt nur für einen neuen Indikator und kann nicht für einen vorhandenen Indikator verwendet werden.
Schweregrad	Schweregrad des Indikators. Die möglichen Werte lauten wie folgt: ○ **Niedrig** ○ **Zuverlässige Anzeige** ○ **Hoch**
RBAC-Gruppennamen	RBAC-Gruppennamen, auf die der Indikator angewendet wird. Die Namen befinden sich in einer kommagetrennten Liste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie Auf **Indikator Erstellen**
9. Validieren Sie die Aktivität und UI-Nachrichten.
10. Klicken Sie auf **Microsoft Defender-Indikator** Registerkarte zum Anzeigen der Ergebnisse.

Aktualisieren Sie Indikatoren in Microsoft Defender for Endpoint

Aktualisieren Sie die vorhandenen Indikatoren in Microsoft Defender for Endpoint Aus dem Listenkontextmenü oder aus der Formularansicht des Microsoft Defender-Indikators.

Vorbereitungen
Erforderliche Rolle: sn_si.admin, sn_si.Analyst

Prozedur

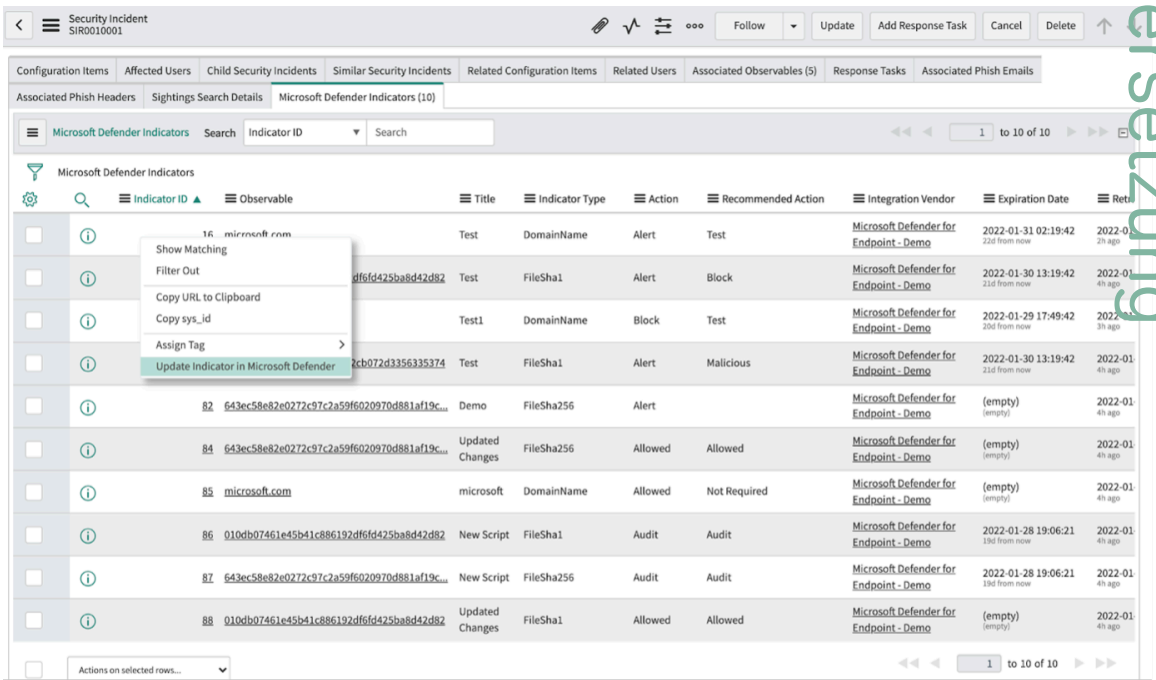
1. Navigieren zu **Security Incidents** > **Alle Incidents anzeigen**an.
2. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und klicken Sie dann auf **Microsoft Defender-Indikatoren** Registerkarte.

Hinweis:

Sie müssen die zugehörige Liste für die Microsoft Defender-Indikatoren konfigurieren, die in den zugehörigen Listen „Security Incident“ angezeigt werden. Weitere Informationen finden Sie unter Formular-UI-Aktionen .

3. Aktualisieren Sie die Microsoft Defender for Endpoint-Indikatoren auf eine der folgenden Arten:
   - Um die Indikatoren aus dem Listenkontextmenü zu aktualisieren, wählen Sie die Zeile des Indikators aus, den Sie aktualisieren möchten, und klicken Sie auf **Aktualisieren Sie den Indikator in Microsoft Defender** Option.

Aktualisieren Sie Indikatoren mithilfe des Listenkontextmenüs

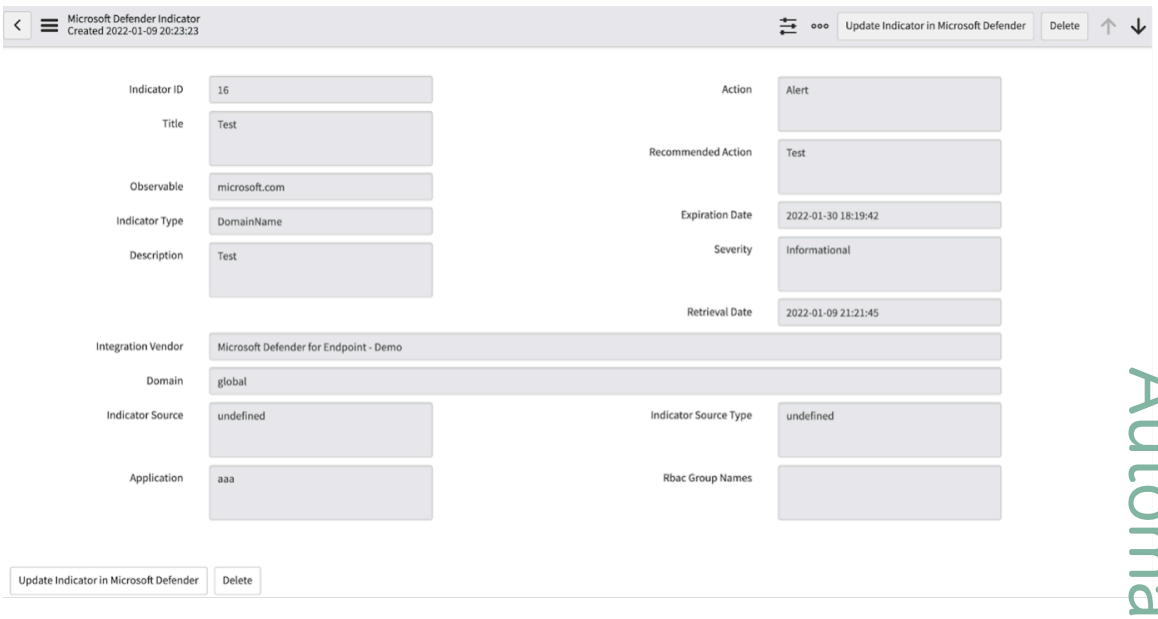


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klicken Sie auf, um die Indikatoren in der Formularansicht zu aktualisieren **Aktualisieren Sie den Indikator in Microsoft Defender** In der Formularansicht.

Aktualisieren Sie Indikatoren mithilfe der Formularansicht



4. Füllen Sie im Formular die Felder aus.

Formular „Microsoft Defender-Indikator“

Feld	Beschreibung
Titel	Titel für den Indikator.
Beschreibung	Beschreibung für den Indikator.
Ablaufzeit	Ablaufzeit für den Indikator.
Empfohlene Aktionen	Empfohlene Aktionen, die für den Indikator ausgeführt werden sollen.
Quelle	Integrationskonfiguration zum Erstellen des Indikators.
Aktion	Aktionen, die ausgeführt werden, wenn der Indikator in der Organisation erkannt wird. Die möglichen Werte lauten wie folgt: ○ **Warnen** ○ **Blockieren** ○ **Audit** ○ **BlockundNachbessern** ○ **Zulässig**
Anwendung	Die Microsoft Defender for Endpoint-Anwendung, die dem Indikator zugeordnet ist. Dieses Feld gilt nur für einen neuen Indikator und kann nicht für einen vorhandenen Indikator verwendet werden.
Schweregrad	Schweregrad des Indikators. Mögliche Werte:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Niedrig** ○ **Zuverlässige Anzeige** ○ **Hoch**
RBAC-Gruppennamen	RBAC-Gruppennamen, auf die der Indikator angewendet wird. Die Namen befinden sich in einer kommagetrennten Liste.

5. Klicken Sie Auf **Indikator Aktualisieren** .
6. Validieren Sie die Aktivität und UI-Nachrichten.

Domänentrennung in Microsoft Defender for Endpoint Integration

Domänentrennung wird in unterstützt Microsoft Defender for Endpoint Integration. Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Supportstufe

Support: Standard

Führen Sie die folgenden Schritte für die Domänentrennung aus:

1. Erstellen Sie einen Anwender mit sn_si.admin Rolle in der jeweiligen Domäne.
2. Führen Sie aus Microsoft Defender for Endpoint Integrationsverfahren in der entsprechenden Domäne.

Quotengrenzkonfiguration in Microsoft Defender for Endpoint Integration

Konfigurieren Sie das Quotenlimit der API und die Zeitüberschreitung für das Quotenlimit für Microsoft Defender for Endpoint Integration.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_si.Analyst (schreibgeschützt)

Prozedur

1. Geben Sie im Navigationsfilter ein `sys.properties.list` .
   Die gesamte Liste der Eigenschaften in der Tabelle „Systemeigenschaften“ [sys_properties] wird angezeigt.
2. Suchen und ändern Sie die folgenden Eigenschaften entsprechend Ihren Anforderungen.

Eigenschaftsname	Beschreibung
sn_sec_Defender_ep.rate_limit_timeout_in_minutes	Wenn eine Anforderung nicht innerhalb des angegebenen Zeitrahmens ausgeführt wird, wird die Ausführung angehalten, und eine entsprechende Fehlermeldung wird angezeigt. Standardwert: 75.
sn_sec_Defender_ep.Request_per_Hour_limit	Wenn der konfigurierte API-Aufruf innerhalb einer Stunde auf demselben Endpunkt erfolgt, wird

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftsname	Beschreibung
	die Anforderung in die Warteschlange gestellt, bis der Schwellenwert oder die konfigurierte Zeitüberschreitung erreicht ist. Standardwert: 1500.
sn_sec_Defender_ep.Request_per_Minute_limit	Wenn der konfigurierte API-Aufruf innerhalb einer Minute auf demselben Endpunkt erfolgt, wird die Anforderung in die Warteschlange gestellt, bis der Schwellenwert oder die konfigurierte Zeitüberschreitung erreicht ist. Standardwert: 100.
sn_sec_Defender_ep.Import_indicator_Request_per_Minute_limit	Wenn der konfigurierte API-Aufruf innerhalb einer Minute auf dem Endpunkt erfolgt, wird die Anforderung in die Warteschlange gestellt, bis der Schwellenwert oder die konfigurierte Zeitüberschreitung erreicht ist. Standardwert: 30.

Microsoft Exchange Online-Integration

Für Microsoft Exchange Online Integrationsanwendung von ServiceNow, ServiceNow AI Platform® Security Incident Response(SIR) Produkt ist in integriert Microsoft Exchange Online Service, einer der cloudbasierten Services in Microsoft Office 365-Suite von Produkten. Ihr Security Operation Center (SOC)-Analyst kann Ihre Unternehmens-E-Mail-Umgebung nach sicherheitsbezogenen Bedrohungen durchsuchen und Phishing-E-Mails mit E-Mail-Such- und -Löschfunktionen entfernen und beheben.

Übersicht über Microsoft Exchange Online Integration

Als Security Incident-Analyst führen Sie die Integration über die Schnittstelle des Sicherheitsanalysten aus, und der Workflow gibt E-Mail-Nachrichtendetails zurück, die den Suchkriterien entsprechen. E-Mail-Suchen basieren auf Kriterien, die Betreffzeilen sowie Absender- und Empfänger-E-Mail-Adressen umfassen. Nachdem die E-Mail-Suche abgeschlossen ist, können Sie verdächtige E-Mails aus dem löschen Microsoft Exchange Online Service, und ein optionaler Genehmigungsprozess kann so konfiguriert werden, dass vor dem Löschen von E-Mails eine Genehmigung angefordert wird.

Diese Integration für E-Mail-Suche und -Löschung kann mit einem breiteren Incident-Workflow oder Runbook für Phishing-Antworten verwendet werden. Nachdem ein Unternehmensanwender oder Mitarbeiter eine verdächtige E-Mail erhalten und sie dem Phishing-Antwortteam oder dem Posteingang des Unternehmens gemeldet hat, wird die gemeldete E-Mail an weitergeleitet ServiceNow AI Platform Und als Security Incident kategorisiert. Nachdem Sie verifiziert haben, dass eine E-Mail ein Phishing-Angriff ist, können Sie als Analyst, der für die Untersuchung von Phishing-Incidents verantwortlich ist, eine E-Mail-Suche initiieren, um festzustellen, ob andere Unternehmensanwender diese Phishing-E-Mail erhalten haben. Mit der Suche können Sie zugehörige E-Mails aus derselben Phishing-Kampagne finden und andere potenzielle Opfer identifizieren, die die E-Mail erhalten haben, sie lesen und möglicherweise auch auf eine schädliche URL geklickt oder einen Anhang geöffnet haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselfunktionen

Die Integration umfasst die folgenden wichtigen Funktionen:

- Konfigurieren Sie Suchkriterien für Phishing-Bedrohungen in Security Incident Response basierend auf Kombinationen der Felder Absender, Empfänger und Betreff in E-Mail-Nachrichten.
- Bei großen und langen E-Mail-Suchen wird der Security Incident-Analyst per E-Mail benachrichtigt, wenn die Suche erfolgreich abgeschlossen wurde, zusammen mit der Anzahl der übereinstimmenden Nachrichten.
- Der Status für einzelne Nachrichten informiert Sie, ob Empfänger verdächtige E-Mails gelesen oder gelöscht haben.
- Wenn konfiguriert, stellen optionale Genehmigungsprozesse sicher, dass verdächtige E-Mails nicht ohne vorherige Genehmigung gelöscht werden.
- Ein vollständiger Audit-Pfad für Löschanforderungen, der die Anzahl der gelöschten E-Mails enthält, wird in den Arbeitsnotizen von Security Incidents protokolliert.
- Wenn Tagging konfiguriert ist, werden Sicherheits-Tags aufgezeichnet, wenn E-Mail-Such- und Löschungs-Workflows für Security Incidents initiiert und erfolgreich abgeschlossen werden.

Unterstützt Microsoft Exchange Online Versionen

Diese Integration unterstützt Microsoft Exchange Online Services, die Teil von sind Microsoft Office 365-Suite. Die Integration unterstützt keine gehosteten Elemente Microsoft Exchange-Umgebungen. Microsoft Wird ausgeführt Microsoft Exchange Online Services in der Exchange 2016-Version.

Voraussetzungen

Das Plugin „com.snc.si_dep“ ist für jeden erforderlich ServiceNow AI Platform Version. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Anwendungen.

Folgendes Security Operations Anwendungen müssen über installiert und aktiviert werden ServiceNow Store. Installieren und aktivieren Sie jeweils eine Anwendung in der unten aufgeführten Reihenfolge, um eine reibungslose Installation sicherzustellen:

1. Sicherheits-Integrations-Framework
2. Security Support Common
3. Orchestration Des Sicherheitssupports
4. Security Incident Response

Richten Sie Ihr ein Microsoft Azure-Account

Führen Sie die folgenden Setup-Aufgaben in Ihrem aus Microsoft Azure-Portal vor der Installation von ServiceNow Anwendung für diese Integration. Dieser Account ermöglicht den Zugriff auf Microsoft Exchange Online Mandant für E-Mail-Nachrichtendetails.

Vorbereitungen

Erforderliche Rolle: Microsoft Azure-Portal-Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Account ist für den Zugriff auf erforderlich Microsoft Exchange Online Mandant zum Sammeln zusätzlicher E-Mail-Nachrichtendetails und zum Löschen von E-Mail-Nachrichten. Dieser Account wird in eingerichtet Microsoft Azure-Portal.

Die Images in den folgenden Aufgaben sind privilegiert und proprietär und werden mit der Berechtigung von verwendet Microsoft. Dieser Inhalt unterliegt Aktualisierungen von Microsoft. Informationen zum Überprüfen, ob Sie Zugriff auf den neuesten Inhalt haben, finden Sie unter Microsoft-Dokument Website.

In den folgenden Bildern: ServiceNow Inc.. Wird für den Accountnamen in den Beispielen für das Azure-Portal angezeigt. In Ihrem Azure-Portal-Account wird der Unternehmensname für Ihren Account im Azure-Portal angezeigt.

Prozedur

Wenn Sie keine Anwendungs-ID für die OAUTH-Authentifizierung in erstellt haben Microsoft Führen Sie die folgenden Schritte aus: Azure-Portal.

a. Melden Sie sich bei an Microsoft Azure-Portal mit Ihren Azure-Portal-Administratoranmeldeinformationen.

b. Geben Sie Ein **App-Registrierungen** In **Suchen** Feld.

c. Wählen Sie Aus **Neue Registrierung** .

d. Füllen Sie das angezeigte Formular „Anwendung registrieren“ aus.

Feld	Beschreibung
Name	Name für die Anwendung. In diesem Beispiel ServiceNow Exchange Online-Integration Ist eingegeben.
Unterstützte Account-Typen	Wählen Sie für diesen Account unter unterstützte Accounttypen die Option aus **Accounts nur in diesem Organisationsverzeichnis (Name der Organisation)** . Diese Domäne wird für die E-Mail-Suche verwendet.
Umleitungs-URL (optional)	Wenn Sie einen Wert für dieses Feld eingeben, wird er nicht von der Integration verwendet.

e. Wählen Sie **Registrieren** aus.
Eine Anwendungs-ID wird erstellt. Diese ID ähnelt einem Anwendernamen. Sie geben diesen Wert auf der Konfigurationsseite in ein **OAUTH-Anwendungs-ID** Feld während des Konfigurationsschritts in Ihrem ServiceNow AI Platform Instanz, die in beschrieben wird Konfigurieren Sie Microsoft Exchange Online Integration.

f. Unter **Verwalten** Auswählen, **Manifest** .

g. Suchen Sie nach **ErforderlichResourceAccess** Eintrag (in oder über Zeile 52).

h. Ändern **ResourceAppId** , **ResourceAccess-ID** , Und **ResourceAccess-Typ** Werte mit dem folgenden Code-Fragment:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"requiredResourceAccess": [
        {
                "resourceAppId": "00000003-0000-0000-c000-000000000000",
                "resourceAccess": [
                        {
                                "id": "e2a3a72e-5f79-4c64-b1b1-878b674786c9",
                                "type": "Role"
                        },
                        {
                                "id": "dd98c7f5-2d42-42d3-a0e4-633161547251",
                                "type": "Role"
                        }
                ]
        }
  ],
```

i. Wählen Sie **Speichern**.

j. Unter **Verwalten** Auswählen, **API-Berechtigungen** .

k. Wählen Sie Aus **Fügen Sie eine Berechtigung hinzu** .

l. Wählen Sie im angezeigten Bereich API-Berechtigungen anfordern die Option aus **Microsoft Graph** .

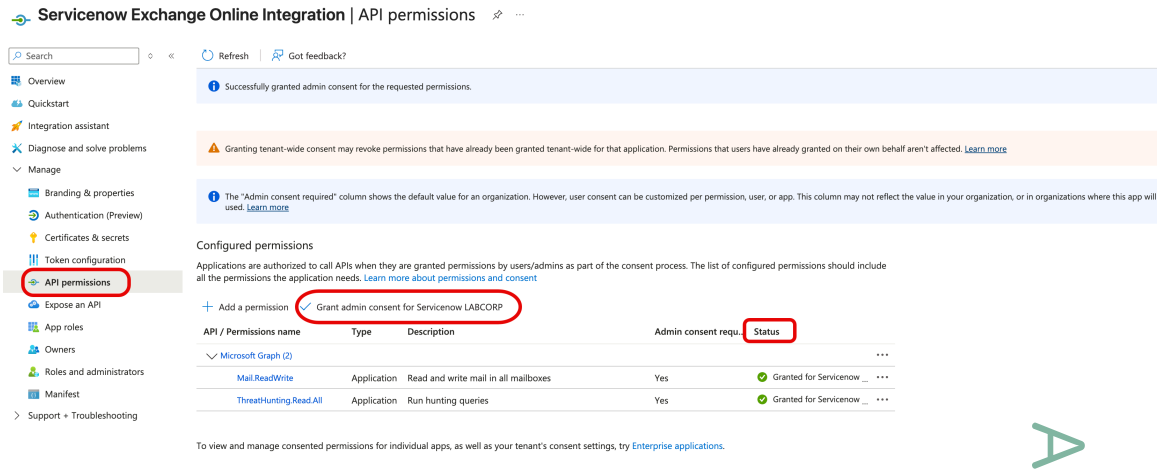
m. Wählen Sie im angezeigten Bereich API-Berechtigungen anfordern die Option aus **Anwendungsberechtigungen** .

n. Geben Sie im angezeigten Feld Berechtigungen auswählen ein **Bedrohung** Und wählen Sie aus **ThreatHunting.Lesen.alle** Kontrollkästchen.

o. Wählen Sie Aus **Erteilen Sie die Zustimmung des Administrators für <Organization>** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

p. Wählen Sie **Ja**.
Die **Status** Wert muss jetzt sein **Gewährt für**



<Organization>.

Nächste Maßnahme

Sie sind bereit, Ihren einzurichten ServiceNow AI Platform® Instanz für die Integration.

Installieren Microsoft Exchange Online Anwendung

Bevor Sie die Integration auf Ihrer Instanz ausführen, installieren Sie Microsoft Exchange Online Anwendung für die Integration aus dem ServiceNow Store.

Vorbereitungen

Bevor Sie die Anwendung aus installieren ServiceNow Store Auf Ihrem ServiceNow AI Platform Führen Sie alle Aufgaben aus, die in den erforderlichen Prüflisten aufgeführt sind.

Erforderliche Rolle: Administrator

Prozedur

1. Wenn Sie die Anwendung für die Integration nicht installiert haben, finden Sie weitere Informationen unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Nachdem Sie die Anwendung über installiert haben ServiceNow Store, Konfigurieren Sie es, um eine Verbindung mit herzustellen ServiceNow AI Platform Instanz.

Konfigurieren Sie Microsoft Exchange Online Integration

Nachdem Sie die Anwendung über installiert haben ServiceNow Store, Konfigurieren Sie es, um eine Verbindung mit herzustellen ServiceNow AI Platform Instanz. Diese Aktivierung aktiviert die Such- und Löschungs-Workflows.

Vorbereitungen

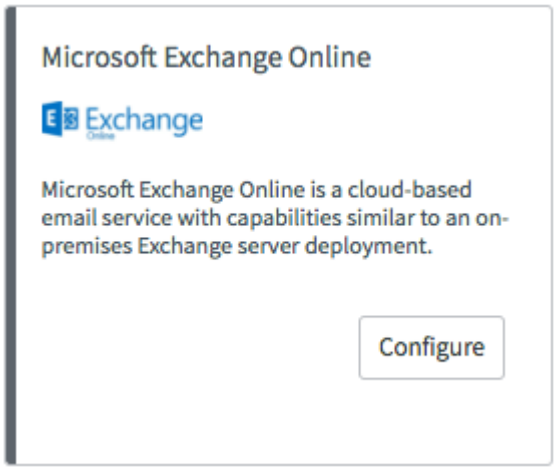
Erforderliche Rolle: sn_si.admin

Prozedur

1. In Ihrem ServiceNow AI Platform Instanz, navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
2. Suchen Sie nach Microsoft Exchange Online Kachel.
3. Klicken Sie auf **Konfigurieren**.

Automatische Übersetzung

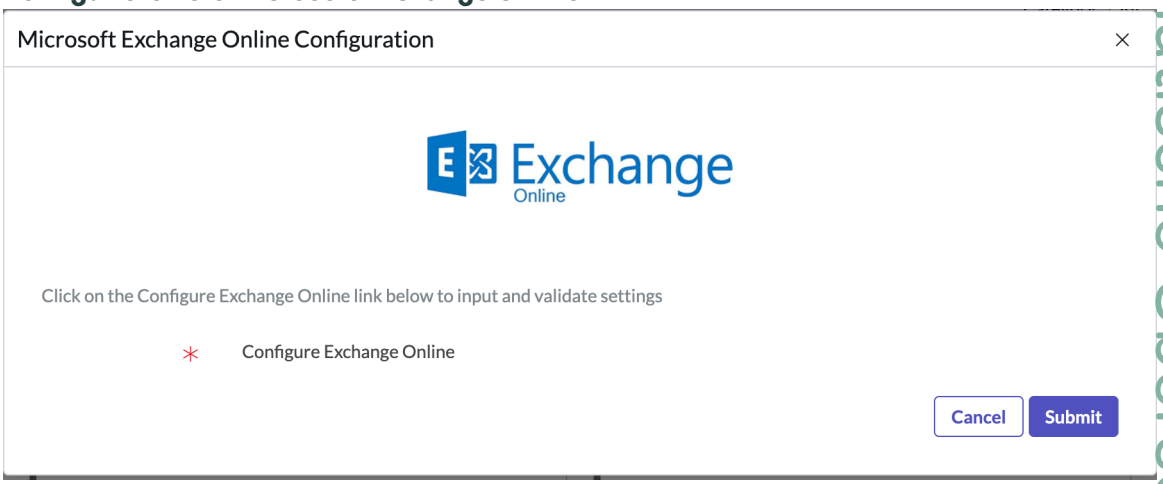
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



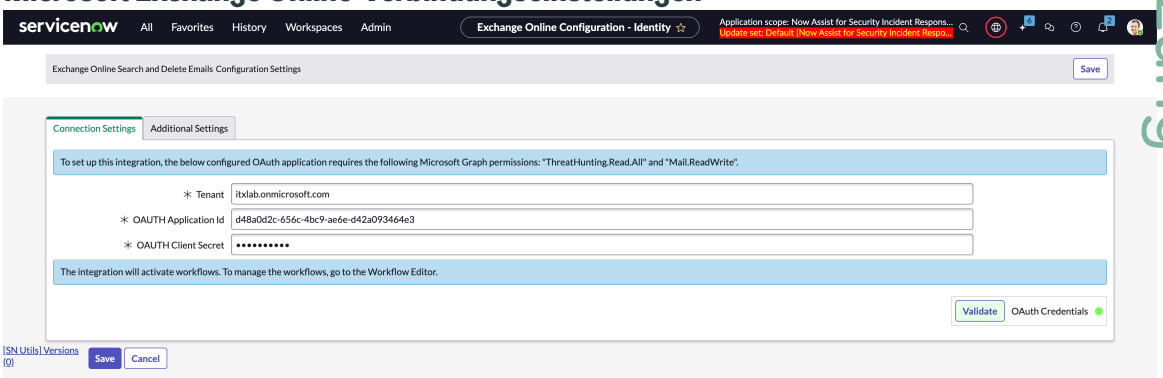
4. In Microsoft Exchange Online Klicken Sie auf das angezeigte Konfigurationsdialogfeld **Konfigurieren Sie Exchange Online** .

   Ein Beispiel für ein ausgefülltes und validiertes Formular folgt der Tabelle.

Konfigurieren Sie Microsoft Exchange Online



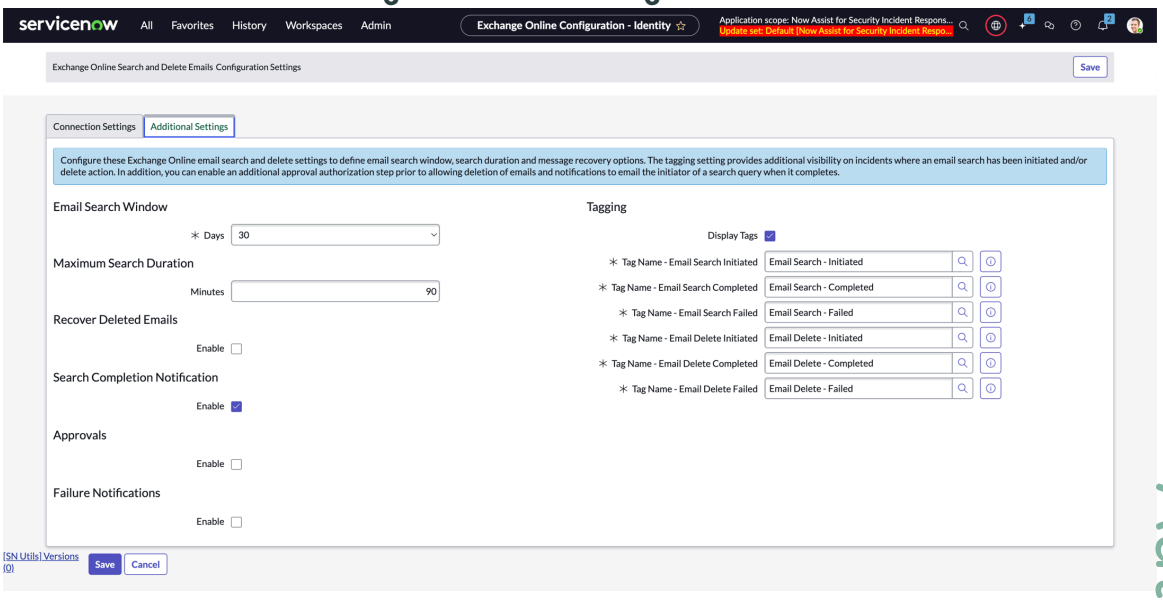
Microsoft Exchange Online-Verbindungseinstellungen



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Microsoft Exchange Online-Einstellungen



5. Wählen Sie eine, um fortzufahren.

Trouble?
Wenn eine Fehlermeldung angezeigt wird oder einer oder mehrere der Indikatoren rechts neben der Schaltfläche Validieren rot sind, überprüfen Sie, ob die von Ihnen eingegebenen Anwenderaccount-Anmeldeinformationen gültig sind. Geben Sie Ihre Anmeldeinformationen ein und klicken Sie auf **Speichern** Erneut.

Weitere Informationen zu finden Sie in der folgenden Tabelle **Validieren** Schaltfläche und die farbigen Symbole.

Status der Schaltfläche „Validieren“ und der Indikatoren	Beschreibung
Die Schaltfläche „Validieren“ ist grün, und alle kleinen farbigen Indikatoren sind grün.	Gibt an, dass die MID-Server-Verbindung und die Anmeldeinformationen gültig sind.
Die Schaltfläche „Validieren“ ist hellrot mit einem blauen Rahmen, und einer oder alle kleinen farbigen Indikatoren sind orange.	Die Validierung wird ausgeführt. Die Validierung kann einige Minuten dauern.
Die Schaltfläche „Validieren“ ist hellrot, und einer oder alle kleinen farbigen Indikatoren sind rot.	• Die Schaltfläche „Exchange Online-zertifikatbasierte Authentifizierung“ oder „OAuth-Anmeldeinformationen“ ist rot: Gibt an, dass die Exchange Online-Anmeldeinformationen ungültig sind. • Die Schaltflächen „Exchange Online-zertifikatbasierte Authentifizierung“ und „MID-Server bereit“ sind rot: Gibt an, dass der MID-Server nicht erreichbar ist und daher die zertifikatbasierte Exchange

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status der Schaltfläche „Validieren“ und der Indikatoren	Beschreibung
	Online-Authentifizierung über den MID-Server fehlgeschlagen ist. • Der Indikator für die zertifikatbasierte Authentifizierung von Exchange Online ist rot, aber die Schaltfläche „MID-Server bereit“ ist grün: Gibt an, dass der MID-Server aktiv und korrekt konfiguriert ist, die zertifikatbasierte Authentifizierung von Exchange Online jedoch falsch ist.

Definieren Sie E-Mail-Suchkriterien, und fordern Sie eine Suche im an Microsoft Exchange Online Service

Definieren Sie als Anwender mit der Rolle „sn_si.Analyst“ Suchkriterien, und senden Sie eine E-Mail-Suchanforderung basierend auf Incident-Details in einem Security Incident-Datensatz.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Die Zahlen in diesem Verfahren werden mit angezeigt **Formulare mit Registerkarten** In Systemeinstellungen ausgewählt. Weitere Informationen zum Auswählen und Löschen von Formularen mit Registerkarten finden Sie im Abschnitt Formulare mit Registerkarten anzeigen in Formularlayout für konfigurieren ServiceNow-Produktdokumentationswebsite .

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Der Status einzelner Nachrichten, die der Suchabfrage entsprechen, und die Suchergebnisse werden im Security Incident-Datensatz gemeldet. Wenn E-Mail-Benachrichtigungen aktiviert sind, können Sie die Suchergebnisse aus einer E-Mail-Nachricht anzeigen.

Suchkriterien können Absenderadressen, Empfängeradressen oder Betreffnamen von Nachrichten umfassen. Die folgenden Kombinationen von Suchparametern für Nachrichtenbetreff, Absender und Empfänger werden häufig verwendet, um Phishing-bezogene E-Mail-Nachrichten zu finden, die Teil einer einzelnen Phishing-Kampagne sein können:

- Alle ursprünglichen E-Mails suchen, die von einem Phishing-Account gesendet wurden: Suche nach Absender.
- Suchen Sie alle ursprünglichen E-Mails für eine einzelne Phishing-Kampagne: Suchen Sie nach Betreff und Absender.
- Alle E-Mails suchen, die für eine einzelne Phishing-Kampagne empfangen wurden (Original und weitergeleitet, beliebiger Absender): Suche nach Betreff.
- Suchen Sie alle weitergeleiteten E-Mails für eine einzelne Phishing-E-Mail von einem einzelnen Anwender: Suchen Sie nach Empfänger + Betreff.
- Suchen Sie alle Phishing-bezogenen E-Mails, die an einen einzelnen Anwender gesendet wurden: Suchen Sie nach Absender + Empfänger.

Hinweis:

Suchvorgänge werden anhand von E-Mails durchgeführt, die innerhalb der letzten 30 Kalendertage gesendet oder empfangen wurden, es sei denn, während des ersten Setups wird ein kürzeres Suchfenster konfiguriert. Eine erfolgreiche E-Mail-Suche ist erforderlich, bevor Sie E-Mails löschen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beispiel zeigt, wie Sie eine Suche von einem aus initiieren ServiceNow AI Platform Security Incident. Ein Security Incident wird basierend auf der ursprünglichen E-Mail eines vermuteten Phishing-Angriffs in erstellt Microsoft Exchange Online Server Ihrer Organisation. In diesem Beispiel sind die Suchkriterien Absender (von) plus Betreff (wobei) Von Ist phisher@cbazyx.com , Und Betreff Ist Melden Sie sich bei Ihrem Account an .

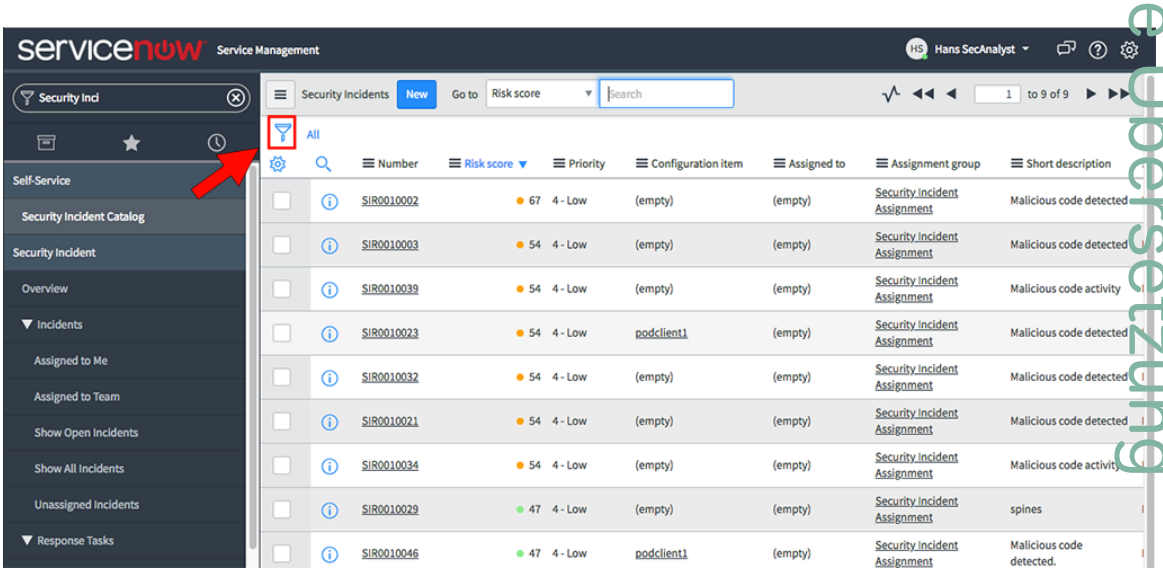
Ergebnisse für die Suche nach Themen werden zurückgegeben, wenn die Suche Textzeichenfolgen findet, die Schlüsselwörter enthalten, die den eingegebenen Suchkriterien entsprechen. In diesem Beispiel lautet der Betreff Melden Sie sich bei Ihrem Account an . Verwenden Sie **UND** Operator zum Trennen der Suchbedingungen von und Betreff, um Ergebnisse für alle E-Mail-Nachrichten zurückzugeben, die diese angegebenen Suchkriterien enthalten. Die folgenden Schritte beschreiben, wie Sie eine Suche einrichten, die nur E-Mails findet, die Betreffzeilentext enthalten, der von einem bestimmten Phishing-Account gesendet wird.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen** Und suchen Sie den Security Incident, mit dem Sie arbeiten.
2. Alternativ führen Sie die folgenden Schritte aus, um einen Filter festzulegen und auszuführen, sodass nur Security Incidents angezeigt werden, die durch Phishing-Ereignisse erstellt wurden.

   a. Navigieren zu **Security Incident** > **Alle Incidents anzeigen** Zum Öffnen der Liste Security Incidents.

   b. Klicken Sie in der oberen linken Ecke der angezeigten Liste auf das Filtersymbol.

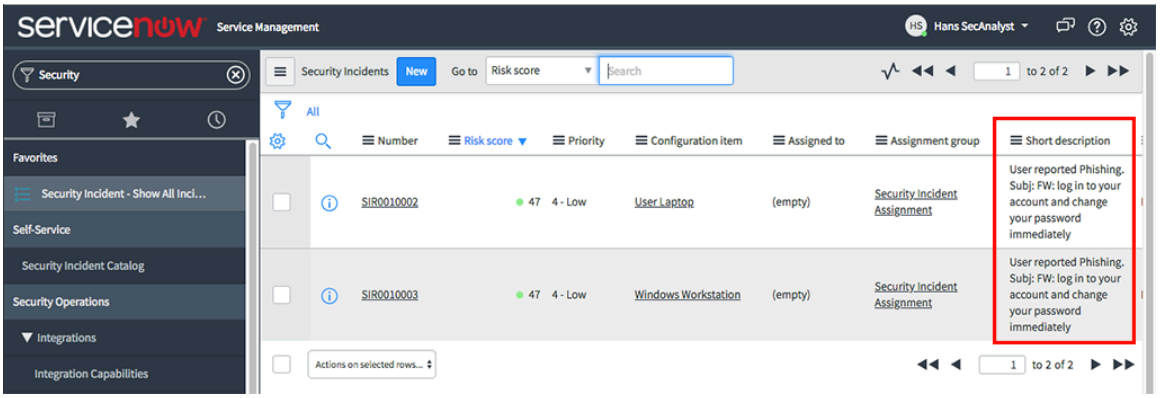


   c. Wählen Sie in den angezeigten Feldern die Option aus **Kurzbeschreibung** > **enthält** Geben Sie in den Auswahllisten ein **Anwender hat Phishing gemeldet** Und klicken Sie auf **Ausführen** .

   Die Phishing-bezogenen Security Incidents werden angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

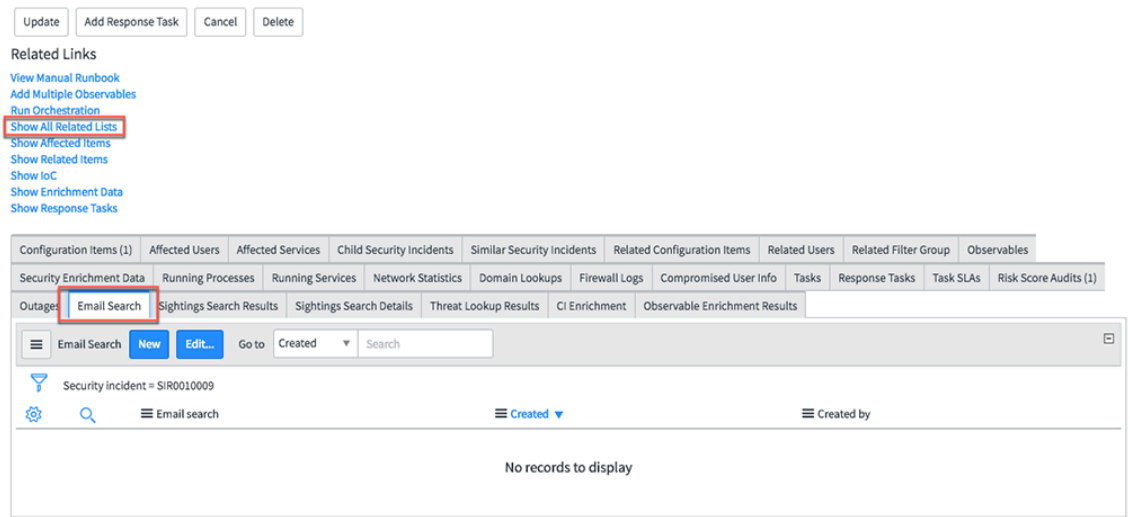


d. Verwenden Sie den Text in der Spalte „Kurzbeschreibung“, um den Security Incident zu finden, mit dem Sie arbeiten.

e. Klicken Sie in der Spalte Nummer auf einen Security Incident, um einen Datensatz zu öffnen.

3. Scrollen Sie zum Ende des Security Incident-Datensatzes, und klicken Sie auf die zugehörige Liste E-Mail-Suche.

Wenn die zugehörige Liste E-Mail-Suche nicht angezeigt wird, klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Zugehöriger Link zum Anzeigen dieser zugehörigen Liste.



4. Klicken Sie in der zugehörigen Liste E-Mail-Suche auf **Neu** Dient zum Erstellen eines neuen E-Mail-Suchdatensatzes.
Das Formular „E-Mail-Suche“ wird angezeigt. Wenn Sie feststellen, dass Sie diese Suchabfrage für denselben Phishing-bezogenen Incident mit geringfügigen Änderungen erneut ausführen möchten, können Sie diesen Suchabfragedatensatz erneut verwenden. Es ist jedoch unwahrscheinlich, dass Sie diese Suche für einen anderen Phishing-bezogenen Incident verwenden, da Phishing-Kampagnen dynamisch sind und sich die Absender- und Nachrichtenfelder häufig ändern.

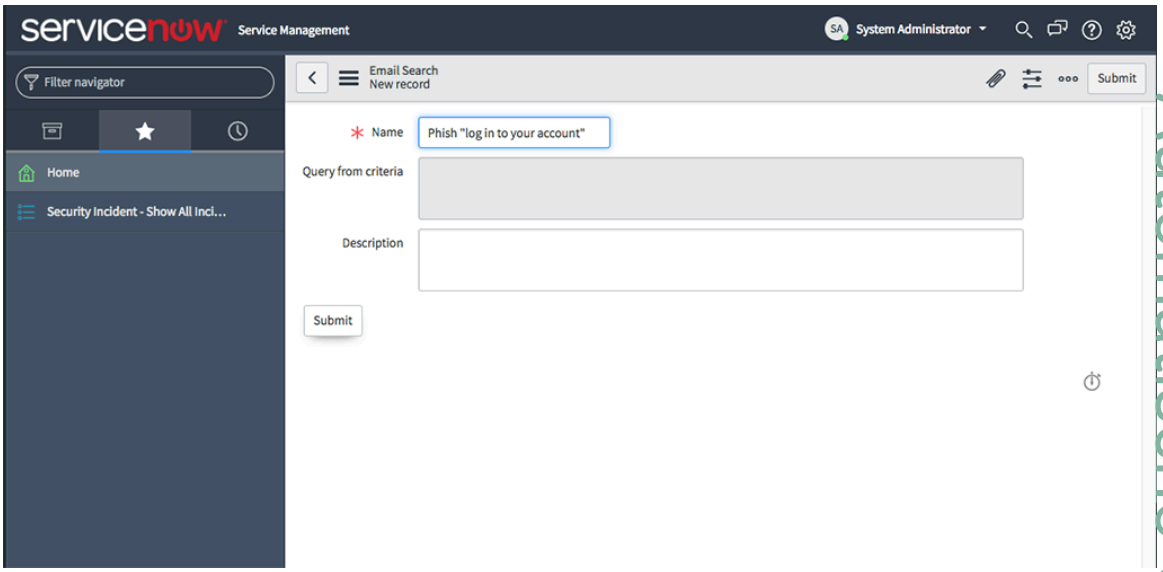
5. **Wahlweise:** Klicken Sie auf, um einen vorhandenen Suchabfragedatensatz zu bearbeiten **Bearbeiten** .

6. Füllen Sie die Felder im Formular „E-Mail-Suche“ aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

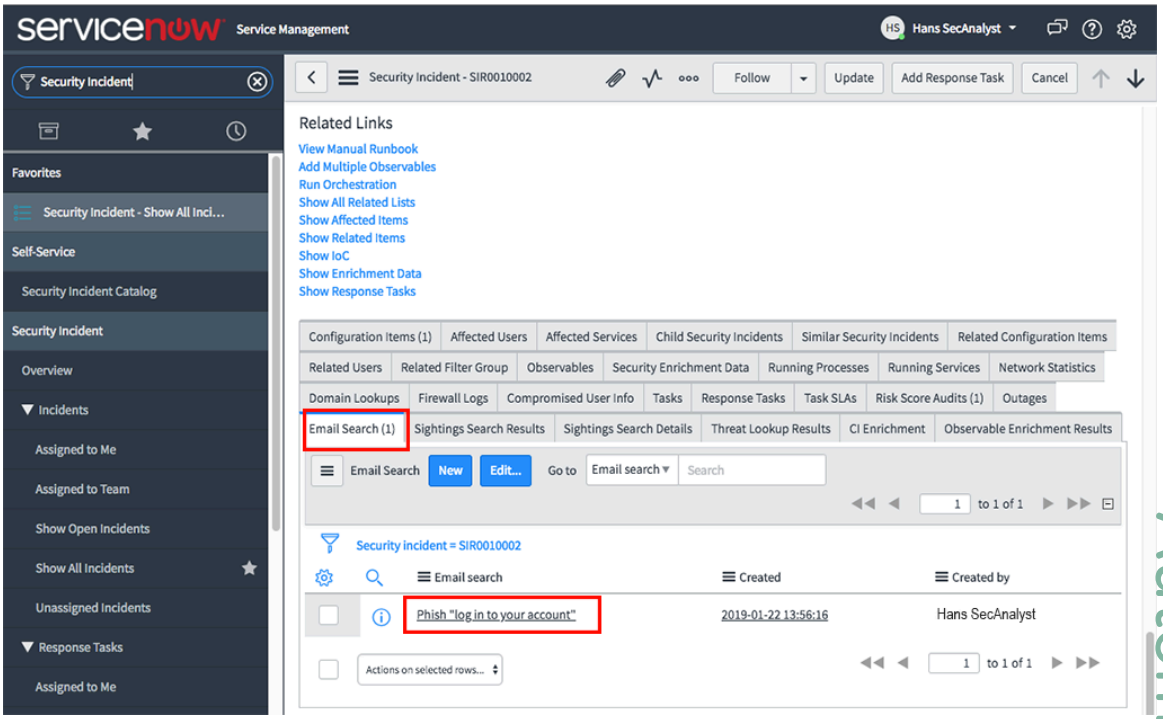
Feld	Beschreibung
Name	Informationen zur Beschreibung der Art der Suche. In diesem Beispiel ist ein Name für eine von + Betreffsuche Phishing „bei Ihrem Account anmelden“ .
Beschreibung	Informationen zur Suche auf dem E-Mail-Server. Ein Beispiel für diese Suche ist Ab=phisher@cbazyx.com + Betreff=melden Sie sich bei Ihrem Account an .



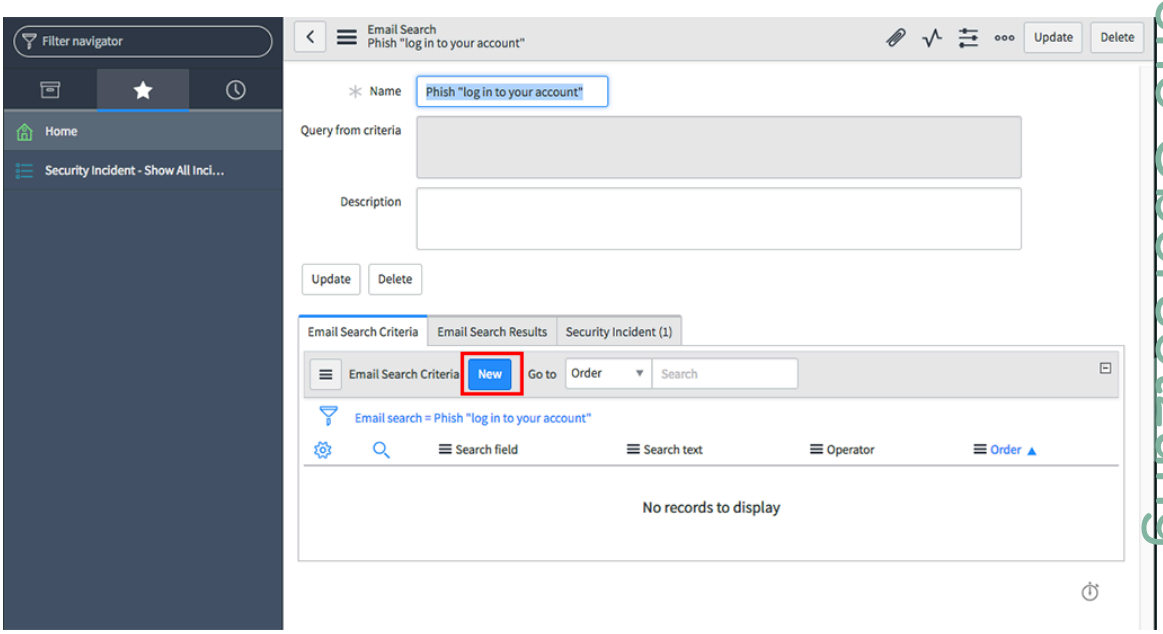
7. Klicken Sie auf **Absenden**.
   Der Security Incident wird angezeigt, und der Name der E-Mail-Suche wird in der Spalte E-Mail-Suche in der zugehörigen Liste E-Mail-Suche angezeigt. Bevor Sie diese neue Suchabfrage verwenden können, müssen Suchkriterien für den Suchdatensatz definiert werden.
8. Um Suchkriterien zu definieren, klicken Sie in der Spalte E-Mail-Suche auf die zugehörige Liste E-Mail-Suche **Phishing „bei Ihrem Account anmelden“** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Klicken Sie im angezeigten E-Mail-Suchdatensatz auf die zugehörige Liste E-Mail-Suchkriterien, und klicken Sie auf **Neu** .



10. Füllen Sie die Felder im Formular „E-Mail-Suchkriterien“ aus.

Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

Feld	Beschreibung
E-Mail-Suche	Das Feld wird automatisch mit dem Namen ausgefüllt, den Sie für den E-Mail-Suchdatensatz eingegeben haben.

Automatische Übersetzung

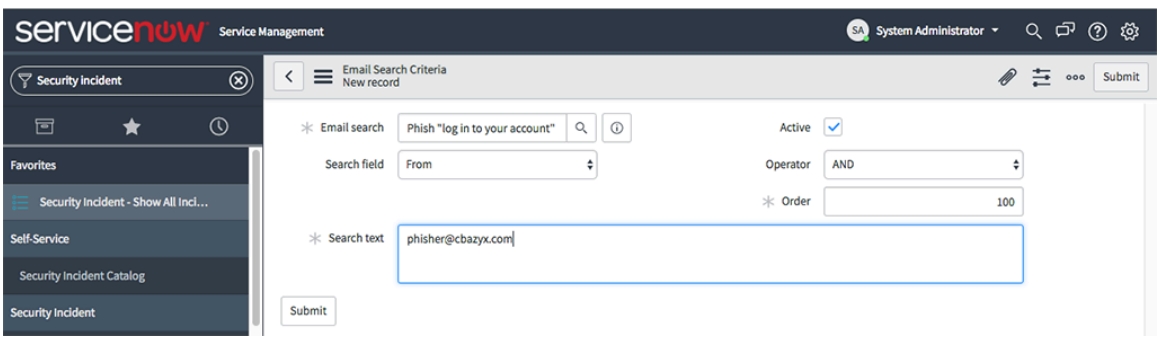
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Suchsymbol	Suchen Sie mithilfe der Liste. Eine Liste gespeicherter Suchvorgänge. Klicken Sie auf das Symbol, um eine Liste der gespeicherten E-Mail-Suchen zu öffnen. Klicken Sie auf ein Element in dieser Liste, um die aktuelle Suche zu entfernen und eine zuvor gespeicherte E-Mail-Suche auszuwählen.
Informationssymbol	Symbol zum Anzeigen des E-Mail-Suchdatensatzes. Klicken Sie auf das Symbol, um den E-Mail-Suchdatensatz anzuzeigen.
Suchfeld	Suchkriterium (**Betreff** , **Von** , Oder **Empfänger**). Wählen Sie das Suchkriterium aus der Auswahlliste aus, und definieren Sie einen Wert, nach dem Sie im Textfeld suchen möchten. Beginnen Sie in diesem Beispiel mit ab `phisher@cbazyx.com` (Die E-Mail-Adresse des Absenders der Phishing-E-Mail).
Aktiv	Option zum Aktivieren der Suche. Die Suche ist standardmäßig aktiviert. Wenn Sie diese Option deaktivieren, wird dieser Datensatz nicht in eine Suche aufgenommen.
Operator	Operatoren (**UND** , **ODER**), um Ihre Suche weiter zu definieren. **UND** : Das System sucht nach den Bedingungen getrennt durch **UND** Und gibt nur Ergebnisse zurück, wenn alle Bedingungen erfüllt sind. Verwenden Sie für die Suche nach Absender und Betreff die **UND** Operator, damit beide Suchbedingungen während der E-Mail-Suche erfüllt werden. Verwenden Sie für dieses Beispiel die **UND** Operator, damit die Abfrage von (Absender) = stammt `phisher@cbazyx.com` **UND** Betreff = `Melden Sie sich bei Ihrem Account an` . **ODER** : Das System sucht und gibt Ergebnisse zurück, wenn eine der Bedingungen durch getrennt ist **ODER** Sind erfüllt. Ein Beispiel ist von (Absender) = `phisher@cbazyx.com` **ODER** Von (Absender) = `phisher-2@cbazyx.com` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Reihenfolge	Wenn Sie mehr als zwei Suchbedingungen eingeben, verwenden Sie Reihenfolge, um die Bedingungen zu priorisieren. 100 ist der Standard. Geben Sie für jede Bedingung einen Wert zwischen 1 und 100 ein, z. B. 100, 95, 90, 80. Die Bedingung mit der niedrigsten zugewiesenen Zahl hat die höchste Suchpriorität innerhalb einer Gruppe von Bedingungen.
Suchtext	Die Textwerte (Stichwörter) für die Suche (E-Mail-Adressen oder Betreffzeilen). Das Suchfeld enthält den in der Suche verwendeten Text, z. B. phisher@cbazyx.com . Damit die Suche Ergebnisse für die Absender- und Empfängersuche genau zurückgibt, müssen die Suchzeichenfolgen genau übereinstimmen. Bei Betreffsuchen kann die Suchzeichenfolge Stichwörter enthalten, die Teil einer größeren Zeichenfolge sind. Beispielsweise kann ein Betreff die genaue Suchzeichenfolge enthalten, die in einem weitergeleiteten Header oder einem Antwortnachrichten wie abgeglichen wird FW: Melden Sie sich bei Ihrem Account an, und ändern Sie Ihr Passwort sofort . Beispiel: Melden Sie sich bei Ihrem Account an Sind genaue Stichwörter in der Zeichenfolge Melden Sie sich bei Ihrem Account an, und ändern Sie Ihr Passwort sofort . Zur Unterstützung von ist keine Platzhalterbezeichnung (*) erforderlich *Enthält* Typ der Suche. Derzeit ist keine Filtermethode zum Abgleichen einer genauen Suchzeichenfolge vorhanden, die nicht Teil einer größeren Textzeichenfolge ist.

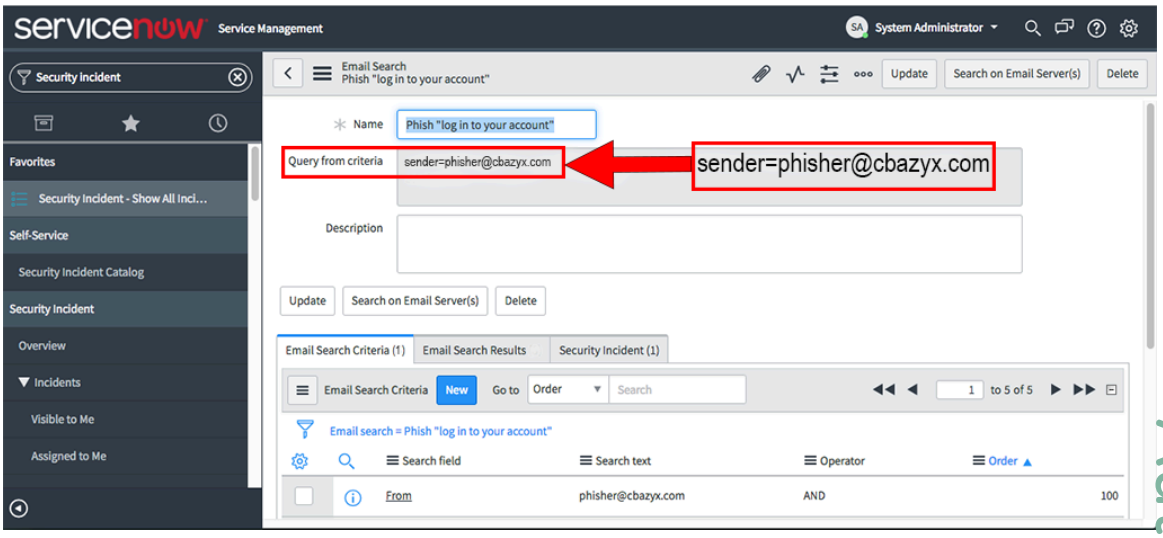
Automatische Übersetzung



11. Klicken Sie auf **Absenden**.

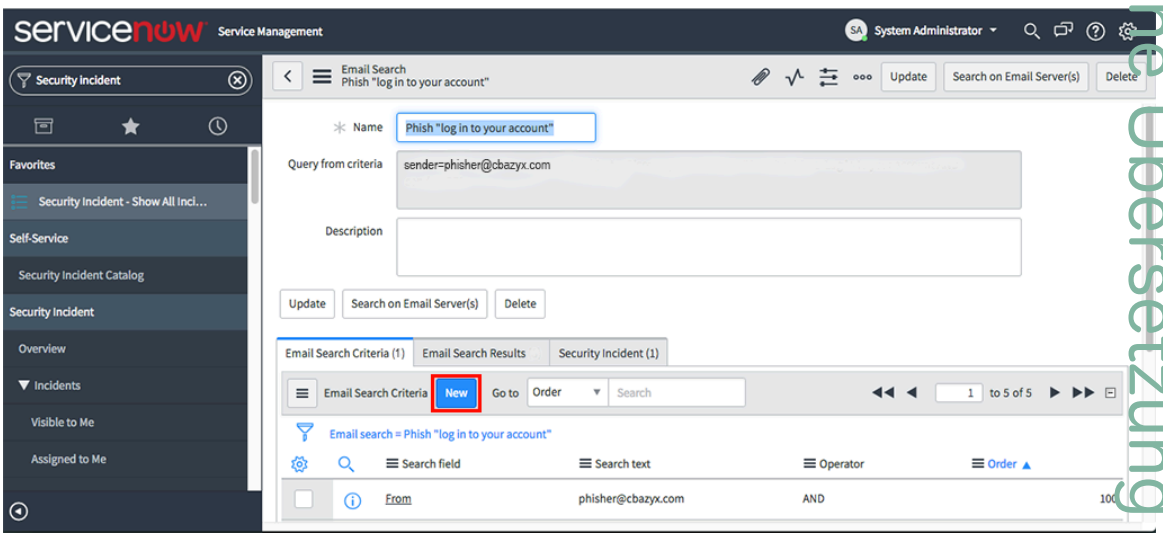
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Datensatz „E-Mail-Suche“ wird angezeigt. In **Abfrage aus Kriterien** Feld werden die Suchkriterien angezeigt, die Sie für den Absender (von) hinzugefügt haben.



12. Um diese E-Mail-Suchkriterien mit weiteren Informationen zu aktualisieren, damit die Abfrage die gewünschte Bedingung „Betreff plus Absender“ enthält, führen Sie die Schritte aus, um eine weitere Suchbedingung hinzuzufügen.

a. Klicken Sie in der zugehörigen Liste E-Mail-Suchkriterien auf **Neu** .



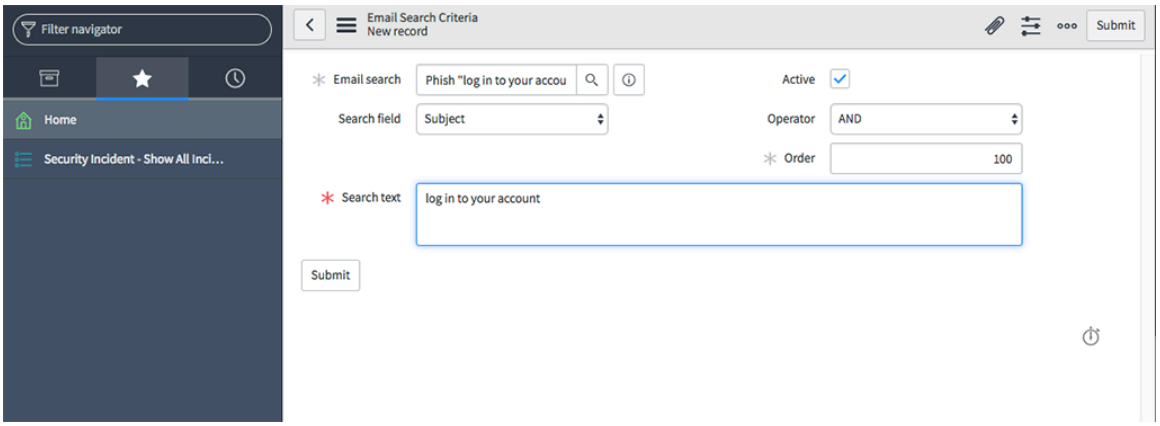
b. Von **Suchfeld** Wählen Sie im angezeigten Datensatz für E-Mail-Suchkriterien die Option aus **Betreff** .

c. Wählen Sie in der Liste Operator die Option aus **UND** Oder **ODER** .
Wenn Sie auswählen **ODER** , Die Suche gibt Ergebnisse zurück, wenn entweder Stichwörter in der Textzeichenfolge der Betreffzeile übereinstimmen oder die Bedingung der E-Mail-Adresse erfüllt ist. **UND** Ist für dieses Beispiel ausgewählt, damit die Suche nur Ergebnisse für E-Mails zurückgibt, die die Stichwörter der Betrefftextzeichenfolge enthalten und der E-Mail-Adresse des Absenders entsprechen.

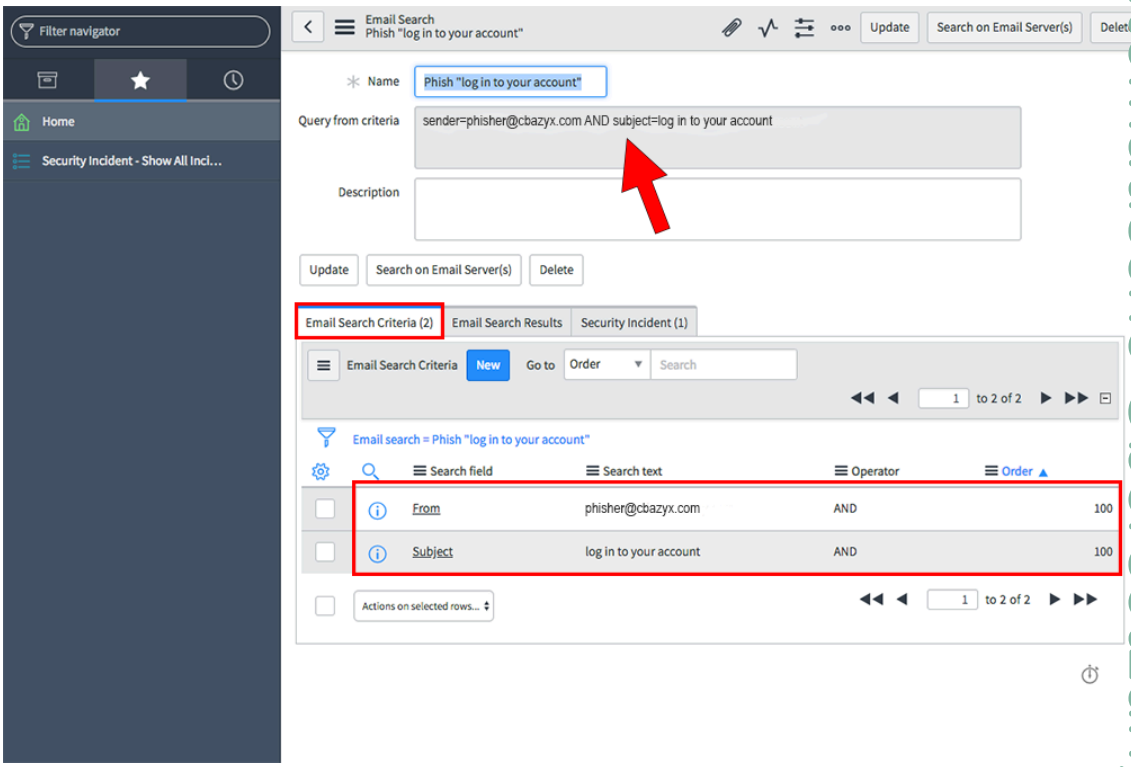
d. In **Suchtext** Feld den Wert für Betreffzeilentext eingeben, Melden Sie sich bei Ihrem Account an .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Klicken Sie auf **Absenden**.
Die neue Bedingung wird in der zugehörigen Liste E-Mail-Suchkriterien angezeigt, und beide Bedingungen werden in angezeigt **Abfrage aus Kriterien** Feld durch getrennt **UND** Operator.



Automatische Übersetzung

f. Wahlweise: Wenn Sie mehr als zwei Suchbedingungen haben, und wählen Sie aus **UND** Um jede Bedingung zu trennen, legen Sie den Reihenfolgenwert fest, um sie zu priorisieren.

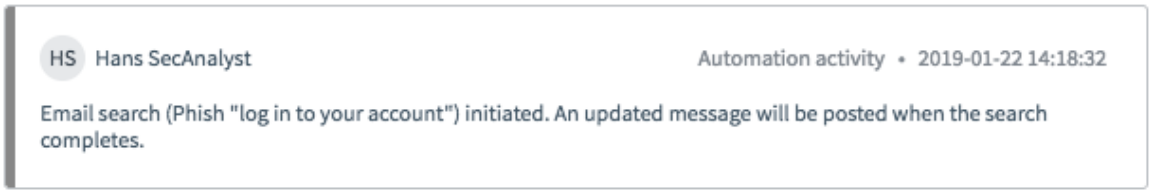
g. Fahren Sie mit dem Hinzufügen, Ändern oder Entfernen von Suchkriterien nach Bedarf fort, und klicken Sie auf **Aktualisieren** Um Ihre Änderungen am Datensatz zu speichern.

13. Wählen Sie eine Option aus, um fortzufahren.

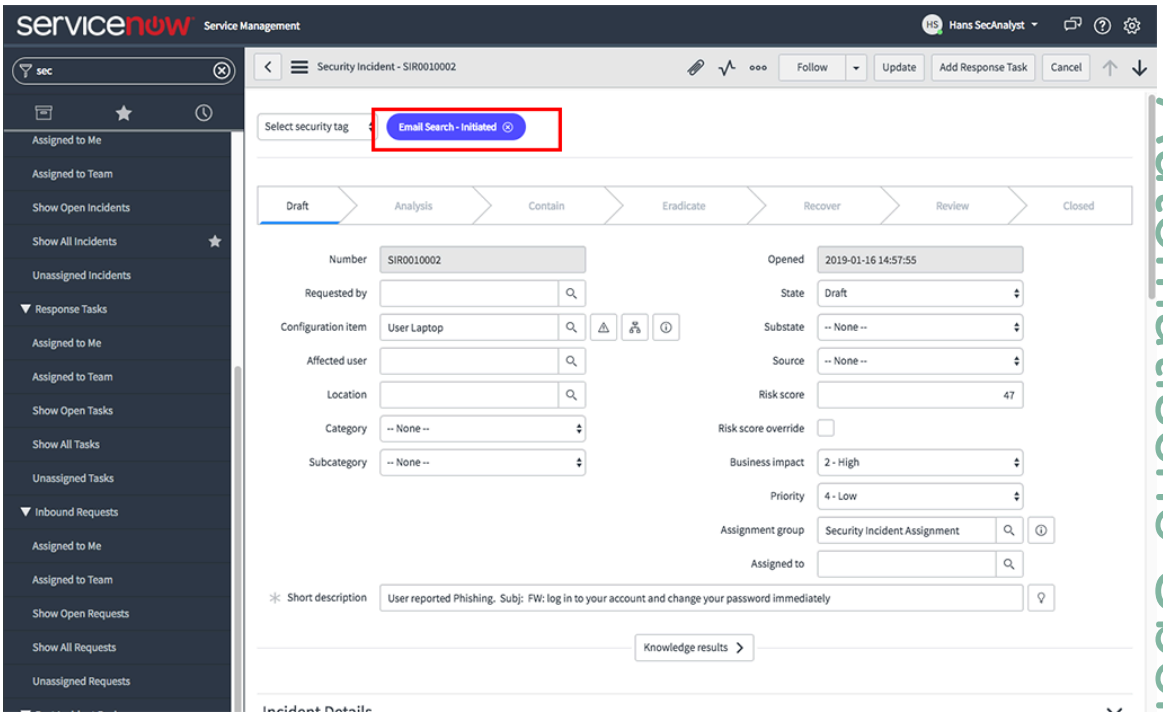
14. Um eine E-Mail-Suche zu initiieren, klicken Sie im E-Mail-Suchdatensatz auf **E-Mail-Server durchsuchen** .
Eine Nachricht wird angezeigt, die angibt, dass die Suchanforderung übermittelt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Security Incident-Datensatz wird eine Arbeitsnotiz angezeigt, die angibt, dass eine Suche initiiert wurde.



Wenn Tagging aktiviert ist, wird oben im Security Incident-Datensatz der E-Mail-Suche – Initiiert Sicherheits-Tag wird angezeigt.



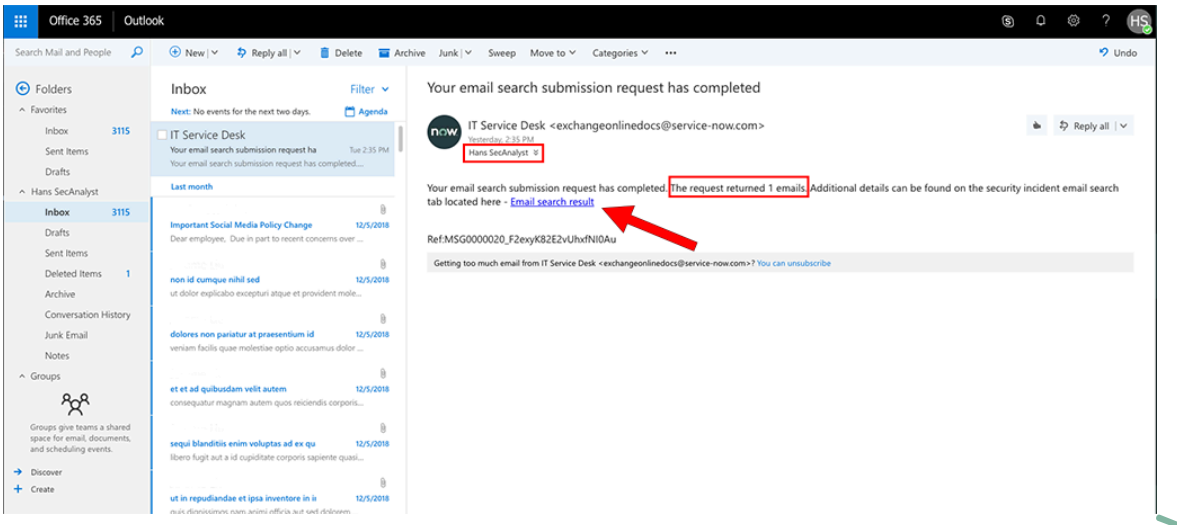
Wenn die Suche erfolgreich abgeschlossen wurde und E-Mail-Benachrichtigungen aktiviert sind, wird eine E-Mail an die E-Mail-Adresse der Person gesendet, die die Suche initiiert hat.

In diesem Beispiel wird der Anwender mit der Rolle „sn_si.Analyst“ Hans SecAnalyst , Hat diese Suche übermittelt. Die folgende Abbildung zeigt, dass diese Benachrichtigung an einen Account in gesendet wird Microsoft Exchange Online. Diese Benachrichtigungen können jedoch bei Bedarf an einen anderen E-Mail-Service gesendet werden.

Mit dieser Benachrichtigung können Sie alle übereinstimmenden Ergebnisse anzeigen, die Nachverfolgung und Löschung erfordern. Das folgende Beispiel zeigt, dass es eine E-Mail gibt, die den Suchkriterien entspricht. Ein E-Mail-Suchergebnislink zum E-Mail-Suchergebnisdatensatz in Ihrem ServiceNow AI Platform Instanz wird ebenfalls bereitgestellt. Wenn Sie den Suchdatensatz anzeigen möchten, klicken Sie auf diesen Link.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

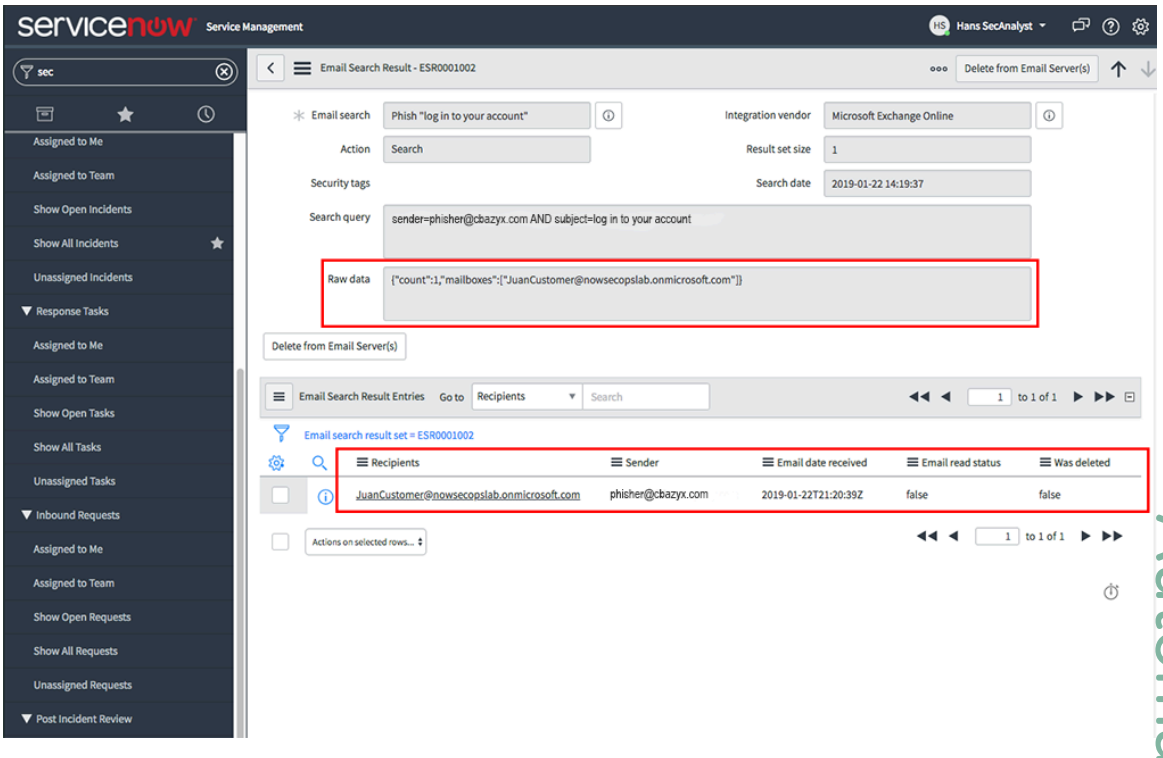


15. Klicken Sie in dieser E-Mail auf , um die Suchergebnisse anzuzeigen **E-Mail-Suchergebnis** Link.
Der Datensatz des E-Mail-Suchergebnisses wird angezeigt. In diesem Datensatz können Sie die folgenden Daten überprüfen und überprüfen.

- In **Rohdaten** Feld, die E-Mail-Anzahl für die Anzahl der E-Mails, die den Suchkriterien entsprechen {"count":1} , Und die Postfachadressen, in denen die E-Mails gefunden wurden, werden angezeigt [" JuanCustomer@nowsecopslab.onmicrosoft.com"] .
- In der Spalte Empfänger ist der Empfänger (JuanCustomer@nowsecopslab.onmicrosoft.com).
- In Absender Spalte, wird die Quelle der E-Mail angezeigt.
- In E-Mail-Empfangsdatum Spalte werden Datum und Uhrzeit des Empfangs der E-Mail angezeigt, um die Zeitlinien der Phishing-Kampagne nachzuverfolgen.
- In E-Mail-Lesestatus Spalte, die E-Mail in diesem Beispiel wurde nicht gelesen (Falsch). Wenn eine E-Mail gelesen wurde, Wahr Wird angezeigt.
- In Wurde gelöscht Spalte, die E-Mail in diesem Beispiel wurde nicht gelöscht. Wenn eine E-Mail gelöscht wurde, Wahr Wird angezeigt.

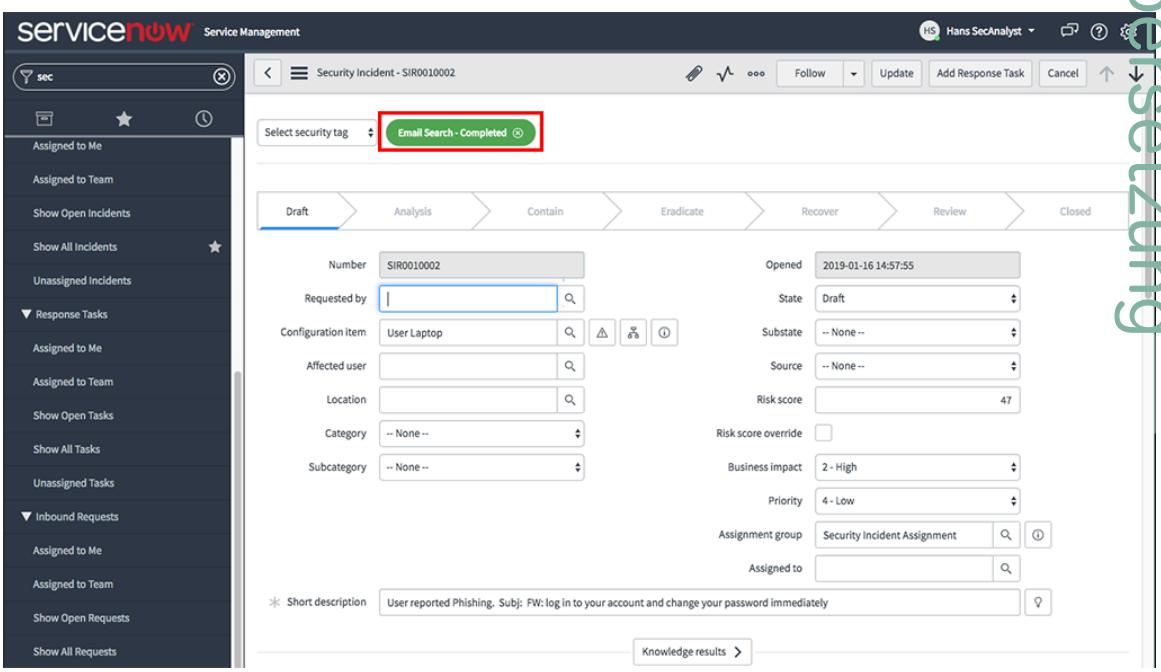
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



16. Alternativ können Sie die folgenden Schritte ausführen, um die Suchergebnisse aus dem Security Incident anzuzeigen.

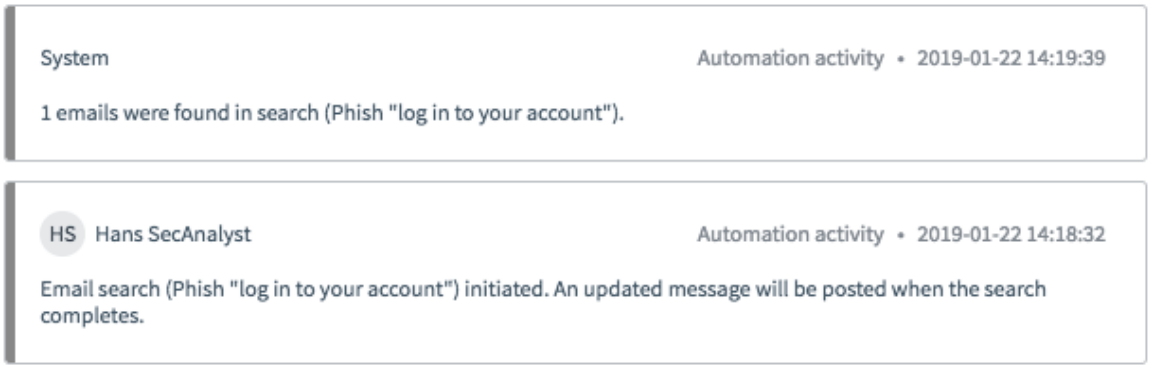
a. Navigieren zu **Security Incident** > **Incidents** Und öffnen Sie den Security Incident, mit dem Sie arbeiten.
Wenn die Suche erfolgreich abgeschlossen wurde, wird oben im Datensatz die angezeigt E-Mail-Suche: Abgeschlossen Sicherheits-Tag ersetzt E-Mail-Suche – Initiiert Sicherheits-Tag.



Arbeitsnotizen werden angezeigt, dass die Suche erfolgreich abgeschlossen wurde und eine übereinstimmende E-Mail gefunden wurde.

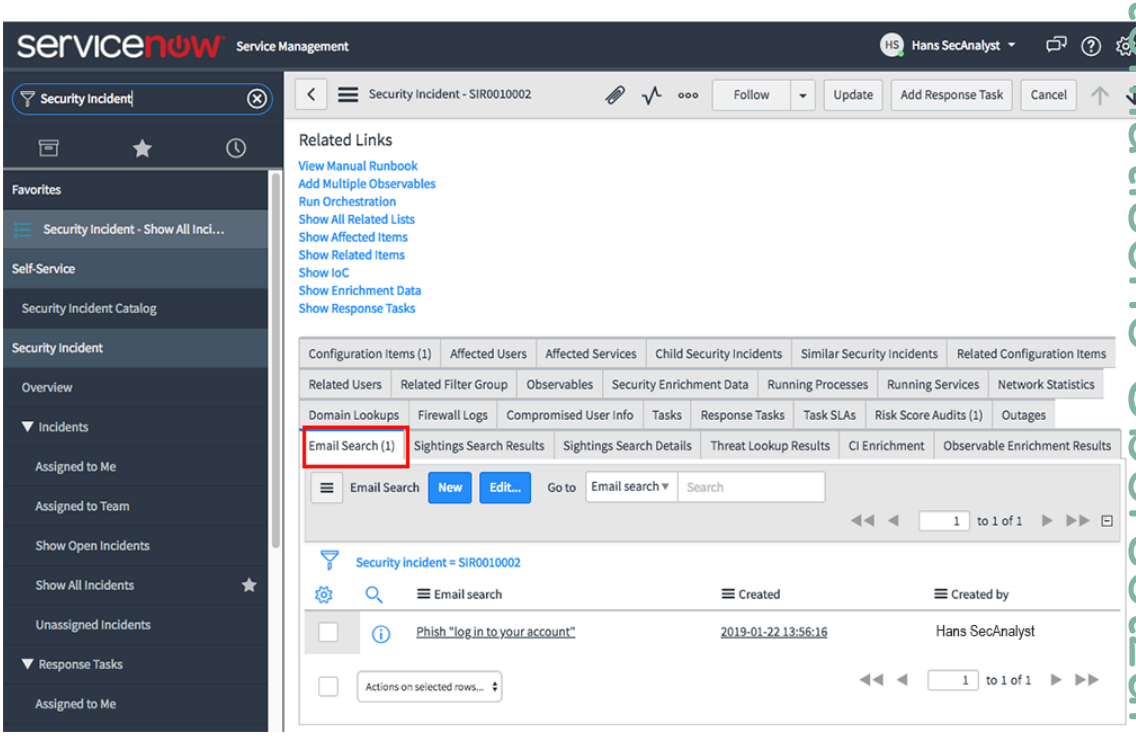
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



b. Scrollen Sie zum Ende des Security Incident-Datensatzes, und klicken Sie auf die zugehörige Liste E-Mail-Suche.

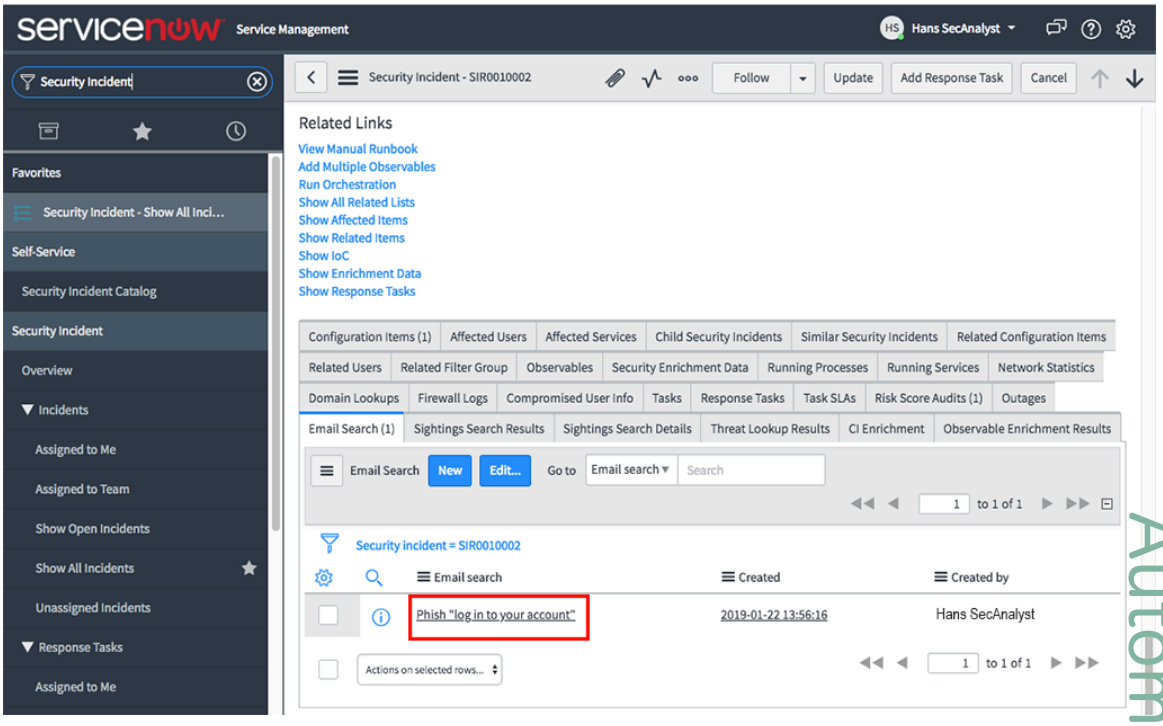
Wenn die zugehörige Liste E-Mail-Suche nicht angezeigt wird, klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Zugehöriger Link zum Anzeigen dieser zugehörigen Liste.



c. Wenn die zugehörige Liste E-Mail-Suche ausgewählt ist, klicken Sie in der Spalte E-Mail-Suche auf den Namen Ihrer Suche.

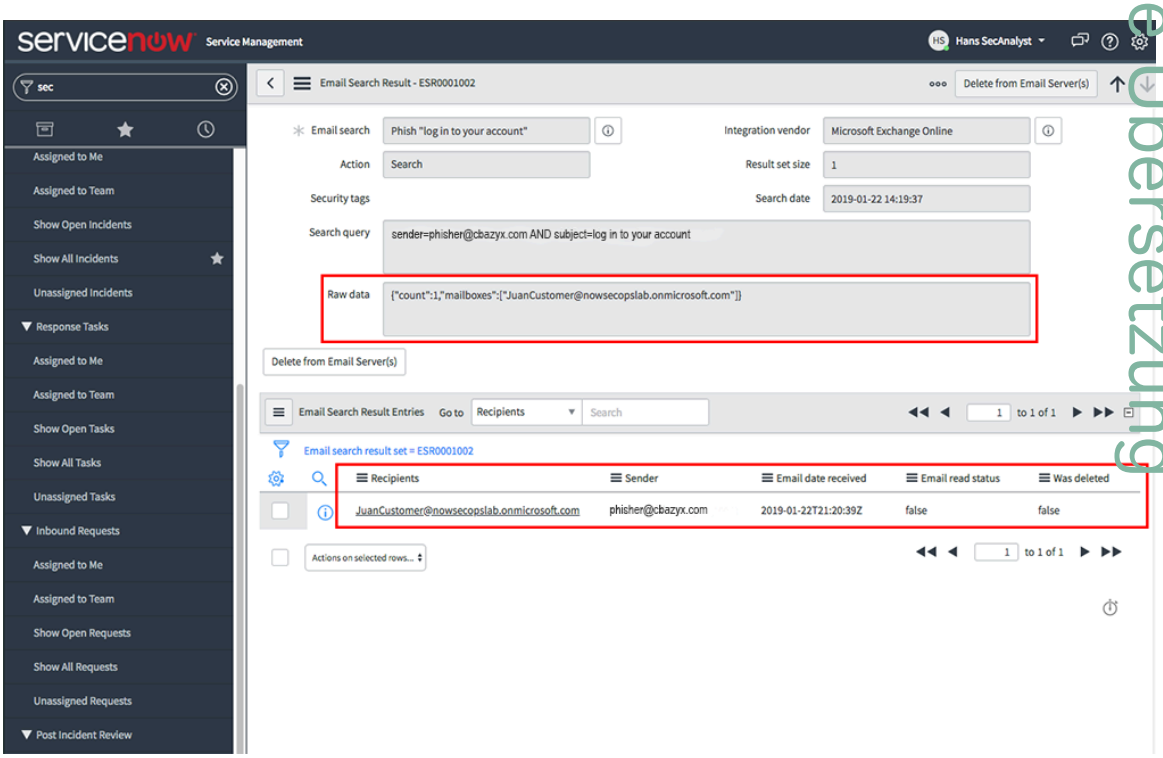
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Klicken Sie im Datensatz E-Mail-Suche auf die zugehörige Liste E-Mail-Suchergebnisse.

e. Klicken Sie in der Spalte Suchdatum auf das Datum Ihrer Suche, um die Daten anzuzeigen. Der Datensatz des E-Mail-Suchergebnisses wird angezeigt.



Nachdem eine E-Mail-Suche erfolgreich abgeschlossen wurde, bewerten Sie die Ergebnisse. Wenn Sie feststellen, dass E-Mails korrigiert werden müssen, sind Sie jetzt bereit, E-Mails zu löschen oder eine Löschgenehmigung anzufordern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fordern Sie die Löschgenehmigung für E-Mails im Microsoft Exchange-Onlineservice an

Nachdem eine E-Mail-Suche erfolgreich abgeschlossen wurde und übereinstimmende Nachrichten identifiziert wurden, können Sie alle verdächtigen E-Mails, die sich auf den Security Incident und die Phishing-Kampagne beziehen, dauerhaft aus dem Microsoft Exchange-Onlineservice löschen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Das System führt Löschungen für Ihre letzten erfolgreichen Suchergebnisse durch.

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Genehmigungen und E-Mail-Benachrichtigungen aktiviert sind, senden Sie eine Anforderung zum Löschen von E-Mails an eine Genehmigungsgruppe, bevor Sie die E-Mail entfernen.

E-Mail-Suchergebnisse werden mit allen empfangenen Nachrichten angezeigt. Um sicherzustellen, dass Phishing-E-Mails erfolgreich gelöscht werden, werden die Löschergebnisse in den Arbeitsnotizen des zugehörigen Security Incidents veröffentlicht. Wenn Tagging aktiviert ist, wird auch im zugehörigen Security Incident ein Sicherheits-Tag angezeigt. Wenn die E-Mail-Adresse nicht erfolgreich gelöscht wurde, werden Sie auch in den Arbeitsnotizen benachrichtigt.

Abhängig von Ihren Organisationsrichtlinien müssen Sie möglicherweise eine Genehmigung anfordern, bevor Sie Phishing-E-Mails löschen. Der Löschgenehmigungsprozess erfordert Informationen zur Anzahl der zu löschenden E-Mails und möglicherweise Zugriff auf andere Nachrichtendetails. Für die Verarbeitung der Löschanforderung wird in einer E-Mail-Benachrichtigung ein Genehmiger mit der Anzahl der übereinstimmenden E-Mail-Nachrichten, dem Security Incident-Link für den Zugriff auf vollständige Nachrichtendetails sowie Links zum Genehmigen oder Ablehnen bereitgestellt. Die Links in dieser E-Mail ermöglichen es einem Genehmiger, die Löschanforderung aus der E-Mail-Benachrichtigung anzunehmen oder abzulehnen. Ein vollständiger Audit-Pfad mit einem Zeitstempel ist ebenfalls verfügbar, der nachverfolgt, wann sich der Genehmigungsstatus in Arbeitsnotizen geändert hat. Wenn eine Genehmigungsgruppe zugewiesen ist, kann ein Anwender in der Gruppe die Anforderung für die gesamte Gruppe verarbeiten. Jedes Mitglied der Genehmigungsgruppe erhält eine E-Mail-Benachrichtigung für die Anforderung.

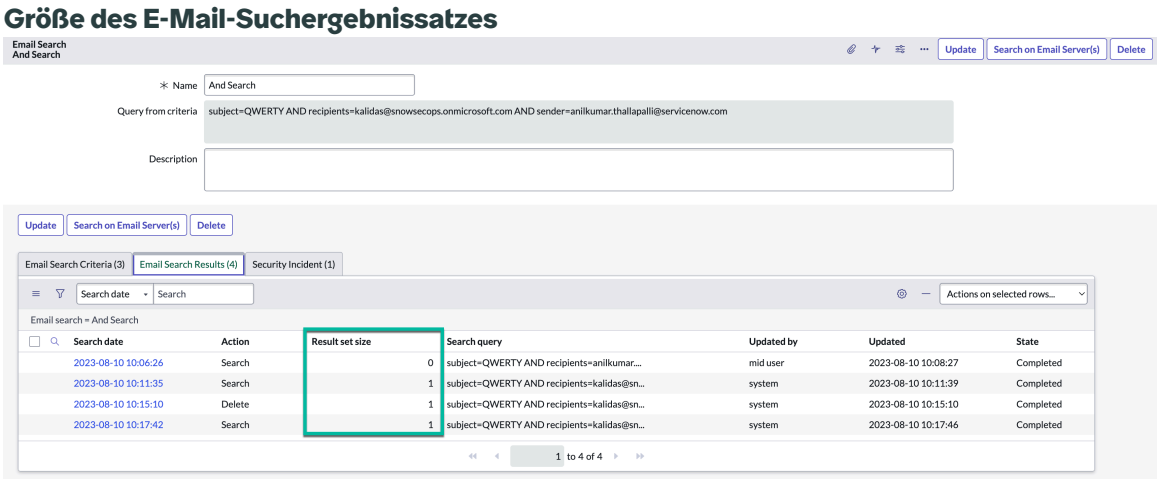
Wenn Sie als Anwender mit der Rolle „sn_si.Analyst“ feststellen, dass E-Mails korrigiert werden müssen, befolgen Sie die erforderlichen Schritte, um E-Mails zu löschen. Wenn Genehmigungen aktiviert sind, fordern Sie die Genehmigung an, um E-Mails aus dem zu löschen Microsoft Exchange Online Service.

Prozedur

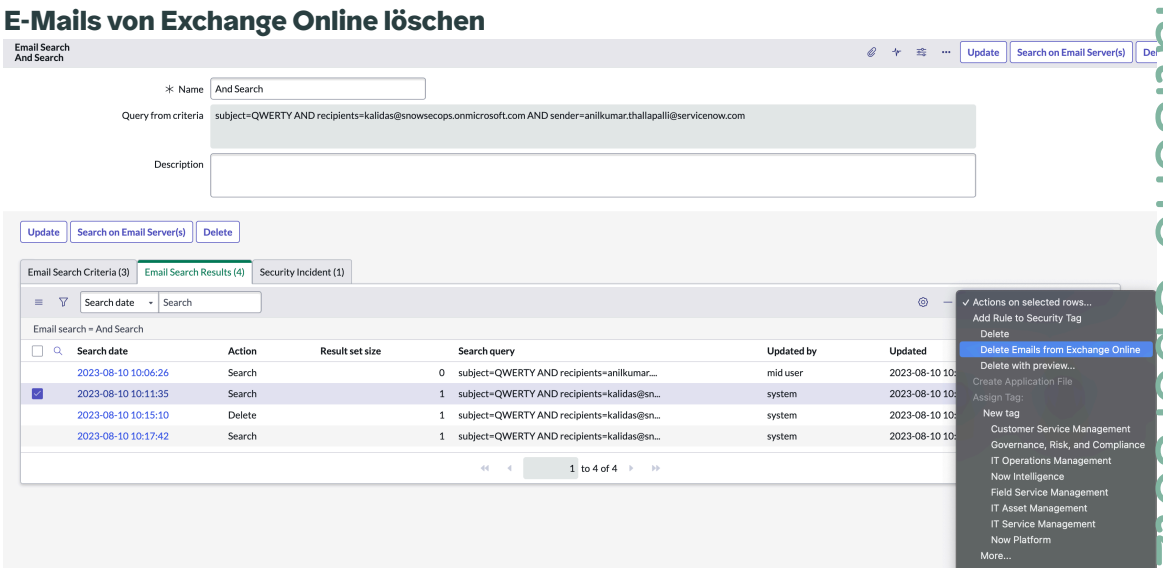
1. Navigieren zu **Alle** > **Security Incident > Alle Incidents Anzeigen**an.
2. Klicken Sie auf **E-Mail-Suche** Zugehörige Liste.
3. Wenn die zugehörige Liste E-Mail-Suche ausgewählt ist, klicken Sie in der Spalte E-Mail-Suche auf den Namen Ihrer Suche.
   Die Suchergebnisse werden in der zugehörigen Liste E-Mail-Suchergebnisse angezeigt.

   In diesem Beispiel wurden bei dieser Suche E-Mails gefunden, die Ihren Suchkriterien entsprechen. Im Datensatz sind zwei Suchaktionen aufgeführt. Eine Suche hat keine Übereinstimmungen (0), und die andere Suche hat eine übereinstimmende E-Mail (1).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Um E-Mail-Elemente zu löschen, die einer Suche zugeordnet sind, aktivieren Sie links neben der Spalte „Suchdatum“ das Kontrollkästchen eines Suchergebnissatzes.
   Sie können einen einzelnen Ergebnissatz oder mehrere Ergebnissätze aus der Liste auswählen.
5. Wählen Sie die Ergebnissätze aus, die Sie löschen möchten.



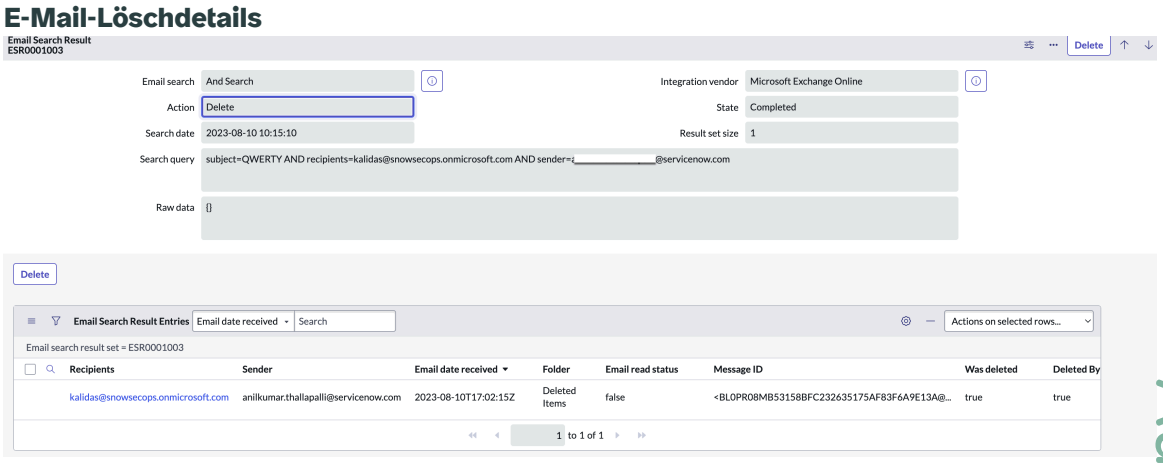
6. Wählen Sie unten in der zugehörigen Liste E-Mail-Suchergebnisse in der Liste Aktionen für ausgewählte Zeilen die Option aus **Löschen Sie E-Mails aus Exchange Online** Zum Löschen aller E-Mail-Elemente, die einem oder mehreren Ergebnissätzen zugeordnet sind, vom Exchange Online-Server.
   Wenn ein Ergebnissatz mehr als eine E-Mail enthält, müssen Sie den Datensatz „E-Mail-Suchergebnis“ nicht öffnen und einzelne E-Mails auswählen, um sie zu löschen. Alle E-Mail-Elemente mit dem Status Falsch In der Spalte wurde gelöscht im Datensatz E-Mail-Suchergebnis werden gelöscht, nachdem Sie ausgewählt haben **Löschen Sie E-Mails aus Exchange Online** .

   Wenn ein E-Mail-Element in einem Ergebnissatz bereits gelöscht wurde, lautet der Status in der Spalte wurde gelöscht im Datensatz „E-Mail-Suchergebnis“ Wahr . Diese Elemente werden nicht erneut gelöscht.

   Wenn die Genehmigungsoption während des Konfigurationsschritts deaktiviert ist, nachdem Sie ausgewählt haben **Löschen Sie E-Mails aus Exchange Online** , Die dem Ergebnissatz zugeordneten E-Mails werden gelöscht. Der Ergebnissatz selbst wird nicht gelöscht. Der Status aller gelöschten E-Mail-Elemente des Ergebnissatzes wird jedoch

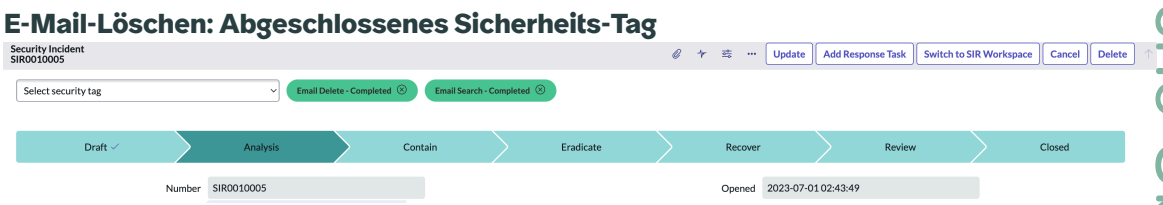
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auf aktualisiert Wahr In der Spalte wurde gelöscht des E-Mail-Suchergebnisdatensatzes. Weitere Informationen zur Genehmigungsfunktion finden Sie unter Konfigurieren Sie Microsoft Exchange Online Integration.



Diese E-Mails werden aus gelöscht Microsoft Exchange Online Mandant, für den Sie die Suche durchgeführt haben. Wenn die E-Mails erfolgreich gelöscht wurden, wird eine Arbeitsnotiz angezeigt.

Im Security Incident-Datensatz die E-Mail Löschen: Abgeschlossen Sicherheits-Tag wird angezeigt.



Wenn Genehmigungen für Löschanforderungen deaktiviert sind, haben Sie E-Mails erfolgreich aus gelöscht Microsoft Exchange Online Mandant.

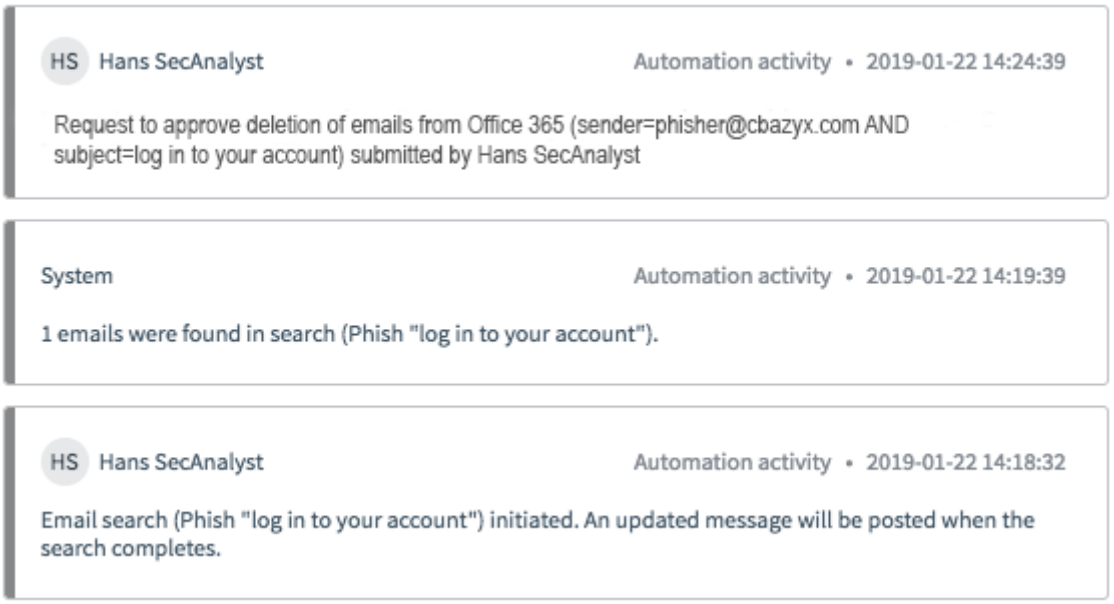
Wenn Genehmigungen für Löschanforderungen während des Konfigurationsschritts aktiviert sind, nachdem Sie ausgewählt haben **Löschen Sie E-Mails aus Exchange Online** , Eine E-Mail-Benachrichtigung wird an jedes Mitglied der Genehmigungsgruppe gesendet, die Sie während des Konfigurationsschritts ausgewählt haben.

Wenn Tagging während des Konfigurationsschritts aktiviert ist, wird E-Mail-Löschen: Initiiert Das Sicherheits-Tag wird im zugehörigen Security Incident-Datensatz angezeigt. Weitere Informationen zum Tagging finden Sie unter Konfigurieren Sie Microsoft Exchange Online Integration.

Arbeitsnotizen werden angezeigt, dass eine Anforderung zum Löschen von E-Mails vom Anwender mit der Rolle sn_si.Analyst (Hans SecAnalyst).

Automatische Übersetzung

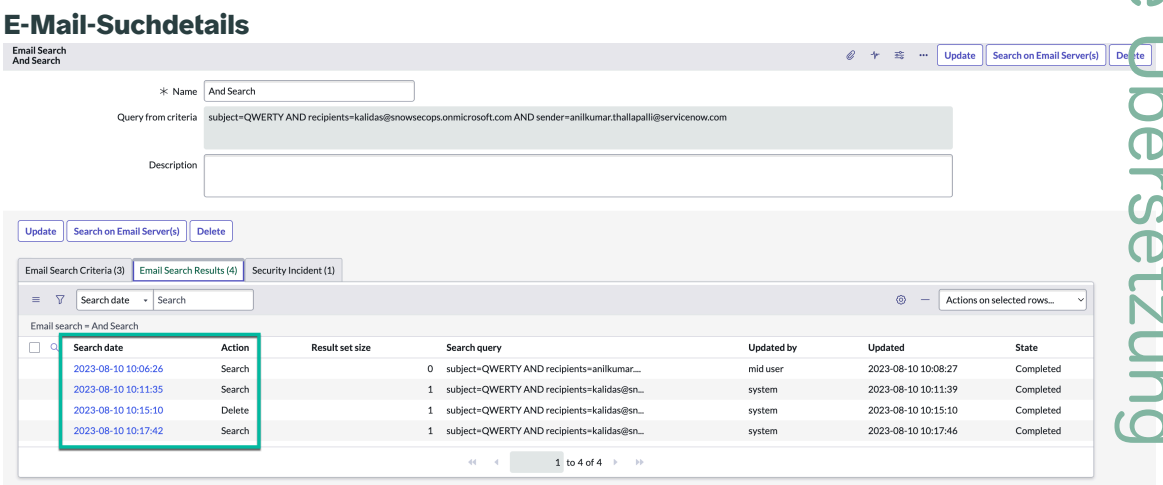
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Genehmigungen aktiviert sind, besteht der nächste Schritt in der Verarbeitung der Löschanforderung.

7. Alternativ können Sie die folgenden Schritte ausführen, wenn Sie die Details und einzelnen E-Mail-Elemente eines Suchdatensatzes anzeigen möchten, bevor Sie ihn löschen oder eine Löschanforderung senden.

   a. Wenn die zugehörige Liste E-Mail-Suchergebnisse ausgewählt ist, klicken Sie in der Spalte Suchdatum auf das Datum einer Suche, die Sie überprüfen möchten.



Die folgenden Informationen zu den E-Mails werden angezeigt:

- Empfänger
- Absender
- Empfangsdatum der E-Mail
- E-Mail-Lesestatus (Wahr Oder Falsch)
- Wurde gelöscht (Wahr Oder Falsch)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Von Integration Gelöscht (Wahr Oder Falsch)

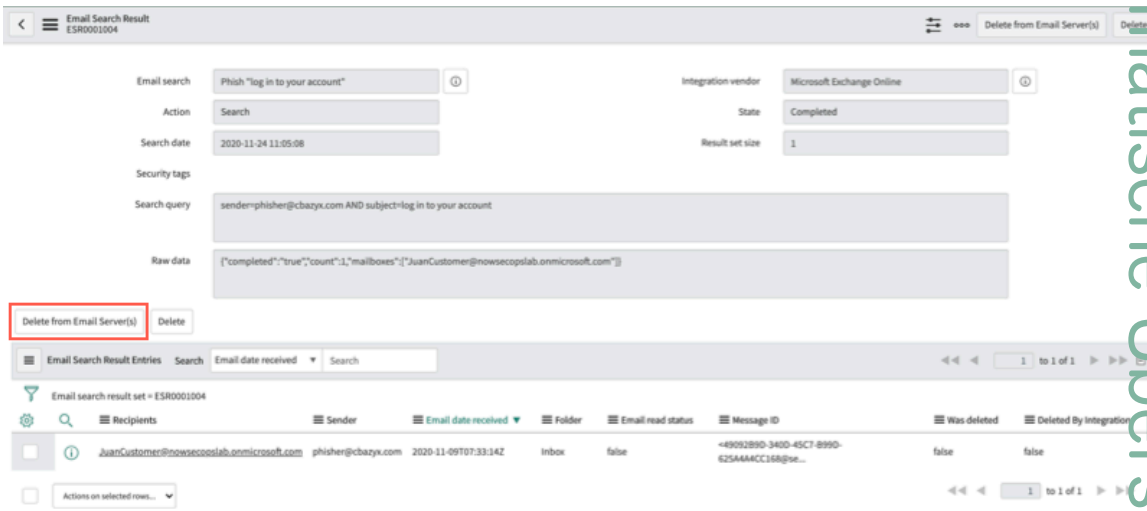
Hinweis:

Der Wert wird auf „wahr“ festgelegt, wenn die E-Mail gelöscht wird, wenn der Analyst das Löschen von E-Mail-Servern initiiert.

Die Arbeitsnotizen werden mit der Gesamtzahl der gelöschten Datensätze aktualisiert, einschließlich der von der Integration und dem Anwender gelöschten Datensätze.

b. Nachdem Sie die Daten überprüft haben, klicken Sie auf, um alle E-Mails zu löschen oder eine Anforderung zum Löschen aller E-Mails zu senden **Aus E-Mail-Server(n) löschen** .

Wie im vorherigen Beispiel beschrieben, müssen Sie, wenn im Suchergebnisdatensatz mehr als eine E-Mail aufgeführt ist, die einzelnen E-Mails nicht auswählen, um sie zu entfernen. Die Löschanforderung entfernt alle E-Mails, die der Suche zugeordnet sind, wenn Falsch Wird in der Spalte wurde aus den neuesten Suchergebnissen gelöscht angezeigt.



Wenn Genehmigungen aktiviert sind, haben Sie erfolgreich eine Anforderung zum Löschen von E-Mails übermittelt. Die Sicherheits-Tags und Arbeitsnotizen werden im zugehörigen Security Incident-Datensatz angezeigt, wie im vorherigen Beispiel beschrieben. Als Genehmiger besteht der nächste Schritt in der Verarbeitung der Löschanforderung.

Genehmigen Sie E-Mail-Anforderungen zum Löschen für Microsoft Exchange Online Integration

Wenn die Genehmigungsoption in aktiviert ist ServiceNow AI Platform Instanz werden Anforderungen zum Löschen von E-Mails per E-Mail an jedes Mitglied der Genehmigungsgruppe gesendet. Sie wählen die Genehmigungsgruppe während des Konfigurationsschritts aus. Genehmigungen bieten Ihrer Organisation eine zusätzliche Kontrolle über das Löschen von E-Mails.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Überprüfen Sie, ob Sie über verfügen **Genehmigungen** Option, die auf der Registerkarte zusätzliche Einstellungen des Formulars „Konfigurationseinstellungen für Exchange Online-Suche und E-Mails löschen“ ausgewählt ist.

Überprüfen Sie, ob Sie die E-Mail aktiviert haben **E-Mail-Senden aktiviert** Und **E-Mail-Empfang aktiviert** Optionen in Ihrem ServiceNow AI Platform Instanz für Genehmigungsanforderungen.

Wenn der Anwender mit der Rolle „sn_si.Analyst“ E-Mail-Anforderungen zum Löschen übermittelt, werden diese Anforderungen standardmäßig per E-Mail an sn_si.admin gesendet. Wenn Sie eine Genehmigungsgruppe erstellt haben, erhält jedes Mitglied der Gruppe eine Benachrichtigung. Genehmiger können E-Mail-Löschanforderungen direkt aus der E-Mail-Benachrichtigung verarbeiten. Alternativ können Anforderungen aus den E-Mail-Suchergebnisdatensätzen in verarbeitet werden ServiceNow AI Platform Instanzen. In diesem Thema werden beide Genehmigungsmethoden angezeigt.

Die folgenden Informationen beschreiben die Anforderung in der E-Mail-Benachrichtigung:

E-Mail-Suchergebnisdatensatznummer

Eindeutige Nummer, die dem Suchdatensatz von zugewiesen ist ServiceNow AI Platform Als Teil des Audit-Pfads.

Name des Analysten, der die Anforderung übermittelt hat

Name der Person, die die Anforderung als Teil des Audit-Pfads übermittelt hat.

Link zum Security Incident

Ein Link zum Security Incident im Zusammenhang mit dem Phishing-Ereignis. Zeigen Sie den Security Incident mit den Arbeitsnotizen, E-Mail-Suchen und E-Mail-Suchergebnissen direkt aus der E-Mail an.

Genehmigen oder lehnen Sie Links ab

Links zum Genehmigen oder Ablehnen der Anforderung aus der E-Mail-Benachrichtigung. Nachdem Sie auf einen der Links geklickt haben, initiiert das System automatisch den zugehörigen Workflow, und eine Arbeitsnotiz wird im Security Incident-Datensatz veröffentlicht.

Erforderliche Rolle: sn_si.admin oder alle Mitglieder einer zugewiesenen Genehmigungsgruppe.

Prozedur

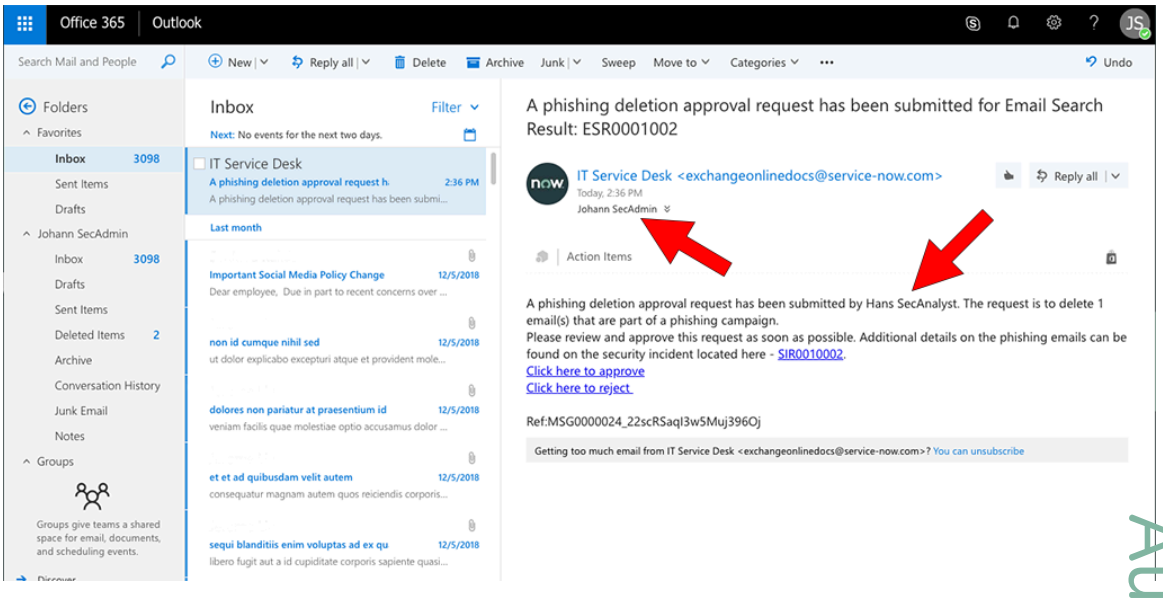
1. Führen Sie die folgenden Schritte aus, um die Löschanforderung aus der E-Mail-Benachrichtigung zu verarbeiten.

   a. Suchen Sie als Genehmiger die Benachrichtigungs-E-Mail im E-Mail-Account, den Sie in konfiguriert haben ServiceNow AI Platform Anwenderaccount.

      In diesem Beispiel sendet der Anwender mit der Rolle „sn_si.Analyst“ (Hans SecAnalyst) eine Anforderung zum Löschen einer E-Mail. Johann SecAdmin ist Mitglied der Genehmigungsgruppe.

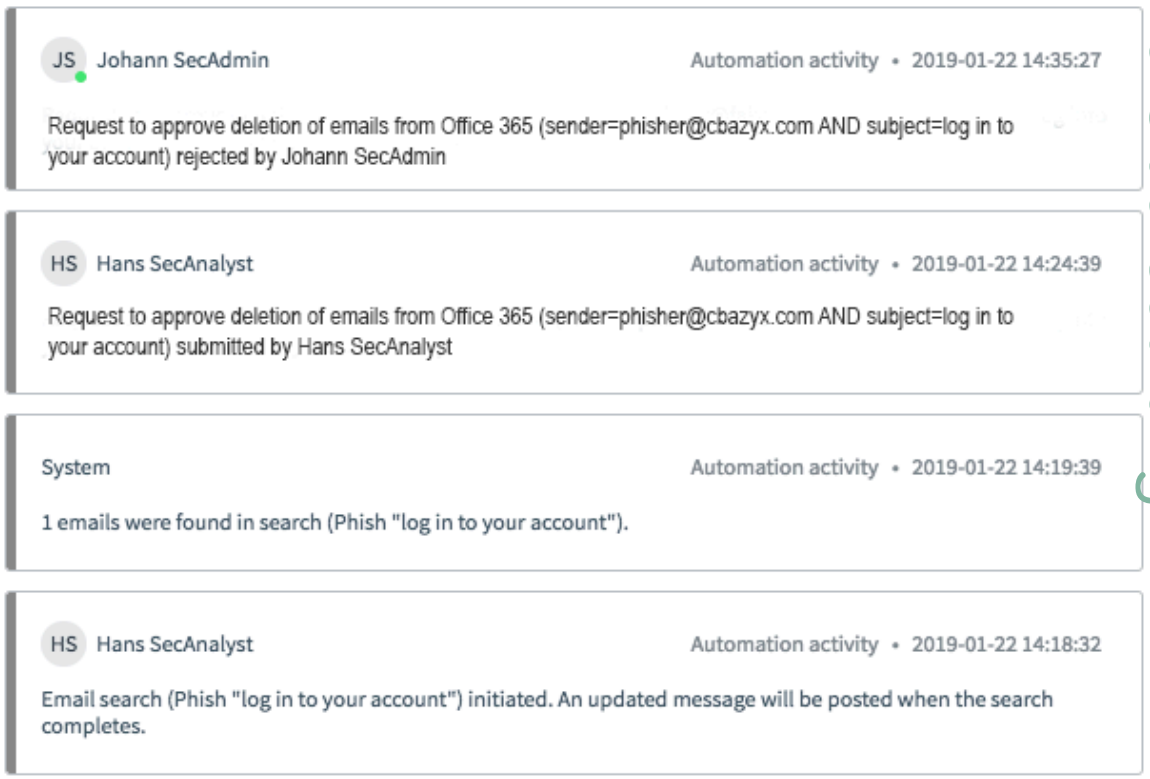
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



b. Wählen Sie in der E-Mail-Benachrichtigung eine Option aus, um fortzufahren.

Die folgende Abbildung zeigt ein Beispiel für den Audit-Pfad, der von den Arbeitsnotizen im zugehörigen Security Incident-Datensatz für dieses Beispiel erstellt wurde. Wenn die Anforderung von einem Genehmiger aus der E-Mail-Benachrichtigung abgelehnt wird, wird eine Arbeitsnotiz von der Person veröffentlicht, die die Anforderung abgelehnt hat. Johann SecAdmin lehnt diese Anforderung ab.



In ServiceNow AI Platform Instanz der Person, die die Anforderung abgelehnt hat (Johann SecAdmin), in **Selfservice > Meine Genehmigungen**, Abgelehnt Wird in der Spalte Status angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

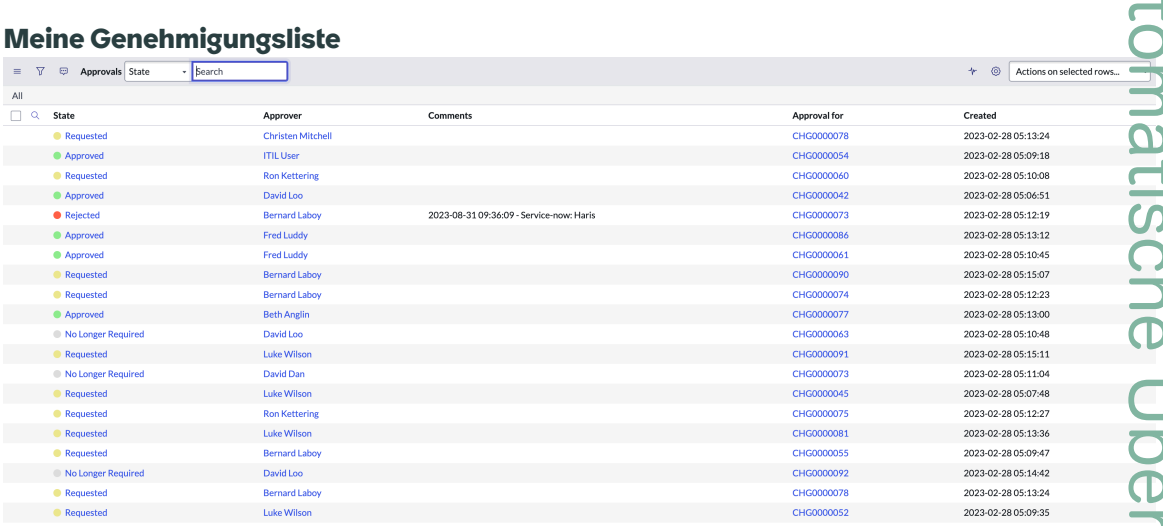
Nachdem eine Anforderung von einem einzelnen Mitglied der Genehmigungsgruppe abgelehnt wurde, müssen Sie als Anwender mit der Rolle „sn_si.Analyst“ eine neue Anforderung zum Löschen dieser E-Mails übermitteln, wenn Sie festlegen, dass sie gelöscht werden sollen.

In diesem Beispiel sendet der Anwender mit der Rolle „sn_si.Analyst“ eine neue Anforderung, nachdem die Anforderung abgelehnt wurde.

Ein anderes Mitglied der Genehmigungsgruppe, John-Genehmiger, erhält eine E-Mail ähnlich der im vorherigen Beispiel gezeigten. Der John-Genehmiger kann diese Anforderung auch verarbeiten.

2. Alternativ können Genehmiger zu navigieren **Selfservice > Meine Genehmigungen** In ihren ServiceNow AI Platform Instanzen zum Anzeigen und Verarbeiten von Löschanforderungen.
Dient zum Verarbeiten einer Anforderung von **Meine Genehmigungen** , Führen Sie die folgenden Schritte aus.

   a. Navigieren zu **Selfservice > Meine Genehmigungen**an.



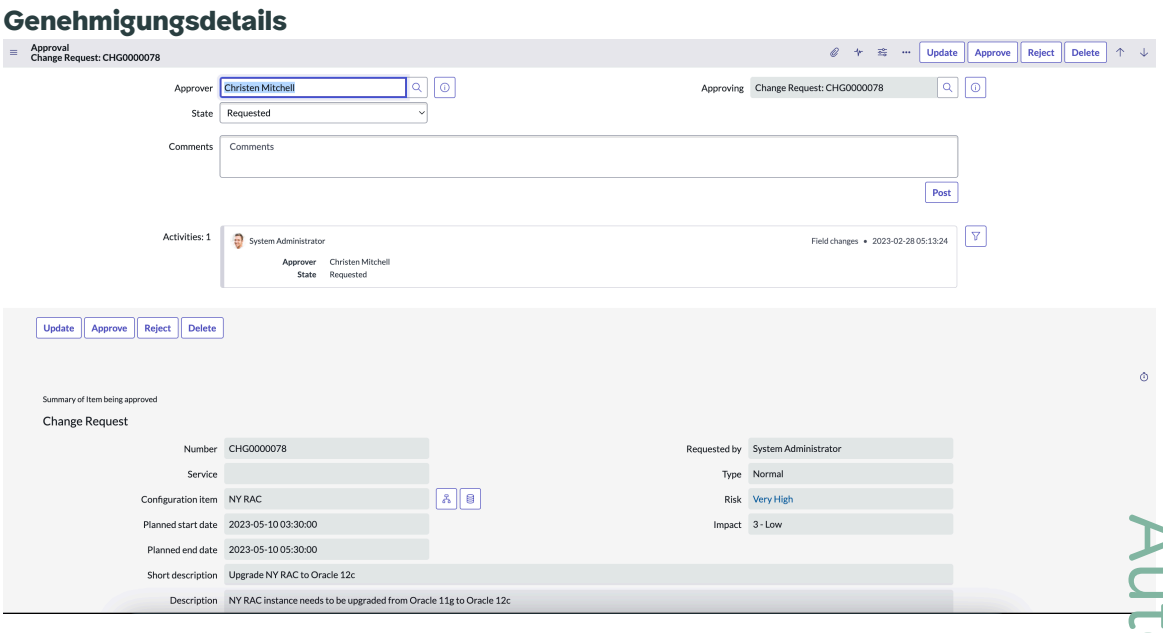
State	Approver	Comments	Approval for	Created
Requested	Christen Mitchell		CHG0000078	2023-02-28 05:13:24
Approved	ITIL User		CHG0000054	2023-02-28 05:09:18
Requested	Ron Kettering		CHG0000060	2023-02-28 05:10:08
Approved	David Loo		CHG0000042	2023-02-28 05:06:51
Rejected	Bernard Laboy	2023-08-31 09:36:09 - Service-now: Haris	CHG0000073	2023-02-28 05:12:19
Approved	Fred Luddy		CHG0000086	2023-02-28 05:13:12
Approved	Fred Luddy		CHG0000061	2023-02-28 05:10:45
Requested	Bernard Laboy		CHG0000090	2023-02-28 05:15:07
Requested	Bernard Laboy		CHG0000074	2023-02-28 05:12:23
Approved	Beth Anglin		CHG0000077	2023-02-28 05:13:00
No Longer Required	David Loo		CHG0000063	2023-02-28 05:10:48
Requested	Luke Wilson		CHG0000091	2023-02-28 05:15:11
No Longer Required	David Dan		CHG0000073	2023-02-28 05:11:04
Requested	Luke Wilson		CHG0000045	2023-02-28 05:07:48
Requested	Ron Kettering		CHG0000075	2023-02-28 05:12:27
Requested	Luke Wilson		CHG0000081	2023-02-28 05:13:36
Requested	Bernard Laboy		CHG0000055	2023-02-28 05:09:47
No Longer Required	David Loo		CHG0000092	2023-02-28 05:14:42
Requested	Bernard Laboy		CHG0000078	2023-02-28 05:13:24
Requested	Luke Wilson		CHG0000052	2023-02-28 05:09:35

   b. Klicken Sie in der Spalte Status auf das angeforderte Element.

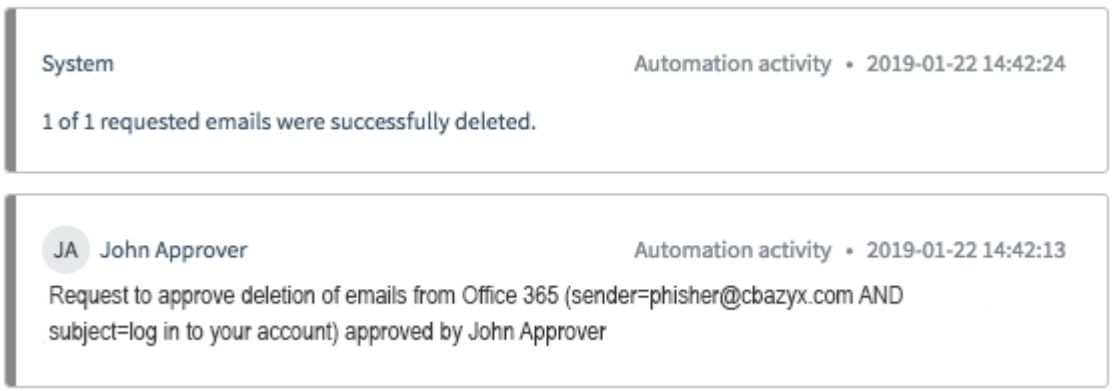
      Im angezeigten Genehmigungsdatensatz werden Daten zur Suche, zur Suchanforderung und zu den Suchergebnissen aufgelistet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Klicken Sie in diesem Datensatz auf **Genehmigen** Um die Anforderung zu genehmigen. Nachdem die Anforderung genehmigt wurde, initiiert das System den Löschworkflow, um die E-Mails zu entfernen. Die folgende Abbildung zeigt ein Beispiel für den Audit-Pfad, der von den Arbeitsnotizen im zugehörigen Security Incident-Datensatz für dieses Beispiel erstellt wurde. Nachdem diese Löschanforderung erneut übermittelt wurde, wird sie genehmigt. Unabhängig davon, welche Methode zum Genehmigen einer Anforderung verwendet wird, wird die Anzahl der erfolgreich gelöschten E-Mails in einer Arbeitsnotiz veröffentlicht.



Nachdem die E-Mails erfolgreich gelöscht wurden, wird im zugehörigen Security Incident-Datensatz, wenn Tagging aktiviert ist, die E-Mail Löschen: Abgeschlossen Tag ersetzt E-Mail-Löschen: Initiiert Tag.

Ein **Selfservice > Meine Genehmigungen** Für den Genehmiger (John-Genehmiger) ändert sich der Status von Angefordert Bis Genehmigt .

Ein **Selfservice > Meine Genehmigungen** Für andere Mitglieder der Genehmigungsgruppe, z. B. Johann SecAdmin, ändert sich der Status in Nicht Mehr Erforderlich Nachdem die Anforderung genehmigt wurde.

3. Alternativ können Sie die folgenden Schritte ausführen, um zu bestätigen, dass E-Mails im Datensatz „E-Mail-Suchergebnis“ im zugehörigen Security Incident-Datensatz gelöscht werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

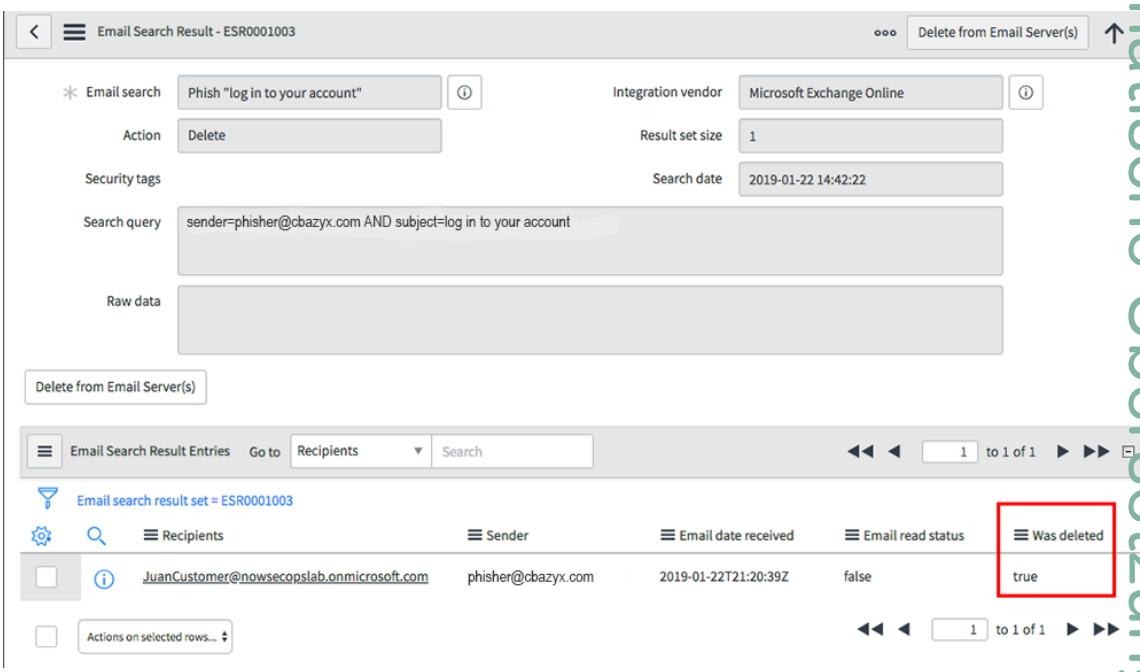
a. Navigieren zu **Security Incidents > Alle Incidents Anzeigen** Und suchen Sie den Phishing-bezogenen Security Incident.
Unten im Datensatz werden die zugehörigen Listen angezeigt.

b. Klicken Sie auf **E-Mail-Suche** Zugehörige Liste.

c. Klicken Sie in der Spalte E-Mail-Suche auf den Namen der Suche (Phishing „bei Ihrem Account anmelden“).
Der Datensatz „E-Mail-Suche“ wird angezeigt. Wenn die zugehörige Liste E-Mail-Suche nicht sichtbar ist, klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Link.

d. Klicken Sie auf **E-Mail-Suchergebnisse** Zugehörige Liste.
In der Spalte Suchdatum werden die Aktionen E-Mail-Suche und E-Mail-Löschen mit den entsprechenden Daten angezeigt.

e. Klicken Sie in der Spalte Suchdatum auf das Element, das der Löschaktion entspricht.
Im angezeigten Datensatz „E-Mail-Suchergebnis“ zeigt der Spaltenstatus wurde gelöscht an, dass die E-Mail gelöscht wurde (Wahr).



Sie haben E-Mail-Löschanforderungen erfolgreich aus einer E-Mail-Benachrichtigung und einem Genehmigungsdatensatz genehmigt und bestätigt, dass E-Mails gelöscht werden. Weitere Informationen zum Suchen des Datensatzes „E-Mail-Suchergebnis“ finden Sie unter Definieren Sie E-Mail-Suchkriterien, und fordern Sie eine Suche im an Microsoft Exchange Online Service.

Gelöschte E-Mails auf wiederherstellen Microsoft Exchange Online Service

(Optional) als Microsoft Exchange-Administrator können Sie gelöschte E-Mails wiederherstellen, wenn die Behebung von Incidents erfordert, dass Sie die vom Workflow dieser Integration gelöschten E-Mails wiederherstellen müssen.

Vorbereitungen

Weitere Informationen zum Löschen von E-Mails durch diese Integration finden Sie unter Konfigurieren Sie Microsoft Exchange Online Integration.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für weitere Informationen zur Administratorrolle in Microsoft Office 365-Produkt, einschließlich Informationen zur Wiederherstellung gelöschter Elemente in einem Anwenderpostfach, siehe Über die Exchange Online-Administratorrolle .

Erforderliche Rolle: administrator, Microsoft Exchange-Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie auswählen **Gelöschte E-Mails Wiederherstellen** Option auf der Registerkarte „zusätzliche Einstellungen“ während des Konfigurationsschritts aktivieren Sie die Wiederherstellung gelöschter E-Mails in Ihrem Microsoft Exchange Online Mandant. E-Mails, die mit dem Löschworkflow dieser Integration gelöscht wurden, werden im Unterordner „Gelöschte Elemente“ des Ordners „wiederherstellbare Elemente“ im Postfach des Anwenders auf der platziert Microsoft Exchange Online Service. Wenn der Account des Anwenders in konfiguriert ist Microsoft Exchange Online Mandant damit der Anwender den Ordner „Gelöschte Elemente“ anzeigen kann, kann der Anwender diese E-Mails mithilfe von wiederherstellen Microsoft Outlook-Service im Web. Alternativ dazu Microsoft Exchange Online Der Administrator kann gelöschte E-Mails aus einem Ordner „gelöschte Elemente“ eines Anwenders wiederherstellen. Siehe Gelöschte Elemente oder E-Mails in Outlook Web App wiederherstellen Weitere Informationen finden Sie unter .

Erforderliche Rolle: Microsoft Exchange Online Administrator oder Microsoft Globaler Administrator zum Wiederherstellen gelöschter E-Mails.

Erforderliche Rolle: sn_si.admin in ServiceNow AI Platform Zum Aktivieren der Option gelöschte E-Mails wiederherstellen.

Erforderliche Rolle: sn_si.Analyst in ServiceNow AI Platform Zum Abschließen einer erfolgreichen Suche nach E-Mails und zum Überprüfen, ob E-Mails vor der Wiederherstellung erfolgreich gelöscht wurden.

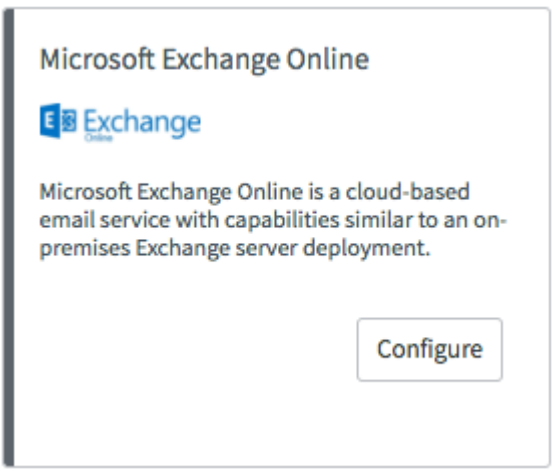
Prozedur

Um die E-Mail-Wiederherstellungsoption zu aktivieren, führen Sie die folgenden Schritte aus.

a. Navigieren zu **Security Operations** > **Integrationen** > **Konfigurationen**an.

b. Suchen Sie nach Microsoft Exchange Online Kachel.

c. Klicken Sie auf **Konfigurieren**.

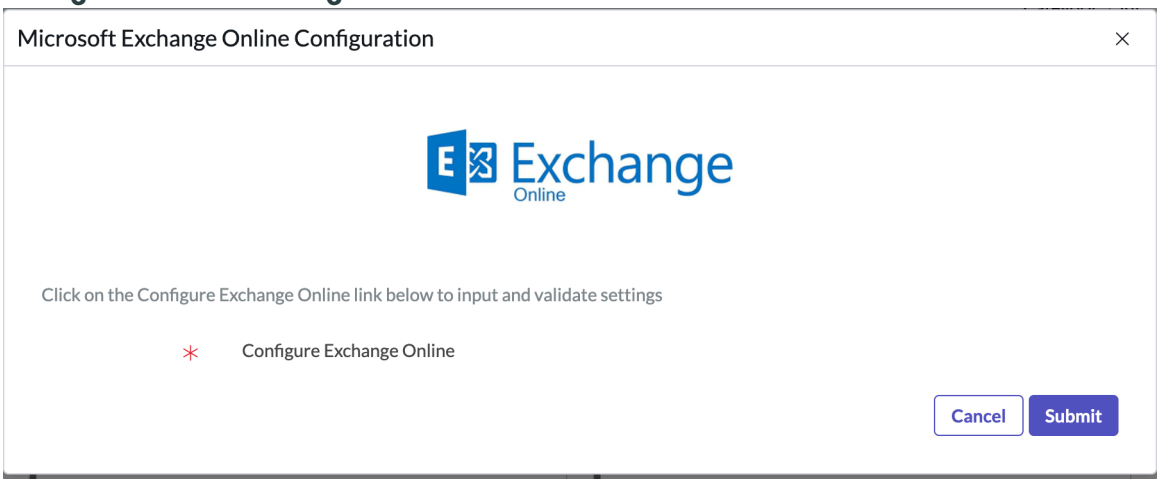


d. In Microsoft Exchange Online Klicken Sie auf das Konfigurationsdialogfeld, das angezeigt wird **Konfigurieren Sie Exchange Online** .

Automatische Übersetzung

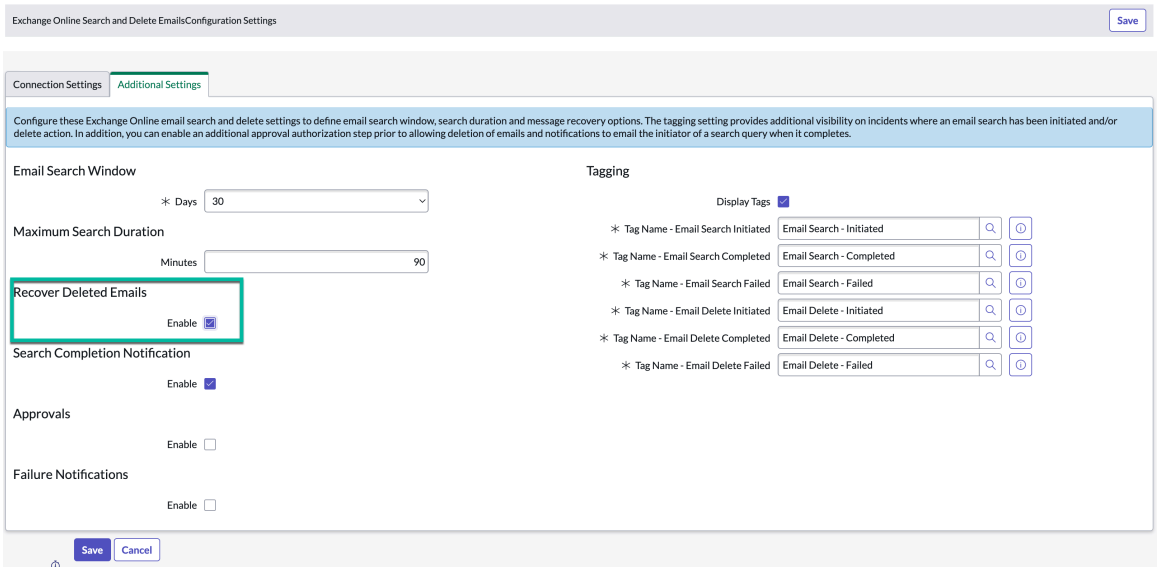
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Exchange Online



e. Auf der Zusätzliche Einstellungen Registerkarte unter Gelöschte E-Mails Wiederherstellen , Wählen Sie aus **Aktivieren** Kontrollkästchen.

Gelöschte E-Mails wiederherstellen



f. Überprüfen Sie alle anderen Einstellungen, und klicken Sie auf **Übermitteln** .

g. Um sicherzustellen, dass die Suche und Löschung von E-Mail-Nachrichten für die E-Mail-Nachrichten erfolgreich abgeschlossen wurde, die Sie wiederherstellen möchten, navigieren Sie zu dem Security Incident, der die E-Mail-Such- und Löschungs-Workflows protokolliert hat.

h. Suchen Sie die Arbeitsnotizen, und überprüfen Sie, ob das System die Nachrichten erfolgreich gelöscht hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Als Microsoft Exchange Online Administrator oder globaler Administrator, melden Sie sich bei an Microsoft Office 365-Account.

j. Führen Sie die in beschriebenen Schritte aus Gelöschte Elemente oder E-Mails in Outlook Web App wiederherstellen Auf der Microsoft Dokumentations-Website.

Bearbeiten Sie Sicherheits-Tags für Microsoft Exchange Online Integration

Sie können die Namen und Farben der Sicherheits-Tags in bearbeiten ServiceNow AI Platform® Instanz für Microsoft Exchange Online Integration. Diese Sicherheits-Tags helfen Ihnen, schnell zu identifizieren, wann die E-Mail-Suche abgeschlossen ist oder fehlschlägt. Sie identifizieren auch, wann Anforderungen zum Löschen von E-Mails initiiert werden und wann die E-Mail-Elemente erfolgreich gelöscht wurden.

Vorbereitungen

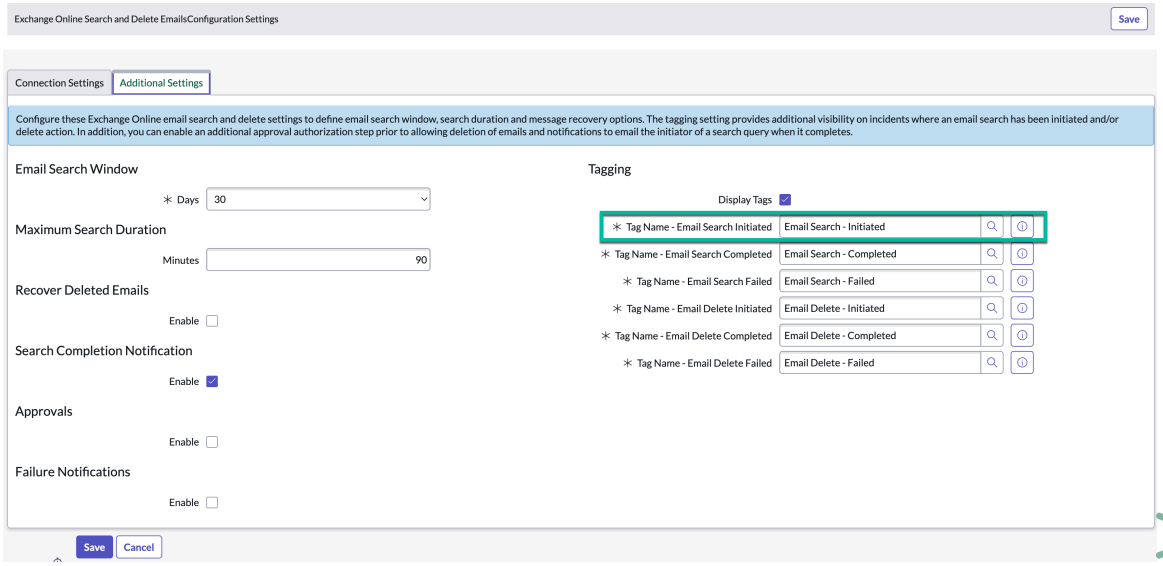
Standardmäßig sind die Sicherheits-Tags in aktiviert ServiceNow AI Platform® Instanz, wenn Sie auswählen **Tags Anzeigen** Option während des Konfigurationsschritts. Sie können Tag-Farben und -Namen bearbeiten und Sicherheits-Tag-Gruppen Tags zuweisen, um sie in Ihrem zu organisieren ServiceNow AI Platform® Instanz. Sie können beispielsweise die Farben von Tags so ändern, dass das Start-Tag einer Fähigkeit eine Farbe hat und das Abschluss-Tag eine andere Farbe hat, um den anderen Sicherheits-Tags zu entsprechen, die in aktiviert sind ServiceNow AI Platform® Instanz. Diese verschiedenen Farben können Ihnen helfen, schnell zu erkennen, wann Workflows beginnen und erfolgreich abgeschlossen wurden. Wenn Sie entscheiden, dass Sie kein bestimmtes Tag benötigen, ohne das Tagging für die Integration zu deaktivieren, können Sie auch ein einzelnes Tag aus dem Tag-Datensatz deaktivieren. Wenn diese Option deaktiviert ist, wird dieses Tag nicht mehr in den zugehörigen Security Incidents angezeigt. Weitere Informationen zum Einrichten von Sicherheits-Tag-Gruppen und -Tags finden Sie unter Sicherheits-Tag-Gruppen und -Tags einrichten im ServiceNow-Produktdokumentationswebsite .

Erforderliche Rolle: sn_si.admin

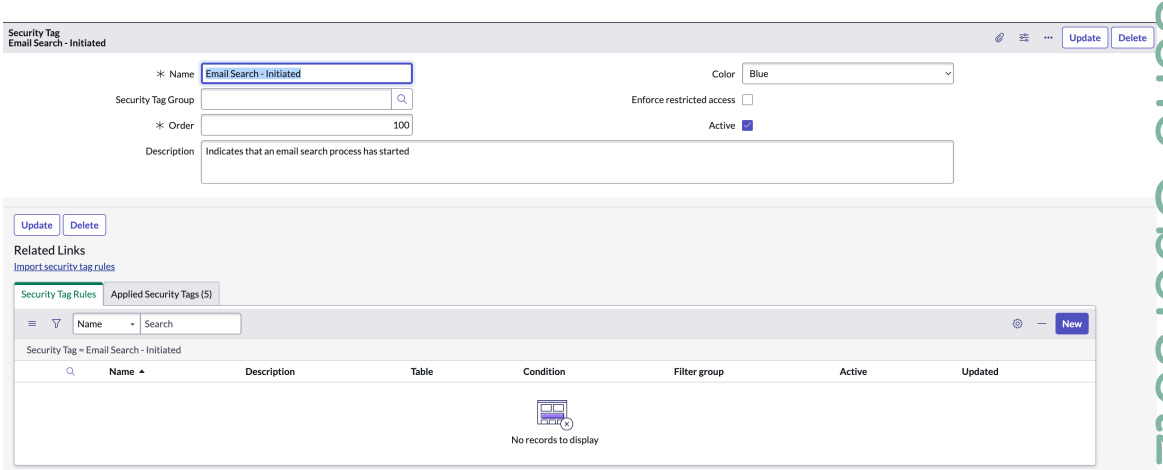
Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Exchange Online-Einstellungen**an.
2. Klicken Sie auf **Zusätzliche Einstellungen** Registerkarte, um sie auszuwählen.
3. Auf der Registerkarte, die angezeigt wird, wenn **Tags Anzeigen** Option ist gelöscht. Wählen Sie sie aus, um Tag-Namen anzuzeigen.
4. Klicken Sie rechts neben einem Tag auf das Informationssymbol, wenn die Tag-Namen angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie im angezeigten Dialogfeld „Sicherheits-Tag“ auf **Öffnen Sie Den Datensatz** .
6. Bearbeiten Sie die Felder im angezeigten Datensatz.
7. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.



Sie haben jetzt den Tag-Datensatz für ein Sicherheits-Tag erfolgreich bearbeitet.

Integration mit Microsoft Exchange lokal

Die Microsoft Exchange Die lokale Integration bietet Sicherheitsanalysten Tools zur Eindämmung und Beseitigung von Phishing-E-Mail-Bedrohungen in lokalen Instanzen.

Erkunden	**Einrichten**
Security Incident Response-Integrationen	Erste Schritte mit der lokalen Microsoft Exchange-Integration
Verwenden	**Entwickeln**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Suchen und löschen Sie Phishing-E-Mails

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie Komponenten, die mit einer Anwendung installiert sind

---

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Erste Schritte mit der lokalen Microsoft Exchange-Integration

Die Microsoft Exchange Die lokale Integration bietet Sicherheitsanalysten Tools zum Eindämmen und Beheben von Phishing- und Phishing-E-Mail-Bedrohungen in lokalen Instanzen. Bevor Sie verwenden können Microsoft Exchange Lokale Integration, müssen Sie sie aus herunterladen ServiceNow Store Und identifizieren Sie die entsprechenden Exchange- und MID-Server.

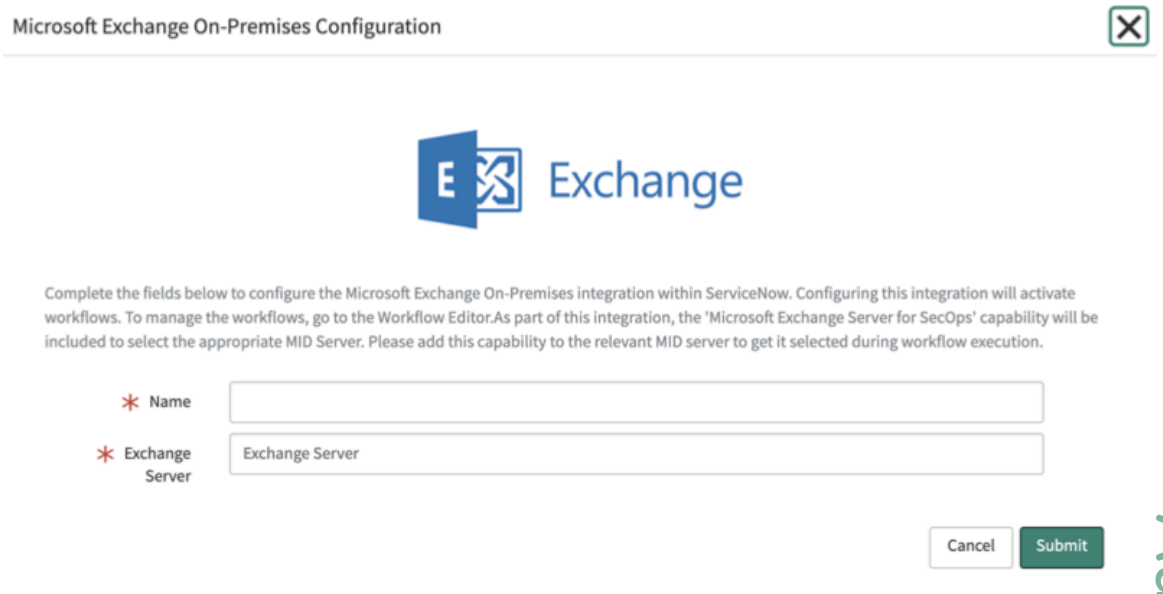
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Navigieren Sie nach Abschluss der Installation des bs zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. In Microsoft Exchange Lokale Karte klicken Sie auf **Neu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



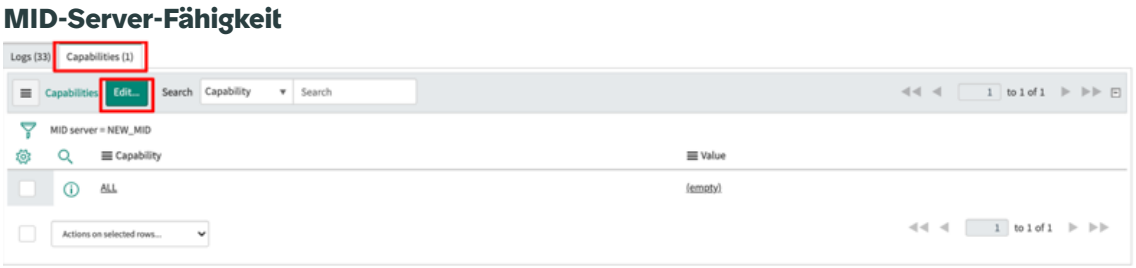
4. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Exchange Server	Geben Sie den zu verwendenden Exchange-Server an.

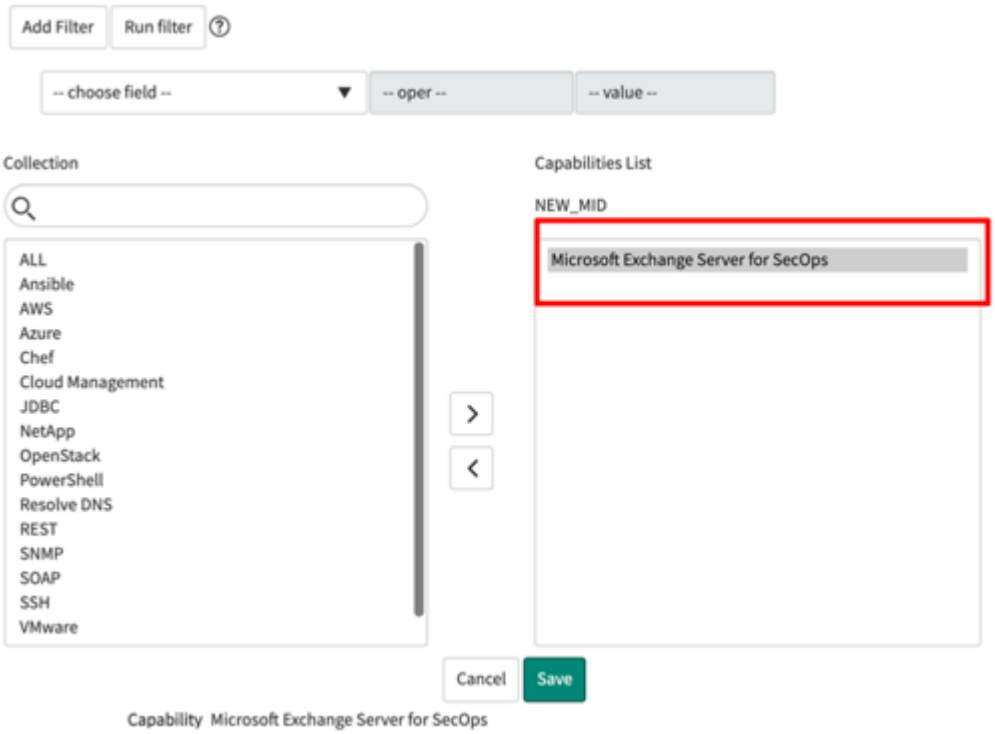
Hinweis:
Durch die Konfiguration dieser Integration werden Flows aktiviert. Navigieren Sie zum Verwalten der Flows zu **Workflow-Studio/Flow Designer.** .

5. Klicken Sie auf **Absenden**.
Die Integrationskonfigurationskarte wird angezeigt.
6. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf klicken **Konfigurieren** Oder **Löschen** Zum Ändern oder Löschen der Konfiguration.
7. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie aus **Nein** Von **Konfigurationen Anzeigen** Dropdown-Liste.
8. Navigieren zu **Orchestration** > **MID-Server**an.
9. Öffnen Sie den Datensatz, und überprüfen Sie den Status des MID-Servers, der für den Exchange-Server und seine erreichbar ist **Status** Option ist auf festgelegt **Aktiv** Und **Validiert** Option als **Ja** .
10. Fügen Sie die MID-Server-Fähigkeit hinzu:
    - Wählen Sie den entsprechenden MID-Server aus, um die Fähigkeit hinzuzufügen.
    - Klicken Sie auf **Fähigkeiten** Zugehörige Liste, und klicken Sie auf **Bearbeiten** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Entfernen **Alle** Und hinzufügen **Microsoft Exchange Server für SecOps** .



- Wählen Sie aus **IP-Bereiche** Von **Zugehörige Listen** Abschnitt und legen Sie den Wert auf einen der beiden fest **ALLE** Oder ein beliebiger gewünschter Wert.
- Wählen Sie aus **Unterstützte Anwendungen** Von **Zugehörige Listen** Abschnitt und legen Sie den Wert entweder auf ALLE oder Orchestration fest.
- **Speichern** Der Datensatz.

11. Validieren Sie die Verbindungen und Anmeldeinformationen.
12. Sobald die Anmeldeinformationen validiert wurden, ist die Konfiguration in der ServiceNow-Instanz abgeschlossen und kann mit dieser Integration E-Mail-Such- und -Löschvorgänge durchführen.

Microsoft Exchange – Durchführen des Flows für E-Mail-Suche und -Löschung

Wenn **Microsoft Exchange: E-Mail-Suche und -Löschung durchführen** Flow wird ausgeführt, durchsucht den Exchange-Server mithilfe der angegebenen Suchabfrage und gibt die Details an die lokale Instanz zurück.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Die **Microsoft Exchange: E-Mail-Suche und -Löschung durchführen** Flow wird ausgeführt, wenn E-Mail-Suchen eingerichtet werden und die **Aus E-Mail-Server(n) löschen** Oder **E-Mail-Server suchen** Schaltfläche wird gedrückt.

Aktionen, die für diese Integration spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Die Flow-Aktionen umfassen:

- Compliance-Suchaktion Erstellen
- Aktion „Compliance-Suchstatus Überprüfen“

Vorschau-Aktion für Compliance-Suche erstellen

Die Aktion „Vorschau der Compliance-Suche erstellen“ erstellt eine neue Compliance-Suchaktion vom Typ „Vorschau“ auf dem Exchange-Server für die erstellte Compliance-Suche.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
targetId	Obligatorisches Feld für Zielhost-Bezeichner, in dem sich der Exchange Server befindet.
SearchName	Obligatorischer Name der Compliance-Suche, die auf dem Exchange-Server erstellt wurde.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

Austrittsbedingungen

Variable	Beschreibung
Abschließen	Wenn die Compliance-Suchaktion erfolgreich erstellt wurde.
Fehler Beim Erstellen Der Aktion	Wenn die Erstellung der Compliance-Suchaktion aufgrund einer Ausnahme im Exchange-Server fehlschlägt.
Fehler	Wenn in der Flow-Aktion eine Ausnahme auftritt.

Status der Vorschauaktion überprüfen

Der Status der Vorschauaktion überprüft den Status der Compliance-Suchaktion vom Typ „Vorschau“ und gibt die Vorschauinformationen der gefundenen E-Mails zurück, z. B. Empfänger, Absender, Betreff, E-Mail-Empfangsdatum.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
targetId	Obligatorisches Feld für Zielhost-Bezeichner, in dem sich der Exchange Server befindet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
SearchName	Obligatorischer Name der Compliance-Suche, die auf dem Exchange-Server erstellt wurde.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response	Enthält den Status der Compliance-Suchaktion und die Vorschauinformationen der E-Mail, die als Teil der Compliance-Suche gefunden wurde.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

Austrittsbedingungen

Variable	Beschreibung
Vorschau wird ausgeführt	Wenn der Status der Compliance-Suchaktion „in Bearbeitung“ lautet.
Keine E-Mail Gefunden	Wenn der Status der Compliance-Suchaktion abgeschlossen ist und keine E-Mails als Teil der Compliance-Suche gefunden werden.
Vorschau Abgeschlossen	Wenn der Status der Compliance-Suchaktion abgeschlossen ist und E-Mails als Teil der Compliance-Suche gefunden werden.
Fehler Beim Überprüfen Des Status	Wenn die Statusüberprüfung aufgrund einer Ausnahme im Exchange-Server fehlschlägt.
Fehler	Wenn eine Ausnahme in der Workflow-Aktivität auftritt.

Lösch-Aktion für Compliance-Suche erstellen

Mit der Aktion „Compliance-Suche erstellen – Löschen“ wird eine neue Compliance-Suchaktion vom Typ „Löschen“ auf dem Exchange-Server für die erstellte Compliance-Suche erstellt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
targetId	Obligatorisches Feld für Zielhost-Bezeichner, in dem sich der Exchange Server befindet.
SearchName	Obligatorischer Name der Compliance-Suche, die auf dem Exchange-Server erstellt wurde.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Austrittsbedingungen

Variable	Beschreibung
Abschließen	Wenn die Compliance-Suchaktion erfolgreich erstellt wurde.
Fehler Beim Erstellen Der Aktion	Wenn die Erstellung der Compliance-Suchaktion aufgrund einer Ausnahme im Exchange-Server fehlschlägt.
Fehler	Wenn in der Flow-Aktion eine Ausnahme auftritt.

Status der Löschaktion überprüfen

Die Option Status der Aktion „Löschen überprüfen“ überprüft den Status der Compliance-Suchaktion vom Typ „Löschen“ und führt den Soft-Delete-Vorgang auf dem Exchange-Server für die E-Mails aus, die als Teil der Compliance-Suche gefunden wurden.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
targetId	Obligatorisches Feld für Zielhost-Bezeichner, in dem sich der Exchange Server befindet.
SearchName	Obligatorischer Name der Compliance-Suche, die auf dem Exchange-Server erstellt wurde.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response	Enthält den Status der Compliance-Suchaktion und die Anzahl der gelöschten E-Mails, die als Teil der Compliance-Suche gefunden wurden.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

Austrittsbedingungen

Variable	Beschreibung
Löschen in Bearbeitung	Wenn der Status der Compliance-Suchaktion „in Bearbeitung“ lautet.
Keine E-Mail Gefunden	Wenn der Status der Compliance-Suchaktion abgeschlossen ist und keine E-Mails als Teil der Compliance-Suche gelöscht werden.
Löschen abgeschlossen	Wenn der Status der Compliance-Suchaktion abgeschlossen ist und E-Mails als Teil der Compliance-Suche gelöscht werden.
Fehler Beim Überprüfen Des Status	Wenn die Statusüberprüfung aufgrund einer Ausnahme im Exchange-Server fehlschlägt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Austrittsbedingungen (Fortsetzung)

Variable	Beschreibung
Fehler	Wenn in der Flow-Aktion eine Ausnahme auftritt.

Compliance-Suchaktion Entfernen

Die Aktion Compliance-Suche entfernen entfernt die erstellte Compliance-Suche vom Exchange-Server.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
targetId	Obligatorisches Feld für Zielhost-Bezeichner, in dem sich der Exchange Server befindet.
SearchName	Obligatorischer Name der Compliance-Suche, die auf dem Exchange-Server erstellt wurde.

Integration der Microsoft Graph-Sicherheits-API-Warnungserfassung

Verwenden Sie Microsoft Graph-Sicherheits-API Integration, um Warnungen von Microsoft Graph-Sicherheitsanbietern zu erfassen und automatisch Security Incidents zu erstellen.

Übersicht

Die Microsoft Graph-Sicherheits-API Ist ein intermediärer Service (oder Broker), der eine einzige programmgesteuerte Schnittstelle zum Verbinden mehrerer Sicherheitsanbieter (nativ für Microsoft sowie ServiceNow-Partner) bietet.

Die Microsoft Graph-Sicherheits-API Die Integration behebt diese Probleme mithilfe von Microsoft Graph-Sicherheits-API Um eine Verbindung mit verschiedenen Microsoft-Sicherheitstechnologien wie Azure Sentinel, Microsoft Defender Advanced Threat Protection und Azure Advanced Threat Protection herzustellen. Warnungen von Microsoft-Sicherheitsanbietern werden erfasst, und Security Incidents werden automatisch in erstellt Security Incident Response.

Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Discovery von Microsoft Graph-Sicherheits-API Warnungen, die Kandidaten für Security Incidents sind und die Erstellung von Security Incidents automatisieren.
- Zuordnung von Warnungsfeldern zu Security Incident-Feldern.
- Zusammenfassung ähnlicher Warnungen zu vorhandenen offenen Security Incidents, anstatt doppelte Security Incidents zu erstellen.
- Zeigen Sie eine Vorschau der Warnungsfeldwerte an, und validieren Sie ihre Zuordnungen im Security Incident.
- Automatische Aktualisierung des Warnungsstatus für die Erstellung und Schließung von Security Incidents.
- Richten Sie die geplante Erfassung von Warnungen ein, um regelmäßig Security Incidents zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie Ihre Now Platform-Instanz für die Integration der Microsoft Graph-Sicherheits-API ein

Im folgenden Abschnitt werden die Setup-Aufgaben aufgeführt, die Sie in ausführen müssen ServiceNow AI Platform® Instanz vor der Installation der Anwendung über ServiceNow Store.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Überprüfen Sie anhand der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform® Und Security Incident Response Rollen.	Die folgenden Rollen sind für die Installation, das Setup und die Verwendung der Integration in erforderlich ServiceNow AI Platform® Instanz. • Ein Anwender mit ServiceNow AI Platform® Die Administratorrolle (admin) installiert die Anwendung aus dem ServiceNow Store Und weist die Rolle Security Incident-Administrator (sn_si.admin) zu. • Ein Anwender mit der Rolle „sn_si.admin“ überwacht die folgenden Aufgaben in ServiceNow AI Platform®: ◦ Benennt, erstellt und bearbeitet Warnungsprofile. ◦ Wählt Warnungsdatenfelder der Microsoft Graph-Sicherheits-API aus und ordnet sie den Security Incident-Feldern zu. ◦ Zeigt vor dem Abschluss der Konfiguration eine Vorschau der Security Incident-Details auf Richtigkeit an. ◦ Plant die laufende Warnungserfassung. ◦ Aktiviert Warnungsaktualisierungen, wenn ein Security Incident Response Incident wird erstellt und geschlossen. ◦ Weist die Rolle Security Incident Analyst (sn_si.Analyst) zu. ◦ Anwender mit sn_si.Analyst arbeiten mit Security Incidents. Weitere Informationen zu Rollen und dem Zuweisen von Rollen an Anwender finden Sie unter Rollen im ServiceNow-Produktdokumentationswebsite .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
Registrieren Sie Ihre Anwendung in Microsoft Azure Portal.	Bevor Sie Warnungen erfassen können, müssen Sie Ihre Anwendung in konfigurieren Microsoft Azure Portal. Details siehe Konfigurieren Sie das Microsoft Azure-Portal.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. **1.** Security Incident Response **2.** Ereignis- und Warnungserfassung für Security Operations: Diese Anwendung erfordert: ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit ○ Com.Glide.Hub.action_STEP.Rest => ServiceNow IntegrationHub Aktionsschritt – REST **Hinweis:** Die Integration Hub-Komponenten werden zusammen mit dem Plugin „Ereignis- und Warnungserfassung“ installiert. Wenn diese nicht installiert sind, wenden Sie sich an den Kundensupport, um Unterstützung zu erhalten. Weitere Informationen zur Installation von finden Sie Security Operations Kernanwendungen, siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

Konfigurieren Sie das Microsoft Azure-Portal

Dient zum Abrufen von Sicherheitswarnungen für eine Anwendung, die im Microsoft Azure-Mandanten mit verfügbar ist Microsoft Graph-Sicherheits-API, Sie müssen die Anwendung in registrieren Microsoft Azure Portal und gewähren Sie Lese- und Schreibzugriff für Sicherheitsereignisse auf die Anwendung.

Vorbereitungen

Erforderliche Rolle:

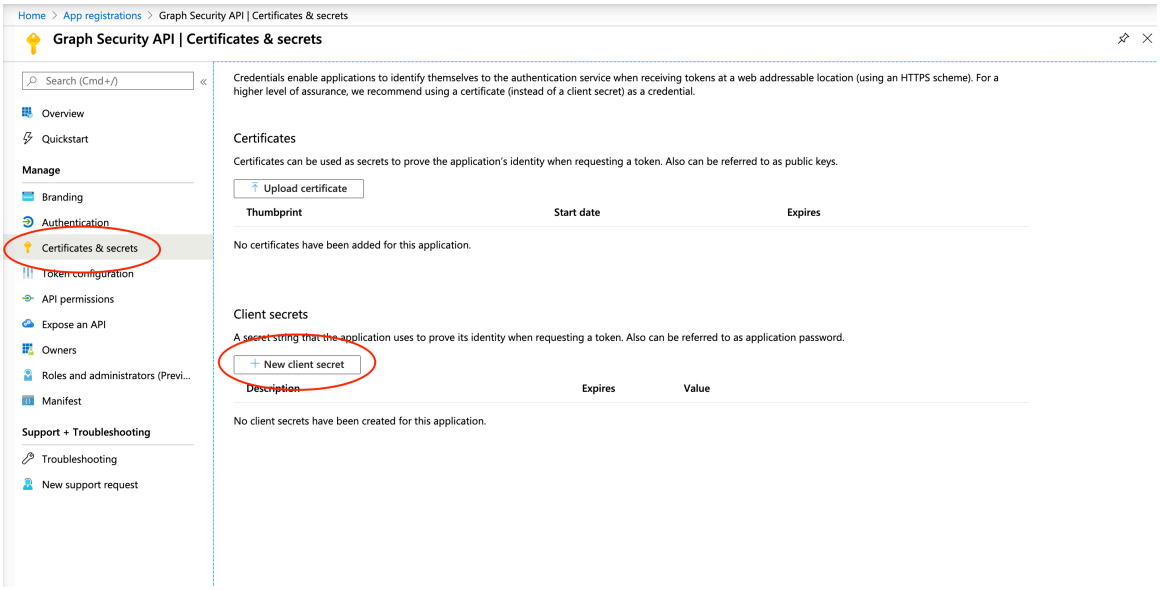
- Anwendungsentwickler: Erforderlich für die Registrierung der Anwendung.
- Mandantenadministrator: Der Microsoft Azure Der Mandantenadministrator muss der Anwendung Berechtigungen gewähren, indem er den Endpunkt der Administratoreinwilligung anruft.

Prozedur

1. Melden Sie sich bei an Microsoft Azure Portal.
2. Geben Sie Ein **App-Registrierungen** In **Suchen** Feld.
3. Klicken Sie auf **New registration (Neue Registrierung)**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie einen Namen für Ihre Anwendung und den Umleitungs-URI ein, z. B. http://localhost, und klicken Sie auf **Registrieren** .
   Der Umleitungs-URI wird verwendet, wenn der Administrator die Zustimmung für die Anwendung erteilt.
5. Wählen Sie auf der Seite „App-Registrierungen“ die Anwendung aus, die Sie registriert haben, z. B. Graph-Sicherheitsdemo.
6. Unter **Verwalten** , Wählen Sie aus **Zertifikate und Geheimnisse** .



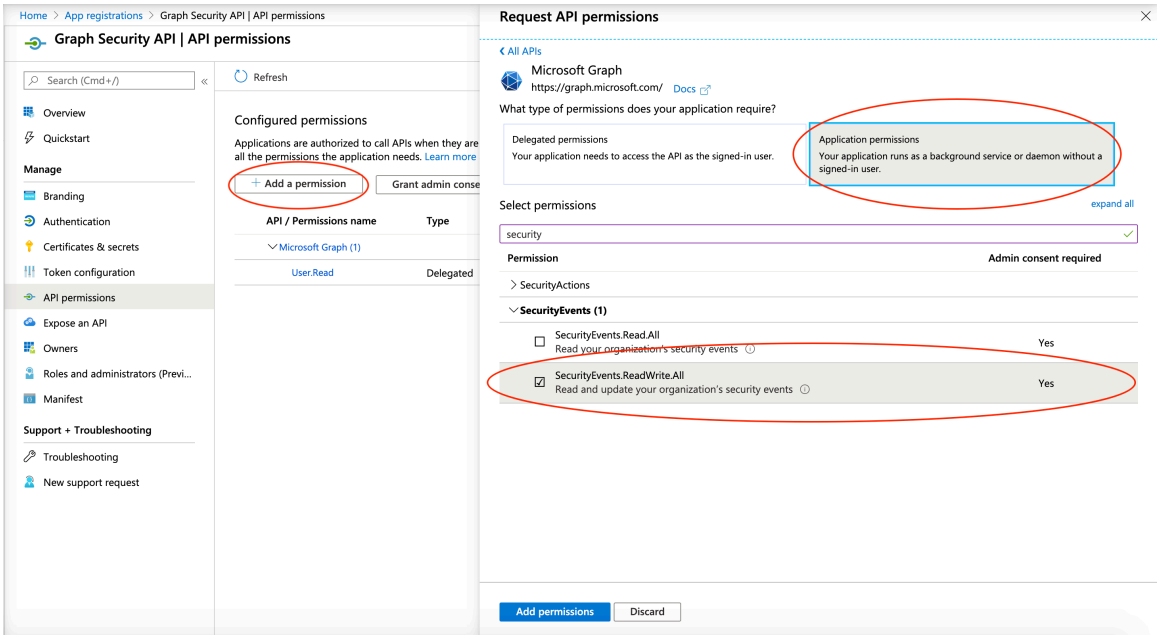
7. Wählen Sie Aus **Neues geheimes Clientgeheimnis** Dient zum Erstellen eines geheimen Clientschlüssels.
   Kopieren Sie das geheime Clientgeheimnis, und speichern Sie es, da es später nicht sichtbar ist. Wenn Sie das geheime Clientgeheimnis vergessen haben, können Sie ein neues geheimes Clientgeheimnis generieren.

   Hinweis:
   Wenn Sie das geheime Clientgeheimnis vergessen, können Sie ein neues generieren, indem Sie die Anweisungen in den Schritten 4 und 5 befolgen.

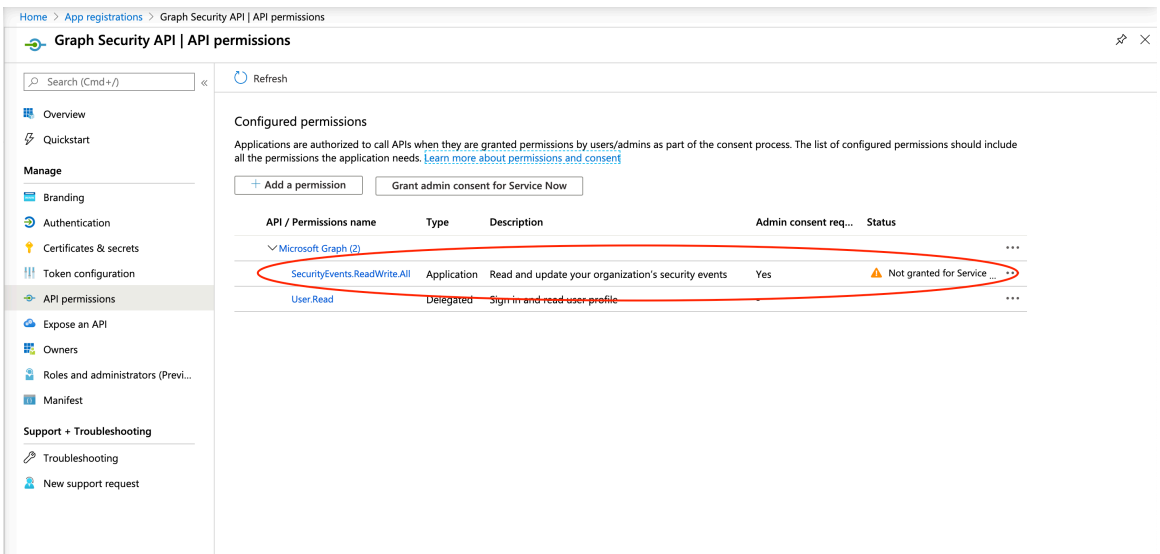
8. Klicken Sie Auf **Zeigen Sie API-Berechtigungen an** Auf der Seite „Übersicht“.
9. Fügen Sie neue API-Berechtigungen auf Anwendungsebene für Sicherheitsereignisse.Lesen.Schreiben.alle Sicherheitsereignisse hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Gewähren Sie die Zustimmung des Administrators für die neu hinzugefügten API-Berechtigungen. Weitere Informationen finden Sie unter Microsoft Graph-Berechtigungsreferenz Microsoft Graph-Berechtigungsmodell.



11. Melden Sie sich als Mandantenadministrator an, und geben Sie die Zustimmung für die Anwendung ein. Die Schritte sind unten aufgeführt:

a. Navigieren Sie zur folgenden URL: https://login.microsoftonline.com/common/adminconsent?client_id=APPLICATION_ID&state=12345

Geben Sie die APPLICATION_ID der Anwendung ein, die Sie registriert haben.

12. Klicken Sie Auf **Akzeptieren** Um Berechtigungen zu akzeptieren, die von der oben erstellten Anwendung angefordert wurden.
Sie können dann die Anwendung verwenden, um Sicherheitsereignisse zu lesen. Siehe Microsoft Graph-Sicherheitsautorisierung Dokumentation für weitere Details.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie die ServiceNow-Anwendung für die Integration der Microsoft Graph-Sicherheits-API-Warnungserfassung

Bevor Sie die Integration für ausführen ServiceNow AI Platform® Führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in integriert wird Security Incident Response Und Security Operations Produkte auf Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn Sie den nicht installiert haben Microsoft Graph-Sicherheits-API Anwendung aus dem ServiceNow Store Informationen zur Integration finden Sie unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie die Kachel Microsoft Graph-Sicherheits-API – Warnungserfassung.

3. Klicken Sie auf , um die Anwendung zu konfigurieren **Konfigurieren** .
4. Füllen Sie die Felder im angezeigten Dialogfeld „Konfiguration der Warnungserfassung“ aus.
5. Klicken Sie auf **Absenden**.
   Nachdem sie erfolgreich validiert und übermittelt wurde, wird jede Serverkonfiguration für Warnungserfassungen auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, klicken Sie oben rechts auf der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja** .

Nächste Maßnahme

Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht darin, ein Warnungsprofil zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Profil für die Integration der Microsoft Graph-Sicherheits-API-Warnungserfassung

Als Anwender mit der Rolle sn_si.admin erstellen Sie in ein Warnungsprofil ServiceNow AI Platform Instanz und bestimmen, welche Warnungen Security Incidents erstellen. Bevor Security Incidents aus erfassten Warnungen erstellt werden, werden die Feldwerte aus Warnungen in einem Layout von angezeigt ServiceNow AI Platform Security Incident, damit Sie eine Vorschau darauf anzeigen können, wie der tatsächliche Security Incident angezeigt wird.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Mit der Integration können Sie verschiedene Arten von Warnungen erfassen, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese Warnungen werden basierend auf den Profilen erfasst, die Sie in konfigurieren Security Operations Umgebung Ihrer Instanz. Alle Warnungen werden anfänglich für einen konfigurierten Warnungstyp in einem Profil erfasst. Erfasste Warnungen können dann weiter gefiltert werden, um anzugeben, welche Warnungen Security Incidents erstellen.

Sie können beispielsweise Filter bevorzugen, die Security Incidents nur für Warnungen erstellen, die als hohes Risiko identifiziert werden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Warnungen erstellt, werden einzelne Feldwerte in den gefilterten Warnungen den entsprechenden Feldern in einem Layout von Security Incidents zugeordnet, um eine Vorschau anzuzeigen. Alle Warnungen, die die Auswahlkriterien in erfüllen Microsoft Azure Mandanten und sind über verfügbar Microsoft Graph-Sicherheits-API Werden anfänglich in erfasst ServiceNow AI Platform Instanz.

Identifizieren Sie die Quelle für das Profil

Geben Sie den Namen und die Quelle für das Profil an.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Um ein Profil für eine Warnung in zu erstellen ServiceNow AI Platform Instanz, navigieren Sie zu **Microsoft Graph-Sicherheits-API – Integration** > **Microsoft Graph-Sicherheits-API-Profil**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

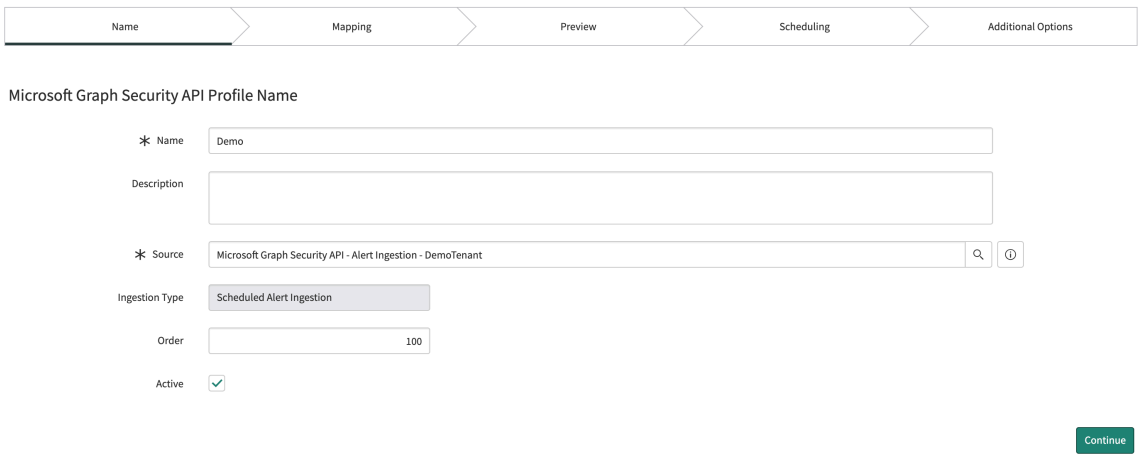
   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

Feld	Beschreibung
Name	Eindeutiger Name für das Profil. Wenn Namen nicht eindeutig sind, wird ein Fehler angezeigt, und doppelte Profilnamen werden nicht gespeichert. Profilnamen in Ihrem ServiceNow AI Platform Instanz muss eindeutig sein.
Aktiv	Das Kontrollkästchen ist standardmäßig deaktiviert. Wenn diese Option deaktiviert ist, ist das Profil nicht aktiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Sie sollten alle Abschnitte im Profil abschließen, bevor Sie es aktivieren.
Quelle	Die Microsoft Azure Mandant, den Sie zum Erfassen von Warnungen konfiguriert haben. Wenn Sie mehrere Mandanten konfiguriert haben, wählen Sie den entsprechenden Mandanten für die Warnungstypen aus, die Sie für das Profil erfassen möchten. Sie müssen einen Wert eingeben.
Reihenfolge	Der Standardwert ist 100. Wenn Sie mehrere Profile erstellt haben, gibt dieser Wert eine Laufzeitausführungspriorität an, wenn zwei oder mehr Profile dieselben Auslösebedingungen haben. Je niedriger der Reihenfolgewert, desto höher die Priorität.
(Optional) Beschreibung	Zusätzlicher Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.



Nächste Maßnahme

Der nächste Schritt besteht darin, die Warnungsfelder zuzuordnen.

Zuordnung von Warnungsfeldern für die Integration der Microsoft Graph-Sicherheits-API-Warnungserfassung

Nachdem Sie die Quellen für die geplante Warnungserfassung identifiziert haben, besteht der nächste Schritt darin, einzelne Warnungsfelder den Feldern in einem zuzuordnen ServiceNow AI Platform SIR Security Incident.

Für den Zuordnungsschritt müssen Sie zuerst Beispielwarnungen aus dem erfassen Microsoft Azure Mandant. Dann müssen Sie sicherstellen, dass alle relevanten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsfelddaten dem entsprechenden Ort in zugeordnet sind SIR Incident-Formular und visualisieren Sie dann SIR Incident im Vorschauabschnitt.

Die Zuordnung der Beispiel-Warnungsfelder umfasst Folgendes:

- Erfassen Sie Beispielwarnungen der Microsoft Graph-Sicherheits-API
- Zuordnung von Warnungen zu Security Incident Response-Feldern

Erfassen Sie Beispielwarnungen der Microsoft Graph-Sicherheits-API

Erfassen Sie Beispielwarnungen von Ihrem Microsoft Azure Mandant.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

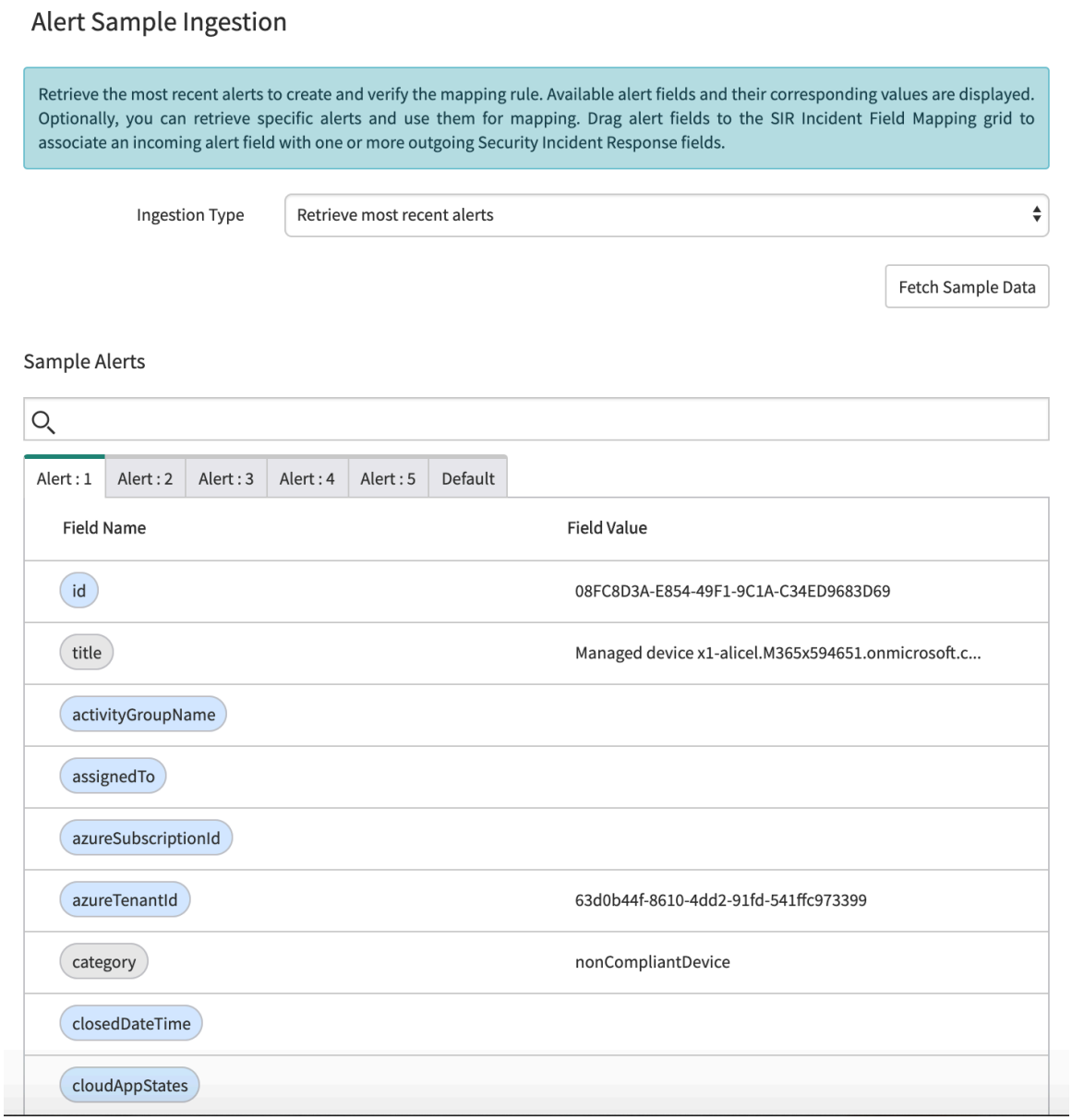
Prozedur

1. Sie können entweder die 5 neuesten Beispielwarnungen abrufen oder die eindeutigen Warnungs-IDs für die spezifischen Warnungen angeben, die Sie für Ihre Zuordnungs-Experience verwenden möchten.
   Von **Erfassungseinstellung** Auswahlliste wählen Sie eine der folgenden Optionen aus:
   - Neueste Warnungen abrufen: Die 5 neuesten Warnungen werden abgerufen.
   - Warnungen basierend auf Warnungen-ID auswählen: Geben Sie die Warnungs-ID für die abzurufenden Warnungen an. Sie können maximal 5 durch Kommas getrennte Warnungs-IDs angeben.
2. Klicken Sie Auf **Rufen Sie Beispieldaten Ab** Zum Abrufen der neuesten Beispielwarnungsdaten aus dem Microsoft Azure Mandant.
   Der Abruf für Beispielwarnungen kann einige Minuten dauern.

   Die Beispielwarnungsfeldwerte werden auf der linken Seite des Formulars ausgefüllt, wenn Beispielwarnungen vom Profil erfasst werden. Dies sind die Warnungen, die Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dem zuordnen SIR Security Incident-Felder. Die Ergebnisse der Warnungsfelder und -Werte werden als einzelne Registerkarten angezeigt.



Nächste Maßnahme

Nachdem Sie die Beispieldaten abgerufen haben, ordnen Sie die Warnungsfelder dem Security Incident zu.

Zuordnung von Warnungen zu Security Incident Response-Feldern

Ordnen Sie einzelne Warnungsfelder aus ausgelösten Warnungen Feldern in einem zu ServiceNow AI Platform Security Incident.

Warnungsfeldzuordnung

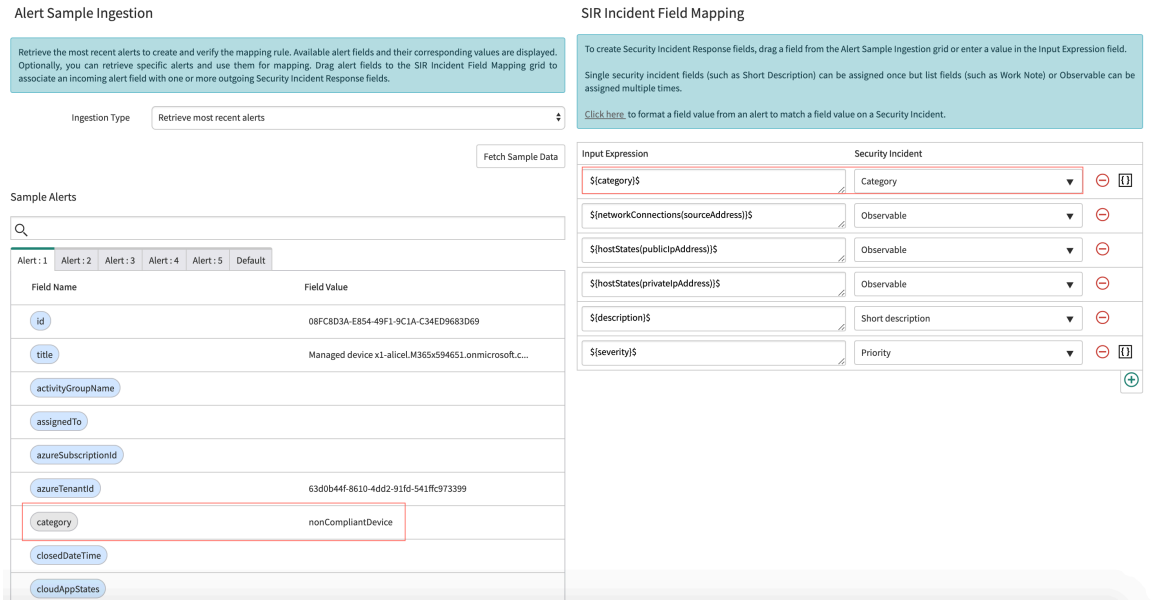
Verwenden Sie als Anwender mit der Rolle sn_si.admin die Felder aus dem Abschnitt Beispielwarnungen auf der linken Seite, und ordnen Sie sie den Security Incident-Feldern in der Spalte SIR-Incident-Feldzuordnung im rechten Bereich zu. Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Warnungsfelder von der linken Seite ziehen und auf dem ablegen SIR Incident-Zuordnungsabschnitt auf der rechten Seite. Die Zuordnung auf der rechten Seite ordnet das Feld für eingehende Warnungen einem Feld für ausgehende Security Incidents zu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Nachdem Sie die Beispieldaten abgerufen haben, ordnen Sie die Warnungsfelder dem Security Incident zu. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf der linken Seite des Formulars auf einen blauen Feldnamen.
2. Ziehen Sie den Feldnamen, z. B. Kategorie , Und legen Sie es in einem Feld in der Spalte „Eingabeausdruck“ neben einem Feldnamen in der Spalte „Security Incident“ ab.

   Der Feldwert wird in der Spalte „Eingabeausdruck“ angezeigt. In der folgenden Abbildung: Kategorie Ist dem zugeordnet Kategorie Feld im Security Incident.



Sie können jedoch einen beliebigen Wert von der linken Seite mit einem Feld auf der rechten Seite abgleichen. Stellen Sie sicher, dass der Wert dem Security Incident während des Vorschauschritts korrekt zugeordnet ist.

Damit Sie sicherstellen können, dass im Zuordnungsprozess keine Warnungsfelder übersehen oder dupliziert werden, sind Felder farbcodiert. Die Farbcodierung der Warnungsfelder hilft Ihnen, die Warnungswerte nachzuverfolgen, die Sie bereits zugeordnet haben, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder blau angezeigt werden. Auf diese Weise können Sie besser visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Warnungsinformationen nicht zugeordnet sind.

Hellblaue Felder auf der linken Seite zeigen an, dass noch kein Warnungsfeld ausgewählt und dem Security Incident zugeordnet ist. Möglicherweise möchten Sie ein eingehendes Warnungsfeld mit mehr als einem Feld in einem Security Incident verknüpfen. Ein graues Feld gibt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

a. Um einen Wert manuell in das Feld Eingabeausdruck einzugeben, geben Sie ihn im Format ${fieldname}$ ein. Das Warnungsfeld wird dem Security Incident-Feld zugeordnet.

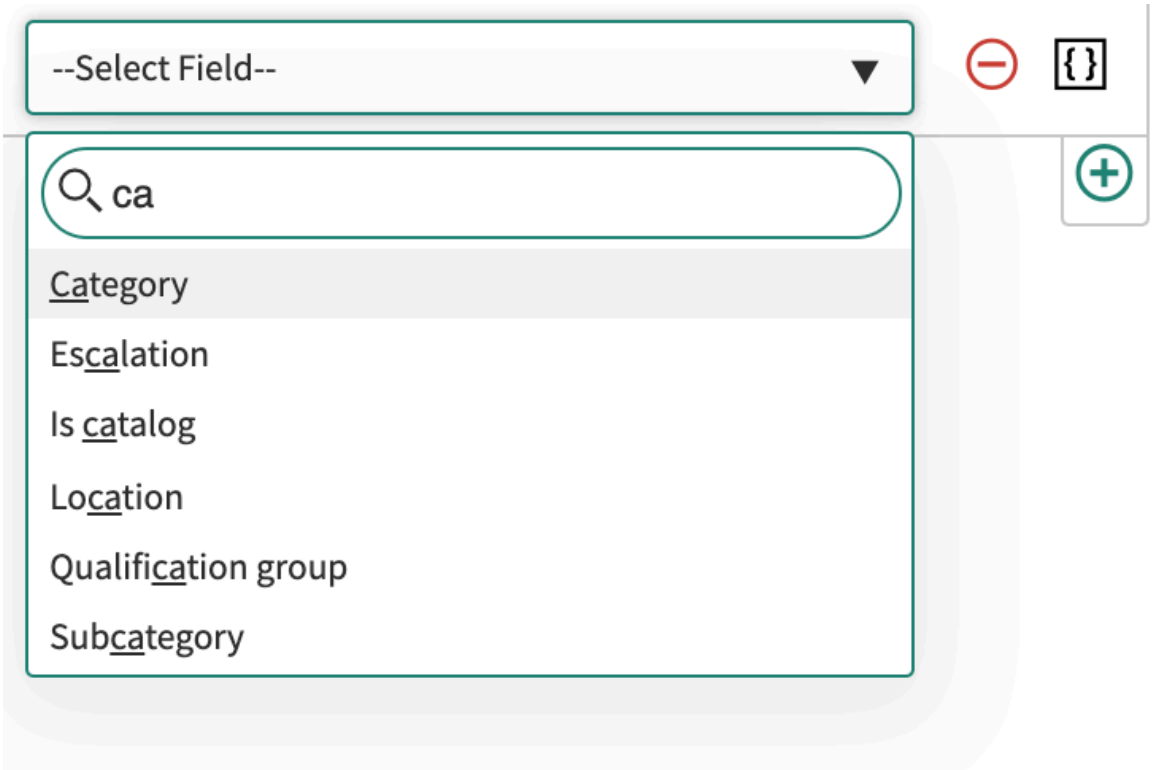
b. Sie können erfasste Warnungen nicht dem zuordnen MITRE-ATT&CK Framework-Felder im Abschnitt „Security Incident-Zuordnung“. Wenn Sie die Felder weiterhin zuordnen, sind die Informationen nicht als Teil von verfügbar MITRE-ATT&CK Karte in MITRE-ATT&CK Framework-Abschnitt im Security Incident-Formular. Um zuzuordnen MITRE-ATT&CK-Techniken verwenden Automatische Extraktionsfunktion Verfügbar als Teil von MITRE-ATT&CK Framework in Threat Intelligence Modul.

3. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen.

a. Rechts neben dem Formular in SIR Klicken Sie im Abschnitt „Incident-Feldzuordnung“ unten im Raster auf das Plus-Symbol (+). Ein neues Feld wird angezeigt.

b. Erweitern Sie in der Spalte Security Incident die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung hat Kategorie einen grauen Hintergrund, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Warnungsfelder auf der linken Seite des Formulars hilft diese Farbcodierung für die Security Incident-Felder auf der rechten Seite Ihnen, die bereits zugeordneten nachzuverfolgen SIR Incident-Felder.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Da mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „erkennbares Element“ mehrmals verschiedenen Werten zugeordnet werden. Ebenso unterstützen die Felder „Konfigurationselement“ und „Arbeitsnotizen“ mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

c. Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.

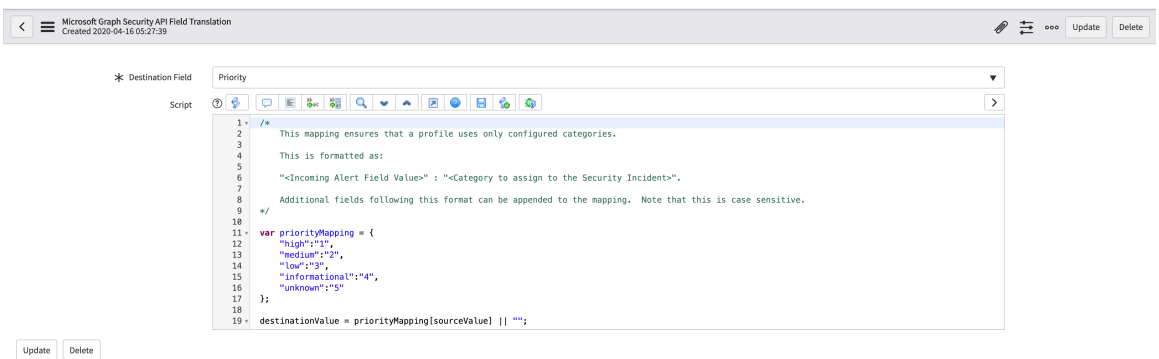
d. Klicken Sie auf der linken Seite des Formulars mit der linken Maustaste, um die gewünschte Warnungs-ID im Feld Eingabeausdruck auszuwählen. Ordnen Sie sie mit der Drag-and-Drop-Funktion neben Ihrem neuen Feld zu.

4. Fahren Sie mit der Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder entfernen.
5. Nachdem Sie die vorherigen Feldzuordnungsschritte abgeschlossen haben, können Sie dieselben Feldwerte im Generator für Incident-Generierungsbedingungen verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Warnung erfüllen muss, um einen Security Incident zu erstellen. Um Bedingungen für die Incident-Generierung festzulegen, gehen Sie wie folgt vor.

Formatfeldübersetzung

In bestimmten Fällen werden Warnungsfeldwerte in angezeigt Microsoft Graph-Sicherheits-API Kann nicht direkt in die Felder des SIR Security Incident übersetzt werden. Für diese Werte können Sie einen Skripteditor verwenden, um Feldwerte für den Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind. Beispielsweise kann ein Kategoriewert von Malware-Warnung und Virusinfektion mit dem Skript-Editor verschiedene Feldwerte für die Quellkategorie haben, aber beide Werte können mithilfe der Funktionalität Formatierungsfeldübersetzung in eine allgemeine schädliche Code-Aktivität im Feld Kategorie des SIR Security Incident übersetzt werden.

Um den Skript-Editor zu verwenden, klicken Sie auf das Symbol {}. Der Skripteditor wird angezeigt.



Bedingungen für die Incident-Generierung

Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, damit Sie angeben können, welche Warnungen Security Incidents erstellen sollen und welche Warnungen herausgefiltert werden sollen, z. B. Warnungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

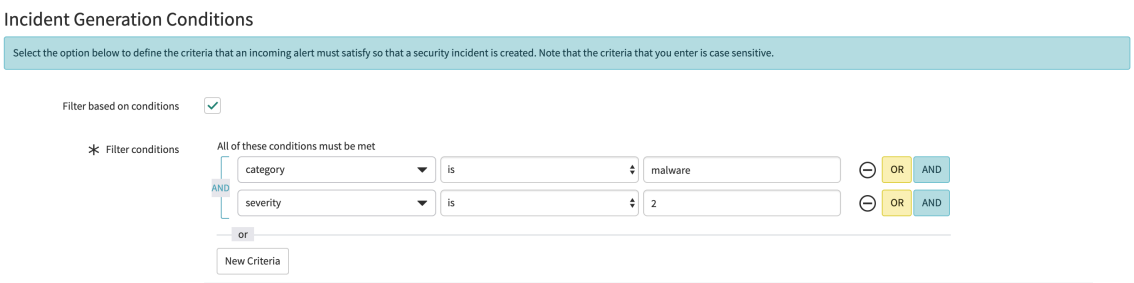
mit niedriger Priorität. Sie können dieselben Feldwerte im Generator für Incident-Generierungsbedingungen verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Warnung erfüllen muss, um einen Security Incident zu erstellen. Um Bedingungen für die Incident-Generierung festzulegen, gehen Sie wie folgt vor.

1. Scrollen Sie im Formular zum Abschnitt Bedingungen für die Incident-Generierung, und wählen Sie die Option Filter basierend auf Bedingungen aus. Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den spezifischen Bedingungen entsprechen, die in den Feldern beschrieben werden.

   Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen entsprechen den Feldern, die im Abschnitt „Warnungsbeispielerfassung“ für die von Ihnen erfasste Warnung angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach der Warnung, die Sie erfassen, wobei die Groß-/Kleinschreibung beachtet wird, und sie müssen genau mit den Werten der Warnung übereinstimmen. Wenn Sie sich nicht sicher sind, welche Werte in die Filterfelder eingegeben werden sollen, können Sie zu Ihrem Microsoft Azure-Mandanten zurückkehren und Ihre Warnungen auf die Stichwörter überprüfen.

2. Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** Oder **ODER** .
   - Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden.
4. Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest

   Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt werden müssen, bevor Security Incidents erstellt werden.



   Sie haben die Auslösebedingungen so festgelegt, dass Security Incidents nur erstellt werden, wenn beide von Ihnen eingegebenen Filterbedingungen erfüllt sind.

   Diese Art der Filterung hilft Ihnen, Sicherheitswarnungen zu isolieren, und begrenzt die Anzahl der von Ihnen erstellten Security Incidents. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur erforderliche Warnungen erfasst, ohne die Abfrage oder die Konfiguration der ausgelösten Warnungen ändern zu müssen.

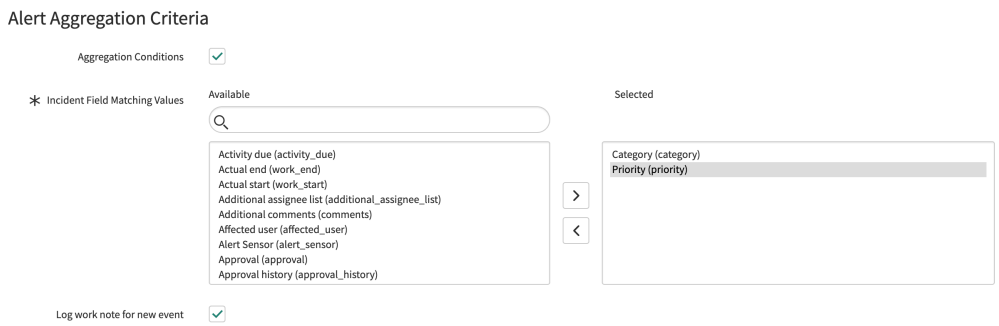
Warnungszusammenfassungskriterien, um ähnliche Warnungen zu behandeln und doppelte Incidents zu verhindern

Definieren Sie zusätzliche Warnungszusammenfassungskriterien, die eine eingehende Warnung zu einer vorhandenen aggregieren SIR Security Incident anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Mithilfe von Feldübereinstimmungswertkriterien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl aktiver, sich überschneidender Security Incidents reduzieren, indem alle zugehörigen Warnungsdaten auf einen einzelnen Security Incident gesetzt werden. Um die Kriterien festzulegen, führen Sie die folgenden Schritte aus:

1. Scrollen Sie im Formular zum Abschnitt Warnungszusammenfassungskriterien, und wählen Sie die Option Zusammenfassungsbedingungen aus. Die Spalten „Incident-Feld-Übereinstimmungswerte“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die in konfiguriert sind SIR Security Incident.
2. Wählen Sie in der Liste verfügbar die Feldwerte aus, die Sie für vorhandene Security Incidents in abgleichen möchten ServiceNow AI Platform Und verschieben Sie sie in die Liste ausgewählt. Alle von Ihnen ausgewählten Feldwerte müssen abgeglichen werden, um diese eingehende Warnung an einen vorhandenen Security Incident anzuhängen. Dies umfasst Felder, z. B. erkennbare Elemente und Konfigurationselemente, denen möglicherweise mehrere Warnungsfeldwerte zugeordnet sind. Alle Werte müssen übereinstimmen. Wenn nur eine Teilmenge der Werte übereinstimmt, werden die Bedingungen für die Warnungszusammenfassung nicht erfüllt, und ein neuer Security Incident wird erstellt. Siehe Screenshot unten für die Feldzuordnung mit mehreren Werten.



Wenn eine neue Warnung allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird die Warnung automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Anwender mit der Rolle „sn_si.Analyst“, der mit Security Incidents arbeitet, können Sie alle hinzugefügten aggregierten Warnungen in einer zugehörigen Liste zu einem Security Incident anzeigen. Alle zusammengefassten Warnungen zu einem Security Incident werden in der zugehörigen Liste „zusammengefasste Microsoft Graph-Warnungen“ angezeigt. Diese Liste enthält Details zu zugehörigen Zeitstempeln und zusammengefassten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum Warnungen vorhandenen Security Incidents hinzugefügt werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie unter zugehörige Links zur linken Seite des Datensatzes, und klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Link.

3. (Optional) um eine Arbeitsnotiz für eine neue Warnung zu protokollieren, die kürzlich zum Security Incident hinzugefügt wurde, aktivieren Sie das Kontrollkästchen, um diese Option zu aktivieren. Die Arbeitsnotiz protokolliert, dass eine neue Warnung hinzugefügt wurde, zusammen mit einem Link zu den Warnungsdetails und allen anderen Details, die dem Feld Arbeitsnotiz in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

   Sie haben Werte aus einer Warnung erfolgreich zu Feldern in einem zugeordnet SIR Security Incident. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellung von Security Incidents mit Filterkriterien einzuschränken. Sie haben auch Warnungen oder Ereignisse an vorhandene angehängt SIR Security Incidents.

4. Klicken Sie Auf **Fahren Sie Fort** Um mit der Profilkonfiguration fortzufahren. Der nächste Schritt besteht darin, eine Vorschau der Felder anzuzeigen, die Sie einem SIR Security Incident zugeordnet haben

Zeigen Sie eine Vorschau des Security Incidents für die Microsoft Graph Security API-Integration an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem zugeordnet haben ServiceNow AI Platform SIR Security Incident. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Warnungsfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Vorbereitungen

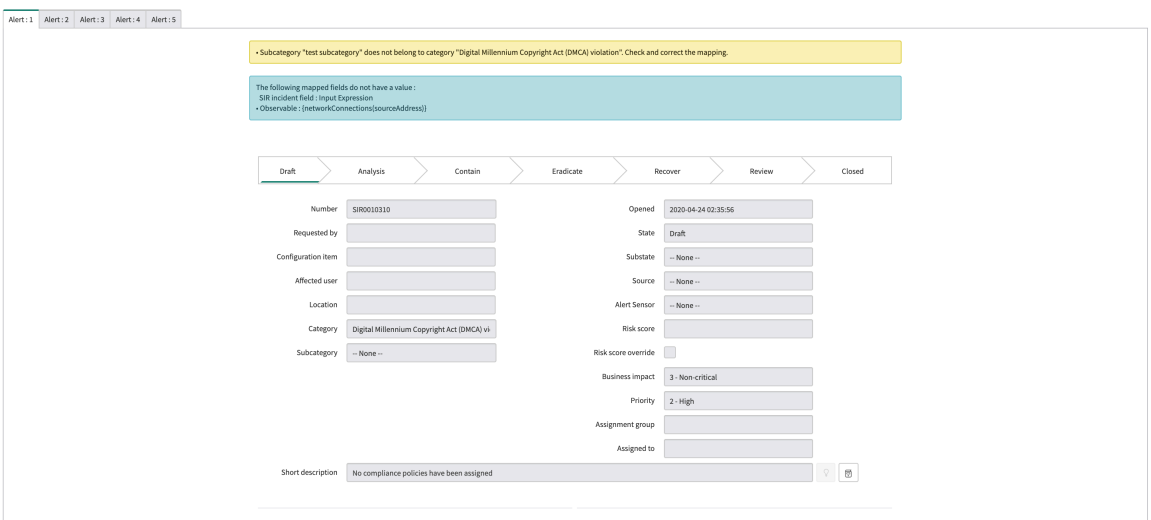
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Als Anwender mit der Rolle „sn_si.admin“ können Sie eine Vorschau eines Security Incidents anzeigen und die Zuordnung nach Bedarf erneut bearbeiten, um Felder mit Fehlern zu beheben oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wurde, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen von SIR Security Incidents werden nicht als tatsächliche Incidents in gespeichert Security Incident Response Produkt.

Prozedur

1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie auf **Vorschau** In der Fortschrittsleiste.
   Alle erfassten Warnungen und die Feldzuordnungen, die auf der Seite „Zuordnung“ definiert sind, werden angezeigt.
2. Klicken Sie auf eine Warnungs-ID, um eine Vorschau des Security Incident anzuzeigen.
   Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.
3. Überprüfen Sie die Feldzuordnung der Warnungswerte für den Security Incident.



Das vorherige Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler der erfassten Beispiele.

4. Klicken Sie auf, um diesen Fehler zu beheben **Zuordnung** In der Fortschrittsleiste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie erneut eine Vorschau der Zuordnung an, und beheben Sie alle Fehler, die in Fehlermeldungen beschrieben werden.

Nächste Maßnahme
Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind, besteht der nächste Schritt darin, den Zeitplan zu definieren.

Definieren Sie einen Zeitplan für die Integration der Microsoft Graph-Sicherheits-API

Überprüfen Sie die Standardeinstellungen für den Warnungsabruf, oder ändern Sie die Planung nach Bedarf. Mit diesem Schritt können Sie Ihren Warnungsabruf basierend auf einem Datumsbereich filtern.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie wählen auch aus, wie oft Sie nach zukünftigen Warnungen abfragen, die der Warnungsprofilkonfiguration entsprechen. Bei Profilen zur automatisierten Warnungserfassung überprüfen und ändern Sie die Planung und den Warnungsabruf, bevor das Profil aktiviert wird. Dieser Schritt ist für geplante Warnungsprofile erforderlich.

Als Benutzer mit der Rolle sn_si.admin konfigurieren Sie diese Abfrageintervalle pro Profil. Die Leistung von Microsoft Graph-Sicherheits-API Die Integration der Warnungserfassung wird von den verschiedenen Abfrageintervallen beeinflusst. Bei der Planung ziehen Sie es möglicherweise vor, die Systemlast gegen die Dringlichkeit des Incident auszugleichen. Für jedes Profil ist ein fünf-Minuten-Standardwert festgelegt. Sie können diese Einstellung jedoch basierend auf der Dringlichkeit des Incident und der erwarteten Belastung Ihres Systems ändern.

Prozedur
1. Wenn die Seite „Zeitplanung“ im Fortschrittsbalken nicht angezeigt wird, wählen Sie aus **Zeitplanung** .
2. Wählen Sie eine aus, um zu planen, wie und wann Warnungen aus abgerufen werden Microsoft Azure Mandant.

3. Klicken Sie Auf **Fahren Sie Fort** Um zur Seite „zusätzliche Optionen“ zu navigieren.

Automatisieren Sie Warnungsaktualisierungen und -Abschlüsse basierend auf dem SIR-Incident-Status

Die Microsoft Graph-Sicherheits-API Die Integration der Warnungserfassung verfügt über eine bidirektionale Schnittstelle, mit der sowohl Warnungen Security Incidents erstellen als auch die Möglichkeit haben, die Warnungen zu aktualisieren, sobald der Security Incident erstellt und/oder mit relevanten Incident-Details geschlossen wurde, z. B. SIR Incident-Nummer, Zuweisungsgruppe, SIR Incident-URL usw. T

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Hinweis:
Der Status der anfänglichen Warnung und der Abschlusswarnung werden nur aktualisiert, wenn diese Funktionalität vom Service Provider unterstützt wird. Weitere Informationen finden Sie unter Microsoft Graph-Sicherheits-API Dokumentation und Dokumentation des Sicherheitsanbieters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn die Seite „zusätzliche Optionen“ im Fortschrittsbalken nicht angezeigt wird, wählen Sie aus **Zusätzliche Optionen** .
2. Befolgen Sie die folgenden Anweisungen, um die Konfiguration für die Aktualisierung von Warnungen abzuschließen, wenn der Security Incident erstellt wird.
3. Klicken Sie Auf **Beenden** Um die Konfiguration abzuschließen und das Profil in zu verschieben **Warten** status.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um Warnungen aus dem abzurufen Microsoft Azure Mandant basierend auf Ihrer Planung. Innerhalb von 24 Stunden können maximal 1000 Security Incidents erstellt werden.

Konfigurationseinstellungen der Microsoft Graph-Sicherheits-API-Integration

Verwenden Sie diese Option, um zu ändern Microsoft Graph-Sicherheits-API Standardsystemeigenschaften der Erfassungsintegration.

Vorbereitungen

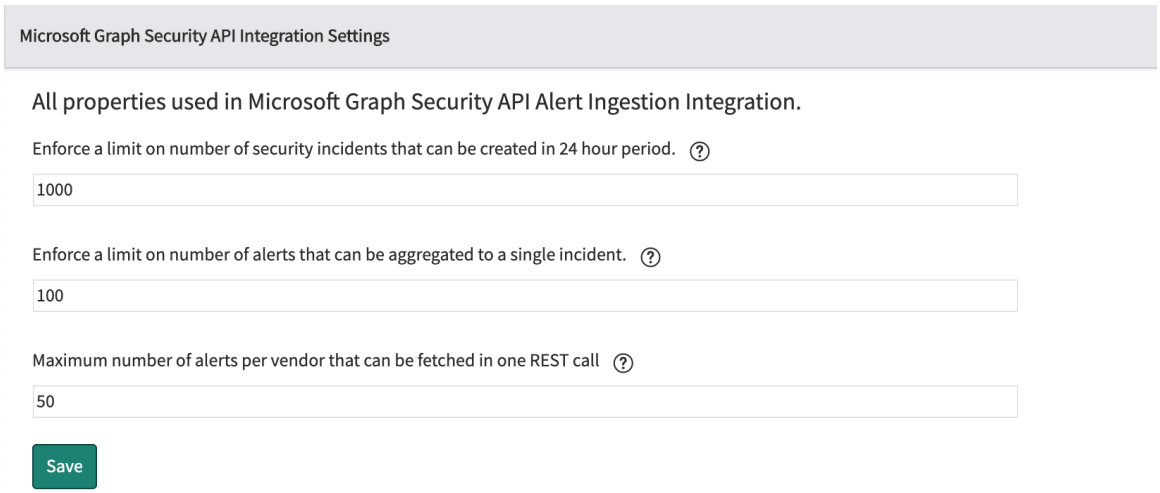
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Ändern Sie die Standardkonfigurationseigenschaften, um die Anzahl der Security Incidents zu beschränken, die innerhalb von 24 Stunden erstellt werden können, oder die Anzahl der Warnungen, die in einem Security Incident zusammengefasst werden können.

Um die Systemeigenschaften zu ändern, melden Sie sich als Anwender mit an *sn_si.admin* Rolle und navigieren Sie zu **Microsoft Graph-Sicherheits-API – Integration** > **Microsoft Graph-Sicherheits-API – Integrationseinstellungen**an.

Die Standardkonfigurationseinstellungen werden angezeigt. Sie können diese Einstellungen bei Bedarf ändern.



Alle geänderten Integrationseinstellungen werden während des nächsten Abfrageintervalls angewendet, wie im Profil definiert.

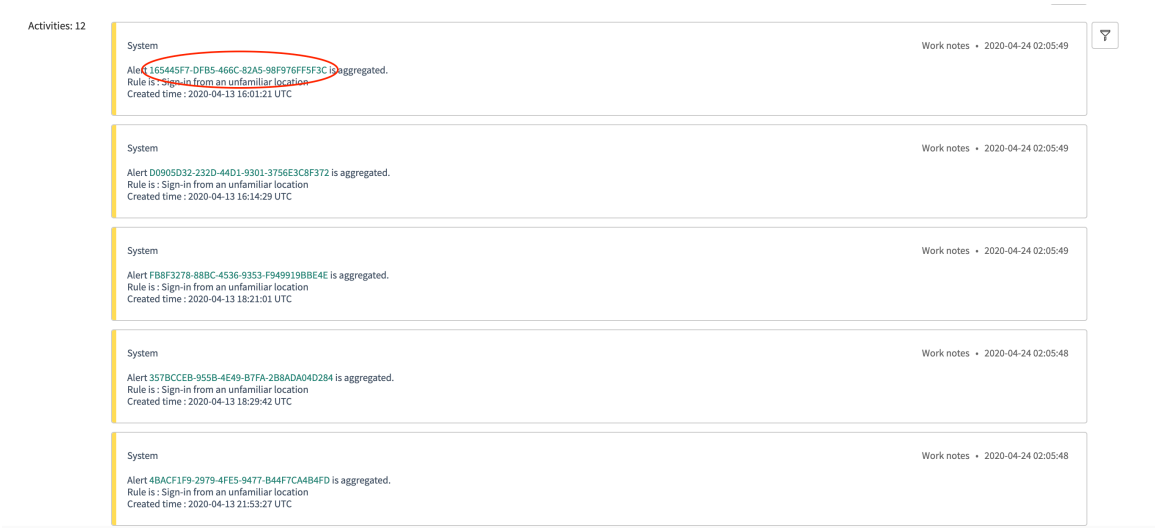
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Security Incident Response“ nach Warnungserfassung

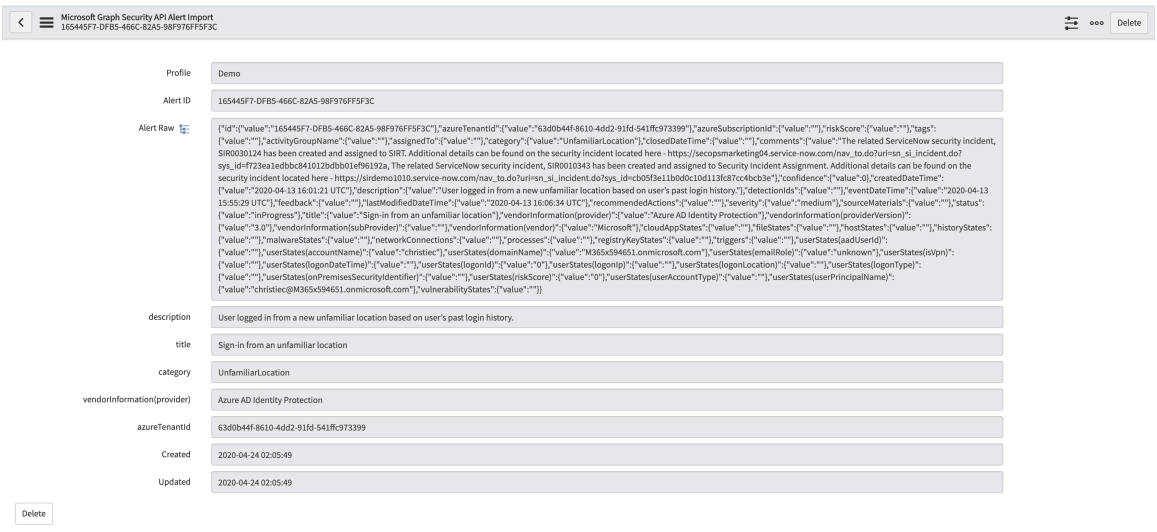
Nach einem Microsoft Graph-Sicherheits-API Warnung wurde erfasst, ein Security Incident wird erstellt, und die entsprechenden Aktualisierungen werden am Security Incident-Datensatz vorgenommen.

Arbeitsnotiz

Wenn Sie ausgewählt haben **Arbeitsnotiz für neue Warnung protokollieren** Option in den Warnungszusammenfassungskriterien wie in beschrieben Zuordnung von Warnungen zu Security Incident Response-Feldern, Eine Arbeitsnotiz wird veröffentlicht, wenn die Warnung aggregiert wird.



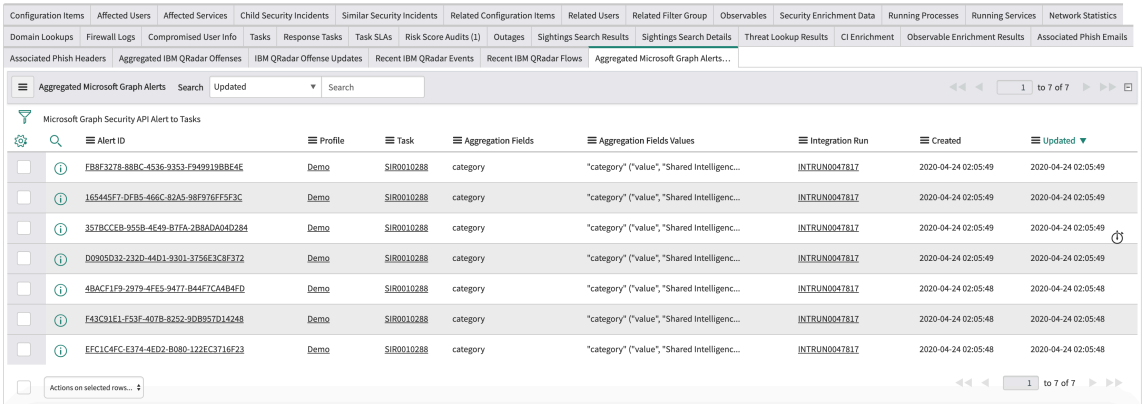
Klicken Sie auf den Warnungslink, um zum internen Warnungsimportdatensatz zu navigieren, der Rohwarnungsdaten enthält.



Aggregierte Warnungen

Klicken **Zugehörige Listen** > **Zusammengefasste Microsoft Graph-Sicherheitswarnungen** Zum Anzeigen der Warnungen, die zum Security Incident zusammengefasst sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- **Erstellen Sie einen Security Incident** : Wählen Sie eine Warnung aus der Liste aus, klicken Sie auf **Aktionen** Menü und klicken Sie auf **Erstellen Sie einen Security Incident** . Diese Option erstellt einen neuen Security Incident für die Warnung, und diese Warnung wird vom übergeordneten Security Incident deaggregiert.
- **Warnungsdatensatz löschen** : Wählen Sie eine Warnung aus der Liste aus, klicken Sie auf **Aktionen** Menü und klicken Sie auf **Löschen** . Mit dieser Option wird der Warnungsdatensatz gelöscht.

Optional: Kopieren Sie ein Microsoft Graph-Sicherheits-API-Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, sollten Sie Profile kopieren, um Zeit zu sparen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie als Anwender mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), sodass es vor Abschluss der Konfiguration nicht versehentlich aktiviert wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und verifiziert haben.

Prozedur

1. Navigieren zu **Alle** > **Microsoft Graph-Sicherheits-API – Integration** > **Microsoft Graph-Sicherheits-API-Profil**an.
2. In Microsoft Graph-Sicherheits-API Profilliste, die angezeigt wird, wählen Sie ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren** . Das Profil wird kopiert und in der Liste angezeigt. Die Kopie verfügt über alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (Wahr), die Kopie ist zu diesem Zeitpunkt deaktiviert (Falsch). Möglicherweise möchten Sie Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf auf das neue Profil angewendet werden.

   Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass **Aktiv** Der Spaltenstatus wird auf „falsch“ festgelegt, da das Profil aktiviert werden muss.

Nächste Maßnahme

Sie werden aufgefordert, das neue Profil zu aktivieren (zu aktivieren), nachdem Sie die Konfigurationsschritte abgeschlossen haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänentrennung und Microsoft Graph-Sicherheits-API Warnungserfassung

Domänentrennung wird für diese Anwendung unterstützt. Die Microsoft Graph-Sicherheits-API Die Integration erfasst Warnungen von Microsoft Graph-Sicherheitsanbietern und erstellt automatisch Security Incidents. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

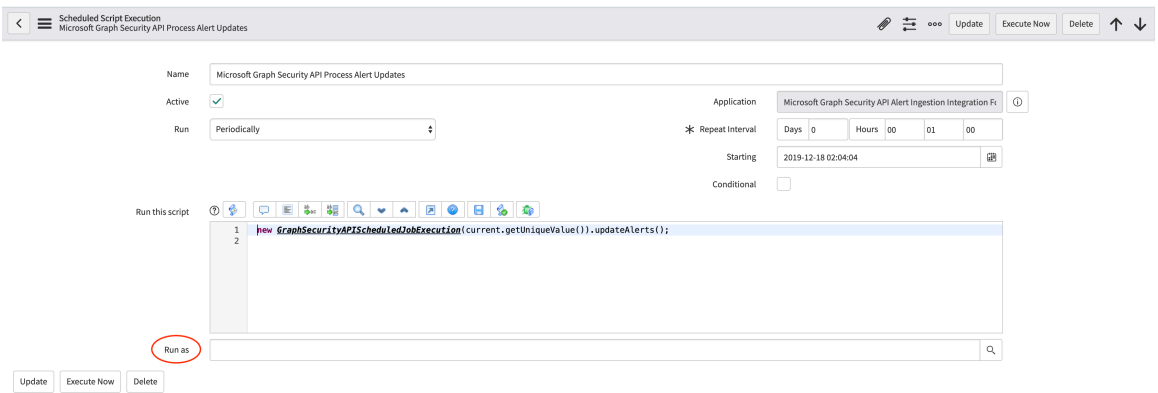
- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

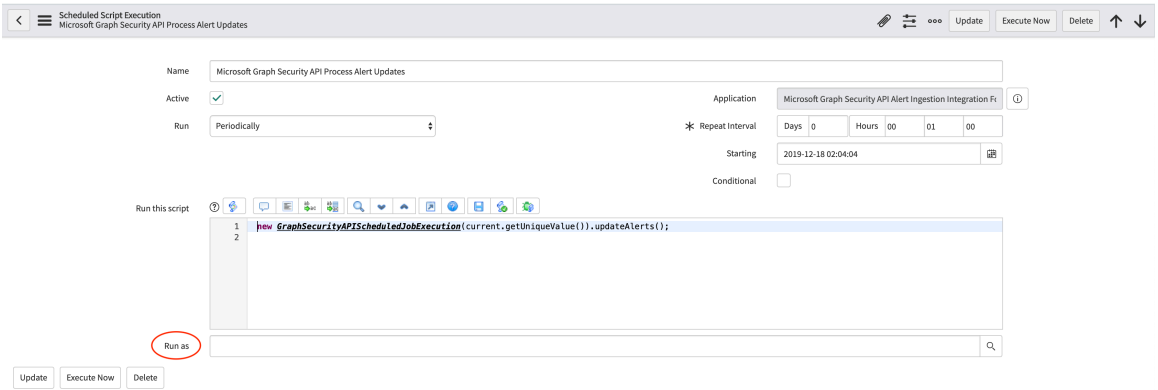
Funktionsweise der Domänentrennung in Microsoft Graph-Sicherheits-API

Um die Domänentrennung zu erreichen, replizieren Sie Microsoft Graph-Sicherheits-API Profilprozess und SIR Prozesswarnung aktualisiert geplante Aufgaben und ändert **Ausführen als** Anwender. Standardmäßig führen die Systemanwender diese geplanten Aufgaben aus. Ändern Sie **Ausführen als** An einen Anwender mit der Rolle „sn_si.admin“ in der jeweiligen Domäne, und führen Sie die geplante Aufgabe aus.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zugehörige Informationen

Domänentrennung für Service Provider

Nutzung von Flow Designer und Integration Hub in der Microsoft Graph-Sicherheits-API-Integration

Mit der Flow Designer- und Integration Hub-Funktionalität wurden mehrere Subflows und Aktionen als Teil von erstellt Microsoft Graph-Sicherheits-API Integration.

Die folgenden Subflows sind verfügbar:

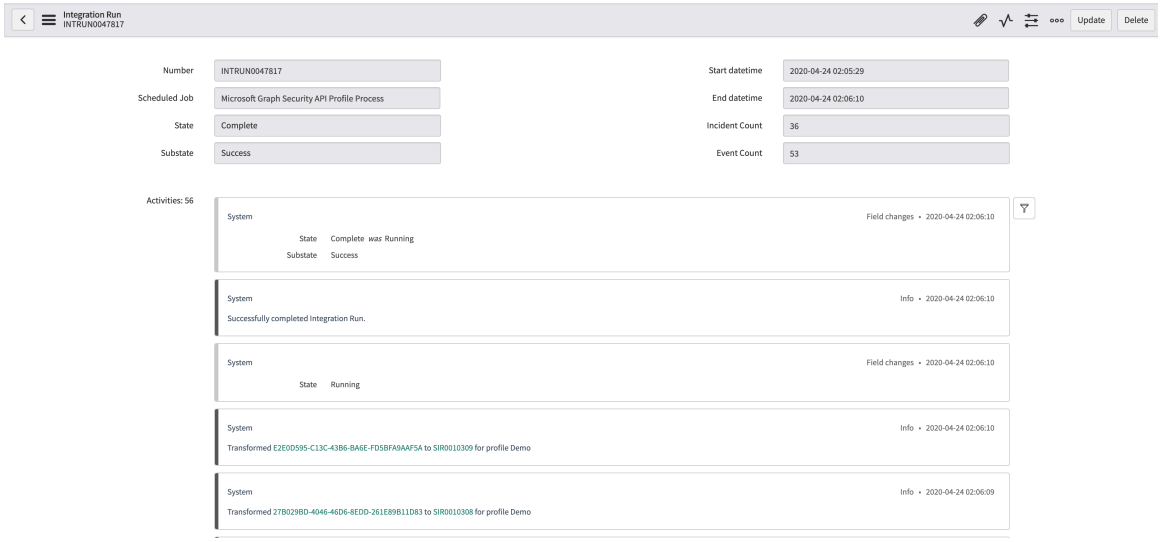
- Microsoft Graph-Sicherheits-API Konfigurationsvalidierung: Wird in der Konfigurationskachel verwendet, um die Anmeldeinformationen beim ersten Setup zu validieren.
- REST-Aufruf für Microsoft Graph-Sicherheits-API: Wird für alle Interaktionen mit der Microsoft Graph-Sicherheits-API mithilfe von REST-Aufrufen verwendet.
- Beispielwarnungen abrufen: Dies wird im Abschnitt „Zuordnung“ des Profil-Setups verwendet, um Beispieldaten abzurufen. Dieser Subflow wird asynchron ausgelöst.

Problembehandlung bei der Integration der Microsoft Graph-Sicherheits-API

In diesem Abschnitt werden wichtige Tipps zur Fehlerbehebung und häufig gestellte Fragen im Zusammenhang mit behandelt Microsoft Graph-Sicherheits-API Integration der Warnungserfassung.

- **Integrationsausführung** : Wenn die Ausführung einer geplanten Aufgabe beginnt, wird ein Datensatz der Integrationsausführung mit Protokollen, Fehlern und Warnungen angezeigt. Die Anzahl der abgerufenen Warnungen und die Anzahl der Incidents, die in einer geplanten Aufgabenausführung erstellt wurden, werden ebenfalls angezeigt. Anwender mit sn_si.Analyst Die Rolle kann erkennen, ob das Abrufen von Fehlern/ Profilen während der Integrationsausführung fehlgeschlagen ist. Anwender mit sn_si.Analyst Die Rolle kann überprüfen sn_event_ingestion_Integration_Run Tabelle für alle aufgetretenen Fehler. Um Integrationsprobleme zu beheben, müssen Sie zuerst die Integrationsausführung überprüfen. Fehler werden als Arbeitsnotizen in den Datensätzen der Integrationsausführung für jede geplante Aufgabenausführung protokolliert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- **Unvollständiges Profil** : Beim Konfigurieren des Profils in den zusätzlichen Optionen (Automatisieren Sie Warnungsaktualisierungen und -Abschlüsse basierend auf dem SIR-Incident-Status) Abschnitt müssen Sie auf klicken **Beenden** Schaltfläche, um sicherzustellen, dass das Profil in den Status „Warten“ verschoben wird, um anzuzeigen, dass es auf die Erfassung wartet.
- **Validieren Sie das Profil** : Um zu validieren, ob die Integration ordnungsgemäß funktioniert, überprüfen Sie die profilstatus, das Datum des letzten Abrufs des Profils, die Warnungsimporttabelle und die Warnung an die Datensätze der Aufgabentabelle.
- **SSL-Probleme** : Bei Verbindung über Microsoft Graph-Sicherheits-API Stellen Sie sicher, dass die Instanz über ein gültiges CA-Zertifikat verfügt, das noch nicht abgelaufen ist. Sie können RSA- oder eigene Zertifikate in die Plattform importieren und sicherstellen, dass der allgemeine Name des Zertifikats mit dem Hostnamen übereinstimmt. Siehe KB0778285 Für Details.

Palo Alto Networks – AutoFocus-Integration

Die Palo Alto Networks – AutoFocus Das Integrationsbasissystem enthält einen Workflow und eine Reihe von Workflow-Aktivitäten, die Sie für die Integration verwenden können Palo Alto Networks – AutoFocus Mit Ihrer Instanz.

Erkunden

Security Incident Response-Integrationen

Einrichten

Aktivieren und konfigurieren Palo Alto Networks – AutoFocus Integration

---

Verwenden

- Security Operations Palo Alto Networks – Wert-Workflow überprüfen und blockieren
- Abrufen des Autofokus-Sitzungsinformationsanreicherungs-Flows

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

- Entwicklerdokumentation
- Suchen Sie Komponenten, die mit einer Anwendung installiert sind

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Aktivieren und konfigurieren Palo Alto Networks – AutoFocus Integration

Mit der Integrationskonfigurationsfunktion können Sie Sicherheitsintegrationen von Drittparteien schnell aktivieren und einrichten, einschließlich Palo Alto Networks – AutoFocus. Bevor Sie verwenden können Palo Alto Networks – AutoFocus, Sie müssen es aus herunterladen ServiceNow Store.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie eine Anwendung aus dem herunter ServiceNow Store Zum ersten Mal.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf die Support-Website von Palo Alto Networks zu, und erhalten Sie den API-Schlüssel.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationskonfiguration**an.
4. Klicken Sie auf der Karte „Palo Alto Networks-Autofokus“ auf **Konfigurieren** .
5. Geben Sie ein (oder fügen Sie ein) **API-Schlüssel** Sie haben von der Palo Alto Networks-Support-Website erworben.
6. Klicken Sie auf **Absenden**.

Abrufen des Autofokus-Sitzungsinformationsanreicherungs-Flows

Wenn **Security Operations Palo Alto Networks: Ergänzung der Autofokus-Sitzungsinformationen abrufen** Flow wird ausgeführt. Er stellt eine Suchabfrage mit Autofokus in die Warteschlange, um Informationen zu einer angegebenen Quell-IP zu sammeln. Wenn der Autofokus über vorherige Sitzungen verfügt, die von dieser IP-Adresse stammen, wird ein JSON-formatierter Bericht zurückgegeben.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

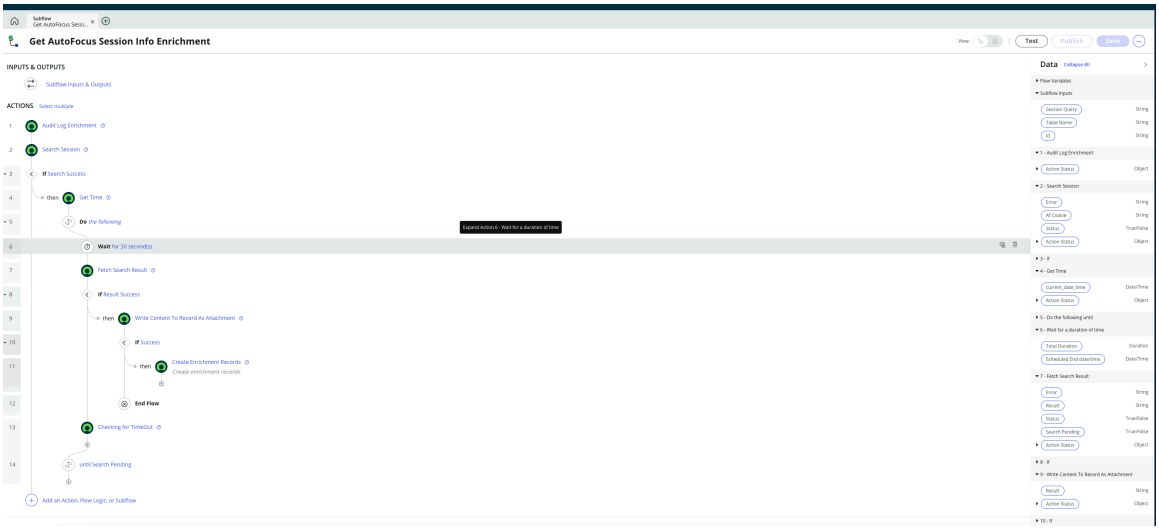
Warum und wann dieser Vorgang ausgeführt wird

Die **Security Operations Palo Alto Networks: Ergänzung der Autofokus-Sitzungsinformationen abrufen** Flow wird ausgeführt, wenn **Quell-IP** Das Feld in einem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident wird geändert, und der Datensatz wird aktualisiert. Der Flow ruft die IP-Adresse ab und sendet eine Abfrageanforderung an den Autofokus. Wenn der Autofokus zuvor Sitzungen identifiziert hat, die von der IP-Adresse stammen, wird ein JSON-formatierter Bericht zurückgegeben.

Security Operations Palo Alto Networks – Flow Zur Datenanreicherung Von Wildfire Abrufen



Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**an.
2. Klicken Sie auf **Kompromittierungsindikatoren** Registerkarte und füllen Sie aus **Quell-IP** Feld.
3. Klicken Sie auf **Aktualisieren**.
   Der Autofokus scannt die Informationen aus der IP-Adresse, und eine Textdatei im JSON-Format wird an den Security Incident angehängt.

   Aktionen, die für diese Integration spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Aktion für Autofokus-Suchsitzung

Die **Autofokus-Suchsitzung** Die Flow-Aktion lädt Informationen aus einer IP-Adresse hoch, die einem Security Incident zugewiesen ist, um den Autofokus zu aktivieren, und stellt sie für eine Suchabfrage in die Warteschlange.

Eingabevariablen

Hinweis:

Wenn die Aktion ausgeführt wird, wird eine Suchabfrage mit Autofokus in die Warteschlange gestellt, um Informationen für eine angegebene Quell-IP zu sammeln. Wenn der Autofokus zuvor Sitzungen identifiziert hat, die von dieser IP-Adresse stammen, wird ein JSON-formatierter Bericht zurückgegeben.

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Variable	Beschreibung
SearchSessionQuery [Zeichenfolge]	Die Suchabfrage für Sitzungsinformationen.

Aktion „Suchergebnisse“ abrufen

Die **Suchergebnisse Abrufen** Flow-Aktion ruft Suchergebnisse ab, die durch ein Cookie identifiziert wurden, an die von initiierte Suchabfrage **Autofokus-Suchsitzung** Aktion.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Eingabevariablen

Variable	Beschreibung
Afcookie [Zeichenfolge]	Das Autofokus-Cookie für die von generierte Suchanforderung Aktion für Autofokus-Suchsitzung.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
SearchAusstehend [Boolesch]	„Wahr“, wenn die Suchanforderung im Autofokus noch verarbeitet wird.
Ergebnis [Zeichenfolge]	Die Suchergebnisdaten.
Status [boolescher Wert]	„Wahr“, wenn die Suche abgeschlossen ist und Ergebnisse erfolgreich generiert wurden.
Fehler [Zeichenfolge]	Der Fehler, falls vorhanden, der in der Aktion aufgetreten ist.

Palo Alto Networks – Firewall-Integration

Durchzuführen Palo Alto Networks – Firewall Integration: Stellen Sie sicher, dass Sie über eine verfügen MID-Server Richten Sie mit SSH-Anmeldeinformationen ein. Wenn noch keine Firewall eingerichtet ist, fügen Sie eine hinzu.

Erkunden

Security Incident Response-Integrationen

Einrichten

- Aktivieren und konfigurieren Sie die Palo Alto Networks-Firewall-Integration
- Richten Sie SSH-Anmeldeinformationen für den MID-Server ein

---

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Verwenden	Entwickeln
Palo Alto Networks Firewall-Startprogramm-Workflow	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie Komponenten, die mit einer Anwendung installiert sind

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Richten Sie SSH-Anmeldeinformationen für den MID-Server ein

Die Palo Alto Networks-Firewall sendet API-Aufrufe an den MID-Server. Stellen Sie daher sicher, dass SSH-Anmeldeinformationen für den MID-Server erstellt wurden.

Vorbereitungen

- Das Orchestration-Plugin muss aktiviert sein.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Orchestration** > **Anmeldeinformationen und Verbindungen** > **Anmeldeinformationen**an.
2. Klicken Sie auf **Neu**.
3. Klicken Sie im Interceptor-Bildschirm auf **SSH-Anmeldeinformationen** .
4. Füllen Sie die Felder nach Bedarf aus.

SSH-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen Namen für die Anmeldeinformationen ein.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diese Anmeldeinformationen zu aktivieren.
Betrifft	Wählen Sie Aus **Alle MID-Server** Oder **Bestimmte MID-Server** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID-Server	Wenn Sie ausgewählt haben **Bestimmte MID-Server** Klicken Sie auf das Sperrsymbol, und wählen Sie die MID-Server aus, auf die Sie diese Anmeldeinformationen anwenden möchten.
Reihenfolge	Wählen Sie die Reihenfolge aus, in der die Anmeldeinformationen vom Server versucht werden. Kleinere Zahlen werden zuerst versucht.
Anwendername	Geben Sie den Anwendernamen des Anwenders ein, der diesen Anmeldeinformationen zugeordnet ist, falls vorhanden.
Passwort	Wenn Sie einen eingegeben haben **Anwendername** , Geben Sie das Passwort des Anwenders ein.
Tag	Geben Sie ein Tag ein, das für Suchkriterien verwendet werden soll. Die **Tag** Das Feld muss denselben Wert wie das enthalten **Name** .

Aktivieren und konfigurieren Sie die Palo Alto Networks-Firewall-Integration

Mit der Integrationskonfigurationsfunktion können Sie Sicherheitsintegrationen von Drittparteien schnell aktivieren und einrichten, einschließlich Palo Alto Networks – Firewall. Bevor Sie verwenden können Palo Alto Networks – Firewall, Sie müssen es aus herunterladen ServiceNow Store.

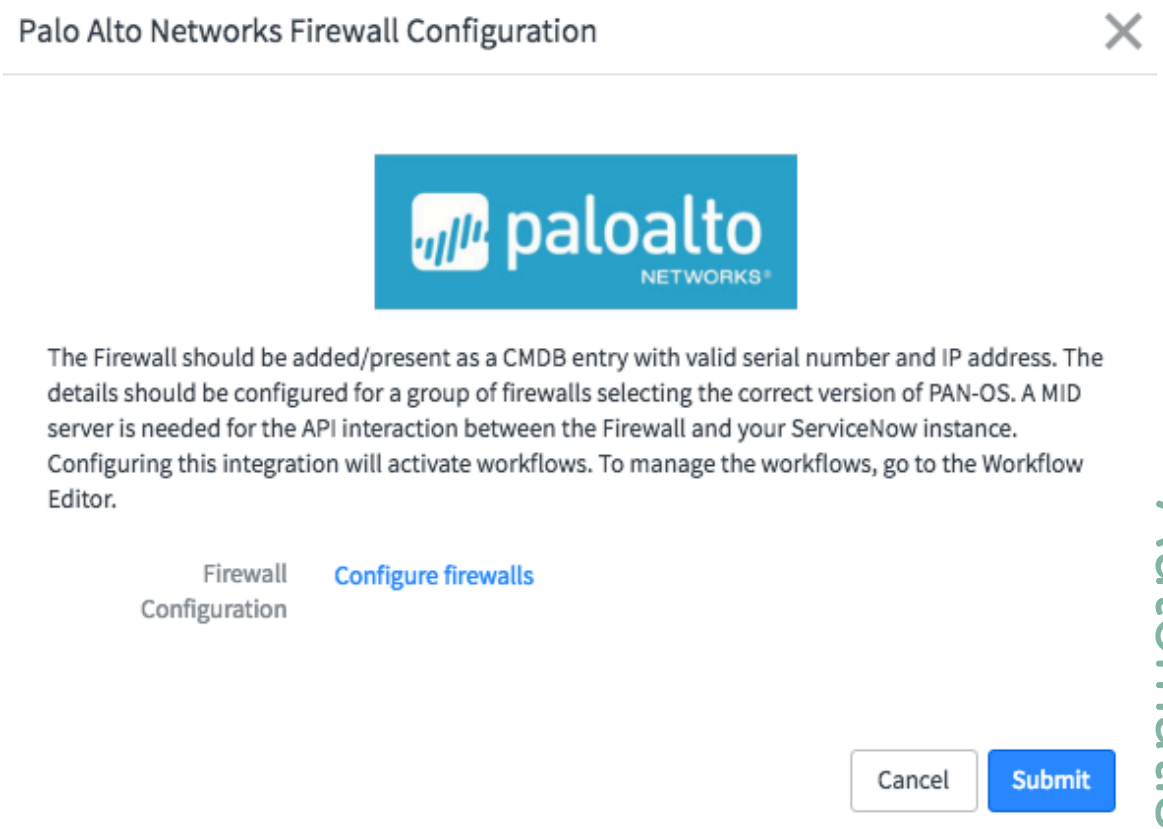
Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Bevor Sie die Integration aktivieren und konfigurieren, greifen Sie auf das Dashboard „Palo Alto Networks Firewall“ zu.
   Beachten Sie die Namen der dynamischen IP-Liste, der dynamischen URL-Liste oder der dynamischen Domänenliste, die Sie für die Firewall-Blockierung verwenden.
2. Laden Sie die Integration aus dem herunter ServiceNow Storean.
3. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationskonfiguration**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. Klicken Sie auf der Karte Palo Alto Networks Firewall auf **Konfigurieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie Auf **Konfigurieren Sie Firewalls** .
6. Klicken Sie im Bildschirm Firewall-Konfigurationen auf **Neu** .
7. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Firewalls	Klicken Sie auf das Schlosssymbol, und wählen Sie die zu konfigurierende Firewall aus.
Firewall-Version	Wählen Sie die Firewall-Version von Palo Alto Networks aus.**PAN-OS-7,1** Ist die empfohlene Version. Die Auswahl früherer Versionen kann inkonsistente Ergebnisse zurückgeben.
Anwendername	Geben Sie den Anwendernamen ein, der bei der Verbindung mit der Firewall über REST-Endpunkte verwendet werden soll.
Passwort	Geben Sie das Passwort für den verbindenden Anwender ein.
Dynamische IP-Liste	Geben Sie den Namen der externen dynamischen Liste oder der dynamischen Blockliste ein, die Sie für IP-Adressen verwenden.
Dynamische URL-Liste	Geben Sie den Namen der externen dynamischen Liste oder der dynamischen Blockliste ein, die Sie für URLs verwenden.
Dynamische Liste Der Domänen	Geben Sie den Namen der externen dynamischen Liste oder der dynamischen Blockliste ein, die Sie für Domänen verwenden.

8. Klicken Sie auf **Absenden**.

Automatische Übersetzung

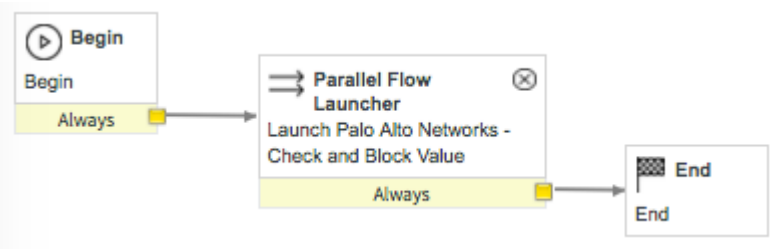
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Palo Alto Networks Firewall-Startprogramm-Workflow

Security Operations-Integration Palo Alto Networks Firewall-Startprogramm Workflow ist die von gestartete Palo Alto Networks-Firewall-Implementierung **Integration Von Security Operations – Anforderung Blockieren** Fähigkeits-Workflow.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Workflow-Prozessaktivitäten umfassen: Security Operations Palo Alto Networks – Wert-Workflow überprüfen und blockieren.



Security Operations Palo Alto Networks – Wert-Workflow überprüfen und blockieren

Da Security Incidents erstellt und selektiert werden, um potenzielle Bedrohungen zu identifizieren, können Sie verwenden **Security Operations Palo Alto Networks: Wert überprüfen und blockieren** Workflow zum automatischen Überprüfen und Aktualisieren von IP-Adressen, URLs und Domänen mithilfe externer dynamischer Listen, die in definiert sind Palo Alto Networks – Firewall.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

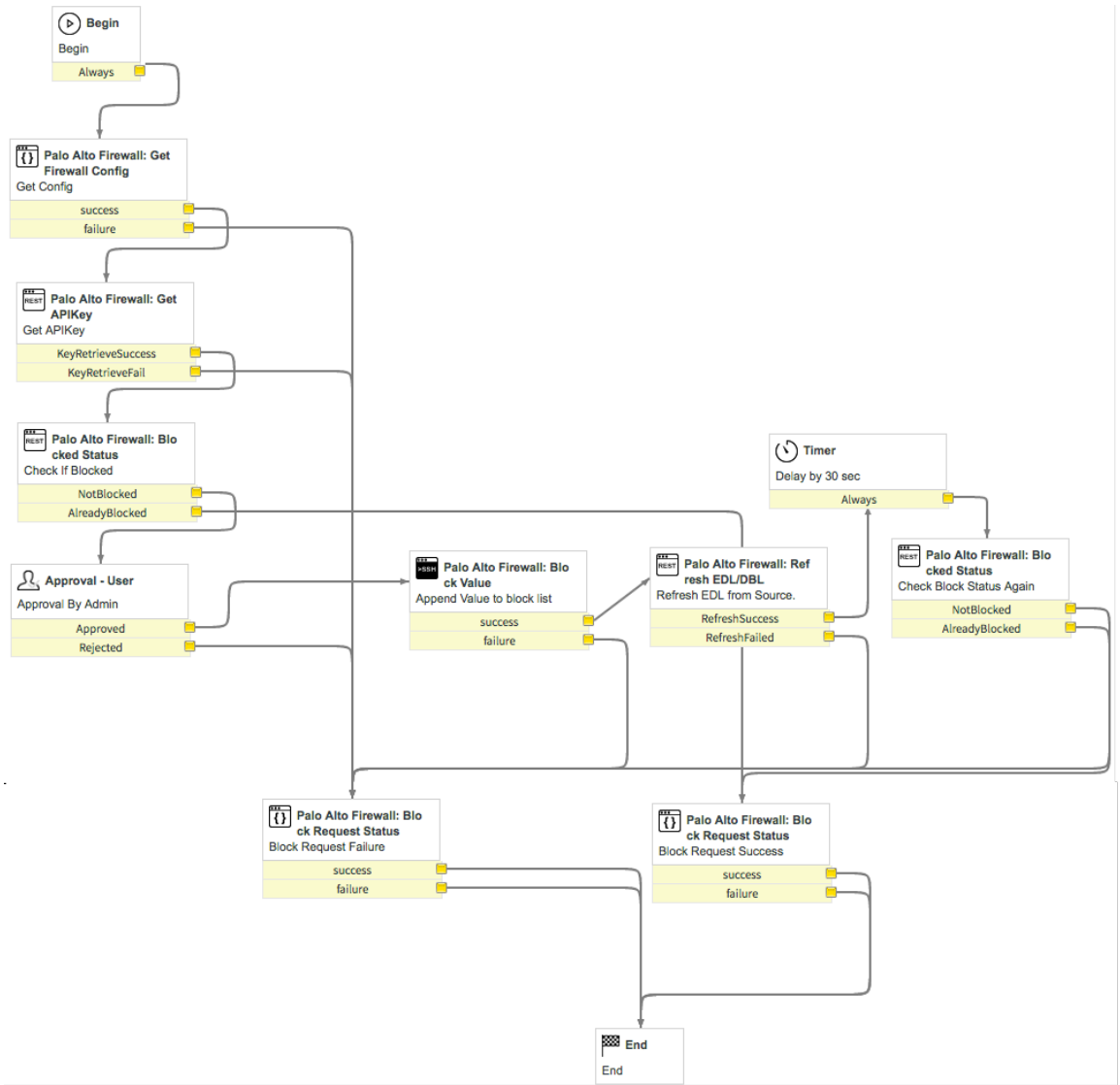
Warum und wann dieser Vorgang ausgeführt wird
Die **Security Operations Palo Alto Networks: Wert überprüfen und blockieren** Workflow wird ausgeführt, wenn Firewall-Blockanforderungen übermittelt werden. Die Blockanforderung gibt die zu verwendende Firewall, den Typ des zu überprüfenden und zu blockierenden erkennbaren Elements (falls erforderlich) und den Blockwert an. Das ist die IP-Adresse, URL oder Domäne in Frage.

Während der Workflow-Ausführung werden Befehle unter definiert **Integration mit Palo Alto Networks** > **Firewall** > **Befehle** Werden ausgeführt. Die Befehle „Typ anzeigen“ (z. B. „Show-IP-ExternalDynamicList“) bestimmen, ob der Wert in der Firewall vorhanden ist. Die Aktualisierungstyp-Befehle (z. B. Refresh-IP-ExternalDynamicList) fügen der Blockliste Werte hinzu, die in der Firewall nicht vorhanden sind.

Nach Sperrstatus Aktivität wird ausgeführt. Die Genehmigung durch einen Systemadministrator ist erforderlich, bevor der Workflow fortgesetzt werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations Palo Alto Networks – Wert-Workflow überprüfen und blockieren



Prozedur

1. Navigieren zu **Integration mit Palo Alto Networks** > **Firewall** > **Anforderungen Blockieren**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Firewall	Wählen Sie die zu verwendende Firewall aus.
Blocktyp	Wählen Sie den Typ des zu prüfenden Werts aus: ○ IP ○ URL ○ DOMAIN

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Blockwert	Geben Sie den Wert des ausgewählten Typs ein, der in der Firewall überprüft werden soll.

4. Klicken Sie auf **Absenden**.

Palo Alto-Firewall: Aktivität „Anforderungsstatus blockieren“

Diese Aktivität wird von anderen Aktivitäten aufgerufen, um den Status der Firewall-Blockanforderung auf Erfolg oder Fehler festzulegen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
FirewallBlockRequestSysid [Zeichenfolge]	Die System-ID der Firewall-Blockanforderung. Diese Eingabevariable ist obligatorisch.
Status [Zeichenfolge]	Gibt an, ob der Aktualisierungsauftrag ausgeführt wurde: Erfolg oder Fehler.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
Ergebnis [Zeichenfolge]	Gibt an, ob der Aktualisierungsauftrag erfolgreich oder fehlgeschlagen ist.

Palo Alto-Firewall: Blockwertaktivität

Nachdem der Workflow einen Wert identifiziert hat, der sich nicht in der Firewall befindet, wird der Datensatz zur Genehmigung weitergeleitet. Nach der Genehmigung stellt diese Aktivität über Ihre SSH-Anmeldeinformationen eine Verbindung zum MID-Server her und ruft ein Skript auf, das den Wert der Liste der externen Firewall-Blockierungen hinzufügt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Hinweis:
Sie müssen die Eingabevariablen für diese Aktivität und dann manuell eingeben Veröffentlichen Sie den Workflow . Wenn der Workflow nicht veröffentlicht wird, werden die Eingabevariablen für nicht-Administratoranwender nicht gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Variable	Beschreibung
ToBeBlockedValue [Zeichenfolge]	Der Wert, der der EDL hinzugefügt werden soll, falls nicht bereits vorhanden. Diese Eingabevariable ist obligatorisch.
TypeToBeBlocked [Zeichenfolge]	Der Typ des zu blockierenden Werts: IP, URL oder Domäne. Diese Eingabevariable ist obligatorisch.
ZielHost [Zeichenfolge]	Der MID-Server, auf dem das Skript ausgeführt wird.
SSHCredentialTag [Zeichenfolge]	Die Auf dem MID-Server definiertes SSH-Anmeldeinformations-Tag .
ScriptCommand [Zeichenfolge]	Das Skript AppendValueToList.sh, das zum Hinzufügen des Werts zur EDL verwendet wird. Erfordert den vollständigen Pfad zum MID-Server.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ergebnis [Zeichenfolge]	Das Ergebnis wurde an die EDL übergeben.

Palo Alto-Firewall: Aktivität „blockierter Status“

Diese Aktivität überprüft, ob der Wert (IP, URL oder Domäne) in der entsprechenden externen dynamischen Liste/dynamischen Blockliste (EDL/DBL) in der Firewall enthalten ist. Die EDL-/DBL-Details werden mithilfe eines Betriebsbefehls von der Firewall abgerufen, und es wird eine Routine durchgeführt, um zu überprüfen, ob der Wert in der Firewall blockiert ist.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität. Alle aufgelisteten Eingabevariableneinträge sind obligatorisch.

Eingabevariablen

Variable	Beschreibung
Wertbis geprüft [Zeichenfolge]	Der Wert in der Blockanforderung.
ShowEDLDetailsCommand [Zeichenfolge]	Der Befehl „externe dynamische Liste“, der verwendet wird, um zu bestimmen, ob der Wert in der Firewall vorhanden ist.
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der verwendeten Firewall.
FirewallApiKey [Zeichenfolge]	Der Firewall-API-Schlüssel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie Daten, die dynamisch mithilfe der Palo Alto Firewall Operational Command API-Nachricht generiert werden.

Ausgabevariablen

Variable	Beschreibung
CommandResult [Zeichenfolge]	Die Ergebnisse aus der Firewall für den Befehl „EDL-Details anzeigen“.
BlockedStatus [Boolesch]	„Wahr“ gibt „blockiert“ an. „Falsch“ bedeutet, dass sie nicht blockiert ist.
CommandResponse [Zeichenfolge]	Der Antwortstatus, der von der Firewall für den Befehl „EDL-Details anzeigen“ abgerufen wurde.

Palo Alto-Firewall: API-Schlüsselaktion abrufen

Mit dieser Aktion wird der API-Schlüssel aus der Firewall abgerufen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion. Alle aufgelisteten Eingabevariableneinträge sind obligatorisch.

Eingabevariablen

Variable	Beschreibung
Anwendername [Zeichenfolge]	Der Anwendername des Firewall-Administrators.
Passwort [Zeichenfolge]	Das Passwort des Firewall-Administrators.
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der Firewall.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
ApiKey [Zeichenfolge]	Der Firewall-API-Schlüssel.

Palo Alto Firewall: Firewall-Konfigurationsaktion Abrufen

Die **Palo Alto Firewall: Firewall-Konfiguration Abrufen** Die Flow-Aktion ruft alle zugehörigen Firewall-Konfigurationsinformationen aus der Datenbank ab und stellt sie zur Verwendung durch die nachfolgende Aktion bereit.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Variable	Beschreibung
Firewall-Sysid [Zeichenfolge]	Die System-ID der Firewall. Diese Eingabevariable ist obligatorisch.
TypeOfValueToBeBlocked [Zeichenfolge]	Der Typ des Werts, der in der Firewall blockiert werden soll: IP, URL oder Domäne.
FirewallIPAddress [Zeichenfolge]	Die IP-Adresse der Firewall.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
IpEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für IP-Adressen.
UrlEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für URLs.
DomainEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für Domänen.
FirewallVersionSysId [Zeichenfolge]	Die System-ID für die Firewall-Version.
Refresh EDLCommand [Zeichenfolge]	Der Befehl, der zum Aktualisieren der EDL aus der Quelle verwendet werden soll.
ShowEDLDetailsCommand [Zeichenfolge]	Der Befehl, der zum Abrufen der EDL-Details verwendet werden soll.
Status [boolescher Wert]	„Wahr“ gibt den Erfolg an. „Falsch“ gibt einen Fehler an.
Fehler [Zeichenfolge]	Der Fehler, falls vorhanden, der in der Aktion aufgetreten ist.
Endpunkt [verschlüsselt]	Der verschlüsselte Endpunkt aus der Datenbank.

Palo Alto-Firewall: EDL-/DBL-Aktivität aktualisieren

Diese Aktivität führt einen Betriebsbefehl für die Firewall aus, um die externe dynamische Liste aus der in der Firewall konfigurierten Quelle zu aktualisieren. Die Ausgabe dieser Aktivität gibt an, ob der Aktualisierungsauftrag in die Warteschlange gestellt wurde.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität. Alle aufgelisteten Eingabevariableneinträge sind obligatorisch.

Eingabevariablen

Variable	Beschreibung
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der Firewall, die aktualisiert wird.
FirewallApiKey [Zeichenfolge]	Der aktualisierte Firewall-API-Schlüssel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen (Fortsetzung)

Variable	Beschreibung
FirewallCommand [Zeichenfolge]	Der Betriebsbefehl, der ausgeführt werden soll, um den Aktualisierungsauftrag in die Warteschlange zu stellen.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
Aktivität.Ausgabe.Ergebnis [Zeichenfolge]	Eine Textzeichenfolge, die angibt, ob der Aktualisierungsauftrag zur Ausführung in die Warteschlange gestellt wurde: Erfolg oder Fehler.

Protokolldaten-Flow Abrufen

Wenn Security Incident Response, Threat Intelligence, Und Palo Alto Networks – Firewall Sind aktiviert, die **Security Operations Palo Alto Networks – Protokolldaten Abrufen** Der Flow wird automatisch ausgeführt, wenn die Quell-IP für erkennbare Elemente in einem Security Incident geändert wird.

Vorbereitungen

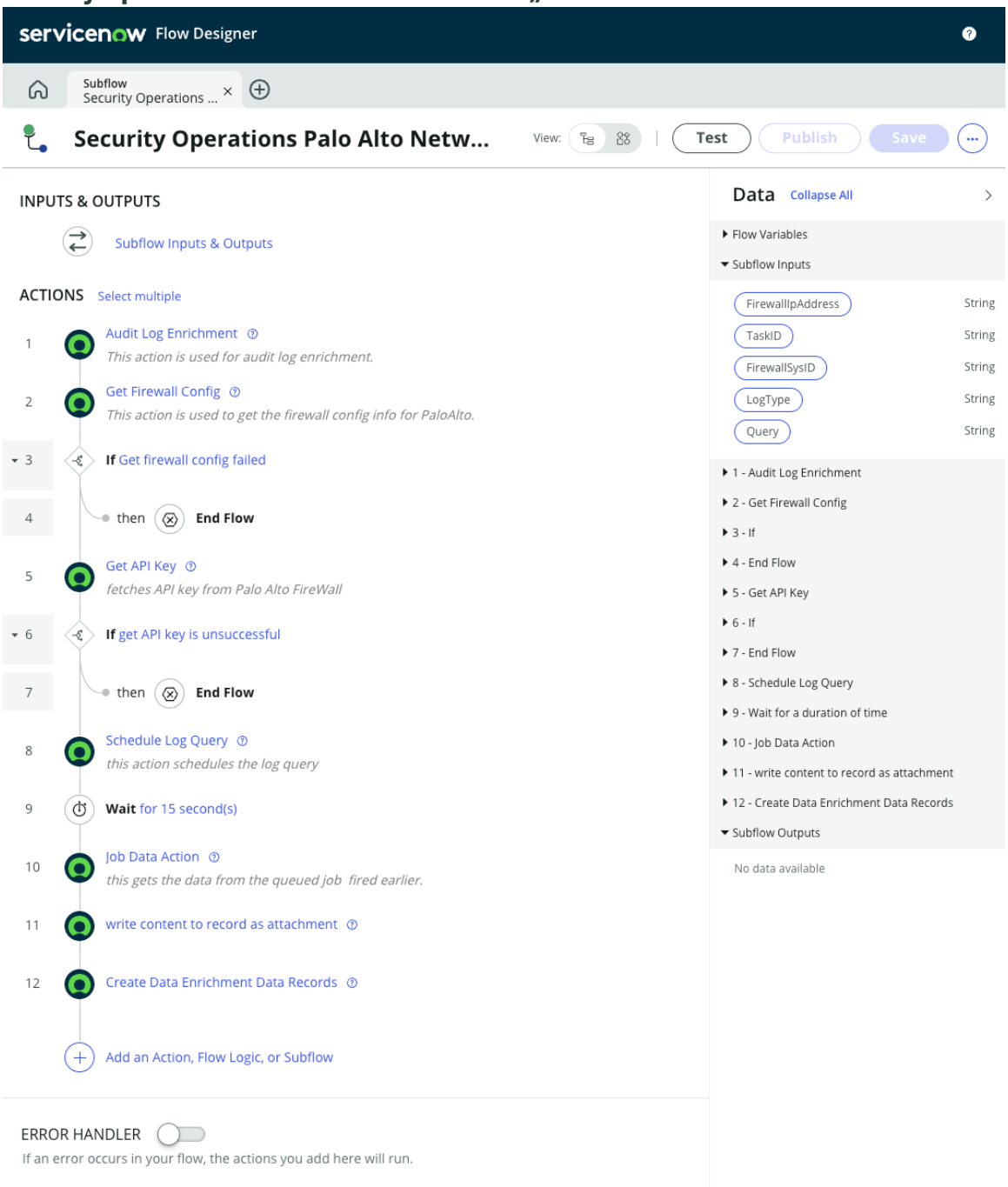
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Während der Flow-Ausführung werden Firewall-Konfigurationsinformationen aus der Datenbank abgerufen, und der API-Schlüssel wird aus der Firewall abgerufen. Mit der Aktion „Protokoll abrufen“ wird eine Suchabfrage in der Firewall in die Warteschlange gestellt. Wenn die Abfrage ausgeführt wird, wird eine Auftrags-ID zurückgegeben, die zum Abrufen von Bedrohungsprotokolldaten von der Firewall verwendet wird. Die Protokolldaten werden als XML-Datei an den Security Incident angehängt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations Palo Alto Networks – Flow „Protokolldaten abrufen“



Automatische Übersetzung

Prozedur

1. Navigieren Sie zu einem Security Incident, der erkennbare Elemente enthält.
2. Klicken Sie auf **Erkennbare Security Incident-Elemente** Registerkarte.
3. In **Quell-IP** , Fügen Sie die IP-Adresse hinzu, oder ändern Sie sie.
4. Klicken Sie auf **Aktualisieren**.
   Die **Security Operations Palo Alto Networks – Protokolldaten Abrufen** Flow wird ausgeführt, und angereicherte Bedrohungsprotokolldaten werden an den Security Incident angehängt. Die Informationen werden auch analysiert und in angezeigt **Firewall-Protokolle** Abschnitt unter **Ergänzungsdaten** Registerkarte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Palo Alto-Firewall: API-Schlüsselaktion abrufen

Mit dieser Aktion wird der API-Schlüssel aus der Firewall abgerufen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion. Alle aufgelisteten Eingabevariableneinträge sind obligatorisch.

Eingabevariablen

Variable	Beschreibung
Anwendername [Zeichenfolge]	Der Anwendername des Firewall-Administrators.
Passwort [Zeichenfolge]	Das Passwort des Firewall-Administrators.
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der Firewall.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
ApiKey [Zeichenfolge]	Der Firewall-API-Schlüssel.

Palo Alto Firewall: Firewall-Konfigurationsaktion Abrufen

Die **Palo Alto Firewall: Firewall-Konfiguration Abrufen** Die Flow-Aktion ruft alle zugehörigen Firewall-Konfigurationsinformationen aus der Datenbank ab und stellt sie zur Verwendung durch die nachfolgende Aktion bereit.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Eingabevariablen

Variable	Beschreibung
Firewall-Sysid [Zeichenfolge]	Die System-ID der Firewall. Diese Eingabevariable ist obligatorisch.
TypeOfValueToBeBlocked [Zeichenfolge]	Der Typ des Werts, der in der Firewall blockiert werden soll: IP, URL oder Domäne.
FirewallIPAddress [Zeichenfolge]	Die IP-Adresse der Firewall.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Variable	Beschreibung
IpEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für IP-Adressen.
UrlEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für URLs.
DomainEDLName [Zeichenfolge]	Der Name der externen dynamischen Liste für Domänen.
FirewallVersionSysId [Zeichenfolge]	Die System-ID für die Firewall-Version.
Refresh EDLCommand [Zeichenfolge]	Der Befehl, der zum Aktualisieren der EDL aus der Quelle verwendet werden soll.
ShowEDLDetailsCommand [Zeichenfolge]	Der Befehl, der zum Abrufen der EDL-Details verwendet werden soll.
Status [boolescher Wert]	„Wahr“ gibt den Erfolg an. „Falsch“ gibt einen Fehler an.
Fehler [Zeichenfolge]	Der Fehler, falls vorhanden, der in der Aktion aufgetreten ist.
Endpunkt [verschlüsselt]	Der verschlüsselte Endpunkt aus der Datenbank.

Palo Alto-Firewall: Protokollaktion Abrufen

Die **Palo Alto-Firewall: Protokoll Abrufen** Die Flow-Aktion plant eine Abfrage in der Firewall, um Protokolle abzurufen, und gibt eine JobID zurück, die zum Abrufen der Protokolldaten verwendet wird.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Eingabevariablen

Variable	Beschreibung
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der Firewall. Diese Eingabevariable ist obligatorisch.
FirewallApiKey [Zeichenfolge]	Der API-Zugriffsschlüssel der Firewall. Diese Eingabevariable ist obligatorisch.
FirewallLogType [Zeichenfolge]	Der Typ der abzurufenden Protokolldaten (auf Bedrohung festgelegt). Diese Eingabevariable ist obligatorisch.
FirewallLogFilterQuery [Zeichenfolge]	Die Abfrage, die ausgeführt werden soll, um nach Protokollen in der Firewall zu suchen. Diese Eingabevariable ist obligatorisch.
LogDirection [Zeichenfolge]	Gibt an, ob Protokolle älteste erste (rückwärts) oder neueste erste (vorwärts) Reihenfolge angezeigt werden.
Protokollnummer [Zeichenfolge]	Gibt die Anzahl der abzurufenden Protokolle an.
LogSkipCount [Zeichenfolge]	Gibt die Anzahl der Protokolle an, die beim Abruf eines Protokolls übersprungen werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
WarteschlangenJobID [Zeichenfolge]	Die von der Firewall zurückgegebene Auftrags-ID.
Jobgeplant [Zeichenfolge]	Gibt (Erfolg oder Fehler) an, ob der Auftrag an die Firewall gesendet wurde.
Fehler [Zeichenfolge]	Alle Fehler wurden zurückgegeben.

Palo Alto-Firewall: Auftragsdatenaktion

Nach **Palo Alto-Firewall: Protokoll Abrufen** Mit der Aktion wird die Suchabfrage an die Firewall in die Warteschlange gestellt, und der Auftrag wird ausgeführt **Palo Alto Firewall: Auftragsdatenaktion** Aktion ruft die Bedrohungsprotokolldaten von der Firewall ab.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion. Alle Eingabefelder sind Pflichtfelder.

Eingabevariablen

Variable	Beschreibung
FirewallIpAddress [Zeichenfolge]	Die IP-Adresse der Firewall.
FirewallApiKey [Zeichenfolge]	Der API-Zugriffsschlüssel der Firewall.
JobId [Zeichenfolge]	Die ID des Auftrags in der Warteschlange.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können. Die Ausgabe besteht aus Daten aus der Firewall-Konfiguration sowie dynamisch generierten Daten.

Ausgabevariablen

Variable	Beschreibung
CommandStatus [Zeichenfolge]	Gibt (Erfolg oder Fehler) an, ob Daten von der Firewall abgerufen wurden.
JobData [Zeichenfolge]	Die von der Firewall erfassten Daten.
Fehler [Zeichenfolge]	Alle Fehler wurden zurückgegeben.

Palo Alto Networks – WildFire-Integration

Palo Alto Networks – WildFire Ist eine cloudbasierte Anwendung, die mit Ihrer System-Firewall interagiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkunden	Einrichten
Security Incident Response-Integrationen	Palo Alto Networks – WildFire aktivieren
Verwenden	**Entwickeln**
Wildfire-Datenanreicherungs-Flow abrufen	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie Komponenten, die mit einer Anwendung installiert sind

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Palo Alto Networks – WildFire aktivieren

Bevor Sie die Integration Security Operations Palo Alto Networks – Wildfire verwenden können, müssen Sie die Integration aus herunterladen ServiceNow Store.

Vorbereitungen

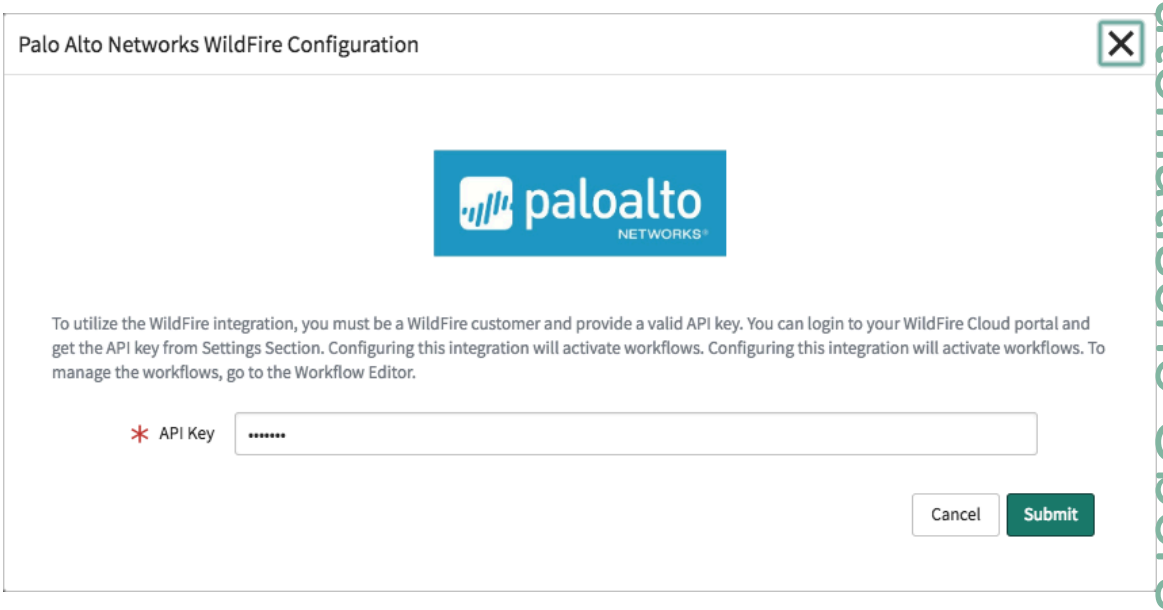
Erforderliche Rolle: Administrator

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. In Carbon Black Karte, klicken Sie auf **Konfigurieren** .



4. Geben Sie den API-Schlüssel ein, und klicken Sie auf **Übermitteln** .
   Die Integrationskonfigurationskarte wird angezeigt.
5. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie aus **Nein** Von **Konfigurationen Anzeigen** Dropdown-Liste.

Wildfire-Datenanreicherungs-Flow abrufen

Wenn **Security Operations Palo Alto Networks – Wildfire-Datenanreicherung abrufen** Flow wird ausgeführt, eine Hash-Datei wird in Wildfire hochgeladen. Die Daten werden angereichert, und Berichte werden in die Instanz heruntergeladen, um potenzielle Malware-Angriffe zu verarbeiten.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

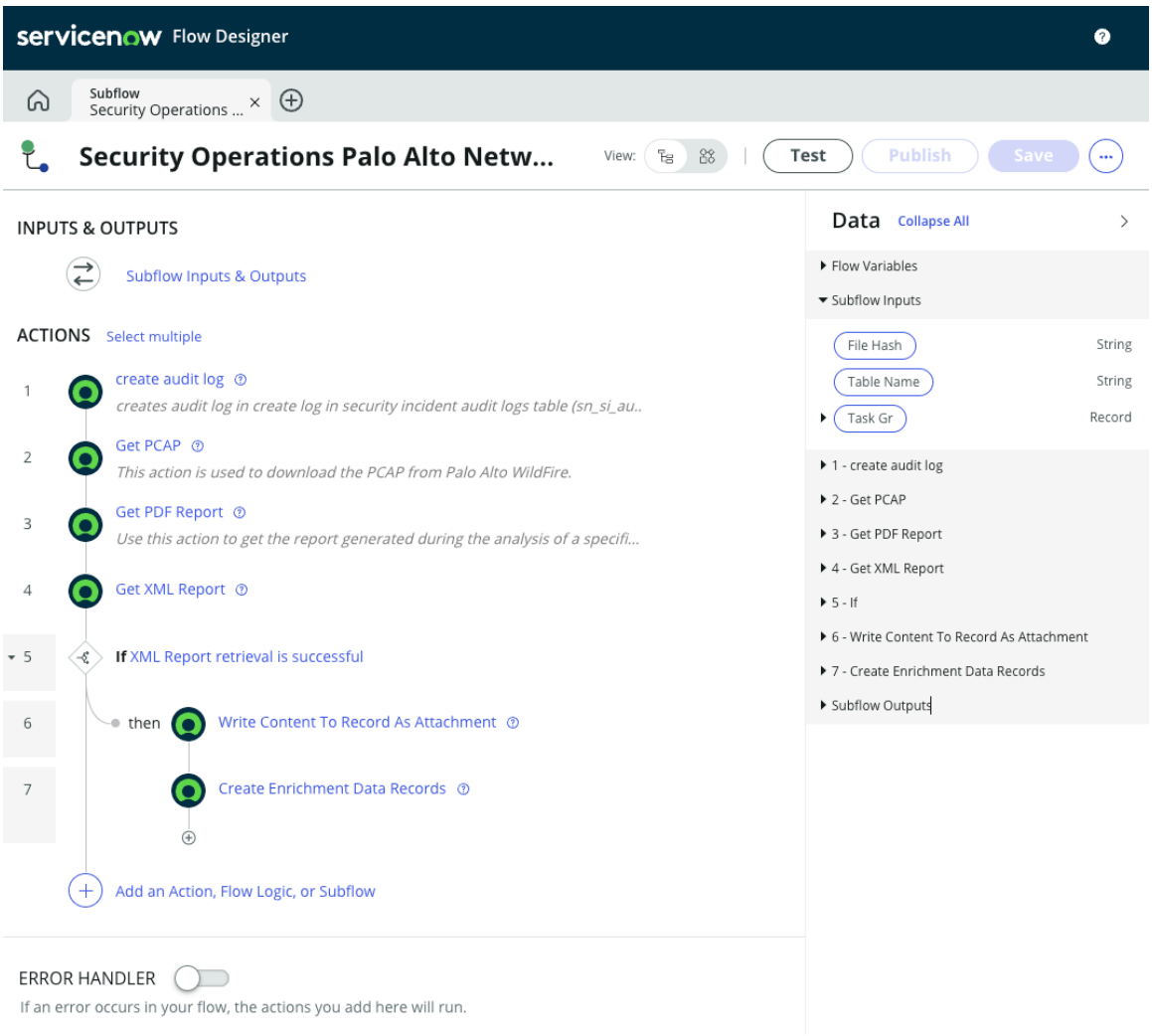
Die **Security Operations Palo Alto Networks – Wildfire-Datenanreicherung abrufen** Flow wird ausgeführt, wenn ein Security Incident aus einer Warnung erstellt wird, die von der Palo Alto Network Firewall-Anwendung empfangen wurde. Ein Malware-Hash aus der von der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Firewall empfangenen E-Mail-Benachrichtigung wird in eingegeben **IOC** Registerkarte des Security Incident, und der Datensatz wird aktualisiert.

Security Operations Palo Alto Networks – Flow zur Datenanreicherung von Wildfire abrufen



Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Offene Incidents anzeigen**an.
2. Suchen und öffnen Sie basierend auf der von der Firewall empfangenen E-Mail-Benachrichtigung den erstellten Security Incident.
3. Klicken Sie auf **Kompromittierungsindikatoren** Registerkarte und füllen Sie aus **Malware-Hash** Mit dem Hash, den Sie in der Warnung erhalten haben.
4. Klicken Sie auf **Aktualisieren**.
   Der Flow bewirkt, dass die Hash-Datei in Wildfire hochgeladen wird, wo die Daten angereichert werden. Berichte im PDF- und XML-Format werden an den Datensatz (Security Incident oder IOC) in Ihrer Instanz angehängt, um potenzielle Malware-Angriffe zu verarbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn die angereicherten Daten Informationen zur Paketerfassung enthalten, werden auch PCAP-Informationen heruntergeladen. PCAP-Daten erfassen, welche Aktionen die Datei ausgeführt hat. Zum Beispiel kann er melden, welche Server die Datei kontaktiert hat. Zum Anzeigen von PCAP-Dateien benötigen Sie eine Paketanalyse, z. B. Wireshark .

Beispiel-PDF, die von Wildfire generiert wurde

1 File Information

File Type	PE
File Signer	None
SHA-256	ab35e8bb15bdc434cd643fa5d5a6470066edf38b12128a846814bfcabbac82c2
SHA-1	8b80bb3dc5bd89a098ab4bc107abecfe955b6dbc
MD5	26cafca052a58bebdeb976e8b9723152
File Size	55296bytes
First Seen Timestamp	2016-05-04 17:53:43 UTC
Verdict	Malware
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains an invalid checksum

The PE file checksum is required for drivers, boot-time DLLs, and other DLLs loaded into secure system processes. Malware often ignores this value or sets it to zero.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

Wildfire: PCAP-Aktion abrufen

Die **Wildfire: PCAP abrufen** Die Flow-Aktion ruft die PCAP-Informationen (Packet Capture) ab, die während der Analyse eines angegebenen Datei-Hash in Wildfire generiert wurden. Das Ergebnis dieser Aktion wird an einen bestimmten Datensatz angehängt, wie von identifiziert **Tabellenname** Und **Record-ID** .

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Variable	Beschreibung
FileSHA256Hash [Zeichenfolge]	Der Hash der Datei, die von der Palo Alto Network Firewall-Anwendung empfangen wurde.
Tabellenname [Zeichenfolge]	Die betroffene Tabelle.
Record-ID [Zeichenfolge]	Der Security Incident oder IOC, der aktualisiert wird.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
CommandStatus [Boolesch]	„Wahr“, wenn ein Ergebnis erfolgreich abgerufen und angehängt wird.
errorMessage	Der Fehler, falls vorhanden, der in der Aktion aufgetreten ist.

Wildfire: Aktion zum Abrufen des PDF-Berichts

Die **Wildfire: PDF-Bericht abrufen** Die Flow-Aktion ruft den während der Analyse eines angegebenen Datei-Hash in Wildfire generierten Bericht im PDF-Format ab. Das Ergebnis dieser Aktion wird an einen bestimmten Datensatz angehängt, wie von identifiziert **Tabellenname** Und **Record-ID** .

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Eingabevariablen

Variable	Beschreibung
Tabellenname [Zeichenfolge]	Die betroffene Tabelle.
FileSHA256Hash [Zeichenfolge]	Der Hash der Datei, die von der Palo Alto Network Firewall-Anwendung empfangen wurde.
Record-ID [Zeichenfolge]	Der Security Incident oder IOC, der aktualisiert wird.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
CommandStatus [Boolesch]	„Wahr“, wenn ein Ergebnis erfolgreich abgerufen und angehängt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen (Fortsetzung)

Variable	Beschreibung
errorMessage	Der Fehler, falls vorhanden, der in der Aktion aufgetreten ist.

Wildfire: XML-Berichtsaktion abrufen

Die **Wildfire: XML-Bericht abrufen** Die Flow-Aktion ruft den Bericht ab, der während der Analyse eines angegebenen Datei-Hash in Wildfire im XML-Format generiert wurde. Das Ergebnis dieser Aktion wird an einen bestimmten Datensatz angehängt, wie von identifiziert **Tabellenname** Und **Record-ID** .

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Eingabevariablen

Variable	Beschreibung
Tabellenname [Zeichenfolge]	Die betroffene Tabelle.
FileSHA256Hash [Zeichenfolge]	Der Hash der Datei, die von der Palo Alto Network Firewall-Anwendung empfangen wurde.
Record-ID [Zeichenfolge]	Der Security Incident oder IOC, der aktualisiert wird.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
CommandStatus [Boolesch]	„Wahr“, wenn ein Ergebnis erfolgreich abgerufen und angehängt wird.
errorMessage	Der Fehler, falls vorhanden, der in der Aktion aufgetreten ist.

Palo Alto Networks Next-Generation Firewall-Integration

Nach der Installation und Konfiguration verwendet der Security Incident-Analyst diese Integration, um schädliche IP-Adressen, URLs und Domänen mithilfe von EDL-Funktionen (External Dynamic List) mit zu blockieren ServiceNow Security Incident Response(SIR) Produkte. Der Security Incident-Analyst erstellt Einträge für eine EDL aus erkennbaren Elementen, die für schädlich festgestellt wurden ServiceNow SIR Security Incidents.

Eine EDL ist eine Textdatei, die auf einem externen Webserver gehostet wird. Für diese Integration ist dieser Webserver Ihr ServiceNow AI Platform Instanz, die zulässt Palo Alto Networks Next-Generation Firewall Dient zum Importieren von Objekten, die in der Liste enthalten sind, IP-Adressen, URLs und Domänen und zum Erzwingen der Richtlinie.

Um die Richtlinie für EDL-Einträge durchzusetzen, wird in einer Richtlinienregel oder einem Profil auf die Liste verwiesen. Wenn die EDL-Einträge geändert werden, importiert die Firewall die Liste dynamisch im konfigurierten Intervall und erzwingt die Richtlinie ohne Konfigurationsänderung oder Commit für die Firewall. Für diese Integration ServiceNow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AI Platform Hat eine Tabelle erstellt, die EDL-Einträge enthält, die von einer autorisierten Person abgerufen werden Palo Alto Networks Next-Generation Firewall In den konfigurierten Abrufintervallen.

Die Integration umfasst die folgenden Funktionen:

- Flexibilität zum Erstellen mehrerer EDLs, die für verschiedene Firewall-Deny- oder Allow-Richtlinien gelten.
- Detaillierte Berichterstellung zu den Arten der blockierten Websites (Phishing, Malware und zulässige Websites).
- Tagging von ServiceNow AI Platform Security Incidents mit EDL-Einträgen nach erkennbarem Typ (URL, Domäne, IP-Adresse).
- Konfigurieren von EDL-Ablaufzeiträumen, um die EDL-Listengröße beizubehalten, indem ältere Einträge automatisch ablaufen oder entfernt werden.
- EDL-Einträge zwischen EDL-Listen werden gesucht, gelöscht oder migriert.
- Verknüpfen von EDL-Einträgen mit Datensätzen erkennbarer Elemente und Security Incidents, die Threat Intelligence-Ergebnisse und Details dazu enthalten, warum ein Eintrag blockiert ist.

Die Integration erfordert, dass die Plugins (com.snc.security_incident) und (com.snc.secops.orchestration) aus dem Security Incident Response Produkt ist aktiviert.

Diese Integration unterstützt nur Palo Alto Networks(PAN-OS 8.x). Frühere Versionen werden nicht unterstützt.

Diese Integration ist mit den Releases Kingston, London, Madrid und New York von kompatibel ServiceNow AI Platform®.

Hinweis:
Die folgenden Themen sind nummeriert. Um eine reibungslose Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse zu gewährleisten, befolgen Sie die Themen in der Reihenfolge, in der sie angezeigt werden.

Erstellen Sie ein Zertifikatprofil für Palo Alto Networks Next-Generation Firewall

Die Integration erfordert ein Zertifikatprofil, um die sichere Verbindung zwischen zu validieren und zu authentifizieren ServiceNow AI Platform® Server und Palo Alto Networks Next-Generation Firewall Server.

Erforderliche Rolle: Palo Alto Networks Next-Generation Firewall Administrator.

A Palo Alto Networks Next-Generation Firewall Authentifiziert sich bei ServiceNow AI Platform® Instanz ruft EDL-Einträge aus der Datenbanktabelle ab und integriert die Einträge in die entsprechenden Firewall-Richtlinienregeln. Dieser Abruf erfordert die API-Anwenderaccount-Rolle in der ServiceNow AI Platform® Instanz, die vom PAN-Firewall-Administrator für den Zugriff auf verwendet wird ServiceNow AI Platform® API.

Führen Sie die folgenden Schritte aus, um DigiCertificates herunterzuladen und das Zertifikatprofil zu konfigurieren.

1. Laden Sie das DigiCert- oder Entrust-CA-Gateway-Zertifikat basierend auf dem Anwendungsfall herunter. Weitere Informationen finden Sie unter KB1702083 artikel in Now Support Knowledge Base.
2. Konfigurieren Sie das Zertifikatprofil. Weitere Informationen finden Sie unter Palo Alto Networks-Dokumentation .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

„Konfigurieren eines Zertifikatprofils“ im PAN-OS 10,0-Administratorhandbuch

Richten Sie ein, und installieren Sie es Palo Alto Networks Next-Generation Firewall

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation erforderlich.

Vorbereitungen

Erforderliche Rolle: (administrator)

Setupaufgabe	Beschreibung
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow AI Platform Und Security Incident Response Rollen zugewiesen.	Die folgenden Rollen sind erforderlich: • Der Systemadministrator (Administrator) installiert die App und weist die Rolle Security Incident-Administrator (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und erstellt, aktiviert und entfernt EDLs. Diese Rolle weist auch die Rolle sn_si.Analyst zu. • Der (Administrator) weist den zu ServiceNow AI Platform® API-Account-Rolle (sn_sec_panfw.api_Account_Access), die ausschließlich für die Eingabe von Anmeldeinformationen verwendet wird, die für die Authentifizierung in erforderlich sind Palo Alto Networks Damit die Firewalls EDLs aus abrufen können ServiceNow AI Platform®. • (sn_si.Analyst) oder Security Operations Center (SOC) Analyst erstellt EDL-Einträge und arbeitet mit Security Incidents.
Überprüfen Sie, ob Sie verwenden Palo Alto Networks Next-Generation Firewall Version-OS 9.x und 10.x.	Diese Integration unterstützt nur Palo Alto Networks Next-Generation Firewall OS 9,0 und höher.
Richten Sie EDL-Profile, Sicherheitsrichtlinienregeln und Zertifikatprofile in ein Palo Alto Networks Wie in empfohlen Palo Alto Networks Dokumentation.	Siehe Palo Alto Networks Allgemeine Dokumentation und Anforderungen an: Dokumentationswebsite für Paloalto Networks .
Überprüfen Sie, ob Sie das DigiCert-Stammzertifikat heruntergeladen und konfiguriert haben.	Die Integration erfordert dieses Zertifikat, um die sichere Verbindung zwischen zu validieren und zu authentifizieren ServiceNow AI Platform Server und Palo Alto Networks Next-Generation Firewall Server. Weitere Informationen zum Einrichten des Zertifikats finden Sie unter „Konfigurieren eines Zertifikatprofils“ im PAN-OS 10,0-Administratorhandbuch . Informationen zum Download finden Sie unter Erstellen Sie ein Zertifikatprofil für Palo Alto Networks Next-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	Generation Firewall Und Vertrauenswürdige DigiCert-Stammzertifikate .
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	Madrid und spätere Release-Anforderungen Für das Madrid-Release und spätere Familienveröffentlichungen Security Incident Response Abhängigkeits-Plugin (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Für die Integration erforderliche Anwendungen. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. **1.** Security Incident Response **2.** Sicherheits-Integrations-Framework **3.** Security Support Common **4.** Orchestration Des Sicherheitssupports Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz für die Integration finden Sie unter Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.
Wenn Ihre Organisation hat ServiceNow AI Platform® Change-Management- und Genehmigungsprozesse für das Löschen von E-Mails. Stellen Sie sicher, dass die Funktion zum Senden/ Empfangen von E-Mails aktiviert ist.	Um sicherzustellen, dass die Funktion zum Senden/ Empfangen von E-Mails in Ihrem aktiviert ist ServiceNow AI Platform® Instanz, navigieren Sie zu **E-Mail-Eigenschaften** > **Administration** > **E-Mail-Eigenschaften**an. Überprüfen Sie unter Konfiguration ausgehender E-Mails **E-Mail wird gesendet** Und **E-Mail-Empfang** Sind ausgewählt.

Prozedur

Wenn Sie die Anwendung für die Integration nicht installiert haben, finden Sie weitere Informationen unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie die API-Account-Rolle für Palo Alto Networks Next-Generation Firewall

In ist eine API-Account-Rolle erforderlich ServiceNow AI Platform® Instanz für diese Integration. Der Anwendername und das Passwort, die diesem Account zugeordnet sind, werden in erstellt ServiceNow AI Platform® Und in eingegeben Palo Alto Networks Also die Palo Alto Networks Next-Generation Firewall Authentifiziert sich mit ServiceNow AI Platform® Beim Abrufen von EDL-Einträgen.

Vorbereitungen

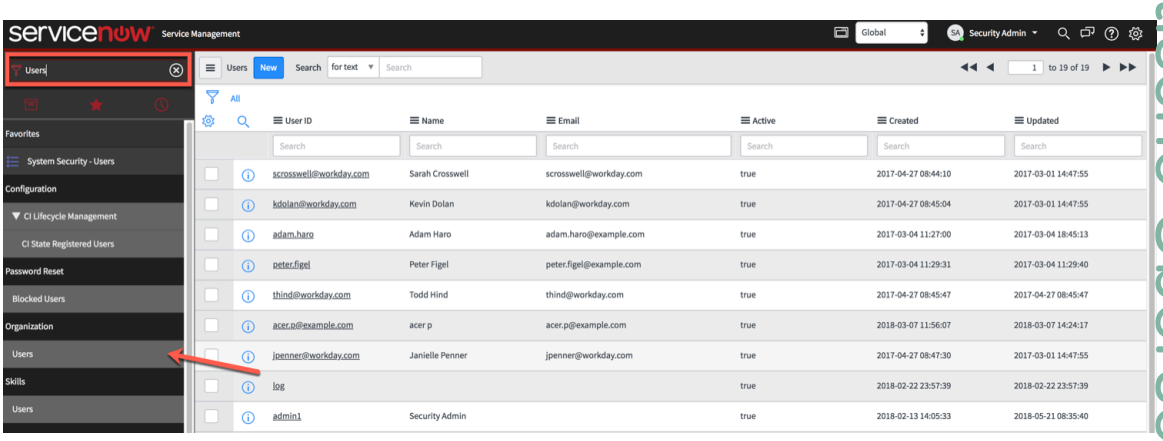
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

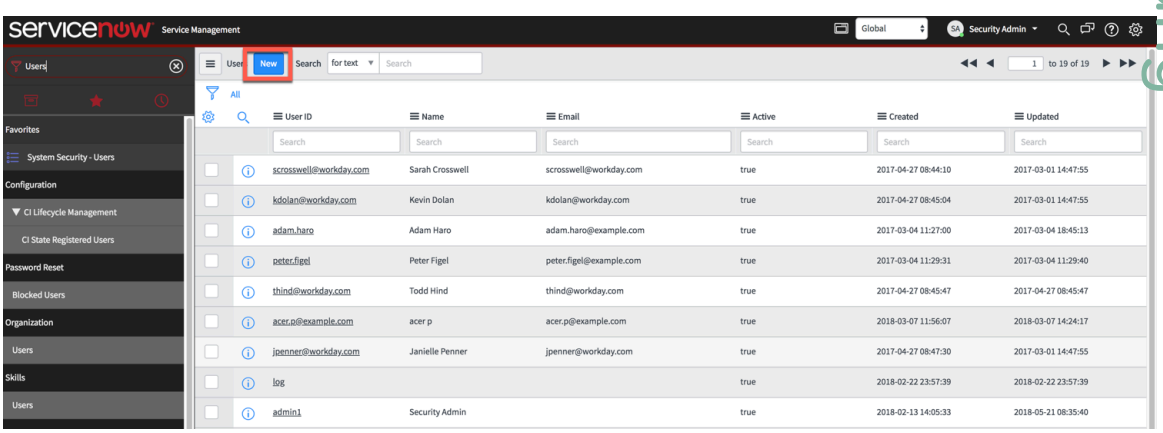
Die ServiceNow AI Platform® der administrator erstellt eine API-Account-Rolle (sn_sec_panfw.api_Account_Access). Dieser Account wird ausschließlich für die Eingabe von Anmeldeinformationen verwendet, die für die Authentifizierung in erforderlich sind Palo Alto Networks Damit die Firewalls EDLs aus abrufen können ServiceNow AI Platform®. Dieser Account ist ein separater, eindeutiger API-Anwenderaccount in ServiceNow AI Platform® Instanz und zugewiesen an Palo Alto Networks Next-Generation Firewall Administrator.

Prozedur

1. Navigieren zu **Alle** > **Organisation** > **Anwender**an.
2. Klicken Sie auf **Anwender** Modul.



3. Klicken Sie in der angezeigten Liste Anwender auf **Neu** .



Ein neues Anwenderformular wird angezeigt.

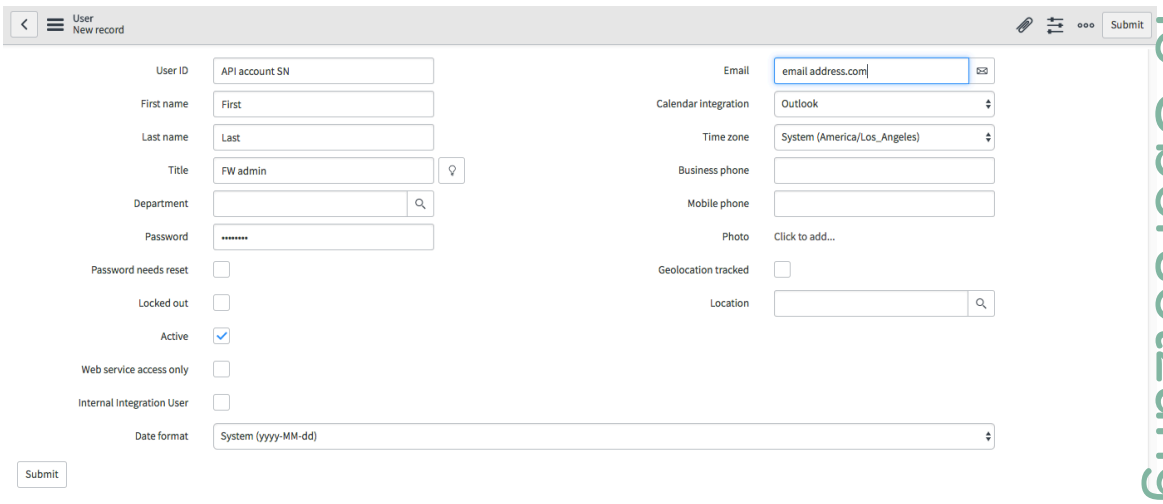
4. Füllen Sie das Formular aus.

Automatische Übersetzung

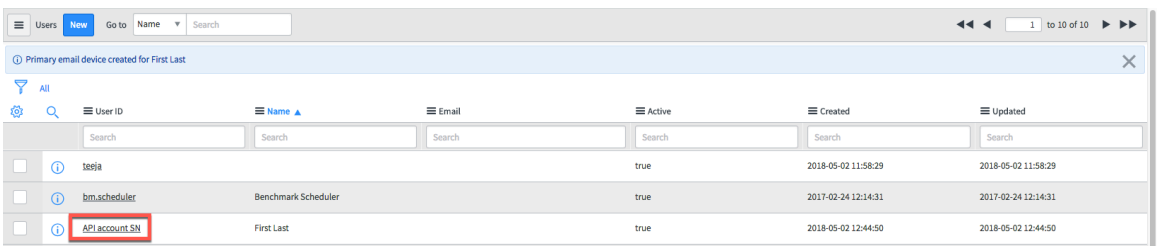
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Die in der folgenden Tabelle und Abbildung angezeigten Werte für Anwender-ID-Titel und E-Mail-Adresse sind Beispielwerte.

Feld	Beschreibung
Anwender-ID	Eindeutige Anwender-ID für die Rolle in Ihrem ServiceNow AI Platform® Instanz. Diese Anwender-ID wird in eingegeben **Anwendername** Feld in **Client-Authentifizierung** Abschnitt des Dialogfelds „externe dynamische Listen“ auf der Palo Alto Networks Website. Ein Beispiel ist `API-Account-SN` .
Vorname	Person, die Sie zuweisen.
Nachname	Person, die Sie zuweisen.
Titel	Stellenbezeichnung, z. B. `FW-Administrator` .
Passwort	Eindeutiges Passwort, das für diese Rolle erstellt wurde. Dieses Passwort wird in eingegeben **Passwort** Feld in **Client-Authentifizierung** Abschnitt des Dialogfelds „externe dynamische Listen“ auf der Palo Alto Networks Website.
E-Mail	Eindeutige E-Mail-Adresse.



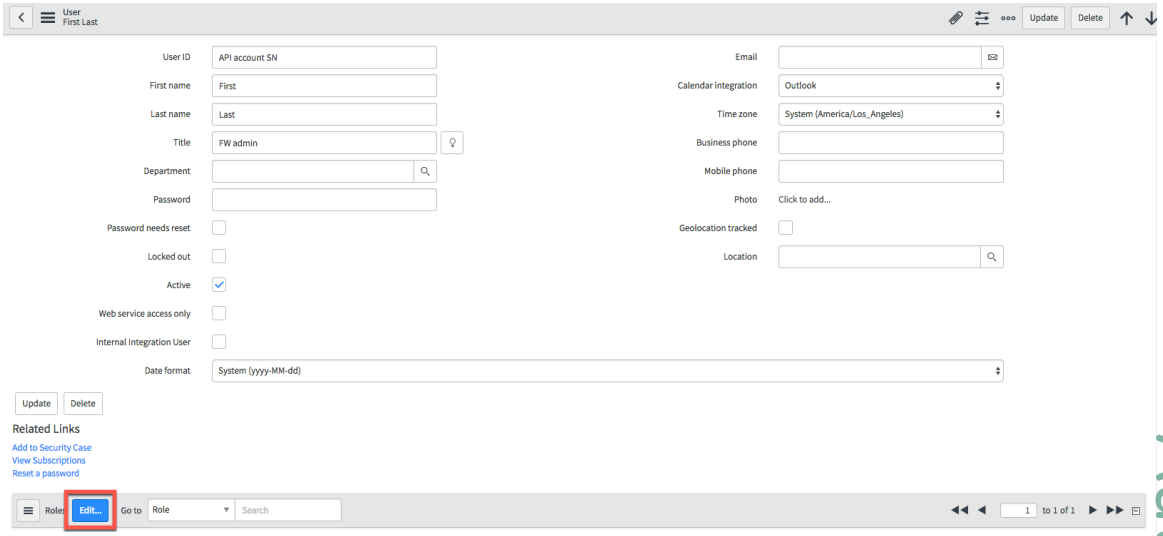
5. Klicken Sie auf **Absenden**.
   Nach der Übermittlung können Sie die Rolle zuweisen.
6. In der Liste Anwender in **Anwender-ID** Spalte auf den Namen der von Ihnen eingegebenen Anwender-ID klicken, `API-Account-SN` , Zum Beispiel.



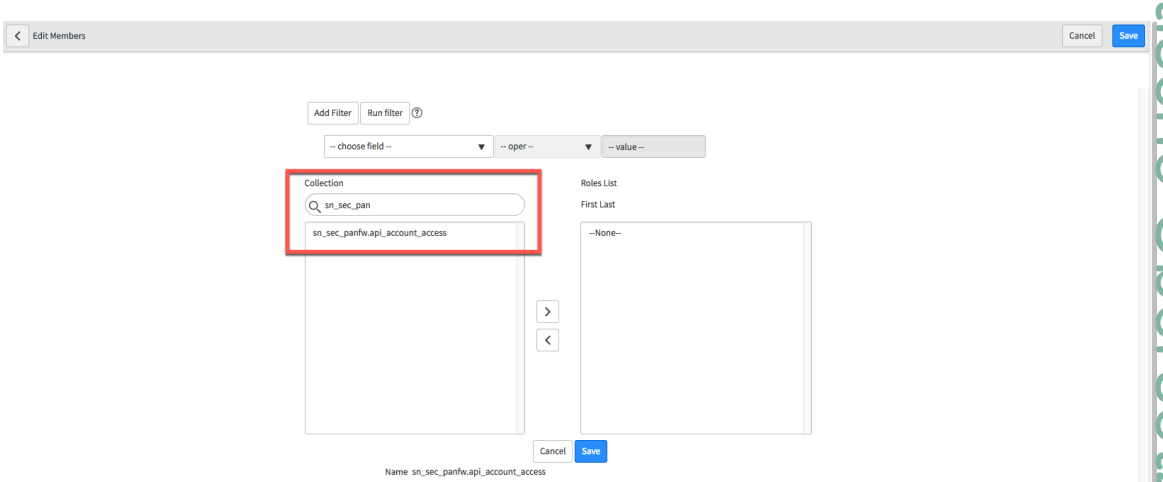
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

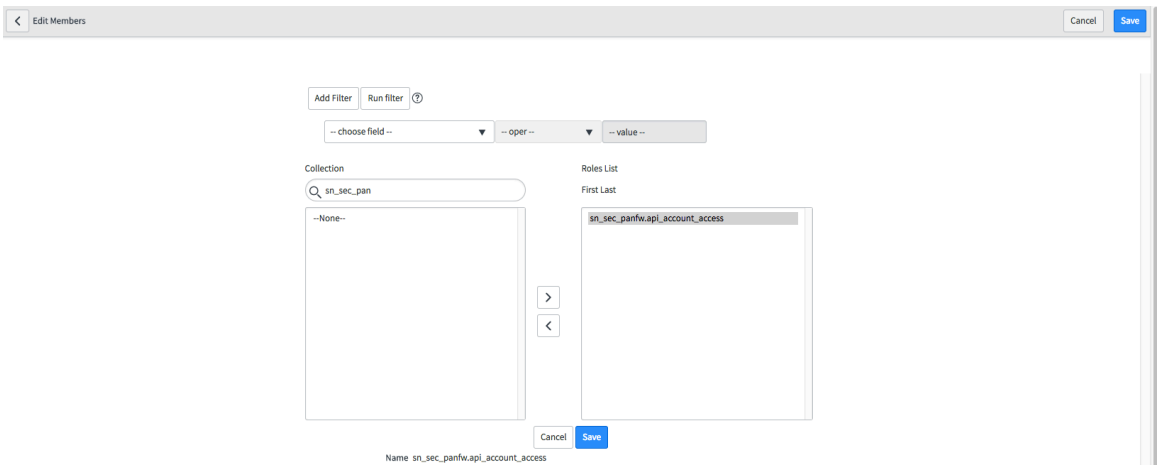
7. Klicken Sie im Abschnitt „Rollen“ im Datensatz öffnen auf **Bearbeiten** .



8. Auf der **Bearbeiten Sie Mitglieder** Formular, das angezeigt wird, geben Sie ein sn_sec_panfw.api_Account_Access In **Sammlung** Feld.
Unter **Sammlung** Feld wird die Rolle in der Spalte angezeigt.



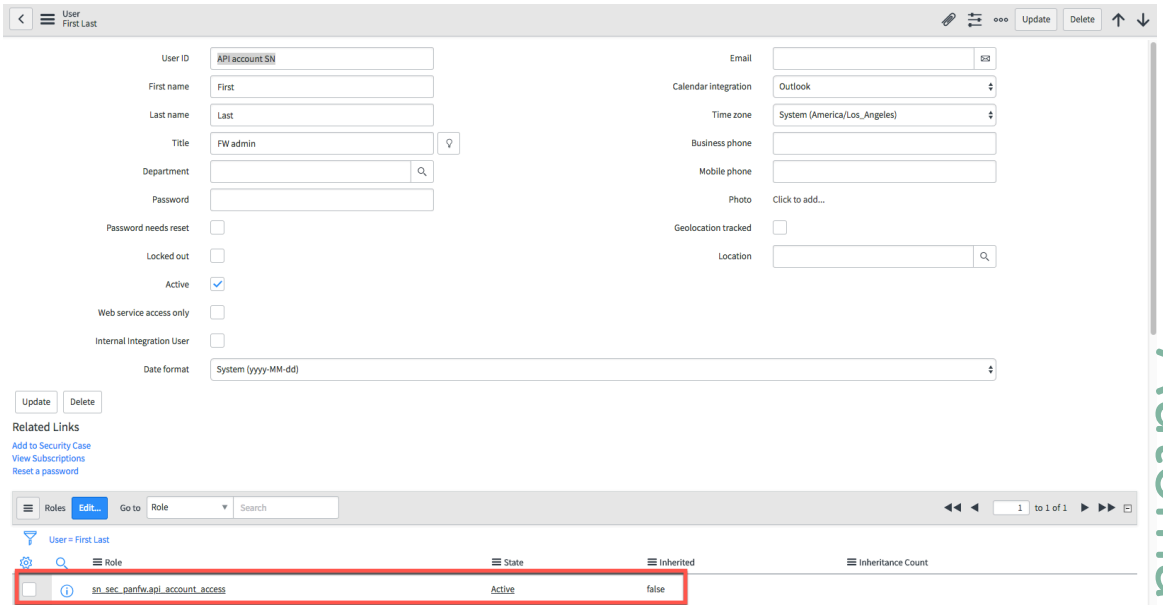
9. In **Sammlung** Spalte, wählen Sie dann Verschieben aus sn_sec_panfw.api_Account_Access Zu **Rollenliste** .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Klicken Sie auf **Speichern**.
11. Navigieren Sie zu **Anwender** , Und in **Anwender** Klicken Sie in der Liste auf den ID-Namen, den Sie für die Rolle erstellt haben (API-Account-SN).



Der Anwenderdatensatz wird angezeigt. Dieser Datensatz verifiziert, dass der Anwenderaccount zugewiesen wurde. Die **Status** Ist aktiv, und die Rolle wird nicht geerbt.

Unterstützte externe dynamische Listen für Palo Alto Networks Next-Generation Firewall

Die ServiceNow Palo Alto Networks Next-Generation Firewall Die Integration unterstützt externe dynamische Listen (EDLs), die IP, URL und erkennbare Domänenelemente akzeptieren.

Unterstützte EDLs und erkennbare Elemente

Ein *Externe Dynamische Liste* Ist eine Textdatei, die auf einer externen gehostet wird *Webserver* , Die für diese Integration ist ServiceNow AI Platform Instanz. Die Palo Alto Networks Next-Generation Firewall Kann dann in der Liste enthaltene Objekte – IP-Adressen, URLs, Domänen – importieren und die Richtlinie durchsetzen. Um die Richtlinie für EDL-Einträge durchzusetzen, wird in einer Richtlinienregel oder einem Profil auf die Liste verwiesen.

Diese Integration unterstützt drei Arten von EDLs:

- IP (umfasst eine einzelne IP-Adresse sowie CIDR-Adressblöcke (Adressbereiche)).
- URL
- Domäne

Die folgende Tabelle enthält Beschreibungen der von dieser Integration unterstützten erkennbaren Elemente und Beispielformate für jeden Typ.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte erkennbare Elemente und Beispielformate

Erkennbares Element	Beispielformate	Beschreibung
IP-Adresse	• 95.153.103.54 (IPv4) • (IPV6): 2001:00B8:130F:FE03:0000:0900:980F:130B	Stellt eine einzelne, eindeutige Schnittstellenadresse dar. Die Integration unterstützt IPv4-, IPv6- und CIDR-Formate. Die Unterstützung für erkennbare IP-Adressen umfasst CIDR-Bereiche (Classless Inter-Domain Routing), z. B. 95.153.100.0/22. Hinweis: Eine Fehlermeldung wird angezeigt, wenn Sie versuchen, eine einzelne IP-Adresse an eine EDL anzuhängen, die Sie bereits als Teil eines CIDR-Bereichs blockiert haben. Beispielsweise ist die einzelne Adresse 95.153.103.54 Teil des CIDR-Bereichs, der durch 95.153.100.0/22 (95.153.100.0-95.153.103.255) dargestellt wird.
URL	• www.example.com • www.example.com/article.html • example.com • *.example.com	Platzhalter werden unterstützt. Die ServiceNow AI Platform Formatiert URL-Einträge neu, um sie zu erfüllen Palo Alto Networks EDL-Formatanforderungen.
Domäne	• www.example.com • example.com • mail.example.com	Platzhalter werden nicht unterstützt.

Weitere Informationen zu Formatierungsrichtlinien und EDLs finden Sie unter „Formatierungsrichtlinien für eine externe dynamische Liste“ im PAN-OS 10,0-Administratorhandbuch Auf der Palo Alto Networks Website.

Erstellen Sie eine EDL für die Palo Alto Networks Next-Generation-Firewall

Erstellen Sie eine externe dynamische Liste (EDL) in Ihrem ServiceNow AI Platform Instanz. Nach der Genehmigung und Aktivierung können Sie Einträge für EDLs aus erkennbaren Elementen erstellen, die für schädlich festgestellt wurden ServiceNow AI Platform Security Incident Response(SIR) Incidents und fordern Sie die Genehmigung an, um sie zu blockieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie die EDL auf Ihrem ServiceNow AI Platform Instanz, damit die Firewall Objekte importieren kann – IP-Adressen, URLs, Domänen – die in der Liste enthalten sind und die Richtlinie durchsetzen kann. Um die Richtlinie für EDL-Einträge durchzusetzen, wird in einer Richtlinienregel oder einem Profil auf die Liste verwiesen.

Die Zahlen im folgenden Abschnitt werden mit angezeigt **Formulare mit Registerkarten** In Systemeinstellungen gelöscht. Weitere Informationen zum Auswählen und Löschen von Formularen mit Registerkarten finden Sie im Abschnitt „Formulare mit Registerkarten anzeigen“ in Configuring the form layout .

Prozedur

1. Navigieren Sie nach Abschluss der Anwendungsinstallation zu **Integrationen** > **Integrationskonfigurationen**an.
2. Suchen Sie nach Palo Alto Networks Next-Generation Firewall Kachel und klicken Sie auf **Konfigurieren** .

3. Klicken Sie Auf **Erstellen Sie eine neue EDL-Liste** .

4. Füllen Sie im Formular die Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Palo Alto Networks Formular „externe dynamische Firewall-Liste“

Feld	Beschreibung
Name	Palo Alto Networks Name der dynamischen Firewall-Liste. Fügen Sie den Typ des erkennbaren Elements (URL, IP, Domäne) in dieses Feld ein, damit der Sicherheitsanalysten die Absicht der EDL leicht anhand ihres Namens erkennen kann. Der Name muss auch deutlich angeben, welcher Firewall-Richtlinie diese EDL-Objekte zugeordnet sind. Einige Beispiele für EDL-Namen sind: Ausgehende Malware-IP oder ausgehende Phishing-URL.
Aktiv	Dieses Kontrollkästchen ist standardmäßig deaktiviert, um anzugeben, dass die EDL inaktiv ist. Wenn die EDL inaktiv ist, kann sie keine zusätzlichen Einträge erhalten. Wenn das Kontrollkästchen aktiviert ist, wird EDL aktiviert und ist für EDL-Einträge verfügbar.
Tag anzeigen	Das Kontrollkästchen ist standardmäßig aktiviert, um das erkennbare Element und den zugehörigen Security Incident-Datensatz automatisch zu kennzeichnen, wenn das erkennbare Element in einer EDL blockiert ist. Wenn diese Option ausgewählt ist, sind die Felder Tag-Typ und EDL-Tag für erkennbare Elemente im Formular verfügbar. **Hinweis:** Ein Tag-Name wird standardmäßig aus dem Wert erstellt, den Sie in eingeben **Name** Feld mit *EDL* – Präfix, z. B. ausgehende EDL-Malware-IP. Sie können den Tag-Namen und die Farbe ändern. Siehe: (Optional) Bearbeiten Sie den Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall. Der Tag-Name wird im Feld EDL-Tag für erkennbare Elemente angezeigt, sobald die EDL gespeichert wurde. Wenn das Kontrollkästchen deaktiviert ist, wird kein Tag erstellt, und die Felder Tag-Typ und EDL-Tag für erkennbare Elemente sind im Formular nicht verfügbar.
Erkennbarer Typ	Wählen Sie einen Typ des erkennbaren Elements aus der Auswahlliste aus, den diese EDL akzeptiert: IP (einschließlich CIDR), URL oder Domäne.

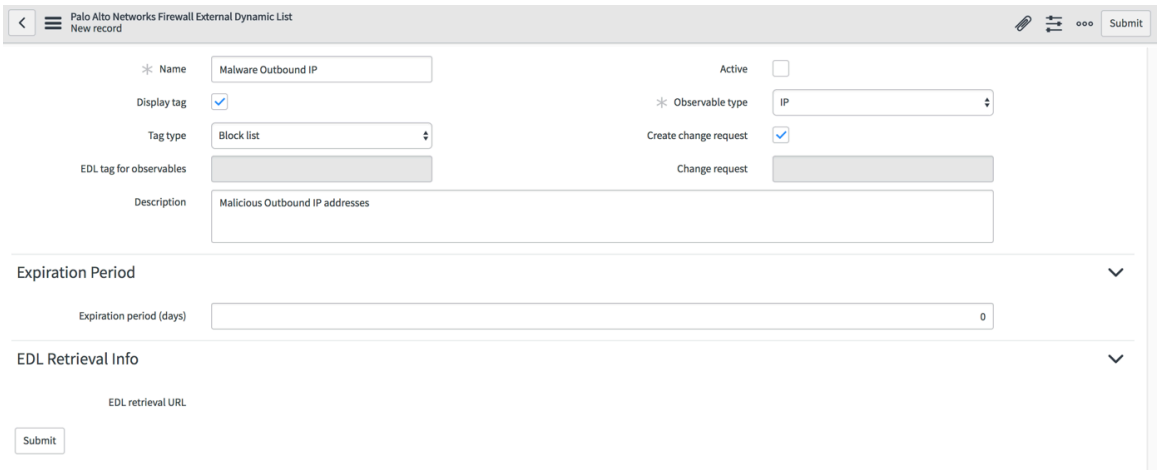
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tag-Typ	Tags, die in der Auswahlliste verfügbar sind. Eine Sperrliste ist eine Liste der erkennbaren Elemente, die Sie verwenden möchten Palo Alto Networks Next-Generation Firewall Zum Blockieren. Eine Allow-Liste ist eine Liste der erkennbaren Elemente, die Sie verwenden möchten Palo Alto Networks Next-Generation Firewall Zu zulassen. Standardmäßig ist die Tag-Farbe „Liste blockieren“ schwarz und die Tag-Farbe „Liste zulassen“ grau. Sie können die Farbe ändern. Siehe: (Optional) Bearbeiten Sie den Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall.
Erstellen Sie eine Change-Anforderung	Dieses Kontrollkästchen ist standardmäßig aktiviert, um automatisch eine Change-Anforderung und Change-Aufgaben in zu erstellen ServiceNow AI Platform Instanz, die an den EDL-Datensatz angehängt sind. Die Change-Anforderung wird verwendet, um die EDL-Listenabruf-URL in zu konfigurieren Palo Alto Networks Next-Generation Firewall Server. Diese Option wird empfohlen, wenn Ihr Firewall-Administrator auch verwendet ServiceNow AI Platform Für Firewall-Richtlinien- oder -Regeländerungen. Wenn Sie eine Anforderung erstellen, wird die EDL-Liste automatisch aktiviert, sobald sie geschlossen wurde. Deaktivieren Sie das Kontrollkästchen, um die EDL manuell zu aktivieren, nachdem Sie vom Firewall-Administrator per E-Mail darüber informiert wurden, dass die Konfiguration aktiviert wurde Palo Alto Networks Ist abgeschlossen. Wenn das Kontrollkästchen Change-Anforderung erstellen deaktiviert ist, ist das Feld Change-Anforderung nicht verfügbar.
EDL-Tag für erkennbare Elemente	Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen Tag anzeigen aktiviert ist. Das Feld wird automatisch ausgefüllt, nachdem die EDL mit einem Standardwert aus dem Feld Name gespeichert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

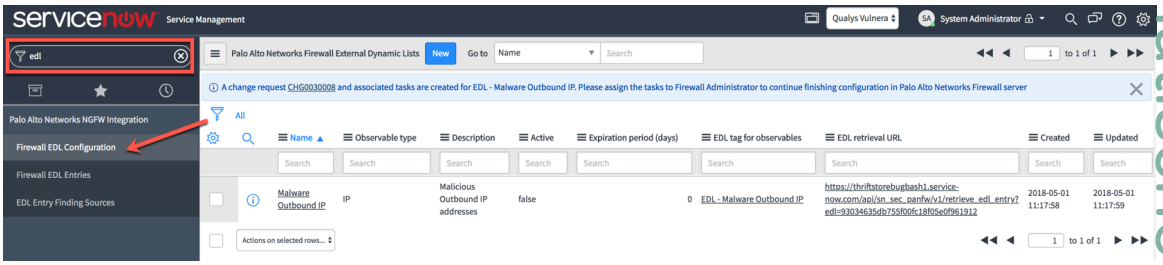
Feld	Beschreibung
	Weitere Informationen zum Ändern des Standard-Tag-Namens und der Farbe finden Sie unter (Optional) Bearbeiten Sie den Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall
Change-Anforderung	Wenn das Kontrollkästchen Change-Anforderung erstellen aktiviert ist, wird die Change-Anforderungsnummer auf angezeigt ServiceNow AI Platform Instanz, sobald die EDL gespeichert wurde. Wenn das Kontrollkästchen Change-Anforderung erstellen deaktiviert ist, wird dieses Feld nicht angezeigt.
Beschreibung	Beschreibung der dynamischen Liste der Palo Alto Networks-Firewall. Der Name enthält im Allgemeinen die Typen von Sites und erkennbaren Elementen, die Sie in dieser EDL erwarten, und Sie können dieses Feld für weitere Details verwenden.
Ablaufzeitraum (in Tagen)	Ablaufzeitraum der EDL. 0 (Standard) gibt an, dass der EDL-Eintrag nie abläuft. Wenn Sie diesen Wert ändern, ist dieser Eintrag für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben, und es gibt keinen Höchstwert. Beispiel: Wenn Sie eingeben 30 Tage um 14:01 Uhr am 1. Mai läuft die EDL um 14:01 Uhr am 31. Mai ab. Alle Einträge in dieser EDL erben diesen Wert standardmäßig, es sei denn, Sie überschreiben den Wert für einzelne Einträge.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

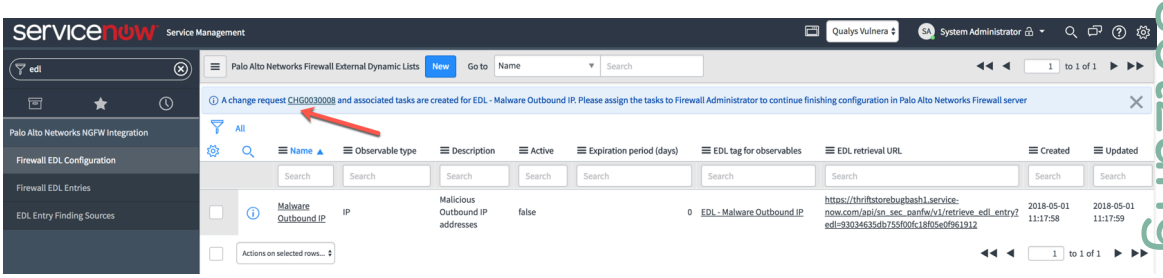


5. Klicken Sie auf **Absenden**.

6. Wenn die Liste „externe dynamische Listen der Palo Alto Networks-Firewall“ nicht angezeigt wird, navigieren Sie zu **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Konfiguration** Und klicken Sie auf **Firewall-EDL-Konfiguration** .



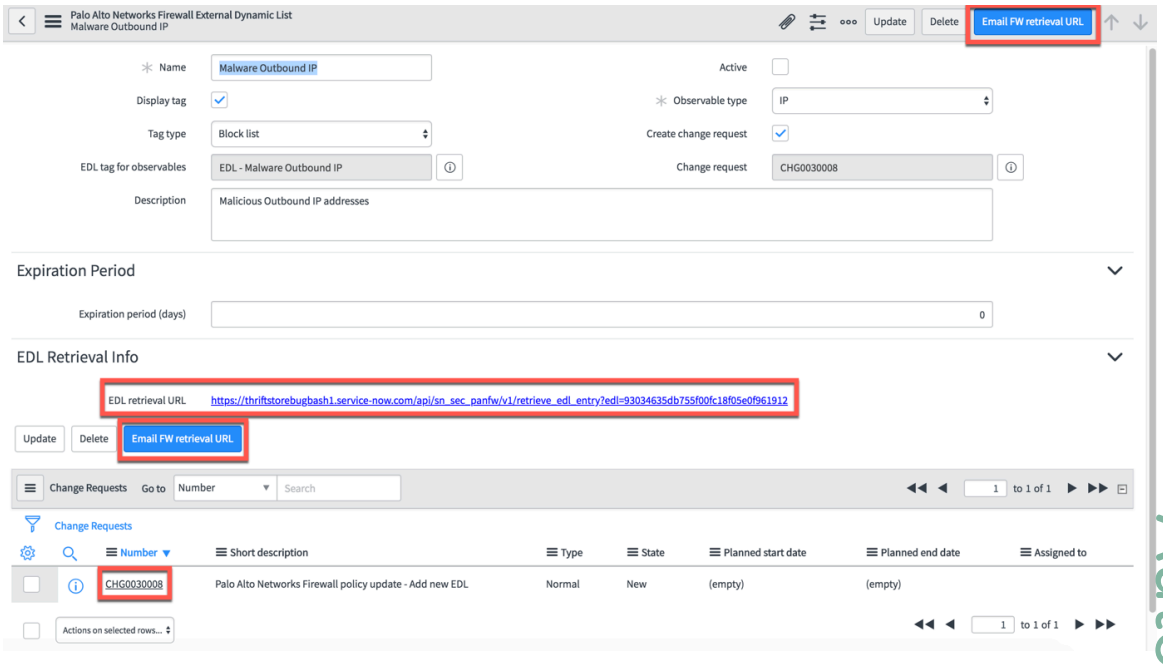
Die neue EDL wird angezeigt. Der EDL-Status ist noch inaktiv (Falsch), was bedeutet, dass die EDL nicht zum Akzeptieren von Einträgen verfügbar ist. Wenn **Erstellen Sie eine Change-Anforderung** Wurde konfiguriert, wird eine Meldung angezeigt, die angibt, dass in Ihrem eine Change-Anforderung und Aufgaben erstellt wurden ServiceNow AI Platform Instanz.



7. In **Name** Spalte auf ein Element klicken, um den Datensatz zu öffnen.
Der EDL-Datensatz wird angezeigt. Dieses Beispiel zeigt eine EDL für ausgehende Malware-IP. Die folgenden Felder, Optionen und Links werden nach der Übermittlung im neuen Datensatz angezeigt und in der folgenden Tabelle beschrieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Abruf-URL und Change-Anforderungs-Links im EDL-Datensatz

Option	Beschreibung
FW-Abruf-URL mailen	Per E-Mail erhalten Sie einen Hinweis, dass der EDL-Link für die Konfiguration für verfügbar ist Palo Alto Networks Firewall-Administrator.
EDL-Abruf-URL	Diese URL wird in platziert **Quelle** Feld im Dialogfeld „externe dynamische Listen – Authentifizierung“ auf der **Liste Erstellen** Registerkarte im Palo Alto Networks Website. Die URL-Verknüpfung mit Palo Alto Networks Firewall-Administrator verwendet für die Konfiguration in Palo Alto Networks Firewall wird automatisch generiert und angezeigt. **Hinweis:** Wenn Ihre Systemeinstellungen auf festgelegt sind **Formulare mit Registerkarten** , Dieser Link wird auf angezeigt **EDL-Abrufinformationen** Registerkarte unten im Datensatz.
ServiceNow AI Platform Change-Anforderung	Ein Link zum Change-Anforderungsdatensatz wird im Abschnitt „Change-Anforderungen“ angezeigt, wenn konfiguriert, und die Anforderungsnummer wird im Feld „Change-Anforderung“ angezeigt.
Aktualisieren	Ändern Sie Daten, und aktualisieren Sie die bearbeitbaren Felder.
Löschen	Löschen Sie den Datensatz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Erstellen Sie nach Bedarf weitere EDLs, und fügen Sie sie hinzu.
   Die EDLs werden im angezeigt Palo Alto Networks Externe dynamische Listen-Liste.

Nächste Maßnahme

Aktivieren Sie eine EDL manuell oder mit ServiceNow AI Platform Change-Anforderung.

Aktivieren Sie eine EDL

Nachdem die externe dynamische Liste (EDL) in erstellt wurde ServiceNow AI Platform® Und die URL ist verfügbar, die Palo Alto Networks Der Firewall-Administrator konfiguriert die EDL im Palo Alto Networks Next-Generation Firewall. Die Abruf-URL wird von verwendet Palo Alto Networks Firewall-Administrator zum Konfigurieren der EDL in Palo Alto Networks Next-Generation Firewall Server. Bevor EDL-Einträge akzeptiert werden können, muss die EDL in konfiguriert werden Palo Alto Networks Und in aktiviert ServiceNow AI Platform®.

Vorbereitungen

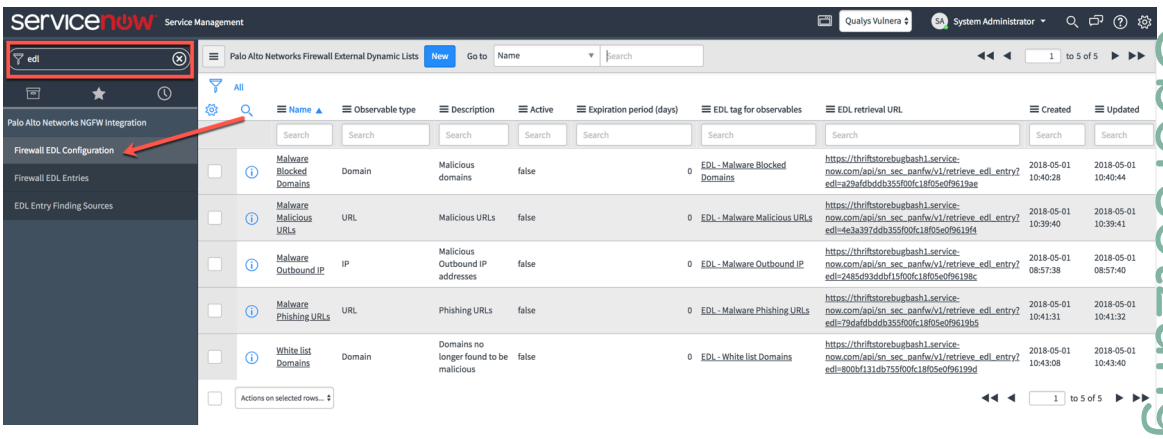
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Nachdem die EDL konfiguriert wurde, können Sie als Security Incident-Administrator die EDL manuell aktivieren, oder die EDL wird automatisch nach Abschluss von aktiviert ServiceNow AI Platform® Change-Anforderung. Die EDL muss genehmigt und vom inaktiven Status in den aktiven Status verschoben werden, bevor sie EDL-Einträge akzeptieren kann.

Prozedur

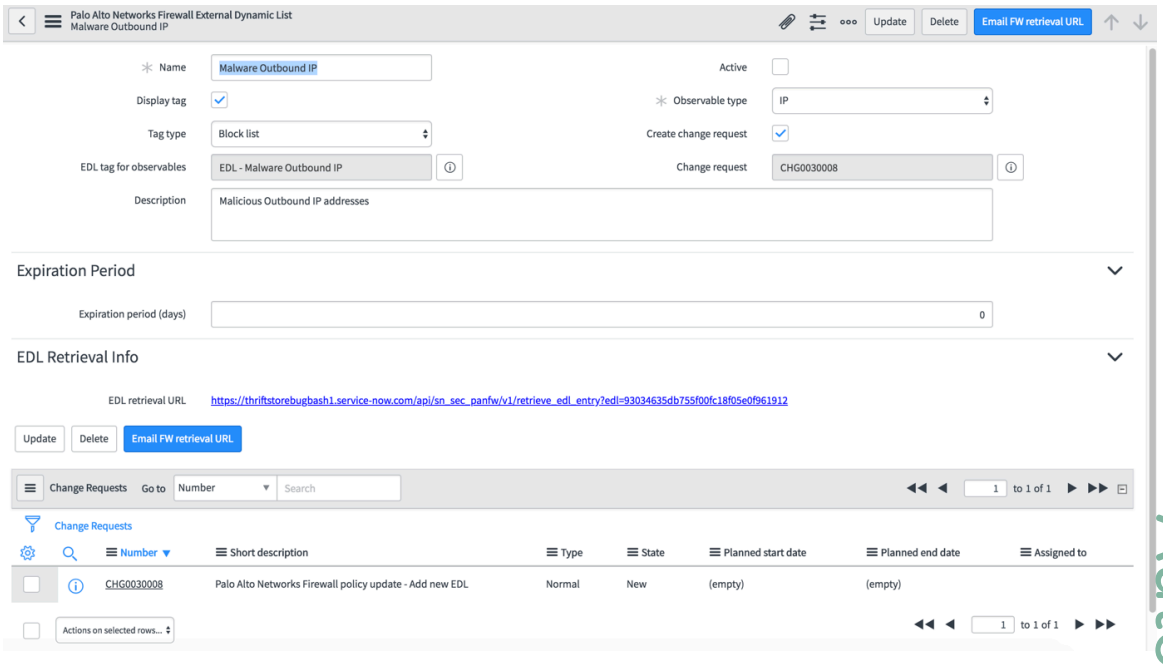
1. Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Konfiguration** Und wählen Sie aus **Firewall-EDL-Konfiguration** Modul.



2. Wählen Sie in der angezeigten Liste „Palo Alto Networks-Firewall – dynamische Listen“ Ihre neue EDL in der Spalte Name aus.
3. Notieren Sie sich im angezeigten Datensatz **E-Mail-FW-Abruf-URL** Schaltflächen, der aktive Link für EDL-Abruf-URL und, falls konfiguriert, die ServiceNow AI Platform® Change-Anforderung im Abschnitt Change-Anforderungen.
   Stellen Sie sicher, dass **Aktiv** Kontrollkästchen ist deaktiviert.

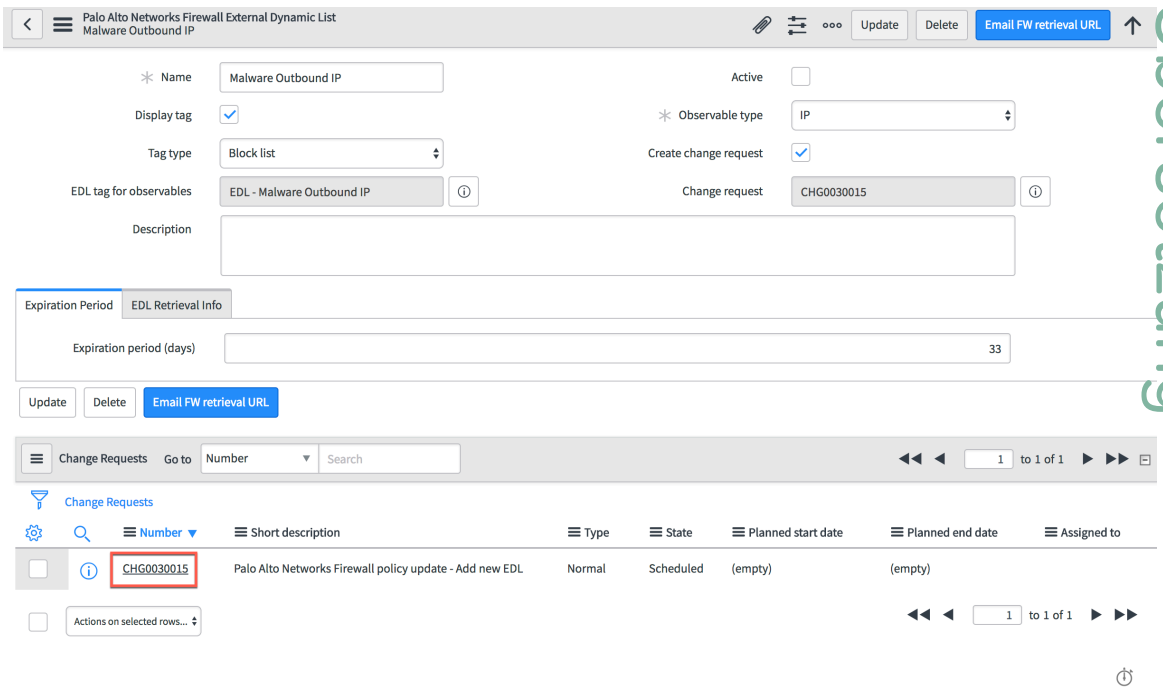
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Mit **Formulare mit Registerkarten** In Ihren Systemeinstellungen gelöscht, wird die EDL-Abruf-URL in angezeigt **EDL-Abrufinformationen** Abschnitt, wie in der vorherigen Abbildung gezeigt.

Die folgende Abbildung zeigt **EDL-Abrufinformationen** Wird als Registerkarte mit angezeigt **Formulare mit Registerkarten** In Ihren Systemeinstellungen ausgewählt. Klicken Sie auf **EDL-Abrufinformationen** Registerkarte zum Anzeigen der Abruf-URL. Der Link zur Change-Anforderung (**CH0030015**) Wird ebenfalls angezeigt.



4. Um die Konfiguration abzuschließen und die EDL von inaktiv in aktiv zu verschieben, müssen Sie eine der folgenden Optionen auswählen, um den Firewall-Administrator darüber zu informieren, dass die Abruf-URL verfügbar ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie den Firewall-Administrator darüber informiert haben, dass die Abruf-URL verfügbar ist, und Sie bestätigt haben, dass die EDL in konfiguriert wurde Palo Alto Networks, Als Security Incident-Administrator müssen Sie als Nächstes die EDL aktivieren. Sie aktivieren die EDL entweder manuell oder verwenden, falls konfiguriert, die ServiceNow AI Platform Change-Anforderungsformular zum Aktivieren der EDL.

Zugehörige Informationen

Konfigurieren Sie eine EDL

Aktivieren Sie eine EDL manuell

Wenn der Palo Alto Networks-Firewall-Administrator nicht verwendet ServiceNow AI Platform, Und Sie werden direkt benachrichtigt, dass Palo Alto Networks Next-Generation Firewall Ist konfiguriert, können Sie die externe dynamische Liste (EDL) manuell aktivieren.

Vorbereitungen

In Palo Alto Networks, Weisen Sie der von Ihnen erstellten EDL ein EDL-Objekt, eine Richtlinie und die Quell-URL zu. Weitere Informationen zum Konfigurieren der EDL für den Palo Alto Networks Next-Generation Firewall In Palo Alto Networks, Siehe Konfigurieren Sie eine EDL.

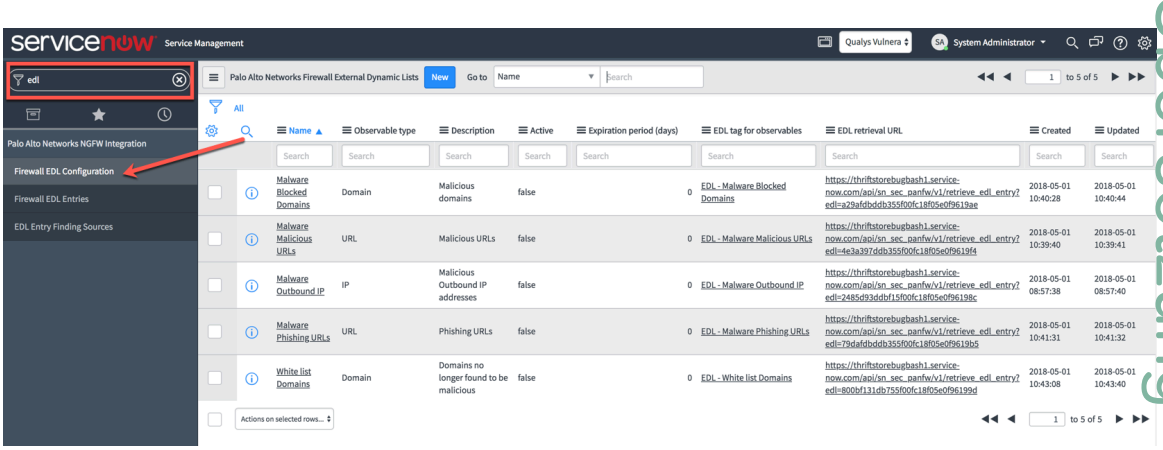
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Als ServiceNow AI Platform Security Incident-Administrator, werden Sie von benachrichtigt Palo Alto Networks Firewall-Administrator, wenn die EDL-Konfiguration in abgeschlossen ist Palo Alto Networks Next-Generation Firewall.

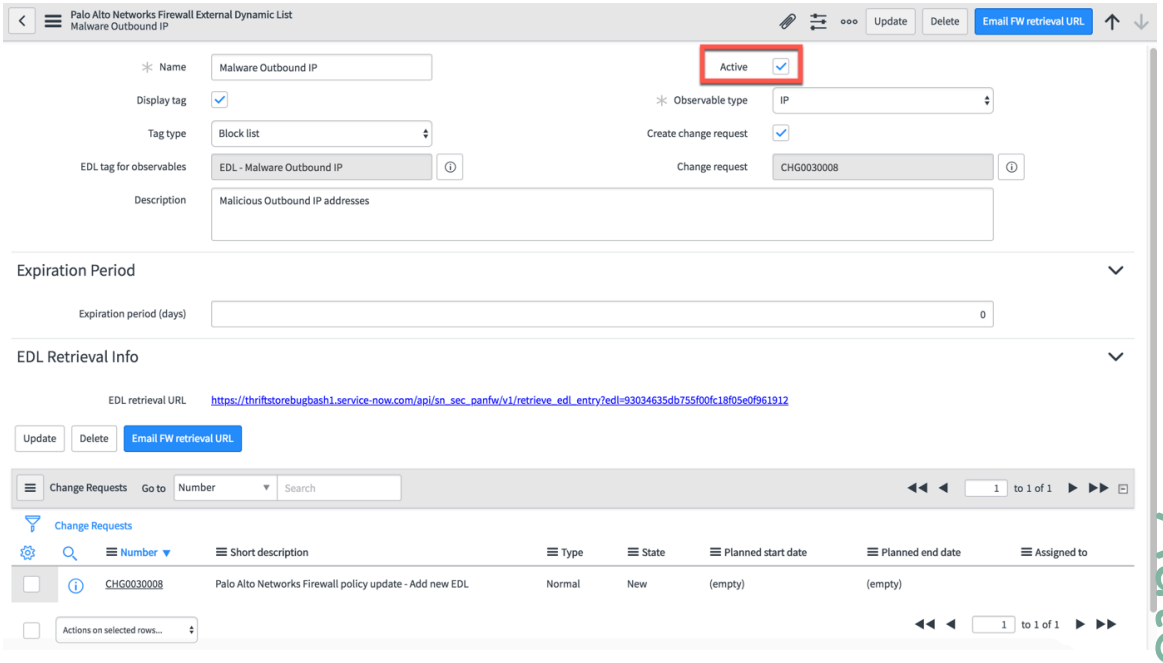
Prozedur

1. Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Konfiguration**an.

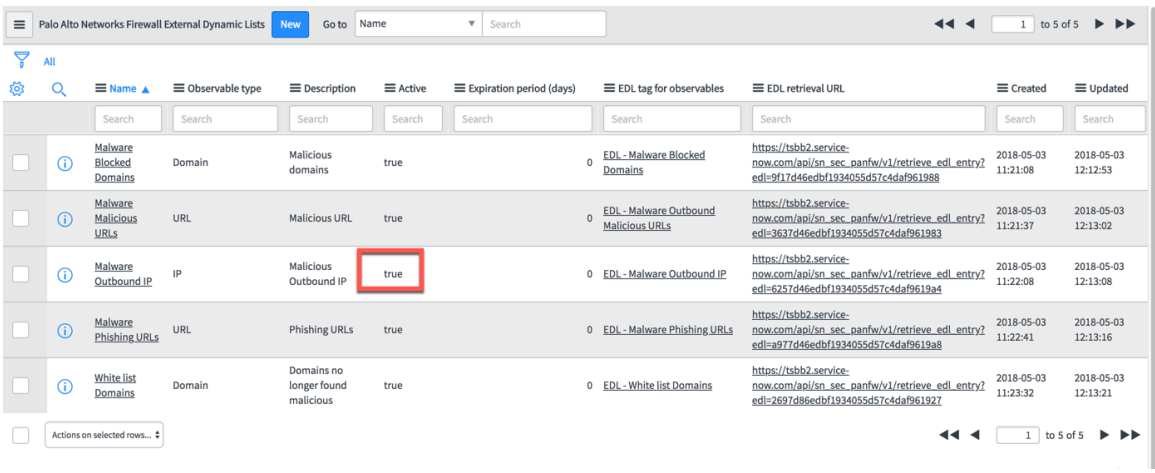


2. Wählen Sie aus **Firewall-EDL-Konfiguration** Modul.
3. Klicken Sie in der Liste „externe dynamische Listen der Palo Alto Networks-Firewall“ auf ein Element im **Name** Spalte zum Öffnen.
4. Wählen Sie im Datensatz, der geöffnet wird, die aus **Aktiv** Kontrollkästchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Aktualisieren**.
   In **Aktiv** Spalte der Liste der externen dynamischen Listen der Palo Alto Networks-Firewall, Wahr Wird für den Status der EDL angezeigt.



Ergebnisse

Die EDL ist aktiviert und bereit für den Empfang von EDL-Einträgen

Nächste Maßnahme

Übermitteln Sie EDL-Einträge aus einem Security Incident oder aus der Blockliste.

Konfigurieren Sie eine EDL

Die Palo Alto Networks Der Firewall-Administrator konfiguriert eine EDL für den Palo Alto Networks Next-Generation Firewall Nach der Benachrichtigung ist die Abruf-URL über verfügbar ServiceNow AI Platform. Bevor die EDL EDL EDL-Einträge akzeptieren kann, muss sie in konfiguriert werden Palo Alto Networks, Und in aktiviert ServiceNow AI Platform®.

Vorbereitungen

Erforderliche Rolle: Palo Alto Networks Firewall-Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

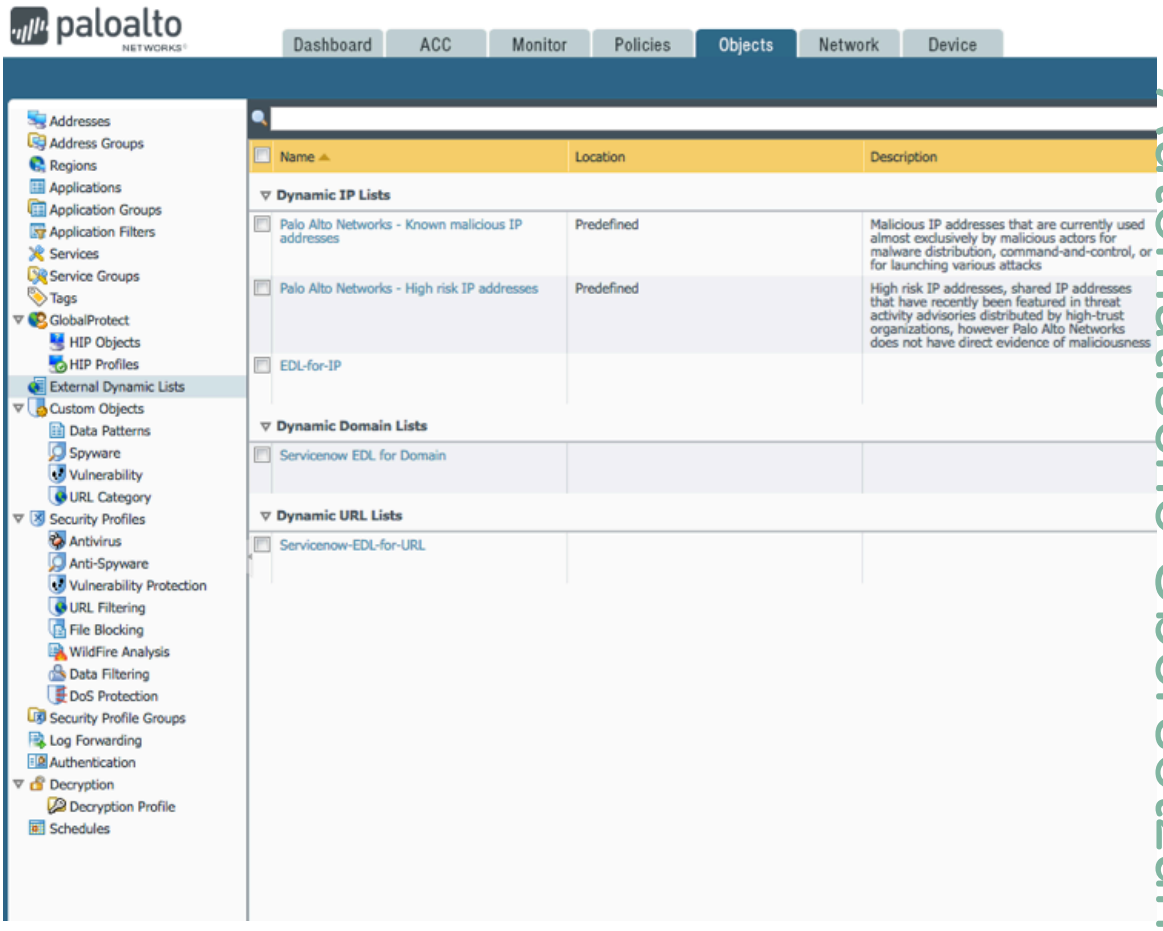
Warum und wann dieser Vorgang ausgeführt wird

Die Palo Alto Networks Next-Generation Firewall Der Administrator erstellt ein EDL-Objekt und weist der EDL die Quell-URL (Abruf) und die Richtlinie zu. Diese Aufgaben werden in ausgeführt Palo Alto Networks Bevor die EDL in aktiviert wird ServiceNow AI Platform.

Die Images im folgenden Abschnitt werden mit Berechtigung verwendet und sind PRIVILEGIERT und PROPRIETÄR.

Prozedur

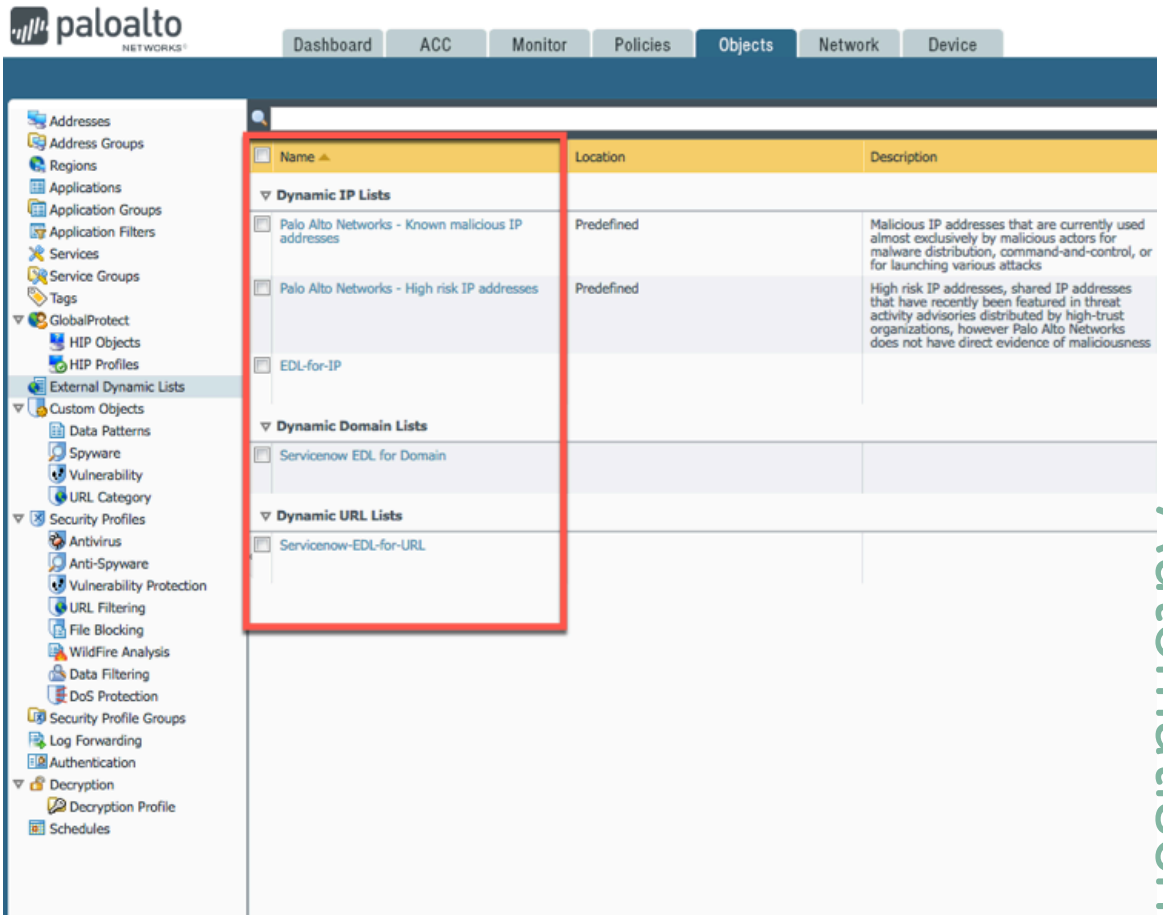
1. Wenn Sie die EDL nicht für die Firewall konfiguriert haben, navigieren Sie zu **Externe Dynamische Listen** > **Objekte** in Palo Alto Networks.



2. In **Name** Wählen Sie die Spalte aus ServiceNow EDL, die Sie aus der Liste konfigurieren möchten, z. B. **ServiceNow EDL für URL** .

Automatische Übersetzung

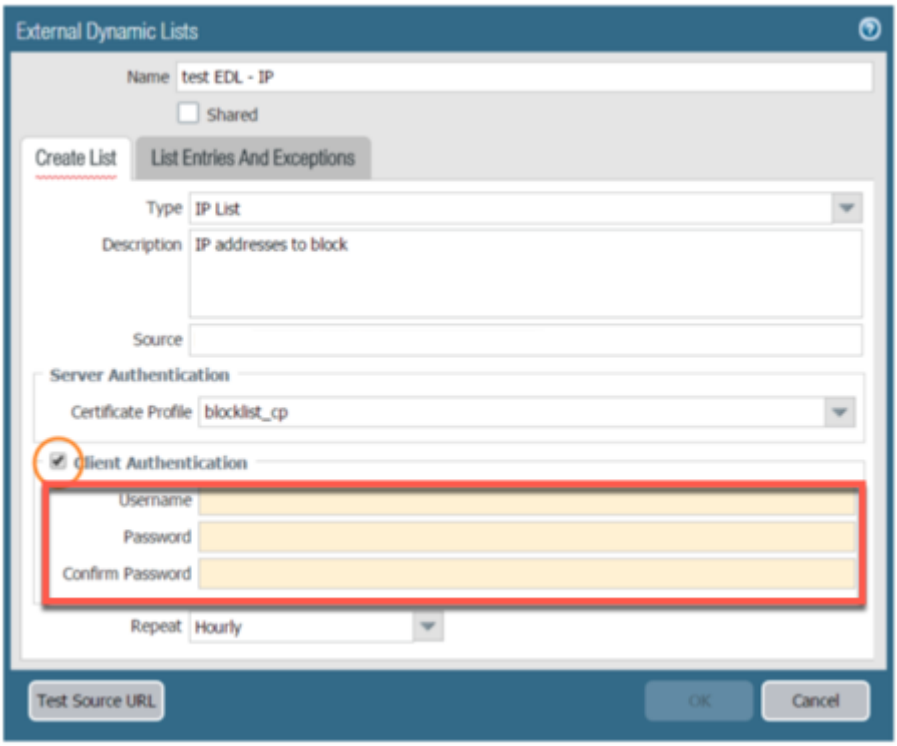
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



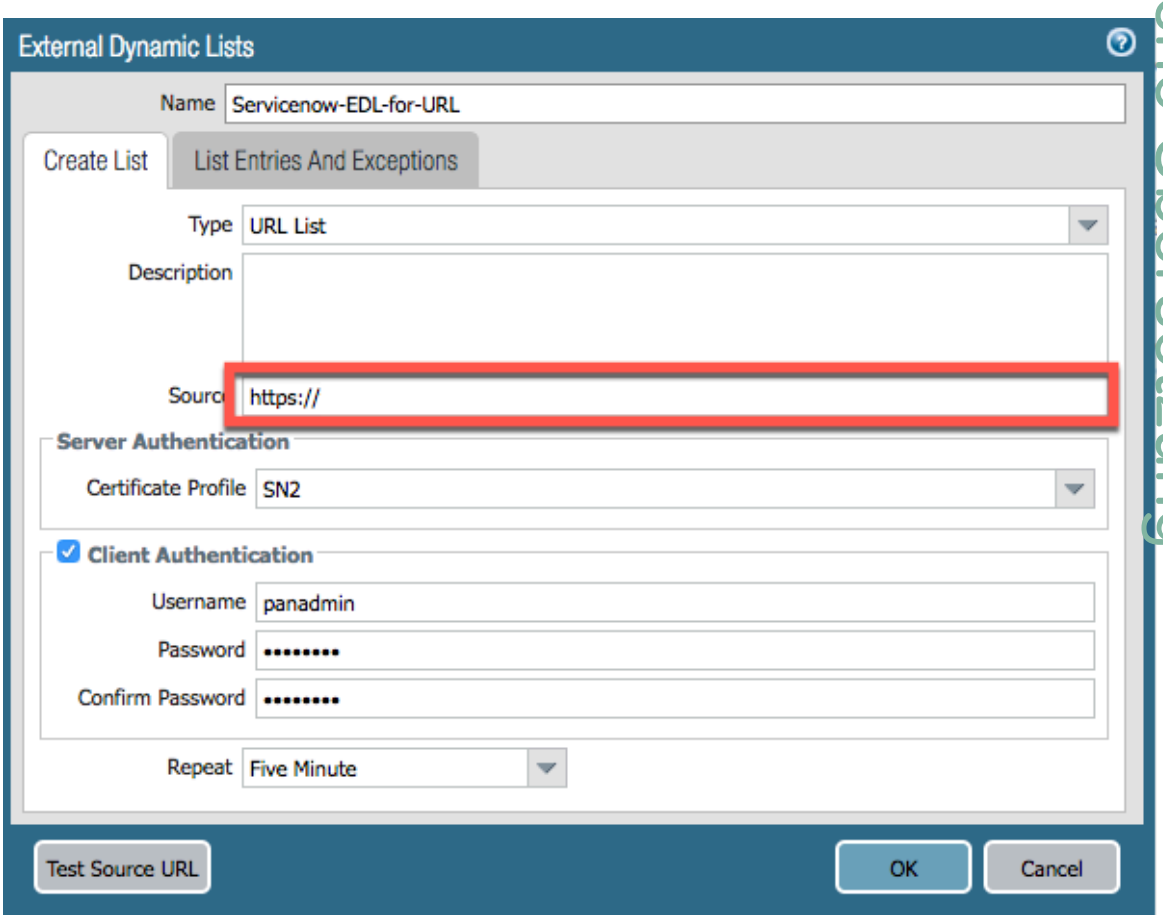
3. Geben Sie im Dialogfeld externe dynamische Listen den Anwendernamen und das Passwort ein, um sich bei zu authentifizieren ServiceNow AI Platform®.
Diese Anmeldeinformationen sind der Anwendername und das Passwort, die Sie für die API-Account-Rolle (sn_sec_panfw.api_Account_Access) in Ihrem erstellt haben ServiceNow Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie im Feld Quelle die URL ein, die in der EDL-Liste in generiert wurde ServiceNow Instanz.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie ein Zertifikatprofil aus der Auswahlliste aus. SN2 , Zum Beispiel.
6. Klicken Sie auf OK.

Aktivieren Sie eine EDL für Palo Alto Networks Next-Generation Firewall Mit einer Change-Anforderung

Wenn konfiguriert, wird ServiceNow Das Change-Anforderungsformular wird verwendet, um die externe dynamische Liste (EDL) zu aktivieren. Diese Option wird empfohlen, wenn Ihr Firewall-Administrator auch verwendet ServiceNow AI Platform Für Firewall-Richtlinien- oder -Regeländerungen. Die EDL wird automatisch aktiviert und ist bereit, EDL-Einträge nach Abschluss von zu erhalten ServiceNow AI Platform Change-Anforderung.

Vorbereitungen

Hinweis:

Die Zahlen im folgenden Abschnitt werden mit angezeigt **Formulare mit Registerkarten** In Systemeinstellungen ausgewählt. Weitere Informationen zum Auswählen und Löschen von Formularen mit Registerkarten finden Sie im Abschnitt Formulare mit Registerkarten anzeigen in Formularlayout für konfigurieren ServiceNow-Produktdokumentationswebsite .

Erforderliche Rolle: sn_si.admin zum Genehmigen der Change-Anforderung und der Change-Aufgaben

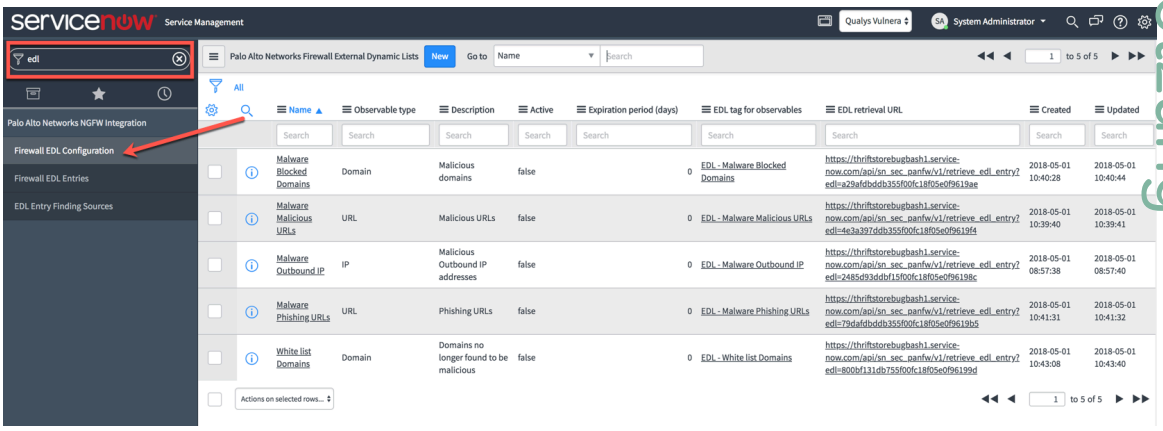
Palo Alto Networks Firewall-Administrator zum Abschließen von Konfigurationsaufgaben in Palo Alto Networks

Warum und wann dieser Vorgang ausgeführt wird

Wenn konfiguriert, überwachen Sie Ihren ServiceNow AI Platform Change-Anforderung und weisen Sie alle Aufgaben zu, die zum Konfigurieren von erforderlich sind Palo Alto Networks Next-Generation Firewall. Nachdem diese Aufgaben abgeschlossen sind, schließen Sie ServiceNow AI Platform Change-Anforderung zum automatischen Aktivieren der EDL.

Prozedur

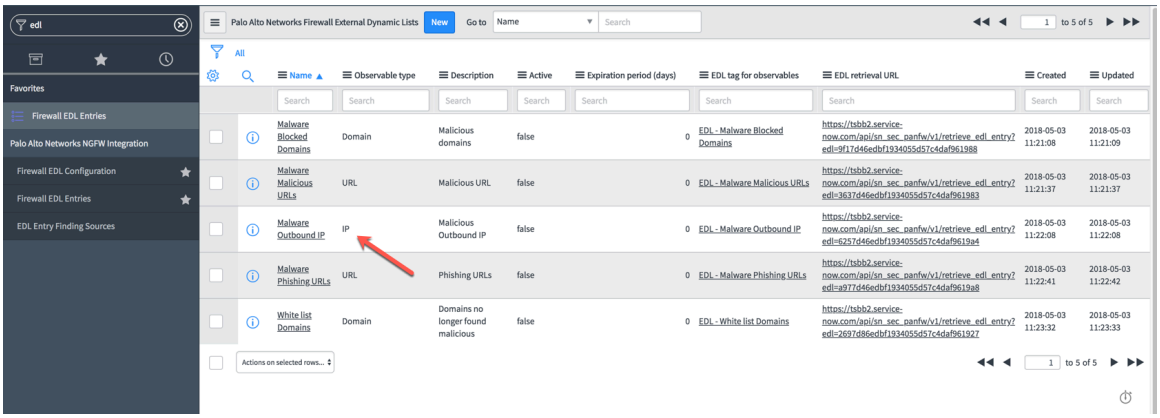
1. Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Konfiguration**an.



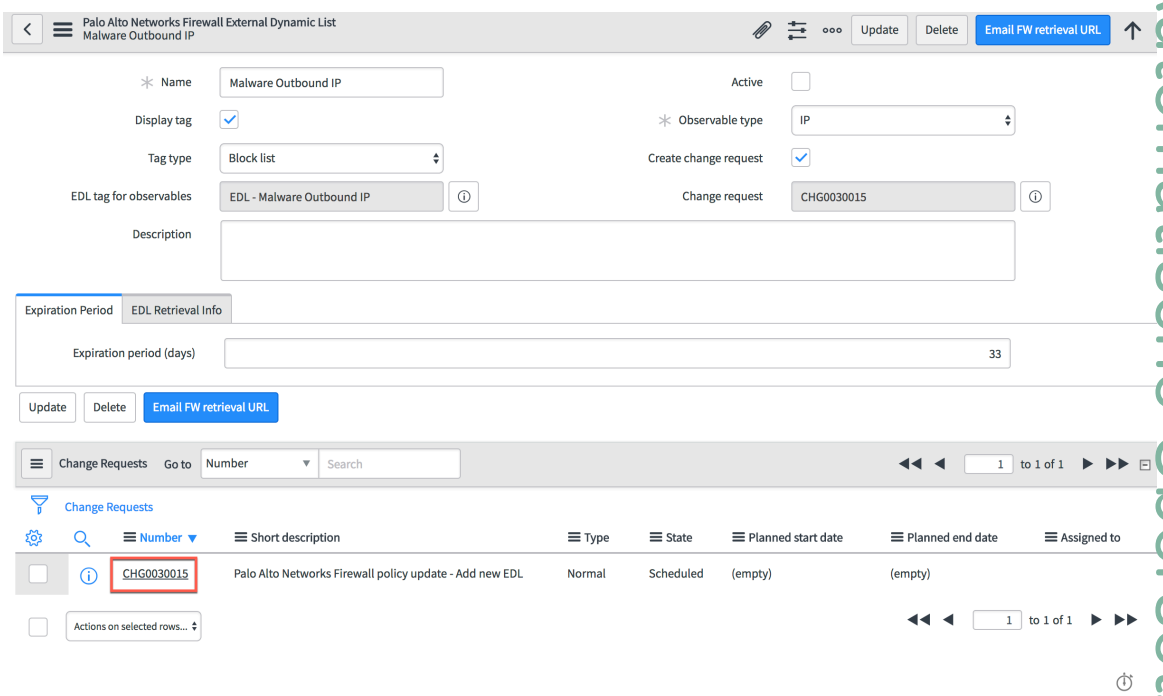
2. Wählen Sie das EDL-Modul aus, und klicken Sie im auf eine EDL **Name** Spalte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



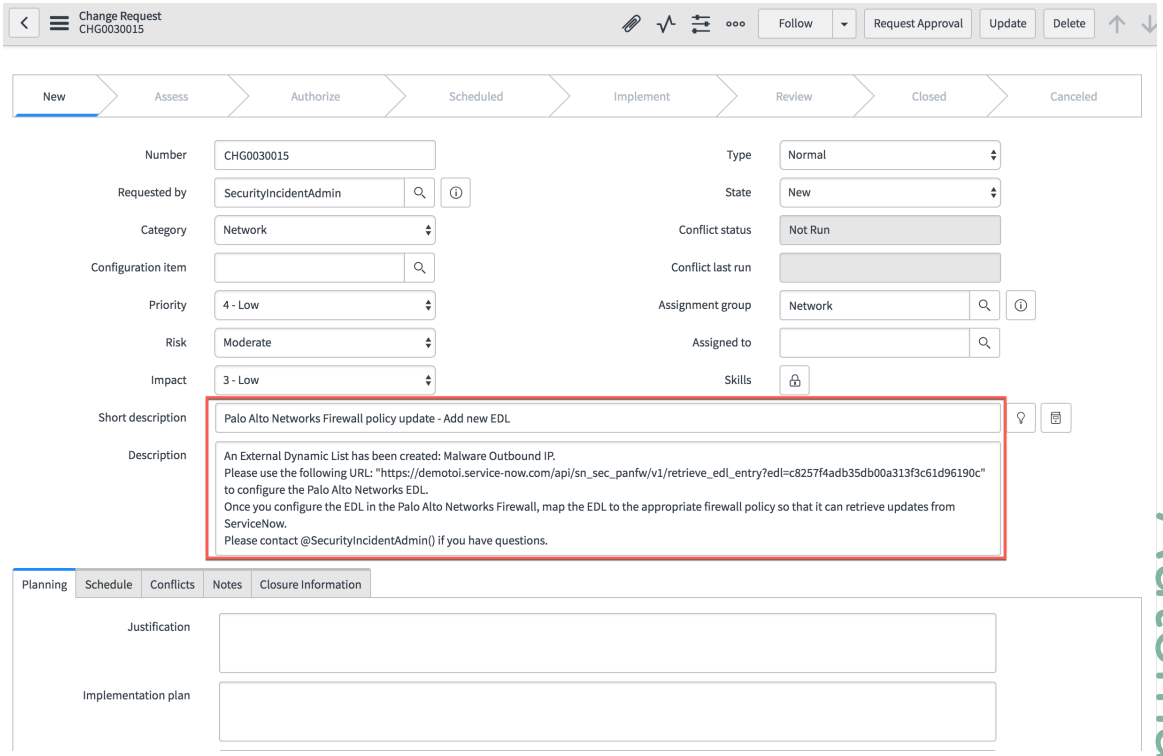
3. Klicken Sie im offenen EDL-Datensatz in der zugehörigen Liste Change-Anforderungen auf die Nummer der Change-Anforderung.



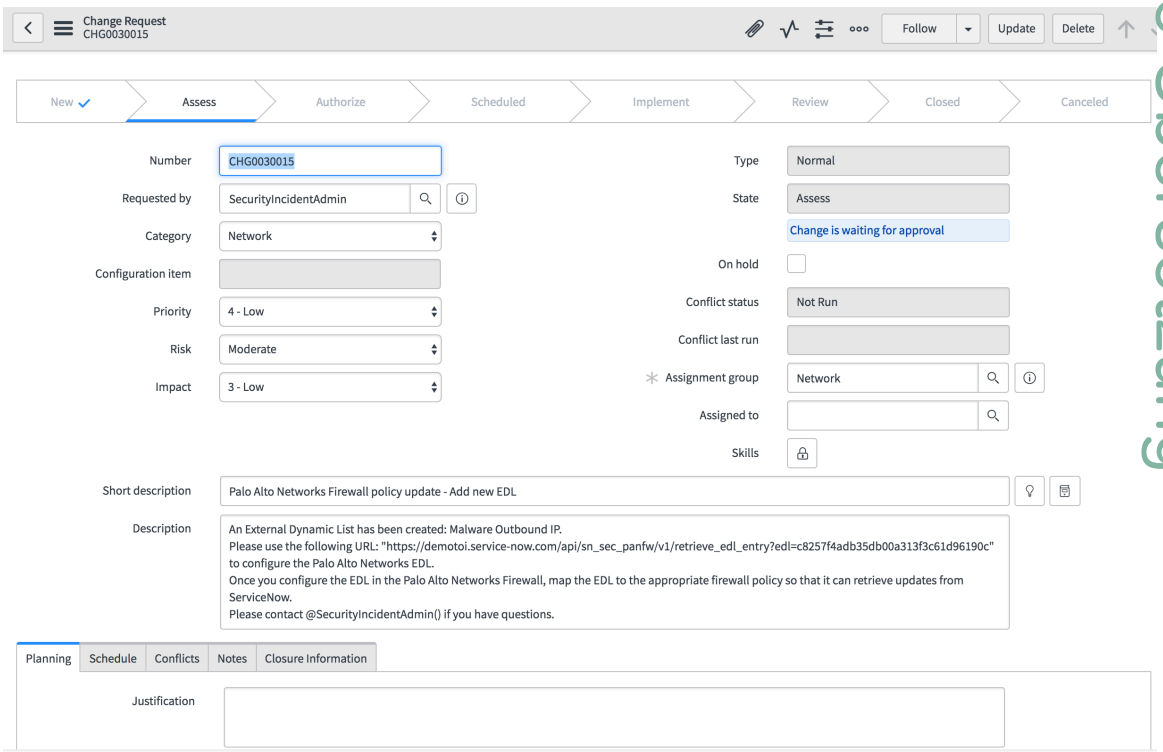
Der Change-Anforderungsdatensatz wird angezeigt. Die **Beschreibung** Feld listet die Abruf-URL auf, die zum Konfigurieren von verwendet wird Palo Alto Networks EDL. Details zum Zuordnen der EDL zum entsprechenden Palo Alto Networks Next-Generation Firewall Richtlinie ist ebenfalls enthalten. In **Kurzbeschreibung** Feld gibt ein Kommentar an, dass eine Anforderung zum Hinzufügen einer neuen EDL vorhanden ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie in der oberen rechten Ecke des Datensatzes auf **Genehmigung Anfordern** .
Der Status ändert sich in Bewerten, und es wird eine Meldung angezeigt, dass die Change-Anforderung auf Genehmigung wartet.

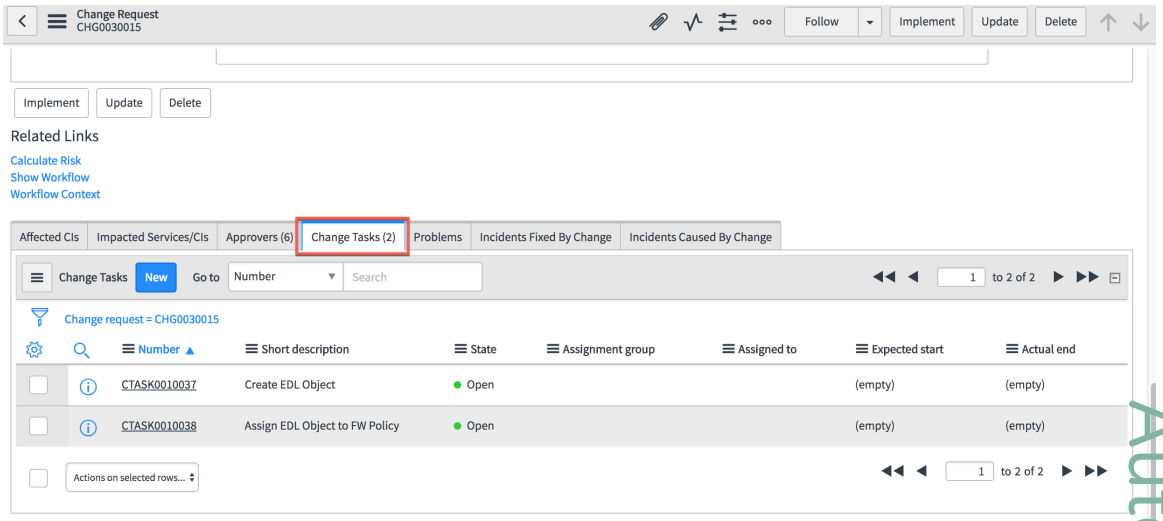


5. Um die Change-Anforderung abzuschließen und die EDL zu aktivieren, führen Sie die Schritte aus, um die Aufgaben zuzuweisen und die Change-Anforderung zu schließen.

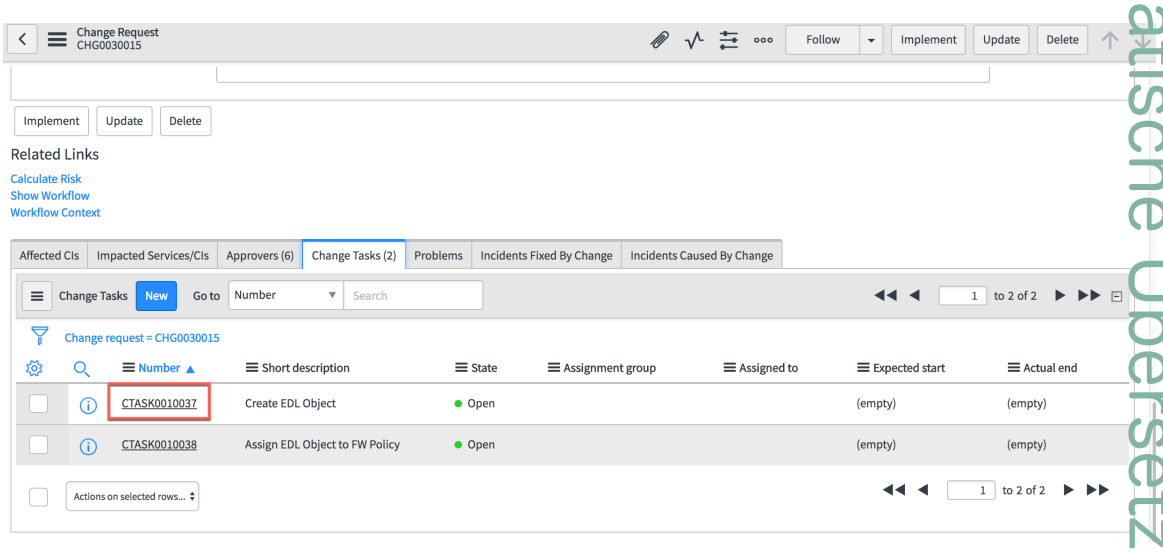
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wenn nicht angezeigt, öffnen Sie die Change-Anforderung, und wählen Sie aus **Change-Aufgaben** Registerkarte.



b. Klicken Sie auf die Aufgabe, die der Erstellung des EDL-Objekts zugeordnet ist, um es zu öffnen.



c. Weisen Sie im angezeigten Datensatz die Aufgabe zu Palo Alto Networks Firewall-Administrator, und klicken Sie auf **Aktualisieren** .
Der Firewall-Administrator wird benachrichtigt und erstellt das EDL-Objekt in der Palo Alto Networks Next-Generation Firewall.

Um das EDL-Objekt zu erstellen, die ServiceNow AI Platform Abruf-URL wird kopiert Palo Alto Networks Um **Externe Dynamische Listen** > **Listen Erstellen** > **Quelle**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

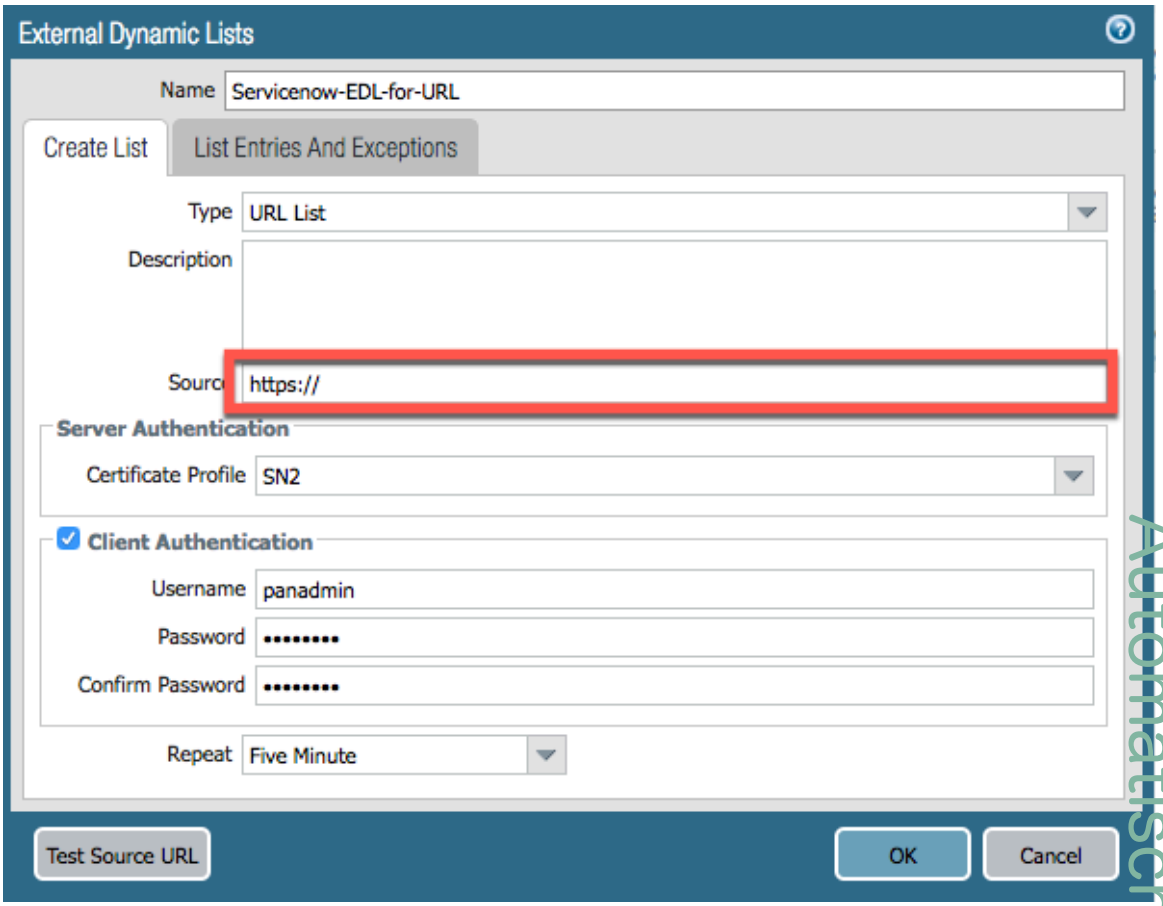


Image wird mit Berechtigung verwendet und ist PRIVILEGIERT und PROPRIETÄR.

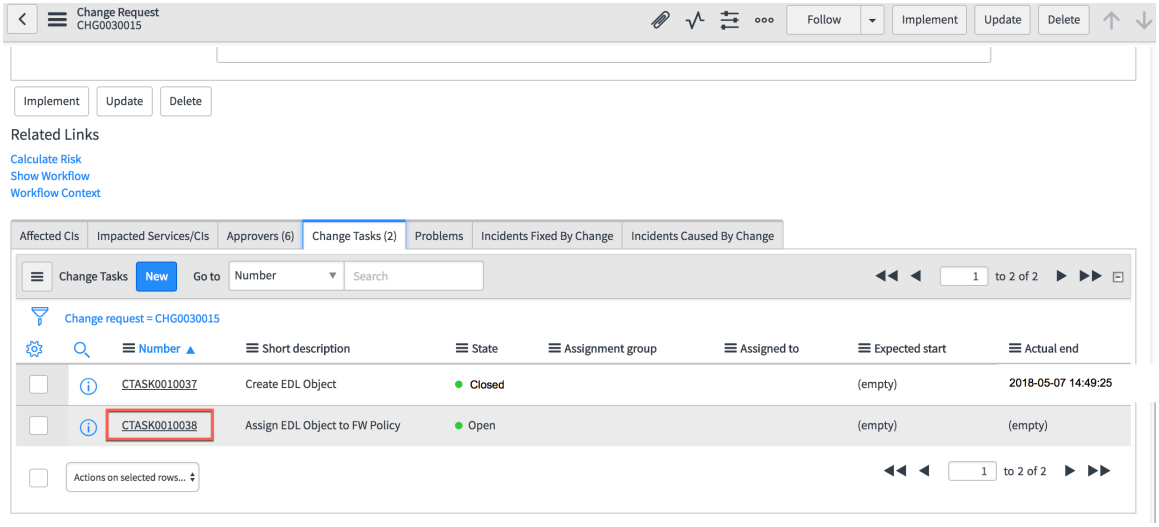
d. Nachdem Sie überprüft haben, dass das EDL-Objekt in erstellt wurde Palo Alto Networks, In ServiceNow AI Platform, Navigieren Sie zu der Change-Anforderung, die der Erstellung des EDL-Objekts zugeordnet ist, und klicken Sie auf **Schließen Sie die Aufgabe** .

Im Aufgabendatensatz für dieses Beispiel CTASK0010037 Wurde für diese Aufgabe geschlossen.

e. Navigieren Sie zur Registerkarte Change-Aufgaben, und klicken Sie auf die Aufgabe zum Zuweisen einer Firewall-Richtlinie zum EDL-Objekt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Status für CTASK0010037 Ist Geschlossen .

f. Öffnen Sie den Datensatz, und weisen Sie die nächste Aufgabe zu.

Nachdem die Aufgabe zugewiesen wurde, in Palo Alto Networks, Der Firewall-Administrator navigiert zu **Richtlinien** Registerkarte zum Zuweisen der Richtlinie.

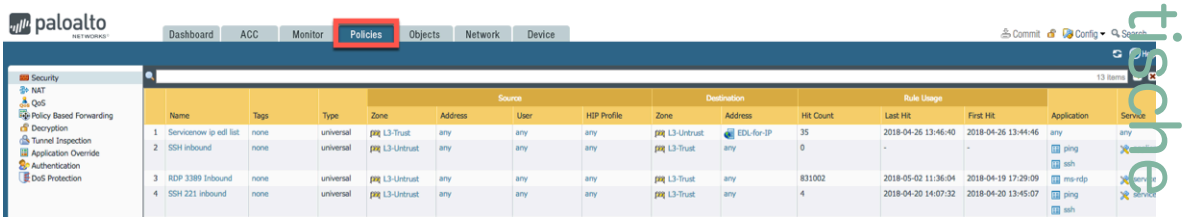


Image wird mit Berechtigung verwendet und ist PRIVILEGIERT und PROPRIETÄR.

g. In **Name** Suchen und klicken Sie auf die Sicherheitsrichtlinienregel, der Sie die EDL hinzufügen möchten, z. B. **ServiceNow-ip-edl-Liste** .

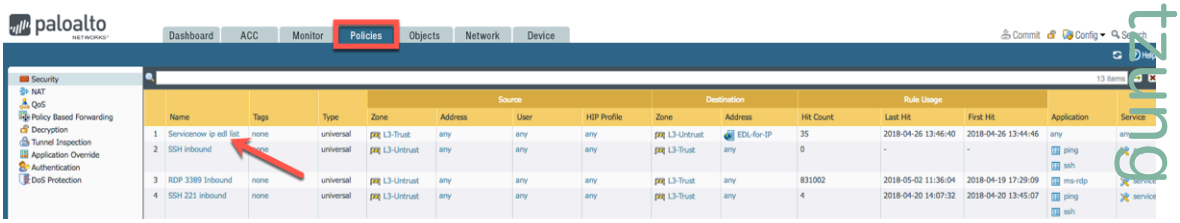


Image wird mit Berechtigung verwendet und ist PRIVILEGIERT und PROPRIETÄR.

h. Wählen Sie im Dialogfeld Sicherheitsrichtlinienregel die aus **Ziel** Registerkarte zum Hinzufügen einer EDL in **Zieladresse** Feld.

i. Klicken Sie auf , um alle verfügbaren EDLs anzuzeigen **Hinzufügen** Symbol.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

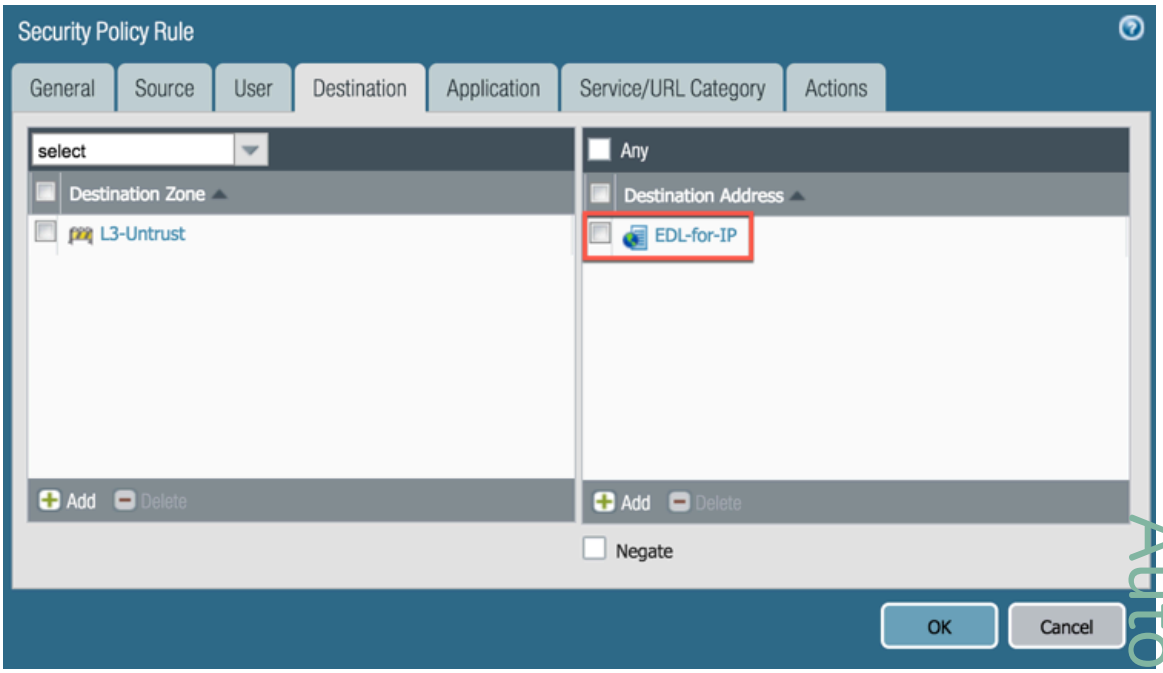


Image wird mit Berechtigung verwendet und ist PRIVILEGIERT und PROPRIETÄR.

j. Klicken Sie auf **OK**.

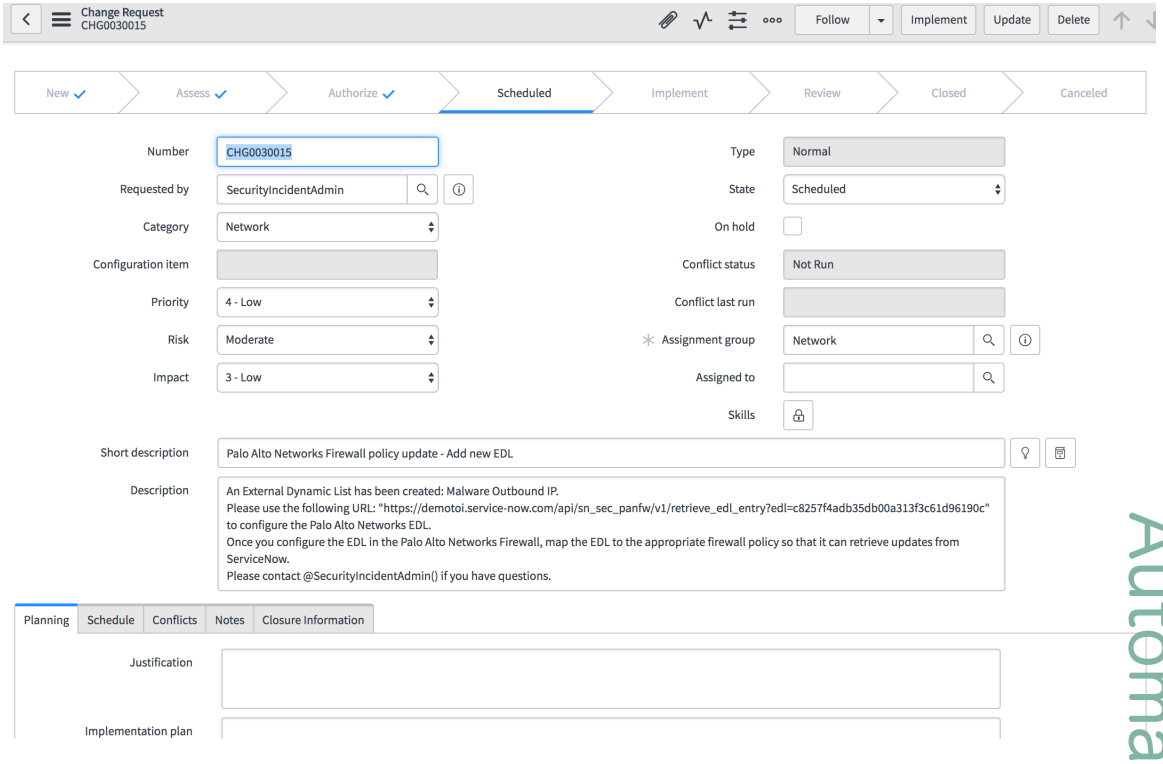
k. Nachdem Sie überprüft haben, dass das EDL-Objekt einer Sicherheitsrichtlinie zugewiesen wurde, in ServiceNow AI Platform, Navigieren Sie zur Change-Anforderung, öffnen Sie die Aufgabe, die der Zuweisung des EDL-Objekts zugeordnet ist, und klicken Sie auf **Schließen Sie die Aufgabe** . Nachdem beide Aufgaben geschlossen wurden, kann die Change-Anforderung genehmigt werden.

l. Klicken Sie im Change-Anforderungsdatensatz auf **Genehmiger** Zugehörige Liste, und wählen Sie ein Element in aus **Status** Spalte zum Öffnen der Anforderung, die zum Erstellen der EDL verwendet wird.

m. Klicken Sie im Formular „Genehmigungsanforderung öffnen“ auf **Genehmigen** .
Der Status der Change-Anforderung wird in geplant verschoben.

Automatische Übersetzung

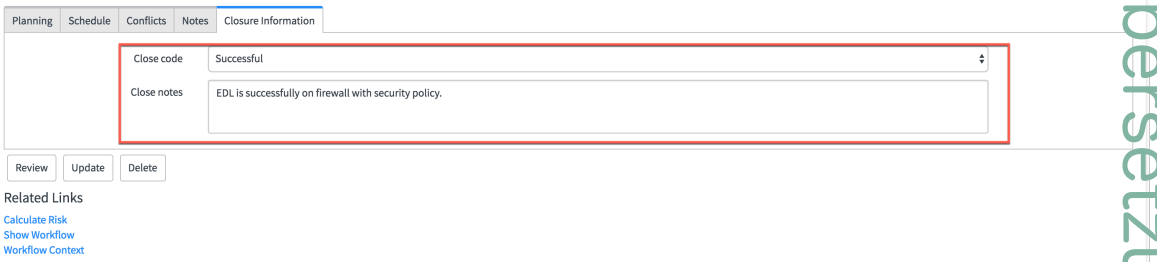
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



n. Klicken Sie auf **Implementieren**.

o. Klicken Sie auf **Abschlussinformationen** Registerkarte „Zugehörig“ und geben Sie Notizen ein, um die Anforderung zu schließen.

Ein Eintrag in diesem Feld ist erforderlich, um die Change-Anforderung zu schließen.

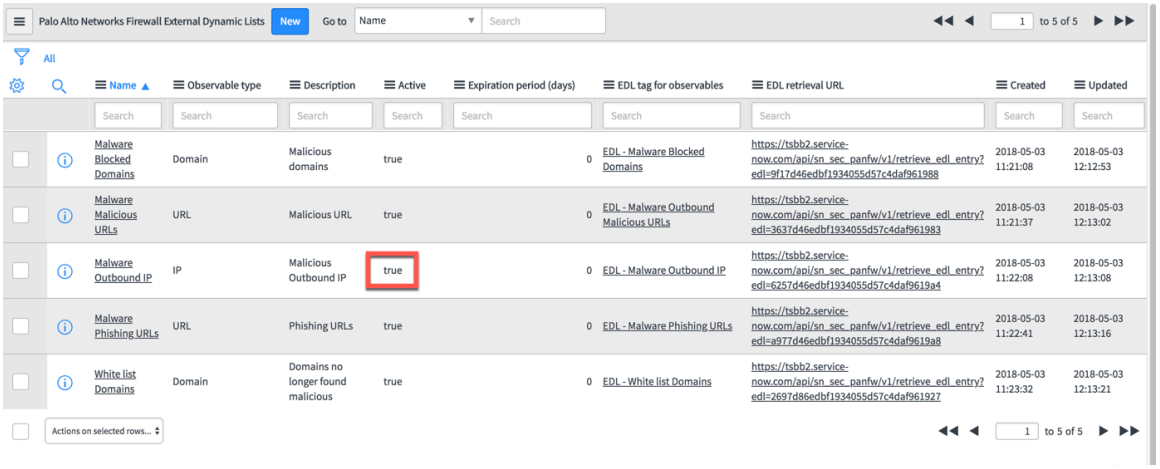


Nachdem die Change-Anforderung geschlossen wurde, wird die EDL automatisch aktiviert. Wenn Sie nicht verifiziert haben, dass die EDL aktiviert ist, navigieren Sie zu **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Konfiguration**an.

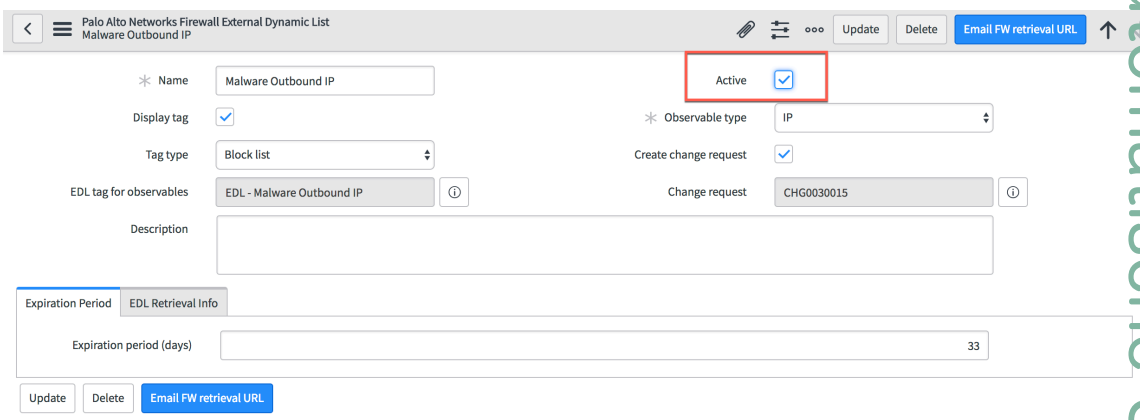
Beachten Sie in der Spalte aktiv in der Liste, dass der Status für die EDL (Wahr).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Klicken Sie in der Spalte Name auf den EDL-Namen, und beachten Sie im offenen Datensatz, dass **Aktiv** Das Kontrollkästchen ist ebenfalls aktiviert.



Die EDL ist jetzt bereit, EDL-Einträge zu akzeptieren.

Nächste Maßnahme

Übermitteln Sie EDL-Einträge aus einem Security Incident oder aus der Blockliste.

Übermitteln Sie EDL-Einträge aus einem Security Incident-Datensatz für Palo Alto Networks Next-Generation Firewall

Erkennbare Elemente, die an einen Security Incident-Datensatz angehängt sind, werden als EDL-Einträge (External Dynamic List) an EDLs übermittelt. Ein Genehmigungsprozess für EDL-Einträge ist Teil des vorkonfigurierten Workflows. Die Firewall importiert EDL-Einträge – IP-Adressen, URLs, Domänen –, die in EDL-Listen enthalten sind, und erzwingt die Richtlinie.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst zum Senden von EDL-Einträgen. Zum Genehmigen von EDL-Einträgen: Die Genehmigung ist standardmäßig sn_si.admin zugewiesen, diese Berechtigung kann jedoch nach Bedarf von Ihrer Organisation zugewiesen werden.

Warum und wann dieser Vorgang ausgeführt wird

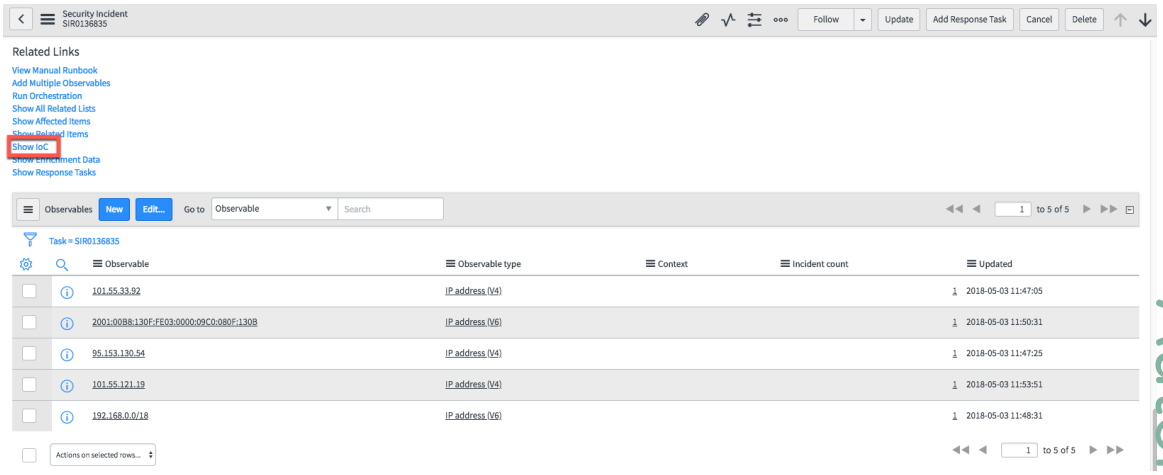
Anwender mit der Rolle „sn_si.Analyst“ übermitteln EDL-Einträge, indem sie eine Blockierung für erkennbare Elemente anfordern, die an einen Security Incident-Datensatz angehängt sind. Nach der Übermittlung wird ein EDL-Eintrag mit dem Status Ausstehend generiert und zur Genehmigung gesendet. Das folgende Beispiel zeigt eine Blockanforderung für ein erkennbares URL-Element.

Automatische Übersetzung

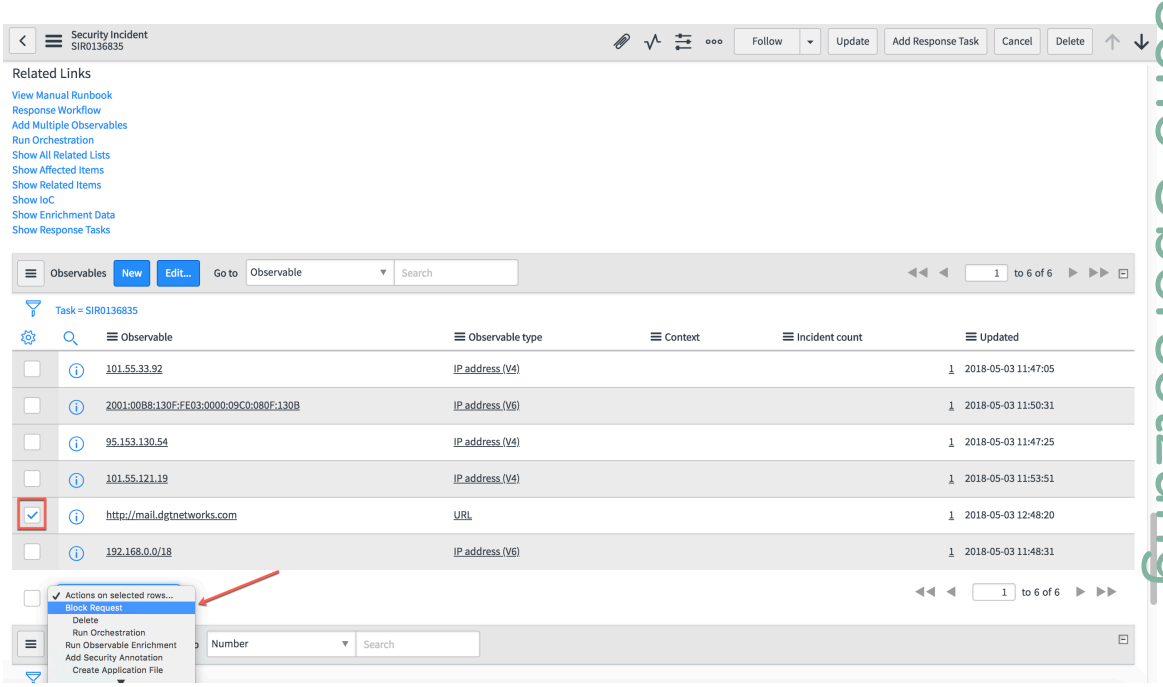
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**, Und klicken Sie auf einen Security Incident-Datensatz, um ihn zu öffnen.
2. Klicken Sie auf **IOC anzeigen** Zugehöriger Link.



3. Wählen Sie in der zugehörigen Liste erkennbare Elemente die erkennbaren Elemente aus, die Sie blockieren möchten, und aus **Aktionen für ausgewählte Zeilen** Liste, wählen Sie aus **Anforderung Blockieren** .

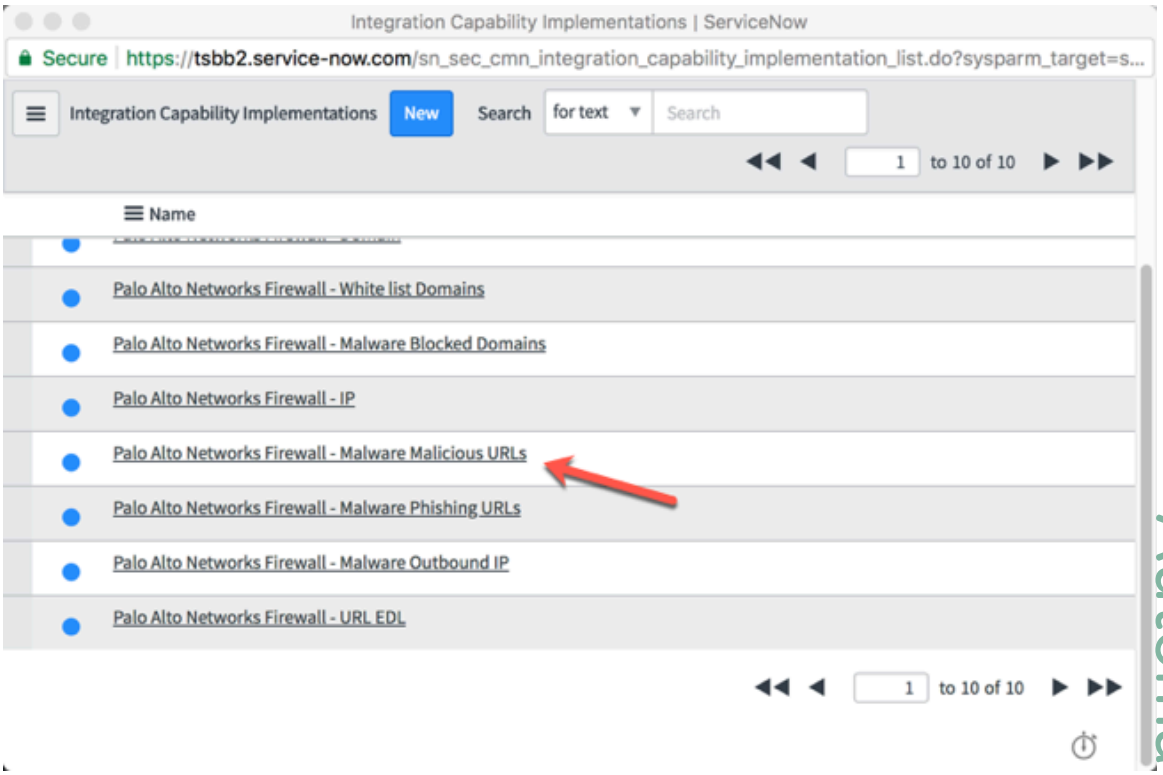


4. Klicken Sie im angezeigten Dialogfeld auf das Suchsymbol ( ).
5. Wählen Sie in der angezeigten Liste die EDL aus, an die Sie diesen Eintrag anhängen möchten.

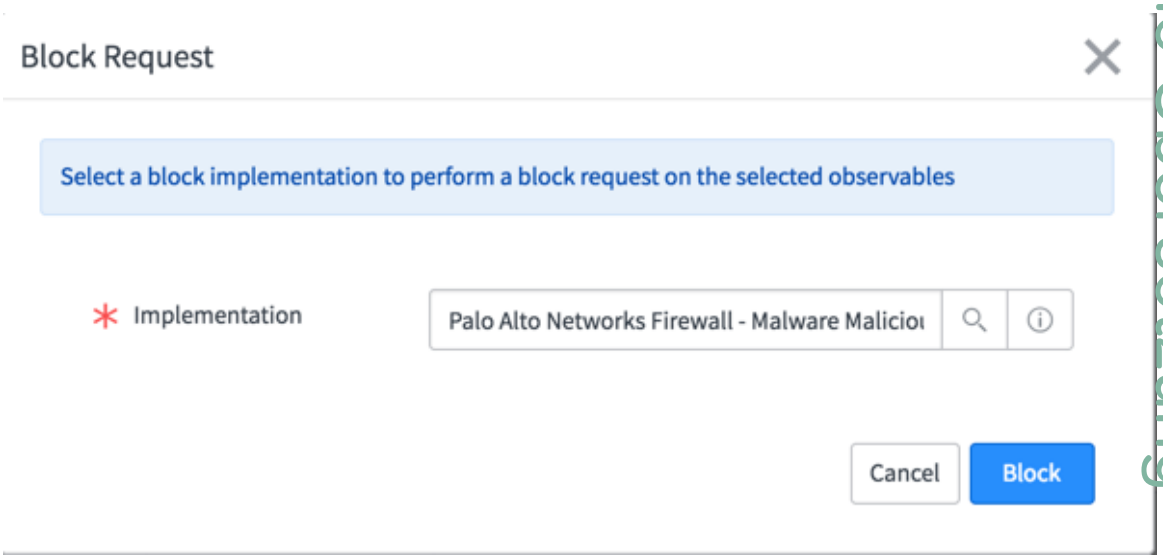
Hinweis:
In diesem Beispiel muss der Eintrag „erkennbarer Typ“ (URL) mit dem erkennbaren EDL-Typ (URL) übereinstimmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



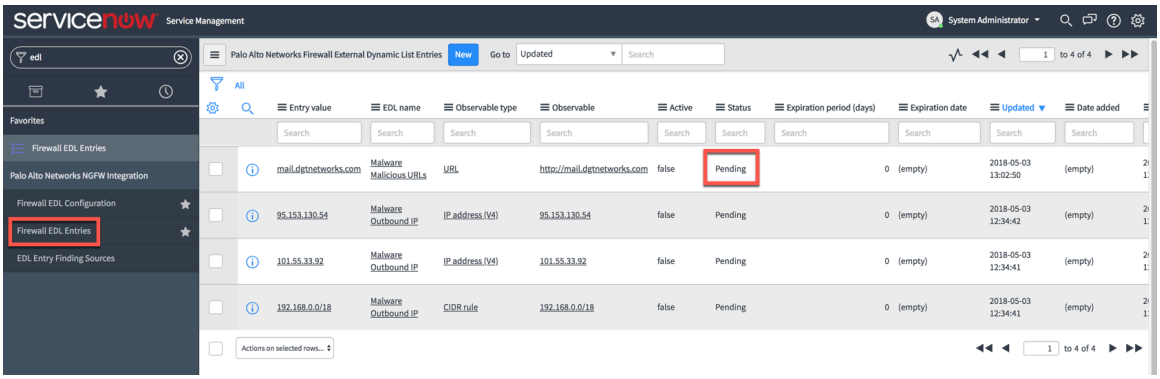
6. Im Dialogfeld „Blockieranforderung“ mit dem EDL-Namen, der in angezeigt wird **Implementierung** Feld klicken Sie auf **Blockieren** .



7. Navigieren zu **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Einträge** Und klicken Sie auf **Firewall-EDL-Einträge** .

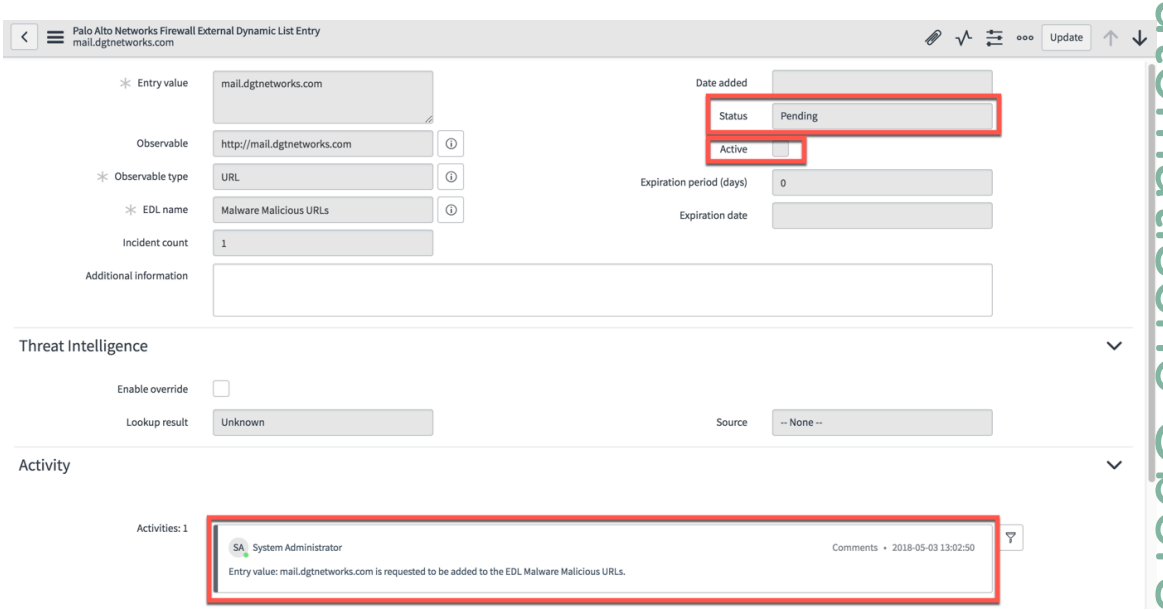
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Klicken Sie in der Liste „externe dynamische Listeneinträge der Palo Alto Networks-Firewall“ auf Ihr erkennbares Element im **Eingabewert** Spalte zum Öffnen des Datensatzes.

In diesem Beispiel der Datensatz für **mail.dgtnetworks.com** Wird angezeigt.

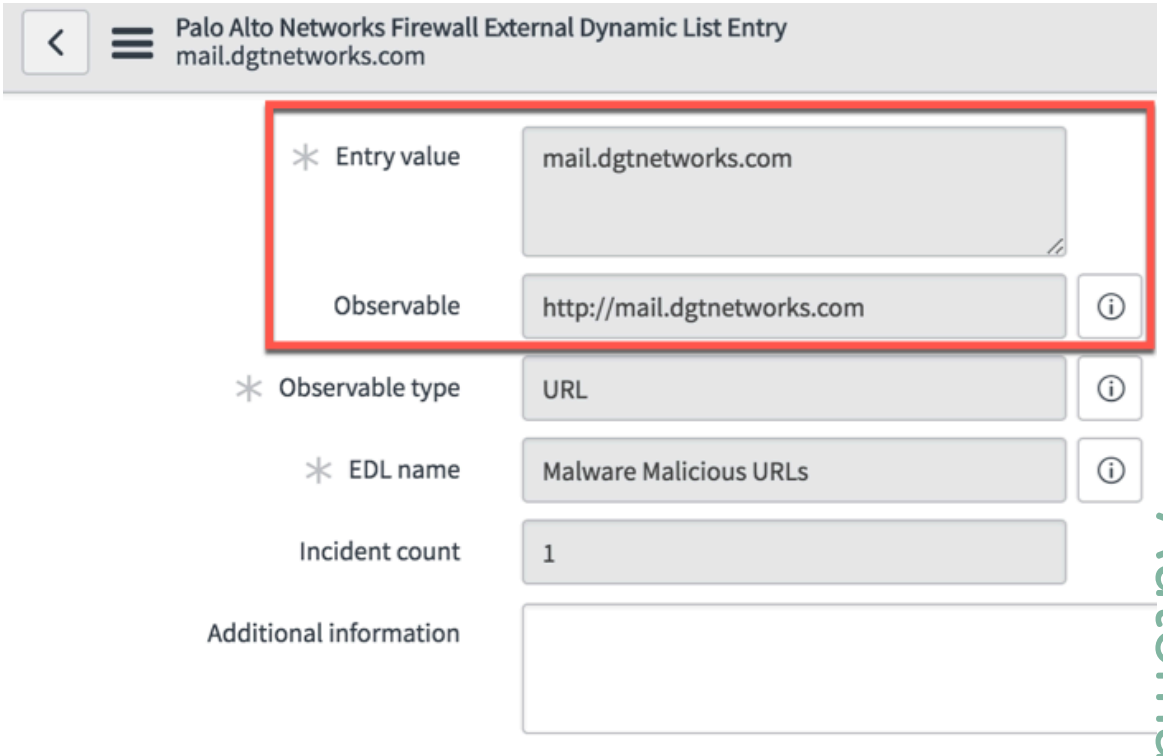


Der Status ist Ausstehend, das Kontrollkästchen aktiv ist deaktiviert, und die Arbeitsnotizen zeigen an, dass eine Anforderung zum Hinzufügen des erkennbaren Elements vorhanden ist. Diese EDL-Eintragsanforderung ist bereit zur Genehmigung.

Die Felder „Eintragswert“ und „erkennbares Element“ zeigen verschiedene Formate für das erkennbare URL-Element an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Symbol neben dem Erkennbares Element Das Feld ist ein Link zu ServiceNow AI Platform® Tabelle des erkennbaren Elements.

Der Wert in Erkennbares Element Feld (http://mail.dgtnetworks.com) Verknüpft mit der Tabelle des erkennbaren Elements und stimmt mit dem Format überein, das von übernommen wurde Security Incident Response Incident-auslösendes Ereignis.

Die ServiceNow AI Platform® Kann EDL-Einträge automatisch so ändern, dass sie mit kompatibel sind Palo Alto Networks EDL-URL-Format.

In diesem Beispiel wurde das erkennbare Element mit dem Protokoll http:// (http://mail.dgtnetworks.com), und dieses Format wird im Feld erkennbares Element angezeigt. Das HTTP://-Protokoll wird vom automatisch aus dem erkennbaren Element entfernt ServiceNow AI Platform® Daher ist es kompatibel mit Palo Alto Networks Und können abgerufen werden. Infolgedessen mail.dgtnetworks.com Wird in angezeigt Eingabewert Feld.

Nächste Maßnahme

Genehmigen Sie EDL-Einträge.

Zugehörige Informationen

EDL-Eintragsausnahmen für Palo Alto Networks Next-Generation Firewall

Übermitteln Sie EDL-Einträge aus der Blockliste für Palo Alto Networks Next-Generation Firewall

Für erkennbare Elemente, die als schädlich eingestuft und keinem bestimmten zugeordnet sind ServiceNow AI Platform Security Incident senden Sie EDL-Einträge (External Dynamic List) aus der Blockliste.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Automatische Übersetzung

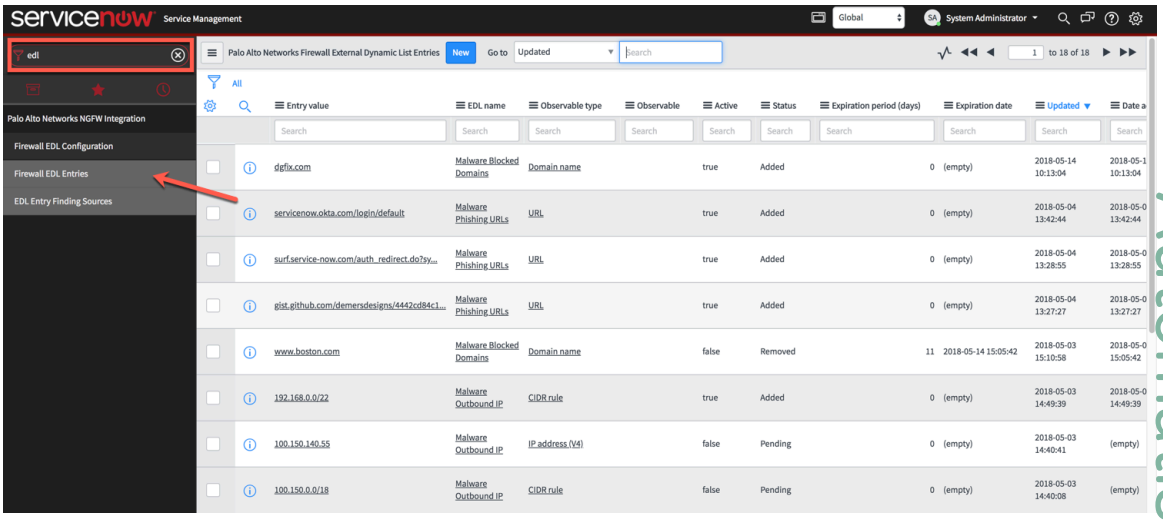
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein erkennbares Element blockieren möchten, das Sie als böswillig eingestuft haben, oder zulassen möchten, dass ein erkennbares Element nicht böswillig ist und das erkennbare Element keinem bestimmten zugeordnet ist ServiceNow AI Platform Security Incident-Datensatz senden Sie EDL-Einträge direkt aus der Blockliste. Beispiele für diese Arten von EDL-Einträgen können URLs oder Domänen für bestimmte Sites sein.

Prozedur

1. Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Einträge**an.



2. Klicken Sie auf **Firewall-EDL-Einträge** Modul.
3. Klicken Sie in der Liste „externe dynamische Listeneinträge der Palo Alto Networks-Firewall“ auf **Neu** .
4. Im neuen Datensatz, der angezeigt wird, in **Eingabewert** Geben Sie einen Wert für Ihr erkennbares Element ein.
   Die beiden möglichen Ergebnisse dieses Eintrags:

   Die verbleibenden Felder im Formular werden automatisch ausgefüllt.

   Ein übereinstimmendes erkennbares Element wurde gefunden, und es wird eine Meldung angezeigt, dass ein übereinstimmendes erkennbares Element vorhanden ist. Wählen Sie die EDL aus, an die Sie diesen Eintrag anhängen möchten, und klicken Sie auf **Übermitteln** . Wählen Sie die EDL aus, an die Sie diesen Eintrag anhängen möchten, bevor Sie den Ablaufzeitraum festlegen.

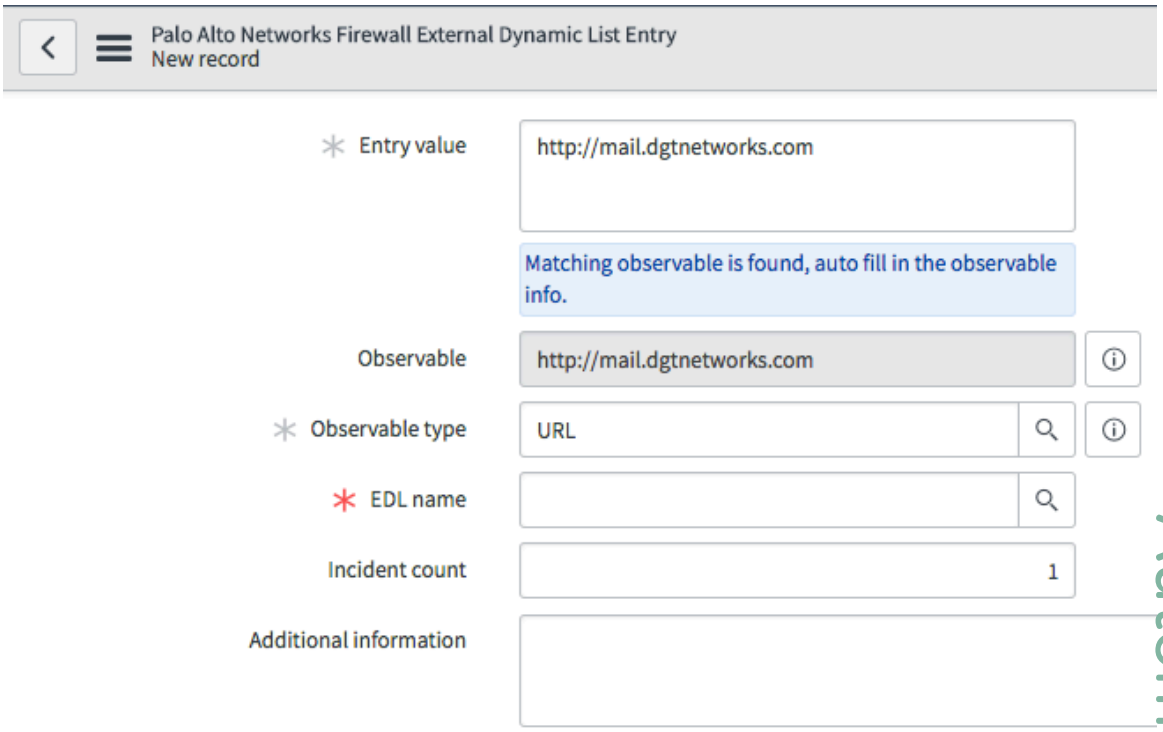
   Es wird eine Nachricht angezeigt, die Sie anweist, das Formular auszufüllen.

   Es wurde kein übereinstimmendes erkennbares Element gefunden, und Sie müssen das Formular ausfüllen. Wählen Sie nach Abschluss die EDL aus, an die Sie das erkennbare Element anhängen möchten, und klicken Sie auf **Übermitteln** . Ein Datensatz eines erkennbaren Elements wird erstellt.

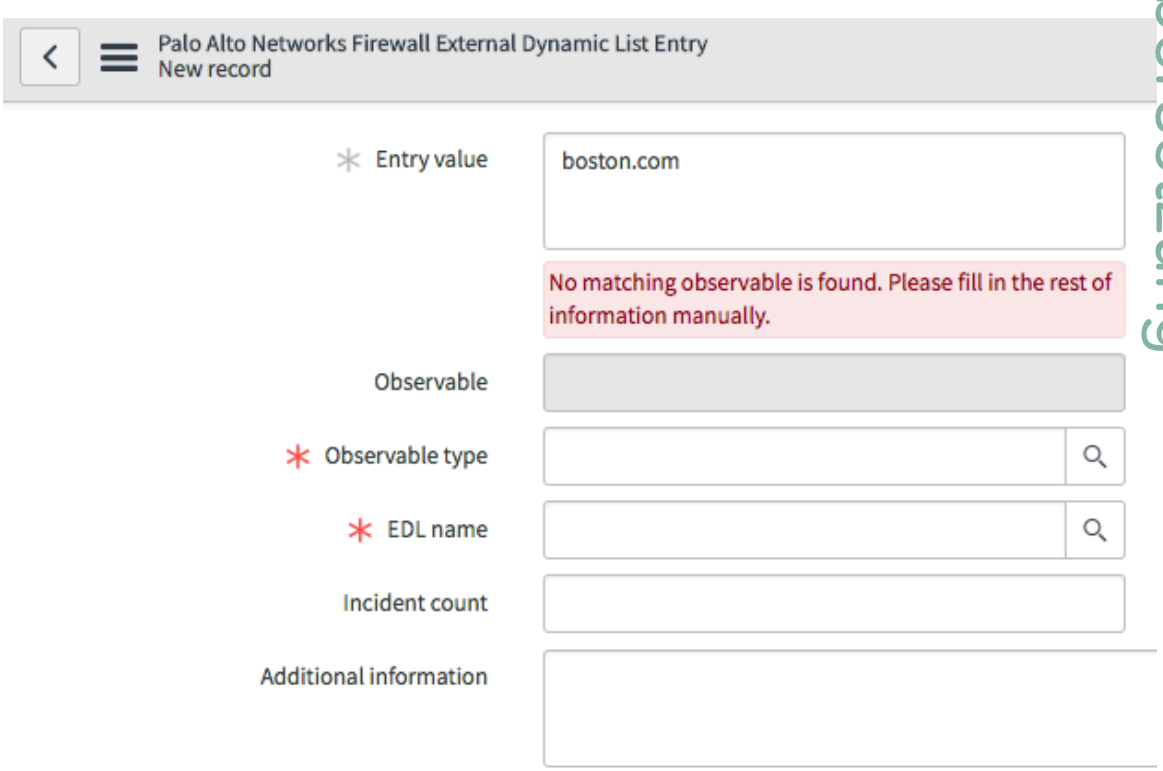
   Die folgende Abbildung zeigt ein Beispiel für ein vorhandenes erkennbares Domänenelement und wie die Felder automatisch ausgefüllt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



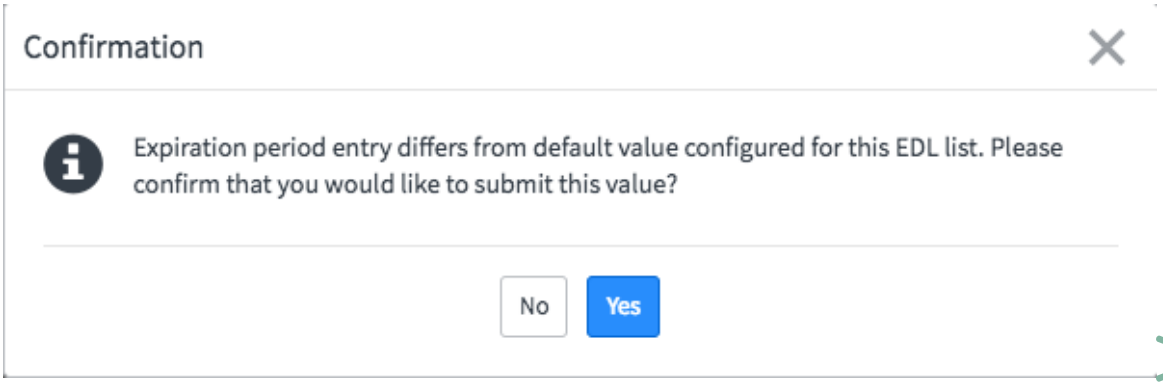
5. Klicken Sie auf das Suchsymbol, um die EDL auszuwählen, an die Sie den Eintrag anhängen möchten.
6. Klicken Sie auf **Absenden**.
   Wenn Sie in Ihrem Workflow eine E-Mail-Genehmigung konfiguriert haben, wird eine Genehmigungs-E-Mail-Anforderung gesendet.
7. Wenn eine Nachricht angezeigt wird, in der Sie aufgefordert werden, den Rest der Informationen manuell auszufüllen, füllen Sie die Felder aus.



Automatische Übersetzung

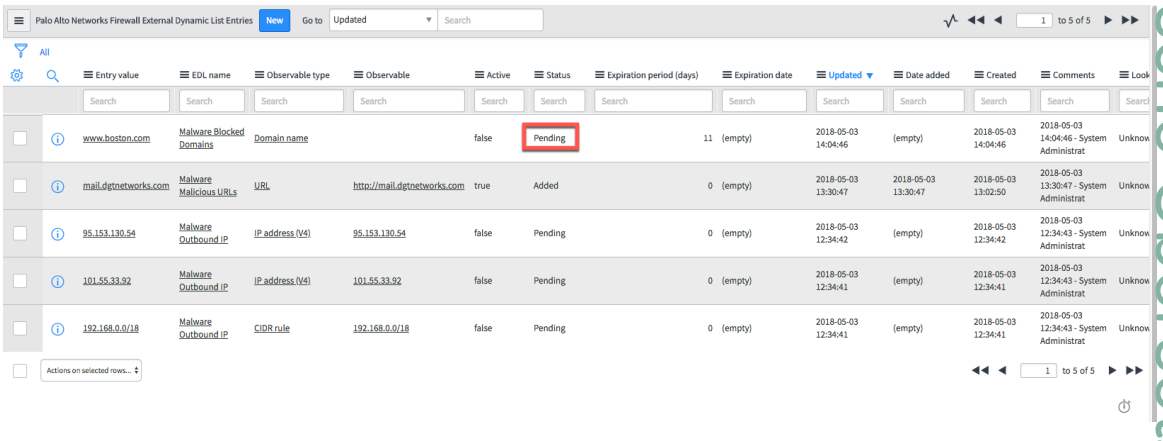
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf **Absenden**.
   Wenn Sie den standardmäßigen Ablaufzeitraum des EDL-Eintrags geändert haben, wird ein Bestätigungsdialogfeld für Warnungen angezeigt, das angibt, dass sich der Zeitraum vom ausgewählten EDL unterscheidet.



9. Wählen Sie eine Option aus, um den Ablaufzeitraum zu konfigurieren.

10. Wenn nicht angezeigt, navigieren Sie zu **Externe Dynamische Listeneinträge Der Palo Alto Networks-Firewall** Listen Sie auf, und beachten Sie, dass der Status für den Eintrag „Ausstehend“ lautet.



Der Eintrag ist jetzt zur Genehmigung bereit.

Nächste Maßnahme
Genehmigen Sie EDL-Einträge.

Zugehörige Informationen

EDL-Eintragsausnahmen für Palo Alto Networks Next-Generation Firewall

Genehmigen Sie EDL-Einträge

Ein Genehmigungsprozess für EDL-Einträge (External Dynamic List) ist Teil des vorkonfigurierten Workflows. Sie genehmigen EDL-Einträge, bevor die Einträge für EDLs aktiviert werden. Sobald Sie den EDL-Eintrag genehmigen, ruft die Firewall den Eintrag ab, und Ihr erkennbares Element wird von diesem Punkt an blockiert.

Vorbereitungen
Erforderliche Rolle: Die Genehmigung für EDL-Einträge ist standardmäßig sn_si.admin zugewiesen, diese Berechtigung kann jedoch nach Bedarf von Ihrer Organisation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugewiesen werden. Im folgenden Beispiel ServiceNow AI Platform administrator hat Genehmigungsberechtigung.

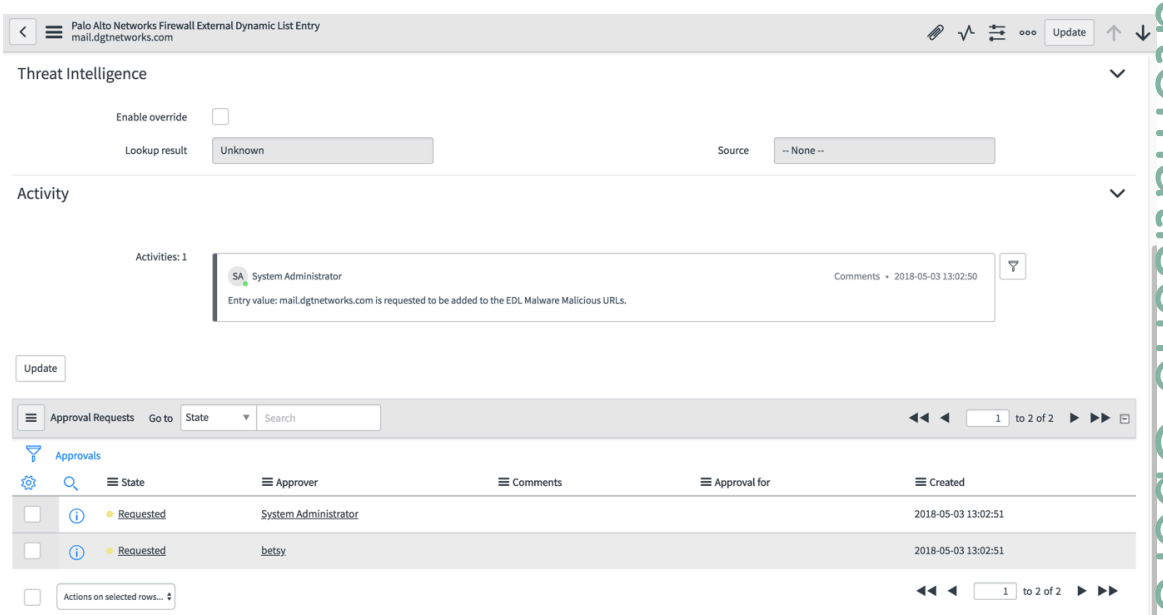
Warum und wann dieser Vorgang ausgeführt wird

Wenn der Genehmigungsprozess aktiviert ist, wird ein EDL-Eintrag erst dann in der EDL aktiviert oder deaktiviert, wenn er genehmigt wurde.

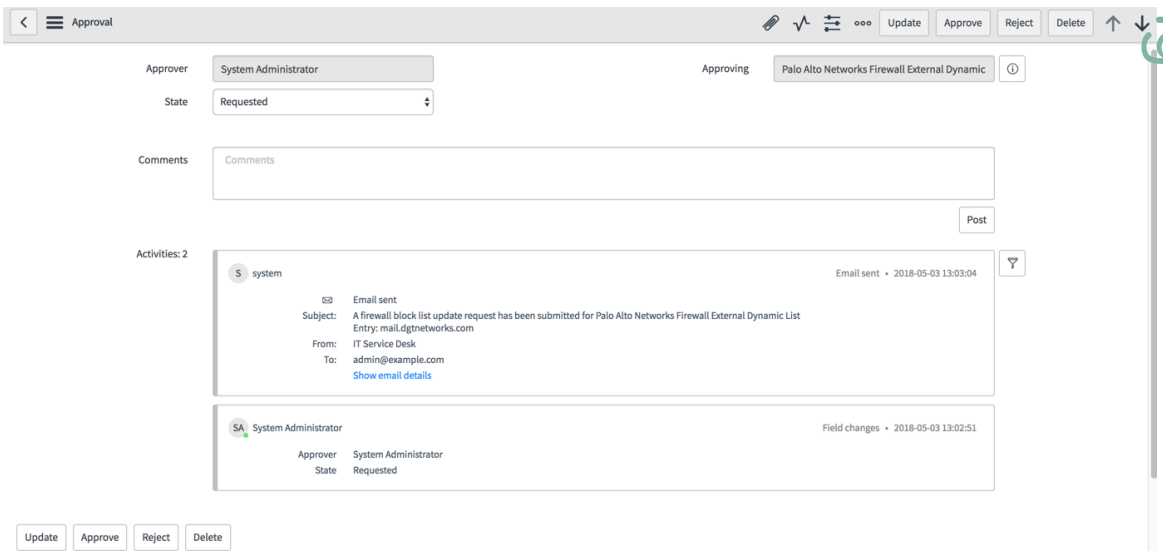
Prozedur

1. Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Einträge** Und öffnen Sie den EDL-Datensatz.
2. Scrollen Sie im EDL-Datensatz zum Abschnitt Genehmigungsanforderungen.

Hinweis:
Wenn Sie Formulare mit Registerkarten in Systemeinstellungen ausgewählt haben, wird der Abschnitt als Registerkarte im Datensatz angezeigt.



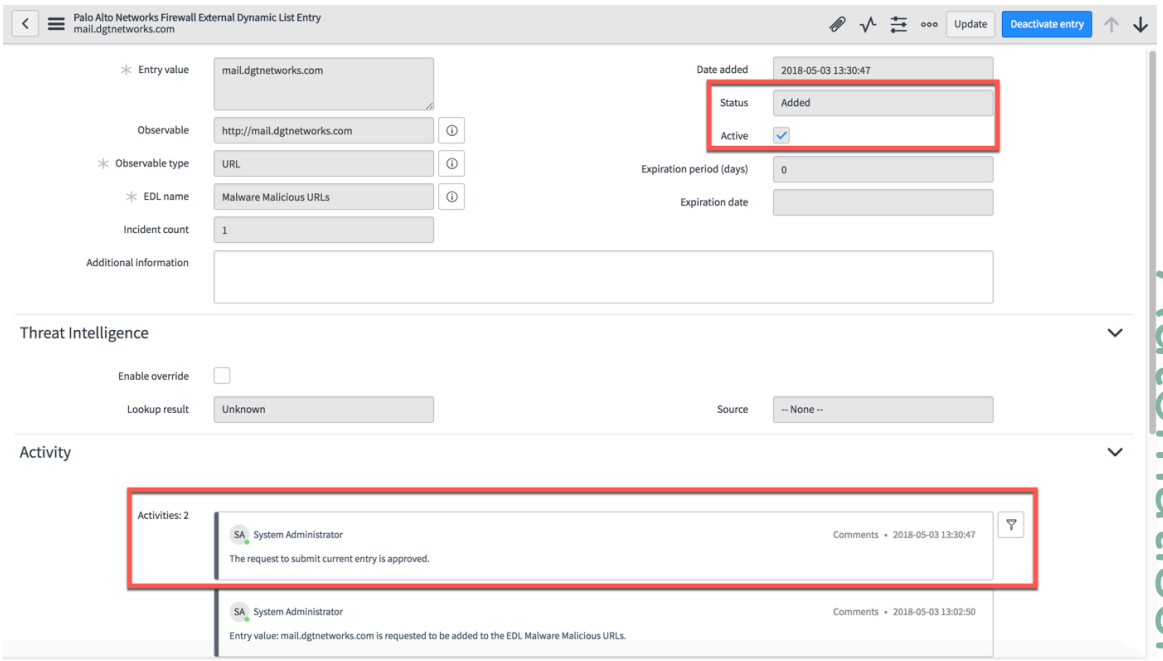
3. Klicken Sie unter Genehmigungsanforderungen auf ein Element in der **Status** Spalte zum Öffnen.
Der Genehmigungsdatensatz wird angezeigt.



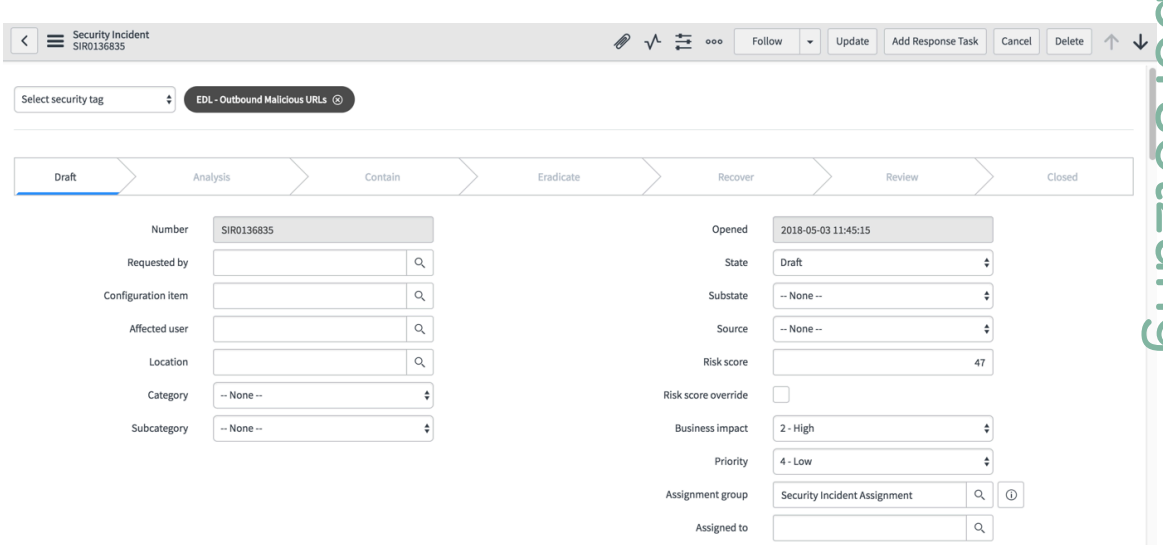
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie eine Option zum Genehmigen des EDL-Eintrags aus.
   Nachdem Sie den EDL-Eintrag genehmigt haben und er aktiviert ist, wird der Palo Alto Networks Next-Generation Firewall Ruft den EDL-Eintrag nach dem nächsten Abrufintervall ab. Nachdem der Eintrag abgerufen wurde, wird das erkennbare Element von diesem Punkt an blockiert. Beachten Sie in der folgenden Abbildung, dass das Kontrollkästchen aktiv aktiviert ist, der Status hinzugefügt wird und die Arbeitsnotizen anzeigen, dass die Anforderung genehmigt wurde.



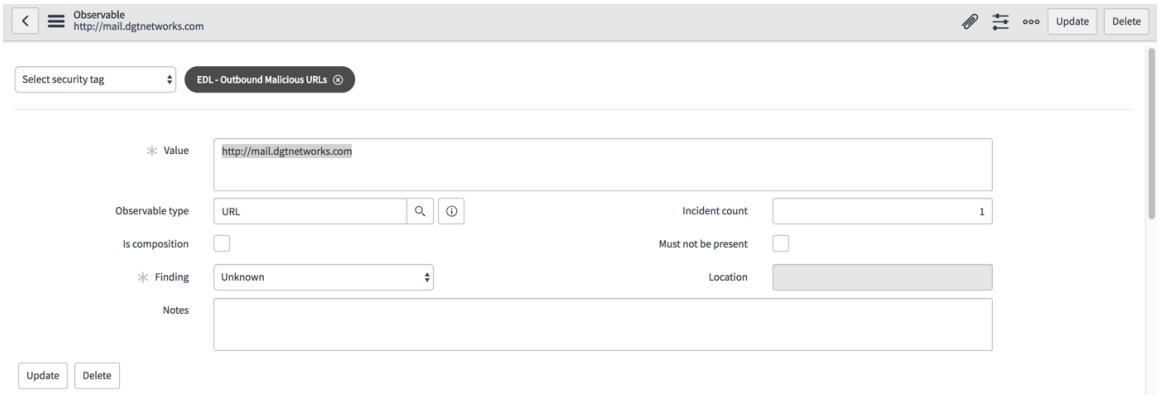
Nachdem der EDL-Eintrag genehmigt und aktiviert wurde, wird der Security Incident-Datensatz mit einem Sicherheits-Tag markiert. Das Tag wird oben im Datensatz angezeigt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Sicherheits-Tag wird auch im Datensatz des erkennbaren Elements angezeigt.



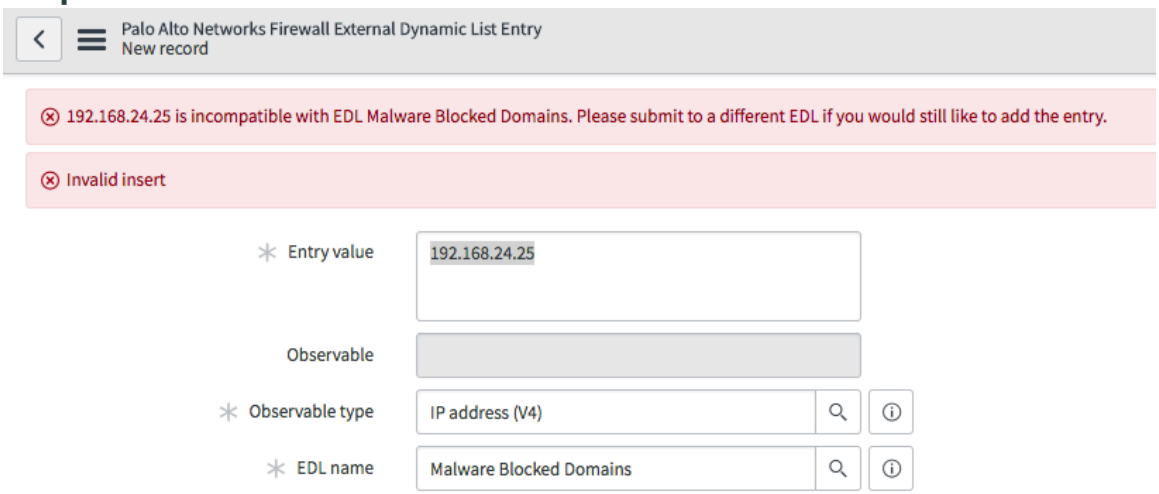
EDL-Eintragsausnahmen für Palo Alto Networks Next-Generation Firewall

Es gibt Einschränkungen für das Hinzufügen von EDL-Einträgen (External Dynamic List) zu EDLs. Wenn beim Versuch, EDL-Einträge zu EDLs hinzuzufügen, Duplikat-, Kompatibilitäts- oder CIDR-Konflikte (Classless Inter-Domain Routing) vorhanden sind, werden Fehlermeldungen angezeigt, die Ihnen helfen, diese Fehler zu beheben.

Kompatibilitätsausnahme

Jede EDL akzeptiert nur Einträge, die mit ihrem erkennbaren Typ kompatibel sind. Wenn Sie eine Domänen-EDL erstellen und versuchen, eine erkennbare IP-Adresse anzuhängen, wird eine inkompatible Fehlermeldung angezeigt. Beispielsweise kann eine Domänen-EDL nur erkennbare Domänenelemente akzeptieren, wie in der folgenden Abbildung dargestellt.

Kompatibilitätsfehler

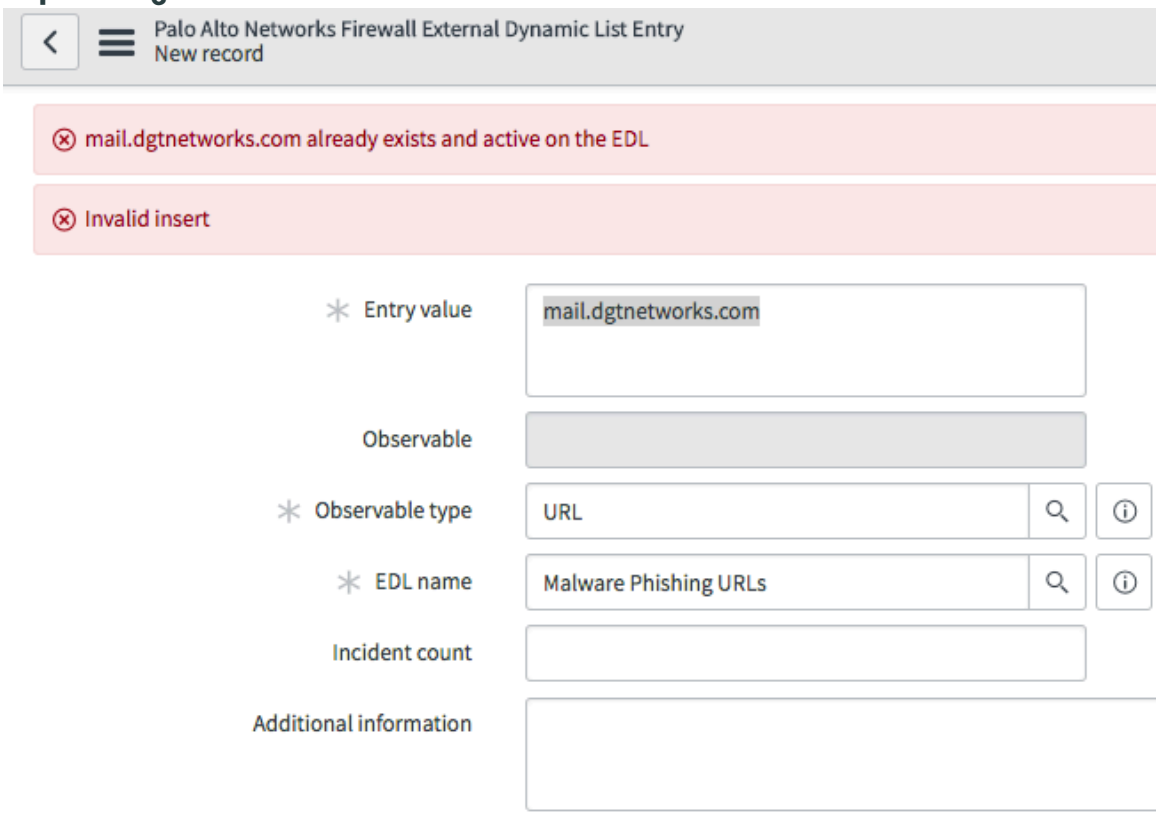


Duplizierungsausnahme

Ein erkennbares Element kann nicht für mehrere EDLs desselben erkennbaren Elements-Typs aktiviert werden. Wenn ein erkennbares URL-Element bereits in einer URL-EDL aktiviert ist und Sie versuchen, dasselbe erkennbare Element in einer Phishing-URL-EDL zu aktivieren, wird eine Duplikationsfehlermeldung angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Duplizierungsfehler

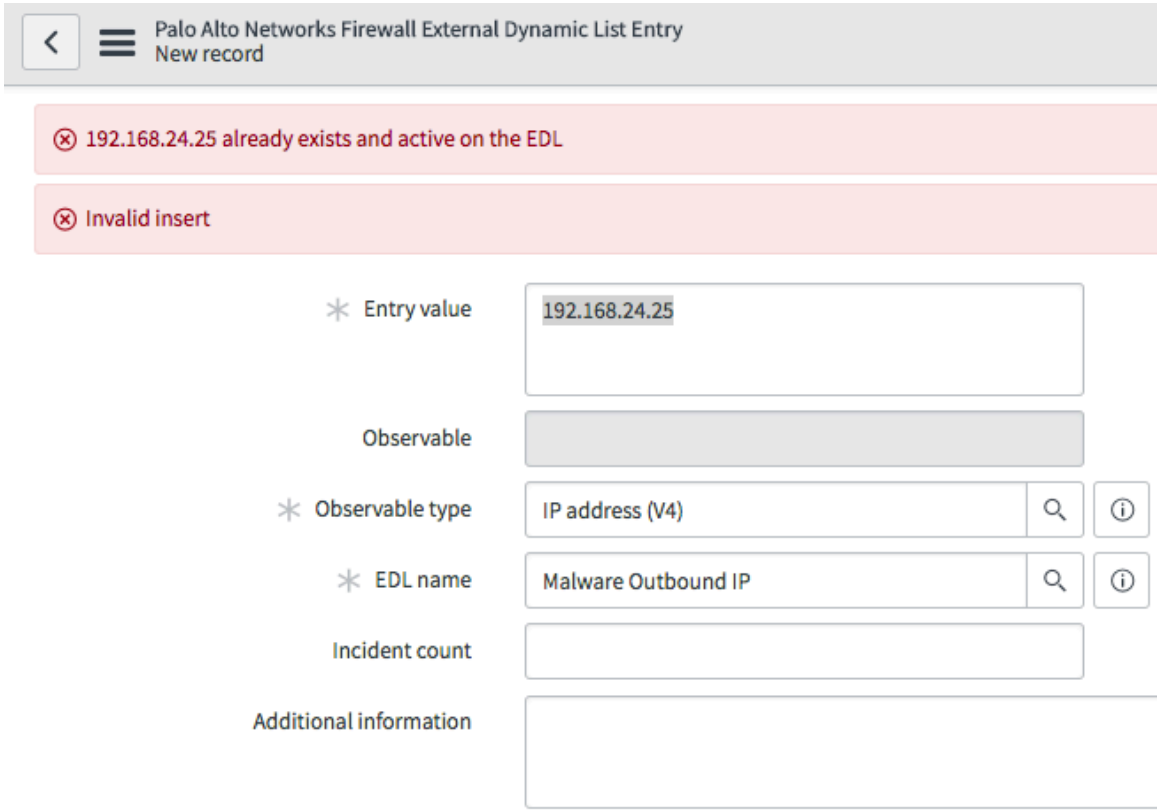


CIDR-Ausnahme (Classless Inter-Domain Routing)

Wenn Sie versuchen, eine einzelne IP-Adresse an eine EDL anzuhängen und diese IP-Adresse Teil eines erkennbaren CIDR-Elements ist, das sich bereits in einer EDL befindet, wird ein CIDR-Konfliktfehler angezeigt. Dieser Fehler gibt an, dass die einzelne IP-Adresse bereits als Teil des erkennbaren CIDR-Elements in der EDL enthalten ist. Beispiel: `192.168.24.25` Ist Teil des CIDR-Blocks `192.168.0.0/22` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIDR-Konflikt



(Optional) Bearbeiten Sie den Sicherheits-Tag-Namen für Palo Alto Networks Next-Generation Firewall

Wenn **Tag anzeigen** Das Kontrollkästchen ist aktiviert, wenn Sie den EDL-Datensatz (External Dynamic List) erstellen. Sie können die Tag-Namen und Farben der Sicherheits-Tags bearbeiten. Sicherheits-Tags helfen Ihnen, erkennbare Elemente nachzuverfolgen, die bereits blockiert sind.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

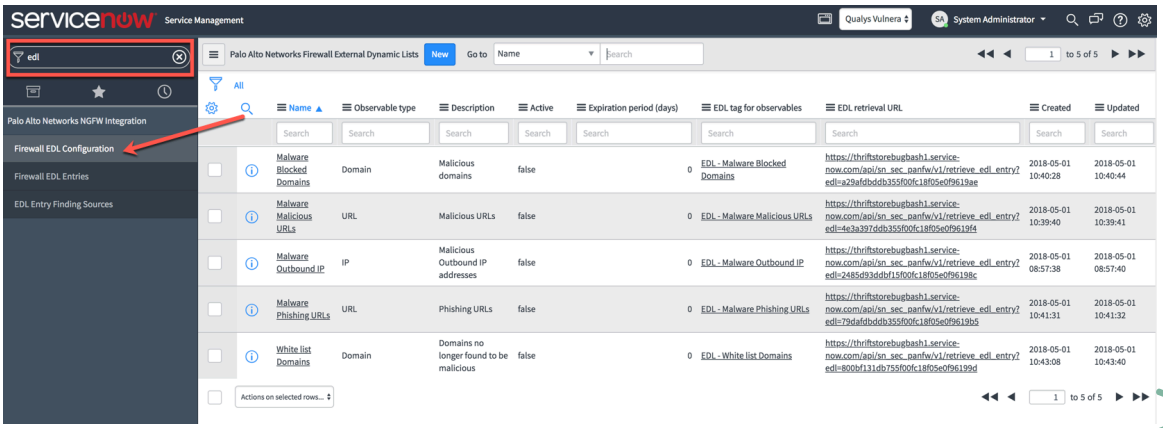
Warum und wann dieser Vorgang ausgeführt wird

Sicherheits-Tags helfen Ihnen, schnell zu identifizieren, welche Security Incidents erkennbare Elemente auf einer Sperrliste enthalten. Tags helfen Ihnen auch zu identifizieren, ob ein erkennbares Element bereits blockiert ist oder ob es aus einer EDL entfernt wurde. Standardmäßig ist die Farbe des Sicherheits-Tags für Blocklisteneinträge schwarz und für Allow-Listeneinträge grau. Sie können die Namen und Farben der Tags ändern, damit Sie bestimmte Tags leichter erkennen können.

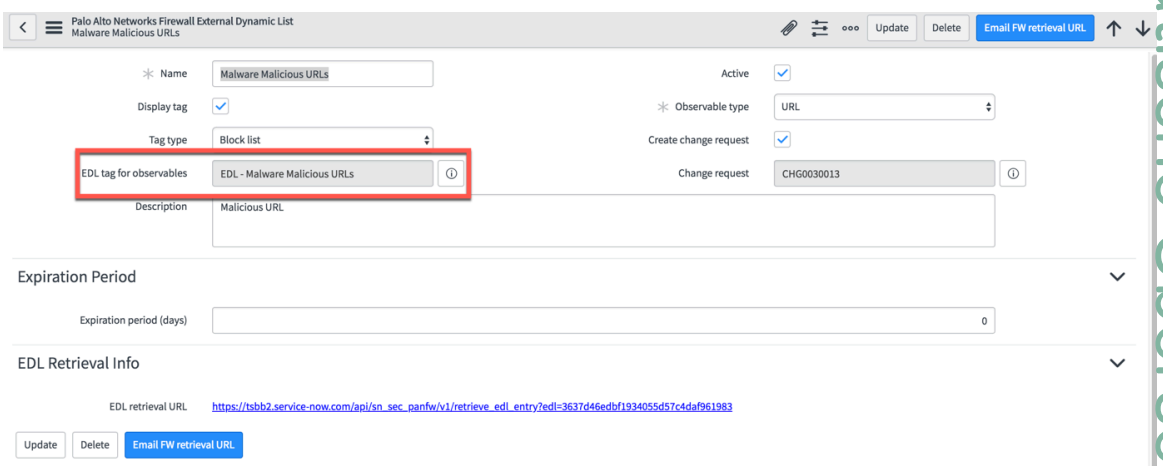
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

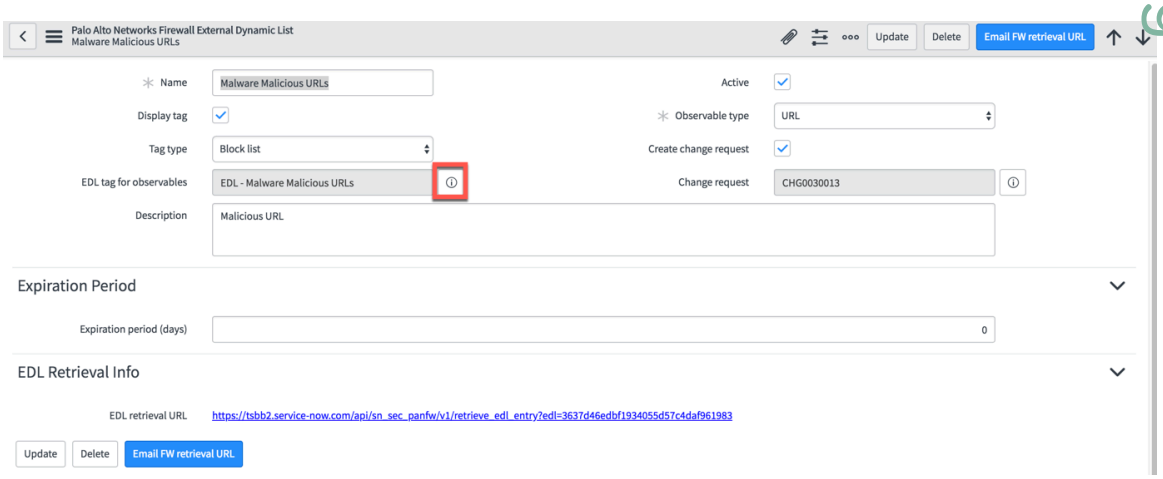
1. Navigieren zu **Alle** > **Palo Alto Networks – NGFW-Integration** > **Firewall-EDL-Konfiguration**an.



2. Klicken Sie auf ein Element im **Name** Spalte zum Öffnen
   Der EDL-Datensatz wird angezeigt. Standardmäßig entspricht der Sicherheits-Tag-Name dem Wert, den Sie in eingegeben haben **Name** Feld der EDL, wenn Sie sie erstellt haben. Standardmäßig enthält der Name auch einen *EDL* Präfix, z. B. EDL – schädliche URLs für Malware.



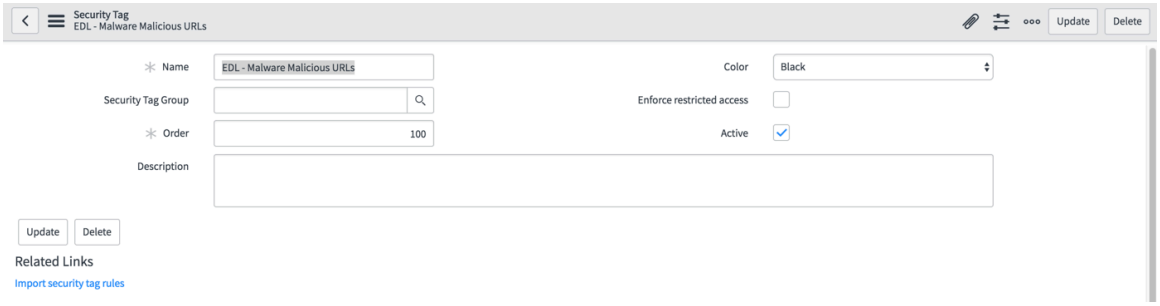
3. Klicken Sie auf das Informationssymbol ( ) Neben **EDL-Tag für erkennbare Elemente** Dann **Datensatz öffnen** .



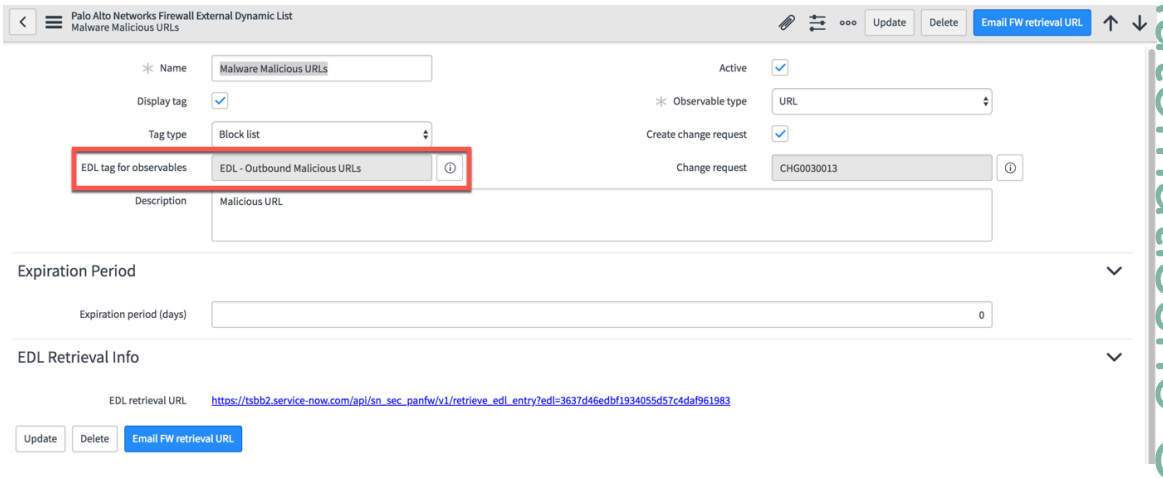
   Das Sicherheits-Tag-Formular wird angezeigt.

Automatische Übersetzung

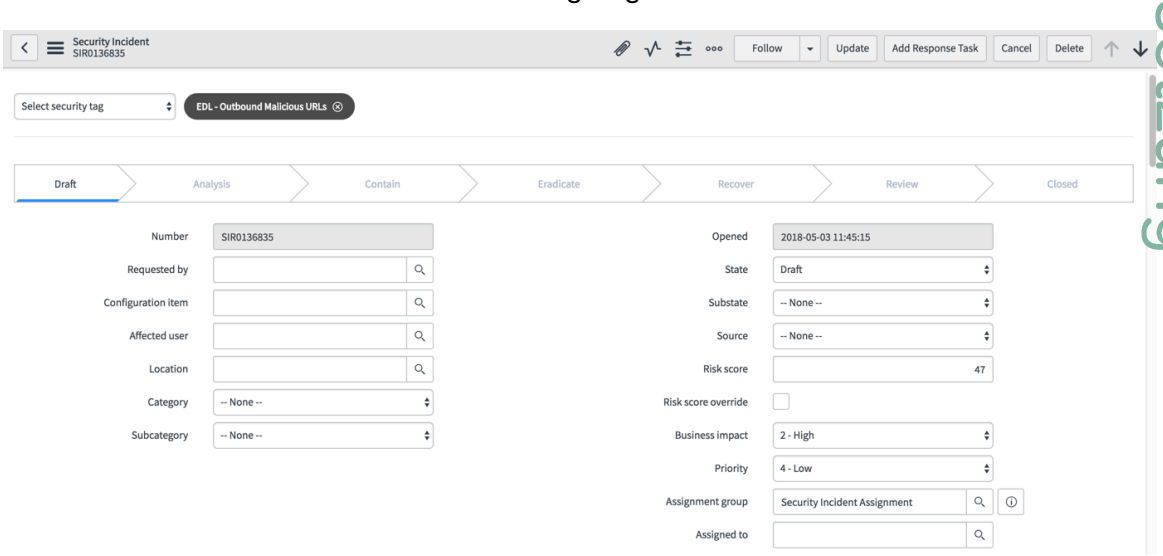
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. In **Name** Ändern Sie den Sicherheits-Tag-Namen, und klicken Sie auf **Aktualisieren** .
   Der aktualisierte EDL-Datensatz wird mit dem geänderten Tag-Namen angezeigt. Im folgenden Beispiel: `Ausgehend` Wurde dem Tag-Namen hinzugefügt. Behalten Sie die bei `EDL` Präfix in Ihrem neuen Tag-Namen, damit Sie identifizieren können, dass das Tag mit verknüpft ist Palo Alto Networks Next-Generation Firewall Integration.



Die Sicherheits-Tags werden für jeden erkennbaren Typ (IP, URL, Domäne) im Security Incident-Datensatz und im Datensatz des erkennbaren Elements jedes Mal angezeigt, wenn dieses erkennbare Element einer EDL hinzugefügt wird.



Wenn einem EDL bereits ein erkennbares Element hinzugefügt wurde und in einem Security Incident für dieses erkennbare Element ein Sicherheits-Tag angezeigt wird, wird das EDL-Sicherheits-Tag auch automatisch in allen nachfolgenden Security Incident-Datensätzen angezeigt, die erstellt werden. Diese Duplizierung teilt Ihnen mit, dass

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sich das erkennbare Element bereits in einer Blockliste befindet. Sie müssen dieses erkennbare Element nicht hinzufügen und erneut blockieren.

Wenn ein erkennbares Element nicht mehr blockiert ist, wird im Security Incident-Datensatz oder im Datensatz des erkennbaren Elements kein Sicherheits-Tag angezeigt. In dieser Instanz gibt kein Sicherheits-Tag an, dass das Ablaufdatum des erkennbaren Elements möglicherweise überschritten ist oder das erkennbare Element in einer EDL deaktiviert wurde.

Deinstallieren

Wenn Sie deinstallieren möchten Palo Alto Networks Next-Generation Firewall Von Ihrem ServiceNow AI Platform Instanz und alle Reste aus der Integration entfernen, siehe ServiceNow Dokumentationswebsite für Anweisungen zum Deinstallieren von Anwendungen.

Vorbereitungen

Erforderliche Rolle: Systemadministrator (Administrator)
Weitere Informationen finden Sie unter Anwendungen deinstallieren im ServiceNow-Produktdokumentationswebsite .

PhishTank-Integration

PhishTank Ist ein Community-basiertes Phishing-Verifizierungssystem, in das Anwender vermutete Bedrohungen übermitteln und andere Anwender im System abstimmen, um festzustellen, ob die Phishing-Bedrohungen legitim sind. Bei Integration mit ServiceNow AI Platform Security Operations Produkt bieten die Threat Intelligence-Ergebnisse Analysten zusätzlichen Einblick in Phishing-bezogene Security Incidents oder -Untersuchungen.

Die PhishTank Die Integration führt Suchen nach potenziellen Phishing-Site-URLs durch.

Der Workflow überprüft nach neuen erkennbaren Elementen, wenn sie in Security Incidents ankommen. Wenn die erkennbaren Elemente von einem Typ sind, der von der API-Integration erkannt wird, werden die erkennbaren Elemente ausgewertet. Erkennbare Elemente, die als schädlich eingestuft werden, werden gekennzeichnet.

PhishTank installieren und konfigurieren

Bevor Sie die Integration auf Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte so aus PhishTank Die Anwendung ist ordnungsgemäß in integriert ServiceNow AI Platform Security Operations.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Der Systemadministrator (Administrator) installiert die App und weist die Rolle Security Incident-Administrator (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

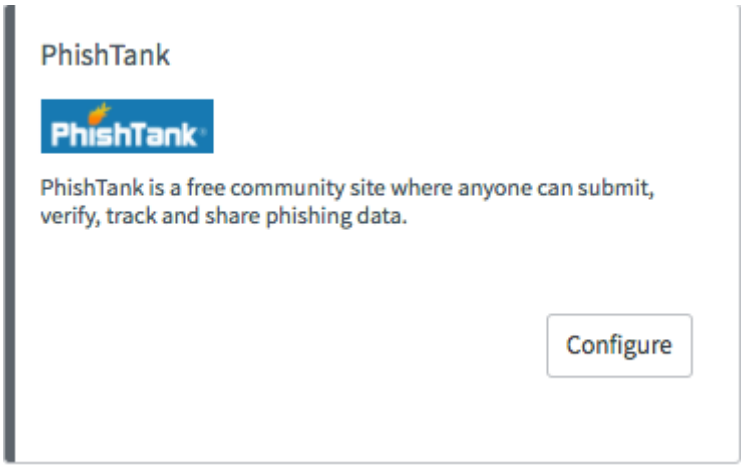
Setupaufgaben	Beschreibung
	und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf Security Operations Modul.
Rufen Sie einen API-Schlüssel ab.	Besuchen Sie PhishTank Website für Informationen zu API-Schlüsseln und zum Erstellen eines Accounts: PhishTank-Website .
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	Madrid und spätere Release-Anforderungen Für das Madrid-Release und spätere Familienveröffentlichungen Security Incident Response Abhängigkeits-Plugin (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Für die Integration erforderliche Anwendungen. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. **1.** Security Incident Response **2.** Sicherheits-Integrations-Framework **3.** Security Support Common **4.** Orchestration Des Sicherheitssupports Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz für die Integration finden Sie unter Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

Erforderliche Rolle: Administrator

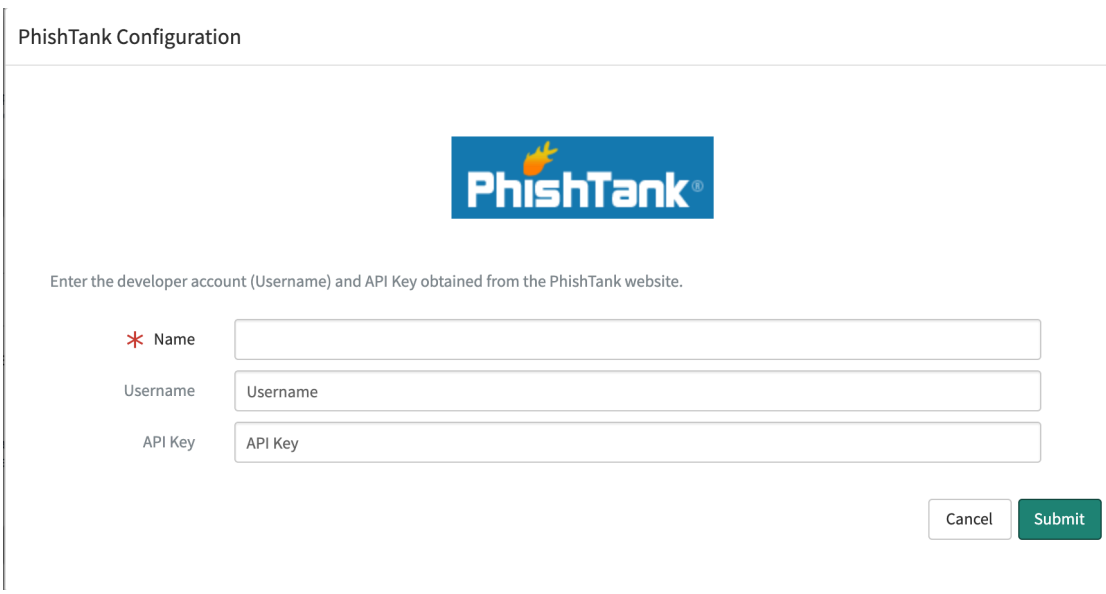
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn Sie die Anwendung für die Integration nicht installiert haben, finden Sie weitere Informationen unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie PhishTank Kachel.
3. Klicken Sie auf **Konfigurieren**.



4. In **PhishTank-Konfiguration** Geben Sie den Namen der Konfiguration, den Anwendernamen (in PhishTank erstellte Entwickleraccount) und den API-Schlüssel ein, den Sie vom erhalten haben PhishTank Website und klicken Sie auf **Übermitteln** .



5. Überprüfen Sie die erfolgreiche Konfiguration.
   Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, eine Fehlermeldung wird angezeigt.

Trouble?

Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, wird PhishTank API-Schlüssel ist möglicherweise ungültig.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie die erwarteten Ergebnisse für PhishTank

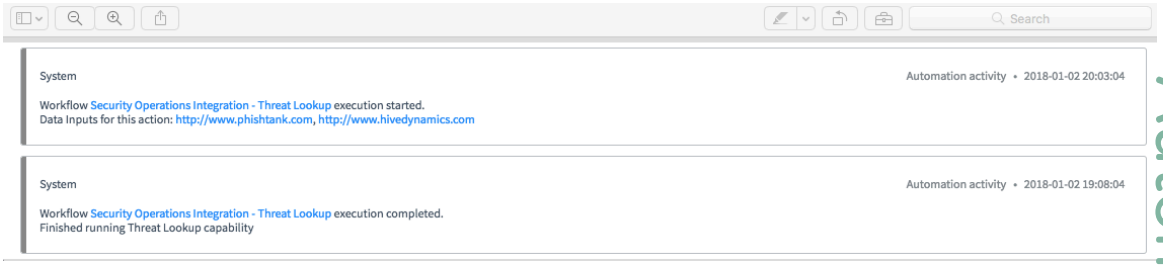
Erkennbare Elemente werden automatisch von einem Security Incident generiert und von der Anwendung gescannt. Suchergebnisse werden auf der Registerkarte Ergebnisse der Bedrohungssuche am unteren Rand des Security Incident-Datensatzes angezeigt.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Öffnen Sie das Security Incident-Formular, mit dem Sie arbeiten, und überprüfen Sie, ob die Suche erfolgreich ausgeführt wurde.

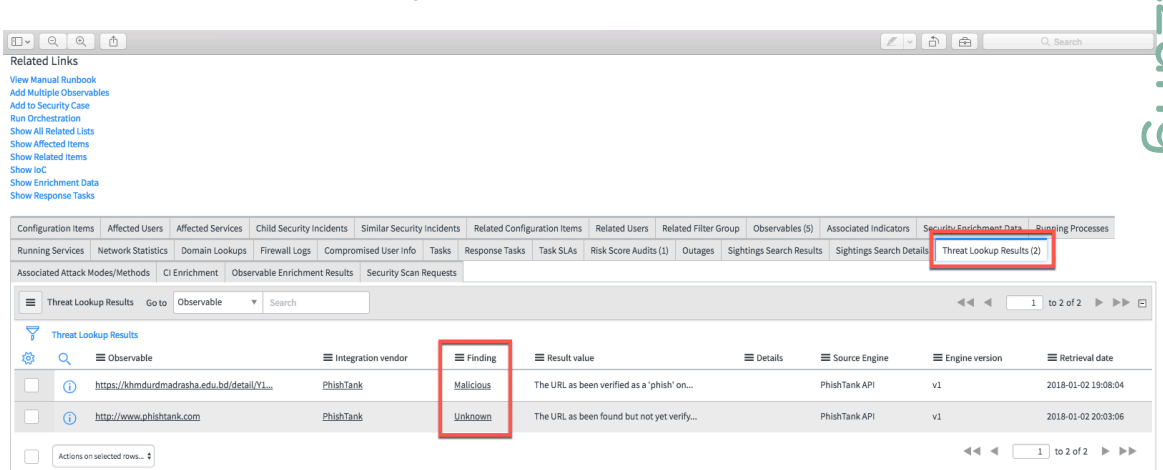


   Nachdem die Anwendung konfiguriert wurde, wird der Flow bei der Incident-Erstellung automatisch gestartet. Der Ausführungs- und Abschlussstatus der Suche wird dann in den Arbeitsnotizen im Security Incident-Datensatz angezeigt.

2. Überprüfen Sie die Arbeitsnotizen, um weitere Informationen zu erhalten und zu erfahren, wie Sie fortfahren können, wenn Sie nicht verifizieren können, dass die Suche erfolgreich ausgeführt wurde.

3. Navigieren Sie zum Ende des Security Incident, und klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Zugehöriger Link.

   Hinweis:
   Die Zahlen in den folgenden Schritten werden mit angezeigt **Formulare mit Registerkarten** Einstellung in den Systemeinstellungen aktiv. Wenn Formulare mit Registerkarten nicht angezeigt werden, klicken Sie in der oberen rechten Ecke des Bannerrahmens auf das Symbol für Einstellungen. In **Systemeinstellungen** Klicken Sie auf das Dialogfeld, das angezeigt wird **Formulare** Und verifizieren Sie das **Formulare mit Registerkarten** Und **Mit dem Formular** Sind ausgewählt.



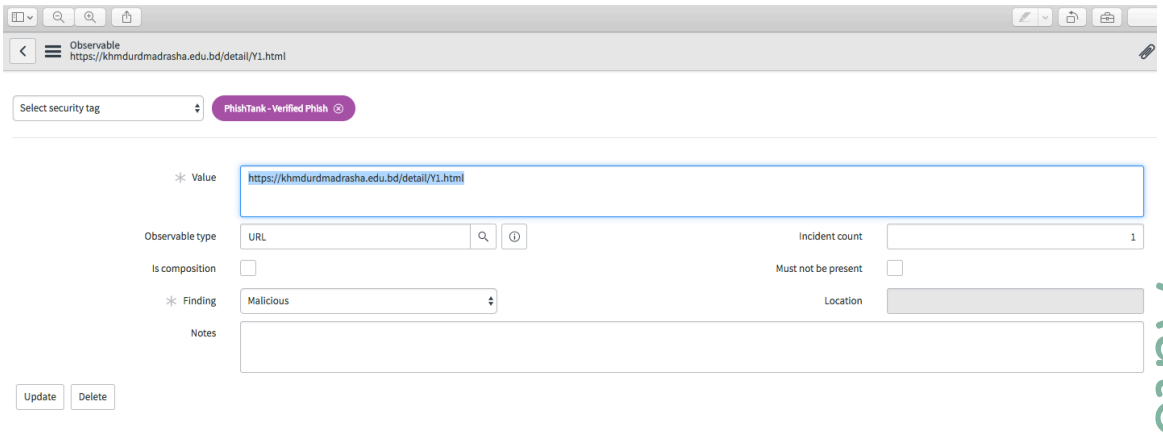
   Die **Ergebnisse Der Bedrohungssuche** Auf der Registerkarte unten im Security Incident-Datensatz werden die Suchergebnisse angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die **Ergebnis** Spaltenanzeigen Unbekannt Für Datensätze, die nicht als schädlich eingestuft wurden. Für Ergebnisse, die schädlich sind, Böswillig Wird in angezeigt **Ergebnis** Spalte.

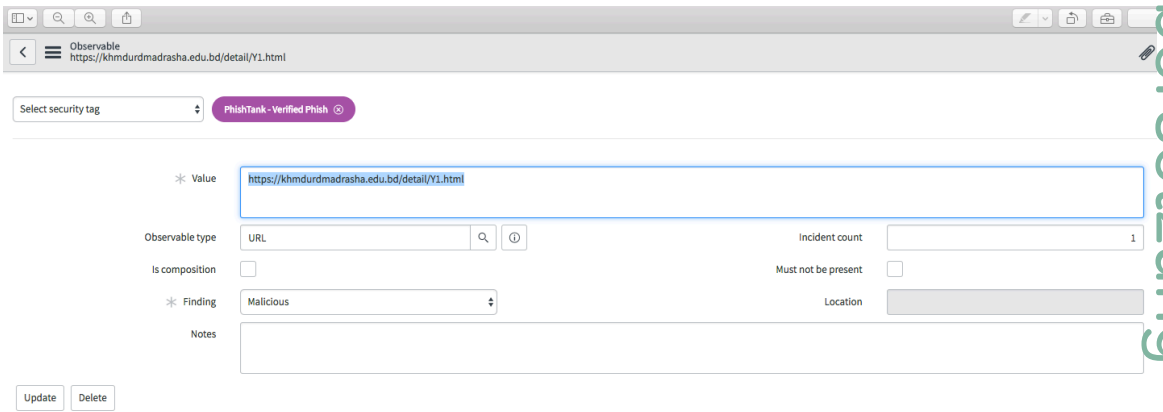
4. In **Erkennbares Element** Spalte auf ein erkennbares Element klicken, um einen Datensatz zu öffnen und weitere Informationen anzuzeigen.



Im Datensatz des erkennbaren Elements für Suchvorgänge, die mit böswilligen Elementen übereinstimmen, Böswillig Wird angezeigt **Ergebnis** Feld. Das erkennbare Element ist mit gekennzeichnet Threat Intelligence Quelle, die festgestellt hat, dass es böswillig ist, in diesem Fall die PhishTank Anwendung.

5. Um Rohdaten anzuzeigen, navigieren Sie zurück zum Security Incident, und klicken Sie auf das blaue Informationssymbol neben einem erkennbaren Element.

6. Klicken Sie im angezeigten Fenster auf **Öffnen Sie Den Datensatz** .



Der von der API und der erstellte Link **Ergebnis** Feld, das mit den Ergebnissen angezeigt wird.

Trouble?

Wenn unter keine Ergebnisse angezeigt werden **Ergebnisse Der Bedrohungssuche** Überprüfen Sie, ob das erkennbare Element ein Typ ist, der für die Suche durch die Integration unterstützt wird.

(Optional) Fügen Sie ein erkennbares Element für manuell an PhishTank

Sie können erkennbare Elemente manuell an einen Security Incident anhängen. Sie hängen erkennbare Elemente manuell an, wenn Sie Bedrohungssuchen für erkennbare Elemente durchführen möchten, die nicht an einen Security Incident beim ersten Ereignisauslöser

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

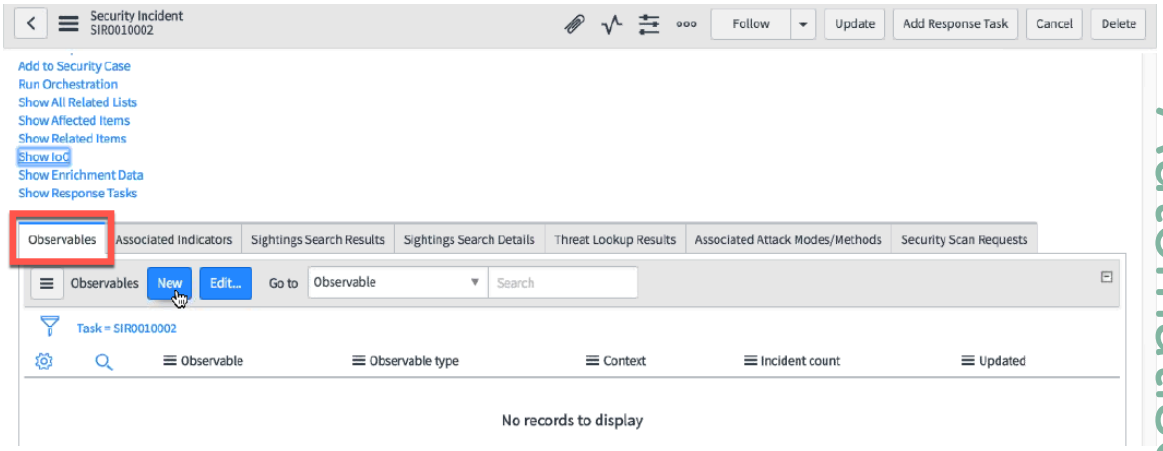
angehängt sind. Sie können diese Aufgabe auch ausführen, wenn Sie weitere Informationen zu einem zugehörigen erkennbaren Element wünschen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

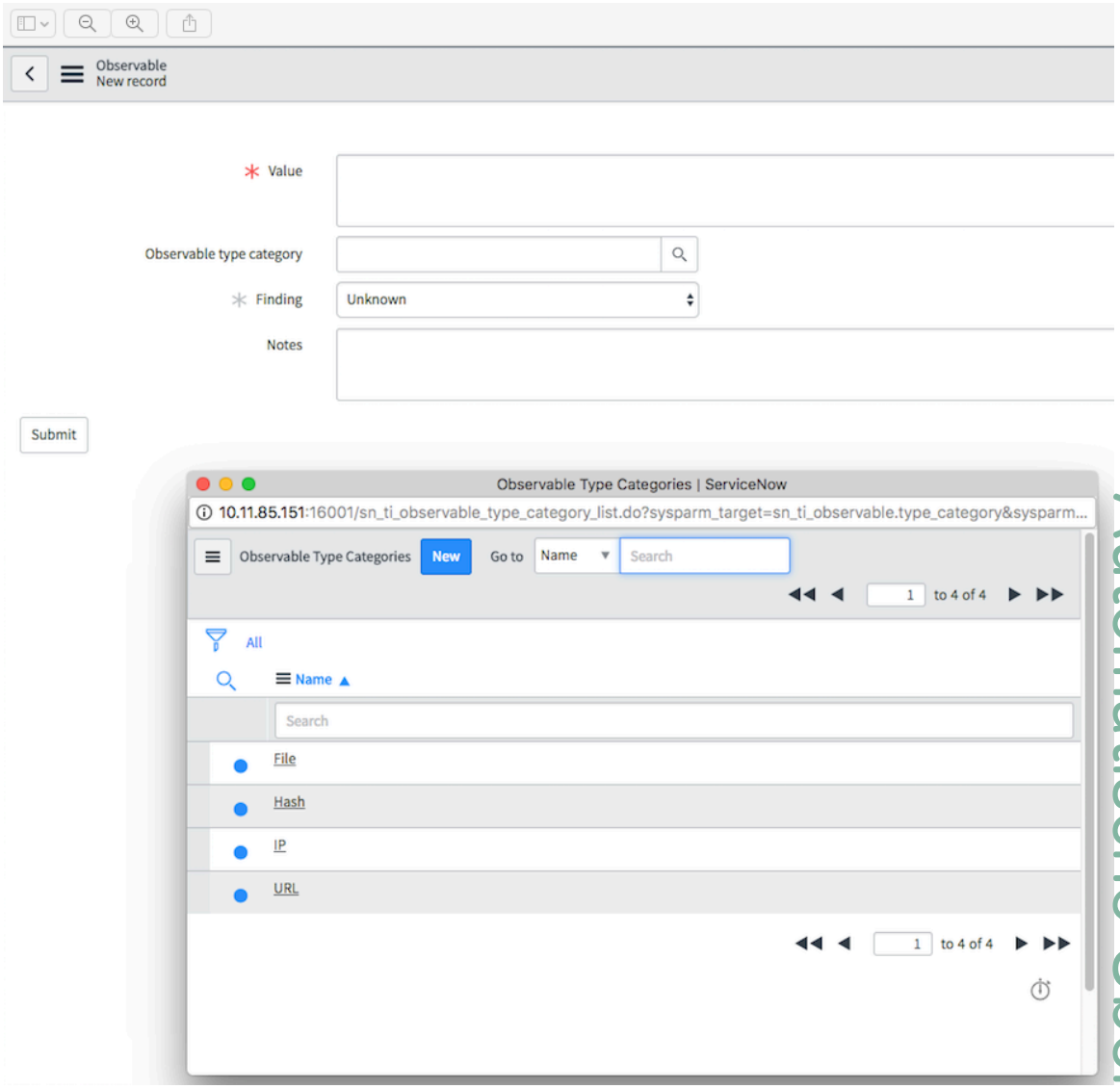
1. Navigieren Sie zu Ihrem offenen Security Incident.
2. Klicken Sie im Datensatz „offener Security Incident“ auf **IOC anzeigen** Link in **Zugehörige Links** Um anzuzeigen **Erkennbare Elemente** Registerkarte.



3. Klicken Sie auf **Neu**.
   Das Formular „erkennbares Element“ wird angezeigt.
4. In **Wert** Geben Sie eine URL ein.
5. Klicken Sie auf das Suchsymbol und im **Typkategorien Des Erkennbaren Elements** Klicken Sie auf das Dialogfeld **URL** In der Liste, um das Feld auszufüllen.

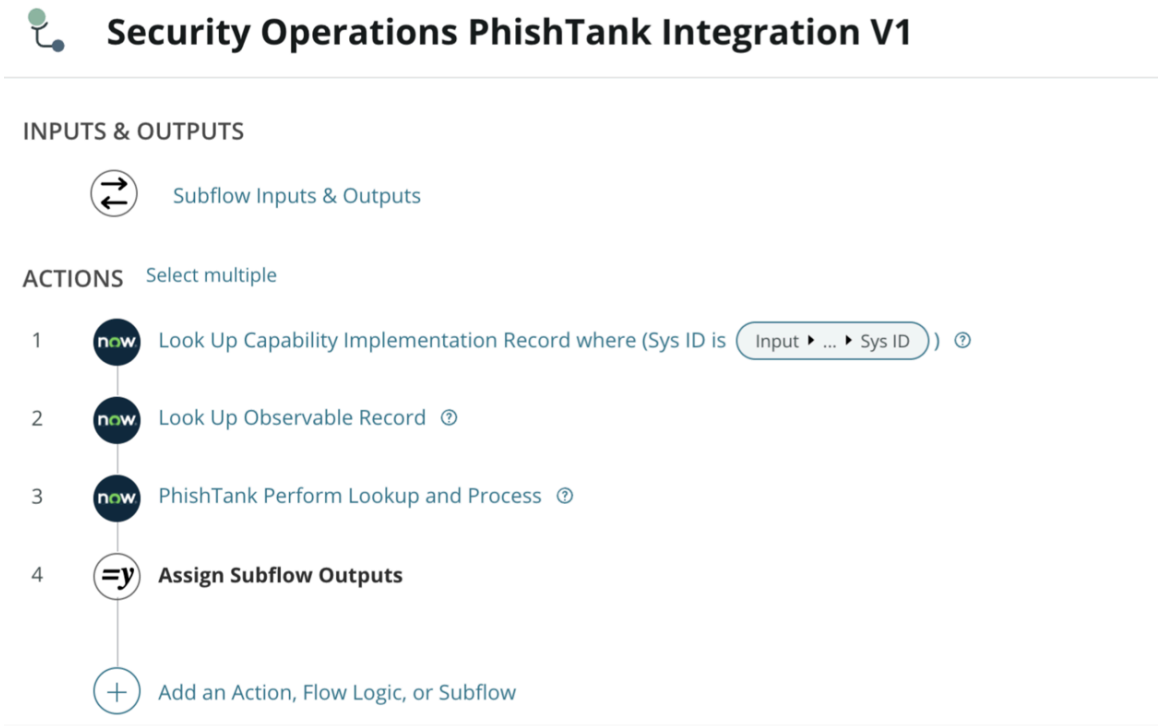
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

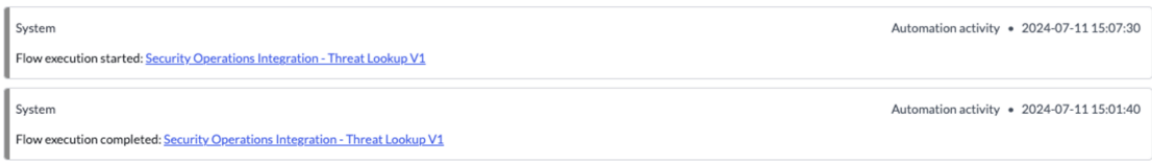


6. Klicken Sie auf **Absenden**.
Der Flow wird gestartet und überprüft, ob das neue erkennbare Element vorhanden ist. Der Ausführungs- und Abschlussstatus wird im Abschnitt „Arbeitsnotizen“ im Security Incident-Datensatz angezeigt.

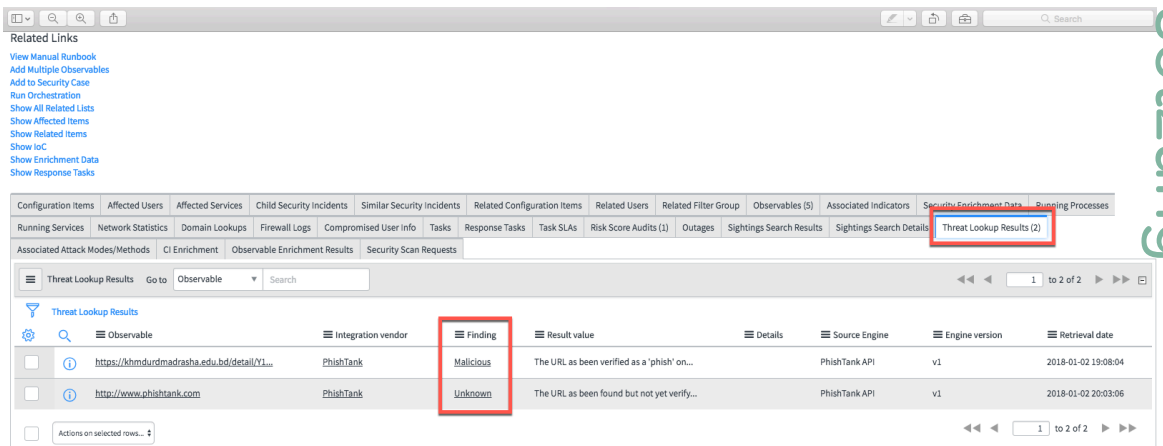
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Navigieren Sie zu Ihrem Security Incident, und überprüfen Sie die Arbeitsnotizen.



8. Klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Zugehöriger Link am unteren Rand des Security Incidents.
9. Klicken Sie auf **Ergebnisse Der Bedrohungssuche** Registerkarte zum Anzeigen der Ergebnisse.



10. In **Erkennbares Element** Klicken Sie auf das blaue Informationssymbol neben einem bestimmten erkennbaren Element, um weitere Informationen und Rohdaten zu erhalten.

11. Klicken Sie im angezeigten Dialogfeld auf **Öffnen Sie Den Datensatz** .

Automatische Übersetzung

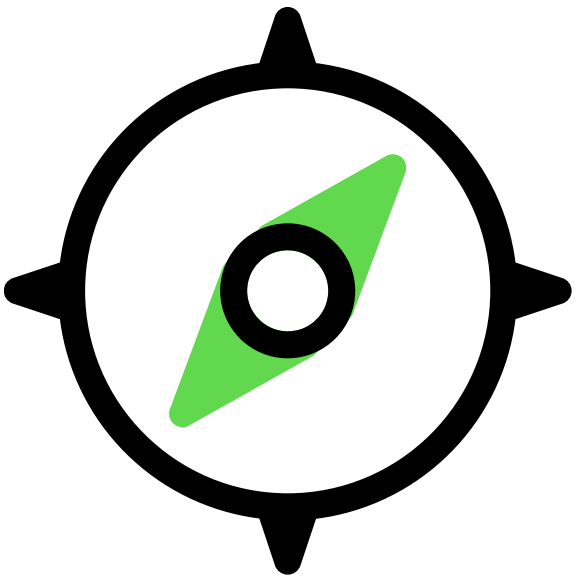
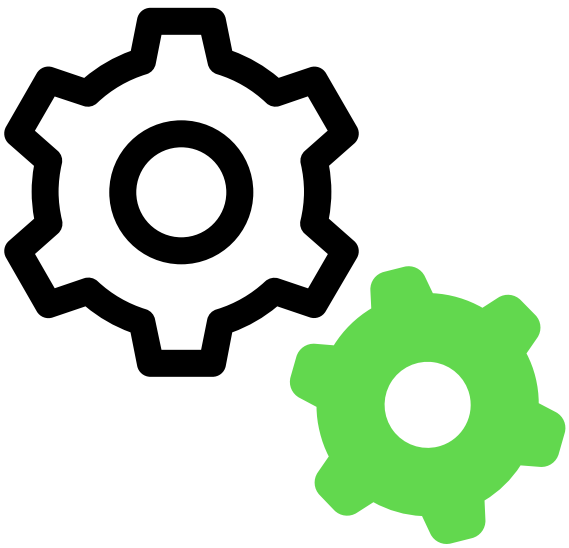
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trouble?
Überprüfen Sie die Arbeitsnotizen, um weitere Informationen zu erhalten und zu erfahren, wie Sie fortfahren können, wenn Sie nicht verifizieren können, dass die Suche erfolgreich ausgeführt wurde.

Proofpoint Integration für Security Operations

Die Proofpoint Die SIR-Integration unterstützt die Erfassung von Ereignissen aus Proofpoint. SIR erstellt für jedes erfasste Ereignis einen Incident, den Analysten überprüfen oder bearbeiten können.

Erste Schritte

Untersuchen	Konfigurieren
	
Erfahren Sie mehr über Proofpoint Integration	Konfigurieren Proofpoint Für SIR Workspace

Erkunden Sie Proofpoint Integration für Security Operations

Sie können Ereignisprofile in SIR konfigurieren, um Ereignisse aus aufzunehmen Proofpoint. SIR erstellt für jedes erfasste Ereignis einen Incident, den Analysten überprüfen oder bearbeiten können.

Proofpoint Integration für Security Operations Anwender

Anwender

Anwender	Beschreibung
Sicherheitsadministrator	Erstellen Sie Ereignisprofile zum Filtern der erfassten Ereignisse. SIR erstellt Incidents für diese erfassten Ereignisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Proofpoint Integration für Security Operations Vorteile

Proofpoint Integration für Security Operations Vorteile

Leistung	Funktion	Anwender
Rufen Sie Ereignisdaten in Ihre Instanz ab, und erstellen Sie Security Incidents. Überprüfen Sie Security Incidents von einem zentralen Ort aus auf Ereignisse, die als verdächtig oder böswillig gelten.	Wenn die zugestellten E-Mail-Nachrichten und zulässigen Klicks später als schädlich eingestuft werden, werden diese Nachrichten wahrscheinlich von Ihren Mitarbeitern geöffnet und mit ihnen interagiert. Um diese Nachrichten zur Überprüfung nachzuverfolgen, erstellen Sie automatisch Security Incidents basierend auf den Ereignisprofilen, die Sie für den Nachrichtenverkehr für die Integration erstellen und konfigurieren. Darüber hinaus können Sie auch die Erstellung von Security Incidents für die blockierten Nachrichten und Klicks zu Audit-Zwecken aktivieren.	Manager

Automatische Übersetzung

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Proofpoint finden Sie unter:

- Konfigurieren von Proofpoint Integration für Security Operations
- Überprüfen Sie die Einstellungen für die Proofpoint-Integration
- Zeigen Sie an Proofpoint Analytics-Dashboard

Konfigurieren von Proofpoint Integration für Security Operations

Konfigurieren Sie Ihre Implementierung von Proofpoint Integration für Security Operations .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration – Übersicht

1. Installieren und konfigurieren Sie Proofpoint Integration.

   Laden Sie die Integrationsanwendung herunter, installieren und aktivieren Sie sie.

2. Erstellen Sie ein Ereignisprofil für Proofpoint Integration für Security Operations.

   Erstellen Sie ein Ereignisprofil, um die Ereignisse zu identifizieren, die Sie aus importieren möchten Proofpoint Produkt und die Bedingungen, die Sie zum Erstellen von Security Incidents aus den importierten Daten verwenden möchten.

3. Konfigurieren von Proofpoint Integration für Security Operations

   Überprüfen Sie die Integrationseinstellungen für die Erstellung der Ereignisprofile.

Installieren und konfigurieren Sie Proofpoint Integration

Installieren und konfigurieren Sie Proofpoint Integration für Security Operations Anwendung aus dem ServiceNow® Store Auf Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Laden Sie herunter Proofpoint Integration für Security Operations Anwendung aus dem ServiceNow® Store Und installieren Sie es.
   Weitere Informationen finden Sie unter Installieren Sie eine ServiceNow Store-Anwendung .
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie nach Proofpoint Integration für Security Operations Kachel und wählen Sie aus **Konfigurieren** .
4. Füllen Sie im Formular die Felder aus.

Proofpoint Formular „Integrationskonfiguration“

Feld	Beschreibung
Name	Name des Proofpoint Integration für Security Operations-Konfiguration.
Service-Prinzipal	Anwendername von Proofpoint Mandant.
Geheimnis	Die ID von Proofpoint Mandant.

5. Wählen Sie **Absenden**.

Ergebnisse

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die Integration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Erstellen Sie ein Ereignisprofil für Proofpoint Integration für Security Operations

Erstellen Sie ein Ereignisprofil, um die Ereignisse zu identifizieren, die Sie aus importieren möchten Proofpoint Produkt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie erstellen ein Ereignisprofil, indem Sie Ereignistypen, Zuordnungen und Importzeitpläne konfigurieren. Ein Fortschrittsbalken auf der Seite zeigt alle Schritte an und wird für die derzeit aktive Konfiguration hervorgehoben.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Navigieren zu **Alle** > **SIR-Integration mit Proofpoint** > **Proofpoint-Ereignisprofil**an.
2. Wählen Sie auf der Seite „Ereignisprofile“ die Option aus **Neu** .
3. Füllen Sie im Formular die Felder aus.

   Der Fortschrittsbalken wird mit Name beginnend angezeigt.

   Proofpoint-Profilformular

Feld	Beschreibung
Name	Name für das Ereignisprofil. Erwägen Sie, einen Namen zu verwenden, der den zugehörigen Ereignistyp enthält: ○ Klicks blockiert ○ Klicks zugelassen ○ Nachrichten blockiert ○ Nachrichten zugestellt
Quelle	Die für die Integration auf der Seite „Integrationskonfigurationen“ konfigurierte Quelle.
Reihenfolge	Die Reihenfolge, in der dieses Profil ausgeführt wird. Der Standardwert ist 100.
Aktiv	Option zum Aktivieren des Profils.
Beschreibung	Optionale Beschreibung für dieses Ereignisprofil.

4. Wählen Sie **Fortsetzen**.
5. Wählen Sie einen oder mehrere Ereignistypen aus, indem Sie sie aus verschieben **Verfügbar** Spalte zu **Ausgewählt** Spalte.
   Die verfügbaren Ereignistypen sind:
   - Klicks blockiert
   - Klicks zugelassen
   - Nachrichten blockiert
   - Nachrichten zugestellt
6. Wählen Sie **Fortsetzen**.

   Die Konfigurationsschritte im Zusammenhang mit dem ausgewählten Ereignistyp oder den ausgewählten Ereignistypen werden in der Fortschrittsleiste angezeigt.

   Die Werte für die Felder „Quelle“ werden aus den TAP-Daten (Targeted Attack Protection) in Ihrer Umgebung als Referenz bereitgestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Standardzuordnung der Quellfelddaten zu den Zielfeldern wird auf der Seite angezeigt. Basisdaten sind als Leitfaden enthalten, Sie können diese Zuordnung jedoch ändern.

7. **Wahlweise:** Wählen Sie aus **f(x)** Symbol zum Anzeigen der Standardübersetzungen, die in der Anwendung enthalten sind.

   (Optional) Mehrere Werte für ein Feld werden durch Kommas getrennt.

8. Wählen Sie **Fortsetzen**.
9. Konfigurieren Sie auf der Seite „Filtern und Zusammenfassungen“ die Eigenschaften in der folgenden Tabelle.

Filter- und Zusammenfassungseigenschaften

Option	Beschreibung
Basierend auf Bedingungen für Nachrichtenereignisse filtern	Option zum Aktivieren der Filterung basierend auf Nachrichtenereignissen.
Filterbedingungen für Nachrichtenereignisse	Filterbedingungen für Nachrichtenereignis.
Basierend auf Bedingungen für Klickereignisse filtern	Option zum Aktivieren der Filterung basierend auf Klickereignissen.
Filterbedingungen für Klickereignisse	Klicken Sie auf Ereignisfilterbedingungen.
Zusammenfassungsbedingungen	Option, mit der ein eingehender Incident an einen offenen Security Incident angehängt werden kann, anstatt einen neuen zu erstellen.
Incident-Felder mit übereinstimmenden Werten	Fügen Sie hinzu Security Incident Response Felder, deren Werte abgeglichen werden müssen, damit ein Incident in eine Zusammenfassung aufgenommen werden kann.
Protokoll-Arbeitsnotiz für neuen Incident	Option zum Aktivieren der Protokollierung von Arbeitsnotizen im übergeordneten Element Security Incident Response.
Aktivieren Sie die ThreatID-Beziehung	Option zum Aktivieren der Zusammenfassung aller Incidents mit übereinstimmenden ThreatIDs.

10. Wählen Sie **Fortsetzen**.
11. Wählen Sie einen der Importtypen aus und wie oft Sie Ereignisdaten importieren möchten.
12. Wählen Sie **Fertigstellen** aus.

Ergebnisse

Das neu erstellte Ereignisprofil ist in der Liste der vorhandenen Ereignisprofile auf der Seite „Ereignisprofile“ enthalten.

Überprüfen Sie die Einstellungen für die Proofpoint-Integration

Überprüfen Sie die Einstellungen für die Proofpoint-Integration, damit Sie die Systemeigenschaften für Ihre Umgebung ändern können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si_admin

Prozedur

1. Navigieren zu **Alle** > **SIR-Integration mit Proofpoint** > **Proofpoint-Integrationseinstellungen**an.
2. Ändern Sie die folgenden Einstellungen.

Proofpoint-Integrationseinstellungen

Eigenschaftsname	Beschreibung
Zeitüberschreitung für die restAPI-Aufrufe. sn_sec_proofpoint.http_timeout	Die Zeitüberschreitung (in Sekunden) für das Abrufen von Daten aus den api-Aufrufen. Typ: Ganzzahl Standardwert: 3000
Protokollierungsebene – Debugging, Information, Warnung, Fehler sn_sec_proofpoint.Logging_verbosity	Die Protokollausführlichkeitsstufe der Anwendung, d. h. der Name des Informationstyps. Sie können den Wert auf die folgenden Optionen aktualisieren: ○ Fehler ○ warnen ○ Info ○ debuggen Standardwert: info
Erzwingt einen Grenzwert für die Anzahl von Proofpoint-Ereignissen, die zu einem einzelnen Incident aggregiert werden können. sn_sec_proofpoint.max_aggregations_per_si	Die maximale Anzahl von Proofpoint-Ereignissen, die zu einem Incident zusammengefasst werden können. Typ: Ganzzahl Standardwert: 100
Grenzwert für die Anzahl von Security Incidents erzwingen, die innerhalb von 24 Stunden erstellt werden können. sn_sec_proofpoint.max_si_per_day	Die maximale Anzahl von Incidents, die in 24 Stunden erstellt werden können. Typ: Ganzzahl Standardwert: 1000
Anzahl der Tage, die wir im api-Aufruf für Top-Klicker verwenden müssen, vap. sn_sec_proofpoint.default_days	Die Anzahl der Tage, die für Top-Klicker und VAP abgerufen werden sollen. Sie können den Wert auch auf die folgenden Optionen aktualisieren: ○ 14 ○ 30 ○ 90.0 Typ: Ganzzahl Standardwert: 90

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftsname	Beschreibung
Boolesche Kennzeichnung. Wenn diese Option aktiviert ist, erfolgt ein api-Aufruf und füllt Topclicker-Details aus. sn_sec_proofpoint.call_topclickers_api	Aktivieren Sie die Option zum Aktivieren und Abrufen von Daten für Top-Klicker. Typ: Boolesch Standardwert: True
Boolesche Kennzeichnung. Wenn diese Option aktiviert ist, erfolgt ein api-Aufruf und füllt VAP-Details aus. sn_sec_proofpoint.call_vap_api	Aktivieren Sie die Option zum Aktivieren und Abrufen von VAP-Daten. Typ: Boolesch Standardwert: False
Sie dient dazu, die maximale Anzahl von Anwendern zu beschränken, die für topClickers und VAP-Anwender angezeigt werden sollen. sn_sec_proofpoint.maxresults	Die maximale Anzahl von Anwendern, die für Top-Klicker und VAP-Anwender angezeigt werden sollen. Typ: Ganzzahl Standardwert: 100
Aktiviert/deaktiviert die Verwendung des überlappenden Zeitraums während der geplanten Abfrage von Proofpoint-Ereignissen. sn_sec_proofpoint.allow_overlap	Aktivieren oder deaktivieren Sie den überlappenden Zeitraum, wenn die geplante Abfrage konfiguriert ist. Typ: Boolesch Standardwert: False
Überlappungszeit in Minuten, die während der geplanten Abfrage von ProofpointEvents verwendet werden soll, wenn Überlappung aktiviert ist. sn_sec_proofpoint.overlap_time	Die Überschneidungszeit in Minuten, wenn die geplante Abfrage konfiguriert ist. Typ: Ganzzahl Standardwert: 5

3. Wählen Sie **Speichern**.

Ergebnisse
Konfiguriert die Integrationseinstellungen mit neuen Werten.

Zeigen Sie an Proofpoint Analytics-Dashboard

Die Proofpoint Analytics-Dashboard bietet Details zu VAP-Anwendern und Top-Klickern.

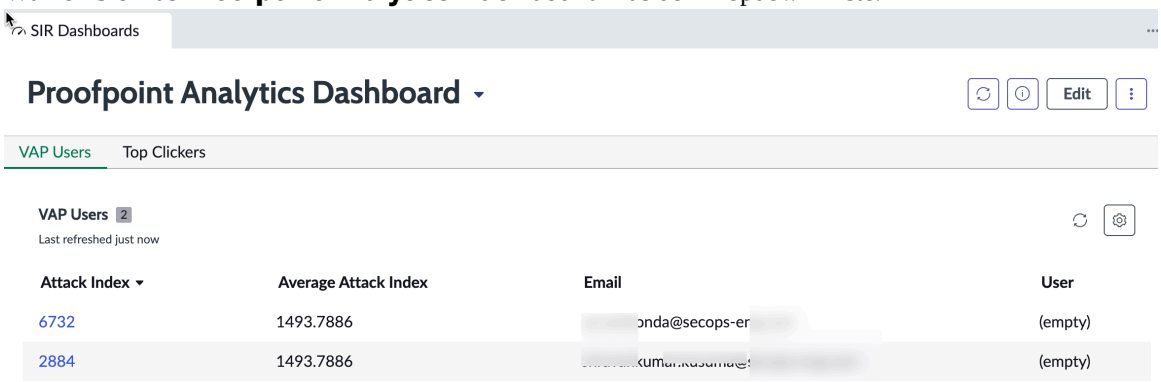
Warum und wann dieser Vorgang ausgeführt wird
Anwender, die hauptsächlich auf Sicherheitsangriffe abzielen, werden als VAP-Anwender betrachtet. Mitarbeiter, die häufig auf verdächtige Links und Phishing-Links klicken, gelten als Top-Klicker.

Vorbereitungen
Erforderliche Rolle: sn_si_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Arbeitsbereich für Security Incident Response**an.
2. Wählen Sie Aus **SIR-Dashboards** .
3. Wählen Sie Aus **Proofpoint Analytics-Dashboard** Aus der Dropdown-Liste.



4. Zeigen Sie Informationen zu VAP-Anwendern an.
   a. Zeigen Sie die Liste der VAP-Anwender an, indem Sie auswählen **VAP-Anwender** Registerkarte.
   b. Zeigen Sie die Details eines VAP-Anwenders an, indem Sie den Anwendernamen auswählen.
5. Zeigen Sie Informationen zu Top-Klickern an.
   a. Zeigen Sie die Liste der Top-Klicker an, indem Sie auswählen **Top-Klicker** Registerkarte.
   b. Zeigen Sie die Details eines Top-Klicks an, indem Sie den Anwendernamen auswählen.

Reverse Whois-Integration

Reverse Whois Ist ein Service, der nach Domänennamen sucht, die von Einzelpersonen oder Organisationen registriert sind.

Führen Sie Domänensuchen mithilfe von Suchbegriffen in erkennbaren Elementen durch, die Sie an einen Security Incident anhängen. Die Reverse Whois Die API durchsucht Domänendatensätze basierend auf von Ihnen eingegebenen Suchbegriffen und gibt alle Datensätze zurück, die diesen Begriffen entsprechen.

Analysten verwenden diese Integration manchmal zusammen mit Whois Integration für Security Incident Research. Die Whois Die Integration bietet zusätzliche Ergänzungsinformationen basierend auf den Domänensuchen aus dem Reverse Whois Integration.

Reverse Whois installieren und konfigurieren

Bevor Sie die Integration auf Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte so aus Reverse Whois Die Anwendung ist ordnungsgemäß in integriert Security Operations Produkt.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow Rollen.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Der Systemadministrator (Administrator) installiert die App und weist die Rolle Security Incident-Administrator (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration. Der Security Incident-Administrator weist auch die Rolle Security Incident Analyst (sn_si.Analyst) zu. • Der Security Incident Analyst (sn_si.Analyst) führt Domänensuchen mit durch Reverse Whois Und analysiert Security Incidents und arbeitet mit ihnen.
Rufen Sie einen API-Schlüssel ab.	Besuchen Sie die WhoisXML-API-Website, um Informationen zu API-Schlüsseln zu erhalten und einen Account zu erstellen: WhoisXML-API-Website . Die Konfiguration erfordert, dass Sie die API-Schlüssel eingeben.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	Madrid und spätere Release-Anforderungen Für das Madrid-Release und spätere Familienveröffentlichungen Security Incident Response Abhängigkeits-Plugin (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Für die Integration erforderliche Anwendungen. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. **1.** Security Incident Response **2.** Sicherheits-Integrations-Framework

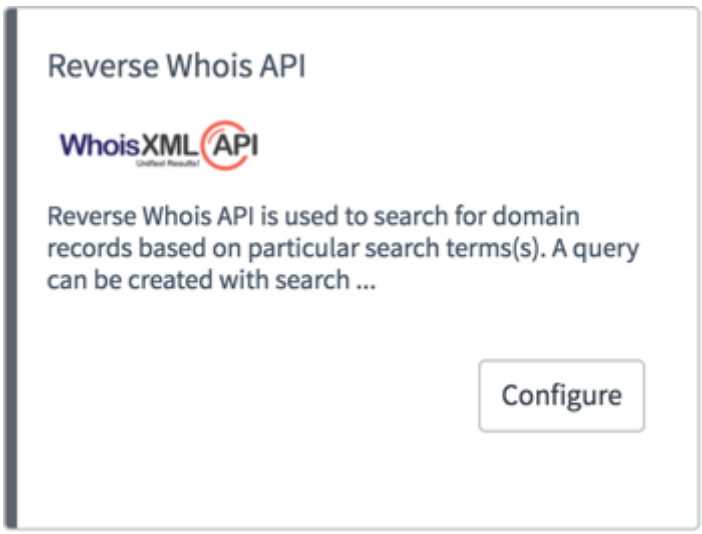
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	3. Security Support Common **4.** Orchestration Des Sicherheitssupports Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz für die Integration finden Sie unter Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

Erforderliche Rolle: Administrator

Prozedur

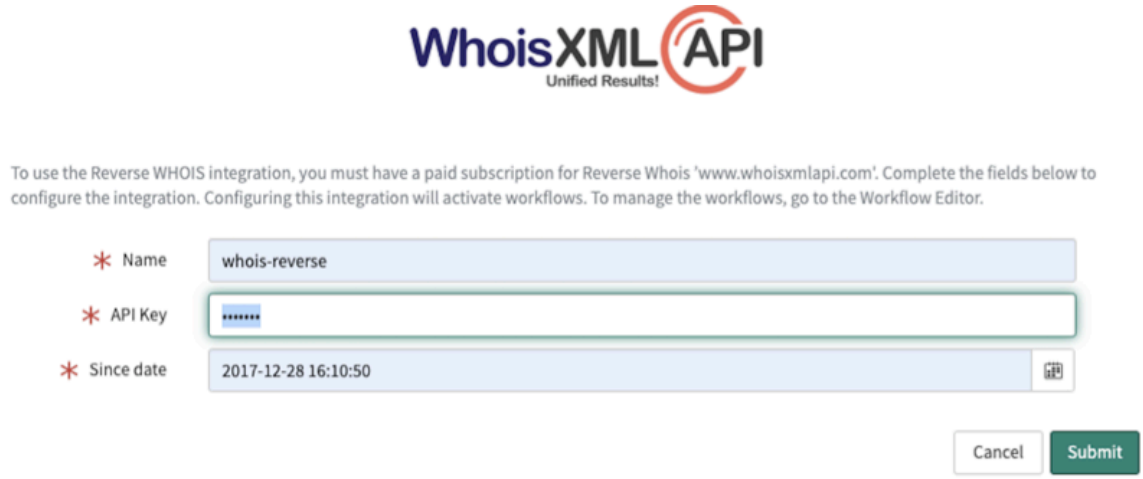
1. Wenn Sie bereits installiert und konfiguriert haben Reverse Whois Führen Sie die folgenden Schritte aus:
   a. Löschen Sie die vorhandene Konfiguration.
   b. Installieren und erstellen Sie eine neue Konfiguration mit dem von Ihnen erhaltenen API-Schlüssel.
2. Wenn Sie die Anwendung für die Integration nicht installiert haben, finden Sie weitere Informationen unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
3. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie Reverse Whois API-Kachel.
4. Klicken Sie auf **Konfigurieren**.



5. In **Whois-API-Konfiguration umkehren** Geben Sie den API-Schlüssel ein, den Sie aus dem erhalten haben Whois XML-API-Website.
6. Wählen Sie eine Option in der folgenden Tabelle aus, um Domänensuchen nach Ihren Suchbegriffen zu filtern.
   Diese Konfigurationseinstellungen bleiben gespeichert, bis Sie sie ändern, und gelten für alle Reverse Whois API-Suchen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Absenden**.
   Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, eine Fehlermeldung wird angezeigt.

Trouble?
Wenn eine Fehlermeldung angezeigt wird, ist der API-Schlüssel möglicherweise ungültig.

Fehlermeldung

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

(Optional) Installieren und konfigurieren Whois

Installieren Sie Whois Plugin, um zusätzliche Ergänzungsinformationen zu Ihren Domänensuchen aus bereitzustellen Reverse Whois API. Diese Suche bietet zusätzliche Ergänzungsdaten zur Domäne, z. B. das Registrierungsdatum, den Namen der Registrierungsstelle und das Herkunftsland.

Vorbereitungen

1. Wenn Sie keine Berechtigung für die Anwendung angefordert haben, finden Sie unter Berechtigung für abrufen Security Operations Produkt oder Anwendung Für Whois Anwendung aus dem ServiceNow Store.
2. Rufen Sie Anmeldeinformationen für ab Whois API-Schlüssel von der Produktwebsite: WHOIS-API-Website .

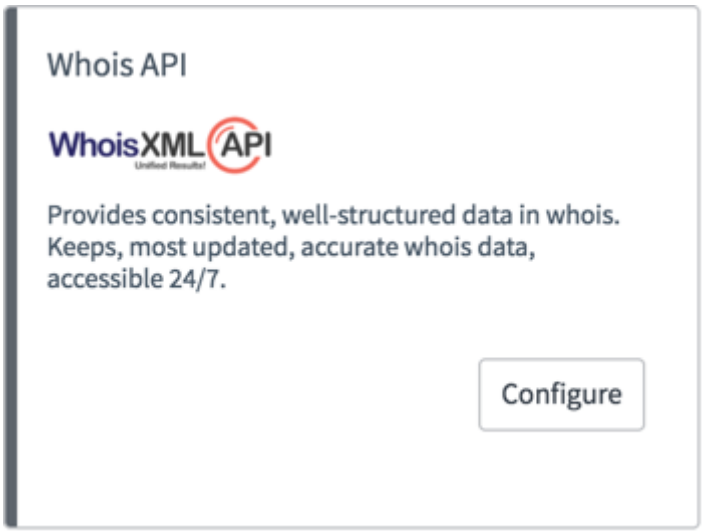
Erforderliche Rolle: Administrator

Prozedur

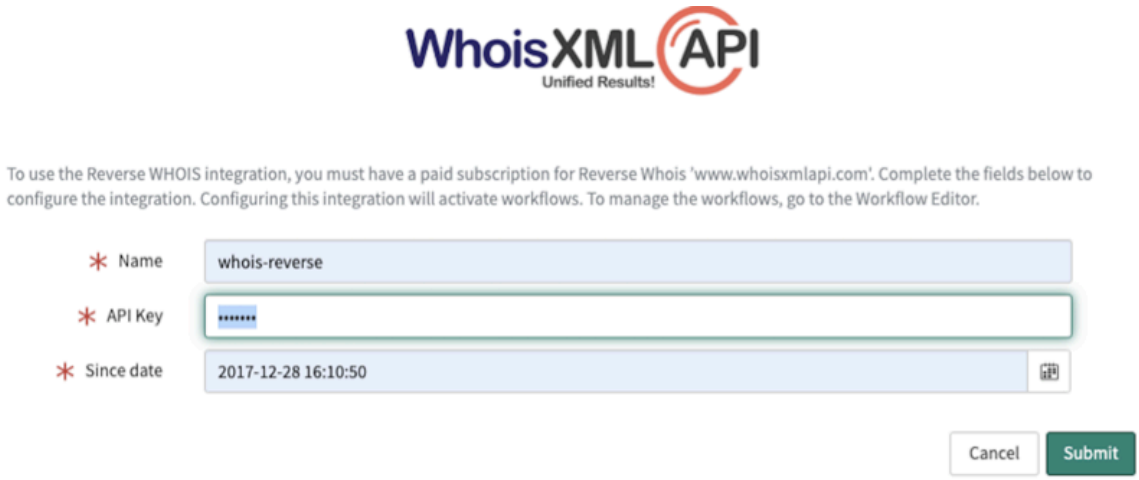
1. Wenn Sie die Anwendung nicht installiert haben, finden Sie unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie Whois API-Kachel.
3. Klicken Sie auf **Konfigurieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



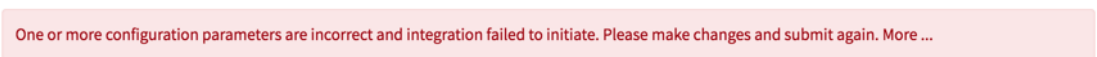
4. In **WHOIS-API-Konfiguration** Dialogfeld: Geben Sie den API-Schlüssel ein, den Sie von der Produktwebsite erhalten haben.



5. Klicken Sie auf **Absenden**.
   Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, eine Fehlermeldung wird angezeigt. Sie können jetzt Ergänzungssuchen für die von zurückgegebenen Domänen ausführen Reverse Whois Integration.

Trouble?
Wenn eine Fehlermeldung angezeigt wird, ist der API-Schlüssel möglicherweise ungültig.

Problembehandlung



Suche für initiieren Reverse Whois

Initiieren Sie Domänensuchen mithilfe von Suchbegriffen in erkennbaren Elementen, die Sie manuell an einen Security Incident-Datensatz anhängen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Automatische Übersetzung

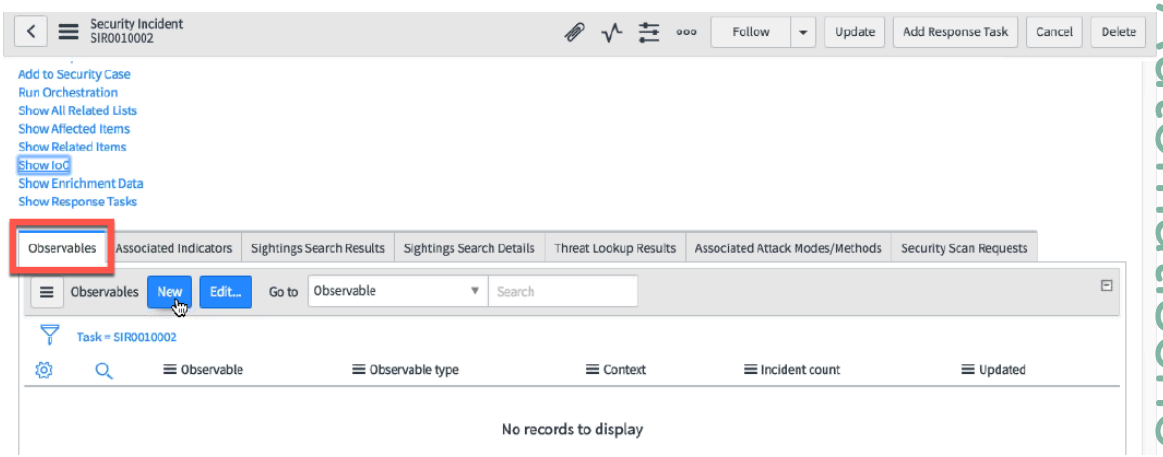
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn nicht geöffnet, navigieren Sie zu **Security Incident** > **Incidents** > **Alle Incidents anzeigen** Und öffnen Sie den Security Incident, mit dem Sie arbeiten.
2. Klicken Sie unten im Datensatz auf **IOC anzeigen** Zugehöriger Link zum Anzeigen der Registerkarte erkennbare Elemente.

Hinweis:

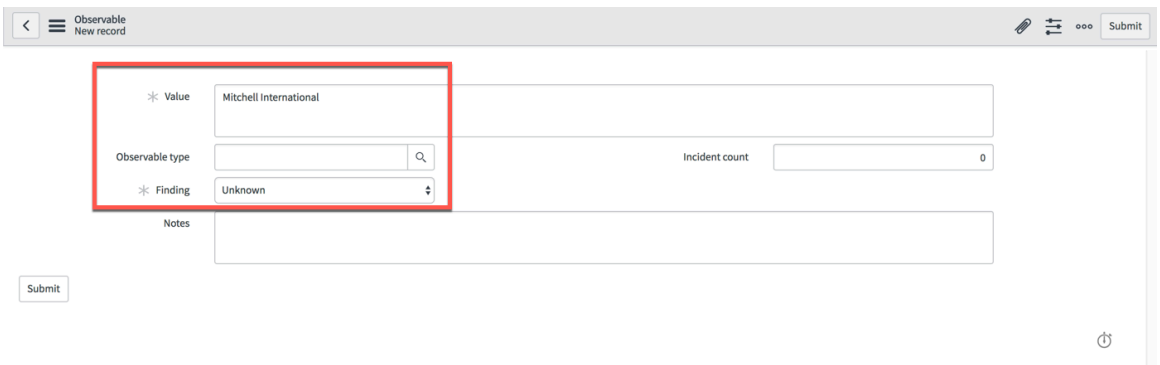
Die Zahlen in den folgenden Schritten werden mit angezeigt **Formulare mit Registerkarten** Einstellung in den Systemeinstellungen aktiv. Wenn keine Registerkarten im Security Incident angezeigt werden, klicken Sie in der oberen rechten Ecke des Bannerrahmens auf **Einstellungen** Zahnradsymbol. In **Systemeinstellungen** Klicken Sie auf das Dialogfeld, das angezeigt wird **Formulare** Und verifizieren Sie das **Formulare mit Registerkarten** Und **Mit dem Formular** Sind ausgewählt.



3. Klicken Sie auf der Registerkarte erkennbare Elemente auf **Neu** .
4. Füllen Sie die Felder aus.

Pflichtfelder im neuen Datensatz

Feld	Beschreibung
Wert	Eindeutiger Suchbegriff für eine Domäne.
Typ des erkennbaren Elements	Dieses Feld wird automatisch gelöscht.
Ergebnis	Dieses Feld wird automatisch auf festgelegt **Unbekannt** .



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Absenden**.
   Sie kehren zum Security Incident-Datensatz zurück, und der Flow initiiert die Suche.

Nächste Maßnahme

Überprüfen Sie die Suchergebnisse für den Security Incident. Weitere Informationen finden Sie unter Überprüfen Sie die erwarteten Ergebnisse für Reverse Whois.

Überprüfen Sie die erwarteten Ergebnisse für Reverse Whois

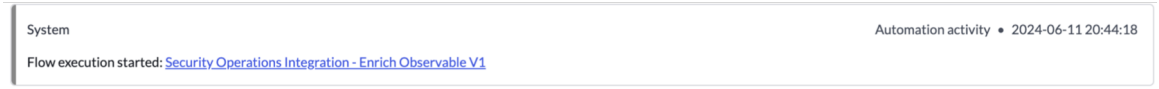
Ergänzungsergebnisse werden auf angezeigt **ReverseWhois-Domänen** Registerkarte unten im Security Incident-Datensatz. Suchen Sie die Suchergebnisse, um sicherzustellen, dass die Suche erfolgreich ausgeführt wurde.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

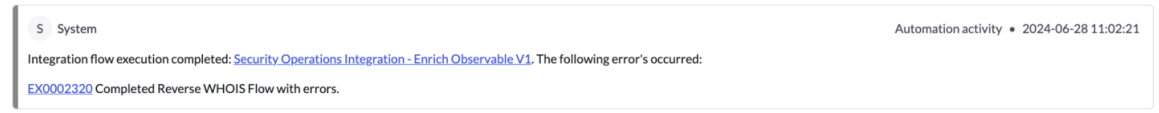
Prozedur

1. Wenn nicht bereits geöffnet, navigieren Sie zu **Security Incidents** > **Incidents** > **Alle Incidents anzeigen** Und suchen Sie den Security Incident, mit dem Sie arbeiten.



   Nachdem die Anwendung konfiguriert wurde und Sie ein erkennbares Element angehängt haben, wird der Flow automatisch gestartet. Die Arbeitsnotizen im Security Incident-Datensatz zeigen den Ausführungs- und Abschlussstatus der Suche an.

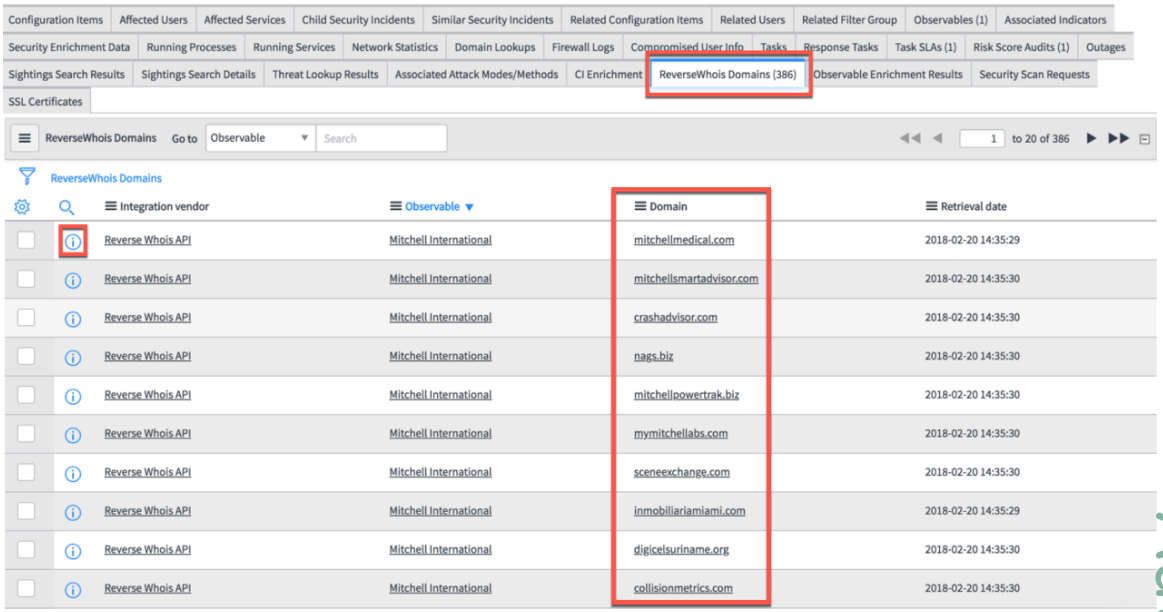
2. Wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde, lesen Sie die Arbeitsnotizen, um weitere Informationen zum Fortfahren zu erhalten.



3. Navigieren Sie zum Ende des Security Incident, und klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Zugehöriger Link.

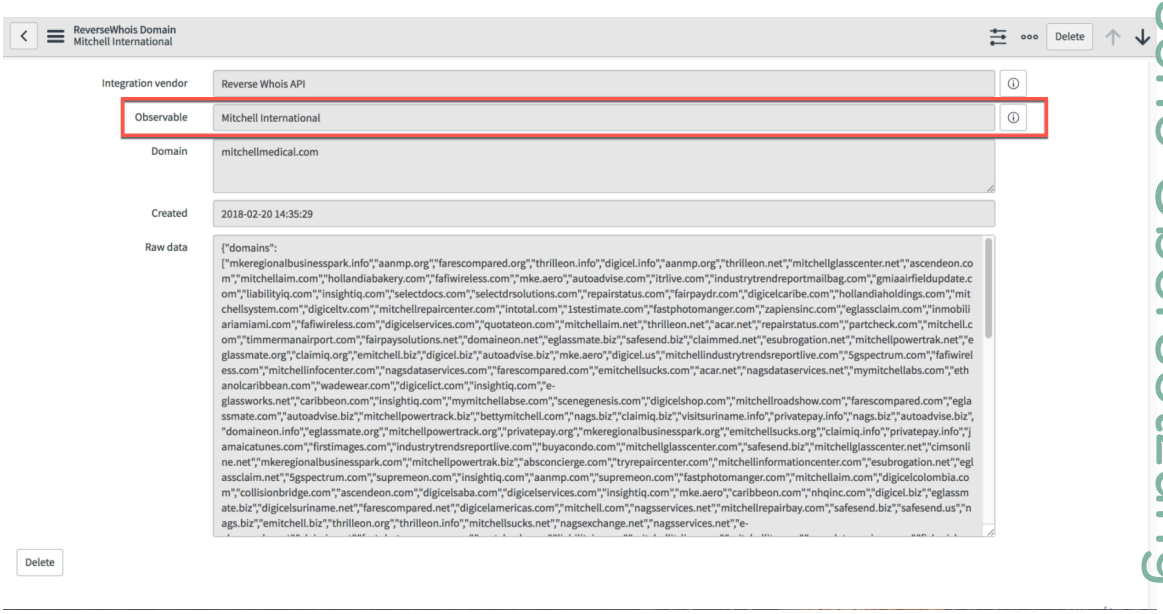
> **Hinweis:**
> Für die gefilterten Suchergebnisse, die in der folgenden Abbildung angezeigt werden, die Konfigurationseinstellungen in Reverse Whois API-Konfigurationskachel wurde mit gespeichert **01.06.1991** In eingegeben **Seit Datum** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ergänzungsergebnisse werden auf angezeigt **ReverseWhois-Domänen** Registerkarte. Die aktiven Domänen für dieses erkennbare Element werden in angezeigt **Domäne** Spalte.

4. Klicken Sie auf das blaue Informationssymbol neben einem Element, und klicken Sie dann auf **Datensatz öffnen** Im angezeigten Dialogfeld.

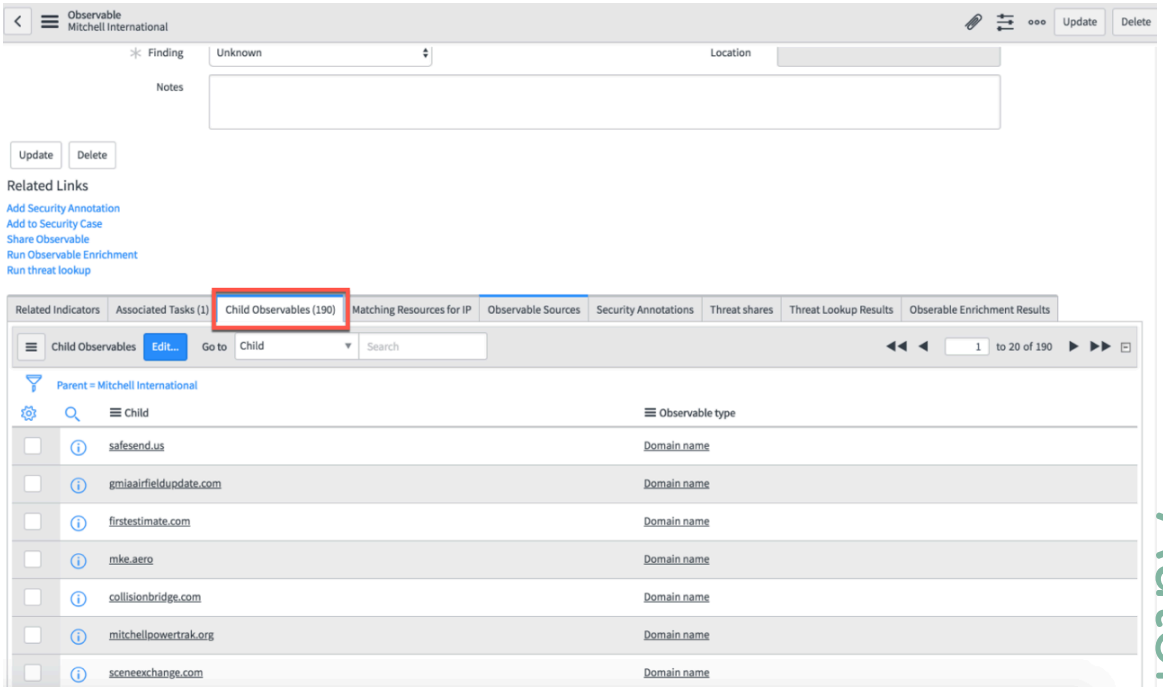


Der Datensatz wird mit Ergänzungsdetails angezeigt, einschließlich der Rohdaten.

5. Navigieren Sie zurück zum Security Incident und mit **ReverseWhois-Domänen** Registerkarte ausgewählt, klicken Sie auf ein erkennbares Element im **Erkennbares Element** Spalte zum Öffnen eines Datensatzes.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die untergeordneten erkennbaren Elemente werden im angezeigt **Untergeordnete Erkennbare Elemente** Registerkarte im Datensatz des erkennbaren Elements. Die untergeordneten erkennbaren Elemente werden nur generiert, wenn die Reverse Whois Anwendung hat Domänen zurückgegeben.

Trouble?

Wenn die Suche nicht erfolgreich abgeschlossen wird, überprüfen Sie, ob die von Ihnen eingegebenen Suchbegriffe von der Integration unterstützt werden. Weitere Informationen finden Sie in den Arbeitsnotizen.

Nächste Maßnahme

Um weitere Ergänzungsdaten zu den Ergebnissen der Domänensuche zu erhalten, können Sie ausführen Whois Integration zum Durchführen von Ergänzungssuchen für die untergeordneten erkennbaren Elemente, die von zurückgegeben werden Reverse Whois Integration. Diese Ergänzungsdaten zu den untergeordneten erkennbaren Elementen enthalten Informationen zum Registrierungsdatum, zum Namen der Registratur und zum Herkunftsland.

(Optional) Ergänzungssuche ausführen und erwartete Ergebnisse für überprüfen Whois

Führen Sie aus Whois Integration zum Durchführen von Ergänzungssuchen für die von zurückgegebenen Domänen Reverse Whois Integration.

Vorbereitungen

Überprüfen Sie, ob Sie installiert und konfiguriert haben Reverse Whois Und Whois Plugins. Führen Sie diese Schritte erst aus, nachdem Sie die Domänensuche mit ausgeführt haben Reverse Whois Plugin erfolgreich.

Erforderliche Rolle: sn_si.Analyst

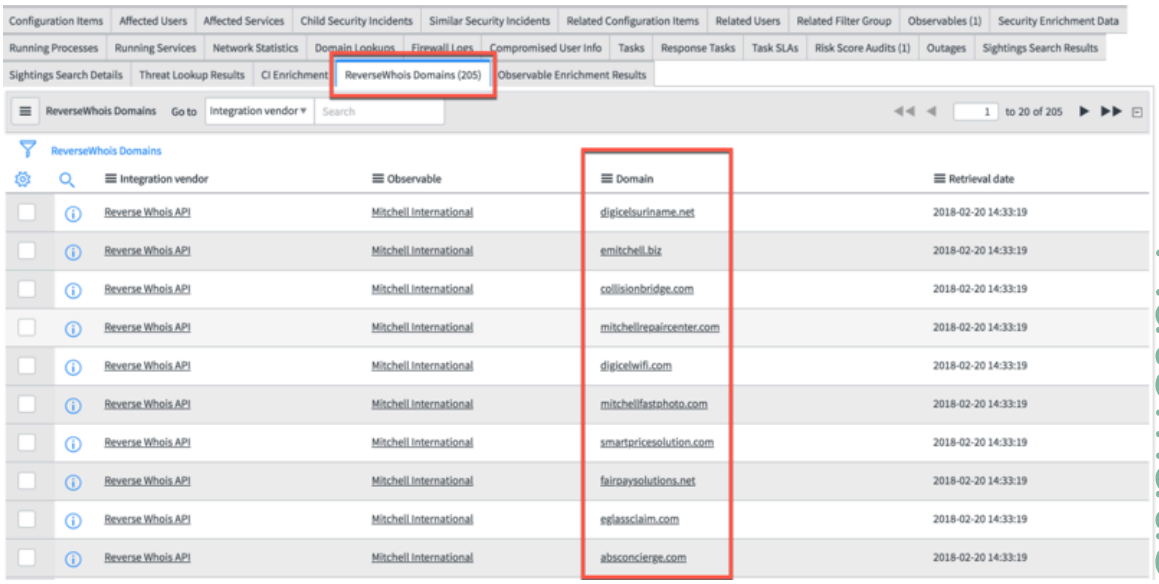
Warum und wann dieser Vorgang ausgeführt wird

Ergebnisse werden auf angezeigt **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte im Datensatz des erkennbaren Elements.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

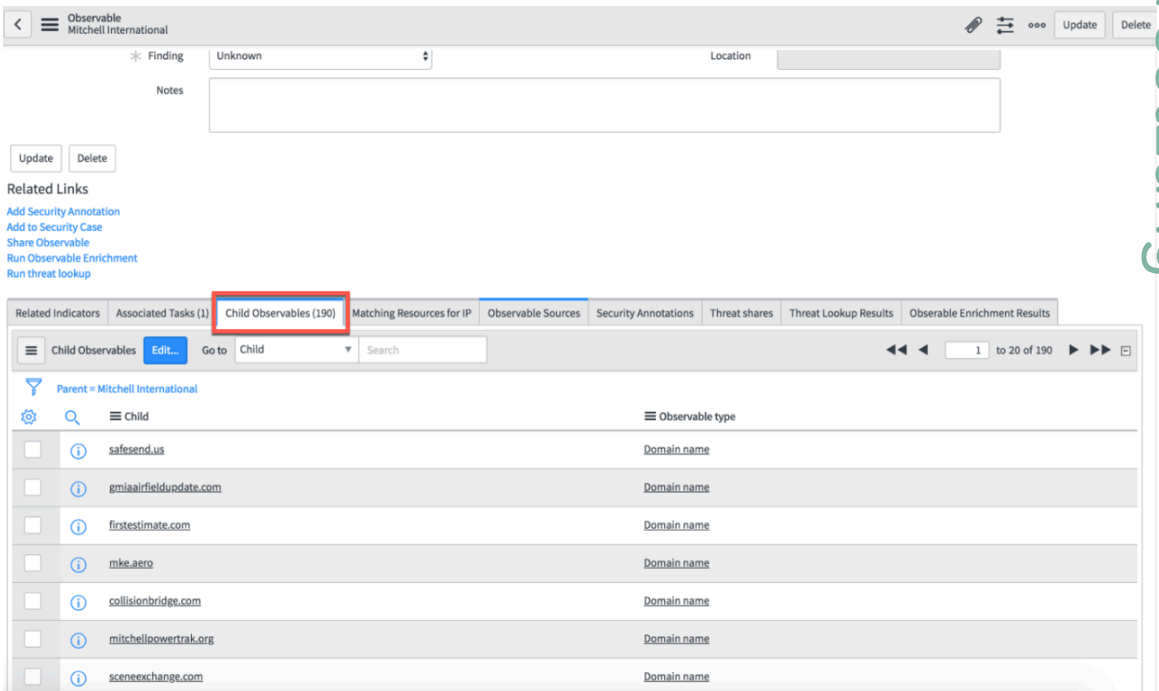
Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Incidents** > **Alle Incidents anzeigen** Und suchen Sie den Security Incident, mit dem Sie arbeiten, der die Domänensuche erfolgreich ausgeführt hat.
2. Öffnen Sie den Datensatz, und klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Zugehöriger Link.
3. Wählen Sie aus **Whois-Domänen Umkehren** Registerkarte unten im Datensatz.



In **Domänen** Spalte, die Liste der zurückgegebenen Domänen wird angezeigt.

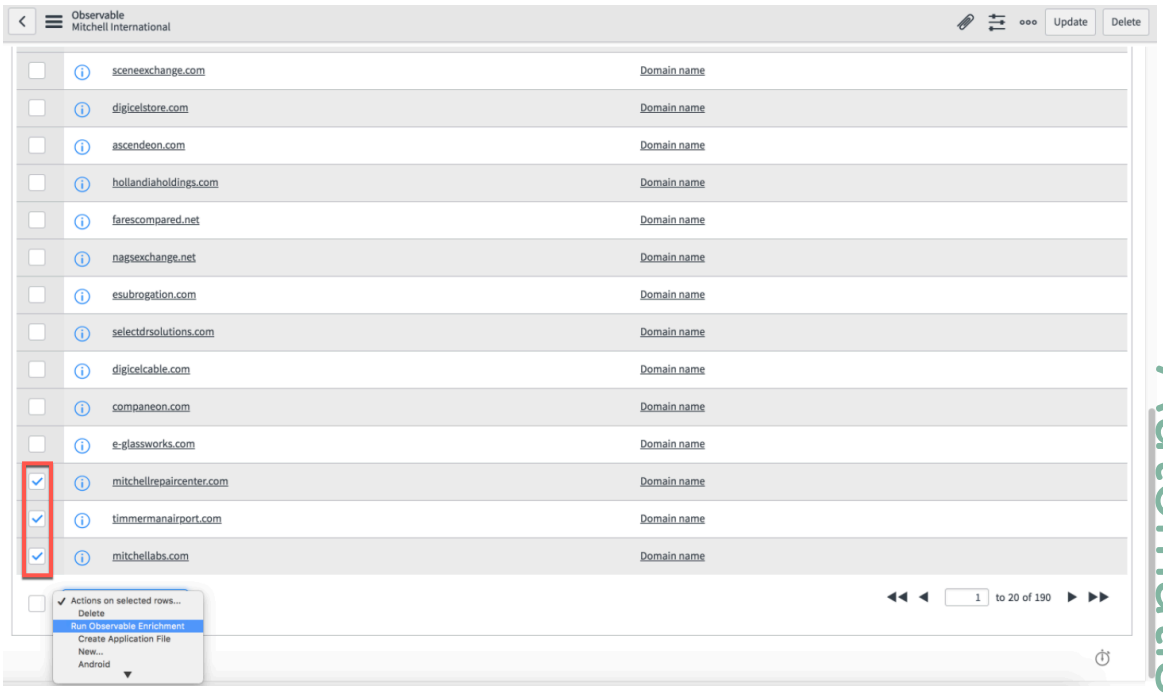
4. In **Erkennbares Element** Spalte auf ein erkennbares Element klicken.
   Auf der **Untergeordnete Erkennbare Elemente** Registerkarte werden die untergeordneten erkennbaren Elemente angezeigt. Die untergeordneten erkennbaren Elemente werden nur generiert, wenn der erste Scan des erkennbaren Elements durch den durchgeführt wird Reverse Whois Anwendung hat Domänen zurückgegeben.



Automatische Übersetzung

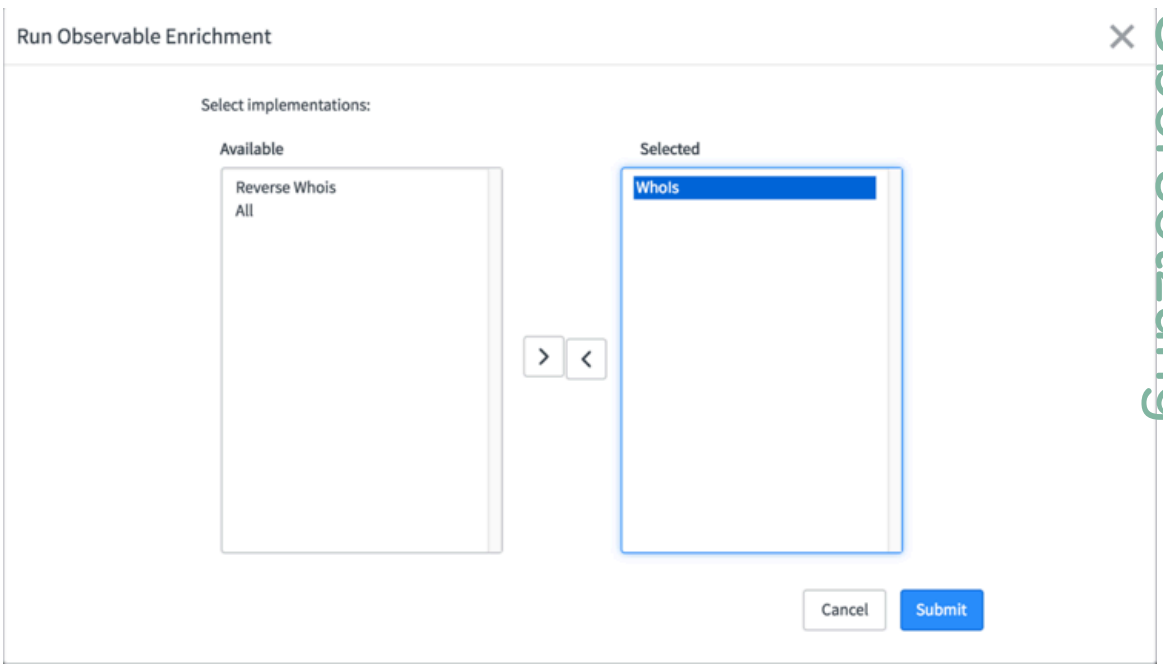
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie die untergeordneten erkennbaren Elemente aus, für die Sie die Ergänzung erkennbarer Elemente ausführen möchten, und im aus **Aktion für ausgewählte Zeilen** Auswahlliste auswählen **Ergänzung Erkennbarer Elemente Ausführen** .



Die **Ergänzung Erkennbarer Elemente Ausführen** Dialogfeld wird angezeigt.

6. Verschieben Sie Whois Integration von **Verfügbar** Bis **Ausgewählt** Und klicken Sie auf **Übermitteln** .

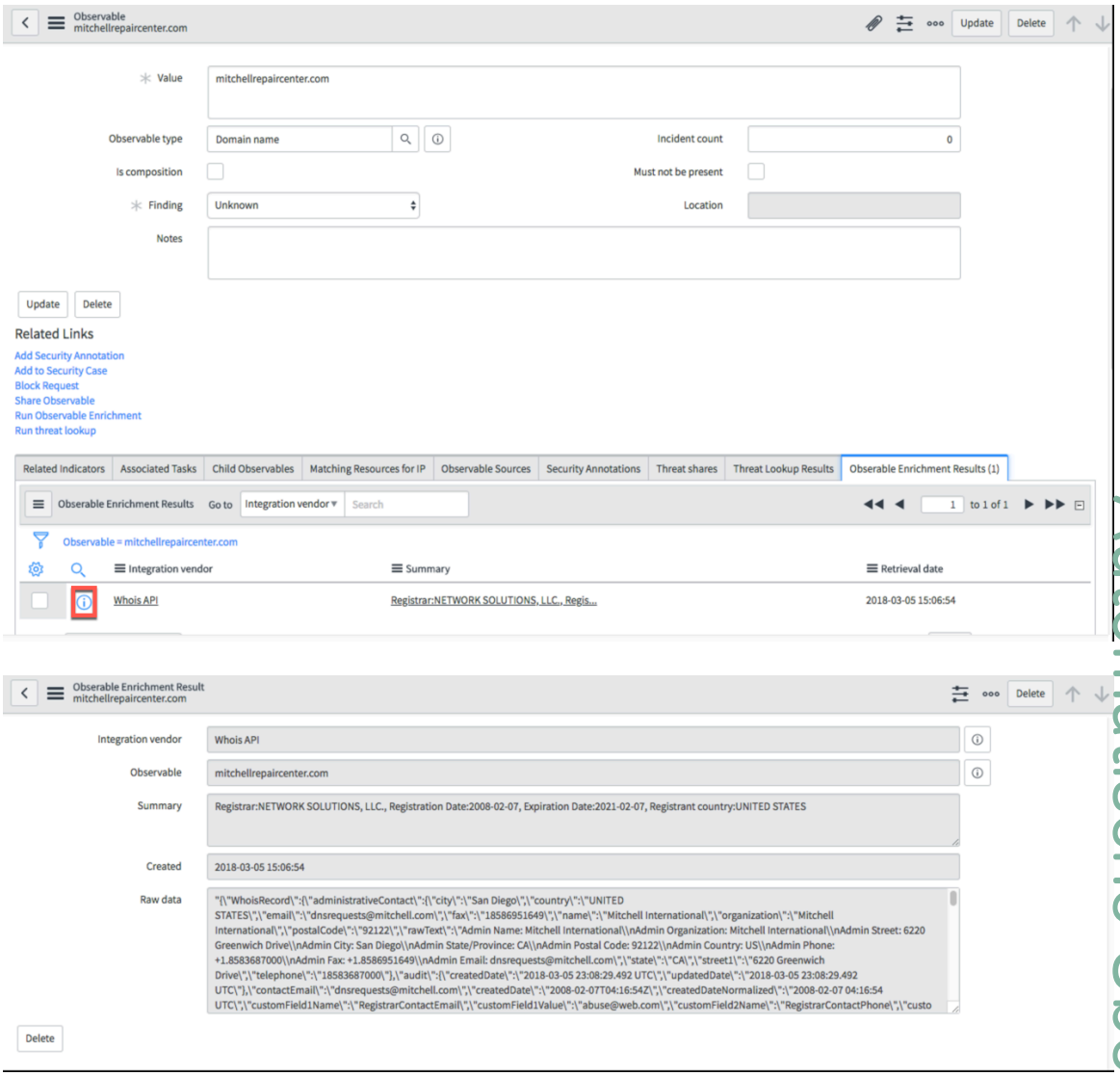


Ergebnisse werden auf angezeigt **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte des Datensatzes des erkennbaren Elements.

7. Klicken Sie auf das blaue Informationssymbol, und klicken Sie dann auf **Öffnen Sie Den Datensatz** Im angezeigten Dialogfeld.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Weitere Informationen und Rohdaten im Zusammenhang mit der ursprünglichen Domänensuche werden angezeigt, z. B. Registrierungsdatum, Name der Registrierungsstelle und Herkunftsland.

Trouble?
Wenn Sie untergeordnete erkennbare Elemente oder Ergänzungsergebnisse nicht finden können, überprüfen Sie, ob Reverse Whois Integration wurde erfolgreich ausgeführt und Domänen zurückgegeben. Weitere Informationen finden Sie auch in den Arbeitsnotizen im Datensatz.

Zugehörige Informationen

Reverse Whois installieren und konfigurieren

Überprüfen Sie die erwarteten Ergebnisse für Reverse Whois

Integration von RISKIQ und WHOISIQ

Mit der Integration von RISKIQ Und WHOISIQ APIs mit ServiceNow AI Platform® Security Operations Produkt- und Sicherheitsanalysten erhalten zusätzliche Ergänzungsdaten und Einblicke in die Gültigkeit von Websites.

Die RISKIQ Die API für SSL-Zertifikate führt Suchen nach SSL-Zertifikaten durch, die Details zur ausstellenden Zertifizierungsstelle, zu Organisationen, die Zertifikate anfordern, zu den Entitätszertifikaten, für die ausgestellt werden, und zur Domäne enthalten. SSL-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsuchen werden automatisch durchgeführt, wenn Security Incidents erstellt werden.

Die RISKIQ WHOISIQ Die API führt Suchen nach anderen erkennbaren Elementen durch, z. B. Domäne, E-Mail, Nameserver, Organisation, Adresse und Telefonnummer. URL und erkennbare Domänenelemente werden automatisch ergänzt, wenn Security Incidents erstellt werden.

Die -Integration erfordert Security Incident Response Und Threat Intelligence Produkte.

Unterstützte erkennbare Elemente für RISKIQ Und RISKIQ WHOISIQ

Die RISKIQ Die API unterstützt automatische SSL-Zertifikatsuchen für erkennbare Elemente wie IP-Adresse, Datei-Hash, Zertifikatseriennummer, Domäne und URL. URL und erkennbare Domänenelemente werden automatisch mit ergänzt WHOISIQ API. Zur Ergänzung erkennbarer Elemente für andere Arten von erkennbaren Elementen mit WHOISIQ API, erstellen Sie erkennbare Elemente, und führen Sie manuell Suchvorgänge aus der Tabelle erkennbarer Elemente aus.

Unterstützte erkennbare Elemente

In der folgenden Tabelle sind der Typ der in dieser Integration verwendeten APIs und die erkennbaren Elemente aufgeführt, die von jeder API unterstützt werden. Die Tabelle gibt auch an, ob eine Suche automatisch erfolgt, wenn Security Incidents erstellt werden, oder ob die Suche manuell aus der Tabelle erkennbarer Elemente ausgeführt wird.

Unterstützte erkennbare Elemente und Suche

API	Unterstützte erkennbare Elemente	Suche (automatisiert oder manuell)
RISKIQ SSL-Zertifikat-API	• IP-Adresse • Datei-Hash (Fingerabdruck des Zertifikats). In der folgenden Abbildung finden Sie ein Beispiel für einen Datei-Hash. • Zertifikatseriennummer oder Seriennummer. Diese Zeichenfolge ist eine eindeutige ID für die Entität. In der folgenden Abbildung finden Sie ein Beispiel für eine Zertifikatseriennummer. • Domäne (`www.site.com` , Oder `site.com`)	Automatisierte Suche, wenn Incidents erstellt werden. Ergebnisse werden auf angezeigt **SSL-Zertifikate** Registerkarte des Security Incident-Datensatzes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte erkennbare Elemente und Suche (Fortsetzung)

API	Unterstützte erkennbare Elemente	Suche (automatisiert oder manuell)
	• URL **Hinweis:** Automatische Scans werden für das URL-Format mit ausgeführt `https://` protokoll, z. B. `https://example.com/index.html`	
RISKIQ WHOISIQ API	• Domäne • URL	Automatisierte Suche, wenn Incidents erstellt werden. Ergebnisse werden auf angezeigt **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte im Security Incident-Datensatz.
RISKIQ WHOISIQ API	• E-Mail-Adresse • Organisationsname • Telefonnummer • Postanschrift	Die manuelle Suche wird über die Tabelle erkennbarer Elemente ausgeführt. Ergebnisse werden auf angezeigt **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte im Datensatz des erkennbaren Elements.

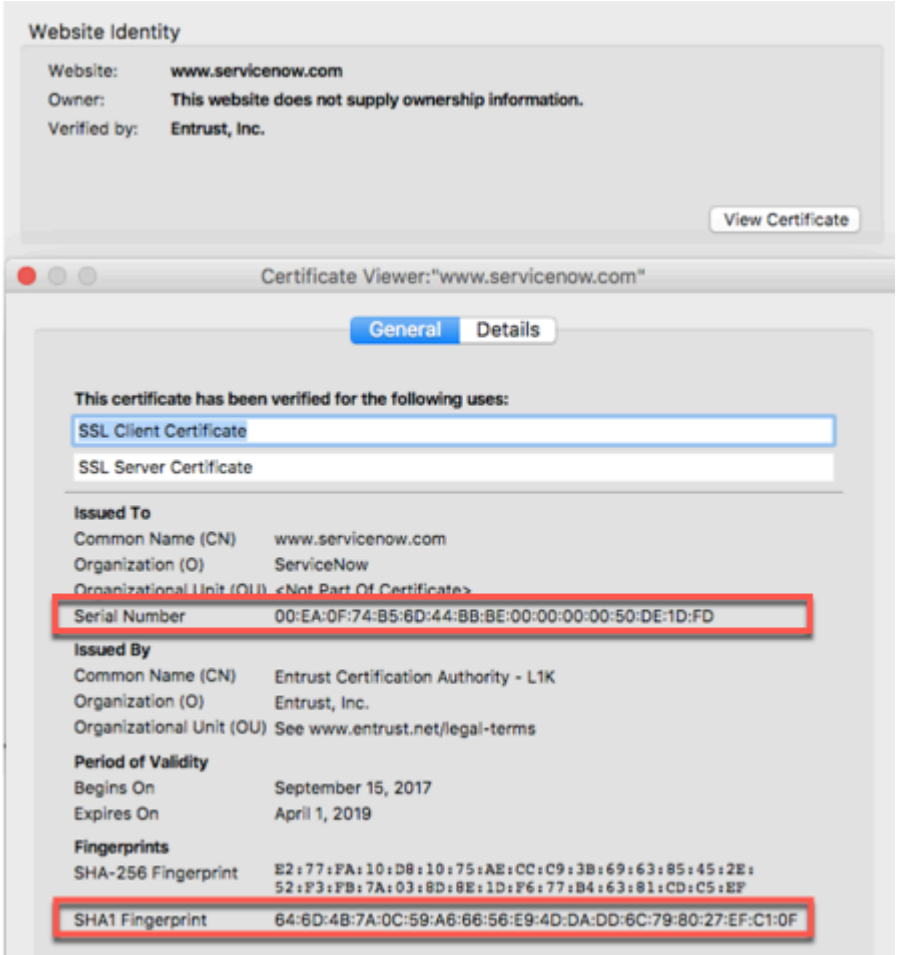
Beispiel für einen Datei-Hash und eine Zertifikatseriennummer

Diese Abbildung zeigt ein Beispiel für die erkennbaren Elemente für Datei-Hash und Zertifikatseriennummer, die für die SSL-Zertifikatsuchen für diese Integration verwendet werden. Der Datei-Hash bezieht sich auf einen SHA-1Fingerabdruck. Dieser Wert wird in angezeigt ServiceNow AI Platform Instanz ohne Doppeltrennzeichen. Beispiel: `646D4B7A0C59A66656E94DDAD6C798027EFC10F` .

Die erkennbare Zertifikatseriennummer bezieht sich auf die eindeutige ID oder Seriennummer für die Entität. Dieser Wert wird auch ohne Doppeltrennzeichen angezeigt. Beispiel: `00EA0F74B56D44BBBE0000000050DE1DFD` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datei-Hash und Seriennummer des Zertifikats



Installieren und konfigurieren RISKIQ Und WHOISIQ

Bevor Sie die Integration auf Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte so aus RISKIQ Und WHOISIQ Anwendungen ordnungsgemäß in integrieren ServiceNow AI Platform Security Operations.

Vorbereitungen

Erforderliche Rolle: administrator, RISKIQ Und WHOISIQ administrator.

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderlichen Rollen zugewiesen haben.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Der Systemadministrator (Administrator) installiert die App und weist die Rolle Security Incident-Administrator (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf Security

Automatische Übersetzung

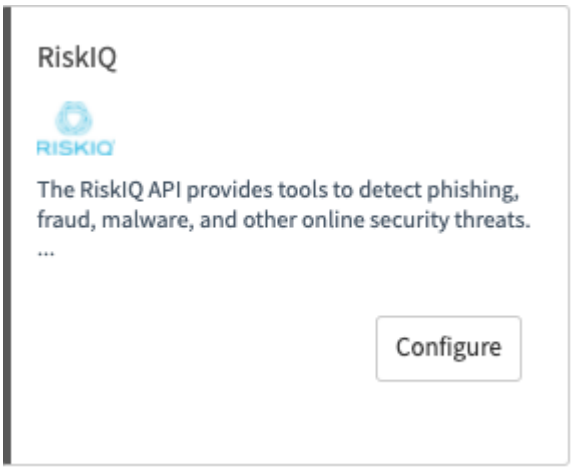
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
	Operations Modul und weist die Rolle Security Incident Analyst (sn_si.Analyst) zu. • Der Security Incident-Analyst (sn_si.Analyst) arbeitet mit Security Incident-Datensätzen.
Erhalten Sie einen Anwendernamen und einen API-Schlüssel.	Besuchen Sie die Website, um Informationen zum API-Schlüssel und zum Erstellen eines Accounts zu erhalten: RISKIQ-Website . Die Konfiguration erfordert, dass Sie den API-Schlüssel eingeben.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	Madrid und spätere Release-Anforderungen Für das Madrid-Release und spätere Familienveröffentlichungen Security Incident Response Abhängigkeits-Plugin (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Für die Integration erforderliche Anwendungen. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. **1.** Security Incident Response **2.** Sicherheits-Integrations-Framework **3.** Security Support Common **4.** Orchestration Des Sicherheitssupports Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz für die Integration finden Sie unter Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

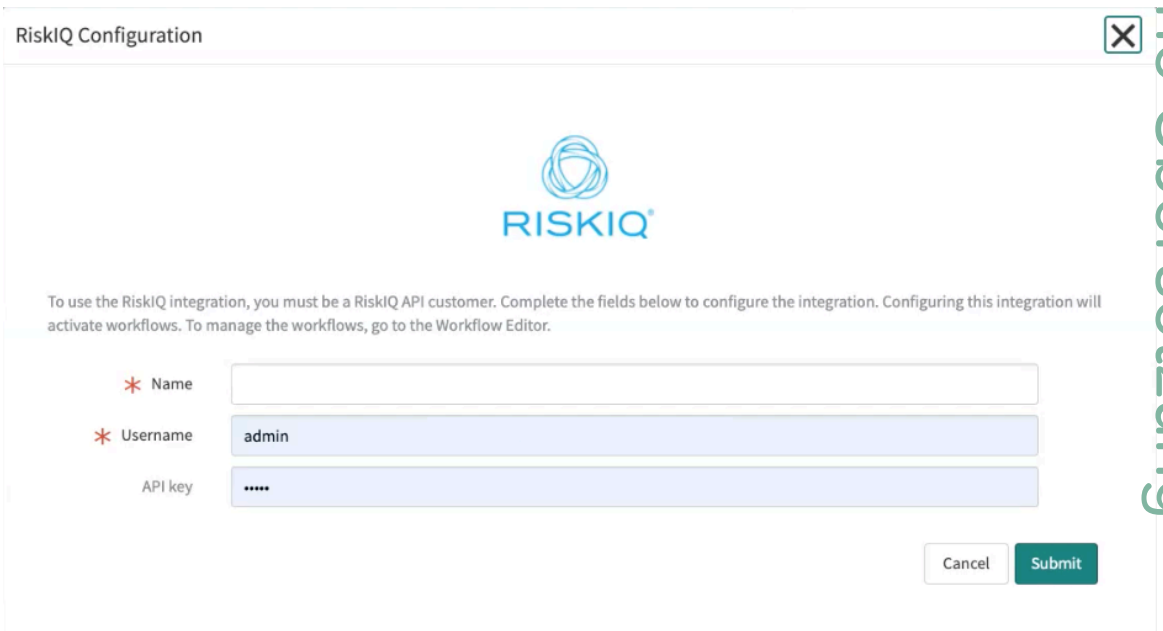
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn Sie die Anwendung für die Integration nicht installiert haben, finden Sie weitere Informationen unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Sobald die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen** Und suchen Sie die API-Kachel.
3. Klicken Sie auf **Konfigurieren**.



4. Geben Sie im angezeigten Dialogfeld „RiskIQ-Konfiguration“ ein **Anwendername** Und **API-Schlüssel** .



5. Klicken Sie auf **Absenden**.
6. Überprüfen Sie die erfolgreiche Konfiguration.
   Wenn die Konfiguration erfolgreich abgeschlossen ist, wird die Seite „Sicherheitsintegrationen“ mit den Integrationskacheln angezeigt.

Trouble?

Wenn eine Fehlermeldung angezeigt wird, ist der Anwendername oder API-Schlüssel möglicherweise ungültig. Überprüfen Sie, ob Ihr Anwendername und der API-Schlüssel korrekt sind:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung

One or more configuration parameters are incorrect and integration failed to initiate. Please make changes and submit again. More ...

Überprüfen Sie die erwarteten Ergebnisse für RISKIQ SSL-Zertifikatsuchen

Wenn ein Security Incident erkennbare Elemente für URLs, Domänen, IP-Adressen, Zertifikatdatei-Hashes (SHA-1-Fingerabdruck) und Zertifikatseriennummern generiert, verwenden Security Incident-Analysten die Ergebnisse der SSL-Zertifikatsuche, um sicherzustellen, dass Sites Zertifikate haben, die von einer vertrauenswürdigen öffentlichen Zertifizierungsstelle (Public Certificate Authority, CA) ausgestellt wurden.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Für unterstützte erkennbare Elemente ServiceNow AI Platform Scannt nach dem neuesten Auftreten von URLs, Domänen, IP-Adressen, Zertifikatdatei-Hashes (SHA-1-Fingerabdruck) und Zertifikatseriennummern. Dies sind mögliche Ergebnisse des Scans:

Eine genaue Übereinstimmung wurde gefunden

Ein gültiger Aussteller eines SSL-Zertifikats wird im Security Incident-Datensatz aufgeführt.

Es wurden keine Zertifikatergebnisse gefunden

Im Security Incident-Datensatz werden keine Ergebnisse aufgeführt.

Für ein selbst signiertes oder intern generiertes Zertifikat wurde eine genaue Übereinstimmung gefunden

Ergebnisse für ein intern generiertes SSL-Zertifikat werden im Security Incident-Datensatz angezeigt.

Für ein primäres SSL-Zertifikat wurde keine genaue Übereinstimmung gefunden

Ein Suchwert gibt mehrere Einträge zurück, und ein primäres Zertifikat kann nicht identifiziert werden. Im Security Incident-Datensatz wird eine Zusammenfassungsnachricht angezeigt.

Prozedur

1. Um die erkennbaren Elemente anzuzeigen und Suchergebnisse zu überprüfen, öffnen Sie den Security Incident-Datensatz, mit dem Sie arbeiten, und suchen Sie die Arbeitsnotizen.

Example

Um Beispiele für die möglichen Suchergebnisse für diese Integration zu veranschaulichen, nehmen Sie an, dass ein Security Incident mit den folgenden erkennbaren Elementen generiert wurde:

- community.servicenow.com
- invalidsubdomain.servicenow.com
- mail.dgnetworks.com
- servicenow.com

Erkennbare Elemente und Speicherort der Suchergebnisse

Erkennbares Element (Beispiel)	Scan-Ergebnisse	Beschreibung und Standort
community.servicenow.com	Zertifikat mit SHA1-Hash gefunden.	Eine genaue Übereinstimmung wurde gefunden, und ein gültiger Aussteller eines SSL-Zertifikats wird aufgelistet. Ergebnisse für

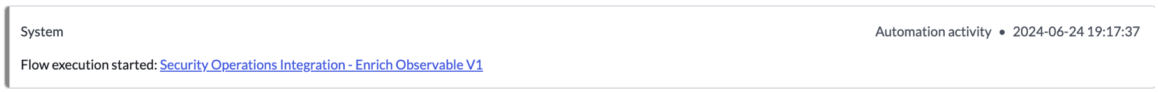
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennbares Element (Beispiel)	Scan-Ergebnisse	Beschreibung und Standort
		die genaue Übereinstimmung werden auf angezeigt **SSL-Zertifikate** Registerkarte im Security Incident-Datensatz.
invalidsubdomain.servicenow.com	Keine Zertifikate gefunden.	Eine Zusammenfassung, die angibt, dass keine Zertifikatergebnisse gefunden wurden, wird auf der angezeigt **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte im Security Incident-Datensatz.
mail.dgnetworks.com	Zertifikat mit SHA1-Hash gefunden.	Eine genaue Übereinstimmung wird für ein selbst signiertes oder intern generiertes Zertifikat aufgelistet. Ergebnisse werden auf angezeigt **SSL-Zertifikate** Registerkarte im Security Incident-Datensatz.
servicenow.com	Suche hat 138 Zertifikate zurückgegeben, und ein einzelnes primäres Zertifikat konnte nicht identifiziert werden.	Für ein primäres SSL-Zertifikat wurde keine genaue Übereinstimmung gefunden, da ein Suchwert mehrere Zertifikate zurückgibt. Eine Zusammenfassung, die angibt, dass kein primäres Zertifikat gefunden wurde, wird auf der angezeigt **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte im Security Incident-Datensatz.

Nachdem die Anwendung konfiguriert wurde, wird der Flow automatisch gestartet. Der Suchstatus und die erkennbaren Elemente werden in den Arbeitsnotizen angezeigt.

2. Überprüfen Sie, ob die Suche erfolgreich ausgeführt wurde.



Trouble?
Wenn Sie die erwarteten Ergebnisse nicht anzeigen können, stellen Sie sicher, dass das erkennbare Element von der SSL-Zertifikatsuche für die Integration unterstützt wird.

Zugehörige Informationen

Unterstützte erkennbare Elemente für RISKIQ Und RISKIQ WHOISIQ

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

RISKIQ SSL-Zertifikatsuchen, die eine genaue Übereinstimmung zurückgeben

RISKIQ Die Ergebnisse der SSL-Zertifikatsuche für eine genaue Übereinstimmung werden auf der angezeigt **SSL-Zertifikate** Registerkarte im Security Incident-Datensatz. Eine genaue Übereinstimmung bietet einen gültigen Zertifizierungsstellennamen, der einem Security Incident-Analyst hilft, die Gültigkeit einer Website zu bestimmen.

Example: Genaue Übereinstimmung für ein gültiges SSL-Zertifikat

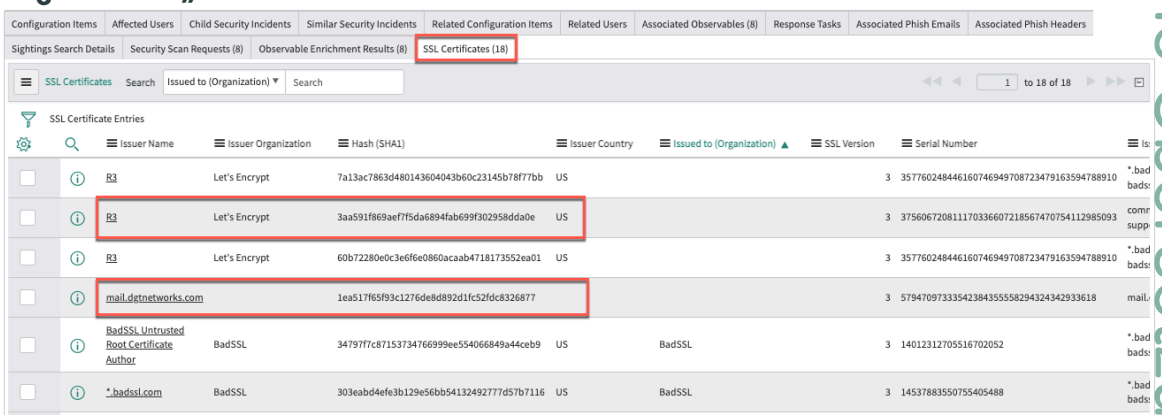
Das folgende Beispiel zeigt einen gültigen Aussteller eines SSL-Zertifikats aus einer genauen Übereinstimmung in den Suchergebnissen. Führen Sie die Schritte aus, um die Ergebnisse und Rohdaten anzuzeigen.

Hinweis:
Die Zahlen in den folgenden Beispielen werden mit angezeigt **Formulare mit Registerkarten** Einstellung in den Systemeinstellungen aktiv. Wenn Ihr Bildschirm nicht mit der unten angezeigten Ansicht übereinstimmt, führen Sie die Schritte aus, um Formulare mit Registerkarten festzulegen.

1. Klicken Sie in der oberen rechten Ecke des Bannerrahmens auf das Symbol Einstellungen.
2. In **Systemeinstellungen** Klicken Sie auf das Dialogfeld, das angezeigt wird **Formulare** Und verifizieren Sie das **Formulare mit Registerkarten** Und **Mit dem Formular** Sind ausgewählt.

1. Klicken Sie im Security Incident-Datensatz auf **SSL-Zertifikate** Registerkarte.

Registerkarte „SSL-Zertifikate“



Informationen über den Namen des Zertifikatausstellers, die Organisation des Ausstellers und die Person, an die das Zertifikat ausgestellt wird (Organisation), werden zusammen mit anderen Daten angezeigt.

18 Elemente werden in angezeigt **Ausstellername** Spalte. Das zweite Element (R3) Stellt einen gültigen Zertifizierungsstellennamen bereit (Verschlüsseln wir) In **Ausstellerorganisation** Spalte.

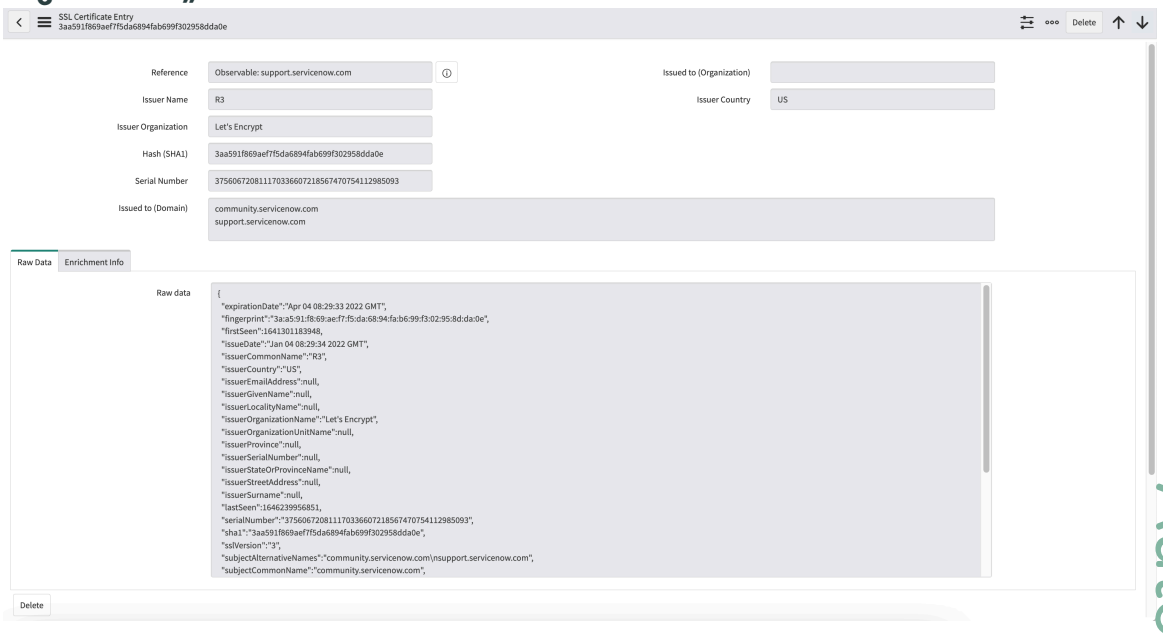
Keine Informationen in **Ausstellerorganisation** Und **Ausgestellt an** Spalten werden für das zweite Element (mail.dgtnetworks.com).

2. Klicken Sie auf das zweite Element in **Ausstellername** Spalte, die (**R3**), um den Eintragsdatensatz zu öffnen. Alternativ können Sie auf das Informationssymbol neben dem Element und gefolgt von klicken **Datensatz öffnen** .
3. Wählen Sie aus **Rohdaten** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Rohdaten“



Der SSL-Zertifikateintrag-Datensatz enthält das erkennbare Element in **Rohdaten** Registerkarte unter **Entitätsname** Spalte sowie andere Daten.

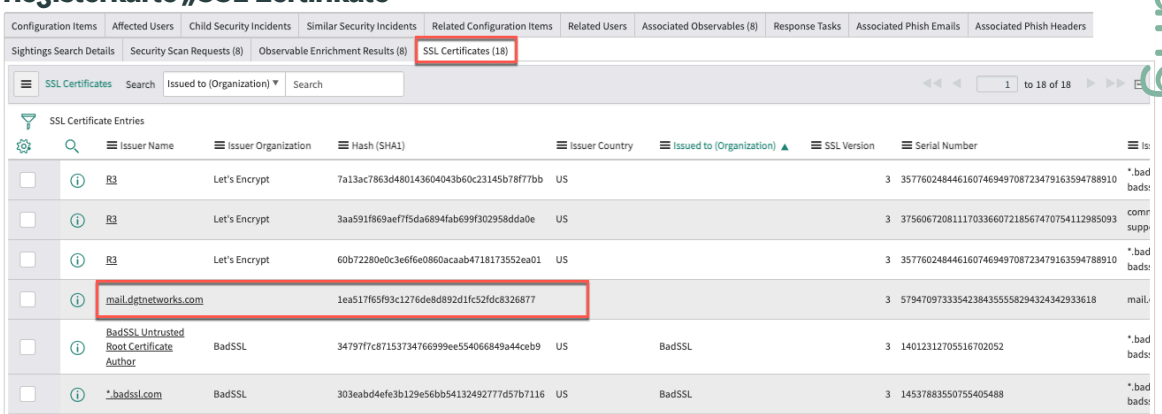
Hinweis in **Kategorie** Spalte, die Betreff , Und Aussteller Entsprechen erkennbaren Entitäten in **Entitätsname** Spalte. Der Aussteller dieses Zertifikats ist höchstwahrscheinlich gültig und stammt von einer vertrauenswürdigen öffentlichen Zertifizierungsstelle. Beachten Sie auch, dass Betreff , Und Aussteller Sind verschiedene Entitäten. Diese separaten Entitäten geben an, dass das Zertifikat kein intern signiertes Zertifikat einer unbekannten Zertifizierungsstelle ist.

Example: Genaue Übereinstimmung für ein selbst signiertes SSL-Zertifikat

Das folgende Beispiel zeigt Ergebnisse für ein selbstsigniertes SSL-Zertifikat aus der Suche. Führen Sie die Schritte aus, um die Ergebnisse und Rohdaten anzuzeigen.

1. Navigieren Sie zurück zum Security Incident-Datensatz. In **Ausstellername** Klicken Sie auf das andere Element (**mail.dgtnetworks.com**).

Registerkarte „SSL-Zertifikate“

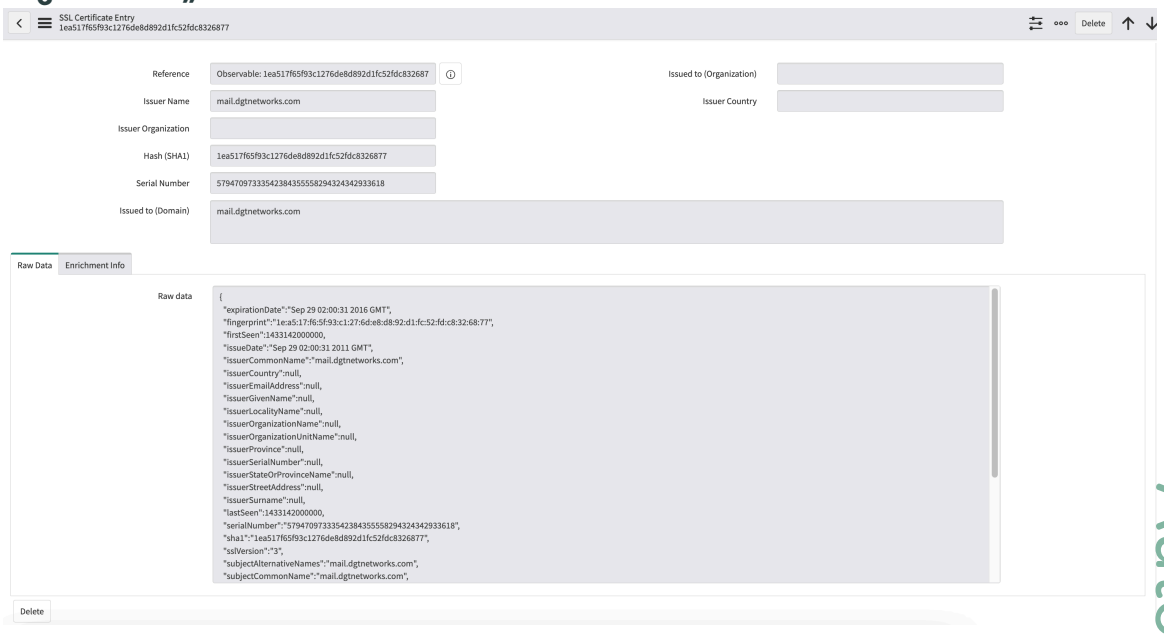


2. Wählen Sie im offenen Datensatz die aus **Rohdaten** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Rohdaten“



Die **Kategorie** Spalte gibt an Aussteller (mail.dgtnetworks.com Und Dgtsbs.DGTNetworks.Local) Sind keine vertrauenswürdigen öffentlichen Zertifizierungsstellen. Beachten Sie auch Aussteller Und Betreff Sind dieselbe Entität (Dgtsbs.DGTNetworks.Local), und jedes enthält den Namen des erkennbaren Elements (DB). Dieses Zertifikat ist möglicherweise ein selbstsigniertes Zertifikat. Selbst signierte Zertifikate können weitere Untersuchungen erfordern, da diese Zertifikate nicht von einer bekannten Zertifizierungsstelle ausgestellt werden.

RISKIQ SSL-Zertifikatsuchen, die mehrere Zertifikate oder keine Zertifikate zurückgeben

Ein Security Incident-Analyst kann mehrere SSL-Zertifikatergebnisse verwenden, um zu bestimmen, ob eine Site Teil einer gemeinsamen, erkennbaren Entität ist. Keine Ergebnisse von SSL-Zertifikaten können darauf hindeuten, dass Websites mit obskuren oder verdächtigen Namen keine vertrauenswürdigen Zertifikate haben. Suchergebnisse für erkennbare Elemente, die keine SSL-Zertifikate zurückgeben oder mehrere SSL-Zertifikate zurückgeben, werden im angezeigt Ergebnisse Der Anreicherung Erkennbarer Elemente Registerkarte im Security Incident-Datensatz.

Example: Keine SSL-Zertifikatergebnisse oder mehrere SSL-Zertifikatergebnisse

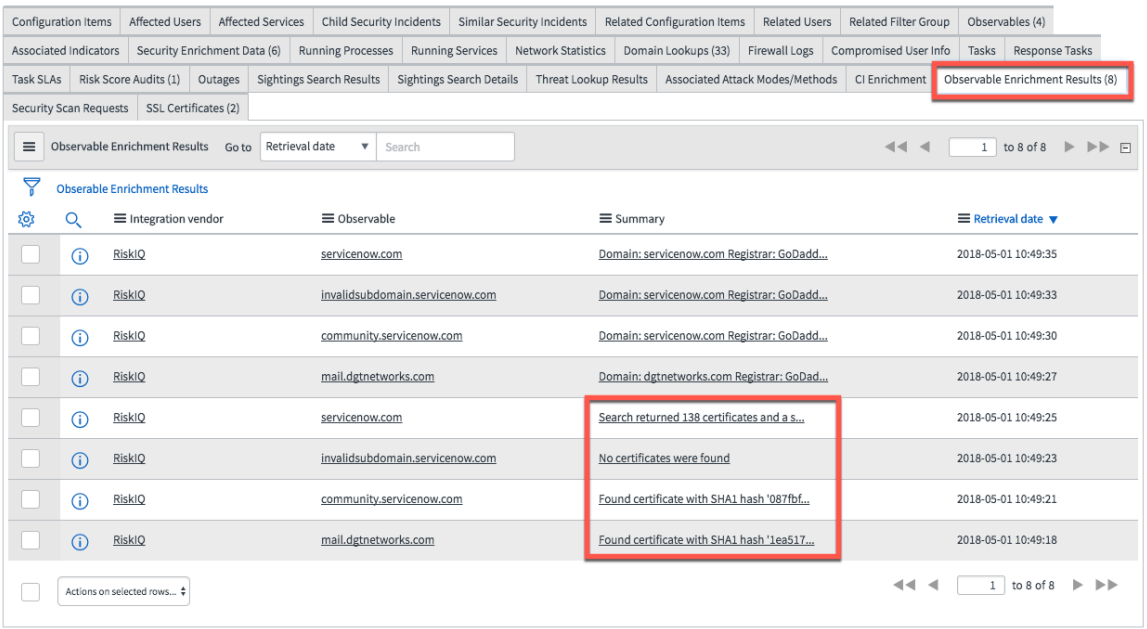
Führen Sie die Schritte aus, um die Ergebnisse für erkennbare Elemente anzuzeigen, die keine SSL-Zertifikate oder mehrere Zertifikate zurückgeben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Klicken Sie im Security Incident-Datensatz auf **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte.

Registerkarte „Ergebnisse der Anreicherung erkennbarer Elemente“

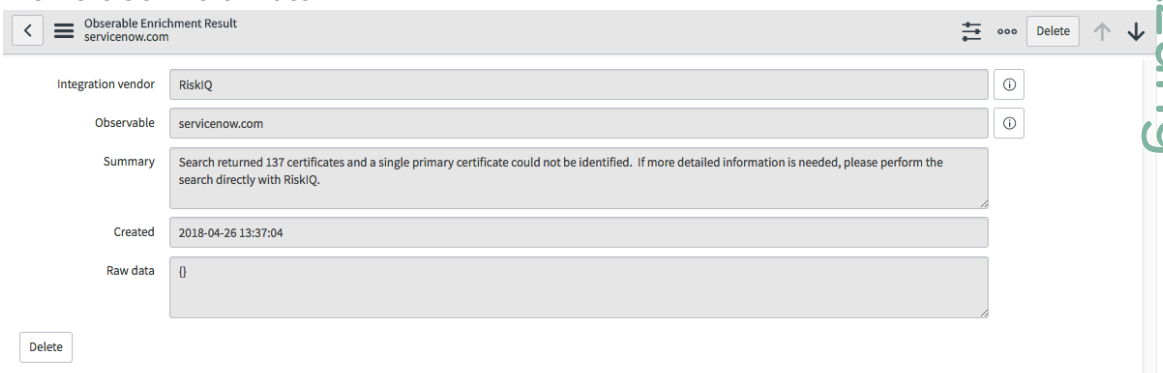


Die Ergänzungsergebnisse erkennbarer Elemente für RISKIQ Und WHOISIQ Suche wird angezeigt.

In **Erkennbares Element** Spalte, servicenow.com Entspricht Suche hat 138 Zertifikate zurückgegeben Nachricht in **Zusammenfassung** Spalte. In Ähnlicher Weise invalidsubdomain.servicenow.com Entspricht Es wurden keine Zertifikate gefunden In **Zusammenfassung** Spalte. Diese Zusammenfassungen zeigen an, dass mehrere SSL-Zertifikate gefunden wurden und dass keine genauen Übereinstimmungen für SSL-Zertifikate gefunden wurden.

2. In **Erkennbares Element** Klicken Sie auf die Spalte **servicenow.com** .

Mehrere SSL-Zertifikate



Die Zusammenfassungsnachricht, die im Datensatz angezeigt wird, gibt an, dass mehrere Ergebnisse für SSL-Zertifikate für zurückgegeben wurden servicenow.com , Und ein primäres SSL-Zertifikat konnte nicht abgeglichen werden. Diese Nachricht wird häufig bei Suchen zurückgegeben, die allgemeine Domänennamen enthalten, z. B. servicenow.com .

Wenn Sie weitere Informationen zu einer allgemeinen Domäne benötigen, können Sie die Suche direkt mit durchführen RISKIQ API.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Navigieren Sie zurück zu **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte und in der **Erkennbares Element** Klicken Sie auf die Spalte **invalidsubdomain.servicenow.com** .

Hinweis:

- Wenn für das aktuelle erkennbare Element keine SSL-Zertifikate gefunden werden, wird im Feld Zusammenfassung die folgende Meldung angezeigt: Es wurden keine Zertifikate gefunden .
- Wenn für das aktuelle erkennbare Element keine aktiven SSL-Zertifikate gefunden werden, wird im Feld Zusammenfassung die folgende Meldung angezeigt: Es wurden keine aktiven Zertifikate gefunden .

Überprüfen Sie die erwarteten Ergebnisse für WHOISIQ URL-Suchen

Wenn ein Security Incident erkennbare Elemente für URLs oder Domänen generiert, wird der WHOISIQ Die API führt die Ergänzung erkennbarer Elemente bei der Erstellung von Security Incidents automatisch durch. Die Suchergebnisse werden auf angezeigt **Ergebnisse Der Anreicherung Erkennbarer Elemente** Und **SSL-Zertifikate** Registerkarten im Security Incident-Datensatz.

Vorbereitungen

Hinweis:

Die Zahlen in den folgenden Schritten werden mit angezeigt **Formulare mit Registerkarten** Einstellung in den Systemeinstellungen aktiv.

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

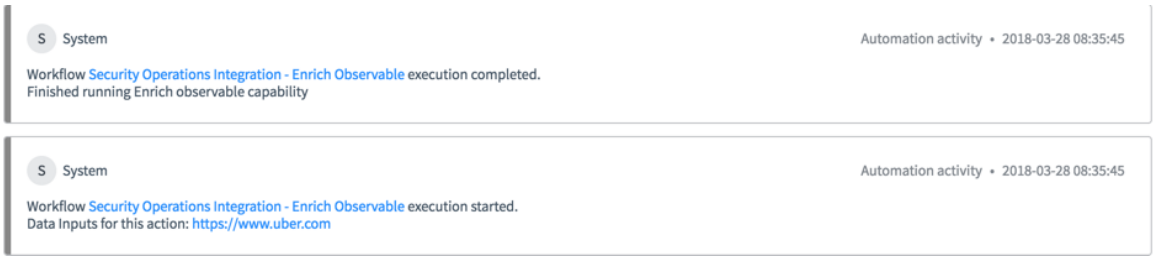
Ergänzungsergebnisse erkennbarer Elemente werden auf angezeigt **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte unten im Security Incident-Datensatz. Für unterstützte erkennbare Elemente wird auch eine SSL-Zertifikatsuche ausgeführt, und die Ergebnisse werden im angezeigt **Registerkarte „SSL-Zertifikate“** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie den Security Incident-Datensatz, mit dem Sie arbeiten, und überprüfen Sie, ob die Suche in den Arbeitsnotizen erfolgreich ausgeführt wurde.



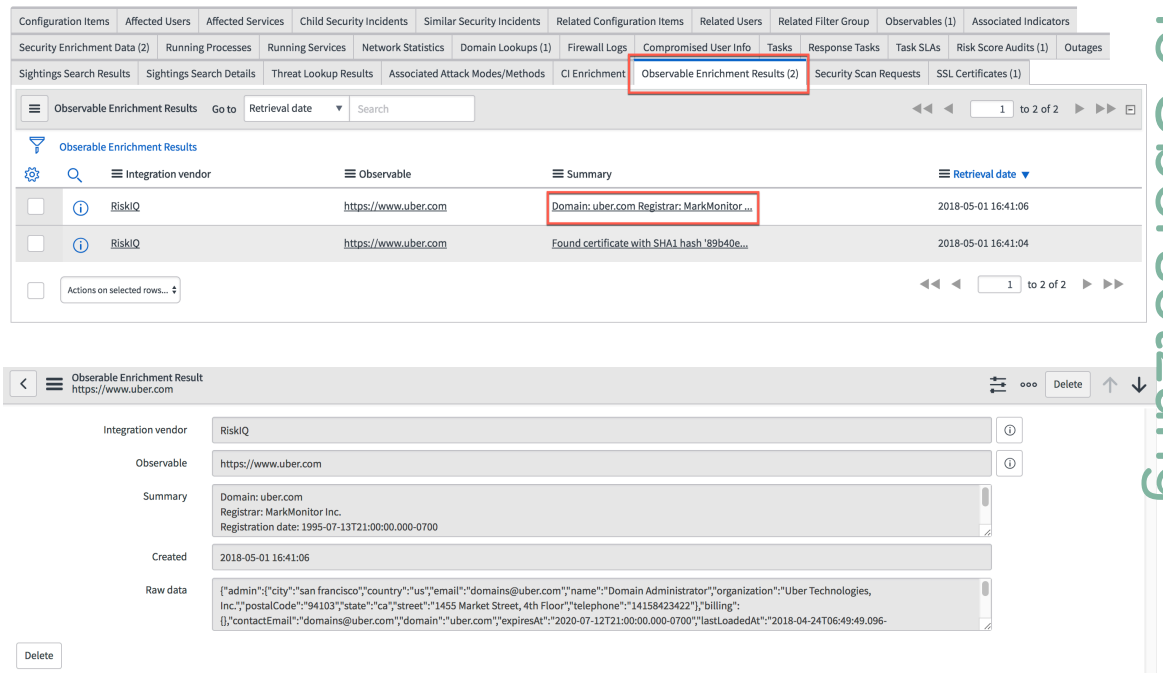
   Sobald die Anwendung konfiguriert ist, wird der Flow bei der Incident-Erstellung automatisch gestartet. Der Ausführungs- und Abschlussstatus der Suche wird in den Arbeitsnotizen im Security Incident-Datensatz angezeigt.

2. Wenn Sie nicht überprüfen können, ob die Suche erfolgreich ausgeführt wurde, lesen Sie die Arbeitsnotizen, um weitere Informationen zum Fortfahren zu erhalten.

3. Klicken Sie im offenen Security Incident auf **Alle Zugehörigen Listen Anzeigen** Zugehöriger Link.

4. Klicken Sie auf **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte, um sie auszuwählen.

5. In **Zusammenfassung** Spalte auf das erste Element klicken, **Domäne: uber.com Registrierungsstelle: MARKMONITOR...** .

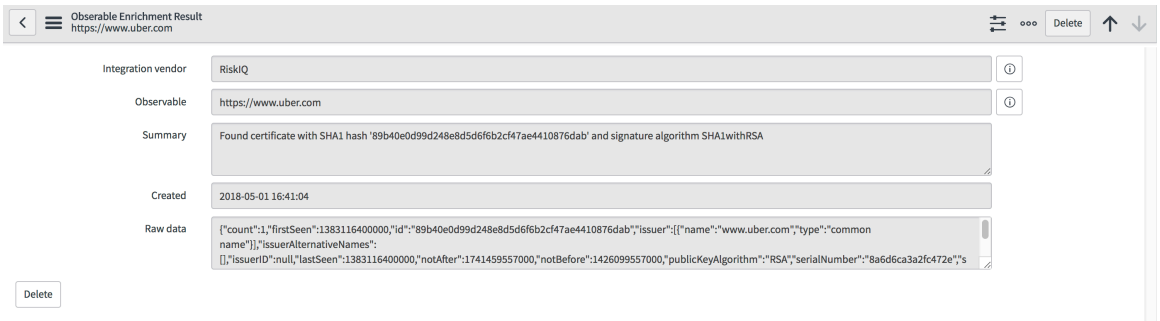


   Der angezeigte Datensatz enthält Informationen zur Domäne.

6. Navigieren Sie zurück zu **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte und in der Registerkarte **Zusammenfassung** Spalte auf das zweite Element klicken, **Zertifikat mit SHA1-Hash gefunden...** .

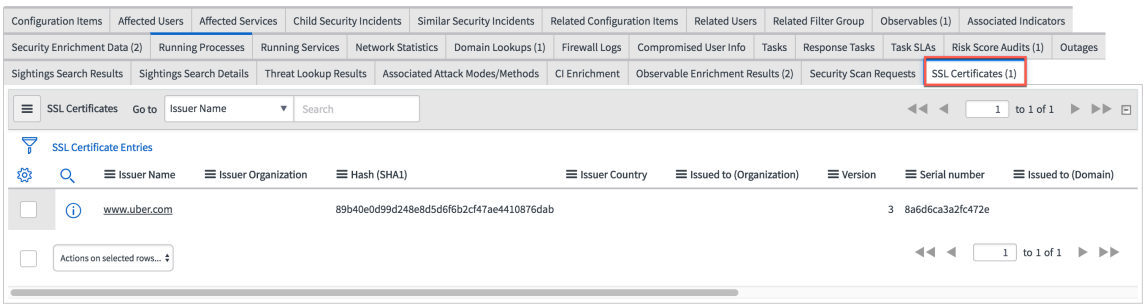
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieser Datensatz gibt an, dass ein SSL-Zertifikat mit einem Datei-Hash gefunden wurde.

7. Navigieren Sie zurück zum Security Incident-Datensatz, und klicken Sie auf **SSL-Zertifikate** Registerkarte.



Die SSL-Zertifikatergebnisse für den Datei-Hash werden auch hier angezeigt.

Trouble?

Wenn Sie die erwarteten Ergebnisse nicht anzeigen können, überprüfen Sie die Arbeitsnotizen. Stellen Sie außerdem sicher, dass das erkennbare Element für die Suche durch die Integration unterstützt wird.

Zugehörige Informationen

Unterstützte erkennbare Elemente für RISKIQ Und RISKIQ WHOISIQ

Erstellen Sie ein erkennbares Element für manuell WHOISIQ Suchvorgänge

Security Incident-Analysten verwenden Informationen aus der Ergänzung erkennbarer Elemente mit WHOISIQ API, um mehr über die E-Mail-Adressen, Namen und Telefonnummern von Organisationen zu erfahren.

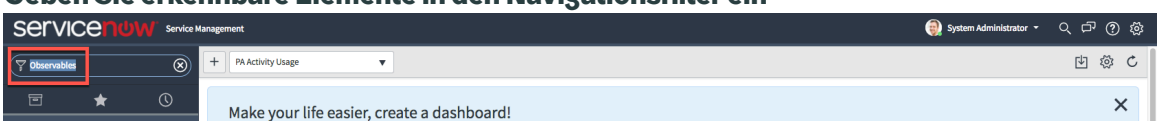
Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Alle** > **IoC-Repository** > **Erkennbare Elemente**an.

Geben Sie erkennbare Elemente in den Navigationsfilter ein

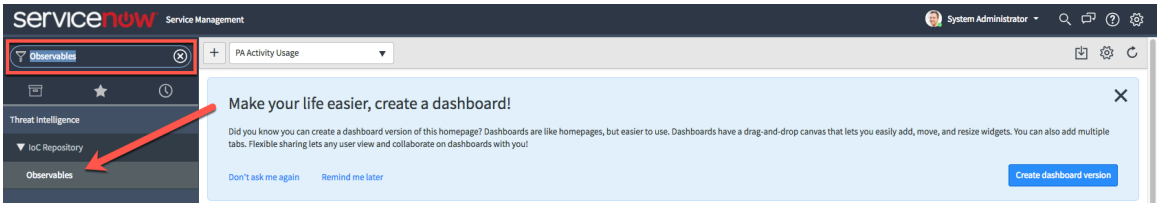


Im Navigationsbereich wird das Modul erkennbare Elemente angezeigt.

Automatische Übersetzung

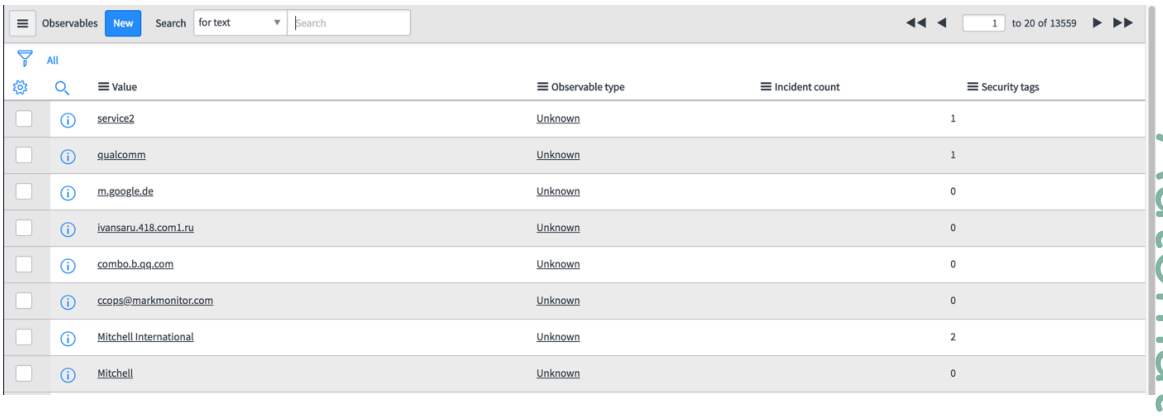
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul „erkennbare Elemente“



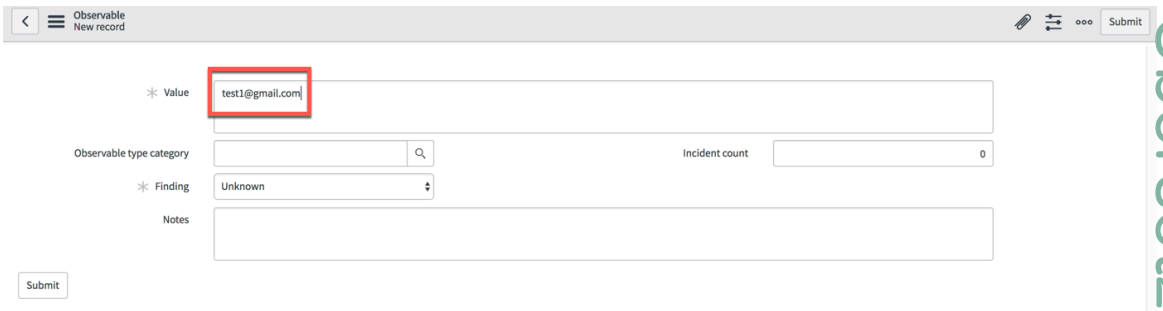
2. Klicken Sie auf **Erkennbare Elemente** Modul zum Anzeigen der Liste erkennbarer Elemente.

Liste erkennbarer Elemente



3. Klicken Sie Auf **Neu** Um ein neues erkennbares Element zu erstellen.
4. Füllen Sie die Felder im Formular „erkennbares Element“ aus.

Erstellen Sie ein neues erkennbares Element



5. Klicken Sie auf **Absenden**.
   Sie kehren zur Liste erkennbarer Elemente zurück. In **Wert** Spalte, wird Ihr neues erkennbares Element angezeigt.

> **Hinweis:**
> Wenn Sie Ihr erkennbares Element in dem angezeigten Teil der Liste nicht finden können, verwenden Sie die Suchfunktion, um es zu finden.

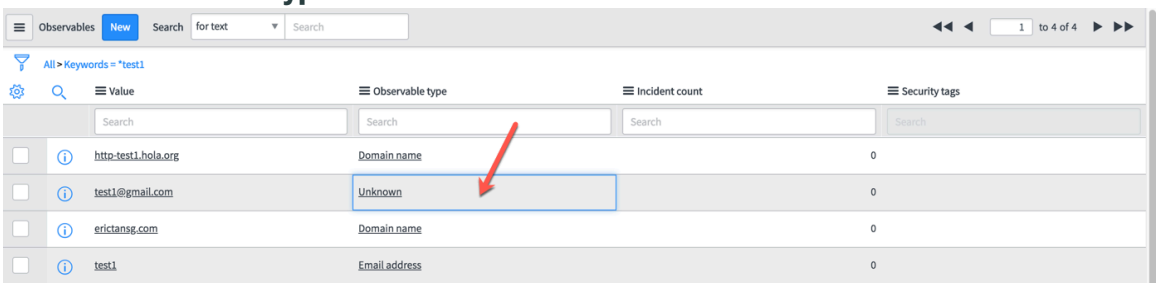
6. Bearbeiten Sie **Typ des erkennbaren Elements** Feld, aus dem der Typ geändert werden soll **Unbekannt** Bis **E-Mail-Adresse** Um Ihrem erkennbaren Element zu entsprechen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. In **Typ des erkennbaren Elements** Spalte, Einzelklick rechts neben **Unbekannt** Text zum Auswählen.

Wählen Sie das Feld Typ des erkennbaren Elements aus

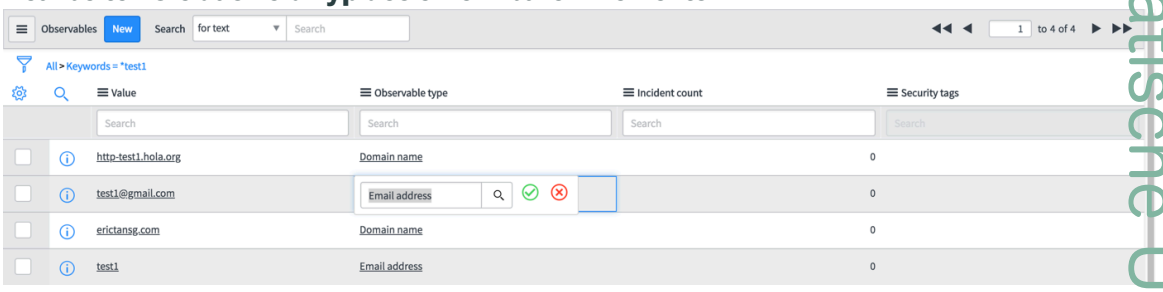


Das ausgewählte Feld ist blau umrissen.

b. Doppelklicken Sie auf eine beliebige Stelle innerhalb des hervorgehobenen Felds, um den Editor zu öffnen.

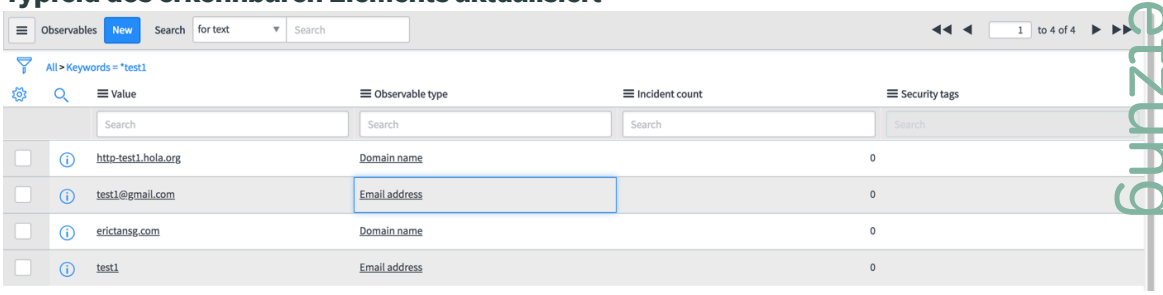
c. Geben Sie im angezeigten Feld den Typ des erkennbaren Elements ein (E-Mail-Adresse) Und klicken Sie auf das grüne Häkchen, um den Wert zu speichern.

Bearbeiten Sie das Feld Typ des erkennbaren Elements



In **Typ des erkennbaren Elements** Spalte in der Liste, E-Mail-Adresse Wird für Ihr neues erkennbares Element angezeigt.

Typfeld des erkennbaren Elements aktualisiert



Nächste Maßnahme

Wenn Sie ein erkennbares Element für die Suche erstellt und bearbeitet haben, führen Sie die Ergänzungssuche für erkennbare Elemente aus dem Datensatz erkennbarer Elemente mit aus WHOISIQ API.

Überprüfen Sie die erwarteten Ergebnisse für manuell WHOISIQ Suchvorgänge

Führen Sie eine manuelle Suche nach einem erkennbaren Element aus, wenn es nicht automatisch einen Security Incident generiert. Für Ergänzungssuchen erkennbarer Elemente mit WHOISIQ API für E-Mail-Adressen, Organisationsnamen, Telefonnummern oder Mailadressen initiieren Sie die Suche manuell aus der Tabelle erkennbarer Elemente.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

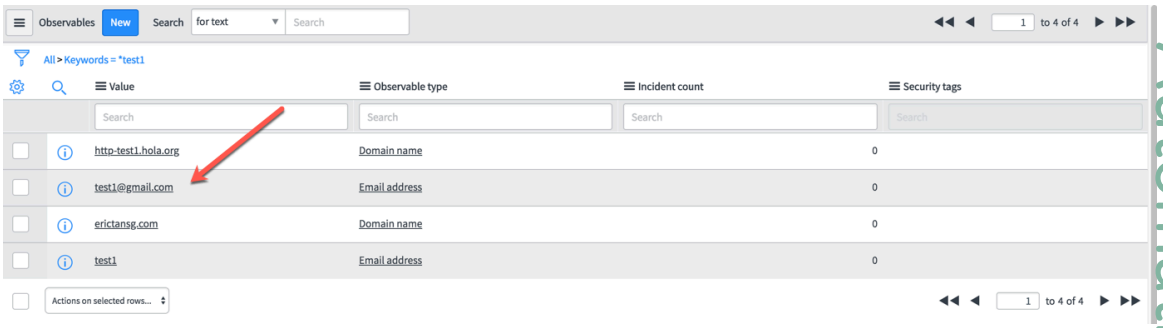
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

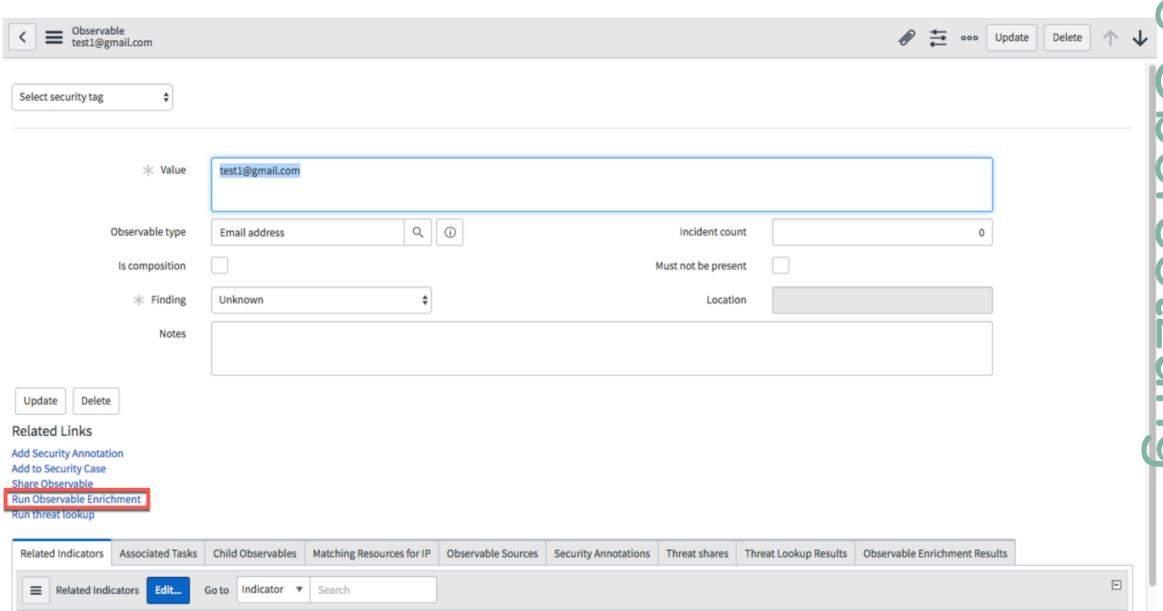
Erstellen Sie ein erkennbares Element für eine manuelle Suche mit WHOISIQ API. Weitere Informationen zum Erstellen und Bearbeiten eines erkennbaren Elements finden Sie unter Erstellen Sie ein erkennbares Element für manuell WHOISIQ Suchvorgänge.

Prozedur

1. Navigieren zu **Alle** > **IoC-Repository** > **Erkennbare Elemente** Und suchen Sie das erkennbare Element in der Liste, mit der Sie arbeiten.
2. Klicken Sie im auf Ihr erkennbares Element **Wert** Spalte zum Öffnen des Datensatzes.



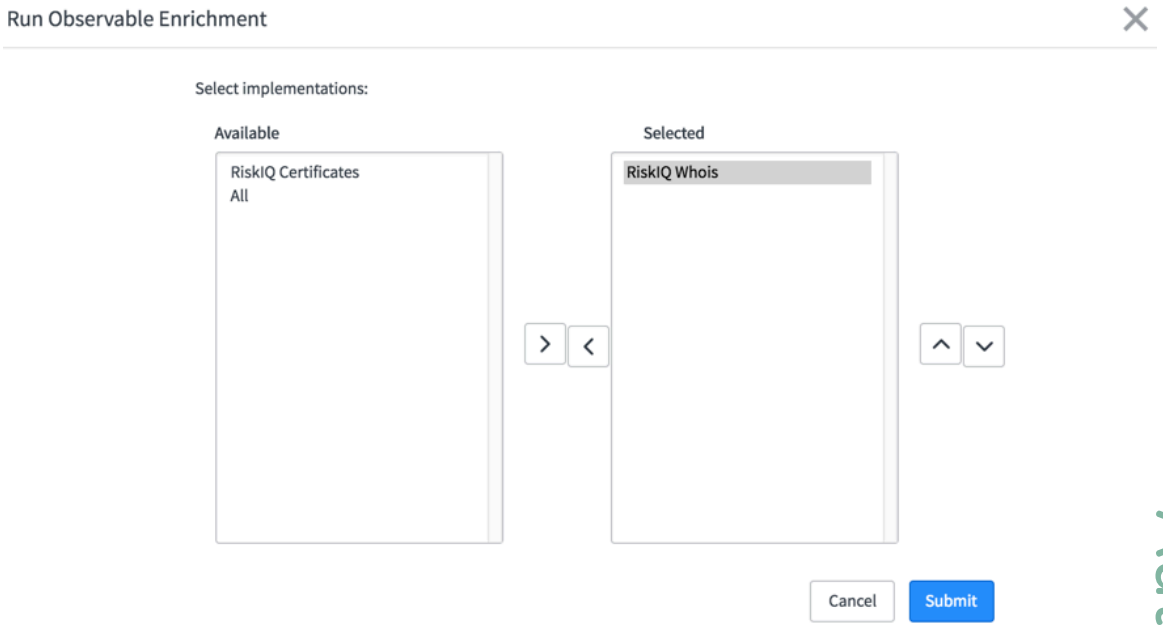
3. Klicken Sie auf **Ergänzung Erkennbarer Elemente Ausführen** Zugehöriger Link zum Ausführen der Suche.



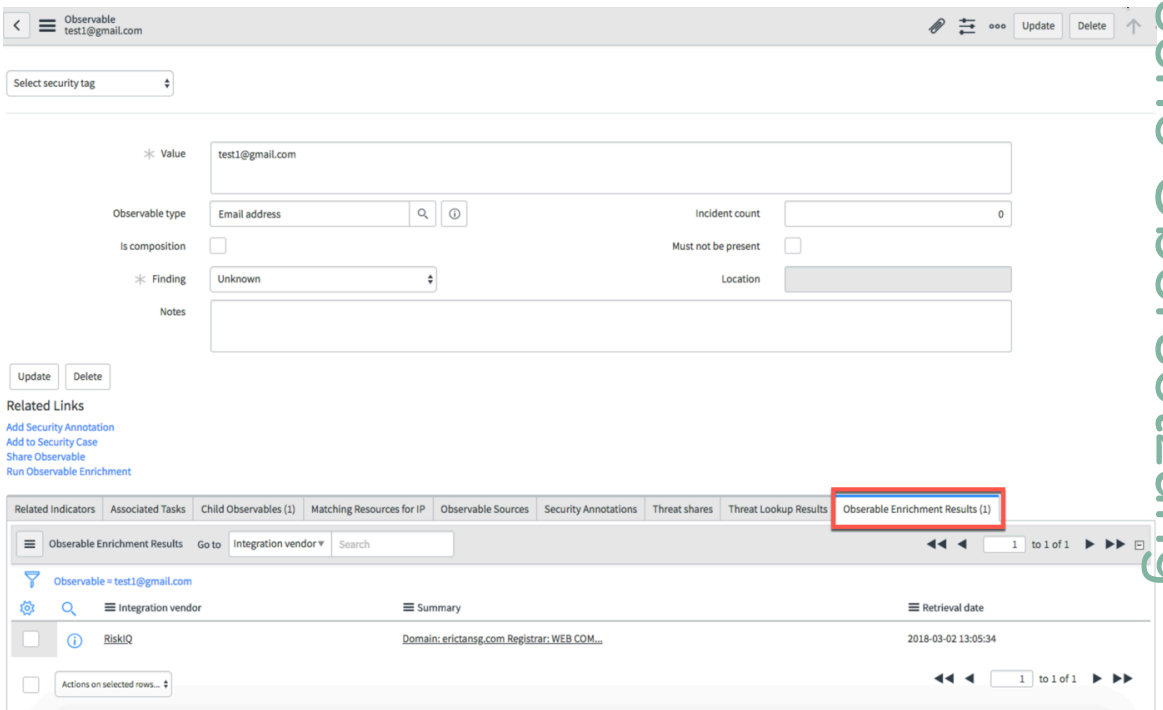
4. In **Ergänzung Erkennbarer Elemente Ausführen** Fenster, verschieben **RiskIQ-Whois** Zur ausgewählten Liste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Absenden**.
   Suchergebnisse werden auf angezeigt **Ergebnisse Der Anreicherung Erkennbarer Elemente** Registerkarte im Datensatz des erkennbaren Elements.



Trouble?
Wenn für das erkennbare Element keine Ergebnisse zurückgegeben werden, wird eine Meldung in angezeigt **Zusammenfassung** Spalte. Wenn keine Ergebnisse angezeigt werden, stellen Sie sicher, dass das erkennbare Element von der API unterstützt wird.

Zugehörige Informationen

Unterstützte erkennbare Elemente für RISKIQ Und RISKIQ WHOISIQ

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Shodan-Integration

Shodan Ist eine Suchmaschine, die Servicebannerinformationen von verbundenen Geräten auf der ganzen Welt analysiert. Servicebanner enthalten Informationen zu einem Computersystem, z. B. Hostname, Gerätetyp, Betriebssystem, geografischer Standort und verbundener ISP. Bei Integration mit ServiceNow AI Platform Security Operations Produkt bieten diese Servicebannerinformationen Analysten zusätzliche Ergänzungsdaten und Einblicke für Security Incidents oder Untersuchungen.

Die -Integration erfordert Security Incident Response Und Threat Intelligence Plugins.

Die Shodan Die Integration führt eine Ergänzung für die folgenden erkennbaren Elemente durch:

- IP-Adressen
- URLs

Die Anwendung sucht alle fünf Minuten nach neuen erkennbaren Elementen. Wenn die erkennbaren Elemente vom Typ sind, der von erkannt wird Shodan Integration, werden die erkennbaren Elemente angereichert.

Installieren und konfigurieren

Bevor Sie die Integration auf Ihrer Instanz ausführen, führen Sie die Installations- und Konfigurationsschritte so aus Shodan Die Anwendung ist ordnungsgemäß in integriert ServiceNow AI Platform Security Operations.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Setupaufgaben	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Der Systemadministrator (Administrator) installiert die App und weist die Rolle Security Incident-Administrator (sn_si.admin) zu. • Der Security Incident-Administrator (sn_si.admin) überwacht die Konfiguration und überprüft die erwarteten Ergebnisse. Diese Rolle hat auch Zugriff auf Security Operations Modul.
Beziehen Sie sich auf Shodan API-Schlüssel.	Erstellen Sie einen Account, und rufen Sie den API-Schlüssel aus dem ab Shodan Website: SHODAN-Website .
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	Für das Madrid-Release und spätere Familienveröffentlichungen Security Incident Response Abhängigkeits-Plugin (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle

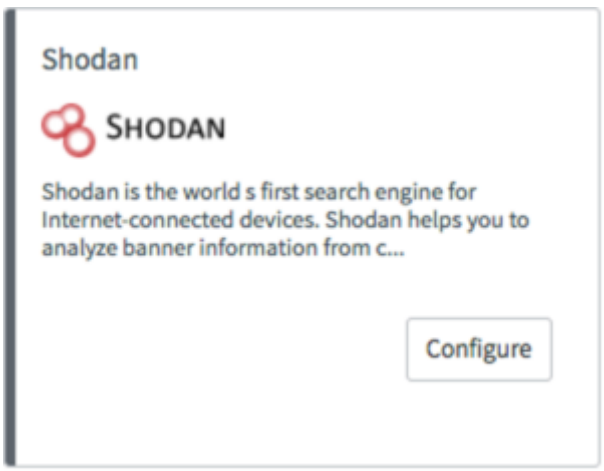
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgaben	Beschreibung
	Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Für die Integration erforderliche Anwendungen. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. **1.** Security Incident Response **2.** Sicherheits-Integrations-Framework **3.** Security Support Common **4.** Orchestration Des Sicherheitssupports Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz für die Integration finden Sie unter Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

Erforderliche Rolle: Administrator

Prozedur

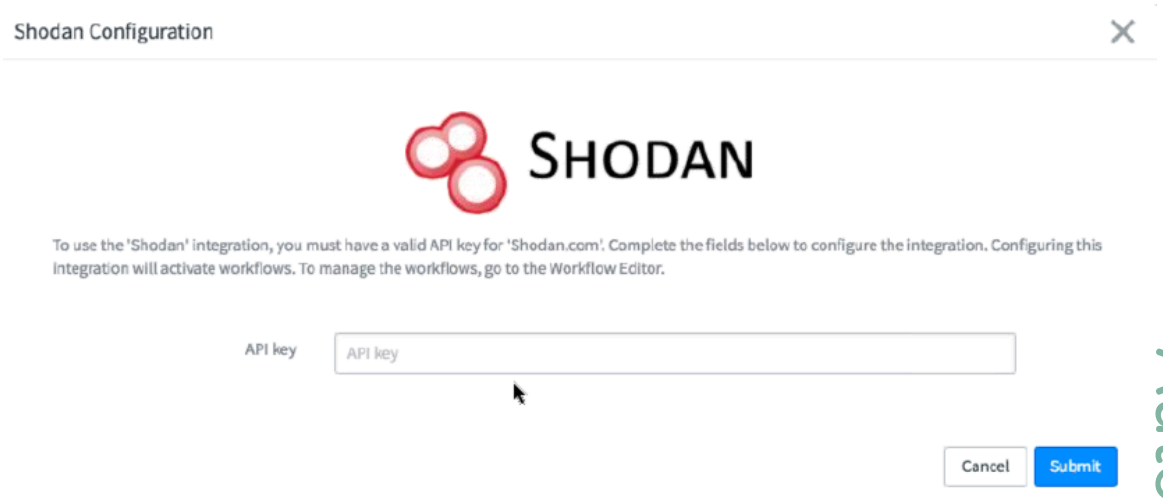
1. Wenn Sie die Anwendung für die Integration nicht installiert haben, finden Sie weitere Informationen unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Navigieren Sie nach Abschluss der Installation zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie Shodan Kachel.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Konfigurieren**.
4. In **Shodan-Konfiguration** Geben Sie den API-Schlüssel ein, den Sie aus dem erhalten haben Shodan Website und klicken Sie auf **Übermitteln** .



5. Überprüfen Sie die erfolgreiche Konfiguration.
   Die Konfiguration wurde erfolgreich abgeschlossen, es sei denn, eine Fehlermeldung wird angezeigt.

   Trouble?

   Wenn während der Konfiguration eine Fehlermeldung angezeigt wird, wird Shodan API-Schlüssel ist möglicherweise ungültig.

Überprüfen Sie die erwarteten Ergebnisse

Erkennbare Elemente werden automatisch von einem Security Incident generiert und von der Anwendung gescannt. Ergänzungsergebnisse werden auf angezeigt **Ergebnisse Der Anreicherung Erkennbarer Elemente** Und **Netzwerkbanner** Registerkarten.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst.

Prozedur

1. Öffnen Sie den Security Incident, mit dem Sie arbeiten, und überprüfen Sie, ob die Suche erfolgreich ausgeführt wurde.

   Sobald die Anwendung konfiguriert ist, wird der Workflow bei der Incident-Erstellung automatisch gestartet. Der Ausführungs- und Abschlussstatus der Suche wird in den Arbeitsnotizen im Security Incident angezeigt.

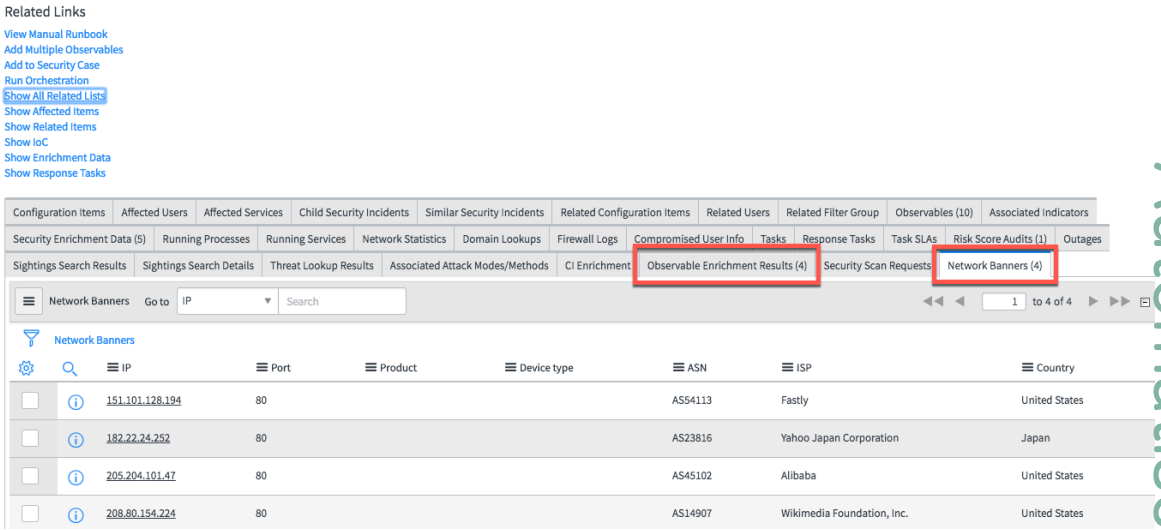
2. Überprüfen Sie die Arbeitsnotizen, um weitere Informationen zu erhalten und zu erfahren, wie Sie fortfahren können, wenn Sie nicht verifizieren können, dass die Suche erfolgreich ausgeführt wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Navigieren Sie zum Ende des Security Incident, und klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Link in **Zugehörige Links** .

   Hinweis:
   Die Zahlen in den folgenden Schritten werden mit angezeigt **Formulare mit Registerkarten** Einstellung in den Systemeinstellungen aktiv. Wenn Formulare mit Registerkarten nicht angezeigt werden, klicken Sie in der oberen rechten Ecke des Bannerrahmens auf das Symbol für Einstellungen. In **Systemeinstellungen** Klicken Sie auf das Dialogfeld, das angezeigt wird **Formulare** Und verifizieren Sie das **Formulare mit Registerkarten** Und **Mit dem Formular** Sind ausgewählt.



   Ergebnisse werden in angezeigt **Ergebnisse Der Anreicherung Erkennbarer Elemente** Und **Netzwerkbanner** Registerkarten unten im Security Incident.

4. Mit **Netzwerkbanner** Klicken Sie auf der ausgewählten Registerkarte neben einem erkennbaren Element auf das blaue Informationssymbol.

5. Klicken Sie im angezeigten Dialogfeld auf **Öffnen Sie Den Datensatz** Zum Anzeigen von Rohdaten und weiteren Details.

Trouble?
Wenn unter keine Ergebnisse angezeigt werden **Ergebnisse Der Anreicherung Erkennbarer Elemente** Und **Netzwerkbanner** Stellen Sie sicher, dass das erkennbare Element ein Typ ist, der für die Suche durch die Integration unterstützt wird.

(Optional) Fügen Sie ein erkennbares Element für manuell an Shodan

Sie können erkennbare Elemente manuell an einen Security Incident anhängen. Sie hängen erkennbare Elemente manuell an, wenn Sie Bedrohungssuchen für erkennbare Elemente durchführen möchten, die nicht an einen Security Incident beim ersten Ereignisauslöser angehängt sind. Sie können diese Aufgabe auch ausführen, wenn Sie weitere Informationen zu einem zugehörigen erkennbaren Element wünschen.

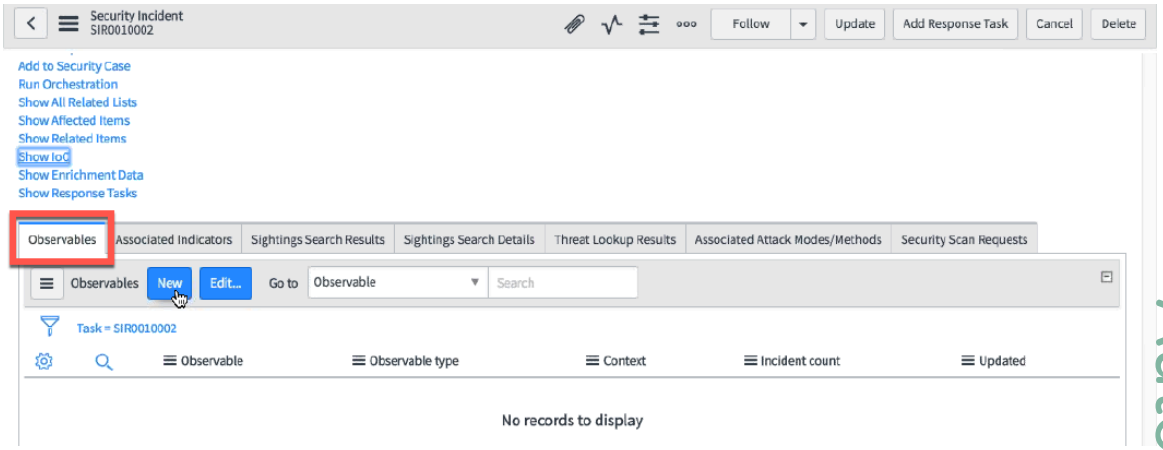
Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

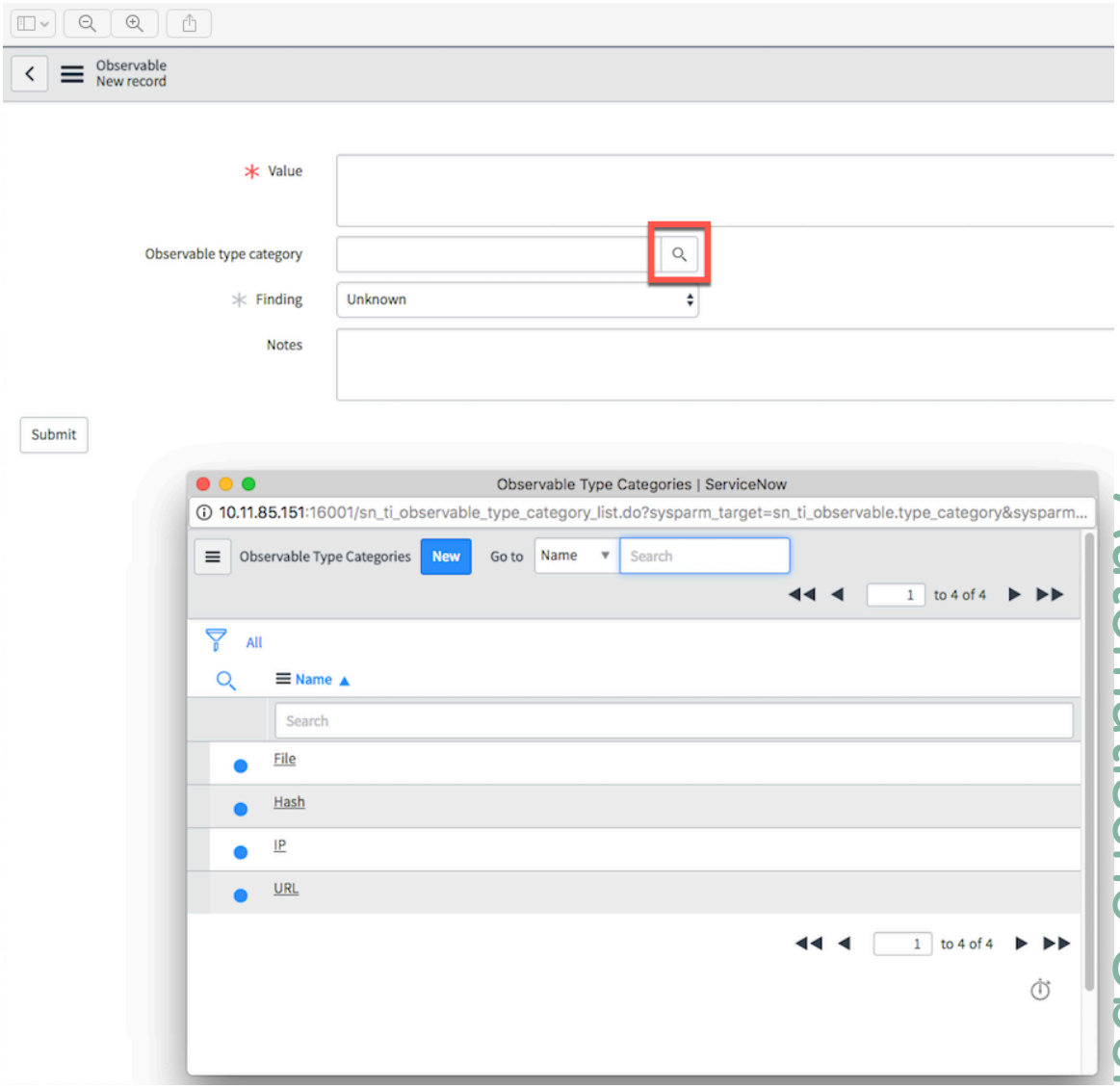
1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen** Und öffnen Sie einen Security Incident, an den Sie das erkennbare Element anhängen möchten.
2. Klicken Sie unten im Datensatz auf **IOC anzeigen** Link in **Zugehörige Links** .



3. Auf der **Erkennbare Elemente** Klicken Sie auf die Registerkarte **Neu** .
   Das Formular „erkennbares Element“ wird angezeigt.
4. In **Wert** Feld ein erkennbares Element (IP-Adresse oder URL) eingeben.
5. Klicken Sie auf das Suchsymbol und im **Typkategorien Des Erkennbaren Elements** Dialogfeld auf den gewünschten erkennbaren Typ in der Liste klicken, um das Feld auszufüllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

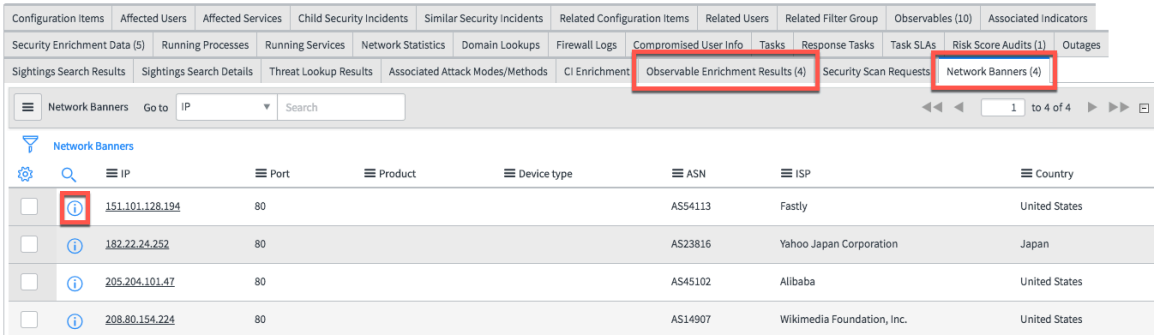


Automatische Übersetzung

6. Klicken Sie auf **Absenden**.
   Der Workflow wird gestartet und überprüft, ob das neue erkennbare Element vorhanden ist. Der Ausführungs- und Abschlussstatus wird im Abschnitt „Arbeitsnotizen“ im Security Incident-Datensatz angezeigt.
7. Navigieren Sie zu Ihrem Security Incident, und überprüfen Sie die Arbeitsnotizen.

8. Klicken Sie unten im Datensatz auf **Alle Zugehörigen Listen Anzeigen** Zugehöriger Link.
9. Klicken Sie auf **Ergebnisse Der Anreicherung Erkennbarer Elemente** Oder **Netzwerkbanner** Registerkarten für Ergebnisse, und klicken Sie auf das blaue Informationssymbol neben einem erkennbaren Element, um weitere Informationen zu einem bestimmten Element zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Klicken Sie im angezeigten Dialogfeld auf **Öffnen Sie Den Datensatz** Zum Anzeigen von Rohdaten und weiteren Details.
11. **Wahlweise:** Klicken Sie auf das blaue Einstellungssymbol neben dem Suchsymbol, um die Spaltenausgabe und die Reihenfolge zu personalisieren.
12. In **Personalisieren Sie Listenspalten** Wählen Sie verfügbare Einstellungen aus, und verschieben Sie sie in **Ausgewählt** Und klicken Sie auf **OK** .

Trouble?
Überprüfen Sie **Arbeitsnotizen** Um weitere Informationen zu erhalten und zu erfahren, wie Sie fortfahren können, wenn Sie nicht verifizieren können, ob die Suche erfolgreich ausgeführt wurde.

Secureworks CTP Ticketerfassungsintegration

Die Secureworks Counter Threat Platform Mit der Integration der Ticketerfassung können Sie automatisch abrufen Secureworks CTP Tickets konvertieren Sie sie in Security Incidents, und führen Sie automatisierte Antwortaktionen aus.

Die wichtigsten Funktionen dieser Integration umfassen:

- Automatische Erfassung ausgewählter Tickets (einschließlich Anhänge) basierend auf einem vordefinierten Zeitplan.
- Zuordnung von Ticket- und Ereignisfeldern zu Security Incident Response Felder.
- Vorschau der Security Incidents, die den Ticketfeldern zugeordnet sind.
- Filterung und Zusammenfassung von Tickets.
- Abruf von Ereignissen bei Bedarf, die einem Ticket zugeordnet sind.
- Regelmäßige Nachverfolgung wichtiger Updates von Tickets.
- Automatisieren von Ticketaktualisierungen und -Abschlüssen basierend auf dem SIR-Incident-Status
- Master-Ticket-Update.
- Synchronisierung von SecureWorks-Arbeitsprotokollen mit Security Incident Response Arbeitsnotizen.

Richten Sie Ihr ein ServiceNow AI Platform Instanz für Secureworks CTP Integration der Ticketerfassung

Im folgenden Abschnitt werden die Setup-Aufgaben aufgeführt, die Sie in ausführen müssen ServiceNow AI Platform Instanz vor der Installation der Anwendung über ServiceNow Store.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Überprüfen Sie anhand der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform Und Security Incident Response Rollen.	Die folgenden Rollen sind für die Installation, das Setup und die Verwendung der Integration in erforderlich ServiceNow AI Platform Instanz. • Ein Anwender mit ServiceNow AI Platform Die Administratorrolle (admin) installiert die Anwendung aus dem ServiceNow Store Und weist zu SIR Administratorrolle (sn_si.admin). • Ein Anwender mit der Rolle „sn_si.admin“ überwacht die folgenden Aufgaben in ServiceNow AI Platform: ◦ Namen, erstellt und bearbeitet Profile. ◦ Auswahl und Zuordnung Secureworks CTP Ticketfelder für die Security Incident-Felder. ◦ Zeigt vor dem Abschluss der Konfiguration eine Vorschau der Security Incident-Details auf Richtigkeit an. ◦ Plant die laufende Ticketerfassung. ◦ Aktiviert Ticketaktualisierungen, wenn ein SIR SIR Incident wird erstellt und geschlossen. ◦ Weist die Rolle Security Incident Analyst (sn_si.Analyst) zu. ◦ Anwender mit sn_si.Analyst arbeiten mit Security Incidents. Weitere Informationen zu Rollen und dem Zuweisen von Rollen an Anwender finden Sie unter Managing roles
Überprüfen Sie, ob Sie die folgenden Versionen verwenden: • SecureWorks-Ticket-API 4,0 • SecureWorks-Ereignis-API 1,0 • SecureWorks-Anreicherungs-API 1,0	Wenn Sie Zugriff auf haben Secureworks CTP Portal haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein anderes spezielles Setup erforderlich.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden	Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setupaufgabe	Beschreibung
installiert und aktiviert, bevor Sie die Anwendung für die Integration installieren.	ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. **1.** Security Incident Response **2.** Ereignis- und Warnungserfassung für Security Operations(Erforderlich für SIEM-Integrationen): Diese Anwendung erfordert: ○ com.glide.hub.integration.runtime => ServiceNow IntegrationHub-Laufzeit ○ Com.Glide.Hub.action_STEP.Rest => ServiceNow IntegrationHub Aktionsschritt – REST **Hinweis:** Die Integration Hub-Komponenten werden zusammen mit dem Plugin „Ereignis- und Warnungserfassung“ installiert. Wenn diese nicht installiert sind, wenden Sie sich an den Kundensupport, um Unterstützung zu erhalten. Weitere Informationen zur Installation von finden Sie Security Operations Kernanwendungen, siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

Installieren und konfigurieren Sie ServiceNow Anwendung für die Integration der SecureWorks CTP-Ticketerfassung

Bevor Sie die Integration für ausführen ServiceNow AI Platform Führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in integriert wird Security Incident Response Und Security Operations Produkte auf Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn Sie den nicht installiert haben Secureworks CTP Ticketanwendung aus dem ServiceNow Store Informationen zur Integration finden Sie unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie Secureworks CTP Kachel „Integration der Ticketerfassung“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf , um die Anwendung zu konfigurieren **Neu** .
4. Alternativ, wenn ein **Konfigurieren** Die Schaltfläche wird auf einer Kachel angezeigt. Klicken Sie darauf, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie die Felder im angezeigten Dialogfeld aus.
6. Klicken Sie auf **Absenden**.
   Nachdem sie erfolgreich validiert und übermittelt wurde, wird jede Konfiguration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Ergebnisse

Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden. In der oberen rechten Ecke der Seite, von **Konfigurationen Anzeigen** Auswahlliste klicken Sie auf **Ja** .

Erstellen Sie ein Profil für die Integration der SecureWorks CTP-Ticketerfassung

Erstellen Sie ein Profil in Ihrem ServiceNow AI Platform Instanz instand setzen und bestimmen, welche Tickets erfasst werden müssen und welche zum Erstellen von Security Incidents verwendet werden. Bevor Security Incidents aus erfassten Tickets erstellt werden, werden die Feldwerte aus Tickets in einem Layout von angezeigt ServiceNow AI Platform Security Incident, damit Sie eine Vorschau darauf anzeigen können, wie der tatsächliche Security Incident angezeigt wird.

Mit der Integration können Sie Tickets basierend auf den Profilen erfassen, die Sie in konfigurieren Security Operations Umgebung Ihrer Instanz. Alle Tickets werden anfänglich für einen konfigurierten Tickettyp in einem Profil erfasst. Erfasste Tickets können dann weiter gefiltert werden, um anzugeben, welche Tickets Security Incidents erstellen.

Sie können beispielsweise Filter bevorzugen, die Security Incidents nur für Tickets erstellen, die als hohes Risiko identifiziert werden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Tickets erstellt werden, werden einzelne Feldwerte in den Tickets den entsprechenden Feldern in einem Layout von Security Incidents zugeordnet, um eine Vorschau anzuzeigen.

Identifizieren Sie die Quelle des Profils

Geben Sie den Namen und die Quelle des Profils an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Um ein Profil für ein Ticket in zu erstellen ServiceNow AI Platform Instanz, navigieren Sie zu **Integration Der Secureworks-Ticketerfassung** > **Secureworks-Profile**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder aus.

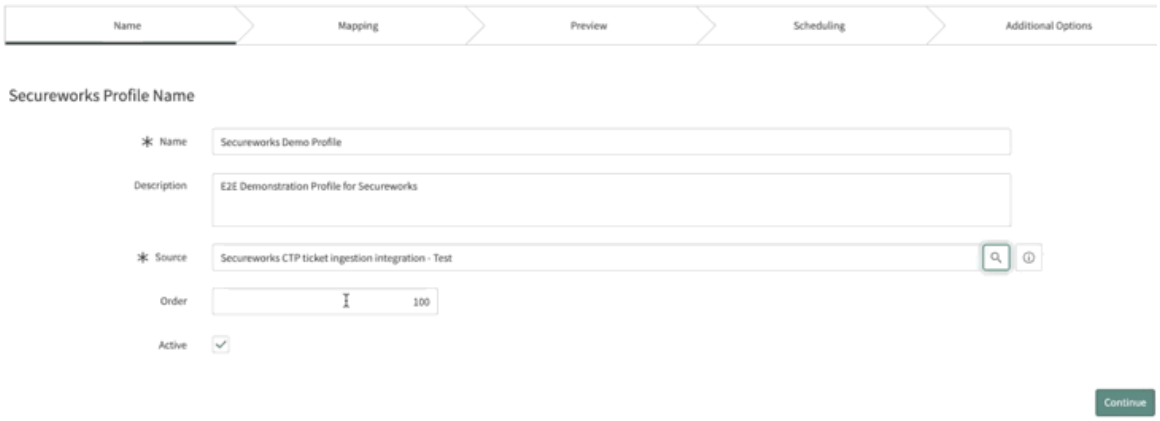
Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

Feld	Beschreibung
Name	Eindeutiger Name für das Profil. Wenn Namen nicht eindeutig sind, wird ein Fehler angezeigt, und doppelte Profilnamen werden nicht gespeichert. Profilnamen in Ihrem ServiceNow AI Platform Instanz muss eindeutig sein.
Quelle	Wählen Sie die Quelle aus, aus der Sie die Daten erfassen möchten.
Reihenfolge	Der Standardwert ist 100. Wenn Sie mehrere Profile erstellt haben, gibt dieser Wert eine Laufzeitausführungspriorität an, wenn zwei oder mehr Profile dieselben Auslösebedingungen haben. Je niedriger der Reihenfolgewert, desto höher die Priorität.
Aktiv	Diese Option ist standardmäßig deaktiviert. Wenn diese Option deaktiviert ist, ist das Profil nicht aktiv. **Hinweis:** Sie sollten alle Abschnitte im Profil abschließen, bevor Sie es aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular.



Nächste Maßnahme
Ordnen Sie die Ticketfelder zu.

Zuordnung von Ticketfeldern für die SecureWorks CTP-Integration

Ordnen Sie die Ticket- und Ereignisfelder den Feldern im Security Incident-Formular zu.

Für den Zuordnungsschritt müssen Sie zuerst Beispieltickets erfassen und dann sicherstellen, dass alle relevanten Ticketfelder der entsprechenden Stelle im zugeordnet sind Security Incident Response Formular und visualisieren Sie dann den Security Incident im Vorschauabschnitt.

Die Zuordnung der Beispielticketfelder umfasst Folgendes:

- Beispieldaten werden abgerufen und ausgefüllt: Siehe Beispiel für SecureWorks-Tickets werden erfasst
- Zuordnung der Ticketfelder zum Security Incident: Siehe Zuordnung von SecureWorks-Ticketfeldern zu Security Incident Response-Feldern

Beispiel für SecureWorks-Tickets werden erfasst

Wählen Sie die Beispieltickets aus, die erfasst werden sollen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie auf **Zuordnung** Auf der Fortschrittsleiste.
2. Sie können entweder die fünf neuesten Beispieltickets abrufen oder die eindeutigen Ticket-IDs für die spezifischen Tickets angeben, die Sie für Ihre Zuordnungs-Experience verwenden möchten.
   Von **Erfassungseinstellung** Auswahlliste wählen Sie eine der folgenden Optionen aus:
   - Neueste Tickets abrufen: Die 5 neuesten Tickets werden abgerufen.
   - Tickets basierend auf Ticket-ID auswählen: Geben Sie die Ticket-ID für das abzurufende Ticket an. Sie können maximal 5 Ticket-IDs durch Kommas getrennt angeben.
3. Klicken Sie Auf **Rufen Sie Beispieldaten Ab** Zum Abrufen der neuesten Beispielticketdaten aus dem Secureworks CTP Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Abruf für Beispieltickets kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt. Die abgerufenen Tickets werden als einzelne Registerkarten angezeigt. Klicken Sie auf eine Registerkarte, um die Ticketdaten anzuzeigen. Für jedes Ticket können Sie die Ticketfelder und ihre Werte sowie Details zum beitragenden Ereignis anzeigen, das das Ticket ausgelöst hat.

Hinweis:
Details zu beitragenden Ereignissen werden nur angezeigt, wenn sie in den letzten 7 Tagen aufgetreten sind. Ereignisse, die älter als 7 Tage sind, werden nicht angezeigt.

Nächste Maßnahme
Nachdem Sie die Beispieldaten abgerufen haben, ordnen Sie die Ticketfelder dem Security Incident zu.

Zuordnung von SecureWorks-Ticketfeldern zu Security Incident Response-Feldern

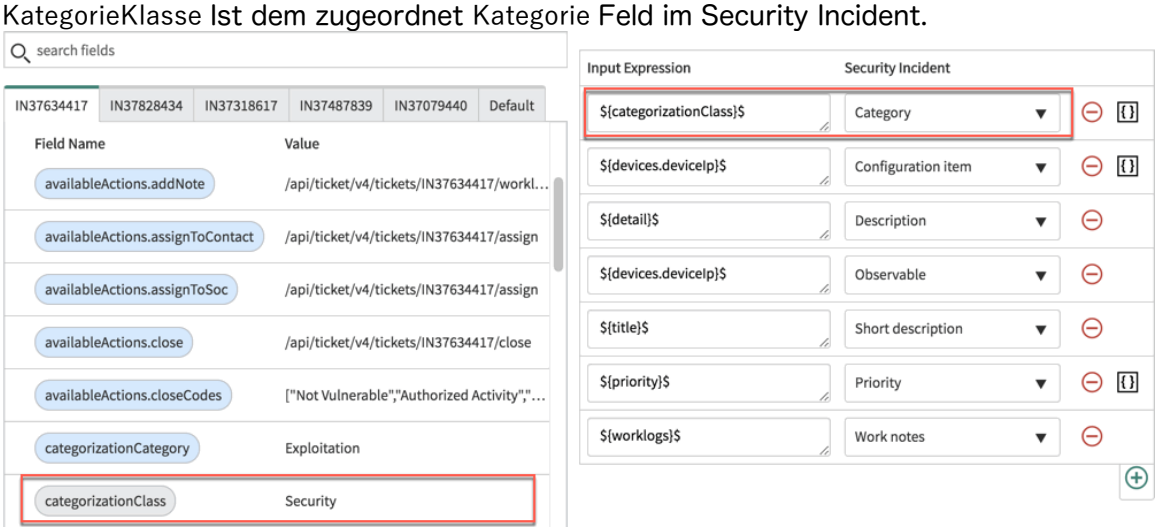
Ordnen Sie einzelne Ticket- oder Ereignisfelder Feldern auf einem zu ServiceNow AI Platform SIR Security Incident.

Ticketfeldzuordnung

Verwenden Sie als Anwender mit der Rolle sn_si.admin die Felder aus dem Abschnitt Beispieltickets auf der linken Seite, und ordnen Sie sie den Security Incident-Feldern in zu **SIR-Incident-Feldzuordnung** Spalte. Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Ticket- oder Ereignisfelder von der linken Seite ziehen und sie im Abschnitt SIR Incident-Feldzuordnung auf der rechten Seite ablegen. Die Zuordnung auf der rechten Seite ordnet das Feld für eingehende Tickets einem Feld für ausgehende Security Incidents zu.

1. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf der linken Seite des Formulars auf einen blauen Feldnamen.
2. Sie können den Feldnamen manuell in die Spalte „Eingabeausdruck“ eingeben oder den Feldnamen per Drag-and-Drop verschieben. Beispiel: Beschreibung , Und legen Sie es in einem Feld in ab **Eingabeausdruck** Spalte neben einem Feldnamen in **Security Incident** Spalte.

   Der Feldwert wird in der Spalte „Eingabeausdruck“ angezeigt. In der folgenden Abbildung: KategorieKlasse Ist dem zugeordnet Kategorie Feld im Security Incident.



Hinweis:
Wenn Sie den Ereignisfeldnamen manuell in eingeben **Eingabeausdruck** Abschnitt, müssen Sie ein Präfix als hinzufügen `${Event:eventfield}$` Vor dem Namen des zugeordneten Felds.

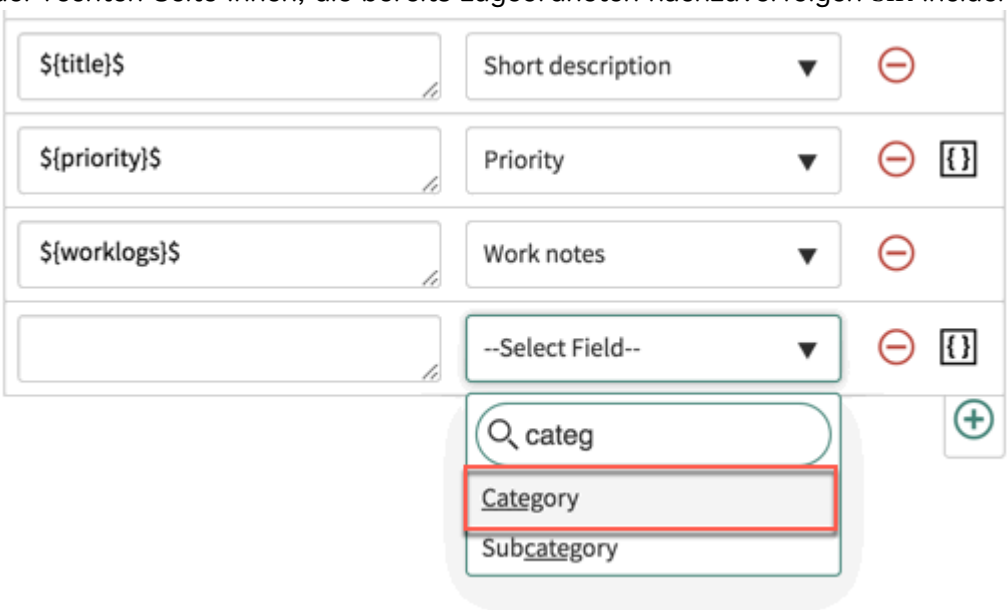
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Damit Sie sicherstellen können, dass im Zuordnungsprozess keine Ticket- oder Ereignisfelder übersehen oder dupliziert werden, sind Felder farbcodiert. Die Farbcodierung der Ticketfelder hilft Ihnen, die Ticketwerte nachzuverfolgen, die Sie bereits zugeordnet haben, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder blau angezeigt werden. Auf diese Weise können Sie besser visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Ticketinformationen nicht zugeordnet sind.

Hellblaue Felder auf der linken Seite zeigen an, dass noch kein Ticketfeld ausgewählt und dem Security Incident zugeordnet ist. Möglicherweise möchten Sie ein eingehendes Ticket- oder Ereignisfeld mehreren Feldern in einem Security Incident zuordnen. Ein graues Feld gibt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.

3. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen:
   a. Rechts neben dem Formular in SIR Klicken Sie im Abschnitt „Incident-Feldzuordnung“ unten im Raster auf das Plus-Symbol (+). Ein neues Feld wird angezeigt.
   b. Erweitern Sie in der Spalte Security Incident die angezeigte Auswahlliste, und wählen Sie ein Feld aus.

      In der erweiterten Auswahlliste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung hat Kategorie einen grauen Hintergrund, da sie im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Ticketfelder auf der linken Seite des Formulars hilft diese Farbcodierung für die Security Incident-Felder auf der rechten Seite Ihnen, die bereits zugeordneten nachzuverfolgen SIR Incident-Felder.



Hinweis:
Da mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „erkennbares Element“ mehrmals verschiedenen Werten zugeordnet werden. Ebenso unterstützen die Felder „Konfigurationselement“ und „Arbeitsnotizen“ mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Auswahlliste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Auswahlliste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.

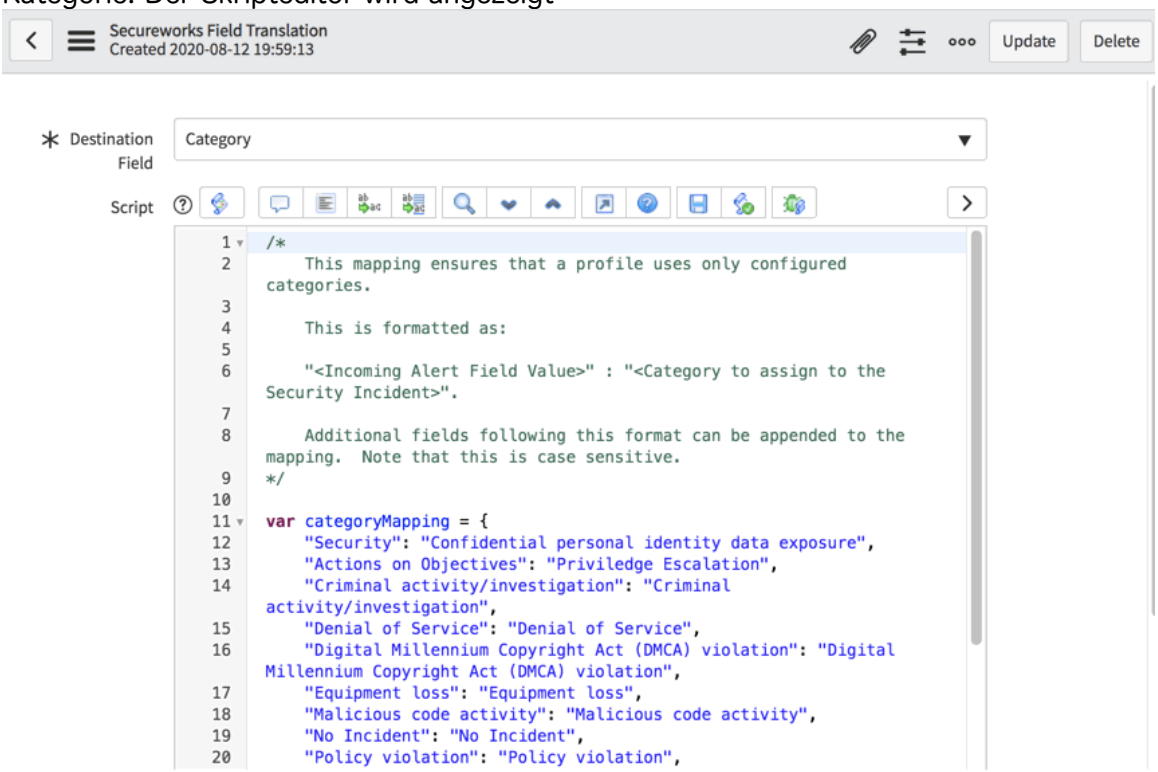
d. Wählen Sie auf der linken Seite des Formulars das Ticketfeld aus, und ziehen Sie es per Drag-and-Drop in ein entsprechendes Security Incident-Feld auf der rechten Seite.

4. Entfernen Sie Felder, indem Sie das Symbol „ –“ neben dem Feldnamen im Abschnitt „SIR-Incident-Feldzuordnung“ verwenden.
5. Fahren Sie mit der Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder entfernen.

Formatierungsfeldübersetzung

In bestimmten Fällen werden Ticketfelder möglicherweise nicht direkt in die Felder im übersetzt SIR Security Incident. Für diese Werte können Sie einen Skripteditor verwenden, um Feldwerte für den Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind. Beispielsweise kann ein Kategoriewert „Malware-Warnung“ und „Virusinfektion“ mit dem Skripteditor unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können in eine allgemeine schädliche Code-Aktivität im Feld Kategorie übersetzt werden SIR Security Incident mithilfe der Funktionalität „Formatierungsfeldübersetzung“.

Um den Skript-Editor zu verwenden, klicken Sie auf das {}-Symbol neben dem Feld Kategorie. Der Skripteditor wird angezeigt



.

Geben Sie alle Änderungen am Skript ein, und klicken Sie auf **Aktualisieren** Um die Änderungen zu speichern und zur Zuordnungsseite zurückzukehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingungen für die Incident-Generierung

Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, damit Sie angeben können, welche Tickets Security Incidents erstellen sollen und welche Tickets herausgefiltert werden sollen, z. B. Tickets mit niedriger Priorität. Sie können dieselben Feldwerte im Generator für Incident-Generierungsbedingungen verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes Ticket erfüllen muss, um einen Security Incident zu erstellen. Um Bedingungen für die Incident-Generierung festzulegen, gehen Sie wie folgt vor.

1. Scrollen Sie zu **Bedingungen Für Die Incident-Generierung** Abschnitt im Formular, und wählen Sie aus **Filtern Sie basierend auf Bedingungen** Kontrollkästchen zum Aktivieren der Option.

   Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den spezifischen Bedingungen entsprechen, die in den Feldern beschrieben werden.

   Die Optionen in den Auswahllisten für das erste Feld im Generator für Filterbedingungen entsprechen den Feldern, die auf angezeigt werden **Beispiel Für Ticketerfassung** Abschnitt für die erfassten Tickets. Diese Felder sind dynamisch und ändern sich je nach den von Ihnen erfassten Tickets. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden und müssen genau mit den Werten von übereinstimmen Secureworks CTP Ticket. Wenn Sie sich nicht sicher sind, welche Werte in die Filterfelder eingegeben werden sollen, kehren Sie möglicherweise zu zurück Secureworks CTP Konsole und überprüfen Sie Ihre Tickets auf die Stichwörter.

   Hinweis:
   Die `Arbeitsprotokolle` , `Geräte` , `Anhänge` , `Beobachter` , `VerfügbarAktionen` , Und `CloseCodes` Ticketfelder können mehrere Werte haben (da die Werte in Arrays gespeichert werden). Da die Filterbedingung nur Zeichenfolgen abrufen kann, müssen Sie verwenden `Enthält` Filterbedingung für diese Felder, um sicherzustellen, dass die Daten korrekt gefiltert werden.

2. Legen Sie mithilfe der Auswahllisten und Felder des Bedingungsgenerators Filter für die erste Zeile fest.
3. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** Oder **ODER** .
   - Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden.
4. (Optional) Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

   Diese Art der Bedingungsfilterung für die Incident-Generierung hilft Ihnen, die Tickets einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegende Regel oder Filter zu ändern. Wenn zusätzliche Filterkriterien festgelegt sind, werden Security Incidents nur Tickets zugeordnet, die allen Kriterien entsprechen.

Ticketzusammenfassungskriterien, um ähnliche Tickets zu verarbeiten und doppelte Incidents zu verhindern

Definieren Sie zusätzliche Ticketzusammenfassungskriterien, die ein eingehendes Ticket zu einem vorhandenen aggregieren SIR Security Incident anstatt ähnliche, potenziell doppelte Incidents zu erstellen. Mithilfe von Feldübereinstimmungswertkriterien für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl aktiver, sich überschneidender Security Incidents reduzieren, indem alle zugehörigen Ticketdaten in einem einzelnen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

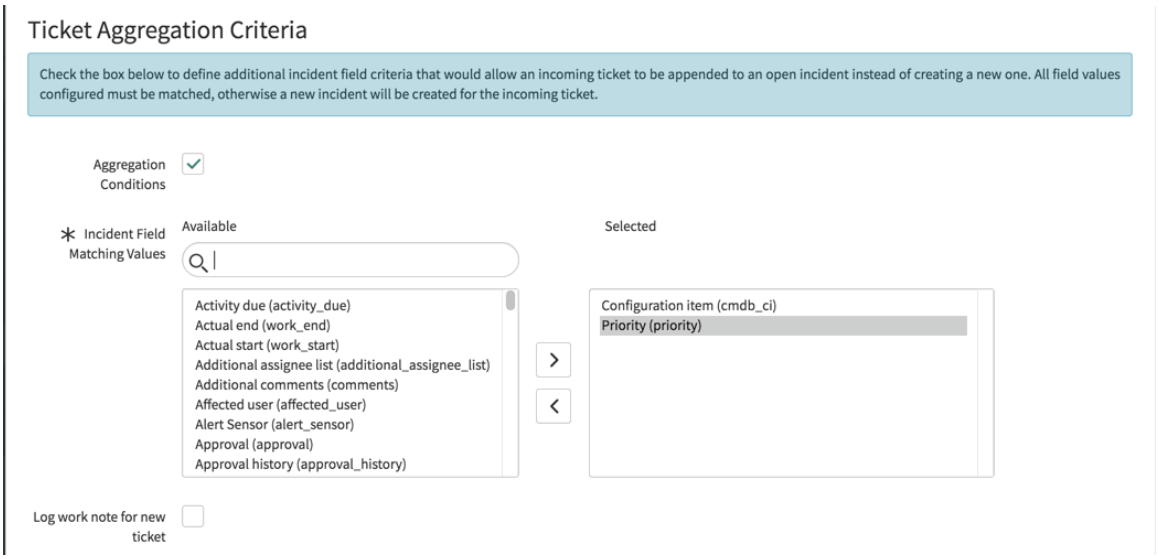
Security Incident platziert werden. Um die Kriterien festzulegen, führen Sie die folgenden Schritte aus:

1. Scrollen Sie zu **Kriterien Für Ticketzusammenfassung** Abschnitt im Formular, und wählen Sie aus **Zusammenfassungsbedingungen** Kontrollkästchen zum Aktivieren dieser Option.

   Die Spalten „Incident-Feld-Übereinstimmungswerte“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die in konfiguriert sind SIR Security Incident.

2. Wählen Sie in der Liste verfügbar die Feldwerte aus, die Sie für vorhandene Security Incidents in Ihrer NOW Platform abgleichen möchten, und verschieben Sie sie in die Liste ausgewählt.

   Alle von Ihnen ausgewählten Feldwerte müssen abgeglichen werden, um dieses eingehende Ticket an einen vorhandenen Security Incident anzuhängen. Dies umfasst Felder, z. B. erkennbare Elemente und Konfigurationselemente, denen möglicherweise mehrere Ticketfeldwerte zugeordnet sind. Alle Werte müssen übereinstimmen.
   Wenn nur eine Teilmenge der Werte übereinstimmt, werden die Bedingungen für die Ticketzusammenfassung nicht erfüllt, und ein neuer Security Incident wird erstellt. Siehe Screenshot unten für die Feldzuordnung mit mehreren Werten.



Wenn ein neues Ticket allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird das neue Ticket automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Anwender mit der Rolle „sn_si.Analyst“, der mit Security Incidents arbeitet, können Sie alle hinzugefügten aggregierten Tickets in einer zugehörigen Liste zu einem Security Incident anzeigen. Diese Liste enthält Details zu zugehörigen Zeitstempeln und zusammengefassten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum diese Tickets zu vorhandenen Security Incidents aggregiert werden. Wenn diese Registerkarte in einem Security Incident nicht angezeigt wird, scrollen Sie unter zur linken Seite des Datensatzes **Zugehörige Links** Und klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Link.

Hinweis:

Die zugehörige Liste „zusammengefasste SecureWorks-Tickets“ ist mit dem Basissystem nicht verfügbar. Sie müssen das Layout der zugehörigen Liste konfigurieren und es explizit in die anderen zugehörigen Listen aufnehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. (Optional) um eine Arbeitsnotiz für ein neues Ticket zu protokollieren, das kürzlich dem Security Incident hinzugefügt wurde, aktivieren Sie das Kontrollkästchen, um diese Option zu aktivieren. In der Arbeitsnotiz wird protokolliert, dass ein neues Ticket hinzugefügt wurde, zusammen mit einem Link zu den Ticketdetails und allen anderen Details, die dem Feld „Arbeitsnotiz“ in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

   Sie haben erfolgreich Werte aus einem zugeordnet Secureworks CTP Ticket für Felder in einem Security Incident. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung einzuschränken. Sie haben Tickets auch an vorhandene Security Incidents angehängt, wenn Ticketfeldwerte den konfigurierten Zusammenfassungskriterien entsprechen.

4. Klicken Sie Auf **Fahren Sie Fort** Um mit der Profilkonfiguration fortzufahren. Der nächste Schritt besteht darin, eine Vorschau der Felder anzuzeigen, die Sie einem zugeordnet haben SIR Security Incident

Zeigen Sie eine Vorschau der zugeordneten Werte im Security Incident an

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem zugeordnet haben SIR Security Incident. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Ticketfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

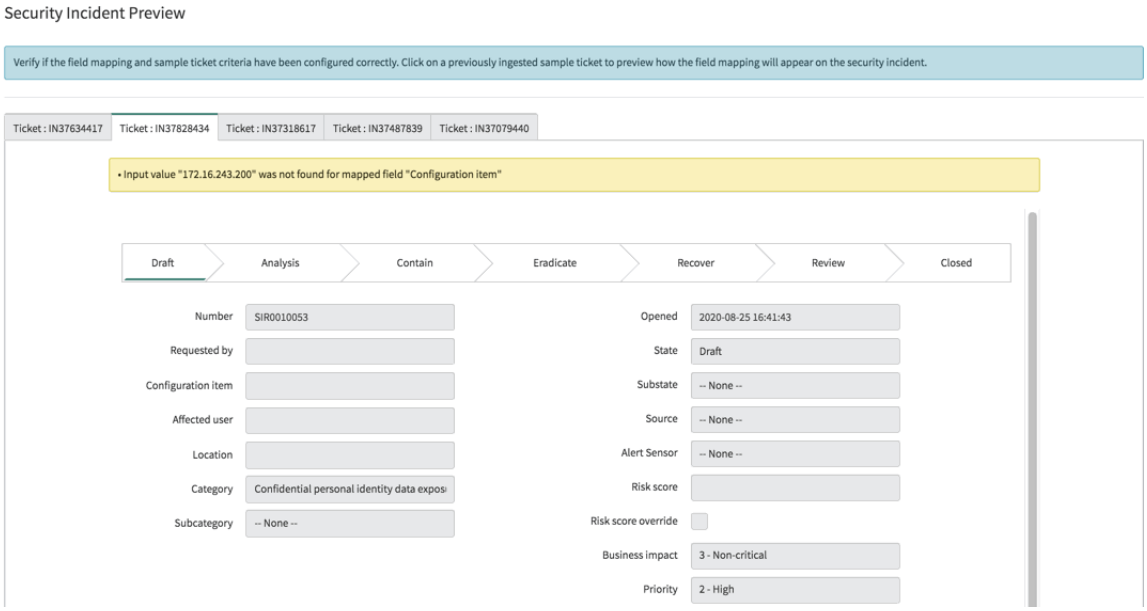
Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Zeigen Sie eine Vorschau eines Security Incidents an, und bearbeiten Sie die Zuordnung nach Bedarf erneut, um Felder mit Fehlern zu beheben oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wurde, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen von SIR Security Incidents werden nicht als tatsächliche Incidents im Produkt Security Incident Response gespeichert.

Prozedur

1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie auf **Vorschau** In der Fortschrittsleiste.
   Die Tickets werden als Registerkarten angezeigt.
2. Klicken Sie auf eine Registerkarte, um eine Vorschau des Security Incident anzuzeigen.
   Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.
3. Überprüfen Sie die Feldzuordnung der Ticketwerte für den Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das vorherige Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler der erfassten Beispiele.

4. Klicken Sie auf, um diesen Fehler zu beheben **Zuordnung** In der Fortschrittsleiste.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie erneut eine Vorschau der Zuordnung an, und beheben Sie alle Fehler, die in Fehlermeldungen beschrieben werden.

Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind. Definieren Sie den Zeitplan.

Definieren Sie einen Zeitplan für die SecureWorks CTP-Ticketerfassung

Überprüfen Sie die Standardeinstellungen für den Ticketabruf, oder ändern Sie die Planung nach Bedarf. Mit diesem Schritt können Sie Ihren Ticketabruf basierend auf einem Datumsbereich und einem Abfrageintervall filtern.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

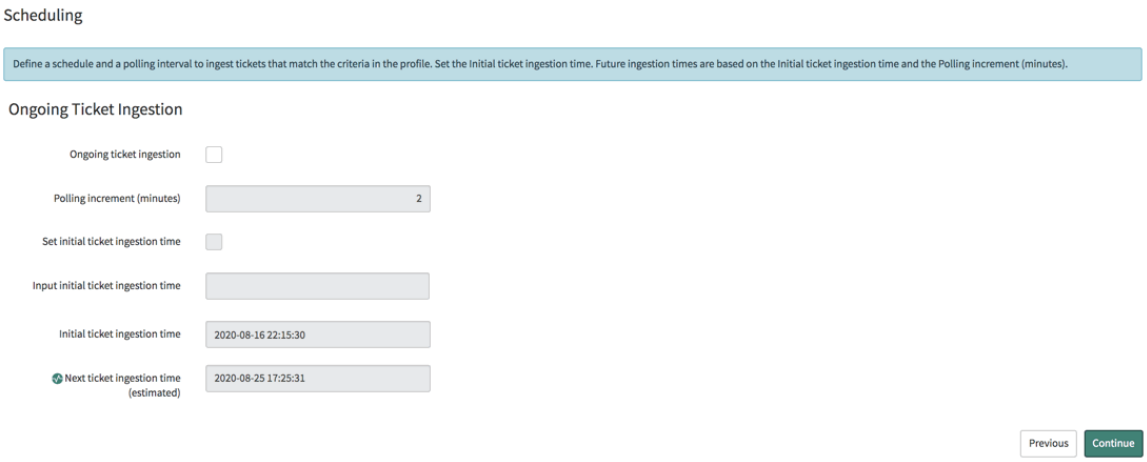
Sie wählen auch aus, wie oft Sie nach zukünftigen Tickets abfragen, die der Ticketprofilkonfiguration entsprechen. Konfigurieren Sie diese Abfrageintervalle pro Profil. Bei der Planung ziehen Sie es möglicherweise vor, die Systemlast gegen die Dringlichkeit des Incident auszugleichen. Für jedes Profil ist ein einminütiger Standardwert festgelegt. Sie können diese Einstellung jedoch basierend auf der Dringlichkeit des Incident und der erwarteten Belastung Ihres Systems ändern.

Prozedur

1. Wenn die Seite „Zeitplanung“ im Fortschrittsbalken nicht angezeigt wird, wählen Sie aus **Zeitplanung** .
2. Wählen Sie eine aus, um zu planen, wie und wann Tickets aus abgerufen werden Secureworks CTP Portal.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie Auf **Fahren Sie Fort** Um zur Seite „zusätzliche Optionen“ zu navigieren.

Automatisieren Sie Ticketaktualisierungen und -Abschlüsse basierend auf dem SIR-Incident-Status

Die Secureworks CTP Die Integration der Ticketerfassung verfügt über eine bidirektionale Schnittstelle, mit der sowohl Tickets Security Incidents erstellen können, als auch die Möglichkeit, die Tickets zu aktualisieren, sobald der Security Incident erstellt und/oder geschlossen wurde, mit relevanten Incident-Details wie Security Incident-Nummer, Zuweisungsgruppe, Security Incident-URL usw.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Wenn die Seite „zusätzliche Optionen“ im Fortschrittsbalken nicht angezeigt wird, wählen Sie aus **Zusätzliche Optionen** .
2. Schließen Sie die Konfiguration für die Aktualisierung von Tickets ab, wenn der Security Incident erstellt wird.
3. Klicken Sie Auf **Beenden** Um die Konfiguration abzuschließen und das Profil in zu verschieben **Warten** status.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Profil erfolgreich eingerichtet. Aktivieren Sie dieses Profil, um Tickets aus der abzurufen Secureworks CTP Portal basierend auf Ihrer Planung.

Optional: Kopieren Sie ein SecureWorks CTP-Profil

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, sollten Sie Profile kopieren, um Zeit zu sparen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie als Anwender mit der Rolle sn_si.admin ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), sodass es vor Abschluss der Konfiguration nicht versehentlich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktiviert wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und verifiziert haben.

Prozedur

1. Navigieren zu **Alle** > **Integration Der Secureworks-Ticketerfassung** > **Secureworks-Profil**an.
2. Wählen Sie in der angezeigten Liste SecureWorks-Profile ein Profil aus, das Sie kopieren möchten, und aus **Aktionen für ausgewählte Zeilen** Auswahlliste klicken Sie auf **Kopieren** .
   Das Profil wird kopiert und in der Liste angezeigt. Die Kopie verfügt über alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält (Kopie). Obwohl das ursprüngliche Profil aktiviert ist (Wahr), die Kopie ist zu diesem Zeitpunkt deaktiviert (Falsch). Möglicherweise möchten Sie Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf auf das neue Profil angewendet werden.

   Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert. Beachten Sie, dass **Aktiv** Der Spaltenstatus wird auf „falsch“ festgelegt, da das Profil aktiviert werden muss.

Nächste Maßnahme

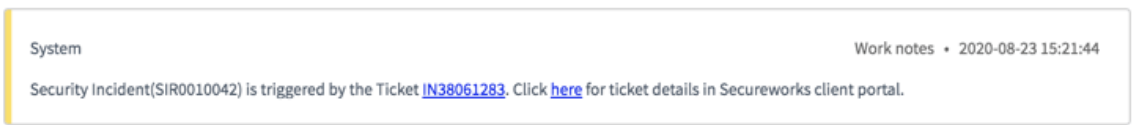
Sie werden aufgefordert, das neue Profil zu aktivieren (zu aktivieren), nachdem Sie die Konfigurationsschritte abgeschlossen haben.

Das Formular „Security Incident Response“ ändert sich nach der Ticketerfassung

Nach einem Secureworks CTP Ticket wurde erfasst, ein Security Incident wird erstellt, und die entsprechenden Aktualisierungen werden am Security Incident-Datensatz vorgenommen.

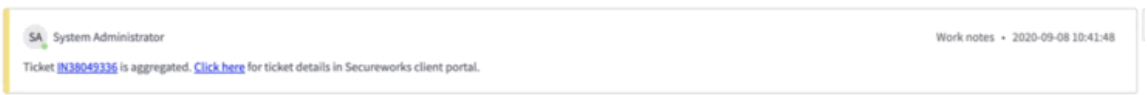
Arbeitsnotiz

Eine Arbeitsnotiz wird mit Details des Tickets veröffentlicht, das den Security Incident ausgelöst hat.



Klicken Sie auf den Ticket-Link, um zum internen SecureWorks-Ticket-zu-Aufgabe-Datensatz zu navigieren. Die **Klicken Sie hier** Hyperlink führt Sie zu Secureworks CTP Dashboard, in dem Sie die Ticketdetails anzeigen können.

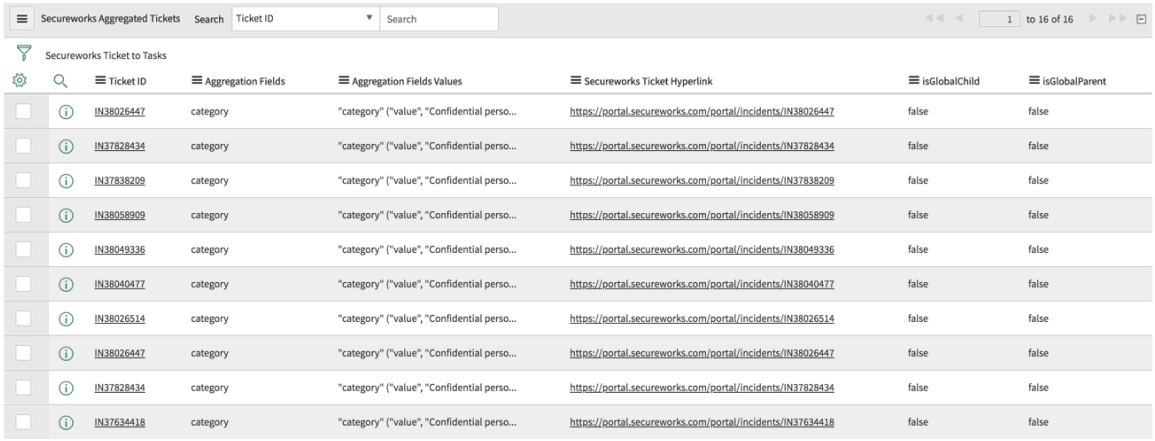
Wenn Sie ausgewählt haben **Arbeitsnotiz für neues Ticket protokollieren** Option in den Ticketzusammenfassungskriterien, wie auf der Seite „Profil erstellen: Zuordnung“ beschrieben, wird bei der Zusammenfassung des Tickets eine Arbeitsnotiz veröffentlicht.



Zusammengefasste Tickets

Klicken **Zugehörige Listen** > **Zusammengefasste Secureworks-Tickets** Um das zum Security Incident zusammengefasste Ticket anzuzeigen. Klicken Sie auf den Ticket-Hyperlink, um das Ticket in anzuzeigen Secureworks CTP Dashboard.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



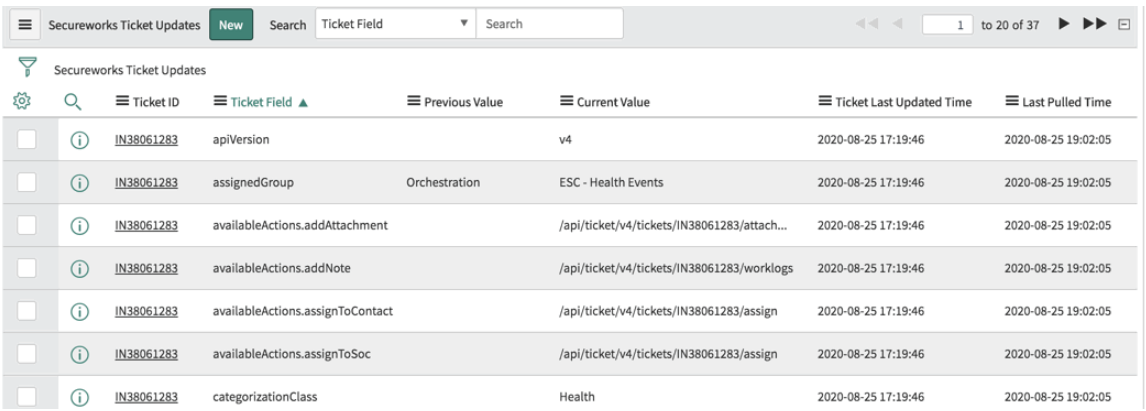
Ticket ID	Aggregation Fields	Aggregation Fields Values	Secureworks Ticket Hyperlink	isGlobalChild	isGlobalParent
IN38026447	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38026447	false	false
IN37828434	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN37828434	false	false
IN37838209	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN37838209	false	false
IN38058909	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38058909	false	false
IN38049336	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38049336	false	false
IN38040477	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38040477	false	false
IN38026514	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38026514	false	false
IN38026447	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN38026447	false	false
IN37828434	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN37828434	false	false
IN37634418	category	"category" ("value", "Confidential perso...	https://portal.secureworks.com/portal/incidents/IN37634418	false	false

Security Incident erstellen: Wählen Sie ein Ticket aus der Liste aus, und klicken Sie auf **Aktionen** Menü und klicken Sie auf **Erstellen Sie einen Security Incident** . Diese Option erstellt einen neuen Security Incident für das Ticket, und dieses Ticket wird vom übergeordneten Security Incident deaggregiert.

Ticketdatensatz löschen: Wählen Sie ein Ticket aus der Liste aus, und klicken Sie auf **Aktionen** Menü und klicken Sie auf **Löschen** . Mit dieser Option wird der Ticketdatensatz gelöscht.

SecureWorks-Ticket-Updates

Dadurch werden die Standardticketfelder angezeigt und Änderungen an den Tickets während jedes Abfrageintervalls nachverfolgt. Dies ist hilfreich, da Sie alle Ticketaktualisierungen direkt anzeigen können, ohne zu navigieren Secureworks CTP Dashboard. Alle Änderungen an den Werten werden in den Feldern „vorheriger Wert“ und „Aktueller Wert“ angezeigt.

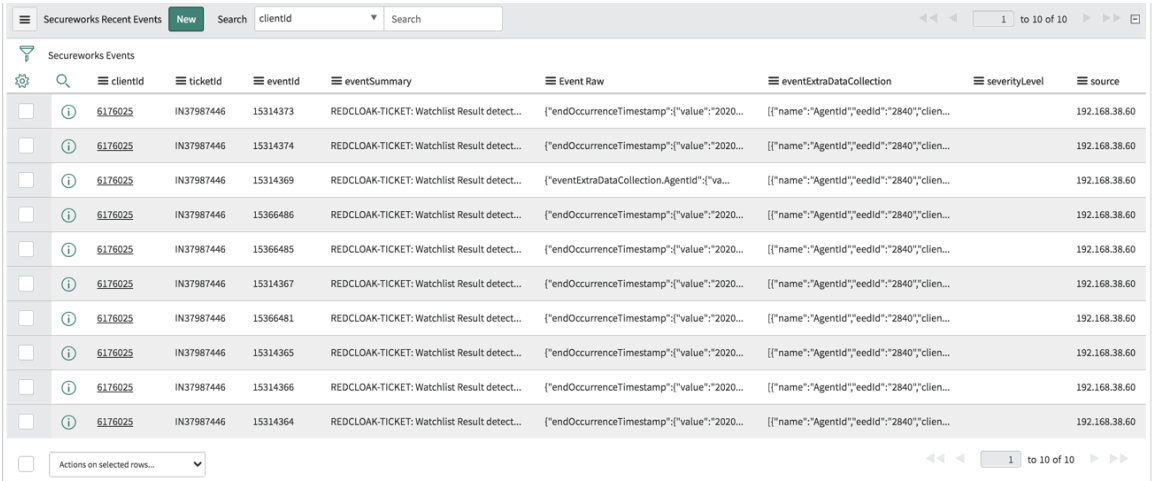


Ticket ID	Ticket Field ▲	Previous Value	Current Value	Ticket Last Updated Time	Last Pulled Time
IN38061283	apiVersion		v4	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	assignedGroup	Orchestration	ESC - Health Events	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.addAttachment		/api/ticket/v4/tickets/IN38061283/attach...	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.addNote		/api/ticket/v4/tickets/IN38061283/worklogs	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.assignToContact		/api/ticket/v4/tickets/IN38061283/assign	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	availableActions.assignToSoc		/api/ticket/v4/tickets/IN38061283/assign	2020-08-25 17:19:46	2020-08-25 19:02:05
IN38061283	categorizationClass		Health	2020-08-25 17:19:46	2020-08-25 19:02:05

Letzte Secureworks-Ereignisse

Klicken Sie auf **Ruft Die Letzten Secureworks-Ereignisse Ab** Option unter **Zugehörige Links** Zum Anzeigen der neuesten SecureWorks-Ereignisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Standardmäßig wird eine maximale Anzahl von 50 Ereignissen angezeigt. Sie können diese Standardeinstellung in den SecureWorks-Integrationseinstellungen ändern.

Zeigen Sie die SecureWorks-Tickets und die entsprechenden Security Incidents an

Importiert Secureworks CTP Tickets werden anfänglich in der Tabelle „Ticketimport“ gespeichert. Zeigen Sie alle an Secureworks CTP Tickets, die importiert wurden, bevor Filterbedingungen angewendet werden.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Integration Der Secureworks-Ticketerfassung** > **Sicherer Ticketimport**an.
2. Sie können alle anzeigen Secureworks CTP Tickets, die importiert wurden, bevor sie aggregiert oder Filterbedingungen angewendet werden.
3. Klicken Sie auf eine Ticket-ID, um die Rohticketdaten anzuzeigen.
4. Navigieren zu **Secureworks-Ticketerfassung** > **SecureWorks-Ticket zu Aufgabe**an.
   Die Secureworks CTP Tickets mit den entsprechenden Security Incidents werden angezeigt.

Abschlussmitteilung für SecureWorks CTP-Master-Ticket

Bevor Sie einen Security Incident schließen, der von erstellt wurde Secureworks CTP Master-Ticket: Sie müssen sicherstellen, dass alle untergeordneten Tickets, die dem Master-Ticket zugeordnet sind, geschlossen sind.

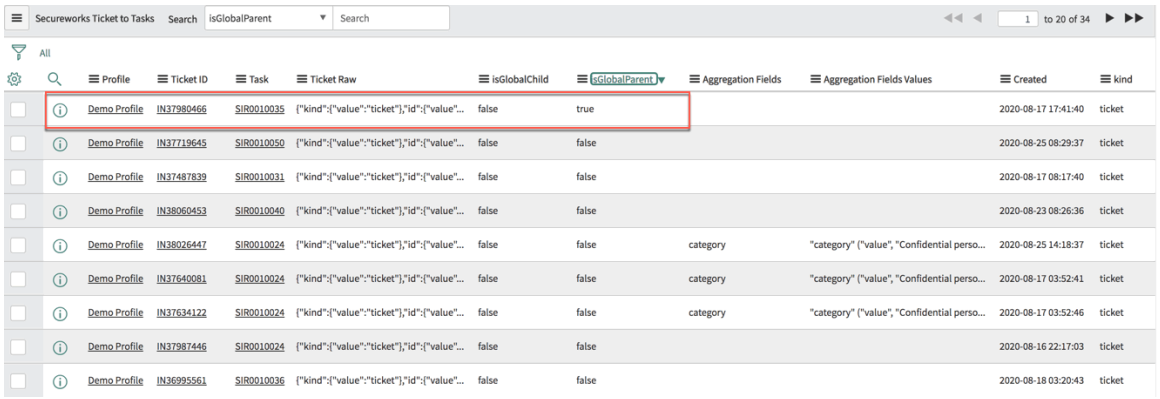
Vorbereitungen

Erforderliche Rolle: sn_si.admin

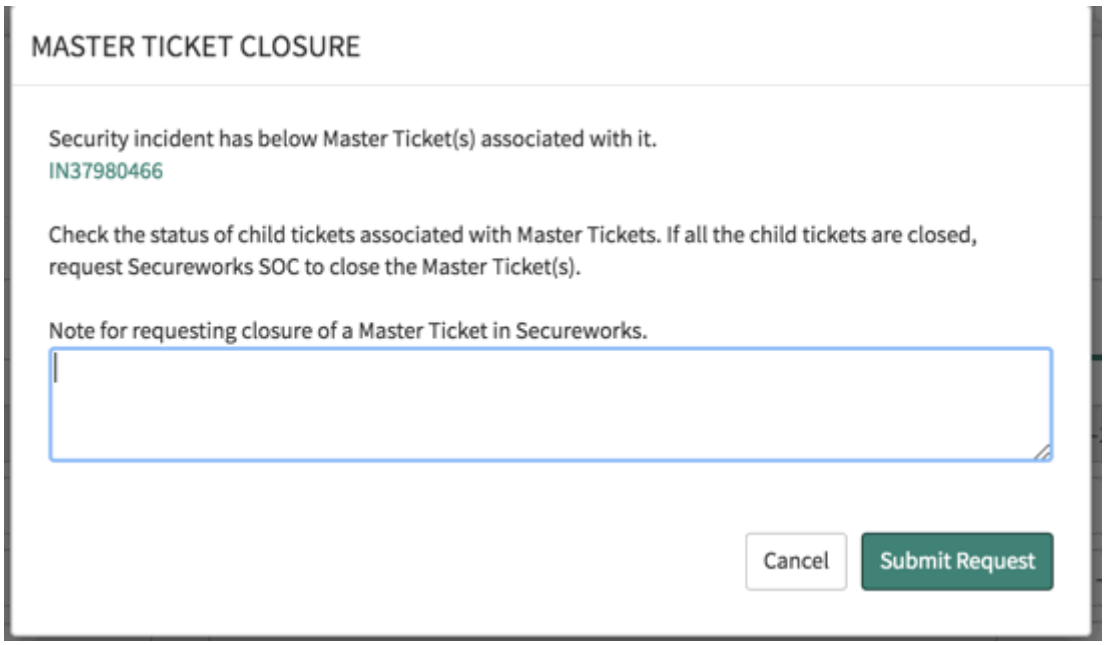
Prozedur

1. Navigieren zu **Alle** > **Secureworks-Ticketerfassung** > **SecureWorks-Ticket zu Aufgabe**an.
   Die Secureworks CTP Tickets mit den entsprechenden Security Incidents werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Klicken Sie mit auf den Security Incident **Ist GlobalParent** Feld auf festgelegt **Wahr.**
3. Ändern Sie den Status des Security Incidents in **Geschlossen** Geben Sie die Abschlusscodes an, und klicken Sie auf **Speichern** .
   Das folgende Dialogfeld wird angezeigt.



Dieser Security Incident ist einem SecureWorks Master Ticket zugeordnet. Einem Master-Ticket können ein oder mehrere untergeordnete Tickets zugeordnet sein. Bevor das Master-Ticket geschlossen werden kann, müssen Sie zuerst überprüfen, ob alle untergeordneten Tickets, die diesem Master-Ticket zugeordnet sind, geschlossen sind.

4. Fügen Sie eine Notiz hinzu, um den Abschluss des Master-Tickets in SecureWorks anzufordern, und klicken Sie auf **Anforderung Übermitteln** .
   Das Master-Ticket wird jetzt dem SecureWorks SOC-Team zugewiesen.
5. Sobald die Anforderung übermittelt wurde, können Sie den Security Incident schließen.
6. Navigieren zu **Anwendung** > **Modul**an.

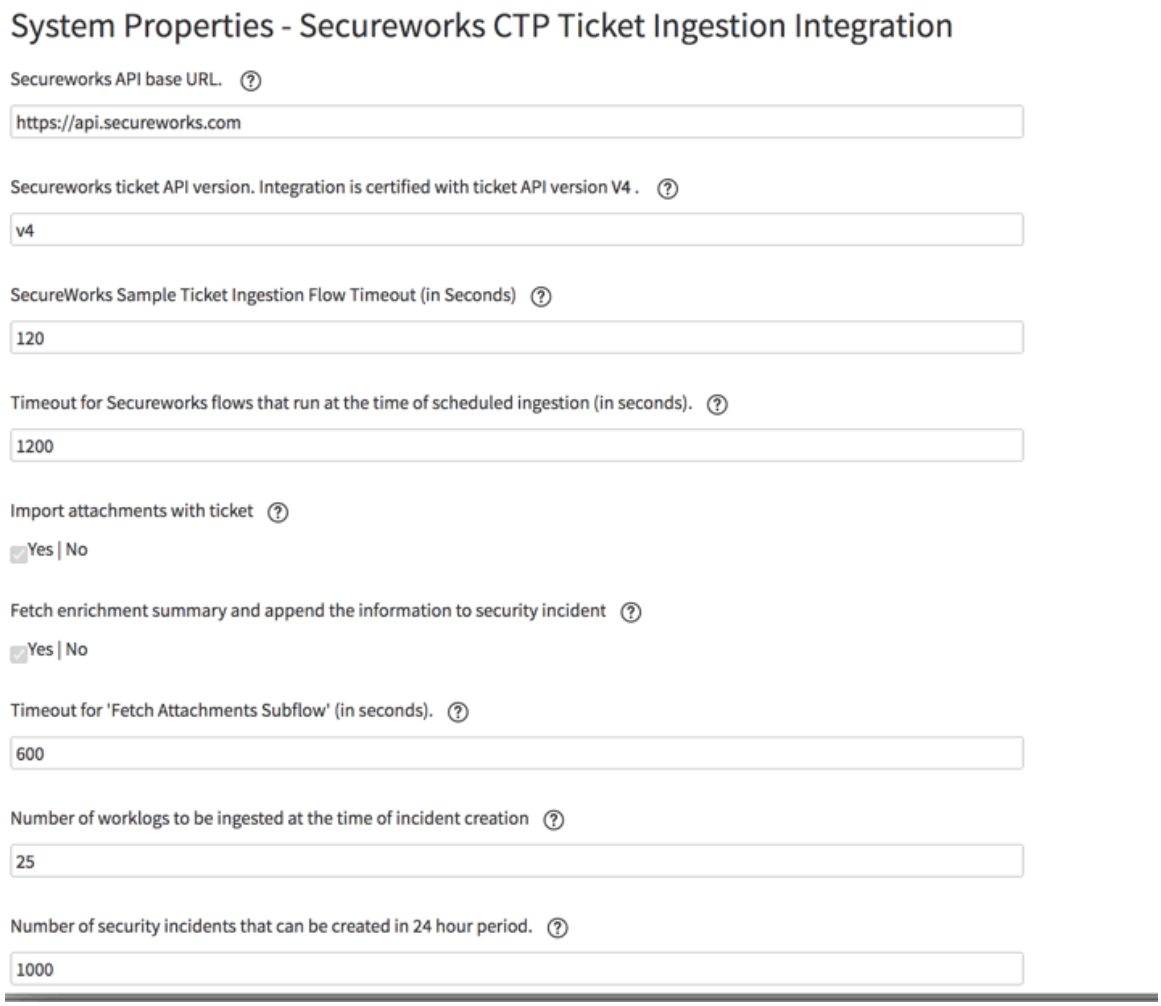
Konfigurationseinstellungen

Verwenden Sie diese Option, um zu ändern Secureworks CTP Standardsystemeigenschaften der Ticketerfassungsintegration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um die Systemeigenschaften zu ändern, melden Sie sich als Anwender mit an `sn_si.admin` Rolle und navigieren Sie zu **Integration Der Secureworks-Ticketerfassung** > **Einstellungen Für Secureworks-Integration**an.

Die Standardkonfigurationseinstellungen werden angezeigt. Sie können diese Einstellungen bei Bedarf ändern.



Alle geänderten Integrationseinstellungen werden während des nächsten Abfrageintervalls angewendet, wie im Profil definiert.

Integration von Security Incident Response mit zScaler

Sie können verwenden Integration von Security Incident Response mit zScaler Produkt zum Verbinden von Zscaler Internet Access Serverprotokolle (ZIA) mit ServiceNow AI Platform. Mit dieser Integration können Sie Dashboards anzeigen, anwenderdefinierte Warnungen erstellen und Security Incidents untersuchen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht

Die Zscaler internet- und Webgateway-Produkt wird aus der Cloud bereitgestellt. Es bietet Ihnen die wichtigsten Datenpunkte und Einblicke in Ihre Sicherheitsumgebung Ihres Unternehmens. Integration von Security Incident Response mit zScaler Verbindet Zscaler Internet Access Produkt mit Ihrem ServiceNow AI Platform Instanz. Mithilfe von Zscaler Produkt auf der ServiceNow AI Platform, Erhalten Sie weitere Einblicke in die Internetnutzung Ihrer Organisation.

Schlüsselfunktionen der Integration

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Reputationssuche von erkennbaren Elementen für die globale Bedrohungsbibliothek, die Zscaler Produktverwaltungen.

  Hinweis:
  Die Zscaler Die globale Bedrohungsbibliothek listet Bedrohungen nach Trends, Ursprungsland, Zielziel, Volumen und verschiedenen Bedrohungskategorien auf. Mit dieser globalen Bedrohungsbibliothek können Sie Ihre erkennbaren Elemente anhand der globalen Bedrohungslandschaft untersuchen.

- Wartung von erkennbaren Elementen in einer Block- oder Allow-Liste im Zscaler Produkt.
- Möglichkeit, Sandbox-Berichte aus der abzurufen und zu überprüfen Zscaler Produkt für einen MD5-Hash. Die Cloud-Sandbox-Funktion in Zscaler Das Produkt wird in einer virtuellen Umgebung ausgeführt und analysiert, um schädliches Verhalten zu erkennen.
- Sicherheitswarnungen aus Patienten 0-Ereignissen, die in generiert werden Zscaler Produkt, wenn ein Anwender eine unbekannte schädliche Datei herunterlädt.
- Mehrere URL-Kategorielisten, die als Blocklisten oder Allow-Listen fungieren, wie in definiert Zscaler Produkt.
- ServiceNow AI Platform Security Incidents, die getaggt werden können, um die URL-Kategorie zu identifizieren, der die erkennbaren Elemente hinzugefügt werden.
- Ablaufzeiträume, die die Größe der URL-Kategorielisteneinträge beibehalten, indem die älteren Einträge automatisch ablaufen oder entfernt werden.
- Genehmigungs-Workflow zum Hinzufügen und Entfernen erkennbarer Elemente aus den URL-Kategorielisten.
- URL-Kategorieeinträge, die mit Datensätzen erkennbarer Elemente und Security Incidents verknüpft werden können, die Threat Intelligence-Ergebnisse und Details dazu enthalten, warum ein Eintrag blockiert ist.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
Zscaler Produktdokumentations-Website	Website der ZScaler-Produktdokumentation
ServiceNow Produktdokumentations-Website	ServiceNow-Produktdokumentationswebsite

Erste Schritte mit Integration von Security Incident Response mit zScaler

Aktivieren und richten Sie ein Zscaler Internet Access Produkt, das mit verbunden werden soll ServiceNow AI Platform Instanz und Security Incident Response Produkt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste

Setupaufgabe	Beschreibung

Weisen Sie die erforderlichen zu, und verifizieren Sie sie ServiceNow AI Platform Und Security Incident Response Rollen.	Diese Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich:
	• Die Administratorrolle installiert die Integration aus dem ServiceNow Store Und weist die Rolle sn_si.admin zu.
	• Die Rolle sn_si.admin führt die folgenden Aufgaben aus:
	  ○ Konfiguriert die Integration.
	  ○ Erstellt, aktiviert und entfernt die URL-Kategorielisten.
	  ○ Weist die Rolle „sn_si.Analyst“ zu.
	• Die Rolle „sn_si.Analyst“ erstellt Einträge und arbeitet mit Security Incidents.

Überprüfen Sie, ob ServiceNow Kernanwendungen werden installiert und aktiviert, bevor Sie diese Integration konfigurieren.	Die ServiceNow IntegrationHub Enterprise-Paket-Installationsprogramm [Plugin com.glide.hub.integrations.enterprise] ist erforderlich. Die Security Incident Response Plugin (com.snc.security_incident) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten für Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Anwendungen für die Integration. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn diese Anwendungen noch nicht installiert sind, installieren und aktivieren Sie jede Anwendung einzeln in der folgenden Reihenfolge: **1.** Security Incident Response Abhängigkeit (com.snc.si_dep) **2.** Sicherheits-Integrations-Framework **3.** Security Support Common **4.** Orchestration Des Sicherheitssupports **5.** Threat Intelligence Support Allgemein **6.** Trusted Security Circles

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	7. Security Operations Setup-Assistent **8.** Security Incident Response
Verifizieren Sie Zscaler Versionen.	• Diese Integration wird in unterstützt Zscaler Internet Access Version 1,0 oder höher. • Diese Integration wird mit den folgenden getestet Zscaler Versionen: ○ Zscaler Client Connector für Windows – 3,0 ○ Zscaler-Client-Connector für macOS – 3,0 ○ Zscaler Client Connector für Linux – Beta ○ Zscaler Cloud Connector – 6,1
Stellen Sie sicher, dass Sie über die erforderlichen verfügen Zscaler Berechtigungen und haben konfiguriert Zugriff auf Zscaler Internet Access APIsan.	• Sie müssen über die Administratoranmeldeinformationen für verfügen Zscaler Internet Access. • Sie benötigen ein gültiges Cloud-Service-API-Abonnement. Zscaler Support muss Ihren Schlüssel bereitstellen. • Sie müssen haben Zscaler Internet Access administratoranmeldeinformationen (Anwendername und Passwort). Die API-Authentifizierung basiert auf einer Kombination aus dem API-Schlüssel und Zscaler Internet Access administrator-Anmeldeinformationen. **Hinweis:** Weitere Informationen zum Verwalten von finden Sie Zscaler Internet Access API-Schlüssel, siehe Zscaler-Dokumentation .

Konfigurieren Sie den Zugriff auf Zscaler Internet Access APIs

Konfigurieren Sie den Zugriff auf Zscaler Internet Access Server zur Authentifizierung der sicheren Verbindung zwischen ServiceNow AI Platform Instanz und Zscaler Server.

Vorbereitungen

Erforderliche Rolle: Zscaler Internet Access Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Nach Zscaler Aktiviert Ihr API-Abonnement für den Cloud-Service Ihrer Organisation. Es ist in verfügbar Zscaler Internet Access API-Schlüsselverwaltungsseite mit der Basis-URL. Ihre Organisation kann nur einen API-Schlüssel oder ein Token haben. Löschen Sie den vorhandenen Schlüssel oder Token, bevor Sie einen neuen hinzufügen.

Die Basis-URL für die API ist `${Cloud_Name}/api/v1` . Überprüfen Sie Zscaler Cloud-Name, der für Ihre Organisation bereitgestellt wurde, und verwenden Sie ihn zum Ersetzen `{Cloud_Name}` Im Basis-URI. Einige Beispiele für die Basis-URL sind:

- example.zscalerbeta.net
- example.zscalerone.net
- example.zscalertwo.net
- example.zscaler.net
- example.zscloud.net

Hinweis:
Weitere Informationen zu finden Zscaler Internet Access Administrationsportal, siehe Dokumentation zur Schlüsselverwaltung der Zscaler-API Und Dokumentation zum Zscaler-Portal .

Prozedur

1. Melden Sie sich als Administrator bei an Zscaler Internet Access Administrationsportal.
2. Navigieren zu **Administration** > **Sicherheit der Cloud-Service-API**an.
3. Klicken Sie Auf **Fügen Sie einen API-Schlüssel hinzu** .
   Wenn Sie nicht sehen **Fügen Sie einen API-Schlüssel hinzu** Option, löschen Sie den vorhandenen Schlüssel.
   Der neue API-Schlüssel ist sofort gültig und wird auf der Registerkarte angezeigt.

Ergebnisse

Sie haben die Basis-URL und den API-Schlüssel für die Konfiguration des Zugriffs auf abgerufen Zscaler Von ServiceNow AI Platform Instanz.

Integration von Security Incident Response mit zScaler installieren und konfigurieren

Installieren und konfigurieren Sie Integration von Security Incident Response mit zScaler Internetzugriffsprodukt über ServiceNow Store Um mit der Verwendung der Integration auf Ihrem zu beginnen ServiceNow AI Platform Instanz.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Laden Sie herunter Integration von Security Incident Response mit zScaler Produkt aus dem ServiceNow Store Und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie nach Integration von Security Incident Response mit zScaler Kachel und klicken Sie auf **Konfigurieren** > **Neue Konfiguration erstellen**an.
4. Füllen Sie im Formular die Felder aus.

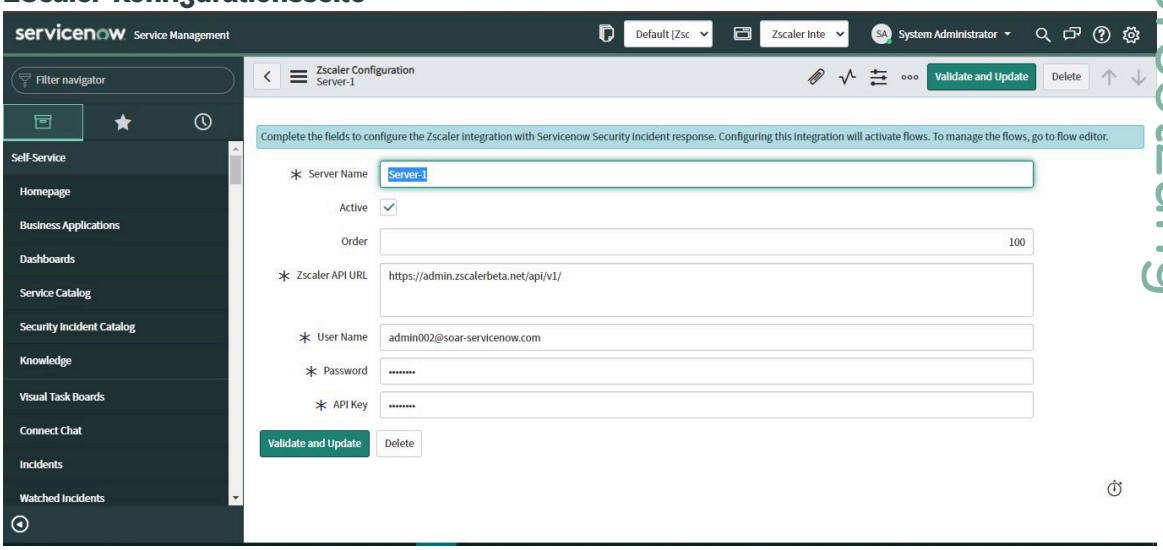
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zscaler Konfigurationsformular

Feld	Beschreibung
Servername	Zscaler Servername. Beispiel: ZSserver.
Aktiv	Indikator, dass das Profil aktiv ist.
Reihenfolge	Flow-Priorität. Der Wert für dieses Feld gibt die Reihenfolge der Workflows an, wenn zwei oder mehr Profile Auslösebedingungen teilen. Der Flow mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Beispiel: 100, 200, 300, 400. Der Standardwert ist 100.
Zscaler API-URL	Basis-URL, die hostet Zscaler API. Beispiel: https://example.zscalerbeta.net
Anwendername	Anwendername für Zscaler Internet Access administrator-Account.
Passwort	Passwort für Zscaler Internet Access administrator-Account.
API-Schlüssel	API-Schlüssel, den Sie vom erhalten haben Zscaler Internet Access Administrationsportal.

Das folgende Beispiel zeigt die Zscaler-Konfigurationsseite.

ZScaler-Konfigurationsseite



5. Klicken Sie Auf **Validieren und aktualisieren** .

Ergebnisse

Nachdem Sie diese Konfiguration validiert und gespeichert haben, kehren Sie zu zurück Zscaler Konfigurationsseite.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinzufügen Zscaler Internet Access URL-Kategorielisten

Fügen Sie die URL-Kategorien hinzu, die in verfügbar sind Zscaler Internetzugriffsprodukt auf ServiceNow AI Platform Instanz zum Angeben einer Aktion für jede URL, damit Sie einfachen Zugriff für granulare Filterung und Richtlinienerstellung haben.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Die Integration von Security Incident Response mit zScaler Stellt eine standardmäßige Allow-Liste und Deny-Listen-URL-Kategorielisten bereit, um Inhalte zu filtern.

Die URL-Kategorien, die Sie in hinzufügen ServiceNow AI Platform Instanz muss sich bereits in befinden Zscaler Internet Access Umgebung. Sie können nicht verwenden Integration von Security Incident Response mit zScaler Dient zum Erstellen von URL-Kategorien für Zscaler.

Hinweis:
Für weitere Informationen zu URL-Kategorielisten in Zscaler Produkt, siehe Zscaler-Dokumentation zu URL-Kategorien .

Prozedur

1. Navigieren zu **Alle** > **ZScaler-Integration** > **ZScaler-URL-Kategorielisten**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Zscaler Formular „URL-Kategorielisten“

Feld	Beschreibung
Quelle	Name des Servers. Sie können nur die zuvor konfigurierten anzeigen Zscaler Internet Access Server aus der URL-Kategorieliste.
Aktiv	Indikator, dass die URL-Kategorieliste aktiv ist.
URL-Kategorie	Feld, das aktiviert wird, nachdem Sie die Quelle ausgewählt haben. Sie können die Liste der URL-Kategorien anzeigen, die in erstellt werden Zscaler.
Ablaufzeitraum (in Tagen)	Ablaufzeitraum der URL-Kategorieliste. 0 (standardmäßig) gibt an, dass der URL-Kategorielisteneintrag nie abläuft. Durch Ändern dieses Werts ist jedes erkennbare Element, das dieser URL-Kategorie hinzugefügt wurde, für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben. Wenn Sie beispielsweise den Ablaufzeitraum auf 30 Tage festlegen, werden die Einträge nach 30 Tagen aus der Kategorieliste entfernt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tag anzeigen	Sicherheits-Tag, das auf angezeigt wird SIR Security Incident. Wenn Sie aktivieren **Tag Anzeigen** Option, die Zscaler Tag für das Feld „erkennbare Elemente“ ist im Formular verfügbar.
Change-Anforderung erstellen	Change-Anforderung und Change-Aufgaben in Ihrem ServiceNow AI Platform Instanz für die Datensätze, die an die URL-Kategorieliste angehängt sind. Wenn Sie aktivieren **Erstellen Sie Eine Change-Anforderung** Option, die **Change-Anforderung** Feld ist im Formular verfügbar.
Genehmigung erforderlich	Liste der Genehmigergruppen. Nachdem Sie eine Anforderung übermittelt haben, ist eine Genehmigung von der Gruppe erforderlich, um die Anforderung abzuschließen. Wenn Sie aktivieren **Genehmigung Erforderlich** Option, die **Genehmiger zum Hinzufügen erkennbarer Elemente** Und **Genehmiger zum Entfernen erkennbarer Elemente** Felder sind im Formular verfügbar. ○ **Genehmiger zum Hinzufügen erkennbarer Elemente** : Wählen Sie die Genehmiger mithilfe der Suche aus, um die erkennbaren Elemente aus der hinzuzufügen **Zscaler-URL-Kategorieliste** Seite. Mit dieser Option können Sie die Anwendergruppe(n) für Genehmigungen hinzufügen. ○ **Genehmiger zum Entfernen erkennbarer Elemente** : Wählen Sie die Genehmiger zum Entfernen der erkennbaren Elemente mithilfe der Suche aus **Zscaler-URL-Kategorieliste** Seite. Mit dieser Option können Sie die Anwendergruppe(n) aus der Genehmigungsliste entfernen.
Beschreibung	Beschreibung von Zscaler URL-Kategorieliste. Verwenden Sie dieses Feld, um weitere Details zum URL-Kategoriedatensatz hinzuzufügen.

4. Klicken Sie auf **Absenden**.
   Eine erfolgreiche Übermittlung löst eine E-Mail-Benachrichtigung an die Genehmigungsgruppe aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übermitteln Sie erkennbare Elemente aus einem Security Incident-Datensatz an eine URL-Kategorieliste

Übermitteln Sie erkennbare Elemente, die an einen Security Incident-Datensatz angehängt sind, mithilfe der Anforderung Zulassen oder Blockieren an eine konfigurierte URL-Kategorieliste. Durch das Hinzufügen erkennbarer Elemente zur Allow- oder Block-Liste für Sicherheitsscans können Anwender Inhalte aus diesen URLs überprüfen und Zugriff auf vertrauenswürdige Inhalte erhalten.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

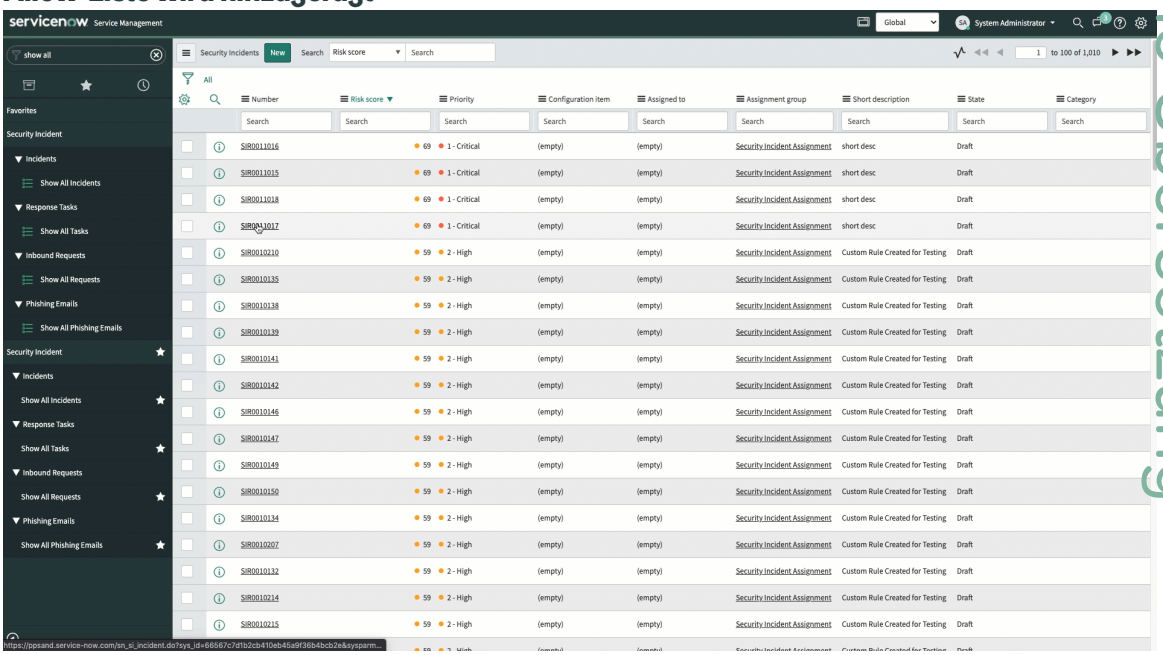
Warum und wann dieser Vorgang ausgeführt wird

Sie übermitteln Einträge erkennbarer Elemente, indem Sie die Aktion Anforderung zulassen oder blockieren aus der zugehörigen Liste der zugehörigen erkennbaren Elemente verwenden. Erkennbare Elemente sind Artefakte, die in einem Netzwerk oder Betriebssystem gefunden werden und wahrscheinlich auf einen Angriff hinweisen. Verwenden Sie die Liste von Zuvor konfigurierte URL-Kategorien Um das erkennbare Element auszuwählen, das Sie übermitteln möchten. Nachdem Sie die Anforderung übermittelt haben, wird eine Genehmigungsanforderung an Ihre Genehmigungsgruppe gesendet.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**an.
   In diesem Beispiel erfahren Sie, wie Sie einen Security Incident und ein erkennbares Element auswählen und eine Allow-Liste hinzufügen.

Allow-Liste wird hinzugefügt



2. Wählen Sie den Security Incident aus, den Sie dem zuordnen möchten Zscaler Anforderung zulassen oder blockieren.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und **Zugeordnete Erkennbare Elemente** Registerkarte.
   Wenn Sie keine erkennbaren Elemente finden, klicken Sie auf **Neu** .
4. Wählen Sie ein erkennbares Element aus, und klicken Sie dann im Aktionsmenü auf **Anforderung Zulassen/Blockieren** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im Dialogfeld „Anforderung zulassen/blockieren“ aus, ob die Anforderung „Zulassen“ oder „Blockieren“ für das erkennbare Element ausgeführt werden soll.
6. Klicken Sie auf **Absenden**.
7. Zeigen Sie die Arbeitsnotizen an, um den Status Ihrer Übermittlung und die Sicherheits-Tags anzuzeigen. Klicken Sie auf die Links in den Arbeitsnotizen, um weitere Informationen zum Status zu erhalten oder die Details zu zu analysieren Workflow-Studio. Sicherheits-Tags sind Metadaten im Antwortdatensatz und definieren, wer Zugriff auf bestimmte Arten von Sicherheitsinhalten haben soll.
8. Um den Status des ausgewählten erkennbaren Elements anzuzeigen, navigieren Sie zu **Zscaler-Integration** > **Einträge in Liste der Zscaler-URL-Kategorien**an.
9. Klicken Sie auf der Zscaler-URL-Kategorielisteneinträge auf das erkennbare Element, um den Datensatz anzuzeigen.

Genehmigen Sie erkennbare Elemente für URL-Kategorielisten

Genehmigen Sie erkennbare Elemente, die einer URL-Kategorieliste hinzugefügt werden, damit sich Einträge erkennbarer Elemente in den entsprechenden Allow- oder Deny-Listen befinden.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Alle** > **Zscaler-Integration** > **Zscaler-Genehmigungen**an.
2. Wählen Sie den zu genehmigenden Datensatz aus.
3. Klicken Sie auf **Genehmigen**.
   Die Genehmigergruppe erhält eine E-Mail-Benachrichtigung für die Genehmigungsanforderung. Nachdem die Genehmiger auf geklickt haben **Genehmigen/Ablehnen** Link in der E-Mail ändert sich der Status in genehmigt.

Übermitteln Sie den Security Incident an Zscaler URL-Kategorieliste

Übermitteln Sie Einträge direkt für erkennbare Elemente, die keinem bestimmten zugeordnet sind ServiceNow AI Platform Security Incident-Datensatz, damit sich Einträge erkennbarer Elemente in den entsprechenden Allow- oder Deny-Listen befinden.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können der URL-Kategorieliste auch erkennbare Elemente direkt aus dem Datensatz des erkennbaren Elements hinzufügen.

Prozedur

1. Navigieren zu **Alle** > **Zscaler-Integration** > **Einträge in Liste der Zscaler-URL-Kategorien**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Zscaler Formular „URL-Kategorielisteneinträge“

Feld	Beschreibung
Eingabewert	Name des erkennbaren Elements.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn ein übereinstimmendes erkennbares Element gefunden wird, wird der Rest des Formulars automatisch ausgefüllt. Wenn kein übereinstimmendes erkennbares Element gefunden wird, müssen Sie die restlichen Informationen manuell eingeben.
Erkennbares Element	Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist.
Erkennbarer Typ	Klassifizierung erkennbarer Elemente, z. B. eine IP-Adresse oder ein Datei-Hash.
Liste der URL-Kategorien	URL-Kategorie. Wenn eine Organisation beispielsweise example.com für Office 365-Services verwendet, dann Zscaler Kategorisiert example.com als Professional Services und Office 365.
Quelle	Name des Servers. Sie können nur die zuvor konfigurierten anzeigen Zscaler Server aus der URL-Kategorieliste.
Incident-Anzahl	Anzahl der Incidents, in denen dieses erkennbare Element angezeigt wird. Dieser Wert wird automatisch aktualisiert, wenn das erkennbare Element manuell oder über einen Workflow einem anderen Incident hinzugefügt wird.
Aktiv	Indikator, dass die URL-Kategorieliste aktiv ist.
Status	Status, wenn das erkennbare Element genehmigt oder abgelehnt wurde.
Ablaufzeitraum (in Tagen)	Ablaufzeitraum der URL-Kategorieliste. 0 (standardmäßig) gibt an, dass der URL-Kategorielisteneintrag nie abläuft. Durch Ändern dieses Werts ist jedes erkennbare Element, das Sie dieser URL-Kategorie hinzufügen, für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben. Wenn Sie beispielsweise den Ablaufzeitraum auf 30 Tage festlegen, werden die Einträge nach 30 Tagen aus der Kategorieliste entfernt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn Sie den standardmäßigen Ablaufzeitraum des URL-Kategorielisteneintrags ändern, wird eine Warnung angezeigt, dass der Zeitraum von dem Zeitraum abweicht, der in der ausgewählten URL-Kategorieliste konfiguriert ist.
Zusätzliche Informationen	Feld, in dem Sie weitere Details zum erkennbaren Element hinzufügen können.

4. Klicken Sie auf **Absenden**.

Führen Sie eine Bedrohungssuche mit aus Zscaler Globale Bedrohungsbibliothek

Führen Sie mithilfe von eine Bedrohungssuche für ein erkennbares Element aus Zscaler Internet Access Globale Bedrohungsbibliothek des Produkts. Zscaler Unterstützt Suchen nach IPs, URLs und Domänen erkennbarer Elemente.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Threat Intelligence-Suchen für ein oder mehrere erkennbare Elemente durchführen, um festzustellen, ob sie bekannten Sicherheitsbedrohungen zugeordnet sind. Wenn ein erkennbares Element zum ersten Mal einem Security Incident zugeordnet wird, werden alle aktiven Implementierungen der Bedrohungssuche in durchgeführt ServiceNow AI Platform Führen Sie eine automatische Bedrohungssuche durch. Sie können die Ergebnisse für die zugehörige Liste „Ergebnisse der Bedrohungssuche“ anzeigen.

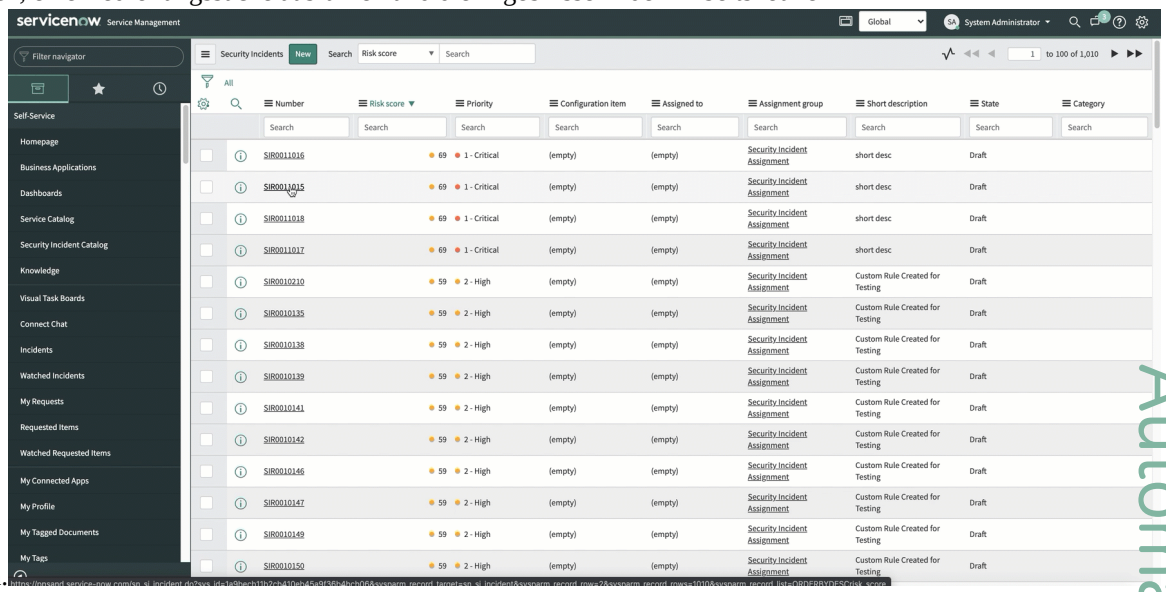
Standardmäßig wird die Konfiguration mit der geringsten Reihenfolge ausgewählt, um die Bedrohungssuche für durchzuführen Zscaler Internet Access Globale Bedrohungsbibliothek des Produkts. Sie können die Bedrohungssuche auch manuell durchführen.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, für den Sie die Bedrohungssuche ausführen möchten.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und **Zugeordnete Erkennbare Elemente** Registerkarte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü Aktionen auf **Bedrohungssuche Ausführen** .
   In diesem Beispiel erfahren Sie, wie Sie einen Security Incident und ein erkennbares Element auswählen, eine Bedrohungssuche ausführen und die Ergebnisse in den Arbeitsnotizen anzeigen.



Ergebnisse

Nachdem Sie die Bedrohungssuche initiiert haben, können Sie die Arbeitsnotizen anzeigen, um den Status Ihrer Übermittlung anzuzeigen.

Senden an Zscaler Sandbox-Analyse

Verwenden Sie Zscaler Internet Access Produkte-Sandbox-Service zum Analysieren von Dateien in einer virtuellen Umgebung, um schädliches Verhalten zu erkennen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen erstellen Zscaler Konfiguration, A Zscaler Die Sandbox-Übermittlung wird standardmäßig im Zscaler-Sandbox-Konfigurationsmodul erstellt.

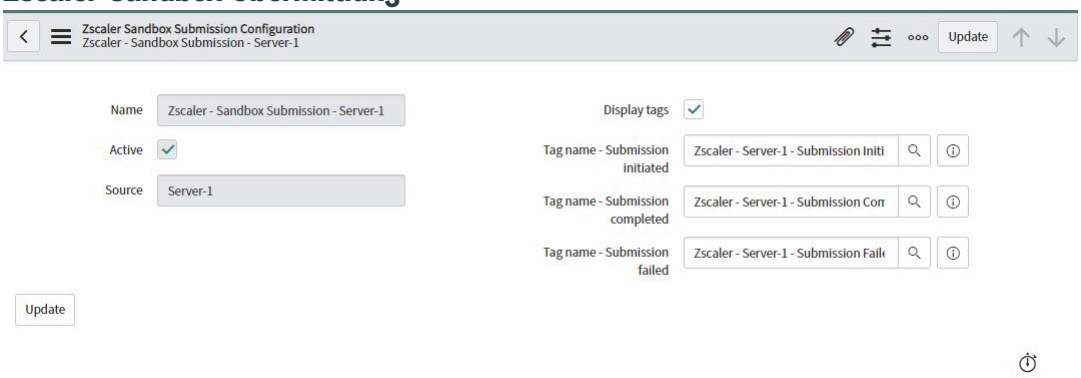
Die Felder „Name“ und „Quelle“ werden automatisch ausgefüllt, und die Konfiguration ist standardmäßig aktiviert. Sie können nur das Anzeige-Tag und die aktiven Optionen bearbeiten. Zscaler Internet Access Mit dem Produkt können Sie nur den Sandbox-Bericht für erkennbare Elemente vom Typ MD5-Hash abrufen.

Die Analyse für die Datei, die dem MD5-Hash zugeordnet ist, muss abgeschlossen sein, und der entsprechende Bericht muss sich im befinden Zscaler Sandbox. Wenn der von Ihnen gesendete MD5-Hash keinen Bericht in enthält Zscaler, Sie erhalten eine Fehlermeldung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zscaler-Sandbox-Übermittlung



Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, für den Sie die Sandbox-Analyse ausführen möchten.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und **Zugeordnete Erkennbare Elemente** Registerkarte.
4. Wählen Sie ein erkennbares Element vom Typ MD5-Hash aus, und wählen Sie dann im Menü Aktionen die Option aus **An Sandbox senden** .
   Erstellen Sie ein erkennbares Element vom Typ MD5-Hash, wenn Sie kein vorhandenes erkennbares Element vom Typ MD5-Hash finden.
5. Wählen Sie im Dialogfeld Dateiübermittlung die Option aus **Zscaler – Sandbox-Übermittlung – Server** Option in der Übermittlungskonfiguration, und klicken Sie auf **An Sandbox senden** .
   Nachdem Sie die Sandbox-Übermittlung initiiert haben, können Sie die Arbeitsnotizen anzeigen, um den Status Ihrer Übermittlung anzuzeigen. An den Security Incident wird auch ein Tag angehängt.
6. Klicken Sie in den Arbeitsnotizen auf den Link im Ergebnisbeitrag der Sandbox-Übermittlung.

Ergebnisse

Sie können die Ergebnisse auch auf der Registerkarte „alle zugehörigen Listen anzeigen“ und „Sandbox-Übermittlungsergebnisse“ anzeigen.

Richten Sie E-Mail-Warnungen für Ereignisse von Patient 0 ein

Konfigurieren Zscaler Internet Access Produkt zum Identifizieren und Scannen unbekannter, potenziell schädlicher Dateien, z. B. Patienten 0-Ereignisse, damit Sie Ihr Netzwerk vor schädlichen Dateien schützen können.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, Zscaler Internet Access Administrator

Warum und wann dieser Vorgang ausgeführt wird

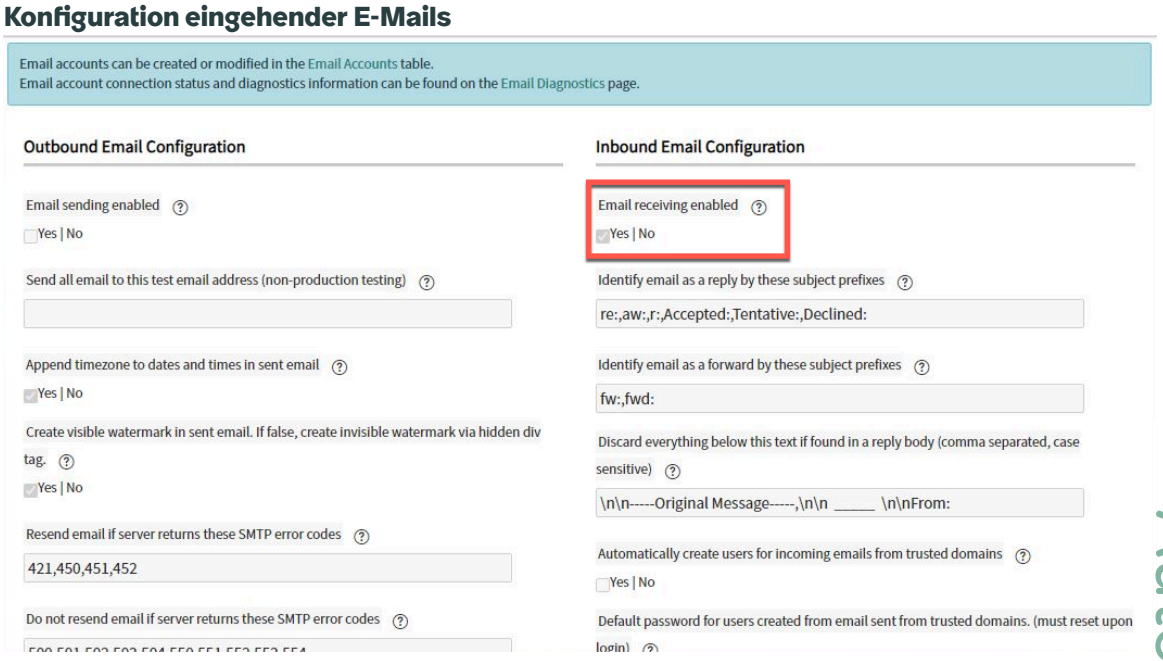
Patient O ist eine Warnungsklasse, die eine unbekannte Datei enthält, die heruntergeladen werden darf, aber als schädlich befunden wurde. Das Ereignis „Patient 0“ wird als kritisch klassifiziert. Sie können einrichten ServiceNow AI Platform Dient zum Empfangen von E-Mail-Warnungen in regelmäßigen Abständen für Ereignisse von Patient 0.

Prozedur

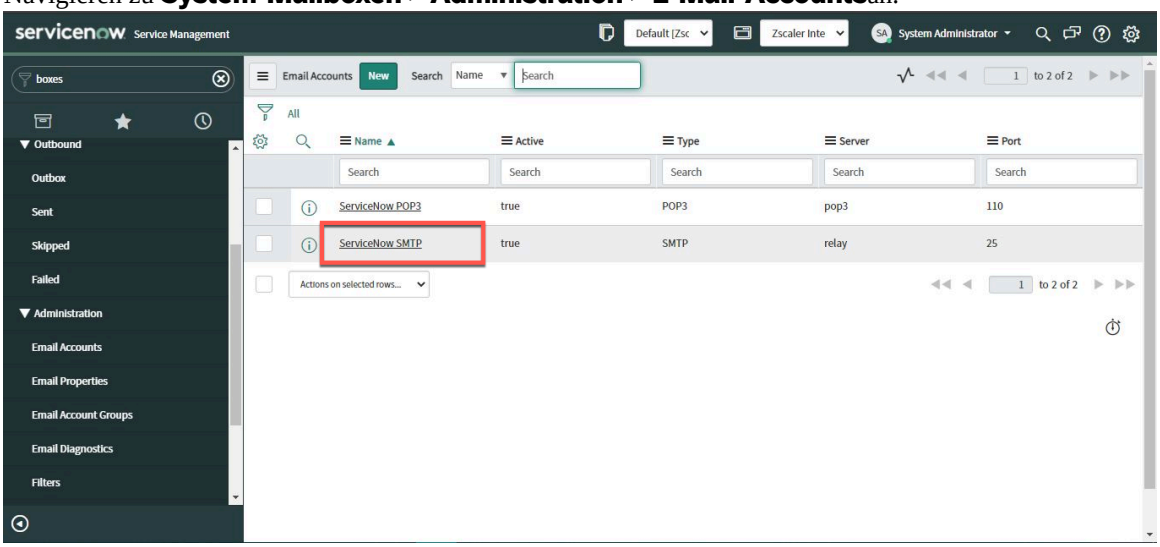
1. Navigieren zu **Alle** > **System-Mailboxen** > **Administration** > **E-Mail-Eigenschaften**an.
2. Wählen Sie im Abschnitt Konfiguration eingehender E-Mails die aus **E-Mail-Empfang aktiviert** Option.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **Speichern**.
4. Navigieren zu **System-Mailboxen** > **Administration** > **E-Mail-Accounts**an.

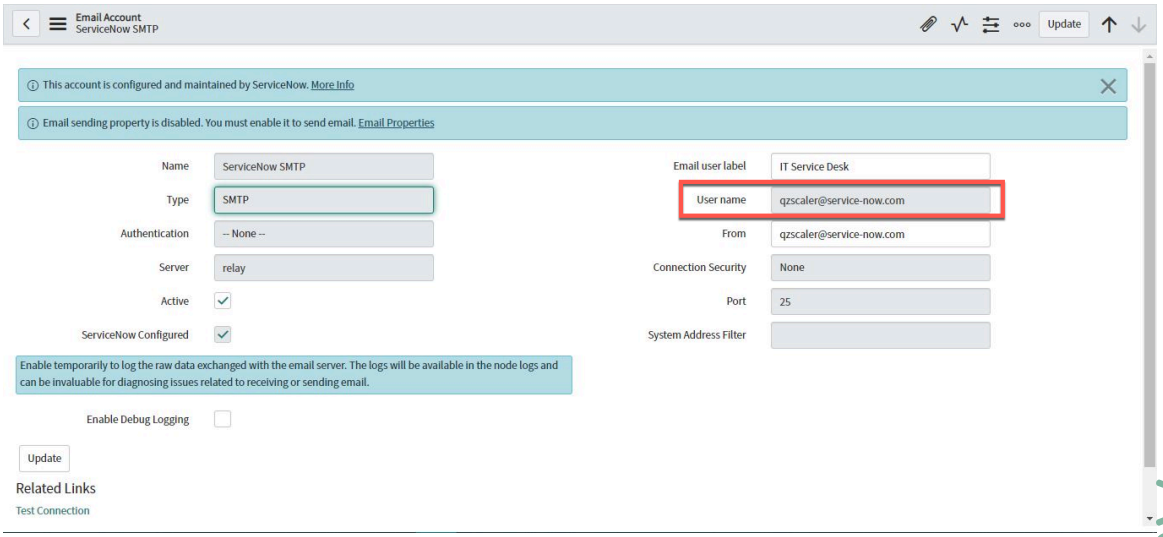


5. Wählen Sie aus **ServiceNow-SMTP** E-Mail-Account.
   Beachten Sie den Anwendernamen. Der hier identifizierte Anwendername ist ServiceNow AI Platform E-Mail-Adresse, die Sie zum Konfigurieren in verwenden Zscaler Für Patienten 0 Warnungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendername für ServiceNow AI Platform SMTP-Account



6. Melden Sie sich bei an Zscaler Internet Access Administrationsportal.

> **Hinweis:**
> Weitere Informationen zu finden Zscaler Internet Access Administrationsportal, siehe Zscaler-Dokumentation .

7. Navigieren zu **Administration** > **Alerts** > **Warnungen Veröffentlichen**an.
8. Klicken Sie Auf **Fügen Sie Ein Warnungsabonnement Hinzu** .
9. Füllen Sie im Formular die Felder aus.

Formular „Warnungsabonnement hinzufügen“

Feld	Beschreibung
E-Mail	ServiceNow AI Platform E-Mail-Adresse des SMTP-Accounts.
Beschreibung	Feld zum Hinzufügen weiterer Details zu den Warnungen von Patient 0.

10. Klicken Sie auf **Speichern**.

ServiceNow Security Operations Add-on für Splunk-Übersicht

Die ServiceNow Security Operations Add-on für Splunk Ermöglicht einen Splunk Softwareadministrator zum Sammeln von Daten und Erstellen von Incidents und Ereignissen in ServiceNow AI Platform.

Das Add-on wird von installiert Splunkbase.

> **Wichtig:**
> Splunk Wird auch für die Umgebung des Managed Service Providers (MSP) unterstützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setup der Splunk-Integration

Setup-Verfahren für ServiceNow Security Operations Das Add-on für Splunk umfasst das Herunterladen der Add-on-Datei in Splunk, die Installation des Add-ons und die Einrichtung von ServiceNow Instanz, in der Security Incidents und Ereignisse erstellt werden.

Erforderliche Rolle

Bevor Sie Verfahren zum Setup der Splunk-Integration ausführen, müssen Sie einen Integrationsanwender mit den Rollen sn_si.integration_user und sn_si.Analyst in Ihrer ServiceNow-Instanz definieren. Um Importe durchzuführen, benötigen Sie außerdem die Rolle „Import_Transformer“, um Lese- und Schreibberechtigungen für die Sicherheitstabellen zu erhalten. Die Rolle sn_si.integration_user muss mit dem Teil „Import_Transformer“ der Rolle definiert werden.

Laden Sie die Anwendung ServiceNow Security Operations herunter

Der erste Schritt beim Einrichten der ServiceNow-to-Splunk-Integration besteht darin, den herunterzuladen ServiceNow Security Operations Anwendung aus Splunkbase.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie Splunkbase.
2. Suchen Sie nach ServiceNow Security Operations-Integration .
3. Laden Sie die Anwendung herunter.

Installieren Sie das ServiceNow Security Operations-Add-on für Splunk

Installieren Sie **ServiceNow Security Operations-Add-on für Splunk** Zum Verknüpfen von Splunk mit ServiceNow.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie Splunk.
2. Klicken Sie entweder auf **Apps** Zahnradsymbol, oder **Apps Verwalten** Verknüpfungsmenüelement.
3. Klicken Sie Auf **Installieren Sie die App aus der Datei** .
4. Klicken Sie Auf **Wählen Sie Datei** Wählen Sie sn_sec_OPS.spl aus, und klicken Sie auf **Hochladen** .
5. Starten Sie bei Aufforderung neu Splunk.
   Die ServiceNow Security Operations Das Add-on für Splunk ist installiert und kann eingerichtet werden.

Richten Sie die Instanz ein, in der Incidents oder Ereignisse erstellt werden, oder ändern Sie sie

Zum Einrichten oder Ändern von ServiceNow Instanz, in der neue Security Incidents und Security Events erstellt werden, verwenden Sie die Aktion Setup in der Anwendungsliste.

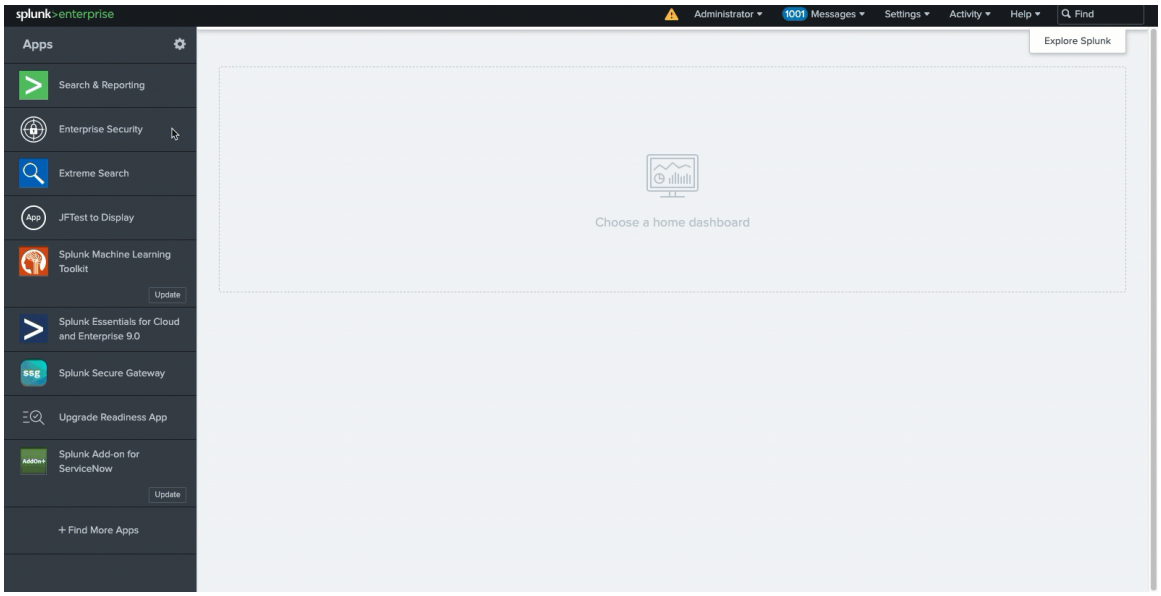
Vorbereitungen
Erforderliche Rolle: sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen **Splunk** .
2. Klicken Sie entweder auf **Apps** Zahnradsymbol, oder **Apps Verwalten** Verknüpfungsmenüelement.
3. Suchen Sie in der Liste der Anwendungen nach **ServiceNow** Apps, die den Filter verwenden.
4. Suchen Sie nach **ServiceNow Security Operations-Integration** , Und klicken Sie auf die entsprechende **Einrichten** Aktion.
5. Füllen Sie im Formular die Felder aus.



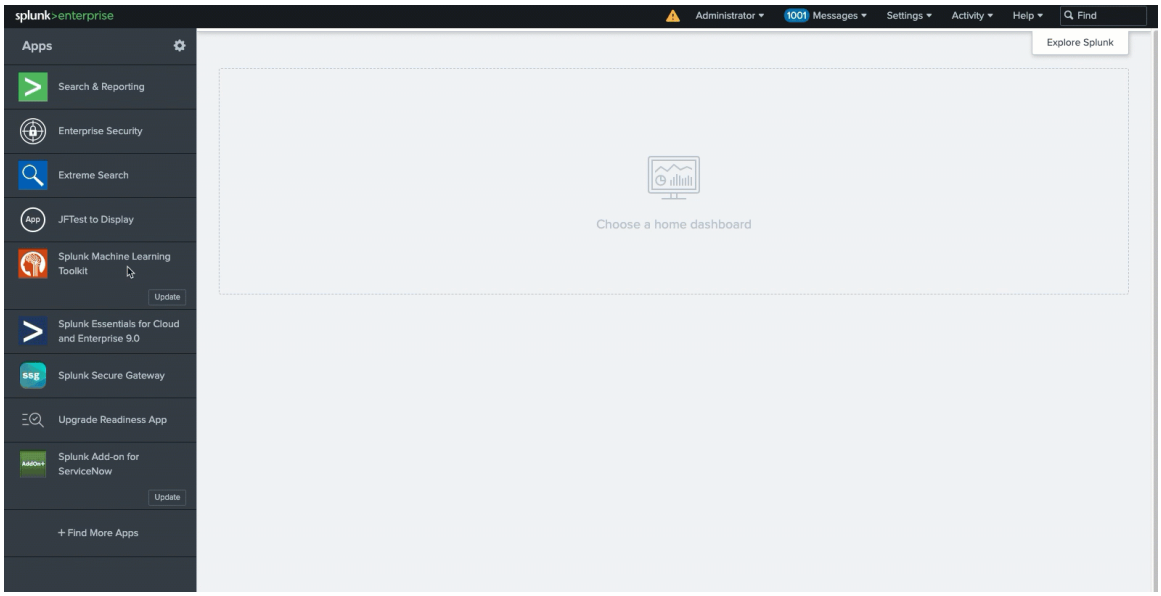
6. Klicken Sie auf **Speichern**.
7. Alternativ suchen Sie nach **ServiceNow-Ereigniserfassungsintegration** , Und klicken Sie auf die entsprechende **Einrichten** Aktion.

   Die ServiceNow-Ereigniserfassungs-Integration ist in drei verschiedene Registerkarten konfiguriert.

   - **Primärer Splunk** : Die Standard- oder primäre Splunk-Konfiguration.
   - **Splunk Sekundär** : (Optional) die Sicherung oder zweite Splunk-Konfiguration.
   - **Protokollierungsebene** : Die Ebene der durch die Integration generierten Berichterstellungsprotokolle, d. h. der Name des Informationstyps.
8. Wählen Sie aus **Primärer Splunk** Registerkarte.
9. Füllen Sie im Formular die Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. **Wahlweise:** Wählen Sie aus **Splunk Sekundär** Registerkarte.
11. **Wahlweise:** Füllen Sie im Formular die Felder aus.
12. Wählen Sie aus **Protokollierungsebene** Registerkarte.
13. Füllen Sie im Formular die Felder aus.
14. Klicken Sie auf **Speichern**.
    Nachdem die Validierung erfolgreich abgeschlossen wurde, wird die Seite „Sicherheitsintegrationen“ mit jeder Ihrer Konfigurationen angezeigt. Auf jeder gültigen Konfigurationskachel **Aktualisieren** Und **Löschen** Schaltflächen werden wie in der folgenden Abbildung angezeigt.

    Hinweis:
    Sie müssen entweder die Standardauthentifizierung oder nur die OAuth 2,0-Authentifizierung verwenden. Aktivieren Sie eine der Authentifizierungen, und geben Sie die entsprechenden Authentifizierungsdetails ein. Wenn Sie beide aktivieren, wird ein Fehler angezeigt.

    Nachdem es erfolgreich validiert und übermittelt wurde, werden alle Ereigniserfassungen durchgeführt Splunk Die Serverkonfiguration wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, klicken Sie in der oberen rechten Ecke der Seite in der Liste Konfigurationen anzeigen auf **Ja** .

Konfigurieren Sie die Anwendungsregistrierung auf der ServiceNow-Instanz

Registrieren Sie die Anwendung bei der Instanz, um die OAuth-Autorisierung zu verwenden.

Vorbereitungen

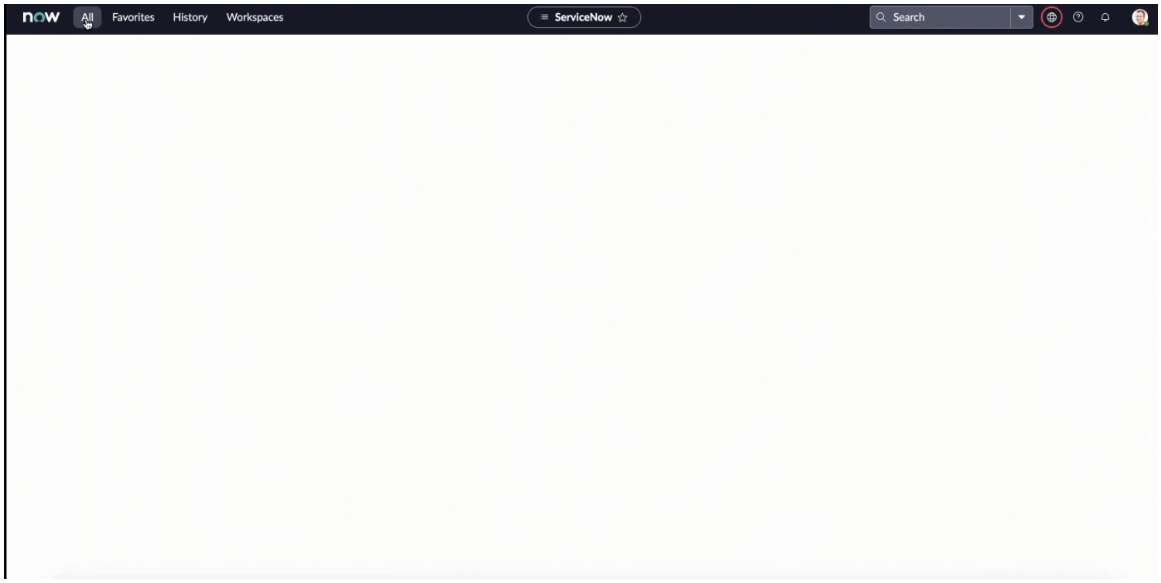
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung**an.
2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie Auf **Erstellen Sie einen OAuth-API-Endpunkt für externe Clients** .
4. Füllen Sie im Formular die Felder aus.



5. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.
6. Klicken Sie auf **Absenden**.

Befehle für manuelle Suche

Manuelle Suchbefehle werden in jedem Suchfenster eingegeben. Sie können einen Security Incident oder ein Security Incident erstellen. Nach dem Befehl werden Paare von Feldnamen und Werten verwendet, um den gewünschten Datensatz zu erstellen.

Sicherheitsereignis

Der Befehl zum Sicherheitsereignis **Snsecevent** , Erstellt ein Ereignis in ServiceNow Mit der Sicherheitsklassifizierung.

Diese Ereignisse können einzeln oder in Warnungsregeln überprüft werden ServiceNow Oder manuelle Aktionen können ein Ereignis oder eine Sammlung von Ereignissen in einen Security Incident verwandeln.

Wenn das Ereignis zu einem Security Incident wird und jeder Parameter in das Ereignis gesendet wird, werden diese Daten verwendet, um den Security Incident wie folgt auszufüllen:

Sicherheitsereignis

Parametername	Erforderlich	Verwenden	In Security Incident verwenden
Knoten	Ja	Der Knoten stellt den Server oder das Konfigurationselement für das Ereignis dar. Idealerweise ist dieser Knoten einem vorhandenen CI in zugeordnet ServiceNow.	In Security Incident verwenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsereignis (Fortsetzung)

Parametername	Erforderlich	Verwenden	In Security Incident verwenden
type	Ja	Die Kategorie des Ereignisses.	Kurzbeschreibung
Ressource	Ja	Das Konfigurationselement.	Kurzbeschreibung
Quelle	Nein	Die Herkunft dieser Daten. Standardmäßig generiert der Splunk-Server die Daten.	Aktivitätsprotokoll
External_url	Nein	Die in zu verwendende Drilldown-URL ServiceNow Um zu den Splunk-Daten zu diesem Ereignis zurückzukehren. Standardmäßig enthält diese URL den Ergebnislink für jede Warnung oder einen Link zur standardmäßigen Splunk-Suchseite.	Externe URL, auf die über zugegriffen wird **Drilldown** Schaltfläche im Security Incident-Formular
time_of_event	Nein	Die Zeit, zu der das Ereignis in Splunk protokolliert wurde.	N/V
Alle anderen Werte (Kategorie, Unterkategorie im Beispiel)	Nein	Jedes Feld, das nicht Teil des Informationsfelds im Ereignis ist. Wenn ein Security Incident erstellt wird, wird er verwendet.	Wenn das Feld vorhanden und nicht ausgefüllt ist, verwendet der Security Incident diesen Wert. Beispielsweise wird die durch das Ereignis übergebene Kategorie zur Kategorie des neuen Security Incident. Wenn kein Feld mit diesem Namen vorhanden ist, wird der Wert im Aktivitätsprotokoll platziert.

Security Incident

Der Befehl „Security Incident“ **SnsecIncident** , Erstellt einen Security Incident in ServiceNow Instanz.

Security Incident

Parameter	Erforderlich	Verwenden
short_description	Ja	Eine kurze, einzeilige Beschreibung des Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident (Fortsetzung)

Parameter	Erforderlich	Verwenden
Kategorie	Nein	Die Kategorie des Security Incidents. Wenn diese Kategorie nicht vorhanden ist, wird sie erstellt.
Unterkategorie	Nein	Die Unterkategorie. Wenn diese Unterkategorie nicht vorhanden ist, wird sie erstellt.
cmdb_ci	Nein	Das Konfigurationselement für den Security Incident. Idealerweise ist dieses Element einem vorhandenen CI in zugeordnet ServiceNow.
Beschreibung	Nein	Die längere, detaillierte Beschreibung des Incident.

Es gibt viele mögliche nützliche Spalten – alles in der Security Incident-Transformationszuordnung kann verwendet werden. Wenn dem Security Incident neue Spalten hinzugefügt werden, werden sie ebenfalls verwendet, solange sie sich in der Transformationszuordnung befinden. Einige nützliche Spalten: Location, Priority, Assignation_Group, assigned_to, affected_user, Attack_Vector und watch_list.

Splunk-Ereignisaktionen

Bei der Überprüfung von Splunk-Protokollen können Sie mithilfe der Ereignisaktionen schnell Sicherheits-Ereignisse und Security Incidents aus jedem Element im Protokoll erstellen.

Wenn Sie auf eine dieser Aktionen klicken, wird ein manueller Suchbefehl erstellt, der mit den Daten im Protokolleintrag gefüllt ist, und führen Sie ihn aus, um den neuen Datensatz zu generieren.

Diese Aktionen können einfach konfiguriert werden, um Ihren normalisierten Daten Felder hinzuzufügen. In Splunk mit **Einstellungen** > **Felder** > **Workflow-Aktionen**, Sie können eine dieser Aktionen mithilfe der manuellen Suchfelder auswählen und bearbeiten.

Sie können auswählen, wo und für welche Felder die Aktion angezeigt wird, und die Suchzeichenfolge ändern, die einen Suchbefehl enthält, um Ihren Datensatz zu erstellen.

Splunk-Warnungen mit einem Datensatz

In jeder Warnung können Sie Sicherheitsereignisse oder Security Incidents angeben, die erstellt werden sollen, wenn die Warnung ausgelöst wird.

Öffnen oder erstellen Sie Ihre Warnung, und wählen Sie beim Bearbeiten von Aktionen den gewünschten Datensatztyp aus, und füllen Sie das Warnungsdialogfeld aus.

Splunk-Warnungen für anwenderdefinierte Felder mit mehreren Datensätzen

Warnungen mit mehreren Datensätzen (definiert mit **Erstellen Sie mehrere ServiceNow Security Incidents** Und **Erstellen Sie mehrere ServiceNow-Sicherheitsereignisse** Auslöseraktionen) kann automatisch Datensätze mit einem beliebigen Satz von unterstützten Feldern erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese verhalten sich anders als die anderen Warnungsaktionen, da Standardwerte angegeben werden. Die meisten Daten stammen jedoch aus dem Suchergebnis für diese Warnung.

Hinweis:
In früheren Versionen des Add-ons und dieser Dokumentation wurden geskriptete Warnungen unterstützt. Diese Funktion wurde veraltet und durch diese Anweisungen ersetzt.

Erstellen Sie eine Splunk-Warnung für ein anwenderdefiniertes Feld mit mehreren Datensätzen

Um eine Splunk-Warnung mit mehreren Datensätzen mit anwenderdefinierten Feldern zu erstellen, müssen Sie eine Suche erstellen, die den ServiceNow-Spalten entspricht, die Sie ausfüllen möchten.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren Sie zu **Suchen** .
2. In **Suchen** Erstellen Sie eine Suche, die Ihre Datensatzdaten generiert.
   Siehe Beispiele Für empfohlene Suchkriterien.
3. Klicken Sie Auf **Speichern Unter** Und wählen Sie aus **Warnung** .
4. Legen Sie den Namen, die Berechtigungen und den Zeitplan nach Bedarf fest.
5. Klicken Sie Auf **Aktionen Hinzufügen** .
6. Treffen Sie eine der folgenden Auswahlmöglichkeiten.
   - Um ein Ereignis pro Ergebnis aus Ihrer Suche zu erstellen, wählen Sie aus **Erstellen Sie mehrere ServiceNow-Sicherheitsereignisse** .
   - Um einen Incident pro Ergebnis aus Ihrer Suche zu erstellen, wählen Sie aus **Erstellen Sie mehrere ServiceNow Security Incidents** .
7. Legen Sie alle Standardwerte nach Bedarf fest.
   Wenn das Feld im Suchergebnis leer ist oder nicht vorhanden ist, werden die Standardwerte verwendet. Wenn das Ergebnis einen Wert enthält, werden die Standardwerte überschrieben.

Splunk-Warnungsbeispiele mit mehreren Datensätzen und anwenderdefinierten Feldern

Wenn Sie Splunk-Warnungen für mehrere Datensätze mit anwenderdefinierten Feldern erstellen, müssen Sie Suchkriterien für die Generierung von Warnungsdaten definieren. Beispiele für Suchkriterien für Security Incidents und Security Events werden angezeigt.

Security Incident-Suche

Für einen Security Incident erstellt dieses Kriterium eine Suche, um Spalten in der Security Incident-Tabelle auszufüllen.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval contact_type="Monitoring" |
eval cmdb_ci=host |
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsereignissuche

Für ein Sicherheitsereignis ist dies dieselbe Suche, aber stattdessen werden Ereignisfelder ausgefüllt. Wenn dieses Ereignis in einen Security Incident umgewandelt wird und alle Felder ausgefüllt werden, die im Ereignis nicht vorhanden sind, werden sie an den Security Incident übertragen. Andernfalls verbleiben sie im Feld „zusätzliche Informationen“ des Ereignisses und der Warnung.

```
host=Development source="/CodeArchive/password/password_decrypt.cpp" |
eval type="Monitoring" |
eval node=host |
eval source=source
eval subcategory="Sensitive Data Monitoring" |
eval description=_raw |
eval source_ip=found_ip
```

Hinweis:
Die von Ihnen verwendeten Suchkriterien fügen so viele Datensätze hinzu, wie in der Suche gefunden werden. Es können 5 oder 10.000.000.000 Datensätze hinzugefügt werden. Daher ist dies keine empfohlene Methode für die Massenübertragung von Daten. Die Absicht dieser Methode besteht darin, der ServiceNow-Instanz pro REST-Aufruf einen Datensatz hinzuzufügen.

Splunk-Fehlerberichterstellung

Immer wenn ein Konnektivitätsproblem mit Ihrer ServiceNow-Instanz auftritt, wird in Splunk ein Fehler mit Informationen zur Beschreibung des Problems protokolliert.

Fehlermeldungen werden in einem neuen Index mit dem Namen gespeichert **servicenow** Mit Quelltyp **servicenow** .

Um nach Fehlerprotokollen zu suchen, stellen Sie sicher, dass Sie angeben **servicenow** Index in Ihrer Suche. Alternativ finden Sie in der aktuellen Splunk-Dokumentation, wie Sie neue hinzufügen **servicenow** Index zu den Standardsuchindizes.

Splunk Enterprise Event Ingestion Integration für Security Operations Bis ServiceNow

Die Splunk Enterprise Integration von Ereignis- und Warnungsdaten mit Security Incident Response(SIR) Mit dem Produkt können Security Incident-Analysten Sicherheitsprotokolle und zugehörige Ereignisdaten erfassen und verarbeiten.

Übersicht

Daten werden in Echtzeit erfasst und von Analysten verwendet, um potenzielle Cyberbedrohungen zu identifizieren und zu melden. Die gesammelten Sicherheitsereignisse können in ausgelöste Warnungen verarbeitet werden, die mit dieser Integration automatisch erfasst werden. Außerdem können einzelne Sicherheitsereignisse bei Bedarf manuell vom weitergeleitet werden Splunk Enterprise Such- und Berichterstellungsschnittstelle in Security Incident Response Produkt von ServiceNow AI Platform Dient zum Erstellen von Security Incidents. Sie können wichtige Ereignisse aus abrufen Splunk Enterprise Suchen Sie mit der Suchkopf-Clusterkonfiguration. Sie können dies erreichen, indem Sie die URL und den API-Port eines beliebigen Suchkopfs verwenden, der Teil des Clusters ist.

Diese Integration bietet einem Analysten des Security Operations Center (SOC) Transparenz für Ereignisse und zugehörige Warnungsdaten. Diese Daten können in integriert werden ServiceNow AI Platform Security Incident Response(SIR) Security Incidents zur weiteren Untersuchung und Korrektur. Profile für Splunk Laufende erfasste Warnungen und weitergeleitete Ereignisse werden in erstellt ServiceNow AI Platform Instanz. Diese Profile passen den Unterschied an Splunk Warnungs- und Ereignisfelder werden in angezeigt SIR

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incidents. Eine Standardzuordnung von Warnungsfeldern wird bereitgestellt, die bearbeitet und erweitert werden kann, um kundenspezifische Anforderungen zu erfüllen.

Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Erstellen Sie mehrere Warnungserfassungsprofile, um SIR Security Incidents für bestimmte Arten von Bedrohungen wie Phishing und Malware zu erstellen.
- Erstellen Sie mehrere Ereignisprofile für die Ereignisweiterleitung bei Bedarf von Ihrem Splunk Konsole zum Erstellen von SIR Security Incidents.
- Drag-and-Drop-Zuordnung von Splunk Warnungs- und Ereignisfeldwerte zu zugehörigen SIR Security Incident-Feldern.
- Eine Vorschau von SIR Security Incident-Layout basierend auf Beispielwarnungen oder -Ereignissen zur Validierung der Profilkonfiguration.
- Erfassen Sie historische Warnungen sowie laufende, zukünftige Warnungen in konfigurierbaren Intervallen.
- Ereignisse oder Warnungen in vorhandenen aggregieren SIR Security Incidents basierend auf übereinstimmenden Feldwerten, um doppelte Security Incidents zu vermeiden.

Unterstützt ServiceNow AI Platform Versionen

Das Plugin „com.snc.si_dep“ ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Anwendungen.

Folgendes Security Operations Anwendungen müssen über installiert und aktiviert werden ServiceNow Store. Installieren und aktivieren Sie jeweils eine Anwendung in der unten aufgeführten Reihenfolge, um eine reibungslose Installation sicherzustellen:

1. Sicherheits-Integrations-Framework
2. Security Support Common
3. Orchestration Des Sicherheitssupports
4. Security Incident Response

Weitere Informationen zur Installation von finden Sie Security Operations Kernanwendungen, siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

ServiceNow Zusätze

Die ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Ist nur erforderlich, wenn Sie Ereignisse manuell von Ihrem weiterleiten möchten Splunk Enterprise-Konsole in Ihrem ServiceNow AI Platform Instanz. Dies ServiceNow Add-on ist in verfügbar Splunkbase .

Dies ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Anwendung in splunkbase ist für die automatisierte Warnungserfassung, die von der Integration unterstützt wird, nicht erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Splunk unterstützte Versionen

Diese Integration unterstützt Version 6,0 oder höher von Splunk Enterprise. Die -Integration unterstützt auch Splunk Enterprise-Cloud-Service.

MID-Server

Diese Integration erfordert einen installierten und konfigurierten MID-Server in Ihrem ServiceNow AI Platform® Instanz, die mit verbunden werden soll Splunk Service, wenn Splunk Server wird in Ihrem Unternehmensnetzwerk bereitgestellt. Wenn Sie verwenden Splunk Cloud Service, ein MID-Server ist nicht erforderlich. Weitere Informationen zu MID-Servern finden Sie unter MID-Server .

Integrationsarchitektur und Systemverbindung

Weitere Informationen zur Architektur der Integration, einschließlich Schlüsselbegriffen und Verbindungsdetails zu externen Systemen, finden Sie unter Integrationsarchitektur und Verbindung mit externen Systemen für Splunk Enterprise Event Ingestion Integration.

Prüfliste

Eine druckbare Prüfliste dieser Themen finden Sie unter Prüfliste für Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung. Sie können diese Liste verwenden, um Ihren Fortschritt bei der Bearbeitung der Aufgaben der Integration zu überwachen.

Die in den folgenden Themen verwendeten Images wurden für das Kingston-Release von generiert ServiceNow AI Platform. Informationen zur San Diego-Anwenderoberfläche finden Sie unter Verwalten Sie Sicherheitsbedrohungen mit dem Sicherheitsanalysten-Arbeitsbereich .

Die folgenden Themen sind nummeriert. Befolgen Sie die unten aufgeführten Themen in der Reihenfolge, in der sie angezeigt werden, um eine reibungslose Installation und Konfiguration der Anwendung zu gewährleisten.

Richten Sie Ihr ein ServiceNow AI Platform® Instanz für Splunk Enterprise Event Ingestion Integration

Im folgenden Abschnitt werden die Setup-Aufgaben aufgeführt, die Sie in ausführen müssen ServiceNow AI Platform® Instanz vor der Installation der Anwendung über ServiceNow Store.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Überprüfen Sie anhand der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

Prozedur

1. Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform® Und Security Incident Response-Rollen (SIR).

   Die folgenden Rollen sind für die Installation, das Setup und die Verwendung der Integration in erforderlich ServiceNow AI Platform® Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Anwender mit ServiceNow AI Platform® Die Administratorrolle (admin) installiert die Anwendung aus dem ServiceNow Store Und weist die Rolle Security Incident-Administrator (sn_si.admin) zu.
- Wenn Sie Ereignisse manuell von weiterleiten möchten Splunk Enterprise Für diese Integration ein Anwender mit ServiceNow AI Platform® Die administratorrolle weist einem Anwender die Rolle (sn_sec_splunk_v2.api_Account_Access) in zu ServiceNow AI Platform®. Diese Rolle ermöglicht einem Anwender die Verwendung von Splunk Enterprise Administratorrolle für den Zugriff auf die API in ServiceNow AI Platform® Dies ist für die manuelle Ereignisweiterleitung für diese Integration erforderlich.

  Die Rolle (sn_sec_splunk_v2.api_Account_Access) ist für die Integration nicht erforderlich, wenn Sie Warnungen automatisch von erfassen Splunk Enterprise In Ihren ServiceNow AI Platform® Instanz.

- Ein Anwender mit **sn_si.ingestion_profile_admin** Die Rolle überwacht die folgenden Aufgaben in ServiceNow AI Platform®:
  - Benennt, erstellt und bearbeitet Warnungs- und Ereignisprofile.
  - Wählt Werte aus Warnungen und Ereignissen aus und ordnet sie zu ServiceNow AI Platform® Security Incidents.
  - Zeigt vor dem Abschluss der Konfiguration eine Vorschau der Security Incident-Details auf Richtigkeit an.
  - Plant die laufende Warnungserfassung.
  - Weist die Rolle Security Incident Analyst (sn_si.Analyst) zu.
  - Anwender mit sn_si.Analyst arbeiten mit Security Incidents.

Weitere Informationen zu Rollen und dem Zuweisen von Rollen an Anwender finden Sie unter Managing roles .

2. Stellen Sie sicher, dass Sie Version 6,0 oder höher von verwenden Splunk API.

   Wenn Sie Zugriff auf haben Splunk Enterprise Konsole haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein anderes spezielles Setup erforderlich.

3. Überprüfen Sie, ob Sie einen MID-Server installiert und konfiguriert haben.

   Ein MID-Server in Ihrem ServiceNow AI Platform® Instanz ist erforderlich, um eine Verbindung mit herzustellen Splunk Service, wenn Splunk Server wird in Ihrem Unternehmensnetzwerk bereitgestellt. Weitere Informationen zu MID-Servern finden Sie unter MID-Server

   Wenn Sie verwenden Splunk Cloud Service, ein MID-Server ist nicht erforderlich.

4. Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert.

   Die Security Incident Response Abhängigkeits-Plugin (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Für die Integration erforderliche Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen.

a. Security Incident Response

b. Sicherheits-Integrations-Framework

c. Security Support Common

d. Orchestration Des Sicherheitssupports

Weitere Informationen zur Installation von finden Sie Security Operations Kernanwendungen, siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

Nächste Maßnahme

Sie haben erfolgreich eingerichtet ServiceNow AI Platform® Instanz für die Integration. Der nächste Schritt besteht in der Installation von Splunk Enterprise Event Ingestion Anwendung aus dem ServiceNow Store Für die Integration. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie ServiceNow Anwendung für Splunk Enterprise Event Ingestion Integration.

Wenn Sie keine Suchvorgänge in gespeichert haben Splunk Enterprise Konsole für Erfassung oder wenn Sie das erste Setup für diese Integration in durchführen Splunk Enterprise Konsole und Security Operations Produkt von ServiceNow AI Platform® Instanz gleichzeitig, siehe Speichern Sie Suchvorgänge in Splunk Enterprise-Konsole für Splunk Enterprise Event Ingestion Integration Weitere Informationen finden Sie unter .

Wenn Sie Ereignisse manuell und bei Bedarf aus exportieren möchten Splunk Enterprise Konsole für die Integration finden Sie unter Richten Sie Ihr ein Splunk Umgebung für die manuelle Ereigniserfassung für Splunk Enterprise Integration der Ereigniserfassung Weitere Informationen finden Sie unter .

Installieren und konfigurieren Sie ServiceNow Anwendung für Splunk Enterprise Event Ingestion Integration

Bevor Sie die Integration für ausführen ServiceNow AI Platform® Führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in integriert wird Security Incident Response Und Security Operations Produkte auf Ihrem ServiceNow AI Platform® Instanz.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

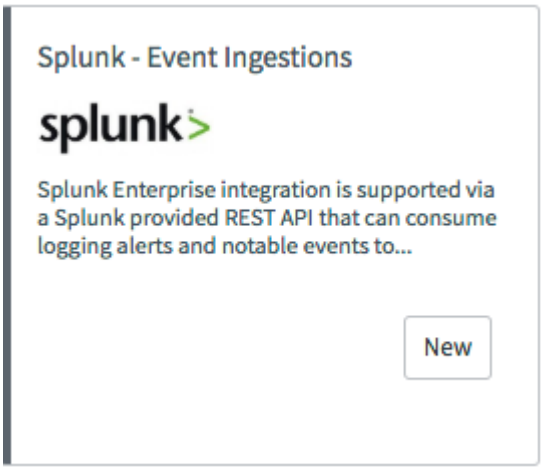
Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Wenn Sie den nicht installiert haben Splunk Enterprise Event Ingestion Anwendung aus dem ServiceNow Store Informationen zur Integration finden Sie unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie Splunk Kachel „Ereigniserfassungen“.

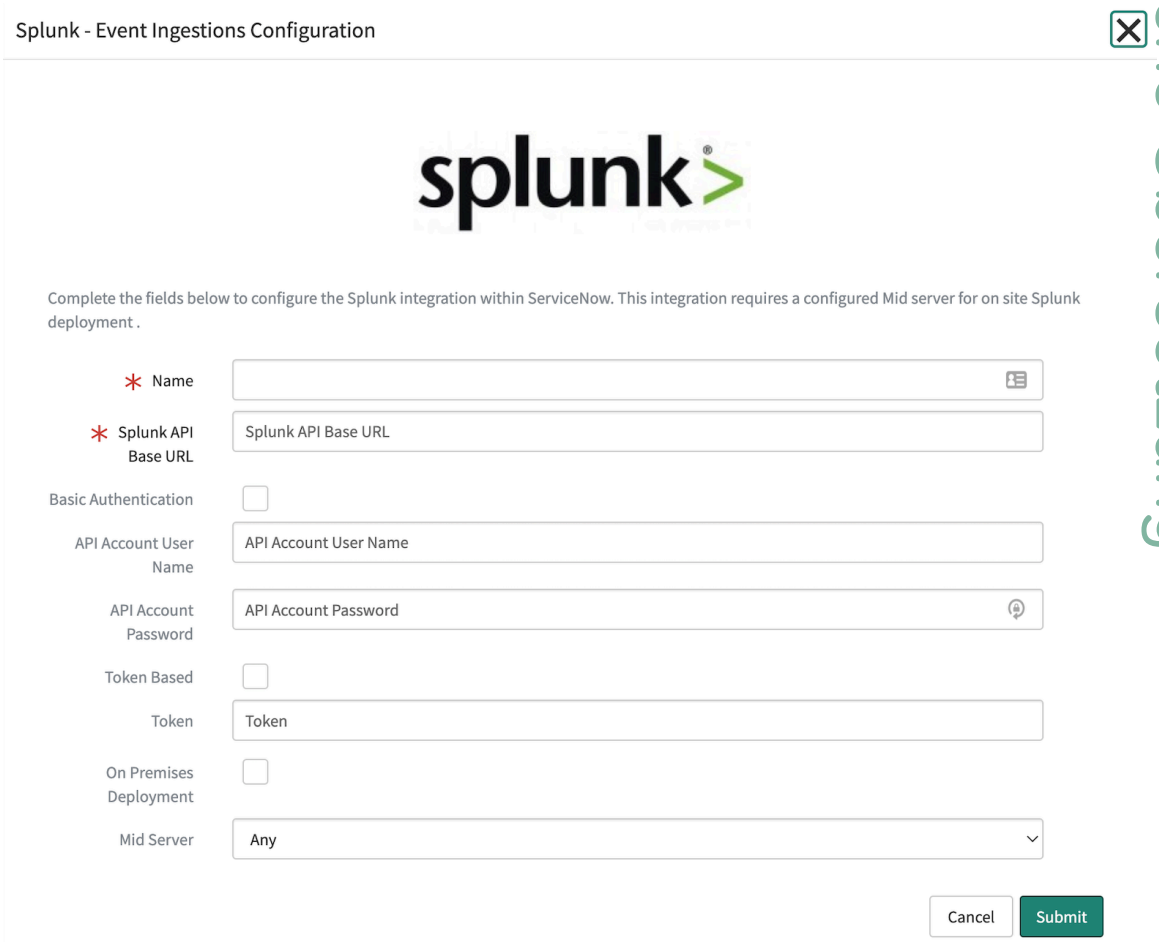
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf , um die Anwendung zu konfigurieren **Neu** .



4. Alternativ, wenn ein **Konfigurieren** Die Schaltfläche wird auf einer Kachel angezeigt. Klicken Sie darauf, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie die Felder im angezeigten Dialogfeld „Konfiguration der Ereigniserfassungen“ aus.

   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für eine Konfiguration einer lokalen Version von Splunk Enterprise Mit einem MID-Server.



Automatische Übersetzung

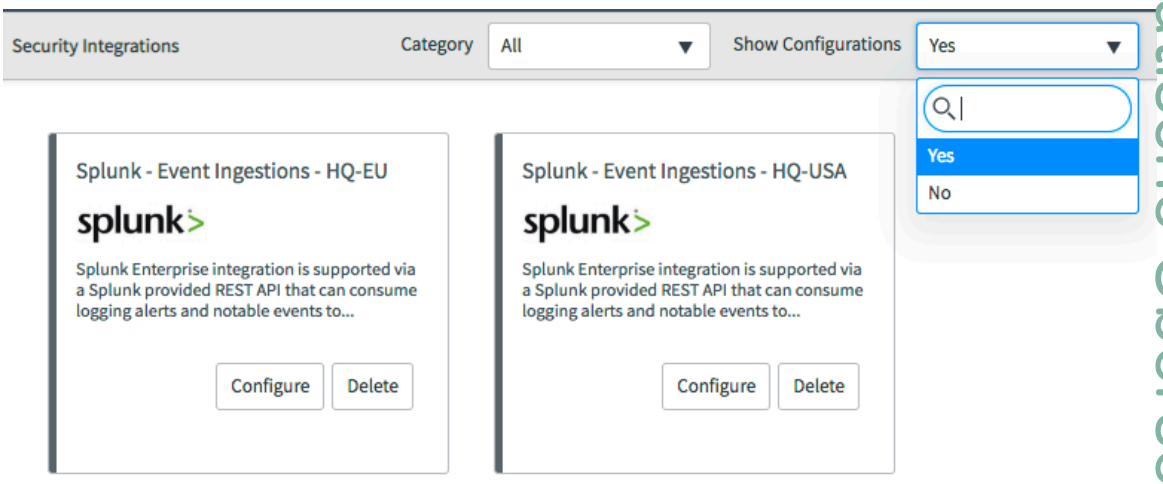
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jeweils Splunk Enterprise Warnung, die Sie von erfassen Splunk Enterprise Die -Konsole erfordert ein eindeutiges Ereignisprofil in Ihrem ServiceNow AI Platform® Instanz. Die Quelle, die Sie im Formular „Konfiguration der Ereigniserfassungen“ konfigurieren, kann jedoch für mehrere wiederverwendet werden ServiceNow AI Platform® Profile, solange jedes Profil eindeutig erfasst wird Splunk Ausgelöste Warnungen.

6. Klicken Sie auf **Absenden**.
   Nachdem die Validierung erfolgreich abgeschlossen wurde, wird die Seite „Sicherheitsintegrationen“ mit jeder Ihrer Konfigurationen angezeigt. Auf jeder gültigen Konfigurationskachel **Konfigurieren** Und **Löschen** Schaltflächen werden wie in der folgenden Abbildung angezeigt.

   Hinweis:
   Sie müssen entweder nur die Standardauthentifizierung oder die tokenbasierte Authentifizierung verwenden. Aktivieren Sie eine der Authentifizierungen, und geben Sie die entsprechenden Authentifizierungsdetails ein. Wenn Sie beide aktivieren, wird ein Fehler angezeigt.

   Nachdem es erfolgreich validiert und übermittelt wurde, werden alle Ereigniserfassungen durchgeführt Splunk Die Serverkonfiguration wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, klicken Sie oben rechts auf der Seite in der Auswahlliste Konfigurationen anzeigen auf **Ja**.



Trouble?

Wenn eine Fehlermeldung angezeigt wird, nachdem Sie auf geklickt haben **Übermitteln** Geben Sie Ihre Informationen erneut ein, und klicken Sie auf **Übermitteln**.

Nächste Maßnahme

Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht darin, ein Ereignisprofil zu erstellen.

Konfigurieren Sie die Einstellungen für die Splunk Enterprise-Ereigniserfassung

Verwenden Sie die Einstellungen für die Splunk Enterprise-Ereigniserfassung, um die voreingestellten Konfigurationen und ihre Werte gemäß Ihren Anforderungen zu ändern.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Navigieren zu **Alle** > **Splunk Integration** > **Einstellungen von Splunk Integration**an.
2. Füllen Sie die Felder im Formular aus.

Einstellungen von Splunk Integration

Feld	Beschreibung
Maximale Anzahl von Warnungen, die bei der Profilerstellung angezeigt werden sollen. sn_sec_splunk_v2.max_Alerts_to_Display	Option zum Definieren der maximalen Anzahl von Warnungen, die Sie beim Erstellen eines Ereignisprofils anzeigen möchten. Standardmäßig ist der Wert auf 500 festgelegt.
Maximale Anzahl von Security Incidents, die an einem Tag erstellt werden sollen. sn_sec_splunk_v2.max_si_per_day	Option zum Definieren der maximalen Anzahl von Security Incidents, die an einem Tag erstellt werden können. Standardmäßig ist der Wert auf 1000 festgelegt.
Maximale Anzahl von Ereignissen, die pro Aufruf aus Splunk abgerufen werden sollen. sn_sec_splunk_v2.max_Events_per_call	Option zum Definieren der maximalen Anzahl von Ereignissen, die für jeden Anruf aus Splunk abgerufen werden sollen. Standardmäßig ist der Wert auf 100 festgelegt.
Die Anzahl der Tage, die ein Element in der Warteschlangentabelle verbleibt, nachdem es zu Informations- oder Debugging-Zwecken abgeschlossen/fehler gemacht hat. sn_sec_splunk_v2.Queue_item_expire	Option zum Definieren der Anzahl der Tage, die ein Element nach Abschluss oder Auftreten eines Fehlers aufgrund von Informationen oder Debugging-Zwecken in der Warteschlangentabelle verbleiben soll. Standardmäßig ist der Wert auf 14 festgelegt.
Anzahl der Tage, um den Ereignisimport, das Ereignis in die Aufgabe und die Daten der ausgelösten Warnungen beizubehalten. sn_sec_splunk_v2.Retention_period	Option zum Bestimmen der Anzahl der Tage, die Sie den Ereignisimport, das Ereignis zu Aufgabe und die Daten ausgelöster Warnungen beibehalten möchten. Standardmäßig ist der Wert auf 30 festgelegt.
Aktivieren Sie diese Einstellung, um vorhandene Splunk-Quellkonfigurationen für die Unterstützung der tokenbasierten Authentifizierung zu aktualisieren. Sie müssen	Option zum Aktualisieren der vorhandenen Splunk-Quellkonfiguration auf die tokenbasierte Authentifizierungsunterstützung von einer vorhandenen Version.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
die Integrationskonfiguration mit Tokendetails aktualisieren, sobald diese Einstellung aktiviert ist. sn_sec_splunk_v2.Upgrade_existing_TIle	**Hinweis:** Nach dem Upgrade auf die neue Version ist das Token-Feld nicht mehr verfügbar. Sie müssen diese Einstellung aktivieren, um die tokenbasierte Authentifizierung abzurufen. Danach müssen Sie die Integrationskonfiguration mit Tokendetails aktualisieren. Standardmäßig ist der Wert auf Nein festgelegt
Protokollierungsebene: Debuggen, Info, Warnung, Fehler. sn_sec_splunk_v2.Logging.verbosity	
Gültigkeitsdauer der Splunk-Suche in Sekunden. sn_sec_splunk_v2.sid_ttl	Standardmäßig ist der Wert auf 14 festgelegt.
Anzahl der Minuten, die beim Abrufen der Ereignisse aus Splunk hinzugefügt werden sollen (um die Indexierungsverzögerung von Splunk zu überwinden). sn_sec_splunk_v2.overlap_time	Standardmäßig ist der Wert auf 0 festgelegt.
Batchgröße der Warnungsregel, die zum Auslösen von Splunk-Suchabfragen während der Erfassung verwendet werden soll. sn_sec_splunk_v2.rules_batch_size	Standardmäßig ist der Wert auf 50 festgelegt.
Ereignisgrenzwert pro ausgelöster Warnung zur Behandlung von Spitzen. sn_sec_splunk_v2.Spike_Events_limit	Standardmäßig ist der Wert auf 1000 festgelegt.
Das Trennzeichen zum Aufteilen der Werte in Feldzuordnungen. sn_sec_splunk_v2.delimiter	

3. Wählen Sie **Speichern**.

Erstellen und benennen Sie ein Ereignisprofil

Erstellen Sie ein Ereignisprofil in Ihrem ServiceNow AI Platform Instanz und bestimmen, welche Splunk Warnungen erstellen Security Incidents.

Vorbereitungen
Erforderliche Rolle: sn_si.ingestion_profile_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Vor ServiceNow AI Platform Security Incident Response(SIR) Security Incidents werden aus erfassten Warnungen erstellt, die Feldwerte aus Warnungen werden in einem Layout von angezeigt ServiceNow AI Platform Security Incident, damit Sie eine Vorschau darauf anzeigen können, wie der tatsächliche Security Incident angezeigt wird.

Aus Integrationsperspektive mithilfe verfügbarer APIs: Splunk Ereignisse werden einzeln und manuell als diskrete Ereignisse weitergeleitet oder zu ausgelösten Warnungen kombiniert, die automatisch in erfasst werden Security Operations Umgebung von ServiceNow AI Platform Instanz. Die Integrations-Workflows erfassen verschiedene Arten von Warnungen, z. B. nicht autorisierte Zugriffsversuche und Malware.

Diese Warnungen werden basierend auf den Profilen erfasst, die Sie in konfigurieren Security Operations Umgebung Ihrer Instanz. Alle Warnungen werden anfänglich für einen konfigurierten Warnungstyp in einem Profil erfasst. Erfasste Warnungen können dann weiter gefiltert werden, um anzugeben, welche Warnungen Security Incidents erstellen. Sie können beispielsweise Filter bevorzugen, die Security Incidents nur für Warnungen erstellen, die als hohes Risiko identifiziert werden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten Warnungen erstellt, werden einzelne Feldwerte in den gefilterten Warnungen den entsprechenden Feldern in einem Layout von Security Incidents zugeordnet, um eine Vorschau anzuzeigen.

Warnungsnamen für Ereignisprofile in Ihrem ServiceNow AI Platform Die Instanz muss eindeutig sein und kann jeweils nur einem aktiven Ereignisprofil zugeordnet werden. Dies sind die Namen der ausgelösten Warnungen, die Sie in konfiguriert haben Splunk Service als Teil des Setups für die Integration. Weitere Informationen zum Konfigurieren von Warnungen in finden Sie in Splunk Enterprise Umgebung, siehe Speichern Sie Suchvorgänge in Splunk Enterprise-Konsole für Splunk Enterprise Event Ingestion Integration.

Die ServiceNow AI Platform Erfasst bestimmte Warnungen mithilfe der Workflows der Integration. Alle Warnungen, die die Auswahlkriterien in erfüllen Splunk enterprise-Konsole wird anfänglich in erfasst ServiceNow AI Platform Instanz.

Ein Profil in Ihrem ServiceNow AI Platform Ist eine Kapselung von Splunk Warnung in Ihrem Splunk enterprise-Konsole. Es besteht eine 1-zu-1-Beziehung zwischen Warnungen, die mit einem Profil erfasst werden, und Verbindungen mit Ihrem Splunk enterprise-Konsole: Eine Warnung für eine Verbindung. Es gibt eine einzelne HTTP-Verbindung zu einem Suchkopf in Ihrem Splunk Enterprise Konsole. Mehrere Warnungen können von einem einzigen Suchkopf stammen. Wenn Sie eine Verbindung zu mehreren Suchköpfen in herstellen Splunk Enterprise-Konsole müssen Sie mehrere Profile in erstellen ServiceNow AI Platform Instanz zum Erfassen dieser Warnungen.

Schritte zum Erstellen von Profilen für die geplante Warnungserfassung

Prozedur

1. Um ein Ereignisprofil für eine Warnung zu erstellen, in ServiceNow AI Platform Instanz, navigieren Sie zu **Splunk ES-Integration** > **Splunk ES-Ereignisprofile**an.
2. Wenn Splunk Formular „Ereignisprofil“ wird nicht angezeigt. Klicken Sie auf **Name** In der Fortschrittsleiste.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

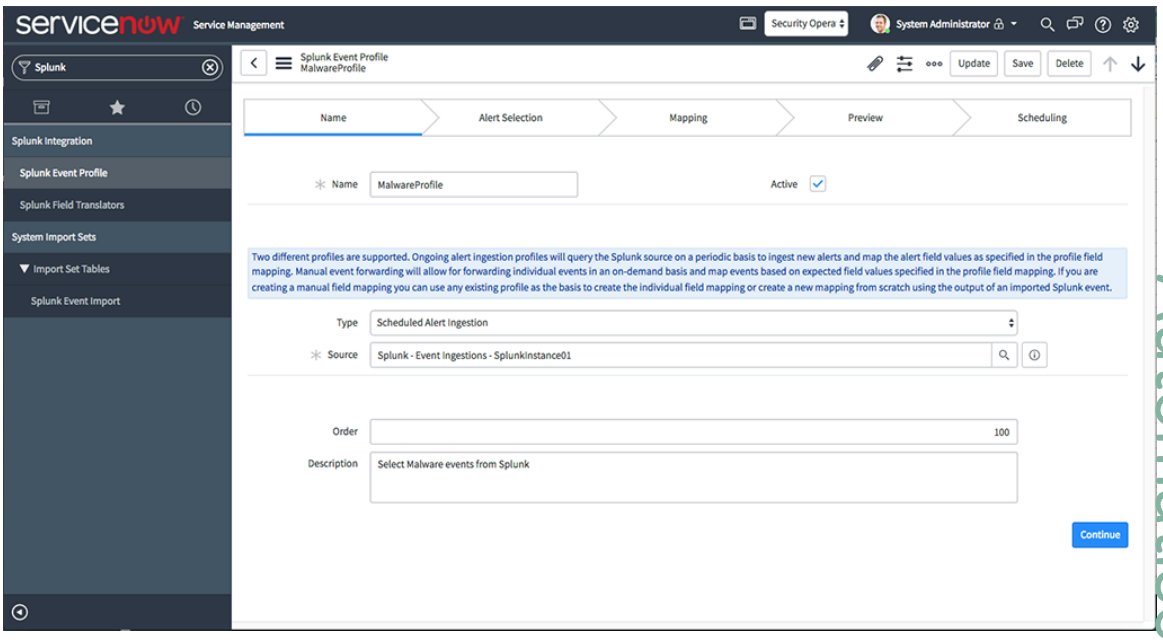
Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

Feld	Beschreibung
Name	Eindeutiger Name für das Profil. Wenn Namen nicht eindeutig sind, werden keine doppelten Profilnamen gespeichert. Profilnamen in Ihrem ServiceNow AI Platform Instanz muss eindeutig sein.
Aktiv	Das Kontrollkästchen ist standardmäßig deaktiviert. Die Option aktiv ist deaktiviert und kann erst ausgewählt werden, wenn Sie alle Konfigurationsschritte des Profils abgeschlossen haben und auf klicken **Beenden** .
Typ	Wählen Sie den Profiltyp aus der Auswahlliste aus. ○ Geplante Warnungserfassung: Dieser Profiltyp unterstützt ausgelöste Warnungen, die nach einem von Ihnen konfigurierten Zeitplan erfasst werden. Füllen Sie die Felder aus, und klicken Sie auf **Fahren Sie Fort** Um mit dem Schritt „Warnungsauswahl“ des Profils fortzufahren. ○ Manuelle Ereignisweiterleitung: Dieser Profiltyp unterstützt einzelne Ereignisse, die manuell von Ihrem weitergeleitet werden Splunk Enterprise Konsole bei Bedarf. Lesen Sie die folgenden Schritte, um das Formular für diese Profiltypen auszufüllen.
Quelltyp	Splunk Server- oder Suchende, die Sie zum Erfassen von Warnungen konfiguriert haben. Wenn Sie mehrere haben Splunk Server konfiguriert, wählen Sie den entsprechenden Server für die Warnungstypen aus, die Sie für das Profil erfassen möchten. Sie müssen einen Wert eingeben.
Reihenfolge	Der Standardwert ist 100. Belassen Sie diese Einstellung auf den Standardwert. Wenn Sie mehrere Profile erstellt haben, gibt dieser Wert eine Laufzeitausführungspriorität an, wenn zwei oder mehr Profile dieselben Auslösebedingungen haben. Der Workflow im Profil mit der niedrigsten Zahl hat die höchste Priorität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
(Optional) Beschreibung	Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für eine geplante Warnung.



5. Wählen Sie für ein Profil mit einer geplanten Warnung eine Option aus, um mit der Profilkonfiguration fortzufahren.
   Schritte zum Erstellen von Profilen für die manuelle Ereignisweiterleitung
6. Führen Sie die folgenden Schritte aus, um ein Profil zu erstellen, das die manuelle Ereignisweiterleitung unterstützt.

   Für Ereignisse, die Sie bei Bedarf von Ihrem weiterleiten Splunk enterprise-Konsole können Sie die individuelle Feldzuordnung auf einem beliebigen vorhandenen Profil basieren. Alternativ können Sie ein neues Zuordnungsraster für exportierte Anhangsdaten erstellen. Ereignisse, die Sie manuell weiterleiten, sind im Ereignisprofil nicht geplant.

   a. Wenn nicht bereits ausgewählt, wählen Sie in der Auswahlliste für das Feld Typ die Option aus **Manuelle Ereignisweiterleitung** .

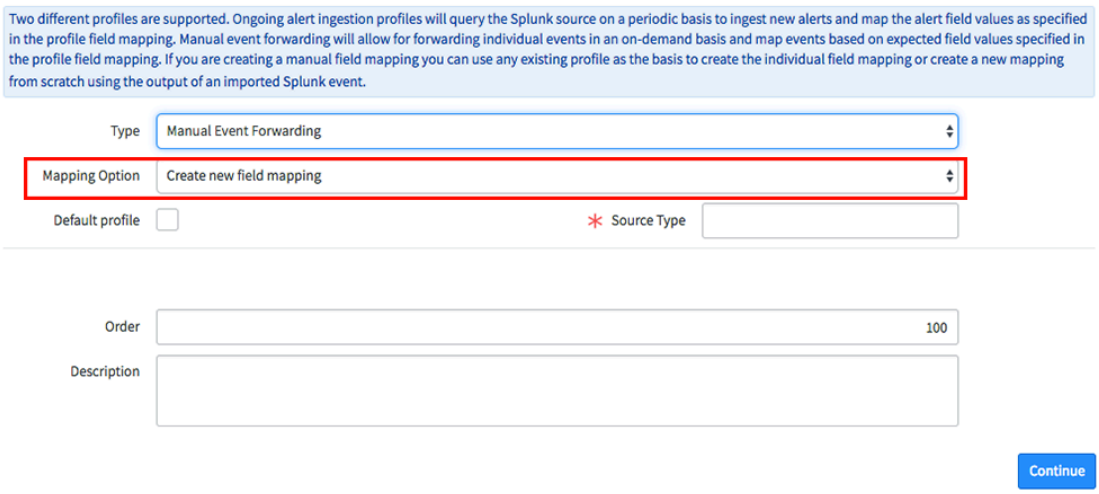
   b. Wählen Sie im angezeigten Feld Zuordnungsoption aus der Auswahlliste eine Zuordnungsoption aus, um fortzufahren.

      Weitere Informationen zu den verfügbaren Zuordnungsoptionen in der Auswahlliste Zuordnungsoptionen finden Sie in den folgenden Abbildungen und Tabellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine neue Feldzuordnungsoption



Option „neue Feldzuordnung erstellen“

Option oder Feld	Beschreibung
Erstellen Sie eine neue Feldzuordnungsoption	Neue Feldzuordnung für Ihr Ereignis. Wenn Sie keine Feldzuordnung haben, die dem Profil ähnelt, das Sie erstellen, wählen Sie diese Option aus, um eine neue Zuordnung zu erstellen.
Standardprofil	Standardmäßiges Ereignisweiterleitungsprofil für alle Splunk Ereignisse. Standard ist gelöscht (deaktiviert). Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die manuelle Ereignisweiterleitung. Dieses Profil ist das einzige Profil, das für jeden aktiv ist und verwendet wird Splunk Ereignisfeldzuordnung zu SIR Security Incident. Ein Profil passt auf alle weitergeleiteten Ereignisse. Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist.
Quelltyp	Splunk Server. Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist. Falls verfügbar, ermöglicht die Option Quelltyp die Zuordnung eindeutiger

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
	Ereignisfelder zu Security Incident-Feldern basierend auf Splunk Quelltyp. Wenn Sie Firewall-Protokollereignisse anders als Endpunkterkennungsereignisse verwalten möchten und sich unterscheiden Splunk Quelltypen können Sie verschiedene Ereignisprofile basierend auf Quelltypen erstellen, um diese Anforderung zu erfüllen.
Reihenfolge	Der Standardwert ist 100. Belassen Sie diese Einstellung auf den Standardwert. Wenn Sie eine große Anzahl von Profilen erstellt haben, bietet dieser Wert eine Laufzeitausführungspriorität, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam haben. Der Workflow im Profil mit der niedrigsten Zahl hat die höchste Priorität.
(Optional) Beschreibung	Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Überprüfen Sie für ein Profil mit einer neuen Feldzuordnung, ob Sie einen Wert in das Feld Quelltyp eingegeben haben, und klicken Sie auf **Fahren Sie Fort** Um mit dem Zuordnungsschritt der Konfiguration fortzufahren.

Weitere Informationen zu einem Profil mit einer vorhandenen Feldzuordnung finden Sie in der folgenden Abbildung und Tabelle.

Wählen Sie ein vorhandenes Profil für die Feldzuordnungsoption aus

Wählen Sie ein vorhandenes Profil für die Feldzuordnungsoption aus

Option oder Feld	Beschreibung
Vorhandenes Profil für Feldzuordnung auswählen	Eine vorhandene Feldzuordnung für Ihr Ereignis. Das Feld aus Profil kopieren wird angezeigt. Führen Sie die folgenden Schritte aus, um eine vorhandene Feldzuordnung für dieses Profil zu kopieren. **i.** Klicken Sie links neben dem angezeigten Feld aus Profil kopieren auf das Suchsymbol. **ii.** In Splunk Liste der Ereignisprofile, die angezeigt wird, klicken Sie auf den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
	Profilnamen, der die zu kopierende Zuordnung enthält. Der Profilname wird im Feld aus Profil kopieren angezeigt.
Standardprofil	Standardmäßiges Ereignisweiterleitungsprofil für alle Splunk Ereignisse. Standard ist gelöscht (deaktiviert). Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die manuelle Ereignisweiterleitung. Dieses Profil ist das einzige aktive Profil. Wird für jeden verwendet Splunk Ereignisfeldzuordnung zu SIR Security Incident. Ein Profil passt auf alle weitergeleiteten Ereignisse. Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist.
Quelltyp	Splunk Server. Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption ausgewählt ist. Falls verfügbar, ermöglicht die Option Quelltyp die Zuordnung eindeutiger Ereignisfelder zu Security Incident-Feldern basierend auf Splunk Quelltyp. Wenn Sie Firewall-Protokollereignisse anders als Endpunkterkennungsereignisse verwalten möchten und sich unterscheiden Splunk Quelltypen können Sie verschiedene Ereignisprofile basierend auf Quelltypen erstellen, um diese Anforderung zu erfüllen.
Reihenfolge	Der Standardwert ist 100. Belassen Sie diese Einstellung auf den Standardwert. Wenn Sie mehrere Profile erstellt haben, gibt dieser Wert eine Laufzeitausführungspriorität an, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam haben. Der Workflow im Profil mit der niedrigsten Zahl hat die höchste Priorität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
(Optional) Beschreibung	Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Klicken Sie unten im Formular zur Auswahl einer vorhandenen Zuordnung für Ihr Profil auf **Beenden** Um die Profilkonfiguration abzuschließen.

Nächste Maßnahme

Sie haben die Schritte zum Erstellen von Profilen für geplante Warnungen und die manuelle Ereignisweiterleitung erfolgreich abgeschlossen. Für Profile für die manuelle Ereignisweiterleitung haben Sie die Profilkonfiguration abgeschlossen. Der nächste Schritt besteht darin, Anhangsdaten im Zuordnungsschritt zu laden.

Für Profile für geplante Warnungen besteht der nächste Schritt darin, Warnungen für die automatische Erfassung auszuwählen.

Wählen Sie geplante Warnungen für aus Splunk Enterprise Event Ingestion Integration

Nachdem Sie ein Profil für eine geplante Warnung erstellt haben, wählen Sie ein aus Splunk Warnung für dieses Profil, das Sie einem zuordnen möchten ServiceNow AI Platform Security Incident Response Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die verfügbaren Warnungen in Ihrem an ServiceNow AI Platform Instanz, damit Sie wissen, welche Feldwerte für die Zuordnung verfügbar sind. Wählen Sie eine Warnung aus, um sicherzustellen, dass Sie die erwarteten Ergebnisse im Standardformularlayout erhalten, bevor Sie die Werte Feldern in zuordnen SIR Security Incidents. Sie können in diesem Formular nur eine Warnung aus der Liste auswählen.

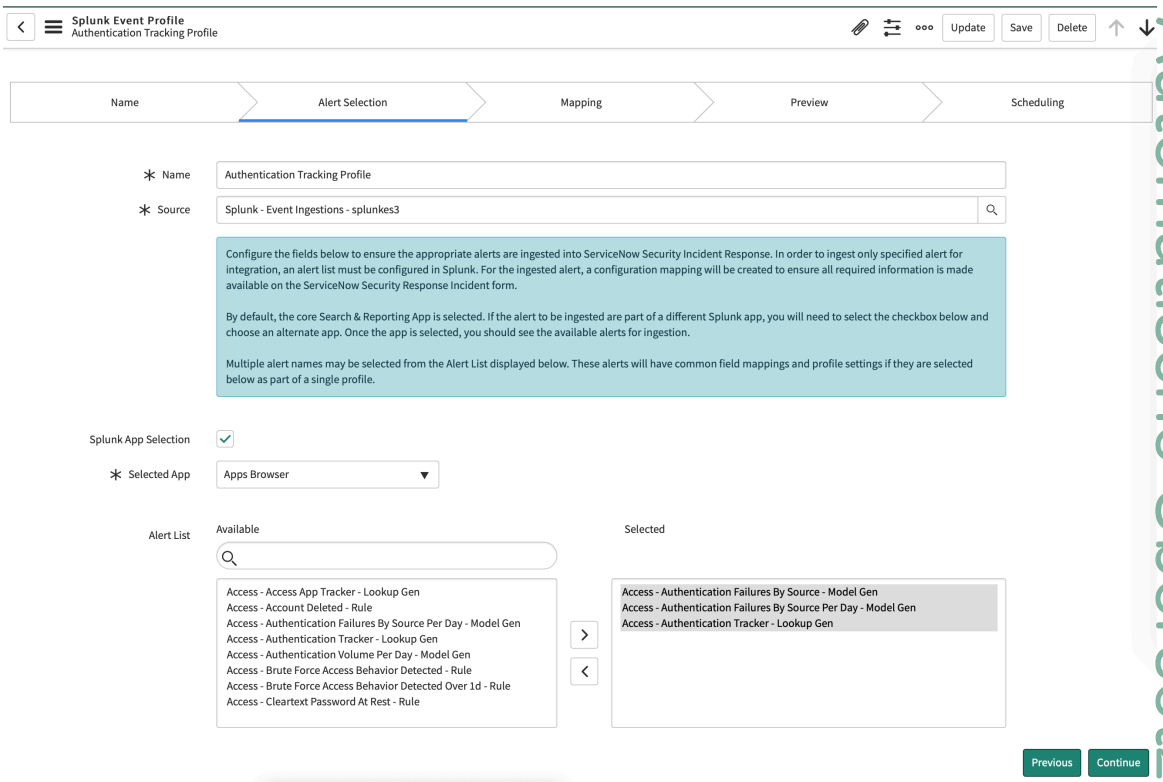
Prozedur

1. Wenn die Seite „Warnungsauswahl“ nicht angezeigt wird, wählen Sie sie in der Fortschrittsleiste aus, um sie anzuzeigen.
   Standardmäßig ist die Core-Such- und Reporting-App ausgewählt.
2. Wenn die zu erfassende Warnung Teil einer anderen ist Splunk App, wählen Sie aus **Splunk-App-Auswahl** Und wählen Sie aus Splunk App aus dem **Ausgewählte App** Liste.
3. Von **Warnungsliste** , Wählen Sie eine Warnung aus, und verschieben Sie sie von zu **Verfügbar** Spalte zu **Ausgewählt** Spalte.
   Sie können auch mehrere Warnungen auswählen. Wenn die Warnungen als Teil eines einzelnen Profils ausgewählt werden, verfügen die Warnungen über allgemeine Feldzuordnungen und Profileinstellungen.

   Die Liste der Warnungen in diesem Formular stimmt mit der Liste der Warnungen in überein Splunk Konsole. In diesem Formular werden bis zu 500 Warnungen angezeigt. Wenn in Ihrer Splunk-Konsole auf der Seite „Warnungen“ mehr als 500 Warnungen aufgeführt sind, werden nur die ersten 500 Warnungen in diesem Formular in angezeigt ServiceNow AI Platform Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Geben Sie im Suchfeld Warnungsliste Text ein.	Die Spalte unter dem Suchfeld wird basierend auf dem von Ihnen eingegebenen Text mit verfügbaren Optionen gefiltert. Wählen Sie eine Warnung aus, und verschieben Sie den ausgewählten Alarm mit den Pfeiltasten aus **Verfügbar** Bis **Ausgewählt** .
Doppelklicken Sie in der Warnungsliste auf eine Warnung.	Die **Ausgewählt** Spalte wird mit Ihrer Auswahl ausgefüllt.
Klicken Sie in der Warnungsliste einmal auf eine Alarmregel.	Der Alarm ist ausgewählt. Verschieben Sie die ausgewählte Warnung mit den Pfeiltasten aus **Verfügbar** Bis **Ausgewählt** .



4. Wählen Sie eine Option aus, um fortzufahren.

Automatische Übersetzung

Nächste Maßnahme

Sie haben erfolgreich eine Warnung für ein geplantes Warnungsprofil ausgewählt. Der nächste Schritt ist die Zuordnung von Warnungswerten zu Feldern in einem Security Incident.

Zuordnung von Warnungen und Ereignissen für Splunk Enterprise Event Ingestion Integration

Nachdem Sie die Quellen für die geplante Warnungserfassung oder die manuelle Ereignisweiterleitung identifiziert haben, werden im nächsten Schritt einzelne Ereignisfelder den Feldern in zugeordnet ServiceNow AI Platform Security Incident Response(SIR) Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

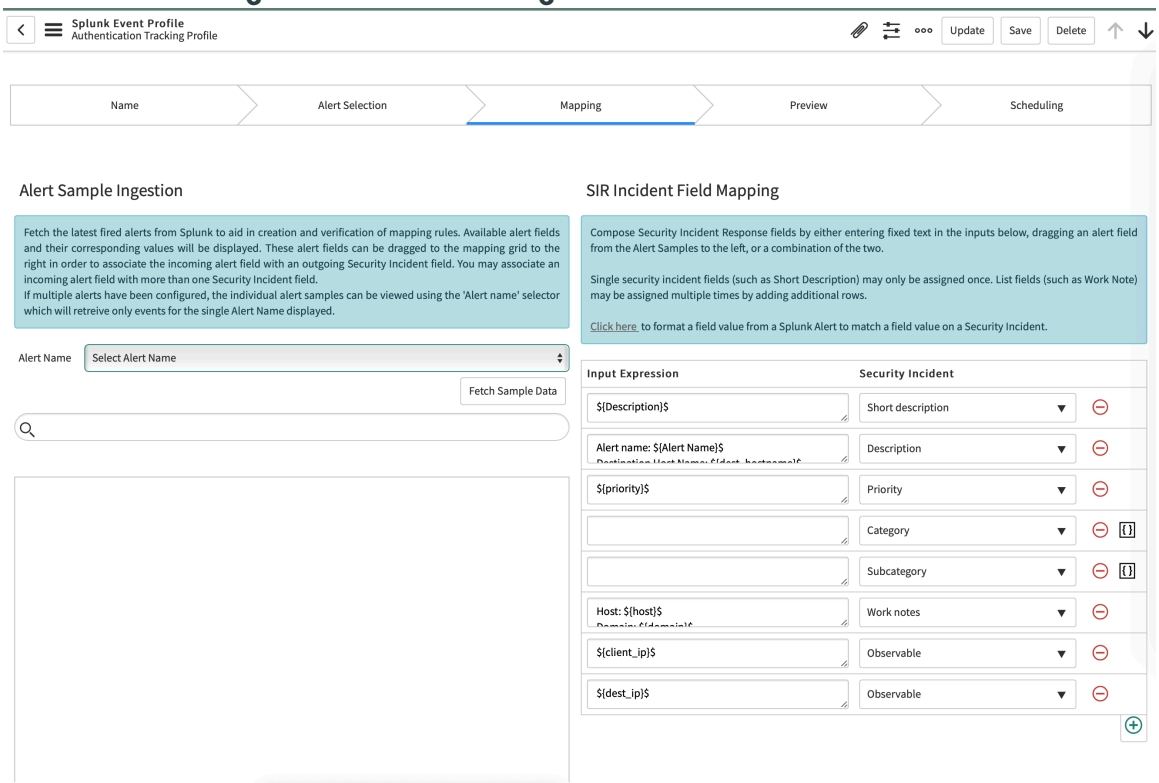
Übersicht über die Zuordnung von Warnungen und Ereignissen

Für den Zuordnungsschritt als Anwender mit **sn_si.ingestion_profile_admin** Rolle, erfassen Sie Beispielwarnungen von Ihrem Splunk Enterprise-Konsole, oder Sie exportieren Ereignisdaten für eine Splunk Enterprise Ereignis.

Die folgenden Abbildungen sind Beispiele für die standardmäßigen Zuordnungsraster, die für jeden Ereignisprofiltyp bereitgestellt werden. Diese Standardzuordnung kann bearbeitet werden. Mit dieser Änderung können Sie die Felder anpassen, die den Security Incident ausfüllen. Mit dem Zuordnungsschritt können Sie visualisieren, wie sich das Hinzufügen oder Entfernen von Ereignisfeldern auf auswirkt SIR Security Incident-Feldwerte.

Wählen Sie aus **Warnungsname** , Und nachdem Sie auf geklickt haben **Rufen Sie Beispieldaten Ab** , Splunk Warnungsfeldwerte werden auf der linken Seite des Formulars ausgefüllt, wenn Beispielwarnungen vom Profil erfasst werden. Dies sind die Splunk Warnungsfelder, die Sie dem zuordnen SIR Security Incident-Felder.

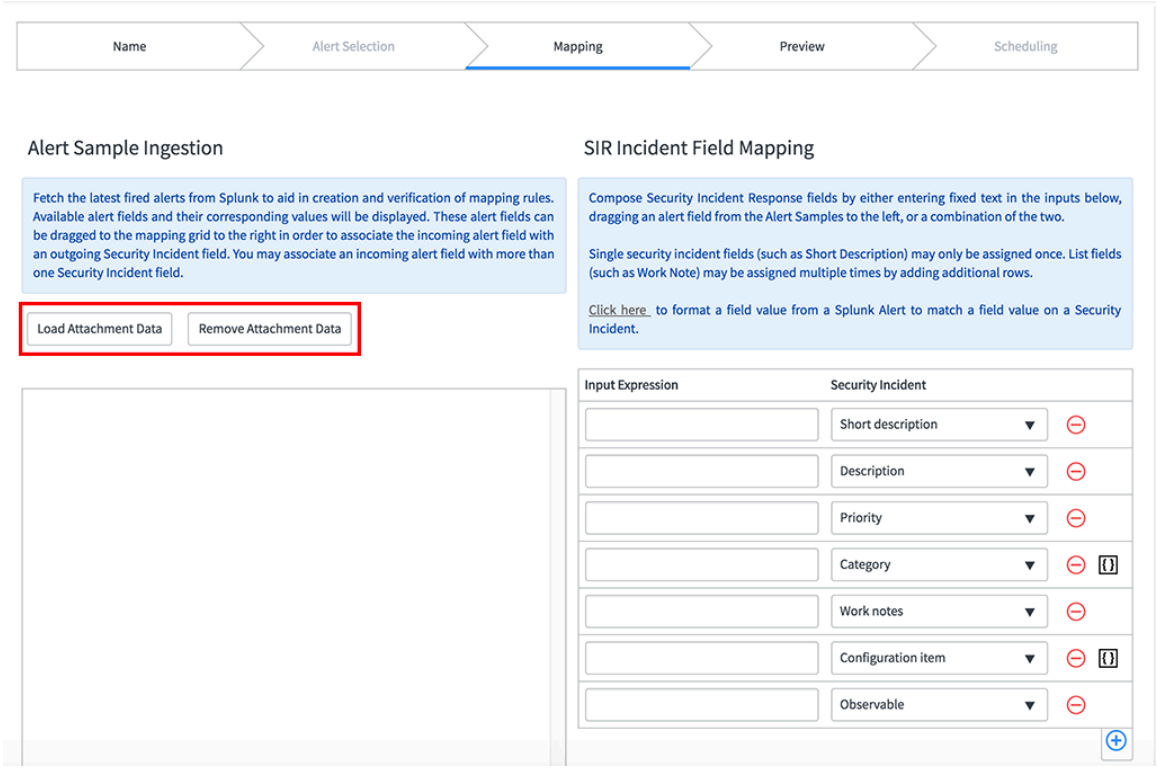
Standardzuordnungsformular für Warnungen



Nachdem Sie zum Laden von Anhangsdaten für weitergeleitete Ereignisse auf geklickt haben Splunk Ereignisfelder werden auf der linken Seite des Formulars ausgefüllt. Dies sind die Splunk Datenfelder, die dem zugeordnet sind SIR Security Incident-Felder.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardzuordnungsformular für weitergeleitete Ereignisse



Möglicherweise möchten Sie einige Beispielwarnungen für überprüfen Splunk Konsole, die für den Konfigurationsschritt der Feldzuordnung erfasst werden soll. Dieser Schritt ist beschriftet, **Zuordnung** Auf der Fortschrittsleiste. Wenn diese Seite nicht angezeigt wird, klicken Sie auf **Zuordnung** Auf der Fortschrittsleiste.

Ordnen Sie Warnungen zu und exportieren Sie Ereignisse bei Bedarf aus Ihrem Splunk Die enterprise-Konsole enthält die folgenden Konzepte und Aufgaben:

- Rufen Sie Beispieldaten für automatisch erfasste Warnungsprofile ab. Nachdem Daten aus einer ausgelösten Warnung auf abgerufen (abgerufen) wurden Splunk Enterprise Konsole, verfügbare Warnungsfelder und die entsprechenden Werte werden in einem Standardzuordnungslayout auf der linken Seite des Zuordnungsformulars angezeigt. Registerkarten werden angezeigt, auf denen Sie die Werte für eine von Ihnen abgerufene Warnungs-ID anzeigen können. Überprüfen Sie, ob alle kritischen Felder aus dem Abschnitt „Warnungsbeispielerfassung“ auf der linken Seite des Formulars dem Raster auf der rechten Seite des Formulars zugeordnet sind.
- Laden Sie bei Bedarf Ereignisbeispieldaten für alle manuell weitergeleiteten Ereignisprofile. Beispieldaten für diese Ereignisse werden in exportiert .Xml Datei aus dem Splunk Enterprise-Konsole und in geladen ServiceNow AI Platform® Instanz. Die importierten Daten werden im Abschnitt „Warnungsbeispielerfassung“ auf der linken Seite des Formulars angezeigt.
- Bearbeiten Sie die Zuordnungskonfiguration, indem Sie Warnungen von der linken Seite ziehen und im Zuordnungsraster auf der rechten Seite ablegen. Das Zuordnungsraster auf der rechten Seite ordnet das Feld „eingehende Warnung“ einem Feld für ausgehende Security Incidents zu.
- Passen Sie das Zuordnungsraster an, indem Sie Felder hinzufügen oder entfernen. Verfolgen Sie übersehene oder duplizierte Felder mit der bereitgestellten Farbcodierung nach.
- Legen Sie Filterbedingungen fest, damit Sie angeben können, welche Warnungen in erfasst werden SIR Anwendung und welche Warnungen herausgefiltert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

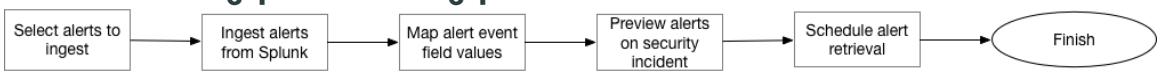
Automatische Übersetzung

- Definieren Sie zusätzliche Incident-Feldkriterien, die eine eingehende Warnung zu einer vorhandenen aggregieren SIR Security Incident, um doppelte Incidents zu verhindern. Diese zusätzliche Filterung kann die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen Security Event-Daten in einem einzelnen Security Incident platziert werden.
- In bestimmten Fällen Ereignisfeldwerte in Splunk Enterprise-Konsole kann nicht direkt in die Felder auf übersetzt werden SIR Security Incident. Für diese Werte können Sie einen Skripteditor verwenden, um Feldwerte für den Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind. Beispiel: Mit dem Skripteditor die Feldwerte Malware-Warnung und Virusinfektion im Splunk Konsole beide in schädliche Code-Aktivität übersetzen im Feld Kategorie auf der SIR Security Incident.

Profile für geplante Warnungen

Nach dem Erstellen eines geplanten Warnungsprofils wird der Prozess-Flow für die Konfiguration in der folgenden Abbildung angezeigt.

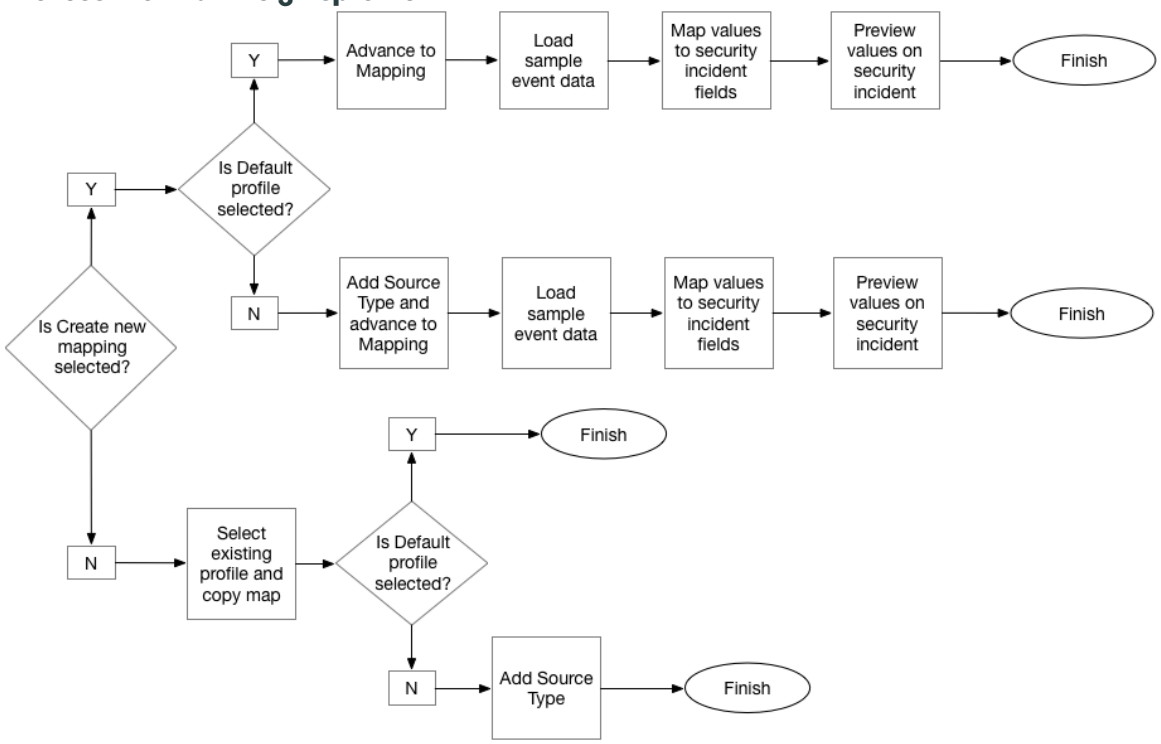
Prozess-Flow für geplante Warnungsprofile



Profile für manuelle Ereignisweiterleitung

Nach dem Erstellen eines Profils für ein Ereignis wird der Prozess-Flow für die Konfiguration in der folgenden Abbildung angezeigt.

Prozess-Flow für Ereignisprofile



Der nächste Schritt besteht darin, ausgelöste Warnungen zu erfassen oder Daten zu exportieren und Werte dem zuzuordnen SIR Security Incident-Felder.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ordnen Sie Warnungen für zu Splunk Enterprise Event Ingestion Integration

Während des Schritts „Ereignisfeldzuordnung“ ordnen Sie einzelne Ereignisfelder aus ausgelösten Warnungen oder importierten Ereignisdaten Feldern auf einem zu ServiceNow AI Platform Security Incident Response(SIR) Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Das vorkonfigurierte Zuordnungsraster der standardmäßigen Security Incident-Felder kann bearbeitet werden. Die Farbcodierung der Ereignisfelder hilft Ihnen, die Feldwerte zu überwachen, die Sie bereits zugeordnet haben. Mit diesem Schritt können Sie visualisieren, wie sich Ihre Änderungen auf die Felder für den Security Incident auswirken.

Ordnen Sie bis zu fünf Warnungen aus der Spalte „Warnungsbeispielerfassung“ auf der linken Seite des Formulars den Security Incident-Feldern in der Spalte „SIR-Incident-Feldzuordnung“ auf der rechten Seite zu.

Erstellen Sie anwenderdefinierte Karten, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie zuordnen Splunk Felder, die nicht im Standardzuordnungsraster auf angezeigt werden SIR Security Incident.

Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie auf **Zuordnung** Auf der Fortschrittsleiste.
2. Wählen Sie für ein Profil mit einer geplanten Warnung unter „Alarmbeispielerfassung“ die Warnung im aus **Warnungsname** Und klicken Sie auf **Rufen Sie Beispieldaten Ab** Zum Abrufen der neuesten Instanz einer ausgelösten Warnung aus dem Splunk Enterprise Konsole.

   Die Warnungen werden als Registerkarten angezeigt. Sie können bis zu fünf der neuesten Warnungen erfassen.

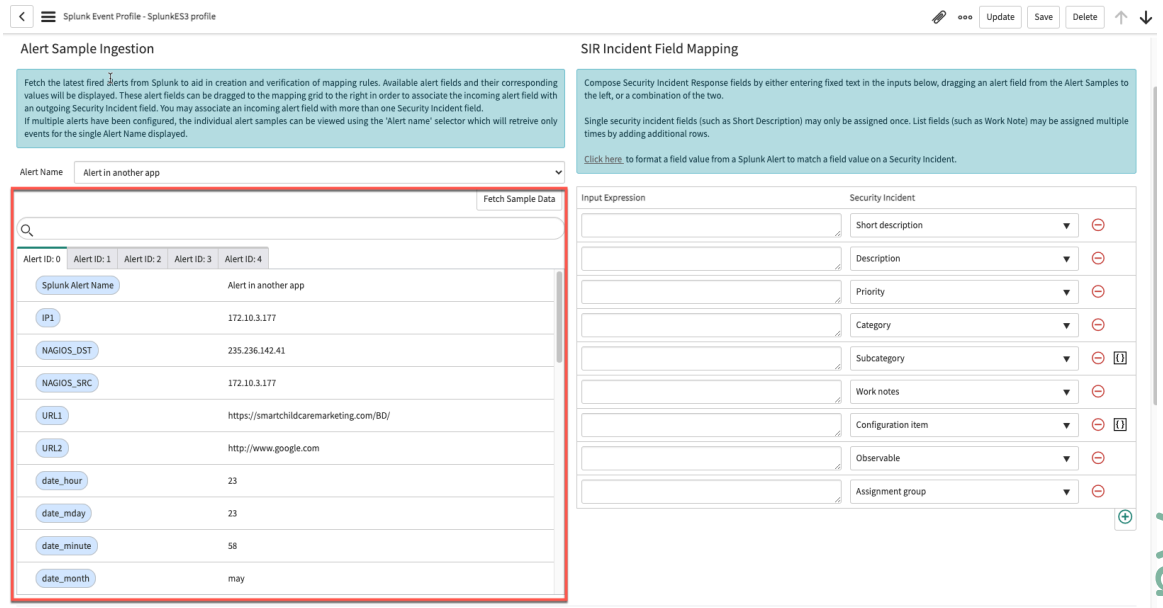
   Der Abruf für Beispielereignisse kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt.

   Hinweis:
   Ein zusätzliches Zuordnungsfeld, **Splunk-Warnungsname** , Wird von der Integration hinzugefügt, um ein Ereignis bis zur Quellwarnungsregel in nachzuverfolgen Splunk. Dies kann in Szenarien hilfreich sein, in denen mehrere auftreten Splunk Warnungen werden in einem einzelnen Profil kombiniert.

   Wenn ein einzelnes Feld mehrere Werte enthält, werden diese Werte analysiert und einzelnen Feldeinträgen im SIR-Incident-Feldzuordnungsabschnitt zugeordnet. Beispielsweise können die Quell-IP-Adressen, Asset-Namen oder URLs mehrere erkennbare Feldeinträge oder mehrere CIs aufweisen. Diese werden analysiert und einzelnen Feldeinträgen im SIR-Incident-Feldzuordnungsabschnitt zugeordnet.

   In der folgenden Abbildung werden die Feld-Name-Wert-Paare für die erfasste Warnung oder das importierte Beispielereignis auf der linken Seite dieses Formulars angezeigt, nachdem der Abruf abgeschlossen ist. Diese Werte sind die Werte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Fahren Sie für geplante Warnungsprofile mit Schritt fünf fort, um die Werte zuzuordnen.
4. Alternativ für ein Profil für einen Ereignistyp, den Sie aus exportieren möchten Splunk Enterprise Konsole führen Sie die folgenden Schritte aus, um Anhangsdaten in hochzuladen ServiceNow AI Platform® Instanz.
   a. Wenn Sie sich noch nicht angemeldet haben, melden Sie sich bei an Splunk Enterprise Konsole.
   b. Navigieren Sie zur Registerkarte Suche, und geben Sie einen Namen für eine Suche mit den Ereignisdaten ein, die Sie exportieren möchten.

      Beispielsweise ist Malware ein Suchbegriff, der für alle Malware-Ereignisse verwendet wird, die Sie mit dem Workflow dieser Integration weiterleiten können.

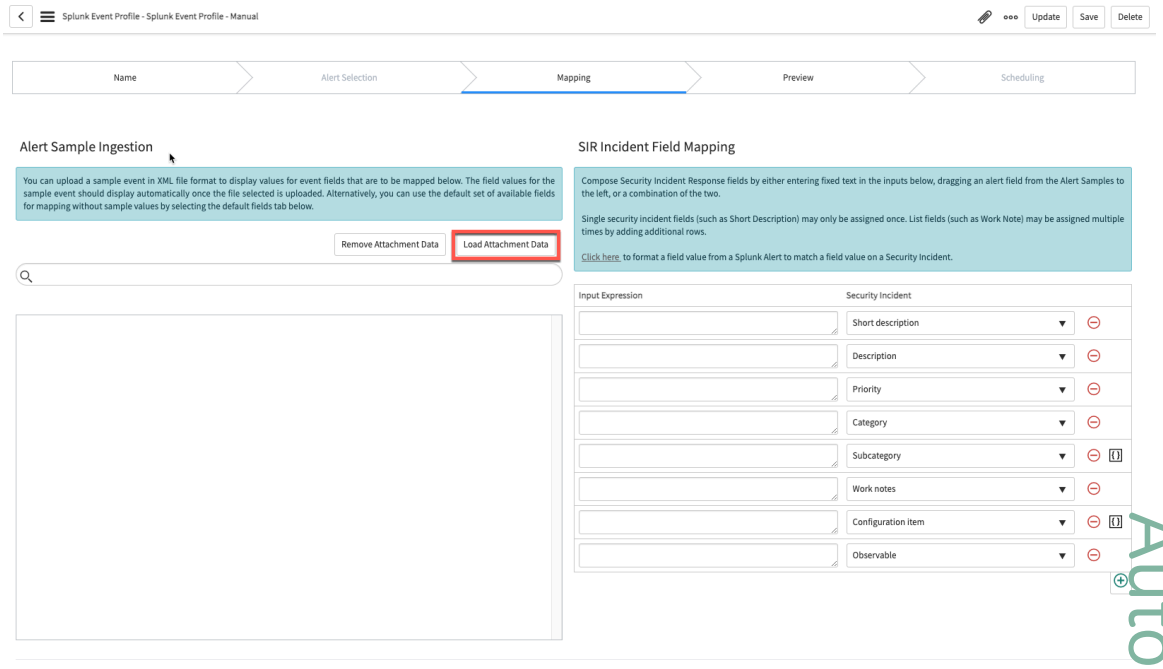
   c. Erweitern Sie das Ereignis, und wählen Sie in der Spalte Feld die Felder aus, die Sie importieren möchten.

      Diese Felder sind die Feld-Wert-Paare, die exportiert und auf der Zuordnungsseite in angezeigt werden ServiceNow AI Platform® Instanz.

   d. In Ihrem Splunk Enterprise Konsole klicken Sie oben rechts auf der Suchseite auf **Exportieren** Symbol.
   e. Klicken Sie in der Liste für das Feld Format im angezeigten Dialogfeld auf **XML-Format** .
   f. **Wahlweise:** Geben Sie einen neuen Dateinamen ein.
   g. Klicken Sie auf **Exportieren**.
      Die Datei wird auf heruntergeladen ServiceNow AI Platform® Instanz.
   h. Wenn die Zuordnungsseite nicht bereits in angezeigt wird ServiceNow AI Platform® Instanz, klicken Sie auf **Zuordnung** In der Fortschrittsleiste.
   i. Klicken Sie in der Spalte Warnungsbeispielerfassung auf **Laden Sie Anhangsdaten** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



j. Klicken Sie im angezeigten Dialogfeld auf **Wählen Sie Dateien aus** Und navigieren Sie zu .Xml Datei, die Sie exportiert haben, und klicken Sie auf **Öffnen** .
Die Wertpaare für die Felder, die Sie für das Ereignis exportiert haben, werden auf der linken Seite des Zuordnungsformulars angezeigt.

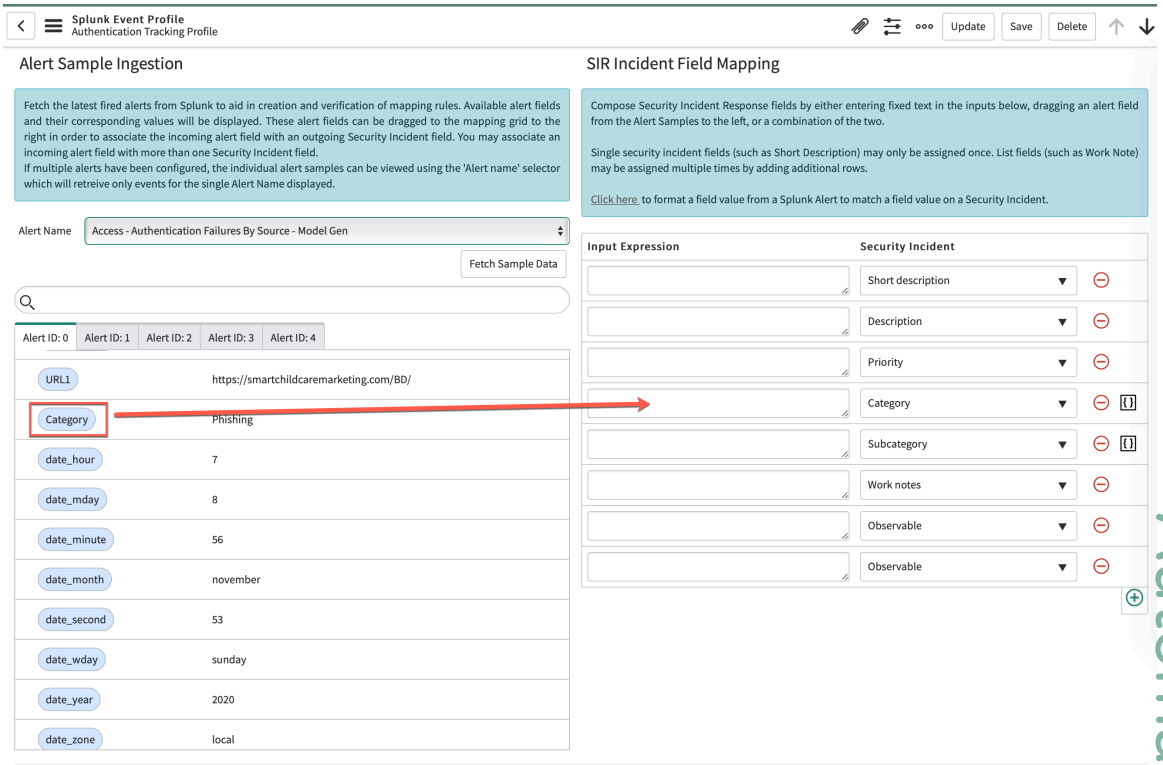
In der folgenden Abbildung werden die Datenpaare für eine erfasste geplante Warnung auf der linken Seite dieses Formulars angezeigt. Wertepaare für importierte Ereignisse werden auch auf dieser Seite des Formulars angezeigt. Diese Werte sind die Feldwerte, die Sie den Security Incident-Feldern auf der Seite „Sir Incident-Feldzuordnung“ des Formulars zuordnen.

5. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf der linken Seite des Formulars auf einen blauen Feldnamen.

6. Ziehen Sie den Feldnamen, z. B. Kategorie , Und legen Sie es in einem Feld in der Spalte „Eingabeausdruck“ neben einem Feldnamen in der Spalte „Security Incident“ ab.

Automatische Übersetzung

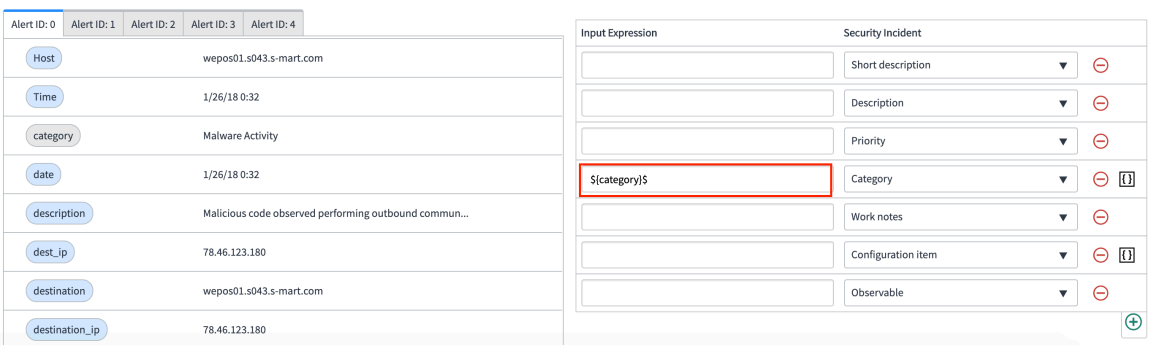
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Feldwert wird in der Spalte „Eingabeausdruck“ angezeigt. In der folgenden Abbildung: Kategorie Ist dem zugeordnet Kategorie Feld im Security Incident. Sie können jedoch einen beliebigen Wert von der linken Seite mit einem Feld auf der rechten Seite abgleichen. Stellen Sie sicher, dass der Wert dem Security Incident während des Vorschauschritts korrekt zugeordnet ist.

Damit Sie sicherstellen können, dass im Zuordnungsprozess keine Ereignisse übersehen oder dupliziert werden, sind Felder farbcodiert. Hellblaue Felder auf der linken Seite zeigen an, dass noch kein Feld ausgewählt und dem Security Incident zugeordnet ist. Möglicherweise möchten Sie ein eingehendes Warnungsfeld mit mehr als einem Feld in einem Security Incident verknüpfen.

Ein graues Feld gibt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen, da Warnungsereignisfelder in bestimmten Fällen nur einmal zugewiesen werden können. Beispielsweise können Sie Feldern wie Kurzbeschreibung nur einmal Werte zuweisen. Sie können jedoch Listenfelder wie Arbeitsnotiz mehrmals zuweisen, indem Sie dem Zuordnungsraster zusätzliche Zeilen hinzufügen.

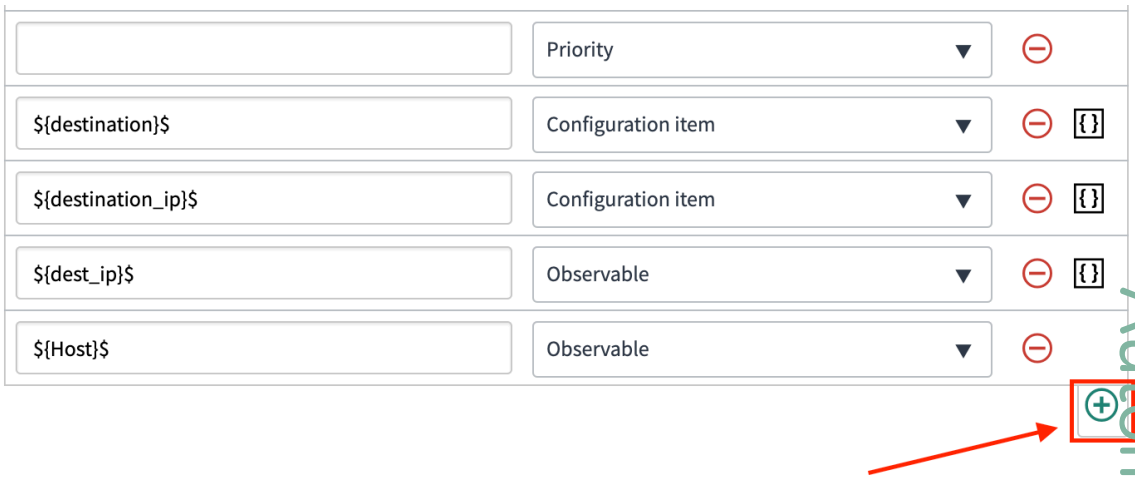


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Führen Sie die folgenden Schritte aus, um der Standardzuordnung des Security Incident auf der rechten Seite des Formulars Felder hinzuzufügen.

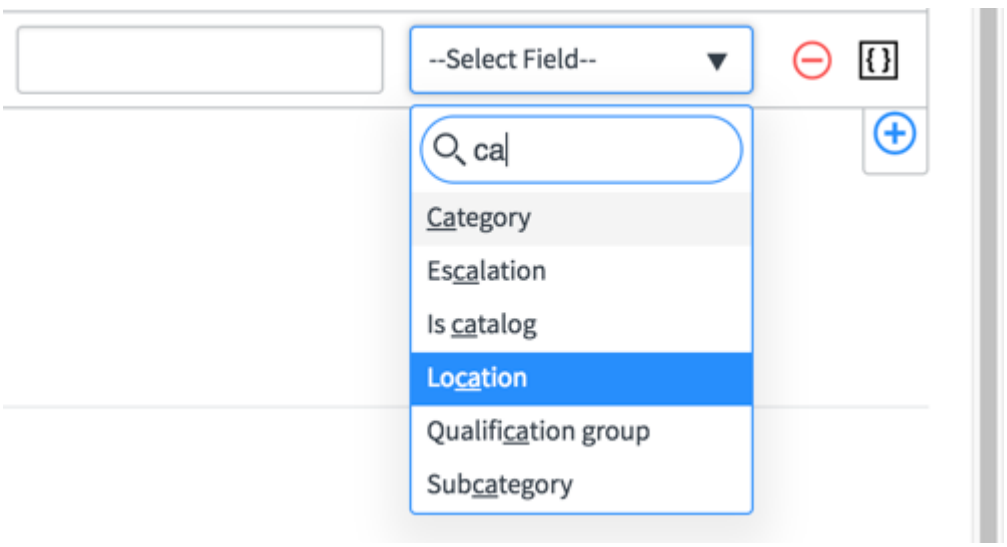
   a. Klicken Sie auf der rechten Seite des Formulars im Abschnitt „SIR-Incident-Feldzuordnung“ unten im Raster auf das Plus-Symbol.



   Ein neues Feld wird angezeigt.

   b. Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie ein Feld aus.

   In der erweiterten Liste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung: Kategorie Hat einen grauen Hintergrund, da er im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für Warnungsfelder auf der linken Seite des Formulars hilft diese Farbcodierung für die Security Incident-Felder auf der rechten Seite Ihnen, die Zuordnung nachzuverfolgen.



Automatische Übersetzung

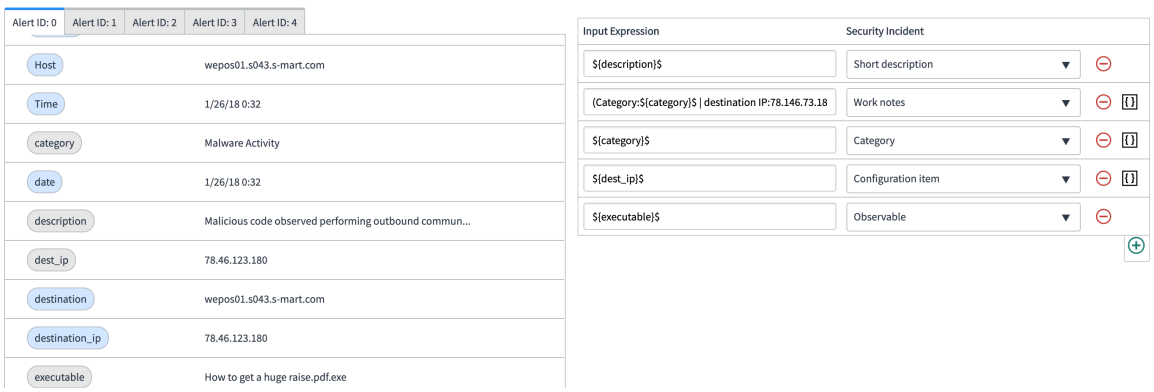
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Damit mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „erkennbares Element“ mehrmals verschiedenen Werten zugeordnet werden. Ebenso unterstützen die Felder „Konfigurationselement“ und „Arbeitsnotizen“ mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Liste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

c. Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.

d. Klicken Sie auf der linken Seite des Formulars mit der linken Maustaste, um auszuwählen **Warnungs-ID**
Die Sie im Feld Eingabeausdruck wünschen.
Ordnen Sie sie mit der Drag-Funktion neben Ihrem neuen Feld zu.

8. Fahren Sie mit der Zuordnung fort, indem Sie Felder hinzufügen oder entfernen und der Zuordnung Werte hinzufügen.
Die folgende Abbildung zeigt ein Beispiel für ein bearbeitetes Zuordnungsraster. Im unteren Feld rechts wird das Feld Arbeitsnotizen hinzugefügt, das mehr als einen Wert hat. Die Werte sind durch Leerzeichen und Interpunktionszeichen (Kategorie:${category} | Ziel-IP:78.146.73.180).



In der Vorschau werden diese Werte in den Arbeitsnotizen zum Security Incident angezeigt. Da der Wert für ein Feld gilt, das Sie dem Raster hinzugefügt haben, und dem Feld Arbeitsnotizen mehrere Werte zugeordnet sind, werden die Werte wie eingegeben angezeigt. In diesem Beispiel werden die Leerzeichen und Interpunktionszeichen, die Sie in das Feld eingegeben haben, im Abschnitt „zugehörige Elemente“ als Arbeitsnotiz in der Vorschau des Security Incident angezeigt.

Die folgende Abbildung zeigt, wie die Werte im vorherigen Bild für den Security Incident angezeigt werden.

Filterbedingungen für die Incident-Generierung

9. Wahlweise: Nachdem Sie die vorherigen Zuordnungsschritte auf Feldebene abgeschlossen haben, können Sie dieselben Feldwerte im Generator für Filterbedingungen verwenden, um zusätzliche Kriterien zu definieren, die eine eingehende Warnung erfüllen muss, um einen zu erstellen SIR Security Incident.

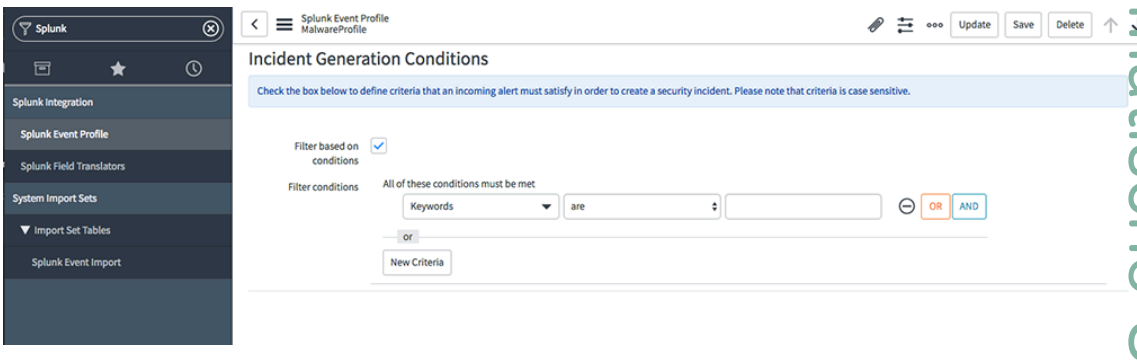
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um Filterbedingungen festzulegen, gehen Sie wie folgt vor.

a. Scrollen Sie im Formular zum Abschnitt Bedingungen für die Incident-Generierung, und wählen Sie aus **Filtern Sie basierend auf Bedingungen** Kontrollkästchen zum Aktivieren der Option.

(Optional) Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den spezifischen Bedingungen entsprechen, die in den Feldern beschrieben werden.

Die Optionen in den Listen für das erste Feld im Generator für Filterbedingungen entsprechen den Feldern, die im Abschnitt „Warnungsbeispielerfassung“ für die von Ihnen erfasste Warnung angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach Splunk Warnung, die Sie erfassen, oder das Ereignis, das Sie manuell weiterleiten. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden und müssen genau mit den Werten von übereinstimmen Splunk Enterprise Warnung oder Ereignis. Wenn Sie sich nicht sicher sind, welche Werte in die Filterfelder eingegeben werden sollen, kehren Sie möglicherweise zu zurück Splunk Enterprise Konsole und überprüfen Sie Ihre Warnungen und Ereignisse auf die Stichwörter.

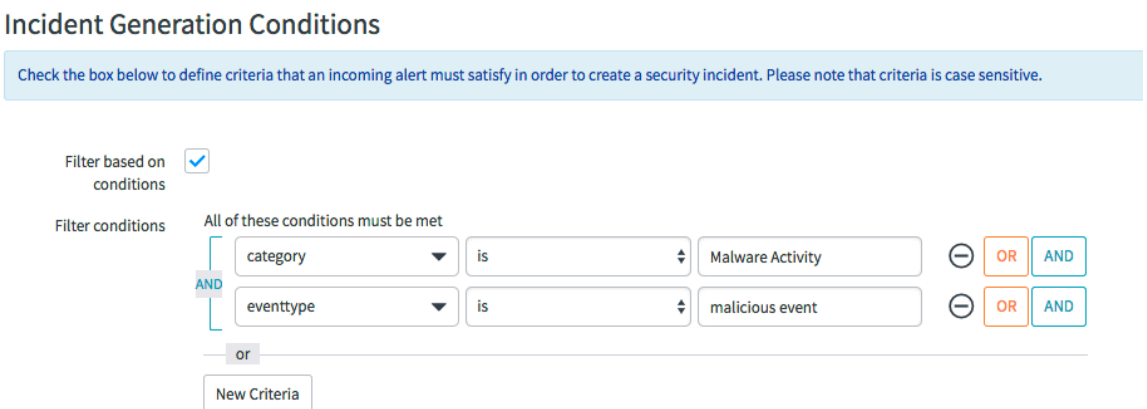


b. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators Filter für die erste Zeile fest.

c. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** Oder **ODER** . Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden.

d. **Wahlweise:** Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

(Optional) Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt werden müssen, bevor Security Incidents erstellt werden.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Optional) Sie haben die Auslösebedingungen so festgelegt, dass Security Incidents nur erstellt werden, wenn beide von Ihnen eingegebenen Filterbedingungen erfüllt sind.

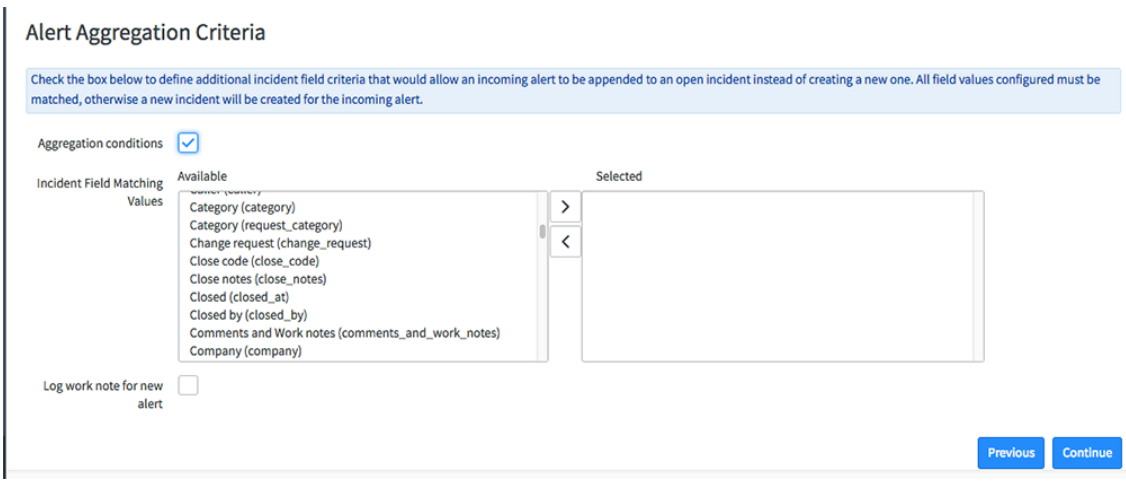
Diese Art der Filterung hilft Ihnen, Sicherheitsereignisse zu isolieren und die Anzahl der von Ihnen erstellten Security Incidents zu begrenzen. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur erforderliche Warnungen erfasst, ohne dass geändert werden muss Splunk Abfrage oder Konfiguration der ausgelösten Warnung.

Zusammenfassungswarnungen, um doppelte Incidents zu verhindern

10. **Wahlweise:** Um zu vermeiden, dass doppelte Security Incidents erstellt werden, definieren Sie zusätzliche Incident-Feldkriterien, damit eingehende Warnungen zu einem offenen Security Incident zusammengefasst werden.
Um diese Kriterien festzulegen, führen Sie die folgenden Schritte aus.

   a. Scrollen Sie im Formular zum Abschnitt Warnungszusammenfassungskriterien, und aktivieren Sie das Kontrollkästchen Aggregatbedingungen, um diese Option zu aktivieren.

   (Optional) Die Spalten „Incident-Feld-Übereinstimmungswerte“ werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die in konfiguriert sind SIR Security Incident.



   b. Wählen Sie in der Liste verfügbar die Feldwerte aus, die Sie für vorhandene Security Incidents in abgleichen möchten ServiceNow AI Platform Und verschieben Sie sie in die Liste ausgewählt.

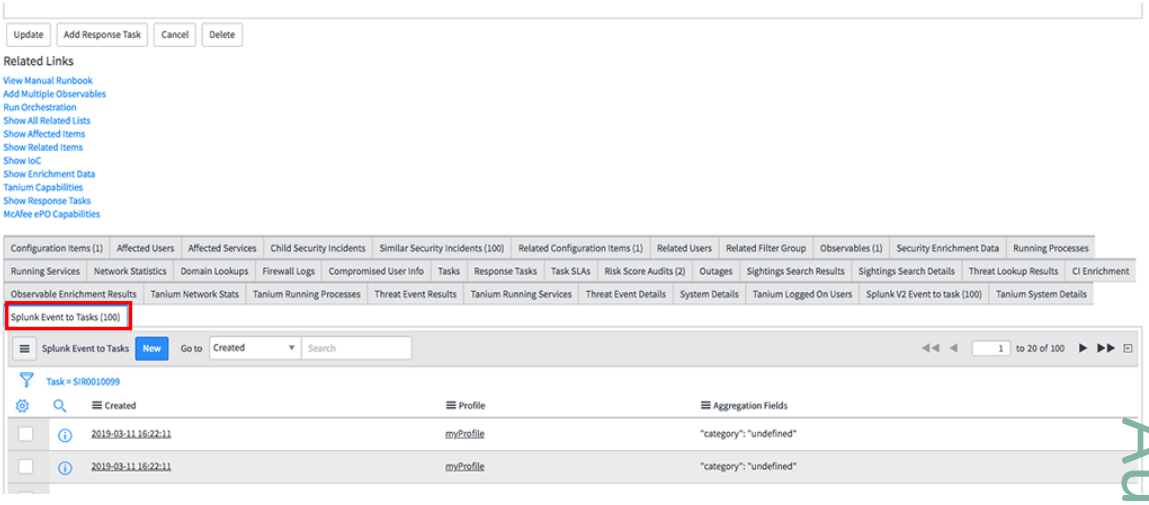
   (Optional) Alle von Ihnen ausgewählten Feldwerte müssen abgeglichen werden, um diese eingehende Warnung an einen vorhandenen Security Incident anzuhängen. Wenn Sie Feldwerte für Security Incidents überprüfen möchten, die für diese Kriterien verwendet werden sollen, navigieren Sie zu **Incidents** > **Alle Incidents anzeigen**an.

   Wenn eine neue Warnung allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird die Warnung automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Anwender mit der Rolle „sn_si.Analyst“, der mit Security Incidents arbeitet, können Sie alle hinzugefügten aggregierten Warnungen in einer zugehörigen Liste zu einem Security Incident anzeigen. Alle zusammengefassten Warnungen zu einem Security Incident werden auf der angezeigt Splunk Zugehörige Liste „Ereignis zu Aufgaben“. Diese Liste enthält Details zu zugeordneten Zeitstempeln und zusammengefassten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum Warnungen vorhandenen Security Incidents hinzugefügt werden. Wenn diese

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte nicht angezeigt wird, scrollen Sie unter zugehörige Links zur linken Seite des Datensatzes, und klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Link.



c. **Wahlweise:** Um eine Arbeitsnotiz für eine neue Warnung zu protokollieren, die kürzlich zum Security Incident hinzugefügt wurde, aktivieren Sie das Kontrollkästchen, um diese Option zu aktivieren.
Die Arbeitsnotiz protokolliert, dass eine neue Warnung zusammen mit einem Link zu den Warnungsdetails hinzugefügt wurde.

Sie haben erfolgreich Werte aus einem zugeordnet Splunk Warnung oder Ereignis an Felder in einem SIR Security Incident. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien einzuschränken. Sie haben auch Warnungen oder Ereignisse an vorhandene angehängt SIR Security Incidents.

11. **Wahlweise:** Öffnen Sie den Skripteditor, und fahren Sie mit der Bearbeitung fort.

(Optional) Weitere Informationen zum Skript-Editor finden Sie unter Verwenden Sie den Skript-Editor, um Warnungswerte für zu formatieren Splunk Enterprise Event Ingestion Integration.

12. Wählen Sie eine Option aus, um mit der Profilkonfiguration fortzufahren.

Nächste Maßnahme

Der nächste Schritt besteht darin, eine Vorschau der Werte anzuzeigen, die Sie dem Security Incident zugeordnet haben.

Vorschau des Security Incidents für anzeigen Splunk Enterprise Event Ingestion Integration

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem zugeordnet haben ServiceNow AI Platform® Security Incident Response(SIR) Security Incident. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle Warnungsfelder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie eine Vorschau eines Security Incidents an, und bearbeiten Sie die Zuordnung nach Bedarf erneut, um Felder mit Fehlern zu beheben oder fehlende Daten auszufüllen.

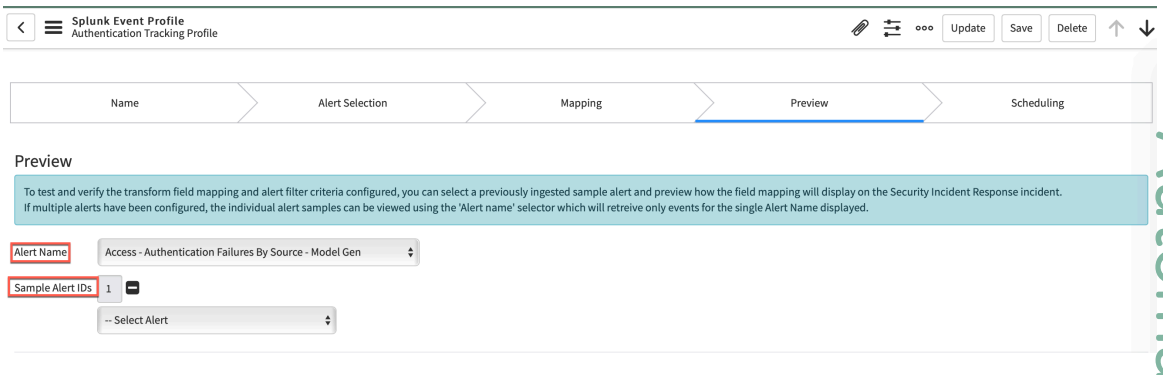
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Vorschau nicht erfolgreich abgeschlossen wurde, können Sie nicht mit dem Planungsschritt fortfahren. Vorschauen von SIR Security Incidents werden nicht als tatsächliche Incidents in gespeichert SIR Produkt.

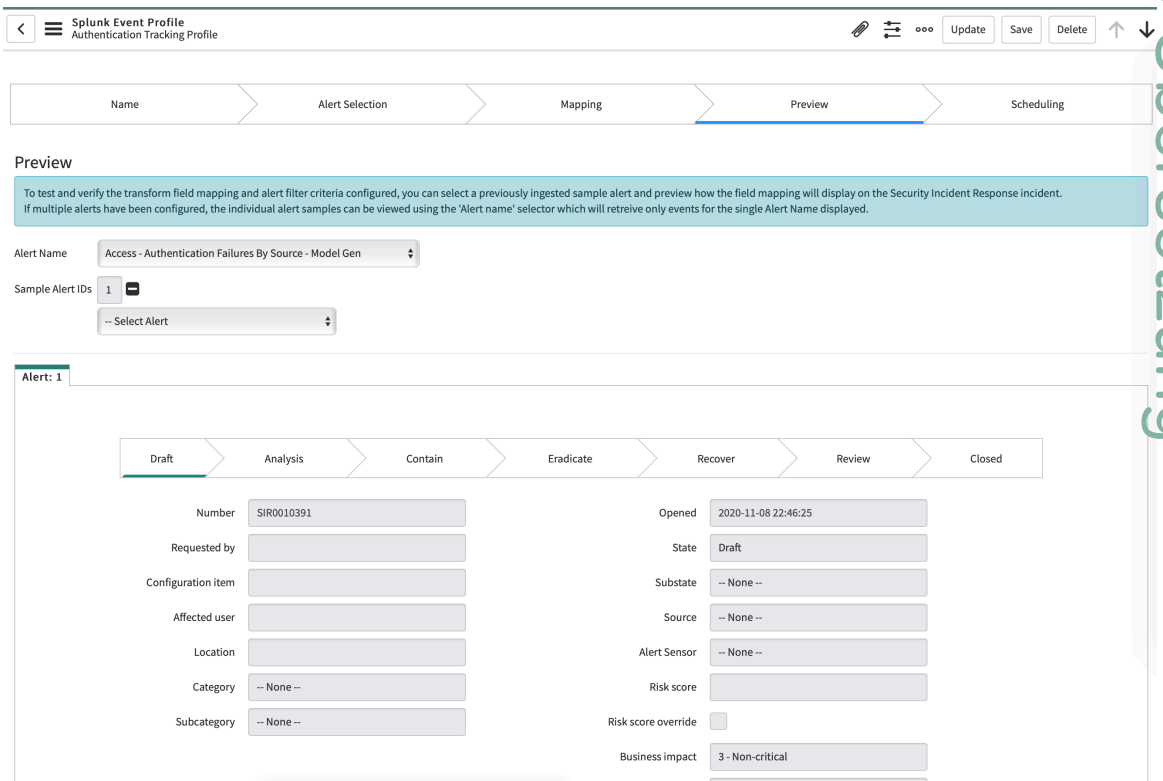
Prozedur

1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie auf **Vorschau** In der Fortschrittsleiste.
2. Wählen Sie aus **Warnungsname** Und wählen Sie dann ein Element aus der aus **Beispiel für Warnungs-IDs** Liste.



Der Security Incident wird angezeigt. Ändern Sie keine Informationen in den Feldern. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.

3. Überprüfen Sie die Feldzuordnung der Warnungswerte für den Security Incident.



Das vorangegangene Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler. In diesem Beispiel ist für einen Wert kein Feld im Security Incident vorhanden, oder das Feld unterstützt den von Ihnen zugeordneten Wert nicht. Eine Fehlermeldung wird

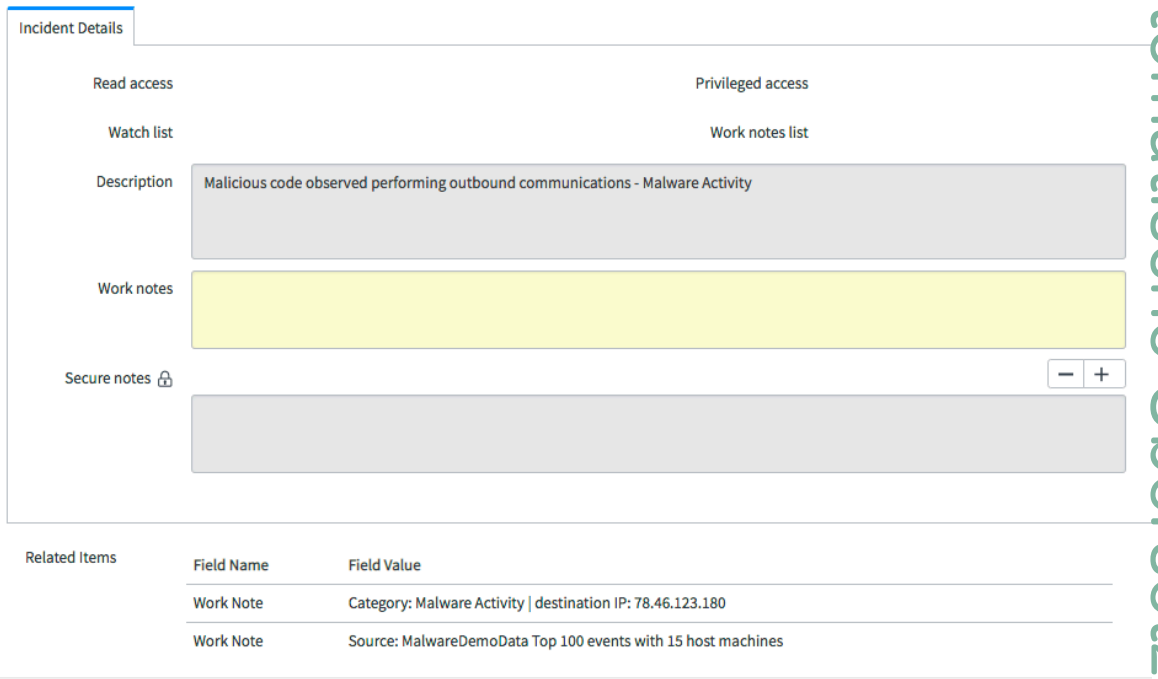
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angezeigt, die angibt, dass für keinen Eingabewert gefunden wurde Konfigurationselement Feld.

4. Klicken Sie auf, um diesen Fehler zu beheben **Zuordnung** In der Fortschrittsleiste.
5. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
6. Zeigen Sie erneut eine Vorschau der Zuordnung an, und beheben Sie alle Fehler, die in Fehlermeldungen beschrieben werden.

   Die folgende Abbildung ist ein Beispiel für die Registerkarte Incident-Details in der unteren Hälfte von SIR Security Incident, nachdem alle Fehlermeldungen gelöst wurden. In diesem Beispiel wurden die Felder Beschreibung und Arbeitsnotizen zugeordnet, und diese Felder werden mit den Werten aus den Wertepaaren ausgefüllt, die aus abgerufen wurden Splunk Enterprise Konsole. Das erste Feld „Arbeitsnotizen“ hat keinen Wert. Dieses Feld wurde während des Zuordnungsschritts im Zuordnungsraster leer gelassen. Die zusätzlichen Arbeitsnotizfelder mit Werten wurden dem Zuordnungsraster während des Zuordnungsschritts hinzugefügt.



7. Nachdem Sie Fehler behoben und überprüft haben, ob die Felder so sind, wie Sie sie möchten, wählen Sie eine Option aus, um fortzufahren.

Automatische Übersetzung

Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind, ist der nächste Schritt bis Planen und rufen Sie Warnungen für ab Splunk Enterprise Event Ingestion Integration.

Planen und rufen Sie Warnungen für ab Splunk Enterprise Event Ingestion Integration

Bei Profilen der automatisierten Warnungserfassung ist dieser Schritt der letzte Schritt der Ereignisprofilkonfiguration. Während dieses Schritts können Sie die Standardeinstellungen für den Warnungsabruf überprüfen oder die Planung nach Bedarf ändern. Mit diesem Schritt können Sie Ihren Warnungsabruf basierend auf einem Datumsbereich filtern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:

Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie alle Schritte im Fortschrittsbalken für die Profilkonfiguration wie in der folgenden Abbildung gezeigt abgeschlossen haben, haben Sie die Konfiguration für Profile für die manuelle Ereignisweiterleitung abgeschlossen. Für manuell von Ihrem weitergeleitete Ereignisse ist keine Planung verfügbar Splunk Enterprise Konsole. Für Profile für die automatisierte Warnungserfassung wählen Sie aus, ob Sie während des Planungsschritts historische Warnungen erfassen möchten. Sie wählen auch aus, wie oft Sie nach zukünftigen Warnungen abfragen, die der Warnungsprofilkonfiguration entsprechen.

Fortschrittsbalken

Bei Profilen zur automatisierten Warnungserfassung überprüfen und ändern Sie die Planung und den Warnungsabruf, bevor das Profil aktiviert wird. Dieser Schritt ist der letzte Schritt des Ereignisprofilkonfigurationsprozesses für geplante Warnungsprofile.

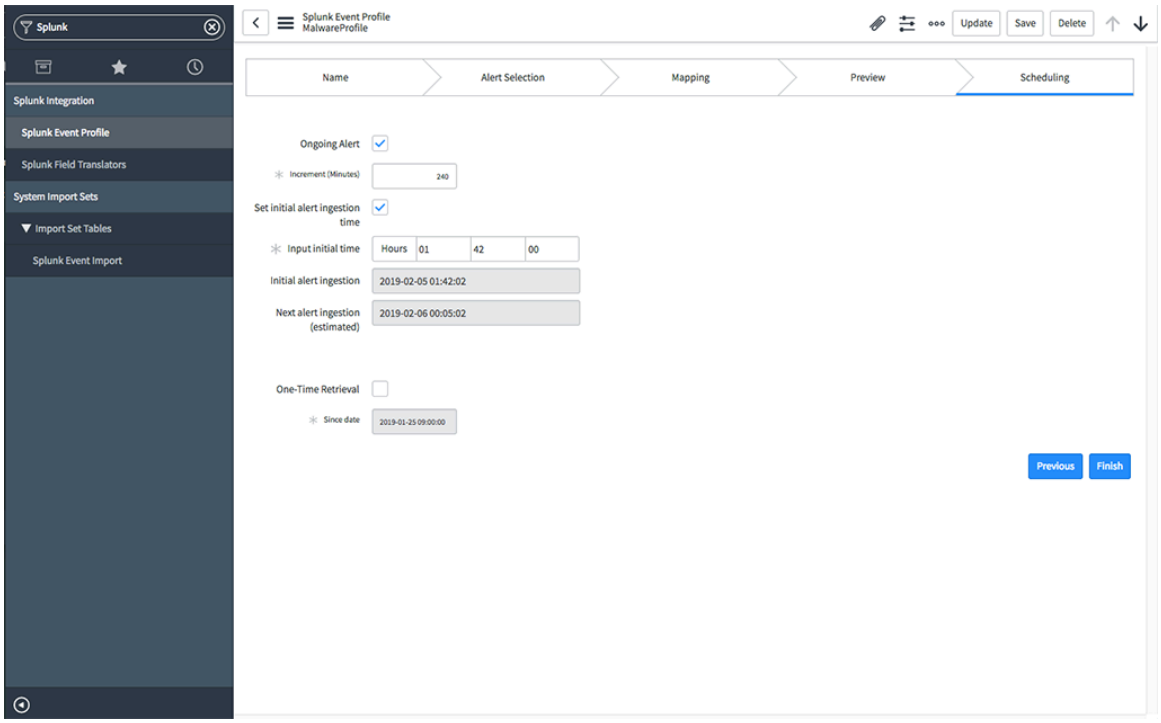
Konfigurieren Sie diese Abfrageintervalle pro Profil. Die Leistung von Splunk Die Integration der Ereigniserfassung wird von den verschiedenen Abfrageintervallen beeinflusst. Bei der Planung ziehen Sie es möglicherweise vor, die Systemlast gegen die Dringlichkeit des Incident auszugleichen. Für jedes Profil ist ein fünf-Minuten-Standardwert festgelegt. Sie können diese Einstellung jedoch basierend auf der Dringlichkeit des Incident und der erwarteten Belastung Ihres Systems ändern.

In Splunk Enterprise-Konsole legen Sie eine auslösende Warnung fest, die auf Inkrementen oder einer bestimmten Zeit basiert. Verwenden Sie diese Einstellung, um die Planung in zu konfigurieren ServiceNow AI Platform Instanz, sodass die Zeit in Ihrem erhöht wird Splunk Enterprise Konsole synchronisieren mit der Planung, die Sie in eingerichtet haben ServiceNow AI Platform Instanz.

Prozedur

1. Wenn die Seite „Zeitplanung“ im Fortschrittsbalken nicht angezeigt wird, wählen Sie aus **Zeitplanung** .
2. Wählen Sie eine aus, um zu planen, wie und wann Warnungen aus abgerufen werden Splunk Enterprise Konsole.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beispiel für die Planung, wenn Sie täglich eine haben Splunk Warnung, die einmal täglich um 4 Uhr Ortszeit ausgeführt wird. Sie können das entsprechende Warnungsprofil in einrichten ServiceNow AI Platform Instanz, die um 4:05 UHR Ortszeit ausgeführt werden soll, um die Warnung sofort zu erfassen und einen Security Incident zu erstellen. Geben Sie Ein `04 05 00` In **Erste Warnungserfassung** Feld. In **Inkrement (Minuten)** Feld eingeben `1440` (24 Stunden) zum Planen der nächsten Warnungserfassung für 24 Stunden ab der ersten Warnungserfassung. In den Feldern werden sowohl die Zeit der ersten Warnungserfassung als auch die Zeit der nächsten Warnungserfassung angezeigt.

3. Um die Einstellungen für dieses Beispiel zu konfigurieren, führen Sie die folgenden Schritte aus.

   a. Wenn die Seite „Zeitplanung“ angezeigt wird, wählen Sie aus **Laufende Warnung** Kontrollkästchen zum Aktivieren dieser Option.

   b. In **Inkrement (Minuten)** Feld eingeben `1440` (24 Stunden).

   c. Klicken Sie auf **Wählen Sie erste Warnungserfassung aus** Kontrollkästchen zum Aktivieren der Bearbeitung der Felder „erste Warnungserfassung“ und „nächste Warnungserfassung“.

   d. Geben Sie im Feld erste Warnungserfassung ein `04 05 00` .
   In **Die nächste Warnungserfassung (geschätzt)** Feld wird die Zeit der nächsten Warnungserfassung angezeigt.

4. Klicken Sie Auf **Beenden** Um die Konfiguration abzuschließen.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Dieses Profil ist aktiviert und ruft Warnungen aus ab Splunk Enterprise Konsole basierend auf Ihrer Planung. Es gibt ein Limit von 1.000 Security Incidents, die innerhalb von 24 Stunden erstellt werden können. Pro ausgelöster Warnung werden bis zu 100 Ereignisse ausgeführt. Nachfolgende Ereignisse werden ignoriert, nachdem die Grenzwerte erreicht wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrationsarchitektur und Verbindung mit externen Systemen für Splunk Enterprise Event Ingestion Integration

Im folgenden Thema wird die Integrationsarchitektur beschrieben, die entwickelt wurde, um die Erfassung ausgelöster Warnungen von zu unterstützen Splunk Enterprise Konsole. Diese Informationen verdeutlichen auf allgemeiner Ebene den konzeptionellen Betrieb der Integration. Es wird auch erklärt, warum Setup-Schritte erforderlich sind, bevor die Anwendung über installiert wird ServiceNow Store.

Schlüsselbegriffe, die für diese Integration verwendet werden

Die folgenden Schlüsselbegriffe werden während der Installation und Konfiguration verwendet. Weitere Informationen zu diesen Begriffen finden Sie unter ServiceNow-Produktdokumentationswebsite Und Splunk-Website Und -Ressourcen auf Splunk-Ressourcen Seite.

ServiceNow AI Platform

Ein Unternehmen ServiceNow Produkt. Die ServiceNow AI Platform Ist die Basis, auf der einzelne Komponenten wie basieren Security Incident Response(SIR), IT Service Management (ITSM) und andere Produkte werden erstellt.

ServiceNow Splunkbase-Add

A ServiceNow Anwendung, die auf installiert ist Splunk Enterprise Konsole, die die manuelle Ereignisweiterleitungsoption der Integration unterstützt. Die manuelle Ereignisweiterleitung ist eine optionale Funktion der Integration. Dies ServiceNow Splunkbase-Add-on ist für die automatisierte Warnungserfassung, die von der Integration bereitgestellt wird, nicht erforderlich.

Security Incident Response (SIR)

A ServiceNow AI Platform Anwendung, die den Fortschritt von Security Incidents von der Erkennung und ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur endgültigen Überprüfung und Schließung von Security Incidents nachverfolgt.

Splunk Enterprise

Ein automatisiertes Security Incident Event Management (SIEM)-Produkt oder Cloud-Service, das Daten erfasst, die für die Analyse und das Management von Incidents verwendet werden. Dieser Service befindet sich auf einem Host, der manchmal auch als bezeichnet wird SplunkKonsole in diesem Handbuch.

Splunk Warnung

Eine Suche, die Sie in konfigurieren und speichern Splunk Dient zum Scannen nach bestimmten Daten basierend auf den Parametern, die Sie in eingerichtet haben Splunk Enterprise Service. Wenn Sie Warnungen aus abrufen Splunk, Sie rufen auch alle Ereignisse ab, die dieser Warnung zugeordnet sind.

Splunk Ausgelöste Warnung

Eine konfigurierte Suche in Splunk Enterprise Konsole, die Ergebnisse zurückgibt und diese Ergebnisse als ausgelöste Warnungen kennzeichnet. Die ausgelösten Warnungen werden aus erfasst Splunk-Konsole in Ihrem ServiceNow AI Platform Instanz für diese Integration. Ausgelöste Warnungen haben mindestens eine Splunk Ereignisse.

Splunk Termin

Ein oder mehrere Datenelemente, die zu den ausgelösten Warnungen des führen Splunk Service. Von Ihrem ServiceNow AI Platform Instanz können Sie nachschlagen, welche Splunk Ereignisse ausgelöst ServiceNow AI Platform Security Incidents.

MID-Server

Diese Anwendung erleichtert die Kommunikation und das Verschieben von Daten zwischen ServiceNow AI Platform Und externe Anwendungen, Datenquellen und Services. Diese

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung ist normalerweise für die Integration mit lokalen Technologien und erforderlich Splunk Enterprise Event Ingestion Integration erleichtert der MID-Server die Kommunikation zwischen ServiceNow AI Platform Und die lokale Instanz von Splunk Enterprise. Ein MID-Server ist nicht erforderlich, wenn Sie Ihren integrieren ServiceNow AI Platform Instanz mit Splunk Cloud Instanz.

Security Incident-Administrator (sn_si.admin)

Der Anwender mit dieser Rolle überwacht die Konfiguration der Integration mit SIR Produkt in Ihrem ServiceNow AI Platform Instanz.

Security Incident-Analyst (sn_si.Analyst)

Der Anwender mit dieser Rolle interagiert mit Security Incidents in und analysiert sie ServiceNow Security Incident Response Produkt.

Security Incident-Profiladministrator (sn_si.ingestion_profile_admin)

Der Anwender mit dieser Rolle konfiguriert das Plugin, erstellt, bearbeitet, löscht und verwaltet Erfassungsprofile für Azure Sentinel, Splunk und Splunk es Integration für SIR Produkt in Ihrem ServiceNow AI Platform Instanz.

Externe Systemverbindung

Ein Ereignisprofil ist ein Container, den Sie für eine singuläre Verbindung und einen Aufruf an erstellen, benennen und konfigurieren Splunk Service zum Abrufen der aktuell ausgelösten Warnungen, die bestimmten Kriterien entsprechen. Nachdem ausgelöste Warnungen abgerufen wurden, die Ihrem Profil entsprechen Splunk, Wählen Sie aus, welche dieser Warnungen als angezeigt werden sollen ServiceNow AI Platform Security Incident Response SIR Security Incident. Eine Standardansicht von Splunk Enterprise Warnungsfelder sind verfügbar, und Sie bearbeiten diese Zuordnung von Warnungsfeldern zu den Feldern in einem SIR Security Incident, der Ihren Anforderungen entspricht. Sie zeigen eine Vorschau Ihrer Zuordnung an, um sicherzustellen, dass alle erforderlichen Warnungsfeldwerte im ausgefüllt sind SIR Security Incident. Um die Konfiguration des Warnungsprofils abzuschließen, planen Sie den Abruf von Warnungen und aktivieren dann das Profil. Nachdem Sie das Profil in aktiviert haben ServiceNow AI Platform, Sie sind bereit, historische und laufende Aufnahmen zu erfassen Splunk Warnungen automatisch.

Wenn Sie als Anwender mit der Rolle sn_si.admin feststellen, dass eine neue ausgelöste Warnung den zuvor erfassten Warnungen ähnelt, können Sie neue ausgelöste Warnungen zu vorhandenen aggregieren SIR Security Incidents. Sie legen Kriterien fest, um übereinstimmende Zielfeldwerte in anzugeben Splunk Enterprise Warnungsprofil, das definiert, wann ein vorhandener Security Incident aktualisiert und wann ein neuer Security Incident erstellt wird. Wenn die Zusammenfassungsfunktion in Ihrem Ereignisprofil aktiviert ist, wenn der Importsatz umgewandelt wird, ist Ihr ServiceNow AI Platform Die Instanz sucht nach einem vorhandenen Datensatz in der Zieltabelle, der denselben Wert in den Ziel- und Quellfeldern hat. Wenn ein vorhandener Datensatz mit einem übereinstimmenden Wert in der Zieltabelle gefunden wird, wird dieser Datensatz aktualisiert. Wenn kein übereinstimmender Datensatz gefunden wird, wird ein neuer Datensatz in der Zieltabelle erstellt. Wenn diese Option aktiviert ist, aktualisiert die Zusammenfassungsoption vorhandene Security Incidents mit neuen ausgelösten Warnungen, und Sie vermeiden das Erstellen mehrerer Security Incidents. Weitere Informationen zum Aktualisieren von Datensätzen mithilfe von Zusammenfassungsoptionen finden Sie unter Datensätze werden mithilfe von Zusammenfügungen aktualisiert .

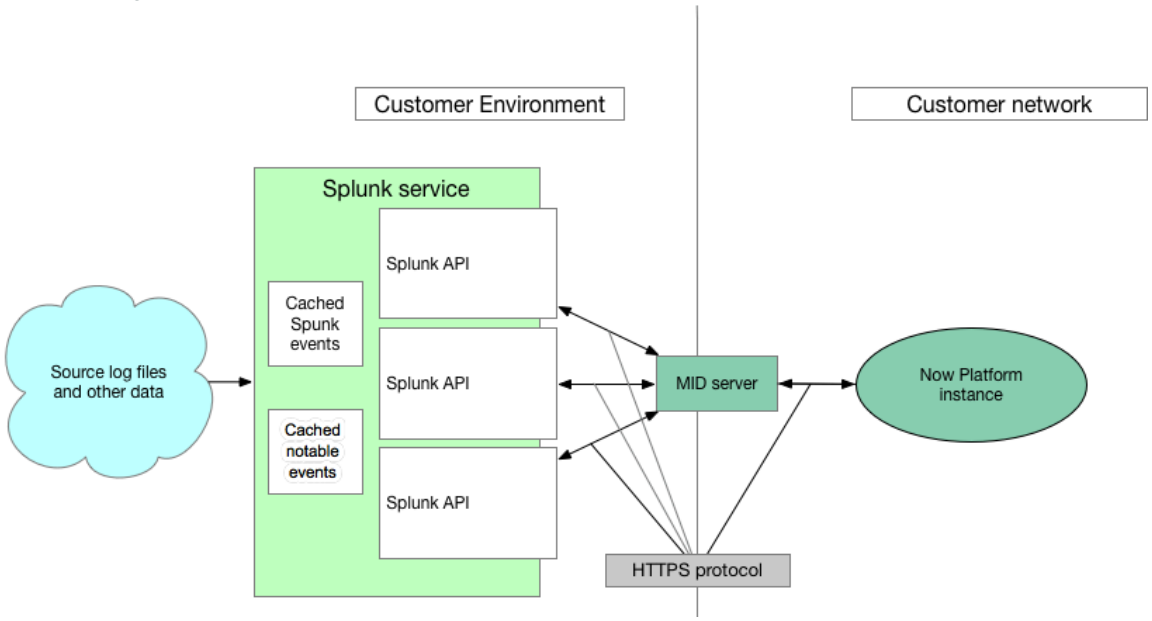
Diese Anwendung verwendet Splunk API-Service zum Abrufen von Informationen aus Splunk Service. Eine ausgehende HTTPS-Verbindung vom MID-Server zu dieser Umgebung ist erforderlich, damit die Integration ordnungsgemäß funktioniert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

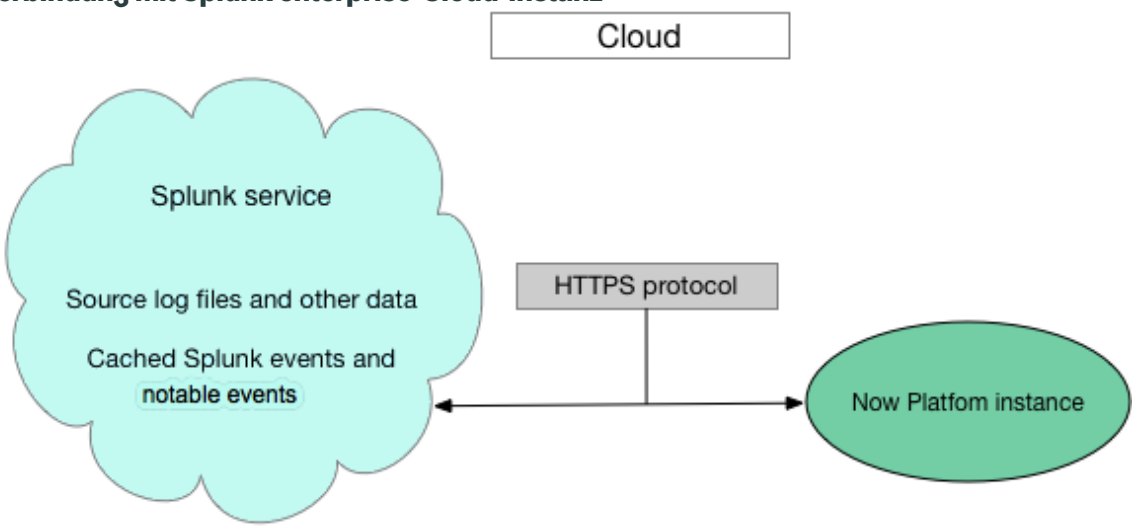
Nachdem es mit verbunden wurde Splunk Service unterstützt die Integration das Abrufen und Erfassen ausgelöster Warnungen und Ereignisse, die Security Incidents auslösen.

Der Basisdaten-Flow wird in den folgenden Abbildungen dargestellt. In jeder Abbildung ist Ihr ServiceNow AI Platform Ruft (erfasst) Daten ab. Splunk Sendet keine Daten für geplante Warnungen.

Verbindung zu lokal Splunk enterprise-Service mit einzelnen MID s Fehler



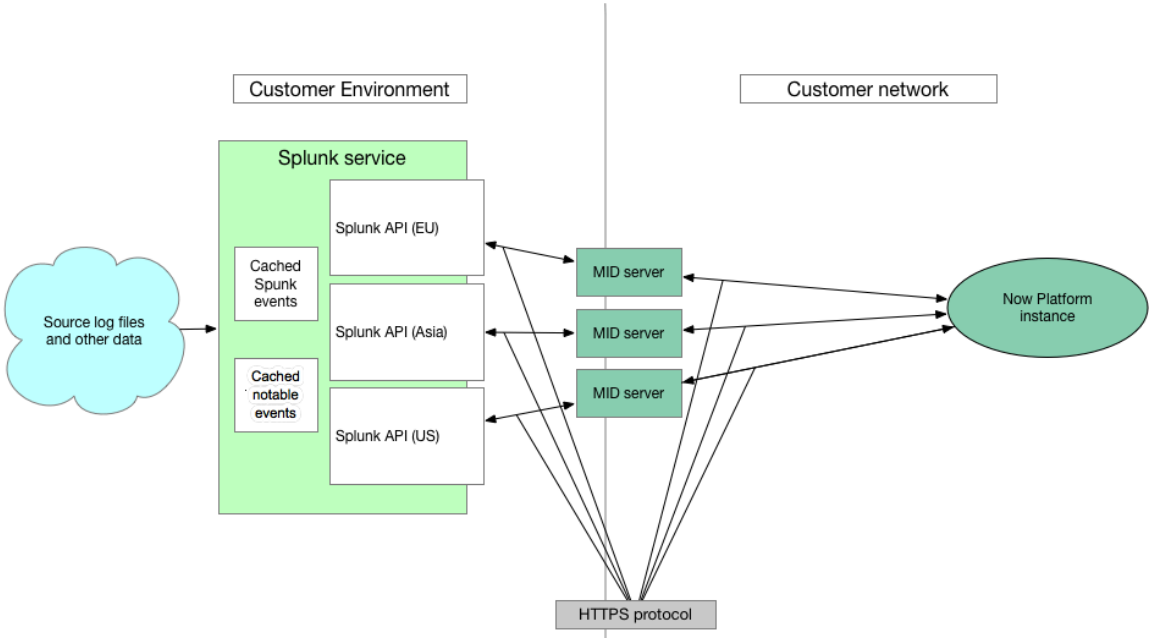
Verbindung mit Splunk enterprise-Cloud-Instanz



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehrere Verbindungen mit Splunk enterprise-Service mit mehreren MID-Servern



Kopieren Splunk Enterprise Event Ingestion Profile von einer Instanz zu einer anderen mithilfe der Export-/Importfunktion

Sie können exportieren und importieren Splunk Enterprise Event Ingestion Profileinstellungen von einem ServiceNow AI Platform Instanz zu einer anderen ServiceNow AI Platform Instanz.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Mit dieser Funktionalität kann der Sicherheitsadministrator Profile kopieren, die für eines getestet und verifiziert wurden ServiceNow AI Platform Instanz, z. B. außerhalb der Produktion, an eine andere ServiceNow AI Platform Instanz, z. B. Produktion, ohne dass alle Konfigurationseinstellungen wiederholt werden müssen. Zu den Einstellungen, die exportiert und importiert werden, gehören Profilname, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Konfigurationskachel-Quellinformationen.

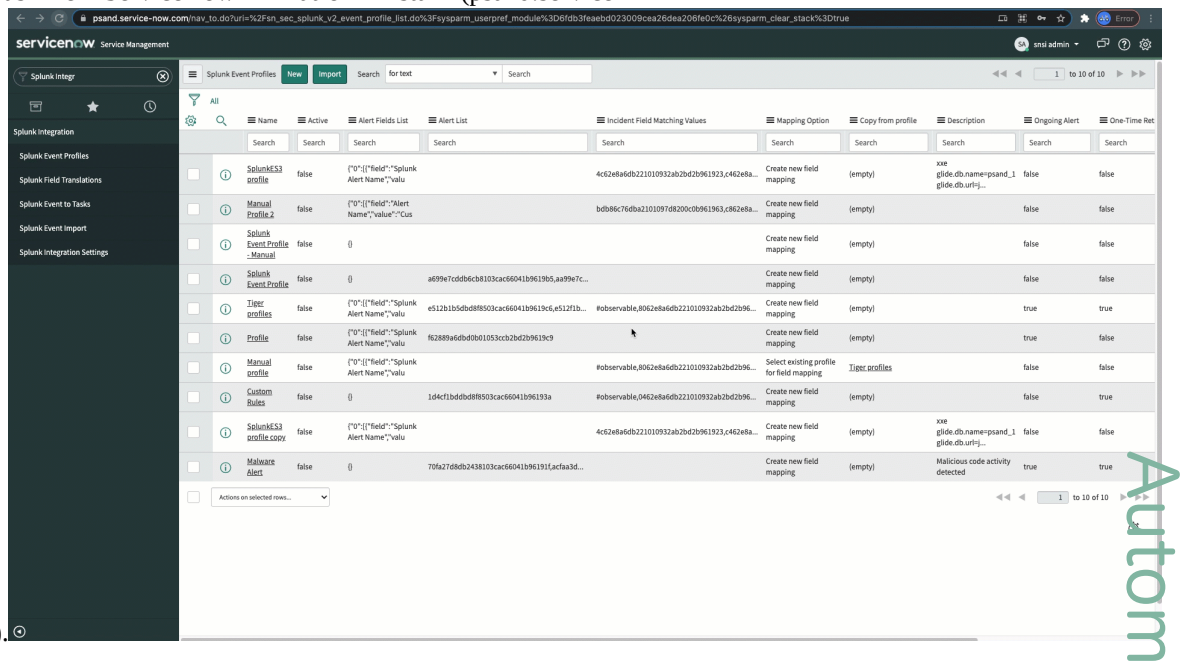
Hinweis:
Wenn Sie einen Profiltyp für die manuelle Ereignisweiterleitung exportieren, werden die für die Beispielfeldzuordnung verwendeten Anhangsdaten kopiert, die Anhangsdatei selbst wird jedoch nicht exportiert.

Prozedur

1. Navigieren zu **Alle** > **Splunk Integration** > **Splunk-Ereignisprofile**an.
2. Wählen Sie ein Profil aus, das Sie in ein anderes exportieren möchten ServiceNow AI Platform Instanz. Sie können mehrere Profile für den Export auswählen.
3. Klicken Sie im Menü Aktionen auf **Exportieren** .
4. Sobald die Meldung „Export abgeschlossen“ angezeigt wird, klicken Sie auf **Herunterladen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt den Export von Splunk Profil (Manuelles Profil 2) aus Ihrem ServiceNow AI Platform Instanz (psand.service-now.com).



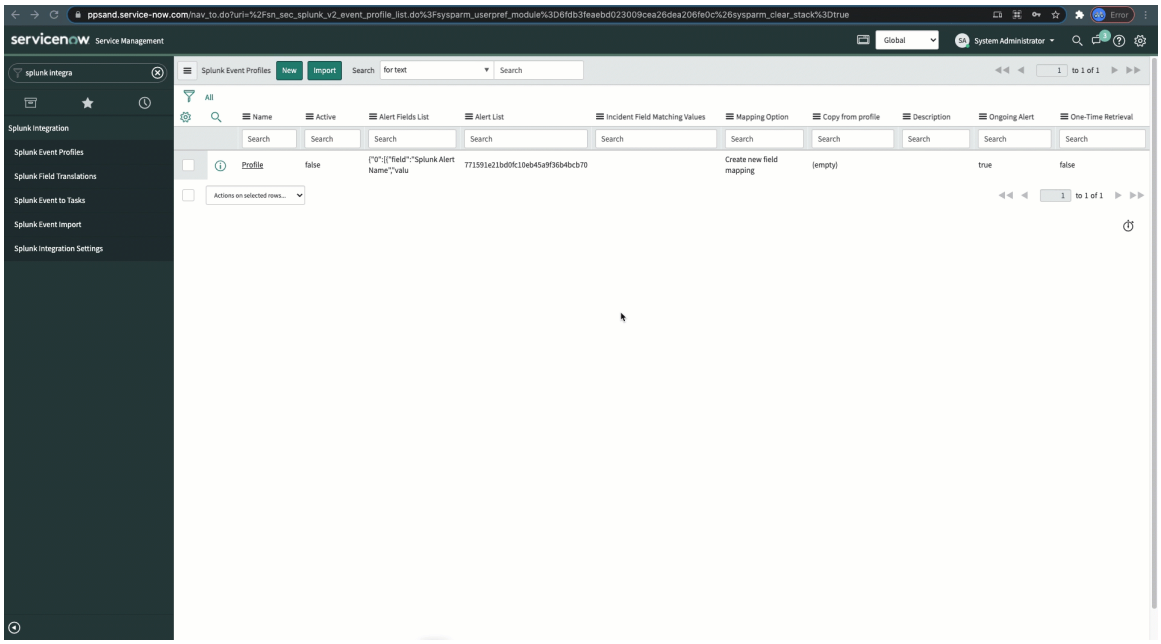
Die exportierte Datei payload.xml wird auf Ihren Computer heruntergeladen. Die Datei enthält den Profilnamen, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Konfigurationskachel-Quellinformationen. Wenn Sie mehrere Profile auswählen und herunterladen, werden sie in derselben Datei payload.xml angezeigt.

Sie können jetzt mit dem Import des Profils in ein anderes fortfahren ServiceNow AI Platform Instanz.

5. Navigieren zu **Splunk Integration** > **Splunk-Ereignisprofile**an.
6. Klicken Sie auf **Importieren**.
7. Klicken Sie Auf **Wählen Sie die Datei aus** Und wählen Sie die XML-Datei auf Ihrem Computer aus.
8. Klicken Sie auf **Hochladen**.
9. Klicken Sie Auf **Profile schließen und neu laden** .
   Die folgende Abbildung zeigt den Import von Splunk Profil (Manuelles Profil 2) aus dem ServiceNow AI Platform Instanz (psand.service-now.com) zu einer anderen ServiceNow AI Platform Instanz (ppsand.service-now.com).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie haben das Profil erfolgreich aus einem anderen importiert ServiceNow AI Platform Instanz.

Überprüfen Sie, ob die exportierte Quelle (Splunk API-Account und Splunk Server-URL) und MID-Server-Konfigurationseinstellungen sind gültig und in importiert verfügbar ServiceNow AI Platform Instanz. Aktualisieren Sie Ihren Splunk Enterprise Event Ingestion Konfiguration, falls erforderlich.

10. **Wahlweise:** Überprüfen Sie die MID-Server-Einstellungen nach dem Importieren eines Profils.
11. **Wahlweise:** Navigieren zu **Security Operations** > **Integrationskonfigurationen**an.
12. **Wahlweise:** Wählen Sie aus Splunk Enterprise Event Ingestion Konfigurationskachel und klicken Sie auf **Aktualisieren** .
13. **Wahlweise:** Überprüfen und aktualisieren Sie die Quell- und MID-Server-Details nach Bedarf.

Kopieren Sie ein Ereignisprofil für Splunk Enterprise Event Ingestion Integration

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, sollten Sie möglicherweise Alarmprofile kopieren, um Zeit zu sparen.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Das Kopieren eines vorhandenen Profils und der zugehörigen Einstellungen ist optional.

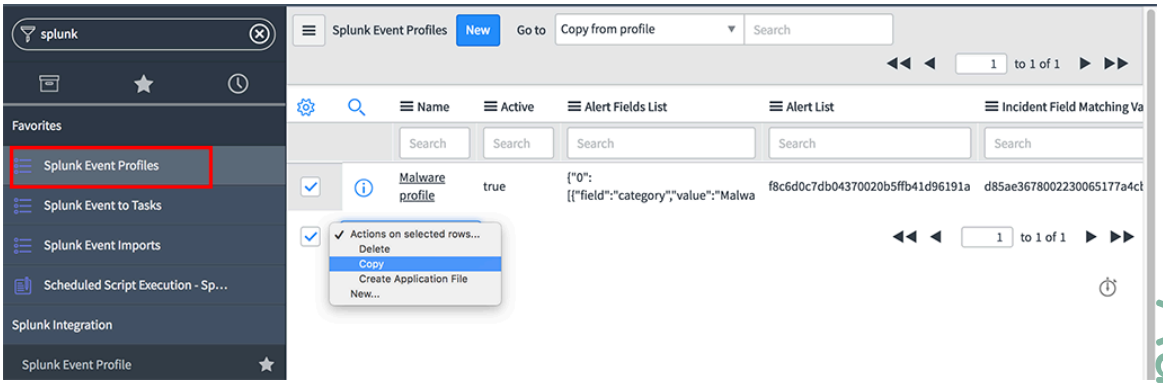
Wenn Sie ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus ist das kopierte Profil deaktiviert (falsch), sodass es vor Abschluss der Konfiguration nicht versehentlich aktiviert wird. Kopieren Sie Profile, und verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und verifiziert haben.

Automatische Übersetzung

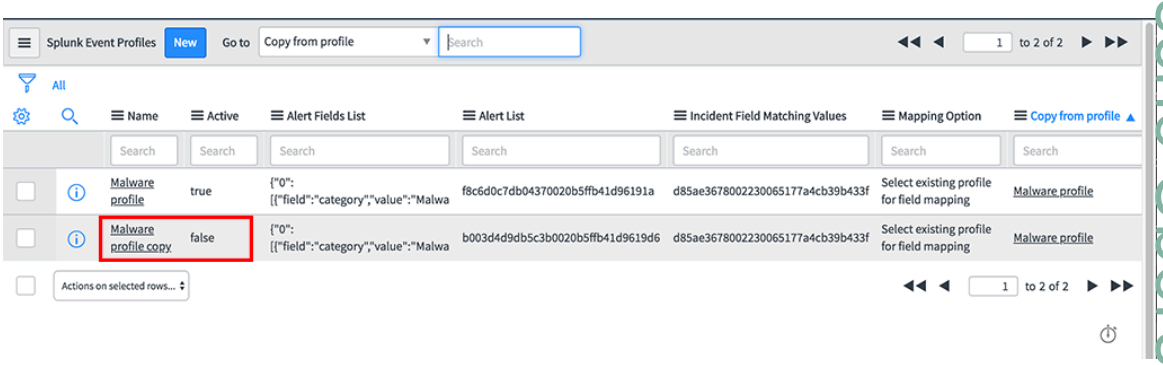
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Splunk Integration** > **Splunk-Ereignisprofil**an.
2. In Splunk Liste „Ereignisprofile“, die angezeigt wird, wählen Sie ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren** .



Das Profil wird kopiert und in der Liste angezeigt. Die Kopie verfügt über alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (Wahr), die Kopie ist zu diesem Zeitpunkt deaktiviert (Falsch). Möglicherweise möchten Sie Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf auf das neue Profil angewendet werden.



Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert.

Nächste Maßnahme

Sie werden aufgefordert, das neue Profil zu aktivieren (zu aktivieren), nachdem Sie die Konfigurationsschritte abgeschlossen haben.

Richten Sie Ihr ein Splunk Umgebung für die manuelle Ereigniserfassung für Splunk Enterprise Integration der Ereigniserfassung

Wenn Sie Ereignisse manuell und bei Bedarf aus exportieren möchten Splunk Enterprise-Konsole für diese Integration installieren und einrichten ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Anwendung in Ihrem Splunk enterprise-Konsole oder Splunk-Cloud-Instanz.

Vorbereitungen

Überprüfen Sie, ob Sie die Anwendung für diese Integration über installiert haben ServiceNow Store Vor der Installation des Add-on-Plugins aus splunkbase, das für die manuelle Ereigniserfassung erforderlich ist. Wenn Sie die Anwendung für die Integration nicht über installiert haben ServiceNow Store, Siehe Installieren und konfigurieren Sie ServiceNow

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung für Splunk Enterprise Event Ingestion Integration Und befolgen Sie die Anweisungen zur Installation.

Erforderliche Rolle: ServiceNow AI Platform Administrator (Administrator)

Warum und wann dieser Vorgang ausgeführt wird
Installieren und Einrichten von ServiceNow Addon für Security Operations-Ereigniserfassung ist optional.

Wenn Sie Ereignisse manuell und bei Bedarf aus exportieren möchten Splunk Enterprise Konsole für die -Integration herunterladen, installieren und einrichten ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Aus SPLunkbase in Ihrem Splunk Enterprise Konsole.

Dies ServiceNow Das Erweiterungs-Add-on ist erforderlich, damit Security Incidents aus manuell exportierten Ereignissen in erstellt werden können ServiceNow AI Platform Instanz. Dies ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Anwendung ist für verfügbar Splunkbase .

Für die manuelle Ereignisweiterleitung können Sie bis zu zwei verschiedene identifizieren ServiceNow AI Platform Endpunkte (Instanzen) in Ihrem Splunk Enterprise Konsole. Sie leiten die Ereignisse manuell an den Endpunkt oder Endpunkte weiter, um Security Incidents zu erstellen. Sie können beispielsweise sowohl eine Bereitstellungs-(Entwicklungs-)Instanz als auch eine Produktionsinstanz angeben. Indem Sie separate Instanzen angeben und primäre und sekundäre Workflows für jede Instanz benennen, können Sie auswählen, wohin Sie verschiedene Ereignisse weiterleiten möchten.

Prozedur

1. Wenn Sie noch nicht installiert haben ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise, Führen Sie die folgenden Schritte aus, um es zu installieren und zu konfigurieren.

   a. Navigieren Sie zu Splunkbase .

   b. Suchen Sie nach ServiceNow Security Operations Security Operations-Ereigniserfassungs-Add für Splunk Enterprise.

   Hinweis:
   Überprüfen Sie, ob Sie ausgewählt haben ServiceNow Security Operations Ereigniserfassungs-Add-on für Splunk Enterprise. Es gibt zusätzliche ServiceNow add-ons, die in dieser Liste angezeigt werden. Diese Add-ons sind für verschiedene bestimmt ServiceNow Splunk Integrationen und sind für diese Integration nicht erforderlich.

   c. Laden Sie die Anwendung herunter.

   d. Öffnen Sie Ihren Splunk Enterprise Account.

   e. Klicken Sie auf der Seite „Apps“ auf das Zahnradsymbol oder auf **Apps Verwalten** Verknüpfung in der Dropdown-Liste des Menüs.

   f. Klicken Sie oben links auf der angezeigten App-Seite auf **Installieren Sie die App aus der Datei** .

   g. Klicken Sie Auf **Wählen Sie Datei** , Wählen Sie aus ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise, Und klicken Sie auf **Hochladen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Starten Sie bei Aufforderung neu Splunk Enterprise.
Die ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Ist in installiert Splunk Enterprise enterprise-Konsole. Der nächste Schritt zum Einrichten des Add-ons.

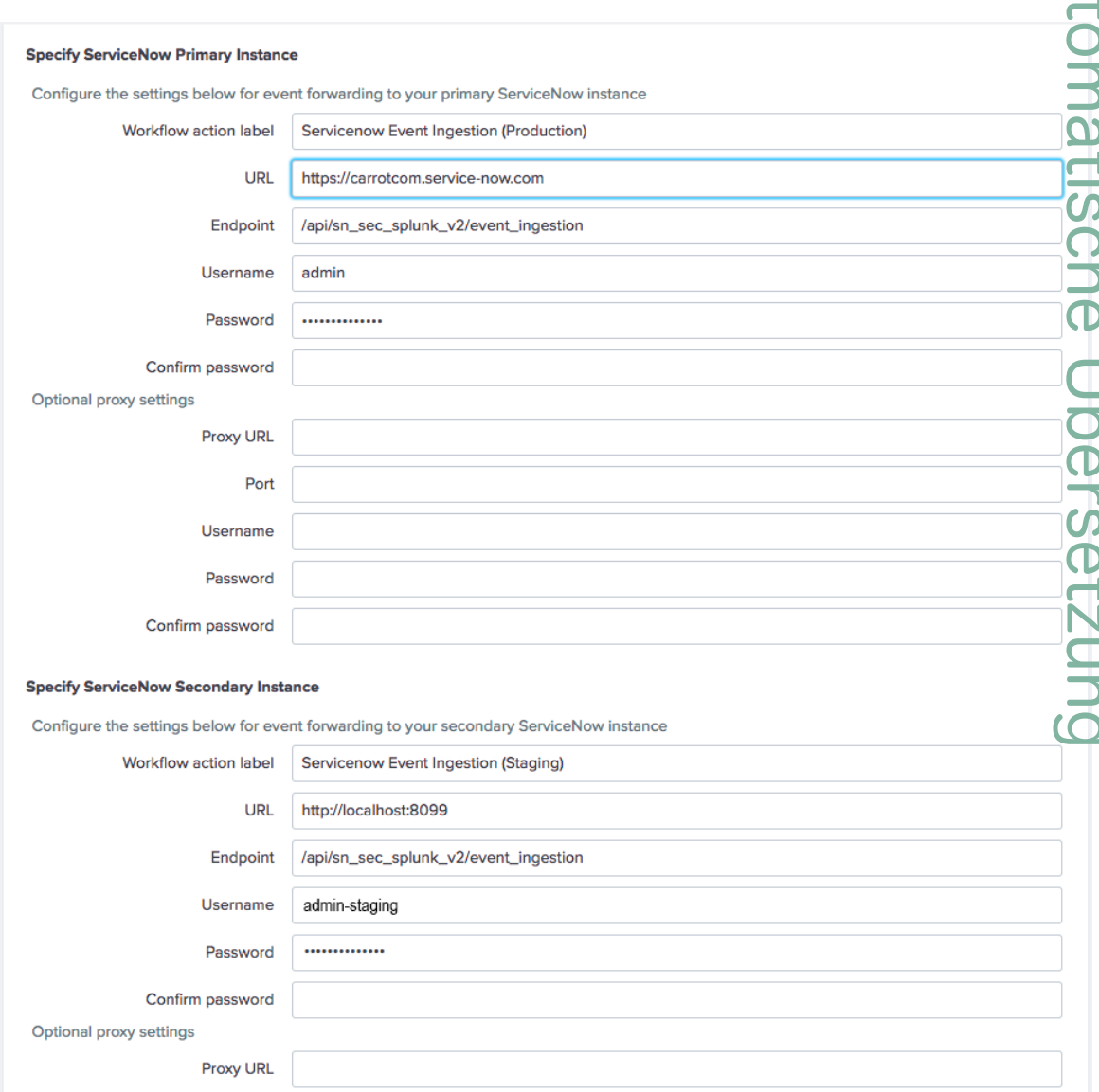
2. Führen Sie die folgenden Schritte aus, um das Add-on einzurichten.

a. In Splunk Enterprise, Klicken Sie auf **Apps** Zahnradsymbol oder **Apps Verwalten** In der Dropdown-Liste des Menüs.

b. In der Liste der Anwendungen, die in angezeigt wird **Aktionen** Klicken Sie auf die Spalte **Einrichten** Für ServiceNow Security Operations Ereigniserfassungs-Add-on für Splunk Enterprise.

c. Füllen Sie das Formular aus.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular in Ihrem Splunk Enterprise Konsole.

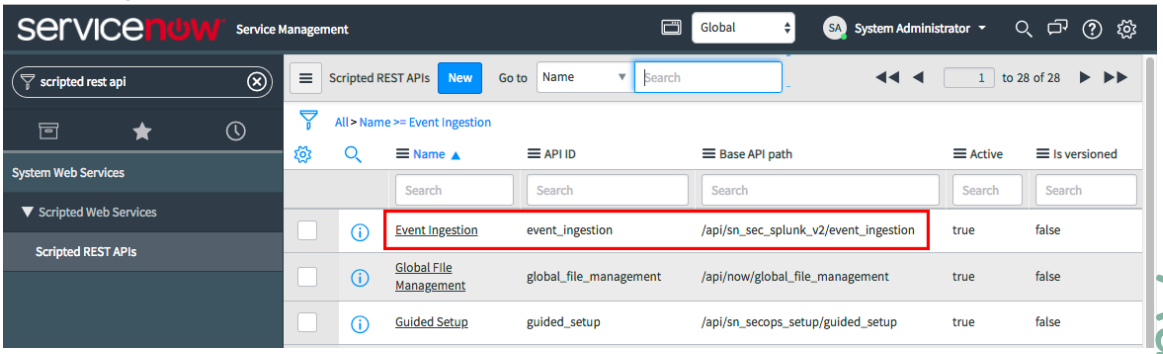


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung ist ein Beispiel für die Liste geskriptete REST APIs in Ihrem ServiceNow AI Platform. In der Liste wird die Position des Endpunktwerts von angezeigt ServiceNow AI Platform Instanz, die Sie im Rahmen der Einrichtung für in das Formular eingeben ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Erweiterung in Ihrem Splunk Enterprise Konsole.

Liste der geskripteten REST-APIs in ServiceNow AI Platform



3. Im Setup-Formular in Ihrem Splunk Enterprise Konsole, klicken Sie auf **Speichern** Um Ihre Änderungen zu speichern.

   Nach einigen Minuten oben links im Formular in Ihrem Splunk Enterprise Konsole wird eine Nachricht angezeigt, dass der Datensatz erfolgreich aktualisiert wurde.

   Nachdem Sie das Formular gespeichert haben, werden die Namen (Workflow-Aktionsbezeichnungen) für gespeichert ServiceNow AI Platform Instanzen, die Sie im Formular erstellt haben, sind in der Auswahlliste Ereignisaktionen für ein ausgewähltes Ereignis einer Suche in verfügbar Splunk Enterprise Konsole.

Nächste Maßnahme

Wenn Sie Suchvorgänge noch nicht in gespeichert haben Splunk Enterprise-Konsole besteht der nächste Schritt darin, Suchvorgänge als Warnungen in Ihrer zu speichern Splunk Enterprise Konsole.

Speichern Sie Suchvorgänge in Splunk Enterprise-Konsole für Splunk Enterprise Event Ingestion Integration

Die folgenden Schritte zum Speichern von Suchen in Ihrem Splunk Enterprise-Konsole wird für einen Anwender mit bereitgestellt Splunk Enterprise Administratorrolle.

Vorbereitungen

Wenn Sie bereits gespeicherte Suchen und ausgelöste Warnungen in Ihrem haben Splunk Enterprise Konsole, müssen Sie diese Suchvorgänge für diese Integration nicht ändern.

Die Integration von ServiceNow AI Platform® Security Operations Produkt mit Splunk Der Ereignisbenachrichtigungsservice ruft Ereignis- und Warnungsinformationen aus ab Splunk.

Bevor Warnungen in erfasst werden Security Operations Umgebung, konfigurieren Sie Suchen in Ihrer Splunk Enterprise Konsole, damit Sie die relevanten Sicherheitsereignisse automatisch in abrufen können Splunk Enterprise Die Sie als Warnungen speichern möchten.

Wenn Sie keine gespeicherten Suchen und ausgelösten Warnungen für die Benachrichtigung eingerichtet haben, wenn wichtige Sicherheitsereignisse in auftreten Splunk Enterprise Konsole führen Sie die folgenden Schritte aus, um Suchvorgänge zu speichern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Splunk Enterprise Administrator

Prozedur

1. Melden Sie sich bei Ihrem Splunk Enterprise-Konto an.
2. Klicken Sie auf **Suchen** Registerkarte.
3. Geben Sie im angezeigten Feld neue Suche einen Wert für die Warnung ein, z. B. Malware.
4. Um die Ereignisse im Zusammenhang mit Ihrer Suche anzuzeigen, klicken Sie rechts neben dem Feld neue Suche auf das Suchsymbol, oder drücken Sie die Eingabetaste.
   Die Suchergebnisse mit Ereignissen werden angezeigt.
5. Um die Suche als Warnung zu speichern, erweitern Sie oben rechts auf der Seite die Auswahlliste Speichern als, und wählen Sie aus **Warnung** .
6. Füllen Sie die Felder im angezeigten Formular aus.
7. Klicken Sie auf **Speichern**.
   Ihre Warnung wird gespeichert und auf der Registerkarte Warnungen auf der Suchseite angezeigt.
   Die Splunk Der Service ruft die Ereignisse ab, indem er den Kriterien entspricht, die Sie in der Warnung konfiguriert haben. Die Ereignisse werden zwischengespeichert, und Sie fordern diese Ereignisse dann aus Ihren Profilen an, die Sie in eingerichtet haben ServiceNow AI Platform Instanz. Da der Abruf von Ereignissen aus einem Cache in erfolgt Splunk Service, diese Erfassung von Ihrem ServiceNow AI Platform Hat keine Auswirkungen auf die Leistung von Splunk Plattform.

Nächste Maßnahme

Sie haben das erforderliche Setup für die Integration in erfolgreich abgeschlossen Splunk Enterprise Konsole. Wenn Sie die Anwendung für die Integration noch nicht über installiert haben ServiceNow Store, Der nächste Schritt besteht darin, die Anwendung für die Integration zu installieren und zu konfigurieren.

Verwenden Sie den Skript-Editor, um Warnungswerte für zu formatieren Splunk Enterprise Event Ingestion Integration

Verwenden Sie den Skript-Editor, um Feldwerte für den Security Incident während des Zuordnungsschritts zu formatieren.

Vorbereitungen

Zusätzlich zu den direkt zugeordneten Feldern aus den abgerufenen Warnungswerten und den Warnungswerten, die Sie manuell eingeben, können Sie optional den Skript-Editor verwenden, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren. Der Skripteditor ändert die Werte von Splunk Warnung, damit Werte, die von unterstützt werden ServiceNow AI Platform® Security Incident Response Security Incidents werden den Feldern Kategorie, Konfigurationselement (CI) und erkennbares Element zugeordnet.

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

In bestimmten Fällen Splunk Enterprise Warnungswerte werden den Feldern Kategorie, Konfigurationselement (CI) und erkennbares Element in zugeordnet SIR Incident und werden nicht unterstützt. Möglicherweise möchten Sie die zugeordneten Werte bearbeiten. Wenn

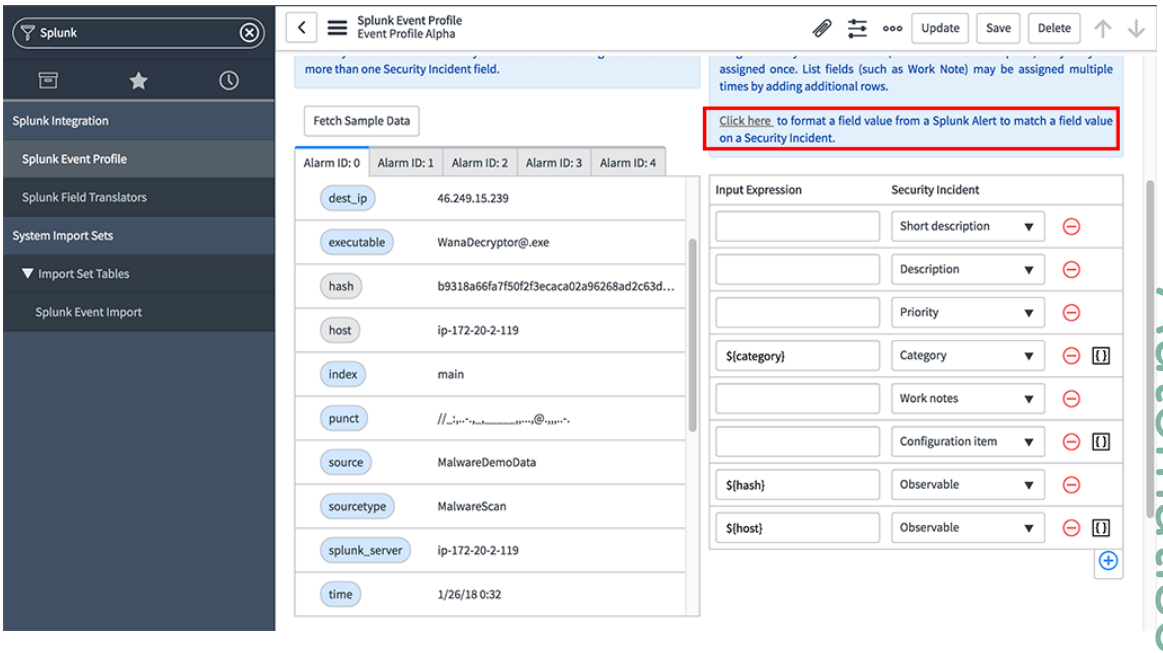
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie den Wert von übersetzen möchten Splunk Enterprise Warnung zu einem Wert, der von diesen Feldern auf unterstützt wird SIR Security Incident verwenden Sie den Skript-Editor.

Prozedur

1. Klicken Sie bei angezeigtem Zuordnungsformular auf den Link, um den Skript-Editor zu öffnen.

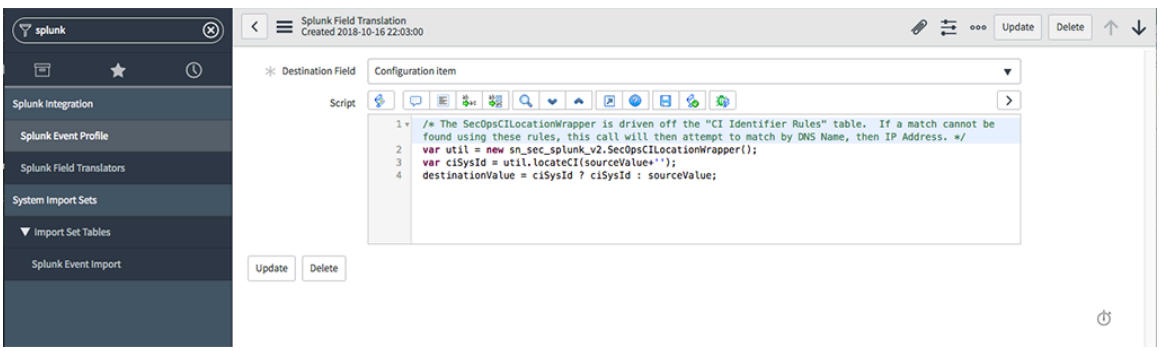


2. Wählen Sie in der Auswahlliste ein Zielfeld für den Wert aus, den Sie bearbeiten möchten.
3. Alternativ können Sie im Abschnitt SIR-Incident-Feldzuordnung auf das Klammern-Symbol klicken [{}] Neben einem Feld, um den Skripteditor für dieses Feld zu öffnen.

   In bestimmten Fällen kann eine Skripteinbindung für das Feld Konfigurationselement geeignet sein. Für eine Warnung kann beispielsweise kein Wert für das Konfigurationselement übereinstimmen.

   Wie in der folgenden Abbildung gezeigt, kann eine Übereinstimmung für einen Hostnamen nicht in gefunden werden ServiceNow AI Platform® CMBD für das Feld Konfigurationselement können Sie die Regel so bearbeiten, dass, wenn eine IP-Adresse gefunden wird, das Feld Konfigurationselement ausgefüllt wird. Wenn für den Alarm kein Wert vorhanden ist, wird das Feld im Security Incident auf null festgelegt.

   Der Editor wird geöffnet, wobei das Feld im Zielfeld angezeigt wird. Die folgende Abbildung zeigt den Editor mit Konfigurationselement Feld als Zielfeld.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie alle Änderungen am Skript ein, und klicken Sie auf **Aktualisieren** Um Ihre Änderungen zu speichern.
   Die Splunk Die Tabelle „Feldübersetzungen“ wird angezeigt.
5. Schließen Sie die Tabelle, um zum Zuordnungsformular zurückzukehren.

Prüfliste für Splunk Enterprise Event Ingestion Integration

Verwenden Sie diese Prüfliste, um Sie durch alle Aufgaben der Integration zu führen. Die folgende Prüfliste enthält Setup- und Installationsaufgaben sowie Beispiele für Anwendungsfälle, die die erwarteten Ergebnisse für die Integration enthalten.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Verfolgen Sie Ihren Fortschritt beim Setup, der Installation und der Konfiguration der Integration mit der folgenden Tabelle. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren. Jede Zeile der Tabelle listet Aufgaben auf und gibt die Rollen an, die zur Ausführung der Aufgaben erforderlich sind. Nummerierte Themen des Installations- und Konfigurationsleitfadens werden ebenfalls referenziert.

Erforderliche Rollen: Rollen werden für jeden Schritt unten aufgeführt.

Prozedur

1. Als Anwender mit ServiceNow AI Platform administratorrolle, richten Sie Ihr ein ServiceNow AI Platform Instanz.
   - Weisen Sie Anwender mit zu **sn_si.ingestion_profile_admin** (Oder sn_si.admin) und sn_si.Analyst-Rollen nach Bedarf.
   - Installieren und konfigurieren Sie einen MID-Server, wenn dies der Fall ist Splunk Server wird in Ihrem Unternehmensnetzwerk bereitgestellt.
   - Überprüfen Sie, ob ServiceNow Security Incident Response Plugins werden für Ihr Release von aktiviert ServiceNow AI Platform.
   - Wenn Sie Ereignisse manuell von Ihrem weiterleiten möchten Splunk Enterprise-Konsole in Ihrem ServiceNow AI PlatformÜberprüfen Sie, ob Sie einem Anwender mit die Rolle (sn_sec_splunk_v2.api_Account_Access) zugewiesen haben Splunk Enterprise enterprise-Administratorberechtigung.

   Weitere Informationen finden Sie unter Richten Sie Ihr ein ServiceNow AI Platform Instanz für Splunk Enterprise Event Ingestion Integration.

   Sie haben die Einrichtungsschritte erfolgreich abgeschlossen und die erwarteten Ergebnisse für die Integration verifiziert.
2. Als Anwender mit ServiceNow AI Platform administratorrolle installieren und konfigurieren Splunk Enterprise Event Ingestion Anwendung aus dem ServiceNow Store.
   a. Laden Sie die Anwendung herunter, und installieren Sie sie auf Ihrem ServiceNow AI Platform Instanz.
   b. Konfigurieren Sie die Anwendung, und stellen Sie eine Verbindung mit her Splunk Enterprise Konsole.

   Weitere Informationen finden Sie unter Installieren und konfigurieren Sie ServiceNow Anwendung für Splunk Enterprise Event Ingestion Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. **Wahlweise:** Wenn Sie Ereignisse manuell aus exportieren möchten Splunk Enterprise-Konsole zu Ihrem ServiceNow AI Platform Führen Sie die folgenden Aufgaben aus:

   a. Als Splunk Enterprise Administrator, installieren, einrichten und aktivieren ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Aus SPLunkbase in Ihrem Splunk Enterprise Konsole.

   b. Als Splunk Enterprise Administrator, falls nicht bereits konfiguriert, speichern Sie Suchen als Warnungen in Ihrem Splunk Enterprise Konsole.

   (Optional) Weitere Informationen finden Sie unter Richten Sie Ihr ein Splunk Umgebung für die manuelle Ereigniserfassung für Splunk Enterprise Integration der Ereigniserfassung und Speichern Sie Suchvorgänge in Splunk Enterprise-Konsole für Splunk Enterprise Event Ingestion Integration.

4. Als Anwender mit ServiceNow AI Platform **sn_si.ingestion_profile_admin** Rolle, erstellen und benennen Sie ein Ereignisprofil.

   Wählen Sie den Profiltyp aus der Auswahlliste aus. Optionen sind ein geplantes Warnungsprofil, das Sie zum Erfassen von Beispieldaten verwenden, oder ein Ereignisprofil, das Sie zum manuellen Exportieren von Anhangsdaten aus Ihrem verwenden Splunk Enterprise Konsole.

   - Wählen Sie für eine geplante Warnung eine verfügbare Warnung aus.
   - Erstellen Sie für ein Profil für manuell exportierte Daten eine neue Zuordnung, oder kopieren Sie eine vorhandene Zuordnung.

   Weitere Informationen finden Sie unter Erstellen und benennen Sie ein Ereignisprofil.

5. Als Anwender mit ServiceNow AI Platform **sn_si.ingestion_profile_admin** Rolle, Zuordnungswerte, die erfasst wurden, oder Anhangsdaten, die aus exportiert werden Splunk Enterprise Bis ServiceNow AI Platform Security Incidents.

   a. Ruft Beispieldaten für eine geplante Warnung ab.

   b. Exportieren Sie Anhangsdaten manuell aus Splunk Enterprise Für ein Ereignis.

   c. Bearbeiten Sie die Standardzuordnungskonfiguration.

   d. Fügen Sie optional Filterkriterien hinzu, fügen Sie eine Warnung an einen vorhandenen Security Incident an, und verwenden Sie den Skripteditor.

   Weitere Informationen finden Sie unter Zuordnung von Warnungen und Ereignissen für Splunk Enterprise Event Ingestion Integration und Ordnen Sie Warnungen für zu Splunk Enterprise Event Ingestion Integration.

6. Als Anwender mit ServiceNow AI Platform **sn_si.ingestion_profile_admin** Rolle, zeigen Sie eine Vorschau der Daten von an Splunk Enterprise Die auf einer angezeigt wird ServiceNow AI Platform Security Incident.

   Beheben Sie Fehler, oder fügen Sie fehlende Daten hinzu, damit keine Fehlermeldungen angezeigt werden.

   Weitere Informationen finden Sie unter Vorschau des Security Incidents für anzeigen Splunk Enterprise Event Ingestion Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Als Anwender mit ServiceNow AI Platform **sn_si.ingestion_profile_admin** Rolle: Planen Sie den Warnungsabruf für ein Profil mit einer geplanten Warnung.

   Weitere Informationen finden Sie unter Planen und rufen Sie Warnungen für ab Splunk Enterprise Event Ingestion Integration.

Splunk Enterprise Security Integration der Ereigniserfassung

Die Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung mit Security Incident Response(SIR) Mit dem Produkt können Security Incident-Analysten wichtige Ereignisdaten erfassen und verarbeiten (als beachtliche Ereignisse bezeichnet).

Übersicht über Splunk Enterprise Security Integration der Ereigniserfassung

Daten werden kontinuierlich basierend auf einem konfigurierten Abfragungsplan erfasst und von Analysten verwendet, um potenzielle Cyberbedrohungen zu identifizieren und darauf zu reagieren. Gesammelte Sicherheitsereignisse können in zu bedeutenden Ereignissen korreliert werden Splunk Enterprise Security Und wird dann automatisch mit dieser Integration erfasst. Außerdem können einzelne wichtige Ereignisse bei Bedarf manuell vom weitergeleitet werden Splunk Enterprise Security Incident-Überprüfungskonsole und Berichterstellungsschnittstelle in die Security Incident Response Produkt von ServiceNow AI Platform Dient zum Erstellen von Security Incidents.

Diese Integration bietet einem Analysten des Security Operations Center (SOC) Einblick in wichtige Ereignisse und zugehörige beitragende Ereignisdaten. Diese Daten können in integriert werden ServiceNow AI Platform Security Incident Response(SIR) Security Incidents zur weiteren Untersuchung und Korrektur. Profile werden in erstellt ServiceNow AI Platform Instanz zur Verarbeitung verschiedener wichtiger Ereignistypen, die über Korrelationssuchen in erstellt werden Splunk Enterprise Security. Diese Profile passen den Unterschied an Splunk Ereignisfelder werden in angezeigt SIR Security Incidents.

Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Erstellen Sie mehrere wichtige Ereigniserfassungsprofile, um SIR Security Incidents für bestimmte Arten von Bedrohungen wie Phishing und Malware und nicht autorisierte Zugriffsversuche zu erstellen.
- Erstellen Sie mehrere Ereignisprofile für die Ereignisweiterleitung bei Bedarf von Ihrem Splunk ES Incident-Überprüfungskonsole zum Erstellen von SIR Security Incidents.
- Drag-and-Drop-Zuordnung von Splunk Wichtige Ereignisfeldwerte zu zugehörigen SIR Security Incident-Feldern.
- Eine Vorschau von SIR Security Incident-Layout basierend auf Beispielereignissen zur Validierung der Ereigniszuordnungsdetails.
- Erfassen Sie wichtige historische Ereignisse sowie laufende, neue und aktualisierte wichtige Ereignisse in konfigurierbaren Intervallen.
- Filtern Sie wichtige Ereignisse heraus, die die SIR-Incident-Generierungskriterien nicht erfüllen, z. B. Ereignisse mit niedriger Priorität, Ereignisse, die noch einen bestimmten Status erreichen müssen usw.
- Ereignisse oder Warnungen in vorhandenen aggregieren SIR Security Incidents basierend auf übereinstimmenden Feldwerten, um doppelte Security Incidents zu vermeiden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktualisieren Sie wichtige Ereignisse basierend auf SIR-Incident-Erstellungs- und/oder Abschlussbedingungen über eine bidirektionale Schnittstelle, um sie beizubehalten Splunk ES Wichtige Ereignisaktualisierungen werden synchronisiert mit aktualisiert ServiceNow SIR-Incident-Status.

Unterstützt ServiceNow AI Platform Versionen

Das Plugin com.snc.si_dep ist für diese Integration erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Anwendungen.

Folgendes Security Operations Anwendungen müssen über installiert und aktiviert werden ServiceNow Store. Installieren und aktivieren Sie jeweils eine Anwendung in der unten aufgeführten Reihenfolge, um eine reibungslose Installation sicherzustellen:

1. Sicherheits-Integrations-Framework
2. Security Support Common
3. Security Incident Response

Weitere Informationen zur Installation von finden Sie Security Operations Kernanwendungen, siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

ServiceNow Zusätze

Die ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk ES Ist nur erforderlich, wenn Sie Ereignisse manuell von Ihrem weiterleiten möchten Splunk Enterprise Security Incident-Überprüfungskonsole in Ihrem ServiceNow AI Platform Instanz. Dies ServiceNow Add-on ist in verfügbar Splunkbase .

Dies ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Anwendung in splunkbase ist für die automatisierte Warnungserfassung, die von der Integration unterstützt wird, nicht erforderlich.

Von Splunk unterstützte Versionen

Diese Integration wurde mit getestet Splunk Enterprise Version 8.0.1 und mit Splunk Enterprise Security Anwendungsversion 6,2.1.

MID-Server

Diese Integration erfordert einen installierten und konfigurierten MID-Server in Ihrem ServiceNow AI Platform® Instanz, die mit verbunden werden soll Splunk Service, wenn Splunk Server wird in Ihrem Unternehmensnetzwerk bereitgestellt. Wenn Sie verwenden Splunk Cloud Service, ein MID-Server ist nicht erforderlich. Siehe MID-Server Weitere Informationen zu MID-Servern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Referenzen

Referenz	Dokumentbezeichner	Dokumententitel
1	Splunk Produkt-Website	Splunk Enterprise Security-Produkt-Website .

Prüfliste

Eine druckbare Prüfliste dieser Themen finden Sie unter Prüfliste für Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung. Sie können diese Liste verwenden, um Ihren Fortschritt bei der Bearbeitung der Aufgaben der Integration zu überwachen.

Schlüsselbegriffe, die in dieser Integration verwendet werden

In diesem Abschnitt werden einige der Schlüsselbegriffe beschrieben, die in dieser Integration verwendet werden.

Die folgenden Schlüsselbegriffe werden während der Installation und Konfiguration verwendet. Weitere Informationen zu diesen Begriffen finden Sie unter ServiceNow-Produktdokumentationswebsite Und Splunk-Website Und -Ressourcen auf Splunk-Ressourcen Seite.

ServiceNow AI Platform

Ein Unternehmen ServiceNow Produkt. Die ServiceNow AI Platform Ist die Basis, auf der einzelne Komponenten wie basieren Security Incident Response(SIR), IT Service Management (ITSM) und andere Produkte werden erstellt.

ServiceNow Splunkbase-Add

A ServiceNow Anwendung, die auf installiert ist Splunk Enterprise Security Konsole, die die manuelle Ereignisweiterleitungsoption der Integration unterstützt. Die manuelle Ereignisweiterleitung ist eine optionale Funktion der Integration. Dies ServiceNow Das Splunkbase-Add-on ist für die automatisierte Erfassung bedeutender Ereignisse nicht erforderlich, die von der Integration bereitgestellt wird, aus der Ereignisse abgerufen werden Splunk.

Security Incident Response (SIR)

A ServiceNow AI Platform Anwendung, die den Fortschritt von Security Incidents von der Erkennung und ersten Analyse über die Eindämmung, Beseitigung und Wiederherstellung bis hin zur endgültigen Überprüfung und Schließung von Security Incidents nachverfolgt.

Splunk Enterprise Security

Splunk Enterprise Security Hilft Teams, organisationsweite Transparenz und Security Intelligence für kontinuierliche Überwachung, Reaktion auf Incidents, SOC-Vorgänge zu erhalten und Führungskräften ein Fenster in das Geschäftsrisiko zu bieten. Splunk Enterprise Security Ist eine Premium-Sicherheitslösung, die eine kostenpflichtige Lizenz erfordert. Dieser Service befindet sich auf einem Host oder einem Splunk-Cloud-Angebot, das als bezeichnet wird SplunkKonsole in diesem Handbuch.

Splunk Enterprise Security Bemerkenswertes Ereignis

Wenn eine Korrelationssuche ein Ereignis oder ein Muster von Ereignissen identifiziert, wird ein bemerkenswertes Ereignis erstellt. Korrelationssuchen filtern die Sicherheitsdaten und korrelieren über Ereignisse hinweg, um einen bestimmten Incident-Typ (oder ein Muster von Ereignissen) zu identifizieren, und erstellen dann wichtige Ereignisse.

Splunk Termin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein oder mehrere Datenelemente, die zu den bedeutenden Ereignissen von führen Splunk Service. Von Ihrem ServiceNow AI Platform Instanz können Sie nachschlagen, welche Splunk Ereignisse ausgelöst ServiceNow AI Platform Security Incidents.

MID-Server

Diese Anwendung erleichtert die Kommunikation und das Verschieben von Daten zwischen ServiceNow AI Platform Und externe Anwendungen, Datenquellen und Services. Diese Anwendung ist normalerweise für die Integration mit lokalen Technologien und erforderlich Splunk Enterprise Security Integration der Ereigniserfassung erleichtert der MID-Server die Kommunikation zwischen ServiceNow AI Platform Und die lokale Instanz von Splunk Enterprise Security. Ein MID-Server ist nicht erforderlich, wenn Sie Ihren integrieren ServiceNow AI Platform Instanz mit Splunk Cloud Instanz.

Security Incident-Administrator (sn_si.admin)

Der Anwender mit dieser Rolle überwacht die Konfiguration der Integration mit SIR Produkt in Ihrem ServiceNow AI Platform Instanz.

Security Incident-Analyst (sn_si.Analyst)

Der Anwender mit dieser Rolle interagiert mit Security Incidents in und analysiert sie ServiceNow Security Incident Response Produkt.

Richten Sie Ihr ein ServiceNow AI Platform® Instanz für Splunk Enterprise Security Integration

Im folgenden Abschnitt werden die Setup-Aufgaben aufgeführt, die Sie in ausführen müssen ServiceNow AI Platform® Instanz vor der Installation der Anwendung über ServiceNow Store.

Erforderliche Rolle: sn_si.ingestion_profile_admin.

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Überprüfen Sie anhand der folgenden Tabelle, ob Sie alle aufgeführten Aufgaben abgeschlossen haben, bevor Sie die Anwendung herunterladen und installieren, um eine reibungslose Installation und Konfiguration zu gewährleisten.

1. Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform® Und Security Incident Response(SIR) Rollen.

   Die folgenden Rollen sind für die Installation, das Setup und die Verwendung der Integration in erforderlich ServiceNow AI Platform® Instanz.

   - Ein Anwender mit ServiceNow AI Platform® Die Administratorrolle (admin) installiert die Anwendung aus dem ServiceNow Store Und weist die Rolle Security Incident-Administrator (sn_si.admin) zu.
   - Wenn Sie wichtige Ereignisse manuell von weiterleiten möchten Splunk Enterprise Security Für diese Integration ein Anwender mit ServiceNow AI Platform® Die administratorrolle weist einem Anwender die Rolle (sn_sec_splunkes.api_Account_Access) in zu ServiceNow AI Platform®. Diese Rolle ermöglicht einem Anwender die Verwendung von Splunk Enterprise Security Administratorrolle für den Zugriff auf die API in ServiceNow AI Platform® Dies ist für die manuelle Ereignisweiterleitung für diese Integration erforderlich.

     Die Rolle (sn_sec_splunkes.api_Account_Access) ist für die Integration nicht erforderlich, wenn Sie wichtige Ereignisse automatisch aus erfassen Splunk Enterprise Security In Ihren ServiceNow AI Platform® Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Anwender mit **sn_si.ingestion_profile_admin** Die Rolle überwacht die folgenden Aufgaben in ServiceNow AI Platform®:
  - Benennt, erstellt und bearbeitet Ereignisprofile.
  - Wählt Werte aus und ordnet sie zu Splunk Enterprise Security Bis ServiceNow AI Platform® Security Incidents.
  - Zeigt vor dem Abschluss der Konfiguration eine Vorschau der Security Incident-Details auf Richtigkeit an.
  - Plant die laufende Erfassung wichtiger Ereignisse.
  - Aktiviert Aktualisierungen wichtiger Ereignisse, wenn ein SIR-Incident erstellt und geschlossen wird.
  - Weist die Rolle Security Incident Analyst (sn_si.Analyst) zu.
  - Anwender mit sn_si.Analyst arbeiten mit Security Incidents.

Weitere Informationen finden Sie unter Managing roles .

2. Weisen Sie zu Splunk Anwenderrolle.

   Weisen Sie in eine Sicherheitsanalyst-Anwenderrolle (ess_Analyst) zu Splunk Es, um alle integrationsbezogenen Aktivitäten für durchzuführen Splunk Server.

3. Stellen Sie sicher, dass Sie Version 7.2.6 oder höher von verwenden Splunk API. Frühere Versionen werden nicht unterstützt.

   Wenn Sie Zugriff auf haben Splunk Enterprise Security Konsole haben Sie Zugriff auf die API, die für diese Integration erforderlich ist. Für die API ist kein anderes spezielles Setup erforderlich.

4. Überprüfen Sie, ob Sie einen MID-Server installiert und konfiguriert haben.

   A MID-Server In Ihrem ServiceNow AI Platform® Instanz ist erforderlich, um eine Verbindung mit herzustellen Splunk Service, wenn Splunk Server wird in Ihrem Unternehmensnetzwerk bereitgestellt. Informationen finden Sie unter MID-Server .

   Wenn Sie verwenden Splunk Enterprise Security Cloud-Service, A MID-Server Ist nicht erforderlich.

5. Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert.

   Die Security Incident Response Abhängigkeits-Plugin (com.snc.si_dep) ist erforderlich. Dieses Plugin installiert automatisch alle Abhängigkeiten, die zur Unterstützung von erforderlich sind Security Incident Response Produkt. Installieren und aktivieren Sie dieses Plugin, bevor Sie das andere installieren und aktivieren Security Operations Für die Integration erforderliche Anwendungen.

   Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Security Incident Response

b. Sicherheits-Integrations-Framework

c. Sicherheitssupport Allgemein

Weitere Informationen zur Installation von finden Sie Security Operations Kernanwendungen, siehe Berechtigung für abrufen Security Operations Produkt oder Anwendung Und Aktivieren Sie einen ServiceNow Store Anwendung.

Sie haben erfolgreich eingerichtet ServiceNow AI Platform® Instanz für die Integration. Der nächste Schritt besteht in der Installation von Splunk Enterprise Security Anwendung zur Erfassung von bemerkenswerten Ereignissen aus der ServiceNow Store Für die Integration. Weitere Informationen finden Sie unter Installieren und konfigurieren Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung.

Wenn Sie wichtige Ereignisse manuell und bei Bedarf aus exportieren möchten Splunk Enterprise Security Konsole für die Integration finden Sie unter Richten Sie Ihr ein Splunk Umgebung für die manuelle Ereigniserfassung für Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung Weitere Informationen finden Sie unter .

Installieren und konfigurieren Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung

Bevor Sie die Integration für ausführen ServiceNow AI Platform® Führen Sie diese Installations- und Konfigurationsschritte aus, damit die Anwendung ordnungsgemäß in integriert wird Security Incident Response Und Security Operations Produkte auf Ihrem ServiceNow AI Platform® Instanz.

Vorbereitungen

Erforderliche Rolle: ess_Analyst

Weisen Sie in Splunk es eine Anwenderrolle „Sicherheitsanalyst“ (ess_Analyst) zu, um alle integrationsbezogenen Aktivitäten auf dem Splunk-Server auszuführen.

Prozedur

1. Wenn Sie den nicht installiert haben Splunk Enterprise Security Ereigniserfassungsanwendung aus dem ServiceNow Store Informationen zur Integration finden Sie unter Installieren Sie ein Security Operations Integration Und führen Sie die Schritte aus, um es zu installieren.
2. Nachdem Sie die Anwendung erfolgreich installiert haben, navigieren Sie zu **Integrationen** > **Integrationskonfigurationen** Und suchen Sie Splunk Kachel „Ereigniserfassungen“.
3. Klicken Sie auf , um die Anwendung zu konfigurieren **Neu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Alternativ, wenn ein **Konfigurieren** Die Schaltfläche wird auf einer Kachel angezeigt. Klicken Sie darauf, um eine vorhandene Konfiguration zu bearbeiten.
5. Füllen Sie die Felder im angezeigten Dialogfeld „Konfiguration der Ereigniserfassungen“ aus.

   Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für eine Konfiguration einer lokalen Version von Splunk Enterprise Security Mit einem MID-Server.

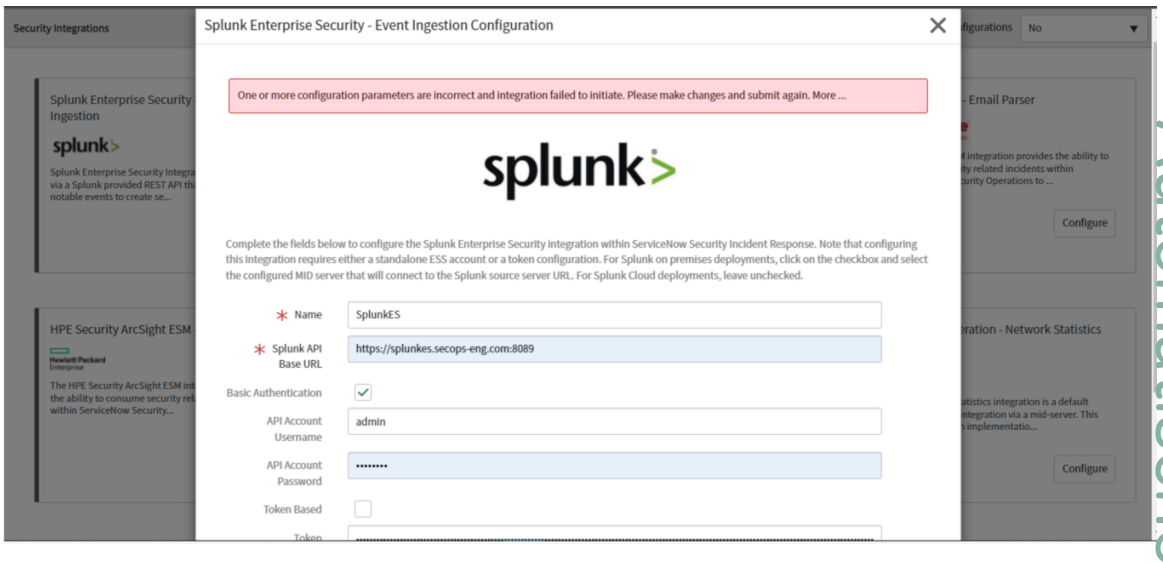
   Jeweils Splunk Enterprise Security Bemerkenswerter Ereignistyp, den Sie aus erfassen Splunk Enterprise Security Die Incident-Überprüfungskonsole erfordert ein eindeutiges Ereignisprofil in Ihrem ServiceNow AI Platform® Instanz. Die Quelle, die Sie im Formular „Konfiguration der Ereigniserfassungen“ konfigurieren, kann jedoch für mehrere wiederverwendet werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow AI Platform® Profile, solange jedes Profil eindeutige wichtige Ereignistypen erfasst.

6. Klicken Sie auf **Absenden**.
   Nachdem die Validierung erfolgreich abgeschlossen wurde, wird die Seite „Sicherheitsintegrationen“ mit jeder Ihrer Konfigurationen angezeigt. Auf jeder gültigen Konfigurationskachel **Aktualisieren** Und **Löschen** Schaltflächen werden wie in der folgenden Abbildung angezeigt.

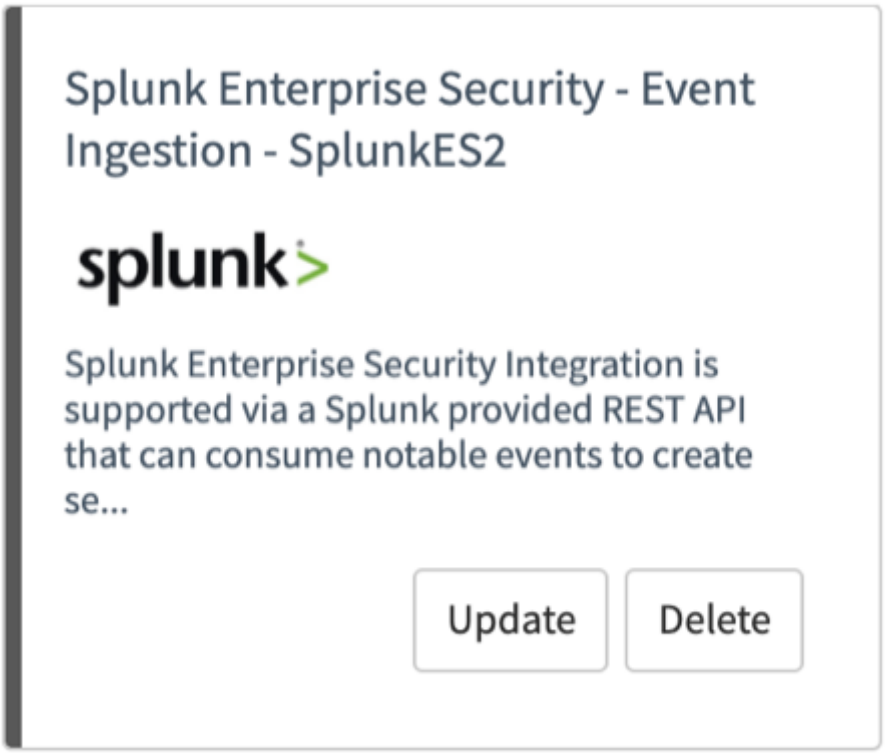
Hinweis:
Anwender müssen entweder die Standardauthentifizierung oder die Token-basierte Authentifizierung verwenden. Wenn Sie beide aktivieren, wird der folgende Fehler ausgegeben.



Hinweis:
Wenn Anwender die vorhandenen Konfigurationskacheln auf tokenbasiert aktualisieren möchten, müssen sie diese Einstellung aktivieren, um vorhandene zu aktualisieren Splunk Quellkonfigurationen für die Einstellung zur Unterstützung der tokenbasierten Authentifizierung in Splunk Modul „Enterprise-Einstellungen“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nachdem es erfolgreich validiert und übermittelt wurde, werden alle Ereigniserfassungen durchgeführt Splunk Die Serverkonfiguration wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert. Wenn Ihre gespeicherten Konfigurationskacheln nicht auf der Seite „Sicherheitsintegrationen“ angezeigt werden, wählen Sie in der oberen rechten Ecke der Seite in der Liste Konfigurationen anzeigen die Option aus **Ja** .

Nächste Maßnahme

Sie haben die Anwendung erfolgreich installiert und konfiguriert. Der nächste Schritt besteht darin, ein Ereignisprofil zu erstellen.

Konfigurieren Splunk Enterprise-Sicherheitseinstellungen

Verwenden Sie Splunk Enterprise Security (es)-Einstellungen zum Ändern der voreingestellten Konfigurationen und ihrer Werte gemäß Ihren Anforderungen.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Navigieren zu **Alle** > **Splunk ES-Integration** > **Splunk ES-Einstellungen**an.
2. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Splunk ES-Einstellungen

Feld	Beschreibung
Erzwingen Sie einen Grenzwert für die Anzahl der wichtigen Ereignisse, die zu einem einzelnen Incident zusammengefasst werden können.	Option zum Erzwingen eines Grenzwerts für die Anzahl Ihrer wichtigen Ereignisse, die Sie zu einem einzelnen Incident aggregieren möchten. Standardmäßig ist der Wert auf 100 festgelegt.
Erzwingen Sie einen Grenzwert für die Anzahl der Security Incidents, die innerhalb von 24 Stunden erstellt werden können.	Option zum Erzwingen eines Grenzwerts für die Anzahl der Security Incidents, die innerhalb von 24 Stunden erstellt werden können. Standardmäßig ist der Wert auf 1000 festgelegt.
Erzwingen Sie einen Grenzwert für die Anzahl der Werte, die in jedem von empfangenen Feld analysiert werden sollen Splunk.	Option zum Erzwingen eines Grenzwerts für die Anzahl der Werte, die Sie für jedes von empfangene Feld analysieren möchten Splunk. Standardmäßig ist der Wert auf 1000 festgelegt.
Anzahl der Korrelationsregeln, aus denen abgerufen werden soll Splunk.	Option zum Definieren der Anzahl der Korrelationsregeln, aus denen abgerufen werden soll Splunk. Standardmäßig ist der Wert auf 500 festgelegt.
Der Parameter für die Gültigkeitsdauer für Splunk Suchauftrag in Sekunden.	Option zum Definieren des Parameters „Time-to-Live“ für Splunk Suche in Sekunden. Standardmäßig ist der Wert auf 600 festgelegt.
Anzahl der wichtigsten Typen, die in einer Suche in Batch ausgeführt werden sollen.	Option zum Definieren der Gesamtzahl der wichtigen Typen, die in einer einzigen Suche Batch-Dateien verwendet werden sollen. Standardmäßig ist der Wert auf 20 festgelegt.
Anzahl der Tage, die beibehalten werden sollen Splunk Suchauftragsmetadaten in ServiceNow	Option zum Definieren der Anzahl der Tage, in denen Sie die Metadaten des Splunk-Suchauftrags beibehalten möchten ServiceNow. Standardmäßig ist der Wert auf 30 festgelegt.
Das Trennzeichen zum Aufteilen der Werte in Feldzuordnungen.	Option zum Definieren des Trennzeichens, um die Werte in Feldzuordnungen aufzuteilen. Standardmäßig ist der Wert auf (,) festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anzahl der Minuten, die beim Abrufen der Ereignisse hinzugefügt werden sollen Splunk(Um die Indexierungsverzögerung von Splunk zu überwinden)	Option zum Definieren der Anzahl der Überschneidungsminuten, die beim Abrufen der Ereignisse aus hinzugefügt werden sollen Splunk Um die Indexierungsverzögerung von zu überwinden Splunk. Standardmäßig ist der Wert auf 30 festgelegt.
Aktualisierte bedeutende Ereignisse abrufen	Option zum Abrufen aktualisierter wichtiger Ereignisse. Standardmäßig ist der Wert auf Nein festgelegt
Aktivieren Sie diese Einstellung, um vorhandene zu aktualisieren Splunk Quellkonfigurationen für die Unterstützung der tokenbasierten Authentifizierung. Sie müssen die Integrationskonfiguration mit Tokendetails aktualisieren, nachdem diese Einstellung aktiviert wurde.	Option zum Aktualisieren vorhandener Elemente Splunk Quellkonfiguration für tokenbasierte Authentifizierungsunterstützung von einer vorhandenen Version. **Hinweis:** Nach dem Upgrade auf die neue Version ist das Token-Feld nicht mehr verfügbar. Sie müssen diese Einstellung aktivieren, um die tokenbasierte Authentifizierung abzurufen. Danach müssen Sie die Integrationskonfiguration mit Tokendetails aktualisieren. Standardmäßig ist der Wert auf Nein festgelegt
Aktivieren Sie das Kontrollkästchen, um geschlossene wichtige Elemente während der Erfassung abzurufen.	Option zum Abrufen der geschlossenen Ereignisse in ServiceNow Splunk Es-Instanz. Wenn diese Option deaktiviert ist, werden nur aktive Ereignisse in die Instanz abgerufen. Standardmäßig ist der Wert auf Nein festgelegt

3. Klicken Sie auf **Speichern**.

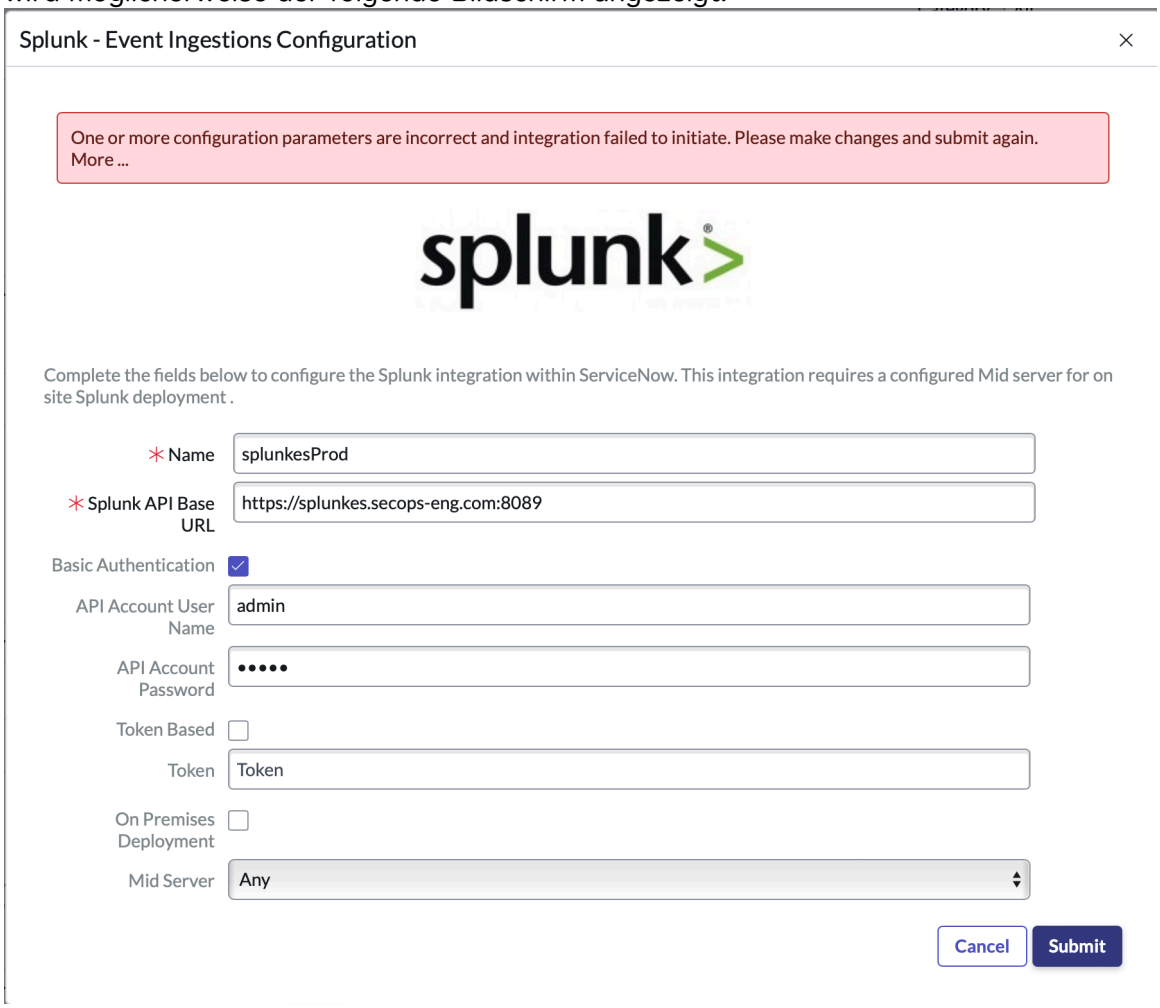
Authentifizierungsfehler

In diesem Abschnitt werden einige häufige Authentifizierungsfehler beschrieben und beschrieben, wie sie behoben werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

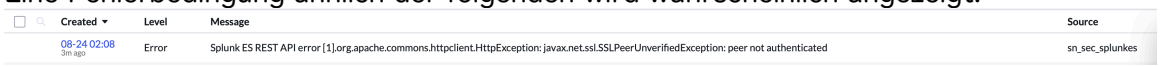
Problem bei der Zertifikatvalidierung

Wenn während der Authentifizierung ein Fehler auftritt, wird möglicherweise der folgende Bildschirm angezeigt:



Wenn Sie verifiziert haben, dass Ihre API-Account-Anmeldeinformationen und die Splunk-Basis-URL-Informationen korrekt sind, kann dieser Fehler auf ein Problem mit dem Splunk-Zertifikat für die Kommunikation mit Port 8089 zurückzuführen sein. ServiceNow® Die Instanz erfordert ein gültiges Zertifikat mit einem allgemeinen Namen, der dem Serverhostnamen entspricht, um sichere Verbindungen herzustellen. Weitere Informationen finden Sie unter Zertifikate . Wenn dieser Fehler angezeigt wird, können Sie überprüfen, ob das Problem auf ein Zertifikatproblem zurückzuführen ist, indem Sie die Systemprotokolle anzeigen.

Eine Fehlerbedingung ähnlich der folgenden wird wahrscheinlich angezeigt:



Um mit der Authentifizierung fortzufahren, müssen Sie das Splunk-Standardzertifikat ersetzen, das für den API-Zugriff auf Port 8089 bereitgestellt wird. Detaillierte Anweisungen zum Ersetzen des SSL-Zertifikats finden Sie unter KB0778285 .

Erstellen und benennen Sie ein Ereignisprofil für Splunk Enterprise Security Integration der Ereigniserfassung

Sie erstellen ein Ereignisprofil in Ihrem ServiceNow AI Platform Instanz und bestimmen, welche Splunk Wichtige Ereignisse erstellen Security Incidents.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:

Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Vor ServiceNow AI Platform Security Incident Response(SIR) Security Incidents werden aus erfassten wichtigen Ereignissen erstellt, die Feldwerte aus Warnungen werden in einem Layout von angezeigt ServiceNow AI Platform Security Incident, damit Sie eine Vorschau anzeigen können, wie der tatsächliche Security Incident erstellt wird.

Aus Integrationsperspektive mithilfe der verfügbaren APIs Splunk ES Bemerkenswerte Ereignisse werden einzeln und manuell als diskrete bemerkenswerte Ereignisse weitergeleitet oder automatisch in erfasst Security Operations Umgebung von ServiceNow AI Platform Instanz abhängig vom definierten Profiltyp.

Die Integrations-Workflows erfassen verschiedene Arten wichtiger Ereignisse, z. B. nicht autorisierte Zugriffsversuche und Malware. Diese wichtigen Ereignisse werden basierend auf den Profilen erfasst, die Sie in konfigurieren Security Operations Umgebung Ihrer Instanz.

Alle wichtigen Elemente werden anfänglich für einen konfigurierten Korrelationssuchtyp in einem Profil erfasst. Erfasste wichtige Elemente können dann weiter gefiltert werden, um anzugeben, welche wichtigen Personen Security Incidents erstellen. Sie können beispielsweise Filter bevorzugen, die Security Incidents nur für wichtige Ereignisse erstellen, die als hohes Risiko identifiziert werden. Bevor ein Profil aktiviert wird und Security Incidents aus erfassten wichtigen Ereignissen erstellt werden, werden einzelne Feldwerte in den wichtigen Ereignissen den entsprechenden Feldern in einem Layout des Security Incident zugeordnet, um eine Vorschau anzuzeigen.

Prozedur

1. Namen für die Ereignisprofile in Ihrem ServiceNow AI Platform Die Instanz muss eindeutig sein und kann jeweils nur einem aktiven Ereignisprofil zugeordnet werden.
2. Die ServiceNow AI Platform Erfasst bestimmte wichtige mithilfe der Workflows der Integration.
   Alle wichtigen Ereignisse, die die Auswahlkriterien in erfüllen Splunk ES Konsole wird anfänglich in erfasst ServiceNow AI Platform Instanz.
3. Ein Profil in Ihrem ServiceNow AI Platform Ist eine Kapselung eines bedeutenden Ereignisses in Ihrem Splunk ES Konsole.
   Es besteht eine 1-zu-1-Beziehung zwischen wichtigen Ereignissen, die mit einem Profil erfasst werden, und Verbindungen mit Ihrem Splunk ES Konsole: Ein bemerkenswerter Ereignistyp für eine Verbindung.
4. Informationen zum Erstellen von Profilen für geplante wichtige Ereignisse finden Sie unter Richten Sie ein Profil für die geplante Erfassung bedeutender Ereignisse ein.
5. Informationen zum Erstellen von Profilen für die manuelle Ereignisweiterleitung finden Sie unter Richten Sie ein Profil für die manuelle Ereignisweiterleitung ein.

Richten Sie ein Profil für die geplante Erfassung bedeutender Ereignisse ein

Abhängig vom definierten Profil Splunk ES Wichtige Ereignisse werden automatisch in erfasst Security Operations Umgebung von ServiceNow AI Platform Instanz.

Die folgende Tabelle zeigt die Liste der Aufgaben, die Sie ausführen müssen, um ein Profil für die geplante Erfassung wichtiger Ereignisse einzurichten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritte zum Einrichten eines Profils für die geplante Erfassung bedeutender Ereignisse

Aufgabe	Abschnitt
Erstellen Sie ein Ereignisprofil	Siehe Erstellen Sie Profile für die geplante Erfassung wichtiger Ereignisse
Wählen Sie wichtige Ereignisse basierend auf dem Namen der Korrelationssuche aus	Siehe Wählen Sie wichtige Ereignisse basierend auf dem Namen der Korrelationsregel für das Profil für aus Splunk ES Integration der Ereigniserfassung
Ordnen Sie wichtige Ereignisfelder zu	Siehe Zuordnung von wichtigen Ereignisfeldern für Splunk Enterprise Security Integration
Erstellen Sie anwenderdefinierte Zuordnungen	Siehe Erstellen Sie Zuordnungen für Splunk ESÜberprüfung von auffälligen Ereignis-Incidents und Details zu beitragenden Ereignissen (geplante Erfassung)
Zeigen Sie eine Vorschau des Security Incidents an	Siehe Vorschau des Security Incidents für anzeigen Splunk Enterprise Security Integration der Ereigniserfassung
Planen und rufen Sie neue und aktualisierte wichtige Ereignisse ab	Siehe Planen und rufen Sie neue und aktualisierte wichtige Ereignisse für ab Splunk Enterprise Security Integration der Ereigniserfassung
Automatisieren Sie Aktualisierungen und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status	Siehe Automatisieren Sie Aktualisierungen und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status

Erstellen Sie Profile für die geplante Erfassung wichtiger Ereignisse

Sie können ein Profil einrichten, damit wichtige Ereignisse automatisch erfasst werden.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

1. Dient zum Erstellen eines Ereignisprofils für ein bemerkenswertes Ereignis oder einen Korrelationsregeltyp in Ihrem ServiceNow AI Platform Instanz, navigieren Sie zu **Splunk Integration** > **Splunk-Ereignisprofil**an.
2. Wenn Splunk Formular „Ereignisprofil“ wird nicht angezeigt. Klicken Sie auf **Name** In der Fortschrittsleiste.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die Felder aus.

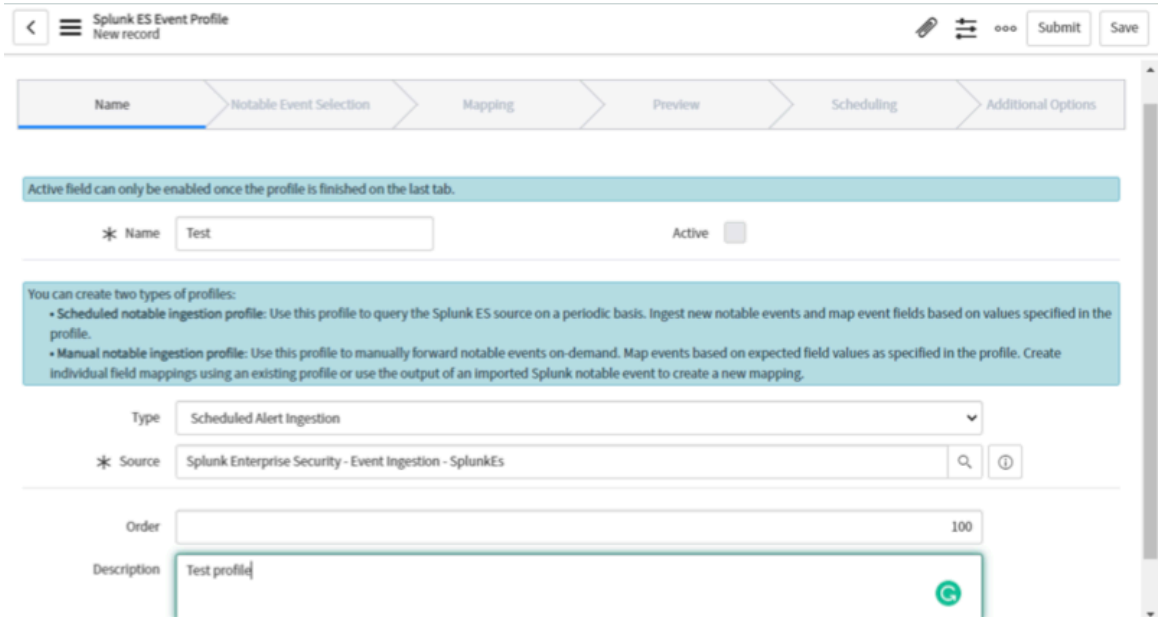
   Ein Beispiel für ein ausgefülltes Formular folgt der Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Eindeutiger Name für das Profil. Wenn Namen nicht eindeutig sind, wird ein Fehler angezeigt, und doppelte Profilnamen werden nicht gespeichert. Profilnamen in Ihrem ServiceNow AI Platform Instanz muss eindeutig sein.
Aktiv	Das Kontrollkästchen ist standardmäßig deaktiviert und deaktiviert. Sie sollten alle Abschnitte im Profil abschließen, bevor Sie es aktivieren.
Typ	Wählen Sie den Profiltyp aus der Auswahlliste aus. ○ Geplante Ereigniserfassung: Dieser Profiltyp unterstützt wichtige Ereignisse, die in einem konfigurierten Zeitplan erfasst werden. Füllen Sie die Felder aus. ○ Manuelle Ereignisweiterleitung: Dieser Profiltyp unterstützt wichtige Ereignisse, die manuell von Ihrem weitergeleitet werden Splunk Enterprise Security Incident-Überprüfungskonsole bei Bedarf. Lesen Sie die folgenden Schritte, um das Formular für diese Profiltypen auszufüllen.
Quelle	Splunk Server- oder Suchende, die Sie für die Erfassung wichtiger Ereignisse konfiguriert haben. Wenn Sie mehrere haben Splunk Server konfiguriert, wählen Sie den entsprechenden Server für die wichtigsten Ereignistypen aus, die für das Profil erfasst werden. Sie müssen einen Wert eingeben.
Reihenfolge	Der Standardwert ist 100. Wenn Sie mehrere Profile erstellt haben, gibt dieser Wert eine Laufzeitausführungspriorität an, wenn zwei oder mehr Profile dieselben Auslösebedingungen haben. Der Workflow im Profil mit der niedrigsten Zahl hat die höchste Priorität.
(Optional) Beschreibung	Zusätzlicher Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular für einen geplanten Ereignistyp mit wichtigen Elementen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie für ein Profil mit einem geplanten bedeutenden Ereignis eine Option aus, um mit der Profilkonfiguration fortzufahren.

Nächste Maßnahme

Der nächste Schritt besteht darin, wichtige Ereignisse für die automatische Erfassung auszuwählen.

Wählen Sie wichtige Ereignisse basierend auf dem Namen der Korrelationsregel für das Profil für aus Splunk ES Integration der Ereigniserfassung

Nachdem Sie ein Profil für eine geplante Erfassung eines bedeutenden Ereignistyps erstellt haben, wählen Sie ein aus Splunk Enterprise Security Name der Korrelationsregel für dieses Profil, für das Sie entsprechende wichtige Ereignisse einem zuordnen möchten ServiceNow AI Platform Security Incident Response Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die verfügbaren Korrelationsregeln in an ServiceNow AI Platform Instanz, damit Sie die wichtigen Ereignistypen kennen, für die Sie Security Incidents erfassen und erstellen möchten. Wählen Sie eine Korrelationsregel aus. Sie können in diesem Formular ein oder mehrere wichtige Ereignisse aus der Liste auswählen.

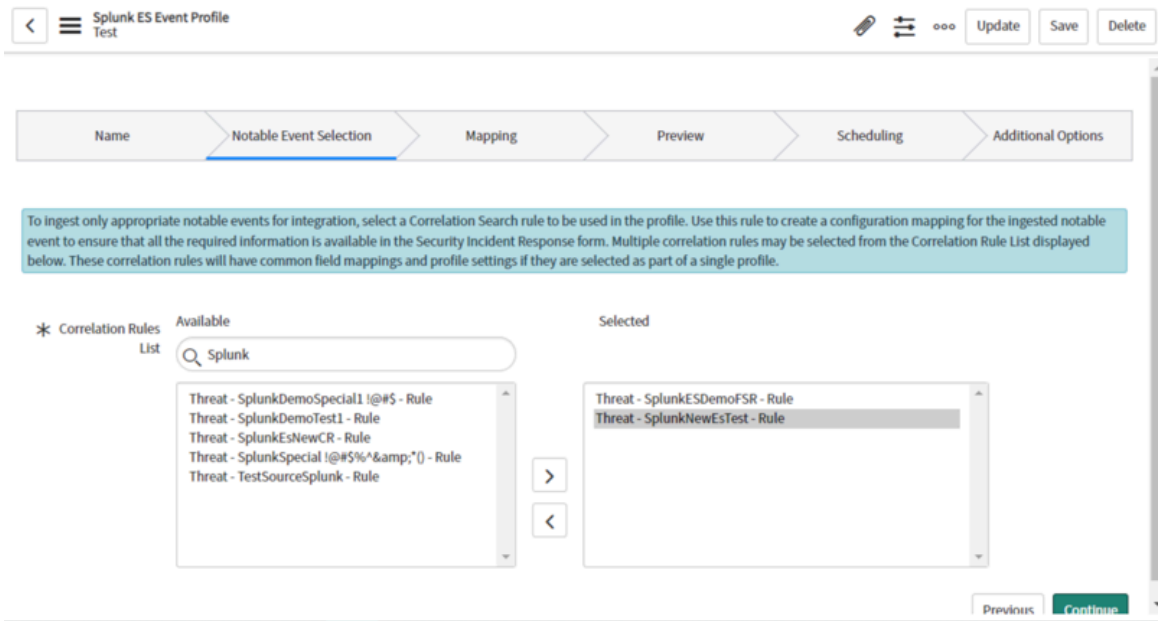
Prozedur

1. Wenn die Seite „Auswahl des nennenswerten Ereignisses“ nicht angezeigt wird, wählen Sie sie in der Fortschrittsleiste aus, um sie anzuzeigen.
2. Wählen Sie in der Liste der Korrelationsregeln eine der folgenden Optionen aus, um eine einzelne Korrelationsregel oder mehrere Korrelationsregeln auszuwählen, sie zu verschieben und sie von der Spalte verfügbar in die Spalte ausgewählt zu verschieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Liste der Korrelationsregeln in diesem Formular stimmt mit der Liste der Korrelationsregeln in überein Splunk ES Incident-Überprüfungskonsole. In diesem Formular werden bis zu 500 Korrelationsregeln angezeigt. Wenn mehr als 500 Korrelationsregeln in aufgeführt sind Splunk ES, Nur die ersten 500 wichtigen Ereignisse werden in diesem Formular in angezeigt ServiceNow AI Platform Instanz.

Option	Beschreibung
Geben Sie im Suchfeld Korrelationsregelliste Text ein.	Die Spalte unter dem Suchfeld wird basierend auf dem von Ihnen eingegebenen Text mit verfügbaren Optionen gefiltert. Wählen Sie eine Korrelationsregel aus, und verschieben Sie den ausgewählten Alarm mit den Pfeiltasten aus **Verfügbar** Bis **Ausgewählt** .
Doppelklicken Sie in der Korrelationsregelliste auf eine Korrelationsregel.	Die **Ausgewählt** Spalte wird mit Ihrer Auswahl ausgefüllt.
Klicken Sie in der Korrelationsregelliste einmal auf eine Korrelationsregel.	Die Korrelationsregel ist ausgewählt. Verschieben Sie mit den Pfeiltasten die ausgewählte Korrelationsregel aus **Verfügbar** Bis **Ausgewählt** .



3. Wählen Sie eine Option aus, um fortzufahren.

Nächste Maßnahme

Sie haben erfolgreich eine Korrelationsregel für eine geplante ausgewählt Splunk Enterprise Security Profil. Der nächste Schritt besteht darin, Felder in einem Security Incident wichtige Ereigniswerte zuzuordnen.

Zuordnung von wichtigen Ereignisfeldern für Splunk Enterprise Security Integration

Nachdem Sie die spezifische Korrelationsregel und den entsprechenden Ereignistyp für das Profil identifiziert haben, besteht der nächste Schritt darin, den Feldern in einem einzelne

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

relevante Ereignisfelder zuzuordnen ServiceNow AI Platform Security Incident Response(SIR) Security Incident.

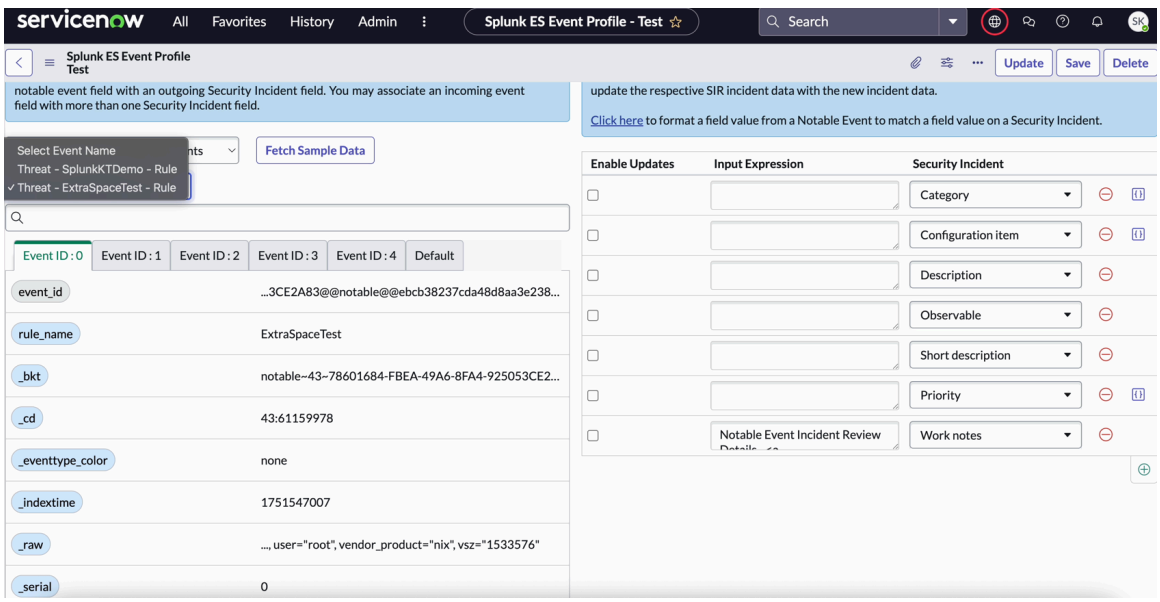
Übersicht über die Zuordnung

Für den Zuordnungsschritt können Sie Beispielereignisse für die ausgewählte Korrelationsregel erfassen oder wichtige Ereignisdaten für manuell weitergeleitete wichtige Ereignisse exportieren. Der Ereigniszuordnungsprozess ist unabhängig vom Profiltyp, den Sie erstellen, identisch.

Die folgenden Abbildungen sind Beispiele für die Standardzuordnungskonfigurationen, die für jeden Ereignisprofiltyp bereitgestellt werden. Sie können die Felder anpassen, die den Security Incident ausfüllen. Während dieser Zuordnungsphase können Sie sicherstellen, dass alle relevanten relevanten Ereignisfelddaten der entsprechenden Stelle im SIR-Incident-Formular zugeordnet werden, und dann den SIR-Incident im Vorschauabschnitt visualisieren.

Wenn mehrere Korrelationen verwendet werden, können beachtliche Ereignisse abgerufen werden, indem erforderliches Ereignis ausgewählt wird. Verwenden **Warnungsname** Um Ihre Warnung auszuwählen, wenn Sie mehrere Warnungen für die Erfassung konfiguriert haben.

Nachdem Sie auf geklickt haben, um Daten abzurufen Splunk Namen der Ereignisfelder und entsprechende Werte werden auf der linken Seite des Formulars ausgefüllt. Dies sind die Splunk Wichtige Ereignisfelder, die zur Zuordnung zu verfügbar sind SIR Security Incident-Felder. Einige Felder können den SIR Security Incident-Feldern mehrmals zugeordnet werden.



Möglicherweise möchten Sie einige Beispiele für wichtige Ereignisse auf Ihrem überprüfen Splunk Konsole, die für den Konfigurationsschritt der Feldzuordnung erfasst werden soll. Dieser Schritt wird auf der Fortschrittsleiste mit Zuordnung bezeichnet. Wenn diese Seite nicht angezeigt wird, klicken Sie auf **Zuordnung** Auf der Fortschrittsleiste. Sie können bis zu fünf Beispiele für wichtige Ereignisse aus erfassen Splunk Enterprise Security Zur Unterstützung des Zuordnungsprozesses für wichtige Ereignisfelder. Es gibt Optionen zum Erfassen der fünf neuesten bemerkenswerten Ereignisse für die ausgewählte Korrelationsregel oder zum Erfassen von bis zu fünf spezifischen bemerkenswerten Ereignissen basierend auf den bemerkenswerten Ereignis-IDs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachfolgend finden Sie eine Zusammenfassung der Schritte, die zum Zuordnen wichtiger Ereignisse erforderlich sind:

- Geplante Erfassung von Beispieldaten für wichtige Ereignisse: Für Beispieldaten, die für automatisch erfasste Profile für wichtige Ereignisse verwendet werden, werden verfügbare Felder für wichtige Ereignisse und ihre entsprechenden Werte in einem Standardzuordnungslayout auf der linken Seite des Zuordnungsformulars angezeigt, sobald die Beispieldaten abgerufen wurden. Registerkarten werden angezeigt, auf denen Sie die Werte für eine bestimmte wichtige Ereignis-ID anzeigen können, die Sie abgerufen haben. Überprüfen Sie, ob alle kritischen Felder aus dem Abschnitt „Stichprobenerfassung für wichtige Ereignisse“ auf der linken Seite des Formulars zugeordnet sind ServiceNow Security Incident-Felder auf der rechten Seite des Formulars.
- Feldzuordnung: Bearbeiten Sie die Zuordnungskonfiguration, indem Sie wichtige Ereignisfelder von der linken Seite ziehen und auf dem ablegen ServiceNow SIR-Incident-Zuordnungsabschnitt auf der rechten Seite. Die Zuordnung auf der rechten Seite ordnet das Feld „eingehendes bedeutendes Ereignis“ einem Feld für ausgehende Security Incidents zu.
- Zuordnungs-Experience: Passen Sie das Zuordnungsraster an, indem Sie Felder mithilfe des +-Symbols unten im SIR-Incident-Feldzuordnungsabschnitt hinzufügen oder entfernen. Verfolgen Sie übersehene oder duplizierte Felder mit der bereitgestellten Farbcodierung nach (zugeordnete Felder sind ausgegraut, blaue Felder sind nicht zugeordnet).
- Bedingungen für die Incident-Generierung: Sobald der Zuordnungsabschnitt abgeschlossen ist, können Sie Filterbedingungen festlegen, um anzugeben, welche wichtigen Ereignisse Security Incidents erstellen sollen und welche wichtigen Ereignisse herausgefiltert werden sollen, z. B. Ereignisse mit niedriger Priorität. Dies geschieht im Abschnitt „Bedingungen für die Incident-Generierung“ unter dem Abschnitt „Zuordnung von wichtigen Ereignissen“.
- Kriterien für Ereigniszusammenfassung: Definieren Sie zusätzliche Kriterien für die Ereigniszusammenfassung, die ein eingehendes Ereignis mit einem vorhandenen zusammenfassen SIR Security Incident stattdessen pf, um ähnliche, potenziell doppelte Incidents zu erstellen. Mithilfe von Feldübereinstimmungswertkriterien für jedes Profil kann diese zusätzliche Zusammenfassungsfunktion die Anzahl der aktiven, sich überschneidenden Security Incidents reduzieren, indem alle zugehörigen sicherheitsrelevanten Ereignisdaten in einem einzelnen Security Incident platziert werden.
- Formatfeldübersetzung: In bestimmten Fällen Ereignisfeldwerte im Splunk Wichtige Enterprise-Ereignisse werden möglicherweise nicht direkt in die Felder auf übersetzt SIR Security Incident. Für diese Werte können Sie einen Skripteditor verwenden, um Feldwerte für den Security Incident während des Zuordnungsschritts zu formatieren. Verwenden Sie den Skript-Editor, wenn Sie Werte formatieren möchten, die ähnlich, aber nicht identisch sind. Beispielsweise kann ein Kategoriewert „Malware-Warnung“ und „Virusinfektion“ mit dem Skripteditor unterschiedliche Feldwerte für die Quellkategorie haben, aber beide Werte können in eine allgemeine schädliche Code-Aktivität im Feld Kategorie übersetzt werden SIR Security Incident mithilfe der Funktionalität „Formatierungsfeldübersetzung“.

Der nächste Schritt besteht darin, wichtige Ereignisse zu erfassen und Werte dem zuzuordnen SIR Security Incident-Felder.

Erstellen Sie Zuordnungen für Splunk ESÜberprüfung von auffälligen Ereignis-Incidents und Details zu beitragenden Ereignissen (geplante Erfassung)

Während des Schritts „Feldzuordnung für nennenswerte Ereignisse“ ordnen Sie einzelne Ereignisfelder aus nennenswerten Ereignissen zu Feldern in einem zu ServiceNow AI Platform Security Incident Response(SIR) Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Das Zuordnungsraster kann für den in der Korrelationsregelauswahl ausgewählten bedeutenden Ereignistyp angepasst werden. Die Farbcodierung der Ereignisfelder hilft Ihnen, die Ereigniswerte nachzuverfolgen, die Sie bereits zugeordnet haben, da sie ausgegraut werden, während alle verbleibenden nicht zugeordneten Felder blau angezeigt werden. Auf diese Weise können Sie besser visualisieren, welche Feldwerte dem Security Incident hinzugefügt wurden und ob verbleibende wichtige Ereignisinformationen nicht zugeordnet sind.

Ordnen Sie bis zu fünf wichtige Ereignisse aus der Spalte „Stichprobenerfassung für bedeutendes Ereignis“ auf der linken Seite des Formulars den Security Incident-Feldern in der Spalte „SIR-Incident-Feldzuordnung“ auf der rechten Seite zu.

Erstellen Sie anwenderdefinierte Zuordnungen, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Standardfelder, die normalerweise ein wichtiges Feld sind, das im Antwortformular für Security Incidents ausgefüllt werden soll, werden angezeigt. Diese Felder können jedoch entfernt werden, und zusätzliche Felder können mit den Schaltflächen + und - angezeigt werden. Erstellen Sie anwenderdefinierte Karten, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie zuordnen Splunk Felder, die nicht im Standardzuordnungsraster auf angezeigt werden SIR Security Incident.

Prozedur

1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie auf **Zuordnung** Auf der Fortschrittsleiste.
2. Klicken Sie für ein Profil mit einer geplanten Erfassung unter „Stichprobenerfassung für auffällige Ereignisse“ auf **Rufen Sie Beispieldaten Ab** Dient zum Abrufen der neuesten Beispiele für wichtige Ereignisse aus dem Splunk Enterprise Konsole für die ausgewählte Korrelationsregel.

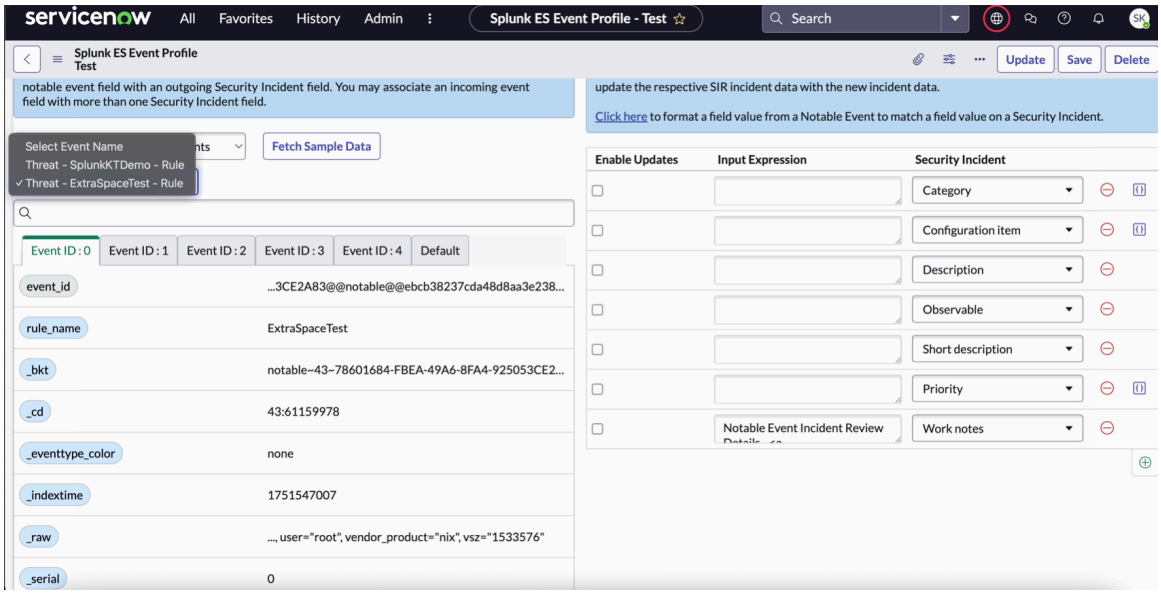
   Hinweis:
   Sie können entweder die neuesten Beispiele für wichtige Ereignisse abrufen oder die eindeutigen Ereignis-IDs für die spezifischen Ereignisse angeben, die Sie für Ihre Experience für die Zuordnung wichtiger Ereignisse verwenden möchten.

   Die Ergebnisse der relevanten Ereignisfelder und -Werte werden als einzelne Registerkarten angezeigt. Sie können bis zu fünf wichtige Ereignisse erfassen.

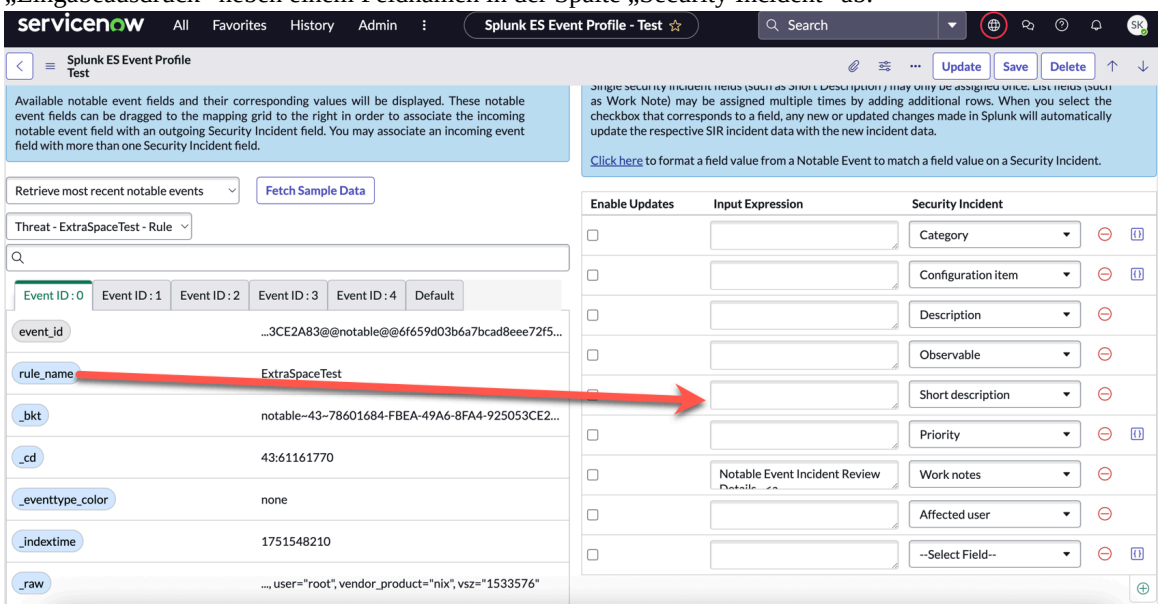
   Der Abruf für Beispiele für wichtige Ereignisse kann einige Minuten dauern. Eine Nachricht, die angibt, dass die Transaktion funktioniert, wird oben auf dem Bildschirm angezeigt.

   In der folgenden Abbildung werden die Feld-Name-Wert-Paare für das erfasste bemerkenswerte Ereignis oder die importierten Beispielereignisse auf der linken Seite dieses Formulars angezeigt, nachdem der Abruf der Erfassung abgeschlossen ist. Diese Werte sind die Werte, die Sie den Security Incident-Feldern auf der Seite „SIR-Incident-Feldzuordnung“ des Formulars zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Um einen Feldwert von der linken Seite des Formulars einem Feld im Security Incident auf der rechten Seite des Formulars zuzuordnen, klicken Sie auf der linken Seite des Formulars auf einen blauen Feldnamen.
4. Ziehen Sie den Feldnamen, z. B. Rule_Name , Und legen Sie es in einem Feld in der Spalte „Eingabeausdruck“ neben einem Feldnamen in der Spalte „Security Incident“ ab.

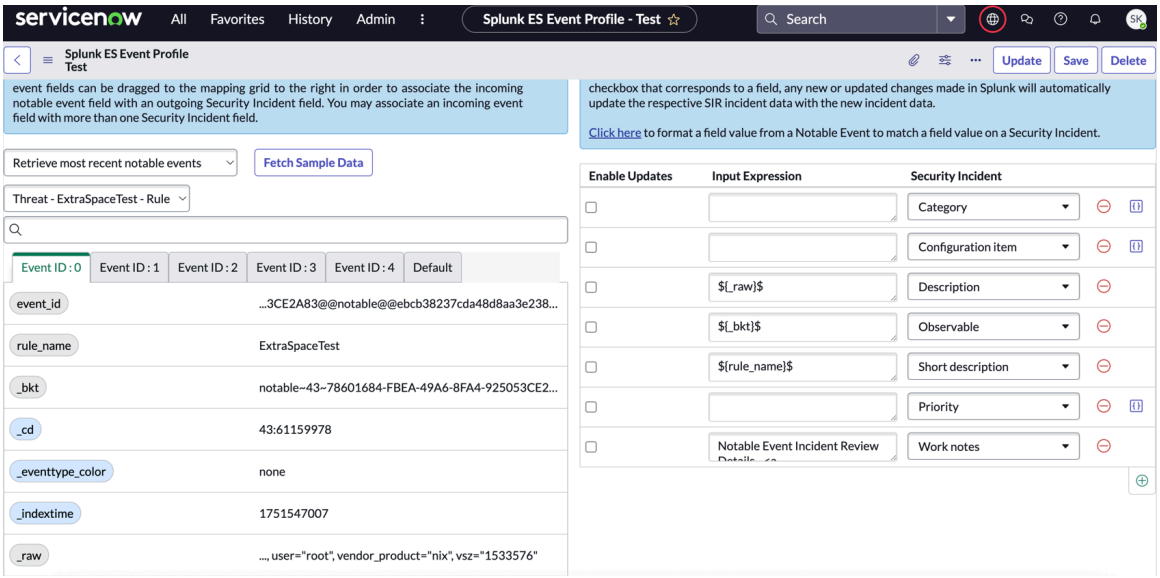


Der Feldwert wird in der Spalte „Eingabeausdruck“ angezeigt. In der folgenden Abbildung: Rule_Name Ist dem zugeordnet Kurzbeschreibung Feld im Security Incident. Sie können jedoch einen beliebigen Wert von der linken Seite mit einem Feld auf der rechten Seite abgleichen. Stellen Sie sicher, dass der Wert dem Security Incident während des Vorschauschritts korrekt zugeordnet ist.

Damit Sie sicherstellen können, dass im Zuordnungsprozess keine Ereignisfelder übersehen oder dupliziert werden, sind Felder farbcodiert. Hellblaue Felder auf der linken Seite zeigen an, dass ein auffälliges Ereignisfeld noch nicht ausgewählt und dem Security Incident zugeordnet ist. Möglicherweise möchten Sie ein eingehendes wichtiges Feld mit mehr als einem Feld in einem Security Incident verknüpfen.

Ein graues Feld gibt an, dass ein Feld ausgewählt und einem Feld im Security Incident zugeordnet wurde. Diese Farbcodierung hilft Ihnen, die Zuordnung nachzuverfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

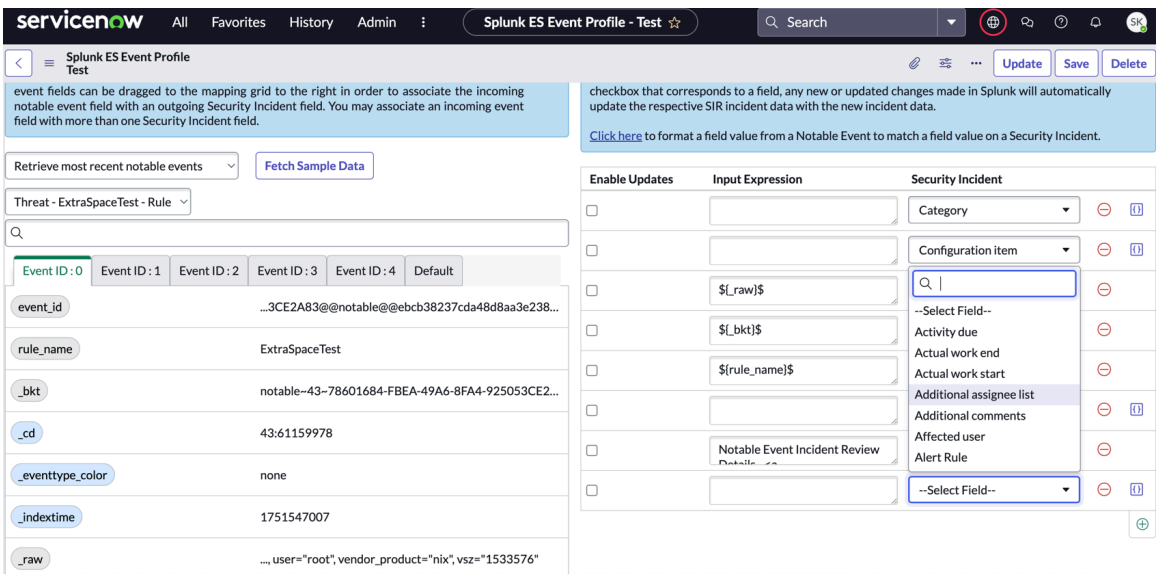


5. Führen Sie die folgenden Schritte aus, um den Standardfeldern, die im Security Incident auf der rechten Seite des Formulars angezeigt werden, Felder hinzuzufügen.

a. Klicken Sie auf der rechten Seite des Formulars im Abschnitt „SIR-Incident-Feldzuordnung“ unten im Raster auf das Plus-Symbol.
Ein neues Feld wird angezeigt.

b. Erweitern Sie in der Spalte Security Incident die angezeigte Liste, und wählen Sie ein Feld aus.

In der erweiterten Liste für das neue Feld sind einige Felder schattiert. In der folgenden Abbildung: Rule_Name Hat einen grauen Hintergrund, da er im Security Incident zugeordnet wurde. Ähnlich wie die Farbcodierung für die Felder für wichtige Ereignisse auf der linken Seite des Formulars hilft diese Farbcodierung für die Security Incident-Felder auf der rechten Seite Ihnen, die bereits zugeordneten SIR-Incident-Felder nachzuverfolgen.



Automatische Übersetzung

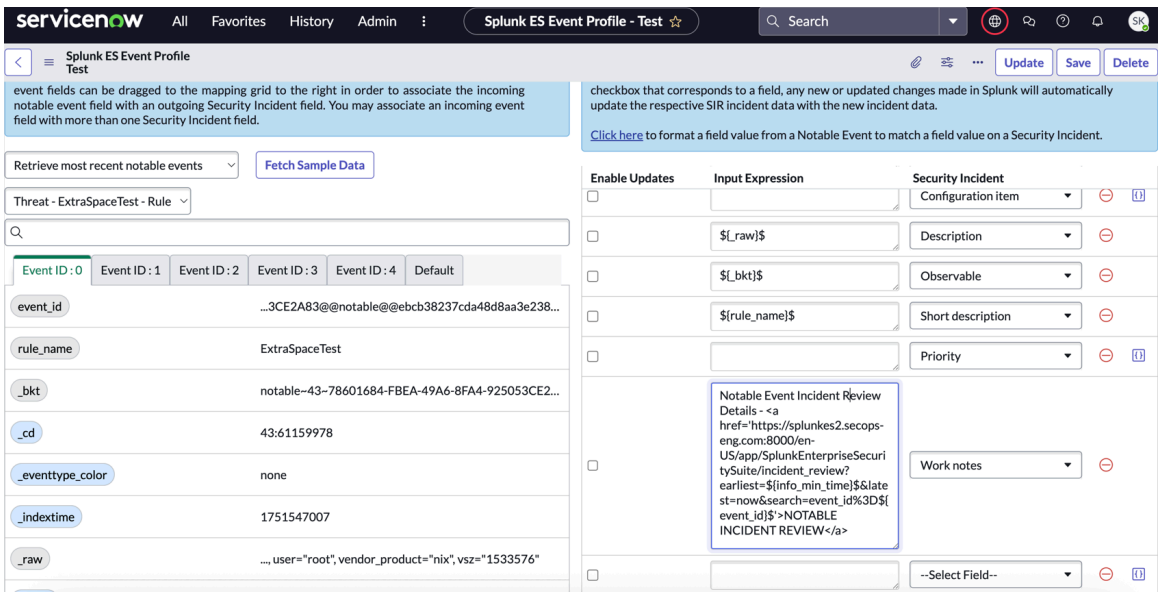
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Damit mehrere erkennbare Elemente für denselben Security Incident angezeigt werden können, kann das Feld „erkennbares Element“ mehrmals verschiedenen Werten zugeordnet werden. Ebenso unterstützen die Felder „Konfigurationselement“ und „Arbeitsnotizen“ mehrere Werte. Wenn Sie versuchen, zwei Werte einem Feld zuzuordnen, das nicht mehrere Werte unterstützen kann, wird bei der Vorschau des Incident eine Fehlermeldung angezeigt, dass für das Feld kein Wert vorhanden ist. Wenn ein Feld in einem Security Incident über eine Liste verfügt, aus der Sie mehrere Optionen auswählen können, und Sie versuchen, diesem Feld eine Option zuzuordnen, die nicht in der Liste angezeigt wird, wird das Feld im Security Incident nicht ausgefüllt.

c. Alternativ können Sie einen Wert in das Suchfeld für die neue Zeile eingeben.

d. Klicken Sie auf der linken Seite des Formulars mit der linken Maustaste, um auszuwählen **Ereignis-ID** Die Sie im Feld Eingabeausdruck wünschen.

6. Fahren Sie mit der Zuordnung fort, indem Sie der Zuordnung Feldwerte hinzufügen oder entfernen.
Die folgende Abbildung ist ein Beispiel für eine bearbeitete Zuordnung. Im unteren Feld rechts wird das Feld Arbeitsnotizen hinzugefügt, das mehr als einen Wert hat. Beachten Sie, dass Sie für das Feld mit langer Textzeichenfolge das Zuordnungsfeld erweitern können, um die vollständige Zeichenfolge anzuzeigen und die Größe nach Bedarf neu zu ändern, indem Sie die untere rechte Ecke des Felds wie im Screenshot unten mit dem Feld „hinzugefügte Arbeitsnotizen“ ziehen:



Warnung:
Beachten Sie dies in **SIR-Incident-Feldzuordnung** Abschnitt, die URL und die Portnummer, die im erwähnt werden **Eingabeausdruck** Das Feld ist nur ein Beispiel und nicht die standardmäßig bereitgestellte URL oder Portnummer.

In der Vorschau werden diese Werte in den Arbeitsnotizen zum Security Incident angezeigt. Da der Wert für ein Feld gilt, das Sie dem Zuordnungsabschnitt hinzugefügt haben, und dem Feld Arbeitsnotizen mehrere Werte zugeordnet sind, werden die Werte wie eingegeben angezeigt. In diesem Beispiel werden die Leerzeichen und Interpunktionszeichen, die Sie in das Feld eingegeben haben, im Abschnitt „zugehörige Elemente“ als Arbeitsnotiz in der Vorschau des Security Incident angezeigt.

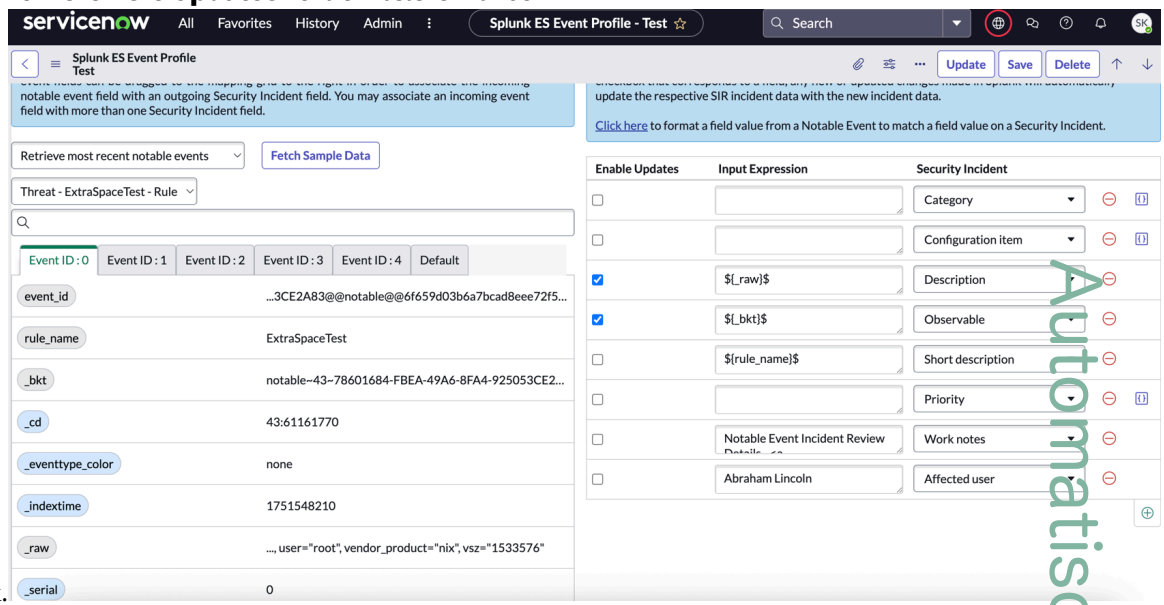
Die folgende Abbildung zeigt, wie die Werte im vorherigen Bild für den Security Incident angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Related Items

Field Name	Field Value
Work Note	Category: Malware Activity | destination IP: 78.46.123.180
Work Note	Source: MalwareDemoData Top 100 events with 15 host machines

7. Um Aktualisierungen für die zugeordneten Felder in SIR zu erhalten, wählen Sie aus **Aktivieren Sie Updates**Kontrollkästchen für den Eingabeausdruck.



8. **Wahlweise:** Nachdem Sie die vorherigen Feldzuordnungsschritte abgeschlossen haben, können Sie dieselben Feldwerte im Generator für Incident-Generierungsbedingungen verwenden, um zusätzliche Kriterien zu definieren, die ein eingehendes Ereignis erfüllen muss, um eine zu erstellen SIR Security Incident.
Um Bedingungen für die Incident-Generierung festzulegen, gehen Sie wie folgt vor.

   a. Scrollen Sie im Formular zum Abschnitt Bedingungen für die Incident-Generierung, und wählen Sie aus **Filtern Sie basierend auf Bedingungen** Kontrollkästchen zum Aktivieren der Option.

      (Optional) Der Generator für Filterbedingungen wird angezeigt. Verwenden Sie diese Filter, um Security Incidents zu erstellen, die den spezifischen Bedingungen entsprechen, die in den Feldern beschrieben werden.

      Die Optionen in den Listen für das erste Feld im Generator für Filterbedingungen stimmen mit den Feldern überein, die im Abschnitt „Stichprobenerfassung für wichtige Ereignisse“ für die von Ihnen erfassten Ereignisse angezeigt werden. Diese Felder sind dynamisch und ändern sich je nach Splunk Wichtige Ereignisse, die Sie erfassen, oder das Ereignis, das Sie für die manuell weitergeleiteten Beispiele für wichtige Ereignisse auswählen. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden und müssen genau mit den Werten von übereinstimmen Splunk Enterprise Security Bemerkenswertes Ereignis. Wenn Sie sich nicht sicher sind, welche Werte in die Filterfelder eingegeben werden sollen, kehren Sie möglicherweise zu zurück Splunk Enterprise Security Konsole und überprüfen Sie Ihre wichtigen Ereignisse auf die Stichwörter.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators Filter für die erste Zeile fest.

c. Um weitere Bedingungen hinzuzufügen, klicken Sie rechts neben den Feldern auf **UND** Oder **ODER** . Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden.

d. **Wahlweise:** Legen Sie in der zweiten Zeile eine zweite Filterbedingung fest.

(Optional) Die folgende Abbildung zeigt ein Beispiel mit zwei Bedingungen, die erfüllt werden müssen, bevor Security Incidents erstellt werden.

(Optional) Sie haben die Bedingungen für die Incident-Generierung so festgelegt, dass Security Incidents nur erstellt werden, wenn beide von Ihnen eingegebenen Filterbedingungen erfüllt sind.

Diese Art der Bedingungsfilterung für die Incident-Generierung hilft Ihnen, die Sicherheitsereignisse einzugrenzen und die Anzahl der unnötigen Security Incidents zu begrenzen, die Sie erstellen, ohne die zugrunde liegende Korrelationssuche oder -Filter in zu ändern Splunk. Wenn zusätzliche Filterkriterien festgelegt sind, werden Incidents nur nennenswerte Ereignisse zugeordnet, die allen Kriterien entsprechen.

Hinweis:
Wenn einer der Ereignisfeldnamen Sonderzeichen wie Anführungszeichen (“), Bindestriche (‘), Unterstriche (-), bei (@) oder ampersands (&) enthält, diese Zeichen müssen möglicherweise zu Zuordnungsübersetzungszwecken ersetzt werden und möglicherweise einen doppelten Ereignisnamen erstellen. Die Zuordnung kann entsprechend erfolgen, es wird jedoch ein numerisches Suffix angehängt, um Felder mit doppelten Ereignisnamen zu unterscheiden. Beispiel: Wenn das erste Ereignisfeld lautet `Warnungen.Warnung` Und das zweite Ereignisfeld ist `Warnungen@Warnungen` , Diese Felder können nicht eindeutig identifiziert werden, da die verbleibenden Standardtextzeichen identisch sind. In diesem Fall wird dem zweiten Ereignisfeld ein Suffix hinzugefügt, und das Feld wird in umbenannt `Warnungen@Alert(1)` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Optional) Kriterien für Ereigniszusammenfassung zur Behandlung ähnlicher wichtiger Elemente und zur Vermeidung doppelter Incidents

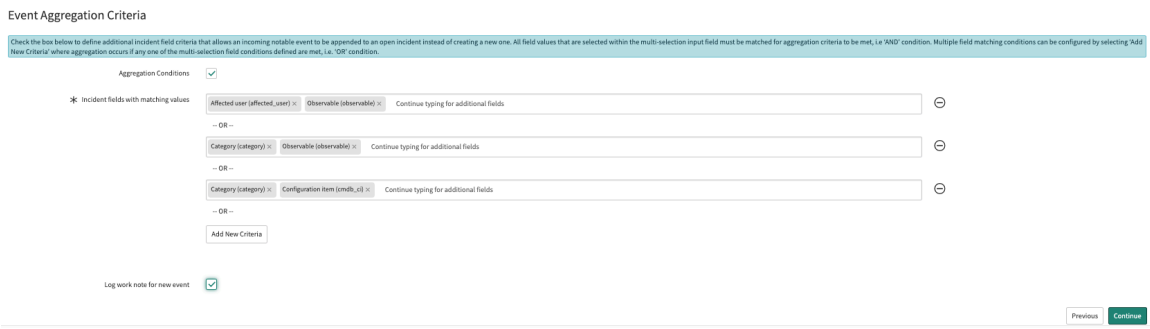
9. **Wahlweise:** Um die Erstellung doppelter Security Incidents zu vermeiden, definieren Sie zusätzliche Ereigniszusammenfassungskriterien, damit eingehende wichtige Ereignisse zu einem offenen Security Incident zusammengefasst werden.
   Um die Kriterien festzulegen, führen Sie die folgenden Schritte aus.

   a. Scrollen Sie im Formular zum Abschnitt „Kriterien für Ereigniszusammenfassung“, und wählen Sie aus **Aggregatbedingungen** Kontrollkästchen zum Aktivieren dieser Option.

      (Optional) Die Incident-Felder mit übereinstimmenden Werten werden angezeigt. Diese Feldnamen sind die Felder im Security Incident, die alle anwenderdefinierten Felder enthalten, die in konfiguriert sind SIR Security Incident.

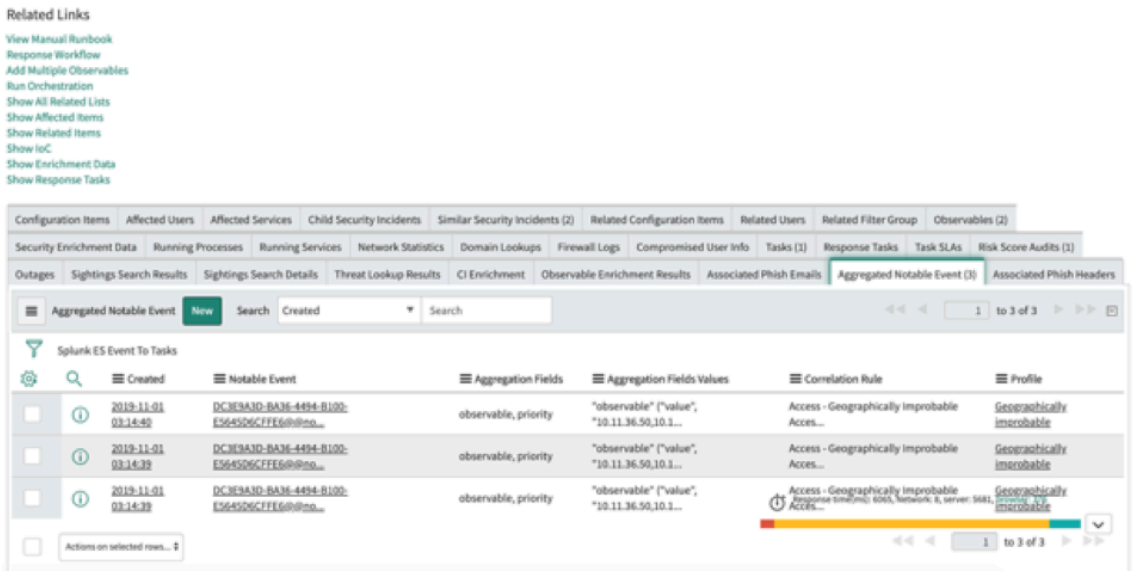
   b. Wählen Sie im Eingabefeld Mehrfachauswahl die Feldwerte aus, die Sie für vorhandene Security Incidents in abgleichen möchten ServiceNow AI Platform.

   c. Verwenden Sie **Fügen Sie Neue Kriterien Hinzu** Zum Auswählen mehrerer Felder, die Bedingungen entsprechen.
      Alle Feldwerte, die Sie im Eingabefeld für Mehrfachauswahl auswählen, werden für Zusammenfassungskriterien mit der Bedingung UND abgeglichen. Klicken Sie Auf **Fügen Sie Neue Kriterien Hinzu** Dient zum Auswählen mehrerer übereinstimmender Felder, bei denen eine Zusammenfassung stattfindet, wenn eine der definierten Bedingungen für mehrere ausgewählte Felder mit der ODER-Bedingung erfüllt wird.



Wenn ein neues bemerkenswertes Ereignis allen Werten entspricht, die im Zuordnungsschritt in den Bedingungen des Zusammenfassungsfelds ausgewählt sind, wird das neue bemerkenswerte Ereignis automatisch dem zuletzt geöffneten Security Incident mit denselben Feldwerten hinzugefügt. Als Anwender mit der Rolle „sn_si.Analyst“, der mit Security Incidents arbeitet, können Sie alle hinzugefügten aggregierten wichtigen Ereignisse in einer zugehörigen Liste zu einem Security Incident anzeigen. Alle zusammengefassten wichtigen Ereignisse in einem Security Incident werden auf angezeigt Splunk Zugehörige Liste „Ereignis zu Aufgaben“. Diese Liste enthält Details zu zugeordneten Zeitstempeln und zusammengefassten Feldwerten. Diese Informationen helfen Ihnen zu verstehen, warum diese wichtigen Ereignisse zu vorhandenen Security Incidents aggregiert werden. Wenn diese Registerkarte nicht angezeigt wird, scrollen Sie unter zugehörige Links zur linken Seite des Datensatzes, und klicken Sie auf **Alle Zugehörigen Listen Anzeigen** Link.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Wahlweise: Um eine Arbeitsnotiz für ein neues bedeutendes Ereignis zu protokollieren, das kürzlich dem Security Incident hinzugefügt wurde, aktivieren Sie das Kontrollkästchen, um diese Option zu aktivieren. In der Arbeitsnotiz wird protokolliert, dass ein neuer wichtiger Eintrag hinzugefügt wurde, zusammen mit einem Link zu den Warnungsdetails und allen anderen Details, die dem Feld „Arbeitsnotiz“ in Ihrem Zuordnungsabschnitt hinzugefügt wurden.

Sie haben erfolgreich Werte aus einem zugeordnet Splunk Bemerkenswertes Ereignis für Felder in einem SIR Security Incident. Außerdem haben Sie zusätzliche Bedingungen konfiguriert, um die Erstellung von Security Incidents mit Filterkriterien für die Incident-Generierung einzuschränken. Sie haben auch wichtige Ereignisse an vorhandene angehängt SIR Security Incidents, wenn die Ereignisfeldwerte den konfigurierten Zusammenfassungskriterien entsprechen.

10. Wählen Sie eine Option aus, um mit der Profilkonfiguration fortzufahren.

Nächste Maßnahme

Der nächste Schritt besteht darin, eine Vorschau der Werte anzuzeigen, die Sie dem Security Incident zugeordnet haben.

Vorschau des Security Incidents für anzeigen Splunk Enterprise Security Integration der Ereigniserfassung

Nachdem Sie den Zuordnungsschritt abgeschlossen haben, zeigen Sie eine Vorschau der Werte an, die Sie in einem zugeordnet haben ServiceNow AI Platform® Security Incident Response(SIR) Security Incident. Mit diesem Vorschauschritt können Sie überprüfen, ob Sie alle wichtigen Felder zugeordnet haben, die im Security Incident angezeigt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

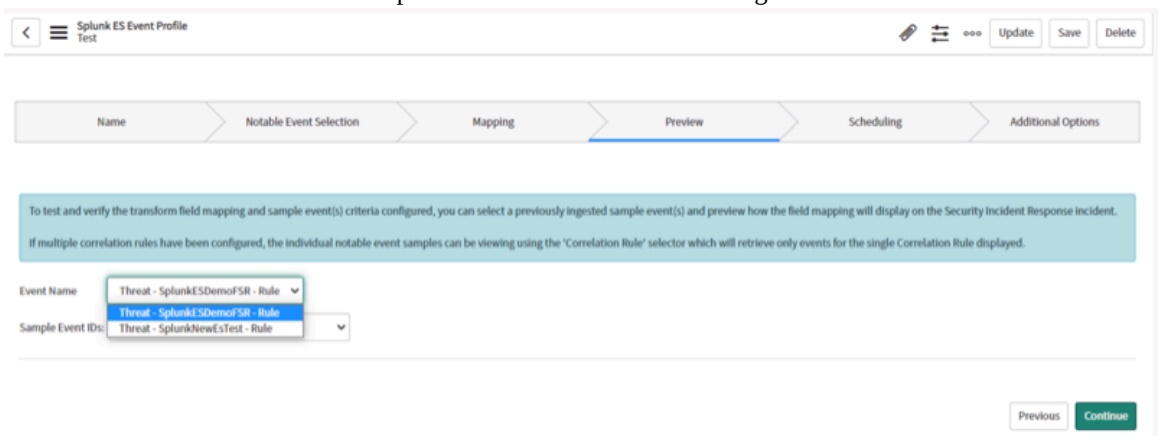
Zeigen Sie eine Vorschau eines Security Incidents an, und bearbeiten Sie die Zuordnung nach Bedarf erneut, um Felder mit Fehlern zu beheben oder fehlende Daten auszufüllen. Wenn die Vorschau nicht erfolgreich abgeschlossen wurde, können Sie nicht mit dem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Planungsschritt fortfahren. Vorschauen von SIR Security Incidents werden nicht als tatsächliche Incidents in gespeichert SIR Produkt.

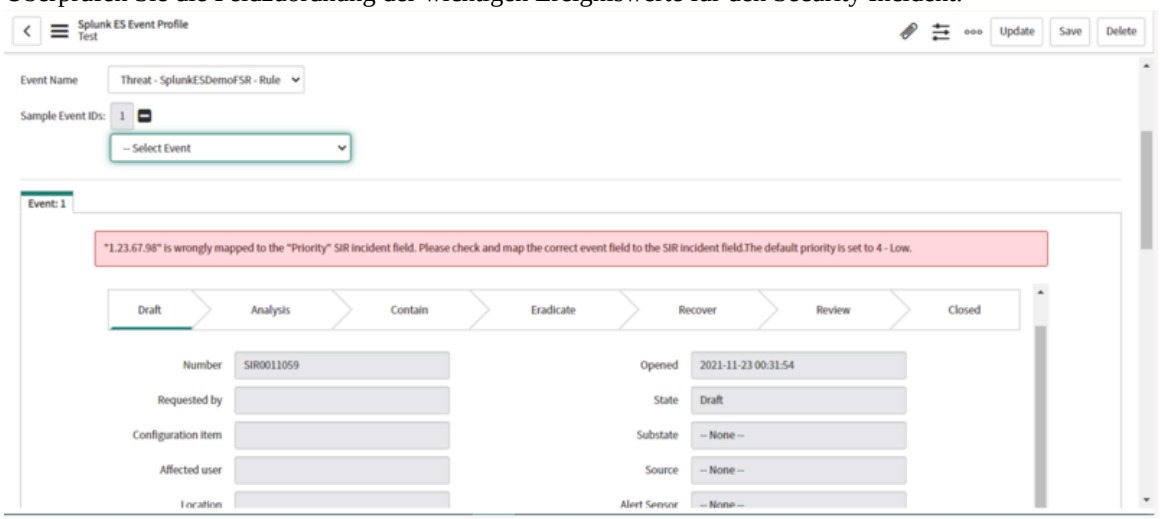
Prozedur

1. Wenn die Security Incident-Vorschau nicht angezeigt wird, klicken Sie auf **Vorschau** In der Fortschrittsleiste.
2. Wählen Sie in der Auswahlliste Ereignisname ein Element aus, wenn mehrere Ereignisse verwendet wurden.
3. Wählen Sie Ereignis-IDs aus der Auswahlliste Beispiel-IDs für bemerkenswerte Ereignisse aus.
4. Wählen Sie in der Auswahlliste Beispiel-IDs für bemerkenswerte Ereignisse ein Element aus.



Der Security Incident wird angezeigt. Ändern Sie keine Informationen in den Feldern. Diese Ansicht ist schreibgeschützt, und ein Datensatz dieses Security Incidents wird nicht gespeichert.

5. Überprüfen Sie die Feldzuordnung der wichtigen Ereigniswerte für den Security Incident.



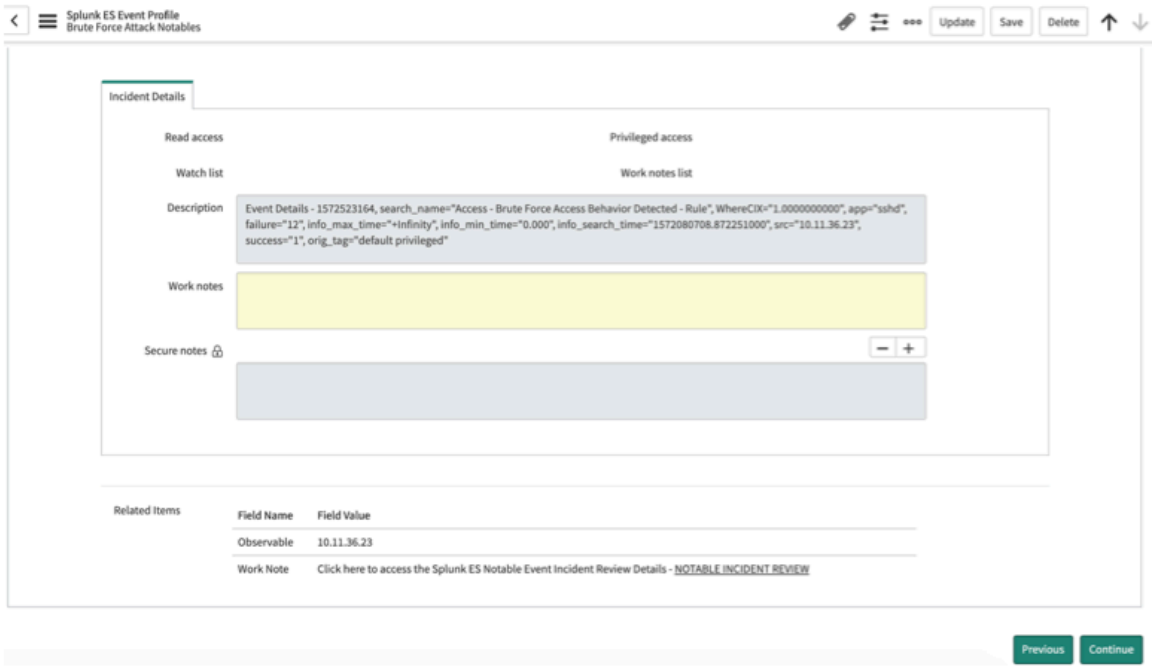
Das vorangegangene Bild ist ein Beispiel für eine Vorschau mit einem Zuordnungsfehler. In diesem Beispiel hat ein Feldwert aus dem bemerkenswerten Ereignis keinen akzeptablen Wert für das Referenzfeld im SIR-Incident-Formular. Eine Fehlermeldung wird angezeigt, die angibt, dass für keinen Eingabewert gefunden wurde Konfigurationselement Feld in ServiceNow® Kundenmanagement-Datenbank (CMDB). Daher wird dieser zugeordnete Feldwert ohne weitere Änderung nicht im SIR Security Incident-Formular angezeigt.

6. Klicken Sie auf, um diesen Fehler zu beheben **Zuordnung** In der Fortschrittsleiste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Bearbeiten Sie die Zuordnung, um falsche Werte zu korrigieren oder fehlende Daten auszufüllen.
8. Zeigen Sie erneut eine Vorschau der Zuordnung an, und beheben Sie alle Fehler, die in Fehlermeldungen beschrieben werden.

   Die folgende Abbildung ist ein Beispiel für die Registerkarte Incident-Details in der unteren Hälfte von SIR Security Incident, nachdem alle Fehlermeldungen gelöst wurden. In diesem Beispiel wurden die Felder Beschreibung und Arbeitsnotizen zugeordnet, und diese Felder werden mit den Werten aus den Wertepaaren ausgefüllt, die aus abgerufen wurden Splunk Enterprise Security Bemerkenswerte Ereignisbeispiele. Das erste Feld „Arbeitsnotizen“ hat keinen Wert. Dieses Feld wurde während des Zuordnungsschritts im Zuordnungsraster leer gelassen. Die zusätzlichen Arbeitsnotizfelder mit Werten wurden dem Zuordnungsabschnitt hinzugefügt.



9. Nachdem Sie Fehler behoben und überprüft haben, ob die Felder so sind, wie Sie sie möchten, wählen Sie eine Option aus, um fortzufahren.

Nächste Maßnahme

Wenn keine Fehlermeldungen angezeigt werden und Sie mit der Feldzuordnung für den Security Incident zufrieden sind, ist der nächste Schritt bis Planen und rufen Sie Warnungen für ab Splunk Enterprise Event Ingestion Integration.

Planen und rufen Sie neue und aktualisierte wichtige Ereignisse für ab Splunk Enterprise Security Integration der Ereigniserfassung

Für automatisierte Erfassungsprofile für wichtige Ereignisse ist dieser Schritt in der Ereignisprofilkonfiguration erforderlich. Während dieses Schritts können Sie die Standardeinstellungen für den Abruf wichtiger Ereignisse überprüfen oder die Planung nach Bedarf ändern. Mit diesem Schritt können Sie auch historische wichtige Ereignisse mithilfe eines Datumsbereichs abrufen.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Bei Profilen für die automatisierte Erfassung bedeutender Ereignisse wählen Sie aus, ob Sie während des Planungsschritts historische wichtige Ereignisse erfassen möchten. Sie wählen auch aus, wie oft Sie nach zukünftigen neuen wichtigen Ereignissen und aktualisierten wichtigen Ereignissen abfragen, die der Warnungsprofilkonfiguration entsprechen.

Bei automatisierten Profilen zur Erfassung bedeutender Ereignisse überprüfen und ändern Sie die Planung und den Warnungsabruf, bevor das Profil aktiviert wird. Dies ist ein erforderlicher Schritt für den gesamten Ereignisprofilkonfigurationsprozess für geplante Warnungsprofile.

Sie konfigurieren diese Abfrageintervalle pro Profil. Die Leistung von Splunk Die Integration der Ereigniserfassung kann durch die verschiedenen Abfrageintervalle beeinträchtigt werden. Bei der Planung möchten Sie möglicherweise die Reduzierung des Abfrageaufwands auf dem abgleichen Splunk Enterprise Security Server gegen den Wunsch, so bald wie möglich benachrichtigt zu werden, wenn ein bemerkenswertes Ereignis erstellt oder aktualisiert wird. Für jedes Profil ist ein fünf-Minuten-Standardwert festgelegt. Sie können diese Einstellung jedoch bei Bedarf auf eine Minute ändern.

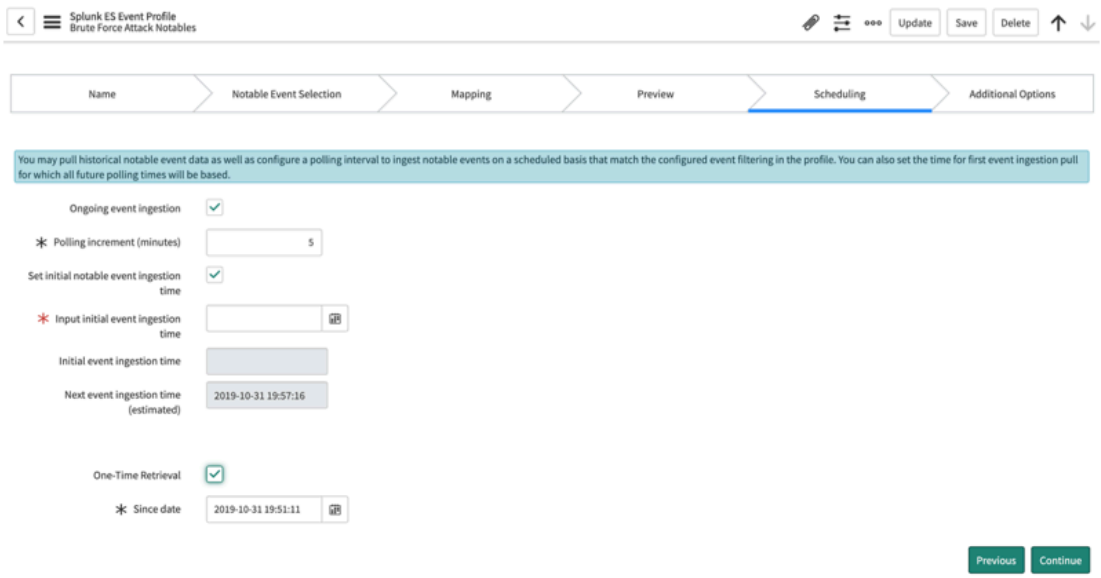
Neue und aktualisierte wichtige Ereignisse werden abgerufen

Wenn der Abfragezeitplan festgelegt ist, ruft die geplante Aufgabe sowohl neue als auch aktualisierte wichtige Ereignisse ab, die zuvor abgerufen wurden, aber die Incident-Filterkriterien nicht erfüllten. Dies bietet Ihnen die Flexibilität, Incidents basierend auf Kriterien zu erstellen, die möglicherweise nicht vorhanden sind, wenn ein wichtiges Ereignis zum ersten Mal erstellt wird, aber verfügbar werden, nachdem ein Update erfolgt ist, z. B. während der Untersuchungsphase. Sobald ein Incident für ein bestimmtes bemerkenswertes Ereignis erstellt wurde, werden seine nachfolgenden Aktualisierungen ignoriert, da erwartet wird, dass der betreffende nun als aktives Ereignis behandelt wird ServiceNow® Security Incident. Alle anderen wichtigen Elemente, die zuvor erfasst wurden, aber die Kriterien für die Incident-Generierung nicht erfüllen, werden weiterhin abgerufen und anhand der Incident-Generierungskriterien überprüft, bis sie Teil eines aktiven Incident werden.

Prozedur

1. Wenn die Seite „Zeitplanung“ im Fortschrittsbalken nicht angezeigt wird, wählen Sie aus **Zeitplanung** .
2. Wählen Sie eines aus, um zu planen, wie und wann wichtige Ereignisse aus abgerufen werden Splunk Enterprise Security Konsole.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ein Beispiel für die Planung einer ersten Zeit der Erfassung eines bedeutenden Ereignisses, wenn Sie täglich eine haben Splunk Sicherheitsprüfung, die einmal täglich um 4 Uhr Ortszeit ausgeführt wird. Sie können das entsprechende Profil für wichtige Ereignisse in Ihrem einrichten ServiceNow AI Platform Instanz, die um 4:05 UHR Ortszeit ausgeführt werden soll, um das Security Failure-Ereignis sofort zu erfassen und einen Security Incident zu erstellen. Geben Sie Ein `04 05 00` Im Feld erste Ereigniserfassung. Geben Sie im Feld Schritt (Minuten) den Wert ein `1440` (24 Stunden) zum Planen der nächsten Ereigniserfassung für 24 Stunden ab der ersten Ereigniserfassung. Sowohl die erste Ereigniserfassungszeit als auch die nächste Ereigniserfassungszeit werden in den Feldern angezeigt.

3. Um die Einstellungen für dieses Beispiel zu konfigurieren, führen Sie die folgenden Schritte aus.

   a. Wenn die Seite „Zeitplanung“ angezeigt wird, wählen Sie aus **Laufende Ereigniserfassung** Kontrollkästchen zum Aktivieren dieser Option.

   b. Geben Sie im Feld Schritt (Minuten) den Wert ein `1440` (24 Stunden).

   c. Klicken Sie auf **Wählen Sie erste Ereigniserfassung aus** Kontrollkästchen zum Aktivieren der Bearbeitung der Felder „erste Ereigniserfassung“ und „nächste Ereigniserfassung“.

   d. Geben Sie im Feld erste Ereigniserfassung ein `04 05 00` .
   Im Feld nächste Ereigniserfassung (geschätzt) wird die Zeit der nächsten Ereigniserfassung angezeigt.

4. Klicken Sie auf eine der folgenden Optionen, um mit der Profilkonfiguration fortzufahren.

Automatisieren Sie Aktualisierungen und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status

Security Incidents können erstellt und aktualisiert werden, nachdem sie mit einer bidirektionalen Schnittstelle mit erstellt wurden Splunk Enterprise Security Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Die Splunk Enterprise Security Die Integration verfügt über eine bidirektionale Schnittstelle, mit der wichtige Ereignisse Security Incidents erstellen und die wichtigen Ereignisse aktualisieren können, nachdem der Security Incident erstellt und/oder geschlossen wurde.

Zu den relevanten Incident-Details gehören SIR Incident-Nummer, Zuweisungsgruppe, SIR Incident-URL. Dieser Abschnitt ist der letzte Teil der Profilkonfigurationseinrichtung, die optionale Funktionen zum Aktualisieren von bietet Splunk Enterprise Security Bemerkenswerte Ereignisse.

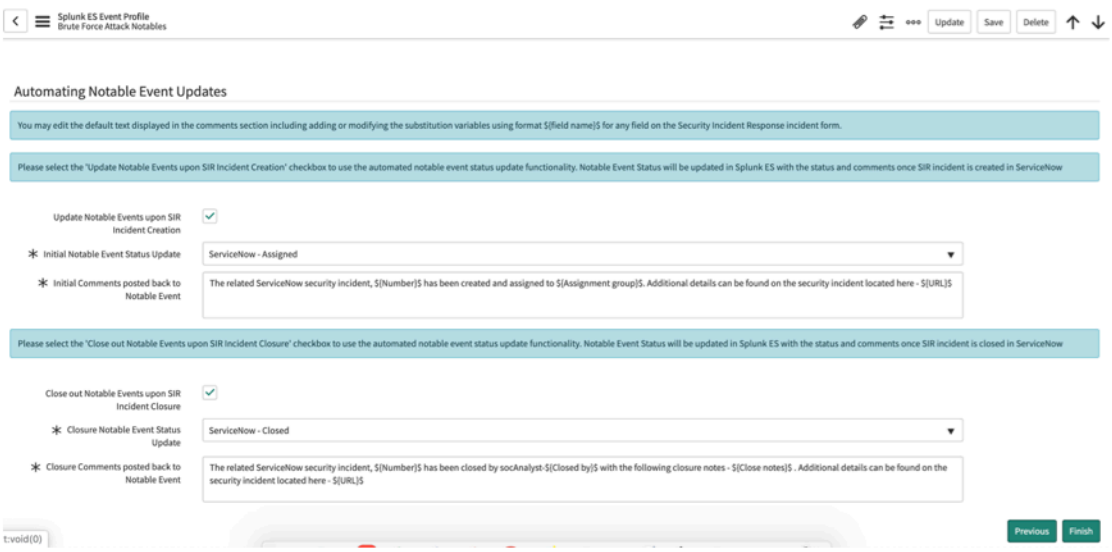
Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

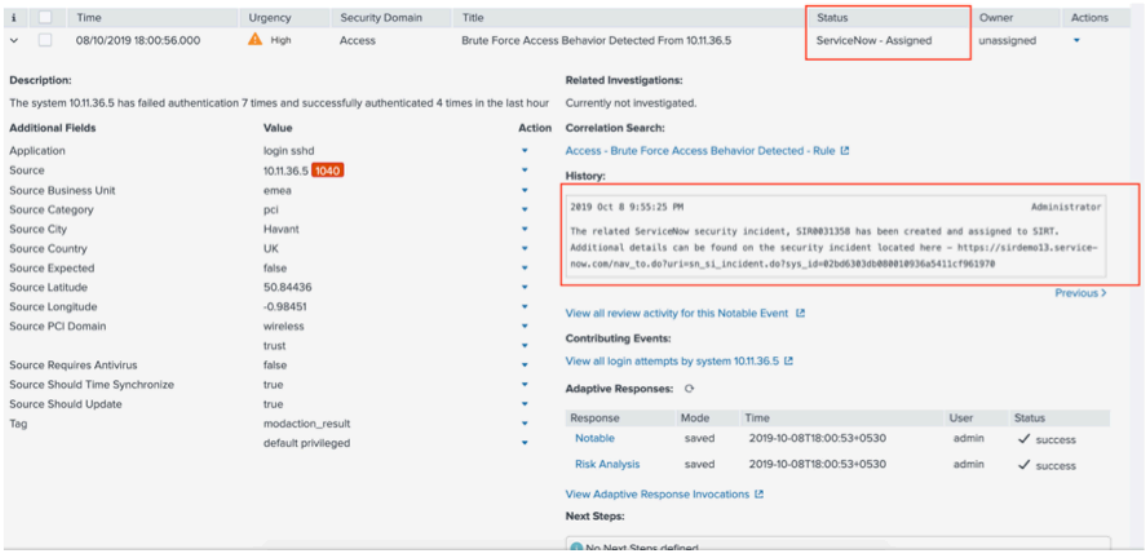
1. Wenn die Seite „zusätzliche Optionen“ im Fortschrittsbalken nicht angezeigt wird, wählen Sie aus **Zusätzliche Optionen** .
2. Befolgen Sie die folgenden Anweisungen, um die Konfiguration für die Aktualisierung wichtiger Ereignisse basierend auf Security Incident-Updates abzuschließen.
3. Klicken Sie Auf **Beenden** Um die Konfiguration abzuschließen.
   Ein Bestätigungsdialogfeld wird angezeigt. Sie haben das Setup und die Konfiguration für die Integration erfolgreich abgeschlossen. Aktivieren Sie dieses Profil, um wichtige Ereignisse aus abzurufen Splunk Enterprise Security Konsole basierend auf Ihrer Planung. Es gibt ein Limit von 1.000 Security Incidents, die innerhalb von 24 Stunden erstellt werden können. Pro ausgelöster Warnung gelten bis zu 100 wichtige Ereignisse. Nachfolgende wichtige Ereignisse werden ignoriert, nachdem die Grenzwerte erreicht wurden.

   Die folgende Abbildung zeigt die Registerkarte „zusätzliche Optionen“ mit ausgefüllten Standardwerten:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Konfiguration „zusätzliche Optionen“ aktiviert ist, zeigt die Incident-Überprüfung eines bedeutenden Ereignisses die Statusänderung und eine Aktualisierung der Verlaufskommentare an:



Richten Sie ein Profil für die manuelle Ereignisweiterleitung ein

Abhängig vom definierten Profil Splunk ES Bemerkenswerte Ereignisse werden manuell als diskrete bemerkenswerte Ereignisse an weitergeleitet Security Operations Umgebung von ServiceNow AI Platform Instanz.

So richten Sie ein Profil für die manuelle Weiterleitung wichtiger Ereignisse ein:

Aufgabe	Abschnitt
Erstellen Sie ein Ereignisprofil	Siehe Erstellen Sie Profile für manuell weitergeleitete Ereignisse
Ordnen Sie wichtige Ereignisfelder zu	Siehe Zuordnung von wichtigen Ereignisfeldern für Splunk Enterprise Security Integration
Erstellen Sie anwenderdefinierte Zuordnungen	Siehe Erstellen Sie Zuordnungen für Splunk ESÜberprüfung von Incidents und Details zu beitragenden Ereignissen (manuelle Weiterleitung)
Zeigen Sie eine Vorschau des Security Incidents an	Siehe Vorschau des Security Incidents für anzeigen Splunk Enterprise Security Integration der Ereigniserfassung
Richten Sie Ihr ein Splunk Umgebung für manuelle Erfassung	Siehe Richten Sie Ihr ein Splunk Umgebung für die manuelle Ereigniserfassung für Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung
Automatisieren Sie Aktualisierungen und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status	Siehe Automatisieren Sie Aktualisierungen und den Abschluss wichtiger Ereignisse basierend auf dem SIR-Incident-Status

Erstellen Sie Profile für manuell weitergeleitete Ereignisse

Sie können ein Profil für manuell weitergeleitete Ereignisse einrichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:

Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Prozedur

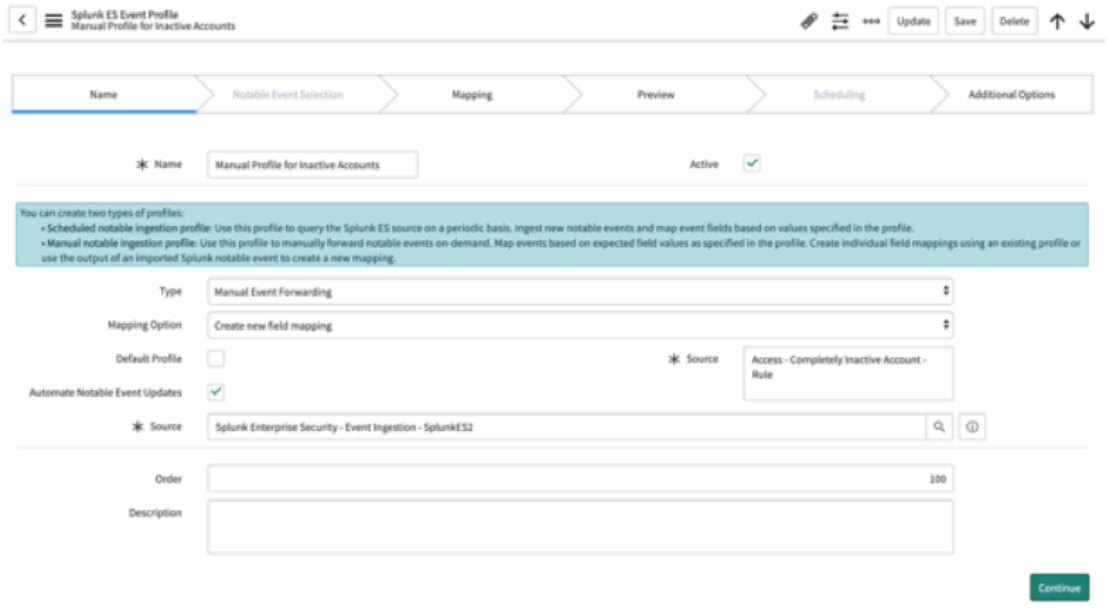
Führen Sie die folgenden Schritte aus, um ein Profil zu erstellen, das die manuelle Ereignisweiterleitung unterstützt.

Für Ereignisse, die Sie bei Bedarf von Ihrem weiterleiten Splunk Enterprise Security Konsole können Sie die individuelle Feldzuordnung auf einem beliebigen vorhandenen Profil basieren. Alternativ können Sie ein neues Zuordnungsraster für exportierte Anhangsdaten erstellen. Ereignisse, die Sie manuell weiterleiten, sind im Ereignisprofil nicht geplant.

a. Wenn nicht bereits ausgewählt, wählen Sie in der Auswahlliste für das Feld Typ die Option aus **Manuelle Ereignisweiterleitung** .

b. Wählen Sie im angezeigten Feld Zuordnungsoption aus der Auswahlliste eine Zuordnungsoption aus, um fortzufahren.

Weitere Informationen zu den verfügbaren Zuordnungsoptionen in der Auswahlliste Zuordnungsoptionen finden Sie in den folgenden Abbildungen und Tabellen.



Option „neue Feldzuordnung erstellen“

Option oder Feld	Beschreibung
Erstellen Sie eine neue Feldzuordnungsoption	Neue Feldzuordnung für Ihr Ereignis. Wenn Sie keine Feldzuordnung haben, die dem Profil ähnelt, das Sie erstellen, wählen Sie diese Option aus, um eine neue Zuordnung zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

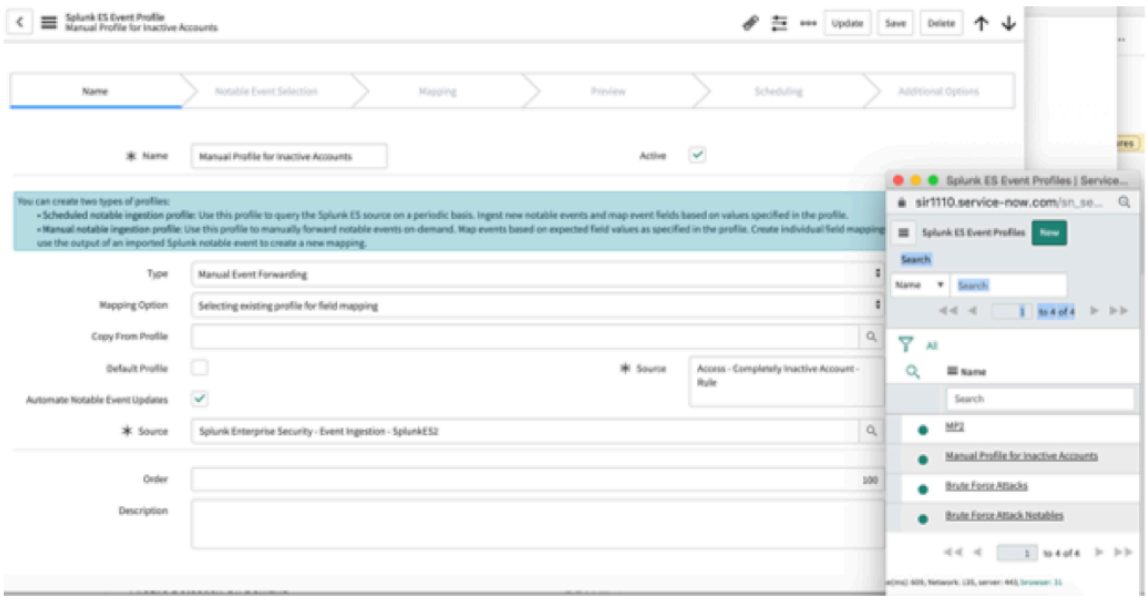
Option oder Feld	Beschreibung
Standardprofil	Standardmäßiges Ereignisweiterleitungsprofil für alle Splunk Ereignisse. Der Standardwert ist gelöscht (deaktiviert). Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die manuelle Ereignisweiterleitung. Dieses Profil wird verwendet, wenn keine Übereinstimmung für die Quelle aus dem manuell weitergeleiteten Ereignis vorhanden ist. Es wird zum Standardprofil für alle Ereignisse mit unbekannten Quellen. Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist.
Quelle (Feld für bemerkenswertes Ereignis)	Dies ist ein Feld, das normalerweise die Korrelationsregel definiert, die das bemerkenswerte ausgelöst hat, z. B. Brute Force-Angriffe. Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist. Falls verfügbar, ermöglicht dieses Feld die Zuordnung eindeutiger Ereignisfelder zu Security Incident-Feldern basierend auf der splunk-Korrelationsregel, die sich normalerweise für verschiedene Ereignistypen unterscheidet. Wenn Sie verschiedene Korrelationsregeln separat verwalten möchten, können Sie verschiedene Profil-Ereignisprofile basierend auf der Korrelationsregel erstellen, um diese Anforderung zu erfüllen.
Aktualisierung bedeutender Ereignisse automatisieren	Aktivieren Sie dieses Kontrollkästchen, wenn Sie den Status des bedeutenden Ereignisses aktualisieren und zusätzliche Kommentare hinzufügen möchten, wenn ein SIR-Incident aus dem bedeutenden Ereignis erstellt wird und/oder wenn der SIR-Incident geschlossen wird. Dies tritt sowohl für die anfänglich auslösenden bedeutenden Ereignisse, die den SIR-Incident erstellen, als auch für zusammengefasste Ereignisse auf.
Quelle (Splunk Server)	Die Splunk Server, den Sie als Quelle für wichtige Ereignisse konfiguriert haben. Wenn Sie mehrere haben Splunk Server konfiguriert, wählen Sie den entsprechenden Server für die wichtigsten Ereignistypen aus, die für das Profil

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
	aktualisiert werden. Sie müssen einen Wert eingeben.
Reihenfolge	Der Standardwert ist 100. Belassen Sie diese Einstellung auf den Standardwert. Wenn Sie eine große Anzahl von Profilen erstellt haben, bietet dieser Wert eine Laufzeitausführungspriorität, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam haben. Der Workflow im Profil mit der niedrigsten Zahl hat die höchste Priorität.
(Optional) Beschreibung	Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Überprüfen Sie für ein Profil mit einer neuen Feldzuordnung, ob Sie einen Wert in das Feld Quelltyp eingegeben haben, und klicken Sie auf **Fahren Sie Fort** Um mit dem Zuordnungsschritt der Konfiguration fortzufahren.

Weitere Informationen zu einem Profil mit einer vorhandenen Feldzuordnung finden Sie in der folgenden Abbildung und Tabelle.



Wählen Sie ein vorhandenes Profil für die Feldzuordnungsoption aus

Option oder Feld	Beschreibung
Vorhandenes Profil für Feldzuordnung auswählen	Verwenden Sie eine vorhandene Feldzuordnung für Ihr neues Profil für wichtige Ereignisse. Das Feld aus Profil kopieren wird angezeigt. Führen Sie die folgenden Schritte aus, um eine vorhandene Feldzuordnung für dieses Profil zu kopieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
	i. Klicken Sie links neben dem angezeigten Feld aus Profil kopieren auf das Suchsymbol. ii. In Splunk Liste „es-Ereignisprofile“, die angezeigt wird, klicken Sie auf den Profilnamen, der die Karte enthält, die Sie kopieren möchten. Der Profilname wird im Feld aus Profil kopieren angezeigt.
Standardprofil	Standardmäßiges Ereignisweiterleitungsprofil für alle Splunk Bemerkenswerte Ereignisse mit nicht übereinstimmender Quelle. Standard ist gelöscht (deaktiviert). Wenn diese Option aktiviert ist, wird dieses Profil zum Standardprofil für die manuelle Ereignisweiterleitung. Das Feld Quelle ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist.
Quelle (Feld für bemerkenswertes Ereignis)	Dies ist ein Feld, das normalerweise die Korrelationsregel definiert, die das bemerkenswerte ausgelöst hat, z. B. Brute Force-Angriffe. Dieses Feld ist nicht verfügbar, wenn die Standardprofiloption aktiviert ist. Falls verfügbar, ermöglicht dieses Feld die Zuordnung eindeutiger Ereignisfelder zu Security Incident-Feldern basierend auf der splunk-Korrelationsregel, die sich normalerweise für verschiedene Ereignistypen unterscheidet. Wenn Sie verschiedene Korrelationsregeln separat verwalten möchten, können Sie verschiedene Profil-Ereignisprofile basierend auf der Korrelationsregel erstellen, um diese Anforderung zu erfüllen.
Automatisieren Sie Wichtige Ereignisse	Aktivieren Sie dieses Kontrollkästchen, wenn Sie den Status des bedeutenden Ereignisses aktualisieren und zusätzliche Kommentare hinzufügen möchten, wenn ein Security Incident aus dem bedeutenden Ereignis erstellt wird oder wenn der Security Incident geschlossen wird. Dies tritt sowohl für die anfänglich auslösenden wichtigen Ereignisse, die den Security Incident erstellen, als auch für zusammengefasste Ereignisse auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option oder Feld	Beschreibung
Quelle (Splunk Server)	Splunk Server- oder Suchende, die Sie als Quelle für wichtige Ereignisse konfiguriert haben. Wenn Sie mehrere haben Splunk Server konfiguriert, wählen Sie den entsprechenden Server für die wichtigsten Ereignistypen aus, die für das Profil aktualisiert werden. Sie müssen einen Wert eingeben.
Reihenfolge	Der Standardwert ist 100. Belassen Sie diese Einstellung auf den Standardwert. Wenn Sie mehrere Profile erstellt haben, gibt dieser Wert eine Laufzeitausführungspriorität an, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam haben. Der Workflow im Profil mit der niedrigsten Zahl hat die höchste Priorität.
(Optional) Beschreibung	Text, der Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

Klicken Sie unten im Formular zur Auswahl einer vorhandenen Zuordnung für Ihr Profil auf **Beenden** Um die Profilkonfiguration abzuschließen.

Erstellen Sie Zuordnungen für Splunk ESÜberprüfung von Incidents und Details zu beitragenden Ereignissen (manuelle Weiterleitung)

Während des Zuordnungsschritts für ein wichtiges Ereignis ordnen Sie einzelne Ereignisfelder aus wichtigen Ereignissen zu Feldern in einem zu ServiceNow AI Platform Security Incident Response(SIR) Security Incident.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Ordnen Sie bis zu fünf wichtige Ereignisse aus der Spalte „Stichprobenerfassung für bedeutendes Ereignis“ auf der linken Seite des Formulars den Security Incident-Feldern in der Spalte „SIR-Incident-Feldzuordnung“ auf der rechten Seite zu.

Erstellen Sie anwenderdefinierte Zuordnungen, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Standardfelder, die normalerweise ein wichtiges Feld sind, das im SIR-Incident-Formular ausgefüllt werden soll, werden angezeigt. Diese Felder können jedoch entfernt werden, und zusätzliche Felder können mit den Schaltflächen + und - angezeigt werden. Erstellen Sie anwenderdefinierte Karten, indem Sie die Felder im Zuordnungsraster auf der rechten Seite des Formulars hinzufügen oder entfernen. Durch das Anpassen der Felder können Sie zuordnen Splunk Felder, die nicht im Standardzuordnungsraster auf angezeigt werden SIR Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

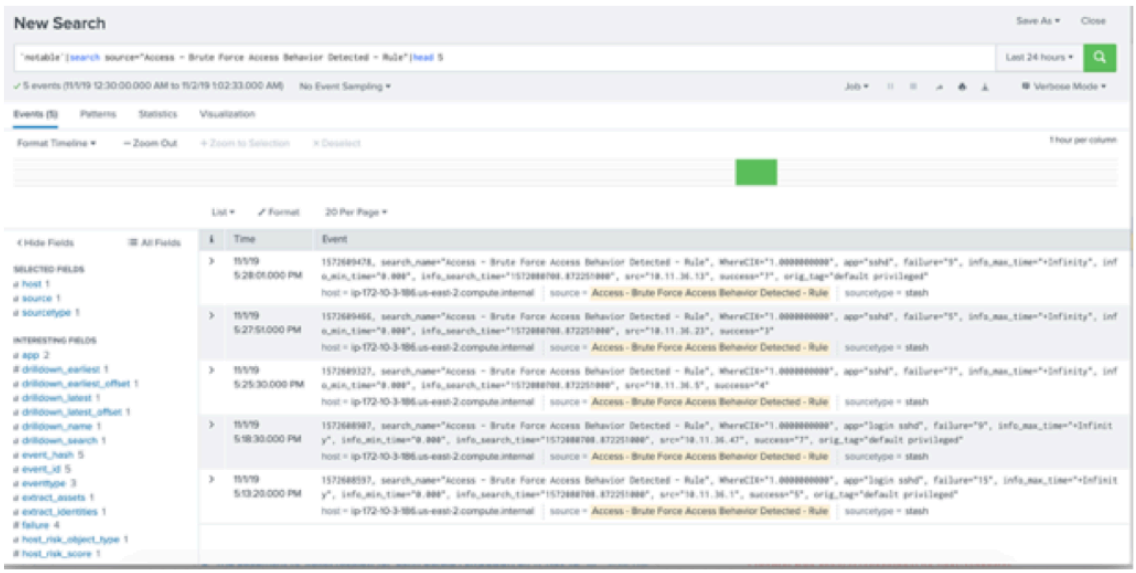
1. Wenn das Zuordnungsformular nicht angezeigt wird, klicken Sie auf **Zuordnung** Auf der Fortschrittsleiste.
2. Führen Sie die folgenden Schritte aus, um Anhangsdaten in hochzuladen ServiceNow AI Platform® Instanz.

   a. Wenn Sie sich noch nicht angemeldet haben, melden Sie sich bei an Splunk Enterprise Konsole.

   b. Navigieren Sie zur Registerkarte Suche, und geben Sie einen Namen für eine Suche ein, die die wichtigen Ereignisdaten enthält, die Sie exportieren möchten.
   Ein Beispiel für ein Suchformat zum Abrufen wichtiger Ereignisse für die Korrelationsregel für Brute-Force-Zugriffsverhalten wäre das folgende: „Notable“|search Source=„Zugriff – Brute-Force-Zugriffsverhalten erkannt – Regel“.

   c. Erweitern Sie das bedeutende Ereignis, und wählen Sie in der Spalte Feld die Felder aus, die Sie importieren möchten.

   Diese Felder sind die Feld-Wert-Paare, die exportiert und auf der Zuordnungsseite in angezeigt werden ServiceNow AI Platform® Instanz.



   d. In Ihrem Splunk Enterprise Konsole klicken Sie oben rechts auf der Suchseite auf **Exportieren** Symbol.

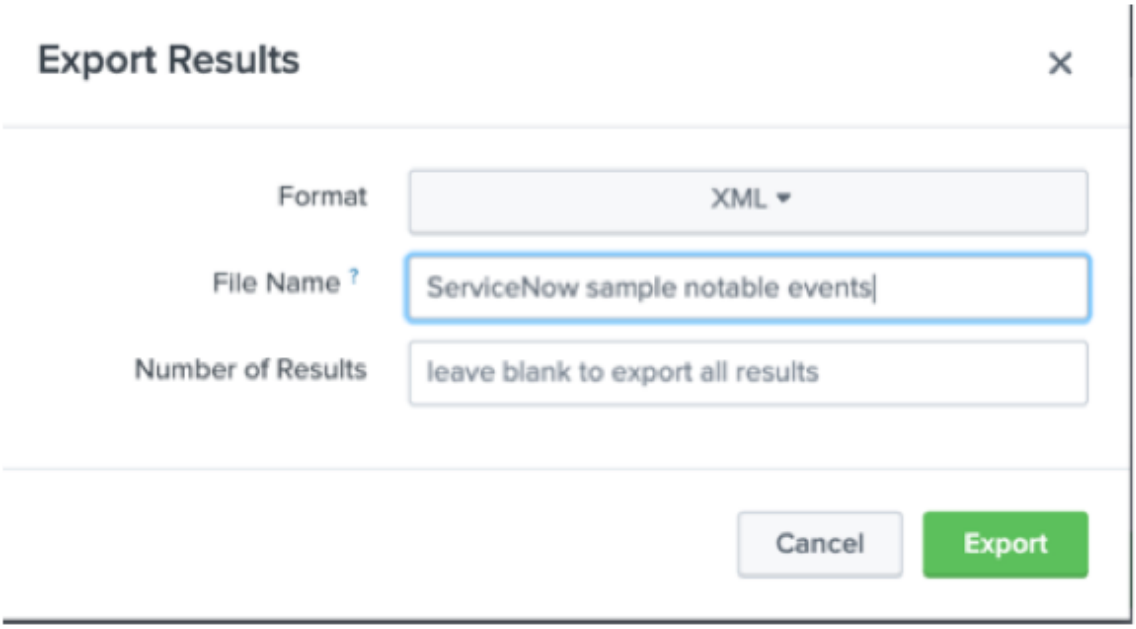
   e. Klicken Sie in der Auswahlliste für das Feld Format im angezeigten Dialogfeld auf **XML-Format** .

   f. **Wahlweise:** Geben Sie einen neuen Dateinamen ein.

   g. Klicken Sie auf **Exportieren**.

Automatische Übersetzung

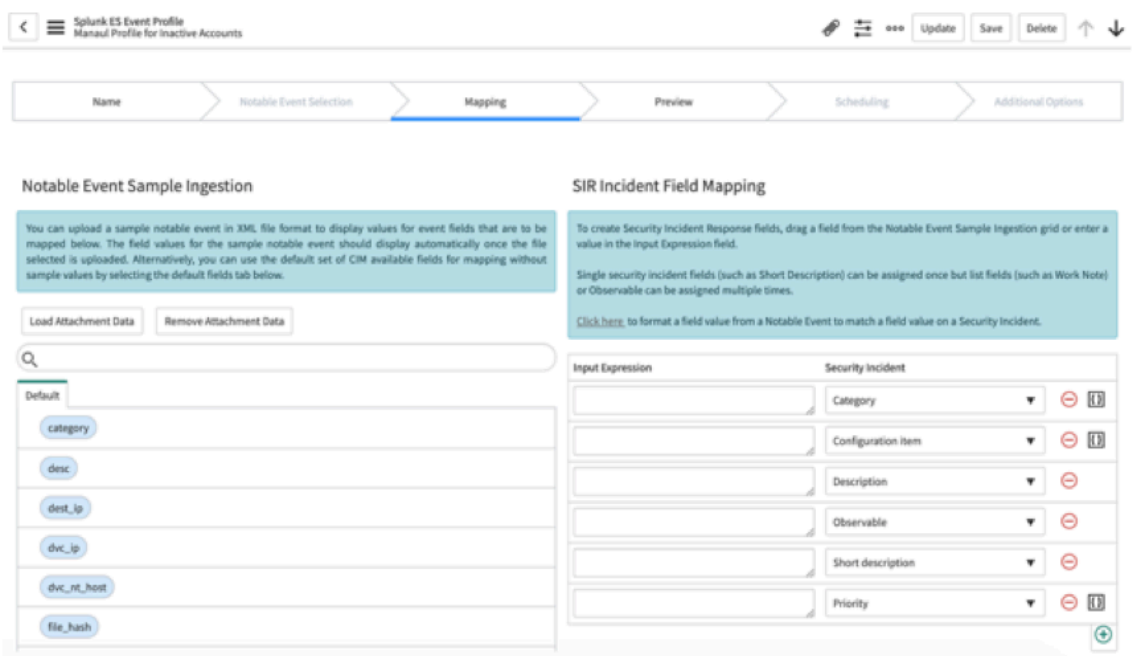
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Exportiert Splunk Die XML-Datei für wichtige Ereignisse muss jetzt auf hochgeladen werden ServiceNow AI Platform® Instanz.

h. Wenn die Zuordnungsseite nicht bereits in angezeigt wird ServiceNow AI Platform® Instanz, klicken Sie auf **Zuordnung** In der Fortschrittsleiste.

i. Klicken Sie in der Spalte Beispielerfassung für ein Ereignis auf **Laden Sie Anhangsdaten** .



j. Klicken Sie im angezeigten Dialogfeld auf **Wählen Sie Dateien aus** Und navigieren Sie zu .Xml Datei, die Sie exportiert haben, und klicken Sie auf **Öffnen** .
Nachdem Sie auf klicken, um Anhangsdaten für manuell weitergeleitete Ereignisse zu laden, die Splunk ES Wichtige Ereignisfelder werden auf der linken Seite des Formulars ausgefüllt. Diese Werte sind die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldwerte, die Sie den Security Incident-Feldern auf der Seite „Sir Incident-Feldzuordnung“ des Formulars zuordnen.
Die Wertpaare für die Felder, die Sie für das Ereignis exportiert haben, werden auf der linken Seite des Zuordnungsformulars angezeigt.

3. Führen Sie die Schritte 5 bis 10 im aus Erstellen Sie Zuordnungen für Splunk ESÜberprüfung von auffälligen Ereignis-Incidents und Details zu beitragenden Ereignissen (geplante Erfassung) Abschnitt.

Richten Sie Ihr ein Splunk Umgebung für die manuelle Ereigniserfassung für Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung

Installieren und richten Sie den ein ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Security Anwendung in Ihrem Splunk enterprise-Konsole oder Splunk-Cloud-Instanz, wenn Sie Ereignisse manuell und bei Bedarf aus exportieren möchten Splunk Enterprise Security Konsole für diese Integration.

Vorbereitungen

Installieren und Einrichten von ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Security Anwendung in Ihrem Splunk enterprise-Konsole oder Splunk-Cloud-Instanz ist optional.

Überprüfen Sie, ob Sie die Anwendung für diese Integration über installiert haben ServiceNow Store Vor der Installation des Add-on-Plugins aus splunkbase, das für die manuelle Ereigniserfassung erforderlich ist. Wenn Sie die Anwendung für die Integration nicht über installiert haben ServiceNow Store, Siehe Installieren und konfigurieren Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung Und befolgen Sie die Anweisungen zur Installation.

Erforderliche Rolle: Splunk Enterprise Security Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie Ereignisse manuell und bei Bedarf aus exportieren möchten Splunk Enterprise Konsole für die -Integration herunterladen, installieren und einrichten ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Security Aus SPLunkbase in Ihrem Splunk Enterprise Security Konsole. Dies ServiceNow Das Erweiterungs-Add-on ist erforderlich, damit Security Incidents aus manuell exportierten Ereignissen in erstellt werden können ServiceNow AI Platform Instanz. Dies ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Security Anwendung ist für verfügbar Splunkbase .

Für die manuelle Ereignisweiterleitung können Sie bis zu zwei verschiedene identifizieren ServiceNow AI Platform Endpunkte (Instanzen) in Ihrem Splunk Enterprise Security Konsole. Sie leiten die Ereignisse manuell an den Endpunkt oder Endpunkte weiter, um Security Incidents zu erstellen. Sie können beispielsweise sowohl eine Bereitstellungs-(Entwicklungs-)Instanz als auch eine Produktionsinstanz angeben. Indem Sie separate Instanzen angeben und primäre und sekundäre Workflows für jede Instanz benennen, können Sie auswählen, wohin Sie verschiedene Ereignisse weiterleiten möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn Sie noch nicht installiert haben ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Security, Führen Sie die folgenden Schritte aus, um es zu installieren und zu konfigurieren.

   a. Navigieren Sie zu Splunkbase .

   b. Suchen Sie nach ServiceNow Security Operations Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Security.

   Hinweis:
   Überprüfen Sie, ob Sie ausgewählt haben ServiceNow Security Operations Ereigniserfassungs-Add-on für Splunk Enterprise Security. Es gibt zusätzliche ServiceNow add-ons, die in dieser Liste angezeigt werden. Diese Add-ons sind für verschiedene bestimmt ServiceNow Splunk Integrationen und sind für diese Integration nicht erforderlich.

   c. Laden Sie die Anwendung herunter.

   d. Öffnen Sie Ihren Splunk Enterprise Security Account.

   e. Klicken Sie auf der Seite „Apps“ auf das Zahnradsymbol oder auf **Apps Verwalten** Verknüpfung in der Dropdown-Liste des Menüs.

   f. Klicken Sie oben links auf der angezeigten App-Seite auf **Installieren Sie die App aus der Datei** .

   g. Klicken Sie Auf **Wählen Sie Datei** , Wählen Sie aus ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Security, Und klicken Sie auf **Hochladen** .

   h. Starten Sie bei Aufforderung neu Splunk Enterprise.
   Die ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Security Ist in installiert Splunk Enterprise Security Konsole. Der nächste Schritt zum Einrichten des Add-ons.

2. Führen Sie die folgenden Schritte aus, um das Add-on einzurichten.

   a. In Splunk Enterprise Security, Klicken Sie auf **Apps** Zahnradsymbol oder **Apps Verwalten** In der Dropdown-Liste des Menüs.

   b. In der Liste der Anwendungen, die in angezeigt wird **Aktionen** Klicken Sie auf die Spalte **Einrichten** Für ServiceNow Security Operations Ereigniserfassungs-Add-on für Splunk Enterprise Security.

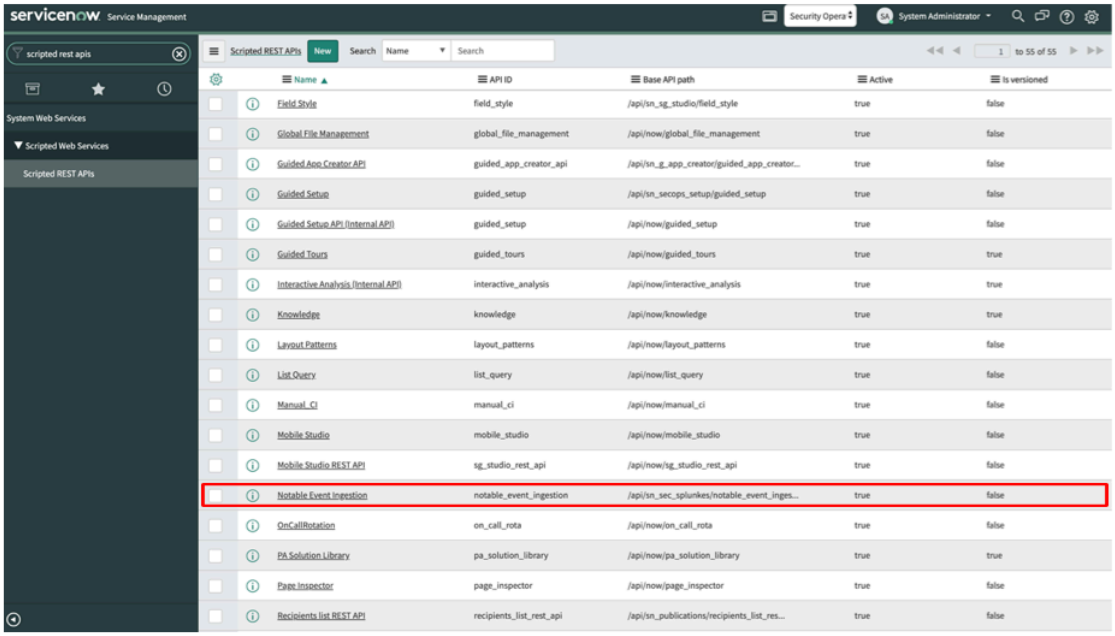
   c. Füllen Sie das Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt ein Beispiel für ein ausgefülltes Formular in Ihrem Splunk Enterprise Security Konsole.

Die folgende Abbildung ist ein Beispiel für die Liste geskriptete REST APIs in Ihrem ServiceNow AI Platform. In der Liste wird die Position des Endpunktwerts von angezeigt ServiceNow AI Platform Instanz, die Sie im Rahmen der Einrichtung für in das Formular eingeben ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Security Erweiterung in Ihrem Splunk Enterprise Security Konsole.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Im Setup-Formular in Ihrem Splunk Enterprise Security Konsole, klicken Sie auf **Speichern** Um Ihre Änderungen zu speichern.

   Nach einigen Minuten oben links im Formular in Ihrem Splunk Enterprise Security Konsole wird eine Nachricht angezeigt, dass der Datensatz erfolgreich aktualisiert wurde.

   Nachdem Sie das Formular gespeichert haben, werden die Namen (Workflow-Aktionsbezeichnungen) für gespeichert ServiceNow AI Platform Instanzen, die Sie im Formular erstellt haben, sind in der Auswahlliste Ereignisaktionen für ein ausgewähltes Ereignis einer Suche in verfügbar Splunk Enterprise Security Konsole.

Nächste Maßnahme

Wenn Sie Suchvorgänge noch nicht in gespeichert haben Splunk Enterprise Security-Konsole besteht der nächste Schritt darin, Suchvorgänge als Warnungen in Ihrer zu speichern Splunk Enterprise Security Konsole.

Kopieren Sie ein Ereignisprofil für Splunk Enterprise Security Integration der Ereigniserfassung

Kopieren Sie ein vorhandenes Profil und die zugehörigen Einstellungen, anstatt neue Profile zu erstellen. Wenn Sie mehrere Profile erstellen und die Einstellungen eines vorhandenen Profils wiederverwenden möchten, sollten Sie möglicherweise Alarmprofile kopieren, um Zeit zu sparen.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein Profil kopieren, wird der Profilname anfänglich geändert, um doppelte Profile zu vermeiden. Darüber hinaus wird das kopierte Profil deaktiviert (falsch), sodass es vor Abschluss der Konfiguration nicht versehentlich aktiviert wird. Kopieren Sie Profile, und

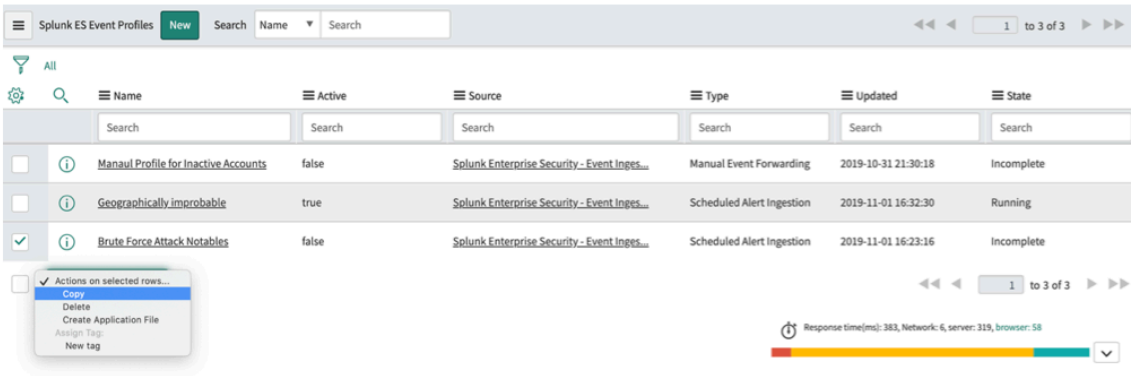
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

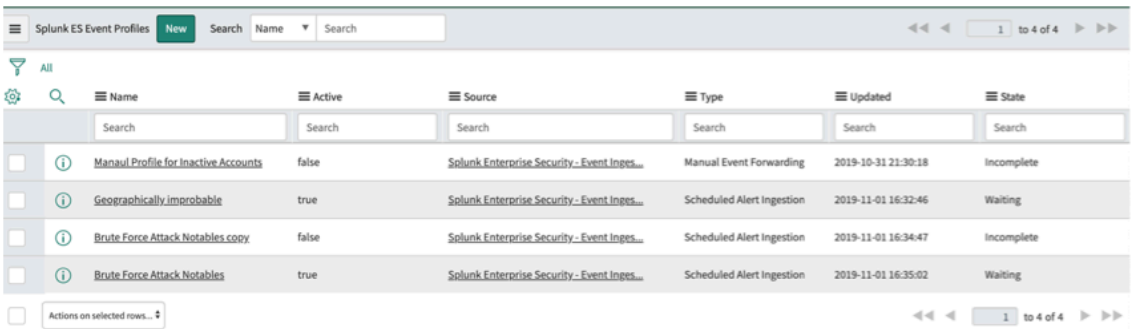
verwenden Sie vorhandene Zuordnungen für Security Incidents, die Sie bereits in der Vorschau angezeigt und verifiziert haben.

Prozedur

1. Navigieren zu **Alle** > **Splunk Integration** > **Splunk-Ereignisprofil**an.
2. In Splunk Liste „Ereignisprofile“, die angezeigt wird, wählen Sie ein Profil aus, das Sie kopieren möchten, und klicken Sie in der Auswahlliste Aktionen für ausgewählte Zeilen auf **Kopieren** .



Das Profil wird kopiert und in der Liste angezeigt. Die Kopie verfügt über alle Einstellungen des ursprünglichen Profils, einschließlich der Zuordnungs- und Planungskonfiguration. Der Name des Profils enthält Kopie. Obwohl das ursprüngliche Profil aktiviert ist (Wahr), die Kopie ist zu diesem Zeitpunkt deaktiviert (Falsch). Möglicherweise möchten Sie Werte des kopierten Profils bearbeiten und umbenennen, damit die Konfigurationseinstellungen nach Bedarf auf das neue Profil angewendet werden.



Sie haben die Einstellungen erfolgreich aus einem vorhandenen Profil in ein neues Profil kopiert.

Nächste Maßnahme

Sie werden aufgefordert, das neue Profil zu aktivieren (zu aktivieren), nachdem Sie den Konfigurationsschritt abgeschlossen haben.

Verwenden Sie den Skript-Editor, um Warnungswerte für zu formatieren Splunk Enterprise Security Integration der Ereigniserfassung

Verwenden Sie zusätzlich zu den direkt zugeordneten Feldern aus den erfassten wichtigen Ereigniswerten und den manuell eingegebenen Werten den Skript-Editor, um Feldwerte im Security Incident während des Zuordnungsschritts zu formatieren.

Vorbereitungen

Erforderliche Rolle: sn_si.ingestion_profile_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

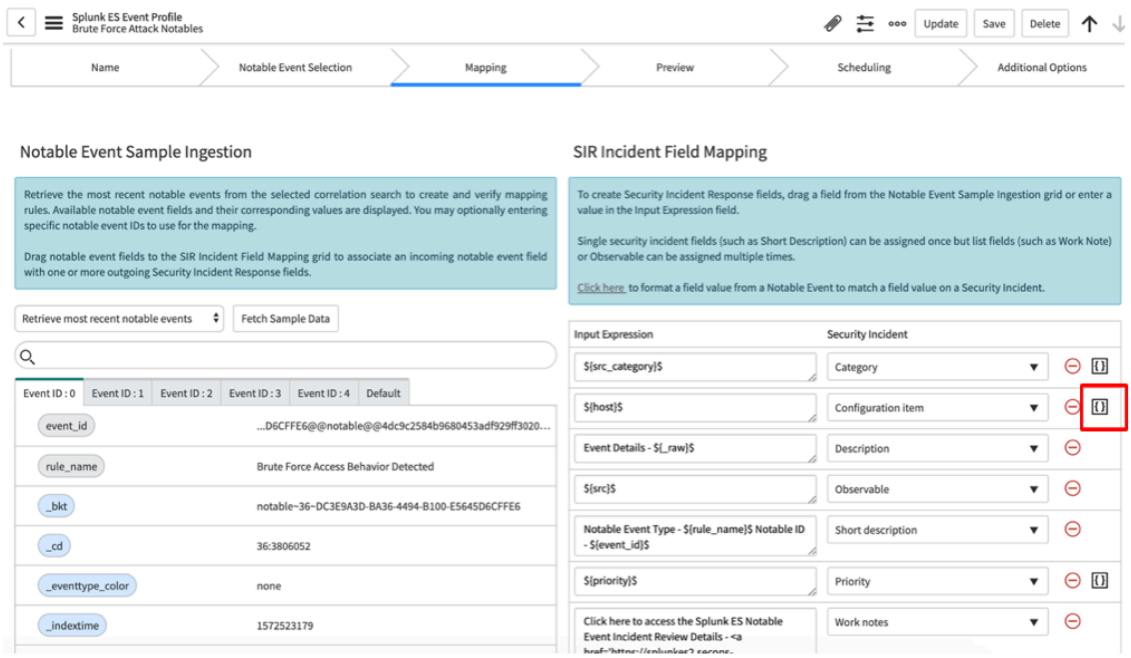
Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

In bestimmten Fällen Splunk Enterprise Security Wichtige Ereigniswerte werden den Feldern Kategorie, Konfigurationselement (CI) und erkennbares Element auf der zugeordnet SIR Incidents werden nicht unterstützt. Möglicherweise möchten Sie die zugeordneten Werte bearbeiten. Wenn Sie den Wert von übersetzen möchten Splunk Enterprise Security Bemerkenswertes Ereignis für einen Wert, der von diesen Feldern im unterstützt wird SIR Security Incident verwenden Sie den Skript-Editor.

Prozedur

1. Klicken Sie bei angezeigtem Zuordnungsformular auf den Link, um den Skript-Editor zu öffnen.



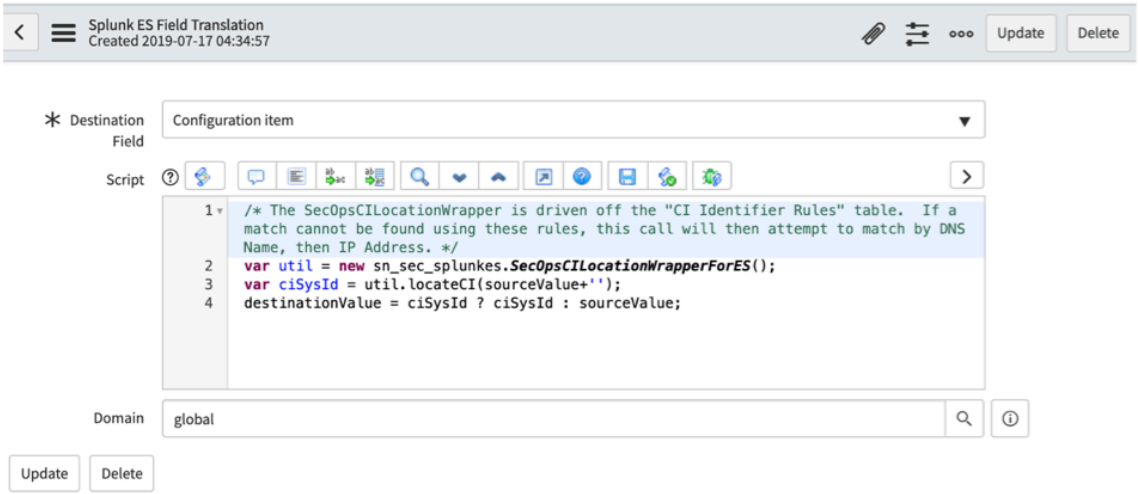
2. Wählen Sie in der Auswahlliste ein Zielfeld für den Wert aus, den Sie bearbeiten möchten.
3. Alternativ können Sie im Abschnitt SIR-Incident-Feldzuordnung auf das Klammern-Symbol klicken [{}] Neben einem Feld, um den Skripteditor für dieses Feld zu öffnen.

   In bestimmten Fällen kann eine Skripteinbindung für das Feld Konfigurationselement geeignet sein. Für ein bemerkenswertes Ereignis kann beispielsweise kein Wert für das Konfigurationselement übereinstimmen.

   Wie in der folgenden Abbildung gezeigt, kann eine Übereinstimmung für einen Hostnamen nicht in gefunden werden ServiceNow AI Platform® CMDB für das Feld Konfigurationselement können Sie die Regel so bearbeiten, dass, wenn eine IP-Adresse gefunden wird, das Feld Konfigurationselement ausgefüllt wird. Wenn für den Alarm kein Wert vorhanden ist, wird das Feld im Security Incident auf null festgelegt.

   Der Editor wird geöffnet, wobei das Feld im Zielfeld angezeigt wird. Die folgende Abbildung zeigt den Editor mit Konfigurationselement Feld als Zielfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie alle Änderungen am Skript ein, und klicken Sie auf **Aktualisieren** Um Ihre Änderungen zu speichern.
   Die Splunk Die Tabelle „Feldübersetzungen“ wird angezeigt.
5. Schließen Sie die Tabelle, um zum Zuordnungsformular zurückzukehren.

Kopieren Splunk Enterprise Security Profile von einer Instanz zu einer anderen mithilfe der Export-/Importfunktion

Sie können exportieren und importieren Splunk Enterprise Security Profileinstellungen von einem ServiceNow AI Platform Instanz zu einer anderen ServiceNow AI Platform Instanz.

Vorbereitungen

Zu den Einstellungen, die Sie exportieren und importieren können, gehören Profilname, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Konfigurationskachel-Quellinformationen.

Erforderliche Rolle: sn_si.ingestion_profile_admin

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Mit dieser Funktionalität kann der Sicherheitsadministrator Profile kopieren, die für eines getestet und verifiziert wurden ServiceNow AI Platform Instanz, z. B. außerhalb der Produktion, an eine andere ServiceNow AI Platform Instanz, z. B. Produktion, ohne dass alle Konfigurationseinstellungen wiederholt werden müssen. Zu den Einstellungen, die exportiert und importiert werden, gehören Profilname, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien, Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Konfigurationskachel-Quellinformationen.

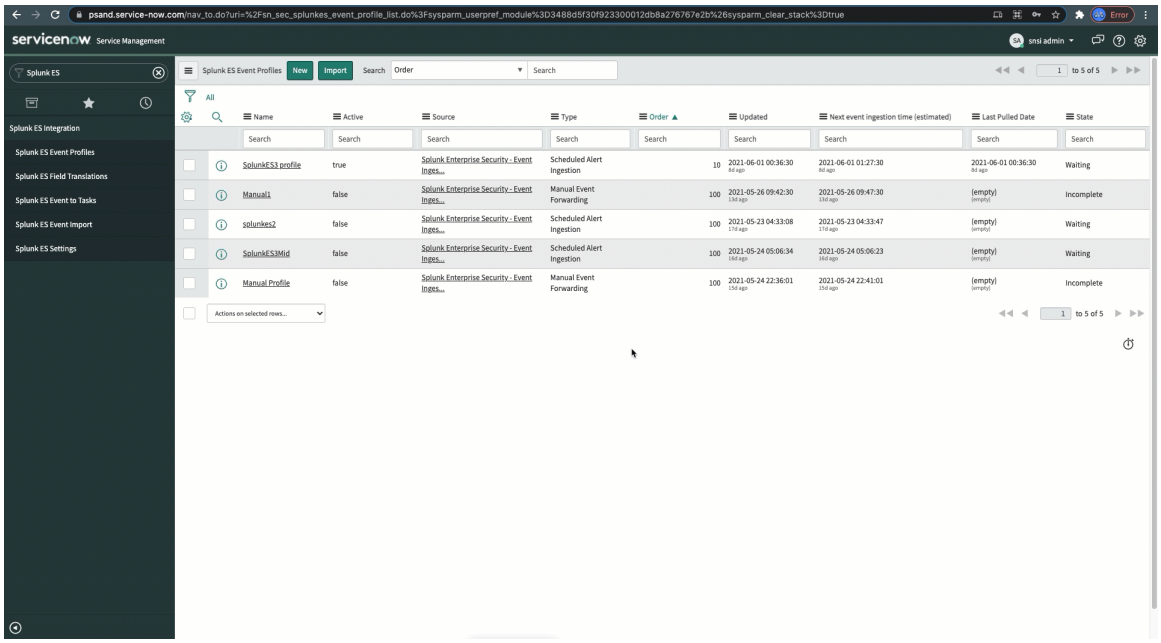
Hinweis:
Wenn Sie einen Profiltyp für die manuelle Ereignisweiterleitung exportieren, werden die für die Beispielfeldzuordnung verwendeten Anhangsdaten kopiert, die Anhangsdatei selbst wird jedoch nicht exportiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Splunk ES-Integration** > **Splunk ES-Ereignisprofile**an.
2. Wählen Sie ein Profil aus, das Sie in ein anderes exportieren möchten ServiceNow AI Platform Instanz. Sie können mehrere Profile für den Export auswählen.
3. Klicken Sie im Menü Aktionen auf **Exportieren** .
4. Sobald die Meldung „Export abgeschlossen“ angezeigt wird, klicken Sie auf **Herunterladen** .

   Die folgende Abbildung zeigt den Export eines Profils (SplunkES3profile) aus dem ServiceNow AI Platform Instanz (psand.service-now.com).



   Die exportierte Datei payload.xml wird auf Ihren Computer heruntergeladen. Die Datei enthält den Profilnamen, Korrelationsregeln, Zuordnungen, Filter, Zusammenfassungskriterien Feldübersetzungen, abgerufene Beispieldaten, Zeitplanung und Konfigurationskachel-Quellinformationen. Wenn Sie mehrere Profile auswählen und herunterladen, werden sie in derselben Datei payload.xml angezeigt.

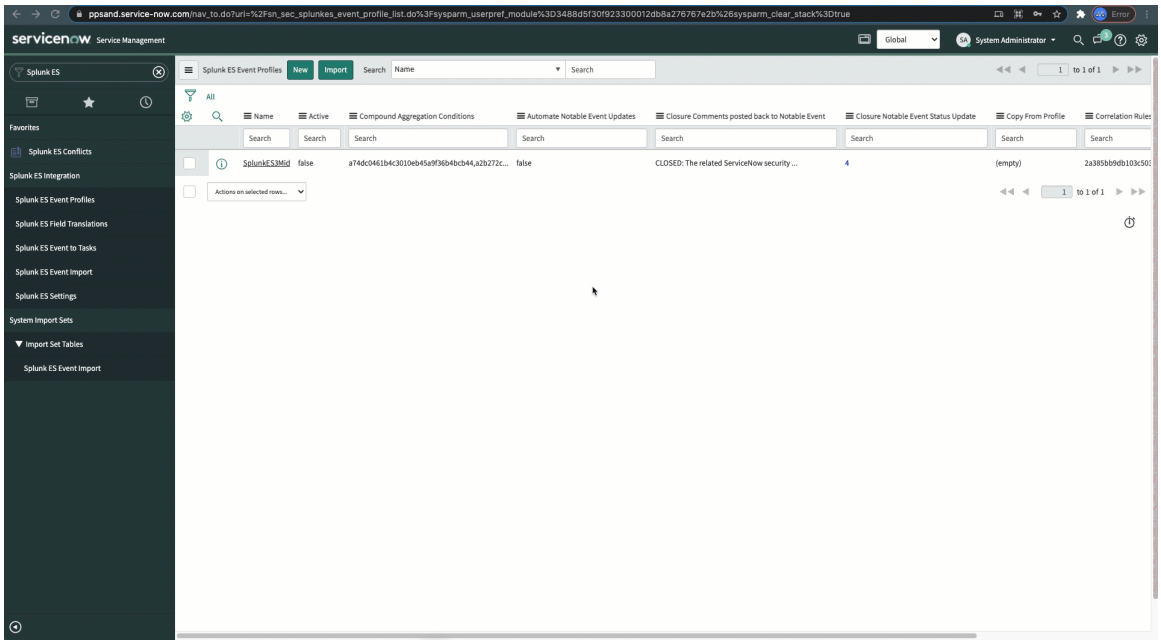
   Sie können jetzt mit dem Import des Profils in ein anderes fortfahren ServiceNow AI Platform Instanz.

5. Navigieren zu **Splunk ES-Integration** > **Splunk ES-Ereignisprofile**an.
6. Klicken Sie auf **Importieren**.
7. Klicken Sie Auf **Wählen Sie die Datei aus** Und wählen Sie die XML-Datei auf Ihrem Computer aus.
8. Klicken Sie auf **Hochladen**.
9. Klicken Sie Auf **Profile schließen und neu laden** .

   Die folgende Abbildung zeigt den Import eines Profils (SplunkES3profile) aus dem ServiceNow AI Platform Instanz (psand.service-now.com) zu ServiceNow AI Platform Instanz (ppsand.service-now.com).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie haben das Profil erfolgreich aus einem anderen importiert ServiceNow AI Platform Instanz.

Überprüfen Sie, ob die exportierte Quelle (Splunk API-Account und Splunk Server-URL) und MID-Server-Konfigurationseinstellungen sind gültig und in importiert verfügbar ServiceNow AI Platform Instanz. Aktualisieren Sie Ihren Splunk Enterprise Security Konfiguration, falls erforderlich.

10. **Wahlweise:** Überprüfen Sie die MID-Server-Einstellungen nach dem Importieren eines Profils.
11. **Wahlweise:** Navigieren zu **Security Operations** > **Integrationskonfigurationen**an.
12. **Wahlweise:** Wählen Sie aus Splunk Enterprise Security Konfigurationskachel und klicken Sie auf **Aktualisieren** .
13. **Wahlweise:** Überprüfen und aktualisieren Sie die Quell- und MID-Server-Details nach Bedarf.

Prüfliste für Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung

Verwenden Sie diese Prüfliste, um Sie durch alle Aufgaben der Integration zu führen. Die folgende Prüfliste enthält Setup- und Installationsaufgaben sowie Beispiele für Anwendungsfälle, die die erwarteten Ergebnisse für die Integration enthalten.

Vorbereitungen

Erforderliche Rollen: sn_si.ingestion_profile_admin, admin, sn_si.admin, sn_si.Analyst, Splunk Enterprise Security Administrator

Hinweis:
Benutzer mit der Rolle „sn_si.admin“ können alle Vorgänge ausführen, die einem Profiladministrator zur Verfügung stehen, da die Rolle „sn_si.admin“ standardmäßig die erforderlichen Berechtigungen erbt.

Warum und wann dieser Vorgang ausgeführt wird

Verfolgen Sie Ihren Fortschritt beim Setup, der Installation und der Konfiguration der Integration mit der folgenden Tabelle. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren. Jede Zeile der Tabelle listet Aufgaben auf und gibt die Rollen an, die zur Ausführung der Aufgaben erforderlich sind. Nummerierte Themen des Installations- und Konfigurationsleitfadens werden ebenfalls referenziert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die für jede Aufgabe erforderlichen Rollen werden mit jedem Schritt in der folgenden Tabelle aufgeführt.

Prozedur

1. Verfolgen Sie Ihren Fortschritt beim Setup, der Installation und der Konfiguration der Integration. Schließen Sie alle Aufgaben für einen Schritt ab, bevor Sie mit dem nächsten Schritt fortfahren.
2. Führen Sie die Schritte in der Tabelle in der Reihenfolge aus, in der sie angezeigt werden.

Prüfliste

☐	Als Anwender mit ServiceNow AI Platform administratorrolle, richten Sie Ihr ein ServiceNow AI Platform Instanz. ○ Weisen Sie Anwender mit zu **sn_si.ingestion_profile_admin** (Oder sn_si.admin) und sn_si.Analyst-Rollen nach Bedarf. ○ Installieren und konfigurieren Sie einen MID-Server, wenn dies der Fall ist Splunk Server wird in Ihrem Unternehmensnetzwerk bereitgestellt. ○ Überprüfen Sie, ob ServiceNow Security Incident Response Plugins werden für Ihr Release von aktiviert ServiceNow AI Platform. ○ (Optional) wenn Sie Ereignisse manuell von Ihrem weiterleiten möchten Splunk Enterprise Security-Konsole in Ihrem ServiceNow AI Platform Instanz: Stellen Sie sicher, dass Sie einem Anwender mit die Rolle (sn_sec_splunkes.api_Account_Access) zugewiesen haben Splunk Enterprise Security Administratorberechtigung. Weitere Informationen finden Sie unter Richten Sie Ihr ein ServiceNow AI Platform Instanz für Splunk Enterprise Security Integration.
☐	Als Anwender mit ServiceNow AI Platform administratorrolle installieren und konfigurieren Splunk Enterprise Security Anwendung aus dem ServiceNow Store. **a.** Laden Sie die Anwendung herunter, und installieren Sie sie auf Ihrem ServiceNow AI Platform Instanz. **b.** Konfigurieren Sie die Anwendung, und stellen Sie eine Verbindung mit her Splunk Enterprise Security Konsole. Weitere Informationen finden Sie unter Installieren und konfigurieren Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung.
☐	(Optional) wenn Sie Ereignisse manuell aus exportieren möchten Splunk Enterprise Security-Konsole zu Ihrem ServiceNow AI Platform Führen Sie die folgenden Aufgaben aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	○ Als Splunk Enterprise Security Administrator, installieren, einrichten und aktivieren ServiceNow Security Operations-Ereigniserfassungs-Add für Splunk Enterprise Security Aus SPLunkbase in Ihrem Splunk Enterprise Security Konsole. ○ Als Splunk Enterprise Security Administrator, falls nicht bereits konfiguriert, speichern Sie Suchvorgänge als wichtige Ereignisse in Ihrem Splunk Enterprise Security Konsole. Weitere Informationen finden Sie unter Richten Sie Ihr ein Splunk Umgebung für die manuelle Ereigniserfassung für Splunk Enterprise Security Integration der bemerkenswerten Ereigniserfassung.
☐	Als Anwender mit ServiceNow AI Platform **sn_si.ingestion_profile_admin** Rolle, erstellen und benennen Sie ein Ereignisprofil. Wählen Sie den Profiltyp aus der Auswahlliste aus. Optionen sind ein geplantes Warnungsprofil, das Sie zum Erfassen von Beispieldaten verwenden, oder ein Ereignisprofil, das Sie zum manuellen Exportieren von Anhangsdaten aus Ihrem verwenden Splunk Enterprise Security Konsole. ○ Wählen Sie für eine geplante Warnung eine verfügbare Warnung aus. ○ Erstellen Sie für ein Profil für manuell exportierte Daten eine neue Zuordnung, oder kopieren Sie eine vorhandene Zuordnung. Weitere Informationen finden Sie unter Erstellen und benennen Sie ein Ereignisprofil für Splunk Enterprise Security Integration der Ereigniserfassung.
☐	Als Anwender mit ServiceNow AI Platform **sn_si.ingestion_profile_admin** Rolle, Zuordnungswerte, die erfasst wurden, oder Anhangsdaten, die aus exportiert werden Splunk Enterprise Security Bis ServiceNow AI Platform Security Incidents. **a.** Ruft Beispieldaten für eine geplante Warnung ab. **b.** (Optional) Exportieren Sie Anhangsdaten manuell aus Splunk Enterprise Security Für ein Ereignis. **c.** Bearbeiten Sie die Standardzuordnungskonfiguration. **d.** Fügen Sie optional Filterkriterien hinzu, fügen Sie eine Warnung an einen vorhandenen Security Incident an, und verwenden Sie den Skripteditor. Weitere Informationen finden Sie unter Zuordnung von wichtigen Ereignisfeldern für Splunk Enterprise Security Integration und Erstellen Sie Zuordnungen für Splunk ESÜberprüfung von auffälligen Ereignis-Incidents und Details zu beitragenden Ereignissen (geplante Erfassung).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

☐	○ Als Anwender mit ServiceNow AI Platform **sn_si.ingestion_profile_admin** Rolle, zeigen Sie eine Vorschau der Daten von an Splunk Enterprise Die auf einer angezeigt wird ServiceNow AI Platform Security Incident. ○ Beheben Sie Fehler, oder fügen Sie fehlende Daten hinzu, damit keine Fehlermeldungen angezeigt werden. Weitere Informationen finden Sie unter Vorschau des Security Incidents für anzeigen Splunk Enterprise Security Integration der Ereigniserfassung.
☐	Als Anwender mit ServiceNow AI Platform **sn_si.ingestion_profile_admin** Rolle: Planen Sie den Warnungsabruf für ein Profil mit einer geplanten Warnung. Weitere Informationen finden Sie unter Planen und rufen Sie neue und aktualisierte wichtige Ereignisse für ab Splunk Enterprise Security Integration der Ereigniserfassung.

Sie haben die Einrichtungsschritte erfolgreich abgeschlossen und die erwarteten Ergebnisse für die Integration verifiziert.

Integration mit Splunk - Incident Enrichment

Die Splunk– Die Incident-Anreicherungsintegration durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.

Erkunden	Einrichtung
Integrationen mit Security Incident Response	Beginnen Sie mit dem Splunk Integration für durchsuchen Security Operations

Verwenden	Entwickeln
• Führen Sie eine Sichtungssuche aus • Integration Von Security Operations: Sichtungssuche-Flow • Integration Von Security Operations – Suchflow Für Splunk-Sichtungen • Sichtungssuchdetails Anzeigen • Zeigen Sie Die Ergebnisse Der Sichtungssuche An	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie Komponenten, die mit einer Anwendung installiert sind

Problembehandlung und zusätzliche Informationen

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Beginnen Sie mit dem Splunk Integration für durchsuchen Security Operations

Splunk Software sucht, überwacht und analysiert maschinell generierte Big Data und lässt sich problemlos in integrieren Security Operations. Bevor Sie verwenden können Splunk–Integration der Incident-Anreicherung. Sie müssen sie aus dem herunterladen ServiceNow Store Und fügen Sie die entsprechende API-Basis-URL und Anmeldeinformationen hinzu.

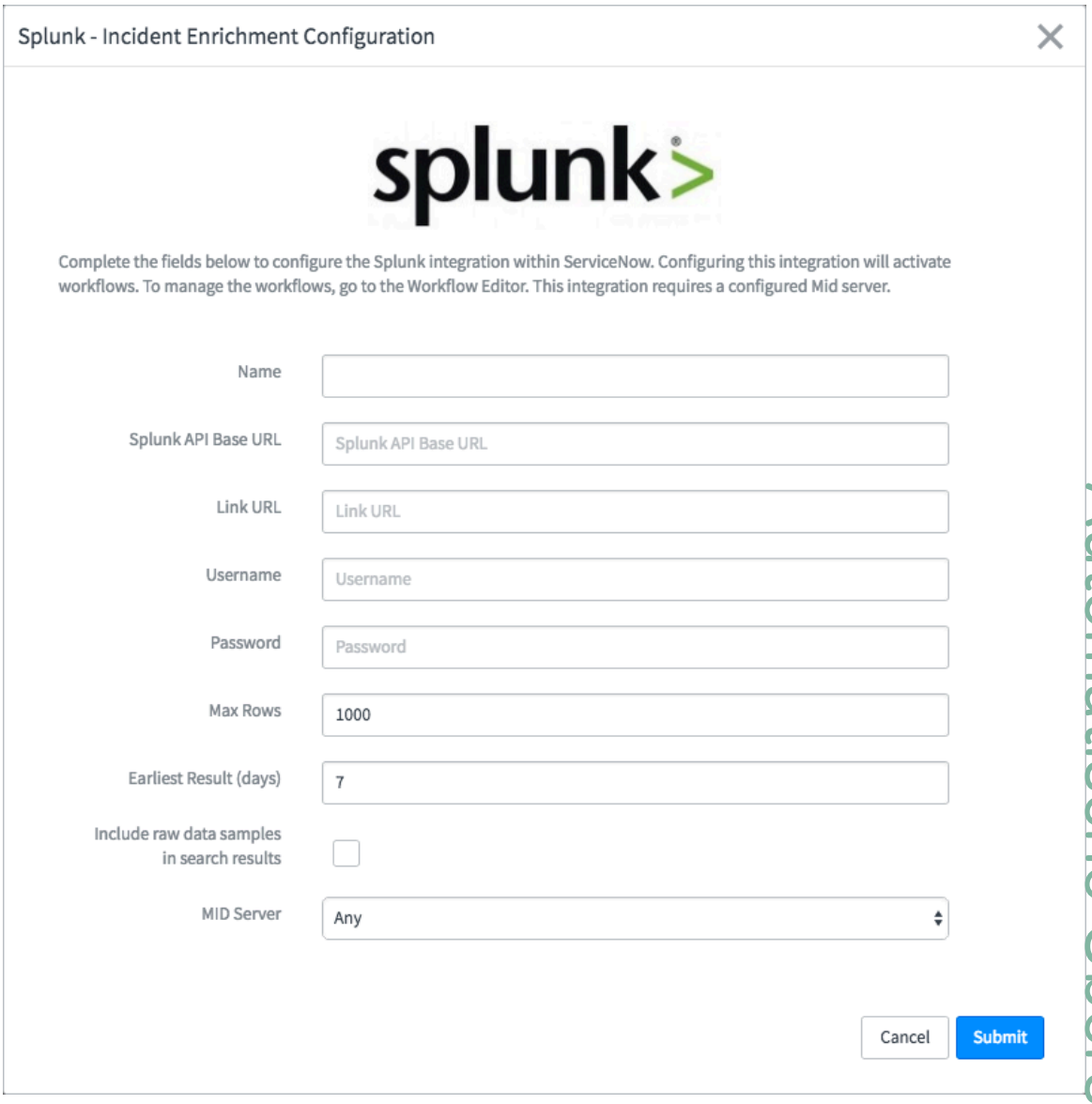
Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf zu Splunk Und erhalten Sie den API-Schlüssel und die API-ID unter Ihrem Profil.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationskonfiguration**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. Klicken Sie auf der Karte Splunk – Incident-Anreicherung auf **Neu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name dieser Konfiguration.
Basis-URL der Splunk-API	Die Basis-URL, die Sie von erworben haben Splunk Website.
Link-URL	[Optional] die Link-URL, die mit verknüpft ist Splunk Webschnittstelle, falls verfügbar.
Anwendername	Ihr Splunk-Anwendername.
Passwort	Ihr Splunk-Passwort.
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie in Tagen anzeigen möchten.
Rohdatenmuster in	Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Suchergebnissen berücksichtigen	hängt von Ihrer Einstellung in ab **Anzahl der Zeilen mit Rohdaten** Eigenschaft in Eigenschaften von Security Incident Response .
MID-Server	Wählen Sie Aus **Beliebig** Um einen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Navigieren Sie zum Verwalten der Workflows zu **Workflow-Editor** .

6. Klicken Sie auf **Absenden**.
   Die Integrationskonfigurationskarte wird angezeigt.
7. Wenn Sie die neue Konfigurationskarte anzeigen, können Sie auf klicken **Konfigurieren** Oder **Löschen** Zum Ändern oder Löschen der Konfiguration.
8. Um zur ursprünglichen Liste der Integrationskonfigurationskarten zurückzukehren, wählen Sie aus **Nein** Von **Konfigurationen Anzeigen** Dropdown-Liste.

Mobile Experience für Security Incident Response

Verwenden Sie Ihr Android- oder iOS-Mobilgerät, um Ihre Aufgaben im Security Operations Center (SOC) zu verwalten.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Security Incident Response

Wenn Sie mit den grundlegenden Konzepten von nicht vertraut sind Security Incident Response(SIR) Produkt auf Ihrem ServiceNow AI Platform® Instanz, siehe Security Incident Response-Dashboard „Übersicht“ Weitere Informationen zu Threat Intelligence und dazu, wie dieses Produkt Sie bei der Priorisierung und Lösung von Cyberbedrohungen für Ihre Organisation unterstützen kann.

Übersicht

Als Security Operations Center (SOC)-Manager oder ein Anwender mit dem ServiceNow AI Platform Sicherheitsanalyst-Rolle (sn_si.Analyst), können Sie sich bei anmelden ServiceNow AI Platform Instanz direkt von Ihrem Mobilgerät aus. Mit Security Incident Response Mobile-App, Können Sie Ihre aktuellsten und kritischen anzeigen, bearbeiten und zuweisen SIR Security Incidents und Antwortaufgaben. Benachrichtigungen informieren Sie, wenn Ihnen zugewiesene kritische Security Incidents ankommen.

Mit Security Incident Response Mobile-App, Sie können Folgendes ausführen SIR-Zugehörige Aufgaben von Ihrem Mobilgerät:

- Zeigen Sie eine Liste kritischer Security Incidents und Antwortaufgaben an.
- Erhalten Sie detaillierte Benachrichtigungen für Security Incidents und Aufgaben, die vordefinierte Benachrichtigungskriterien erfüllen.
- Zeigen Sie Gruppierungen von Security Incidents oder Aufgaben an, die auf einem vordefinierten Satz von Abfragen oder Filtern basieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie die Arbeitsnotizen und zugehörigen Listen von Security Incidents an.
- Aktualisieren Sie Security Incidents, und fügen Sie Arbeitsnotizen oder Anhänge hinzu.
- Bearbeiten Sie die Felder für Security Incidents.
- Weisen Sie Security Incidents sich selbst oder anderen Mitgliedern Ihres Sicherheitsteams zu.

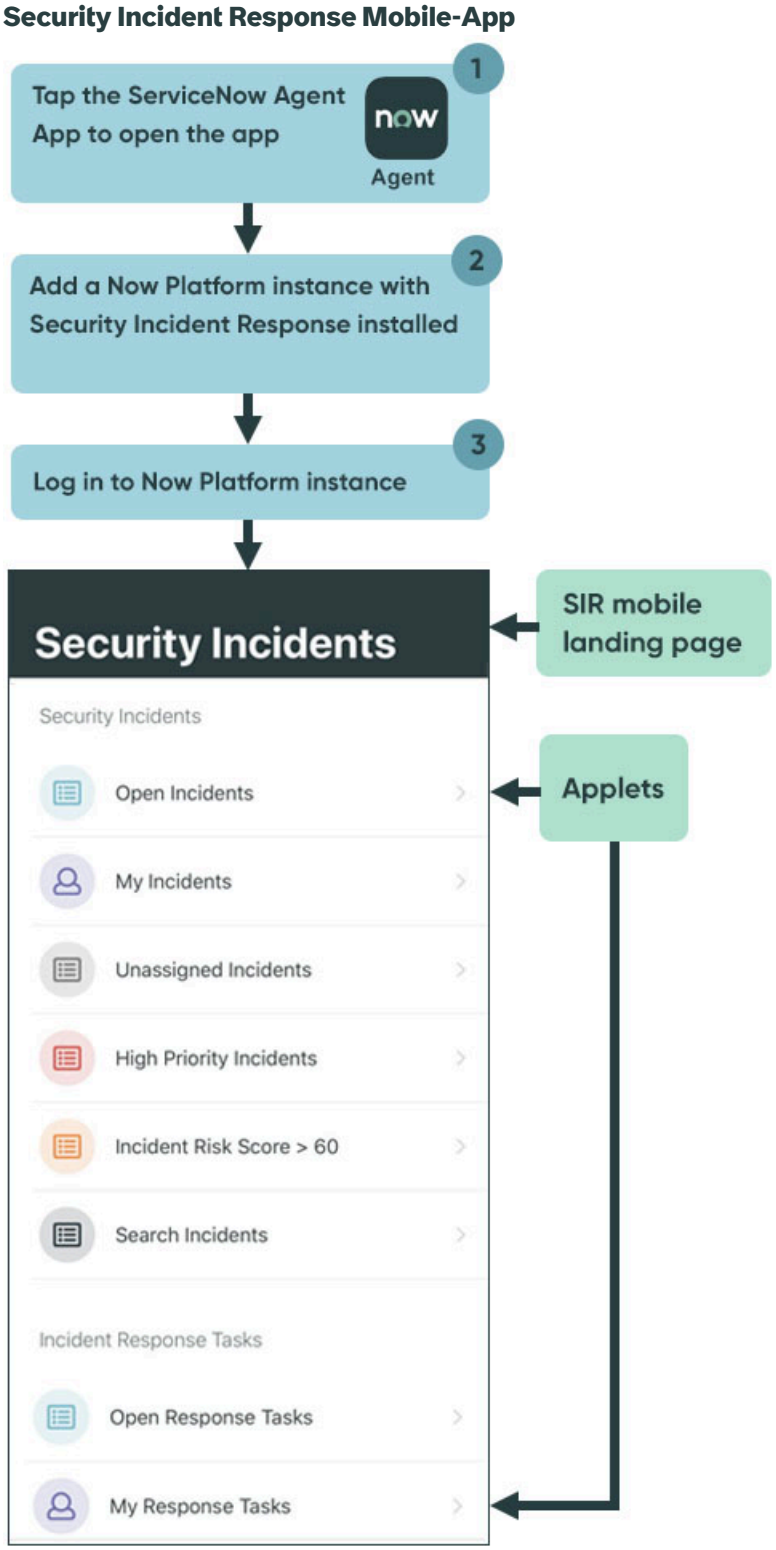
Wenn sie ausgefüllt sind, können Sie die folgenden zugehörigen Listen in anzeigen SIR Security Incidents mit Security Incident Response Mobile-App:

- Konfigurationselement
- Betroffener Anwender
- Betroffene Services
- Untergeordnete Security Incidents
- Ähnliche Security Incidents (nicht unterstützt von ServiceNow AI Platform)
- Erkennbare Elemente
- Antwortaufgaben
- Aufgaben
- Aufgaben-SLA
- Anhänge (nicht unterstützt von ServiceNow AI Platform)

Die folgende Abbildung zeigt, wie Sie sich bei anmelden ServiceNow AI Platform Instanz von Ihrem Mobilgerät und die Struktur des Zielbildschirms von Security Incident Response Mobile-App Die nach der Anmeldung abgespielt wird.

Für Schritt-für-Schritt-Anweisungen zur Einrichtung von ServiceNow AI Platform Instanz und installieren Sie Security Incident Response Mobile-App, Siehe Richten Sie die Prüfliste für ein Security Incident Response Mobile-App. Anweisungen zur Anmeldung finden Sie unter Melden Sie sich bei an Security Incident Response Mobile-App.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Anwendungen

-Anwendungen sind ServiceNow® Softwarekomponenten wie Security Incident Response(SIR), Vulnerability Response(VR), Governance, Risk und Compliance(GRC), die bestimmte Funktionen und Funktionen in Ihrem bereitstellen ServiceNow AI Platform Instanz. Nachdem Sie installiert haben Security Incident Response Core-Anwendung und Security Incident Response Mobile-App Auf Ihrem ServiceNow AI Platform In der Instanz wird das Symbol für die Kernanwendung unten auf Ihrem angezeigt Android Oder iOS Mobilgerät, nachdem Sie sich angemeldet haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response Mobile-App Symbol (Security Incidents)

Ordner

Jeweils ServiceNow® Mobile Die Anwendung enthält Ordner, die die Applets nach Kategorie trennen. Im vorherigen Bild der Zielseite **Security Incidents** Und **Incident-Antwortaufgaben** Sind Ordner.

Applets

Applets sind die verschiedenen Optionen in der Anwendung. Die Symbole unter **Security Incidents** Und **Incident-Antwortaufgaben** Abschnitte sind die verfügbaren Applets von Security Incident Response Mobile-App.

Richten Sie die Prüfliste für ein Security Incident Response Mobile-App

Die folgende Prüfliste enthält die Setup-Aufgaben, die Sie in ausführen müssen ServiceNow AI Platform®-Instanz und auf Ihrem Mobilgerät vor der Verwendung von Security Incident Response Mobile-App.

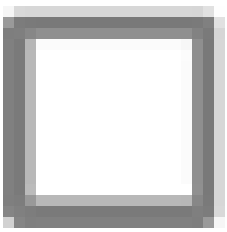
Vorbereitungen

Drucken Sie diese Prüfliste als Option aus, und verwenden Sie sie, um Sie durch die für erforderlichen Einrichtungsaufgaben zu führen Security Incident Response Mobile-App. Stellen Sie sicher, dass jedes Element in der Liste abgeschlossen ist, damit Sie es anzeigen und bearbeiten können SIR Security Incidents auf Ihrem Mobilgerät.

Die Prüflistenelemente werden in hervorgehobenem Text angezeigt. Weitere Informationen folgen jedem Element in der rechten Spalte. Geschätzte Zeit bis zum Abschluss dieser Aufgabe: 15-20 Minuten.

Erforderliche Rollen: admin, sn_si.Analyst

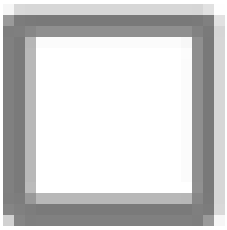
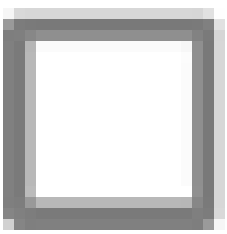
Mobile Prüfliste

Element	Beschreibung
	Stellen Sie als Anwender mit der Administratorrolle sicher, dass Sie über verfügen Security Incident Response Core-Anwendung auf installiert ServiceNow AI Platform Instanz. Dies ist der ServiceNow AI Platform Instanz, die Sie auf Ihrem Mobilgerät anzeigen. **Hinweis:** Die Security Incident Response Core-Anwendung und ServiceNow AI Platform Instanz muss aus demselben Familien-Release stammen. 1. Um zu überprüfen, ob die Kernanwendung auf Ihrer Instanz installiert ist, navigieren Sie zu **Plugins** Und suchen Sie nach Security Incident Response. 2. Wenn Security Incident Response Core-Anwendung ist nicht bereits installiert. Klicken Sie auf **Installieren** Um es zu installieren. Weitere Informationen zur Installation von finden Sie Security Incident Response Kernanwendung, siehe Security Incident Response installieren und konfigurieren. Wenn Security Incident Response Die Kernanwendung ist in Plugins nicht sichtbar. Weitere Informationen zum Installieren von Kernanwendungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mobile Prüfliste (Fortsetzung)

Element	Beschreibung
	und Berechtigungen für Anwendungen finden Sie unter Security Operations Und ServiceNow Store.
	Stellen Sie als Anwender mit der Administratorrolle sicher, dass Sie über verfügen Security Incident Response Mobile-App Auf installiert ServiceNow AI Platform Instanz, die Sie auf Ihrem Mobilgerät anzeigen möchten. **Hinweis:** Die Security Incident Response Mobile-App Und ServiceNow AI Platform Instanz muss aus demselben Familien-Release stammen. Laden Sie herunter, und installieren Sie Security Incident Response Mobile-App Von ServiceNow Store Auf Ihrem ServiceNow AI Platform Instanz. Wenn Sie installieren Security Incident Response Mobile-App, Die Abhängigkeiten com.Glide.sg und com.Glide.sg.Agent_native_Client werden ebenfalls installiert. So überprüfen Sie, ob diese Abhängigkeiten installiert sind: 1. Navigieren Sie zu **Plugins** . 2. Suchen Sie nach den Plugin-IDs (com.Glide.sg und com.Glide.sg.Agent_native_Client). 3. Wenn sie nicht aktiviert sind, aktivieren Sie diese Plugins. Diese Plugins sind für erforderlich Security Incident Response Mobile-App. Weitere Informationen zum Installieren von Anwendungen und Berechtigungen für Anwendungen finden Sie unter Security Operations Und ServiceNow Store.
	Als Anwender mit ServiceNow AI Platform administratorrolle: Stellen Sie sicher, dass Sie mobile Anwender mit den erforderlichen Rollen in Ihrem zugewiesen haben ServiceNow AI Platform Instanz. 1. Um die Rollen anzuzeigen, die einem Anwender zugewiesen sind, navigieren Sie zu **Anwender und Gruppen** > **Anwender**an. 2. Wählen Sie den Anwendernamen gefolgt von der zugehörigen Liste „Rollen“ aus. Alle diesem Anwender zugewiesenen Rollen werden angezeigt. 3. Überprüfen Sie, ob ein Anwender zugewiesen ist, oder weisen Sie einen Anwender mit der Rolle „IT Infrastructure Library“ (itil) zu. Benutzer mit der Rolle itil können Security Incidents erstellen, öffnen, aktualisieren und schließen. Nur Anwendern mit der Rolle itil können Aufgaben zugewiesen werden. 4. Überprüfen Sie, ob ein Anwender zugewiesen ist, oder weisen Sie einen Anwender mit der Rolle „Sicherheitsanalysten“ (sn_si.Analyst) zu. Benutzer mit der Rolle „sn_si.Analyst“ können Security Incident-Datensätze lesen und bearbeiten. Diese Rolle wird automatisch hinzugefügt, wenn Sie die Rolle itil zuweisen. 5. Überprüfen Sie, ob Sie alle erforderlichen Zuweisungsgruppen erstellt und diesen Gruppen mobile Anwender zugewiesen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mobile Prüfliste (Fortsetzung)

Element	Beschreibung
	Hinweis: Wenn Sie eine große Anzahl von Anwendern für die mobile Anwendung haben, können Sie alternativ einer Gruppe die Rolle sn_si.Analyst zuweisen. Jeder Anwender, den Sie der Gruppe hinzufügen, erbt diese Rolle. Weitere Informationen zu Sicherheitsanalysten finden Sie unter Sicherheitsanalysten werden zugewiesen. Weitere Informationen zu Anwendern und zum Zuweisen von Rollen zu Anwendern und Gruppen finden Sie unter Anwenderverwaltung .
☐	Laden Sie als Anwender mit der Rolle „sn_si.Analyst“ die neueste herunter ServiceNow® Agent-App auf Ihrem Mobilgerät. Die aktuelle Version der Agent-App ist auf Apple verfügbar iOS App Store und Google Play Store.
☐	Stellen Sie als Benutzer mit der Rolle „sn_si.Analyst“ sicher, dass Benachrichtigungen auf Ihrem Mobilgerät und in aktiviert sind ServiceNow AI Platform Instanz. Benachrichtigungen informieren Sie, wenn Ihnen oder Ihrer Zuweisungsgruppe kritische Security Incidents zugewiesen werden. Um Sie bei der rechtzeitigen Korrektur zu unterstützen, klicken Sie nach dem Aktivieren von Benachrichtigungen auf eine Benachrichtigung im Security Incident Response Mobile-App Um direkt zum Security Incident zu navigieren. Um Benachrichtigungen in zu aktivieren ServiceNow AI Platform Führen Sie die folgenden Schritte aus, damit sie auf Ihrem Mobilgerät angezeigt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mobile Prüfliste (Fortsetzung)

Element	Beschreibung
	1. Überprüfen Sie, ob Sie heruntergeladen und installiert haben Security Incident Response Mobile-App Auf Ihrem ServiceNow AI Platform Instanz. 2. In Systemeinstellungen in Ihrem ServiceNow AI Platform Stellen Sie unter Benachrichtigungen sicher, dass Sie aktiviert haben **ServiceNow Mobile-Anwendung** . Weitere Informationen zum Festlegen von Benachrichtigungen finden Sie unter Festlegen von Einstellungen für Anwenderbenachrichtigungen in der Core-UI . ServiceNow AI Platform Benachrichtigungen werden auch auf dem Nachrichtenbildschirm auf Ihrem Mobilgerät angezeigt. Überprüfen Sie, ob Benachrichtigungen auch in den Einstellungen Ihres Mobilgeräts aktiviert sind.

Sie haben Ihr Mobilgerät und die erfolgreich eingerichtet ServiceNow AI Platform Für Security Incident Response Mobile-App. Der nächste Schritt besteht darin, sich bei anzumelden ServiceNow AI Platform Instanz mit Ihrem Mobilgerät.

Melden Sie sich bei an Security Incident Response Mobile-App

Öffnen Sie die App Security Incident Response Mobile, und fügen Sie ein hinzu ServiceNow AI Platform® Instanz mit Security Incident Response für Ihr Mobilgerät.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

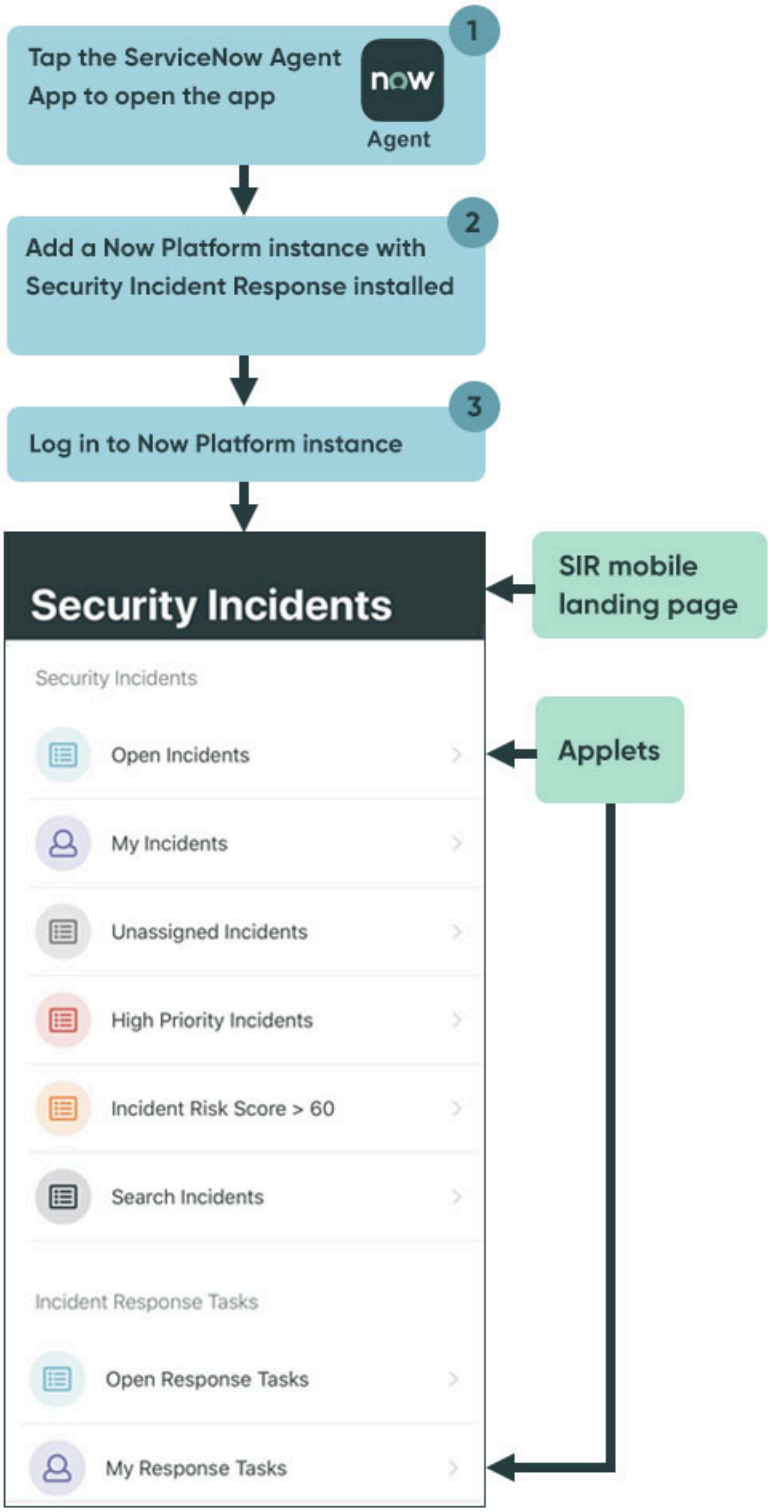
Warum und wann dieser Vorgang ausgeführt wird

Zeit bis zum Abschluss dieser Aufgabe: 5-10 Minuten.

Vergewissern Sie sich, dass Sie die in beschriebenen Setup-Schritte abgeschlossen haben Richten Sie die Prüfliste für ein Security Incident Response Mobile-App.

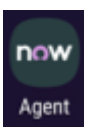
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident Response Mobile-App



Prozedur

1. Tippen Sie auf Ihrem Mobilgerät auf **ServiceNow-Agent** App zum Öffnen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie noch nicht bei angemeldet sind ServiceNow AI Platform Instanz wird der Bildschirm Instanzen angezeigt.

2. Wenn ServiceNow AI Platform Instanz mit Security Incident Response Die Kernanwendung wurde Ihrem Mobilgerät nicht bereits hinzugefügt. Führen Sie die folgenden Schritte aus, um sie hinzuzufügen.

   a. Tippen Sie im angezeigten Bildschirm „Instanzen“ auf .
   Es wird ein Bildschirm angezeigt, der Sie auffordert, eine Adresse eines einzugeben und zu speichern ServiceNow AI Platform Instanz.

   b. Füllen Sie die Felder aus.

Feld	Beschreibung
Geben Sie die Instanzadresse ein, oder scannen Sie einen QR-Code.	Wählen Sie eine aus, um fortzufahren: ▪ Vor .service-now.com , Geben Sie den Namen Ihres ein ServiceNow AI Platform Beispiel: Sirmobileny . ▪ Geben Sie eine Adresse ein. Diese Adresse ist die URL Ihres ServiceNow AI Platform Instanz, die Sie auf Ihrem Mobilgerät anzeigen möchten, z. B. https://sirmobileny.service-now.com. ▪ Scannen Sie einen QR-Code.
(Optional) Geben Sie den Kurznamen ein	Geben Sie einen Spitznamen für diese Instanz ein. Wenn dem Gerät mehrere Instanzen hinzugefügt wurden, können Kurznamen Ihnen helfen, schnell einen zu finden ServiceNow AI Platform Instanz.

   c. Tippen Sie auf **Speichern und anmelden**.

3. Auf der ServiceNow Geben Sie den Anwendernamen und das Passwort für den -Anmeldebildschirm ein, der angezeigt wird ServiceNow AI Platform Instanz, die Sie hinzufügen möchten, und tippen Sie auf **Melden Sie Sich An** .
   Der Zielbildschirm „Security Incidents“ wird angezeigt. Sie haben sich erfolgreich bei angemeldet Security Incident Response Mobile-App.

4. Überprüfen Sie nach der Anmeldung, ob Benachrichtigungen in aktiviert sind Security Incident Response Mobile-App.

   a. Tippen Sie auf dem Zielbildschirm unten auf **Benachrichtigung** .

   b. Tippen Sie im Bildschirm Benachrichtigungen auf **Aktivieren Sie Benachrichtigungen** Wenn nicht aktiviert.
   Benachrichtigungen von ServiceNow AI Platform Werden auf dem Bildschirm Benachrichtigungen in angezeigt Security Incident Response Mobile-App.

5. Nachdem Sie sich auf Ihrem Mobilgerät bei einer Instanz angemeldet haben, ist dies der Standard ServiceNow AI Platform Instanz auf dem Gerät.
   Wenn Sie eine weitere anzeigen möchten ServiceNow AI Platform Auf dem Gerät müssen Sie sich von der Standardinstanz abmelden. So melden Sie sich ab:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Tippen Sie auf das Einstellungssymbol.

b. Tippen Sie Auf **Melden Sie Sich Ab** .
Der Bildschirm „Instanzen“ wird mit einem angezeigt ServiceNow AI Platform Instanzen, die Sie dem Mobilgerät hinzugefügt haben.

c. **Wahlweise:** Tippen Sie auf eine andere Instanz, um sich bei ihr anzumelden, oder führen Sie alternativ die vorherigen Schritte aus, um eine weitere Instanz hinzuzufügen.

Wenn der Bildschirm „Instanzen“ für den Security Incident Response Mobile-App Wird nicht angezeigt, nachdem Sie auf getippt haben **ServiceNow-Agent** App verifizieren Sie auf Ihrem Gerät, dass **ServiceNow-Agent** Ist als vertrauenswürdige App auf Ihrem Gerät zulässig. Um den Zugriff als vertrauenswürdige App zuzulassen, navigieren Sie auf Ihrem Gerät zu den Einstellungen und allgemeiner Geräteverwaltung, und tippen Sie auf die Option (Trust-App usw.), um den Zugriff zu erlauben.

Wenn eine Fehlermeldung angezeigt wird, nachdem Sie Ihre Anmeldeinformationen auf dem Anmeldebildschirm eingegeben haben, überprüfen Sie, ob Ihr Anwendername und Ihr Passwort für den vorhanden sind ServiceNow AI Platform Instanz ist korrekt.

Wenn Sie Probleme beim Anzeigen des Zielbildschirms haben, überprüfen Sie Ihre Netzwerkverbindung.

Wenn Sie den Bildschirm Instanzen nicht anzeigen können, nachdem Sie auf getippt haben **ServiceNow-Agent** Versuchen Sie, die App von Ihrem Gerät zu deinstallieren. Überprüfen Sie, ob Sie über die aktuelle Version der App von Apple verfügen iOS App Store oder der Google Geben Sie den Store wieder, und versuchen Sie, ihn neu zu installieren.

Zeigen Sie offene Security Incidents mit an, bearbeiten Sie sie, und weisen Sie sie zu Security Incident Response Mobile-App

Als Security Incident-Analyst können Sie offen anzeigen, bearbeiten und zuweisen Security Incident Response(SIR) Security Incidents von Ihrem Mobilgerät. Zeigen Sie zugehörige Listen und den Audit-Pfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Weisen Sie sich in der Liste der Datensätze einen offenen Security Incident selbst zu, oder weisen Sie ihn neu zu. Alternativ können Sie die Details und zugehörigen Listen des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5-10 Minuten.

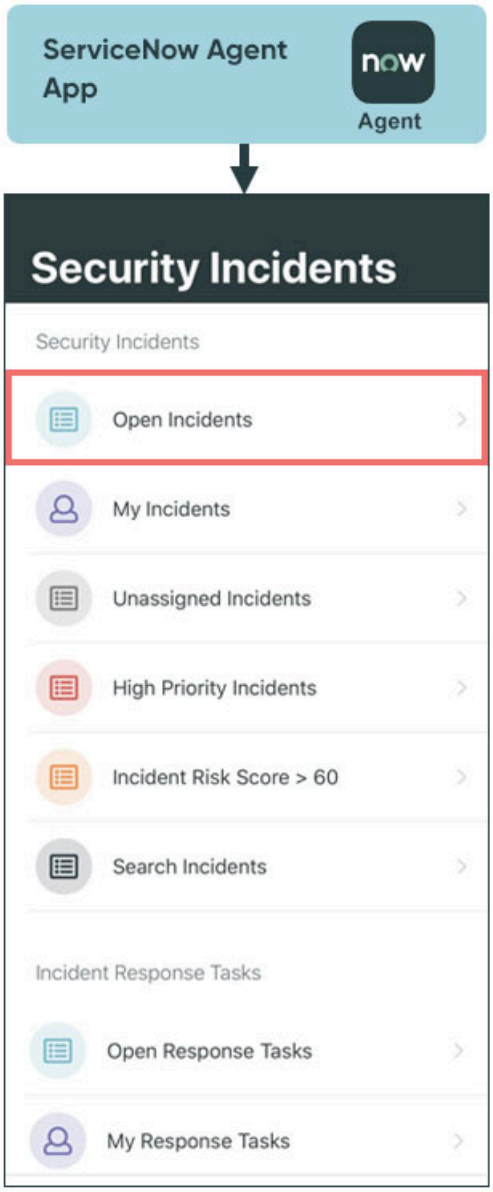
Prozedur

1. Wenn Sie nicht bei angemeldet sind ServiceNow AI Platform Instanz auf Ihrem Mobilgerät, siehe Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie bei angezeigter Zielseite für Security Incidents auf **Offene Incidents** .

Wenn Sie weg von navigieren Security Incident Response Mobile-App Nachdem Sie sich angemeldet haben, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.

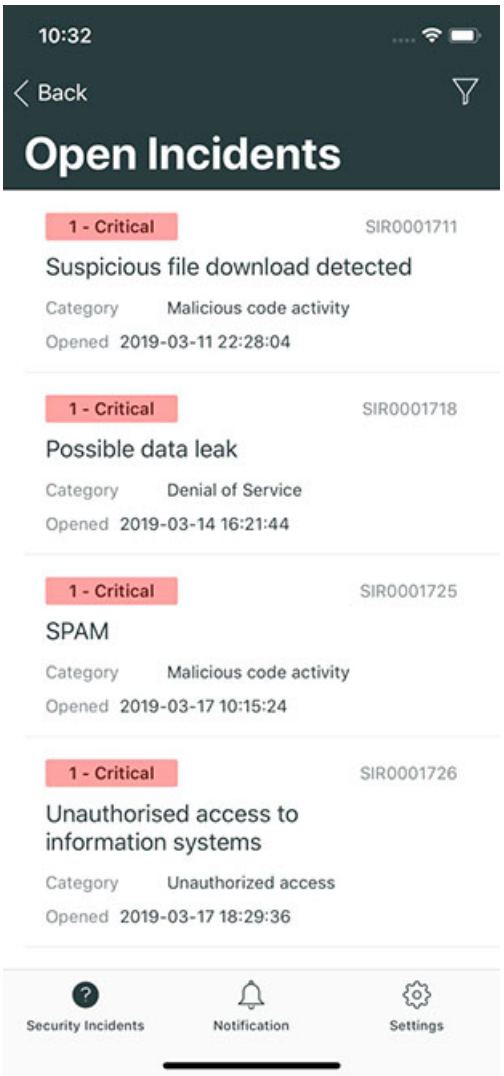
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Bildschirm offene Incidents wird mit einer Liste offener Security Incident-Datensätze angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. **Wahlweise:** Siehe Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App Um nach Security Incidents zu suchen, die bestimmten Kriterien entsprechen.

   Alternativ mit dem Filtersymbol ( ) Angezeigt, Legen Sie Filter fest, um die Anzahl der Datensätze zu begrenzen In der Liste. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator im ServiceNow AI Platform.

4. Um sich selbst einen Incident zuzuweisen oder ihn direkt aus der Liste der offenen Security Incidents neu zuzuweisen, wischen Sie in einem Datensatz nach links, um das Menü zu öffnen.

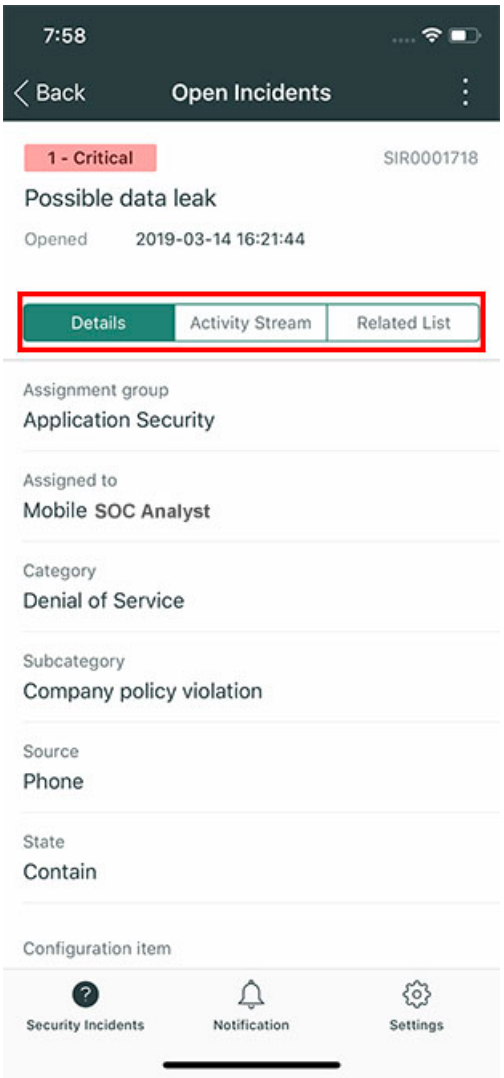
5. Wählen Sie einen aus dem angezeigten Menü aus, um fortzufahren.

6. Alternativ können Sie auf einen Datensatz in der Liste tippen, um die Details eines offenen Security Incident-Datensatzes anzuzeigen und weitere zugehörige Datensätze und zugehörige Listen anzuzeigen, wenn der Bildschirm offene Incidents angezeigt wird.

7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Zeigen Sie Security Incidents an, bearbeiten Sie sie, und weisen Sie sie Ihnen mit der zugewiesenen Security Incidents neu zu Security Incident Response Mobile-App

Als Security Incident-Analyst können Sie sie anzeigen, bearbeiten und neu zuweisen Security Incident Response(SIR) Incidents, die Ihnen zugewiesen sind. Zeigen Sie zugehörige Listen und den Audit-Pfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

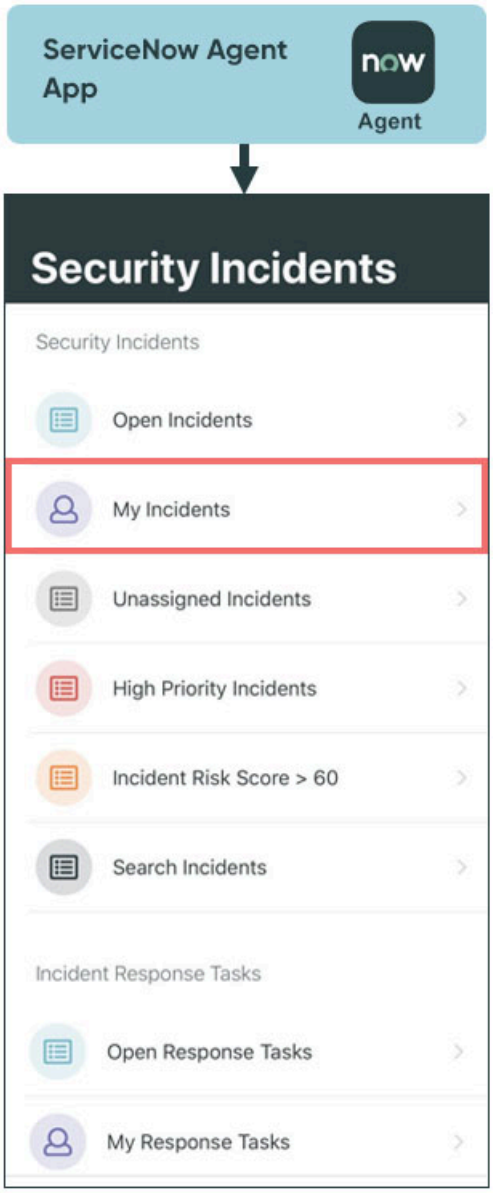
Weisen Sie einen offenen Security Incident aus der Liste der Datensätze einem anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie die Details und zugehörigen Listen des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5-10 Minuten.

Prozedur

1. Wenn Sie nicht bei angemeldet sind ServiceNow AI Platform Instanz auf Ihrem Mobilgerät, siehe Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie auf, während der Zielbildschirm für Security Incidents angezeigt wird **Meine Incidents** .

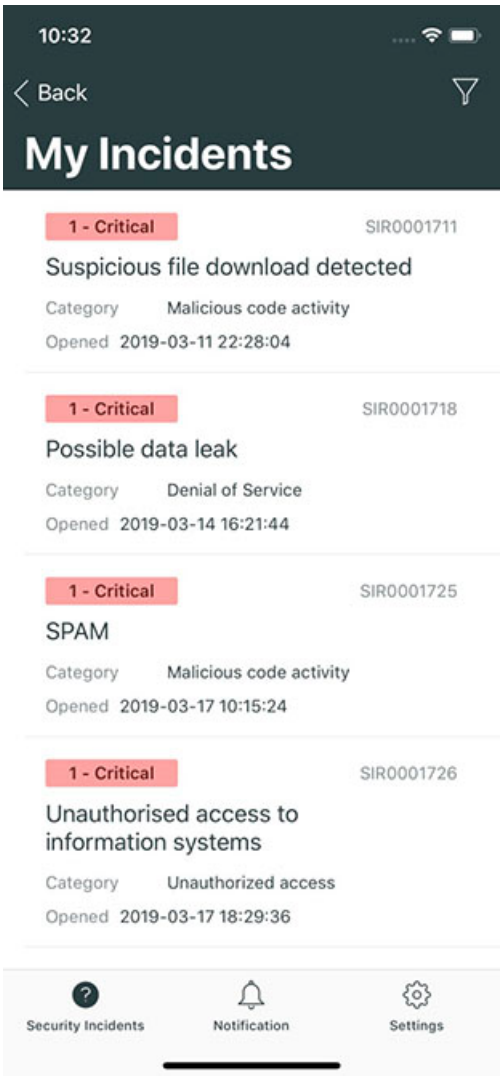
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie weg von navigieren Security Incident Response Mobile-App Nachdem Sie sich angemeldet haben, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm meine Incidents wird mit einer Liste offener Security Incident-Datensätze angezeigt, die Ihnen zugewiesen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

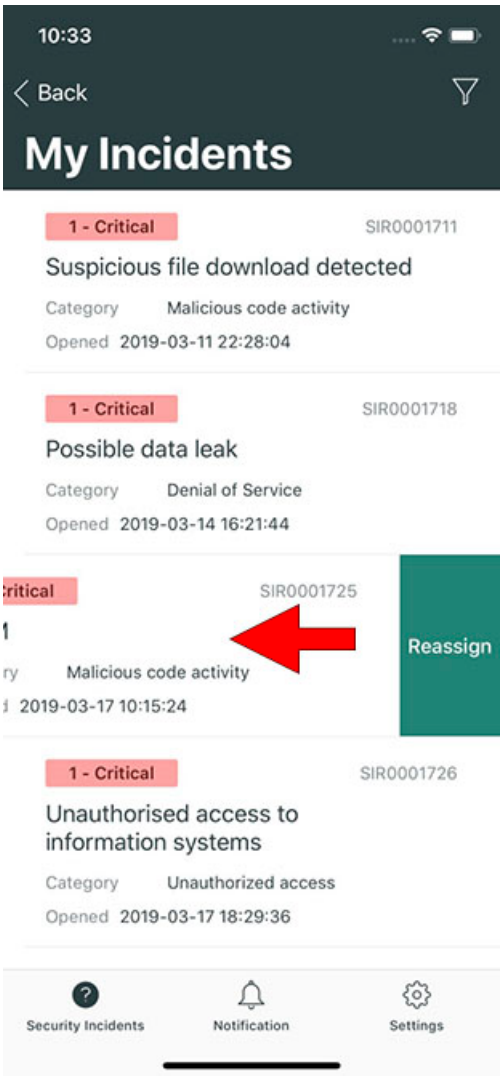


3. **Wahlweise:** Siehe Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App Um nach Security Incidents zu suchen, die bestimmten Kriterien entsprechen.

   Alternativ mit dem Filtersymbol ( ) Angezeigt, Legen Sie Filter fest, um die Anzahl der Datensätze zu begrenzen In der Liste. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator im ServiceNow AI Platform.

4. Um einen Incident direkt aus der Liste neu zuzuweisen, wobei die Liste der offenen Security Incident-Datensätze angezeigt wird, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

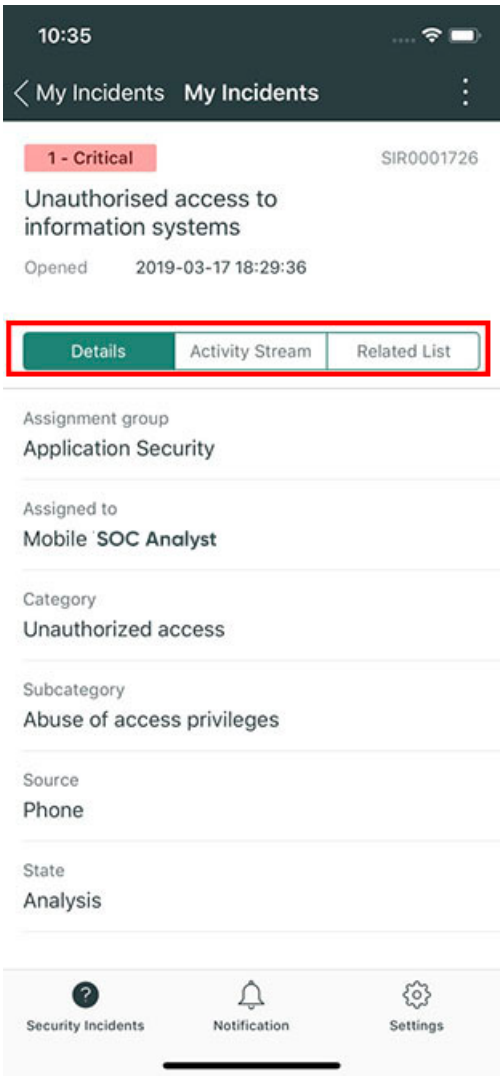


5. Bearbeiten Sie die Felder Zuweisungsgruppe oder Zugewiesen an im angezeigten Menü.

6. Alternativ können Sie auf einen Datensatz in der Liste tippen, um die Details des offenen Security Incident-Datensatzes anzuzeigen, während der Bildschirm meine Incidents angezeigt wird.

7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Mit können Sie nicht zugewiesene Security Incidents anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Zeigen Sie auf Ihrem Mobilgerät nicht zugewiesene Elemente an, bearbeiten Sie sie, und weisen Sie sie zu Security Incident Response(SIR) Incidents. Zeigen Sie zugehörige Listen und den Audit-Pfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

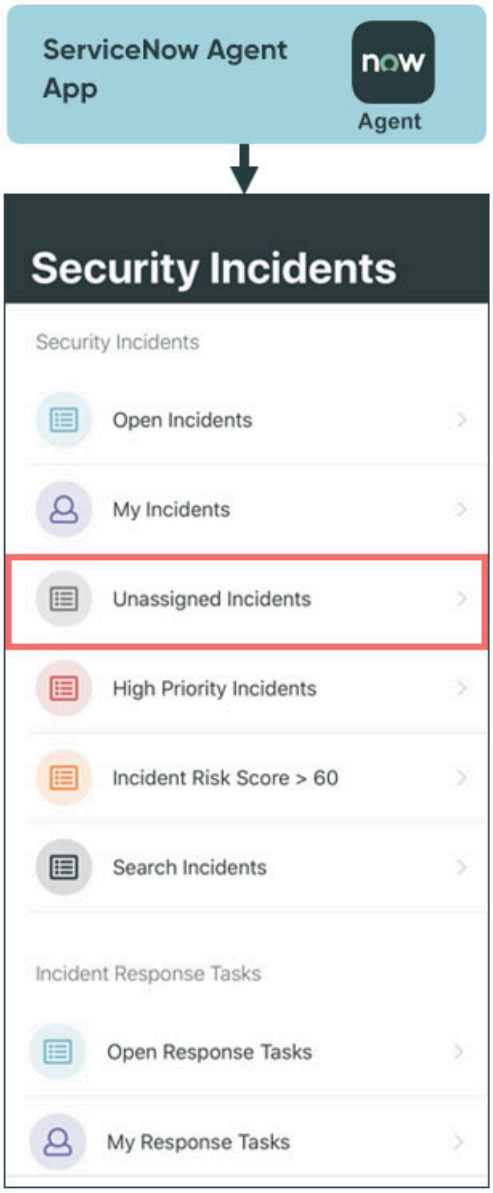
Weisen Sie sich in der Liste der Datensätze selbst oder einem anderen Analysten in Ihrer Gruppe einen offenen, nicht zugewiesenen Security Incident zu. Alternativ können Sie die Details und zugehörigen Listen des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5-10 Minuten.

Prozedur

1. Wenn Sie nicht bei angemeldet sind ServiceNow AI Platform Instanz auf Ihrem Mobilgerät. Weitere Informationen finden Sie unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie auf, während der Zielbildschirm für Security Incidents angezeigt wird **Nicht Zugewiesene Incidents** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

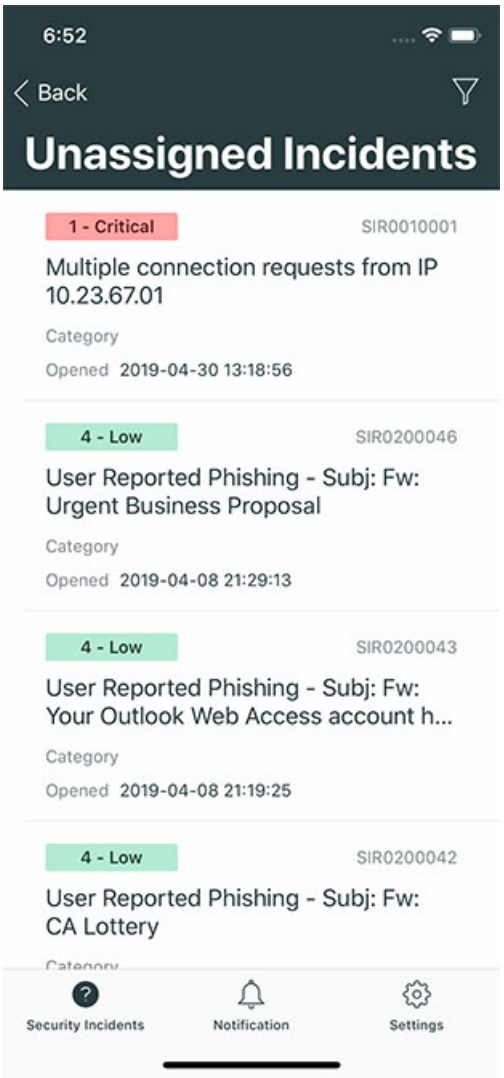
Wenn Sie weg von navigieren Security Incident Response Mobile-App Nachdem Sie sich angemeldet haben, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm nicht zugewiesene Incidents wird mit einer Liste nicht zugewiesener Security Incident-Datensätze angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

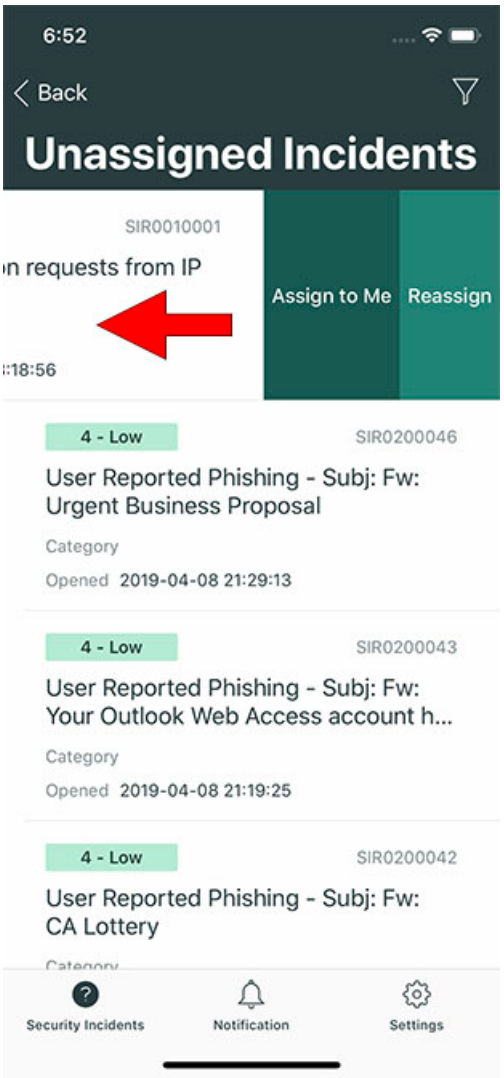


3. **Wahlweise:** Siehe Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App Um nach Security Incidents zu suchen, die bestimmten Kriterien entsprechen.

   Alternativ mit dem Filtersymbol ( ) Angezeigt, Legen Sie Filter fest, um die Anzahl der Datensätze zu begrenzen In der Liste. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator im ServiceNow AI Platform.

4. Um einen offenen Security Incident-Datensatz direkt aus der Liste zuzuweisen oder neu zuzuweisen, wobei die Liste der offenen, nicht zugewiesenen Security Incident-Datensätze angezeigt wird, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

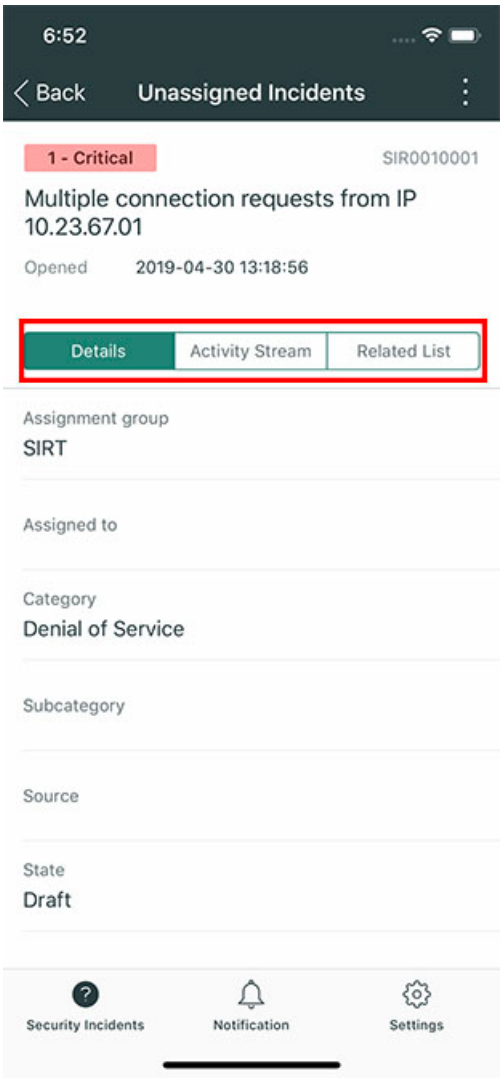


5. Wählen Sie einen aus dem Menü aus, um fortzufahren.

6. Alternativ können Sie, wenn der Bildschirm nicht zugewiesene Incidents angezeigt wird, auf einen Datensatz in der Liste tippen.

7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Mit können Sie Incidents mit hoher Priorität anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Zeigen Sie auf Ihrem Mobilgerät an, bearbeiten Sie sie, und weisen Sie ihnen eine hohe Priorität zu Security Incident Response(SIR) Incidents. Zeigen Sie zugehörige Listen und den Audit-Pfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

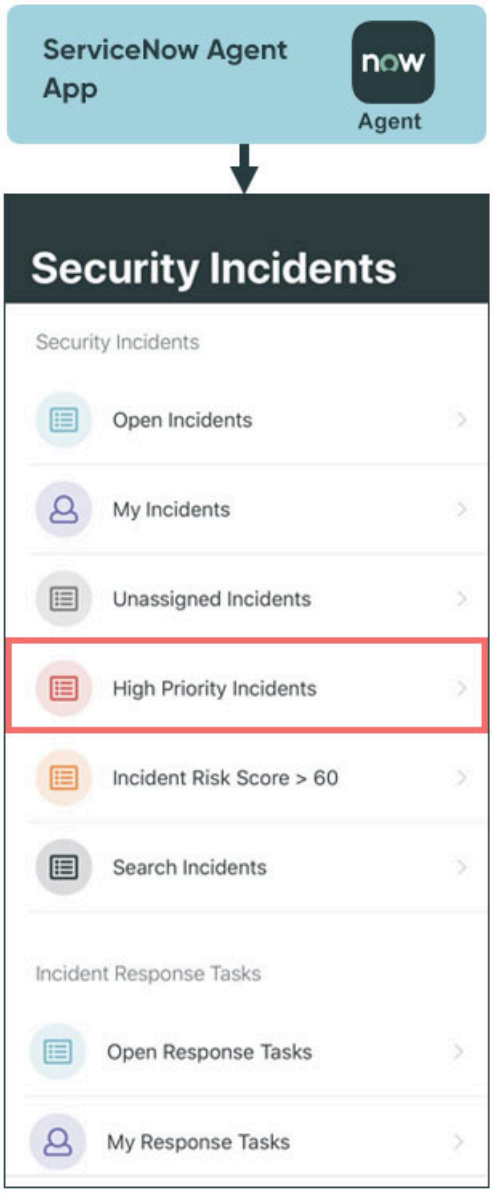
Weisen Sie sich in der Liste der Datensätze selbst oder einem anderen Analysten in Ihrer Gruppe einen offenen, kritischen Security Incident zu. Alternativ können Sie die Details und zugehörigen Listen des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5-10 Minuten.

Prozedur

1. Wenn Sie nicht bei angemeldet sind ServiceNow AI Platform Instanz auf Ihrem Mobilgerät. Weitere Informationen finden Sie unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie auf, während der Zielbildschirm für Security Incidents angezeigt wird **Incidents Mit Hoher Priorität** .

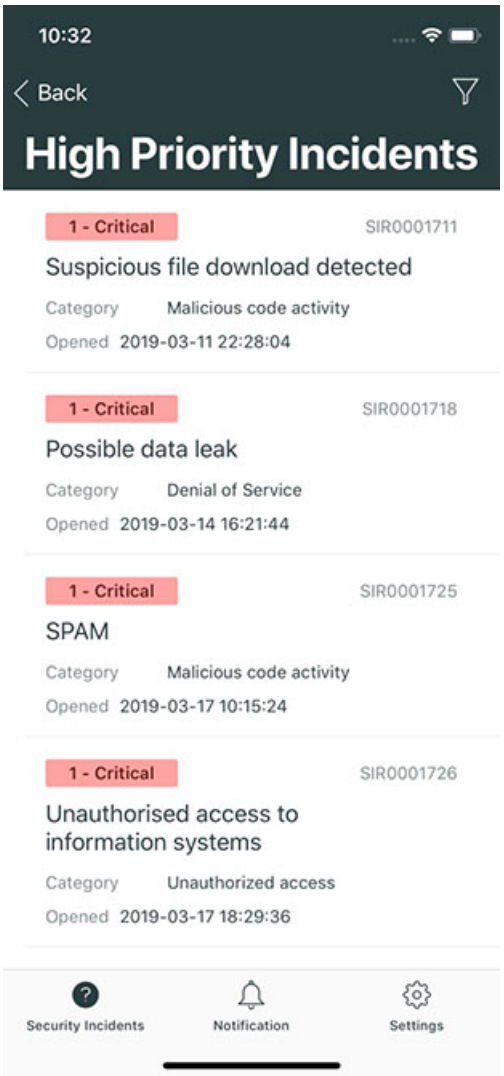
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie weg von navigieren Security Incident Response Mobile-App Nachdem Sie sich angemeldet haben, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm Incidents mit hoher Priorität wird mit einer Liste kritischer Security Incidents mit hoher Priorität angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

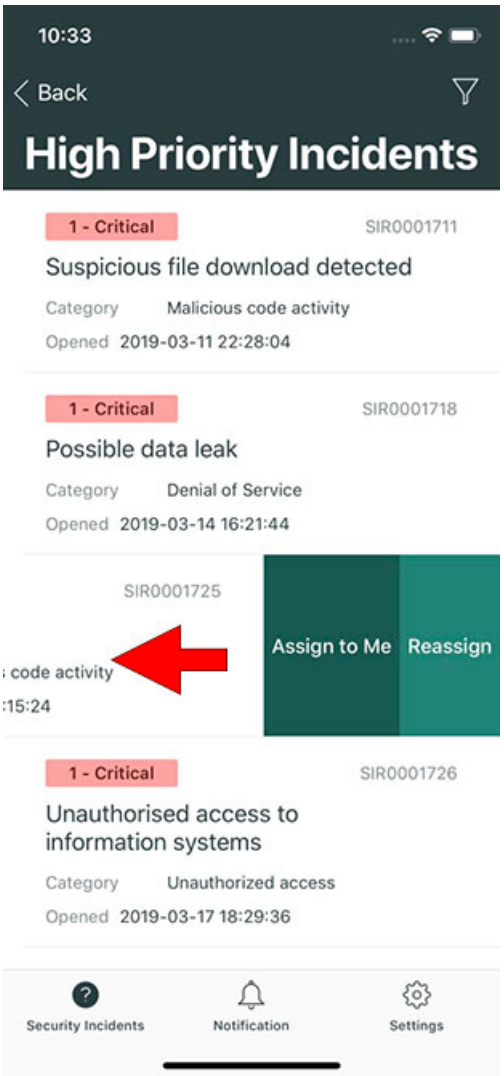


3. **Wahlweise:** Siehe Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App Um nach Security Incidents zu suchen, die bestimmten Kriterien entsprechen.

   Alternativ mit dem Filtersymbol ( ) Angezeigt, Legen Sie Filter fest, um die Anzahl der Datensätze zu begrenzen In der Liste. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator im ServiceNow AI Platform.

4. Wenn die Liste der offenen Security Incident-Datensätze mit hoher Priorität angezeigt wird, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.

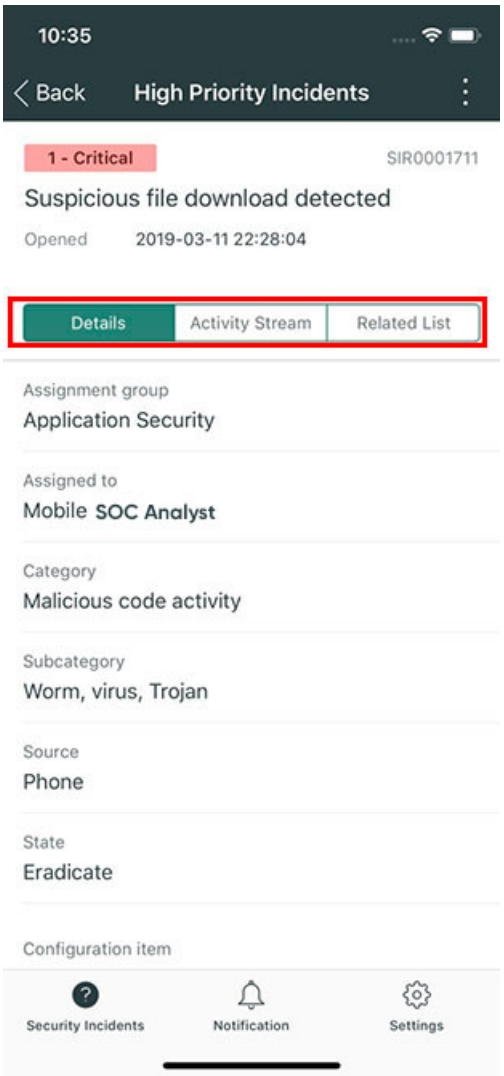
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie eine, um fortzufahren.

6. Um die Details eines offenen Security Incident-Datensatzes anzuzeigen und weitere zugehörige Datensätze und zugehörige Listen anzuzeigen, während der Bildschirm Incidents mit hoher Priorität angezeigt wird, tippen Sie auf einen Datensatz in der Liste.
7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Mit können Sie Security Incidents mit einer Risikopunktzahl größer als 60 anzeigen, bearbeiten und zuweisen Security Incident Response Mobile-App

Zeigen Sie auf Ihrem Mobilgerät an, und bearbeiten Sie sie Security Incident Response(SIR) Incidents mit einem Wert im Feld „Risikopunktzahl“, der größer als 60 ist. Zeigen Sie zugehörige Listen und den Audit-Pfad von Arbeitsnotizen an, um weitere Details zu Incidents zu erhalten.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

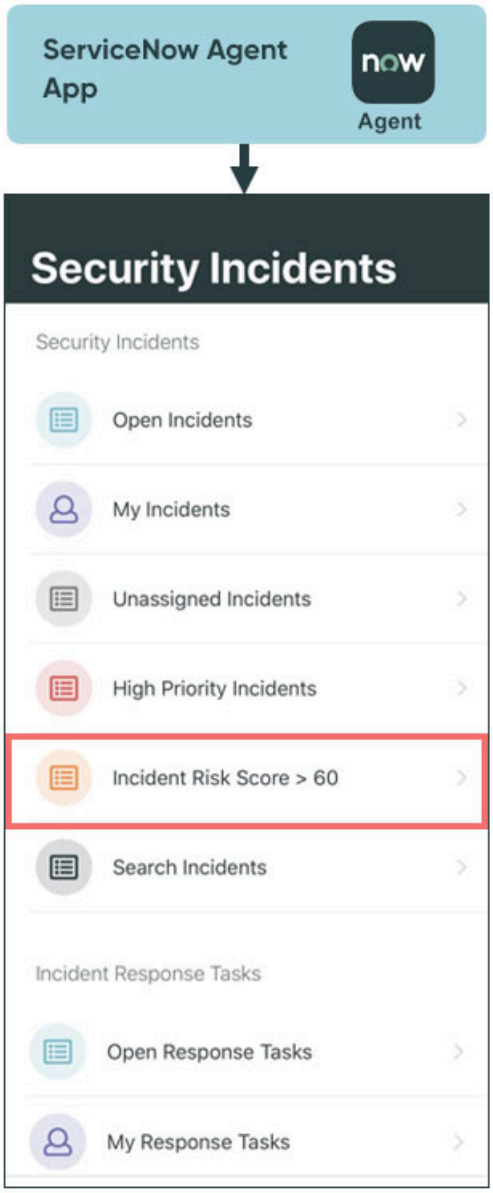
Weisen Sie in der Liste der Datensätze einen offenen Security Incident mit einer Risikopunktzahl von mehr als 60 Ihnen oder einem anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie die Details und zugehörigen Listen des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5-10 Minuten.

Prozedur

1. Wenn Sie nicht bei angemeldet sind ServiceNow AI Platform Instanz auf Ihrem Mobilgerät. Weitere Informationen finden Sie unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie auf, während der Zielbildschirm für Security Incidents angezeigt wird **Risikopunktzahl > 60** .

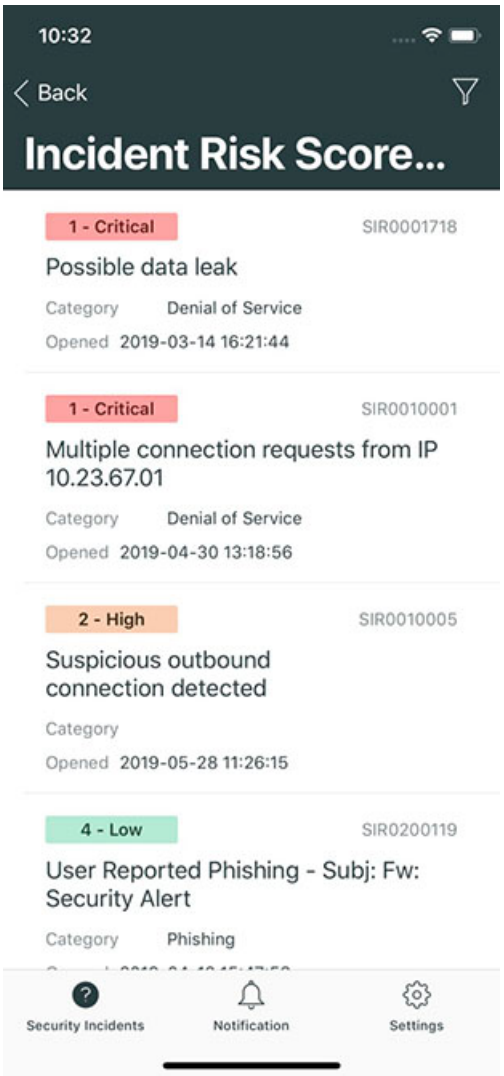
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie weg von navigieren Security Incident Response Mobile-App Nachdem Sie sich angemeldet haben, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm „Incident-Risikopunktzahl“ wird mit einer Liste von Security Incidents angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

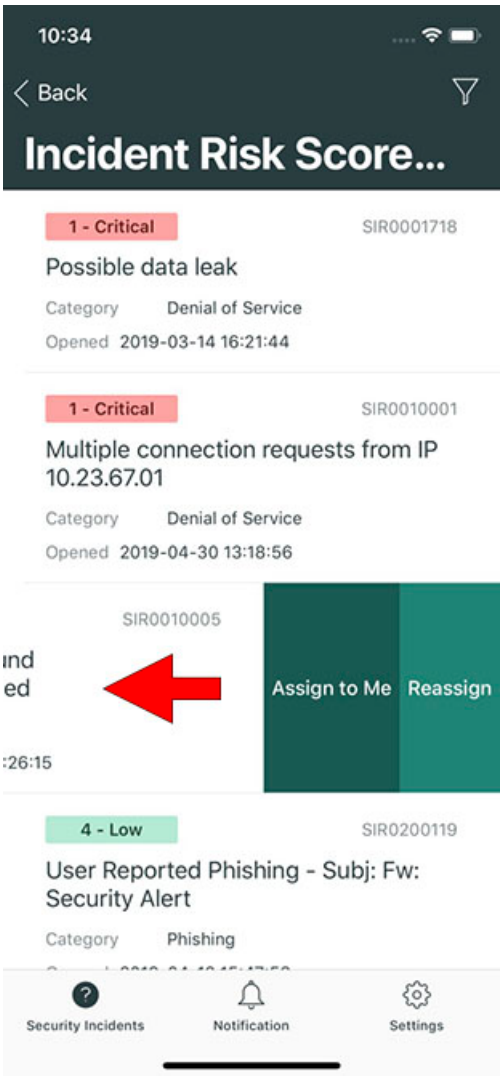


3. **Wahlweise:** Siehe Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App Um nach Security Incidents zu suchen, die bestimmten Kriterien entsprechen.

   Alternativ mit dem Filtersymbol ( ) Angezeigt, Legen Sie Filter fest, um die Anzahl der Datensätze zu begrenzen In der Liste. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator im ServiceNow AI Platform.

4. Um sich selbst einen Security Incident zuzuweisen oder ihn direkt aus der Liste der angezeigten offenen Security Incident-Datensätze neu zuzuweisen, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.

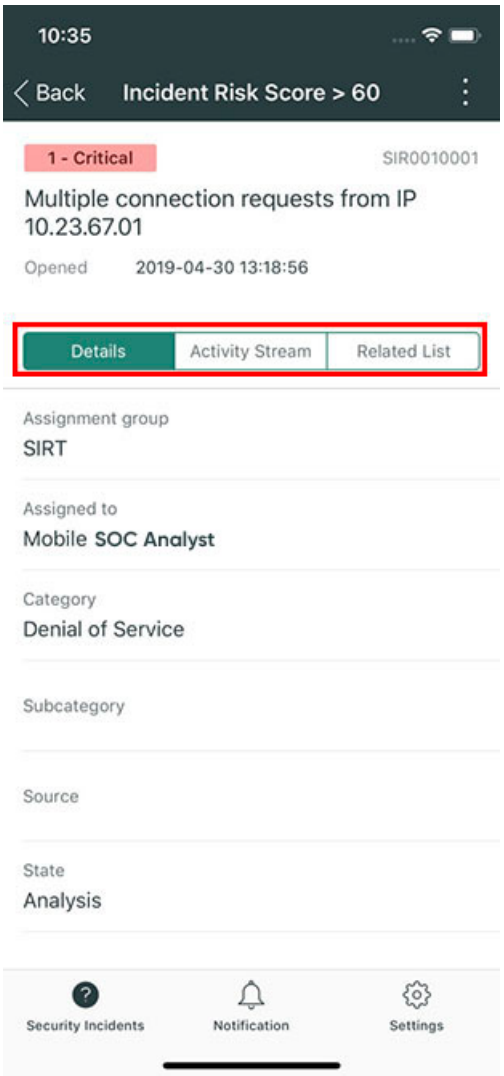
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie eine, um fortzufahren.

6. Alternativ können Sie auf einen Datensatz in der Liste tippen, um die Details eines offenen Security Incident-Datensatzes anzuzeigen und weitere zugehörige Datensätze und zugehörige Listen anzuzeigen, während der Bildschirm „Incident-Risikopunktzahl“ angezeigt wird.
7. Wählen Sie im angezeigten offenen Datensatz eine Option aus der folgenden Tabelle aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App

Suchen Sie nach Security Incident Response(SIR) Security Incidents auf einem ServiceNow AI Platform® Instanz. Es werden nur Incidents angezeigt, die den von Ihnen eingegebenen Suchkriterien entsprechen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

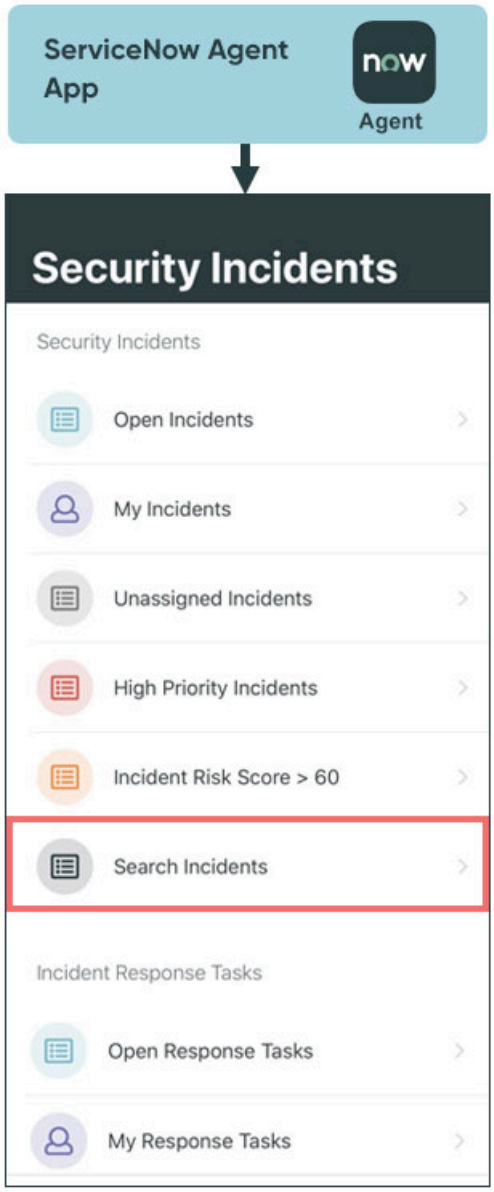
Zeit bis zum Abschluss dieser Aufgabe: 5-10 Minuten.

Prozedur

1. Wenn Sie nicht bei angemeldet sind ServiceNow AI Platform Instanz auf Ihrem Mobilgerät. Weitere Informationen finden Sie unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie auf, während der Zielbildschirm für Security Incidents angezeigt wird **Incidents Durchsuchen** .

   Wenn Sie weg von navigieren Security Incident Response Mobile-App Nachdem Sie sich angemeldet haben, tippen Sie jederzeit auf den Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Um die Anzahl der zurückgegebenen Suchergebnisse zu begrenzen, sollten Sie möglichst viele Felder im Formular ausfüllen.
   Informationen zum Hinzufügen von Suchkriterien finden Sie in der folgenden Tabelle. Befolgen Sie die Anweisungen nach der Tabelle, um vorhandene Suchkriterien zu bearbeiten, Suchkriterien zu löschen oder eine Suche zu übermitteln.

Tippen Sie auf dieses Feld	Zum Hinzufügen eines Eintrags zu Android Geräte	Zum Hinzufügen von und -Einträgen zu iOS Geräte
Anzahl	Geben Sie einen alphanumerischen Wert für einen Security Incident ein, z. B. SIR0010004 . Diese Zahl wird oben rechts im Security Incident angezeigt. Die Funktion sucht nach numerischen Zeichenfolgen	Geben Sie einen alphanumerischen Wert für einen Security Incident ein, z. B. SIR0010004 . Diese Zahl wird oben rechts im Security Incident angezeigt. Die Funktion sucht nach numerischen Zeichenfolgen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tippen Sie auf dieses Feld	Zum Hinzufügen eines Eintrags zu Android Geräte	Zum Hinzufügen von und -Einträgen zu iOS Geräte
	und partiellen numerischen Zeichenfolgen. Geben Sie für detailliertere Suchvorgänge weitere Ziffern ein. Platzhalter (*) werden nicht akzeptiert. Tippen Sie auf ein neues Feld, um weitere Kriterien oder einzugeben Um eine Suche zu übermitteln.	und partiellen numerischen Zeichenfolgen. Geben Sie für detailliertere Suchvorgänge weitere Ziffern ein. Platzhalter (*) werden nicht akzeptiert. Tippen Sie auf ein neues Feld, um weitere Kriterien oder einzugeben **Suchen** Um eine Suche zu übermitteln.
Kurzbeschreibung	Geben Sie Text in das Feld ein, z. B. Malware . Die Funktion sucht im Feld Kurzbeschreibung nach Textzeichenfolgen und Teiltextzeichenfolgen. Geben Sie für detailliertere Suchvorgänge mehr Text ein. Platzhalter (*) werden nicht akzeptiert. Tippen Sie auf ein neues Feld, um weitere Kriterien oder einzugeben Um eine Suche zu übermitteln.	Geben Sie Text in das Feld ein, z. B. Malware . Die Funktion sucht im Feld Kurzbeschreibung nach Textzeichenfolgen und Teiltextzeichenfolgen. Geben Sie für detailliertere Suchvorgänge mehr Text ein. Platzhalter (*) werden nicht akzeptiert. Tippen Sie auf ein neues Feld, um weitere Kriterien oder einzugeben **Suchen** Um eine Suche zu übermitteln.
Priorität	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf das Häkchensymbol, um zum Bildschirm „Incidents durchsuchen“ zurückzukehren.	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie Auf **Fertig** Um zum Bildschirm „Incidents durchsuchen“ zurückzukehren.
Kategorie	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie auf das Häkchensymbol, um zum Bildschirm „Incidents durchsuchen“ zurückzukehren.	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie Auf **Fertig** Um zum Bildschirm „Incidents durchsuchen“ zurückzukehren.
Status	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie	Um einen Eintrag hinzuzufügen, tippen Sie auf ein oder mehrere Elemente, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Tippen Sie Auf **Fertig**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tippen Sie auf dieses Feld	Zum Hinzufügen eines Eintrags zu Android Geräte	Zum Hinzufügen von und -Einträgen zu iOS Geräte
	auf das Häkchensymbol, um zum Bildschirm „Incidents durchsuchen“ zurückzukehren.	Um zum Bildschirm „Incidents durchsuchen“ zurückzukehren.
Zugewiesen an	Wählen Sie einen aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie für keinen Eintrag aus **Keine**.	Wählen Sie einen aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie für keinen Eintrag aus **Keine**.
Zuweisungsgruppe	Wählen Sie einen aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie für keinen Eintrag aus **Keine**.	Wählen Sie einen aus der Liste aus, oder tippen Sie auf das Suchsymbol, und geben Sie einen Eintrag in das Suchfeld ein. Um einen Wert für die Felder Zuweisungsgruppe und Zugewiesen an zu löschen, wählen Sie für keinen Eintrag aus **Keine**.

Für Android Geräte, bei denen der Bildschirm Incidents durchsuchen angezeigt und alle Ihre Kriterien eingegeben werden, wählen Sie eines aus, um fortzufahren.

4. Für iOS Wählen Sie Geräte, bei denen der Bildschirm Incidents durchsuchen angezeigt wird, eines aus, um fortzufahren.

5. **Wahlweise:** Wenn Ihre Suche mehrere Datensätze zurückgibt, können Sie dies tun Datensätze mit filtern Security Incident Response Mobile-App Zum Verfeinern der Suchergebnisse.

Zeigen Sie offene Antwortaufgaben mit an, bearbeiten Sie sie, und weisen Sie sie zu Security Incident Response Mobile-App

Zeigen Sie offene Antwortaufgaben an, bearbeiten Sie sie, und weisen Sie sie zu. Ihre Änderungen werden in der Security Incident Response-Aufgabe des übergeordneten Security Incidents gespeichert.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

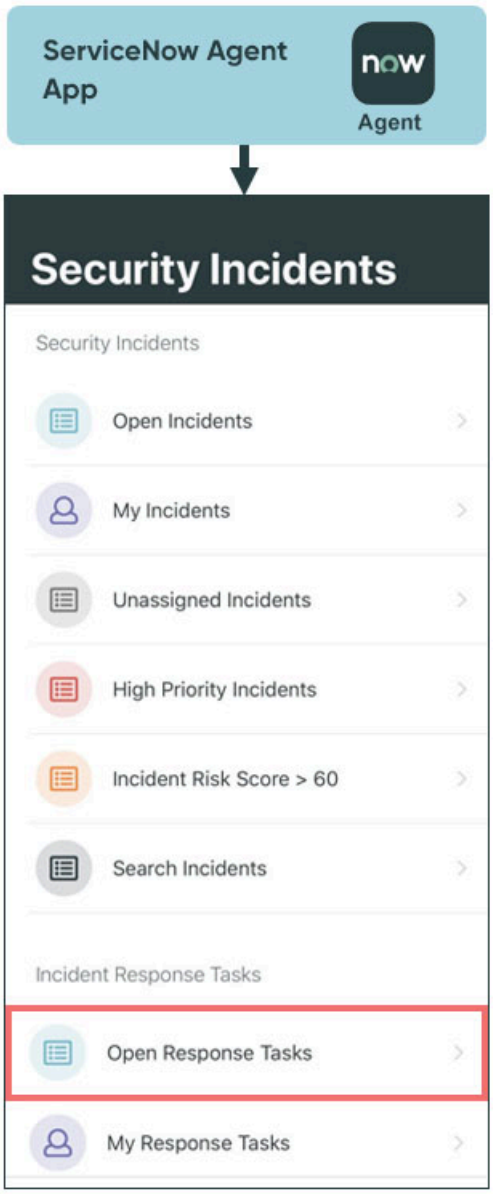
Weisen Sie sich in der Liste der Datensätze selbst oder einem anderen Analysten in Ihrer Gruppe eine offene, nicht zugewiesene Antwortaufgabe zu. Alternativ können Sie die Details des Datensatzes anzeigen oder vor der Zuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5-10 Minuten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wenn Sie nicht bei angemeldet sind ServiceNow AI Platform Instanz auf Ihrem Mobilgerät. Weitere Informationen finden Sie unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie auf, während der Zielbildschirm für Security Incidents angezeigt wird **Öffnen Sie Antwortaufgaben** .

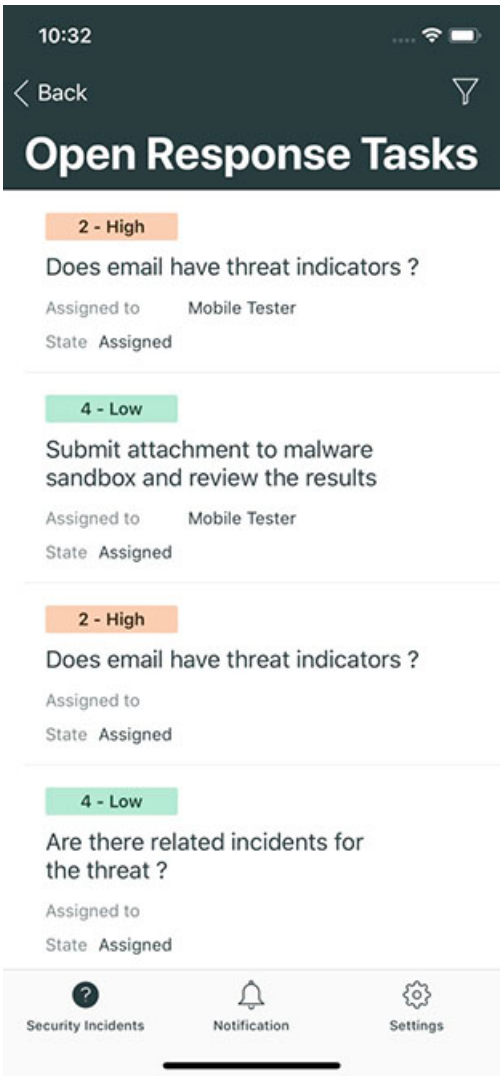
   Wenn Sie weg von navigieren Security Incident Response Mobile-App Nachdem Sie sich angemeldet haben, tippen Sie jederzeit auf die App Now Agent, um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm offene Antwortaufgaben wird mit einer Liste offener Aufgaben angezeigt.

Automatische Übersetzung

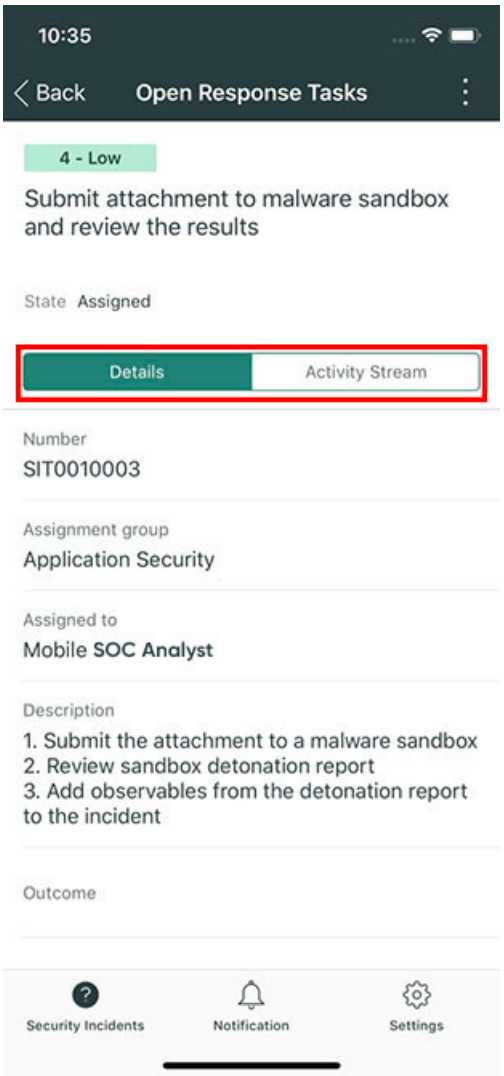
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. **Wahlweise:** Siehe Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App Um nach Aufgaben zu suchen, die bestimmten Kriterien entsprechen.

   Alternativ mit dem Filtersymbol ( ) Angezeigt, Legen Sie Filter fest, um die Anzahl der Datensätze zu begrenzen In der Liste. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator im ServiceNow AI Platform.
4. Wenn die Liste der offenen Antwortaufgaben angezeigt wird, wischen Sie zum Zuweisen oder Neuzuweisen direkt aus der Liste auf einem Datensatz nach links, um das Menü zu öffnen.
5. Wählen Sie eine, um fortzufahren.
6. Alternativ können Sie auf einen Datensatz in der Liste tippen, um die Details eines Datensatzes einer offenen Antwortaufgabe anzuzeigen, wenn der Bildschirm offene Antwortaufgaben angezeigt wird.
7. Wenn die Registerkarten im Antwortaufgabendatensatz angezeigt werden, wählen Sie eine in der folgenden Tabelle aus, um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zeigen Sie Ihre Antwortaufgaben mit an, bearbeiten Sie sie, und weisen Sie sie neu zu Security Incident Response Mobile-App

Zeigen Sie Ihnen zugewiesene Antwortaufgaben an, bearbeiten Sie sie, und weisen Sie sie neu zu. Ihre Änderungen werden in der Security Incident Response-Aufgabe des übergeordneten Security Incidents gespeichert.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

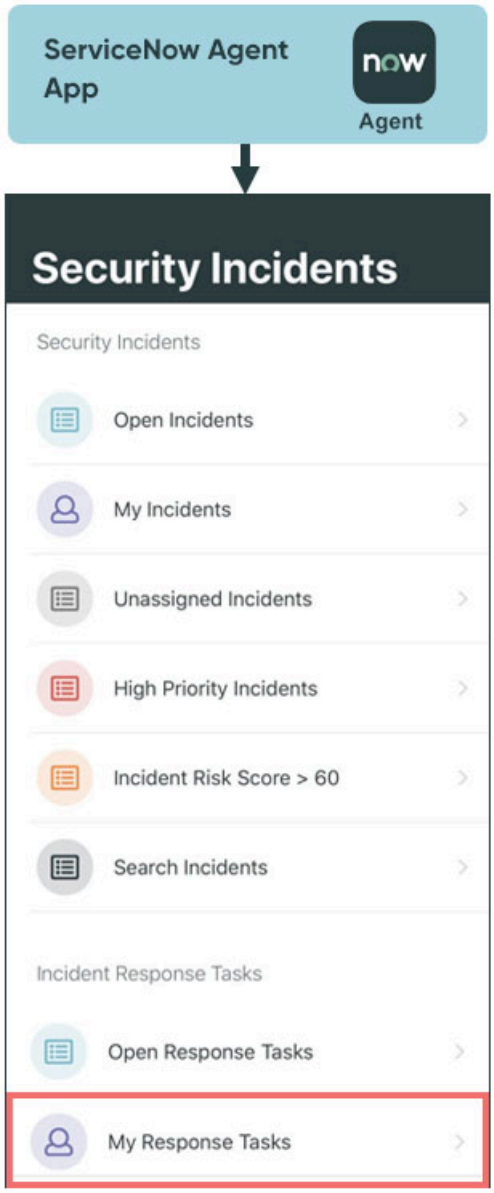
Weisen Sie in der Liste der Datensätze eine offene Antwortaufgabe, die Ihnen zugewiesen ist, einem anderen Analysten in Ihrer Gruppe zu. Alternativ können Sie die Details des Datensatzes anzeigen oder vor der Neuzuweisung eine Arbeitsnotiz hinzufügen. Zeit bis zum Abschluss dieser Aufgabe: 5-10 Minuten.

Prozedur

1. Wenn Sie nicht bei angemeldet sind ServiceNow AI Platform Instanz auf Ihrem Mobilgerät. Weitere Informationen finden Sie unter Melden Sie sich bei an Security Incident Response Mobile-App.
2. Tippen Sie auf, während der Zielbildschirm für Security Incidents angezeigt wird **Meine Antwortaufgaben** .

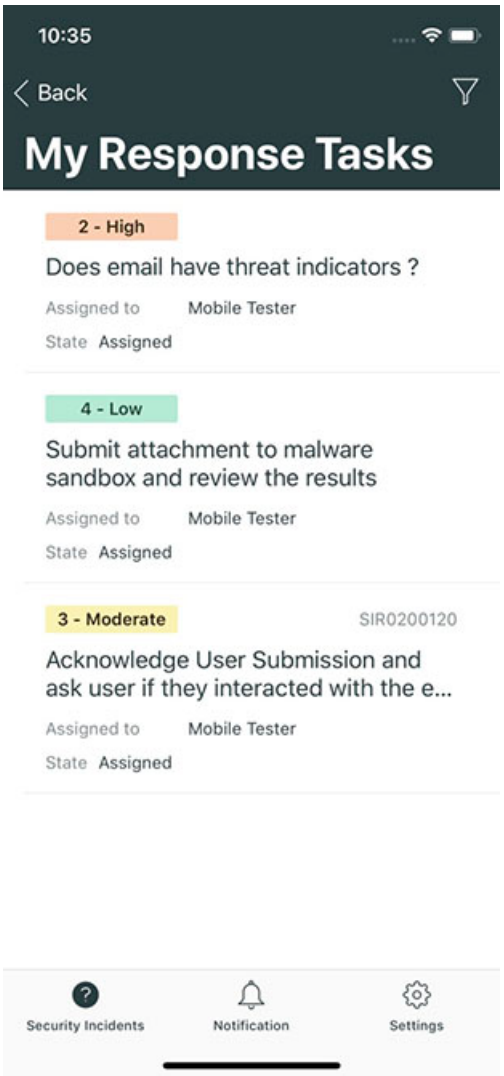
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie weg von navigieren Security Incident Response Mobile-App Nachdem Sie sich angemeldet haben, tippen Sie jederzeit auf die App Now Agent (Erfüller), um zum zuletzt angezeigten Bildschirm zurückzukehren.



Der Bildschirm meine Antwortaufgaben wird mit einer Liste der Ihnen zugewiesenen Antwortaufgaben angezeigt.

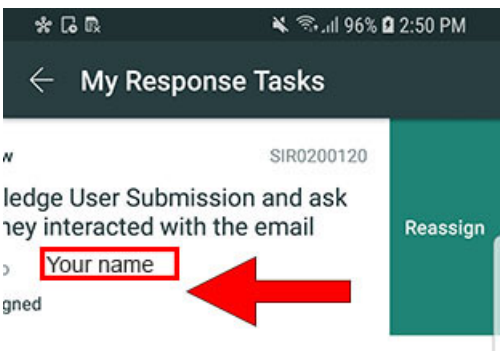
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. **Wahlweise:** Siehe Suchen Sie mit nach Security Incidents Security Incident Response Mobile-App Um nach Aufgaben zu suchen, die bestimmten Kriterien entsprechen.

   Alternativ mit dem Filtersymbol ( ) Angezeigt, Legen Sie Filter fest, um die Anzahl der Datensätze zu begrenzen In der Liste. Das Filtern von Datensätzen auf Bildschirmen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator im ServiceNow AI Platform.

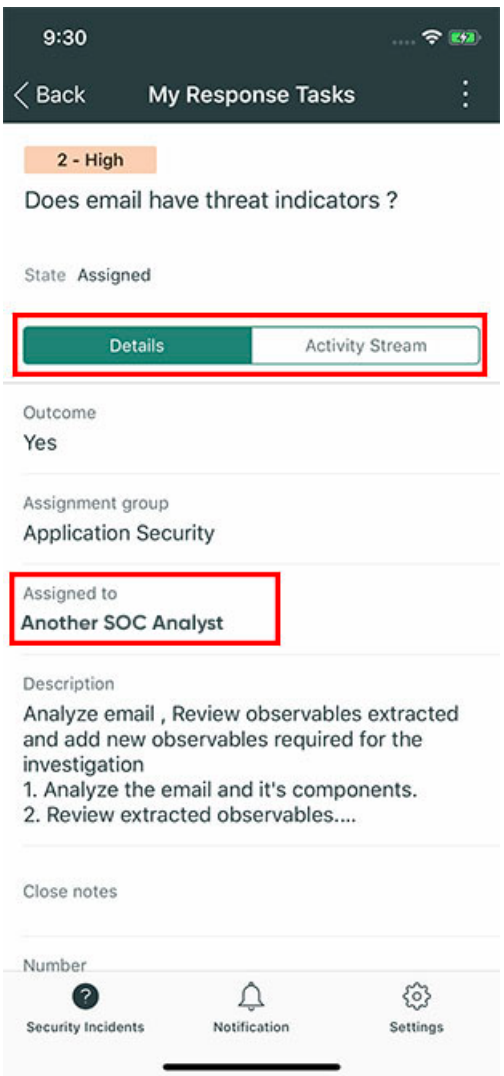
4. Um eine Aufgabe direkt aus der Liste der Ihnen zugewiesenen Aufgabendatensätze neu zuzuweisen, wischen Sie auf einem Datensatz nach links, um das Menü zu öffnen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Tippen Sie Auf **Neu Zuweisen** .
6. Tippen Sie auf dem angezeigten Bildschirm Antwortaufgabe einer anderen zuweisen auf ein Feld, um es zu erweitern, und wählen Sie eine andere Gruppe oder einen anderen Anwender für die Aufgabe aus.
7. Tippen Sie auf das Sendesymbol ( ) Oder **Übermitteln** Um Ihre Änderungen zu speichern und die Antwortaufgabe zu aktualisieren.
   Eine Nachricht wird angezeigt, die bestätigt, dass der Datensatz aktualisiert wurde. Die Aufgabe wird einem neuen Anwender im übergeordneten Security Incident und Ihrem zugewiesen ServiceNow AI Platform Instanz wird aktualisiert.
8. Um die Details einer offenen Antwortaufgabe anzuzeigen und die Arbeitsnotizen anzuzeigen, während der Bildschirm „meine Antwortaufgaben“ angezeigt wird, tippen Sie auf einen Datensatz in der Liste.
9. Wenn die Felder in der Antwortaufgabe angezeigt werden, wählen Sie eines in der folgenden Tabelle aus, um fortzufahren.



Datensätze mit filtern Security Incident Response Mobile-App

Legen Sie zusätzliche Filter fest, um die Anzahl der Datensätze zu begrenzen, die in einem Bildschirm angezeigt werden. Das Filtern von Datensätzen in der Mobile-App funktioniert wie das Filtern mit einem Bedingungsgenerator auf der ServiceNow AI Platform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Zeit bis zum Abschluss dieser Aufgabe: 5 Minuten.

Prozedur

1. Um Ihre Suchergebnisse weiter zu verfeinern oder zusätzliche Filterkriterien in einer angezeigten Liste von Datensätzen einzugeben, tippen Sie auf das Filtersymbol ( ).
2. Wenn der Bildschirm Filter angezeigt wird, tippen Sie auf ein Feld, um es zu erweitern.
3. Tippen Sie in den angezeigten Optionen auf das Kontrollkästchen, oder tippen Sie auf ein Element für Ihren Filter.
   Für viele der Filter können Sie mehr als eine Option auswählen.
4. Tippen Sie auf den zurück-Pfeil ( ) Oder **FERTIG** Um Ihre Änderungen in einem Feld zu speichern.
   Die von Ihnen ausgewählten Kriterien werden auf dem Bildschirm Filter angezeigt. Die Anzahl der Datensätze, die Ihren Kriterien entsprechen, wird ebenfalls oben im Bildschirm angezeigt. Tippen Sie Auf **ZURÜCKSETZEN** Um Filter zu entfernen und die Standardeinstellung wiederherzustellen.
5. **Wahlweise:** Wiederholen Sie die Schritte 1 bis 4 mit dem Bildschirm „Filter“, um mit der Festlegung Ihrer Filterkriterien fortzufahren.
6. Tippen Sie auf das Schnittungssymbol Zum Erstellen von UND-Bedingungen.
   Alternativ können Sie auf das Schnittungssymbol tippen Um ODER-Bedingungen zu erstellen.
7. Nachdem Sie alle gewünschten Kriterien hinzugefügt haben, und der Bildschirm Filter angezeigt wird, tippen Sie auf **FERTIG** .
   Auf dem Bildschirm werden nur die Datensätze angezeigt, die Ihren Filterkriterien entsprechen.

Security Incident Response Orchestration

Security Incident Response Orchestration Mit Aktivitäten können Anwender mithilfe von Workflow-Orchestration mit Windows- oder UNIX-basierten Systemen und Umgebungen interagieren und Daten aus diesen abrufen.

Einrichten

Vor der Verwendung Security Incident Response Orchestration, Führen Sie Schritte zum Einrichten verschiedener Teile des Systems aus, einschließlich Ausfüllen der CMDB, Konfigurieren des MID-Servers und Konfigurieren der Anmeldeinformationen.

Vorbereitungen
Erforderliche Rolle: Administrator
Zu verwenden Security Incident Response, Sie benötigen eine vollständig ausgefüllte CMDB mit Domänennamen. Weitere Informationen finden Sie unter Discovery .

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Aktivieren Security Incident Response Plugin.
2. MID-Server werden konfiguriert .
3. Konfigurieren Sie Anmeldeinformationen für Windows MID Server-Service .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verstehen Sie sich mit Security Incident Response Orchestration-Workflows und Workflow-Vorlagen

Die Security Incident Response Das Basissystem enthält eine Reihe von Workflows und Workflow-Vorlagen, die für die Arbeit mit Security Incident-Datensätzen konzipiert sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Basic

Warum und wann dieser Vorgang ausgeführt wird
Sie können alle Workflows und Workflow-Vorlagen besser an Ihre Anforderungen anpassen, vorausgesetzt, Sie haben die entsprechende Rolle: sn_sec_cmn.admin. Workflows werden im gesamten Security Operations-System verwendet, um eine Vielzahl von Aufgaben auszuführen.
Workflow-Vorlagen werden jedoch durch Auswahl eines Werts im ausgelöst **Kategorie** Feld in einem Security Incident. Wenn dies auftritt, startet die der Auswahl zugeordnete Workflow-Vorlage eine Workflow-Vorlage, die die Sicherheitsanalysten anweist, wie sie mit einer bestimmten Art von Bedrohung umgehen.

Beispiel: Wenn Sie auswählen **Denial of Service** Von **Kategorie** Feld in einem Security Incident, der **Security Incident – Denial of Service – Vorlage** Wird ausgeführt, und der Analyst wird angewiesen, zu bestimmen, ob das Ziel der DOS geschäftskritisch ist. Wenn dies der Fall ist, wird mit der nächsten Aufgabe die Priorität des Security Incidents auf festgelegt **1: Kritisch** , Und führt dann die nächste Aufgabe aus. Und so weiter.

Also Security Incident Response Workflows und Workflow-Vorlagen sind im Wesentlichen identisch, mit der Ausnahme, dass die Vorlagen für einen bestimmten Satz von Funktionen in einem Security Incident verwendet werden.

Prozedur
1. Navigieren zu **Alle** > **Security Operations** > **Workflows** > **Sicherheitsworkflows anzeigen**an.
2. Eine Liste der im Basissystem gelieferten Workflows und Workflow-Vorlagen wird angezeigt.
   Alle neuen Workflows, die Sie in erstellt haben Security Operations Die Anwendungs-Suite ist ebenfalls in der Liste enthalten.
3. Klicken Sie auf den Namen des Workflows oder der Workflow-Vorlage, den Sie anzeigen möchten.

Hinweis:
Workflows können auf verschiedene Arten ausgelöst werden. Beachten Sie, dass die Zuordnung eines Workflows zu einem Workflow-Auslöser nicht unbedingt bedeutet, dass der Workflow aktiv ist.

Security Incident Response Orchestration Workflows und Aktivitäten

Mehrere Workflows und Aktivitäten sind in enthalten Security Incident Response Orchestration.

Nur Anwender mit der Rolle sn_sec_cmn.admin können dies tun Workflow-Editor .

Erstellen Sie einen Suchanforderung für IOC-Changes-Workflow

Die **Antwort auf Security Incident: Suchanforderung für IOC-Changes erstellen** Flow wird durch eine Business-Regel ausgelöst, die automatisch ausgeführt wird, wenn ein IOC hinzugefügt oder geändert wird. Malware-Scans werden nur ausgelöst, wenn neue Daten eingegeben und nur die neuen Daten gescannt werden.

Vorbereitungen
Erforderliche Rolle: sn_si.Basic

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Wenn das IOC leer ist, wird der Workflow nicht ausgeführt. Verlaufsscans werden beibehalten und können in angezeigt werden **Sicherheitsscananforderungen** Registerkarte und Arbeitsnotizen des Security Incidents. Die vorhandenen Security Incidents werden automatisch aktualisiert.

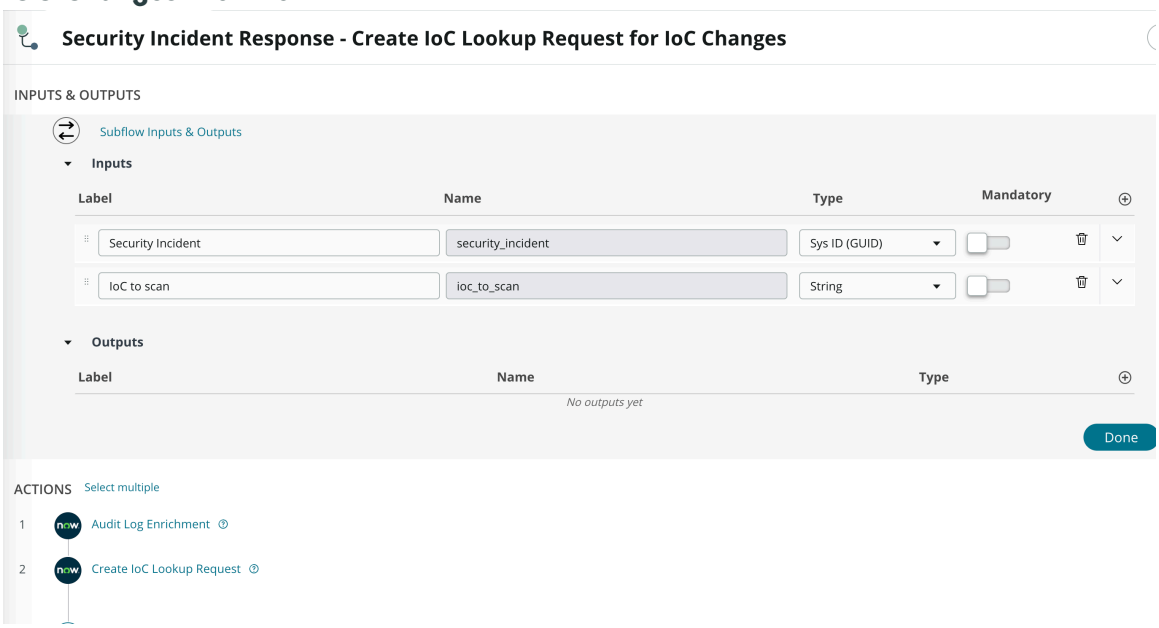
Wichtig:

Die **Antwort auf Security Incident: Suchanforderung für IOC-Changes erstellen** Workflow wird zum Flow Designer migriert. Der Flow wird nur ausgelöst, wenn der sn_ti_Scanner über mindestens einen Datensatz verfügt.

Die Flow Designer-Aktionen umfassen:

- Audit-Protokollanreicherung
- Aktivität „IOC-Suchanforderung erstellen“

IOC-Changes-Workflow



Aktivität „IOC-Suchanforderung erstellen“

Die **Erstellen Sie eine IOC-Suchanforderung** Aktivität kann mit jedem Workflow verwendet werden, um eine Malware-Suchanforderung für hinzugefügte oder geänderte IOC-Felder zu erstellen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Suchanforderung erstellt.
Fehler	Suchanforderung nicht erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Variable	Beschreibung
IocString	JSON-formatierte IOC-Informationen. IP, Hash, url.
siId	Security Incident-Systembezeichner

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
ScnReqID	Bezeichner der Suchanforderung

Security Incident Response: Flow „Netzwerkstatistiken abrufen“

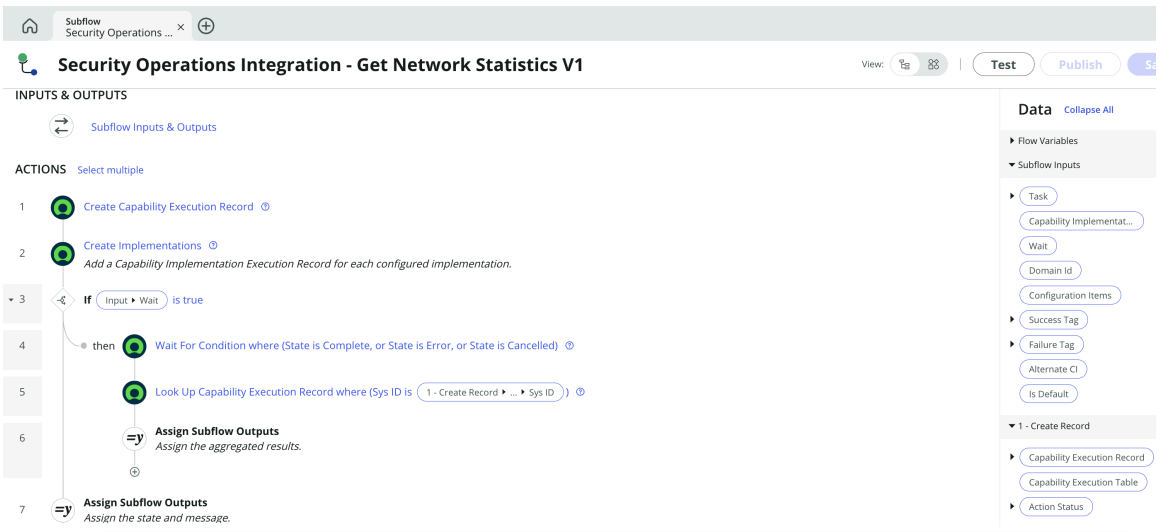
Die zugehörigen Listen namens **Security Incident Response** > **Netzwerkstatistiken abrufen** Flow ruft die Netzwerkstatistiken für eine betroffene Windows-basierte Ressource ab, wenn sie einem Security Incident in hinzugefügt wird **Analyse** status.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Bei neuen Security Incidents, die Konfigurationselemente enthalten, wird der Flow automatisch ausgeführt, wenn sich der Status in ändert **Analyse** .

Vorhandene Security Incidents werden automatisch aktualisiert, wenn Sie sich in befinden **Analyse** status, und Sie fügen ein neues Konfigurationselement hinzu.

Netzwerkstatistiken abrufen



Die Flow-Prozessaktionen umfassen:

FQDN-Flow-Aktion für Konfigurationselement abrufen

Shell-Skript nach Betriebssystem bestimmen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn-Anweisung von Powershell ausgeführt wird

Ausführungsnachverfolgung: Flow-Aktion Starten

Rufen Sie Netzwerkstatistiken über die netstat-Flow-Aktion ab

Nachverfolgung Der Fähigkeitsausführung: Fehler-Flow-Aktion

Flow-Aktion „Ergänzungsdatensätze erstellen“

Nachverfolgung Der Fähigkeitsausführung: Fehler-Flow-Aktion – Gibt die Ergänzungs-ID zurück.

Nachverfolgung Der Fähigkeitsausführung: Flow-Aktion Abschließen

Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie **Status** Bis **Analyse** , Falls erforderlich.
3. Fügen Sie ein Konfigurationselement (Computer, Server oder Ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response Orchestration Stellt Informationen zur Netzwerkstatistik in bereit **Zugehörige Links** > **Anreicherungen Von Security Incidents** Registerkarte Weitere Informationen finden Sie unter Security Operations Ergänzungsdatenzuordnung.

   Aktionen, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Security Incident Response – Workflow „laufende Services abrufen“

Die **Security Incident Response – Workflow „laufende Services abrufen“** Ruft eine Liste der ausgeführten Services von Windows-basiert ab, ServiceNow, Konfigurationselemente (CIs). Dieser Workflow wird für die Ergänzung von Incidents während Untersuchungen verwendet.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Die **Security Incident Response – Workflow „laufende Services abrufen“** Wird automatisch ausgeführt, wenn Sie einem Windows Security Incident ein neues Konfigurationselement hinzufügen, nachdem sich der Status in geändert hat **Analyse** . Die Informationen, die dieser Workflow erhält, werden auf der angezeigt **Anreicherungsdaten Anzeigen** Registerkarten für den Security Incident.

Hinweis:
Wenn der Security Incident in verbleibt **Entwurf** status, der **Security Incident Response – Workflow „laufende Services abrufen“** Workflow wird nicht ausgeführt.

Workflow-Aktivitäten umfassen:

Skriptaktivität für Audit-Protokollanreicherung

FQDN-Flow-Aktion für Konfigurationselement abrufen

Bestimmen Sie das Shell-Skript nach BS-Aktivität

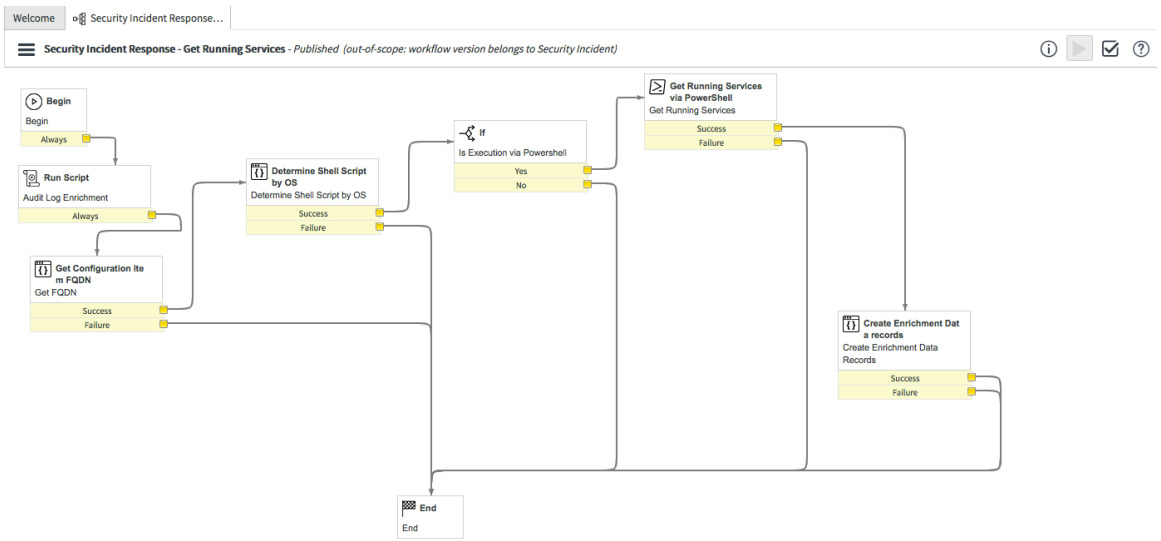
Ist Ausführung über PowerShell-Aktivität

Aktivität „laufende Services abrufen – WMI-Anreicherung“

Flow-Aktion „Ergänzungsdatensätze erstellen“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Laufende Services abrufen



Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie **Status** Bis **Analyse** , Falls erforderlich.
3. Fügen Sie ein Windows-basiertes Konfigurationselement (Server, Laptop oder Ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response Stellt Informationen zu laufenden Services in bereit **Zugehörige Links** > **Anreicherungen Von Security Incidents**Registerkarte Weitere Informationen finden Sie unter Security Operations Ergänzungsdatenzuordnung.

Bestimmen Sie das Shell-Skript nach BS-Aktivität

Die Workflow-Aktivität „Shell-Skript nach Betriebssystem bestimmen“ bestimmt, welches Betriebssystem im Workflow verwendet werden soll

Die Aktivität „Shell-Skript nach Betriebssystem bestimmen“ kann mit jedem Workflow verwendet werden, um zu bestimmen, welches Shell-Skript basierend auf dem Betriebssystem ausgeführt werden soll, das auf dem System ausgeführt wird, das das Konfigurationselement enthält.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Betriebssystem gefunden.
Fehler	Kein Betriebssystem gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
ciSysId	Systembezeichner des Konfigurationselements.
processType	Interner Bezeichner, der definiert, welches Skript aus der Tabelle abgerufen werden soll.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
ProcessScript	ECC-Agent, der den laufenden Prozess erfasst.
ExecutionTemplate	Bestimmt, ob das Skript durch eine Probe oder mithilfe von PowerShell ausgeführt wird.
AnreicherungMappingId	Systembezeichner der Ergänzungszuordnung, die zum Transformieren der Antwortdaten verwendet wird.

Laufende Services abrufen – WMI-Ergänzung

Die **Security Incident Response: Laufende Services Abrufen** Workflow erfasst laufende Services für ein Konfigurationselement, das einem Security Incident hinzugefügt wurde.

Die **Laufende Services abrufen – WMI-Ergänzung** Die Aktivität wird automatisch gestartet, um Informationen zu laufenden Services für einen Windows-Host abzurufen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Ziel [Zeichenfolge]	Der vollqualifizierte Domänenname (FQDN) des Zielsystems.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Antwort [Zeichenfolge]	Eine JSON-Zeichenfolge, die die aktuell ausgeführten Services auf dem Zielsystem darstellt. JSON-Daten umfassen: **name** Der Name des Service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen (Fortsetzung)

Variable	Beschreibung
	pid Der Prozessbezeichner des laufenden Service **service_type** (Optional) der Typ des ausgeführten Service. **Start_Name** Der Systemname für den Service **path** Der Dateipfad der ausführbaren Datei des laufenden Service **Start_Mode** Der Startmodus des laufenden Service. **display_name** Der Name des laufenden Service, wie er dem Anwender angezeigt wird

Beschränkungen

Der MID-Server muss unterstützen **PowerShell** .

SHA-256-Hash erfordert PowerShell V4.

Procdump ausführen Flow

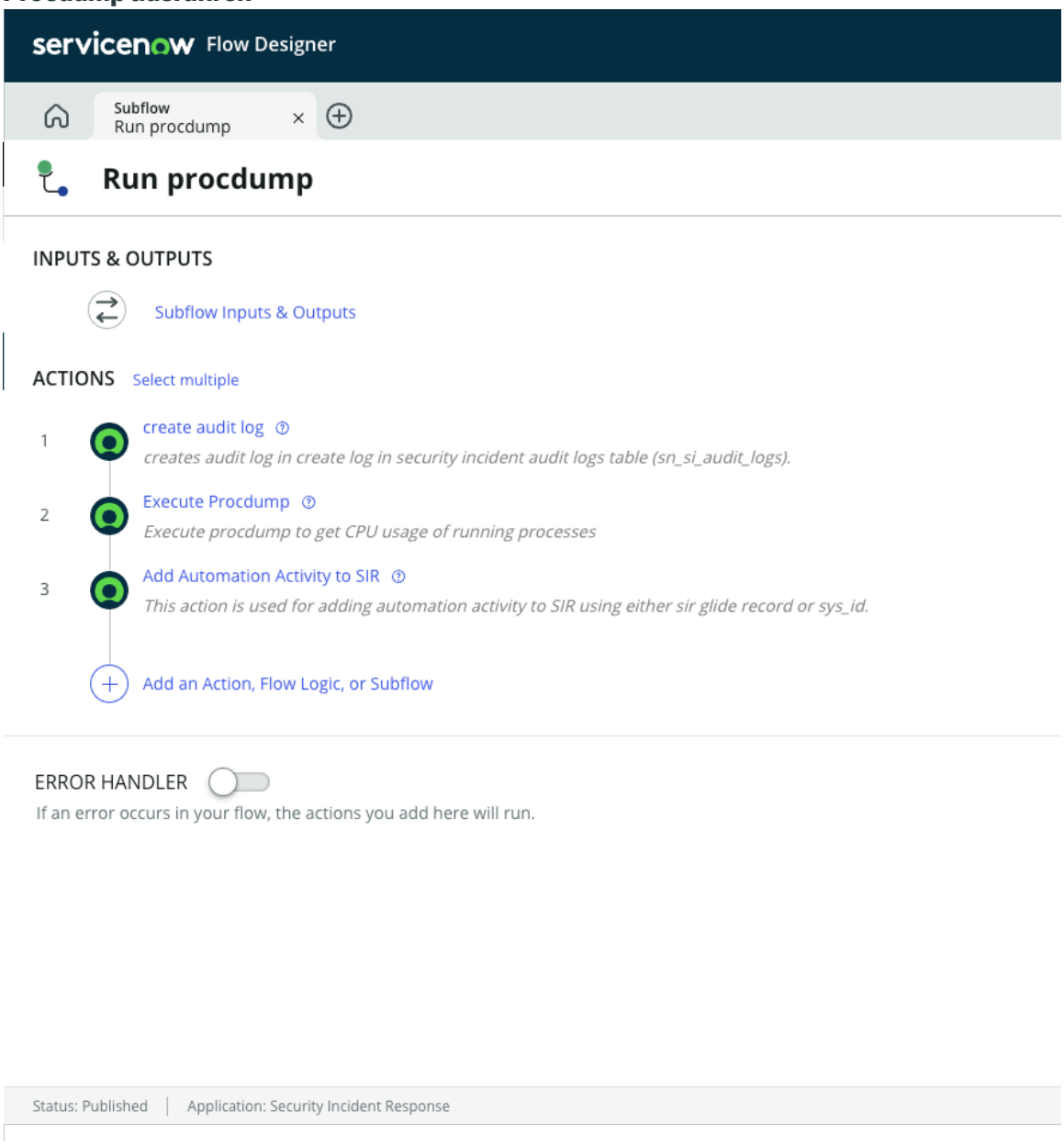
Die **Procdump ausführen** Flow führt einen Prozess-Dump für einen angegebenen Prozess aus und speichert ihn in einer Datei, die von Sicherheitsanalysten angegriffen werden kann.

Erforderliche Rolle: sn_si.Analyst

Dieser Flow wird ausgelöst, wenn angereicherte Prozesse und ausgewählt werden **Procdump ausführen** UI-Aktion wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Procdump ausführen



Gründe, aus denen der procdump fehlschlagen kann:

- Ungültiger Dump-Pfad
- Ungültiger Dateifreigabepfad
- Der vollqualifizierte dominname des Windows-Computers, auf dem der procdump ausgeführt wird, kann nicht abgerufen werden
- Der Prozessname ist nicht angegeben
- Die PROCDUMP-Umgebungsvariable wurde nicht gefunden
- Eine Kopie der Dump-Datei kann nicht aus dem Dump-Pfad in den Dateifreigabepfad kopiert werden

Procdump ausführen Aktion

Procdump ausführen Ist eine powershell-Aktion, die den procdump für die ausgewählten Prozesse ausführt, die Daten in eine Datei ausgibt und sie an einer freigegebenen Website in einem internen Netzwerk postet. Ein Analyst kann dann einen Prozess mit der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ablehnungsliste anzeigen, der in einem Security Incident rot hervorgehoben wird, und zusätzliche Analysen für die Datei durchführen.

Ergebnisse

Mögliche Ergebnisse für diese Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Der procdump wurde erfolgreich für Process_Name ausgeführt, und die Details sind in actionOutput.response verfügbar.
Fehler	Der procdump konnte für Process_Name nicht ausgeführt werden, und die Details sind in actionOutput.response verfügbar.

Eingabevariablen

Eingabevariablen werden zum Erstellen der angeforderten Ausgaben verwendet.

Eingabevariablen

Variable	Beschreibung
targetId	[Obligatorisch] die Ziel-ID, für die der procdump ausgeführt werden soll.
process_name	[Obligatorisch] der Prozessname für den procdump.
Dump_path	[Obligatorisch] der lokale Dateipfad, in dem die generierte Dumpdatei gespeichert wird.
Dump_filename	[Obligatorisch] der Dateiname der vom procdump generierten Datei. Alle Sonderzeichen werden durch Bindestriche (-) aus dem Namen der Dump-Datei ersetzt, wenn die Datei generiert wird.
File_share_path	[Obligatorisch] der Dateifreigabepfad, in den die Dump-Datei kopiert wird.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Freigabepfad	Der Dateifreigabepfad, in den die Dumpdatei kopiert wurde.
response	Eine JSON-Darstellung des Ergebnisses des procdump.
Ergebnis	Das Ergebnis des procdump.

Security Incident: Workflow zum Auswerten des Ergebnisses der Antwortaufgabe

Security Incident – der Ergebnisworkflow der Antwortaufgabe auswerten bestimmt die zu verwendende Aufgabe, ruft einen ausgewählten Workflow und ein Auswertungsskript basierend auf dem Ergebnisauswertungsdatensatz auf, der als Eingabe für den ausgewählten Workflow bereitgestellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow soll gleichzeitig mit der auszuwertenden Aufgabenerstellungsaktivität ausgeführt werden. Das Auswertungsskript fragt die Artefakte (z. B. Sichtungssuchdatensätze oder laufende Prozesse) der konfigurierten Fähigkeit ab, indem Kontextinformationen aus der Antwortaufgabe (z. B. der übergeordnete Security Incident) verwendet werden, um das entsprechende Ergebnis für die Antwortaufgabe zu bestimmen. Das Ergebnis kann potenziell abhängig von der Workflow-Aktivität sein, ist aber im Allgemeinen **ja** Oder **Nein** . Beim Erstellen eines Ergebnisauswertungsdatensatzes nur Funktionen mit konfiguriertem Workflow mit **Ist aufgabenbasierte Fähigkeit** Kontrollkästchen aktiviert, und ein Aufgabeneingabevariablensatz kann ausgewählt werden.

Workflow-Prozessaktivitäten umfassen:

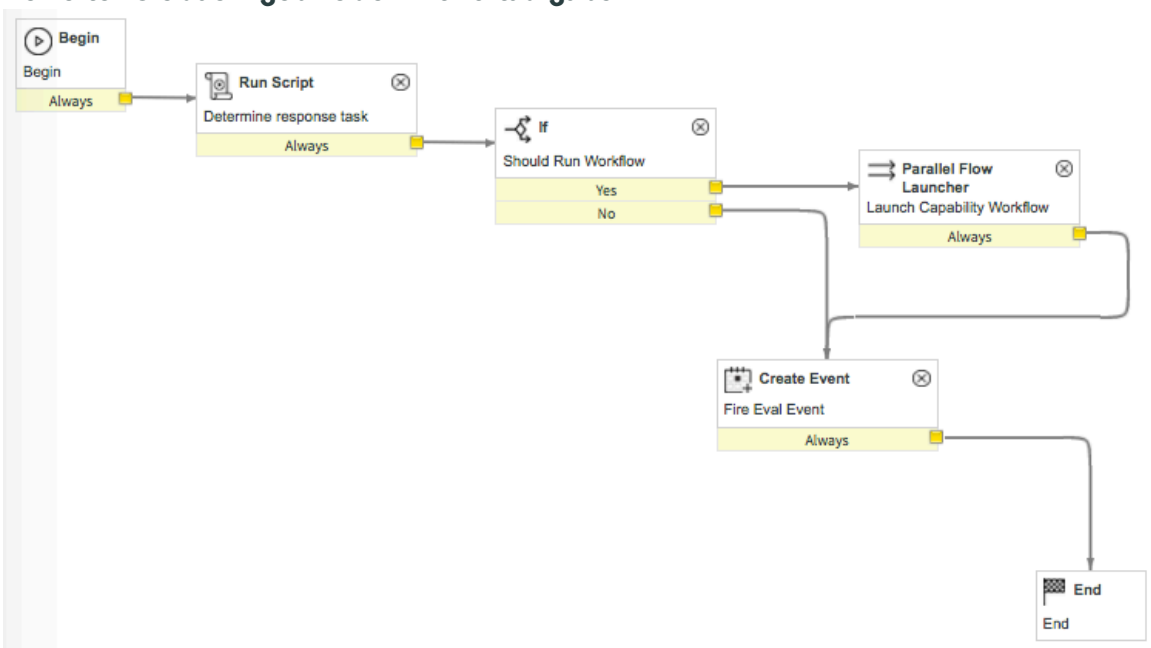
Führen Sie ein Skript aus, um die Antwortaufgabe zu bestimmen

Muss Workflow Ausführen

Workflow Für Startfähigkeit Des Parallelen Flow

Erstellen Sie Ein Auswertungsereignis

Bewerten Sie das Ergebnis der Antwortaufgabe



Workflow-Vorlagen für Security Incident Response

Workflow-Vorlagen werden mit bereitgestellt Security Incident Response Orchestration Damit Sie grundlegende Analyseverfahren im Zusammenhang mit Sicherheitsvorgängen durchführen können. Die Vorlagen können unverändert verwendet werden, oder Sie können sie anpassen, um Workflows zu erstellen, die Ihren spezifischen Anforderungen besser entsprechen. Die Workflow-Vorlagen sind standardmäßig deaktiviert.

Nur Anwender mit der Rolle sn_sec_cmn.admin können dies tun Workflow-Editor .

Workflow-Vorlage für Security Incident – Gefährdung vertraulicher Daten

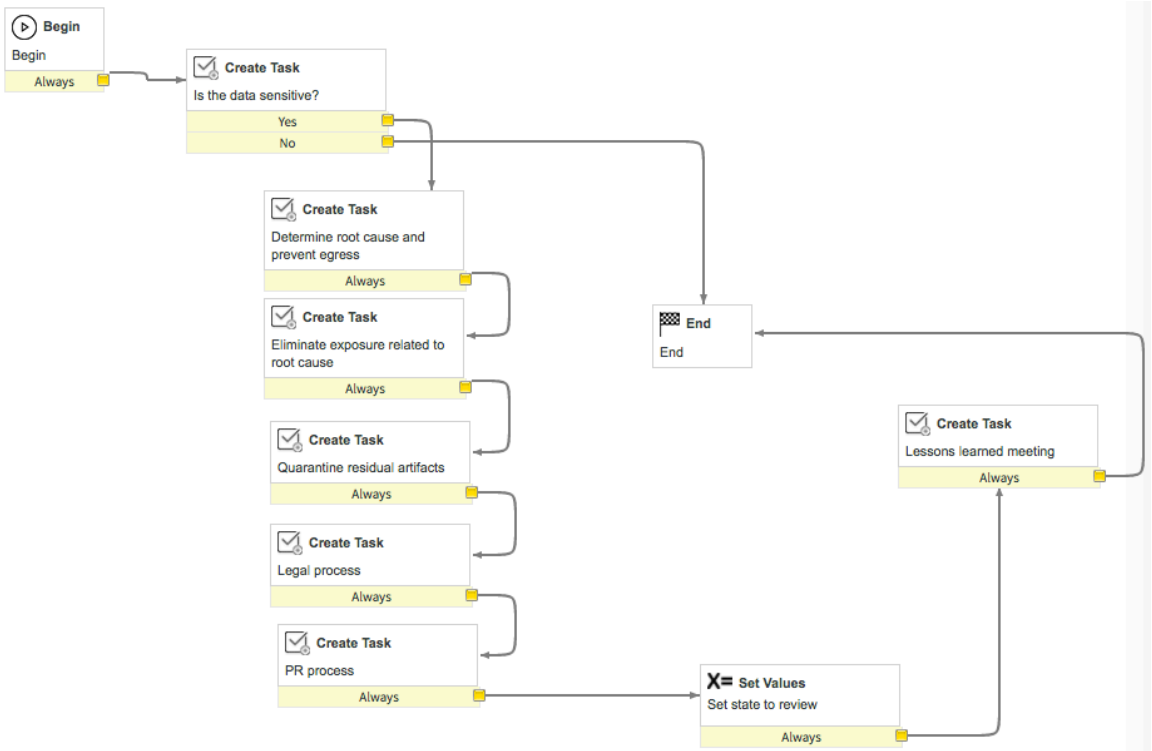
Mit der Vorlage „Security Incident – Offenlegung vertraulicher Daten“ können Sie eine Reihe von Aufgaben ausführen, die für den Umgang mit der Offenlegung vertraulicher Daten konzipiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Der Workflow wird ausgelöst, wenn **Kategorie** In wird ein Security Incident festgelegt oder in geändert **Offenlegung vertraulicher persönlicher Identitätsdaten** . Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

Offenlegung von vertraulichen persönlichen Daten



Prozedur

1. Öffnen Sie den Security Incident, für den Sie das Risiko vertraulicher Daten behandeln möchten, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Offenlegung vertraulicher persönlicher Identitätsdaten** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

Antwortaufgaben in Vorlage für Offenlegung vertraulicher Daten

Antwortaufgabe	Beschreibung	Ergebnisse
Sind die Daten vertraulich?	Bestimmen Sie, ob die mit diesem Security Incident verknüpften Daten vertraulich oder vertraulich sind. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie ausgewählt haben **Ja** , Die nächste Antwortaufgabe wird ausgeführt. Wenn Sie ausgewählt haben **Nein** , Der Flow endet.
Ursache ermitteln und	Bestimmen Sie die Ursache des Angriffs, und fügen Sie Ausgangsfilterung hinzu, um	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Beschreibung	Ergebnisse
Ausgänge verhindern	die Extraktion zu stoppen, und aktualisieren Sie den **Status** Feld in der Aufgabe entsprechend.	**Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Eliminieren Sie das Risiko im Zusammenhang mit der Ursache	Führen Sie basierend auf der Ursache die Schritte aus, um das Risiko zu beseitigen, indem Sie aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Quarantäne von Restartefakten	Führen Sie die Schritte aus, um Restripartefakte unter Quarantäne zu stellen, indem Sie aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Rechtlicher Prozess	Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen, indem Sie aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
PR-Prozess	Führen Sie die Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen, indem Sie aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** .
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die an diesen sensiblen Daten ausgeführte Arbeit zu selektieren und zu aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Der Security Incident verbleibt im **Überprüfen** geben sie an, bis Sie sie schließen.

Workflow-Vorlage für Security Incident Denial of Service

Mit der Vorlage „Security Incident – Denial of Service“ können Sie eine Reihe von Aufgaben ausführen, die für die Behandlung von Denial of Service-Angriffen (DOS) konzipiert sind.

Vorbereitungen

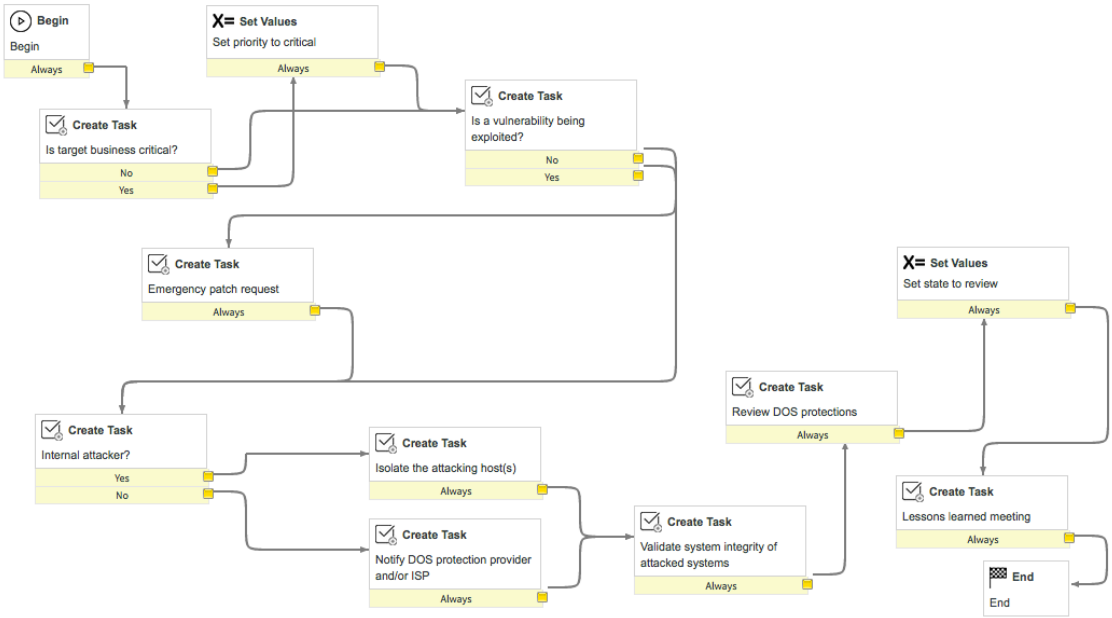
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Denial of Service** . Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Denial of Service (DOS)



Prozedur

1. Öffnen Sie den Security Incident für dieses Denial-of-Service-Ereignis, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Denial of Service** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

Antwortaufgaben in Denial of Service-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Ist das Ziel geschäftskritisch?	Bestimmen Sie, ob das Ziel dieses DOS-Angriffs geschäftskritisch ist. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Legen Sie die Priorität auf „Kritisch“ fest** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt.
Legen Sie die Priorität auf „Kritisch“ fest	Keine Aktion erforderlich.	Die **Priorität** Des Security Incidents wird automatisch in geändert **Kritisch** , Und **Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt.
Wird eine Schwachstelle ausgenutzt?	Bestimmen Sie, ob dieser DOS-Angriff eine Software-Schwachstelle ausnutzt.	Wenn Sie auswählen **Ja** , **Notfall-Patch-Anforderung** Aufgabe wird ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Nein** , **Interner Angreifer?** Aufgabe wird ausgeführt.
Notfall-Patch-Anforderung	Stellen Sie eine Notfall-Patch-Anforderung für die angegriffenen Systeme aus. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Interner Angreifer?	Bestimmen Sie, ob die Quelle dieses DOS-Angriffs in Ihrer Organisation liegt. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Angreifende Hosts isolieren** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Benachrichtigen Sie DOS-Schutzanbieter und/oder ISP** Aufgabe wird ausgeführt.
Angreifende Hosts isolieren	Führen Sie die erforderlichen Schritte aus, um die internen Hosts zu isolieren, die für den Angriff verantwortlich sind. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Nachdem Sie diesen Schritt abgeschlossen haben **Validiert die Systemintegrität der angegriffenen Systeme** Aufgabe wird ausgeführt.
Benachrichtigen Sie DOS-Schutzanbieter und/oder ISP	Führen Sie die erforderlichen Schritte aus, um sich an Ihren Denial-of-Service-Schutzanbieter und/oder Ihren Internetdienstanbieter zu wenden, um sie über den Angriff zu benachrichtigen. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Validiert die Systemintegrität der angegriffenen Systeme	Führen Sie die erforderlichen Schritte aus, um die Integrität der angegriffenen Computer zu bewerten und zu validieren. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Überprüfen Sie die DOS-Schutzmaßnahmen	Überprüfen Sie Ihre vorhandenen DOS-Schutzmaßnahmen und -Verfahren. Führen Sie alle erforderlichen Änderungen durch. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		Die **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Denial-of-Service-Incident ausgeführte Arbeit zu selektieren. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Der Flow endet.

Workflow-Vorlage für Security Incident – verlorene Geräte

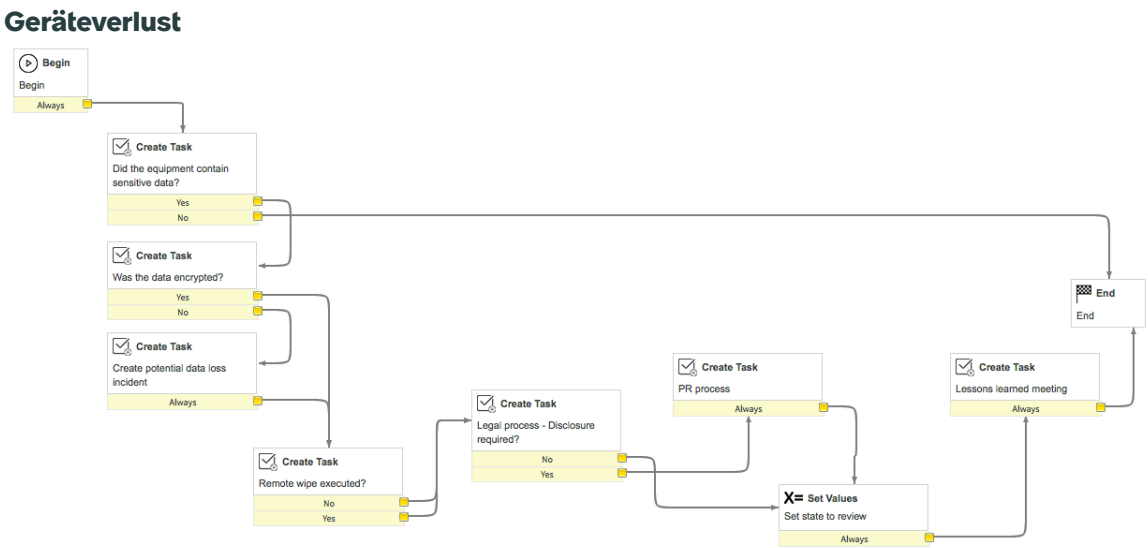
Mit der Vorlage „Security Incident – verlorene Geräte –“ können Sie eine Reihe von Aufgaben ausführen, die für den Umgang mit verlorenen Geräten konzipiert sind.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Geräteverlust** . Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.



Prozedur

1. Öffnen Sie den Security Incident für den Geräteverlust oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Geräteverlust** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgaben in Vorlage für verlorene Ausrüstung

Antwortaufgabe	Aktion	Ergebnisse
Enthielt das Gerät vertrauliche Daten?	Bestimmen Sie, ob die diesem Security Incident zugeordneten Geräte vertrauliche oder vertrauliche Informationen enthielten. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** Entsprechend.	Wenn Sie auswählen **Ja** Die **Wurden die Daten verschlüsselt?** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , Der Flow endet.
Wurden die Daten verschlüsselt?	Bestimmen Sie, ob die vertraulichen Daten auf dem verlorenen Gerät verschlüsselt wurden. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** Entsprechend.	Wenn Sie auswählen **Ja** , **Remote-Löschung erstellt?** Antwortaufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Erstellen Sie einen Incident für potenziellen Datenverlust** Antwortaufgabe wird ausgeführt.
Erstellen Sie einen Incident für potenziellen Datenverlust	Führen Sie die erforderlichen Schritte aus, um einen Incident für potenziellen Datenverlust zu erstellen. Nachdem Sie fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	Die **Remote-Löschung erstellt?** Antwortaufgabe wird ausgeführt.
Remote-Löschung erstellt?	Führen Sie die erforderlichen Schritte aus, um eine Remote-Löschung der verlorenen Geräte auszuführen. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** Entsprechend.	Die **Rechtlicher Prozess: Offenlegung erforderlich** Aufgabe wird ausgeführt.
Rechtlicher Prozess – Offenlegung erforderlich?	Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen. Wählen Sie Aus **Ja** Wenn eine rechtliche Offenlegung erforderlich ist, **Nein** Wenn nicht.	Die **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
PR-Prozess	Führen Sie die erforderlichen Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen. Nachdem Sie fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	Die **Legen Sie den Status auf „Überprüfen" fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf	Es ist keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
„Überprüfen“ fest		
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Incident für verlorene Geräte ausgeführte Arbeit zu selektieren. Nachdem Sie fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	Der Flow endet.

Workflow-Vorlage für Security Incident schädliche Software

Mit der Vorlage „Security Incident – schädliche Software –“ können Sie eine Reihe von Aufgaben ausführen, die für den Umgang mit schädlicher Software in Ihrem Netzwerk konzipiert sind.

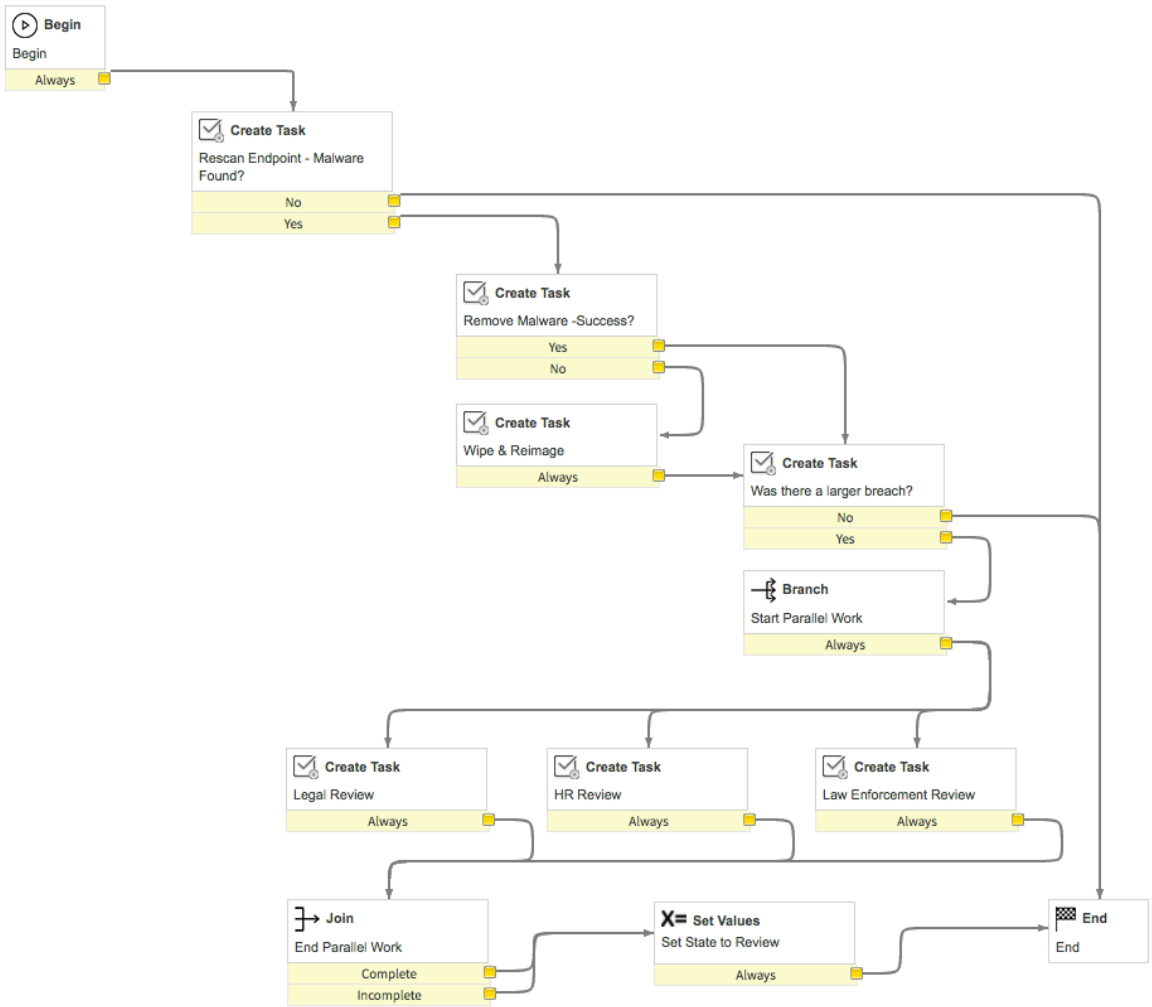
Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Der Workflow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Schädliche Software** . Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Schädliche Software



Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Schädliche Codeaktivität** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Workflow beendet wird

Antwortaufgaben in Vorlage für schädliche Software

Antwortaufgabe	Aktion	Ergebnisse
Scan-Endpunkt – Malware Gefunden?	Ermitteln Sie nach dem Ausführen eines Scans, ob Malware gefunden wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Malware Entfernen – Erfolg?** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , Der Flow endet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
Malware Entfernen – Erfolg?	Bestimmen Sie, ob die Malware erfolgreich entfernt wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Gab es einen größeren Verstoß?** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Löschen Und Neu Erstellen** Aufgabe wird ausgeführt.
Löschen Und Neu Erstellen	Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie in dieser Aufgabe angewiesen, auf den mit der Malware infizierten Computern ein Wischvorgang durchzuführen.	Nachdem die Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Gab es einen größeren Verstoß?	Ermitteln Sie, ob der durch die schädliche Software verursachte Verstoß größer ist als zuerst angenommen. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , Die folgenden Aufgaben werden parallel ausgeführt: ○ Rechtliche Überprüfung ○ HR-Überprüfung ○ Überprüfung Durch Strafverfolgungsbehörden Wenn Sie auswählen **Nein** , Der Flow endet.
Rechtliche Überprüfung HR-Überprüfung Überprüfung Durch Strafverfolgungsbehörden	Führen Sie die Schritte aus, die für jede dieser Abteilungen erforderlich sind, um den Prozess zu überprüfen, den Sie zur Beseitigung der schädlichen Software befolgt haben.	Wenn die Aufgaben abgeschlossen sind, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** , Und der Flow endet.

Vorlage für Security Incident-Phishing-Workflow

Mit der Vorlage „Security Incident – Phishing –“ können Sie eine Reihe von Aufgaben ausführen, die für die Verarbeitung von Spear-Phishing-E-Mails in Ihrem Netzwerk konzipiert sind.

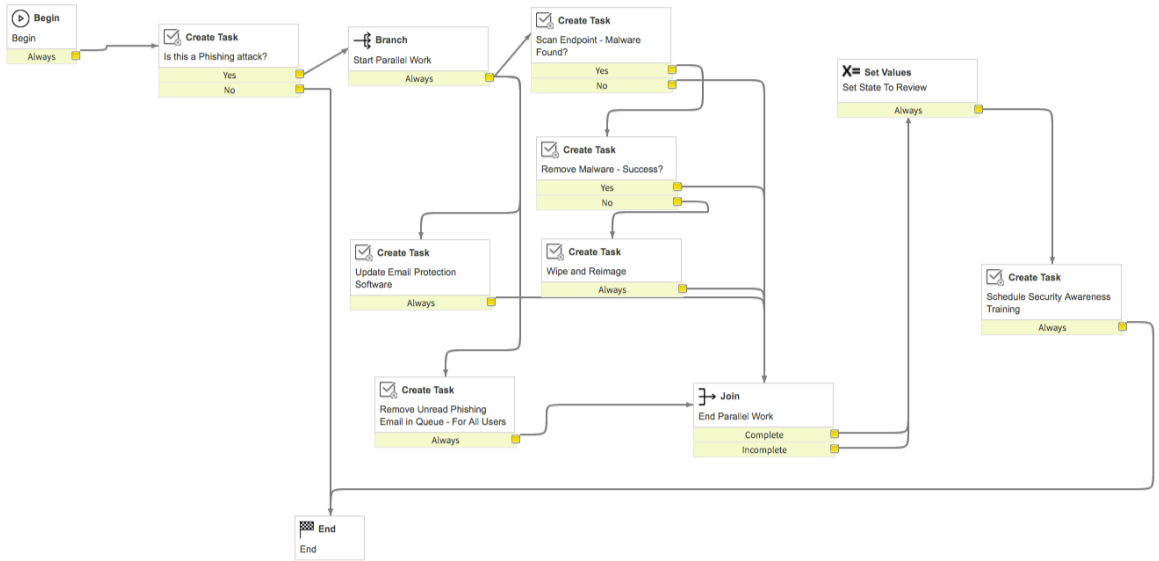
Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Spear-Phishing** . Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Spear-Phishing-Angriff, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Spear-Phishing** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Workflow beendet wird

Antwortaufgaben in Spear Phishing-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Handelt es sich um einen Phishing-Angriff?	Ermitteln Sie, ob es sich um einen Phishing-Angriff handelt. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , Die folgenden Aufgaben werden parallel ausgeführt: ○ Scan-Endpunkt – Malware Gefunden? ○ E-Mail-Schutzsoftware Aktualisieren ○ Ungelesene Phishing-E-Mail in Warteschlange entfernen – für alle Anwender Wenn Sie auswählen **Nein** , Der Flow endet.
Scan-Endpunkt – Malware Gefunden?	Ermitteln Sie nach dem Ausführen eines Scans, ob Malware gefunden wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Malware Entfernen – Erfolg?** Aufgabe wird ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		Wenn Sie auswählen **Nein** , **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Malware Entfernen – Erfolg?	Bestimmen Sie, ob die Malware erfolgreich entfernt wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Löschen und neu erstellen** Aufgabe wird ausgeführt.
Löschen und neu erstellen	Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie in dieser Aufgabe angewiesen, auf den mit der Malware infizierten Computern ein Wischvorgang durchzuführen.	Nachdem die Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
E-Mail-Schutzsoftware Aktualisieren	Wenn festgestellt wurde, dass es sich um einen Phishing-Angriff handelt, werden Sie aufgefordert, Ihre E-Mail-Schutzsoftware entsprechend zu aktualisieren.	Wenn die Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Ungelesene Phishing-E-Mail in Warteschlange entfernen – für alle Anwender	Führen Sie die erforderlichen Schritte aus, um die Phishing-E-Mail zu entfernen, die sich für alle Ihre Anwender noch in der Warteschlange befindet.	Wenn die Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** . Die **Planen Sie Eine Schulung Zum Sicherheitsbewusstsein** Aufgabe wird ausgeführt.
Planen Sie Eine Schulung Zum Sicherheitsbewusstsein	Planen Sie Schulungen, um das Sicherheitsbewusstsein Ihrer Mitarbeiter zu erhöhen. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn die Aufgabe abgeschlossen ist, endet der Flow.

Workflow-Vorlage für Security Incident-Richtlinienverstoß

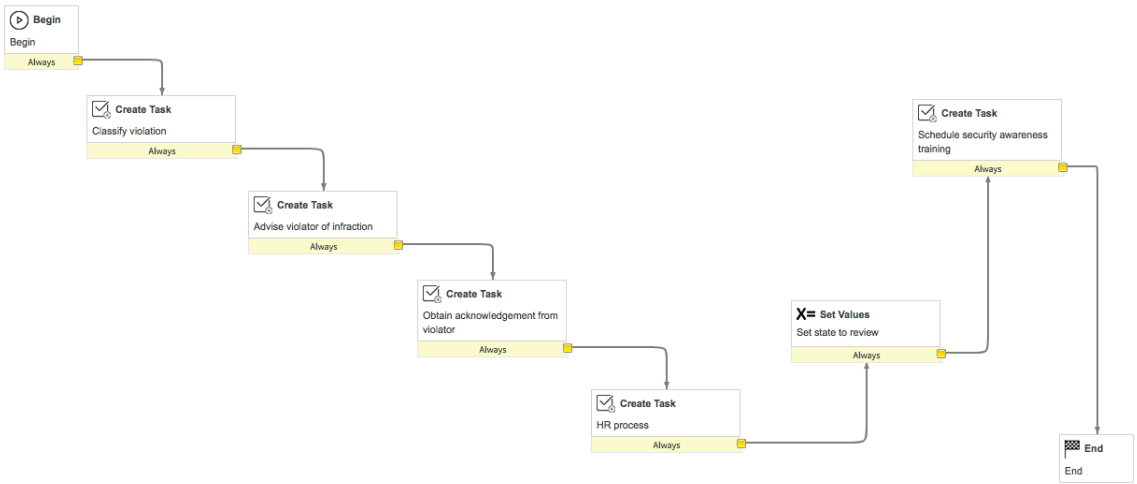
Mit der Vorlage „Security Incident – Richtlinienverstoß –“ können Sie eine Reihe von Aufgaben ausführen, die für die Behandlung von Verstößen gegen Sicherheitsrichtlinien konzipiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Der Workflow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Richtlinienverstoß** . Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

Richtlinienverstoß



Prozedur

1. Öffnen Sie den Security Incident für den Richtlinienverstoß, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Richtlinienverstoß** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Workflow beendet wird

Antwortaufgaben in Richtlinienverstoßvorlage

Antwortaufgabe	Aktion	Ergebnisse
Verstoß klassifizieren	Klassifizieren Sie, wie dieser Verstoß gegen die Sicherheitsrichtlinien Ihrer Organisation verstößt. Aktualisieren Sie **Status** Feld in der Aufgabe, nachdem Sie sie abgeschlossen haben.	Die **Benachrichtigen Sie den Verstoßer über den Verstoß** Antwortaufgabe wird ausgeführt.
Benachrichtigen Sie den Verstoßer über den Verstoß	Teilen Sie dem Verstoßgegner die Art des Verstoßes mit. Aktualisieren Sie **Status** Feld in der Aufgabe, nachdem Sie sie kommuniziert haben.	Die **Holen Sie eine Bestätigung vom Verstoßer ein** Antwortaufgabe wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
Holen Sie eine Bestätigung vom Verstoßer ein	Holen Sie eine Bestätigung des Verstoßes vom Verstoss ein. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Die **HR-Prozess** Antwortaufgabe wird ausgeführt.
HR-Prozess	Teilen Sie HR alle erforderlichen Informationen zu diesem Verstoß mit. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Die **Legen Sie den Status auf „Überprüfen“ fest** Antwortaufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Es ist keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** .
Planen Sie eine Schulung zum Sicherheitsbewusstsein	Führen Sie eine Schulung zum Sicherheitsbewusstsein durch, um Mitarbeiter darin zu Schulen, wie ähnliche Sicherheitsverletzungen in Zukunft verhindert werden können. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Der Flow endet.

Vorlage für Security Incident Reconnaissance-Workflow

Die Aufklärung ist normalerweise ein erster Schritt in Richtung eines weiteren Angriffs, bei dem ein Gerät oder System ausgenutzt werden soll. Mit der Vorlage „Security Incident – Reconnaissance –“ können Sie eine Reihe von Aufgaben ausführen, die für die Durchführung von Aufklärungen in Ihrem Netzwerk konzipiert sind.

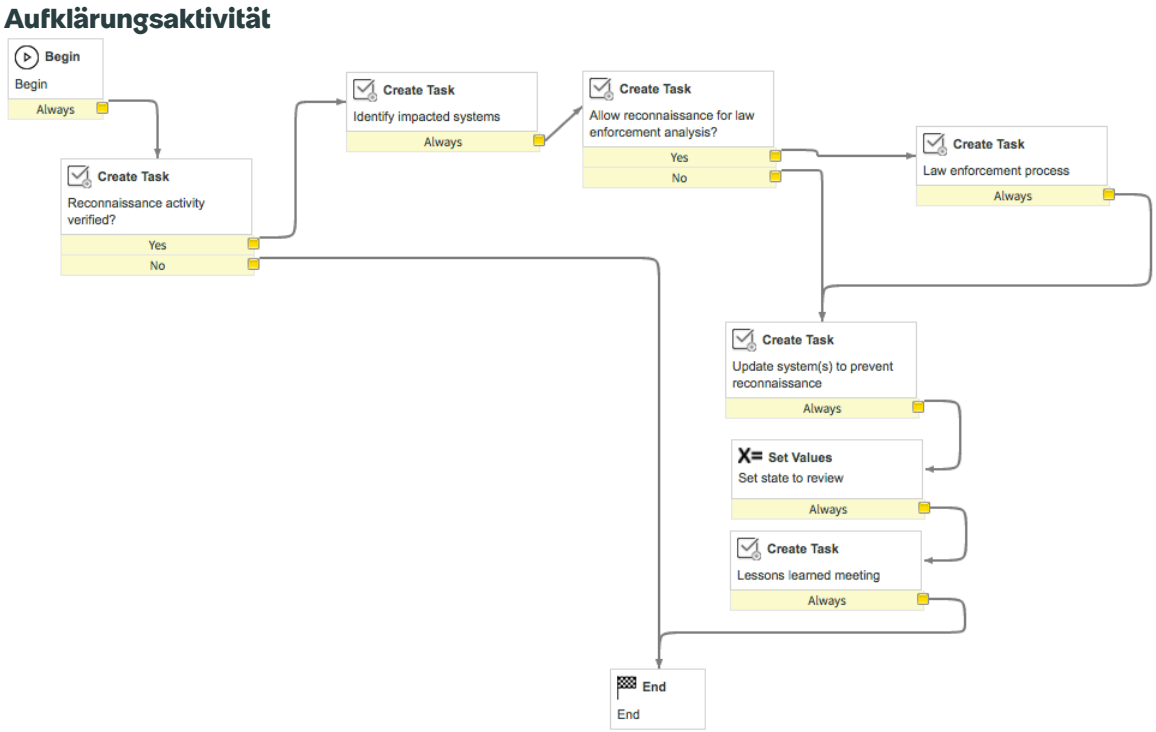
Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Aufklärungsaktivität** . Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Aufklärungsaktivität** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Workflow beendet wird

Antwortaufgaben in Reconnaissance-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Aufklärungsaktivität verifiziert?	Bestimmen Sie, ob eine beobachtete Aufklärung verifiziert wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Identifizieren Sie betroffene Systeme** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , Der Flow endet.
Identifizieren Sie betroffene Systeme	Bestimmen Sie die von der Aufklärung betroffenen Systeme.	Wenn diese Aufgabe abgeschlossen ist, wird **Aufklärung für Analysen der Strafverfolgung zulassen?** Aufgabe wird ausgeführt.
Aufklärung für Analysen der Strafverfolgung zulassen?	Legen Sie fest, ob die Aufklärung von Strafverfolgungsbehörden analysiert werden soll.	Wenn Sie auswählen **Ja** , **Strafverfolgungsprozess** Aufgabe wird ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Nein** , **Aktualisieren Sie System(e), um Aufklärungen zu verhindern** Aufgabe wird ausgeführt.
Strafverfolgungsprozess	Führen Sie den von Ihrem Unternehmen definierten Strafverfolgungsprozess durch.	Wenn diese Aufgabe abgeschlossen ist, wird **Aktualisieren Sie System(e), um Aufklärungen zu verhindern** Aufgabe wird ausgeführt.
Aktualisieren Sie System(e), um Aufklärungen zu verhindern	Führen Sie die erforderlichen Schritte aus, um die von der Aufklärung betroffenen Systeme zu aktualisieren.	Wenn diese Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** , Und **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Erkundungs-Incident ausgeführte Arbeit zu selektieren. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn diese Aufgabe abgeschlossen ist, endet der Flow.

Vorlage für Security Incident Rogue-Server oder Service-Workflow

Mit der Vorlage „Security Incident – Rogue-Server“ oder „Service – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, die für die Verarbeitung von Aktivitäten von nicht autorisierten Servern oder Services konzipiert sind, die sich auf Ihr Netzwerk auswirken.

Vorbereitungen

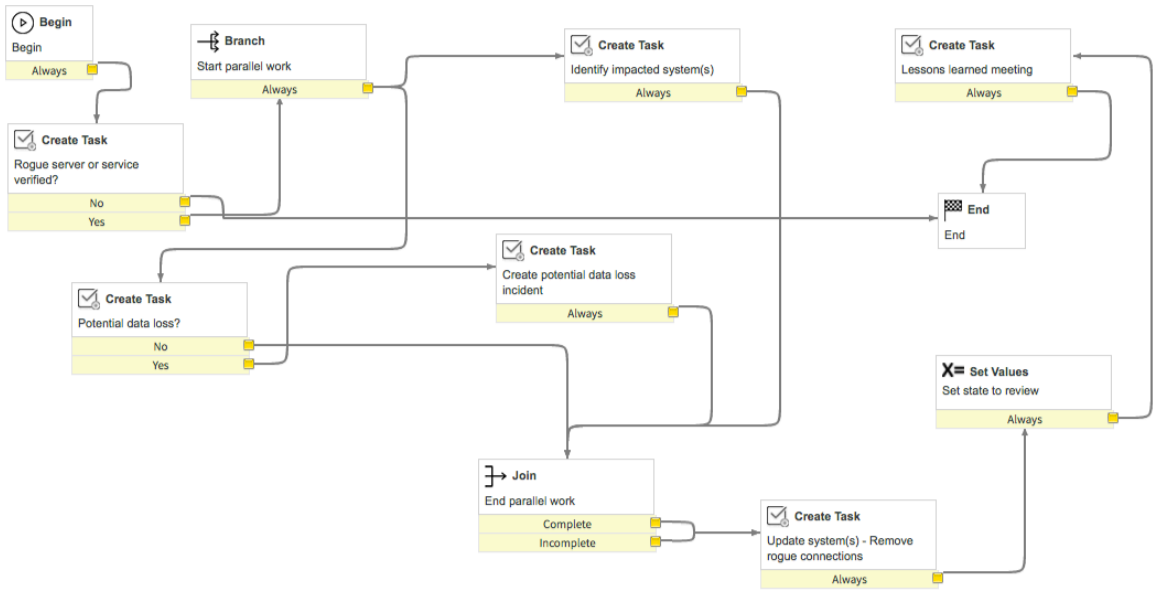
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Nicht autorisierter Server oder Service** . Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nicht autorisierter Server oder Service



Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Nicht autorisierte Server- oder Serviceaktivität** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Workflow beendet wird

Antwortaufgaben in Rogue-Server oder Servicevorlage

Antwortaufgabe	Aktion	Ergebnisse
Nicht autorisierter Server oder Service verifiziert?	Bestimmen Sie, ob eine Verbindung mit einem nicht autorisierten Server oder Service in Ihrem Netzwerk verifiziert wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , Die folgenden zwei Aufgaben werden parallel ausgeführt: ○ **Betroffene Systeme identifizieren** ○ **Potenzieller Datenverlust?** Wenn Sie auswählen **Nein** , Der Flow endet.
Betroffene Systeme identifizieren	Bestimmen Sie die Systeme, die vom Kontakt mit dem nicht autorisierten Server oder Service betroffen sind.	Wenn diese Aufgabe abgeschlossen ist, wird **System(e) aktualisieren – Entfernen Sie nicht autorisierte Verbindungen** Aufgabe wird ausgeführt.
Potenzieller Datenverlust?	Bestimmen Sie, ob die Verbindung mit dem nicht autorisierten Server oder Service zu einem potenziellen Datenverlust geführt hat.	Wenn Sie auswählen **Ja** , **Erstellen Sie einen Incident für potenziellen Datenverlust** Aufgabe wird ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Nein** , **System(e) aktualisieren – Entfernen Sie nicht autorisierte Verbindungen** Aufgabe wird ausgeführt.
Erstellen Sie einen Incident für potenziellen Datenverlust	Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den potenziellen Datenverlust zu erstellen.	Wenn diese Aufgabe abgeschlossen ist, wird **System(e) aktualisieren – Entfernen Sie nicht autorisierte Verbindungen** Aufgabe wird ausgeführt.
System(e) aktualisieren – Entfernen Sie nicht autorisierte Verbindungen	Führen Sie die erforderlichen Schritte aus, um die nicht autorisierten Verbindungen zu entfernen.	Wenn diese Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** , Und **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen nicht autorisierten Server oder Service-Incident ausgeführte Arbeit zu selektieren. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn diese Aufgabe abgeschlossen ist, endet der Flow.

Vorlage für Spam-Workflow für Security Incidents

Mit Security Incident – Spam – Vorlage können Sie eine Reihe von Aufgaben ausführen, die für die Verarbeitung von E-Mail-Spam in Ihrem Netzwerk konzipiert sind.

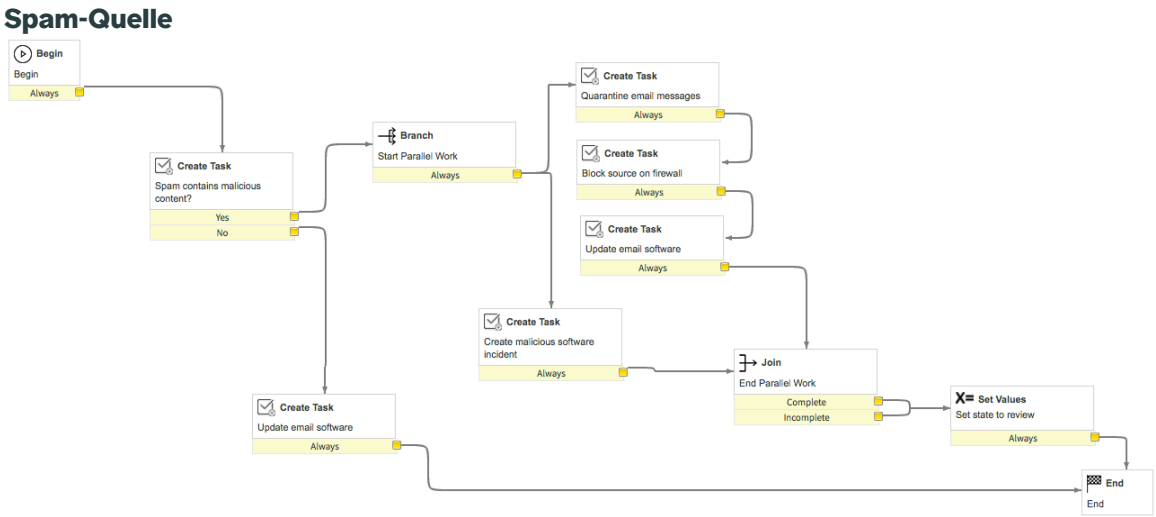
Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn **Kategorie** In wird ein Security Incident festgelegt oder in geändert **Spam-Quelle** . Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Prozedur

1. Öffnen Sie den Security Incident, für den Sie E-Mail-Spam verarbeiten möchten, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Spam-Quelle** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Workflow beendet wird

Antwortaufgaben in Spam-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Spam enthält schädliche Inhalte?	Ermitteln Sie, ob der Spam schädliche Software enthält. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie ausgewählt haben **Ja** , Die folgenden Antwortaufgaben werden ausgeführt: ○ **E-Mail-Nachricht in Quarantäne stellen** ○ **Erstellen Sie einen Incident für schädliche Software** Wenn Sie ausgewählt haben **Nein** , **Aktualisieren Sie die E-Mail-Software** Wird ausgeführt.
Erstellen Sie einen Incident für schädliche Software	Führen Sie die Schritte aus, um einen Security Incident zu erstellen und zu aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Diese Antwortaufgabe wartet, bis die nächsten drei Antwortaufgaben abgeschlossen sind. Der Status des Security Incidents, der dann in übergeht **Überprüfen** .
E-Mail-Nachricht in Quarantäne stellen	Führen Sie die Schritte aus, um den Spam unter Quarantäne zu stellen und zu aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
Quelle in Firewall blockieren	Führen Sie die Schritte aus, um die E-Mail-Adresse in der Firewall zu blockieren, indem Sie aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Aktualisieren Sie die E-Mail-Software	Fügen Sie Ihrer Sperrliste die E-Mail-Adresse hinzu, und aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt. **Hinweis:** Diese Antwortaufgabe wird auch ausgeführt, wenn Sie geantwortet haben **Nein** Zu **Spam enthält schädliche Inhalte?** Antwortaufgabe.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** .

Workflow-Vorlage für Security Incident – nicht autorisierter Zugriff

Mit der Vorlage „Security Incident – nicht autorisierter Zugriff –“ können Sie eine Reihe von Aufgaben ausführen, die für den Umgang mit nicht autorisiertem Zugriff auf Ihr Netzwerk konzipiert sind.

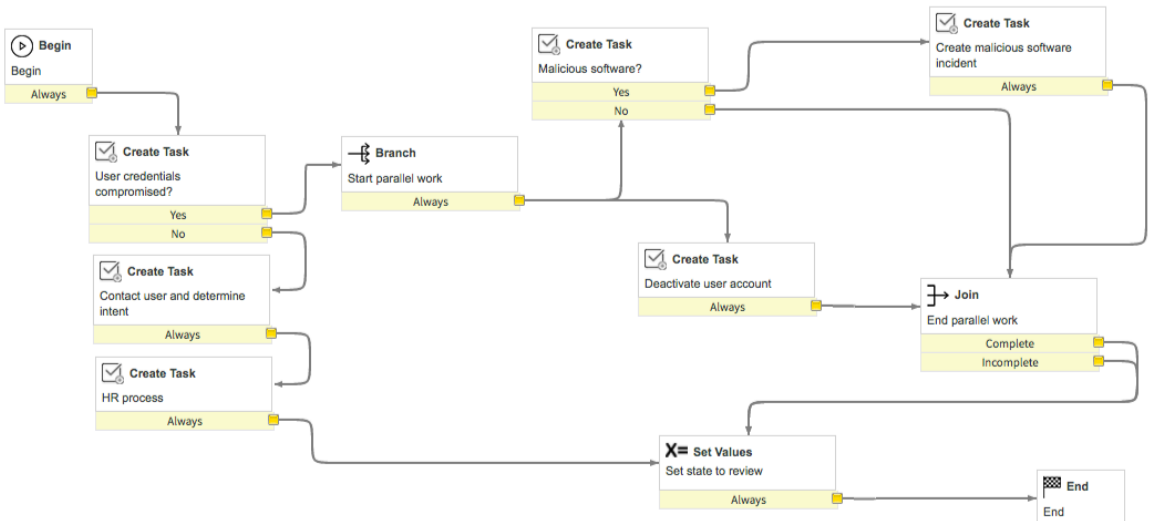
Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Nicht autorisierter Zugriff** . Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

Nicht autorisierter Zugriff



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Nicht autorisierter Zugriff** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Workflow beendet wird

Antwortaufgaben in Vorlage für nicht autorisierten Zugriff

Antwortaufgabe	Aktion	Ergebnisse
Anwenderanmeldeinformationen gefährdet?	Bestimmen Sie, ob Anwenderanmeldeinformationen gefährdet wurden. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , Die folgenden zwei Aufgaben werden parallel ausgeführt: ○ **Schädliche Software?** ○ **Anwender-Account deaktivieren** Wenn Sie auswählen **Nein** , **Wenden Sie sich an den Anwender, und bestimmen Sie die Absicht** Aufgabe wird ausgeführt.
Schädliche Software?	Ermitteln Sie, ob der nicht autorisierte Zugriff zur Einführung schädlicher Software geführt hat. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Erstellen Sie einen Incident für schädliche Software** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Erstellen Sie einen Incident für schädliche Software	Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den nicht autorisierten Zugriff zu erstellen.	Wenn diese Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Anwender-Account deaktivieren	Führen Sie die erforderlichen Schritte aus, um den Account des gefährdeten Anwenders zu deaktivieren.	Wenn diese Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
Wenden Sie sich an den Anwender, und bestimmen Sie die Absicht	Führen Sie die erforderlichen Schritte aus, um den Anwender zu kontaktieren, der für den nicht autorisierten Zugriff verantwortlich ist, und den Grund für den Zugriffsversuch zu bestimmen.	Wenn diese Aufgabe abgeschlossen ist, wird **HR-Prozess** Aufgabe wird ausgeführt.
HR-Prozess	Führen Sie die erforderlichen Schritte aus, um sich an die Personalabteilung zu wenden, um bei Bedarf Disziplinarmaßnahmen zu implementieren.	Wenn diese Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen" fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen" fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** , Und der Flow endet.

Workflow-Vorlage für Security Incident Web/BBS Defacement

Mit der Vorlage „Security Incident – Web/BBS Defacement –" können Sie eine Reihe von Aufgaben ausführen, die zur Behandlung von Vandalismus gegen eine der BBS- oder Websites Ihrer Organisation gedacht sind.

Vorbereitungen

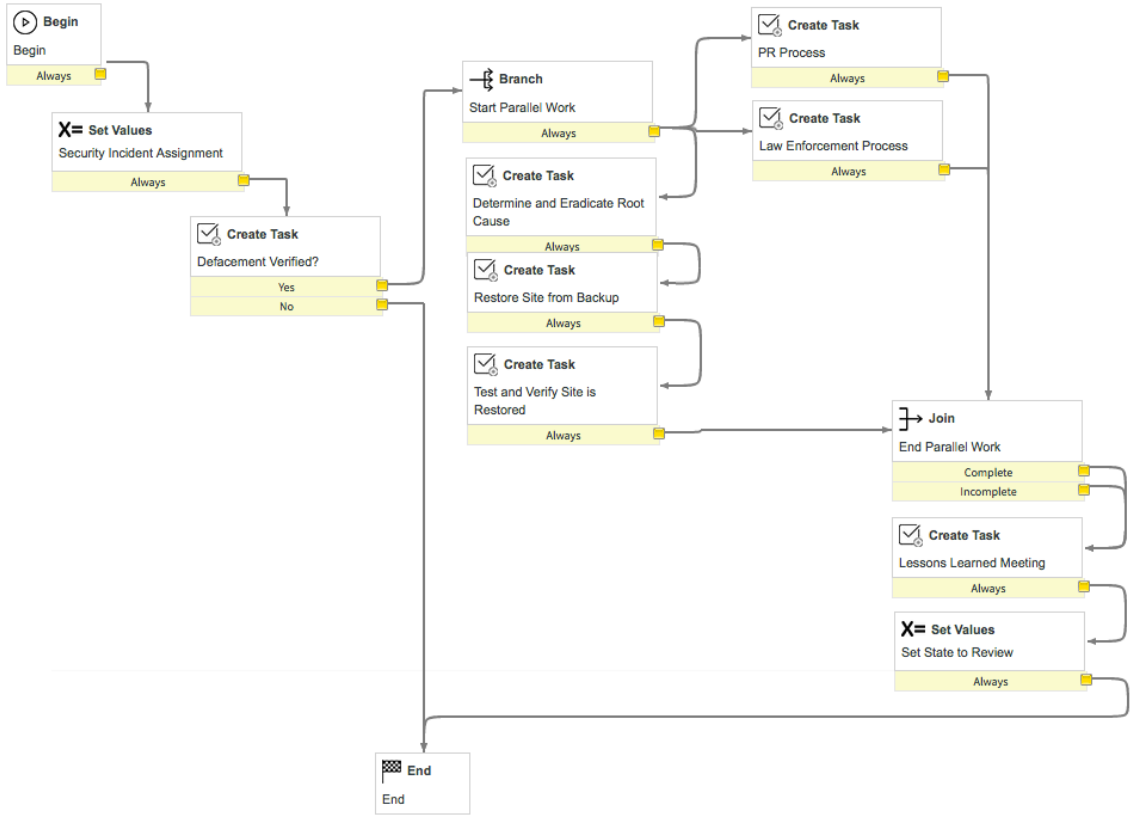
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Der Workflow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Web-/BBS-Defaktionierung** . Mit dieser Aktion wird eine Antwortaufgabe für die erste Aktivität im Workflow erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unleserlichmachen von Web/BBS



Prozedur

1. Öffnen Sie den Security Incident für dieses Vorkommen von Web- oder BBS-Defektierung, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Web-/BBS-Defaktionierung** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Workflow beendet wird

Antwortaufgaben in der Web-/BBS-Abwehrvorlage

Antwortaufgabe	Aktion	Ergebnisse
Security Incident-Zuweisung	Erstellen Sie einen Security Incident für jeden gemeldeten Incident von Website- oder BBS-Defaktionierung.	Die nächste Antwortaufgabe wird ausgeführt.
Defektivierung verifiziert?	Ermitteln Sie, ob die Website oder BBS tatsächlich entschlüsselt wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , Die folgenden Antwortaufgaben werden ausgeführt: ○ **PR-Prozess** ○ **Strafverfolgungsprozess** ○ **Ursache bestimmen und beseitigen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		Wenn Sie auswählen **Nein** , Der Flow endet.
PR-Prozess	Führen Sie die erforderlichen Schritte aus, um die Öffentlichkeit darüber zu informieren, dass die Website oder BBS beschädigt wurde. Wenn Sie mit dem PR-Prozess fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	Die **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
Strafverfolgungsprozess	Führen Sie die erforderlichen Schritte aus, um die entsprechenden Strafverfolgungsbehörden bezüglich des Angriffs zu kontaktieren. Wenn Sie fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	Die **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
Ursache bestimmen und beseitigen	Führen Sie die erforderlichen Schritte aus, um die Ursache der Defaktion zu erkennen und zu beseitigen. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Stellen Sie den Standort aus der Sicherung wieder her	Führen Sie die erforderlichen Schritte aus, um die Website oder BBS zu sichern und wiederherzustellen. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Testen und überprüfen Sie, ob der Standort wiederhergestellt ist	Überprüfen Sie, ob die Site wiederhergestellt ist. Wenn Sie fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	Die **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Website-/BBS-Defaktions-Incident ausgeführte Arbeit zu selektieren. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** . Der Flow endet.

Flow-Vorlagen für Security Incident Response

Die Security Incident Response Das Basissystem enthält eine Reihe von Workflow-Vorlagen, die mit Flow Designer erstellt wurden und mit Security Incident-Datensätzen arbeiten.

Nur Anwender mit der Rolle „sn_sec_cmn.admin“ können Security Operations-Workflow-Vorlagen hinzufügen oder bearbeiten, und Anwender mit der Rolle „sn_si_admin“ sind zum Aktualisieren der Flow-Vorlagen erforderlich.

Wichtige Aktivierungsinformationen

Die mit dem Workflow-Editor erstellten Workflow-Vorlagen und die mit dem Flow Designer erstellten Flow-Vorlagen sind standardmäßig deaktiviert. Die Workflow-Vorlagen können mit aktiviert werden Workflow-Auslöser . Flow Designer-Vorlagen können mit Flow Designer aktiviert werden.

Hinweis:
Sie müssen darauf achten, nicht die gleiche Vorlage jedes Typs zu aktivieren. Vermeiden Sie beispielsweise die Aktivierung von Workflow-Vorlage für Security Incident – Gefährdung vertraulicher Daten Und Flow-Vorlage für Security Incident – Offenlegung vertraulicher Daten. Dies kann zur Ausführung des Workflows und des Flows sowie zur Erstellung doppelter Informationen führen.

Flow-Vorlage für Security Incident – Offenlegung vertraulicher Daten

Mit der Vorlage „Security Incident – Offenlegung vertraulicher Daten“ können Sie eine Reihe von Aufgaben ausführen, die für den Umgang mit der Offenlegung vertraulicher Daten konzipiert sind.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird ausgelöst, wenn **Kategorie** In wird ein Security Incident festgelegt oder in geändert **Offenlegung vertraulicher persönlicher Identitätsdaten** .

Prozedur

1. Öffnen Sie den Security Incident, für den Sie das Risiko vertraulicher Daten behandeln möchten, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Offenlegung vertraulicher persönlicher Identitätsdaten** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe ausgeführt oder der Flow beendet wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgaben in Vorlage für Offenlegung vertraulicher Daten

Antwortaufgabe	Beschreibung	Ergebnisse
Sind die Daten vertraulich?	Bestimmen Sie, ob die mit diesem Security Incident verknüpften Daten vertraulich oder vertraulich sind. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie ausgewählt haben **Ja** , Die nächste Antwortaufgabe wird ausgeführt. Wenn Sie ausgewählt haben **Nein** , Der Flow endet.
Ursache ermitteln und Ausgänge verhindern	Bestimmen Sie die Ursache des Angriffs, und fügen Sie Ausgangsfilterung hinzu, um die Extraktion zu stoppen, und aktualisieren Sie den **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Eliminieren Sie das Risiko im Zusammenhang mit der Ursache	Führen Sie basierend auf der Ursache die Schritte aus, um das Risiko zu beseitigen, indem Sie aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Quarantäne von Restartefakten	Führen Sie die Schritte aus, um Restripartefakte unter Quarantäne zu stellen, indem Sie aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Rechtlicher Prozess	Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen, indem Sie aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
PR-Prozess	Führen Sie die Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen, indem Sie aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** .
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die an diesen sensiblen Daten ausgeführte Arbeit zu selektieren und zu aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Der Security Incident verbleibt im **Überprüfen** geben sie an, bis Sie sie schließen.

Flow-Vorlage für Security Incident-Denial of Service

Mit der Vorlage „Security Incident – Denial of Service“ können Sie eine Reihe von Aufgaben ausführen, die für die Behandlung von Denial of Service-Angriffen (DOS) konzipiert sind.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Denial of Service** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie den Security Incident für dieses Denial-of-Service-Ereignis, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Denial of Service** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Workflow beendet wird

Antwortaufgaben in Denial of Service-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Ist das Ziel geschäftskritisch?	Bestimmen Sie, ob das Ziel dieses DOS-Angriffs geschäftskritisch ist. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Legen Sie die Priorität auf „Kritisch“ fest** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt.
Legen Sie die Priorität auf „Kritisch“ fest	Keine Aktion erforderlich.	Die **Priorität** Des Security Incidents wird automatisch in geändert **Kritisch** , Und **Wird eine Schwachstelle ausgenutzt?** Aufgabe wird ausgeführt.
Wird eine Schwachstelle ausgenutzt?	Bestimmen Sie, ob dieser DOS-Angriff eine Software-Schwachstelle ausnutzt. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Notfall-Patch-Anforderung** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Interner Angreifer?** Aufgabe wird ausgeführt.
Notfall-Patch-Anforderung	Stellen Sie eine Notfall-Patch-Anforderung für die angegriffenen Systeme aus. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Interner Angreifer?	Bestimmen Sie, ob die Quelle dieses DOS-Angriffs in Ihrer Organisation liegt. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Angreifende Hosts isolieren** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Benachrichtigen Sie DOS-Schutzanbieter und/oder ISP** Aufgabe wird ausgeführt.
Angreifende Hosts isolieren	Führen Sie die erforderlichen Schritte aus, um die internen Hosts zu isolieren, die für den Angriff verantwortlich sind.	Nachdem Sie diesen Schritt abgeschlossen haben **Validiert die Systemintegrität der**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	**angegriffenen Systeme** Aufgabe wird ausgeführt.
Benachrichtigen Sie DOS-Schutzanbieter und/oder ISP	Führen Sie die erforderlichen Schritte aus, um sich an Ihren Denial-of-Service-Schutzanbieter und/oder Ihren Internetdienstanbieter zu wenden, um sie über den Angriff zu benachrichtigen. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Validiert die Systemintegrität der angegriffenen Systeme	Führen Sie die erforderlichen Schritte aus, um die Integrität der angegriffenen Computer zu bewerten und zu validieren. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Überprüfen Sie die DOS-Schutzmaßnahmen	Überprüfen Sie Ihre vorhandenen DOS-Schutzmaßnahmen und -Verfahren. Führen Sie alle erforderlichen Änderungen durch. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** . Die **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Denial-of-Service-Incident ausgeführte Arbeit zu selektieren. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Der Flow endet.

Flow-Vorlage für Security Incident – verlorene Geräte

Mit der Vorlage „Security Incident – verlorene Geräte –“ können Sie eine Reihe von Aufgaben ausführen, die für den Umgang mit verlorenen Geräten konzipiert sind.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Geräteverlust** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie den Security Incident für dieses Denial-of-Service-Ereignis, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Geräteverlust** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

Antwortaufgaben in Vorlage für verlorene Ausrüstung

Antwortaufgabe	Aktion	Ergebnisse
Enthielt das Gerät vertrauliche Daten?	Bestimmen Sie, ob die diesem Security Incident zugeordneten Geräte vertrauliche oder vertrauliche Informationen enthielten. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** Entsprechend.	Wenn Sie auswählen **Ja** Die **Wurden die Daten verschlüsselt?** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , Der Flow endet.
Wurden die Daten verschlüsselt?	Bestimmen Sie, ob die vertraulichen Daten auf dem verlorenen Gerät verschlüsselt wurden. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** Entsprechend.	Wenn Sie auswählen **Ja** , **Remote-Löschung erstellt?** Antwortaufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Erstellen Sie einen Incident für potenziellen Datenverlust** Antwortaufgabe wird ausgeführt.
Erstellen Sie einen Incident für potenziellen Datenverlust	Führen Sie die erforderlichen Schritte aus, um einen Incident für potenziellen Datenverlust zu erstellen. Nachdem Sie fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	Die **Remote-Löschung erstellt?** Antwortaufgabe wird ausgeführt.
Remote-Löschung erstellt?	Führen Sie die erforderlichen Schritte aus, um eine Remote-Löschung der verlorenen Geräte auszuführen. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** Entsprechend.	Die **Rechtlicher Prozess: Offenlegung erforderlich** Aufgabe wird ausgeführt.
Rechtlicher Prozess – Offenlegung erforderlich?	Führen Sie die Schritte aus, um die rechtlichen Anforderungen dieser Analyse zu erfüllen.	Die **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
	Wählen Sie Aus **Ja** Wenn eine rechtliche Offenlegung erforderlich ist, **Nein** Wenn nicht.	
PR-Prozess	Führen Sie die erforderlichen Schritte aus, um die PR-Anforderungen dieser Analyse zu erfüllen. Nachdem Sie fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	Die **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Es ist keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** .
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Incident für verlorene Geräte ausgeführte Arbeit zu selektieren. Nachdem Sie fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	Der Flow endet.

Flow-Vorlage für Security Incident böswillige Software

Mit der Vorlage „Security Incident – schädliche Software –“ können Sie eine Reihe von Aufgaben ausführen, die für den Umgang mit schädlicher Software in Ihrem Netzwerk konzipiert sind.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Schädliche Codeaktivität** .

Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Schädliche Codeaktivität** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgaben in Vorlage für schädliche Software

Antwortaufgabe	Aktion	Ergebnisse
Scan-Endpunkt – Malware Gefunden?	Ermitteln Sie nach dem Ausführen eines Scans, ob Malware gefunden wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Malware Entfernen – Erfolg?** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , Der Flow endet.
Malware Entfernen – Erfolg?	Bestimmen Sie, ob die Malware erfolgreich entfernt wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Gab es einen größeren Verstoß?** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Löschen Und Neu Erstellen** Aufgabe wird ausgeführt.
Löschen Und Neu Erstellen	Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie in dieser Aufgabe angewiesen, auf den mit der Malware infizierten Computern ein Wischvorgang durchzuführen.	Nachdem die Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Gab es einen größeren Verstoß?	Ermitteln Sie, ob der durch die schädliche Software verursachte Verstoß größer ist als zuerst angenommen. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , Die folgenden Aufgaben werden parallel ausgeführt: ○ Rechtliche Überprüfung ○ HR-Überprüfung ○ Überprüfung Durch Strafverfolgungsbehörden Wenn Sie auswählen **Nein** , Der Flow endet.
Rechtliche Überprüfung HR-Überprüfung Überprüfung Durch Strafverfolgungsbehörden	Führen Sie die Schritte aus, die für jede dieser Abteilungen erforderlich sind, um den Prozess zu überprüfen, den Sie zur Beseitigung der schädlichen Software befolgt haben.	Wenn die Aufgaben abgeschlossen sind, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** , Und der Flow endet.

Vorlage für Security Incident-Phishing-Flow

Mit der Vorlage „Security Incident – Phishing –“ können Sie eine Reihe von Aufgaben ausführen, die für die Verarbeitung von Spear-Phishing-E-Mails in Ihrem Netzwerk konzipiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Spear-Phishing** .

Prozedur
1. Öffnen Sie den Security Incident für diesen potenziellen Spear-Phishing-Angriff, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Spear-Phishing** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

Antwortaufgaben in Spear Phishing-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Handelt es sich um einen Phishing-Angriff?	Ermitteln Sie, ob es sich um einen Phishing-Angriff handelt. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , Die folgenden Aufgaben werden parallel ausgeführt: ○ Scan-Endpunkt – Malware Gefunden? ○ E-Mail-Schutzsoftware Aktualisieren ○ Ungelesene Phishing-E-Mail in Warteschlange entfernen – für alle Anwender Wenn Sie auswählen **Nein** , Der Flow endet.
Scan-Endpunkt – Malware Gefunden?	Ermitteln Sie nach dem Ausführen eines Scans, ob Malware gefunden wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Malware Entfernen – Erfolg?** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Malware Entfernen – Erfolg?	Bestimmen Sie, ob die Malware erfolgreich entfernt wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Löschen und neu**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		erstellen Aufgabe wird ausgeführt.
Löschen und neu erstellen	Wenn Sie die gefundene Malware nicht erfolgreich entfernt haben, werden Sie in dieser Aufgabe angewiesen, auf den mit der Malware infizierten Computern ein Wischvorgang durchzuführen.	Nachdem die Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
E-Mail-Schutzsoftware Aktualisieren	Wenn festgestellt wurde, dass es sich um einen Phishing-Angriff handelt, werden Sie aufgefordert, Ihre E-Mail-Schutzsoftware entsprechend zu aktualisieren.	Wenn die Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Ungelesene Phishing-E-Mail in Warteschlange entfernen – für alle Anwender	Führen Sie die erforderlichen Schritte aus, um die Phishing-E-Mail zu entfernen, die sich für alle Ihre Anwender noch in der Warteschlange befindet.	Wenn die Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** . Die **Planen Sie Eine Schulung Zum Sicherheitsbewusstsein** Aufgabe wird ausgeführt.
Planen Sie Eine Schulung Zum Sicherheitsbewusstsein	Planen Sie Schulungen, um das Sicherheitsbewusstsein Ihrer Mitarbeiter zu erhöhen. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn die Aufgabe abgeschlossen ist, endet der Flow.

Flow-Vorlage für Security Incident-Richtlinienverstoß

Mit der Vorlage „Security Incident – Richtlinienverstoß –“ können Sie eine Reihe von Aufgaben ausführen, die für die Behandlung von Verstößen gegen Sicherheitsrichtlinien konzipiert sind.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Richtlinienverstoß** .

Prozedur

1. Öffnen Sie den Security Incident für den Richtlinienverstoß, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Richtlinienverstoß** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

Antwortaufgaben in Richtlinienverstoßvorlage

Antwortaufgabe	Aktion	Ergebnisse
Verstoß klassifizieren	Klassifizieren Sie, wie dieser Verstoß gegen die Sicherheitsrichtlinien Ihrer Organisation verstößt. Aktualisieren Sie **Status** Feld in der Aufgabe, nachdem Sie sie abgeschlossen haben.	Die **Benachrichtigen Sie den Verstoßer über den Verstoß** Antwortaufgabe wird ausgeführt.
Benachrichtigen Sie den Verstoßer über den Verstoß	Teilen Sie dem Verstoßgegner die Art des Verstoßes mit. Aktualisieren Sie **Status** Feld in der Aufgabe, nachdem Sie sie kommuniziert haben.	Die **Holen Sie eine Bestätigung vom Verstoßer ein** Antwortaufgabe wird ausgeführt.
Holen Sie eine Bestätigung vom Verstoßer ein	Holen Sie eine Bestätigung des Verstoßes vom Verstoss ein. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Die **HR-Prozess** Antwortaufgabe wird ausgeführt.
HR-Prozess	Teilen Sie HR alle erforderlichen Informationen zu diesem Verstoß mit. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Die **Legen Sie den Status auf „Überprüfen“ fest** Antwortaufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Es ist keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** .
Planen Sie eine Schulung zum Sicherheitsbewusstsein	Führen Sie eine Schulung zum Sicherheitsbewusstsein durch, um Mitarbeiter darin zu Schulen, wie ähnliche Sicherheitsverletzungen in Zukunft verhindert werden können. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Der Flow endet.

Vorlage für Security Incident Reconnaissance-Flow

Die Aufklärung ist normalerweise ein erster Schritt in Richtung eines weiteren Angriffs, bei dem ein Gerät oder System ausgenutzt werden soll. Mit der Vorlage „Security Incident – Reconnaissance –“ können Sie eine Reihe von Aufgaben ausführen, die für die Durchführung von Aufklärungen in Ihrem Netzwerk konzipiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Aufklärungsaktivität** .

Prozedur
1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Aufklärungsaktivität** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

Antwortaufgaben in Reconnaissance-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Aufklärungsaktivität verifiziert?	Bestimmen Sie, ob eine beobachtete Aufklärung verifiziert wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Identifizieren Sie betroffene Systeme** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , Der Flow endet.
Identifizieren Sie betroffene Systeme	Bestimmen Sie die von der Aufklärung betroffenen Systeme.	Wenn diese Aufgabe abgeschlossen ist, wird **Aufklärung für Analysen der Strafverfolgung zulassen?** Aufgabe wird ausgeführt.
Aufklärung für Analysen der Strafverfolgung zulassen?	Legen Sie fest, ob die Aufklärung von Strafverfolgungsbehörden analysiert werden soll. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Strafverfolgungsprozess** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Aktualisieren Sie System(e), um Aufklärungen zu verhindern** Aufgabe wird ausgeführt.
Strafverfolgungsprozess	Führen Sie den von Ihrem Unternehmen definierten Strafverfolgungsprozess durch.	Wenn diese Aufgabe abgeschlossen ist, wird **Aktualisieren Sie System(e), um Aufklärungen zu verhindern** Aufgabe wird ausgeführt.
Aktualisieren Sie System(e), um Aufklärungen zu verhindern	Führen Sie die erforderlichen Schritte aus, um die von der Aufklärung betroffenen Systeme zu aktualisieren.	Wenn diese Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		, Und **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Erkundungs-Incident ausgeführte Arbeit zu selektieren. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn diese Aufgabe abgeschlossen ist, endet der Flow.

Vorlage für Security Incident Rogue-Server oder Service-Flow

Mit der Vorlage „Security Incident – Rogue-Server“ oder „Service – Vorlage“ können Sie eine Reihe von Aufgaben ausführen, die für die Verarbeitung von Aktivitäten von nicht autorisierten Servern oder Services konzipiert sind, die sich auf Ihr Netzwerk auswirken.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Nicht autorisierter Server oder Service** .

Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Nicht autorisierte Server- oder Serviceaktivität** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

Antwortaufgaben in Rogue-Server oder Servicevorlage

Antwortaufgabe	Aktion	Ergebnisse
Nicht autorisierter Server oder Service verifiziert?	Bestimmen Sie, ob eine Verbindung mit einem nicht autorisierten Server oder Service in Ihrem Netzwerk verifiziert wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , Die folgenden zwei Aufgaben werden parallel ausgeführt: ○ **Betroffene Systeme identifizieren** ○ **Potenzieller Datenverlust?** Wenn Sie auswählen **Nein** , Der Flow endet.
Betroffene Systeme identifizieren	Bestimmen Sie die Systeme, die vom Kontakt mit dem nicht autorisierten Server oder Service betroffen sind.	Wenn diese Aufgabe abgeschlossen ist, wird **System(e) aktualisieren – Entfernen Sie nicht autorisierte**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
		Verbindungen Aufgabe wird ausgeführt.
Potenzieller Datenverlust?	Bestimmen Sie, ob die Verbindung mit dem nicht autorisierten Server oder Service zu einem potenziellen Datenverlust geführt hat. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Erstellen Sie einen Incident für potenziellen Datenverlust** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **System(e) aktualisieren – Entfernen Sie nicht autorisierte Verbindungen** Aufgabe wird ausgeführt.
Erstellen Sie einen Incident für potenziellen Datenverlust	Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den potenziellen Datenverlust zu erstellen.	Wenn diese Aufgabe abgeschlossen ist, wird **System(e) aktualisieren – Entfernen Sie nicht autorisierte Verbindungen** Aufgabe wird ausgeführt.
System(e) aktualisieren – Entfernen Sie nicht autorisierte Verbindungen	Führen Sie die erforderlichen Schritte aus, um die nicht autorisierten Verbindungen zu entfernen.	Wenn diese Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** , Und **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen nicht autorisierten Server oder Service-Incident ausgeführte Arbeit zu selektieren. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn diese Aufgabe abgeschlossen ist, endet der Flow.

Vorlage für Security Incident-Spam-Flow

Mit Security Incident – Spam – Vorlage können Sie eine Reihe von Aufgaben ausführen, die für die Verarbeitung von E-Mail-Spam in Ihrem Netzwerk konzipiert sind.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn **Kategorie** In wird ein Security Incident festgelegt oder in geändert **Spam-Quelle** .

Prozedur

1. Öffnen Sie den Security Incident, für den Sie E-Mail-Spam verarbeiten möchten, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Spam-Quelle** .
3. Speichern Sie den Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

Antwortaufgaben in Spam-Vorlage

Antwortaufgabe	Aktion	Ergebnisse
Spam enthält schädliche Inhalte?	Ermitteln Sie, ob der Spam schädliche Software enthält. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie ausgewählt haben **Ja** , Die folgenden Antwortaufgaben werden ausgeführt: ○ **E-Mail-Nachricht in Quarantäne stellen** ○ **Erstellen Sie einen Incident für schädliche Software** Wenn Sie ausgewählt haben **Nein** , **Aktualisieren Sie die E-Mail-Software** Wird ausgeführt.
Erstellen Sie einen Incident für schädliche Software	Führen Sie die Schritte aus, um einen Security Incident zu erstellen und zu aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Diese Antwortaufgabe wartet, bis die nächsten drei Antwortaufgaben abgeschlossen sind. Der Status des Security Incidents, der dann in übergeht **Überprüfen** .
E-Mail-Nachricht in Quarantäne stellen	Führen Sie die Schritte aus, um den Spam unter Quarantäne zu stellen und zu aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Quelle in Firewall blockieren	Führen Sie die Schritte aus, um die E-Mail-Adresse in der Firewall zu blockieren, indem Sie aktualisieren **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Aktualisieren Sie die E-Mail-Software	Fügen Sie Ihrer Sperrliste die E-Mail-Adresse hinzu, und aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt. **Hinweis:** Diese Antwortaufgabe wird auch ausgeführt, wenn Sie geantwortet haben **Nein** Zu **Spam enthält schädliche Inhalte?** Antwortaufgabe.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flow-Vorlage für nicht autorisierten Security Incident-Zugriff

Mit der Vorlage „Security Incident – nicht autorisierter Zugriff –“ können Sie eine Reihe von Aufgaben ausführen, die für den Umgang mit nicht autorisiertem Zugriff auf Ihr Netzwerk konzipiert sind.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Nicht autorisierter Zugriff** .

Prozedur

1. Öffnen Sie den Security Incident für diesen potenziellen Angriff, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Nicht autorisierter Zugriff** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

Antwortaufgaben in Vorlage für nicht autorisierten Zugriff

Antwortaufgabe	Aktion	Ergebnisse
Anwenderanmeldeinformationen gefährdet?	Bestimmen Sie, ob Anwenderanmeldeinformationen gefährdet wurden. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , Die folgenden zwei Aufgaben werden parallel ausgeführt: ○ **Schädliche Software?** ○ **Anwender-Account deaktivieren** Wenn Sie auswählen **Nein** , **Wenden Sie sich an den Anwender, und bestimmen Sie die Absicht** Aufgabe wird ausgeführt.
Schädliche Software?	Ermitteln Sie, ob der nicht autorisierte Zugriff zur Einführung schädlicher Software geführt hat. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , **Erstellen Sie einen Incident für schädliche Software** Aufgabe wird ausgeführt. Wenn Sie auswählen **Nein** , **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgabe	Aktion	Ergebnisse
Erstellen Sie einen Incident für schädliche Software	Führen Sie die erforderlichen Schritte aus, um einen Security Incident für den nicht autorisierten Zugriff zu erstellen.	Wenn diese Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Anwender-Account deaktivieren	Führen Sie die erforderlichen Schritte aus, um den Account des gefährdeten Anwenders zu deaktivieren.	Wenn diese Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Wenden Sie sich an den Anwender, und bestimmen Sie die Absicht	Führen Sie die erforderlichen Schritte aus, um den Anwender zu kontaktieren, der für den nicht autorisierten Zugriff verantwortlich ist, und den Grund für den Zugriffsversuch zu bestimmen.	Wenn diese Aufgabe abgeschlossen ist, wird **HR-Prozess** Aufgabe wird ausgeführt.
HR-Prozess	Führen Sie die erforderlichen Schritte aus, um sich an die Personalabteilung zu wenden, um bei Bedarf Disziplinarmaßnahmen zu implementieren.	Wenn diese Aufgabe abgeschlossen ist, wird **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** , Und der Flow endet.

Vorlage für Security Incident Web/BBS Defacement-Flow

Mit der Vorlage „Security Incident – Web/BBS Defacement –“ können Sie eine Reihe von Aufgaben ausführen, die zur Behandlung von Vandalismus gegen eine der BBS- oder Websites Ihrer Organisation gedacht sind.

Vorbereitungen

Erforderliche Rolle: sn_si.write

Warum und wann dieser Vorgang ausgeführt wird

Dieser Flow wird ausgelöst, wenn **Kategorie** In einem Security Incident ist auf festgelegt **Web-/BBS-Defaktionierung** .

Prozedur

1. Öffnen Sie den Security Incident für dieses Vorkommen von Web- oder BBS-Defektierung, oder Erstellen Sie einen neuen Security Incident .
2. In **Kategorie** , Wählen Sie aus **Web-/BBS-Defaktionierung** .
3. Speichern Sie den Datensatz.
4. Scrollen Sie nach unten, und öffnen Sie **Antwortaufgaben** Zugehörige Liste.
   Die erste einer Reihe von Antwortaufgaben wird angezeigt. Jedes Mal, wenn der Datensatz gespeichert wird, bewirkt Ihre Antwort auf die vorherige Aufgabe, dass entweder die nächste Antwortaufgabe erstellt oder der Flow beendet wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortaufgaben in der Web-/BBS-Abwehrvorlage

Antwortaufgabe	Aktion	Ergebnisse
Security Incident-Zuweisung	Erstellen Sie einen Security Incident für jeden gemeldeten Incident von Website- oder BBS-Defaktionierung.	Die nächste Antwortaufgabe wird ausgeführt.
Defektivierung verifiziert?	Ermitteln Sie, ob die Website oder BBS tatsächlich entschlüsselt wurde. Wählen Sie in der Aufgabe aus **Ja** Oder **Nein** In **Ergebnis** .	Wenn Sie auswählen **Ja** , Die folgenden Antwortaufgaben werden ausgeführt: ○ **PR-Prozess** ○ **Strafverfolgungsprozess** ○ **Ursache bestimmen und beseitigen** Wenn Sie auswählen **Nein** , Der Flow endet.
PR-Prozess	Führen Sie die erforderlichen Schritte aus, um die Öffentlichkeit darüber zu informieren, dass die Website oder BBS beschädigt wurde. Wenn Sie mit dem PR-Prozess fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	Die **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
Strafverfolgungsprozess	Führen Sie die erforderlichen Schritte aus, um die entsprechenden Strafverfolgungsbehörden bezüglich des Angriffs zu kontaktieren. Wenn Sie fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	Die **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.
Ursache bestimmen und beseitigen	Führen Sie die erforderlichen Schritte aus, um die Ursache der Defaktion zu erkennen und zu beseitigen. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Stellen Sie den Standort aus der Sicherung wieder her	Führen Sie die erforderlichen Schritte aus, um die Website oder BBS zu sichern und wiederherzustellen. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in geändert haben **Abgeschlossen** Oder **Abgebrochen** , Die nächste Antwortaufgabe wird ausgeführt.
Testen und überprüfen Sie, ob der Standort wiederhergestellt ist	Überprüfen Sie, ob die Site wiederhergestellt ist.	Die **Besprechung mit gelernten Lektionen** Aufgabe wird ausgeführt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

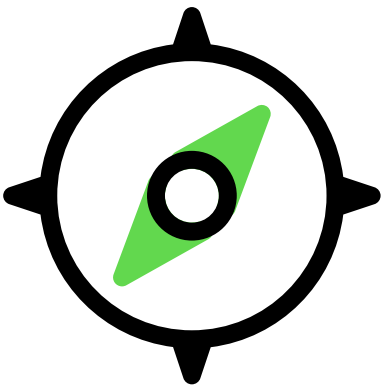
Antwortaufgabe	Aktion	Ergebnisse
	Wenn Sie fertig sind, legen Sie den Status der Aufgabe auf fest **Abgeschlossen** Oder **Unvollständig** Entsprechend.	
Besprechung mit gelernten Lektionen	Führen Sie ein Meeting mit gelernten Lektionen durch, um die für diesen Website-/BBS-Defaktions-Incident ausgeführte Arbeit zu selektieren. Aktualisieren Sie **Status** Feld in der Aufgabe entsprechend.	Wenn Sie den Status der Aufgabe in ändern **Abgeschlossen** Oder **Abgebrochen** , **Legen Sie den Status auf „Überprüfen“ fest** Aufgabe wird ausgeführt.
Legen Sie den Status auf „Überprüfen“ fest	Keine Aktion erforderlich.	Die **Status** Des Security Incidents wird automatisch in geändert **Überprüfen** . Der Flow endet.

Threat Intelligence

Die ServiceNow® Threat Intelligence Mit der Anwendung können Sie Indikatoren für Kompromittierung (IOC) finden und Security Incidents mit Threat Intelligence-Daten anreichern.

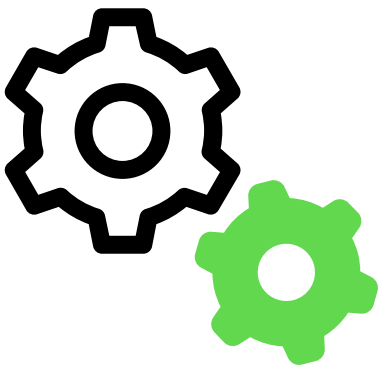
Erste Schritte

Untersuchen



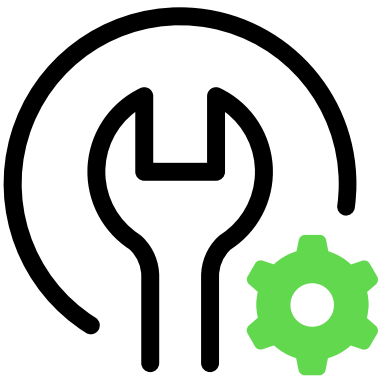
Erfahren Sie mehr über Threat Intelligence-Konzepte und ihre wichtigsten Funktionen.

Konfigurieren



Richten Sie ein, lernen Sie die installierten Komponenten und Anwenderrollen kennen, die erforderlich sind, um Ihre Geschäftsanforderungen zu erfüllen.

Verwalten

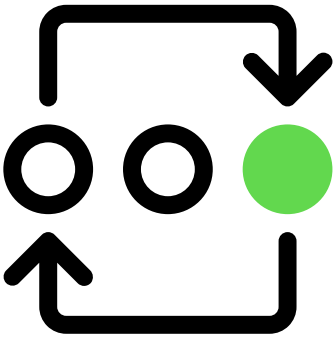


Legen Sie die Eigenschaften für die Anwendung „Threat Intelligence“ fest.

Automatische Übersetzung

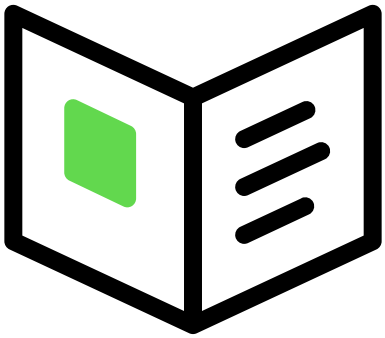
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrieren



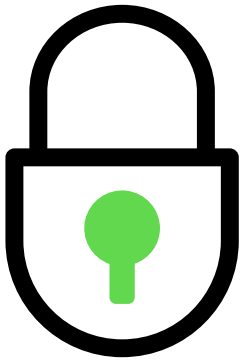
Erweitern Sie die Threat Intelligence-Fähigkeiten durch die Integration mit ServiceNow- und Drittanbieteranwendungen.

Verwenden



Verwalten Sie Indikatoren der Kompromittierung (IOC) und verschiedene Artefakte.

MITRE ATT&CK-Framework



MITRE-ATT&CK-Framework verwalten Identifizieren Sie schnell Bedrohungen und koordinieren Sie die Antworten auf Cyberangriffe.

Security Case Management

Verwalten Sie das Security Case Management, indem Sie Informationen zu verdächtigen Aktivitäten sammeln.

Lernressourcen

- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie Komponenten, die mit einer Anwendung installiert sind

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- Stellen Sie Fragen, und erkunden Sie andere Ressourcen für Threat Intelligence In ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support
- Security Operations-Ressourcenbibliothek
- Security Operations-Community

Threat Intelligence verstehen

Die Threat Intelligence Mit der Anwendung können Sie auf den strukturierten Bedrohungsinformationsausdruck Ihres Unternehmens zugreifen und einen Referenzpunkt bereitstellen (STIX ™) Daten. Enthalten in Threat Intelligence Ist Management von Sicherheitsfällen Anwendung, die eine Möglichkeit zur Analyse von Bedrohungen für Ihre Organisation bietet, die durch gezielte Kampagnen oder Statusakteure verursacht werden.

STIX ist eine Sprache für die standardisierte und strukturierte Beschreibung von Informationen zu Cyberbedrohungen. Verwendung von STIX-Daten und vertrauenswürdigem automatisierten Austausch von Indikatorinformationen (TAXII ™) Profile, können Bedrohungsexperten gemeinsam genutzte Cyberbedrohungsinformationen verwenden, um Bedrohungen zu isolieren, die zuvor von Ihrem Unternehmen und aus anderen Quellen identifiziert wurden. TAXII ermöglicht einen weit verbreiteten automatisierten Austausch von Cyberbedrohungsinformationen.

Threat Intelligence Unterstützt STIX-Versionen 1,1, 2,0 und 2,1.

STIX ™Und TAXII ™Sind Marken der MITRE Corporation.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Domain Separation und Threat Intelligence

Domänentrennung wird in unterstützt Threat Intelligence Modul, das als Teil von Security Incident Response verfügbar ist. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Umfasst die **Basis**-Support-Stufe.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für Domänentrennung .

Übersicht

Im Threat Intelligence-Modul (als Teil der Security Incident Response-Anwendung) ermöglicht die Domänentrennung Service Providern (SPS) die Erstellung und Verwaltung des Threat Intelligence-Repositorys auf folgende Weise:

- Bedrohungsquellen und TAXII-Profile (Trusted Automated Exchange of Indicator Information)
- Erkennbare Elemente
- Kompromittierungsindikatoren
- Bedrohungsangriffsmodi/-Methoden und Fallmanagement für den gesamten Kundenstamm, für den sie zuständig sind, mit niedrigeren Betriebskosten und einer höheren Servicequalität

Durch separate Kundenarbeitsbereiche für Workflows, Dashboards, Berichte usw. wird sichergestellt, dass Kundendaten getrennt werden und niemals anderen Clients zugänglich gemacht werden.

Unterstützung der Domänentrennung in Threat Intelligence Nach Versionsrelease

Domänentrennung für das Threat Intelligence-Modul (als Teil von Security Incident Response Anwendung) deckt die folgenden Produktfunktionen ab:

- Erkennbare Security Incident-Elemente werden an die entsprechende Domäne des Anwenders weitergeleitet, dessen ID/Anmeldeinformationen/Umfang den Incident generiert. Die aus dem Incident extrahierten erkennbaren Elemente werden in der Domäne des Security Incident gespeichert.
- Einrichten von TAXII-Serviceprofilen zum Herunterladen einer oder mehrerer TAXII-Sammlungen, die Informationen zu Cyberbedrohungen bieten. Die Konfiguration wird in der Domäne gespeichert, unter der das Profil eingerichtet wird.
- Einrichten des Downloads von Bedrohungsfeeds in das IOC-Repository in der Domäne, unter der die Konfiguration ausgeführt wird.
- Erstellung von Angriffsmodi/-Methoden in der Domäne der Threat Intelligence-Quelle, die die Informationen automatisch bereitstellt, oder der Domäne, unter der ein neuer Angriffsmodus/-Methode vom Anwender manuell hinzugefügt wird
- Erstellung von Fällen für die langfristige Untersuchung von Incidents, erkennbaren Elementen, CIs, Anwendern und Indikatoren der Kompromittierung (IOC), die dem Fall zugeordnet sind. Der Fall wird in der vom Anwender erstellten Domäne gespeichert.

Hinweis:
In allen obigen Fällen gelten die übergreifenden Prinzipien der Sichtbarkeit in getrennten Domänen in der NOW Platform. Wie immer kann ein Incident in der übergeordneten Domäne auf Artefakte in der untergeordneten Domäne verweisen, aber nicht umgekehrt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionsweise der Domänentrennung in Threat Intelligence(Als Teil von Security Incident Response)

Threat Intelligence ist Teil von Security Incident Response auf den Stufen Professional und Enterprise, jedoch nicht auf der Stufe Standard. Daher ist ein separates Plugin erforderlich. Das Threat Intelligence-Modul (als Teil von Security Incident Response Anwendung) erstellt und verwaltet die Threat Intelligence-Informationen, die Security Incidents in einer Organisation zugeordnet sind. Die folgenden Anwendungsfälle sind auf Domänentrennung ausgerichtet:

- Erstellung erkennbarer Security Incident-Elemente zum Zeitpunkt der Incident-Erstellung
  - Aus E-Mail-Parsern (plattformbasiert, von Anwendern gemeldetes Phishing, anwenderdefiniert)
  - Aus Anwendungen in SIEM-Stores (Security Information and Event Management) von Drittparteien
  - Manuell vom SOC-Analysten eingegeben
- Sammlung erkennbarer Elemente aus Bedrohungs-Feed-Quellen: Threat Intelligence-Quellen aus TAXII-Sammlungen
- Verwalten Sie erkennbare Security Incident-Elemente
  - Ordnen Sie erkennbare Elemente zugehörigen Indikatoren zu
  - Ordnen Sie erkennbare Elemente Security Incidents zu
  - Ordnen Sie erkennbare Elemente untergeordneten erkennbaren Elementen zu
  - Erkennbares Element der Bedrohungs-Feed-Quelle zuordnen
  - Fügen Sie erkennbaren Elementen Sicherheitsanmerkungen hinzu
- Verwalten Sie Kompromittierungsindikatoren
  - Ordnen Sie Indikatoren zugehörigen erkennbaren Elementen zu
  - Ordnen Sie Indikatoren dem Angriffsmodus/-Methode zu
  - Ordnen Sie Indikatoren Indikatortypen zu
  - Ordnen Sie Indikatoren der Bedrohungs-Feed-Quelle zu
  - Fügen Sie Sicherheitsanmerkungen zu Indikatoren hinzu
- Verwalten Sie Fälle
  - Fall erstellen (manuell oder aus einem Incident)
  - Bearbeiten Sie einen neuen Fall, um Details hinzuzufügen (Falltyp und Schweregrad auswählen, Incidents, erkennbare Elemente, Konfigurationselemente, Anwender hinzufügen, Indikatoren)
  - Löschen Sie einen Fall

Domänentrennung – Einrichtung

Das Einrichten der Domänentrennung für Threat Intelligence erfordert keine zusätzlichen Schritte. Alle Threat Intelligence-Tabellen erhalten die Spalte „Domäne“, nachdem die Instanz domänengetrennt wurde.

Domänengetrennte Daten

Daten können domänengetrennt werden, was bedeutet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erkennbare Security Incident-Elemente in einer Domäne können nicht im Umfang anderer Domänen angezeigt werden.
- Kompromittierungsindikatoren in einer Domäne können nicht im Umfang anderer Domänen angezeigt werden.
- Angriffsmodi/-Methoden, die einer Domäne zugeordnet sind, können nicht im Umfang anderer Domänen angezeigt werden.
- TAXII-Serviceprofile, die einer Domäne zugeordnet sind, können nicht im Umfang anderer Domänen angezeigt werden.
- Threat Intelligence-Quellen, die einer Domäne zugeordnet sind, können nicht im Umfang anderer Domänen angezeigt werden.
- Fälle, die einer Domäne zugeordnet sind, können nicht im Bereich anderer Domänen angezeigt werden.

Threat Intelligence-Eigenschaften werden auf globaler Ebene festgelegt und sind daher nicht domänengetrennt. Die Einstellungen umfassen:

- Der Domänenname zum Abrufen zusätzlicher Informationen für IP-Adressen/URLs
- Der API-Schlüssel, der für den Abruf verwendet werden soll
- Suchen Sie nach lokalen IOC-Tabellen, bevor Sie sie an den Remote-Scanner senden
- Anzahl der Tage, an denen lokale erkennbare Elemente berücksichtigt werden
- Angriffsmodus/-Methode wird als inaktiv markiert, wenn sie nicht von bedrohungsinformationsquellen empfangen wird
- Markieren eines Indikators als inaktiv, wenn er für eine angegebene Anzahl von Tagen von keiner Quelle empfangen wurde

Konfiguration

Alle Aspekte der Konfiguration der Threat Intelligence-Funktionalität sind in einer domänengetrennten Umgebung enthalten.

Die folgenden Aufgaben können pro Domäne konfiguriert werden:

1. Erstellung von TAXII-Serviceprofilen
   - Wählen Sie eine Discovery-Servicekonfiguration aus
   - Wählen Sie eine Sammlungsservicekonfiguration aus: Weisen Sie Anwendern und Anwendergruppen Rollen zu
2. Erstellung von Threat Intelligence-Quellen
   - Konfigurieren Sie den REST-Service, der die Threat intel-Informationen bereitstellt
   - Planen Sie den Download von Bedrohungsinformationen
   - Wählen Sie Informationen zu Bedrohungsdetails aus, die der Quelle zugewiesen werden sollen
3. Erstellung von Angriffsmodus/-Methoden (manuell)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Quelle, Malware-Typ, Angriffsmechanismus, Bedrohungsakteurtyp, Beschreibung, Verarbeitung, beabsichtigte Wirkung, zuerst gesehen, zuletzt gesehen
- Zugehörige Indikatoren, untergeordneter Angriffsmodus/-Methode, zugehörige Security Incidents

Hinweis:
Angriffsmodi/-Methoden werden auch aus den Bedrohungs-Feed-Quellen automatisch erstellt.

4. Festlegen von Standardlisten für die folgenden Bedrohungsinformationskategorien:
   - Angriffsmechanismen
   - Discovery-Methoden
   - Feeds
   - Indikatortypen
   - Beabsichtigte Wirkungen
   - Benachrichtigungen
   - Typen von erkennbaren Elementen
   - Quotengrenzdefinitionen
   - Bedrohungsakteurtypen
   - Angriffsmotivationen
   - Infrastrukturtypen
   - Malware-Fähigkeiten
   - Schadsoftwaretypen
   - Berichtstypen
   - Rollen des Bedrohungsakteurs
   - Tooltypen

Wie Mandantendomänen ihre eigenen Anwendungsdaten verwalten

- Mandantendomänenbesitzer können eigene TAXII-Serviceprofile erstellen.
- Mandantendomänenbesitzer können eigene Threat Intelligence-Quellen erstellen.
- Mandantendomänenbesitzer können eigene Angriffsmodi/-Methoden erstellen.
- Mandantendomänenbesitzer können eigene Standardlisten für Bedrohungsinformationskategorien erstellen.

Hinweis:
Geschäftslogik und -Prozesse ermöglichen es, dass Downloadzeitpläne für Threat Intelligence-Quellen domänengetrennt nach Instanzbesitzer sind.

Zugehörige Informationen

Domänentrennung für Service Provider

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence einrichten

Bevor Sie ausführen Threat Intelligence In Ihrer Instanz müssen Sie es aus herunterladen ServiceNow Store. Sie können auch Eigenschaften einrichten und eine Bedrohungsquelle definieren.

Threat Intelligence installieren

Bevor Sie ausführen Threat Intelligence In Ihrer Instanz müssen Sie es aus herunterladen ServiceNow Store.

Vorbereitungen

Führen Sie vor der Installation die folgende Setup-Prüfliste aus. Diese Setup-Aufgaben sind für eine reibungslose Installation und Konfiguration erforderlich.

Setupaufgaben	Beschreibung
Stellen Sie sicher, dass Sie über die erforderlichen verfügen ServiceNow Rollen für Ihre Instanz.	Die folgenden Rollen sind für die Installation, Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Wenn nicht bereits zugewiesen, installiert der Systemadministrator [admin] die Anwendung und weist die Rolle „Bedrohungsadministrator“ [sn_ti.admin] zu. • Der Bedrohungsadministrator [sn_ti.admin] überwacht die Konfiguration und überprüft die erwarteten Ergebnisse.

Erforderliche Rolle: Administrator

Prozedur

Befolgen Sie die Anweisungen für Lädt eine Anwendung aus dem herunter ServiceNow Storean.

Nächste Maßnahme

Festlegen Threat Intelligence Eigenschaften.

Mit Threat Intelligence installierte Komponenten

Bei der Aktivierung des Threat Intelligence-Plugins werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Benutzerrollen.

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
Bedrohungsadministrator [sn_ti.admin]	Hat vollständige Kontrolle über alle Bedrohungseigenschaften, SLAs und Benachrichtigungen.	sn_ti.schreiben
Bedrohungsleser [sn_ti.read]	Hat Lesezugriff auf Bedrohungsinformationen.	sn.sec_cmn.int_read
Bedrohungsschreiber [sn_ti.write]	Hat Schreibzugriff auf Bedrohungsinformationen. Angriffsmodi, Indikatoren und erkennbare Elemente können nicht gelöscht werden. Nur ein Bedrohungsadministrator kann sie löschen.	• sn_sec_cmn.int_write • sn_ti.read
MITRE-Analyst [sn_ti.Mitre_Analyst]	Diese Rolle ermöglicht den Lesezugriff auf MITRE-ATT&CK Module in Threat Intelligence Und zu SIR Modul.	• sn_ti.read • sn_si.read

Installierte Tabellen

Tabelle	Beschreibung
Angriffsmechanismus [sn_ti_Attack_Mechanism]	Organisiert Angriffsmuster hierarchisch basierend auf Mechanismen, die häufig beim Ausnutzen einer Schwachstelle verwendet werden. Die Kategorien, die Mitglieder dieser Ansicht sind, stellen die verschiedenen Techniken dar, die zum Angriff auf ein System verwendet werden.
Angriffsmodus/-methode [sn_ti_Attack_Mode]	Angriffsmodi und -Methoden sind Darstellungen des Verhaltens von Cyberangreifern. Sie charakterisieren, was ein Angreifer tut und wie er dies in zunehmendem Detailgrad tut.
Discovery-Methode [sn_ti_Discovery_method]	Ein Ausdruck, wie ein Incident erkannt wurde.
Feed-Gruppe [sn_ti_Feed]	Wird zum Konfigurieren des Threat Feeds (RSS) in der Bedrohungsübersicht verwendet.
Indikator-Angriffsmodus/-Methode [sn_ti_m2m_indicator_Attack_Mode]	Wird verwendet, um Angriffsmodi/-Methoden Indikatoren zuzuordnen.
Kompromittierungsindikator	Wird verwendet, um bestimmte Muster erkennbarer Elemente in Kombination

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_ti_indicator]	mit kontextbezogenen Informationen zu übermitteln, die Artefakte und/oder Verhaltensweisen von Interesse in einem Cybersicherheitskontext darstellen sollen.
Metadaten für Kompromittierungsindikator [sn_ti_indicator_metadata]	Wird zum Ausfüllen von TAXII-Datensätzen verwendet.
Indikatorquelle [sn_ti_m2m_indicator_Source]	Wird verwendet, um alle Quellen zu erfassen, die den spezifischen Indikator melden.
Indikatortyp [sn_ti_indicator_type]	Charakterisiert einen Cyberbedrohungsindikator, der aus einem Muster besteht, das bestimmte Bedingungen erkennbarer Elemente identifiziert, sowie kontextbezogene Informationen über die Bedeutung der Muster, wie und wann darauf reagiert wird usw.
Zugehöriger Indikatortyp [sn_ti_m2m_indicator_indicator_type]	Verknüpft Indikatoren mit ihren anwendbaren Typen
Incident-Anzahl [sn_ti_Observable]	Anzahl der Security Incidents, die einem erkennbaren Element zugeordnet sind.
Beabsichtigte Wirkung [sn_ti_beabsichtigte_Wirkung]	Wird verwendet, um die beabsichtigte Wirkung eines Bedrohungsakteurs auszudrücken.
IP-Scan-Ergebnis [sn_ti_ip_result]	Wird verwendet, um die Ergebnisse einer IP-Suche anzuzeigen.
Malware-Ratenlimit [sn_ti_rate_limit]	Definiert ein Quotenlimit, das in einer Suchquelle verwendet werden soll.
Malware-Scan [sn_ti_Scan]	Eine Suche. Enthält, was gesucht werden soll, mit welcher Suchquelle und eine Zusammenfassung der Suchergebnisse.
Malware-Scan-Warteschlangeneintrag [sn_ti_Scan_q_entry]	Ein Suchdatensatz, der zur Suche oder Verarbeitung in der Warteschlange steht. Erleichtert die Anforderungen innerhalb der angegebenen Quotengrenzen.
Ergebnis Des Malware-Scans [sn_ti_Scan_result]	Zeigt das Ergebnis einer Suche an.
Malware-Scanner [sn_ti_Scanner]	Definiert Drittpartei-Suchquellen, die beim Durchführen von Suchvorgängen verwendet werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Grenzwert Für Malware-Scanner [sn_ti_Scanner_rate_limit]	Ordnet eine Suchquelle einem Quotenlimit zu.
Malware-Typ [sn_ti_Malware_type]	Wird zum Ausdrücken der Typen von Malware-Instanzen verwendet.
Erkennbares Element [sn_ti_Observable]	Erkennbare Elemente in STIX stellen statusbehaftete Eigenschaften oder messbare Ereignisse dar, die für den Betrieb von Computern und Netzwerken relevant sind.
Kontexttyp für erkennbares Element [sn_ti_observable_context_type]	Speichert den Kontext (Quelle, Ziel einer IP-Adresse usw.) für ein erkennbares Element.
Indikator für erkennbares Element [sn_ti_m2m_observable_indicator]	Wird verwendet, um erkennbare Elemente mit Indikatoren zu verknüpfen.
Quelle erkennbares Element [sn_ti_observable_Source]	Wird verwendet, um erkennbare Elemente mit Bedrohungsquellen zu verknüpfen.
Erkennbarer Typ [sn_ti_observable_type]	Listet die verschiedenen Arten erkennbarer Elemente auf, z. B. IP-Adressen.
Typkategorie des erkennbaren Elements [sn_ti_observable_type_category]	Speichert die erste Kategorisierung von erkennbaren Elementen (z. B. IP-Adressen und URLs). Es wird verwendet, um erkennbare Typen genauer zu bestimmen.
Zugehöriger Angriffsmodus/-Methode [sn_ti_m2m_Attack_Mode_Attack_Mode]	Wird verwendet, um Angriffsmodi miteinander zu verknüpfen.
Zugehörige erkennbare Elemente [sn_ti_m2m_observables]	Wird verwendet, um erkennbare Elemente miteinander zu verknüpfen.
Überprüfungstyp [sn_ti_Scan_type]	Die Definition eines Suchtyps mit anfänglichen Datensätzen für Datei, URL und IP.
Sicherheitsfall [sn_ti_Case]	Speichert Sicherheitsfalldatensätze, die mit Fallmanagement erstellt wurden.
Sicherheitsfall-IoC [sn_ti_Case_ioc]	Wird verwendet, um die Beziehung zwischen erkennbaren Elementen und Fällen zu verwalten.
Zugehörige Aufgabe für Sicherheitsfall [sn_ti_m2m_Case_Task]	Wird verwendet, um die Beziehung zwischen Aufgaben (Security Incidents, Change-Anforderungen usw.) mit Sicherheitsfällen zu verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Beziehungsausschluss für Sicherheitsfall [sn_ti_Case_Relationship_Exclusion]	Stellt die Definition des Einschlusses und Ausschlusses zugehöriger Datensätze in Sicherheitsfällen bereit.
Sighting [sn_ti_Sighting]	Der m2m-Link zwischen dem erkennbaren Element und dem Detailergebnis der Sichtungssuche, das bei der Ausführung einer Sichtungssuchanforderung verwendet wird.
Konfigurationselemente der Sichtung [sn_ti_m2m_Sighting_ci]	Ordnet Konfigurationselemente einer Sichtungssuche zu.
Sichtungssuchdetail [sn_ti_Sighting_search_Detail]	Details einer Sichtungssuche, z. B. die Anzahl der gefundenen internen externen Elemente.
Sichtungssuchergebnis [sn_ti_Sighting_search]	Der Header für eine Sichtungssuche-Ausführung.
Unterstützte Typen von erkennbaren Elementen [sn_ti_m2m_ind_type_obs_type]	Bezieht Indikatortypen auf gültige erkennbare Typen.
Unterstützter Scan-Typ [sn_ti_supported_Scan_type]	Ordnet den Suchtyp einer Suchquelle/ Lieferantenspezifischen Implementierung zu. Gibt an, dass eine bestimmte Suchquelle den Typ unterstützt.
Aufgabenangriffsmodus/-Methode [sn_ti_m2m_Task_Attack_Mode]	Bezieht Angriffsmodi auf Aufgaben.
Aufgabenindikator [sn_ti_m2m_Task_indicator]	Bezieht Indikatoren auf Aufgaben.
Erkennbares Aufgabenelement [sn_ti_m2m_Task_Observable]	Bezieht erkennbare Elemente mit Aufgaben in Beziehung.
Aufgabensichtung [sn_ti_m2m_Task_Sighting]	Speichert Aufgabendatensätze (Security Incidents und Fälle) im Zusammenhang mit einem Sichtungsdatensatz.
TAXII-Sammlung [sn_ti_Taxii_Collection]	Definiert einen Intelligence-Feed für Cyberrisiken, der von einem TAXII-Server importiert werden kann.
TAXII-Profil [sn_ti_Taxii_Profile]	Definiert ein Repository für die Freigabe von Cyberrisikoinformationen. Enthält TAXII-Sammlungen.
Typ des Bedrohungsakteurs [sn_ti_Threat_actor_type]	Bietet Charakterisierungen von böswilligen Akteuren (oder Angreifern), die eine Cyberangriffsbedrohung darstellen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
	einschließlich vermuteter Absicht und historisch beobachtetem Verhalten.
Threat Intelligence-Quelle [sn_ti_Source]	Definiert eine Quelle für den Import von Bedrohungsdaten.
Zugehörige Angriffsmotivation [sn_ti_stix2_m2m_object_Attack_Motivation]	Sammelt alle Angriffsmotivationen, die einem STIX-Objekt zugeordnet sind.
Zugehöriger Infrastrukturtyp [sn_ti_stix2_m2m_infra_type]	Verknüpft die Infrastruktur mit ihren Typen.
Zugehörige Kill Chain-Phase [sn_ti_stix2_m2m_indicator_kill_Chain_Phase]	Verknüpft Kill Chain-Phasen mit Indikatoren.
Zugehörige Kill Chain-Phase [sn_ti_stix2_m2m_object_kill_Chain_Phase]	Verknüpft Kill Chain-Phasen mit STIX-Objekten.
Zugehörige Malware-Fähigkeit [sn_ti_stix2_m2m_Malware_Capability]	Verknüpft Malware mit ihren Fähigkeiten.
Zugehöriger Malware-Typ [sn_ti_stix2_m2m_Malware_Malware_type]	Verknüpft Malware mit ihren Typen.
Zugehöriges erkennbares Element [sn_ti_stix2_m2m_Malware_Observable]	Erfasst alle erkennbaren Elemente, die einer Malware zugeordnet sind.
Zugehöriges erkennbares Element [sn_ti_stix2_m2m_observed_Data_Observable]	Erfasst alle erkennbaren Elemente, die einem beobachteten Daten zugeordnet sind.
Zugehöriger Berichtstyp [sn_ti_stix2_m2m_Report_Report_type]	Verknüpft Bedrohungsberichte mit ihren Typen.
Zugehörige Bedrohungsakteur-Rolle [sn_ti_stix2_m2m_Threat_actor_Threat_actor_role]	Verknüpft Bedrohungsakteure mit ihren Rollen.
Zugehöriger Bedrohungsakteur-Typ [sn_ti_stix2_m2m_Threat_actor_Threat_actor_type]	Verknüpft Bedrohungsakteure mit ihren Typen.
Zugehöriger Tool-Typ [sn_ti_stix2_m2m_Tool_type]	Verknüpft Tools mit ihren Typen.
Angriffsmotivation [sn_ti_stix2_Attack_Motivation]	Die Angriffsmotivation beeinflusst die Intensität und Persistenz eines Angriffs. Bedrohungsakteure und Angriffssätze verhalten sich normalerweise so, dass sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
	ihre zugrunde liegende Emotionen oder Situation widerspiegeln. Dies informiert die Verteidiger über die Art des Angriffs.
Angriffsmuster [sn_ti_stix2_Attack_pattern]	Ein TTP-Typ, der Methoden beschreibt, mit denen Angreifer versuchen, Ziele zu gefährden.
Kampagne [sn_ti_stix2_campaign]	Eine Gruppierung von konversationswidrigen Verhaltensweisen, die eine Reihe böswilliger Aktivitäten oder Angriffe (manchmal als Waves bezeichnet) beschreiben, die über einen bestimmten Zeitraum gegen eine bestimmte Gruppe von Zielen auftreten.
Vorgehensweise [sn_ti_stix2_Kurs_der_Aktion]	Eine Empfehlung eines Erstellers von Intelligenz an einen Verbraucher zu den Aktionen, die er als Reaktion auf Intelligenz ergreifen könnte.
Externe Referenz [sn_ti_stix2_external_reference]	Verweist auf Informationen, die außerhalb von STIX dargestellt werden.
Identitätssichtung [sn_ti_stix2_m2m_Sighting_Identity]	Erfasst alle Identitäten, die einer Sichtung zugeordnet sind.
Identität [sn_ti_stix2_Identität]	Tatsächliche Einzelpersonen, Organisationen oder Gruppen (z. B. ACME, Inc.) sowie Klassen von Einzelpersonen, Organisationen, Systemen oder Gruppen (z. B. Finanzsektor).
Externe Indikator-Referenz [sn_ti_stix2_indicator_external_reference]	Stellt externe Referenzen dar, die Indikatoren zugeordnet sind.
Indikatorsichtung [sn_ti_stix2_indicator_Sighting]	Stellt Sichtungen von Indikatoren dar.
Infrastrukturtyp [sn_ti_stix2_Infrastructure_type]	Stellt die verschiedenen Infrastrukturtypen dar.
Infrastruktur [sn_ti_stix2_Infrastructure]	Ein TTP-Typ, der alle Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen beschreibt, die bestimmte Zwecke unterstützen sollen (z. B. C2-Server, die als Teil eines Angriffs verwendet werden, Geräte oder Server, die Teil der Verteidigung sind, Datenbankserver, die von einem Angriff angegriffen werden usw.).
Installierte Software [sn_ti_stix2_m2m_Malware_Analysis_SW]	Erfasst alle Software (SCO-Softwaretypen), die einer Malware-Analyse zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Angriffssatz [sn_ti_stix2_Intrusion_Set]	Ein gruppierter Satz von konversationswidrigen Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften, von denen angenommen wird, dass sie von einer einzigen Organisation orchestriert werden.
Kill Chain-Phase [sn_ti_stix2_kill_Chain_Phase]	Stellt Kill Chain-Phasen dar, die einer Kill Chain zugeordnet sind.
Kill Chain [sn_ti_stix2_kill_Chain]	Stellt verschiedene Kill Ketten dar.
Standort [sn_ti_stix2_location]	Stellt einen geografischen Standort dar, der über STIX bereitgestellt wird.
Malware-Analyse [sn_ti_stix2_Malware_Analysis]	Die Metadaten und Ergebnisse einer bestimmten statischen oder dynamischen Analyse, die für eine Malware-Instanz oder -Familie durchgeführt wird.
Malware-Fähigkeit [sn_ti_stix2_Malware_Capability]	Stellt allgemeine Fähigkeiten dar, die eine Malware-Familie oder -Instanz aufweist.
Malware-Betriebssystem [sn_ti_stix2_m2m_Malware_Operating_System]	Erfasst alle Betriebssysteme (SCO-Softwaretypen), die Malware zugeordnet sind.
Malware [sn_ti_stix2_Malware]	Ein TTP-Typ, der schädlichen Code darstellt.
Markierungsdefinition [sn_ti_stix2_Marking_Definition]	Stellt Anforderungen für die Verarbeitung oder Freigabe von STIX-Objekten dar.
Objektsichtung [sn_ti_stix2_object_Sighting]	Stellt Sichtungen von STIX-Objekten dar.
Objekt-Indikator-Beziehung [sn_ti_stix2_m2m_object_indicator]	Erfasst alle Beziehungen zwischen STIX-Objekten und STIX-Indikatoren.
Objekt-Objekt-Beziehung [sn_ti_stix2_m2m_object]	Erfasst alle Beziehungen zwischen STIX-Objekten und anderen STIX-Objekten mit Ausnahme der Indikatoren.
Beziehung von Objekt und erkennbarem Element [sn_ti_stix2_m2m_object_observable]	Sammelt alle Beziehungen zwischen STIX-erkennbaren Elementen und STIX-Objekten.
Beobachtete Datensichtung	Erfasst alle beobachteten Datenobjekte, die einer Sichtung zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_ti_stix2_m2m_Sighting_observed_Data]	
Beobachtete Daten [sn_ti_stix2_observed_Data]	Übermittelt Informationen über Cybersicherheitsbezogene Entitäten wie Dateien, Systeme und Netzwerke mithilfe von STIX Cyber-Observable Objects (SCOs).
Berichtstyp [sn_ti_stix2_Report_type]	Stellt den primären Zweck oder Betreff von Bedrohungsberichten dar.
Gemeldetes erkennbares Element [sn_ti_stix2_m2m_Malware_Analysis_Observable]	Erfasst alle erkennbaren Elemente, die der Malware-Analyse zugeordnet sind.
STIX V2-Objekt [sn_ti_stix2_object]	Allgemeine übergeordnete Tabelle für STIX-Objekt.
STIX V2-Sichtung [sn_ti_stix2_Sichtung]	Allgemeine übergeordnete Tabelle für STIX-Sichtungstabellen.
Bedrohungsakteurrolle [sn_ti_stix2_Threat_actor_role]	Stellt Rollen dar, die von Bedrohungsakteuren gespielt werden können.
Bedrohungsakteur [sn_ti_stix2_Threat_actor]	Bedrohungsakteure sind tatsächliche Einzelpersonen, Gruppen oder Organisationen, die vermutlich mit böswilliger Absicht arbeiten.
Bedrohungsgruppierung [sn_ti_stix2_Threat_grouping]	Gruppiert alle STIX-Objekte, die einen gemeinsamen Kontext teilen.
Bedrohungshinweis [sn_ti_stix2_Threat_note]	Stellt Kontext und zusätzliche Analysen bereit, die nicht im entsprechenden STIX-Objekt enthalten sind.
Bedrohungsmeinung [sn_ti_stix2_Threat_opinion]	Bietet eine Bewertung der Genauigkeit von Informationen in einem STIX-Objekt, das von einer anderen Entität erstellt wurde.
Bedrohungsbericht [sn_ti_stix2_Threat_Report]	Berichte sind Sammlungen von Threat Intelligence, die sich auf ein oder mehrere Themen konzentrieren, z. B. eine Beschreibung eines Bedrohungsakteurs, einer Malware oder einer Angriffstechnik, einschließlich Kontext und zugehörigen Details. Sie werden verwendet, um zugehörige Bedrohungsinformationen zusammenzufassen, um sie als umfassende Cyberbedrohungsstory zu veröffentlichen.
Tooltyp	Die Kategorien von Tools, die zum Ausführen von Angriffen verwendet werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sn_ti_stix2_Tool_type]	
Tool [sn_ti_stix2_Tool]	Tools sind legitime Software, die von Bedrohungsakteuren zum Ausführen von Angriffen verwendet wird.
Schwachstelle [sn_ti_stix2_Vulnerability]	Stellt eine Schwachstelle oder einen Fehler in den Anforderungen, Designs oder Implementierungen der Rechenlogik (Beispielcode) dar, die in der Software und einigen Hardwarekomponenten (z. B. Firmware) gefunden wird. Sie können direkt ausgenutzt werden, um die Vertraulichkeit, Integrität oder Verfügbarkeit dieses Systems negativ zu beeinflussen.

Festlegen Threat Intelligence Eigenschaften

Threat Intelligence Mit Eigenschaften können Sie steuern, wie verschiedene Aspekte der Systemfunktion, einschließlich der Einstellung von API-Schlüsseln.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Administration** > **Eigenschaften**an.
2. Legen Sie nach Bedarf die folgenden Eigenschaften fest.

Eigenschaften für Threat Intelligence

Eigenschaft	Beschreibung
Der Domänenname zum Abrufen zusätzlicher Informationen für IP-Adressen/URLs sn_ti.ip_Lookup.Web_Site	Der Domänenname, der zum Abrufen zusätzlicher Informationen in Ihre IOC-Datenbank verwendet werden soll. Diese Eigenschaft wird von verwendet ThreatAdditionalInfo Skripteinbindung zum Ausfüllen zusätzlicher Informationen im Formular „erkennbare Elemente“. Standardwert: http://api.ipinfodb.com/v3/ip-country/

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Hinweis: Die Drittpartei-API pinfodb.com ist ohne Aufpreis verfügbar und wird in vielen kommerziellen Softwareprogrammen verwendet. Wenn Sie ihn durch einen anderen Domänennamen ersetzen, müssen Sie auch den API-Schlüssel im nächsten Feld angeben.
Der API-Schlüssel, der für die Domäne verwendet werden soll, falls vorhanden sn_ti.ip_Lookup.api_key	Der API-Schlüssel, der zum Abrufen zusätzlicher Informationen in Ihre IOC-Datenbank verwendet werden soll. Diese Eigenschaft wird (zusammen mit der Eigenschaft sn_ti.ip_LOOKUP.Web_Site) von verwendet `ThreatAdditionalInfo` Skripteinbindung zum Ausfüllen zusätzlicher Informationen im Formular „erkennbare Elemente“.
Führen Sie keine automatisierte Bedrohungssuche für ein erkennbares Element aus, wenn das erkennbare Element einem IOC zugeordnet ist oder als schädlich erkannt wurde. sn_ti.Scan_ioc_before_Sending **Hinweis:** Sie müssen die Dauer in der Eigenschaft Next (sn_ti.Scan_ioc_num_days) definieren.	Option zum Beenden der automatisierten Bedrohungssuche für ein erkennbares Element, wenn das erkennbare Element für die konfigurierte Dauer (in Tagen) als schädlich oder einem IOC zugeordnet wurde. Wenn Sie die Bedrohungssuche für das erkennbare Element trotzdem ausführen müssen, können Sie dies manuell tun. Standardwert: Ja
Dauer (in Tagen) sn_ti.Scan_ioc_num_days	Option zum Definieren der Dauer, bis zu der die automatisierte Bedrohungssuche des erkennbaren Elements übersprungen wird. Standardwert (in Tagen): 30
Führen Sie keine automatisierte Bedrohungssuche für ein erkennbares Element aus, wenn es bereits ausgeführt wurde. sn_ti.enable_Threat_Lookup_Bypass **Hinweis:** Sie müssen die Dauer in der Eigenschaft Next (sn_ti.Threat_LOOKUP_Bypass_Times) definieren.	Wenn für ein erkennbares Element bereits ein Bedrohungssuchergebnis verfügbar ist, haben Sie die Möglichkeit, die erneute Ausführung der automatisierten Bedrohungssuche für dasselbe erkennbare Element zu überspringen, bis die konfigurierte Dauer abgelaufen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Standardwert: Nein **Hinweis:** Wenn Sie diese Eigenschaft aktivieren, stellen Sie sicher, dass Sie einen entsprechenden Wert hinzufügen.
Dauer (in Minuten) sn_ti.Threat_Lookup_Bypass_time	Option zum Definieren der Dauer, nach der die automatisierte Bedrohungssuche des erkennbaren Elements erneut ausgeführt werden kann. Standardwert (in Minuten): 0
Legen Sie eine Gültigkeitsdauer für Anwenderüberschreibungen für das Ergebnis erkennbarer Elemente fest. sn_ti.enable_observable_finding_System_override **Hinweis:** Sie müssen die Gültigkeit in der Eigenschaft Next (sn_ti.observable_finding_override_expiry) definieren.	Option zum Festlegen einer Gültigkeitsdauer für Anwenderüberschreibungen der Ergebnisse erkennbarer Elemente. Das Ergebnis der Bedrohungssuche des erkennbaren Elements wird während dieser Gültigkeitsdauer vom Basissystem nicht geändert. Standardwert: Nein **Hinweis:** Wenn Sie diese Eigenschaft aktivieren, stellen Sie sicher, dass Sie einen entsprechenden Wert hinzufügen.
Gültigkeit (in Minuten) sn_ti.observable_finding_override_expiry	Option zum Definieren des Gültigkeitszeitraums des Ergebnisses erkennbarer Elemente. Standardwert (in Minuten): Keine
Wenn ein Angriffsmodus bzw. eine Angriffsmethode für die angegebene Anzahl von Tagen von keiner Quelle empfangen wurde, als inaktiv markieren sn_ti.Attack_Mode_inactivate_days	Anzahl der Tage ab dem letzten Empfang eines Angriffsmodus/einer Methode, bis der Datensatz als inaktiv markiert wird. Standardwert: 360 **Hinweis:** Die **Aktiv** Das Kontrollkästchen ist in nicht sichtbar **Angriffsmodus/-Methode** Formular standardmäßig. Sie können es jedoch hinzufügen. Wenn Angriffsmodi/-Methoden inaktiv sind, können sie nicht in anderen Formularen ausgewählt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
Wenn ein Indikator für die angegebene Anzahl von Tagen von keiner Quelle empfangen wurde, als inaktiv markieren sn_ti.indicator_inactivate_days	Anzahl der Tage ab dem letzten Erhalt eines Indikators, der den Datensatz als inaktiv markiert. Standardwert: 180 **Hinweis:** Die **Aktiv** Das Kontrollkästchen ist in nicht sichtbar **Indikator** Formular standardmäßig. Sie können es jedoch hinzufügen. Wenn Indikatoren inaktiv sind, können sie nicht in anderen Formularen ausgewählt werden.
Die maximale Nutzlastgröße (in MB) für einen STIX-Anhang, der analysiert werden kann. sn_ti.stix.max_Payload_size	Gibt die maximale Nutzlastgröße für den STIX-Anhang an, den Sie analysieren können. Standardwert: keiner Maximal zulässiger Wert: Kein Grenzwert.
Maximale Zeit in Sekunden, die eine ausgehende HTTP-Verbindung wartet, um TAXII-Sammlungsdaten abzurufen sn_ti.Taxii.http.max_timeout	Gibt die maximale Zeit an, die eine ausgehende HTTP-Verbindung wartet, bevor das nächste Paket mit TAXII-Sammlungsdaten abgerufen wird. Standardwert: 300
Maximale Anzahl von Objekten, die in einem REST-Aufruf von einem TAXII-Server abgerufen werden (gilt nur für TAXII-Versionen 2.0 und 2.1) sn_ti.Taxii.max_page_size	Gibt die maximale Anzahl von Objekten an, die in einem REST-Aufruf vom TAXII-Server für eine Seite abgerufen werden. Standardwert: 5000 Maximal zulässiger Wert: 50000
Maximale Anzahl von Wiederholungen für einen fehlgeschlagenen TAXII 2.X-REST-Aufruf sn_ti.taxii2.retry_count	Gibt die maximale Anzahl von Wiederholungen für einen fehlgeschlagenen TAXII-REST-Aufruf an. Standardwert: 3

3. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie eine Bedrohungsquelle

Sie können eine Liste von verwalten Threat Intelligence Bedrohungsquellen. Jede Quelle enthält die Möglichkeit, zu definieren, wie oft eine Quelle abgefragt wird. Sie können auch bei Bedarf eine Bedrohungsquelle ausführen, um die erforderlichen STEX-Daten (Structured Threat Information Expression) zu importieren.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Warum und wann dieser Vorgang ausgeführt wird

Threat Intelligence Verwendet zwei Technologien zum Importieren von bedrohungsbezogenen Informationen: STIX und Trusted Automated Exchange of Indicator Information (TAXII).

STIX bietet eine standardisierte, strukturierte Sprache für die Darstellung eines umfangreichen Satzes von Cyberbedrohungsinformationen, einschließlich Indikatoren für kompromittierte Aktivitäten (IOC) (z. B. IP-Adressen und Datei-Hashes) sowie kontextbezogene Informationen zu Bedrohungen, z. B. Angriffsmodi/-Methoden, die zusammen die Motivationen, Fähigkeiten und Aktivitäten eines Cyberangreifers umfassender charakterisieren. Daher liefern STIX-Daten wertvolle Informationen darüber, wie Ihr Unternehmen am besten vor Cyberbedrohungen schützen kann.

Der vertrauenswürdige automatisierte Austausch von Indikatorinformationen (TAXII) wird verwendet, um den automatisierten Austausch von Cyberbedrohungsinformationen zu erleichtern. TAXII definiert eine Reihe von Services und Nachrichtenaustausch, die die Freigabe umsetzbarer Cyberbedrohungsinformationen über Organisations- und Produkt-/Servicegrenzen hinweg ermöglichen, um Cyberbedrohungen zu erkennen, zu verhindern und zu mindern. TAXII-Profile können als Repositorys für die Freigabe von STIX-formatierten Informationen eingerichtet werden. Jedes Profil enthält eine oder mehrere TAXII-Sammlungen oder -Feeds.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Quellen** > **Bedrohungsquellen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name der Bedrohungsquelle.
Anwendung	Die Anwendung, die diesen Datensatz enthält.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Bedrohungsquelle zu aktivieren.
Erweitert	Aktivieren Sie dieses Kontrollkästchen, um die Skripts in anzuzeigen **Integration Factory-Skript** Und **Berichtsprozessor** Felder.
Beschreibung	Eine Beschreibung dieser Bedrohungsquelle.

4. Füllen Sie die Felder im aus **Zeitplan** Abschnitt entsprechend.

Feld	Beschreibung
Ausführen	Die Häufigkeit, mit der die Integration ausgeführt werden soll, täglich, wöchentlich, regelmäßig usw. Wie bereits erwähnt, werden nachfolgende Felder basierend auf der Einstellung dieses Felds angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tag	Der Tag, an dem die Integration ausgeführt werden soll. ○ Wenn Sie ausgewählt haben **Wöchentlich** In **Ausführen** Feld zeigt dieses Feld die Wochentage an. ○ Wenn Sie ausgewählt haben **Monatlich** In **Ausführen** Feld zeigt dieses Feld die Tage des Monats an.
Zeit	Die Zeit, zu der die Integration beginnen soll.
Wiederholungsintervall	Wenn Sie ausgewählt haben **Regelmäßig** In **Ausführen** Feld zeigt dieses Feld die Anzahl der Tage und Stunden an, bevor die Integration erneut ausgeführt wird.
Wird gestartet	Wenn Sie ausgewählt haben **Regelmäßig** In **Ausführen** Feld zeigt dieses Feld die Daten und die Uhrzeit an, die als Ausgangspunkt für regelmäßige Aktualisierungen verwendet werden sollen.
Bedingt	Wählen Sie dieses Feld aus, wenn Sie bedingte Parameter hinzufügen möchten.
Bedingung	Wenn Sie ausgewählt haben **Bedingt** Kontrollkästchen: Geben Sie die Bedingungen hier ein.

5. Füllen Sie die Felder im aus **Bedrohungsdetails** Abschnitt entsprechend.

Feld	Beschreibung
Indikator	Der Indikator, der verwendet werden soll, wenn die Daten keinen explizit angeben. Wenn für Blocklisten leer, wird für jedes erkennbare Element ein neuer Indikator erstellt.
Indikatortyp	Der Indikatortyp, der für Indikatoren verwendet werden soll, die erstellt werden, und die Daten geben nicht explizit einen Indikatortyp an.
Angriffsmodus/-methode	Der Angriffsmodus/die anzuwendende Methode, wenn die Daten keinen explizit angeben.
Erkennbarer Typ	Der Typ des erkennbaren Elements, der für erstellte erkennbare Elemente verwendet werden soll, und die Daten geben nicht explizit einen erkennbaren Typ an.[SI1]
Gewichtung	Geben Sie einen Gewichtungswert für diese Quelle ein, der bei der Konfidenzberechnung verwendet werden soll.

Hinweis:
Die Verwendung von **Indikator** , **Indikatortyp** , **Angriffsmodus/-Methode** , Und **Typ Des Erkennbaren Elements** Felder sind implementierungsspezifisch. Der Standardprozessor, SimpleBlocklistProcessor, verhält sich wie in den Tooltips beschrieben. Eine TAXII-Bedrohungsquelle ist jedoch vollständig datengesteuert. Jeder anwenderdefinierte Bedrohungsquellenprozessor kann seine eigene Strategie verwenden. Diese Felder sind im Wesentlichen Elemente, die der Integration/dem Prozessor zugänglich gemacht werden sollen, und die Implementierung entscheidet, wie sie verwendet werden.

6. Füllen Sie die Felder im aus **Quelldetails** Abschnitt entsprechend.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Endpunkt	Geben Sie die Webservice-Endpunkt-URL ein, von der auf die Bedrohungsquelle zugegriffen wird Threat Intelligence. Klicken Sie auf das Sperrsymbol, um die URL zu sperren.
REST-Nachricht verwenden	Wenn Sie eine REST-Nachricht benötigen, um auf die Bedrohungsquelle zuzugreifen, aktivieren Sie dieses Kontrollkästchen. Die **REST-Nachricht** Und **REST-Methode** Felder werden zu Pflichtfeldern.
REST-Nachricht	Klicken Sie auf das Suchsymbol, und wählen Sie die REST-Nachricht aus der Liste aus, oder klicken Sie auf **Neu** Bis Definieren Sie eine neue REST-Nachricht .
REST-Methode	Klicken Sie auf das Suchsymbol, und wählen Sie die REST-Methode aus der Liste aus, oder klicken Sie auf **Neu** Zum Definieren einer neuen REST-Methode.
Integrationsskript	Das Standardintegrationsskript ist **SimpleRESTSecurityDataIntegration** . Es führt einen einfachen REST-Aufruf aus, speichert die Antwort als Anhang und gibt den Anhang dann an den Prozessor zurück. Dieses Skript erfüllt die Anforderungen der meisten Organisationen. Wenn Sie möchten, können Sie auf das Suchsymbol klicken und ein anderes Integrationsskript auswählen oder ein neues definieren.
Integrationswerksskript	Wenn **Erweitert** Das Kontrollkästchen ist aktiviert. In diesem Feld wird das tatsächliche Skript für die Erstellung des Integrationsskripts angezeigt. Sie können das Skript nach Bedarf bearbeiten. Diese Fähigkeit ist für anwenderdefinierte Implementierungen nützlich. Integrationen im Basissystem benötigen normalerweise keine anwenderdefinierte Konstruktorlogik.
Berichtsprozessor-Skript	Das Standardintegrationsskript ist **SimpleBlocklistProcessor** . Dieses Skript ist ein einfacher Prozessor, der eine einfache Blockliste (einfach, also ein einspaltiges Dokument mit erkennbaren Elementen wie URLs oder IP-Adressen) akzeptiert und erkennbare Elemente erstellt. Es verwendet verschiedene **Bedrohungsdetails** Felder, um zu bestimmen, welche Felder beim Erstellen erkennbarer Elemente festgelegt werden sollen.
Prozessorwerksskript	Wenn **Erweitert** Das Kontrollkästchen ist aktiviert. Dieses Feld zeigt das tatsächliche Skript für die Erstellung des Prozessors an. Sie können das Skript nach Bedarf bearbeiten. Dieses Skript ist im Allgemeinen für anwenderdefinierte Implementierungen nützlich. Die Integrationen im Basissystem benötigen normalerweise keine anwenderdefinierte Konstruktorlogik.

7. Klicken Sie auf **Absenden**.

Hinweis:
Weitere Informationen zum Konfigurieren der Paginierung der Bedrohungsquelle finden Sie unter KB1213825 artikel.

Erstellen Sie ein TAXII-Profil

Sie können TAXII-Profile verwalten, um STIX-formatierte Informationen freizugeben. Jedes Profil enthält eine oder mehrere TAXII-Sammlungen oder -Feeds.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Quellen** > **TAXII-Profile**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die folgenden Felder entsprechend aus.
4. Füllen Sie die Felder im aus **Discovery-Servicekonfiguration** Abschnitt entsprechend.
5. Füllen Sie die Felder im aus **Konfiguration Des Sammlungsservice** Abschnitt entsprechend.
6. Klicken Sie auf **Absenden**.

IoC-Repository

IOC-Repository enthält STIX-Objekte, jedes dieser Objekte enthält eine bestimmte Information.

Wenn Sie STIX-Objekte durch Beziehungen kombinieren, ermöglichen Sie einfache oder komplexe Darstellungen von Cyber Threat Intelligence (CTI).

Threat Intelligence Unterstützt STIX-Versionen 1,1, 2,0 und 2,1.

Angriffsmodi und -Methoden

Angriffsmodi und -Methoden, die manchmal als Taktiken, Techniken und Verfahren (TTPs) bezeichnet werden, sind Darstellungen des Verhaltens von Cyberangreifern. Sie charakterisieren, was diese Angreifer tun und wie sie es tun, in zunehmendem Detailgrad. Angriffsmodi und -Methoden gelten für STIX1,1.

Beispielsweise könnte ein Angriffsmodus/-Methode die Verwendung von Malware zum Diebstahl von Kreditkartenanmeldeinformationen sein. Oder eine andere zugehörige Taktik (auf einer niedrigeren Detailstufe) könnte darin bestehen, gezielte E-Mails mit Anhängen zu senden, die schädlichen Code enthalten, der beim Öffnen ausgeführt wird, Kreditkarteninformationen aus Tastenanschlägen erfasst und HTTP verwendet, um mit einem Befehls- und Steuerungsserver zu kommunizieren, um Informationen zu übertragen.

Angriffsmodi und -Methoden gelten für STIX1,1.

Definieren Sie einen Angriffsmodus/eine Angriffsmethode

Angriffsmodi und -Methoden werden mit STIX-Daten importiert, Sie können jedoch nach Bedarf neue Modi/Methoden hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Klassifizierungs-Tag auswählen	Wenn Sie eingerichtet und aktiviert haben Klassifizierungs-Tags Um dem Datensatz Metadaten hinzuzufügen, können Sie ein oder mehrere Tags auswählen, um den Grad der Empfindlichkeit des Angriffsmodus/der Angriffsmethode anzugeben. Wenn Sie keine Klassifizierungs-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt.
Titel	Geben Sie einen beschreibenden Namen für diesen Angriffsmodus/diese Angriffsmethode ein.
Malware-Typ	Wählen Sie den Malware-Typ für diesen Angriffsmodus/diese Angriffsmethode aus. Die verfügbaren Malware-Typen werden vom Lieferantenserver als STIX-Daten abgerufen.
Quelle	Wählen Sie die Bedrohungsdatenquelle für diesen Angriffsmodus/diese Angriffsmethode aus. Einige Datenquellen sind im Basissystem enthalten. Sie können Erstellen Sie neue Datenquellen Nach Bedarf.
Angriffsmechanismus	Wählen Sie den Angriffsmechanismus für diesen Angriffsmodus/diese Angriffsmethode aus. Angriffsmechanismen stellen die verschiedenen Techniken dar, die zum Angriff auf ein System verwendet werden. Die verfügbaren Angriffsmechanismen werden vom Lieferantenserver als STIX-Daten abgerufen.
Erstmals aufgetreten	Dieses Datum wird vom Lieferantenserver als STIX-Daten abgerufen.
Zuletzt aufgetreten	Dieses Datum wird vom Lieferantenserver als STIX-Daten abgerufen.
Typ Bedrohungsakteur	Wählen Sie den Bedrohungsakteurtyp für diesen Angriffsmodus/diese Angriffsmethode aus. Bedrohungsakteurtypen charakterisieren böswillige Akteure (oder Angreifer), die eine Cyberangriffsbedrohung darstellen, einschließlich vermuteter Absicht und historisch beobachtetem Verhalten. Die verfügbaren Bedrohungsakteurtypen werden vom Lieferantenserver als STIX-Daten abgerufen.
Beschreibung	Geben Sie eine Beschreibung des Angriffsmodus/der Angriffsmethode ein.
Handhabung	Geben Sie eine Anweisung ein, wie dieser Angriffsmodus/diese Angriffsmethode behandelt werden soll.
Beabsichtigte Wirkung	Geben Sie die beabsichtigte Auswirkung dieses Angriffstyps ein.

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.
Sie können eine der folgenden zugehörigen Listen anzeigen, um zusätzliche Informationen anzuzeigen.

Zugehörige Liste	Beschreibung
Zugehörige Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der Bedrohungsquelle identifiziert wurden.
Untergeordneter Angriffsmodus/-Methode	Listet Angriffsmodi/-Methoden auf, die dem übergeordneten Angriffsmodus/-Methode untergeordnet sind.
Zugehörige Aufgaben	Listet Changes auf, die dem übergeordneten Angriffsmodus/der übergeordneten Angriffsmethode zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie einem Angriffsmodus/einer Angriffsmethode ein IOC hinzu

Zusätzlich zum Importieren von Indikatoren als STIX-Daten können Sie einem Angriffsmodus/einer Angriffsmethode IoCs manuell hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**an.
2. Klicken Sie auf den Angriffsmodus, dem Sie ein IOC hinzufügen möchten.
3. Klicken Sie auf **Zugehörige Indikatoren** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um das IOC zu suchen, das Sie hinzufügen möchten.
6. Fügen Sie mit dem Slushbucket das IOC zu hinzu **Zugehörige Indikatoren** Liste.
7. Klicken Sie auf **Speichern**.

Fügen Sie eine zugehörige Angriffsmodusmethode hinzu

Zusätzlich zum Importieren von Angriffsmodi/-Methoden als STEX-Daten können Sie zugehörige Angriffsmodi/-Methoden manuell hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**an.
2. Klicken Sie auf den Angriffsmodus, dem Sie einen zugehörigen Angriffsmodus/eine zugehörige Angriffsmethode hinzufügen möchten.
3. Klicken Sie auf **Untergeordneter Angriffsmodus/-Methode** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Angriffsmodus/-Methode zu suchen, den Sie mit dem aktuellen in Beziehung setzen möchten.
6. Fügen Sie mithilfe des Slushbucket den Angriffsmodus/-Methode zu hinzu **Untergeordneter Angriffsmodus/-Methode** Liste.
7. Klicken Sie auf **Speichern**.

Fügen Sie einem Angriffsmodus/einer Angriffsmethode eine zugeordnete Aufgabe hinzu

Zusätzlich zum Importieren zugehöriger Aufgaben (z. B. Changes und Incidents) wie STEX-Daten können Sie sie manuell einem Angriffsmodus/einer Angriffsmethode hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmodus/-methode**an.
2. Klicken Sie auf den Angriffsmodus, dem Sie eine zugehörige Aufgabe hinzufügen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Zugeordnete Aufgaben** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Aufgaben zu suchen, die Sie dem Angriffsmodus/der Angriffsmethode zuordnen möchten.
6. Fügen Sie mit dem Slushbucket die Aufgabe zu hinzu **Zugeordnete Aufgaben** Liste.
7. Klicken Sie auf **Speichern**.

Kompromittierungsindikatoren

Indikatoren für Kompromittierung (IOC) sind Artefakte, die in einem Netzwerk oder Betriebssystem beobachtet werden und wahrscheinlich auf einen Angriff hinweisen. Typische IoCs sind Virensignaturen und IP-Adressen, MD5-Hashes von Malware-Dateien oder URLs oder Domänennamen. IOC gilt für STIX1,1 und 2.x.

Ein IOC kann ein einzelnes erkennbares Element oder eine Sammlung von erkennbaren Elementen sein (z. B. eine einzelne bekannte ungültige URL oder das Vorhandensein einer bestimmten Datei und einiger bestimmter Registrierungsschlüsselwerte).

Nachdem IoCs in einem Prozess der Reaktion auf Incidents und Computerforensik identifiziert wurden, können sie zur Früherkennung zukünftiger Angriffsversuche mithilfe von Angriffserkennungssystemen und Virenschutzsoftware verwendet werden.

IOC gilt für STIX1,1 und 2.x.

Zeigen Sie ein IOC an

IOCs, manchmal als Indikatoren bezeichnet, werden normalerweise aus einer Bedrohungsdatenquelle als STEX-Daten abgerufen. Bei Bedarf können Sie auch IoCs erstellen.

Vorbereitungen

Erforderliche Rolle: sn_ti.write

Prozedur

1. Nachdem die geplante Aufgabe IOC-Daten von abgerufen hat Definierte Datenquelle , Navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Indikatoren**an.
   Die abgerufenen IoCs werden aufgelistet.
2. Klicken Sie auf das IOC, das Sie anzeigen möchten.
3. Die folgenden Informationen werden angezeigt.

Feld	Beschreibung
Klassifizierungs-Tag auswählen	Wenn Sie eingerichtet und aktiviert haben Sicherheits-Tags Um dem Datensatz Metadaten hinzuzufügen, können Sie ein oder mehrere Tags auswählen, um den Grad der Empfindlichkeit des IOC anzugeben. Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt.
Titel	Ein beschreibender Name für diesen Indikator.
Erstmals aufgetreten	Das erste Datum, an dem dieser Indikator im System beobachtet wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zuletzt aufgetreten	Das letzte Datum, an dem dieser Indikator im System beobachtet wurde.
Aufgetretene Anzahl	Die Anzahl, mit der der der Indikator aufgetreten ist.
Quellenanzahl	Die Anzahl, mit der der der Indikator aus definierten Bedrohungsquellen importiert wurde.
Notizen	Alle zusätzlichen Hinweise zum Indikator. Dieses Feld kann auch JSON-Schlüssel-Wert-Paare enthalten.

4. Sie können auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die mit dem aktuellen Indikator verknüpft sind.
Zugehöriger Angriffsmodus/-Methode	Listet zugehörige Angriffsmodi/-Methoden auf, die als mit diesem Indikator verwandt identifiziert wurden.
Zugeordneter Typ	Listet andere Indikatortypen auf, die diesem IOC zugeordnet sind.
Indikatorquellen	Listet die Quellen dieses Indikators zusammen mit dem Konfidenzniveau der Quelle auf.
Zugehörige Aufgaben	Listet alle Aufgaben, Changes und Incidents auf, die dem IOC zugeordnet sind.
Indikator-Metadaten	Wenn **Notizen** Das Feld enthält gültige JSON-Schlüssel-/Wert-Paare. Sie werden analysiert und angezeigt. Wenn keine JSON-Schlüssel/Wert-Paare vorhanden sind oder die JSON ungültig ist, wird diese zugehörige Liste nicht angezeigt.
Sicherheitsanmerkungen	
Externe Indikator-Referenzen	
Zugehörige Kill Chain-Phasen	Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.

Fügen Sie einem IOC ein zugehöriges erkennbares Element hinzu

Zusätzlich zum Importieren erkennbarer Elemente als STIX-Daten können Sie einem IOC zugehörige erkennbare Elemente manuell hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti.write

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**an.
2. Klicken Sie auf den Indikator, dem Sie ein zugehöriges erkennbares Element hinzufügen möchten.
3. Klicken Sie auf **Zugehörige Erkennbare Elemente** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um das erkennbare Element zu suchen, das Sie mit dem IOC verknüpfen möchten.
6. Fügen Sie mit dem Slushbucket das erkennbare Element zu hinzu **Zugehörige Erkennbare Elemente** Liste.
7. Klicken Sie auf **Speichern**.

Fügen Sie einem IOC einen zugehörigen Angriffsmodus/-Methode hinzu

Zusätzlich zum Importieren zugehöriger Angriffsmodi/-Methoden als STEX-Daten können Sie einem IOC zugehörige Angriffsmodi/-Methoden manuell hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti.write

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**an.
2. Klicken Sie auf den Indikator, dem Sie einen zugehörigen Angriffsmodus/eine zugehörige Angriffsmethode hinzufügen möchten.
3. Klicken Sie auf **Zugehöriger Angriffsmodus/-Methode** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Angriffsmodus/die Angriffsmethode zu finden, den Sie mit dem IOC verknüpfen möchten.
6. Fügen Sie mithilfe des Slushbucket den Angriffsmodus/-Methode zu hinzu **Zugehöriger Angriffsmodus/-Methode** Liste.
7. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identifizieren Sie zugeordnete Indikatortypen

Wenn für ein IOC keine zugehörigen Indikatortypen definiert sind, werden alle Arten erkennbarer Elemente verfolgt. Wenn Sie jedoch einem IOC einen oder mehrere Arten von Indikatoren zuordnen, werden die Arten von erkennbaren Elementen eingeschränkt, die dem IOC zugeordnet werden können.

Vorbereitungen
Erforderliche Rolle: sn_ti.write

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**an.
2. Klicken Sie auf den Indikator, dem Sie einen Indikatortyp zuordnen möchten.
3. Klicken Sie auf **Zugeordneter Typ** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Indikatortyp zu suchen, den Sie dem IOC zuordnen möchten.
6. Fügen Sie mit dem Slushbucket den Indikatortyp zu hinzu **Zugeordneter Typ** Liste.
7. Klicken Sie auf **Speichern**.

Identifizieren Sie Indikatorquellen

Indikatorquellen werden normalerweise automatisch als Teil des Bedrohungsimportprozesses nachverfolgt, es können jedoch weitere Quellen manuell hinzugefügt werden.

Vorbereitungen
Erforderliche Rolle: sn_ti.write

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**an.
2. Klicken Sie auf den Indikator, dem Sie Indikatorquellen hinzufügen möchten.
3. Klicken Sie auf **Indikatorquellen** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Indikatorquelle zu suchen, die Sie dem IOC zuordnen möchten.
6. Fügen Sie mithilfe des Slushbucket die Indikatorquelle zu hinzu **Indikatorquellen** Liste.
7. Klicken Sie auf **Speichern**.

Fügen Sie einem IOC zugeordnete Aufgaben hinzu

Zusätzlich zum Importieren zugeordneter Aufgaben (z. B. Changes und Incidents) wie STEX-Daten können Sie sie manuell einem IOC hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_ti.write

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatoren**an.
2. Klicken Sie auf das IOC, dem Sie eine zugeordnete Aufgabe hinzufügen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Zugeordnete Aufgaben** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Aufgaben zu suchen, die Sie dem IOC zuordnen möchten.
6. Fügen Sie mit dem Slushbucket die Aufgabe zu hinzu **Zugeordnete Aufgaben** Liste.
7. Klicken Sie auf **Speichern**.

Erkennbare Elemente

Erkennbare Elemente stellen statusbehaftete Eigenschaften (z. B. den MD5-Hash einer Datei oder den Wert eines Registrierungsschlüssels) oder messbare Ereignisse (z. B. die Erstellung eines Registrierungsschlüssels oder das Löschen einer Datei) dar, die für den Betrieb von Computern und Netzwerken relevant sind. Erkennbare Elemente gelten für STIX1,1 und 2.x.

Sätze von Cyber-erkennbaren Elementen sind nützlich, um Indikatoren für Gefährdungen zu identifizieren, wenn sie mit kontextbezogenen Informationen kombiniert werden, die das Verhalten von Cyberbedrohungen darstellen.

Erkennbare Elemente gelten für STIX1,1 und 2.x.

Definieren Sie ein erkennbares Element

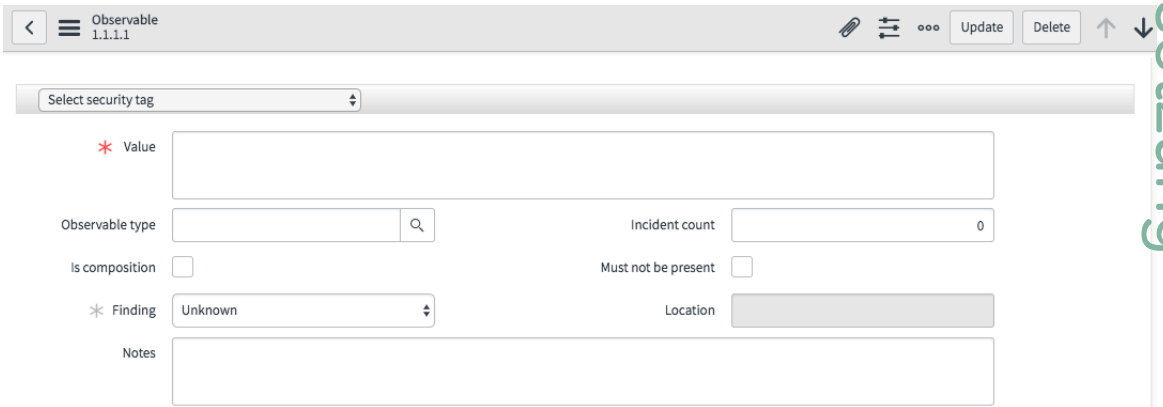
Erkennbare Elemente werden vom Lieferantenserver als STIX-Daten abgerufen. Sie können jedoch erkennbare Elemente nach Bedarf erstellen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**an.
2. Klicken Sie auf **Neu**.



3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Klassifizierungs-Tag auswählen	Wenn Sie eingerichtet und aktiviert haben Sicherheits-Tags Um dem Datensatz Metadaten hinzuzufügen, können Sie ein oder mehrere Tags auswählen, um den Grad der Empfindlichkeit des erkennbaren Elements anzugeben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn Sie keine Sicherheits-Tags eingerichtet oder aktiviert haben, wird diese Dropdown-Liste nicht angezeigt.
Wert	Der Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist. **Hinweis:** Wenn ein Bedrohungsscan durchgeführt wird Bei einer IP-Adresse oder einem Hash, bei der Malware oder einem anderen Fehler zurückgegeben wurde, wird die IP-Adresse oder der Hash-Wert automatisch der Tabelle des erkennbaren Elements [sn_ti_observable] hinzugefügt. Daher kann sie über das Formular „erkennbare Elemente“ gesucht werden.
Typ des erkennbaren Elements	Wählen Sie die Klassifizierung erkennbarer Elemente aus, z. B. eine IP-Adresse oder einen Datei-Hash. Diese Typen erkennbarer Elemente sind in definiert **Typen Erkennbarer Elemente** Modul.
Incident-Anzahl	Gibt an, wie oft der Wert des erkennbaren Elements aufgetreten ist.
Ist Zusammensetzung	Dieses Feld wird erst angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde. Wenn **Typ Des Erkennbaren Elements** Ist auf alles andere festgelegt **Zusammensetzung Erkennbarer Elemente** , Und dieses neue erkennbare Element ist eine Zusammensetzung, aktivieren Sie dieses Kontrollkästchen. Wenn **Typ Des Erkennbaren Elements** Ist bereits auf festgelegt **Zusammensetzung Erkennbarer Elemente** , Das Kontrollkästchen ist aktiviert und schreibgeschützt. Eine Zusammensetzung eines erkennbaren Elements ist ein erkennbares Element, das untergeordnete erkennbare Elemente enthält.
Ergebnis	Wählen Sie eine der folgenden Optionen aus: ○ **Böswillig** : Gibt an, dass das erkennbare Element für die Organisation schädlich ist. ○ **Verdächtig** : Gibt an, dass das erkennbare Element für die Organisation schädlich sein könnte. ○ **Bereinigen** : Gibt an, dass das erkennbare Element für die Organisation nicht schädlich ist. ○ **Unbekannt** : Gibt an, dass wir das Ergebnis des erkennbaren Elements noch bestimmen müssen. ○ Standardwert: Unbekannt. Weitere Informationen finden Sie unter Rechner für Funde der Bedrohungssuche. **Hinweis:** Nach einem Upgrade werden vorhandene erkennbare Elemente als schädlich markiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Operator	Dieses Feld wird nur angezeigt, wenn **Ist Zusammensetzung** Das Kontrollkästchen ist aktiviert. Abhängig von Ihrer Einstellung in diesem Feld werden die erkennbaren Elemente und ihre untergeordneten Elemente bei der Entscheidung berücksichtigt, ob ein zugeordneter Indikator vorhanden ist. Legen Sie dieses Feld auf fest **UND** Wenn alle untergeordneten erkennbaren Elemente vorhanden sein müssen, damit ein zugehöriger Indikator als vorhanden betrachtet wird. Legen Sie sie auf fest **ODER** Ob eines der untergeordneten erkennbaren Elemente vorhanden ist, damit ein zugehöriger Indikator als vorhanden betrachtet wird.
Darf nicht vorhanden sein	Dieses Feld wird erst angezeigt, nachdem der Datensatz des erkennbaren Elements gespeichert wurde. Wenn diese Option ausgewählt ist, gibt dieses Feld an, dass das Fehlen des erkennbaren Elements das potenzielle Problem ist (z. B. ein fehlender Registrierungsschlüssel).
Standort	Mithilfe der Einstellungen in zwei Eigenschaften und einer Skripteinbindungsdefinition können Sie laden Laden Sie weitere IOC-Daten In diesem Feld.
Notizen	Geben Sie zusätzliche Notizen zum erkennbaren Element ein.

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**. Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen.

Zugehörige Liste	Beschreibung
Zugehörige Indikatoren	Listet Indikatoren auf, die von der Bedrohungsquelle identifiziert wurden.
Zugehörige Aufgaben	Listet Changes auf, die dem erkennbaren Element zugeordnet sind.
Untergeordnete erkennbare Elemente	Listet zugehörige erkennbare Elemente auf, die von der Bedrohungsquelle identifiziert wurden.
Übereinstimmende Ressourcen für IP	Wenn das erkennbare Element eine IP-Adresse ist, werden in dieser Liste alle Ressourcen (Konfigurationselemente) angezeigt, die eine übereinstimmende IP-Adresse haben.
Quelle erkennbare Elemente	Listet die Quellen dieses erkennbaren Elements zusammen mit dem Konfidenzniveau der Quelle auf.
Sicherheitsanmerkungen	Listet Sicherheitsanmerkungen auf, die diesem erkennbaren Element hinzugefügt wurden.

Fügen Sie einem erkennbaren Element ein zugehöriges IOC hinzu

Zusätzlich zum Importieren erkennbarer Elemente als STIX-Daten können Sie einem IOC zugehörige erkennbare Elemente manuell hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**an.
2. Klicken Sie auf das erkennbare Element, dem Sie ein zugehöriges IOC hinzufügen möchten.
3. Klicken Sie auf **Zugehörige Indikatoren** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um den Indikator zu suchen, den Sie mit dem erkennbaren Element verknüpfen möchten.
6. Fügen Sie mit dem Slushbucket den Indikator zu hinzu **Zugehörige Indikatoren** Liste.
7. Klicken Sie auf **Speichern**.

Fügen Sie einem erkennbaren Element zugeordnete Aufgaben hinzu

Zusätzlich zum Importieren zugeordneter Aufgaben (z. B. Changes und Incidents) wie STEX-Daten können Sie sie einem erkennbaren Element manuell hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**an.
2. Klicken Sie auf das erkennbare Element, dem Sie eine zugeordnete Aufgabe hinzufügen möchten.
3. Klicken Sie auf **Zugeordnete Aufgaben** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Aufgaben zu suchen, die Sie dem erkennbaren Element zuordnen möchten.
6. Fügen Sie mit dem Slushbucket die Aufgabe zu hinzu **Zugeordnete Aufgaben** Liste.
7. Klicken Sie auf **Speichern**.

Fügen Sie ein zugehöriges erkennbares Element hinzu

Zusätzlich zum Importieren erkennbarer Elemente als STIX-Daten können Sie zugehörige erkennbare Elemente manuell hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**an.
2. Klicken Sie auf das erkennbare Element, dem Sie ein zugehöriges erkennbares Element hinzufügen möchten.
3. Klicken Sie auf **Untergeordnete Erkennbare Elemente** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um das erkennbare Element zu suchen, das Sie mit dem aktuellen Element verknüpfen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Fügen Sie mit dem Slushbucket das erkennbare Element zu hinzu **Untergeordnete Erkennbare Elemente** Liste.
7. Klicken Sie auf **Speichern**.

Laden Sie weitere IOC-Daten

Abhängig von den Einstellungen in zwei Eigenschaften und einer Skripteinbindungsdefinition können Sie Positionsbestimmungsinformationen für IP-Adressen und Websites im Formular „erkennbare Elemente“ laden. Mit weiteren Anpassungen können Sie auch weitere Informationen hinzufügen, z. B. Ländervorwahlen, Ortsnamen.

Vorbereitungen

Die folgenden zwei Eigenschaften müssen festgelegt werden:

- **Der Domänenname zum Abrufen zusätzlicher Informationen für IP-Adressen/URLs** [sn_ti.ip_Lookup.Web_Site]
- **Der API-Schlüssel, der für die obige Domäne verwendet werden soll, falls vorhanden** [sn_ti.ip_Lookup.api_key]

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**an.
2. Klicken Sie auf die IP-Adresse oder URL des erkennbaren Elements, für das Sie weitere IOC-Daten anzeigen möchten.
   Die **Standort** Das Feld zeigt die Positionsbestimmung des IOC an.
3. Klicken Sie auf **Daten anreichern** Schaltfläche zum Laden der zusätzlichen IOC-Daten.
4. Sie können das Formular für erkennbare Elemente auch konfigurieren, um andere standortbezogene Felder hinzuzufügen, z. B. den Ländercode und den Ortscode.

Hinweis:
Um weitere standortbezogene Informationen zu laden, bearbeiten Sie **ThreatAdditionalInfo** Skripteinbindung und entsprechenden API-Schlüssel von der Website bereitstellen, der die zusätzlichen Informationen bereitstellt.

Identifizieren Sie Quellen erkennbarer Elemente

Wenn für ein erkennbares Element keine Quellen definiert sind, werden alle Arten von Quellen verwendet. Wenn Sie einem erkennbaren Element jedoch eine oder mehrere Bedrohungsquellen hinzufügen, werden die verwendeten Quellen eingeschränkt.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**an.
2. Klicken Sie auf das erkennbare Element, dem Sie Quellen erkennbarer Elemente hinzufügen möchten.
3. Klicken Sie auf **Quellen Erkennbarer Elemente** Zugehörige Liste.
4. Klicken Sie auf **Bearbeiten**.
5. Verwenden Sie bei Bedarf die Filter, um die Quelle zu suchen, die Sie dem erkennbaren Element zuordnen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Fügen Sie mit dem Slushbucket die Quelle des erkennbaren Elements zu hinzu **Quellen Erkennbarer Elemente** Liste.
7. Klicken Sie auf **Speichern**.

Führen Sie Suchen nach erkennbaren Elementen durch

Sie können Threat Intelligence-Suchen für ein oder mehrere erkennbare Elemente durchführen, um festzustellen, ob sie bekannten Sicherheitsbedrohungen zugeordnet sind. Welche Scan-Implementierungen ausgeführt werden, hängt von den von Ihnen aktivierten ab.

Vorbereitungen

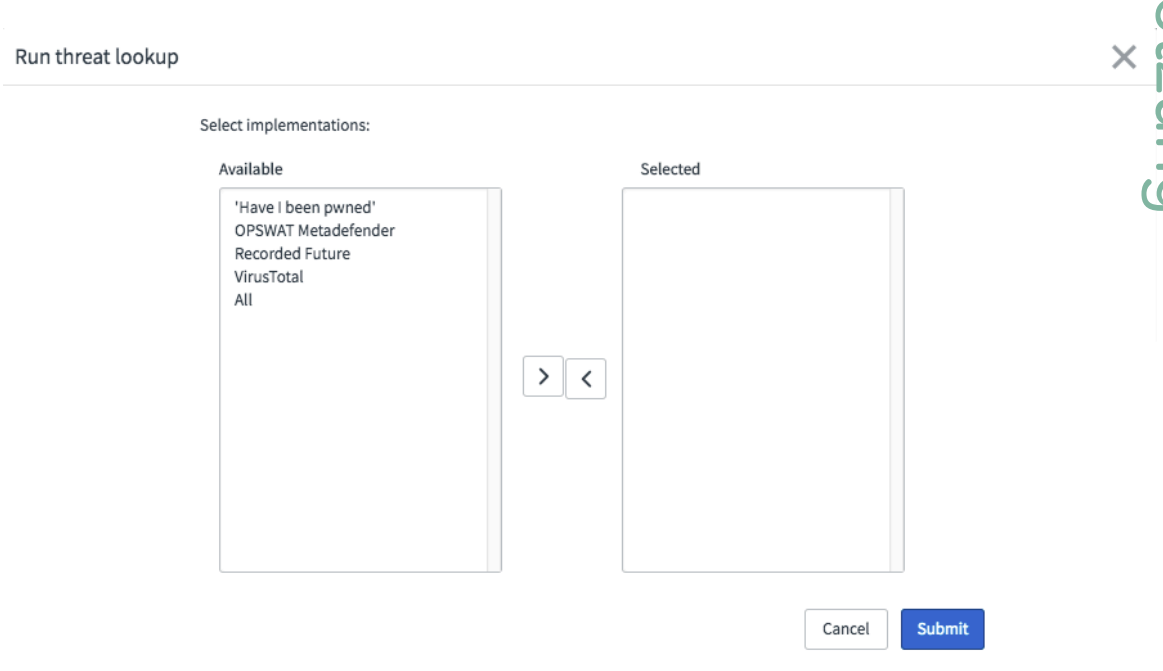
Bevor Sie Suchen durchführen können, müssen Sie das Plugin „Threat Intelligence“ aktivieren. Sie müssen das Plugin auch für eine oder mehrere der Scan-Implementierungen installieren:

- CrowdStrike Falcon Intelligence-Integration
- OPSWAT Metadefender
- Security Operations wurde ich verpfändet?
- VirusTotal

Erforderliche Rolle: sn_ti.write

Prozedur

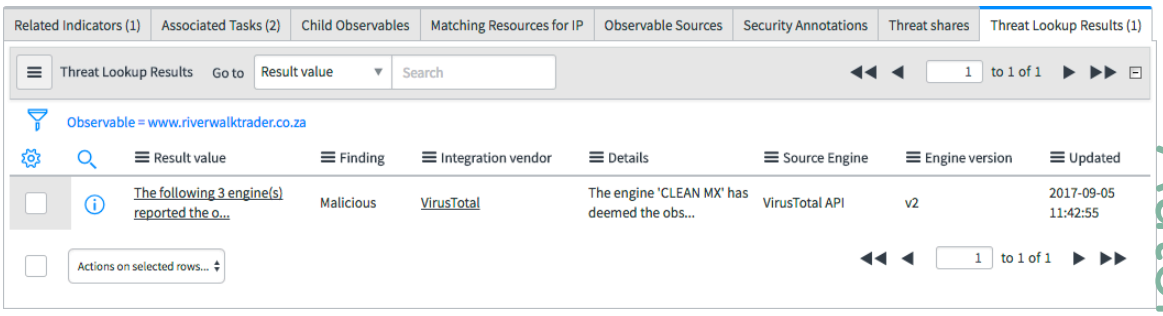
1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**an.
2. Führen Sie einen der folgenden Schritte aus:
   - Um eine Suche nach mehr als einem erkennbaren Element durchzuführen, wählen Sie die erkennbaren Elemente aus, und klicken Sie auf **Aktionen für ausgewählte Zeilen** , Und wählen Sie aus **Bedrohungssuche ausführen** .
   - Um eine Suche nach einem einzelnen erkennbaren Element durchzuführen, öffnen Sie den Datensatz des erkennbaren Elements, und klicken Sie auf **Bedrohungssuche ausführen** Zugehöriger Link.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie die Implementierungen der Bedrohungssuche aus, die Sie verwenden möchten, oder wählen Sie aus **Alle** Um Suchvorgänge mit allen aktiven Implementierungen durchzuführen, klicken Sie auf **Übermitteln** .
   Eine Meldung gibt an, dass die Bedrohungssuchen begonnen haben. Die Integration Von Security Operations: Flow Für Bedrohungssuche Führt die Implementierungs-Workflows für die von Ihnen ausgewählten Implementierungen der Bedrohungssuche aus und führt sie auch aus. Die Suchen werden durchgeführt, und die Ergebnisse werden generiert.
4. Wenn die Suchvorgänge abgeschlossen sind, können Sie auf klicken **Ergebnisse Der Bedrohungssuche** Registerkarte zum Anzeigen der Ergebnisse.



Ergebnis Der Aktuellen Bedrohungssuche : Sie können auch die neuesten oder neuesten Ergebnisse der Bedrohungssuche von jedem Integrationsanbieter anzeigen, wenn Sie auf klicken **Ergebnis Der Aktuellen Bedrohungssuche** Registerkarte.

Hinweis:
Die **Ergebnis Der Aktuellen Bedrohungssuche** Registerkarte ist nicht Teil des Basissystems.

Um diese Registerkarte zu aktivieren, gehen Sie wie folgt vor:

a. Klicken Sie mit der rechten Maustaste auf den Formularheader.

b. Navigieren zu **Konfigurieren** > **Zugehörige Listen**an.

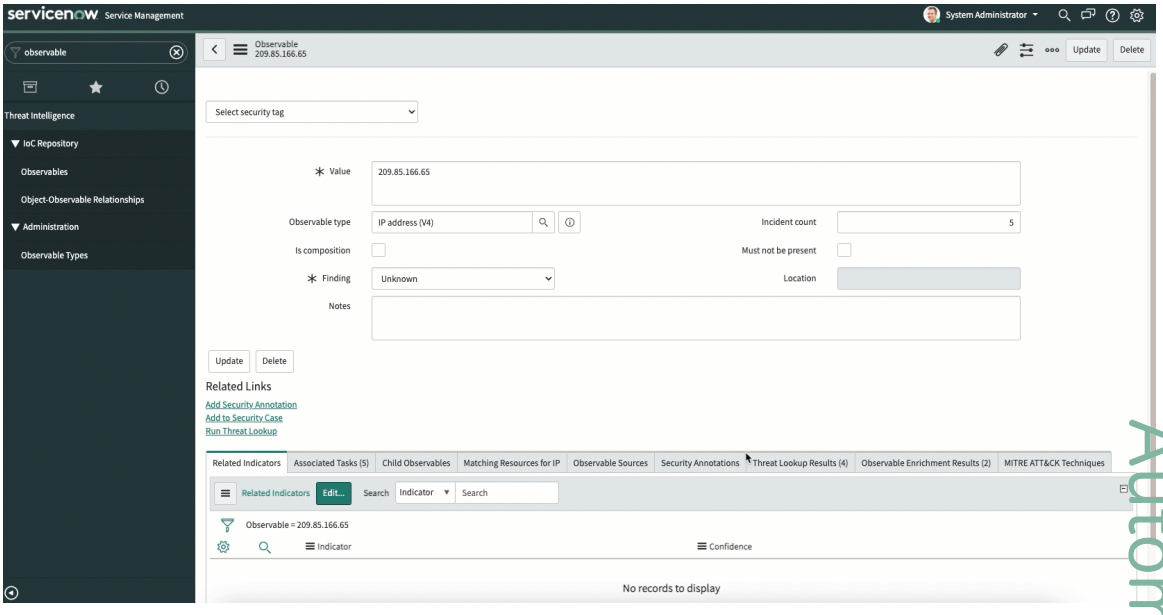
c. Suchen **Aktuelle Ergebnisse Der Bedrohungssuche** In der Liste verfügbar, und verschieben Sie sie in die Liste ausgewählt.

d. Klicken Sie auf **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

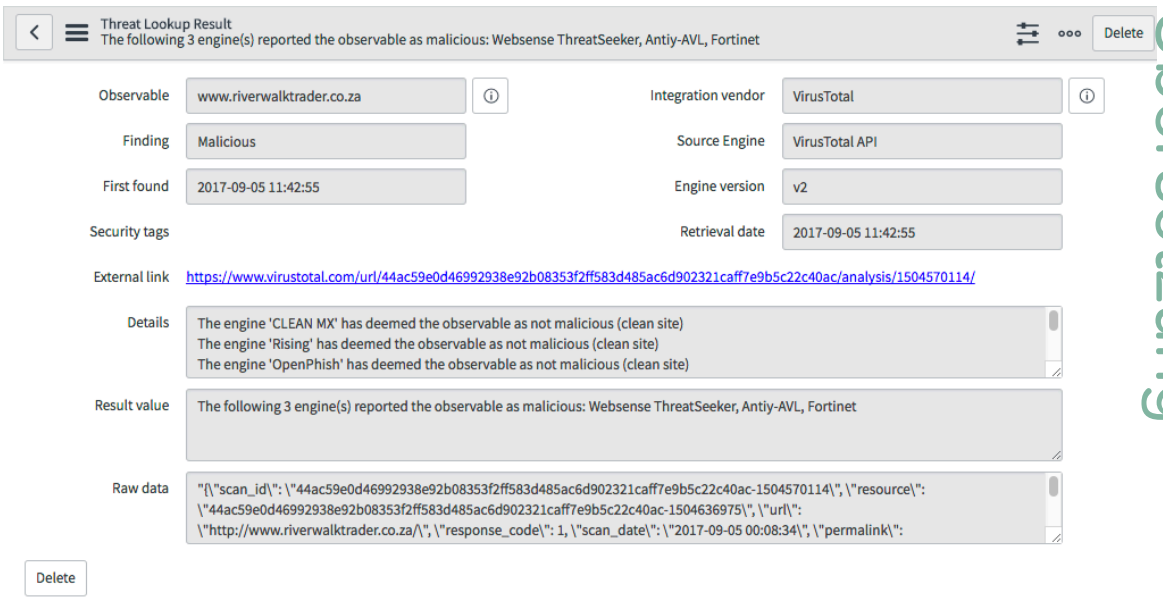
Sie können jetzt die aktuellen Ergebnisse der Bedrohungssuche von jedem Integrationsanbieter in anzeigen **Ergebnis Der Aktuellen Bedrohungssuche** Registerkarte.



5. Um zusätzliche Details anzuzeigen, einschließlich Rohergebnissen für eine bestimmte Suche, klicken Sie auf **Ergebniswert** .

Hinweis:

Wenn die Implementierungen VirusTotal oder OPSWAT Metadefender verwendet werden, werden die Details wie unten gezeigt konsolidiert.



Bedrohungsanreicherung für erkennbare Elemente durchführen

Sie können Threat Intelligence-Ergänzungen für ein oder mehrere erkennbare Elemente durchführen, um zu bestimmen, ob sie bekannten Sicherheitsbedrohungen zugeordnet sind. Welche Implementierungen ausgeführt werden, hängt von denen ab, die Sie aktiviert haben.

Vorbereitungen

Bevor Sie eine Ergänzung durchführen können, müssen Sie das Plugin „Threat Intelligence“ aktivieren. Sie müssen das Plugin auch für eine oder mehrere der Ergänzungsimplementierungen installieren:

Automatische Übersetzung

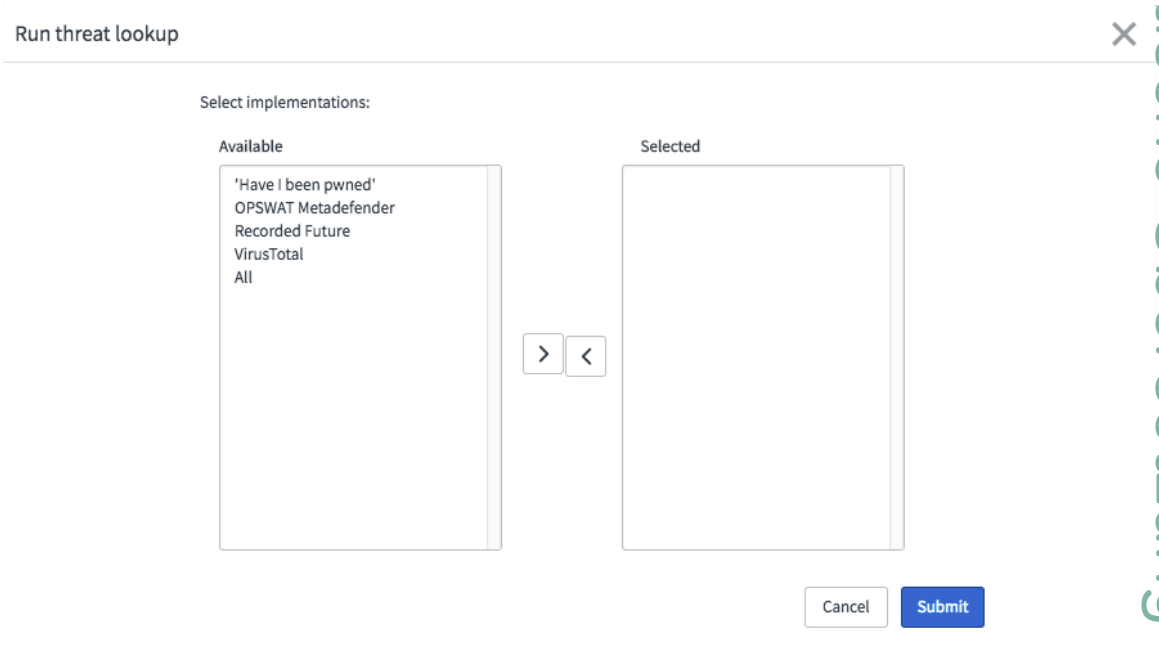
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- CrowdStrike Falcon Intelligence-Integration
- OPSWAT Metadefender
- Security Operations wurde ich verpfändet?
- VirusTotal
- WHOIS?

Erforderliche Rolle: sn_ti.admin

Prozedur

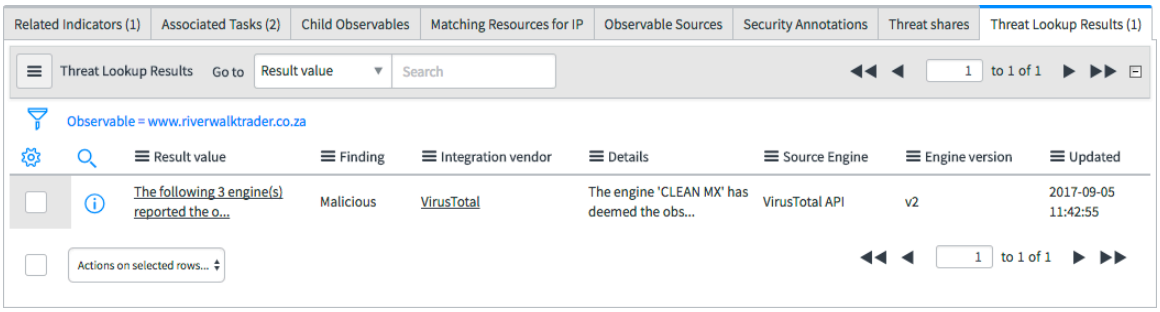
1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**an.
2. Führen Sie einen der folgenden Schritte aus:
   - Um eine Suche nach mehr als einem erkennbaren Element durchzuführen, wählen Sie die erkennbaren Elemente aus, und klicken Sie auf **Aktionen für ausgewählte Zeilen** , Und wählen Sie aus **Bedrohungssuche ausführen** .
   - Um eine Suche nach einem einzelnen erkennbaren Element durchzuführen, öffnen Sie den Datensatz des erkennbaren Elements, und klicken Sie auf **Bedrohungssuche ausführen** Zugehöriger Link.



3. Wählen Sie die Implementierungen der Bedrohungssuche aus, die Sie verwenden möchten, oder wählen Sie aus **Alle** Um Suchvorgänge mit allen aktiven Implementierungen durchzuführen, klicken Sie auf **Übermitteln** .
   Eine Meldung gibt an, dass die Bedrohungssuchen begonnen haben. Die Integration Von Security Operations: Flow Für Bedrohungssuche Führt die Implementierungs-Workflows für die von Ihnen ausgewählten Implementierungen der Bedrohungssuche aus und führt sie auch aus. Die Suchen werden durchgeführt, und die Ergebnisse werden generiert.
4. Wenn die Suchvorgänge abgeschlossen sind, können Sie auf klicken **Ergebnisse Der Bedrohungssuche** Registerkarte zum Anzeigen der Ergebnisse.

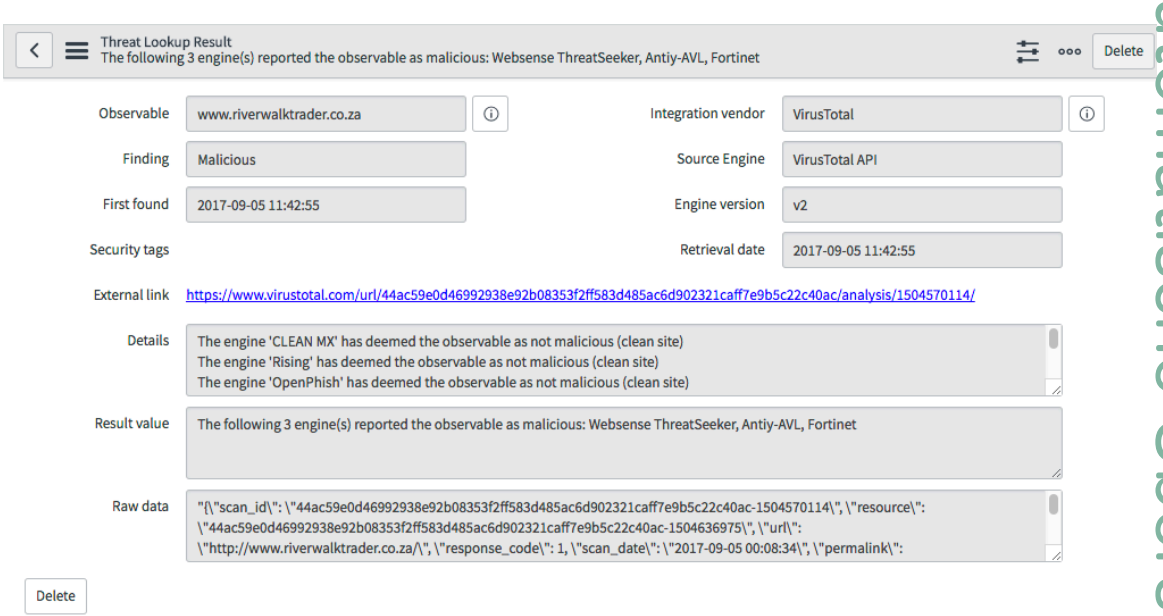
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Um zusätzliche Details anzuzeigen, einschließlich Rohergebnissen für eine bestimmte Suche, klicken Sie auf **Ergebniswert** .

Hinweis:
Wenn die Implementierungen VirusTotal oder OPSWAT Metadefender verwendet werden, werden die Details wie unten gezeigt konsolidiert.



Angriffsmuster

Angriffsmuster sind eine Art von Taktiken, Techniken und Verfahren (TTPs), die die Methoden beschreiben, mit denen Angreifer versuchen, Ziele zu gefährden. Angriffsmuster gelten für STIX 2.x.

Angriffsmuster werden verwendet, um Angriffe zu kategorisieren. Sie verallgemeinern bestimmte Angriffe auf die Muster, denen sie folgen, und stellen detaillierte Informationen zur Durchführung von Angriffen bereit.

Beispielsweise ist Spear-Phishing eine gängige Art von Angriff, bei dem ein Angreifer eine sorgfältig gestaltete E-Mail-Nachricht an eine Partei sendet, mit der Absicht, sie dazu zu bringen, auf einen Link zu klicken oder einen Anhang zu öffnen, um Malware bereitzustellen. Angriffsmuster sind spezifischer, z. B. Spear-Phishing durch einen bestimmten Bedrohungsakteur (z. B. dass das Ziel einen Wettbewerb gewonnen hat), kann auch ein Angriffsmuster sein.

Definieren Sie ein Angriffsmuster

Definieren Sie ein Angriffsmuster, um Angriffe zu kategorisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Angriffsmuster**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Angriffsmuster zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugehörige Kill Chain-Phasen	Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Vorgehensweisen	Listet die diesem Objekt zugeordneten Aktionen auf, bei denen es sich um technische oder automatisierte Antworten handelt (Patches anwenden, Firewalls neu konfigurieren), um einen Angriff zu verhindern.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Kampagnen

Eine Kampagne ist eine Gruppierung von konversationswidrigen Verhaltensweisen. Diese Verhaltensweisen beschreiben eine Reihe böswilliger Aktivitäten oder Angriffe, die im Laufe der Zeit gegen eine bestimmte Gruppe von Zielen auftreten. Kampagnen gelten für STIX 2.x.

Kampagnen haben normalerweise gut definierte Ziele und können Teil eines Angriffssatzes sein.

Kampagnen werden häufig einem Angriffssatz und Bedrohungsakteuren zugeordnet. Die Bedrohungsakteure können bekannte Infrastruktur aus dem Angriffssatz wiederverwenden oder eine neue Infrastruktur einrichten, die speziell für die Durchführung dieser Kampagne geeignet ist.

Kampagnen haben ein gemeinsames Ziel in den Incidents, die sie verursachen, für Personen oder für die von ihnen angestrebten Ressourcen und die von ihnen verwendeten Ressourcen.

Zum Beispiel greift ein Verbrechenssyndikat die Führungskräfte der ACME-Bank an. Sie greifen an, indem sie eine bestimmte Malware-Variante und neue Server verwenden, um geheime Informationen über eine bevorstehende Fusion mit einer anderen Bank zu erhalten.

Definieren Sie eine Kampagne

Definieren Sie eine Kampagne, um konversationswidriges Verhalten zu gruppieren.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Kampagnen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die der Kampagne zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Vorgehensweise

Eine Vorgehensweise ist eine Aktion, die entweder ausgeführt wird, um einen Angriff zu verhindern oder auf einen laufenden Angriff zu reagieren. Die Vorgehensweise gilt für STIX 2.x.

Der Kurs der Aktionen beschreibt technische oder automatisierte Antworten (Anwenden von Patches, Neukonfiguration von Firewalls). Es kann auch Aktionen auf höherer Ebene wie Mitarbeiterschulungen oder Richtlinienänderungen beschreiben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielsweise könnte eine Vorgehensweise zur Minderung einer Schwachstelle die Anwendung des Patch beschreiben, der sie behebt.

Definieren Sie eine Vorgehensweise

Definieren Sie eine Vorgehensweise, um einen Angriff zu verhindern oder auf einen laufenden Angriff zu reagieren.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Vorgehensweisen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Vorgehensweise zugeordnet sind.

Zugehörige Links	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identitäten

Identitäten stellen tatsächliche Einzelpersonen, Organisationen oder Gruppen (ACME, Inc.) und Klassen von Einzelpersonen, Systemen oder Gruppen (Finanzsektor) dar. Identitäten gelten für STIX 2.x.

Das Identitäts-SDO kann grundlegende Identifizierungsinformationen, Kontaktinformationen und die Sektoren erfassen, zu denen die Identität gehört. Identität stellt Ziele von Angriffen, Informationsquellen, Objekterstellern und Identitäten von Bedrohungsakteuren dar.

Definieren Sie Identitäten

Definieren Sie Identitäten, die tatsächliche Einzelpersonen, Organisationen oder Gruppen darstellen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Identitäten**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Identität zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.

Infrastruktur

Das Infrastruktur-SDO stellt eine Art von Taktiken, Techniken und Verfahren (TTPs) dar. Sie beschreiben alle Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen, die einen bestimmten Zweck eines Angriffs unterstützen sollen. Infrastruktur gilt für STIX 2.x.

Die Elemente eines Angriffs werden von anderen SDOs oder SCOs dargestellt. Das Infrastruktur-SDO stellt jedoch eine benannte Gruppe von Daten dar, die die Infrastruktur ausmachen.

Beispiele für Infrastruktur sind C2-Server, die bei einem Angriff verwendet werden, ein Gerät oder ein Server, der Teil einer Verteidigung ist, oder Datenbankserver, die von einem Angriff angegriffen werden sollen.

Definieren Sie die Infrastruktur

Definieren Sie eine Infrastruktur, bei der es sich um alle Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen handelt, die einen Zweck eines Angriffs unterstützen sollen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Infrastruktur**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen anzuzeigen. Sie können der Infrastruktur auch andere Objekte zuordnen.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugeordnete Typen	Listet Indikatortypen auf, die diesem Objekt zugeordnet sind.
Zugehörige Kill Chain-Phasen	Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind.
Zugehörige Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Beobachtete Daten	Listet beobachtete Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Angriffssatz

Ein Angriffssatz ist ein gruppierter Satz von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften. Ein Angriffssatz umfasst normalerweise eine einzelne Organisation. Angriffssatz gilt für STIX 2.x.

Ein Angriffssatz kann mehrere Kampagnen oder andere Aktivitäten erfassen. Diese Aktivitäten teilen Attribute, die auf einen allgemein bekannten oder unbekannten Bedrohungsakteur hinweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue Aktivität kann einem Angriffssatz zugeordnet werden, auch wenn die Bedrohungsakteure hinter dem Angriff nicht bekannt sind. Bedrohungsakteure können von der Unterstützung eines Angriffssatzes zur Unterstützung eines anderen wechseln oder mehrere Angriffssätze unterstützen.

Ein Angriffssatz ist das gesamte Angriffspaket und kann über einen langen Zeitraum in mehreren Kampagnen verwendet werden, um potenziell mehrere Zwecke zu erreichen.

Definieren Sie einen Angriffssatz

Definieren Sie einen Angriffssatz, der ein gruppiertes Set von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften ist.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Einführungssatz**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Angriffssatz zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugehörige Angriffsmotivationen	Listet alle sekundären Motivationen auf, die dieser Angriffssatz erreichen möchte.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Standorte

Ein Standort stellt einen geografischen Standort dar. Standorte werden hauptsächlich verwendet, um anderen SDOs Kontext zu geben. Standorte gelten für STIX 2.x.

Der Standort kann einige oder alle der folgenden Elemente enthalten: Region (Nordamerika), Bürgeranschrift (New York, USA), Breitengrad und Längengrad.

Das Standort-SDO kann sich auf eine Identität oder einen Angriffssatz beziehen, um anzuzeigen, dass sich die Identität oder der Angriffssatz an diesem Standort befindet. Sie kann sich auch auf eine Malware oder ein Angriffsmuster beziehen, um anzuzeigen, dass sich das Zielopfer an einem bestimmten Standort befindet.

Beispielsweise könnte ein Standort in einer Beziehung verwendet werden, um zu beschreiben, dass der Bourgeois Swallow-Intrusion Set aus Osteuropa stammt.

Mindestens eine der folgenden Eigenschaften oder Eigenschaftensätze muss angegeben werden:

- region
- country
- Breitengrad und Längengrad

Definieren Sie Den Standort

Definieren Sie einen geografischen Standort, um anderen SDOs mehr Kontext bereitzustellen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Standorte**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Standort zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.

Malware

Malware ist eine Art von TTP, die schädlichen Code darstellt. Bezieht sich auf ein Programm, das verdeckt in ein System eingefügt wird. Malware gilt für STIX 2.x.

Die Absicht einer Malware besteht darin, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder des Betriebssystems des Opfers zu gefährden.

Das Malware-SDO charakterisiert, identifiziert und kategorisiert Malware-Instanzen und -Familien aus Daten, die aus der Analyse abgeleitet wurden. Dieses SDO erfasst detaillierte Informationen darüber, wie die Malware funktioniert und was sie tut.

Definieren Sie eine Malware

Definieren Sie eine Malware, die schädlichen Code darstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur
1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Malware**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Malware zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugeordnete Typen	Listet Indikatortypen auf, die diesem Objekt zugeordnet sind.
Zugehörige Fähigkeiten	Listet die identifizierten und diesem Objekt zugeordneten Fähigkeiten auf.
Zugehörige Kill Chain-Phasen	Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind.
Zugehörige Malware	Listet die mit diesem Objekt identifizierte zugeordnete Malware auf.
Zugehörige Betriebssysteme	Die Betriebssysteme, auf denen das Objekt ausführbar ist. Dies gilt für virtualisierte Betriebssysteme sowie für solche, die auf Bare Metal ausgeführt werden.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Vorgehensweisen	Listet die diesem Objekt zugeordneten Aktionen auf, bei denen es sich um technische oder automatisierte Antworten handelt (Patches anwenden, Firewalls neu konfigurieren), um einen Angriff zu verhindern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware-Analyse	Listet Malware-Analysedatensätze auf, die diesem Objekt zugeordnet sind.
Gemeldete erkennbare Elemente	Listet erkennbare Elemente auf, die als Teil dieses Objekts gemeldet werden.
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Malware-Analyse

Malware-Analyse erfasst die Metadaten und Ergebnisse einer Malware. Malware-Analyse gilt für STIX 2.x.

Malware-Analyse umfasst statische oder dynamische Analysen, die für eine Malware-Instanz oder -Familie durchgeführt werden.

Definieren Sie die Malware-Analyse

Definieren Sie eine Malware-Analyse, die die Metadaten und Ergebnisse einer bestimmten statischen oder dynamischen Analyse erfasst, die für eine Malware-Instanz oder -Familie durchgeführt wird.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Malware-Analyse**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu den Objekten anzuzeigen, die der Malware-Analyse zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugehörige Malware	Listet die mit diesem Objekt identifizierte zugeordnete Malware auf.
Gemeldete erkennbare Elemente	Listet erkennbare Elemente auf, die als Teil dieses Objekts gemeldet werden.
Installierte Software	Listet alle nicht standardmäßigen Software auf, die auf dem Betriebssystem installiert ist, das für die dynamische Analyse der Malware-Instanz oder -Familie verwendet wird.

Beobachtete Daten

Beobachtete Daten übermitteln Informationen über Entitäten im Zusammenhang mit der Cybersicherheit, z. B. Dateien, Systeme und Netzwerke, die STIX Cyber-Observable Objects (SCOs) verwenden. Beobachtete Daten gelten für STIX 2.x.

Beobachtete Daten erfassen sowohl eine einzelne Beobachtung einer einzelnen Entität (Datei, Netzwerkverbindung) als auch die Zusammenfassung mehrerer Beobachtungen einer Entität.

Sie können beobachtete Daten selbst (ohne Beziehungen) verwenden, um Rohdaten zu übermitteln, die aus einer beliebigen Quelle erfasst wurden. Quellen umfassen Analystenberichte, Sandboxen sowie Netzwerk- und hostbasierte Erkennungstools.

Beispielsweise können beobachtete Daten Informationen zu einer IP-Adresse, einer Netzwerkverbindung, einer Datei oder einem Registrierungsschlüssel erfassen. Beobachtete Daten sind keine Intelligence Assertion, es handelt sich einfach um Rohinformationen ohne Kontext für das, was sie bedeuten.

Beobachtete Daten definieren

Definieren Sie beobachtete Daten, die Informationen über Cyber-sicherheitsbezogene Entitäten wie Dateien, Systeme und Netzwerke mithilfe von STIX Cyber-Observable Objects (SCOs) übermitteln.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Beobachtete Daten**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den beobachteten Daten zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.

Bedrohungsakteure

Bedrohungsakteure sind Einzelpersonen, Gruppen oder Organisationen, die mit böswilliger Absicht handeln. Bedrohungsakteure gelten für STIX 2.x.

Ein Bedrohungsakteur ist kein Angriffssatz, kann jedoch im Laufe der Zeit verschiedene Angriffssätze, Gruppen oder Organisationen unterstützen oder ihnen zugeordnet sein.

Bedrohungsakteure verwenden ihre Ressourcen und die Ressourcen eines Angriffssatzes, um Angriffe durchzuführen und Kampagnen für Ziele auszuführen.

Sie können Bedrohungsakteure anhand ihrer Motive, Fähigkeiten, Ziele, Raffinesse-Ebene, vergangener Aktivitäten, Ressourcen, auf die sie Zugriff haben, und ihre Rolle in der Organisation.

Definieren Sie Bedrohungsakteure

Definieren Sie Bedrohungsakteure, die Einzelpersonen, Gruppen oder Organisationen sind, die mit böswilliger Absicht handeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsakteure**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Bedrohungsakteur zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugeordnete Typen	Listet Indikatortypen auf, die diesem Objekt zugeordnet sind.
Zugeordnete Rollen	Listet die dem Bedrohungsakteur zugeordneten Rollen auf.
Zugehörige Angriffsmotivationen	Listet die dem Bedrohungsakteur zugeordneten Angriffsmotivationen auf.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Bedrohungsgruppierungen

Ein Bedrohungsgruppierungsobjekt bestätigt explizit, dass die referenzierten STIX-Objekte einen gemeinsam genutzten Kontext haben. Bedrohungsgruppierungen gelten für STIX 2.x.

Ein Bedrohungsgruppierungsobjekt stellt einen Satz von Daten dar, die bei ausreichender Analyse ausgereift sind, um einen Incident oder Bedrohungsbericht als STIX-Berichtsobjekt zu übermitteln. Beispielsweise kann eine Gruppierung verwendet werden, um eine laufende Untersuchung eines Sicherheitsereignisses oder Incidents zu charakterisieren.

Ein Bedrohungsgruppierungsobjekt kann auch verwendet werden, um zu bestätigen, dass die referenzierten STIX-Objekte mit einem laufenden Analyseprozess verknüpft sind. Beispielsweise kann ein Bedrohungsanalyst mit anderen in seiner Vertrauensgemeinschaft zusammenarbeiten, um eine Reihe von Kampagnen und Indikatoren zu untersuchen.

Das Bedrohungsgruppierungs-SDO enthält eine Liste von Verweisen auf SDOs, SCOs und SROs, zusammen mit einer expliziten Angabe des vom Inhalt freigegebenen Kontexts, einer Textbeschreibung und dem Namen der Gruppierung.

Definieren Sie Bedrohungsgruppierungen

Definieren Sie Bedrohungsgruppierungen als Objekte mit einem gemeinsam genutzten Kontext.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsgruppierungen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Bedrohungsgruppierung zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Gruppierte Objekte	Listet Objekte auf, die als Teil der Bedrohungsgruppierung gruppiert sind.
Gruppierte Indikatoren	Listet Indikatoren auf, die als Teil der Bedrohungsgruppierung gruppiert sind.
Gruppierte erkennbare Elemente	Listet erkennbare Elemente auf, die als Teil der Bedrohungsgruppierung gruppiert sind.

Markierungsdefinitionen

Das Markierungsdefinitionsobjekt stellt eine bestimmte Markierung dar.

Datenmarkierungen stellen Einschränkungen, Berechtigungen und andere Anleitungen dar, wie Daten verwendet und freigegeben werden können.

Beispielsweise können Daten mit der Einschränkung freigegeben werden, dass sie nicht erneut freigegeben werden dürfen oder dass sie im Ruhezustand verschlüsselt werden müssen.

In STIX werden Datenmarkierungen mithilfe des Markierungsdefinitionsobjekts angegeben. Diese Definitionen werden auf STIX-Objekte mithilfe von Objektmarkierungen und auf einzelne Eigenschaften von STIX-Objekten über granulare Markierungen angewendet.

Definieren Sie Markierungsdefinitionen

Definieren Sie Markierungsdefinitionen, die eine bestimmte Datenmarkierung darstellen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Markierungsdefinitionen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Markierungsdefinition zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
	„Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Markierte Objekte	Listen von Objekten, die mit der Markierungsdefinition markiert sind.
Markierte Indikatoren	Listen von Indikatoren, die mit der Markierungsdefinition markiert sind.

Bedrohungshinweise

Eine Bedrohungshinweis übermittelt informativen Text, um zusätzliche Analysen bereitzustellen, die nicht in den STIX-Objekten, Markierungsdefinitionsobjekten oder Sprachinhaltsobjekten enthalten sind, auf die sich der Hinweis bezieht. Bedrohungshinweise gelten für STIX 2.x.

Beispielsweise kann ein Analyst einem Kampagnenobjekt, das von einer anderen Organisation erstellt wurde, eine Notiz hinzufügen. Der Hinweis kann darauf hinweisen, dass er Posts im Zusammenhang mit dieser Kampagne in einem Hacker-Forum gesehen hat.

Notizen werden normalerweise von menschlichen Analysten erstellt und bestehen aus menschlichem Text. Sie enthalten eine zusätzliche Eigenschaft, um den Autor zu erfassen, der die Notiz erstellt hat.

Definieren Sie Bedrohungshinweise

Definieren Sie Bedrohungshinweise, die Informationen übermitteln, um weiteren Kontext oder Analysen bereitzustellen, die in vorhandenen Objekten nicht verfügbar sind.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungshinweise**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den Bedrohungshinweisen zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Zugehörige Objekte	Listen von Objekten, für die die Bedrohungshinweise gelten.
Zugehörige Indikatoren	Listen von Indikatoren, für die die Bedrohungshinweise gelten.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind.

Bedrohungsmeinungen

Eine Meinung ist eine Bewertung der Genauigkeit der Informationen in einem STIX-Objekt, das von einer anderen Entität erstellt wurde. Bedrohungsmeinungen gelten für STIX 2.x.

Die Eigenschaft „Meinung“ erfasst die Ebene der Zustimmung oder Meinungsverschiedenheit mithilfe einer festen Skala. Die feste Skala unterstützt auch eine numerische Zuordnung, um konsistente statistische Vorgänge über Meinungen hinweg zu ermöglichen.

Beispielsweise kann ein Analyst aus einer verbrauchenden Organisation sagen, dass er einem Kampagnenobjekt „überhaupt nicht zustimmt“, und eine Erklärung dazu geben.

Meinungen sind subjektiv, und in der Spezifikation wird nicht angegeben, wie sie am besten zu interpretieren sind.

Menschliche Analysten erstellen Meinungen und bestehen aus menschlich orientiertem Text. Sie enthalten eine zusätzliche Eigenschaft, um den Autor zu erfassen, der die Meinung erstellt hat.

Definieren Sie Bedrohungsmeinungen

Definieren Sie Bedrohungsmeinungen als Bewertung der Genauigkeit der Informationen in einem STIX-Objekt.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsmeinungen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Bedrohungsmeinung zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
	„Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Zugehörige Objekte	Liste der Objekte, für die die Bedrohungsmeinung gilt.
Zugehörige Indikatoren	Liste der Indikatoren, für die die Bedrohungsmeinung gilt.
Zugehörige erkennbare Elemente	Listet erkennbare Elemente auf, die diesem Objekt zugeordnet sind.

Bedrohungsberichte

Bedrohungsberichte sind Sammlungen von Threat Intelligence, die sich auf ein oder mehrere Themen konzentrieren. Bedrohungsberichte gelten für STIX 2.x.

Bedrohungsberichte enthalten eine Beschreibung eines Bedrohungsakteurs, Malware und Angriffstechnik, einschließlich Kontext und zugehörigen Details. Sie werden verwendet, um zugehörige Bedrohungsinformationen zusammenzufassen, damit sie als umfassende Cyberbedrohungsstory veröffentlicht werden können.

Das Bedrohungsbericht-SDO enthält eine Liste von Verweisen auf STIX-Objekte zusammen mit einer Textbeschreibung und dem Namen des Berichts.

Definieren Sie Bedrohungsberichte

Definieren Sie Bedrohungsberichte, die einen Bedrohungsakteur, Malware und Angriffstechnik beschreiben, einschließlich Kontext und zugehörige Details.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Bedrohungsberichte**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den Bedrohungsberichten zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Zugeordnete Typen	Listet Indikatortypen auf, die diesem Objekt zugeordnet sind.
Gemeldete Objekte	Liste der im Bedrohungsbericht gemeldeten Objekte.
Gemeldete Indikatoren	Listen der im Bedrohungsbericht gemeldeten Indikatoren.
Gemeldete erkennbare Elemente	Listen der im Bedrohungsbericht gemeldeten erkennbaren Elemente.

Sichtungen

Sichtungen geben an, dass ein Indikator oder Objekt gesehen wurde. Objekte können Malware, Tool, Bedrohungsakteur usw. sein.

Sichtungen verfolgen, wer und was das Ziel ist, wie Angriffe ausgeführt werden, und um Trends im Angriffsverhalten nachzuverfolgen.

Das Sichtungsbeziehungsobjekt enthält zusätzliche Eigenschaften, die nicht in den generischen Beziehungsobjekten vorhanden sind. Diese zusätzlichen Eigenschaften stellen Daten dar, die für Sichtungsbeziehungen spezifisch sind.

Zum Beispiel eine Anzahl oder die angibt, wie oft etwas gesehen wurde.

Die Sichtung wird als Beziehung erfasst, da Sie keine Sichtung haben können, es sei denn, Sie haben etwas, das gesichtet wurde.

- Was gesichtet wurde, z. B. Malware, Kampagne oder anderes SDO
- Wer sie gesehen hat und/oder wo sie gesichtet wurde, dargestellt als Identität
- Was in Systemen und Netzwerken gesehen wurde, dargestellt als beobachtete Daten

Definieren Sie Indikatorsichtungen

Definieren Sie Sichtungen, die angeben, dass ein Indikator gesehen wurde.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Indikatorsichtungen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Indikatorsichtung zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Listen	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet beobachtete Daten auf, die diesem Objekt zugeordnet sind.

Objektsichtungen definieren

Definieren Sie die Objektsichtung, die beschreibt, dass ein Objekt (Malware, Tool, Bedrohungsakteur usw.) gesehen wurde.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objektsichtungen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Objektsichtung zugeordnet sind.

Zugehörige Listen	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Beobachtete Daten	Listet beobachtete Daten auf, die diesem Objekt zugeordnet sind.

Tools

Tools sind legitime Software, die von Bedrohungsakteuren zum Ausführen von Angriffen verwendet wird. Tools gelten für STIX 2.x.

Mit Tools können Sie wissen, wie und wann Bedrohungsakteure sie für die Ausführung von Kampagnen verwenden. Im Gegensatz zu Malware werden diese Tools oder Softwarepakete häufig auf einem System gefunden und haben legitime Zwecke für Poweruser, Administratoren, Netzwerkadministratoren oder sogar normale Anwender.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielsweise sind Remote Access Tools (RDP) und Network Scan Tools (Nmap) Tools, die ein Bedrohungsakteur während eines Angriffs verwendet.

Definieren Sie Tools

Definieren Sie Tools als legitime Software, die zum Ausführen von Angriffen verwendet wird.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Tools**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Toolobjekt zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Zugehörige Kill Chain-Phasen	Listet Kill Chain-Phasen auf, die diesem Objekt zugeordnet sind.
Zugeordnete Typen	Listet Indikatortypen auf, die diesem Objekt zugeordnet sind.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Vorgehensweisen	Listet die diesem Objekt zugeordneten Aktionen auf, bei denen es sich um technische oder automatisierte Antworten handelt (Patches anwenden, Firewalls neu konfigurieren), um einen Angriff zu verhindern.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.

Schwachstellen

Eine Schwachstelle ist eine Schwachstelle oder ein Fehler in einer Software- oder Hardwarekomponente, die Angreifer ausnutzen. Schwachstellen gelten für STIX 2.x.

Die Schwachstelle oder der Fehler liegt in den Anforderungen, Designs oder Implementierungen des Codes in einer Software- oder Hardwarekomponente. Diese Schwachstelle wird direkt ausgenutzt, um die Vertraulichkeit, Integrität oder Verfügbarkeit dieses Systems negativ zu beeinflussen.

CVE ist eine Liste von Informationssicherheitsschwachstellen und -Risiken, die allgemeine Namen für öffentlich bekannte Probleme [CVE] bereitstellt.

Wenn beispielsweise eine Malware CVE-2015-12345 ausnutzt, kann ein Malware-Objekt mit einem Schwachstellenobjekt verknüpft werden, das auf CVE-2015-12345 verweist.

Definieren Sie Schwachstellen

Definieren Sie Schwachstelle als Schwachstelle oder Fehler in einer Software- oder Hardwarekomponente, die Angreifer ausnutzen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Schwachstellen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Schwachstellenobjekt zugeordnet sind.

Zugehörige Links und zugehörige Listen	Beschreibung
Beziehungen anzeigen	Öffnet die STIX-Visualisierung, in der Sie die Beziehung des STIX-Objekts anzeigen können. „Beziehungen anzeigen“ wird nur angezeigt, wenn dem Objekt ein Objekt zugeordnet ist.
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Vorgehensweisen	Listet die diesem Objekt zugeordneten Aktionen auf, bei denen es sich um technische oder automatisierte Antworten handelt (Patches anwenden, Firewalls neu konfigurieren), um einen Angriff zu verhindern.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.

Automatische Übersetzung

Beziehungen

Verwenden Sie die Beziehungsobjekte, um zwei SDOs oder STIX Cyber-Observable Objects (SCOs) miteinander zu verknüpfen, um zu beschreiben, wie sie zueinander in Beziehung stehen.

STIX-Beziehungsobjekte (SROs) stellen Arten von Beziehungen zwischen verschiedenen STIX-Objekten dar. Die folgenden Beziehungsobjekte sind verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Objekt-Objekt-Beziehung** : Dieses Objekt definiert Beziehungen zwischen SDOs mit Ausnahme des Indikatorobjekts. Ein Beispiel für eine von Objekt zu Objekt definierte Beziehung ist, dass ein Angriffsmuster eine Malware bereitstellt.
- **Objekt-Indikator-Beziehung** : Dieses Objekt definiert Beziehungen zwischen dem Indikatorobjekt und anderen SDOs. Ein Beispiel für eine definierte Objekt-Indikator-Beziehung besteht darin, dass ein Indikator Beweise für eine Kampagne erkennt.
- **Beziehung Zwischen Objekt Und Erkennbarem Element** : Dieses Objekt definiert Beziehungen zwischen SDOs und dem erkennbaren Objekt (SCO). Ein Beispiel für eine definierte Beziehung zwischen Objekt und erkennbarem Element ist, dass eine Infrastruktur aus Cyber-Objekten besteht, die Informationen zu einem potenziellen Angriff bereitstellen.

STIX-Objektbeziehungen

Beziehungsobjekt	Beispielquelle	Beispielziel	Beispielbeschreibung
Objekt-Objekt-Beziehungen	Angriffsmuster	Malware	Diese Beziehung beschreibt, dass dieses Angriffsmuster zur Bereitstellung dieser Malware-Instanz (oder -Familie) verwendet wird.
Objekt-Indikator-Beziehungen	Indikator	Angriffsmuster, Kampagne, Infrastruktur, Angriffssatz, Malware, Bedrohungsakteur, Tool	Diese Beziehung beschreibt, dass der Indikator Nachweise für das zugehörige Angriffsmuster, die Kampagne, die Infrastruktur, den Angriffssatz, die Malware erkennen kann, Bedrohungsakteur oder Tool. Der Nachweis ist möglicherweise nicht direkt. Beispielsweise kann der Indikator sekundäre Nachweise der Kampagne erkennen, z. B. Malware, die häufig von dieser bestimmten Kampagne verwendet wird.
Objekt-Erkennbares Element-Beziehungen	Infrastruktur	Beobachtete Daten	Diese Beziehung beschreibt, dass der Indikator basierend auf Informationen aus einem beobachteten Datenobjekt erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

STIX-Objektbeziehungen (Fortsetzung)

Beziehungsobjekt	Beispielquelle	Beispielziel	Beispielbeschreibung
			Ein Beispiel für eine definierte Beziehung zwischen Objekt und erkennbarem Element ist, dass eine Infrastruktur aus Cyber-Objekten besteht, die Informationen zu einem potenziellen Angriff bereitstellen.

Definieren Sie Objekt-Objekt-Beziehungen

Definieren Sie Beziehungen zwischen SDOs mit Ausnahme des Indikatorobjekts.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objekt-Objekt-Beziehungen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Definieren Sie Objekt-Indikator-Beziehungen

Definieren Sie Beziehungen zwischen dem Indikatorobjekt und anderen SDOs.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objekt-Indikator-Beziehungen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

Definieren Sie Beziehungen zwischen Objekt und erkennbaren Elementen

Definieren Sie Beziehungen zwischen SDOs und dem erkennbaren Objekt (SCO).

Vorbereitungen
Erforderliche Rolle: sn_ti.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **IoC-Repository** > **Objekt-Erkennbares-Beziehungen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.
4. Klicken Sie auf **Absenden**.

STIX-Visualisierung

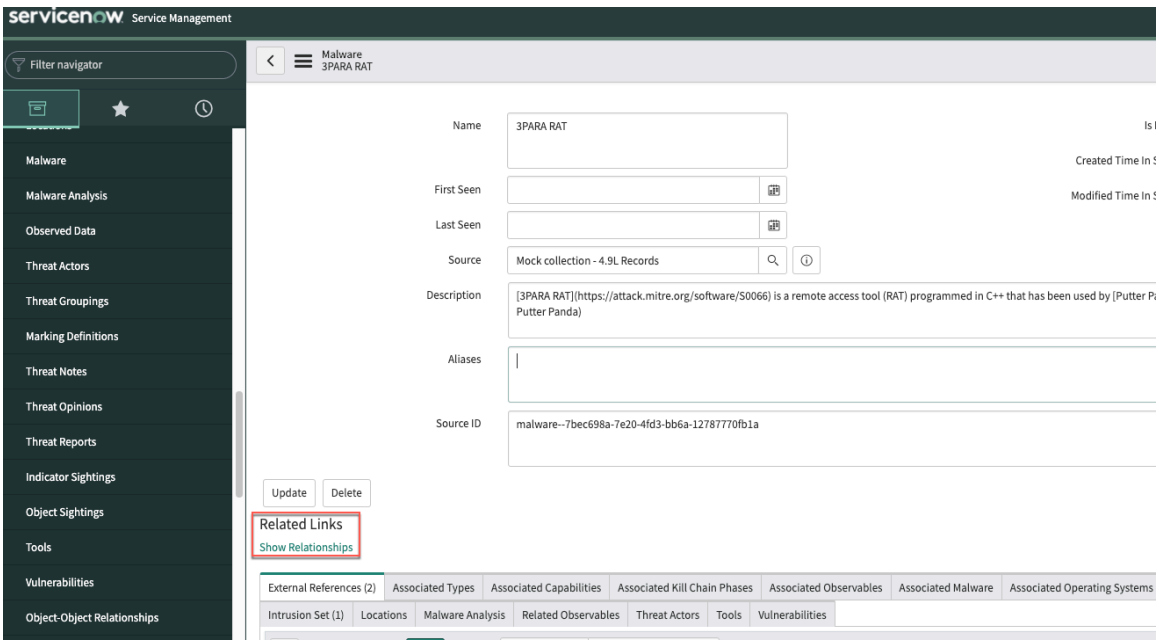
Die STIX-Visualisierung stellt die Struktur des STIX-Objekts und seine Beziehung visuell dar.

Weitere Informationen zum ausgewählten Objekt oder zur ausgewählten Beziehung finden Sie im Detailbereich.

Das Beziehungsdiagramm zeigt die Beziehungen für ein Objekt an und bietet Kontext, den Sie untersuchen können. Sie können auf einen beliebigen Knoten im Diagramm klicken, um weitere Details anzuzeigen.

Hinweis:
Die STIX-Visualisierung ist für alle SDOs mit Ausnahme der Objekte „Bericht“ und „beobachtete Daten“ verfügbar.

Greifen Sie auf STIX Visualizer zu

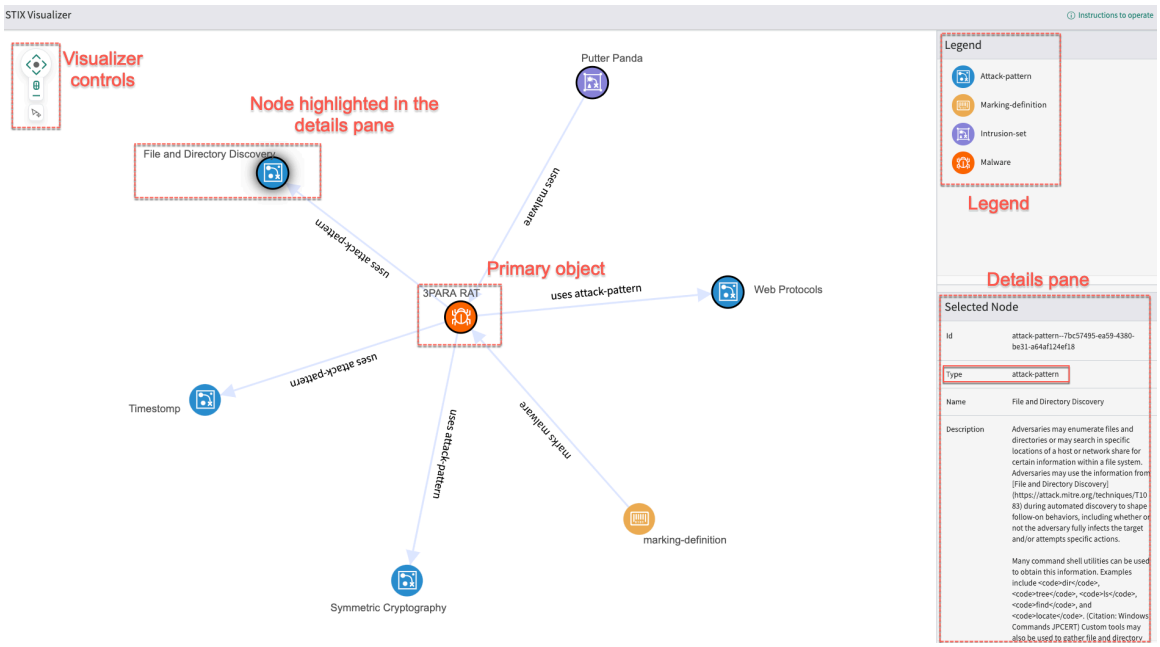


Klicken Sie Auf Beziehungen Anzeigen Im Abschnitt „zugehörige Links“ für einen der SDOs zum Anzeigen der STIX-Visualisierung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Details in STIX Visualizer an



In der Visualisierung können Sie das Objekt und seine Beziehung anzeigen, die Kontext zur weiteren Untersuchung bietet. Die Visualisierung verwendet Farben und Symbole, um verschiedene Informationen zu den Objekten zu veranschaulichen.

Sie können ein Objekt vergrößern, die Knoten ziehen oder anheften, um sich auf eine bestimmte Beziehung zu konzentrieren.

Klicken Sie auf ein beliebiges Objekt, um den Detailbereich zu öffnen. Im Detailbereich finden Sie weitere Informationen, die dem Objekt zugeordnet sind.

MITRE-ATT&CK™ Framework-Übersicht

Die MITRE-ATT&CK Framework ist eine Knowledge Base mit allgemeinen Taktiken, Techniken und Verfahren (TTP), auf die Ihre Organisation zugreifen kann, um spezifische Bedrohungsmodelle und -Methoden gegen Cyberangriffe zu entwickeln.

Übersicht

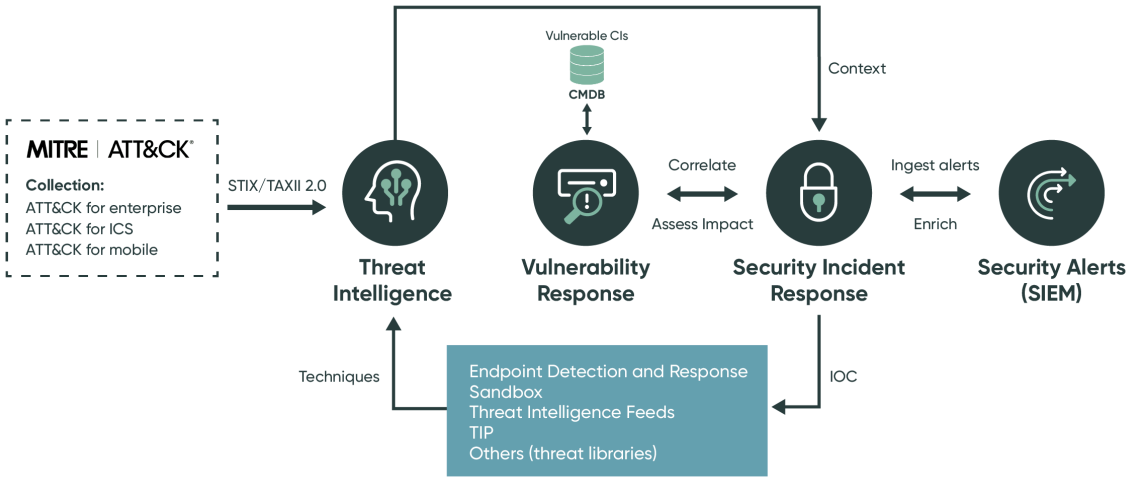
Die MITRE Das Framework für Angreifertaktiken, Techniken und Common Knowledge (ATT&CK) dokumentiert und verfolgt verschiedene Angreifertechniken, die in verschiedenen Phasen eines Cyberangriffs verwendet werden.

Mithilfe von MITRE-ATT&CK Die Knowledge Base des Frameworks, die Community für Cyberbedrohungsinformationen, kann Bedrohungen schnell identifizieren und Antworten auf Cyberangriffe koordinieren.

MITRE-ATT&CK Und Security Operations

Im folgenden Diagramm finden Sie Informationen dazu MITRE-ATT&CK Informations-Flows mit Security Operations Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Die zugehörigen Listen namens Vorab geladen TAXII Client Stellt eine Verbindung mit her TAXII Server zum Erfassen von Datensammlungen Bis Threat Intelligence.
- Vorhanden SIEM-Integrationen (Security Information and Event Manager) Erfassen Sie ihre Bedrohungsdaten (Warnungen und Ereignisse) mit relevanten TTPs und sind Ist Security Incidents zugeordnet .
- Wenn IOC ist einem Security Incident zugeordnet , Threat Intelligence Sucht automatisch Bedrohungsfeeds nach relevanten Informationen und sendet IoCs an Drittparteiquellen wie EDR, Sandbox oder TIP zur zusätzlichen Analyse.
- Wenn eine Drittparteiquelle enthält MITRE-ATT&CK Dann Informationen Threat Intelligence Extrahiert die Technikinformationen Und reichert die Daten in an Threat Intelligence Repository für Korrelation und Analyse.
- MITRE-ATT&CK Gibt auch frei CVE-Kontextinformationen Für jede Technik. Ihr Sicherheitsteam kann die ausgenutzten Techniken in überprüfen Vulnerability Response Um festzustellen, ob Ihre geschäftskritischen Assets bedroht sind.

MITRE-ATT&CK Matrizen, Taktiken und Techniken

Der Kern von MITRE-ATT&CK Framework ist eine Matrix von Angreifertaktiken und -Techniken. Die Sequenz der Taktiken stellt dar, was ein Angreifer in der Phase eines Incident zu erreichen versucht. Wenn Ihr Sicherheitsteam diese Sequenz versteht, haben Sie die Möglichkeit, den nächsten Schritt eines Angreifers zu antizipieren und die Kill Chain zu durchbrechen. ATT&CK besteht aus den folgenden Matrizen:

- Enterprise ATT&CK: Beschreibt das Verhalten und die Aktionen, die ein Angreifer ergreift, um in einem Unternehmensnetzwerk und einer Cloud zu kompromittieren und zu arbeiten.

> **Hinweis:**
> Die Matrix vor ATT&CK wurde von veraltet MITRE Und wird mit der Enterprise-Matrix zusammengeführt.

- ICs ATT&CK: Beschreibt die Aktionen, die ein Angreifer beim Betrieb in einem ICs-Netzwerk (Industrial Control Systems) ausführt.
- Mobile ATT&CK: Beschreibt das Verhalten und die Aktionen von Angreifern, die sich auf Mobilgeräte konzentrieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Taktiken stellen den Grund für eine ATT&CK-Technik dar. Dies ist das taktische Ziel des Angreifers zum Ausführen einer Aktion.

Techniken stellen dar, wie ein Angreifer durch die Ausführung einer Aktion ein taktisches Ziel erreicht.

Techniken können mehreren Taktiken zugeordnet sein. Beispielsweise wird die Manipulation von Zugriffstoken von einem Angreifer verwendet, um entweder die Taktik der Berechtigungseskalation oder der Abwehrumgehung zu erreichen.

Verwendung eines absichtsbasierten Ansatzes für Incident-Antworten

Eine absichtsbasierte Antwort verwendet ein dynamisches und kontextbezogenes Kill Chain-Framework, das Ihrer Organisation helfen kann, Security Incidents zu korrelieren und einen großen Umfang von Angriffen zu identifizieren. Ihr Sicherheitsteam kann eine absichtsbasierte Antwort verwenden, um zu verstehen, wie die Organisation angegriffen wird und was der Angreifer als Nächstes tun könnte. Mit dieser Art von Antwort können Sie das Verhalten eines Angreifers vorhersagen, damit Sie Ihre Ressourcen effektiv fokussieren können.

Verwenden Security Incident Response, Ihr Sicherheitsteam kann den Lebenszyklus jedes Security Incidents von der Analyse bis zur Eindämmung verwalten, indem Sie sich auf Indikatoren für Kompromittierung (IOCs) wie IP-Adressen, Datei-Hashes und Domänen konzentrieren.

Durch Integration Security Incident Response Mit MITRE-ATT&CK Framework, Security Incidents werden bei einem größeren unternehmensweiten Angriff als Links behandelt.

Wie Ihre Organisation davon profitieren kann MITRE-ATT&CK In Security Operations

Mit MITRE-ATT&CK Framework kann Ihrer Organisation bei Folgendem helfen:

- Statten Sie Sicherheitsanalysten mit aus MITRE-ATT&CK Taktiken, Techniken und Verfahren (TTPs), um Security Incidents besser zu analysieren und darauf zu reagieren.
- Automatisieren Sie die Incident-Workflows mithilfe des Playbooks, um Bedrohungen im Kontext von zu erkennen und einzudämmen MITRE-ATT&CK Framework.
- Priorisieren Sie Indikatoren für Kompromittierung und Bedrohungssuche mit MITRE-ATT&CK Informationen.
- Machen Sie sich mit der allgemeinen Sicherheitslage Ihrer Organisation im Kontext von vertraut MITRE-ATT&CK Framework.

MITRE-ATT&CK – Administration

Sie können Datenquellen einrichten, zuordnen, die Gesamterkennungsabdeckung für Technik zuordnen und verwalten MITRE-ATT&CK Repository in ServiceNow AI Platform.

Erste Schritte mit MITRE-ATT&CK Framework

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihres beginnen MITRE-ATT&CK Framework.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform, Threat Intelligence, Und Security Incident Response Rollen.	Die folgenden Rollen werden im verwendet MITRE-ATT&CK Funktionen: • Der Administrator (Administrator) installiert die -Anwendungen aus dem ServiceNow Store Und weist die Rollen Security Incident-Administrator (sn_si.admin) und Threat Intelligence-Administrator (sn_ti.admin) zu. • sn_ti.admin • sn_si.admin • sn_si.analyst • sn_ti.read • sn_ti.schreiben • sn_ti.Mitre_Analyst: Die Rolle „MITRE-Analyst“ wurde eingeführt, um die Quernavigation für zu ermöglichen MITRE Funktionen zwischen Security Incident Response Und Threat Intelligence-Support Common. Mit dieser Rolle können Sie beide anzeigen Threat Intelligence MITRE Modul und Security Incident Response Modul im schreibgeschützten Modus. • sn_si.read Weitere Informationen finden Sie unter Richten Sie Threat Intelligence Ein .
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung von erforderlich sind MITRE-ATT&CK Module sind installiert und aktiviert.	Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. • Unterstützung von Threat Intelligence – Allgemeine UI-Komponenten (sn_ti_seismic) – Version 1,0 oder höher • Threat Intelligence-Support – Allgemein – Version 12,0 oder höher • Threat Intelligence – Version 12,0 oder höher • Security Incident Response – Version 12,0 oder höher Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	für die Integration finden Sie unter Ruft die Berechtigung für ein Security Operations-Produkt ab Oder Anwendung und Aktivieren Sie eine ServiceNow Store-Anwendung .
Domänentrennung	Verifizieren Sie Abschnitt „Domänentrennung“ Wenn Sie Daten, Prozesse und Verwaltungsaufgaben trennen möchten.

Verstehen Sie sich mit MITRE Bis STIX Datenmodell

Überprüfen Sie die von verwendete Terminologie MITRE Und STIX Um effizient zu verwenden und zu verstehen MITRE-ATT&CK™ Framework in ServiceNow AI Platform.

MITRE Objekte bis STIX Zuordnung

STIX Ist eine Sprache für die standardisierte und strukturierte Beschreibung von Informationen zu Cyberbedrohungen. Das übergeordnete Datenmodell in Threat Intelligence Modul sind die STIX Objekte. Während MITRE Objekte sind eine Teilmenge des übergeordneten Elements STIX Datenmodell. In MITRE-ATT&CK Framework, MITRE Stellt Ähnliches bereit STIX Informationen mit bestimmten Bezeichnungen und Objekten.

MITRE Bis STIX Objektzuordnung

MITRE-Terminologie	STIX-Terminologie
Technik	Angriffsmuster
Mitigation	Vorgehensweise
Gruppen	Angriffssätze
Malware	Malware
Tool	Tool

Daten in erweitern Threat Intelligence Modul

Sie können eine Liste von verwalten Threat Intelligence Bedrohungsquellen und importieren Sie die erforderliche STIX Daten, die einen umfangreichen Satz von Informationen zu Cyberbedrohungen enthalten. Sie können auch verwenden TAXII Profile zur Erleichterung des automatisierten Austauschs von Informationen zu Cyberbedrohungen.

Hinweis:
Weitere Informationen finden Sie unter Definieren Sie eine Bedrohungsquelle Und Erstellen Sie ein TAXII-Profil .

Daten in erweitern MITRE-ATT&CK Modul

Sie können die Objekte Malware, Gruppe, Minderung und Tool auf eine Technik in erweitern MITRE-ATT&CK Repository.

Sie können ein Objekt erstellen und eine Beziehung zwischen einer Technik und dem neuen Objekt im MITRE ATT&CK-Repository-Modul herstellen, aber Sie können den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehungstyp in diesem Modul nicht definieren. Um einen Beziehungstyp zu definieren, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Objekt-Objekt-Beziehungen** Modul.

Wenn Sie den Beziehungstyp zwischen einer vorhandenen Technik und einem vorhandenen Objekt zuordnen, müssen Sie die Technik als Zielobjekt und das Objekt als Quellobjekt definieren. Navigieren Sie dazu zu **IoC-Repository** > **Objekt-Objekt-Beziehungen** Modul.

Sie können eine Gruppe erstellen und einem Angriffsmuster zuordnen, aber im MITRE ATT&CK-Repository können Sie nur die Beziehung zwischen der Gruppe und dem Angriffsmuster herstellen. Um den Beziehungstyp „Objekt-zu-Objekt“ zu definieren, müssen Sie dies im IOC-Repository tun.

Hinweis:
Weitere Informationen finden Sie unter Erweitern MITRE-ATT&CK Daten Und IOC-Repository .

Domain Separation und MITRE-ATT&CK

Diese Domänentrennungsübersicht bezieht sich auf MITRE-ATT&CK. Mit Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Supportstufe

Support: Standard.

Funktionsweise der Domänentrennung MITRE-ATT&CK

Führen Sie die folgenden Schritte aus, um die Domänentrennung zu erreichen:

- Erstellen Sie einen Anwender mit den erforderlichen Rollen „sn_ti.admin“ in der jeweiligen Domäne.
- Replizieren Sie Folgendes für jede Domäne:
  - TAXII Sammlungen

    Hinweis:
    - Aktivieren Sie die Sammlungen nicht in der globalen Domäne. Aktivieren Sie nur die Sammlungen, die repliziert und in Ihrer Domäne verfügbar sind.
    - Ändern Sie **Ausführen als** Feld in den Sammlungen für den Anwender mit der Rolle sn_ti.admin in der jeweiligen Domäne.

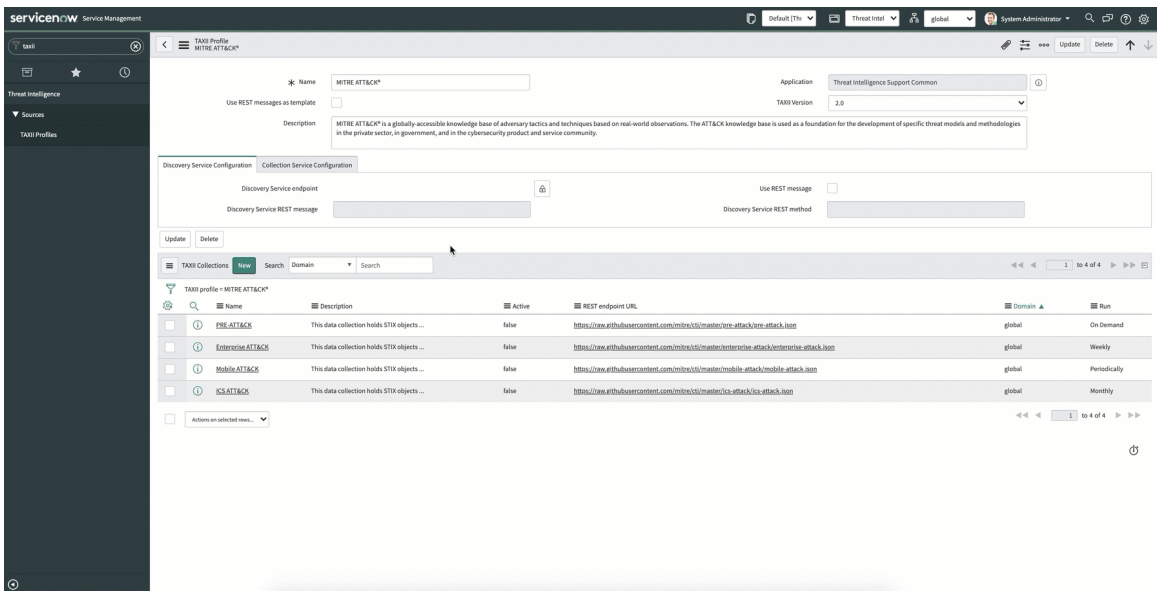
  - Definition Der Technikabdeckung
  - Extraktionsregel für Technik
  - Erkennungsregeln: MITRE ATT&CK-Zuordnungen
  - Minderungsabdeckung
    - Kopieren Sie alle Definitionsdatensätze der Minderungsabdeckung.
    - Kopieren Sie den Rechner zur Verringerung der Abdeckung, oder erstellen Sie einen neuen Rechner für die jeweilige Domäne.
  - Bedrohungsgruppe: Heatmap-Definitionen Der Technik

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TAXII-Sammlung replizieren

1. Navigieren zu **Threat Intelligence** > **Quellen** > **TAXII-Profile**an.
2. Verwenden Sie in der Header-Leiste die Domänenauswahl, um Ihre Domäne auszuwählen.
3. Wählen Sie die TAXII-Sammlung aus, die für Ihre Organisation relevant ist (Enterprise ATT&CK, Mobile ATT&CK oder ICS ATT&CK).
4. Klicken Sie mit der rechten Maustaste in die Kopfzeile, und wählen Sie aus **Einfügen und beibehalten** . Die doppelte TAXII-Sammlung wird unter der ausgewählten Domäne erstellt
5. Navigieren Sie zurück zum MITRE ATT&CK TAXII-Profil, um die doppelte TAXII-Sammlung anzuzeigen.

Die folgende Abbildung zeigt, wie Sie die Domäne TOP/Initech auswählen, die TAXII-Sammlung in der Domäne replizieren und die replizierte TAXII-Sammlung verifizieren.



Richten Sie ein MITRE-ATT&CK™ Framework

Aktivieren Sie MITRE-ATT&CK Profil und richten Sie eine geplante Aufgabe ein, damit Sie einrichten können MITRE-ATT&CK Sammlungen für die Bedrohungserkennung in Ihrer Organisation.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

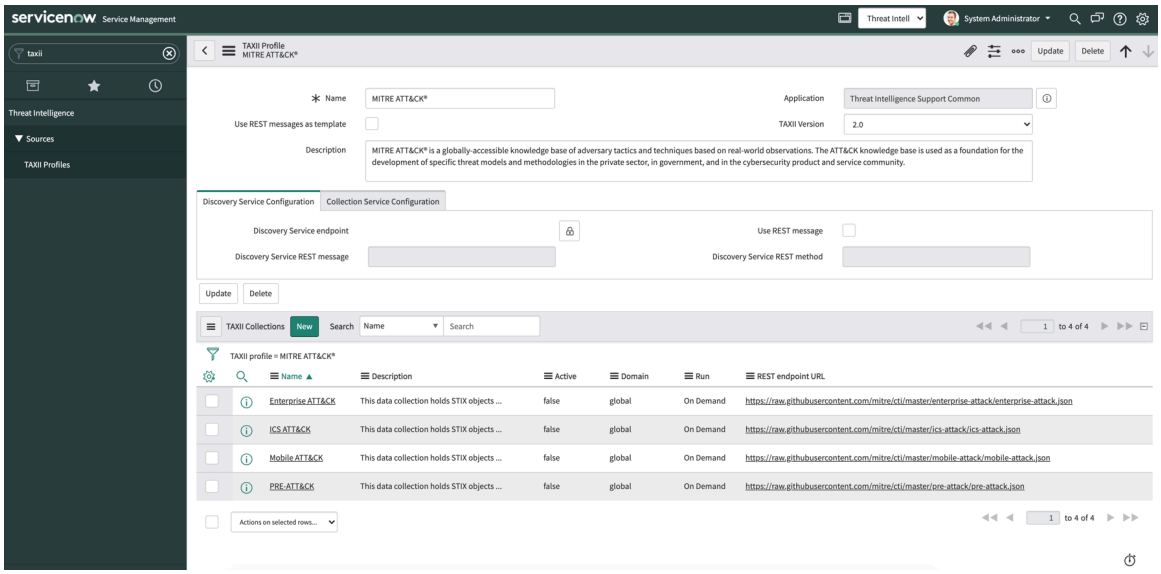
Warum und wann dieser Vorgang ausgeführt wird

Strukturierter Bedrohungsinformationsausdruck (STIX™) Ist eine Sprache für die standardisierte und strukturierte Beschreibung von Informationen zu Cyberbedrohungen. Verwendung von STIX-Daten und vertrauenswürdigem automatisierten Austausch von Indikatorinformationen (TAXII™) Profile, Sicherheitsteams können gemeinsam genutzte Cyberbedrohungsinformationen verwenden, um Bedrohungen zu isolieren, die zuvor von Ihrem Unternehmen und aus anderen Quellen identifiziert wurden.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Quellen** > **TAXII-Profile**an.
   Sie sehen die verfügbar TAXII Profile.
2. Klicken Sie auf **MITRE ATT&CK** Profil, das mit dem Basissystem bereitgestellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Zum Aktivieren von TAXII Sammlung, legen Sie fest **Aktiv** Option auf „wahr“ für TAXII Sammlung, die für Ihre Organisation relevant ist (Enterprise ATT&CK, Mobile ATT&CK oder ICS ATT&CK).

TAXII-Sammlung	Beschreibung
Enterprise ATT&CK	Beschreibt das Verhalten und die Aktionen, die ein Angreifer ergreift, um in einem Unternehmensnetzwerk und in der Cloud zu kompromittieren und zu arbeiten. **Hinweis:** Die Matrix vor ATT&CK wurde von veraltet MITRE Und wird mit der Enterprise-Matrix zusammengeführt.
ATT&CK mobil	Beschreibt das Verhalten und die Aktionen von Angreifern, die sich auf Mobilgeräte konzentrieren.
ICS ATT&CK	Beschreibt die Aktionen, die ein Angreifer beim Betrieb in einem ICs-Netzwerk (Industrial Control Systems) ausführt.

4. Um die Sammlung regelmäßig zu aktualisieren, legen Sie fest **Ausführen** Option entsprechend für Ihre Organisation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig ist diese Option auf „bei Bedarf“ festgelegt.

Hinweis:

a. Sammlungen werden als Teil von verpackt Threat Intelligence Core-Plugin. Durch die Installation oder Aktualisierung von Threat Intelligence Support Common – Version 12,0 oder höher und Threat Intelligence – Version 12,0 oder höher wird sichergestellt, dass Ihre Sammlungsdaten automatisch ausgefüllt werden.

b. Aktivieren Sie TAXII Sammlung nur für die Sammlung, die Sie in Ihrer Organisation verwenden möchten, und deaktivieren Sie die anderen Sammlungen. Wenn Sie beispielsweise die Enterprise ATT&CK-Matrix verwenden möchten, aktivieren Sie Enterprise ATT&CK im TAXII Sammlungsebene und auf der Matrizen Ebene. Deaktivieren Sie die anderen Mobile ATT&CK- und ICs ATT&CK-Matrizen im TAXII Sammlung und auf Matrizenebene.

c. In TAXII Zugehörige Listen für Sammlungen: Wenn Sie die Option „Ausführen“ auf „täglich“ auswählen, tritt ein Fehler auf, und die Option ist standardmäßig auf „bei Bedarf“ festgelegt. Dieser Fehler tritt beim Planen von auf MITRE-ATT&CK Die tägliche Datenaktualisierung ist beschränkt, um die Last auf zu optimieren MITRE Server. Außerdem MITRE Aktualisiert die ATT&CK-Daten nur zweimal im Jahr.

d. Die TAXII Sammlungen werden erst aktualisiert, wenn Sie aktivieren TAXII Sammlung.

e. Aktualisierungen vorhandener Sammlungen können aus abgerufen werden MITRE Server, indem die Ausführungshäufigkeit in jeder Sammlung geplant wird.

f. Die Anpassungen, die Sie an vornehmen MITRE-ATT&CK Repository-Daten (Malware-, Gruppen-, Minderungs- und Tool-Objekte in einer Technik) werden während geplanter Updates gespeichert.

g. MITRE Aktualisiert MITRE-ATT&CK Knowledge Base, in der einige Objekte als widerrufen oder veraltet identifiziert, neue Objekte hinzugefügt oder vorhandene Objekte geändert werden. Wenn MITRE Widerruft jede Taktik oder Technik. Dann werden diese Objekte in als widerrufen markiert ServiceNow AI Platform. Die widerrufenen Objekte werden im Repository beibehalten, sind jedoch nicht zur Verwendung in verfügbar ServiceNow AI Platform.

Nächste Maßnahme

Nachdem das Setup des TAXII-Profils abgeschlossen ist, wird die MITRE-ATT&CK Repository-Daten werden in regelmäßigen Abständen in importiert ServiceNow AI Platform®. Sie können diese Daten anzeigen, indem Sie zu navigieren **MITRE ATT&CK-Repository** > **Matrizen** und **MITRE ATT&CK-Repository** > **Techniken**an.

Verwalten Sie Matrizen

Verwalten Sie die Matrizen, die aus importiert wurden MITRE TAXII Sammlungen. Matrizen sind eine Sammlung von Taktiken und Techniken. Sie können die Matrizen anzeigen, um zu überprüfen, ob Ihre Sammlungen in verfügbar sind MITRE-ATT&CK Repository.

Vorbereitungen

Hinweis:

Überprüfen und überprüfen Sie, ob nur die Matrix, die Sie in Ihrer Organisation verwenden möchten, auf aktiv festgelegt ist, und deaktivieren Sie die anderen Matrizen. Wenn Sie beispielsweise die Enterprise ATT&CK-Matrix verwenden möchten, wird die Enterprise ATT&CK-Matrix im aktiviert TAXII-Sammlung Ebene und in der Matrizenebene. Deaktivieren Sie die anderen Mobile ATT&CK- und ICs ATT&CK-Matrizen im TAXII Sammlung und auf Matrizenebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

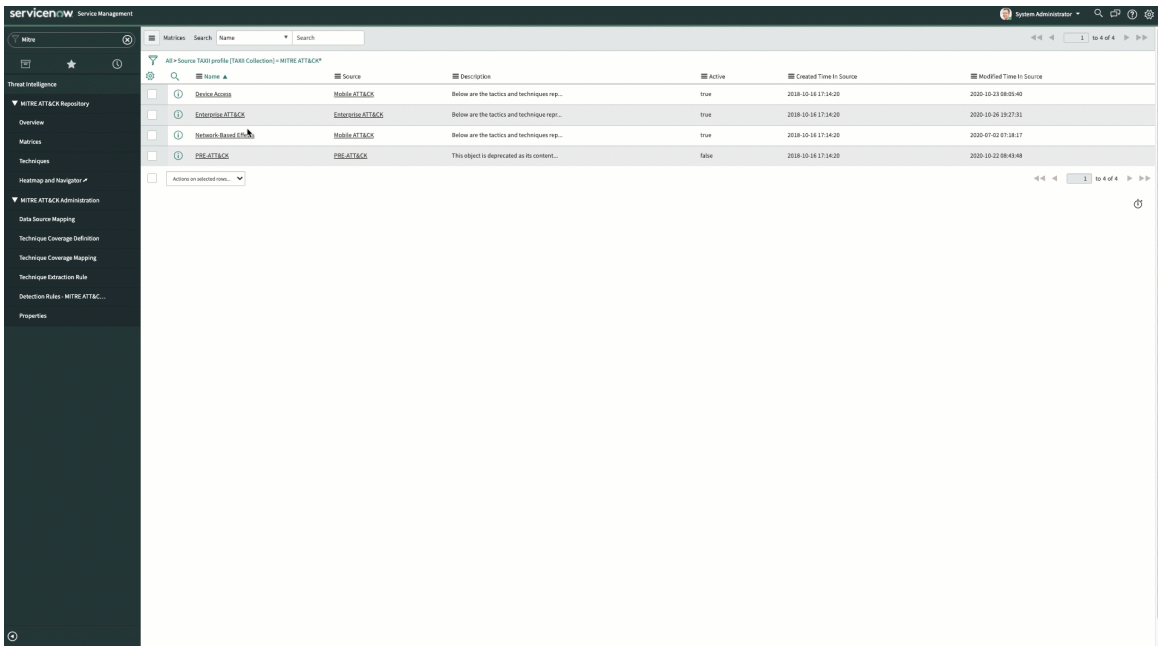
Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Schreibzugriff erstellen

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Matrizen**an.
   Alle Matrizen sind standardmäßig deaktiviert.
2. Zeigen Sie auf, um eine Matrix zu aktivieren **Aktiv** , Doppelklicken Sie auf , und wählen Sie aus **Wahr** .
3. Klicken Sie auf eine Matrix, um alle zugehörigen Informationen anzuzeigen.
4. Um alle Taktiken anzuzeigen, die dieser Sammlung zugeordnet sind, klicken Sie auf **MITRE-Taktiken** Registerkarte.
5. Um zusätzliche Details und die Techniken anzuzeigen, die einer ausgewählten Taktik zugeordnet sind, klicken Sie auf eine Taktik.
6. Unter **MITRE ATT&CK-TECHNIKEN** Registerkarte wählen Sie eine Technik aus.
7. Zeigen Sie unter den zugehörigen Listen die Zuordnungen an, die für die von Ihnen ausgewählte Technik verfügbar sind.

   In der folgenden Abbildung sehen Sie den Navigationspfad von der Enterprise ATT&CK-Matrix bis zur Taktik „anfänglicher Zugriff“ (TA0001) und dann zur Phishing-Technik (T1566). Auf der Seite „Angriffsmuster – Phishing-Technik“ können Sie die zugehörige Liste „Taktik“, „Untertechnik“, „Gruppe“, „Minderung“, „externe Referenzen“ anzeigen. Malware und Tools.



Nächste Maßnahme

Sie können Erweitern Sie die Informationen In einigen dieser zugehörigen Listenobjekte basierend auf der von Ihnen ausgewählten Technik. Sie können beispielsweise neue Informationen für „Gruppe“, „Risikominderung“, „externe Referenzen“, „Malware“ und „Tools“ hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Techniken verwalten

Verwalten Sie die Techniken, die aus importiert wurden MITRE TAXII Sammlungen. Die Techniken enthalten verschiedene Methoden, die Angreifer entwickelt haben, um eine bestimmte Taktik anzuwenden. Sie können Techniken überprüfen und deaktivieren, die für Ihre Organisation nicht relevant sind. In STIX, Techniken werden als Angriffsmuster bezeichnet.

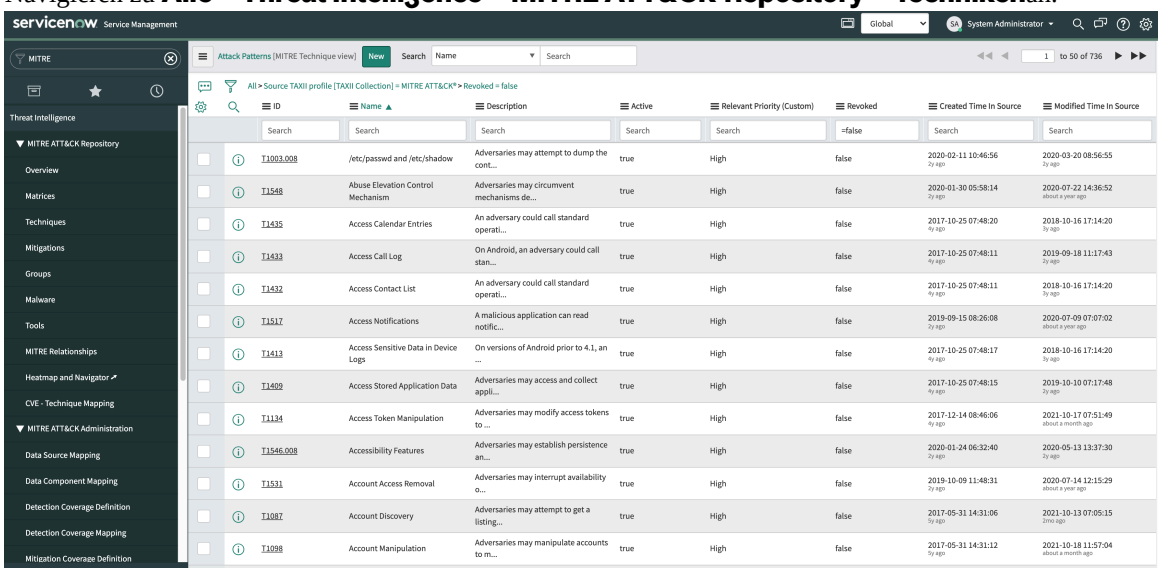
Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Schreibzugriff erstellen

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Techniken**an.



   Die Liste der Techniken und Subtechniken ist jetzt aufgeführt.

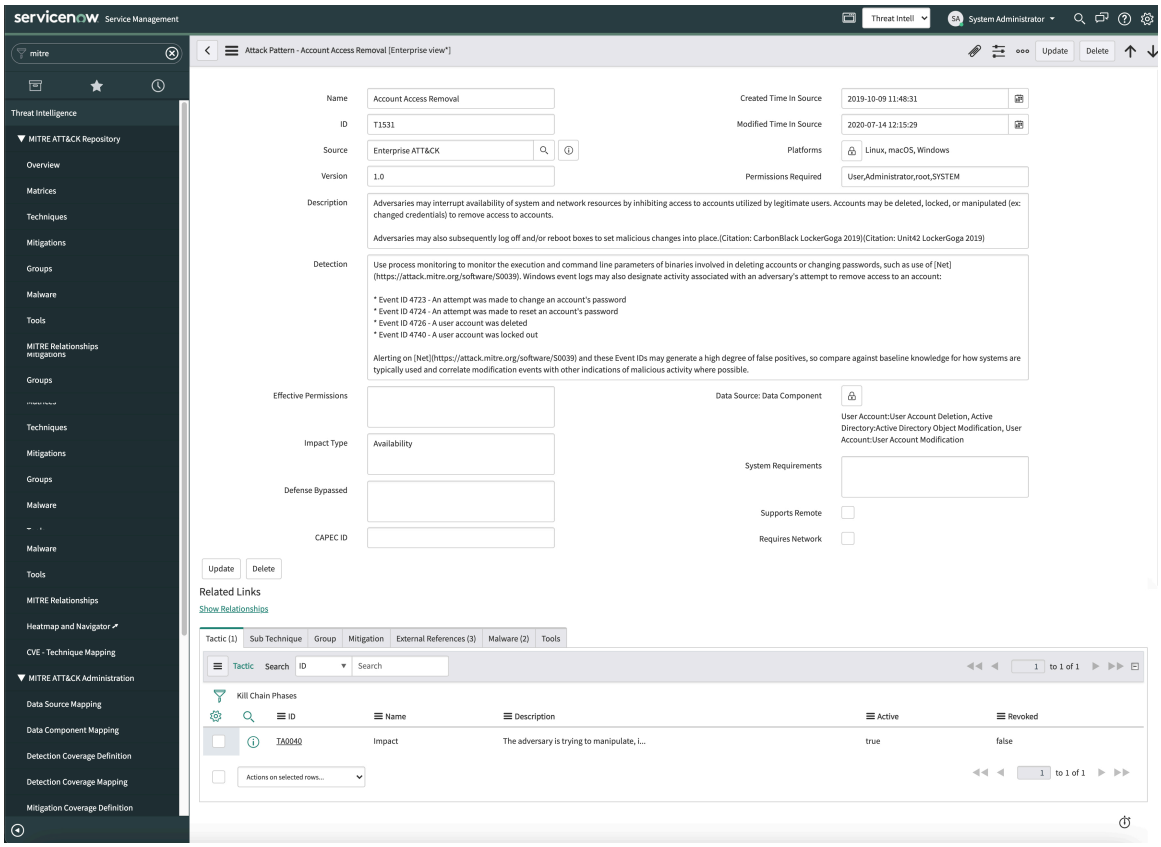
2. Um Techniken zu überprüfen und zu deaktivieren, die für Ihre Organisation nicht relevant sind, wechseln Sie zur Listenansicht für die ausgewählte Technik, und aktualisieren Sie in der Spalte aktiv die Einstellung auf **Falsch** , Und speichern Sie die Einstellung.
   Deaktivieren Sie die Techniken, die nicht von anderen Objekten in verwendet werden MITRE-ATT&CK Repository.

3. Um eine Technik zu priorisieren, weisen Sie im eine Priorität zu **Relevante Priorität (Anwenderdefiniert)** Feld.
   Die für das Basissystem relevante Priorität ist auf „keine“ festgelegt. Die **Relevante Priorität (Anwenderdefiniert)** Feld wird nicht aus importiert MITRE-ATT&CK TAXII Sammlungen, aber ein anwenderdefiniertes Feld wurde in eingeführt ServiceNow AI Platform. Sie können die relevanten Prioritätsinformationen verwenden, um Techniken in den Dashboards, während der Datenquellenzuordnung oder bei der Analyse der Heatmap zu filtern und zu priorisieren.

4. Klicken Sie auf eine Technik, um alle mit dieser Technik verknüpften Informationen anzuzeigen.

   In der folgenden Abbildung können Sie die Details für jede Technik zur Entfernung des Account-Zugriffs, ihre ID, Quelle und andere zugehörige Informationen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Die Datenquelle: Datenkomponentenelement eingeführt von MITRE Ersetzt das vorherige Datenquellenfeld. Die Datenkomponente stellt den Datenquellen eine zusätzliche Unterebene des Kontexts bereit. Wenn Ihr MITRE-ATT&CK Repository enthält das alte TAXII Sammlungen, dann können Sie das Feld Datenquelle anzeigen. Andernfalls können Sie die Datenquellen mit dem zusätzlichen Kontext von Datenkomponenten im Feld Datenquelle: Datenkomponente anzeigen. Sie können das Feld „neue Datenkomponente“ nur anzeigen, wenn die Quelle Enterprise ATT&CK ist. Weitere Informationen finden Sie unter Datenkomponentenzuordnung .

5. Um anzuzeigen, wie diese Objekte zusammenhängen, klicken Sie auf **Beziehungen Anzeigen** .

Nächste Maßnahme

Sie können Erweitern Sie die Informationen In einigen dieser zugehörigen Listenobjekte. Sie können beispielsweise neue Informationen für Gruppen-, Minderung- und externe Referenzen hinzufügen.

Verwalten Sie Minderungen

Verwalten Sie die Minderungen, die aus importiert wurden MITRE TAXII Sammlungen. Mit Minderungen können Sie verhindern, dass Angreifer Techniken oder Untertechniken erfolgreich für Ihre Organisation ausführen. In STIX, Minderungen werden als Handlungsverlauf bezeichnet.

Vorbereitungen

Erforderliche Rolle:

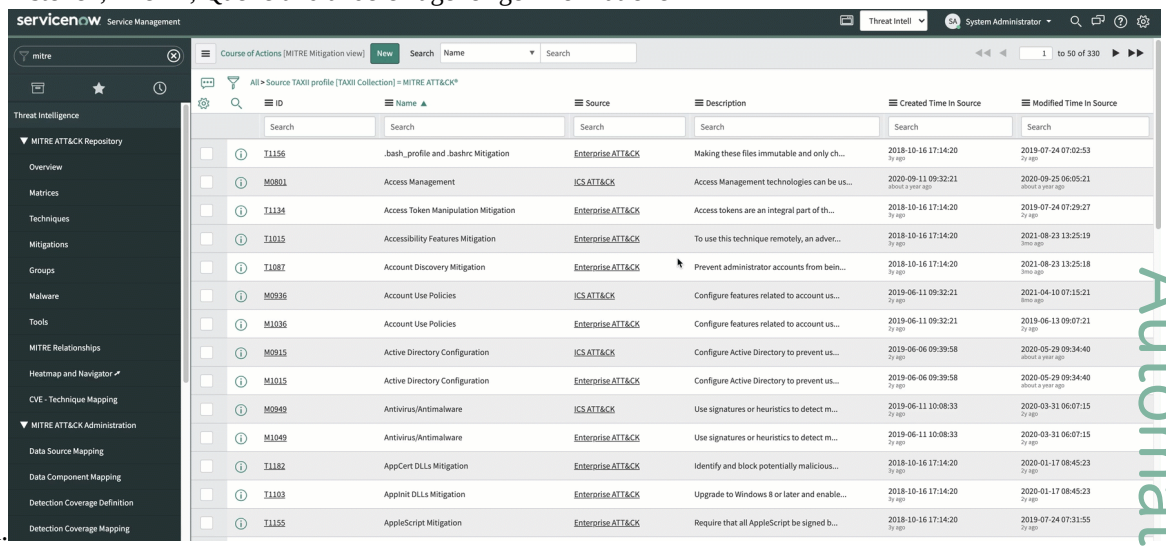
- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Schreibzugriff erstellen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Mitigationen**an.
   Die Minderungen sind jetzt aufgelistet.
2. Klicken Sie auf eine Minderung, um alle zugehörigen Informationen anzuzeigen.
   In der folgenden Abbildung können Sie die Details zur Minderung der Manipulation von Zugriffstoken, ihre ID, Quelle und andere zugehörige Informationen anzeigen.



3. Um anzuzeigen, wie diese Objekte zusammenhängen, klicken Sie auf **Beziehungen Anzeigen** .

Nächste Maßnahme

Verwenden Sie Technikmodul Zum Hinzufügen oder Ändern der Minderungsdaten.

Verwalten Sie Gruppen

Verwalten Sie die Gruppen, die aus importiert wurden MITRE TAXII Sammlungen. Gruppen sind Sätze zugehöriger Angriffsaktivitäten, die von einem allgemeinen Namen in der Sicherheits-Community nachverfolgt werden. Analysten verfolgen Aktivitätencluster mithilfe verschiedener Begriffe wie Bedrohungsgruppen, Aktivitätsgruppen, Bedrohungsakteure, Angriffssätze und Kampagnen. In STIX, Gruppen werden als Angriffssätze bezeichnet.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Schreibzugriff erstellen

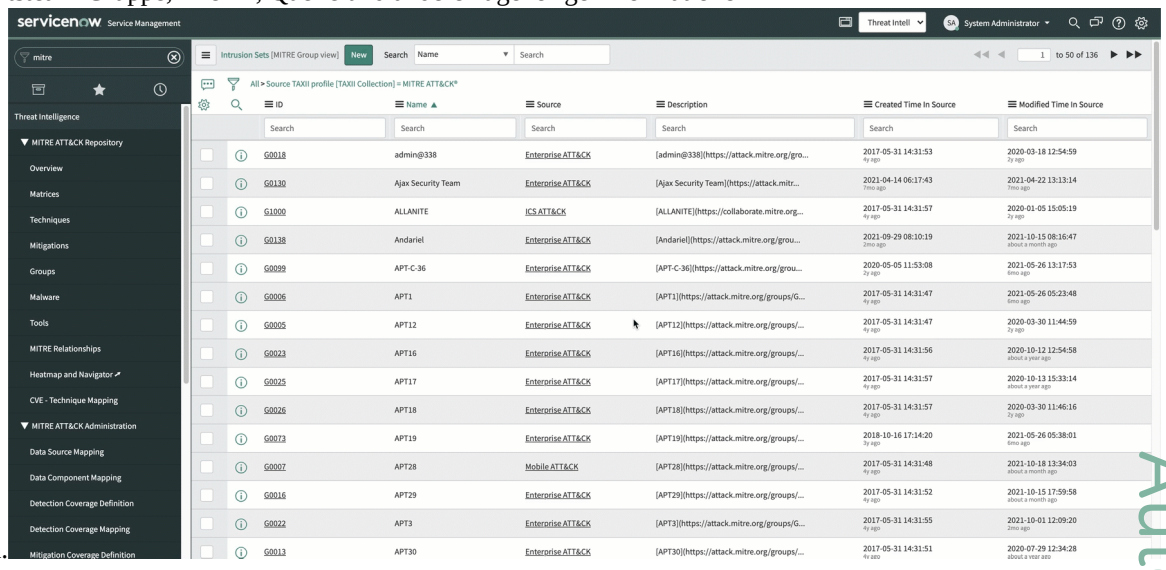
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Gruppen**an.
   Sie können die aufgelisteten Gruppen anzeigen.
2. Klicken Sie auf eine Gruppe, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung können Sie die Details für die Ajax-Sicherheitsteam-Gruppe, ihre ID, Quelle und andere zugehörige Informationen anzeigen.



3. Um anzuzeigen, wie diese Objekte zusammenhängen, klicken Sie auf **Beziehungen Anzeigen** .

> **Hinweis:**
> Um die Bedrohungsgruppen einem Sicherheitsfall für eine eingehendere Untersuchung zuzuordnen, klicken Sie auf **Dem Sicherheitsfall hinzufügen** .

Nächste Maßnahme

Verwenden Sie Technikmodul Zum Hinzufügen oder Ändern der Gruppendaten.

Malware verwalten

Verwalten Sie die Malware-Informationen, die Sie aus importiert haben MITRE TAXII Sammlungen. Malware ist eine Art von TTP, die schädlichen Code darstellt. Bezieht sich auf ein Programm, das verdeckt in ein System eingefügt wird. Die Absicht einer Malware besteht darin, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder des Betriebssystems des Opfers zu gefährden.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Schreibzugriff erstellen

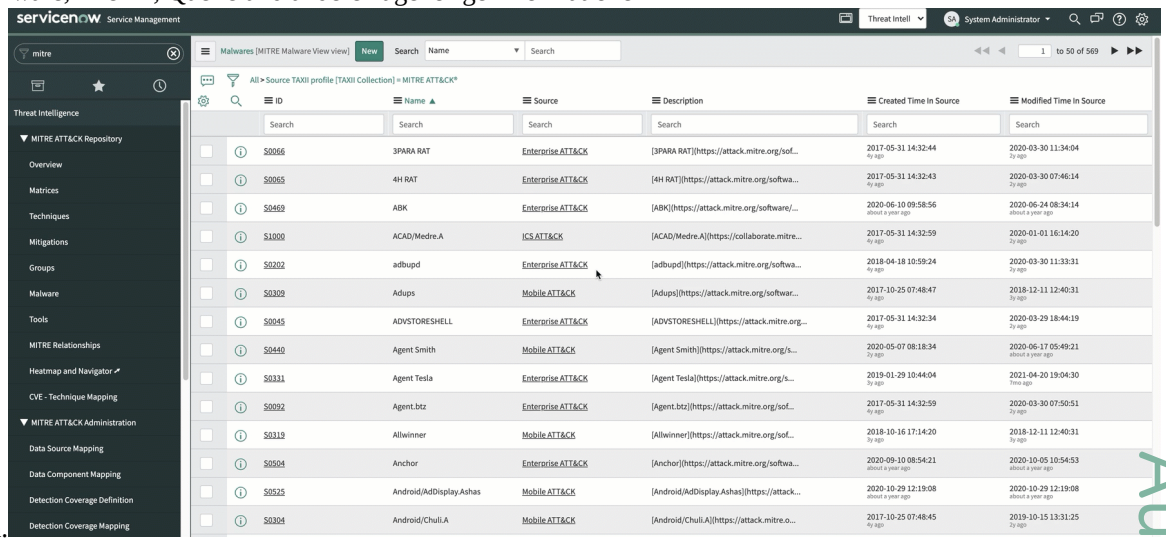
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Malware**an.
   Sie können die aufgelistete Malware anzeigen.
2. Klicken Sie auf eine Malware, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung können Sie die Details für die 3PARA-RAT-Malware, ihre ID, Quelle und andere zugehörige Informationen anzeigen.



3. Um anzuzeigen, wie diese Objekte zusammenhängen, klicken Sie auf **Beziehungen Anzeigen** .

Nächste Maßnahme

Verwenden Sie Technikmodul Zum Hinzufügen oder Ändern der Malware-Daten.

Tools verwalten

Verwalten Sie die Toolinformationen, die Sie aus importiert haben MITRE TAXII Sammlungen. Tools sind legitime Software, die von Bedrohungsakteuren zum Ausführen von Angriffen verwendet wird.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Schreibzugriff erstellen

Warum und wann dieser Vorgang ausgeführt wird

Mit Tools können Sie wissen, wie und wann Bedrohungsakteure sie für die Ausführung von Kampagnen verwenden. Im Gegensatz zu Malware werden diese Tools oder Softwarepakete häufig auf einem System gefunden und haben legitime Zwecke für Poweruser, Administratoren, Netzwerkadministratoren oder sogar normale Anwender.

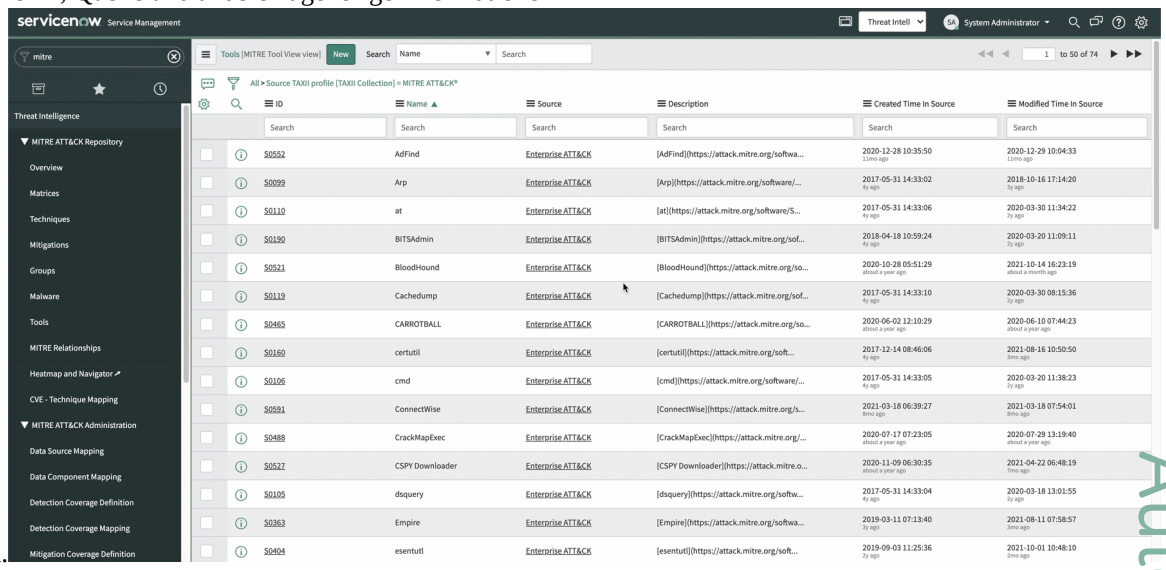
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Tools**an.
   Sie können die aufgeführten Tools anzeigen.
2. Klicken Sie auf ein Tool, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung können Sie die Details für das CARROTBALL-Tool, seine ID, Quelle und andere zugehörige Informationen anzeigen.



3. Um anzuzeigen, wie diese Objekte zusammenhängen, klicken Sie auf **Beziehungen Anzeigen** .

Nächste Maßnahme

Verwenden Sie Technikmodul Zum Hinzufügen oder Ändern der Tooldaten.

Verwalten MITRE Beziehungen

Verwalten Sie MITRE Beziehungsinformationen, die Sie aus importiert haben MITRE TAXII Sammlungen.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Schreibzugriff erstellen

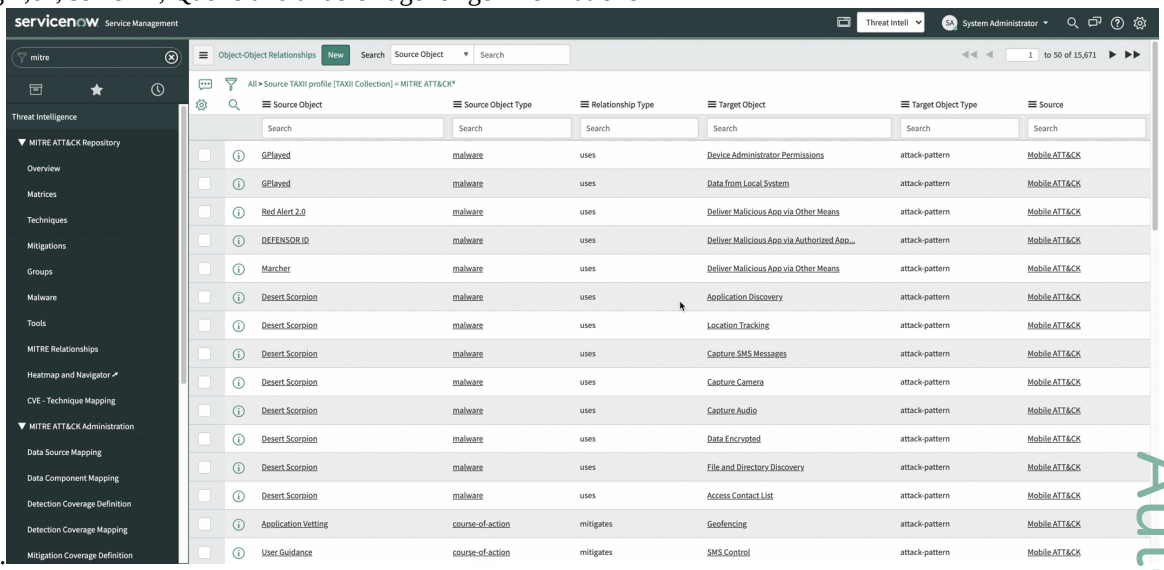
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **MITRE-Beziehungen**an.
   Sie können die aufgeführten Tools anzeigen.
2. Klicken Sie auf ein Quellobjekt, um alle zugehörigen Informationen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung können Sie die Details für das Objekt „rote Warnung 2,0“, seine ID, Quelle und andere zugehörige Informationen anzeigen.



3. Um anzuzeigen, wie diese Objekte zusammenhängen, klicken Sie auf **Beziehungen Anzeigen** .

Nächste Maßnahme

Verwenden Sie Technikmodul Zum Hinzufügen oder Ändern der MITRE-Beziehungsdaten.

Verwalten Sie die CVE- und Technikzuordnung

Verwalten Sie die CVE- und Technikinformationen, die nach dem Importieren von zugeordnet werden MITRE TAXII Sammlungen.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Schreibzugriff erstellen

Hinweis:
Die **CVE-Technikzuordnung** Das Modul ist nur verfügbar, wenn das Vulnerability Response-Produkt in Ihrer Umgebung installiert ist.

Warum und wann dieser Vorgang ausgeführt wird

Sobald Sie importiert haben MITRE TAXII Sammlungen Sie können die CVEs in Ihrer Umgebung und ihre Beziehung zu dem anzeigen MITRE-ATT&CK Techniken. Sie können auch Zuordnungen zu CVEs und den Angriffsmustern erstellen.

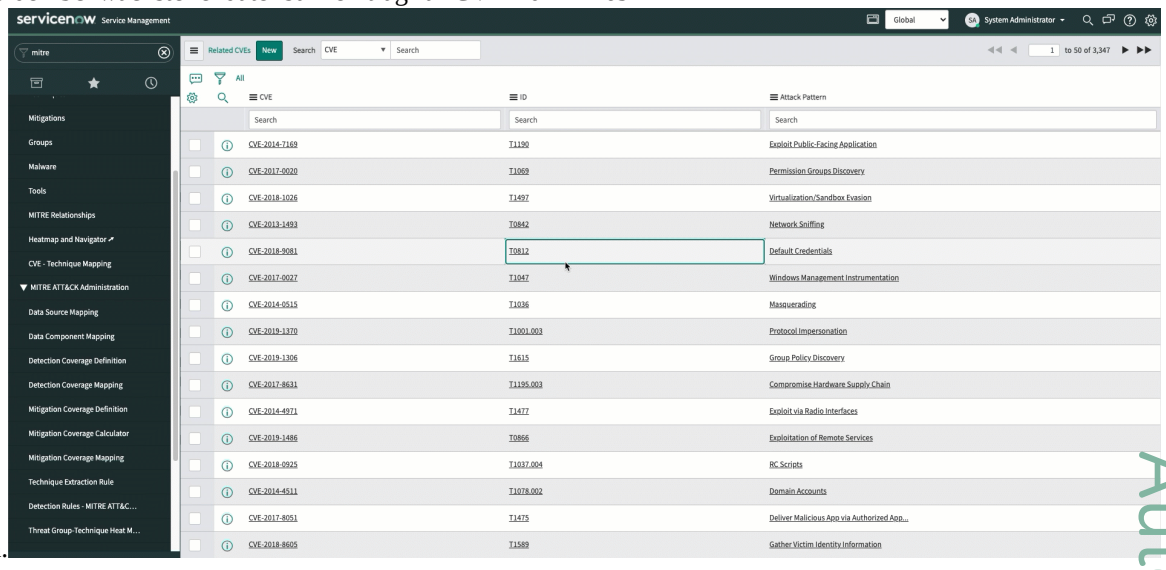
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **CVE – Technikzuordnung**an.
   Sie können die aufgeführten CVEs und Techniken anzeigen.
2. Klicken Sie auf ein CVE, um den Eintrag der Schwachstellendatenbank anzuzeigen.

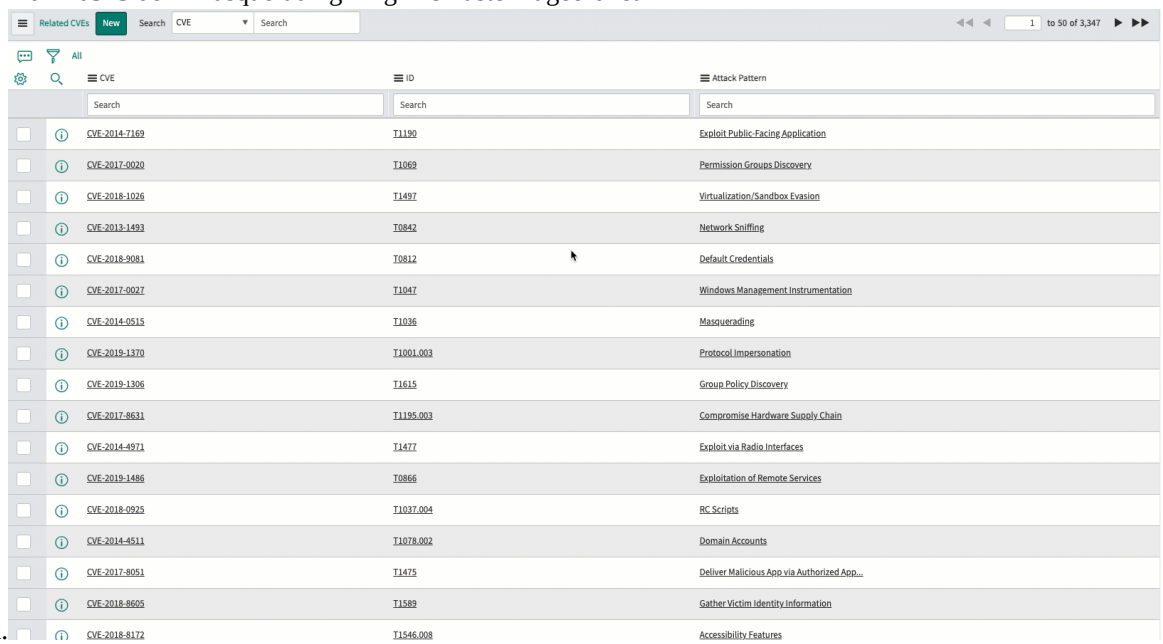
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung können Sie die Details für die CVE-Liste und den Schwachstellendatenbankeintrag für CVE-2014-7169 anzeigen.



3. Klicken Sie auf, um einen Eintrag hinzuzufügen **Neu** , Ordnen Sie das CVE einem Angriffsmuster zu, und klicken Sie auf **Übermitteln** .
   In der folgenden Abbildung wird ein neuer Eintrag erstellt, indem CVE-2014-0515 dem Masquerading-Angriffsmuster zugeordnet wird.



Erweitern Sie MITRE-ATT&CK Daten

Erweitern Sie MITRE-ATT&CK Repository-Daten in ServiceNow AI Platform Durch Anreicherung.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin: Zugriff löschen
- sn_ti.read: Lesezugriff
- sn_ti.write: Schreibzugriff erstellen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Objekte Malware, Gruppe, Minderung und Tool auf eine Technik in erweitern MITRE-ATT&CK Repository.

Sie können ein neues Objekt erstellen und eine Beziehung zwischen einer Technik und dem neuen Objekt im MITRE ATT&CK-Repository-Modul herstellen, aber Sie können den Beziehungstyp in diesem Modul nicht definieren. Weitere Informationen zum Definieren von Beziehungstypen finden Sie unter Objekt-zu-Objekt-Beziehungen . Um einen Beziehungstyp zu definieren, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Objekt-Objekt-Beziehungen** Modul.

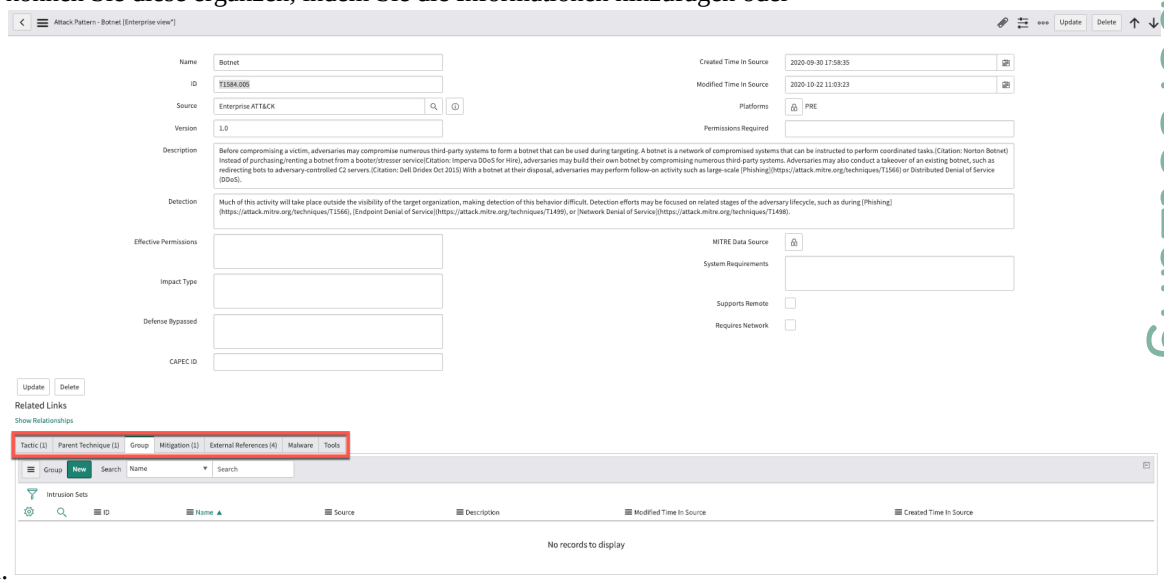
Wenn Sie den Beziehungstyp zwischen einer vorhandenen Technik und einem vorhandenen Objekt zuordnen, müssen Sie die Technik als Zielobjekt und das Objekt als Quellobjekt definieren. Navigieren Sie dazu zu **IoC-Repository** > **Objekt-Objekt-Beziehungen** Modul.

Sie können eine Gruppe erstellen und einem Angriffsmuster zuordnen, aber im MITRE ATT&CK-Repository können Sie nur die Beziehung zwischen der Gruppe und dem Angriffsmuster herstellen. Um den Beziehungstyp „Objekt-zu-Objekt“ zu definieren, müssen Sie dies im IOC-Repository tun.

Hinweis:
Alle Anpassungen, die Sie an den Objekten vornehmen, werden während geplanter Updates gespeichert.

Prozedur

1. Navigieren zu **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Techniken**an.
2. Klicken Sie auf eine Technik oder eine Untertechnik, um alle dieser Technik zugeordneten Informationen anzuzeigen.
   In der folgenden Abbildung sehen Sie, dass die Botnet-Technik (T1584.005) keiner Gruppe zugeordnet ist. Wenn Sie zusätzliche Informationen zu einer Technik oder Untertechnik haben, können Sie diese ergänzen, indem Sie die Informationen hinzufügen oder ändern.

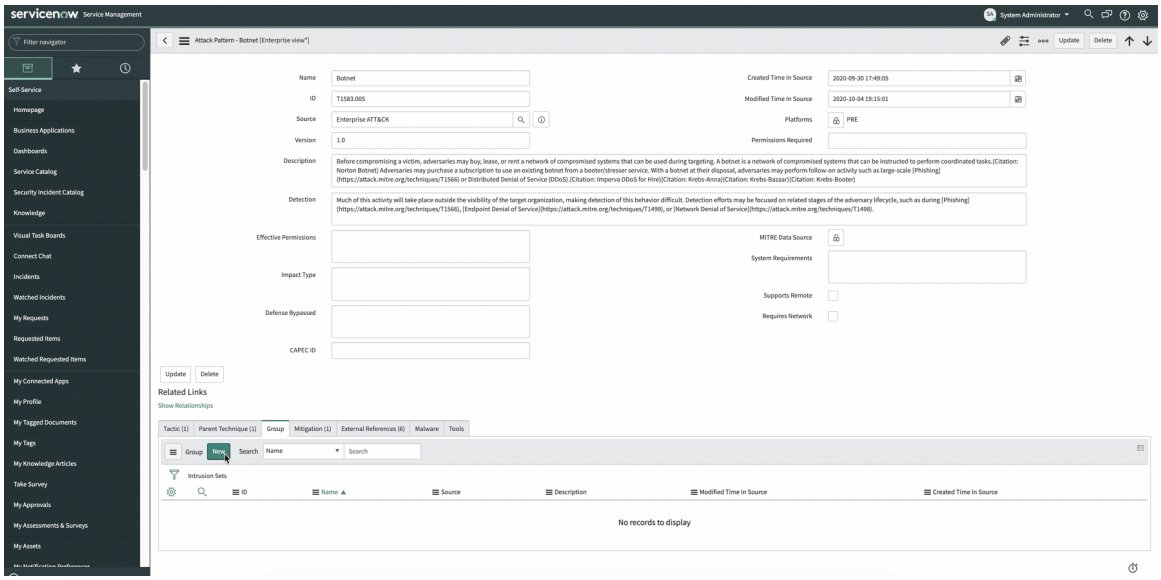


3. Klicken Sie auf eine zugehörige Liste, um ihre Daten so anzureichern, dass sie einer neuen Gruppe zugeordnet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der folgenden Abbildung wurde der Botnet-Untertechnik eine Gruppe, Anwenderdefiniert1, zugeordnet.



Definieren Sie die Datenquellen- und Erkennungstool-Zuordnung

Definieren Sie die Datenquellen- und Erkennungstool-Zuordnung für MITRE-ATT&CK Taktiken und Techniken. Die Datenquellenzuordnung bietet Ihnen Einblicke in die Relevanz und Verfügbarkeit der Datenquellen und der Erkennungstools zur Überwachung der Datenquellen in Ihrer Umgebung.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Schreibzugriff, Löschzugriff
- sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Datenquellen und Erkennungstools identifizieren, die Ihre Organisation benötigt, um die Techniken effektiv zu erkennen.

Wenn sich Ihre Organisation beispielsweise auf 5 Techniken konzentriert, benötigen Sie möglicherweise 10 Datenquellen und 10 Erkennungstools, um diese Quellen zu überwachen. Nehmen wir an, dass Sie feststellen, dass Ihre Organisation nicht über zwei Datenquellen und fünf Erkennungstools verfügt. Diese Übung gibt Ihnen Einblick in die Datenquellen, ihre Relevanz für Ihre Organisation und ermöglicht die Identifizierung von Lücken in der Abdeckung. Sie können sich auch auf die Verbesserung Ihrer Umgebung mit den richtigen Datenquellen und Erkennungstools konzentrieren.

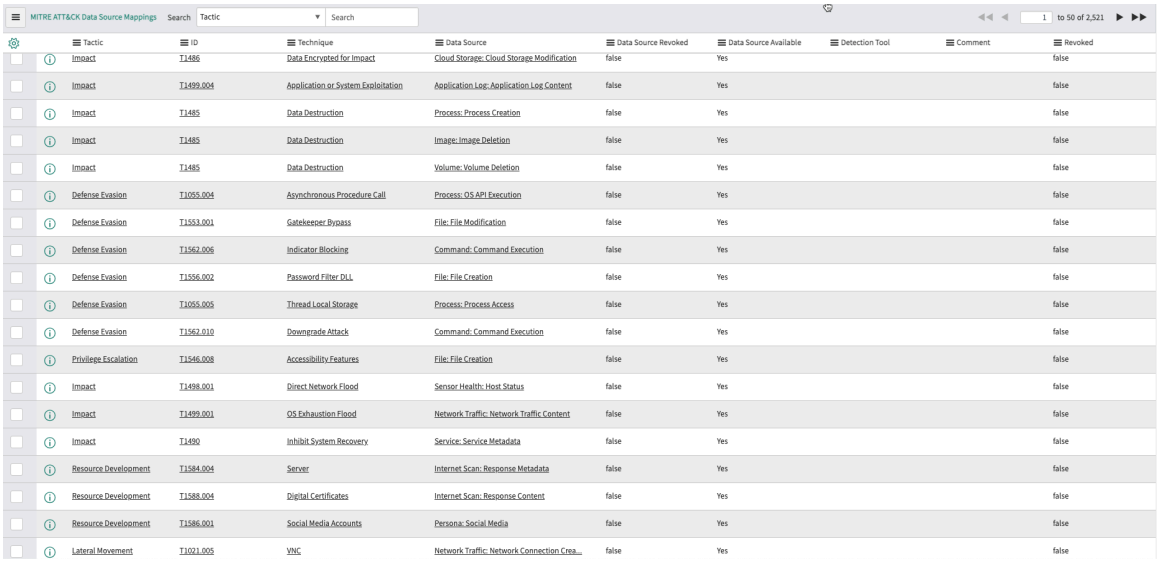
Alle aktiven Taktiken, Techniken, IDs und Datenquellen werden basierend auf automatisch ausgefüllt TAXII Profil

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Datenquellenzuordnung**an.

   Die folgende Abbildung zeigt die Liste der Taktiken, Techniken und deren IDs, die basierend auf Ihren Sammlungsaktualisierungen ausgefüllt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Tactic	ID	Technique	Data Source	Data Source Revoked	Data Source Available	Detection Tool	Comment	Revoked
Impact	T1486	Data Encrypted for Impact	Cloud Storage: Cloud Storage Modification	false	Yes			false
Impact	T1499.004	Application or System Exploitation	Application Log: Application Log Content	false	Yes			false
Impact	T1485	Data Destruction	Process: Process Creation	false	Yes			false
Impact	T1485	Data Destruction	Image: Image Deletion	false	Yes			false
Impact	T1485	Data Destruction	Volume: Volume Deletion	false	Yes			false
Defense Evasion	T1055.004	Asynchronous Procedure Call	Process: OS API Execution	false	Yes			false
Defense Evasion	T1553.001	Gatekeeper Bypass	File: File Modification	false	Yes			false
Defense Evasion	T1562.006	Indicator Blocking	Command: Command Execution	false	Yes			false
Defense Evasion	T1556.002	Password Filter DLL	File: File Creation	false	Yes			false
Defense Evasion	T1055.005	Thread Local Storage	Process: Process Access	false	Yes			false
Defense Evasion	T1562.010	Downgrade Attack	Command: Command Execution	false	Yes			false
Privilege Escalation	T1546.008	Accessibility Features	File: File Creation	false	Yes			false
Impact	T1498.001	Direct Network Flood	Sensor Health: Host Status	false	Yes			false
Impact	T1499.001	OS Exhaustion Flood	Network Traffic: Network Traffic Content	false	Yes			false
Impact	T1490	Inhibit System Recovery	Service: Service Metadata	false	Yes			false
Resource Development	T1584.004	Server	Internet Scan: Response Metadata	false	Yes			false
Resource Development	T1588.004	Digital Certificates	Internet Scan: Response Content	false	Yes			false
Resource Development	T1586.001	Social Media Accounts	Persona: Social Media	false	Yes			false
Lateral Movement	T1021.005	VNC	Network Traffic: Network Connection Crea...	false	Yes			false

Feld	Beschreibung
Taktik	Ziel des Angreifers oder Grund für die Ausführung einer Aktion.
ID	Eindeutige Identität der Technik.
Technik	Wie ein Angreifer durch Ausführen einer Aktion ein taktisches Ziel erreicht.
Datenquelle	Datenquelle, die der Technik zugeordnet ist.
Datenquelle widerrufen	Die Datenquelle wird widerrufen, wenn sie auf „wahr“ festgelegt ist, die Datenquellenzuordnung wird jedoch beibehalten. Wenn der Datenquellenwert in nicht gefunden wird MITRE, Wird der Wert „Datenquelle widerrufen“ automatisch als „wahr“ markiert. Die Datenquellenzuordnung für einen Datensatz wird widerrufen, wenn die Technik- und Datenquellenbeziehungen in der aktualisiert fehlen MITRE Daten. Standardwert: false
Datenquelle verfügbar	Verfügbarkeit der Datenquelle.
Erkennungstool	Tool, das die Datenquelle durch Erkennung der verwendeten Techniken ergänzt. Das Erkennungstool wird dem Warnungssensor in zugeordnet SIR.
Widerrufen	Die Datenquellenzuordnung für einen Datensatz wird widerrufen, wenn die Technik- und Datenquellenbeziehungen in der aktualisiert fehlen MITRE Daten. Standardwert: false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Überprüfen Sie die aufgeführten Datenquellen, und ändern Sie den Wert in **Datenquelle Verfügbar** Feld basierend auf Ihrer Umgebung.

3. **Hinweis:**
   Sie können diesen Eintrag nicht in der Listenansicht bearbeiten.

   In **Erkennungstool** Führen Sie die folgenden Schritte aus:

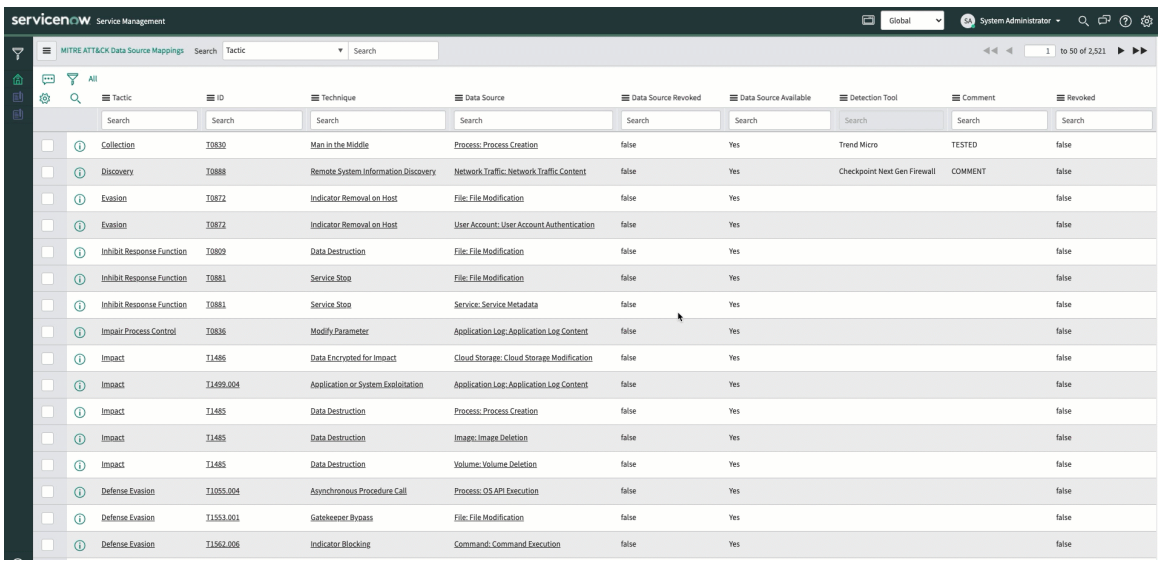
   a. Klicken Sie auf das Informationssymbol und dann auf **Öffnen Sie Den Datensatz** .

   b. Entsperren **Erkennungstool** Eintrag.

   c. Verwenden Sie die Suchliste, um ein Erkennungstool auszuwählen. Sie können Erkennungstools mehrfach auswählen.

   d. Klicken Sie auf **Aktualisieren**.

   In der folgenden Abbildung werden mehrere Erkennungstools hinzugefügt, um die Datenquelle zu überwachen.



Definieren Sie die Datenquellen- und Datenkomponentenzuordnung

Verwenden Sie die Datenkomponentenzuordnung, wenn Sie die neueste verwenden TAXII Sammlungen, und Sie möchten eine Beziehung zwischen den Datenquellen, Datenkomponenten und den verschiedenen Techniken pflegen. Ordnen Sie die Datenquellen dem zusätzlichen Kontext von Datenkomponenten zu, der Datenquellen eine zusätzliche Unterebene des Kontexts bietet, mit der Sie das Verhalten von Angreifern in verstehen können MITRE-ATT&CK Besser.

Vorbereitungen
Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Schreibzugriff, Löschzugriff
- sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird
Die Zuordnung der Datenquellen und Datenkomponenten bietet Einblick in die Datenquellen oder -Komponenten und die Techniken, die für Ihre Organisation relevant sind.

Wenn sich Ihre Organisation beispielsweise auf 7 Techniken konzentriert, benötigen Sie möglicherweise 5 Datenquellen und 10 Datenkomponenten, um diese Quellen zu

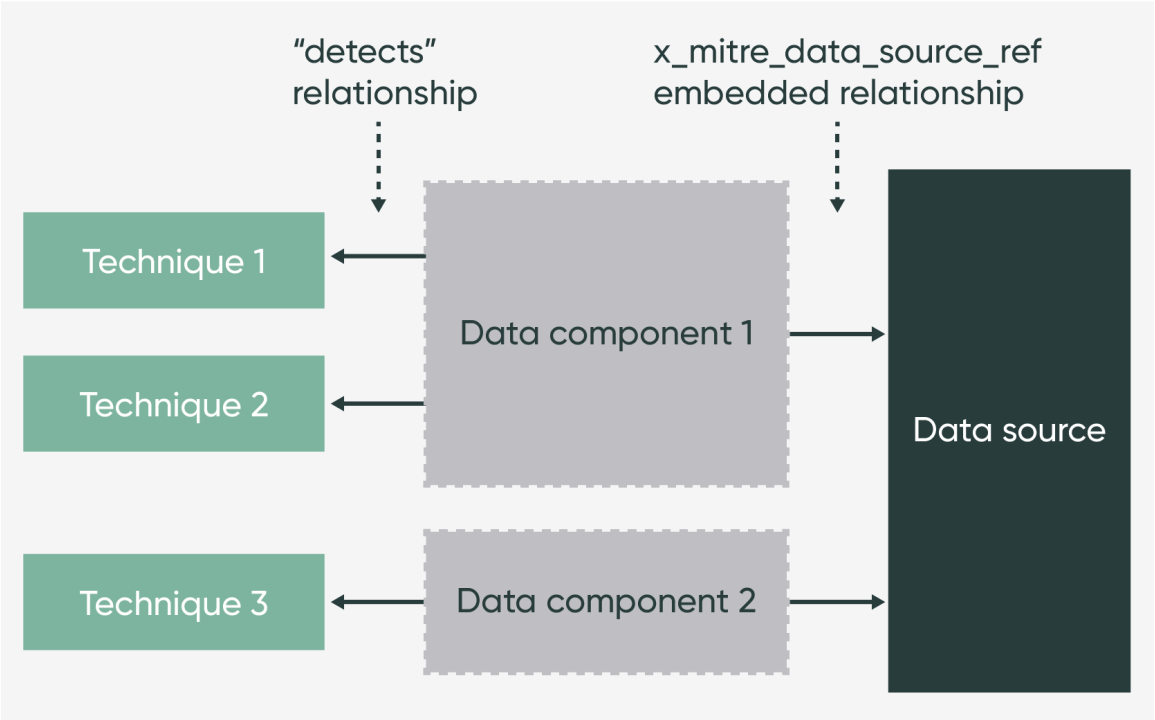
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

überwachen. Ihre Bewertung interner Tools zeigt, dass Ihre Organisation nicht über zwei Datenquellen und vier Datenkomponenten verfügt. Diese Zuordnungsübung bietet Einblick in die Datenquellen, Komponenten und Techniken, ihre Relevanz für Ihre Organisation und ermöglicht die Identifizierung der Abdeckungslücken. Sie können Ihre Investition daher auf die richtigen Datenquellen und Warnsensoren konzentrieren, um Bedrohungen durch Angreifer zu erkennen und zu mindern.

Die MITRE-ATT&CK Framework enthält eine aktualisierte Struktur für die Datenquellen – Datenquelle: Datenkomponente. Diese neue Form der Datenquelle bietet den Datenquellen einen zusätzlichen Kontext. Das Datenquellenobjekt enthält den Namen der Datenquelle sowie wichtige Details zu den erfassten Daten (Datei, Prozess, Netzwerkverkehr usw.) und bestimmte Werte oder Eigenschaften, die zum Erkennen von Angreiferverhalten erforderlich sind.

Die folgende Abbildung zeigt MITRE-ATT&CK STIX™ Strukturdarstellung für Datenquellen und Datenkomponenten. Sie können sowohl die Datenquellen als auch die Datenkomponenten anzeigen, die als anwenderdefiniert erfasst wurden STIX™ Objekte. Die Abbildung zeigt, dass jede Datenquelle eine oder mehrere Datenkomponenten enthält und jede Datenkomponente eine oder mehrere Techniken erkennt.

Allgemeine Struktur von Datenquellen und Datenkomponenten

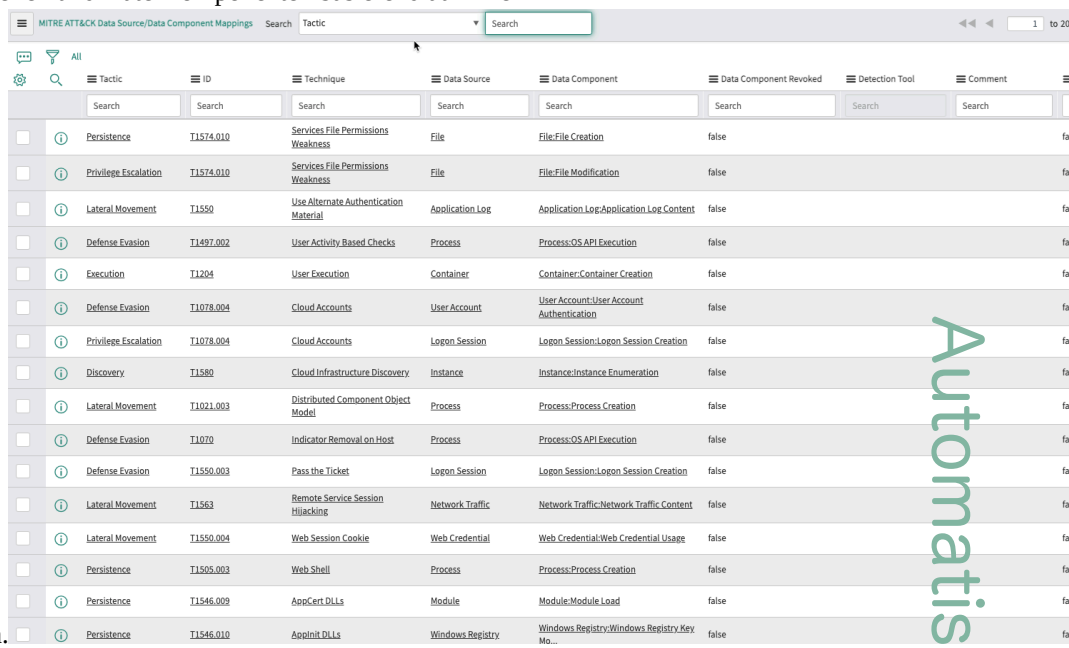


Sie können weiterhin verwenden Datenquellenzuordnung Wenn Ihr MITRE-ATT&CK Repository enthält das alte TAXII Sammlungen und Sie haben Ihre Datenquellen verschiedenen Techniken zugeordnet. Verwenden Sie jedoch Datenkomponentenzuordnung Wenn Sie die neueste verwenden TAXII Sammlungen, und Sie möchten eine Beziehung zwischen den Datenquellen, Datenkomponenten und den verschiedenen Techniken pflegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Datenkomponentenzuordnung**an.
   Die folgende Abbildung zeigt die Liste der Taktiken, IDs, Techniken zusammen mit den Datenquellen und Datenkomponenten basierend auf Ihren Sammlungsaktualisierungen.



Feld	Beschreibung
Taktik	Ziel des Angreifers oder Grund für die Ausführung einer Aktion.
ID	Eindeutige Identität der Technik.
Technik	Wie ein Angreifer durch Ausführen einer Aktion ein taktisches Ziel erreicht.
Datenquelle	Datenquelle, die der Technik zugeordnet ist.
Datenkomponente	Datenkomponente, die der Datenquelle zugeordnet ist. Eine Datenkomponente kann nur eine übergeordnete Datenquelle haben.
Datenkomponente widerrufen	Gibt an, ob die Datenkomponente in widerrufen wurde MITRE-ATT&CKKnowledge Base.
Erkennungstool	Tool, das die Datenquelle durch Erkennung der verwendeten Techniken ergänzt. Das Erkennungstool wird dem Warnungssensor in zugeordnet SIR.
Kommentar	Beschreibung der Datenquelle und der Datenkomponentenzuordnung.
Widerrufen	Gibt an, ob die Datenkomponente für die Technikzuordnung von widerrufen wird MITRE-ATT&CK.

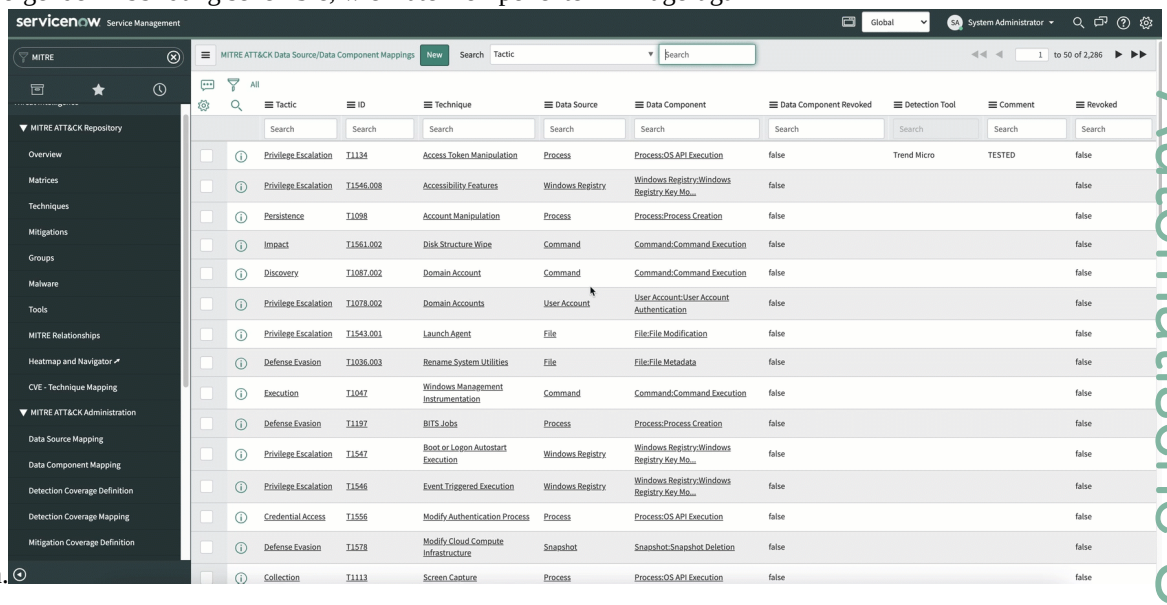
2. Überprüfen Sie die aufgeführten Datenquellen und Datenkomponenten, und ändern Sie die Werte basierend auf Ihrer Umgebung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Führen Sie die folgenden Schritte aus, um eine Datenkomponente hinzuzufügen.
   a. Navigieren zu **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Techniken**an.
   b. Klicken Sie auf eine Technik, für die Sie die Datenquelle ändern möchten: Informationen zur Datenkomponente.
   c. Datenquelle Entsperren: Datenkomponente.
   d. Verwenden Sie die Suchliste, um auszuwählen MITRE-ATT&CK Datenkomponenten.
   e. Datenquelle Sperren: Datenkomponente.
   f. Klicken Sie auf **Aktualisieren**.

In der folgenden Abbildung sehen Sie, wie Datenkomponenten hinzugefügt werden.



Definieren Sie die Abdeckung der Technik-Erkennung

Definieren Sie die Technikerkennungsabdeckung, die Ihre Organisation messen und bestimmte Angreifertechniken erkennen muss.

Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Schreibzugriff
- Erforderliche Rolle: sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

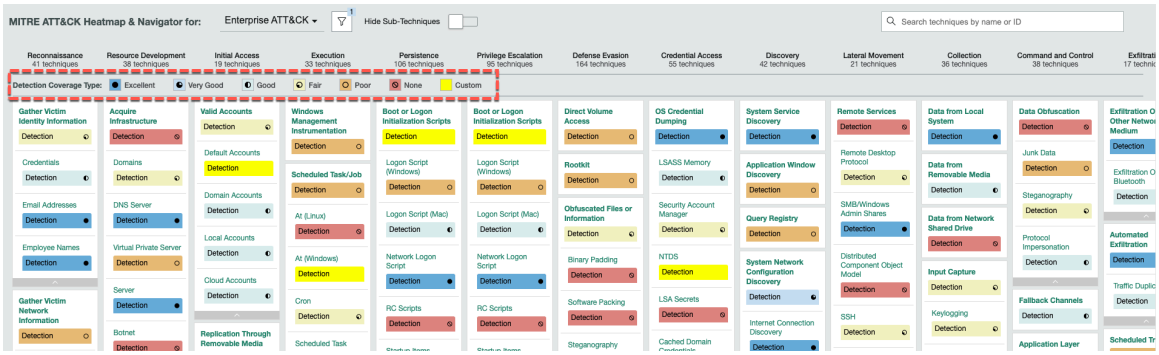
Die Definitionen der Technikabdeckung werden in der allgemeinen Technikerkennungszuordnung verwendet. Sie können die Abdeckung der Basissystemtechnik verwenden. Die Abdeckung der Basissystemtechnik Besteht aus den Abdeckungstypen „keine“, „schlecht“, „fair“, „gut“, „sehr gut“, und ausgezeichnet. Die Abdeckung der Basissystemtechnik ist auch vordefinierten Farben zugeordnet. Sie können die Abdeckungstypeinträge und -Farben anpassen oder eigene Einträge erstellen. Sie können beispielsweise die Abdeckungstypen des Basissystems in „nicht zutreffend“, „Teilabdeckung“ und „Abdeckung abschließen“ ändern. Alternativ können Sie auch numerische Messungen für die Abdeckungstypen erstellen, z. B. 0-25 Prozent, 25 bis 50 Prozent und 50 bis 100 Prozent. Die Art der Änderungen, die an der Basissystemabdeckung vorgenommen werden, ist nicht auf die freigegebenen Beispiele beschränkt.

Die Anpassungen, die Sie am Abdeckungstyp und an der Farbe vornehmen, werden in verwendet Allgemeine Technikerkennungszuordnung Und auch in Heatmap .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie die Abdeckungsdefinition des Basissystems ändern, werden die Symbole für Abdeckungstyp nicht mit den Techniken in der Heatmap angezeigt. Die Heatmap funktioniert erwartungsgemäß, wenn Sie dieselben Felder ändern, wie die vom Basissystem definierten Technikerkennungsfarben und Abdeckungsfarben. Wenn Sie jedoch vorhandene Felder aus der Gesamterkennungsabdeckung für Technik löschen, werden in der Heatmap die Symbole für den Abdeckungstyp nicht angezeigt.



Prozedur

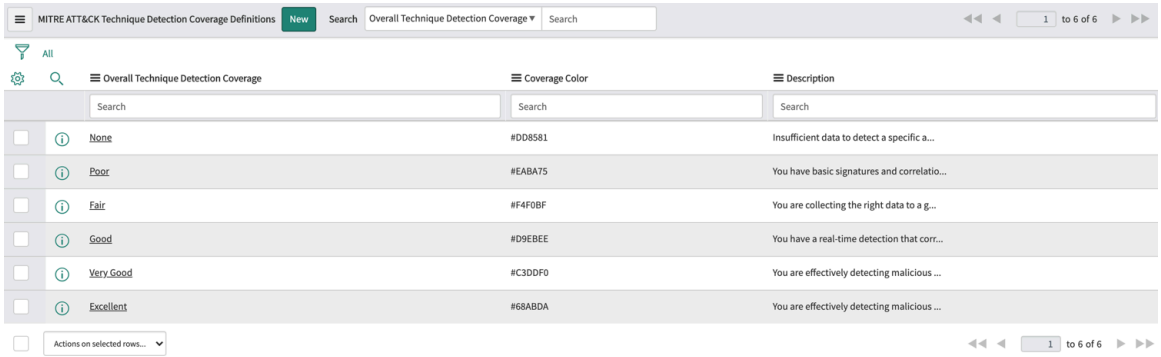
1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Definition der Erkennungsabdeckung**an.
2. Überprüfen Sie die allgemeinen Technikerkennungseinträge, und passen Sie die Einträge für Ihre Umgebung an.

Definition der Erkennungsabdeckung

Feld	Beschreibung
Technik-Erkennungsabdeckung gesamt	Name der allgemeinen Technikerkennungsabdeckung. Die Abdeckung der Basissystemtechnik Besteht aus „keine“, „schlecht“, „fair“, „gut“, „sehr gut“, oder ausgezeichnet.
Abdeckungsfarbe	Farbe, die der Punktzahl der Erkennungsabdeckung zugewiesen ist. Die von Ihnen definierte Farbe wird für die Technikerkennungsabdeckung in der Heatmap verwendet. Sie können die Farben mithilfe von HEX-Codes und RGB(A)-Werten anpassen.
Beschreibung	Gesamterkennungsabdeckung für Technik. Siehe Basissystemdefinition in Bewertungsdefinition .

Die folgende Abbildung zeigt die Liste „Definition der Erkennungsabdeckung“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf, um einen Eintrag hinzuzufügen **Neu** , Vervollständigen Sie die Einträge, und klicken Sie auf **Übermitteln** .

MITRE-ATT&CK Bewertungsdefinition

Definieren Sie die Ihrer Organisation MITRE-ATT&CK Bewertungssystem, mit dem Sie messen können, wie effektiv Ihre Organisation bestimmte Angreifertechniken erkennen kann.

Bewertungsdefinition

Punktzahl	Punktzahlzuordnung	Beschreibung
Keine	0	Unzureichende Daten, um eine bestimmte Angreifertechnik zu erkennen.
Mangelhaft	1	Grundlegende Signaturen und Korrelationsregeln sind vorhanden, um bestimmte Angreifertechniken zu erkennen. Die Bedrohungserkennung erfolgt nicht in Echtzeit und deckt nur eine minimale Anzahl von Aspekten einer Technik ab. Beispielsweise findet die Jagd jeweils nur an einem Endpunkt statt. Ihre Organisation hat möglicherweise noch Tausende oder Hunderte von Ereignissen, die Jäger überprüfen und mit anderen Ereignissen korrelieren müssen, um Ausreißer zu finden. Die Anzahl der falsch positiven Ergebnisse ist hoch.
Befriedigend	2	Die Erfassung der richtigen Daten in großem Umfang und die Datenqualität ist fair. Beispielsweise könnte Ihre Organisation beginnen, Sysmon-Protokolle, ETW, PowerShell-Protokolle usw. hinzuzufügen. Die Bedrohungserkennung erfolgt jedoch immer noch nicht in Echtzeit. Ihre Organisation verfügt möglicherweise nicht über die richtigen Tools, um die Daten effektiv zusammenzufassen und zu analysieren. Jäger müssen manuell Abfragen ausführen und korrelieren, um die Daten genau zu analysieren. Die Anzahl der falsch positiven Ergebnisse ist hoch.
Gut	3	Echtzeiterkennung, die mehrere Daten über Ihre Endpunkte hinweg korreliert und integriert. Die Bedrohungserkennung deckt viele Aspekte der Verfahren einer Technik ab. Ihre Angreifer könnten die Erkennung möglicherweise durch Ausweichen und Verschleierung umgehen. Ihre Organisation kann einfach falsch positive Ergebnisse identifizieren und herausfiltern. Ihre Organisation verwendet grundlegende

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bewertungsdefinition (Fortsetzung)

Punktzahl	Punktzahlzuordnung	Beschreibung
		datenwissenschaftliche Techniken, um die Daten im zentralen Repository zu analysieren.
Sehr gut	4	Erkennen Sie schädliche Techniken effektiv in Echtzeit, und decken Sie die meisten Aspekte der Verfahren einer Technik ab. Die Möglichkeit, dass Ihre Angreifer die Erkennung mit Ausweichungs- und Verschleierungsmethoden umgehen, ist schwieriger als auf einem guten Niveau. Ihre Organisation kann einfach falsch positive Ergebnisse identifizieren und herausfiltern. Ihre Organisation verwendet erweiterte Data Science-Techniken, um die Angreifertechniken zu erkennen.
Ausgezeichnet	5	Erkennen Sie schädliche Techniken effektiv in Echtzeit, und decken Sie alle Aspekte der Verfahren einer Technik ab. Ihre Organisation hat ein gutes Verständnis Ihrer Umgebung mit der richtigen Automatisierung und Datenqualität. Die Möglichkeit, dass Ihre Angreifer die Erkennung mit Ausweichungs- und Verschleierungsmethoden umgehen, ist auf dieser Ebene nicht möglich. Die Anzahl der falsch negativen Elemente ist niedrig.

Ordnen Sie Ihre Technikerkennungsabdeckung einer Technik zu

Ordnen Sie Ihre Gesamterkennungsabdeckung für Technik mit der Technik zu, mit der Ihre Organisation bestimmte Angreifertechniken erkennen kann.

Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Schreibzugriff
- Erforderliche Rolle: sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Technik-Erkennungsabdeckung verwenden, um einen Überblick über die gesamte Technik-Erkennungsabdeckung Ihrer Organisation zu erhalten. Wenn beispielsweise ein Angreifer Ihre Organisation angreift, wird die Art der Abdeckung angezeigt, die Sie benötigen, um die Techniken des Angreifers zu erkennen.

Die Technik und die ID werden automatisch für alle ausgefüllt Sammlungen Und Techniken Die Sie aktiviert haben. Die Abdeckungstyp und Bewertungsdefinition Die Sie definiert haben, sind für als Option verfügbar, die Sie in der Gesamterkennungsabdeckung für Technik auswählen können.

Sie können die gesamte Technikerkennungsabdeckung der Technik zuordnen, um die Zuordnung abzuschließen. Sie können eine Technik nur einer allgemeinen Technikerkennungsabdeckung zuordnen.

Die von Ihnen definierte Zuordnung der Technik-Erkennungsabdeckung wird in verwendet Abdeckungsvisualisierung in der Heatmap .

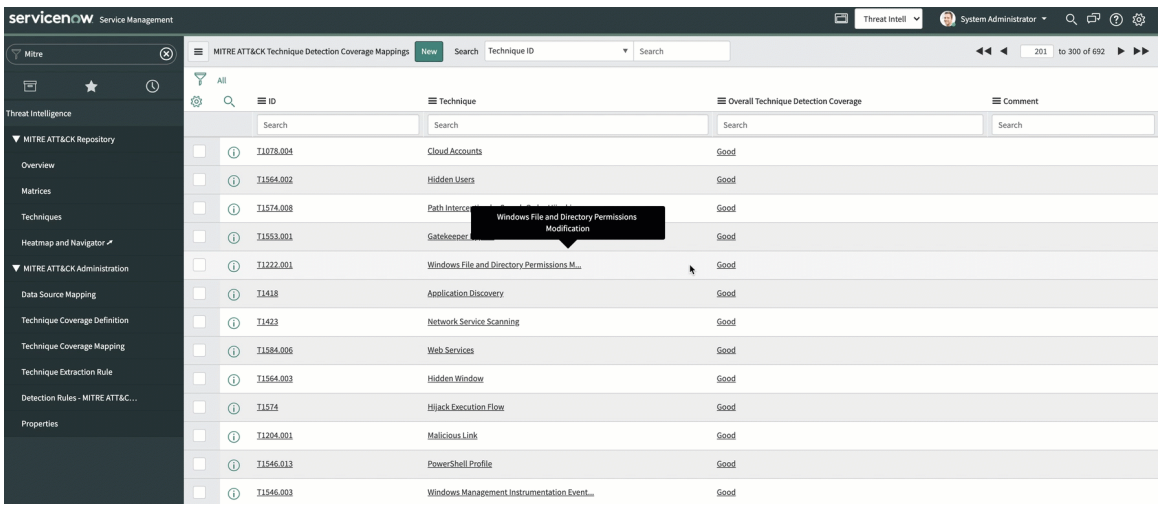
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie können die Gesamterkennungsabdeckung für Technik mithilfe Ihrer organisationsspezifischen Berechnungen erreichen. Sie können beliebige Breach & Attack Simulation (BAS)-Produkte, das Cyber Analytics Repository (CAR) oder andere Methoden nach Bedarf verwenden, um die Bewertungsdefinition zu definieren, und sie in diesem Verfahren für die Zuordnung der Gesamterkennungsabdeckung für Technik verwenden.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Zuordnung der Abdeckung durch Erkennung**an.

   In dieser Abbildung sehen Sie, dass die Untertechnik „Cloud-Accounts“ (T1078.004) eine ausgezeichnete Abdeckung in der Organisation aufweist und dass die Gesamterkennungsabdeckung der Technik zugeordnet ist **Ausgezeichnet** .



2. Überprüfen Sie jede Technik, und ordnen Sie Ihre Gesamterkennungsabdeckung für Technik basierend auf Ihren zu Definition der Erkennungsabdeckung Und die Abdeckungsverfügbarkeit Ihrer Organisation.

Definieren Sie die Minderungsabdeckung

Definieren Sie die Minderungsabdeckung für jede Minderungsmaßnahme, die einer Technik zugeordnet ist, damit Sie Einblick erhalten, wie gut Ihre Organisation die Angriffe verhindern kann, die aufgrund einer bestimmten Technik passieren.

Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- Erforderliche Rolle: sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Die Definitionen der Minderungsabdeckung werden in der Zuordnung der Gesamtreinderung und der Technikabdeckung verwendet. Sie können die Basissystem-Minderungsabdeckung verwenden. Die Basissystem-Minderungsabdeckung besteht aus den Abdeckungstypen „keine“, „schlecht“, „fair“, „gut“, „sehr gut“, „sehr gut“, und ausgezeichnet. Die Abdeckung der Basissystemminderung ist auch mit vordefinierten Farben und Abdeckungsprozentsätzen verknüpft. Sie können die Abdeckungstypen (Abdeckungstypen hinzufügen oder entfernen), Abdeckungsprozentsätze für niedrigere und höhere Grenzwerte und Farben anpassen oder Ihre anwenderdefinierte Minderungsabdeckung erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Anpassungen, die Sie an den Abdeckungstypen, Farben oder Prozentsätzen vornehmen, werden in der Zuordnung der Minderungsabdeckung und auch in verwendet Heatmap .

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Definition der Abdeckung durch Risikominderung**an.
2. Überprüfen Sie die Einträge der Minderungserkennung, und passen Sie die Einträge für Ihre Umgebung an.

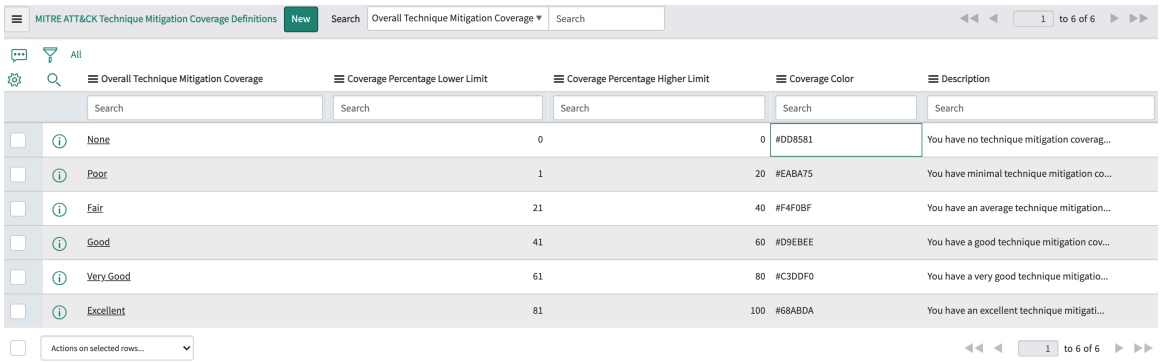
Technik – Definition der Abdeckung durch Risikominderung

Feld	Beschreibung
Abdeckung durch Risikominderung für Techniken gesamt	Name der Abdeckung der Technikminderung. Die Basissystem-Minderungsabdeckung Besteht aus „keine“, „schlecht“, „fair“, „gut“, „sehr gut“, oder ausgezeichnet.
Unterer Grenzwert des Abdeckungsprozentsatzes	Die untere prozentuale Grenze der Minderungsabdeckung. Definieren Sie die numerischen Werte zwischen 0 und 100.
Oberer Grenzwert des Abdeckungsprozentsatzes	Die höhere prozentuale Grenze der Minderungsabdeckung. Definieren Sie die numerischen Werte zwischen 0 und 100.
Abdeckungsfarbe	Farbe, die der Punktzahl der Erkennungsabdeckung zugewiesen ist. Die von Ihnen definierte Farbe wird für die Abdeckung der Technikminderung in der Heatmap verwendet. Sie können die Farben mithilfe von HEX-Codes und RGB(A)-Werten anpassen.
Beschreibung	Gesamtabdeckung der Minderungserkennung. Siehe Basissystemdefinition in Definition der Abdeckung der Technikminderung .

Hinweis:
Stellen Sie sicher, dass Sie die Abdeckungsprozentsatzbereiche nicht überschneiden, wenn Sie die Prozentgrenzen anpassen (niedriger oder höher). Wenn beispielsweise ein Abdeckungsdatensatz die Bereiche 0 bis 20 aufweist, muss der nächste aufeinanderfolgende Datensatz einen unteren Grenzwert von 21 oder höher aufweisen, um zu vermeiden, dass sich der Abdeckungsprozentsatzbereich überschneidet.

Die folgende Abbildung zeigt die Definitionsliste der Minderungsabdeckung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf, um einen Eintrag hinzuzufügen **Neu** , Vervollständigen Sie die Einträge, und klicken Sie auf **Übermitteln** .

Definitionen der Abdeckung der Technikminderung

Definieren Sie die Minderungsabdeckung Ihrer Organisation, damit Sie bestimmte Angreifertechniken effektiv messen und erkennen können.

MITRE ATT&CK – Definitionen für Abdeckung durch Risikominderung für Techniken

Abdeckung durch Risikominderung für Techniken gesamt	Unterer Grenzwert des Abdeckungsprozent	Oberer Grenzwert des Abdeckungsprozent	Abdeckungsfarbe	Beschreibung
Keine	0	0	NR. DD8581	Sie haben keine Abdeckung zur technischen Minderung, und Ihre Verteidigungssteuerungen können in keinem Szenario einen Angriff verhindern.
Mangelhaft	1	20	#EABA75	Sie haben eine minimale Abdeckung zur Verringerung der Technik. Die Wahrscheinlichkeit eines Angriffs ist sehr hoch, und Ihre Verteidigungskontrollen können einen Angriff in 0 bis 20 Prozent der Szenarien verhindern.
Befriedigend	21	40	#F4F0BF	Sie haben eine durchschnittliche Abdeckung zur Verringerung der Technik. Die Wahrscheinlichkeit

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MITRE ATT&CK – Definitionen für Abdeckung durch Risikominderung für Techniken (Fortsetzung)

Abdeckung durch Risikominderung für Techniken gesamt	Unterer Grenzwert des Abdeckungsprozent	Oberer Grenzwert des Abdeckungsprozent	Abdeckungsfarbe	Beschreibung
				eines Angriffs ist hoch, und Ihre Verteidigungskontrollen können einen Angriff in 21 bis 40 Prozent der Szenarien verhindern.
Gut	41	60	#D9EBEE	Sie haben eine gute Abdeckung zur Verringerung der Technik. Die Wahrscheinlichkeit eines Angriffs ist jedoch relativ hoch, und Ihre Verteidigungskontrollen können einen Angriff in 41 bis 60 Prozent der Szenarien verhindern.
Sehr gut	61	80	#C3DDF0	Sie haben eine sehr gute Abdeckung zur Verringerung der Technik. Die Wahrscheinlichkeit eines Angriffs ist gering, und Ihre Verteidigungskontrollen können einen Angriff in 61 bis 80 Prozent der Szenarien verhindern.
Ausgezeichnet	81	100	#68ABDA	Sie verfügen über eine ausgezeichnete Abdeckung zur Verringerung der Technik, und die Wahrscheinlichkeit eines Angriffs mit dieser Technik ist sehr gering, und Ihre Verteidigungskontrollen können einen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MITRE ATT&CK – Definitionen für Abdeckung durch Risikominderung für Techniken (Fortsetzung)

Abdeckung durch Risikominderung für Techniken gesamt	Unterer Grenzwert des Abdeckungsprozent	Oberer Grenzwert des Abdeckungsprozent	Abdeckungsfarbe	Beschreibung
				Angriff in 81 bis 100 Prozent der Szenarien verhindern.

Ordnen Sie Ihre Minderungsabdeckung einer Technik zu

Ordnen Sie Ihre Minderungsabdeckung mit der Technik zu, mit der Sie die allgemeine Minderungsstrategie Ihrer Organisation erkennen können.

Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Schreibzugriff, Löschzugriff
- Erforderliche Rolle: sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Mit Minderungen können Sie verhindern, dass Angreifer Techniken oder Untertechniken erfolgreich für Ihre Organisation ausführen. Jeweils MITRE-ATT&CK Die Technik enthält Minderungen, die Sie in Ihrer Organisation bereitstellen können, um die Wahrscheinlichkeit eines Angriffs zu reduzieren. Sie können die Minderungsabdeckung verwenden, um einen Überblick über die allgemeine Minderungsstrategie Ihrer Organisation zu erhalten. Wenn beispielsweise ein Angreifer Ihre Organisation angreift, wird die Art der Abdeckung angezeigt, die Sie haben, um die Techniken des Angreifers zu mindern.

Die Technik- und Minderungsinformationen werden automatisch für alle von Ihnen aktivierten Sammlungen und Techniken ausgefüllt. Die Definition der Minderungsabdeckung Die Sie definiert haben, können Sie in der Abdeckung zur Verringerung der Technik auswählen.

Sie können Minderungen identifizieren, die für Ihre Organisation relevant sind. Wenn eine Minderung relevant ist, können Sie definieren, ob die Minderungsstrategien bereitgestellt wurden. Sie können angeben, ob die Strategien als Teil der SOC-Richtlinie Ihrer Organisation angewendet werden. Sie können auch identifizieren, ob Ihre Organisation über vorbeugende Tools verfügt, um die Techniken eines Angreifers zu mindern, und Sie können alle Sicherheitskontrollen zuordnen, die Ihre Organisation bereitgestellt hat, um Sicherheitsrisiken zu minimieren. Füllen Sie die Minderungsabdeckung (Prozentsatz) für jeden der Datensätze aus.

Nach der Zuordnung der Informationen für jede der Techniken Rechner für Minderungsabdeckung Füllt die berechnete Abdeckung der Technikminderung automatisch aus. Um die Gesamtabdeckung der Risikominderung für jede Technik zu berechnen, müssen die Zuordnungsdatensätze der Technikminderung aktiv und für die Organisation relevant sein. Die Datensätze, die inaktiv und nicht relevant sind, werden bei der Berechnung der Gesamtabdeckung zur Verringerung der Technik nicht berücksichtigt. Basierend auf den Werten in der berechneten Technikminderungsabdeckung und in Definition der Minderungsabdeckung , Ihre Gesamtabdeckung zur Verringerung der Technik (berechnet) wird ausgefüllt.

Die Anpassungen, die Sie an den Abdeckungstypen, Farben oder Prozentsätzen vornehmen, werden in der Zuordnung der Minderungsabdeckung und auch in verwendet Heatmap .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Zuordnung der Abdeckung durch Risikominderung**an.
2. Überprüfen Sie die einzelnen Techniken zur Risikominderungszuordnung, und aktualisieren Sie die **Minderungsabdeckung (Prozentsatz)** Um die Abdeckungsverfügbarkeit Ihrer Organisation zu berechnen.

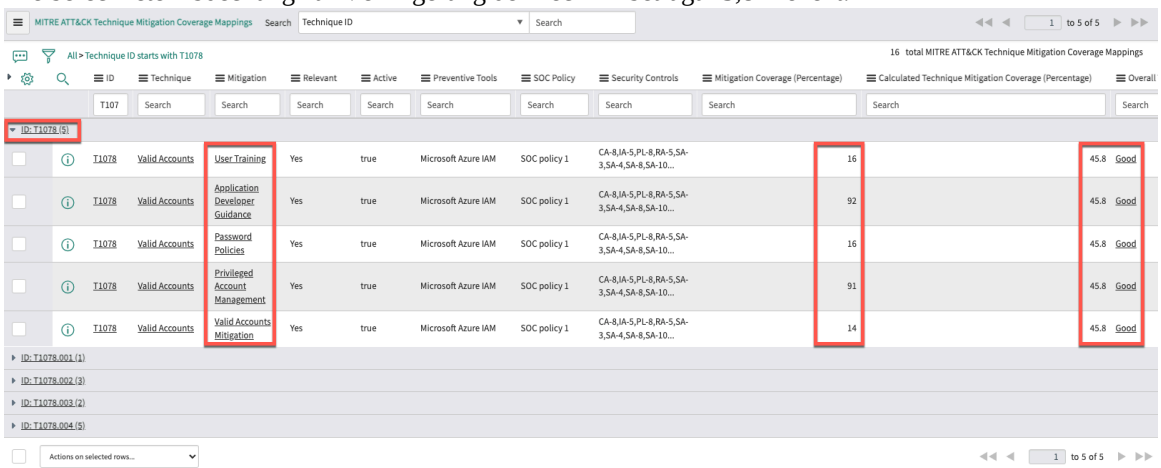
Zuordnungen Der Abdeckung Der Technikverringerung

Feld	Beschreibung
ID	Eindeutige Identität der Technik. Die IDs werden automatisch für alle von Ihnen aktivierten Sammlungen und Techniken ausgefüllt.
Technik	Wie ein Angreifer durch Ausführen einer Aktion ein taktisches Ziel erreicht. Die Technikinformationen werden automatisch für alle von Ihnen aktivierten Sammlungen und Techniken ausgefüllt.
Mitigation	Minderungen, mit denen Sie verhindern können, dass Angreifer Techniken oder Untertechniken erfolgreich für Ihre Organisation ausführen. Die Minderungsinformationen werden automatisch für alle von Ihnen aktivierten Sammlungen und Techniken ausgefüllt.
Relevantes Element	Option, um anzugeben, ob die Minderung für Ihre Organisation relevant ist.
Aktiv	Option, um anzugeben, ob die Minderungsstrategien in Ihrer Organisation bereitgestellt werden. Dies ist eine erforderliche Option, die zum Berechnen der Abdeckung der Technikminderung erforderlich ist.
Tools zur Vorbeugung	Option, um anzugeben, ob Ihre Organisation über vorbeugende Tools verfügt, um die Techniken eines Angreifers zu mindern.
SOC-Richtlinie	Die SOC-Richtlinien, die die Minderungsstrategien in Ihrer Organisation definieren.
Sicherheitskontrollen	Die Sicherheitskontrollen Ihrer Organisation enthalten die Minderungsstrategien zur Minimierung von Sicherheitsrisiken.
Abdeckung durch Risikominderung (Prozentsatz)	Ein Bewertungssystem zur Berechnung der Abdeckung der Technikminderung. Definieren Sie numerische Werte zwischen 0 und 100. Dies ist eine erforderliche Option, die zum Berechnen der Abdeckung der Technikminderung erforderlich ist.
Berechnete Abdeckung durch Risikominderung für Techniken (Prozentsatz)	Die berechnete Abdeckung der Technikminderung in Prozent. Dieser Wert wird basierend auf der in definierten Formel bestimmt Rechner für Minderungsabdeckung .
Abdeckung durch Risikominderung für Techniken insgesamt (berechnet)	Die Gesamtabdeckung zur Verringerung der Technik. Dieser Wert wird basierend auf bestimmt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Minderungsabdeckung, die für Ihre Organisation definiert ist .
Kommentar	Beschreibung der Zuordnung der Technik und der Minderungsabdeckung.
Widerrufen	Die Zuordnung von Technik zu Minderungsabdeckung wird widerrufen.

In dieser Abbildung sehen Sie, dass der Technik „gültige Accounts“ fünf Minderungen zugeordnet sind, jeweils mit einer Minderungsabdeckung von 16 für Anwenderschulungen, 92 für Anleitungen für Anwendungsentwickler und 16 für Passwortrichtlinien, 91 für privilegierte Account-Verwaltung und 14 für die Minderung gültiger Accounts. Die berechnete Abdeckung zur Verringerung der Technik beträgt 45,8 Prozent.



Rechner für die Gesamtabdeckung der Technikverringerung

Die Gesamtabdeckung der Technik zur Minderung wird basierend auf der im Rechner der Minderungsabdeckung definierten Formel bestimmt.

Vorbereitungen

- Erforderliche Rolle: sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- Erforderliche Rolle: sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

- Sie können nur einen Rechner für die Minderungsabdeckung pro Domäne auf „aktiv“ festlegen.
- Der Rechner für die Abdeckung der Minderung des Basissystems ist ein Durchschnittsrechner.
- Alle Anpassungen am Rechnerskript sollten sicherstellen, dass die endgültige Ausgabe ein numerischer Wert zwischen 0 und 100 ist.
- Die Definition der Minderungsabdeckung wird basierend auf dem Bereich der endgültigen Ausgabe angewendet.

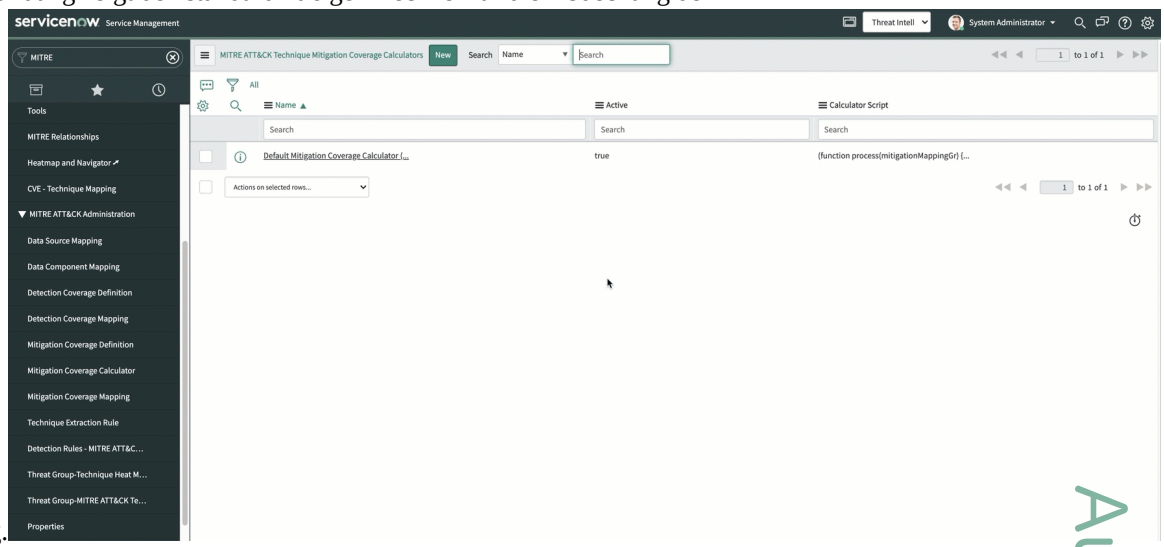
Prozedur

Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Rechner für Abdeckung durch Risikominderung**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt den standardmäßigen Rechner für die Abdeckung der Risikominderung.



Erstellen und ordnen Sie Erkennungsregeln zu

Erstellen Sie Erkennungsregeln, und ordnen Sie sie den Taktiken und Techniken zu. Mit dieser Zuordnung können Sie die Abdeckung für die Erkennungsregeln in Ihrer Organisation anzeigen.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

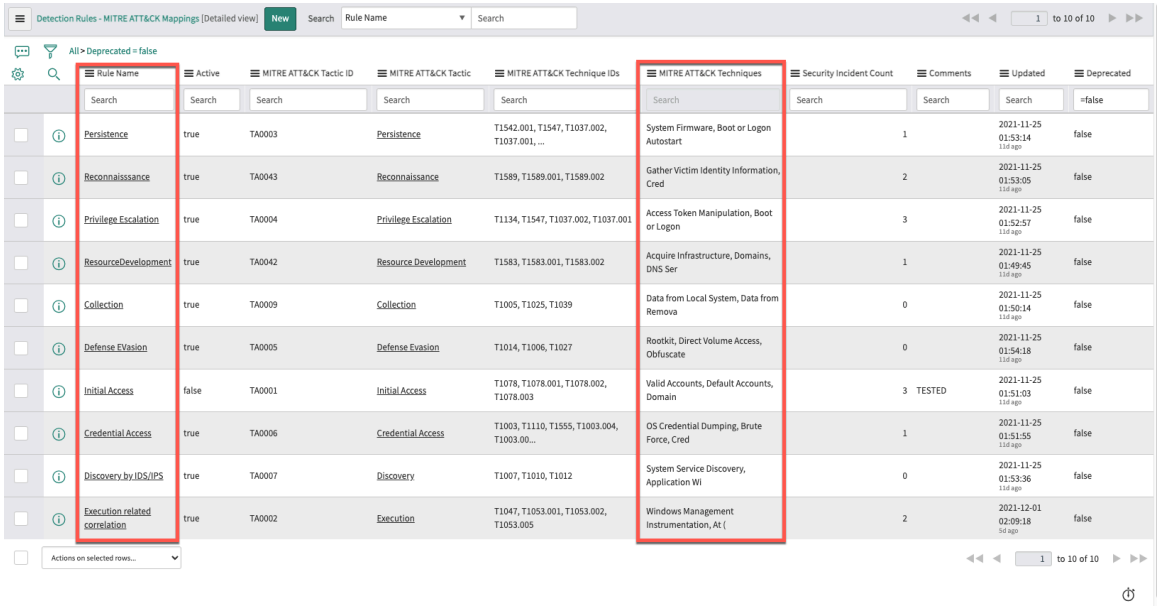
Mit der Erkennungsregelzuordnung kann Ihre Organisation sehen, welche Erkennungsregeln zur Identifizierung bestimmter Techniken verfügbar sind.

Der primäre Zweck der Zuordnung besteht darin, Transparenz zu bieten, wenn Ihre Organisation über die erforderlichen Erkennungsregeln verfügt, um zu identifizieren, wann eine Warnung oder ein Ereignis infolge eines Angriffs durch einen Angreifer mit einer bestimmten Technik ausgelöst wird.

Sehen Sie sich beispielsweise die folgende Abbildung an, die eine Liste der Erkennungsregeln zeigt, die verschiedenen Techniken zugeordnet sind. Sie können diese Informationen auch in anzeigen der/die/das MITRE-ATT&CK navigatoran.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie die automatischen SIEM-Extraktionsregeln des Basissystems nicht verwenden möchten, aktivieren Sie das automatische Rollup von MITRE-ATT&CK TTPs basierend auf der Erkennungsregelzuordnung. Sie können die Warnungs- oder Ereignisregel ausfüllen, die den Security Incident in auslöst Warnungsregel Namensfeld. Sie können auch ausfüllen Warnungsregel Namensfeld mithilfe von SIEM-Integration, E-Mail-Analyse, manueller Erstellung usw. Weitere Informationen finden Sie unter Rollup MITRE-ATT&CK Informationen aus Erkennungsregeln.

Hinweis:

Die Erkennungsregelfunktion wurde aktualisiert und umfasst die Zuordnung einer einzelnen Taktik zu mehreren Techniken. Zuvor konnten Sie eine einzelne Taktik einer einzelnen Technik zuordnen. Wenn Sie ein Upgrade von durchführen Threat Intelligence Plugin von Version 12.0.4 zu einer höheren Version überprüfen Sie dann die folgenden Punkte, bevor Sie die Erkennungsregeln in verwenden MITRE-ATT&CK Modul.

- Sie finden mehrere Datensätze, die in einem einzigen Datensatz zusammengeführt wurden, wenn die Felder – Regelname, Warnungssensor, Quelle, Kategorie, Unterkategorie, und MITRE-ATT&CK Taktiken sind häufig.
- Die alten Datensätze sind in der Spalte „veraltet“ als „wahr“ und in der Spalte „aktiv“ als „falsch“ markiert.
- Die neuen zusammengeführten Datensätze können verwendet werden und sind in der Spalte „veraltet“ als „falsch“ und in der Spalte „aktiv“ als „wahr“ markiert.
- Nachdem Sie das Upgrade verifiziert und angezeigt haben, dass alle Ihre Erkennungsregeln erfolgreich migriert wurden, können Sie die alten Datensätze löschen, die in der Spalte „veraltet“ als „wahr“ markiert sind.

Prozedur

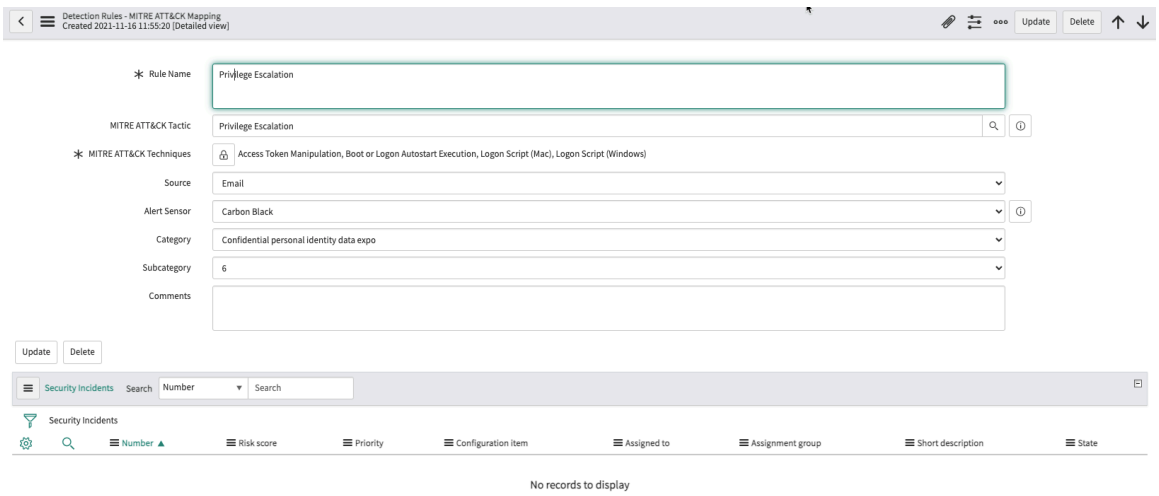
1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Erkennungsregeln – MITRE ATT&CK-Zuordnungen**an.
2. Verwenden Sie eine der folgenden Methoden, um Ihre Erkennungsregel zu erstellen:
   Methode 1: Erkennungsregeln manuell erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie Auf **Neu** Und füllen Sie die Felder im Formular aus.

Erkennungsregeln – MITRE-ATT&CK Zuordnung

Feld	Beschreibung
Regelname	Name der Erkennungsregel.
MITRE-ATT&CK Taktik	Relevant MITRE-ATT&CK Taktik.
MITRE-ATT&CK Techniken	Relevant MITRE-ATT&CK Technik. Sie können mehrere Techniken für eine einzelne Taktik auswählen.
Quelle	Quelle des Security Incidents, z. B. E-Mail, Firewall, Netzwerküberwachung usw.
Warnungssensor	Sicherheitsintegration, über die Sie Warnungs- oder Ereignisdaten wie CarbonBlack, CrowdStrike, McAfee usw. erfassen.
Unterkategorie	Unterkategorie, die das Problem weiter definiert.
Kategorie	Kategorie, die den Typ des Sicherheitsproblems identifiziert.
MITRE-ATT&CK Technik	Relevant MITRE-ATT&CK Technik. Sie können mehrere Techniken für eine einzelne Taktik auswählen.
Anzahl der Security Incidents	Die Anzahl der Security Incidents, an die die Techniken angehängt sind. Diese Anzahl wird angezeigt, wenn Sie das Rollup von aktiviert haben MITRE-ATT&CK Informationen automatisch von Warnungsregeln zu Security Incidents.
Überholt	Die Erkennungsregelzuordnung ist veraltet.
Aktiv	Option zum Festlegen, ob die Erkennungsregel aktiv und in Ihrer Umgebung bereitgestellt ist.



b. Klicken Sie auf **Absenden**.

Methode 2: Importieren und erstellen Sie Erkennungsregeln.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

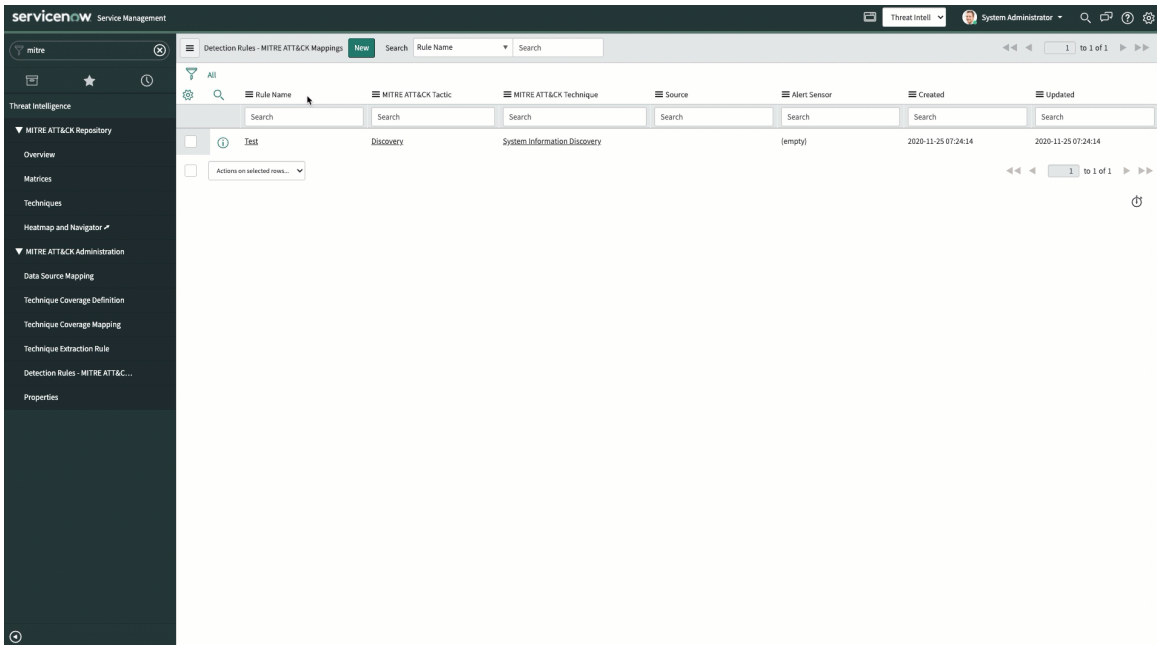
a. Klicken Sie mit der rechten Maustaste auf den Header der Spalte „Regelname“.

b. Klicken Sie in der Liste auf **Importieren** .

c. Klicken Sie Auf **Erstellen Sie eine Excel-Vorlage** .

d. Klicken Sie Auf **Herunterladen** Nachdem der Export abgeschlossen ist. Eine Excel-Vorlage mit dem Dateinamen sn_ti_Alert_rules_Mitre_Attack_technique_Mapping wird auf Ihren Computer heruntergeladen.

In der folgenden Abbildung sehen Sie, wie Sie die Excel-Vorlage exportieren, die Details in der Tabelle ausfüllen, die Datei hochladen, eine Vorschau der Felder anzeigen und wieder in importieren ServiceNow AI Platform.



e. Öffnen Sie die Tabelle, wählen Sie die Registerkarte „zweites Blatt“ aus, und überprüfen Sie, was Sie eingegeben haben. Füllen Sie die Felder im Formular aus, und speichern Sie dann Ihre Datei.

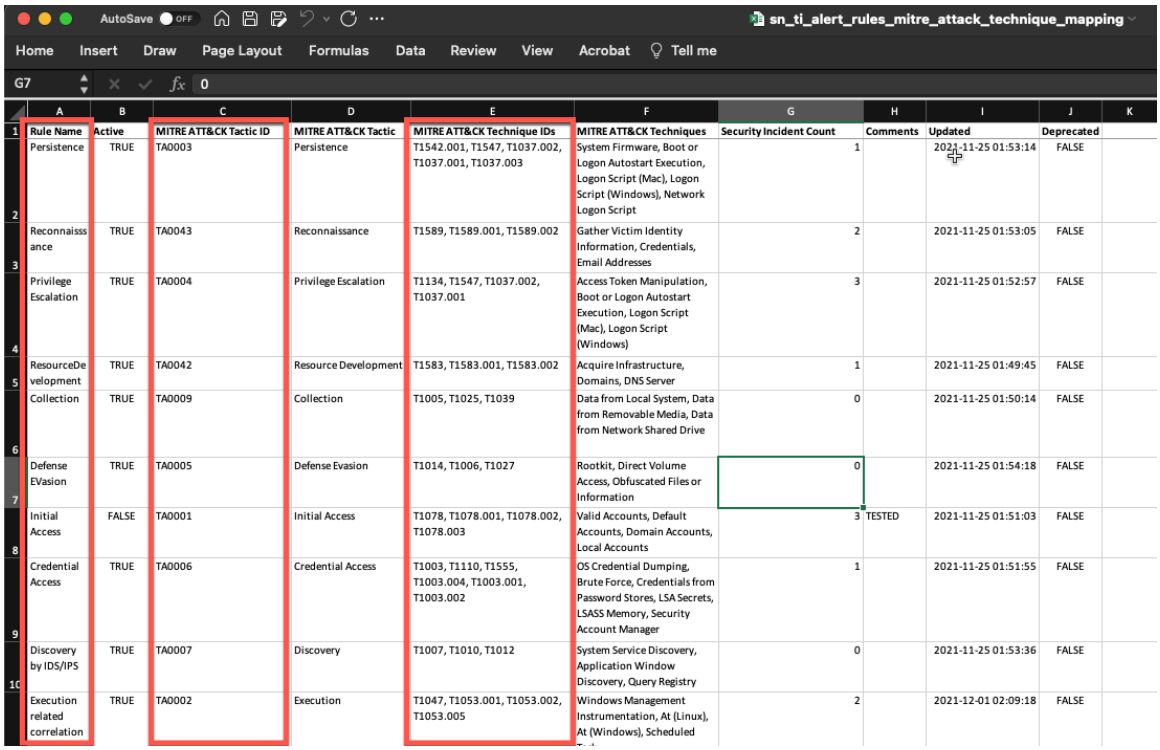
Vorlage importieren

Feld	Beschreibung
Regelname	Name der Erkennungsregel.
Aktiv	Option zum Festlegen, ob die Erkennungsregel aktiv und in Ihrer Umgebung bereitgestellt ist.
Warnungssensor	Sicherheitsintegration, über die Sie Warnungs- oder Ereignisdaten wie CarbonBlack, CrowdStrike, McAfee usw. erfassen.
Kategorie	Kategorie, die den Typ des Sicherheitsproblems identifiziert.
Kommentare	Beschreibung der Erkennungsregel.
Überholt	Die Erkennungsregelzuordnung ist veraltet.
MITRE-ATT&CK Technik-IDs	MITRE-ATT&CK Technik-ID, z. B. T1546.008, für Barrierefreiheitsfunktionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MITRE-ATT&CK Taktik-ID	MITRE-ATT&CK Taktik-ID, z. B. TA0003, für Persistenz.
Anzahl der Security Incidents	Die Anzahl der Security Incidents, an die die Techniken angehängt sind. Diese Anzahl wird angezeigt, wenn Sie das Rollup von aktiviert haben MITRE-ATT&CK Informationen von Warnungsregeln zu Security Incidents automatisch, und die Erkennungsregel ist aktiv.
Quelle	Quelle des Security Incidents, z. B. E-Mail, Firewall, Netzwerküberwachung usw.
Unterkategorie	Unterkategorie, die das Problem weiter definiert.
MITRE-ATT&CK Taktik	Relevant MITRE-ATT&CK Taktik.
MITRE-ATT&CK Technik	Relevant MITRE-ATT&CK Technik.

Die folgende Abbildung zeigt die Tabellenkalkulationsvorlage. Die Pflichtfelder sind rot hervorgehoben – Regelname, MITRE-ATT&CK Taktik-ID und MITRE-ATT&CK Technik-ID.



Rule Name	Active	MITRE ATT&CK Tactic ID	MITRE ATT&CK Tactic	MITRE ATT&CK Technique IDs	MITRE ATT&CK Techniques	Security Incident Count	Comments	Updated	Deprecated
Persistence	TRUE	TA0003	Persistence	T1542.001, T1547, T1037.002, T1037.001, T1037.003	System Firmware, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows), Network Logon Script	1		2021-11-25 01:53:14	FALSE
Reconnaissance	TRUE	TA0043	Reconnaissance	T1589, T1589.001, T1589.002	Gather Victim Identity Information, Credentials, Email Addresses	2		2021-11-25 01:53:05	FALSE
Privilege Escalation	TRUE	TA0004	Privilege Escalation	T1134, T1547, T1037.002, T1037.001	Access Token Manipulation, Boot or Logon Autostart Execution, Logon Script (Mac), Logon Script (Windows)	3		2021-11-25 01:52:57	FALSE
ResourceDevelopment	TRUE	TA0042	Resource Development	T1583, T1583.001, T1583.002	Acquire Infrastructure, Domains, DNS Server	1		2021-11-25 01:49:45	FALSE
Collection	TRUE	TA0009	Collection	T1005, T1025, T1039	Data from Local System, Data from Removable Media, Data from Network Shared Drive	0		2021-11-25 01:50:14	FALSE
Defense EVasion	TRUE	TA0005	Defense Evasion	T1014, T1006, T1027	Rootkit, Direct Volume Access, Obfuscated Files or Information	0		2021-11-25 01:54:18	FALSE
Initial Access	FALSE	TA0001	Initial Access	T1078, T1078.001, T1078.002, T1078.003	Valid Accounts, Default Accounts, Domain Accounts, Local Accounts	3	TESTED	2021-11-25 01:51:03	FALSE
Credential Access	TRUE	TA0006	Credential Access	T1003, T1110, T1555, T1003.004, T1003.001, T1003.002	OS Credential Dumping, Brute Force, Credentials from Password Stores, LSA Secrets, LSASS Memory, Security Account Manager	1		2021-11-25 01:51:55	FALSE
Discovery by IDS/IPS	TRUE	TA0007	Discovery	T1007, T1010, T1012	System Service Discovery, Application Window Discovery, Query Registry	0		2021-11-25 01:53:36	FALSE
Execution related correlation	TRUE	TA0002	Execution	T1047, T1053.001, T1053.002, T1053.005	Windows Management Instrumentation, At (Linux), At (Windows), Scheduled	2		2021-12-01 02:09:18	FALSE

f. Klicken Sie Auf **Wählen Sie die Datei aus** Und wählen Sie die Tabelle auf Ihrem Computer aus.

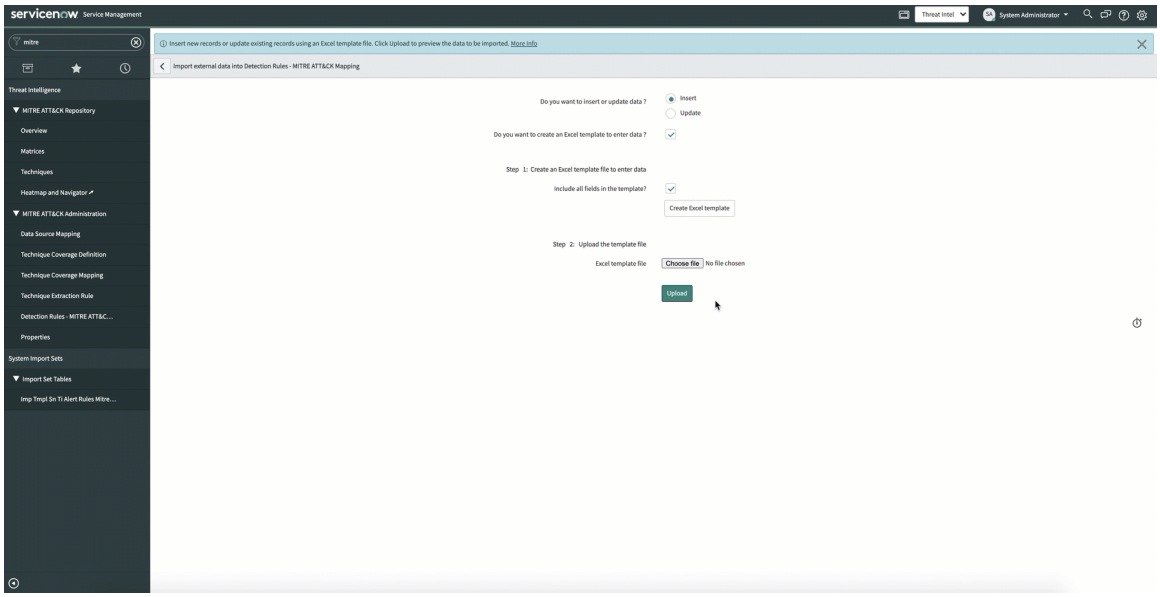
g. Klicken Sie auf **Hochladen**.

h. Klicken Sie Auf **Vorschau Der Importierten Daten Anzeigen** .

i. Zeigen Sie eine Vorschau der Zuordnungen an, und klicken Sie auf **Import Abschließen** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt, wie Sie die Tabelle hochladen, eine Vorschau der Daten anzeigen, Fehler überprüfen und den Importprozess der Erkennungsregelzuordnung abschließen.



Technikregeln für den Import automatisch extrahieren MITRE-ATT&CK Informationen

Verwenden Sie die automatischen Extraktionsregeln des Basissystems, um zu importieren MITRE-ATT&CK Informationen aus vorhandenen Drittpartei-Integrationen.

Automatische Extraktionsregeln für Bedrohungssuche verwenden

Verwenden Sie die Regeln für die automatische Extraktion der Bedrohungssuche, um zu importieren MITRE-ATT&CK Informationen aus vorhandenen Threat Intelligence Drittpartei-Integrationen.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Wenn vorhanden Threat Intelligence Die Integration, z. B. Sandbox oder ein TIPP, unterstützt MITRE-ATT&CK Framework und wenn MITRE-ATT&CK Informationen werden auf jeder Integrationsebene analysiert, und dann werden die Informationen in jedem Ergebnisdatensatz der Bedrohungssuche angezeigt. Jedoch nicht alle Threat Intelligence Integrationen analysieren MITRE-ATT&CK Informationen. Die globale automatische Extraktionsregel für die Bedrohungssuche kann extrahiert werden MITRE-ATT&CK Informationen von allen Threat Intelligence Integrationen.

Sie können einen Rollup von durchführen MITRE-ATT&CK Informationen aus den Ergebnissen der Bedrohungssuche zu einem Security Incident. Für das automatische Rollup von Bedrohungssuchergebnissen zu Security Incidents, Aktivieren Sie die Systemeigenschaft . Alternativ können Sie auch rollup der Informationen manuell Für jede einzelne Bedrohungssuche.

Das Basissystem Threat Intelligence Extrahiert automatisch MITRE-ATT&CK Informationen aus der Rohnutzlast der Drittpartei-Integrationen zum Ergebnisdatensatz der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungssuche, falls vorhanden Threat Intelligence Die Integration bietet Ihnen MITRE-ATT&CK Informationen wie die Technik oder Taktik.

Wenn MITRE-ATT&CK Informationen sind im Feld „Rohnutzlast“ des Bedrohungssuchdatensatzes nicht verfügbar. Sie müssen Ihre eigene Regel für die automatische Extraktion aus der Drittpartei-Integration definieren.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Extraktionsregel für Technik**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „Technik-Extraktionsregel“

Feld	Beschreibung
Name	Name der automatischen Extraktionsregel.
Regeltyp	Regeltyp für automatische Extraktion. Wählen Sie Aus **Bedrohungssuche** .
Automatische Extraktion ignorieren	Einstellung, die standardmäßig gelöscht ist. Diese Einstellung ermöglicht die automatische Extraktion von MITRE-ATT&CK Techniken.
Quell-Engine	Quell-Engine.
Global	Quell-Engine-Einstellung. Wenn Sie die Quell-Engine auf festlegen **Global** , Die Extraktion wird für alle Integrationsergebnisse der Bedrohungssuche ausgeführt.
Beschreibung	Beschreibung der automatischen Extraktionsregel.
Prozessmethode	Regulärer Ausdruck oder eine Skriptmethode, die Sie angeben, um die Technikinformationen aus der Rohnutzlast zu verknüpfen.
Extraktion des regulären Ausdrucks	Option, die Sie für angeben **Zielfeld** Bei Verwendung der Extraktionsmethode des regulären Ausdrucks. Regulärer Ausdruck ist der Standard.
Skriptextraktion	Prozess, den Sie beim Ausführen eines Skripts auswählen. Das Skript überprüft Folgendes: ○ ThreLookupResultSysId:sys_ID des Ergebnisdatensatzes der Bedrohungssuche ○ SourceName: Name der Bedrohungssuchquelle.
Taktik-Extraktion	Option, die Sie angeben, um taktikbezogene Informationen aus der Rohnutzlast zu extrahieren. Wenn eine Nutzlast bestimmte taktische und technikbezogene Informationen enthält, können Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	die Informationen extrahieren und an den Security Incident anhängen.

4. Klicken Sie auf **Absenden**.

Verwenden Sie SIEM-Regeln für automatische Extraktion

Verwenden Sie die SIEM-Regeln für die automatische Extraktion, um zu importieren MITRE-ATT&CK Informationen aus vorhandenen Security Operations SIEM-Drittpartei-Integrationen.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff

Warum und wann dieser Vorgang ausgeführt wird

Die Technikextraktionsregel ist für alle Basissysteme verfügbar Security Operations SIEM-Integrationen wie Splunk-, IBM QRadar- und ArcSight-Integrationen. Wenn ServiceNow AI Platform Erfasst Warnungs- oder Ereignisdaten aus diesen SIEM-Integrationen und enthält sie MITRE-ATT&CK Informationen, die ServiceNow AI Platform Verarbeitet die Rohnutzlast und extrahiert automatisch MITRE-ATT&CK Informationen.

Wenn Ihr ServiceNow AI Platform Enthält SIEM-Integrationen des Basissystems, d. h. die Extraktionsregeln für Technik wurden bereits in erstellt MITRE-ATT&CK Modul. Sie sollten die Regeln nach Bedarf überprüfen und ändern.

Aktivieren Sie entweder die automatische SIEM-Extraktionsregel oder die Warnungsregel gleichzeitig.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Extraktionsregel für Technik**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

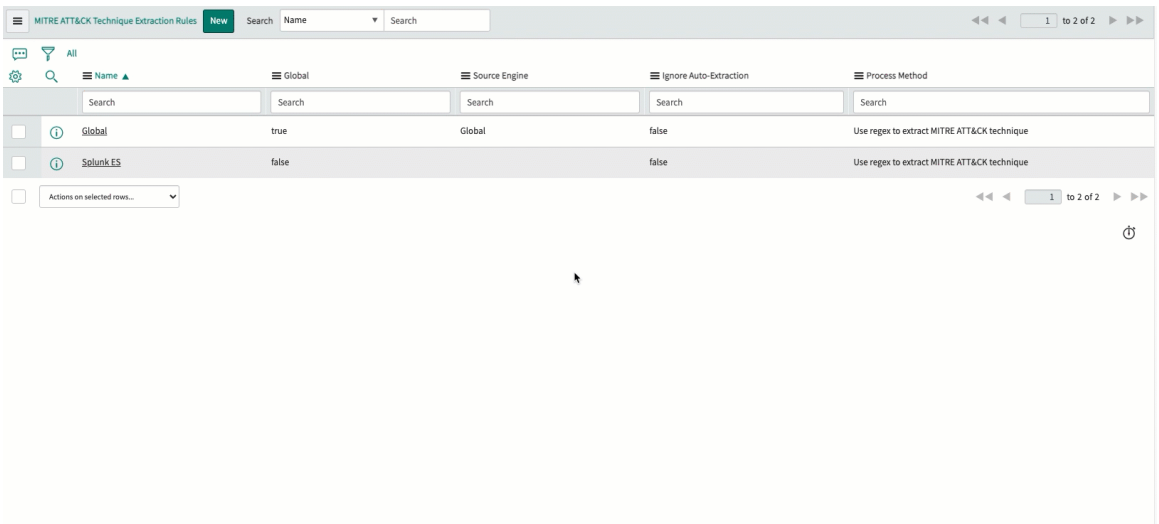
Formular „Technik-Extraktionsregel“

Feld	Beschreibung
Name	Name der automatischen Extraktionsregel.
Regeltyp	Regeltyp für automatische Extraktion. Wählen Sie Aus **SIEM** .
Automatische Extraktion ignorieren	Einstellung, die standardmäßig gelöscht ist. Diese Einstellung ermöglicht die automatische Extraktion von MITRE-ATT&CK Techniken.
Tabelle importieren	Importtabelle, die automatisch für SIEM-Integrationen des Basissystems zugeordnet wird. Überprüfen Sie dieses Feld auf andere SIEM-Integrationen für MITRE-ATT&CK Informationen und Zuordnung entsprechend.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Feld importieren	Importfeld, das automatisch für SIEM-Integrationen des Basissystems zugeordnet wird. Überprüfen Sie dieses Feld auf andere SIEM-Integrationen für MITRE-ATT&CK Informationen und Zuordnung entsprechend.
Beschreibung	Regel für automatische Extraktion.
Prozessmethode	Regulärer Ausdruck oder eine Skriptmethode, die Sie angeben, um die Technikinformationen aus der Rohnutzlast zu verknüpfen.
Extraktion des regulären Ausdrucks	Option, die Sie für angeben **Zielfeld** Bei Verwendung der Methode des regulären Ausdrucks. Die Extraktion des regulären Ausdrucks ist die Standardprozessmethode.
Skriptextraktion	Skriptprozessmethode, die Sie verwenden, wenn Sie anpassen möchten, wie der MITRE-ATT&CK Informationen werden extrahiert.
Taktik-Extraktion	Option, die Sie angeben, um taktikbezogene Informationen aus der Rohnutzlast zu extrahieren. Wenn eine Nutzlast bestimmte taktische und technikbezogene Informationen enthält, können Sie die Informationen extrahieren und an den Security Incident anhängen.

In der folgenden Abbildung sehen Sie ein Beispiel für Splunk Enterprise Extraktionsregel für SIEM-Technik in der Formularansicht. Diese Regel ähnelt allen anderen Extraktionsregeln für SIEM-Technik.



4. Klicken Sie auf **Absenden**.

Überprüfen Sie die Bedrohungsgruppe und MITRE-ATT&CK Technikzuordnung

Überprüfen Sie das Bedrohungsgruppen- und Technikobjekt zu Objektbeziehungszuordnungsinformationen, die aus importiert werden MITRE TAXII Sammlungen. Mit dieser Zuordnung können Sie die Technikgruppe und die entsprechende Technikzuordnung anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

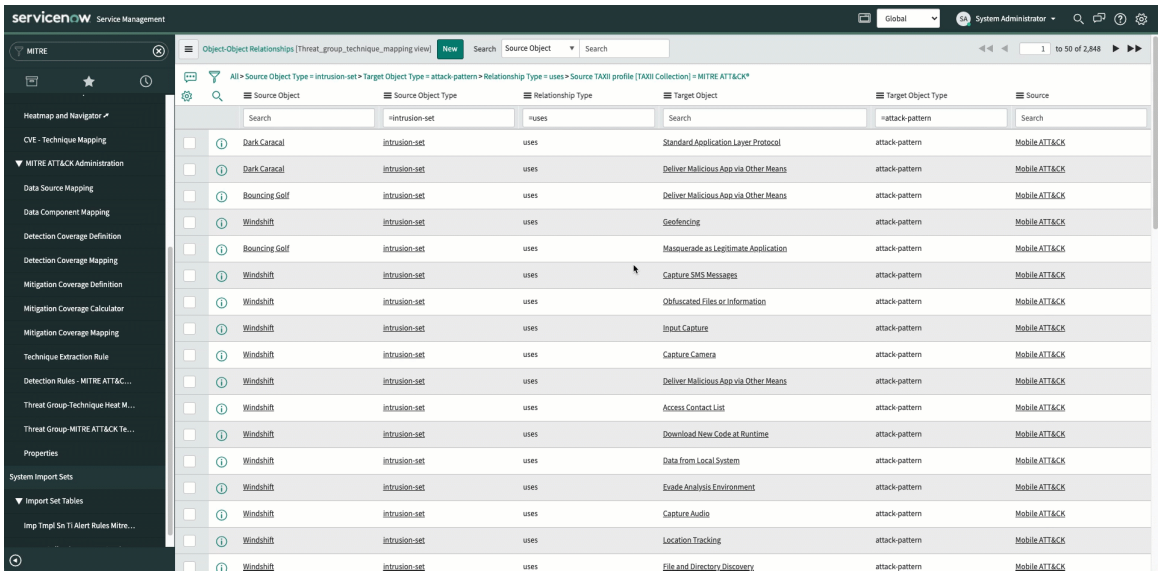
Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Zugriff erstellen, schreiben, löschen
- sn_ti.read: Lesezugriff

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Bedrohungsgruppe – MITRE ATT&CK-Techniken**an.
2. Klicken Sie mit der rechten Maustaste auf **Quellobjekt** Und wählen Sie aus **Nach Quellobjekt Gruppieren** Zum Anzeigen aller Angriffsmuster, die einer Bedrohungsgruppe zugeordnet sind.

   Die folgende Abbildung zeigt die Bedrohungsgruppe admin@338 und die verschiedenen Angriffsmuster dieser Bedrohungsgruppe, die Teil der Enterprise-Angriffsquelle sind.



Heatmap-Definition für Bedrohungsgruppe zu Technik

Definieren Sie die Heatmap-Definition für Bedrohungsgruppe zu Technik, damit Sie auf der Heatmap die Angriffsmuster messen und erkennen können, die Bedrohungsgruppen für Angriffe auf Ihre Organisation verwenden. Die Wahrscheinlichkeit eines Angriffs mit einer bestimmten Technik erhöht sich, wenn Sie eine hohe Anzahl von Angreifern haben.

Vorbereitungen

Erforderliche Rolle:

- sn_ti.admin, sn_si.admin: Schreibzugriff
- sn_ti.read: Lesezugriff

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Definition der Bedrohungsgruppentechnik-Heatmap**an.
2. Überprüfen Sie die Heatmap-Definition für Bedrohungsgruppe zu Technik, und passen Sie die Einträge für Ihre Umgebung an.

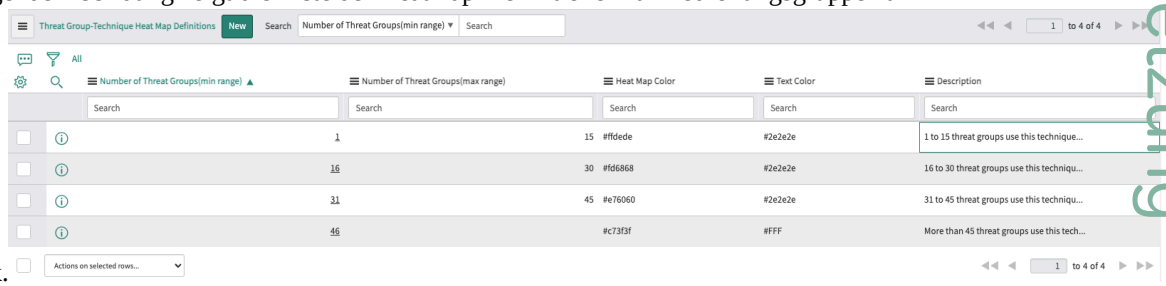
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definitionen der Bedrohungsgruppentechnik-Heatmap

Feld	Beschreibung
Anzahl der Bedrohungsgruppen (Mindestbereich)	Die Mindestanzahl von Bedrohungsgruppen, die eine bestimmte Technik verwenden.
Anzahl der Bedrohungsgruppen (max. Bereich)	Die maximale Anzahl von Bedrohungsgruppen, die eine bestimmte Technik verwenden. Die Wahrscheinlichkeit eines Angriffs mit einer bestimmten Technik erhöht sich, wenn Sie eine hohe Anzahl von Angreifern haben.
Heatmap-Farbe	Farbe, die der Bedrohungsgruppenkategorie zugewiesen ist. Die von Ihnen definierte Farbe wird verwendet, um die Bedrohungsgruppenkategorie in der Heatmap hervorzuheben. Sie können die Farben mithilfe von HEX-Codes und RGB(A)-Werten anpassen.
Textfarbe	Farbe, die dem Text der Bedrohungsgruppe zugewiesen ist. Die von Ihnen definierte Farbe wird verwendet, um die Bedrohungsgruppen in der Heatmap hervorzuheben. Sie können die Farben mithilfe von HEX-Codes und RGB(A)-Werten anpassen.
Beschreibung	Beschreibung des Bedrohungsgruppenbereichs und der Definition.

Hinweis:
Stellen Sie sicher, dass Sie die Anzahlbereiche für Bedrohungsgruppen nicht überschneiden, wenn Sie den Bedrohungsgruppenbereich anpassen (min. Oder max.).

Die folgende Abbildung zeigt die Liste der Heatmap-Definitionen für Bedrohungsgruppe zu Technik.



3. Klicken Sie auf, um einen Eintrag hinzuzufügen **Neu** , Vervollständigen Sie die Einträge, und klicken Sie auf **Übermitteln** .

Überprüfen Sie MITRE-ATT&CK Systemeigenschaften

Überprüfen Sie MITRE-ATT&CK Systemeigenschaftswerte.

Vorbereitungen
Erforderliche Rolle: sn_ti.admin, sn_si.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Administration** > **Eigenschaften**an.
2. Füllen Sie im Formular die Felder aus.

MITRE-ATT&CK Eigenschaftenformular

Feld	Beschreibung
Automatisch ein Rollup von MITRE ATT&CK-Informationen aus erkennbaren Elementen zum Security Incident durchführen [sn_ti.Rollup_Mitre_att&ck_technique_observable_si]	Rollup von MITRE-ATT&CK Informationen von erkennbaren Elementen zum Security Incident. Weitere Informationen finden Sie unter Ordnen Sie MITRE ATT&CK-Informationen erkennbaren Elementen zu . Standardwert: Ja
Automatisch ein Rollup von MITRE ATT&CK-Informationen aus den Ergebnissen der Bedrohungssuche zum Security Incident durchführen [sn_ti.Rollup_Mitre_att&ck_technique_Threat_Lookup_si]	Rollup von MITRE-ATT&CK Informationen aus den Ergebnissen der Bedrohungssuche zum Security Incident. Weitere Informationen finden Sie unter Automatische Extraktion der Bedrohungssuche . Standardwert: Ja
Automatisch ein Rollup von MITRE ATT&CK-Informationen von Warnungsregeln zu Security Incidents durchführen [sn_ti.Rollup_Mitre_att&ck_technique_Alert_rule_si]	Rollup von MITRE-ATT&CK TTP-Informationen automatisch von Warnungsregeln zu Security Incidents. Weitere Informationen finden Sie unter Ordnen Sie Erkennungsregeln zu . Standardwert: Nein
Automatisch ein Rollup von MITRE ATT&CK-Informationen aus untergeordneten Security Incidents zum übergeordneten Security Incident durchführen [sn_ti.Rollup_Mitre_att&ck_technique_Child_si_si]	Rollup durchführen MITRE-ATT&CK Automatisch Informationen von untergeordneten Security Incidents zu übergeordneten Security Incidents. Standardwert: Ja
Durch Aktivieren dieser Eigenschaft können Security Incident-Felder wie Kategorie und Unterkategorie mit Erkennungsregeln in der Tabelle „Erkennungsregeln – MITRE ATT&CK-Zuordnung“ zugeordnet werden [sn_ti.enable_category_Mapping_with_Alert_rule]	Kategorie und Unterkategorie in Erkennungsregeln: MITRE ATT&CK-Zuordnung Seite. Standardwert: Nein
Zeit (in Stunden) zur Berechnung von „CVE – VUL-Anzahl“ [sn_ti.time_to_Compute_cve_vits_count]	Die geplante Zeit in Stunden zur Berechnung der CVE- und ANFECHTUNGSINFORMATIONEN. Standardwert: 24

3. Klicken Sie auf **Speichern**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden MITRE-ATT&CK Zum Erkennen und Analysieren von Bedrohungen

Verwenden Sie MITRE-ATT&CK Framework im gesamten Threat Intelligence Und SIR Modul zum Erkennen und Analysieren von Bedrohungen für Ihre Organisation.

Zuordnen MITRE-ATT&CK™ Informationen zu Security Incidents

Ordnen Sie zu MITRE-ATT&CK Taktiken und Techniken für den Security Incident für eine bessere Analyse von Security Incidents und Bedrohungen.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie hinzu MITRE-ATT&CK Informationen zu Taktiken und Techniken mit dem Security Incident verknüpfen, damit Sie Ihre Security Incident- und Bedrohungsinformationen für eine bessere Analyse korrelieren können. Beispielsweise kann Ihre Organisation Informationen im Zusammenhang mit Taktiken, Techniken und Verfahren (TTP) aus Ihren Drittparteiquellen erhalten, z. B. Threat Intelligence Berichte oder andere Quellen außerhalb von Security Incident Response. Sie fügen diese Informationen dann wieder zu hinzu SIR Für eine bessere Korrelation und Bedrohungsanalyse.

Sie können einen Rollup von durchführen MITRE-ATT&CK Informationen automatisch aus den Ergebnissen der automatischen Extraktion der Bedrohungssuche, aus erkennbaren Elementen oder aus einem untergeordneten Security Incident zu einem Security Incident. Für automatisches Rollup zu Security Incidents, Aktivieren Sie die Systemeigenschaft . Alternativ können Sie die Informationen für jede einzelne Bedrohungssuche oder manuell zusammenfassen Erkennbares Element .

Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit anreichern möchten MITRE-ATT&CK Informationen.
3. Klicken Sie auf **Ordnen Sie DIE MITRE ATT&CK-Technik zu** Zugehöriger Link.
   Der Bereich MITRE ATT&CK-Technik zuordnen wird angezeigt.

   Diese Abbildung zeigt, wie Sie zur zugehörigen Liste navigieren und nach „Zuordnen“ suchen MITRE-ATT&CK Technik, überprüfen Sie die Quelle Enterprise ATT&CK, fügen Sie eine taktische Auswirkung hinzu, und fügen Sie ein Techniksystem herunter/neu starten hinzu.

   Ordnen Sie MITRE-Informationen Security Incident zu
4. Wählen Sie Aus **Quelle** .

   Hinweis:
   Nur die Sammlungen Und Matrizen Aktivierte werden in der Quellliste angezeigt.

   Die Taktiken und Techniken, die der Quelle zugeordnet sind, können ausgewählt werden. Sie können auch mehrere Quellen zuordnen.
5. Wählen Sie aus **Taktik** Und **Techniken** .
6. **Wahlweise:** Überprüfen Sie die Informationen basierend auf der Relevanz für den Security Incident, und gehen Sie wie folgt vor:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um die Zuordnung vollständig zu entfernen, klicken Sie auf das bin-Symbol. Durch Klicken auf dieses Symbol werden die Quelle und die zugehörigen Taktiken und Techniken gelöscht.
- Um eine Taktik zu entfernen, klicken Sie auf das Minussymbol neben der Taktik.
- Um eine Technik zu entfernen, klicken Sie auf das x-Symbol neben der Technik.

7. Klicken Sie auf **Speichern**.

Ergebnisse

Die MITRE-ATT&CK Informationen sind dem Security Incident zugeordnet. Sie können jetzt die zugehörigen Informationen in anzeigen **MITRE ATT&CK-KARTE** .

Zuordnen MITRE-ATT&CK Informationen zu geschlossenen Security Incidents

Sie können jetzt zuordnen MITRE-ATT&CK Taktiken und Techniken für die geschlossenen Security Incidents für eine bessere Analyse von Security Incidents und Bedrohungen.

Ordnen Sie MITRE-Informationen Security Incident zu

Mit MITRE-ATT&CK Karte zum Anzeigen zugehöriger Informationen in einem Security Incident

Sie können verwenden MITRE-ATT&CK Karte zum Anzeigen von MITRE-ATT&CK Zugehörige Informationen in einem Security Incident.

Nachdem die Informationen aus einer Bedrohungssuche, einem erkennbaren Element oder einer SIEM-Integration zusammengefasst wurden, werden sie dem Security Incident hinzugefügt. Dann werden die zusammengefassten Informationen in angezeigt MITRE-ATT&CK Karte. Die **MITRE ATT&CK-KARTE** Bietet zwei Ansichten:

- Navigatoransicht: Diese Ansicht, die der ähnelt MITRE-ATT&CK navigator: Zeigt alle Techniken an, die manuell aus den Tabellen für erkennbare Elemente oder Bedrohungssuche hinzugefügt oder zusammengefasst wurden. **Ursprung der Techniken anzeigen** Zeigt die Quelle der Technik an, wenn sie manuell Rollup durchgeführt wurde oder über eine Quelle geleitet wurde. **ID anzeigen** Zeigt die Technik-ID an.

  Die folgende Abbildung zeigt, wie Sie zu navigieren **MITRE ATT&CK-KARTE** navigatoransicht. Wenn Sie auf einen der verfügbaren Links klicken, werden die Informationen im geöffnet Threat Intelligence Modul.

  MITRE ATT&CK-Karte: Navigatoransicht und Listenansicht

- Listenansicht: Diese Ansicht zeigt die Daten in einem Listen- oder Tabellenformat an. In dieser Ansicht können Sie alle Daten anzeigen, die auf verschiedene Tabellen und Gruppen verteilt sind.

  Die folgende Abbildung zeigt, wie Sie zur Listenansicht der MITRE ATT&CK-Karte navigieren. Wenn Sie auf einen der verfügbaren Links klicken, werden die Informationen im geöffnet Threat Intelligence Modul.

Zuordnen MITRE-ATT&CK Informationen mit erkennbaren Elementen

Zuordnen MITRE-ATT&CK Taktiken und Techniken für ein erkennbares Element für eine bessere Analyse von Security Incidents und Bedrohungen auf granularer Ebene.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

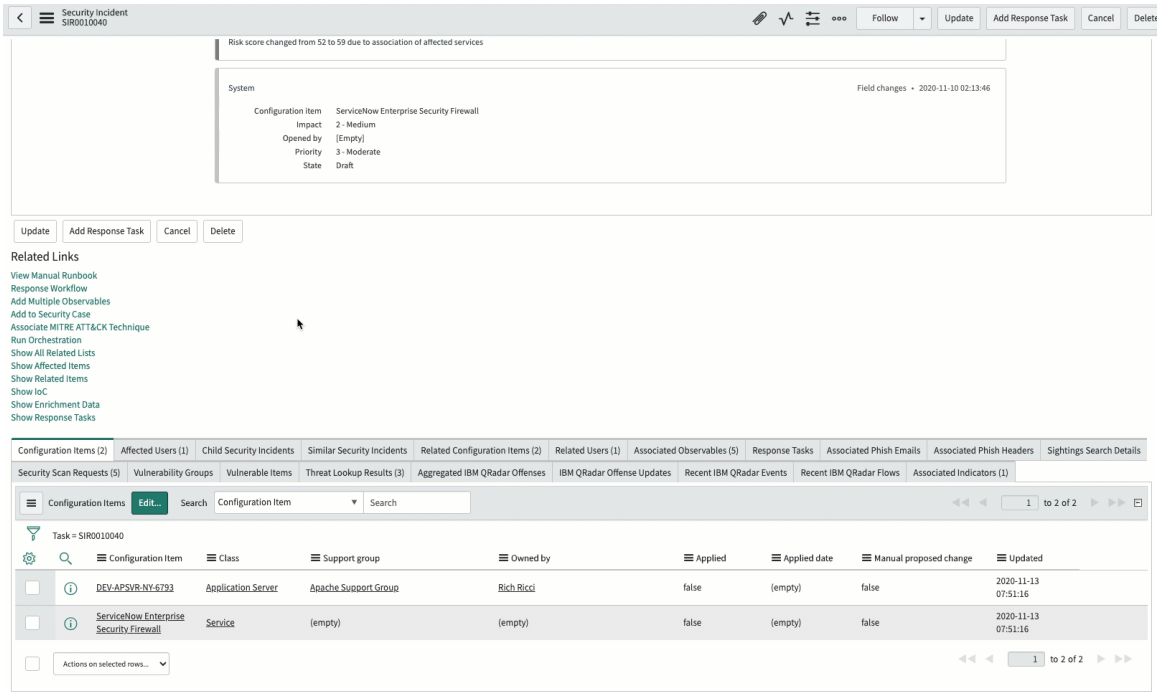
Einige SIEMs können bereitstellen MITRE-ATT&CK Informationen mit Ereignissen, Warnungen oder erkennbaren Elementen. Um zuzuordnen MITRE-ATT&CK Informationen auf granularer Ebene können Sie die Informationen mit einem erkennbaren Element hinzufügen.

Sie können einen Rollup von durchführen MITRE-ATT&CK Informationen automatisch von den erkennbaren Elementen zu einem Security Incident. Für das automatische Rollup von erkennbaren Elementen zu Security Incidents, Aktivieren Sie die Systemeigenschaft . Alternativ können Sie die Informationen für jedes erkennbare Element manuell zusammenfassen.

Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit anreichern möchten MITRE-ATT&CK Informationen.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und **Zugeordnete Erkennbare Elemente** Registerkarte.
4. Zeigen Sie auf das erkennbare Element, das Sie zuordnen möchten, klicken Sie mit der rechten Maustaste, und wählen Sie es aus **Ordnen Sie DIE MITRE ATT&CK-Technik zu** .

   In der folgenden Abbildung sehen Sie, wie Sie von der zugehörigen Liste zu navigieren **Ordnen Sie DIE MITRE ATT&CK-Technik zu** , Überprüfen Sie die Quelle, und fügen Sie eine Taktik und Technik hinzu.



5. Überprüfen Sie in den Quelllisten die **Quelle** .

   Hinweis:
   Nur die Sammlungen Und Matrizen Aktivierte werden in der Quellliste angezeigt.

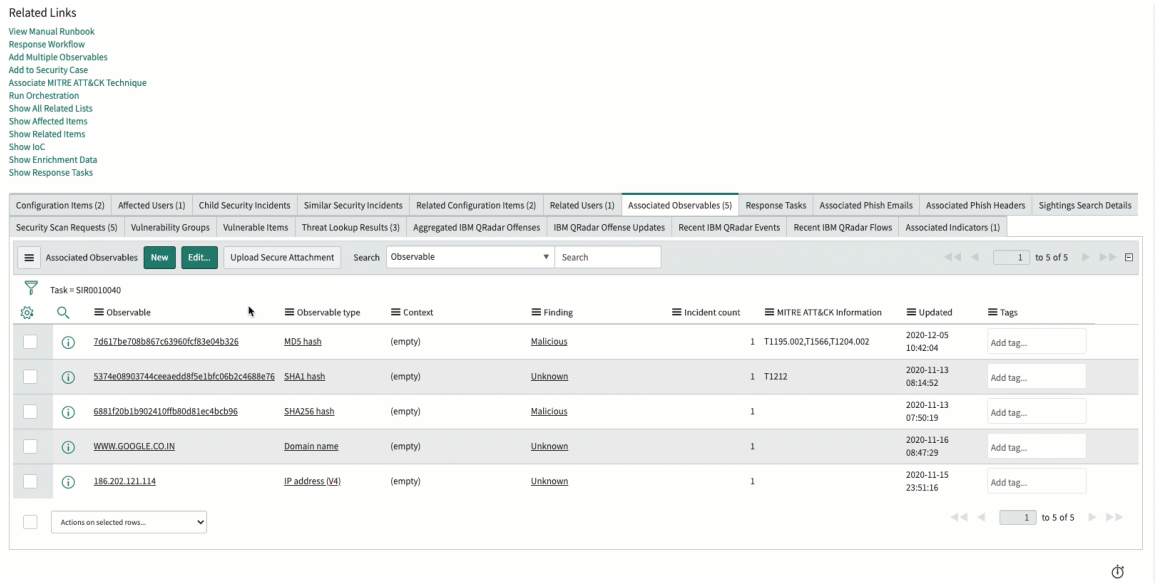
6. Überprüfen Sie **Taktik** Und **Techniken** , Und fügen Sie sie basierend auf der Relevanz für das erkennbare Element hinzu oder entfernen Sie sie.
7. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Taktiken und Techniken, die Sie hinzugefügt haben, werden in angezeigt MITRE-ATT&CK Informationsspalte in der zugehörigen Liste erkennbarer Elemente.

8. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü Aktionen auf **Rollup der MITRE ATT&CK-Informationen zu SI** .
   Wenn Sie aktiviert haben Automatisches Rollup von MITRE-ATT&CK Informationen von erkennbaren Elementen zu Security Incident, Dann werden die Informationen automatisch zusammengefasst. Wenn Sie das automatische Rollup nicht aktiviert haben, müssen Sie dies manuell tun.

   Die folgende Abbildung zeigt, wie ein erkennbares Element ausgewählt und ein Rollup durchgeführt wird MITRE-ATT&CK Informationen zu einem Security Incident.



9. Um eine zusammengefasste Ansicht der Techniken anzuzeigen, die den erkennbaren Elementen zugeordnet sind, wählen Sie zwei oder mehr erkennbare Elemente aus der Liste und dann aus **Aktionen** Klicken Sie in der Liste „ausgewählte Zeilen“ auf das Menü **MITRE ATT&CK-Informationen anzeigen** .

Ergebnisse

Eine zusammengefasste Ansicht der MITRE ATT&CK-Informationen für die ausgewählten erkennbaren Elemente wird angezeigt.

Zuordnen MITRE-ATT&CK Informationen mit Sicherheitsfall

Zuordnen MITRE-ATT&CK Taktiken und Techniken für einen Sicherheitsfall für ein besseres Management von Sicherheitsfällen und die Bedrohungsanalyse auf granularer Ebene.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

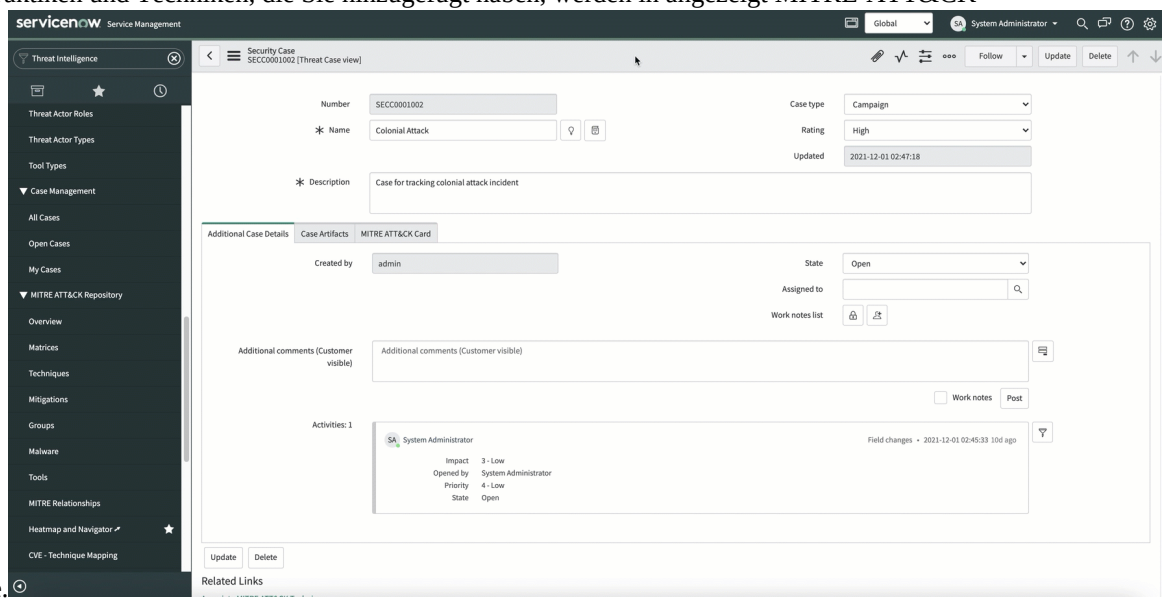
1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallmanagement** > **Alle Fälle**an.
2. Wählen Sie den Sicherheitsfall aus, den Sie mit den MITRE-ATT&CK-Informationen anreichern möchten.
3. Klicken Sie in der zugehörigen Liste auf **Ordnen Sie DIE MITRE ATT&CK-Technik zu** .

   In der folgenden Abbildung sehen Sie, wie Sie von der zugehörigen Liste zu navigieren **Ordnen Sie DIE MITRE ATT&CK-Technik zu** , Überprüfen Sie die Quelle, und fügen Sie eine Taktik und Technik hinzu.

4. Überprüfen Sie in den Quelllisten die **Quelle** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Überprüfen Sie **Taktik** Und **Techniken** , Und fügen Sie sie basierend auf der Relevanz für den Fall hinzu oder entfernen Sie sie.
6. Klicken Sie auf **Speichern**.
   Die Taktiken und Techniken, die Sie hinzugefügt haben, werden in angezeigt MITRE-ATT&CK Karte.



Rollup MITRE-ATT&CK Informationen mit Ergebnissen der Bedrohungssuche

Wenn Sie das automatische Rollup von nicht aktiviert haben MITRE-ATT&CK Informationen können Sie dies manuell tun.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

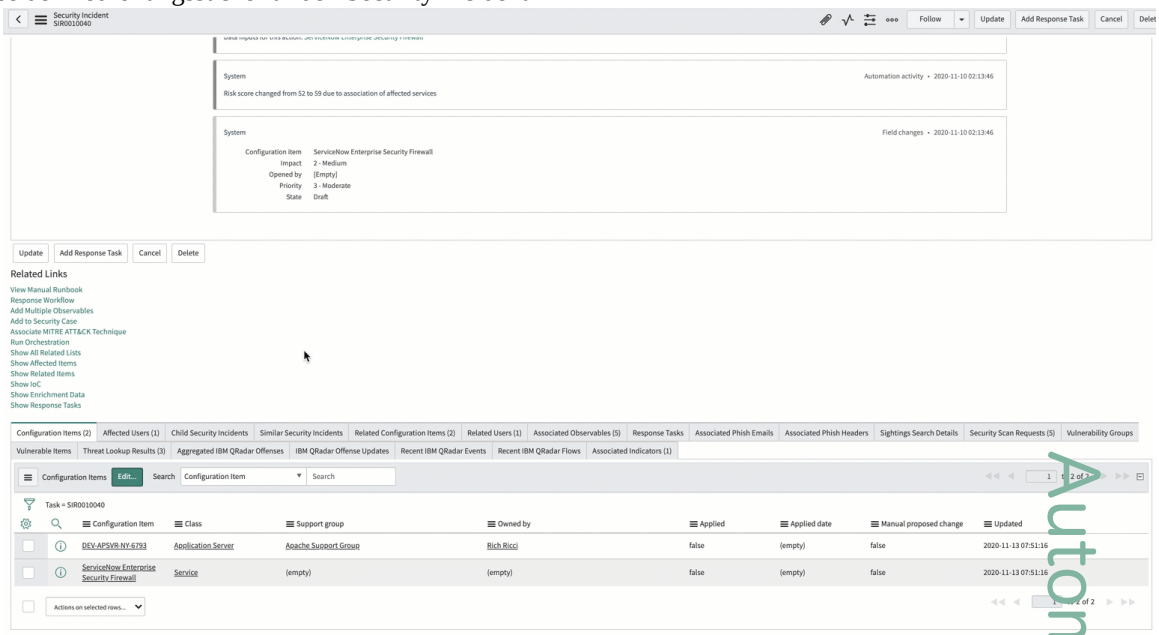
Wenn Sie aktiviert haben Automatisches Rollup von MITRE-ATT&CK Informationen aus Ergebnissen der Bedrohungssuche Für Security Incident werden die Informationen automatisch zusammengefasst. Wenn Sie das automatische Rollup nicht aktiviert haben, können Sie dies manuell tun.

Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit anreichern möchten MITRE-ATT&CK Informationen.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und **Ergebnisse Der Bedrohungssuche** Registerkarte.
4. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü Aktionen auf **Rollup der MITRE ATT&CK-Informationen zu SI** .
   Sie können mehrere erkennbare Elemente auswählen und ein Rollup für die Informationen durchführen.
5. Klicken Sie Auf **Neu Laden** Zum Bestätigen der Änderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt, wie Sie ein erkennbares Element auswählen und die Ergebnisse der Bedrohungssuche für den Security Incident



zusammenfassen.
Sie können anzeigen MITRE-ATT&CK Karte, um zu bestätigen, dass die Ergebnisse der Bedrohungssuche für den Security Incident Rollup durchgeführt wurden.

Rollup MITRE-ATT&CK Informationen aus Erkennungsregeln

Rollup von aktivieren MITRE-ATT&CK Informationen von den Erkennungsregeln bis zu den Security Incidents für eine bessere Analyse von Security Incidents und Bedrohungen.

Vorbereitungen

Erforderliche Rolle: keine

Stellen Sie sicher, dass Sie Folgendes ausgeführt haben:

- Aktivieren Sie Rollup von MITRE ATT&ACK-Informationen automatisch von Warnungsregeln zu Security Incidents Eigenschaft in Eigenschaften Modul. Standardmäßig ist diese Option deaktiviert. Weitere Informationen finden Sie unter Überprüfen Sie die MITRE-ATT&CK-Systemeigenschaften .
- Führen Sie die Zuordnung von Erkennungsregeln zu durch MITRE-ATT&CK TTPs in Erkennungsregeln – MITRE ATT&CK TTP-Zuordnung Modul. Der Name der Erkennungsregel muss mit dem Namen der Warnungsregel übereinstimmen, die den Security Incident auslöst. Weitere Informationen finden Sie unter Erstellen und ordnen Sie Erkennungsregeln zu.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie die automatischen SIEM-Extraktionsregeln des Basissystems nicht verwenden möchten, aktivieren Sie das automatische Rollup von MITRE-ATT&CK TTPs basierend auf der Erkennungsregelzuordnung. Sie können die Warnungs- oder Ereignisregel ausfüllen, die den Security Incident in auslöst Warnungsregel Namensfeld. Sie können auch ausfüllen Warnungsregel Namensfeld mithilfe von SIEM-Integration, E-Mail-Analyse, manueller Erstellung usw.

Automatische Übersetzung

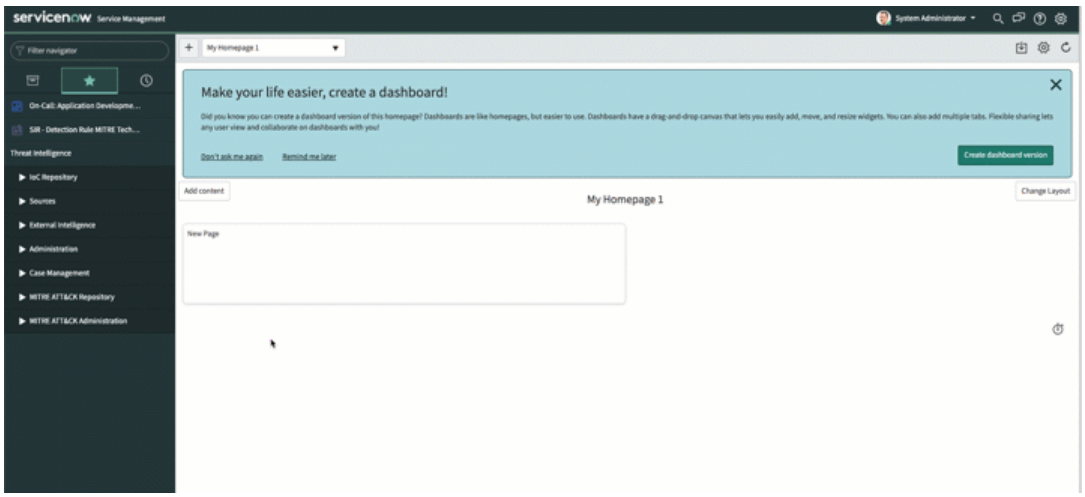
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **MITRE ATT&CK-Administration** > **Eigenschaften**an.
2. Aktivieren Sie die Eigenschaft „MITRE ATT&ACK-Informationen automatisch aus Warnungsregeln zur Eigenschaft „Security Incidents“ Rollup, und klicken Sie auf **Speichern** .
   Standardmäßig ist diese Option deaktiviert.
3. Sie müssen ausfüllen **Warnungsregel** Namensfeld des Security Incidents mit den erforderlichen Warnungsregeln.

   Hinweis:
   Stellen Sie sicher, dass Sie genau hinzufügen Warnungsregel Name. Um mehrere Regeln hinzuzufügen, müssen Sie die Regeln mit einem Kommatrennzeichen hinzufügen.

4. Klicken Sie mit der rechten Maustaste auf das Formular, und klicken Sie auf **Speichern** .
   Wenn der Wert des Warnungsregelnamens im Security Incident mit einem Datensatz im Modul „Erkennungsregel – MITRE ATT&CK TTP MAPPING“ übereinstimmt, werden die entsprechenden Techniken und Taktiken, die der Warnungsregel zugeordnet sind, automatisch mit dem Security Incident verknüpft.



5. Öffnen Sie den Security Incident, und wählen Sie aus **MITRE ATT&CK-KARTE** Und validiert, ob für die Techniken ein Rollup durchgeführt wird.
6. Aktivieren **Ursprung der Techniken anzeigen** Option zum Anzeigen des Ursprungs der Techniken.
   Der Ursprung der Techniken muss sein Erkennungsregel .

Rollup MITRE-ATT&CK Informationen aus untergeordneten Security Incidents

Wenn Sie das automatische Rollup von nicht aktiviert haben MITRE-ATT&CK Informationen können Sie dies manuell tun.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

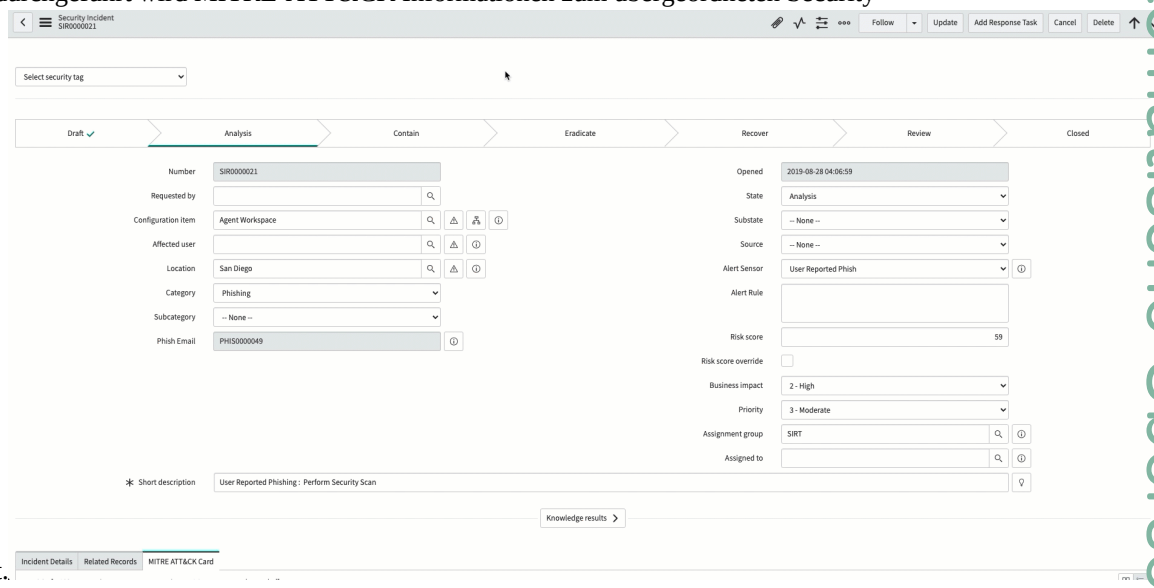
Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie aktiviert haben Automatisches Rollup von MITRE-ATT&CK Informationen aus untergeordneten Security Incidents, Dann werden die Informationen automatisch zusammengefasst. Wenn Sie das automatische Rollup nicht aktiviert haben, können Sie dies manuell tun.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den übergeordneten Security Incident aus, den Sie mit dem untergeordneten Element anreichern möchten MITRE-ATT&CK Informationen.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und **Untergeordnete Security Incidents** Registerkarte.
4. Wählen Sie den untergeordneten Security Incident aus, und klicken Sie dann im Menü Aktionen auf **Rollup der MITRE ATT&CK-Informationen zu SI** .
   Sie können auf klicken **MITRE ATT&CK-Informationen anzeigen** Um die MITRE-Informationen des untergeordneten Security Incidents anzuzeigen, bevor Sie die MITRE ATT&CK-Informationen zusammenfassen.
5. Klicken Sie Auf **Neu Laden** Zum Bestätigen der Änderungen.
6. Klicken Sie auf **MITRE ATT&CK-KARTE** Dient zum Anzeigen des Ursprungs von Techniken.
   Die folgende Abbildung zeigt, wie untergeordnete Security Incidents ausgewählt und ein Rollup durchgeführt wird MITRE-ATT&CK Informationen zum übergeordneten Security Incident.



Sie können die MITRE-ATT&CK-Karte anzeigen, um zu bestätigen, dass der untergeordnete Security Incident vorliegt MITRE-ATT&CK Informationen wurden für den übergeordneten Security Incident zusammengefasst.

Führen Sie mit eine Linkanalyse und Bedrohungssuche durch MITRE-ATT&CK Bestimmte Filter

Korrelieren und führen Sie eine Linkanalyse von erkennbaren Elementen, Security Incidents und durch MITRE-ATT&CK Zugehörige Informationen, damit Ihre Organisation mit der Suche nach Bedrohungen beginnen kann.

Vorbereitungen

Erforderliche Rolle: sn_ti.Mitre_Analyst, sn_si.read

Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie die Security Incidents mit zugeordnet haben MITRE-ATT&CK Informationen können Sie verwenden MITRE-ATT&CK Spezifische Filter für die Bedrohungssuche. Verwenden Sie MITRE-ATT&CK Filter mit vorhandenem Security Incident Response Filter zum Korrelieren und Durchführen einer Linkanalyse.

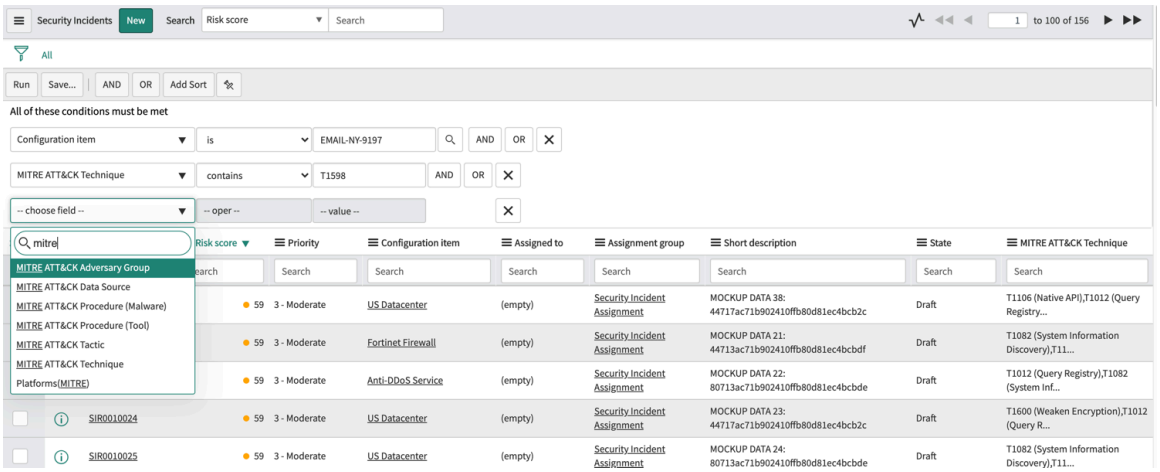
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**an.
2. Klicken Sie Auf **Aktualisieren Sie Die Personalisierte Liste** Zum Hinzufügen von MITRE Spalten.
3. Wählen Sie eine Filterbedingung aus, damit Sie anzeigen können MITRE Zugehörige Informationen und Zuordnungen zu Security Incidents oder erkennbaren Elementen:
   - MITRE-ATT&CK Angreifergruppe
   - MITRE-ATT&CK Datenquelle
   - MITRE-ATT&CK Verfahren (Malware)
   - MITRE-ATT&CK Verfahren (Tools)
   - MITRE-ATT&CK Taktik
   - MITRE-ATT&CK Technik
4. Erstellen Sie eine Filterbedingung, die auf den obigen Kriterien basiert, und klicken Sie auf **Ausführen** Dient zum Durchführen einer Linkanalyse oder Korrelation zwischen Security Incidents, erkennbaren Elementen und MITRE-ATT&CK Zugehörige Informationen.

Hinweis:
Die MITRE-ATT&CK Daten werden als Zeichenfolge gespeichert und können nur verwendet werden **Enthält** Als Operator für Filterbedingungen.

Wenn Sie beispielsweise überprüfen möchten, dass ein Konfigurationselement (Configuration Item, CI) gefährdet ist, wählen Sie ein CI aus. Anschließend korrelieren Sie das CI mit vorhandenen Techniken, indem Sie einen hinzufügen MITRE-ATT&CK Technik-ID. Sie können dann mit dem Erstellen Ihrer Filterkriterien fortfahren, um die Informationen zu korrelieren und die Bedrohungssuche zu ermöglichen.



MITRE-ATT&CK Heatmap und Navigator

Sie können verwenden MITRE-ATT&CK Heatmap und Navigator für die grundlegende Navigation und zur Visualisierung Ihrer Gesamterkennungsabdeckung für Technik.

Übersicht über MITRE-ATT&CK Heatmap und Navigator

Sie können den Navigator mit den primären Filtern für die grundlegende Navigation und Beobachtung von ATT&CK-Matrizen verwenden. Die Heatmap hebt das Spektrum der Erkennungsabdeckung hervor, einschließlich der toten Winkel, für die Ihre Organisation keine Abdeckung hat. Dies ist verfügbar, nachdem Sie zugeordnet haben Technikerkennungsabdeckung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit der Heatmap und dem Navigator können Sie:

- Identifizieren Sie schnell und effizient die Erkennungsfunktionen Ihrer Organisation, und heben Sie Lücken in der Abdeckung der Technikerkennung hervor.
- Suchen Sie mithilfe zugehöriger Funktionen nach Bedrohungen, und führen Sie eine Korrelation von Bedrohungen durch.

Greifen Sie auf zu MITRE-ATT&CK Heatmap und Navigator

Greifen Sie auf zu MITRE-ATT&CK Heatmap und Navigator, damit Sie die Matrix visualisieren können, mit der Sie ATT&CK verwenden können.

Vorbereitungen

Erforderliche Rolle: sn_ti.read, sn_ti.Mitre_Analyst

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Heatmap überprüfen, die Filter zum Korrelieren verwenden und eine Linkanalyse von durchführen MITRE-ATT&CK Informationen, die erkennbaren Elemente und die Security Incidents in Ihrer Organisation.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Heatmap und Navigator**an.
   Die Heatmap und der Navigator werden in einer neuen Registerkarte geöffnet.
2. Wählen Sie die Quelle aus, um die Heatmap auszufüllen.

   Hinweis:
   Nur die Sammlungen Und Matrizen Aktivierte werden in der Quellliste angezeigt.

   In der folgenden Abbildung sehen Sie, wie Sie zur Heatmap und zum Navigator navigieren und die Quelle auswählen, die Enterprise ATT&CK in diesem Beispiel ist.

   Navigieren Sie zu , und wählen Sie die Quelle aus, um die Heatmap auszufüllen
3. Verwenden Sie das Suchfeld, um mithilfe des Namens oder der ID schnell eine bestimmte Taktik oder Technik zu finden.

   Die folgende Abbildung zeigt, wie nach einer Taktik, Technik oder anderen darin enthaltenen Informationen gesucht wird. Verwenden Sie die Suche, um schnell Detailinformationen zu einer bestimmten Taktik oder Technik anzuzeigen.
4. Klicken Sie Auf **Filter** Und wählen Sie einen Filter aus Primär Oder Erweitert Filter.
5. Klicken Sie Auf **Anwenden** Und steuern Sie die Filter wie folgt:
   - So speichern Sie Ihre Filter: Erstellen Sie eine anwenderdefinierte Ansicht . Sie können drei erstellen und speichern Anwenderdefinierte Ansichten .
   - Klicken Sie auf, um die ausgewählten Filter zu entfernen **Standardfilter Wiederherstellen** Zum Laden Ihrer gespeicherten Standardansicht.
   - Um alle Filter und Ihre vorhandene Ansicht zu löschen, klicken Sie auf **Löschen Sie alle Filter** .

   Hinweis:
   Die Ansichten, die Sie speichern, sind spezifisch für einen Anwender.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie Auf **Blenden Sie Untertechniken Aus** Zum Entfernen aller Untertechniken aus der Heatmap-Ansicht.
   Wenn eine Technik über Untertechniken verfügt, können Sie auf das Erweiterungssymbol klicken, um die Untertechniken anzuzeigen.

Mithilfe der anwenderdefinierten Ansichten

Anwenderdefinierte Ansichten in MITRE-ATT&CK Heatmap und Navigator helfen Ihnen, Ihre Lieblingsfilter zu speichern und anzuzeigen, wenn Sie das nächste Mal auf der Heatmap landen.

Hinweis:
Sie können drei anwenderdefinierte Ansichten für jeden erstellen und speichern MITRE-ATT&CK Sammlung pro Anwender.

Erstellen Sie eine Ansicht

Sobald Sie die erforderlichen Filter aus der ausgewählt haben Primär Oder Erweitert Filter, klicken Sie auf die Auslassungspunkte (⋯). Schaltfläche im Header „Filter“, und wählen Sie aus **Erstellen Sie eine neue Ansicht** . Geben Sie den Namen der anwenderdefinierten Ansicht und ein **Ansicht Speichern** .

Standardansichten

Klicken Sie Auf **Speichern Sie dies als Standardansicht** Dient zum direkten Laden der Ansicht, wenn Sie das nächste Mal auf der Heatmap landen. Sie können für jede der Sammlungen eine Standardansicht festlegen.

Hinweis:
Wenn Sie ein Upgrade von durchführen Threat Intelligence Plugin aus einer älteren Version, dann wird Ihre vorhandene Standardansicht aus der alten Version als anwenderdefinierte Ansicht angezeigt.

Abbildung zeigt, wie eine anwenderdefinierte Ansicht in der Heatmap erstellt wird

Aktualisieren Sie eine Ansicht

Sie können Aktualisierungen an einer vorhandenen anwenderdefinierten Ansicht vornehmen, indem Sie die erforderlichen ändern Primär Oder Erweitert Filter. Wählen Sie eine anwenderdefinierte Ansicht aus, aktualisieren Sie die Filter nach Bedarf, und klicken Sie dann auf die Auslassungspunkte (⋯). Schaltfläche im Header „Filter“, und wählen Sie aus **Ansicht aktualisieren** Zum Speichern der Filter.

Diese Darstellung zeigt, wie eine anwenderdefinierte Ansicht aktualisiert wird.

Verwalten Sie anwenderdefinierte Ansichten

Verwenden Sie die Kontrollkästchen neben jeder anwenderdefinierten Ansicht, um den ausgewählten anwenderdefinierten Ansichtsfilter anzuwenden.

Klicken Sie auf die Auslassungspunkte (⋯). Schaltfläche neben jedem Namen der anwenderdefinierten Ansicht, um die anwenderdefinierten Ansichten wie folgt zu steuern:

- Legen Sie eine Standardansicht fest.
- Entfernen Sie eine anwenderdefinierte Ansicht als Standardansicht. Dadurch wird die anwenderdefinierte Ansicht nicht gelöscht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Benennen Sie die anwenderdefinierte Ansicht um.
- Löschen Sie die anwenderdefinierte Ansicht.

Diese Abbildung zeigt, wie anwenderdefinierte Ansichten verwaltet werden.

Exportieren Sie eine gespeicherte Ansicht

Um die gespeicherten anwenderdefinierten Ansichten in JSON-Dateien zu exportieren, klicken Sie auf die Auslassungspunkte (⋯). Wählen Sie im Header Filter die Option aus **Exportieren Sie gespeicherte Ansichten** . Klicken Sie auf das Download-Symbol für die anwenderdefinierte Ansicht, die Sie auf Ihren lokalen Computer herunterladen möchten.

Diese Abbildung zeigt, wie anwenderdefinierte Ansichten exportiert werden.

Importieren Sie eine Ansicht

Sie können nur JSON-Dateien importieren. Um die anwenderdefinierten Ansichten zu importieren, klicken Sie auf die Auslassungspunkte (⋯). Schaltfläche im Header „Filter“, und wählen Sie aus **Importansicht (JSON)** .

Überprüfen Sie beim Importieren von Ansichten die folgenden Bedingungen:

- Sie können nur das JSON-Dateiformat importieren.
- Sie können jeweils nur eine Ansicht oder Datei importieren.
- Sie können nicht importieren, wenn Sie bereits drei anwenderdefinierte Ansichten in Ihren Filtern haben. Löschen Sie eine anwenderdefinierte Ansicht, und importieren Sie eine Ansicht.
- Sie können keine Ansicht mit einem vorhandenen anwenderdefinierten Ansichtsnamen importieren. Benennen Sie eine Ansicht vor dem Import um.

Diese Abbildung zeigt, wie eine Ansicht importiert wird.

Navigator mit primären Filtern

Verwenden Sie die primären Filter, um Techniken in zu filtern MITRE-ATT&CK navigator. Die Informationen in MITRE-ATT&CK Repository kann ausgewählt werden.

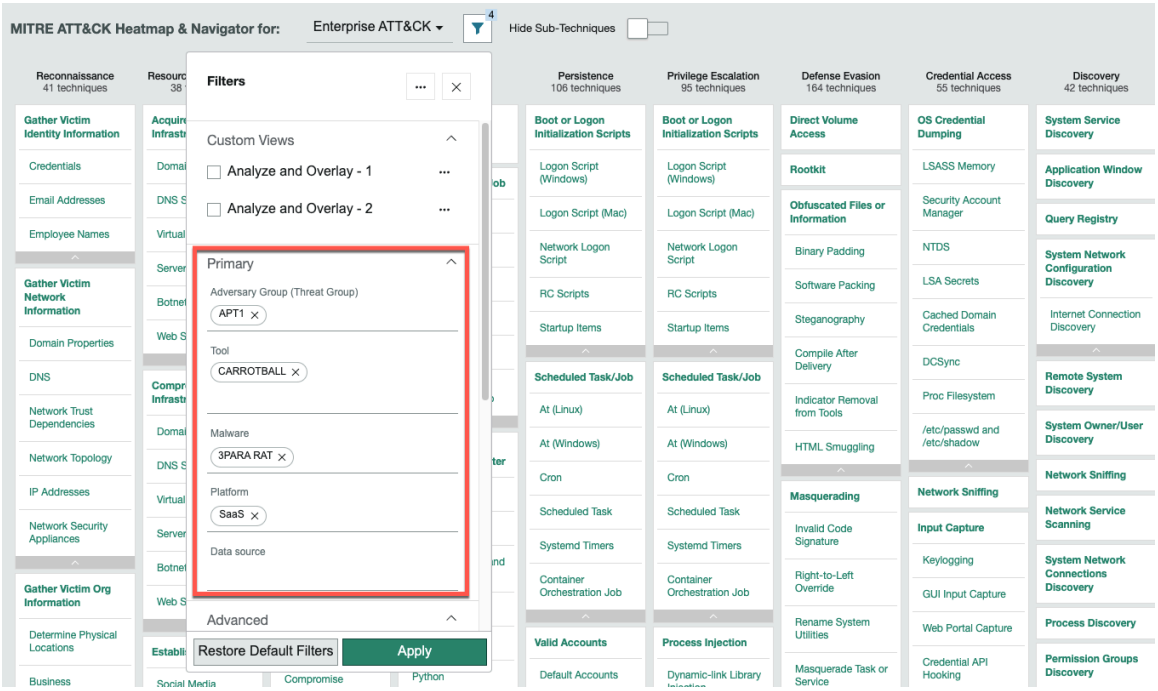
Filter	Beschreibung
Angreifergruppe (Bedrohungsgruppe)	Sätze zugehöriger Angriffsaktivitäten, die von einem allgemeinen Namen in der Sicherheits-Community nachverfolgt werden. Gruppen können verschiedene Bedrohungsgruppen, Aktivitätsgruppen, Bedrohungsakteure, Angriffssätze und Kampagnen bedeuten. Sie können dem mehrere Gruppen hinzufügen **Angreifergruppe (Bedrohungsgruppe)** Filter. Sie fügen beispielsweise APT1 und AT12 hinzu, da beide Bedrohungsgruppen sind, die China zugeordnet sind. Beide Gruppen können zwar auf verschiedene Quellen abzielen, sie könnten jedoch ähnliche Techniken verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filter	Beschreibung
Tool	Legitime Software, die von Bedrohungsakteuren zum Ausführen von Angriffen verwendet wird. Sie können verstehen, wie Bedrohungsakteure Kampagnen ausführen, wenn Sie wissen, wie und welche Tools von Bedrohungsakteuren verwendet werden. Tools enthalten sowohl Software, die nicht auf einem Enterprise-System gefunden wird, als auch Software, die als Teil eines Betriebssystems verfügbar ist, das bereits in einer Umgebung wie Microsoft Windows-Dienstprogrammen vorhanden ist. Beispielsweise ist gsecdump ein öffentlich verfügbarer Anmeldeinformations-Dumper, den die APT11-Angreifergruppe verwendet, um Passwort-Hashes und LSA-Geheimnisse (Local Security Authority) von Microsoft Windows-Betriebssystemen zu erhalten.
Malware	Kommerzielle, anwenderdefinierte Closed Source- oder Open Source-Software, die für böswillige Zwecke von Angreifern verwendet werden soll. Beispiele sind PlugX, CHOPSTICK usw.
Plattform	Taktiken und Techniken, die darstellen MITRE-ATT&CK In einer bestimmten Plattform. Beispiel: MITRE-ATT&CK Unterstützt diese Plattformen in der Enterprise ATT&CK-Matrix: Microsoft Windows, macOS, Linux, PRE, AWS, GCP, Azure, Azure AD, Office 365, SaaS, Netzwerk.
Datenquelle	Datenquellen, die Sie in Ihrer Umgebung erfassen und zur Erkennung verwenden MITRE-ATT&CK Techniken. Beispiele sind DLL-Überwachung und Browsererweiterungen.

Die folgende Abbildung zeigt alle primären Filter, die in verfügbar sind MITRE-ATT&CK navigator.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Verwenden einer Heatmap mit primären und erweiterten Funktionen

Sie können eine Heatmap mit erweiterten Filtern verwenden, um eine Analyse durchzuführen, indem Sie Security Incidents mit korrelieren MITRE-ATT&CK Informationen.

Technik-IDs anzeigen

Sie können anzeigen MITRE-ATT&CK Technik-IDs mit den Techniknamen, wenn Sie auswählen **Technik-IDs anzeigen** Filter.

Zeigen Sie Technik-IDs auf einer Heatmap an

Zeigen Sie relevante Techniken nach Priorität an

Um die Techniken basierend auf ihrer relevanten Priorität im Navigator zu filtern, wählen Sie aus **Filtern Sie nach technikrelevanter Priorität** Filtern und wählen Sie aus **Relevante Priorität** Aus dem Menü. Sie können mehrere Prioritäten für die Filterung zuweisen. Sie können auch auf die Techniken in der Heatmap verweisen, um die Priorität der Technik zu erfahren.

Die relevanten Prioritätsinformationen basieren auf der Priorisierung, die Sie in festgelegt haben Techniken Relevantes Prioritätsfeld.

Diese Abbildung zeigt die Filterung nach relevanter Priorität.

Zeigen Sie die Abdeckung der Technik-Erkennung an

Um die Gesamterkennungsabdeckung der Technik in der Heatmap anzuzeigen, wählen Sie aus **Zeigen Sie die Abdeckung der Technikerkennung an** Filter. Die Heatmap hebt das visuelle Spektrum der Erkennungsabdeckung hervor, einschließlich der toten Winkel, für die Sie keine Abdeckung haben. Die Bewertungsdefinition des Basissystems und die Farben wurden in definiert Technikerkennungsabdeckung . Die Informationen wurden automatisch aus der gesamten Technikerkennungsabdeckung extrahiert.

Beispielsweise weisen Bereiche der Heatmap, die rot markiert sind, auf eine fehlende Erkennung hin. Bereiche, die blau markiert sind, zeigen das Vorhandensein vollständiger

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennungsfunktionen an. Bereiche, die orange, gelb und hellblau markiert sind, spiegeln Teilerkennungsfunktionen wider.

- Die Farbvisualisierung basiert auf Technikdefinition und Farbcodierung Die Sie definieren.
- Die Visualisierung der Abdeckung basiert auf Zuordnung der Technikerkennungsabdeckung Die Sie definieren.
- Wenn Sie die Abdeckungsdefinition des Basissystems ändern, werden die Symbole für Abdeckungstyp nicht mit den Techniken in der Heatmap angezeigt.

Hinweis:
Die Heatmap funktioniert erwartungsgemäß, wenn Sie dieselben Felder ändern, wie die vom Basissystem definierten Technikerkennungsfarben und Abdeckungsfarben.

In dieser Abbildung sehen Sie die Technikerkennungsabdeckung für alle Techniken und Untertechniken und den Abdeckungstyp mit ihren Farben und Symbolen.

Abdeckung der Heatmap-Technik-Erkennung

Zeigen Sie die Abdeckung der Technikminderung an

Um die Gesamtabdeckung der Technikminderung in der Heatmap anzuzeigen, wählen Sie den Filter „Abdeckung der Technikminderung anzeigen“ aus. Die Heatmap hebt das visuelle Spektrum der Minderungsabdeckung hervor, einschließlich der Bereiche, für die Sie keine Abdeckung haben. Die Minderungsabdeckung, die Farben und die Prozentbereiche wurden in definiert Definition Der Minderungsabdeckung . Die Informationen werden aus extrahiert Gesamtabdeckung Der Technikminderung .

Zum Beispiel weisen die rot hervorgehobenen Techniken auf keine Minderungsabdeckung hin, orange auf eine schlechte Minderungsabdeckung und blau auf eine ausgezeichnete Minderungsabdeckung.

- Die Farbvisualisierung basiert auf Definition der Technikminderung und Farbcodierung Die Sie definieren.
- Die Visualisierung der Abdeckung basiert auf Zuordnung der Technikverringerung zur Abdeckung Die Sie definieren.
- Wenn Sie die Definition der Minderungsabdeckung des Basissystems ändern, werden die Symbole für den Typ der Minderungsabdeckung nicht mit den Techniken in der Heatmap angezeigt.

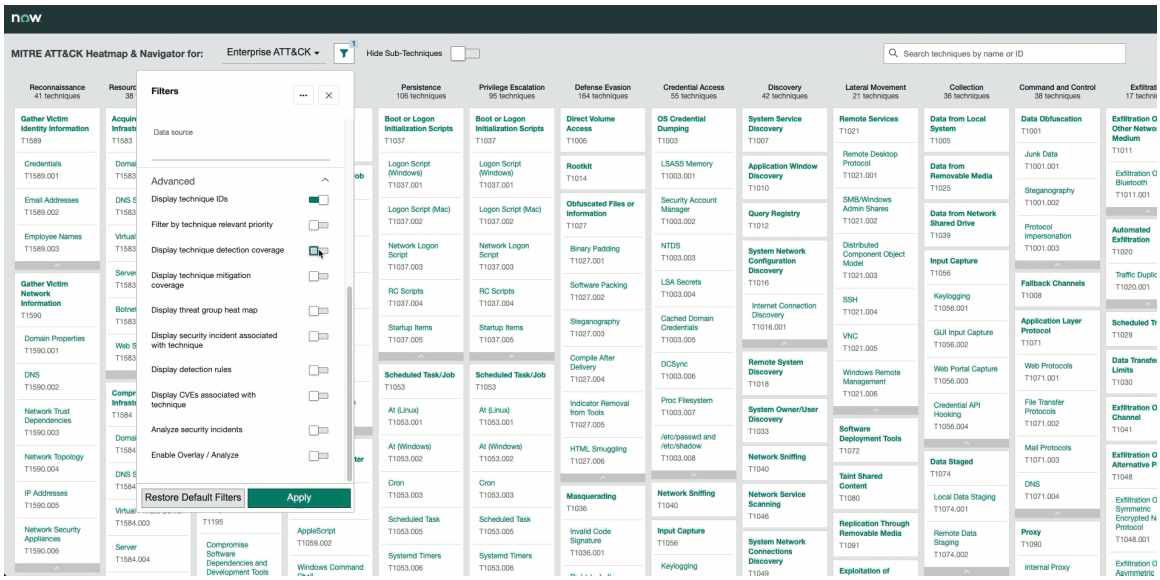
Hinweis:
Die Heatmap funktioniert erwartungsgemäß, wenn Sie dieselben Felder ändern, wie die vom Basissystem definierten Techniken zur Verringerung der Abdeckung und Abdeckungsfarben des Basissystems.

Diese Abbildung zeigt die Heatmap für die Abdeckung der Technikminderung

Zeigen Sie die Erkennung und Minderungsabdeckung an

Sie können die Filter für Technikerkennung und Technikminderung zusammen verwenden, um einen Einblick in die Relevanz der Technikerkennung und der Abdeckung für Ihre Organisation zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Diese Abbildung zeigt, wie der Erkennungs- und Minderungsfilter zusammen verwendet werden.

Bedrohungsgruppe anzeigen

Um Informationen zur Bedrohungsgruppe zu Technik auf der Heatmap anzuzeigen, wählen Sie aus **Bedrohungsgruppen-Heatmap anzeigen** . Sie können die Anzahl der Bedrohungsgruppen messen, die eine bestimmte Technik verwenden. Die Wahrscheinlichkeit eines Angriffs mit einer bestimmten Technik erhöht sich, wenn Sie eine hohe Anzahl von Angreifern haben. Die Bedrohungsgruppenbereiche und Heatmap-Farben wurden in definiert Definition Der Heatmap Für Bedrohungsgruppe – Technik .

- Die Farbvisualisierung für die Heatmap und den Text basiert auf dem Heatmap-Definition für Bedrohungsgruppe zu Technik .
- Die Visualisierung des Bedrohungsgruppenbereichs basiert auf Zuordnung von Bedrohungsgruppe zu Technik .
- Sie können nicht verwenden **Bedrohungsgruppen-Heatmap anzeigen** Filtern Sie, wenn die Abdeckung der Technikerkennung oder die Abdeckung der Technikminderung aktiviert ist.
  Diese Abbildung zeigt die Bedrohungsgruppeninformationen auf der Heatmap.

Zeigen Sie Security Incidents an, die der Technik zugeordnet sind

Um die Techniken anzuzeigen, die in Ihrer Organisation häufig ausgenutzt werden und zu Security Incidents geführt haben, klicken Sie auf **Security Incident anzeigen, der der Technik zugeordnet ist** . Sie können weitere Informationen zu jedem der zugehörigen Security Incidents anzeigen, wenn Sie auf den Link klicken, der in einem neuen Fenster zur Analyse geöffnet wird. Security Incidents, die einer Technik zugeordnet sind.

- Priorität: Wählen Sie Aus **Security Incident-Priorität** Zum Filtern nach der Priorität des Security Incidents.
- Datumsbereich: Wählen Sie aus **Datumsbereich Für Security Incident** Dient zum Filtern von Sicherheitsproblemen nach dem Datumsbereich.
- Falsch positive Ergebnisse: Auswählen **Filtern Sie falsch positive Security Incidents** Um falsch positive Probleme zu entfernen. Wenn Sie diesen Filter auswählen, wird die Anzahl der Security Incidents reduziert, die in der Heatmap angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie diesen Filter mit verwenden **Zeigen Sie die Abdeckung der Technikerkennung an** Filtern, erhalten Sie einen Einblick in die Relevanz der Technikerkennungsabdeckung für Ihre Organisation bis zum ausgewählten Datum.

Wenn Sie beispielsweise beide Filter aktivieren, können Sie sehen, dass unter der Taktik zur Ausweichung der Verteidigung die Maskade-Technik keine Abdeckung hat. Wenn Sie weiter suchen, bezieht sich die Masquerading-Technik auf die Masquerade-Aufgabe oder den Masquerade-Service, der auch einen Security Incident zugeordnet ist. Dies zeigt, dass es eine Lücke in der Technikerkennungsabdeckung für die Masquerading-Technik gibt und Sie die gesamte Technikerkennungsabdeckung überarbeiten möchten.

Zeigen Sie Erkennungsregeln an

Um anzuzeigen, ob die Erkennungsregeln für eine bestimmte Technik definiert sind, klicken Sie auf **Erkennungsregeln anzeigen** . Sie können auch jede zugeordnete Erkennungsregel mit ihrer Definition anzeigen.

Diese Informationen basieren auf Zuordnung von Erkennungsregeln Die Sie definiert haben. Zeigen Sie die zugehörigen Erkennungsregeln an.

Zeigen Sie CVEs an, die der Technik zugeordnet sind

Um die Informationen zu allgemeinen Schwachstellen und Gefährdungen (Common Vulnerabilities and Exposures, CVE) anzuzeigen, die den einzelnen Techniken zugeordnet sind, klicken Sie auf **Zeigt CVEs an, die der Technik zugeordnet sind** . Die CVE-zu-Technik-Informationen basieren auf den Informationen, die in verfügbar sind CVE – Technikzuordnungsmodul . Dies bietet Ihnen Einblicke in bekannte Schwachstellen und informiert Sie, ob Angreifer Ihre Organisation potenziell ausnutzen können.

Wichtig:
Die Heatmap wird erweitert, um nur die relevanten CVEs anzuzeigen, die den Vits zugeordnet sind

Um Vits anzuzeigen, die CVEs und Techniken zugeordnet sind, wählen Sie aus **Vits anzeigen, die CVE und Techniken zugeordnet sind** . Um weitere Filtertechniken ohne Vits zu filtern, wählen Sie außerdem aus **Techniken ohne Vits ausblenden** . Die von Ihnen angezeigten CVE- und VIT-Informationen werden aus abgerufen Vulnerability Response Produkt in Ihrer Umgebung. Sie können die gefilterte Liste der CVEs und Vits in der Heatmap anzeigen und für jede Technik aus der Heatmap zu jedem CVE oder VIT navigieren.

Hinweis:

- Die **Zeigt CVEs an, die der Technik zugeordnet sind** Ist nur verfügbar, wenn Vulnerability Response Produkt ist in Ihrer Umgebung installiert.
- Die VIT- und CVE-Informationen werden basierend auf der geplanten Aufgabe berechnet, die Sie in festgelegt haben MITRE-ATT&CK Eigenschaftenan. Der Planungsauftrag des Basissystems ist auf 24 Stunden festgelegt.

Wenn Sie diesen Filter mit verwenden **Security Incident anzeigen, der der Technik zugeordnet ist** Filtern, können Sie erfahren, ob die bekannten Schwachstellen Security Incidents in Ihrer Organisation verursacht haben.

Sie können weitere Informationen zu jedem CVE anzeigen, um zu analysieren, ob das CVE für Ihre Organisation relevant ist. Zeigen Sie dazu die Schwachstellen-Elemente an. Wenn Schwachstellenelemente erstellt werden, können Sie weitere Informationen zu allen zugehörigen CI-Informationen in anzeigen Vulnerability Response Modul. Sie können auch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

den Schweregrad und die Priorität überprüfen, um fundierte Entscheidungen zu treffen.
Überprüfen Sie CVEs, um fundierte Entscheidungen zu treffen.

Analysieren Sie Security Incidents

Um Security Incidents zu analysieren und die Techniken zu überprüfen, die von einem Angreifer für einen Angriff verwendet werden, klicken Sie auf **Analysieren Sie Security Incidents** . Sie können mehrere Security Incidents zur Analyse hinzufügen, indem Sie kommagetrennte Zeichenfolgen verwenden.

Dieser Filter hilft Ihnen, einen Security Incident zu analysieren. Sie können erfahren, warum der Incident aufgetreten ist, welche Techniken ausgenutzt wurden, ob bekannte Bedrohungsakteure beteiligt waren, ob die Bedrohungsakteure eine bestimmte Sequenz für einen Angriff verwendet haben usw. Da Sie mehrere Security Incidents gleichzeitig analysieren können, können Sie die Informationen korrelieren, um festzustellen, ob sie zugehörig sind oder ob es sich um einen isolierten Incident handelt. Wenn die Security Incidents zusammenhängen und Sie ein Muster beobachten, können Sie ihren Fortschritt in der Auslösekette überprüfen, um den Angriff zu stoppen oder eine Verteidigungsstrategie für Ihre Organisation zu erstellen.

Wenn Sie verwenden **Analysieren Sie Security Incidents** Filter mit primären Filtern, z. B. einem **Angreifergruppe** , Sie können korrelieren, ob bekannte Angreifer beteiligt sind. Wenn beispielsweise mehrere Security Incidents analysiert werden, sind die Techniken, die den Security Incidents zugeordnet sind, in Form einer Kill Chain vorhanden. Wenn Sie die Informationen mit dem Angreifer überschneiden, bemerken Sie eine Überschneidung zwischen den Techniken, die dem Security Incident zugeordnet sind, und den Techniken, die dem Angreifer zugeordnet sind. Nur die Informationen zur überlappenden Technik werden angezeigt, wenn beide Filter aktiviert sind.

Analysieren Sie Security Incidents

Verwenden von Overlay, um Security Incidents und Angreifergruppen zu analysieren

Verwenden Sie **Aktivieren Sie Überlagerung/Analysieren** Filter, um das Verhalten der Angreifer anzuzeigen, einen oder mehrere der Security Incidents zu analysieren und die Informationen zu korrelieren, um zu sehen, ob ein Angriff ein isolierter Incident oder ein koordinierter Angriff eines bekannten Angreifers ist.

Sie können beispielsweise jetzt die Security Incidents und das Verhalten der Kill Chain von Angreifern von Bedrohungen in derselben Ansicht anzeigen. Diese Ansicht enthält Überschneidungsinformationen, die Sie über den Angriff und das bekannte Angreiferverhalten informieren. Auf diese Weise können Sie analysieren, ob es sich um einen isolierten Angriff oder einen koordinierten Angriff eines bekannten Angreifers handelt.

Durch Aktivieren des Überlagerungsfilters „Analysieren“ werden alle primären Filter außer ignoriert **Angreifergruppe** Filtern und ignoriert den erweiterten Filter **Filtern Sie nach technikrelevanter Priorität** Beim Generieren einer Ansicht.

Sobald Sie den Überlagerungsfilter „Analysieren“ aktiviert haben, verwenden Sie die Farbpalette, um Farben für Folgendes zuzuweisen:

- Analysieren Sie Security Incident
- Angreifergruppe
- Überlagerung

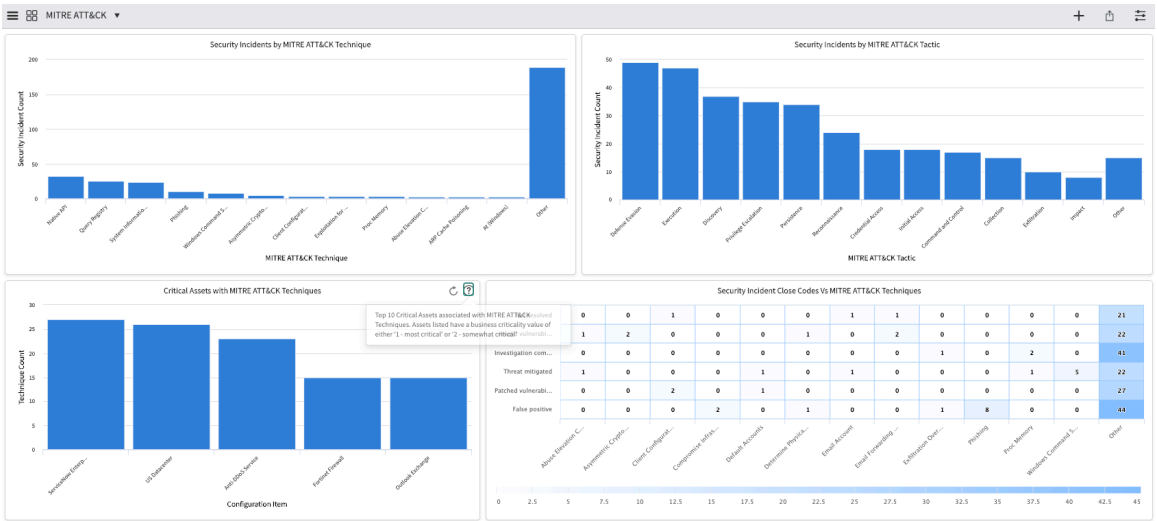
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgende Abbildung zeigt, dass die Angreifergruppe APT18 auf mehrere Techniken und Taktiken in der Kill Chain verteilt ist. Die Analyse zeigt auch, dass es drei Techniken gibt, die die Angreifergruppe und Security Incidents, die Sie nachverfolgen, überlagern. Diese Abbildung zeigt die Überlagerungsinformationen für Angreifer und Security Incident.

Mit MITRE-ATT&CK Dashboard

Die MITRE-ATT&CK Das Dashboard bietet eine Ansicht der Datenquellenabdeckung, -Taktiken und -Techniken, die in Ihrer Organisation verwendet werden.

Die MITRE-ATT&CK Das Übersichtsmodul wird angezeigt MITRE-ATT&CK Informationen zu Security Incidents, einschließlich Trends und Berichte. Sie können auf einen beliebigen Teil eines Widgets (Balken, Datenpunkt, Tabelle usw.) klicken, um Daten anzuzeigen, die für diesen Teil spezifisch sind.



Verwenden Sie MITRE-ATT&CK Dashboard zum Anzeigen Ihrer sicherheitsbezogenen Daten

Verwenden Sie MITRE-ATT&CK Dashboard, um einen Überblick über die Datenquellenabdeckung, -Taktiken und -Techniken zu erhalten, die in Ihrer Organisation verwendet werden.

Vorbereitungen

Erforderliche Rolle: sn_si.ciso, sn_si.Analyst, sn_si.Manager, sn_ti.read

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **MITRE ATT&CK-Repository** > **Übersicht**an.
2. Klicken Sie auf eines der folgenden Widgets, um zusätzliche Details anzuzeigen:
   - Security Incidents von MITRE-ATT&CK Technik
   - Security Incidents von MITRE-ATT&CK Taktik
   - Kritische Assets mit MITRE-ATT&CK Techniken
   - Abschlusscodes Für Security Incidents Vs MITRE-ATT&CK Techniken
   - MITRE-ATT&CK-Techniken nach Erkennungsabdeckung
   - MITRE-ATT&CK-Techniken nach Risikominderungsabdeckung
   - Bedrohungsgruppen nach MITRE-ATT&CK-Technik
   - CVEs nach MITRE-ATT&CK-Technik

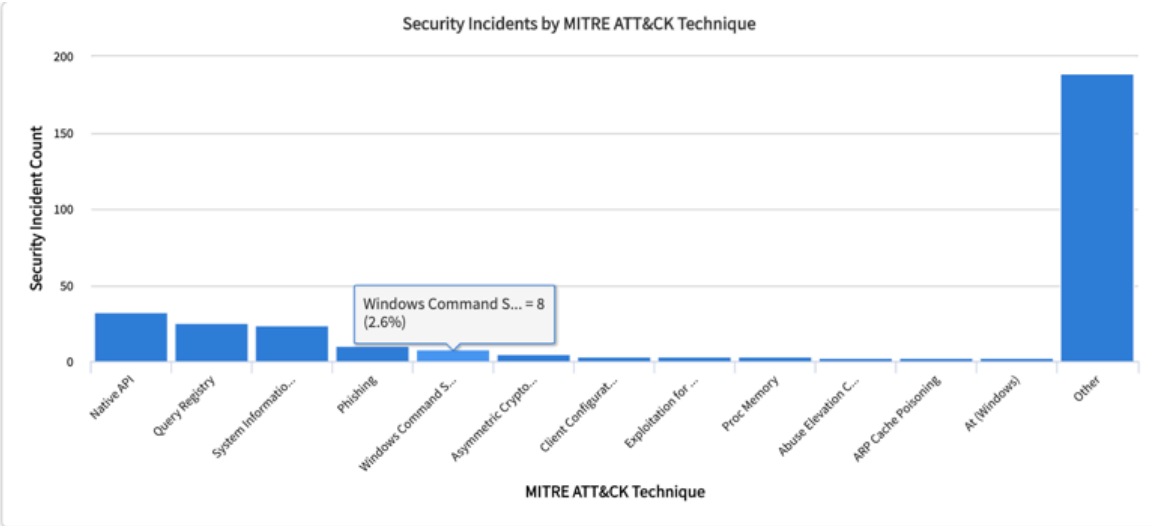
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MITRE-ATT&CK Widgets

Die MITRE-ATT&CK Das Übersichtsmodul besteht aus Widgets, mit denen Sie korrelieren können MITRE-ATT&CK Informationen mit den Security Incident-Informationen in Ihrer Umgebung.

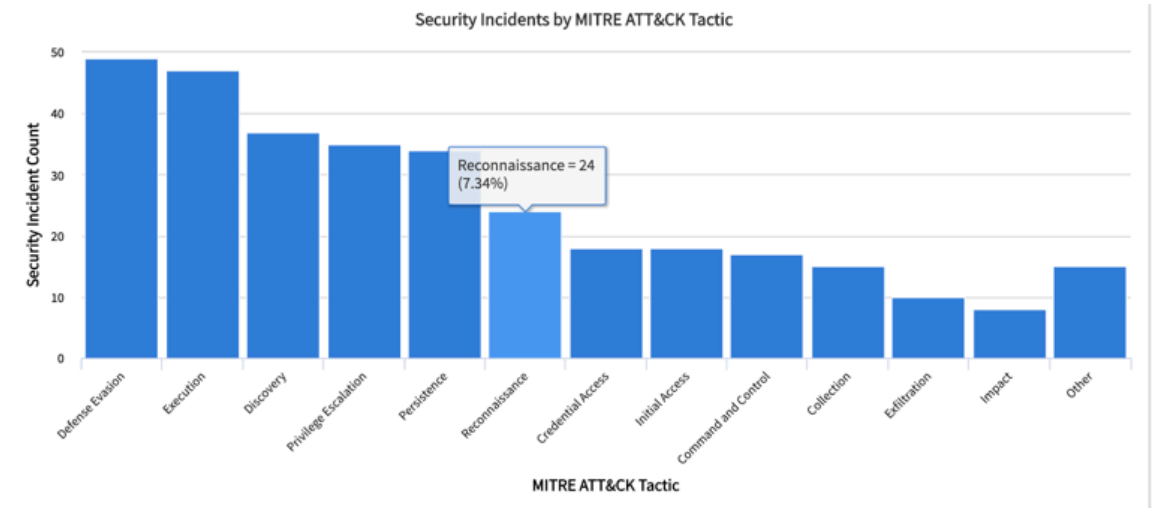
Beispiel für Security Incidents von MITRE-ATT&CK Technik

In diesem Beispiel ist **Security Incidents nach MITRE ATT&CK-Technik** Widget zeigt die Techniken nach Security Incident in der Umgebung einer Organisation in den letzten 90 Tagen an.



Beispiel für Security Incidents von MITRE-ATT&CK Taktik

In diesem Beispiel ist **Security Incidents nach MITRE ATT&CK-Taktik** Widget zeigt die wichtigsten Taktiken nach Security Incident in der Umgebung einer Organisation in den letzten 90 Tagen an.

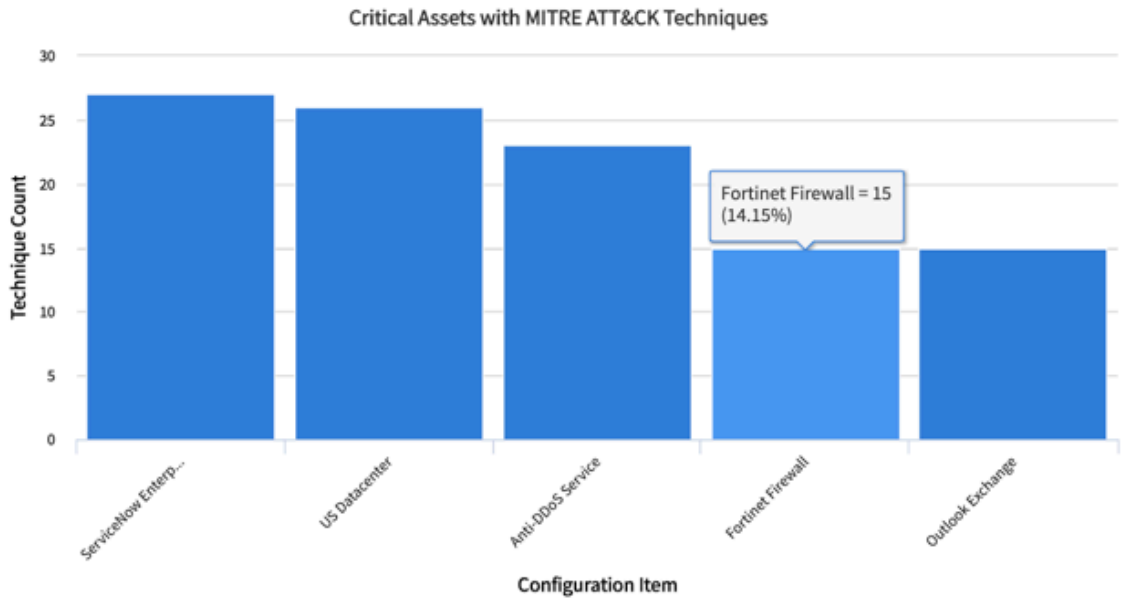


Beispiel für kritische Assets mit MITRE-ATT&CK Techniken

In diesem Beispiel ist **Kritische Assets mit MITRE ATT&CK-Techniken** Widget zeigt die 10 wichtigsten kritischen Assets an, die mit verknüpft sind MITRE-ATT&CK Techniken. Die Assets haben eine Geschäftsrelevanz von entweder 1 (sehr kritisch) oder 2 (etwas kritisch).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

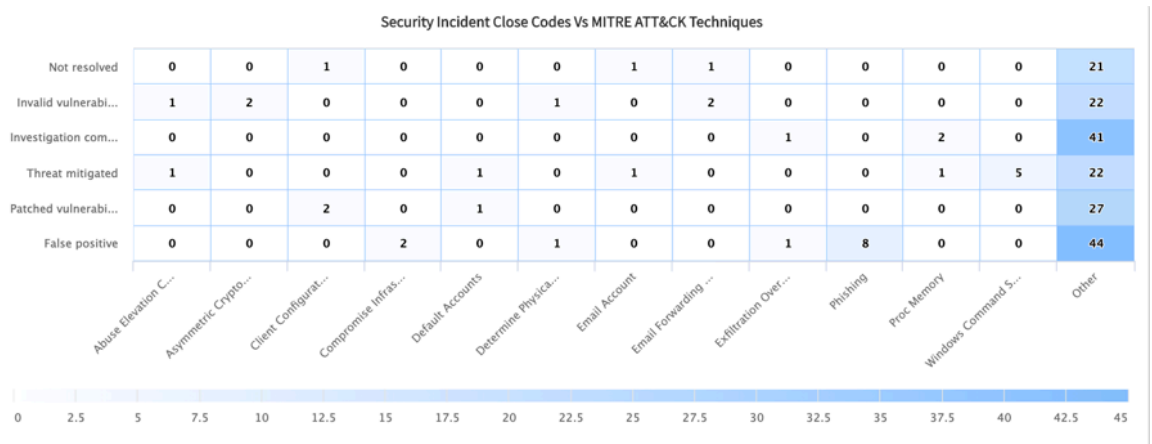
Mit diesem Bericht kann eine Organisation die Typen und die Anzahl der Techniken anzeigen, die für die Übertragung von Angriffen auf kritische Assets verwendet werden.



Beispiel für Abschlusscodes für Security Incidents vs MITRE-ATT&CK Techniken

In diesem Beispiel ist **Abschlusscodes Für Security Incidents Vs** *MITRE-ATT&CK* **Techniken** Widget zeigt die Abschlusscodes für Security Incidents an, die den identifizierten Top-Techniken in der Umgebung einer Organisation zugeordnet wurden.

Auf der x-Achse werden die häufigsten Techniken angezeigt, die zum Übertragen von Angriffen auf das Unternehmen verwendet wurden, und auf der y-Achse werden die geschlossenen Codes angezeigt.

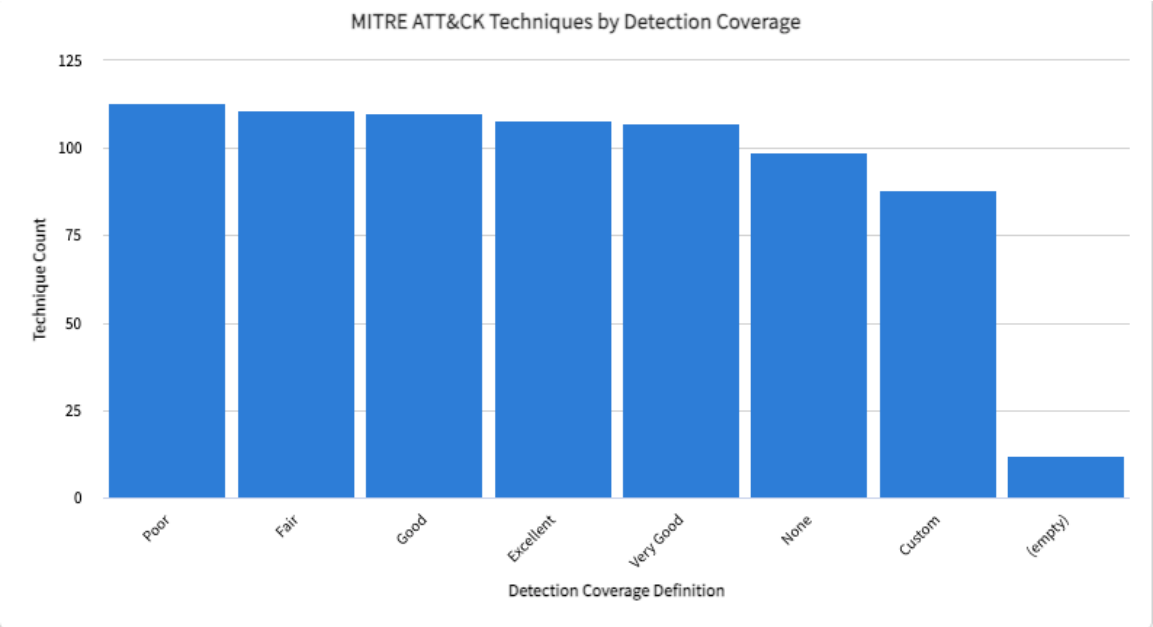


Beispiel für Erkennungsabdeckung durch MITRE-ATT&CK Techniken

In diesem Beispiel ist **MITRE-ATT&CK-Techniken nach Erkennungsabdeckung** Widget zeigt die Technikanzahl nach Erkennungsabdeckung in Ihrer Umgebung an.

Auf der x-Achse wird die Technikanzahl angezeigt, und auf der y-Achse werden die Erkennungsabdeckungstypen angezeigt.

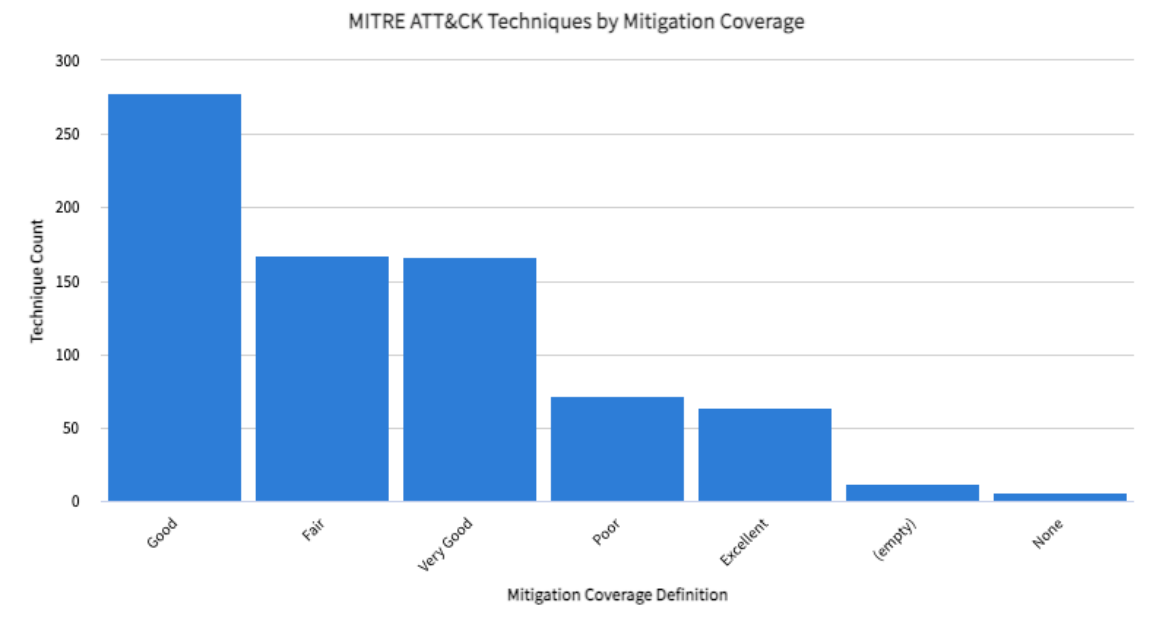
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beispiel für die Minderungsabdeckung durch MITRE-ATT&CK Techniken

In diesem Beispiel ist **MITRE-ATT&CK-Techniken nach Risikominderungsabdeckung** Widget zeigt die Technikanzahl nach der Minderungsabdeckung in Ihrer Umgebung an.

Auf der x-Achse wird die Technikanzahl angezeigt, und auf der y-Achse werden die Abdeckungstypen der Risikominderung angezeigt.

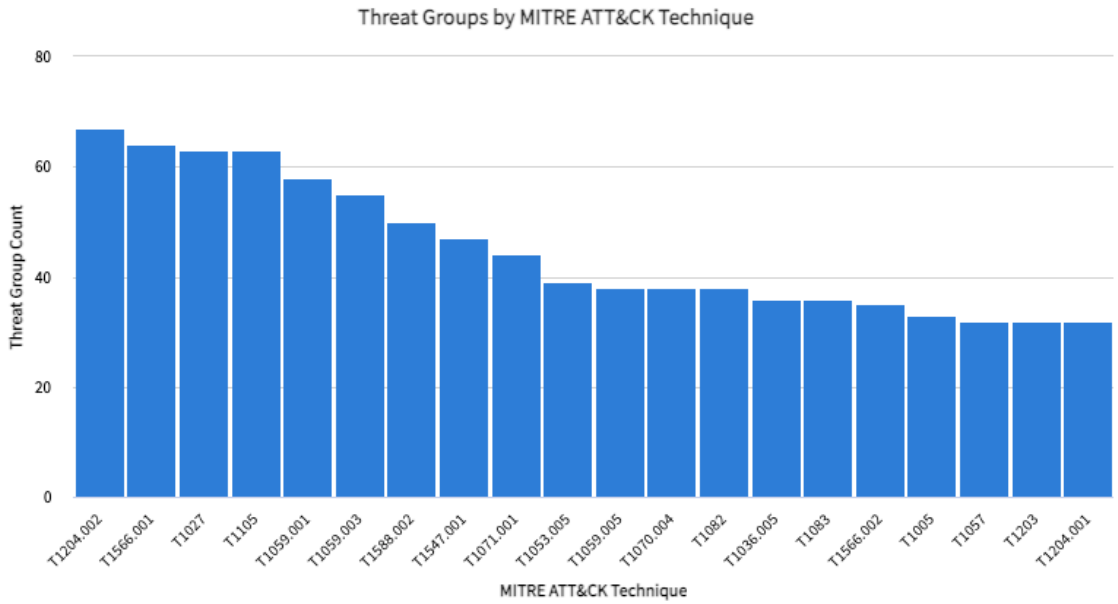


Beispiel für Bedrohungsgruppen nach MITRE-ATT&CK Techniken

In diesem Beispiel ist **Bedrohungsgruppen nach MITRE-ATT&CK-Technik** Widget zeigt die Techniken nach Anzahl der Bedrohungsgruppen an. Dieses Widget zeigt 20 Techniken mit der höchsten Anzahl von Bedrohungsgruppen an.

Auf der x-Achse wird die Anzahl der Bedrohungsgruppen angezeigt, und auf der y-Achse wird angezeigt MITRE-ATT&CK Techniken.

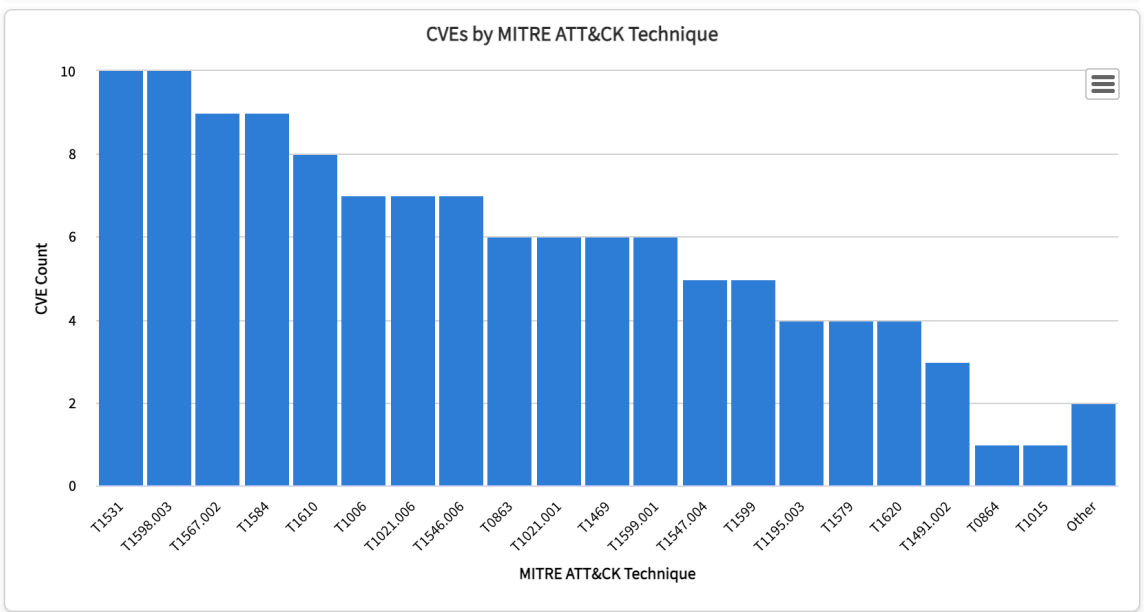
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beispiel für CVEs von MITRE-ATT&CK Techniken

In diesem Beispiel ist **CVEs nach MITRE-ATT&CK-Technik** Widget zeigt die Techniken mit der relevanten CVE-Anzahl in Ihrer Umgebung an.

Auf der x-Achse wird die relevante CVE-Anzahl angezeigt, und auf der y-Achse wird angezeigt MITRE-ATT&CK Techniken.



Threat Intelligence – Administration

Die Threat Intelligence Das Basissystem ist bei der Aktivierung einsatzbereit. Sie können bestimmten Modulen im Anwendungsmenü „Administration“ Datensätze hinzufügen, die meisten sind jedoch bereits mit branchenüblichen Informationen ausgefüllt.

Die folgenden Anwendungen sind unter verfügbar **Verwaltung** Modul von Threat Intelligence Navigationsleiste:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence-Administrationsanwendungen

Anwendung	Beschreibung
Eigenschaften	Threat Intelligence Eigenschaften Mit können Sie steuern, wie verschiedene Aspekte der Systemfunktion einschließlich der Einstellung von API-Schlüsseln.
Angriffsmechanismen	Dieses Modul organisiert Angriffsmuster hierarchisch basierend auf Mechanismen, die häufig beim Ausnutzen einer Schwachstelle verwendet werden.
Angriffsmotivationen	In diesem Modul werden die möglichen Angriffsmotivationen aufgelistet, die die Intensität eines Angriffs durch einen Bedrohungsakteur oder einen Angriffssatz prägen.
Discovery-Methoden	In diesem Modul wird beschrieben, wie Security Incidents erkannt werden.
Feeds	Diese Funktion ist veraltet.
Indikatortypen	Dieses Modul wird verwendet, um Cyberbedrohungsindikatoren zu charakterisieren, die aus Mustern bestehen, die bestimmte Bedingungen erkennbarer Elemente identifizieren, sowie kontextbezogene Informationen über die Bedeutung der Muster und wie und wann darauf reagiert wird.
Infrastrukturtypen	Dieses Modul listet die möglichen Klassifizierungen der Infrastruktur auf.
Beabsichtigte Wirkungen	Diese Anwendung wird verwendet, um die beabsichtigte Wirkung eines Bedrohungsakteurs auszudrücken.
Malware-Fähigkeiten	In diesem Modul werden die möglichen Fähigkeiten von Malware aufgelistet.
Schadsoftwaretypen	Dieses Modul listet die möglichen Klassifizierungen von Malware auf.
Benachrichtigungen	Dieses Modul wird zum Erstellen verwendet E-Mail-Benachrichtigungen . Dies beinhaltet die Angabe, wann sie gesendet werden, wer sie empfängt und was sie enthalten.
Erkennbare Typen	Dieses Modul listet die möglichen Klassifizierungen eines erkennbaren Elements auf, z. B. eine IP-Adresse oder einen Datei-Hash.
Berichtstypen	Dieses Modul listet die möglichen Klassifizierungen von Bedrohungsberichten auf.
Bedrohungsakteurrollen	In diesem Modul werden die Rollen aufgelistet, die die Bedrohungsakteure spielen.
Bedrohungsakteurtypen	Dieses Modul charakterisiert böswillige Akteure (oder Angreifer), die eine Cyberangriffsbedrohung darstellen, einschließlich vermuteter Absicht und historisch beobachtetem Verhalten.
Rechner für Funde der Bedrohungssuche	Dieses Modul berechnet die Ergebnisse basierend auf den empfangenen Antworten. Bei Integrationen von Drittparteien, die die berechneten Ergebnisse liefern, ordnet der Ergebnisrechner der Bedrohungssuche die Ergebnisse den unterstützten Ergebnissen im System zu. Weitere Informationen finden Sie unter Rechner für Funde der Bedrohungssuche.
Tooltypen	Dieses Modul listet die mögliche Klassifizierung von Tools auf.

Rechner für Funde der Bedrohungssuche

Der Ergebnisrechner für die Bedrohungssuche hilft Ihnen, die Ergebnisse erkennbarer Elemente basierend auf den empfangenen Antworten zu berechnen.

Sie können einen Ergebnisrechner für die Bedrohungssuche für Ihre Integration erstellen und mithilfe eines Skripts bestimmen, wie Sie die verschiedenen Ergebnisse erkennbarer Elemente identifizieren möchten. Der Ergebnisrechner für die Bedrohungssuche enthält ein Beispielskript, das im Basissystem enthalten ist, mit dem Sie die Ergebnisse erkennbarer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elemente identifizieren oder dieses Skript entsprechend Ihren Anforderungen ändern können.

Bei Integrationen von Drittparteien, die die berechneten Ergebnisse liefern, ordnet der Ergebnisrechner der Bedrohungssuche die Ergebnisse den unterstützten Ergebnissen im Basissystem zu.

Rollup-Ergebnisse Der Bedrohungssuche

Wenn Sie mehrere Bedrohungssuchergebnisse für ein erkennbares Element von den verschiedenen Integrationsanbietern haben, werden die aktuellen Bedrohungssuchergebnisse aller Lieferanten berücksichtigt, und die allgemeinen Ergebnisse erkennbarer Elemente werden wie folgt markiert:

Rollup-Ergebnisse Der Bedrohungssuche

Letztes Ergebnis Erkennbarer Elemente	Gesamtergebnis Erkennbarer Elemente
Böswillig	Wenn einer der Integrationsanbieter das erkennbare Element als böswillig meldet, wird das Gesamtergebnis des erkennbaren Elements als böswillig markiert.
Verdächtig	Wenn keiner der Integrationsanbieter das erkennbare Element als böswillig meldet, meldet es einer von ihnen als verdächtig, und dann wird das allgemeine Ergebnis erkennbarer Elemente als verdächtig markiert.
Clean	Wenn alle Integrationslieferanten das erkennbare Element als bereinigt melden, wird das Gesamtergebnis des erkennbaren Elements als bereinigt markiert.
Unbekannt	Wenn keiner der Integrationsanbieter das erkennbare Element als böswillig oder verdächtig meldet und einer von ihnen es als Unbekannt meldet, wird das allgemeine Ergebnis erkennbarer Elemente als Unbekannt markiert.

Mithilfe Von Ergebnisrechnern Für Bedrohungssuche

Verwenden Sie den Ergebnisrechner für Bedrohungssuche, um die Ergebnisse erkennbarer Elemente für Ihre Integration zu berechnen.

Vorbereitungen

Erforderliche Rolle: sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Administration** > **Rechner für Funde der Bedrohungssuche**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.
4. Klicken Sie auf **Aktualisieren**.

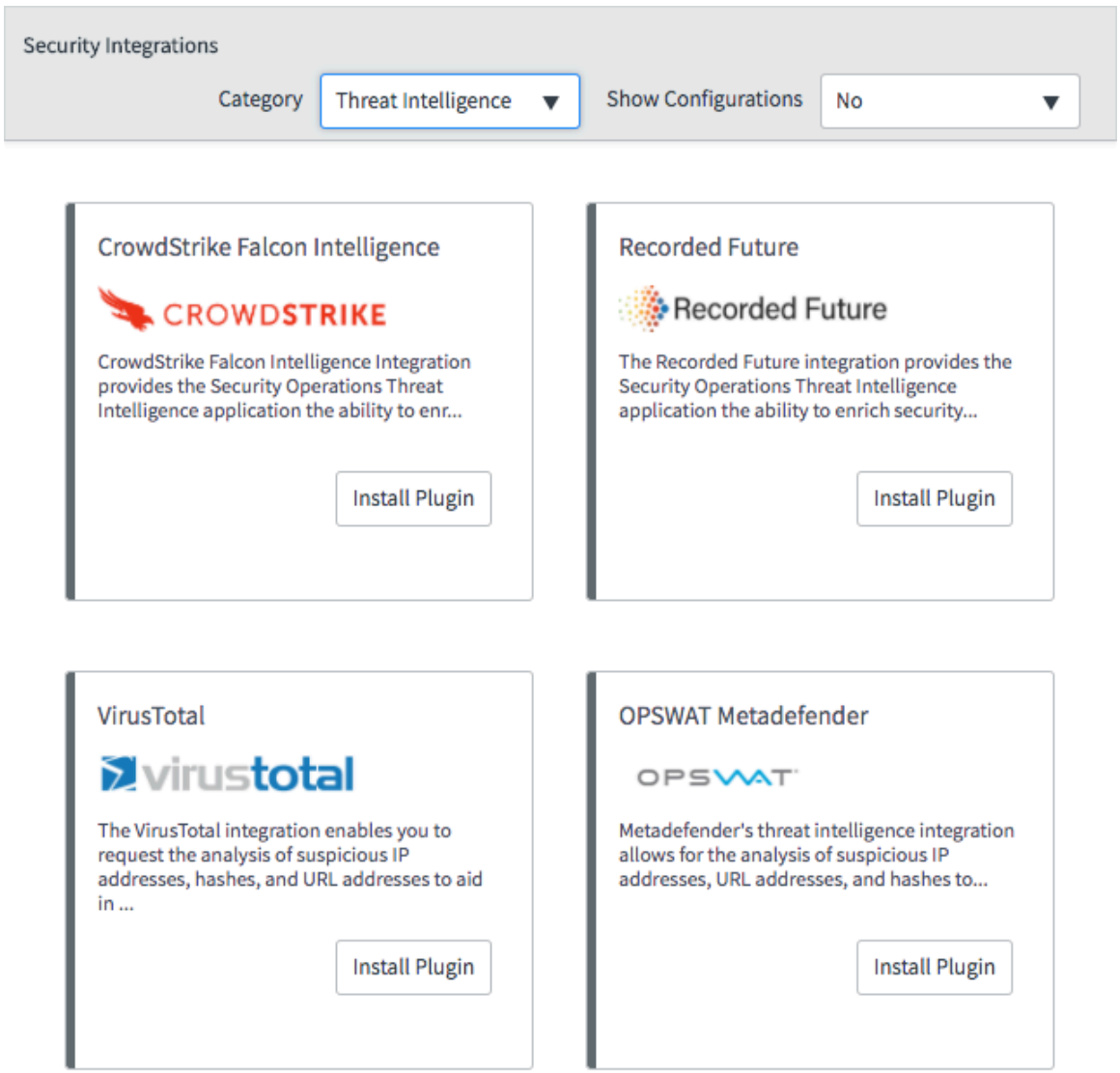
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence-Integrationen

Die Threat Intelligence Das Basissystem enthält Integrationen in Softwarepakete zur Malware-Erkennung von Drittanbietern. Dieser Abschnitt enthält Anweisungen zum Aktivieren der Plugins und zum Konfigurieren beider ServiceNow Und Drittpartei-Integrationen. Ebenfalls enthalten sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten Integrationen, die im Basissystem enthalten sind.

Integrationskonfigurationen

Das Basissystem enthält eine Reihe von „Karten“ für jede der Integrationsimplementierungen, die Sie aktivieren und verwenden können. Außerdem werden Karten für alle im ServiceNow Store veröffentlichten Integrationen angezeigt, die Abhängigkeiten von haben Security Operations Plugins. Die Integrationskarten können angezeigt werden, indem Sie auswählen **Security Operations** > **Integrationskonfigurationen**an.



Sie können die sichtbaren Integrationen mit filtern **Kategorie** Dropdown-Menü. Die **Konfigurationen Anzeigen** Im Dropdown-Menü können Sie mehrere Instanzen von Implementierungen anzeigen, die ihre Erstellung ermöglichen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schaltflächen auf Integrationskarten

Integrationskarten zeigen je nach Status der Integration und Quelle der Karte verschiedene Schaltflächen an.

Schaltfläche	Beschreibung
Plugin installieren	Klicken Sie auf diese Schaltfläche, um das entsprechende Plugin zu installieren, um die Integration zu aktivieren. Nachdem das Plugin installiert wurde, ändert sich die Schaltfläche in **Konfigurieren** .
Konfigurieren	Klicken Sie auf diese Schaltfläche, um Informationen zum Konfigurieren der Integration einzugeben. Bei einigen Integrationen müssen Sie möglicherweise API-Schlüssel oder URLs eingeben, die von der Website der Drittpartei-Integration erworben wurden.
Neu	Mit bestimmten Integrationen wie Carbon Black und IBM QRadar können Sie mehrere Implementierungen derselben Integration definieren. Klicken Sie für diese Integrationen auf **Neu** Nachdem das Plugin aktiviert wurde. Mit den Karten können Sie Plugins installieren (falls zutreffend) und die Implementierungen für die Verwendung konfigurieren.
Seite öffnen	Im -Basissystem führt Ihre Instanz eine Abfrage des ServiceNow Store für alle Anwendungen durch, die Abhängigkeiten von haben Security Operations Plugins. Wenn diese Anwendungen gefunden werden und die zugehörigen Anwendungs-Plugins aktiviert sind, werden Integrationskarten für sie mit den anderen Sicherheitsintegrationskarten angezeigt. Klicken Sie Auf **Öffnen Sie Die Seite** Um auf die Website der Drittparteianwendung zuzugreifen, um die Integration zu konfigurieren. Nachdem Sie die Konfiguration abgeschlossen haben, die **Öffnen Sie Die Seite** Schaltfläche ändert sich in **Konfigurieren** .

CrowdStrike Falcon Intelligence-Integration

CrowdStrike Falcon Intelligence Bereichert Threat Intelligence Mit Daten für Security Incidents und zugehörige erkennbare Elemente.

Erkunden

- Integrationsüberblick CrowdStrike Falcon Intelligence
- Security Incident Response-Integrationen

Einrichten

Aktivieren und konfigurieren Sie CrowdStrike Falcon Intelligence Integration

---

Verwenden

- Führen Sie Suchen nach erkennbaren Elementen durch
- Bedrohungssuche – CrowdStrike Falcon Intelligence Flows

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie Komponenten, die mit einer Anwendung installiert sind

---

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Integrationsüberblick CrowdStrike Falcon Intelligence

CrowdStrike Falcon Intelligence Bietet Cybersicherheits-Intelligence, die einfach in integriert werden kann Security Operations.

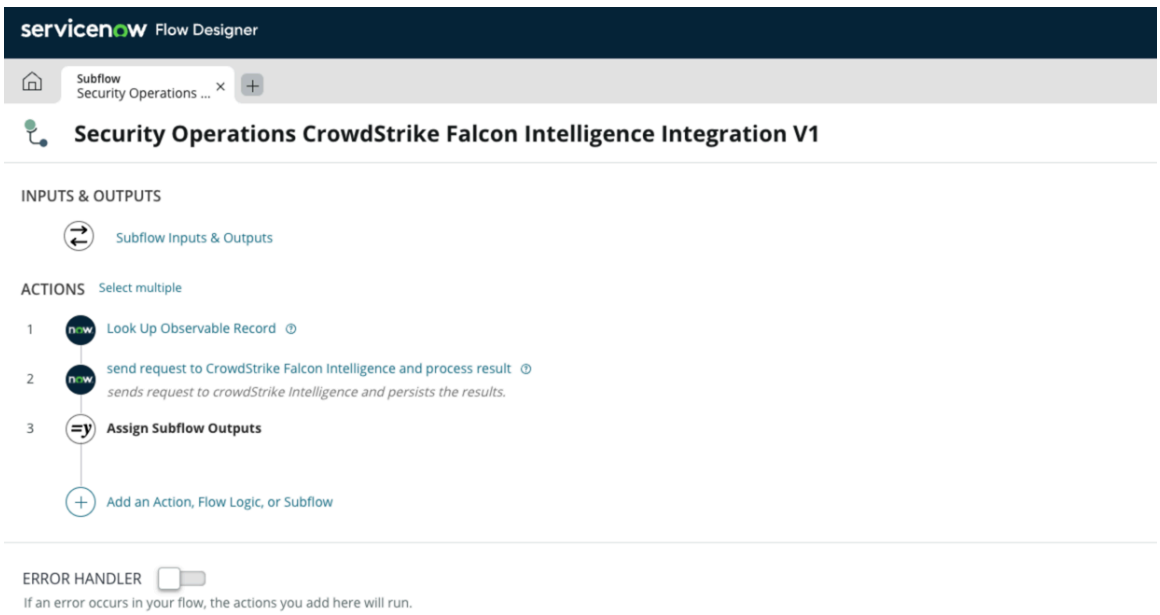
Hinweis:
Die Threat Intelligence Plugin ist erforderlich, um zu implementieren CrowdStrike Falcon Intelligence Integration.

Bedrohungssuche – CrowdStrike Falcon Intelligence Flows

Die Bedrohungssuche – CrowdStrike Falcon Intelligence Flow Designer führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn die erkennbaren Elemente von einem Typ sind, der von erkannt wurde CrowdStrike Falcon Intelligence, Die erkennbaren Elemente werden auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

Dieser Flow wird durch ausgelöst Integration von Security Operations: Fähigkeit zur Bedrohungssuche Wenn Sie ein oder mehrere erkennbare Elemente in einer Beobachtungsliste veröffentlichen und die CrowdStrike Falcon Intelligence-Implementierung ausgewählt ist. Nachdem sie veröffentlicht wurden, können die Beobachtungslisten in der CrowdStrike Falcon Host-Software angezeigt werden.

Erforderliche Rolle: Administrator



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zu den von diesem Flow Designer verwendeten Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Aktivieren und konfigurieren Sie CrowdStrike Falcon Intelligence Integration

Mit der Integrationskonfigurationsfunktion können Sie Sicherheitsintegrationen von Drittparteien, einschließlich, schnell aktivieren und einrichten CrowdStrike Falcon Intelligence Integration. Bevor Sie verwenden können CrowdStrike Falcon Intelligence, Sie müssen es aus herunterladen ServiceNow Store Und fügen Sie den entsprechenden API-Schlüssel und die entsprechende ID hinzu.

Vorbereitungen

Erforderliche Rolle: Administrator

- Die Threat Intelligence Das Plugin muss installiert und aktiviert werden, bevor Sie verwenden können CrowdStrike Falcon Intelligence Integration.
- Rufen Sie die API-Client-ID und das API-Client-Geheimnis unter Ihrem ab CrowdStrike Falcon Intelligence Profil.
- Wenn Sie ein Upgrade durchführen CrowdStrike Falcon Intelligence Integration aus einer vorherigen Version, dann müssen Sie die vorhandene Konfiguration löschen und eine neue Konfiguration einrichten. Die Integration unterstützt die OAUTH2-Authentifizierung. Für dieses Update müssen Sie eingeben **API-Client-ID** Und **API-Client-Geheimnis** Dient zum Authentifizieren und Abschließen der Konfiguration.
- In CrowdStrike Falcon Intelligence Portal **API-Umfänge** , Aktivieren Sie **Lesen** Einstellung für **Indikatoren (Falcon X)** Oder **IOCs (Indikatoren der Gefährdung)** .

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. In CrowdStrike Falcon Intelligence Karte, klicken Sie auf **Konfigurieren** .
4. Füllen Sie im Formular die Felder aus, um die Konfiguration abzuschließen:

CrowdStrike Falcon Intelligence Konfiguration

Feld	Beschreibung
Name	Name der Integration, z. B. `Demo-1` .
API-Client-ID	Die Client-ID, die Sie aus dem Abschnitt „Einstellungen“ Ihres Account-Profils in abrufen CrowdStrike Falcon Intelligence Portal.
API-Client-Geheimnis	Der geheime Clientschlüssel, den Sie im Abschnitt „Einstellungen“ Ihres Account-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Profils in abrufen CrowdStrike Falcon Intelligence Portal.

5. Klicken Sie auf **Absenden**.

Ergebnisse

Nach der Konfiguration CrowdStrike Falcon Intelligence Kann zum Durchführen von Suchen nach erkennbaren Elementen in ausgewählt werden Threat Intelligence Und für erkennbare Elemente in Security Incidents.

Zugehörige Informationen

Führen Sie Suchen nach erkennbaren Elementen durch

Have I Been Pwned?-Integration

Die Security Operations Have I Been Pwned? Mit der Integration können Sie Suchen nach Domänennamen und E-Mail-Adressen übermitteln, um festzustellen, ob personenbezogene Daten des Anwenders durch Datenschutzverletzungen gefährdet wurden.

Erkunden

Security Incident Response-Integrationen

Einrichten

- Have I Been Pwned? Integrationen-Setup
- Aktivieren

Verwenden

Führen Sie Suchen nach erkennbaren Elementen durch Bedrohungssuche – Have I Been Pwned? Flow

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie Komponenten, die mit einer Anwendung installiert sind

Problembehandlung und Hilfe

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Have I Been Pwned? Integrationen-Setup

Have I Been Pwned? Ist eine kostenlose Ressource, die verwendet wird, um zu bewerten, ob jemand möglicherweise gefährdet wurde, da sein Online-Account bei einer Datenschutzverletzung gefährdet oder „pwned“ wurde. Es lässt sich problemlos in integrieren Security Operations.

Bevor Sie verwenden können Have I Been Pwned? Integration müssen Sie das Plugin aktivieren. Bei Bedarf können Sie auch Ihre X509-SSL-Zertifizierung aktualisieren.

Die Security Incident Response, Threat Intelligence, Und Security Operations Have I Been Pwned? Plugins sind erforderlich, um zu implementieren Security Operations Have I Been Pwned? Integration.

Bedrohungssuche – Have I Been Pwned? Flow

Die Bedrohungssuche – Have I Been Pwned? Flow führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn die erkennbaren Elemente von einem Typ sind, der von erkannt wurde Have I Been Pwned?, Die erkennbaren Elemente werden auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

Erforderliche Rolle: sn_si_admin

Dieser Flow wird durch ausgelöst Integration von Security Operations: Fähigkeit zur Bedrohungssuche Wenn Sie eine Bedrohungssuche für ein oder mehrere erkennbare Elemente durchführen, und Have I Been Pwned? Implementierung ist ausgewählt. Weitere Informationen finden Sie unter Führen Sie Suchen nach erkennbaren Elementen durch.

Wurde ich in Flow verschoben

Informationen zu den von diesem Flow verwendeten Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Aktivieren

Mit der Integrationskonfigurationsfunktion können Sie Sicherheitsintegrationen von Drittparteien, einschließlich, schnell aktivieren und einrichten Security Operations Have I Been Pwned? Integration. Bevor Sie verwenden können Have I Been Pwned? Integration müssen Sie sie aus herunterladen ServiceNow Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Die Threat Intelligence Das Plugin muss installiert und aktiviert werden, bevor Sie verwenden können Security Operations Have I Been Pwned? Integration.

Erforderliche Rolle: sn_si_admin

Prozedur

Laden Sie die Integration aus dem herunter ServiceNow Storean.
Diese Integration unterstützt eine offene API und erfordert keine weitere Konfiguration. Have I Been Pwned? Kann jetzt zum Durchführen von Suchen nach erkennbaren Elementen in ausgewählt werden Threat Intelligence Und für erkennbare Elemente in Security Incidents.

Zugehörige Informationen

Führen Sie Suchen nach erkennbaren Elementen durch

Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie eine SSL-Verbindung für die Integration benötigen, gibt es Umstände, in denen das vom Drittanbieter bereitgestellte Zertifikat entweder noch nicht vertrauenswürdig ist ServiceNow Oder ist abgelaufen. Diese Aufgabe ist optional.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Erwerben Sie das SSL-Zertifikat vom Drittanbieter.
   Sie können beispielsweise ein X.509-Zertifikat (PEM) von einem SSL-Endpunkt im Firefox-Browser wie folgt importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/` .

   b. Klicken Sie auf das Schlosssymbol in der Adresszeile.

   c. Klicken Sie Auf **Weitere Informationen** Und klicken Sie auf **Sicherheit** Registerkarte.

   d. Klicken Sie Auf **Zeigen Sie Das Zertifikat An** Und klicken Sie auf **Detail** Registerkarte.

   e. Klicken Sie Auf **Exportieren** Um das PEM in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor-Tool, und kopieren Sie den Inhalt in die Zwischenablage.
   Sie muss mit beginnen `----- ZERTIFIKAT BEGINNEN------` Und enden mit `----- ENDZERTIFIKAT-----` .

2. Navigieren zu **Systemdefinition** > **Zertifikate**an.
3. Klicken Sie Auf **Neu** Und Erstellen Sie einen neuen Datensatz Für die Integration.
4. In **PEM-Zertifikat** , Fügen Sie das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an.

b. Wählen Sie den aktiven Standard-Identitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.

c. Scrollen Sie nach unten zu **X.509-Zertifikate** Zugehörige Liste, und klicken Sie auf **Bearbeiten** .

d. Verschieben Sie das neu erstellte Zertifikat in **Ausgewählt** Spalte.

6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

Hinweis:
Wenn Sie ein abgelaufenes Zertifikat haben, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 ersetzt ein ablaufendes SAML-Zertifikat .

MISP integration for Security Operations

Mit MISP integration for Security Operations, Sie können Security Incidents mit Sichtungssuchen, Ergänzung erkennbarer Elemente untersuchen und Ereignisse in erstellen oder aktualisieren MISP. Verwenden MISP, Sie können zielgerichtete Angriffe schneller untersuchen, das Erkennungsverhältnis verbessern und die Anzahl der falsch positiven Ergebnisse in Ihrer Umgebung reduzieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

MISP Übersicht

MISP, Die für steht Malware Information Sharing Platform, Ermöglicht es Ihnen, Bedrohungsinformationen und Indikatoren der Kompromittierung (Indicators of Commitment, IoCs) über die gezielte Malware und Angriffe in Ihrer Community vertrauenswürdiger Mitglieder auszutauschen und freizugeben. Sie können auch freigeben MISP Informationen mit privaten oder offenen Communities. Durch Austausch MISP Informationen können Sie zielgerichtete Angriffe schneller untersuchen, das Erkennungsverhältnis verbessern und die Anzahl der falsch positiven Ergebnisse in Ihrer Umgebung reduzieren.

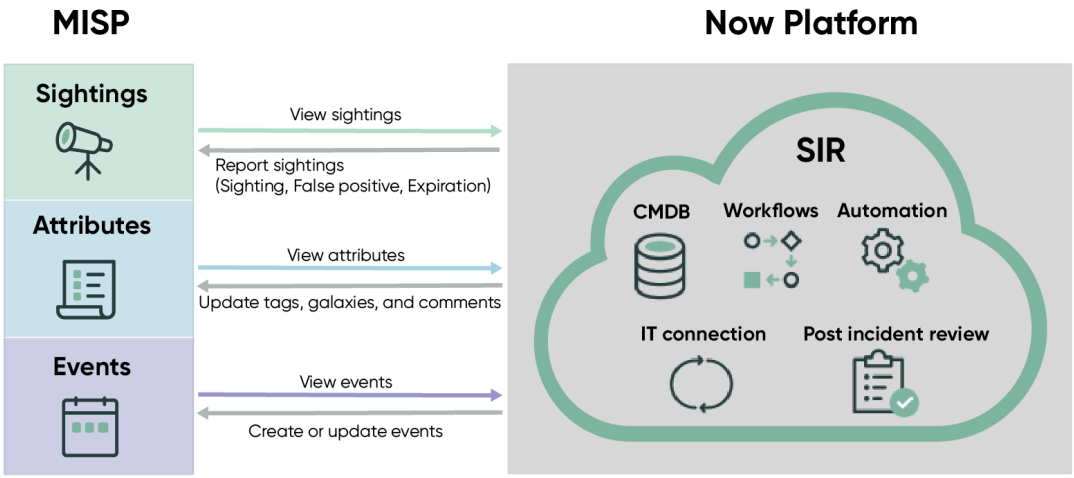
MISP Und Security Operations

Im folgenden Beispiel erfahren Sie, wie es funktioniert MISP Informations-Flows mit Security Operations-Anwendungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über MISP und Security Operations

Now Platform - MISP integration overview



Schlüsselfunktionen

Diese Integration umfasst die Funktionen, die Sie mit ausführen können MISP Wichtige Funktionen:

- Stellen Sie eine Verbindung zu privat und öffentlich her MISP instancesan.
- Unterstützt die manuelle und automatische Sichtungssuche erkennbarer Elemente .
- Sichtungssuche über Fallmanagement ausführen .
- Melden oder aktualisieren Sie Sichtungen für ein Attribut :
  - Erkennbares Element als Sichtung melden (global)
  - Erkennbares Element als falsch positiv melden (global)
  - Melden Sie ein erkennbares Element als abgelaufen
- Unterstützt die manuelle und automatische Ergänzung erkennbarer Elemente . Ergebnisse umfassen MISP Attribut- und Ereignisinformationen, die den erkennbaren Elementen zugeordnet sind.
- Attributanreicherung in MISP Dies umfasst das Hinzufügen oder Aktualisieren Tags , Galaxien , Oder Kommentare .
- Ereigniserstellung in MISP von SIR: Unterstützt die manuelle und automatische Erstellung von Ereignissen in MISP Von SIR.
- Aktualisieren Sie ein MISP Ereignis von SIR Dies umfasst das Hinzufügen oder Aktualisieren Tags , Galaxien , Oder Attribute .
- Fügen Sie einem Security Incident zugeordnete erkennbare Elemente als Attribute hinzu MISP eventan.
- Automatisch extrahieren MITRE-ATT&CK™ Informationen von MISP Attribute Und ordnen Sie die Informationen zu SIR Security Incidents.
- Automatisch hinzufügen SIR MITRE-ATT&CK™ Informationen als Galaxien zu einem MISP eventan.

Schlüsselkonzepte

Diese Integration umfasst die folgenden Schlüsselkonzepte, die Sie kennen müssen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MISP Ist eine Threat Intelligence-Plattform (TIP). Sie verwenden Tipps, um Sicherheitsbedrohungsdaten in Echtzeit zu erfassen, zu korrelieren, zu kategorisieren, freizugeben und zu integrieren, um die Priorisierung von Aktionen zu unterstützen und die Angriffsprävention, -Erkennung und -Reaktion zu unterstützen.
- MISP Ist ein Threat Intelligence Management (TIM). Sie verwenden TIMs, um Bedrohungsdaten durch Kontext in Threat Intelligence umzuwandeln und Bedrohungen automatisch durch anwenderdefinierte Bewertung und Relevanz zu priorisieren.
- MISP Datenebene
  - Ereignisse sind Kapselungen für kontextbezogen verknüpfte Informationen.
  - Attribute sind einzelne Datenpunkte, die Indikatoren oder unterstützende Daten sein können.
  - Objekte sind anwenderdefinierte Vorlagenattribut-Zusammensetzungen.
  - Objektreferenzen sind die Beziehungen zwischen den anderen Bausteinen.
  - Sichtungen sind zeitspezifische Vorkommen eines erkannten Datenpunkts.
- MISP Kontextebene
  - Tags sind Bezeichnungen, die an Ereignisse oder Attribute angehängt sind und aus Taxonomien stammen können.
  - Galaxie-Cluster sind Knowledge Base-Elemente, mit denen Sie Ereignisse oder Attribute kennzeichnen können, die aus Galaxien stammen.
  - Clusterbeziehungen bezeichnen vordefinierte Beziehungen zwischen Clustern.
- Indikatoren enthalten ein Muster, mit dem Sie verdächtige oder böswillige Cyberaktivitäten erkennen können.
- Attribute in MISP Kann Netzwerkindikatoren (IP-Adresse), Systemindikatoren (eine Zeichenfolge im Arbeitsspeicher) oder sogar Bankkontodetails sein. Die Attribute in MISP Werden in anderen SIEMs oder Formaten wie als erkennbare Elemente bezeichnet STIX.
  - Ein Typ beschreibt das Attribut. Beispiel: MD5 oder eine URL.
  - Die Attributkategorie beschreibt ein Attribut. Zum Beispiel eine Nutzlastzustellung.
  - Ein IDS-Tag bestimmt, ob ein Attribut automatisch für die Erkennung verwendet werden kann.

Hinweis:
Weitere Informationen zu finden MISP Konzepte finden Sie unter MISP-Dokumentationswebsite

Wie Ihre Organisation davon profitieren kann MISP integration for Security Operations

Sicherheitsanalysten müssen ein situationsbezogenes Bewusstsein für die Bedrohungslandschaft erlangen und erhalten, was bedeutet, dass sie eine überwältigende Menge von Bedrohungsdaten manuell konsolidieren und integrieren müssen. Das Sammeln, Konsolidieren und Integrieren dieser Daten nimmt wertvolle Zeit in Anspruch, was die Erkennung und Analyse von Bedrohungen verlangsamt. MISP integration for Security Operations Ermöglicht Analysten, durch die Integration von mehr Bedrohungen zu erkennen und schneller zu reagieren MISP Security Intelligence in ein vorhandenes ServiceNow AI Platform Instanz.

Mithilfe von MISP integration for Security Operations, Ihre Organisation kann die folgenden Aktionen ausführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ermöglichen Sie Ihren Sicherheitsanalysten, schnell und mit dem richtigen Kontext zu reagieren.
- Verbessern Sie die Effizienz Ihres Sicherheitsteams, indem Sie die Incident-Flows für die Erkennung und Eindämmung von Bedrohungen automatisieren.
- Reduzieren Sie die Zeit für manuelle Forschung, und ermöglichen Sie Sicherheitsanalysten, Indikatoren innerhalb von zu operationalisieren und zu kuratieren ServiceNow AI Platform.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
MISP Dokumentations-Website	MISP-Dokumentationswebsite
ServiceNow Produktdokumentations-Website	ServiceNow-Produktdokumentationswebsite

MISP – Administration

Sie können einrichten MISP Integration in ServiceNow AI Platform Dient zum Durchführen einer Sichtungssuche, zur Ergänzung erkennbarer Elemente und zum Erstellen und Aktualisieren von Ereignissen in MISP.

Erste Schritte mit MISP integration for Security Operations

Überprüfen Sie die folgenden Informationen, bevor Sie Ihren einrichten MISP integration for Security Operations.

Prüfliste

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform, Threat Intelligence, Und Security Incident Response Rollen.	Die folgenden Rollen werden im verwendet MISP-Funktionen im ServiceNow AI Platform: • Der Administrator (Administrator) installiert die -Anwendungen aus dem ServiceNow Store Und weist die Rollen Security Incident-Administrator (sn_si.admin) und Threat Intelligence-Administrator (sn_ti.admin) zu. • sn_si.admin und sn_ti.admin können die Integration konfigurieren und die automatische einrichten MISP Ereigniserstellungsprofile. • sn_sec_misp.write – die MISP Die Analystenrolle verfügt über Lese- und Schreibberechtigungen für MISP Daten, die die Ereignis- und Attributdaten enthalten. Weitere Informationen finden Sie unter Richten Sie Threat Intelligence Ein .
Weisen Sie die erforderlichen zu MISP Anwenderrollen.	Überprüfung des folgenden Elements: MISP Anwenderrollen und die für die Verwendung von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	erforderlichen Berechtigungen MISP integration for Security Operationsan. **Hinweis:** Für weitere Informationen zu den Anwenderrollen in MISP, Siehe Abschnitt „Rollen“ in MISP-Dokumentationswebsite .
Überprüfen Sie, ob Sie verwenden MISP Version 2.4.137 oder höher.	Die MISP integration for Security Operations Wird mit mindestens getestet MISP Version 2.4.137 an.
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung von erforderlich sind MISP Module sind installiert und aktiviert.	Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen. • Security Incident Response • ServiceNow IntegrationHub Runtime (com.glide.hub.integration.runtime) • ServiceNow IntegrationHub Action Step - REST (com.glide.hub.action_step.rest) Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz für die Integration finden Sie unter Ruft die Berechtigung für ein Security Operations-Produkt ab Oder Anwendung und Aktivieren Sie eine ServiceNow Store-Anwendung .
Domänentrennung	Verifizieren Sie Abschnitt „Domänentrennung“ Wenn Sie Daten, Prozesse und Verwaltungsaufgaben trennen möchten.

MISP Anwenderrollen und Berechtigungen

Überprüfen Sie die Anwenderrollen, die in erforderlich sind MISP integration for Security Operations Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anreicherung erkennbarer Elemente und Sichtungssuchberechtigungen

Hinweis:

- *Alle* **ServiceNow** *MISP-Integrationsfähigkeiten erfordern die grundlegenden Berechtigungen für* **Verwalten Sie Organisationsereignisse** *Und* **Zugriff auf Authentifizierungsschlüssel** *. Stellen Sie sicher, dass Sie über diese grundlegenden Berechtigungen verfügen, bevor Sie fortfahren.*
- *Um lokale Galaxien hinzuzufügen, muss der Anwender, der die Integration konfiguriert, der Host-Organisation des entsprechenden MISP-Servers angehören.*

MISP-Fähigkeit	Tagger	Tag-Editor
Anreicherung erkennbarer Elemente (schreibgeschützt)	#	#
Sichtungssuche (schreibgeschützt)	#	#

Melden Sie Sichtungsberechtigungen

MISP-Fähigkeit	Sichtungsersteller
Sichtung melden	#

Attribut- und Ereignisberechtigungen

MISP-Fähigkeit	Tagger	Tag-Editor
Bearbeiten Sie Ereignis-/Attribut-Tags	#	#
Bearbeiten Sie Ereignis-/Attributgalaxien	#	#
Bearbeiten Sie Attributkommentare	#	#
Fügen Sie dem Ereignis ein neues Attribut hinzu	#	#
Erstellen Sie ein Ereignis in MISP	#	#

Installieren und konfigurieren Sie MISP integration for Security Operations

Installieren und konfigurieren Sie MISP integration for Security Operations Von ServiceNow Store Auf Ihrem ServiceNow AI Platform Instanz, damit Sie mit der Untersuchung von Security Incidents beginnen können MISP Daten.

Vorbereitungen
Stellen Sie sicher, dass Sie die gültigen SSL-Zertifikate auf dem MISP-Server installiert haben.

Erforderliche Rolle: sn_si.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Laden Sie herunter MISP integration for Security Operations Von ServiceNow Store Und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie nach MISP-SIR/TI-Integrationskachel und klicken Sie auf **Konfigurieren** .
4. Füllen Sie im Formular die Felder aus.

MISP – Formular „SIR/TI-Integrationskonfiguration“

Feld	Beschreibung
Name	Name für MISP Instanzkonfiguration.
MISP Server-URL	URL für MISP Server, der als REST-Endpunkt für dient MISP Server.
API-Schlüssel	API-Schlüssel, der für Ihren Anwenderaccount auf konfiguriert ist MISP Server. Der API-Schlüssel entspricht **Authentifizierungsschlüssel** In MISP Server.
Lokale Bereitstellung	Option, die Sie auswählen können, wenn MISP Server wird in einer lokalen Instanz bereitgestellt. Wenn Sie auswählen **Lokale Bereitstellung** Option müssen Sie verwenden MID-Server Um eine Verbindung mit herzustellen MISP Server.
MID-Anwendung	Zeichenfolgenfeld, das den MID-Anwendungsnamen identifiziert, der für die Kommunikation mit verwendet wird MISP. Dieses Feld ist erforderlich, wenn Sie auswählen **Lokale Bereitstellung** Option. Informationen zum Konfigurieren des MID-Servers für Ihre Anwendung finden Sie unter Konfigurieren Sie einen MID-Server für jede Anwendung

5. Klicken Sie auf **Absenden**.

Ergebnisse

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird MISP– SIR/TI-Integration wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Überprüfen Sie MISP Integrationseinstellungen

Überprüfen Sie MISP integration for Security Operations Einstellungen und ändern Sie die Standardsystemeigenschaften entsprechend Ihrer Umgebung.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **MISP-Integration** > **Integrationseinstellungen**an.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MISP-Integrationseinstellungen

Eigenschaftsname		Beschreibung
Ergänzung erkennbarer Elemente	Zeit (in Stunden) vor dem Abrufen neuer Daten	Zeit in Stunden, bevor Sie neue Daten abrufen können. Typ: Ganzzahl Standardwert: 24
Sichtungssuche	Führt automatisch eine Sichtungssuche aus, wenn dem Security Incident neue erkennbare Elemente zugeordnet werden	Sichtungssuche, die immer dann ausgeführt wird, wenn ein neues erkennbares Element einem Security Incident zugeordnet wird. Standardwert: Ja
	Suchintervall (in Tagen) für Sichtungssuche in MISP	Anzahl der Tage, in denen die Sichtungssuchdaten durchsucht werden MISP. Verwenden Sie diese Option nur für die automatische Sichtungssuchfunktion. Standardwert: 90
Datensynchronisierung	Intervallzeitraum (in Minuten) für Tags, die abgerufen und mit MISP synchronisiert werden sollen	MISP Tags, die zum Zeitpunkt der Integrationskonfiguration abgerufen werden. Nachdem sich die Daten in befinden ServiceNow AI Platform, Diese Eigenschaft definiert die Häufigkeit, mit der die Daten mit verwendet werden MISP Server ist synchronisiert. Der Wert wird in Minuten definiert. Standardwert: 1440 (Minuten oder 24 Stunden)
	Intervallzeitraum (in Minuten) zum Aktualisieren von MISP-Galaxien aus konfigurierten Quellen	MISP Galaxien, die zum Zeitpunkt der Integrationskonfiguration abgerufen werden. Nachdem sich die Daten in befinden ServiceNow AI Platform, Diese Eigenschaft definiert die Häufigkeit, mit der die Daten mit verwendet werden MISP Server ist synchronisiert. Der Wert wird in Minuten definiert. Standardwert: 1440 (Minuten oder 24 Stunden)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftsname		Beschreibung
	Intervallzeitraum (in Minuten) für Organisationen, die abgerufen und mit MISP synchronisiert werden sollen	MISP Organisationen, die zum Zeitpunkt der Integrationskonfiguration abgerufen werden. Nachdem sich die Daten in befinden ServiceNow AI Platform, Diese Eigenschaft definiert die Häufigkeit, mit der die Daten mit verwendet werden MISP Server ist synchronisiert. Der Wert wird in Minuten definiert. Standardwert: 1440 (Minuten oder 24 Stunden)
MITRE™ Technikextraktion	Rollup MITRE-ATT&CK Techniken automatisch aus MISP-Erkennbaren Anreicherungsergebnissen (Tags) zu Security Incidents	Rollup von MITRE-ATT&CK Informationen von MISP Ergänzungsergebnisse erkennbarer Elemente (Tags) zum Security Incident. Standardwert: Ja
	Rollup MITRE-ATT&CK Techniken automatisch aus Anreicherungsergebnissen (Galaxien) von MISP erkennbaren Elementen zu Security Incidents	Rollup von MITRE-ATT&CK Informationen aus dem MISP Ergänzungsergebnisse erkennbarer Elemente (Galaxien) zum Security Incident. Standardwert: Ja

Hinweis:

- Zur Verwendung von MITRE™ Extraktionsfunktionen der Technik in MISP, Müssen Sie Aktivieren Sie MITRE-ATT&CK -Funktion in Threat Intelligence Modulan.
- Die MISP integration for Security Operations Führt zwei Basissysteme ein MITRE-ATT&CK Extraktionsregeln für Technik für MISP– MISP Galaxien und MISP Tags. Weitere Informationen zu Regeln für automatische Extraktion finden Sie in MITRE-ATT&CK, Siehe Technische Regeln für den Import von MITRE-ATT&CK-Informationen automatisch extrahieren .

3. Klicken Sie auf **Speichern**.

Ergebnisse

Ihre geänderten Integrationseinstellungen werden gespeichert und angewendet.

Konfigurieren MISP Sichtungssuchen

Konfigurieren Sie ServiceNow AI Platform Um Sichtungssuchen nach erkennbaren Elementen in durchzuführen MISP Instanz. Mit diesen Informationen können Sie bestimmen, wie oft Bedrohungen auftreten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Die für die Verwendung von erforderlich sind MISP bidirektionale Funktionen.
- Erforderliche Rolle: sn_si.admin, sn_ti.admin

Warum und wann dieser Vorgang ausgeführt wird

Die Integration von Security Operations – Sichtungssuche-Workflow Führt die Sichtungssuchen aus. Dieser Workflow akzeptiert eine Liste erkennbarer Elemente, findet alle Implementierungsfähigkeiten, erstellt die Abfragen, die auf den Sichtungssuchkonfigurationen basieren, und führt die Suchen aus, die auf dem konfigurierten Workflow basieren.

Die MISP integration for Security Operations Stellt ein Basissystem-Sichtungssuchprofil bereit, mit dem Sie automatische Sichtungssuchen konfigurieren können. Mit diesem Profil können Sie auf die zugehörigen Sichtungsinformationen erkennbarer Elemente einer Organisation zugreifen und auch die externen Sichtungen aus anderen Organisationen anzeigen.

Prozedur

1. Navigieren zu **Alle** > **MISP-Integration** > **Sichtungssuche: Konfiguration**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „Konfiguration der Sichtungssuche“

Feld	Beschreibung
Name	Name für das Fähigkeitsprofil.
Ist gespeicherte Suche	Suchkonfiguration, die gespeichert wird, wenn Sie diese Option auswählen. Die gespeicherten Suchkonfigurationsabfragen sind Beispielabfragen. Sie können sie durch die Parameter für Ihre Umgebung ersetzen und nach Bedarf zusätzliche gespeicherte Suchkonfigurationen erstellen.
Sichtungssuchquelle	Quelle für die Sichtungssuche. Wählen Sie aus MISP Protokollspeicher als Quelle.
Aktiv	Option, die die gespeicherte Suchkonfiguration aktiviert. Nur aktive Suchkonfigurationen können eine Sichtungssuche durchführen.
Typ des erkennbaren Elements	Typ des erkennbaren Elements, z. B. IP-Adresse, Hash-Wert, URL und Domänenname.
Maximale Anzahl erkennbarer Elemente pro Suche	Maximale Anzahl erkennbarer Elemente, die Sie in einer Suchabfrage anzeigen können.
Suchen	Standardsuchzeichenfolge, d. h. `$(erkennbares Element)` . Sie definieren jedoch Ihre eigene Suchabfrage, indem Sie angeben MISP Unterstützte Parameter des Protokollspeichers.

4. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Sie haben einen erstellt MISP Sichtungssuchkonfigurationsprofil.

Konfigurieren Sie, wie ein automatisches Ereignis erstellt wird

Konfigurieren Sie ServiceNow AI Platform Dient zum automatischen Erstellen von Ereignissen in MISP.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Die für die Verwendung von erforderlich sind MISP bidirektionale Funktionen.
- Erforderliche Rolle: sn_si.admin, sn_ti.admin

Prozedur

1. Navigieren zu **Alle** > **MISP-Integration** > **Profile für die automatische Erstellung von Ereignissen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Namensformular

Feld	Beschreibung
Name	Name des Profils für die automatische Ereigniserstellung.
Beschreibung	Kurze Beschreibung des Profils. Eine detailliertere Beschreibung wird über die Attribute in der nächsten Phase der Erstellung des Ereignisses freigegeben.
Reihenfolge	Reihenfolge des Profils, wenn Auslösebedingungen erfüllt sind. Der Standardwert ist 100. Belassen Sie diese Einstellung auf den Standardwert. Wenn Sie mehrere Profile erstellen, bietet dieser Wert eine Laufzeitausführungspriorität, wenn zwei oder mehr Profile Auslösebedingungen gemeinsam haben. Das Profil mit der niedrigsten Zahl hat die höchste Priorität.
Quelle	MISP Quelle für die Ereigniserstellung.
Aktiv	Option, die angibt, ob das Profil aktiv oder inaktiv ist. Die Option ist standardmäßig deaktiviert, um anzuzeigen, dass das Profil deaktiviert ist. Dieses Profil ist erst aktiv, wenn Sie alle Konfigurationsschritte des Profils abgeschlossen und auf klicken **Beenden** .

4. Klicken Sie auf **Fortsetzen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie Ereignisauslöserbedingungen

Konfigurieren Sie die Ereignisauslöserbedingungen in ServiceNow AI Platform Damit Sie ein Ereignis in automatisch auslösen können MISP Wenn die Bedingungen erfüllt sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Geben Sie im Formular „Auslöserbedingungen“ die Details ein, die ein Ereignis auslösen können.
   Sie können eine zusammengesetzte Logik erstellen, indem Sie die Auslöserbedingungen bereitstellen, die auf Security Incident-Feldern oder Feldern erkennbarer Elemente basieren. Sie können Ereignisse auch in erstellen MISP Wenn erkennbare Elemente kein entsprechendes Ereignis in haben MISP. Sie können eine zusammengesetzte Logik erstellen, indem Sie eine Kombination der drei Auslöserbedingungen verwenden: Auslöser basierend auf Security Incident-Feldern, Auslöser basierend auf erkennbaren Feldern und MISP-Ereignis erstellen, wenn ein erkennbares Element keine entsprechenden Ereignisse in MISP hat. Wenn Sie mehrere Auslöser auswählen, können Sie sie mit der Bedingung UND verbinden. Erwägen Sie, ein Profil mit neuen Bedingungen zu erstellen, wenn Sie die ODER-Bedingung verwenden müssen.

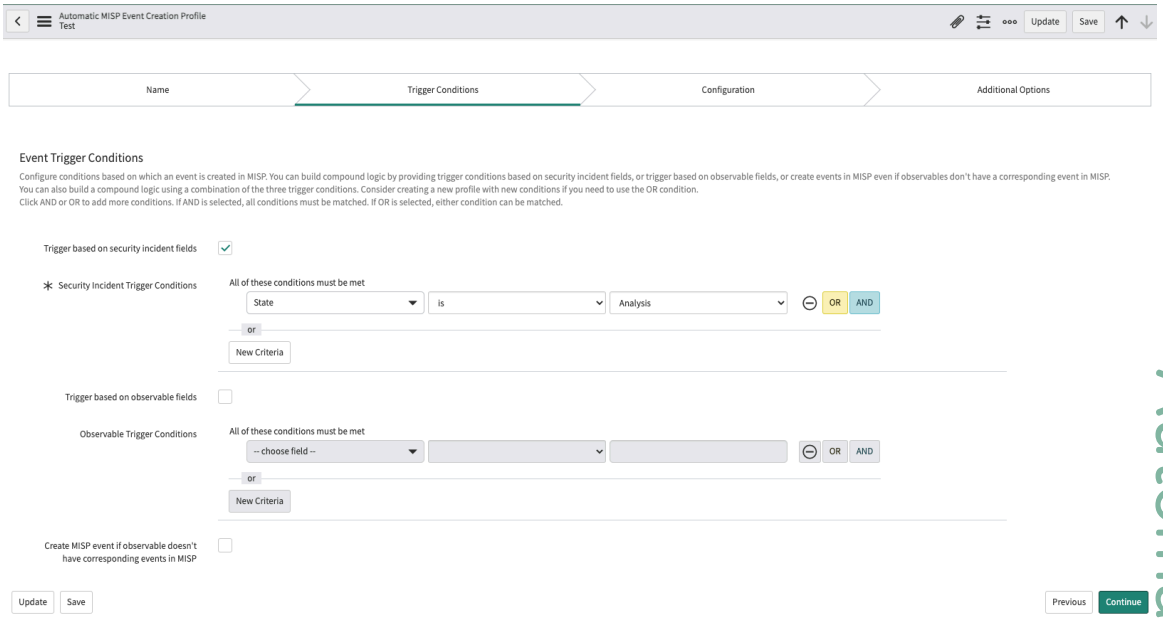
Formular „Ereignisauslöserbedingungen“

Feld	Beschreibung
Auslöser basierend auf Security Incident-Feldern	MISP Ereignis, das Sie erstellen können, wenn alle Auslöserbedingungen für Security Incidents erfüllt sind.
Auslösebedingungen für Security Incident	Filter in der ersten Zeile, die Sie mithilfe der Listen und Felder des Bedingungsgenerators festlegen können. Um weitere Bedingungen hinzuzufügen, klicken Sie auf UND oder oder . Wenn UND ausgewählt ist, müssen alle Bedingungen erfüllt werden. Wenn ODER ausgewählt ist, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien** .
Auslöser basierend auf erkennbaren Feldern	MISP Ereignis, das Sie erstellen können, wenn alle Auslöserbedingungen für erkennbare Elemente erfüllt sind.
Auslösebedingungen für erkennbare Elemente	Filter in der ersten Zeile, die Sie mithilfe der Listen und Felder des Bedingungsgenerators festlegen können. Um weitere Bedingungen hinzuzufügen, klicken Sie auf UND oder oder . Wenn UND ausgewählt ist, müssen alle Bedingungen erfüllt werden. Wenn ODER ausgewählt ist, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien** .
Erstellen Sie ein MISP-Ereignis, wenn das erkennbare Element keine entsprechenden Ereignisse in MISP enthält.	MISP Ereignis, das Sie erstellen können, wenn ein erkennbares Element keine entsprechenden Ereignisse in hat MISP.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignisauslöserbedingungen

Das folgende Beispiel zeigt die Ereignisauslöserbedingungen beim Einrichten von MISP Ereigniserstellungsprofil.



2. Klicken Sie auf **Fortsetzen**.

Ordnen Sie zu MISP Ereignisfelder

Ordnen Sie zu MISP Ereignisfelder in ServiceNow AI Platform Damit Security Incident-Informationen wann verfügbar sind MISP Ereignisse werden erstellt.

Vorbereitungen

Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Füllen Sie im Formular die Felder aus.

Standardmäßiges MISP-Ereignisfeldzuordnungsformular

Feld	Beschreibung
Information zum Ereignis	Ereignisinformationen, die automatisch aus erstellt werden ServiceNow AI Platform Security Incident Response. Die **Ereignisinformationen** Das Feld unterstützt Ersetzungsvariablen durch Verwendung von ${SIR FIELD LABEL}$. Während der Ereigniserstellung werden diese Variablen durch die tatsächlichen Feldwerte für Security Incidents ersetzt. Die Ersetzungsvariable ${URL}$ wird durch die URL des Security Incident ersetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

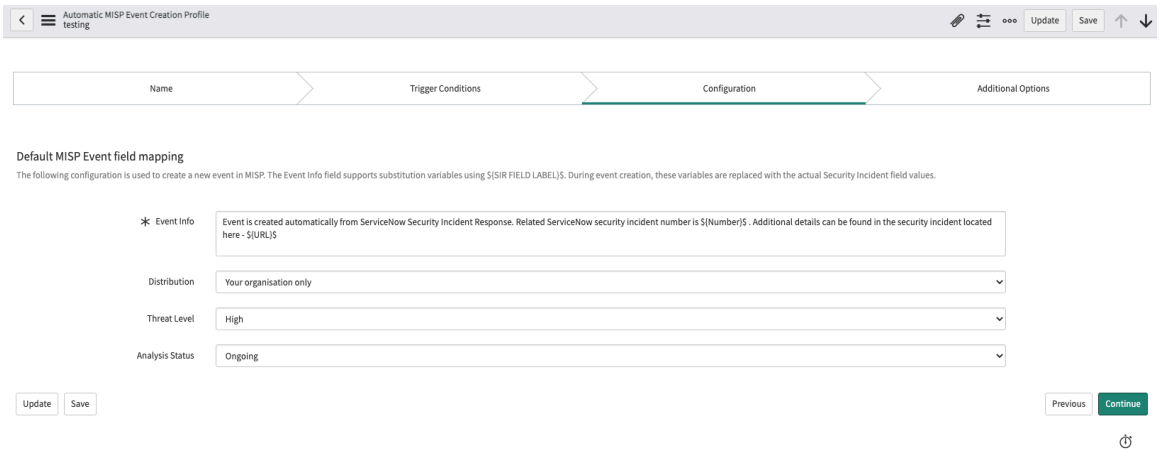
Feld	Beschreibung
Verteilung	Option, die steuert, wer dieses Ereignis nach der Veröffentlichung des Ereignisses anzeigen kann. Diese Option steuert auch, ob das Ereignis mit anderen Servern synchronisiert wird. Die Verteilung wird von den Attributen übernommen, und die restriktivste Einstellung gewinnt. Die Verteilungsoptionen lauten wie folgt: ○ Nur Ihre Organisation: Ermöglicht nur Mitgliedern Ihrer Organisation, dieses Ereignis anzuzeigen. Das Ereignis kann von einem Ihrer Organisationsmitglieder in eine andere Instanz abgerufen werden, wo nur Ihre Organisation Zugriff zum Anzeigen hat. Ereignisse mit dieser Einstellung werden nicht synchronisiert. ○ Nur diese Community: Aktiviert Anwender, die Teil Ihres sind MISP community zum Anzeigen des Ereignisses, einschließlich Ihrer eigenen Organisation, Organisationen zu diesem MISP Server und Organisationen, die ausgeführt werden MISP Server, die mit diesem Server synchronisiert werden. Alle anderen Organisationen, die eine Verbindung zu Ihren verknüpften Servern herstellen, dürfen das Ereignis nicht anzeigen. ○ Verbundene Communities: Ermöglicht Anwendern, die Teil Ihres sind MISP community, um das Ereignis einschließlich aller Organisationen anzuzeigen MISP Server, alle Organisationen auf dem MISP Server, die mit diesem Server synchronisiert werden, und die Hosting-Organisationen von Servern, die eine Verbindung zu einem Server herstellen, der zwei Hops entfernt ist. Alle anderen Organisationen, die mit den verknüpften Servern verbunden sind, die zwei Hops entfernt sind, können das Ereignis nicht anzeigen. ○ Alle Communities: Teilt das Ereignis mit allen MISP communities.
Bedrohungsstufe	Feld, das das Risikostufe des Ereignisses angibt. Sie können Incidents in drei verschiedene Bedrohungskategorien (niedrig, Mittel, hoch) kategorisieren. Dieses Feld kann auch als nicht definiert belassen werden. Die folgenden Optionen sind verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Niedrig: Allgemeine Massen-Malware ○ Mittel: Advanced Persistent Threats (APT) ○ Hoch: Ausgeklügelte APTs und 0-Tage-Angriffe
Analysestatus	Aktuelle Phase der Analyse für das Ereignis mit den folgenden möglichen Optionen: ○ Anfänglich: Die Analyse beginnt gerade erst ○ Laufend: Die Analyse wird ausgeführt ○ Abgeschlossen: Die Analyse ist abgeschlossen

Das folgende Beispiel zeigt das Formular, mit dem Sie ein Ereignis in MISP erstellen können.

Standardmäßige MISP-Ereignisfeldzuordnung



2. Klicken Sie auf **Fortsetzen**.

Zuordnen oder zuordnen SIR Erkennbare Elemente als Attribute für MISP Ereignisse

Ordnen Sie zu Security Incident Response Typen erkennbarer Elemente für MISP Attributtypen aufgrund von MISP Attributtypen und SIR Erkennbare Elemente können unterschiedlich sein.

Vorbereitungen

Erforderliche Rolle: sn_sec_misp.write

Warum und wann dieser Vorgang ausgeführt wird

Die MISP integration for Security Operations Stellt eine Basissystemzuordnung bereit, die Sie beim Hinzufügen verwenden SIR Erkennbare Elemente als Attribute für einen MISP Ereignis.

Sie können die Basissystemzuordnung an Ihre Umgebung anpassen. Sie können beispielsweise mehrere zuordnen SIR Erkennbare Elemente für nur eines MISP Attributtyp. Wenn erkennbare Typen nicht zugeordnet sind, wird **Sonstiges** MISP Der Attributtyp ist standardmäßig ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

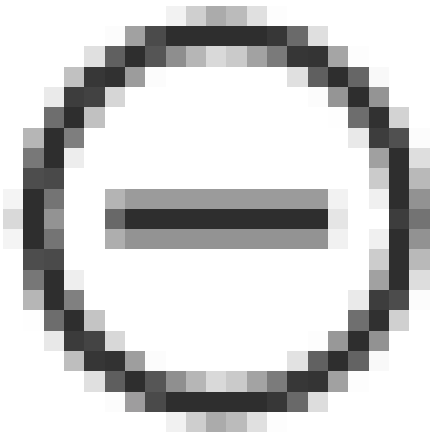
Prozedur

1. Ordnen Sie im Formular „zusätzliche Optionen“ zu SIR Erkennbares Element und MISP Attributtypen.
2. Ordnen Sie zu Security Incident Response Typen erkennbarer Elemente für MISP Attributtypen wie in der folgenden Tabelle beschrieben.

Zuordnung von erkennbarem SIR- und MISP-Attributtyp

Feld	Beschreibung
Alle zugehörigen erkennbaren Elemente als Attribute hinzufügen	Option, die Sie aktivieren, um verfügbare erkennbare Elemente in einem Security Incident zu einem hinzuzufügen MISP Ereignis als Attribute. Diese Option aktiviert die Zuordnung im Abschnitt „Zuordnung erkennbarer Elemente vom Typ zu Attributtyp“.
Zuordnung Von Typ Des Erkennbaren Elements Zu Attributtyp	Option zum Zuordnen von SIR Typen erkennbarer Elemente für MISP Attributtypen. Sie können beispielsweise die CVE-Nummer in zuordnen SIR Zum Schwachstellenattribut in MISP. Sie können hinzufügen SIR Erkennbarer Typ auf nur einen MISP Attributtyp. Das -Basissystem stellt eine Zuordnung von bereit SIR Typen erkennbarer Elemente für MISP Attributtypen. Falls vorhanden SIR Typen erkennbarer Elemente sind keinem zugeordnet MISP Attributtyp, dann wird das erkennbare Element dem zugeordnet **Sonstiges** Attributtyp in MISP. Um eine neue Zuordnung hinzuzufügen, klicken Sie auf **Fügen Sie Den Typ Des Erkennbaren Elements Hinzu** , Suchen Sie nach SIR Typ des erkennbaren Elements und ordnen Sie dann dem entsprechenden zu MISP Attributtyp. Klicken Sie auf das Symbol Zuordnung entfernen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

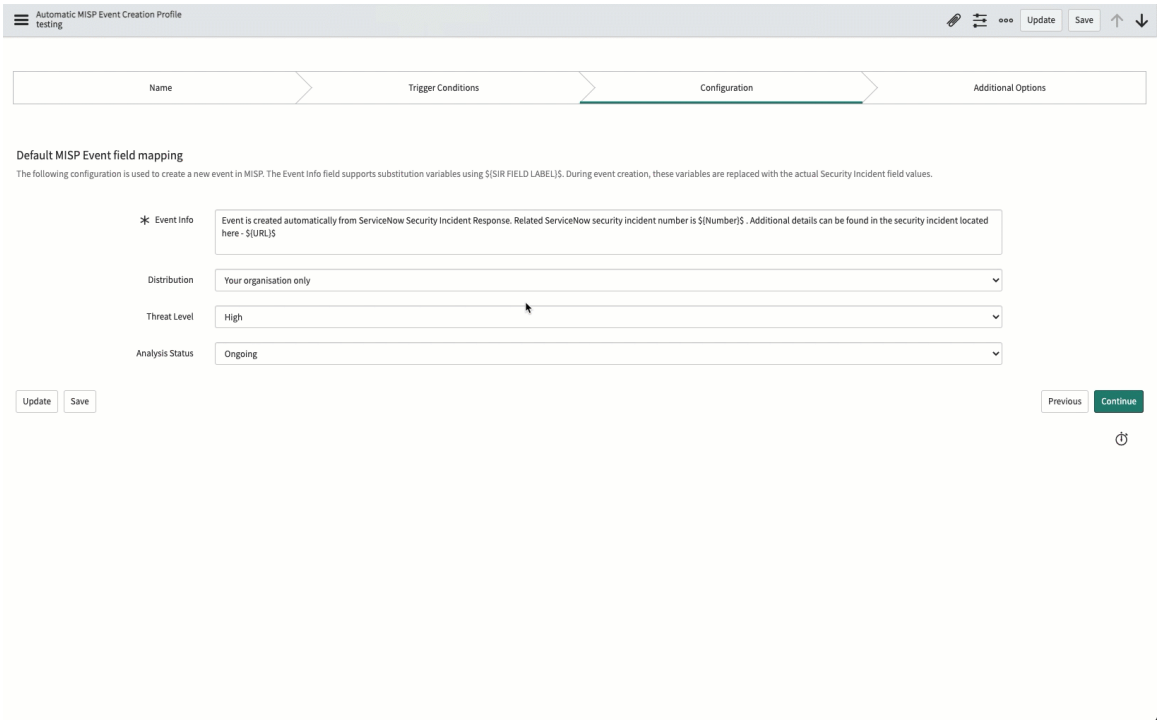
Feld	Beschreibung
	 Um zu entfernen SIR Und MISP Attributzuordnungszuordnung. **Hinweis:** Weitere Informationen zu finden MISP Attributtypen, siehe MISP-Dokumentation .
Erkennbare Elemente anhand von Sicherheits-Tags filtern	Option zum Filtern der erkennbaren Elemente basierend auf den ausgewählten Sicherheits-Tags. **Sicherheits-Tags** : Fügen Sie Tags hinzu, um die erkennbaren Elemente zu filtern. Wenn Sie beispielsweise ein Tag mit der Bezeichnung „von Freigabe blockieren“ oder „TLP: Weiß“ hinzufügen, werden diese erkennbaren Elemente während der Erstellung des MISP-Ereignisses nicht als Attribut zum MISP-Ereignis hinzugefügt, wenn einem der erkennbaren Elemente eines dieser Tags zugeordnet ist.
Legen Sie die Attribut-IDS-Kennzeichnung fest, wenn die Erkennung von erkennbaren Elementen schädlich ist.	Option, mit der Sie wissen, ob ein erkennbares Element in als schädlich markiert ist SIR, Dann das entsprechende Attribut in MISP Hat die IDS-Kennzeichnung aktiviert. Wenn die IDS-Kennzeichnung nicht festgelegt ist, wird das Attribut als kontextbezogene Informationen betrachtet und nicht für die automatische Erkennung von Angriffen verwendet.

Das folgende Beispiel zeigt, wie Sie zur Seite „zusätzliche Optionen“ navigieren. Auf dieser Seite können Sie die Zuordnung der SIR-erkennbaren Elemente und MISP-Attributtypen aktivieren und neu hinzufügen SIR Typen erkennbarer Elemente, z. B. IPV6-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerk und IPV4-Netzwerk, und ordnen Sie es dem zu MISP Attributtyp-IP-Adresse der Domäne.

Zuordnung SIR Erkennbare Elemente und MISP Attributtypen



Synchronisieren MITRE-ATT&CK Informationen zu MISP Ereignisse

Synchronisieren Sie MITRE-ATT&CK Informationen mit MISP Attribute für eine bessere Security Incident- und Bedrohungsanalyse.

Vorbereitungen

Erforderliche Rolle: sn_sec_misp.write

Prozedur

Überprüfen Sie im Formular „zusätzliche Optionen“ die Optionen zum Synchronisieren von MITRE-ATT&CK Informationen mit MISP Attribute.

Formular „Erweiterte Optionen“

Feld	Beschreibung
Security Incident Synchronisieren MITRE-ATT&CK™ Techniken als lokale Galaxien bis MISP Ereignis	Option zum Synchronisieren von ServiceNow AI Platform SIR Security Incident MITRE-ATT&CK™ Techniken als lokale Galaxien in MISP Ereignis. **Hinweis:** Um lokale Galaxien hinzuzufügen, muss der Anwender, der die Integration konfiguriert hat, der Host-Organisation des entsprechenden angehören MISP Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Security Incident Synchronisieren MITRE-ATT&CK™ Techniken als globale Galaxien bis MISP Ereignis	Option zum Synchronisieren von ServiceNow AI Platform SIR Security Incident MITRE-ATT&CK™ Techniken als globale Galaxien in MISP Ereignis.

Ergebnisse
Sie haben ein Profil erstellt, mit dem Sie Ereignisse in automatisch erstellen können MISP Von ServiceNow AI Platform. Sie können die Ereignisse jetzt in der zugehörigen Liste zugeordnete MISP-Ereignisse anzeigen.

Fügen Sie MISP-Tags zu Ereignissen hinzu

Fügen Sie den erstellten MISP-Ereignissen MISP-Tags hinzu.

Vorbereitungen
Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Navigieren Sie im Formular „zusätzliche Optionen“ zu **Wählen Sie MISP-Tags aus, die dem Ereignis hinzugefügt werden sollen** Abschnitt in der Formularansicht.
2. Überprüfen Sie die Optionen zum Hinzufügen von Tags zu den erstellten Ereignissen.

Formular „Erweiterte Optionen“

Feld	Beschreibung
Erstelltem MISP-Ereignis Tags hinzufügen	Option, mit der Sie automatisch MISP-Tags zu Ereignissen hinzufügen können, die in ServiceNow erstellt werden.
Tags (lokal)	Die ausgewählten Tags werden dem MISP-Ereignis als lokale Tags hinzugefügt.
Tags (global)	Die ausgewählten Tags werden dem MISP-Ereignis als globale Tags hinzugefügt.

3. Klicken Sie auf **Speichern**.

Ergebnisse
Das Hinzufügen von MISP-Tags hilft bei der Klassifizierung des Ereignisses.

MISP Ereignisdaten

Sie können überprüfen MISP Ereignisdaten, damit Sie detaillierte Informationen zum anzeigen können MISP Ereignisse.

MISP Ereignisdaten in der Listenansicht

Greifen Sie über auf die Listenansicht zu **MISP** > **MISP-Ereignis-Daten**an.

Verwenden Sie die Listenansicht, um einen schnellen Überblick über zu erhalten MISP Ereignisdaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Listenansicht „MISP-Ereignisse“

Feld	Beschreibung
Ereignis-ID	Ereignis-ID, die von zugewiesen wird MISP Wann das Ereignis zum ersten Mal erstellt oder in importiert wurde MISP Server.
Info	Kurzbeschreibung des Ereignisses.
Analyse	Aktuelle Phase der Analyse für das Ereignis mit den folgenden möglichen Optionen: • Anfänglich: Die Analyse beginnt gerade erst • Laufend: Die Analyse wird ausgeführt • Abgeschlossen: Die Analyse ist abgeschlossen
Bedrohungsstufe	Risikostufe des Ereignisses. Incidents können in drei verschiedene Bedrohungskategorien (niedrig, Mittel, hoch) kategorisiert werden. Dieses Feld kann als nicht definiert belassen werden. Die folgenden Optionen sind verfügbar: • Niedrig: Allgemeine Massen-Malware • Mittel: Advanced Persistent Threats (APT) • Hoch: Ausgeklügelte APTs und 0-Tage-Angriffe
MISP-Tags	Tags, die dem zugeordnet sind MISP Ereignis.
MISP-Galaxien	Galaxien, die mit verknüpft sind MISP Ereignis.
Besitzerorganisation	Organisation, die das Ereignis auf der besitzt MISP Instanz. Dieses Feld ist nur für Administratoren sichtbar.
Organisation des Erstellers	Organisation, die das Ereignis in erstellt hat MISP Instanz.
Verteilung	Verteilung des einzelnen Attributs. Ein Attribut kann eine andere Verteilungsebene haben als das Ereignis.
MISP-Ereignis-Hyperlink	Link zu MISP Ereignis, das auf gespeichert ist MISP Server.
MISP-Quelle	MISP Quelle, in der das Ereignis erstellt wird.

MISP Ereignisdaten in der Formularansicht

Verwenden Sie die Formularansicht, um detaillierte Informationen zu zu erhalten MISP Ereignisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularansicht „MISP-Ereignis“

Feld	Beschreibung
Ereignis-ID	Ereignis-ID, die von zugewiesen wird MISP Wann das Ereignis zum ersten Mal erstellt oder in importiert wurde MISP Server.
UUID	ID, die Ereignisse und Attribute eindeutig identifiziert.
Organisation des Erstellers	Organisation, die das Ereignis in erstellt hat MISP Instanz.
Besitzerorganisation	Organisation, die das Ereignis auf der besitzt MISP Instanz. Dieses Feld ist nur für Administratoren sichtbar.
Erstelleranwender	Anwender, der das Ereignis in erstellt hat MISP.
Letzter Change	Datum, an dem das Ereignis zuletzt geändert wurde.
MISP-Quelle	MISP Quelle, in der das Ereignis erstellt wird.
Erstellungsdatum (in MISP)	Datum, an dem das Ereignis erstellt oder erstmals in importiert wurde MISP Server.
Bedrohungsstufe	Risikostufe des Ereignisses. Incidents können in drei verschiedene Bedrohungskategorien (niedrig, Mittel, hoch) kategorisiert werden. Dieses Feld kann als nicht definiert belassen werden. Die folgenden Optionen sind verfügbar: • Niedrig: Allgemeine Massen-Malware • Mittel: Advanced Persistent Threats (APT) • Hoch: Ausgeklügelte APTs und 0-Tage-Angriffe
Analyse	Aktuelle Phase der Analyse für das Ereignis mit den folgenden möglichen Optionen: • Anfänglich: Die Analyse beginnt gerade erst • Laufend: Die Analyse wird ausgeführt • Abgeschlossen: Die Analyse ist abgeschlossen
Verteilung	Verteilung des einzelnen Attributs. Ein Attribut kann eine andere Verteilungsebene haben als das Ereignis.
Veröffentlicht	Status, der angibt, ob das Ereignis veröffentlicht wurde oder nicht. Durch die Veröffentlichung können die Attribute des Ereignisses für alle berechtigten Exporte verwendet werden, und Anwender, die die Ereigniswarnungen abonniert haben, werden benachrichtigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularansicht „MISP-Ereignis“ (Fortsetzung)

Feld	Beschreibung
MISP-Ereignis-Hyperlink	Link zu MISP Ereignis, das auf gespeichert ist MISP Server.
Info	Kurzbeschreibung des Ereignisses.
Tags (lokal)	Tags, die in der Host-Organisation verfügbar sind MISP Instanz zum Aktivieren von Tagging für Synchronisierung und Exportfilterung. MISP Ereignisse werden nicht geändert, wenn Sie lokale Tags verwenden. Lokale Tags werden immer entfernt, bevor sie mit anderen synchronisiert werden MISP Instanzen und freigegebene Communities.
Tags (global)	Tags, die global verfügbar sind, um sie mit anderen freizugeben und zu synchronisieren MISP Instanzen und freigegebene Communities. Wenn Sie globale Tags zu hinzufügen MISP Instanzen können Sie Ereignisse ändern.
Galaxien (lokal)	Galaxien, die in der Host-Organisation verfügbar sind MISP Instanz für Synchronisierung und Exportfilterung. MISP Ereignisse werden nicht geändert, wenn Sie lokale Galaxien verwenden. Diese lokalen Galaxien werden immer entfernt, bevor sie mit anderen synchronisiert werden MISP Instanzen und freigegebene Communities.
Galaxien (global)	Galaxien, die global verfügbar sind, um mit anderen geteilt und synchronisiert zu werden MISP Instanzen und freigegebene Communities. Wenn Sie globale Galaxien hinzufügen, MISP Sie können Ereignisse ändern.

Zugeordnet MISP Ereignisse

Sie können die zugeordnete verwenden MISP Ereignislistenansicht zum Anzeigen der Ereignisse, die manuell oder automatisch im Kontext eines Security Incidents erstellt wurden.

Zugeordnete MISP-Ereignisse

Feld	Beschreibung
Security Incident	SIR Security Incident. Klicken Sie auf den Security Incident, um den Security Incident anzuzeigen.
MISP-Ereignis	MISP Ereignis-ID. Klicken Sie auf MISP Ereignis zum Anzeigen von MISP Ereignis in ServiceNow AI Platform.
MISP-Quelle	MISP Quelle, in der das Ereignis erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugeordnete MISP-Ereignisse (Fortsetzung)

Feld	Beschreibung
	Klicken Sie auf MISP Quelle zum Anzeigen der Quelle.
Ereigniserstellungsmodus	Status, der angibt, ob das Ereignis manuell oder automatisch mit dem Ereigniserstellungsprofil erstellt wurde. Klicken Sie auf MISP Ereignis zum Anzeigen der zugehörigen MISP Ereignis.
Profil für die automatische Erstellung von Ereignissen	Ereigniserstellungsprofil, das zum Erstellen des automatischen Ereignisses verwendet wird. Klicken Sie auf das Profil, um das Profil für die automatische MISP-Ereigniserstellung anzuzeigen.

MISP Anwenderinformationen

Sie können verwenden MISP Anwenderinformationsseite zum Anzeigen aller zugeordneten Anwender für ServiceNow AI Platform MISP integration for Security Operations.

MISP-Anwenderinformationen

Feld	Beschreibung
Quelle	Anwenderaccounts MISP Quelle.
Anwender-ID	Anwender-ID, die von zugewiesen wird MISP Server, wenn ein Anwenderaccount erstellt wird.
Anwender-E-Mail	E-Mail-Adresse eines Anwenders. Nur Organisationsadministratoren können die E-Mail-Adressen der Anwender ihrer eigenen Organisation anzeigen.
Organisation	Organisation, der ein Anwender angehört.
Rollenname	Rollenname, der die Anwenderberechtigungen definiert, die einem Anwender zugeordnet sind. Für weitere Informationen zu Rollen in MISP, Siehe MISP-Dokumentation .
Rollen-ID	Anwenderrollen-ID in MISP. Zum Beispiel Perm-Administrator, Perm-Audit oder Perm-Tagger usw.
Berechtigung	Berechtigungen, die ein Anwender hat. In MISP sind folgende Berechtigungen verfügbar: • Schreibgeschützt • Eigene Ereignisse verwalten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MISP-Anwenderinformationen (Fortsetzung)

Feld	Beschreibung
	• Verwalten Sie Organisationsereignisse • Verwalten Sie Ereignisse Der Veröffentlichungsorganisation
Sichtungsberechtigung	Berechtigung, mit der ein Anwender Sichtungssuchen durchführen kann.
Tagger-Berechtigung	Berechtigung, mit der ein Anwender Tagging durchführen kann.

Domain Separation und MISP

Die Domänentrennung wird in MISP unterstützt. Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Supportstufe

Support: Standard.

Funktionsweise der Domänentrennung MISP

Führen Sie die folgenden Schritte aus, um die Domänentrennung zu erreichen:

- Erstellen Sie einen Anwender mit Erforderliche Rollen In Ihrer Domäne.
- Führen Sie aus MISP integration for Security Operations Verfahren in Ihrer Domäne.

Fehlerbehebung bei der MISP-Integration

Dieser Abschnitt enthält wichtige Tipps zur Fehlerbehebung, die Ihnen helfen können, häufige Probleme zu lösen, die beim Einrichten oder Ausführen der MISP-Integration auftreten können.

SSL-Probleme

Stellen Sie bei der Verbindung über die MISP-Integration sicher, dass Sie ein gültiges CA-Zertifikat auf dem MISP-Server installiert haben, das noch nicht abgelaufen ist. Sie können RSA- oder eigene Zertifikate in die Plattform importieren und sicherstellen, dass der allgemeine Name des Zertifikats mit dem Hostnamen übereinstimmt. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie MISP integration for Security Operations und MISP Anwenderrollen und Berechtigungen.

Verwenden MISP Dient zur Untersuchung und Analyse von Bedrohungen

Sie können verwenden MISP Daten im gesamten ServiceNow AI Platform Threat Intelligence Modul und ServiceNow AI Platform SIR Modul zum Untersuchen und Analysieren von Bedrohungen für Ihre Organisation.

Sichtungssuchen in MISP

Sie können Sichtungssuchen für erkennbare Elemente in durchführen MISP Instanz, um zu bestimmen, wie oft bestimmte Arten von Angriffen, z. B. Phishing-Angriffe oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kommunikation mit einer schädlichen IP oder URL, in Ihrem Netzwerk auftreten. Jedes Vorkommen wird als Sichtung betrachtet.

Sichtungen in MISP

Sichtungen geben an, dass ein Indikator, Objekt oder Attribut gesehen wurde und seine Gültigkeit bestätigt wurde. Sichtungen in MISP Ist ein System, mit dem Sie auf Attribute für ein Ereignis reagieren können. Es wurde entwickelt, um Anwendern eine einfache Methode zu bieten, um zu bestätigen, dass sie ein bestimmtes Attribut gesehen haben, was ihnen mehr Glaubwürdigkeit verleiht. Sie können ein Attribut mehrmals anzeigen.

Hinweis:
Erkennbare Elemente werden in MISP als Attribute bezeichnet.

Einige Attribute werden als falsch positive Werte betrachtet, was bedeutet, dass sie keine gültigen Sichtungen sind. Andere Attribute sind nur für eine bestimmte Dauer gültig, z. B. eine Phishing-Kampagne, die nur eine Woche lang ausgeführt wird. Sie können den Attributen, die für eine bestimmte Dauer gültig sind, ein Ablaufdatum zuweisen, aber jede Organisation kann einem Attribut nur ein gültiges Ablaufdatum zuweisen.

Sichtungen, die in erstellt werden MISP Anwender von Organisationen, die auf dem entsprechenden MISP-Server als lokal markiert sind, werden als interne Sichtungen bezeichnet. Sichtungen, die in erstellt werden MISP Von Anwendern von Organisationen, die in der entsprechenden als Remote markiert sind MISP Server werden als externe Sichtungen bezeichnet.

Sichtungssuchen in SIR

Die Integration von Security Operations – Sichtungssuche-Workflow Führt die Sichtungssuche aus. Dies Der Flow akzeptiert eine Liste erkennbarer Elemente, sucht nach Implementierungsfähigkeiten, erstellt die Abfragen, die auf den Sichtungssuchkonfigurationen basieren, und führt die Suchen aus, die auf der konfigurierten basieren Flow.

Sichtungssuchen helfen Analysten, die Verbreitung einer Bedrohung im Zeitverlauf zu bestimmen. Sie können einzelne oder mehrere erkennbare Elemente und den Datumsbereich für Ihre Suche aus einem Security Incident auswählen. Ergebnisse sind im Security Incident enthalten Sichtungen , Sichtungssuchergebnisse , Und Sichtungssuchdetails Zugehörige Listen.

Wenn Sie mit der Analyse eines Incident beginnen, können Sie einrichten ServiceNow AI Platform Bis Führt automatisch eine Sichtungssuche durch Oder Führen Sie manuell eine Sichtungssuche für erkennbare Elemente durch Um andere Anwender in Ihrer Organisation zu identifizieren, die von demselben Phishing-Angriff betroffen sind.

Automatische Sichtungssuchen in aktivieren MISP

Aktivieren Sie die Sichtungssuche in MISP Wird automatisch ausgeführt, damit der Workflow „Security Operations Integration – Sichtungssuche“ ausgelöst wird, wenn neue erkennbare Elemente einem Security Incident zugeordnet werden.

Vorbereitungen
Überprüfen Sie, ob Sichtungssuchkonfigurationsprofil für MISP Ist aktiv.

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie aktivieren Die Sichtungssuchfunktion, die automatisch in ausgeführt werden soll MISP Integrationskonfiguration, Die Sichtungssuche in MISP Wird ausgelöst, wenn neue erkennbare Elemente einem

Automatische Übersetzung

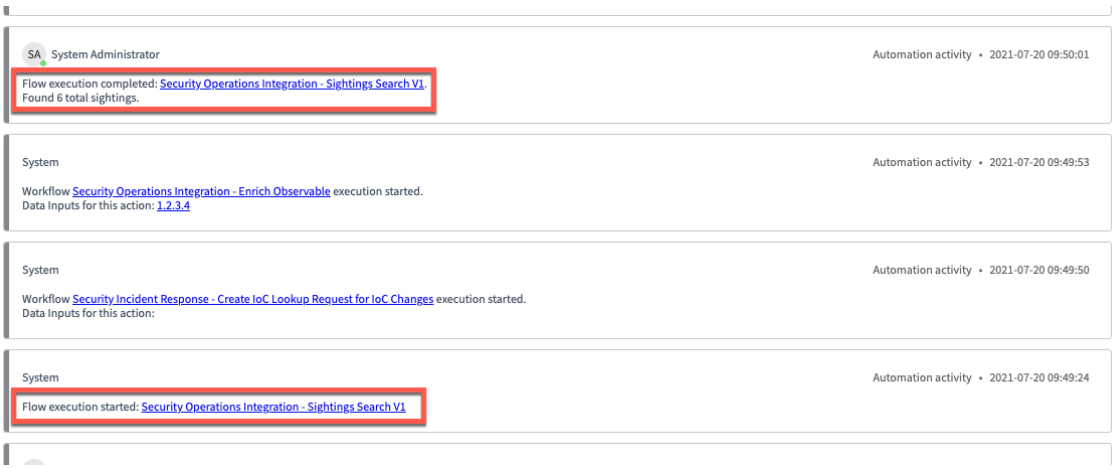
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Incident zugeordnet werden. Standardmäßig ist **Sichtungssuche automatisch ausführen, wenn dem Security Incident neue erkennbare Elemente zugeordnet sind** Option ist aktiviert.

Prozedur

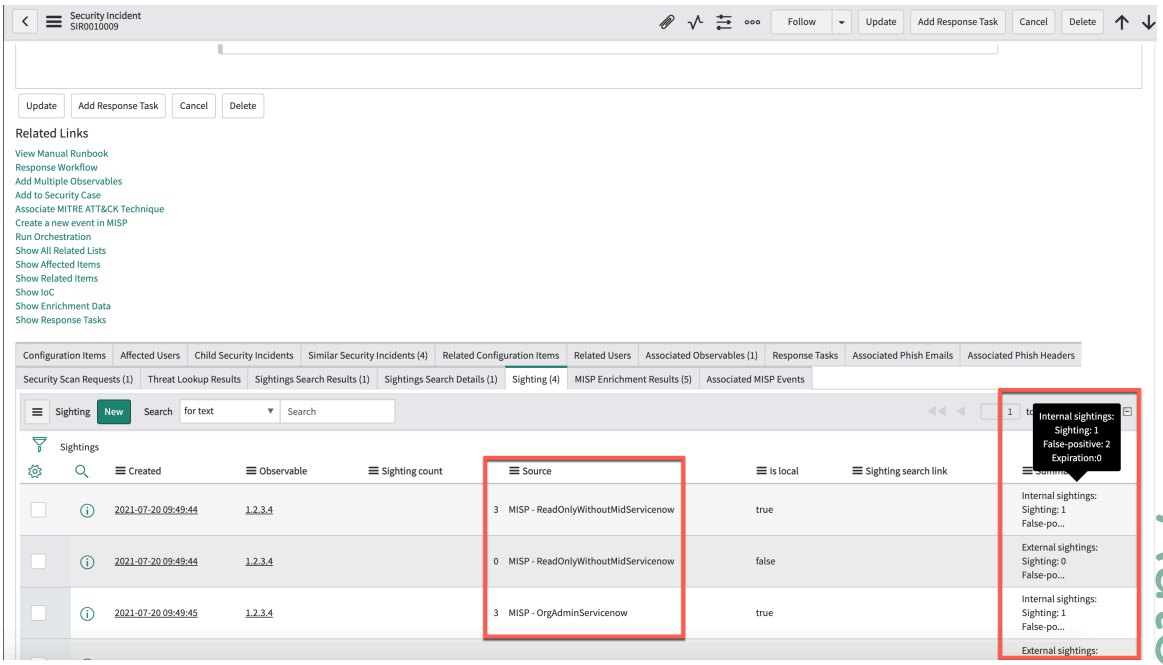
1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, die Sie in anzeigen möchten MISP Sichtungssuchdaten.
3. Überprüfen Sie die Arbeitsnotizen, nachdem dem Security Incident neue erkennbare Elemente zugeordnet wurden.
   Eine Arbeitsnotiz wird veröffentlicht, wenn Integration von Security Operations – Sichtungssuche-Workflow Wurde ausgelöst.

   Das folgende Beispiel zeigt den Abschnitt „Arbeitsnotizen“.



4. Zeigen Sie die zusammengefassten Informationen von erkennbaren Elementen an, die in allen Ereignissen (global) angezeigt und nach ihren internen oder externen Sichtungen kategorisiert werden, nachdem die Workflow-Ausführung abgeschlossen wurde.
   Zeigen Sie die Informationen in an Sichtungen , Sichtungssuchergebnisse Und Sichtungssuchdetails Zugehörige Listen.das folgende Beispiel zeigt den Sichtungssuchdatensatz, der in der zugehörigen Liste Sichtungen erstellt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sichtungssuchdatensatz

Feld	Beschreibung
Erstellt	Datum und Uhrzeit der Erstellung des Sichtungssuchdatensatzes.
Erkennbares Element	Erkennbares Element, das von der Abfrage gesucht wird.
Sichtungsanzahl	Anzahl der internen und externen Sichtungen.
Quelle	Quelle des erkennbaren Elements. Wenn das erkennbare Element aus einem stammt MISP Organisation, dem Datensatz sind die Wörter vorangestellt MISP .
Ist lokal	Status, der angibt, ob die Sichtung von einem internen Anwender gemeldet wurde.
Sichtungssuchlink	Sichtungssuchlink in MISP Instanz.
Zusammenfassung	Typ der Sichtungen, die dem Datensatz zugeordnet sind. Die drei Arten von Sichtungen sind Sichtungen, falsch-positiv und Ablauf. Die Spalte Zusammenfassung wird nur angezeigt, wenn MISP integration for Security Operations Ist installiert. Wenn-Quellen andere als MISP Wird angezeigt, ist der Spalteneintrag „Zusammenfassung“ für diesen Datensatz leer.

Führen Sie eine manuelle Sichtungssuche in durch MISP

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Sichtungssuche in durch ServiceNow AI Platform MISP integration for Security Operations Anwendung zur Bestimmung der Verbreitung einer Bedrohung im Zeitverlauf.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Zur Verwendung von MISP bidirektionale Funktionen.
- Erforderliche Rolle: sn_si.Analyst

Prozedur

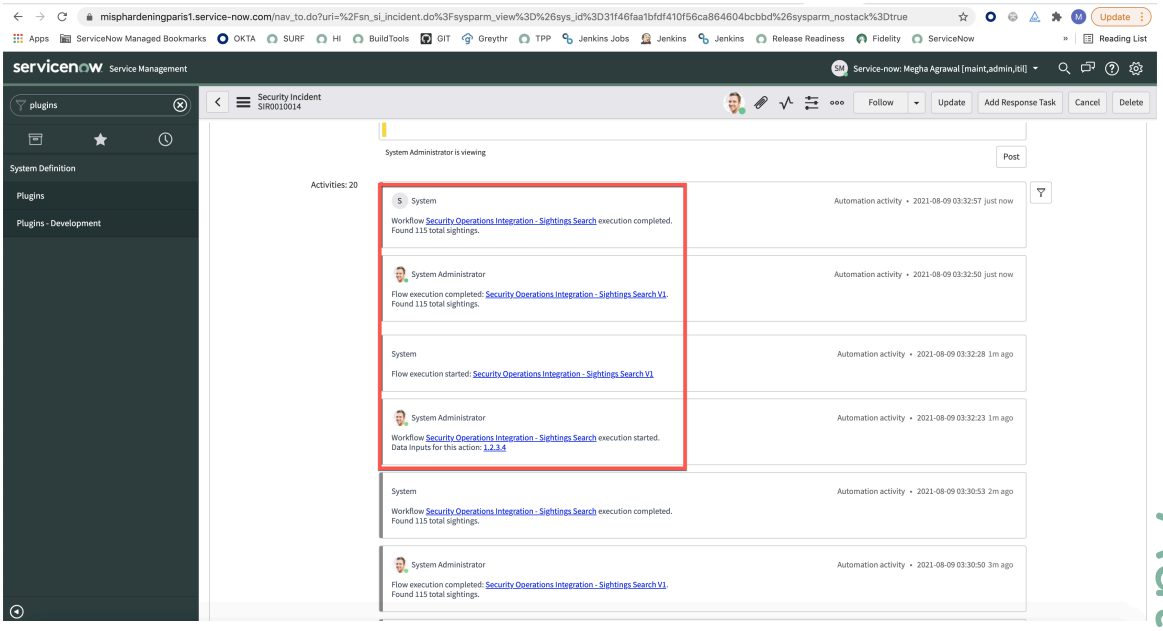
1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, die Sie ausführen möchten MISP Sichtungen suchen nach.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und **Zugeordnete Erkennbare Elemente** Registerkarte.
4. Wählen Sie das erkennbare Element aus, und klicken Sie dann im Menü Aktionen auf **Sichtungssuche Ausführen** .
   Sie können mehrere erkennbare Elemente für eine Sichtungssuche auswählen.
   Das Dialogfeld Sichtungssuche ausführen wird geöffnet.
5. Geben Sie den Datumsbereich für die Suche nach Sichtungssuchdaten an.

Dialogfeld „Sichtungssuche ausführen“

Feld	Beschreibung
Letzte	Anzahl der Stunden oder Tage vor der Erstellung des zu suchenden Incident. Der Standardwert ist 7 Tage. Der Grenzwert beträgt 99 Stunden oder Tage.
zwischen	Bereich der zu suchenden Daten. Standarddaten sind wie folgt: ○ Datum und Uhrzeit der Erstellung des Incident. ○ Datum und Uhrzeit, die sieben Tage vor der Eröffnung des Incident liegt.

6. Klicken Sie auf **Suche**.
   Das folgende Beispiel zeigt die Ergebnisse der manuellen Sichtungssuche in den Arbeitsnotizen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ergebnisse

Ein Sichtungssuchdatensatz wird erstellt. Nachdem die Workflow-Ausführung abgeschlossen ist, können Sie die zusammengefassten Informationen von erkennbaren Elementen anzeigen, die in allen Ereignissen (global) angezeigt und nach internen oder externen Sichtungen kategorisiert werden. Aggregat- und zugehörige Sichtungsdaten werden im Security Incident unter angezeigt Sichtungen , Sichtungssuchergebnisse , Und Sichtungssuchdetails Zugehörige Listen.

Sichtungen melden an MISP

Melden Sie Sichtungen von Bedrohungsdaten, damit Sie auf falsch positive Ergebnisse in Ihren Daten reagieren und Ihr Bewusstsein erhöhen können, wenn eine wirklich positive Bedrohung auftritt. Sie können auch ein Ablaufdatum für ein bestimmtes erkennbares Element oder Attribut hinzufügen.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Zur Verwendung von MISP bidirektionale Funktionen.
- Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Die MISP integration for Security Operations Ermöglicht Ihnen, Sichtungen an zu melden MISP Global über alle Ereignisse hinweg. Um eine Sichtung für ein bestimmtes Ereignis zu melden, müssen Sie verwenden MISP Instanz und lokale Meldung der Sichtung.

Um eine Sichtung an zu melden MISP, Das erkennbare Element oder das Attribut muss in verfügbar sein MISP Instanz.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, denen Sie die Sichtungen melden möchten MISP Für.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und die zugehörige Liste Sichtungen.
4. Wählen Sie das erkennbare Element aus, und wählen Sie im Menü Aktionen eine der folgenden Optionen aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. **Wahlweise:** Wenn Sie ausgewählt haben **MISP: Sichtungen erkennbarer Elemente melden** Option sollten Sie die Felder des Dialogfelds Sichtungen erkennbarer Elemente an MISP melden ausfüllen.

Sichtungen erkennbarer Elemente melden an MISP Dialogfeld

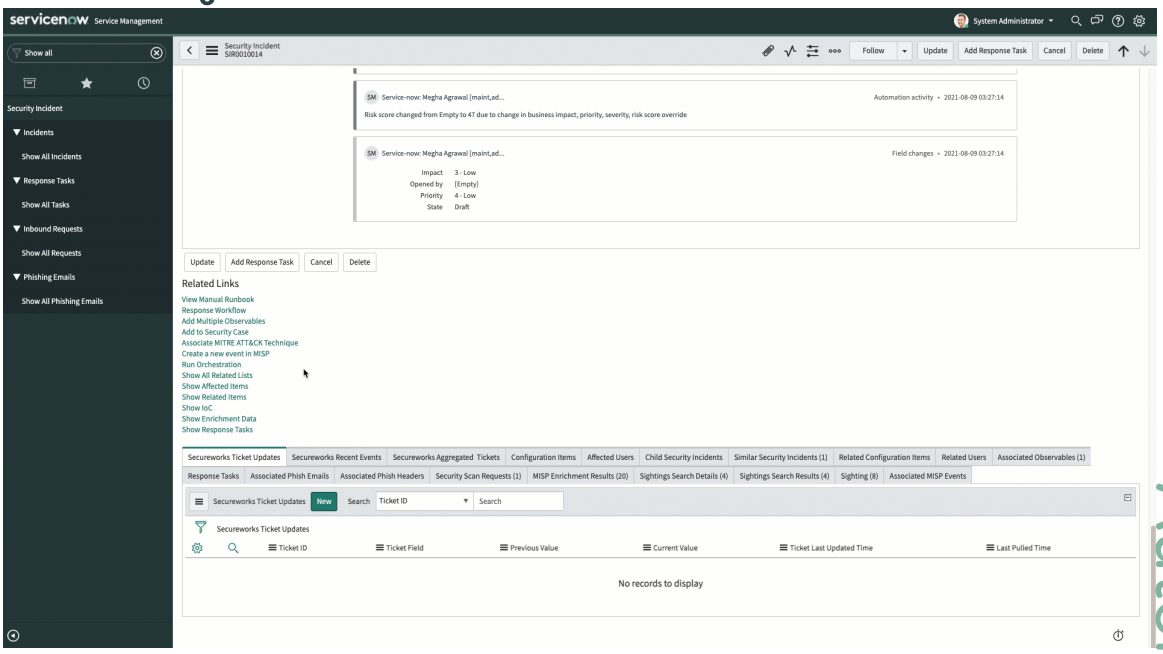
Feld	Beschreibung
Quelle	Quellfeld, das dem entspricht MISP Quelle der Sichtung.
Datum	Datumsfeld, das dem Datum entspricht, an dem das erkennbare Element gesehen wird. Wenn das Datum leer ist, werden das aktuelle Datum und die aktuelle Uhrzeit in eingetragen MISP.

Das folgende Beispiel zeigt, wie Sie im Security Incident zur zugehörigen Liste „Sichtungen“ navigieren. In dieser Liste können Sie ein erkennbares Element auswählen und die Sichtung erkennbarer Elemente an melden MISP. Die Erfolgsmeldung zeigt an, dass die Sichtung erfolgreich an übermittelt wurde MISP.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Meldet Sichtungen erkennbarer Elemente an MISP



a. Klicken Sie Auf **Melden Sie Die Sichtung** .

6. **Wahlweise:** Wenn Sie ausgewählt haben **MISP: Erkennbares Element als falsch positiv melden** Option sollten Sie die Felder des erkennbaren Elements als falsch positiv für melden ausfüllen MISP Dialogfeld.

Erkennbares Element als falsch positiv für melden MISP Dialogfeld

Feld	Beschreibung
Quelle (optional)	Quellfeld, das dem entspricht MISP Quelle. Verwenden Sie dieses Feld, um das erkennbare Element als falsch positiv zu deklarieren.
Datum	Datumsfeld, das dem Datum entspricht, an dem das erkennbare Element als falsch positiv erkannt wurde. Wenn das Datum leer ist, werden das aktuelle Datum und die aktuelle Uhrzeit in eingetragen MISP.

a. Klicken Sie Auf **Falsch Positiv Melden** .

7. **Wahlweise:** Wenn Sie ausgewählt haben **MISP: Erkennbares Element als abgelaufen melden** Option müssen Sie die Felder des Berichts „Ablauf erkennbarer Elemente melden an“ ausfüllen MISP Dialogfeld.

Dialogfeld „Ablauf erkennbarer Elemente an MISP melden“

Feld	Beschreibung
Quelle	Quellfeld, das dem entspricht MISP Quelle. Verwenden Sie dieses Feld, um ein erkennbares Element als abgelaufen festzulegen.
Datum	Datumsfeld, das dem Datum entspricht, an dem das erkennbare Element abgelaufen ist. Wenn das Datum

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	leer ist, werden das aktuelle Datum und die aktuelle Uhrzeit in eingetragen MISP.

a. Klicken Sie Auf **Ablauf Melden** .

Ergebnisse

Die Sichtungen wurden erfolgreich auf aktualisiert MISP Server.

Ergänzung erkennbarer Elemente in MISP

Durch Anreicherung erkennbarer Elemente mit zusätzlichen Informationen aus verschiedenen MISP Quellen während Untersuchungen zur Reaktion auf Incidents können Sie identifizierte Bedrohungen eindämmen.

Aktivieren Sie die automatische Ergänzung erkennbarer Elemente in MISP

Aktivieren Sie die automatische Anreicherung erkennbarer Elemente in ServiceNow AI Platform MISP Wenn dem Security Incident neue erkennbare Elemente zugeordnet sind.

Vorbereitungen

- Aktivieren Sie Security Incident Response Systemeigenschaft für **Aktiviert oder deaktiviert die geplante Aufgabe „erkennbare Security Incident-Elemente suchen“** Option zum Auslösen der Ergänzungsfähigkeit für erkennbare Elemente in SIR.
- Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, in denen Sie die Daten erkennbarer Elemente anreichern möchten MISP Für.
3. Überprüfen Sie die Arbeitsnotizen, nachdem dem Security Incident neue erkennbare Elemente zugeordnet wurden.

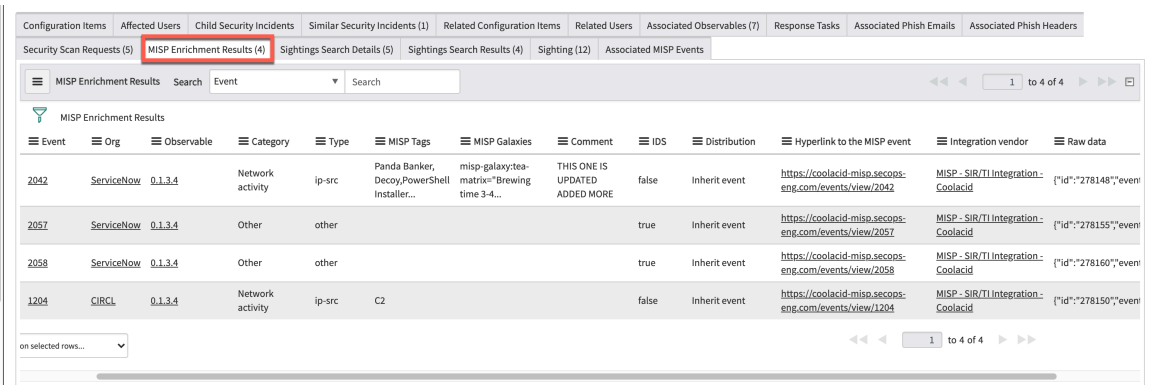
   Das folgende Beispiel zeigt, dass eine Arbeitsnotiz postet, wenn Integration von Security Operations – Flow für erkennbare Elemente anreichern Auslöser.

4. In MISP Zugehörige Liste „Ergänzungsergebnisse“ des Security Incidents. Zeigen Sie die Ergänzungsergebnisse an, nachdem die Flow-Ausführung abgeschlossen ist.

Hinweis:
Sie müssen dies konfigurieren MISP Die zugehörige Liste „Ergänzungsergebnisse“ wird in den zugehörigen Listen „Security Incident“ angezeigt. Weitere Informationen finden Sie unter Konfiguration der zugehörigen Liste .

Das folgende Beispiel zeigt die Ergänzungsergebnisse in MISP.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die folgende Tabelle zeigt die MISP-Ergänzungsergebnisse.

MISP-Datenanreicherungs-Ergebnisse

Feld	Beschreibung
Ereignis	ID des Ereignisses. Klicken Sie auf Öffnen, um den Datensatz in anzuzeigen ServiceNow AI Platform Instanz.
Org	Organisation, die das Ereignis ursprünglich erstellt hat.
Erkennbares Element	Erkennbares Element, das dem Ereignis zugeordnet ist.
Kategorie	Kategorie des Attributs. Zeigen Sie die Liste der Kategorien in an MISP-Dokumentation .
Typ	Typ des Attributs. Zeigen Sie die Liste der Typen in an MISP-Dokumentation .
MISP-Tags	Liste der Tags, die dem zugeordnet sind MISP Attribut.
MISP-Galaxien	Liste der Galaxien, die dem zugeordnet sind MISP Attribut.
Kommentar	Kontextbezogener Kommentar zur weiteren Beschreibung des Attributs. Diese Kommentare werden nicht für Korrelationen verwendet und sind rein informativ.
IDS	Indikator der Kompromittierung, der es ermöglicht, in alle berechtigten Exporte aufzunehmen.
Verteilung	Verteilung des Attributs nach der Veröffentlichung. Ein Attribut kann eine andere Verteilungsebene haben als das Ereignis. In beiden Fällen wird die niedrigste Verteilungsebene verwendet.
Hyperlink zum MISP-Ereignis	Link zu MISP Ereignis, das auf gespeichert wird MISP Server.
IntegrationsVendor	Integrationslieferant, der die Daten zur Ergänzung bereitstellt.
Rohdaten	Rohdaten, die dem zugeordnet sind MISP Attribut.

Führen Sie eine manuelle Ergänzung erkennbarer Elemente in durch MISP

Wählen Sie einzelne oder mehrere erkennbare Elemente aus, und führen Sie eine manuelle Ergänzung erkennbarer Elemente durch, damit Sie erkennbare Elemente mit zusätzlichen Informationen aus verschiedenen ergänzen können MISP Quellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

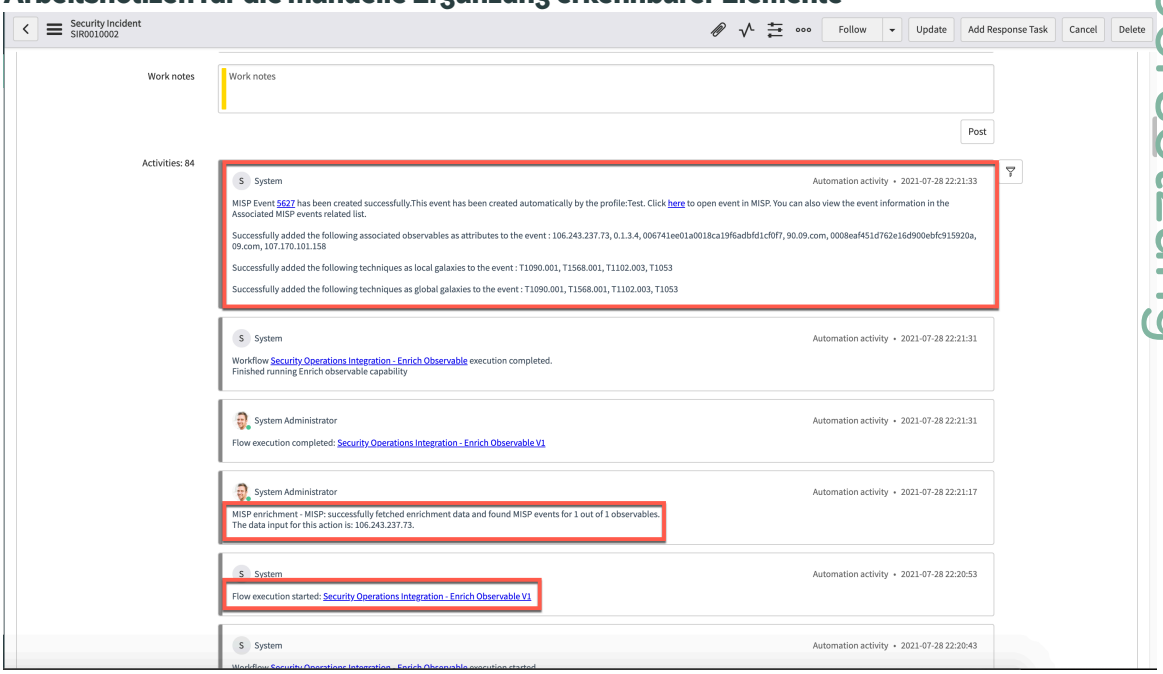
- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Zur Verwendung von MISP bidirektionale Funktionen.
- Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie die Ergänzung durchführen möchten.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und **Zugeordnete Erkennbare Elemente** Registerkarte.
4. Wählen Sie das erkennbare Element aus, und klicken Sie im Menü Aktionen auf **Ergänzung Erkennbarer Elemente Ausführen** .
   Sie können mehrere erkennbare Elemente für eine Sichtungssuche auswählen.
   Das Dialogfeld Anreicherung erkennbarer Elemente ausführen wird angezeigt.
5. Wählen Sie ein aus MISP Quelle und wählen Sie in der Spalte ausgewählt eine Implementierung aus, um die ausgewählten erkennbaren Elemente anzureichern.
6. Klicken Sie auf **Absenden**.
   Eine Arbeitsnotiz zeigt, dass Integration von Security Operations: Bereichern Sie den Workflow für erkennbare Elemente Wurde ausgelöst. Die zugehörigen Implementierungs-Workflows werden ausgeführt, um die Ergänzung durchzuführen. Sie können die Arbeitsnotizen im Security Incident anzeigen, um den Status anzuzeigen.

   Das folgende Beispiel zeigt, wie die Arbeitsnotizen für eine manuelle Ergänzung erkennbarer Elemente angezeigt werden.

Arbeitsnotizen für die manuelle Ergänzung erkennbarer Elemente



In der Ergänzungsnachricht wird das erstellte Ereignis aufgelistet. Sie können das Ereignis in anzeigen ServiceNow AI Platform Oder in MISP Instanz und zeigen Sie die Details des Datensatzes auf der Registerkarte MISP-Anreicherungsergebnisse an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie Tags hinzu, oder entfernen Sie sie MISP Attribute

Fügen Sie Tags in hinzu, oder entfernen Sie sie MISP Zum Klassifizieren von Ereignissen oder Attributen. Sie können das globale Tagging verwenden, um Ihre Klassifizierung zu aktivieren, oder Tags lokal verwenden, wenn Sie es nicht möchten MISP Ereignisse, die während Ihrer Klassifizierung geändert werden sollen.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Zur Verwendung von MISP bidirektionale Funktionen.
- Stellen Sie sicher, dass das Attribut, das Sie bearbeiten, zur selben Organisation gehört wie der MISP Anwender.
- Beachten Sie, dass die Tags und Galaxien, die Ihnen zur Verfügung stehen, auf basieren MISP Quelle und ihre Verteilungsberechtigungen.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente, Attribute oder Ereignisse enthält, für die Sie die Tags hinzufügen möchten.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und die zugehörige Liste MISP-Anreicherungsergebnisse.
4. Klicken Sie auf das Vorschausymbol ⓘ Neben einem Datensatz, und klicken Sie dann auf **Öffnen Sie Den Datensatz** .
   Das folgende Beispiel zeigt, wie Sie überprüfen **MISP-Anreicherungsergebnisse** Und wie man eine öffnet MISP Ergänzungsdatensatz.

   MISP-Ergänzungsergebnisdatensatz
   Der Ergebnisdatensatz der MISP-Anreicherung wird geöffnet

5. Überprüfen Sie den Ergebnisdatensatz der MISP-Anreicherung.

MISP-Anreicherungsergebnis

Feld	Beschreibung
Erkennbares Element	
Ereignis	Ereignis-ID, die von zugewiesen wird MISP Server, auf dem das Ereignis zum ersten Mal erstellt oder in importiert wurde MISP. Zeigen Sie eine Vorschau des Ereignisses an, oder klicken Sie auf den Datensatz, um die Ereignisdaten in anzuzeigen MISP Seite „Ereignisdaten“.
Org	Organisation, die erstellt hat MISP Attribut.
Kategorie	Kategorie des Attributs, das Sie dem bestimmten Ereignis in hinzufügen MISP. Sie können eine Option auswählen, z. B. eine interne Referenz, Netzwerkaktivität, Finanzbetrug usw.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	Typ von MISP Attribut.
IntegrationsVendor	Integrationslieferant, der die Daten für die Ergänzung erkennbarer Elemente bereitstellt.
Erstellungsdatum (in MISP)	Datum, an dem das Ereignis zuerst erstellt oder in importiert wurde MISP.
IDS	Status, der angibt, ob ein erkennbares Element in als schädlich markiert ist SIR. Das entsprechende Attribut in MISP Ist auch als „wahr“ markiert.
Verteilung	Verteilungsoptionen-Steuerungen, z. B. wer dieses Ereignis nach der Veröffentlichung anzeigen kann. Diese Option steuert auch, ob das Ereignis mit anderen Servern synchronisiert wird. Die Verteilung wird von den Attributen übernommen, und die restriktivste Einstellung gewinnt. Die Verteilungsoptionen lauten wie folgt: ○ Nur Ihre Organisation: Ermöglicht nur Mitgliedern Ihrer Organisation, dieses Ereignis anzuzeigen. Das Ereignis kann von einem Ihrer Organisationsmitglieder in eine andere Instanz abgerufen werden, über die nur Ihre Organisation Zugriff zum Anzeigen hat. Ereignisse mit dieser Einstellung werden nicht synchronisiert. ○ Nur diese Community: Aktiviert Anwender, die Teil Ihres sind MISP community zum Anzeigen des Ereignisses, einschließlich Ihrer eigenen Organisation, Organisationen zu diesem MISP Server und Organisationen, die ausgeführt werden MISP Server, die mit diesem Server synchronisiert werden. Alle anderen Organisationen, die mit diesen verknüpften Servern verbunden sind, dürfen das Ereignis nicht anzeigen. ○ Verbundene Communities: Ermöglicht Anwendern, die Teil Ihres sind MISP community zum Anzeigen des Ereignisses, einschließlich aller Organisationen in diesem MISP Server, alle Organisationen auf MISP Server, die mit diesem Server synchronisiert werden, und die Hosting-Organisationen von Servern, die eine Verbindung zu einem Server herstellen, der zwei Hops entfernt ist). Alle anderen Organisationen, die mit den verknüpften Servern verbunden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	sind, die zwei Hops entfernt sind, können das Ereignis nicht anzeigen. ○ Alle Communities: Teilt das Ereignis mit allen MISP communities, mit denen das Ereignis frei verfügbar sein kann.
Hyperlink zum MISP-Ereignis	Link zu MISP Ereignis, das auf gespeichert ist MISP Server.
Rohdaten	Rohdetails für den Datensatz mit Ergänzungsdaten für erkennbare Elemente.
Kommentar	Kommentare, die Sie für die Attribute hinzufügen. Diese Kommentare dienen nur zu Informationszwecken und werden nicht für Korrelationen verwendet.
Tags (lokal)	Tags, die in der Host-Organisation verfügbar sind MISP Instanz zum Aktivieren von Tagging für Synchronisierung und Exportfilterung. MISP Ereignisse werden nicht geändert, wenn Sie lokale Tags verwenden. Diese Tags werden immer entfernt, bevor sie mit anderen synchronisiert werden MISP Instanzen und freigegebene Communities.
Tags (global)	Tags, die global verfügbar sind, um sie mit anderen freizugeben und zu synchronisieren MISP Instanzen und freigegebene Communities. Wenn Sie globale Tags zu hinzufügen MISP Instanzen ändern Sie Ereignisse.
Galaxien (lokal)	Galaxien, die in der Host-Organisation verfügbar sind MISP Instanz für Synchronisierung und Exportfilterung. MISP Ereignisse werden nicht geändert, wenn Sie lokale Galaxien verwenden. Diese Galaxien werden immer entfernt, bevor sie mit anderen synchronisiert werden MISP Instanzen und freigegebene Communities.
Galaxien (global)	Galaxien, die global verfügbar sind, um mit anderen geteilt und synchronisiert zu werden MISP Instanzen und freigegebene Communities. Wenn Sie globale Galaxien hinzufügen, MISP Ereignisse werden geändert.

6. Klicken Sie auf das Bearbeitungssymbol, um entweder ein lokales oder ein globales Tag zu bearbeiten In einer der folgenden Optionen:

- **Tags (lokal)**
- **Tags (global)**

7. Geben Sie im Dialogfeld „MISP-Attribut-Tags“ den Namen des Tags ein, das gesucht und hinzugefügt werden soll.
8. Klicken Sie Auf **Tags auf MISP-Attribut aktualisieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol für die lokalen Tags die Tags C3, Adware, C2 und Botnet 3101 suchen, hinzufügen und den MISP-Server mit den Tags aktualisieren können. Die Bestätigungsnachricht zeigt an, dass alle Tags in aktualisiert wurden MISP.

Hinzufügen lokaler Tags im MISP-Attribut.
Die Tags wurden erfolgreich in aktualisiert MISP Server.

9. Um die Änderungen im Datensatz anzuzeigen, klicken Sie auf **Formular Neu Laden** In der Erfolgsmeldung.

Fügen Sie Galaxien zu hinzu, oder entfernen Sie sie MISP Ereignis oder Attribut

Fügen Sie Galaxien in hinzu, oder entfernen Sie sie MISP Damit Sie diese Objekte in als Cluster klassifizieren können MISP Und hängen Sie sie an an an MISP Ereignisse oder Attribute.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Zur Verwendung von MISP bidirektionale Funktionen.
- Um lokale Galaxien hinzuzufügen, muss der Anwender, der die Integration konfiguriert hat, der Host-Organisation des entsprechenden angehören MISP Server.
- Beachten Sie, dass die Tags und Galaxien, die Ihnen zur Verfügung stehen, auf basieren MISP Quelle und ihre Verteilungsberechtigungen.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Klicken Sie auf das Bearbeitungssymbol In einer der folgenden Optionen.

   - **Galaxien (lokal)**
   - **Galaxien (global)**

2. Geben Sie im Dialogfeld MISP-Ereignisgalaxien die Details ein.

Dialogfeld „MISP-Ereignisgalaxien“

Feld	Beschreibung
Ereignis-ID	Ereignis-ID, die von zugewiesen wird MISP Server, auf dem das Ereignis zum ersten Mal erstellt oder in importiert wurde MISP.
Namespace	Namespace, in dem die Galaxie gespeichert ist. Sie können Namespaces verwenden, um ähnliche Galaxien zu gruppieren.
Galaxien	Galaxie, in der Sie die Clusterinformationen speichern.
Cluster	Informationen zu den Clustern in der Galaxie.

3. Klicken Sie Auf **Aktualisieren Sie Galaxien auf MISP-Attribut** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol für die lokalen Galaxien den veralteten Namespace auswählen, die Galaxie Enterprise Attack – Angriffsmuster auswählen und die Clusterinformationen hinzufügen können. Nachdem die Galaxie-Informationen aktualisiert wurden, können Sie die Erfolgsmeldung anzeigen.

Hinzufügen von Galaxie-Informationen in MISP über den ServiceNow AI Platform

4. Um die Änderungen im Datensatz anzuzeigen, klicken Sie auf **Formular Neu Laden** In der Erfolgsmeldung.

Ergebnisse
Die Galaxie-Informationen wurden erfolgreich in aktualisiert MISP Server.

Fügen Sie Kommentare zu hinzu MISP Attribut

Fügen Sie Kommentare für hinzu MISP Attribute. Die Kommentare, die Sie hinzufügen, dienen nur zu Informationszwecken und werden nicht für die Korrelation von verwendet MISP Daten.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Zur Verwendung von MISP bidirektionale Funktionen.
- Stellen Sie sicher, dass das Attribut, das Sie bearbeiten, zur selben Organisation gehört wie der MISP Anwender.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Klicken Sie auf das Bearbeitungssymbol Im Feld Kommentar.
2. Geben Sie Ihren Kommentar in das Feld Attributkommentar ein.
3. Klicken Sie Auf **Aktualisieren Sie den Kommentar auf das MISP-Attribut** .
   Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol neben dem Kommentarfeld einen Kommentar hinzufügen und dann aktualisieren können MISP Attribut. Nachdem der Kommentar aktualisiert wurde, können Sie die Erfolgsmeldung anzeigen.

   Hinzufügen von Galaxie-Informationen in MISP über den ServiceNow AI Platform.
4. Um die Änderungen im Datensatz anzuzeigen, klicken Sie auf **Formular Neu Laden** In der Erfolgsmeldung.

Ergebnisse
Der Kommentar wurde erfolgreich in aktualisiert MISP Server.

Verwalten von Ereignissen in MISP

Sie können Ereignisse in erstellen MISP Automatisch oder manuell aus dem ServiceNow AI Platform. Sie können die Ereignisdaten auch in bearbeiten MISP Von ServiceNow AI Platform.

Automatisch erstellte Ereignisse in werden überprüft MISP

Sie können die automatisch erstellten Ereignisse überprüfen, nachdem Sie das Ereigniserstellungsprofil in konfiguriert haben ServiceNow AI Platform Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Profil für automatische Ereigniserstellung

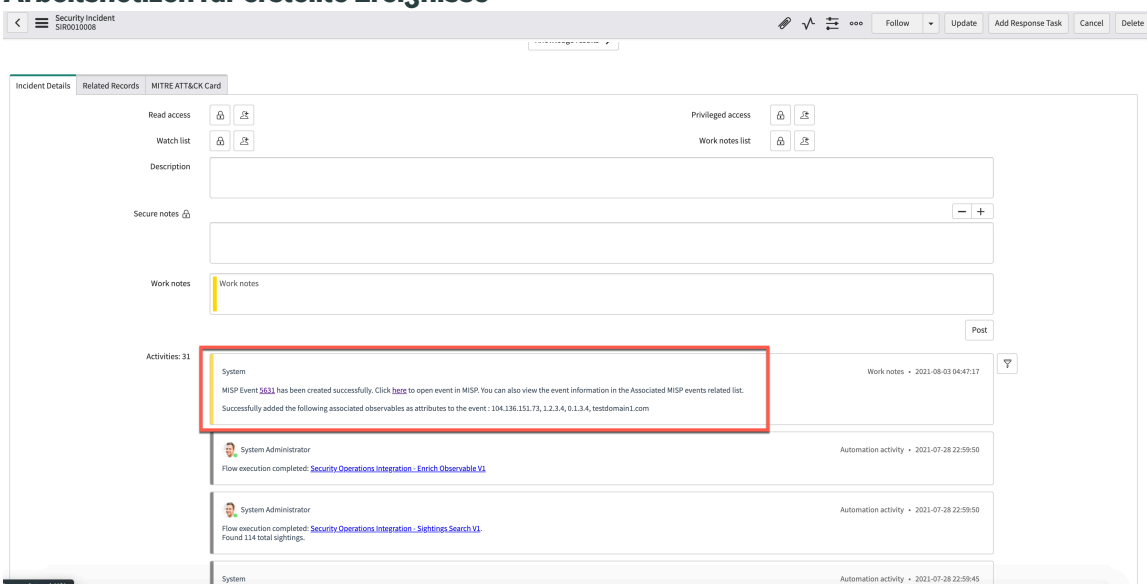
Konfigurieren des Profils für die automatische Ereigniserstellung Wird von den Anwenderrollen sn_si.admin oder sn_ti.admin in ausgeführt **MISP-Integration** > **Profile für die automatische Erstellung von Ereignissen** Modul.

Anzeigen von MISP Ereignisdaten

Sie können die erstellten Ereignisse auf folgende Weise anzeigen:

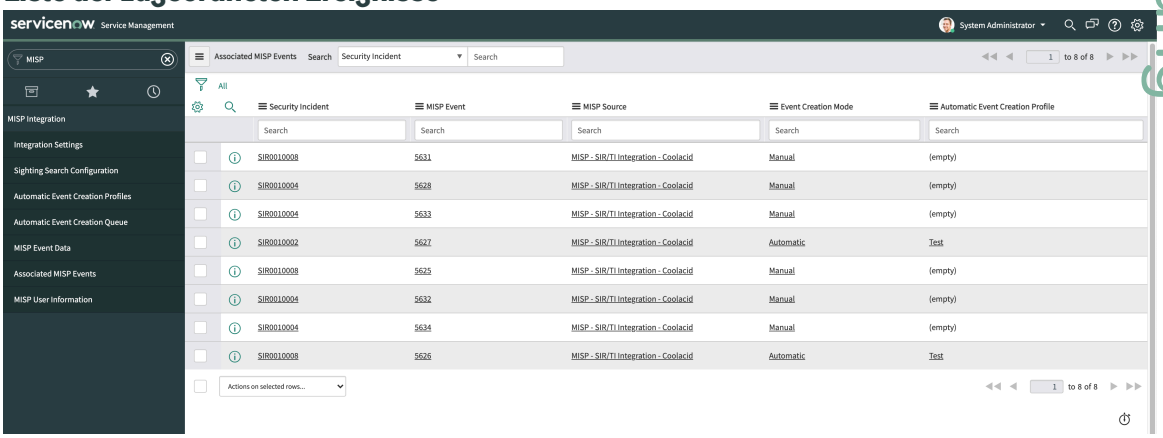
- Zeigen Sie die Arbeitsnotizen für die erstellten Ereignisse an. Sie können die Ereignisdetails in anzeigen ServiceNow AI Platform Instanz und auch wie in angezeigt MISP Server, wie im folgenden Beispiel gezeigt.

Arbeitsnotizen für erstellte Ereignisse



- Klicken Sie auf Zugeordnete MISP-Ereignisse Zugehörige Liste. Hier können Sie das Ereignis in Bezug auf den Security Incident und anzeigen MISP Ressourcen, wie im folgenden Beispiel gezeigt.

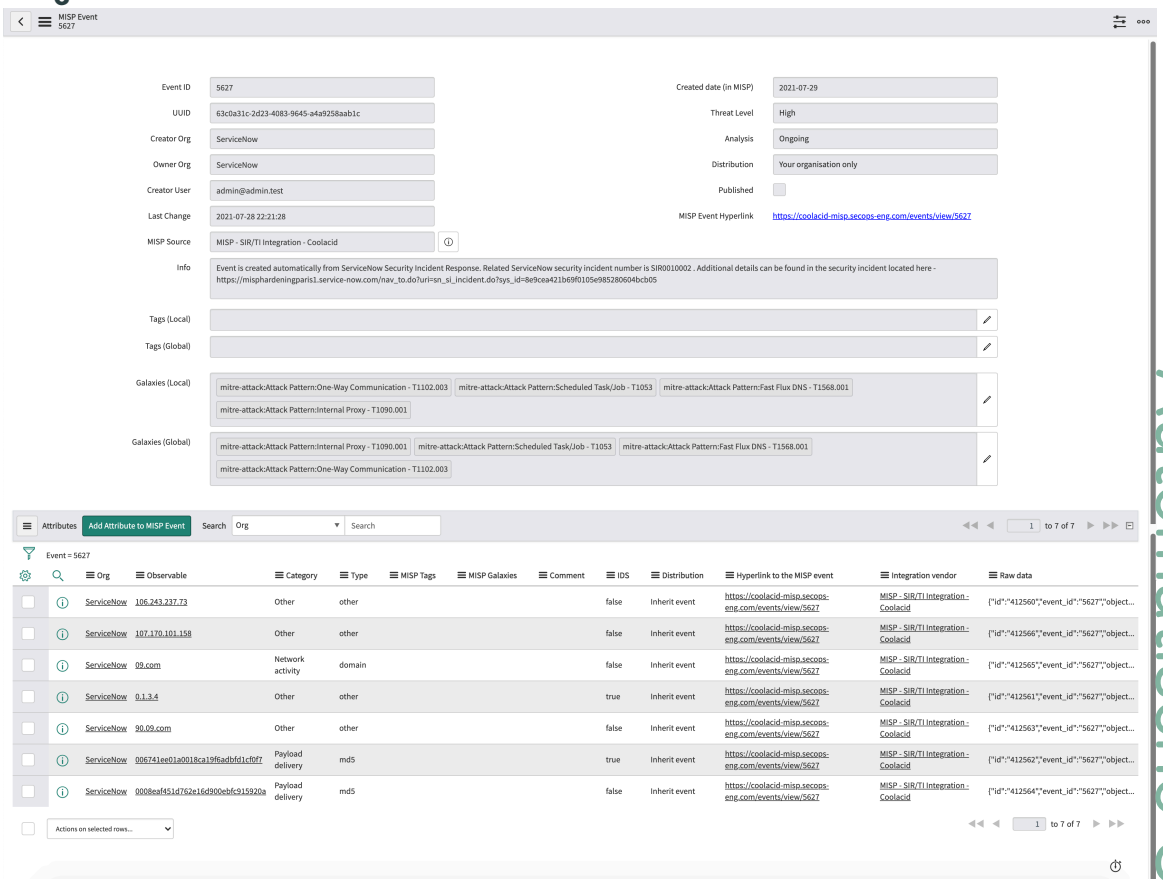
Liste der zugeordneten Ereignisse



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zeigen Sie an MISP Ereignisdaten in der Formularansicht, um die detaillierten Informationen zu zu überprüfen MISP Ereignisse, wie im folgenden Beispiel gezeigt.

Ereignisdaten in der Formularansicht



Erstellen Sie manuell ein Ereignis in MISP

Erstellen Sie Ereignisse in manuell MISP Von ServiceNow AI Platform Dient zum Erfassen kontextbezogener Informationen, die als Attribute und Objekte dargestellt werden.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Zur Verwendung von MISP bidirektionale Funktionen.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, der die erkennbaren Elemente enthält, für die Sie ein Ereignis erstellen möchten.
3. Klicken Sie Auf **Erstellen Sie ein neues Ereignis in MISP** .
4. Geben Sie im Dialogfeld Neues Ereignis in MISP erstellen die Details ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Ereignis im MISP-Dialogfeld

Feld	Beschreibung
Datum	Erstellungsdatum des Ereignisses in MISP.
Information zum Ereignis	Ereignisinformationen, die automatisch aus erstellt werden ServiceNow AI Platform Security Incident Response.
Bedrohungsstufe	Risikostufe des Ereignisses. Sie können die Incidents in drei verschiedene Bedrohungskategorien (niedrig, Mittel, hoch) kategorisieren. Dieses Feld kann auch als nicht definiert belassen werden. Die folgenden Optionen sind verfügbar: ○ Niedrig: Allgemeine Massen-Malware ○ Mittel: Advanced Persistent Threats (APT) ○ Hoch: Ausgeklügelte APTs und 0-Tage-Angriffe
Quelle	MISP Quelle für die Ereigniserstellung.
Verteilung	Option, die steuert, wer dieses Ereignis nach der Veröffentlichung des Ereignisses anzeigen kann. Diese Option steuert auch, ob das Ereignis mit anderen Servern synchronisiert wird. Die Verteilung wird von den Attributen übernommen. Die restriktivste Einstellung gewinnt. Die Verteilungsoptionen lauten wie folgt: ○ Nur Ihre Organisation: Ermöglicht nur Mitgliedern Ihrer Organisation, dieses Ereignis anzuzeigen. Das Ereignis kann von einem Ihrer Organisationsmitglieder in eine andere Instanz abgerufen werden, über die nur Ihre Organisation Zugriff zum Anzeigen hat. Ereignisse mit dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Einstellung werden nicht synchronisiert. ○ Nur diese Community: Aktiviert Anwender, die Teil Ihres sind MISP community zum Anzeigen des Ereignisses, einschließlich Ihrer eigenen Organisation, Organisationen zu diesem MISP Server und Organisationen, die ausgeführt werden MISP Server, die mit diesem Server synchronisiert werden. Alle anderen Organisationen, die mit verknüpften Servern verbunden sind, dürfen das Ereignis nicht anzeigen. ○ Verbundene Communities: Ermöglicht Anwendern, die Teil Ihres sind MISP community zum Anzeigen des Ereignisses, einschließlich aller Organisationen in diesem MISP Server, alle Organisationen auf MISP Server, die mit diesem Server synchronisiert werden, und die Hosting-Organisationen von Servern, die eine Verbindung zu einem Server herstellen, der zwei Hops entfernt ist. Alle anderen Organisationen, die mit den verknüpften Servern verbunden sind, die zwei Hops von diesem Server entfernt sind, können das Ereignis nicht anzeigen. ○ Alle Communities: Teilt das Ereignis mit allen MISP communities.
Analyse	Aktuelle Phase der Analyse für das Ereignis mit den folgenden möglichen Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld		Beschreibung
		○ Anfänglich: Die Analyse beginnt gerade erst ○ Laufend: Die Analyse wird ausgeführt ○ Abgeschlossen: Die Analyse ist abgeschlossen
Erweiterte Optionen	Alle SIR-zugeordneten erkennbaren Elemente als Attribute zum MISP-Ereignis hinzufügen	Option zum Hinzufügen verfügbarer erkennbarer Elemente in einem Security Incident zu einem MISP Ereignis als Attribute. Mit dieser Option wird aktiviert **Legen Sie die Attribut-IDS-Kennzeichnung fest, wenn das Ergebnis erkennbarer Elemente schädlich ist** Option.
	Legen Sie die Attribut-IDS-Kennzeichnung fest, wenn die Erkennung von erkennbaren Elementen schädlich ist.	Erkennbares Element, das in als schädlich markiert ist SIR. Das entsprechende Attribut in MISP Ist auch als „wahr“ markiert.
	Erkennbare Elemente anhand von Sicherheits-Tags filtern	Option zum Filtern der erkennbaren Elemente basierend auf den ausgewählten Sicherheits-Tags. Diese Option bietet die Möglichkeit, MISP-Ereignisse in Threat Intelligence zu unterscheiden und zu verwalten. **Sicherheits-Tags** : Fügen Sie Tags hinzu, um die erkennbaren Elemente zu filtern. Wenn Sie beispielsweise ein Tag mit der Bezeichnung „von Freigabe blockieren“ oder „TLP: Weiß“ hinzufügen, werden diese erkennbaren Elemente während der Erstellung des MISP-Ereignisses nicht als Attribut zum MISP-Ereignis hinzugefügt, wenn einem der erkennbaren Elemente eines dieser Tags zugeordnet ist.
	Synchronisieren Sie MITRE ATT&CK-Techniken für Security Incident als lokale Galaxien mit dem MISP-Ereignis	Option zum Synchronisieren von ServiceNow AI Platform SIR Security Incident MITRE-

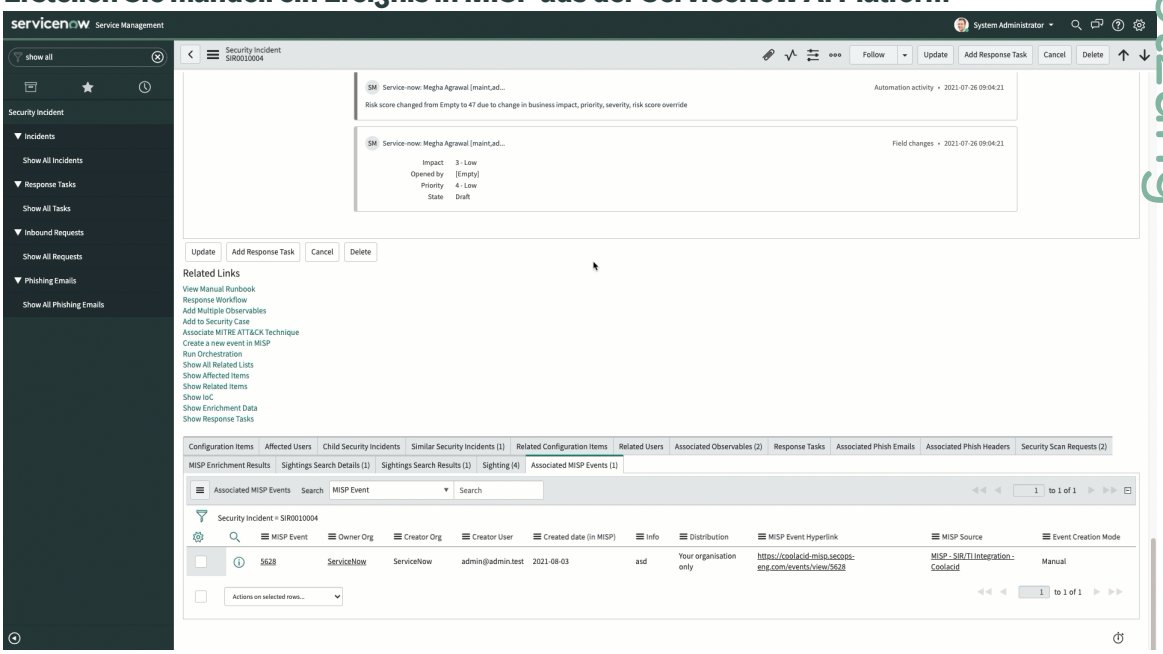
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld		Beschreibung
		ATT&CK™ Techniken als lokale Galaxien in MISP Ereignis.
	MITRE ATT&CK-Techniken des Security Incident als globale Galaxien im MISP-Ereignis synchronisieren	Option zum Synchronisieren von ServiceNow AI Platform SIR Security Incident MITRE-ATT&CK™ Techniken als globale Galaxien in MISP Ereignis.
	MISP-Ereignis Tags hinzufügen	Option, mit der Sie den in ServiceNow erstellten Ereignissen MISP-Tags hinzufügen können. Diese Option zeigt die folgenden Optionen an: ○ **Lokal (Tags):** Die ausgewählten Tags werden dem MISP-Ereignis als lokale Tags hinzugefügt. ○ **Global (Tags):** Die ausgewählten Tags werden dem MISP-Ereignis als globale Tags hinzugefügt.

5. Klicken Sie Auf **Erstellen Sie ein neues MISP-Ereignis** .

Das folgende Beispiel zeigt das durch Erstellen eines Ereignisses in MISP, Sie können die Ergebnisse im Security Incident anzeigen. Sie können auch die Arbeitsnotizen und das Ereignis in anzeigen ServiceNow AI Platform Instanz und das Ereignis in der MISP Server, wie im folgenden Beispiel gezeigt.

Erstellen Sie manuell ein Ereignis in MISP aus der ServiceNow AI Platform



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die Ergebnisse auf folgende Weise anzeigen:

- Oben auf der Security Incident-Seite wird eine Erfolgsmeldung angezeigt. Sie können die Ereignisdetails in anzeigen ServiceNow AI Platform Instanz und auch wie in angezeigt MISP Server.
- In den Arbeitsnotizen können Sie die Erfolgsmeldung mit weiteren Details anzeigen. Sie können die Ereignisdetails auch in anzeigen ServiceNow AI Platform Instanz und auch wie in angezeigt MISP Server.
- In Zugeordnete MISP-Ereignisse Zugehörige Liste können Sie das Ereignis in Bezug auf den Security Incident und anzeigen MISP Ressourcen.

Fügen Sie einem Attribute hinzu MISP Ereignis

Fügen Sie einem Ereignis Attribute hinzu, z. B. Typ, Kategorie und andere kontextbezogene Informationen zum Ereignis.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Zur Verwendung von MISP bidirektionale Funktionen.
- Stellen Sie sicher, dass das Ereignis, das Sie hinzufügen oder aktualisieren, zur selben Organisation gehört wie der MISP Anwender.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Navigieren zu **Alle** > **MISP** > **Zugeordnete MISP-Ereignisse**an.
   Sie können auch in jedem Security Incident zur zugehörigen Liste zugehöriges MISP-Ereignis navigieren.
2. Klicken Sie auf das MISP-Ereignis, für das Sie ein Attribut hinzufügen möchten.
3. Klicken Sie Auf **Fügen Sie dem MISP-Ereignis ein Attribut hinzu** .
4. Geben Sie im Dialogfeld Attribut zu Ereignis hinzufügen die Details ein.

Dialogfeld „Attribut zu Ereignis hinzufügen“

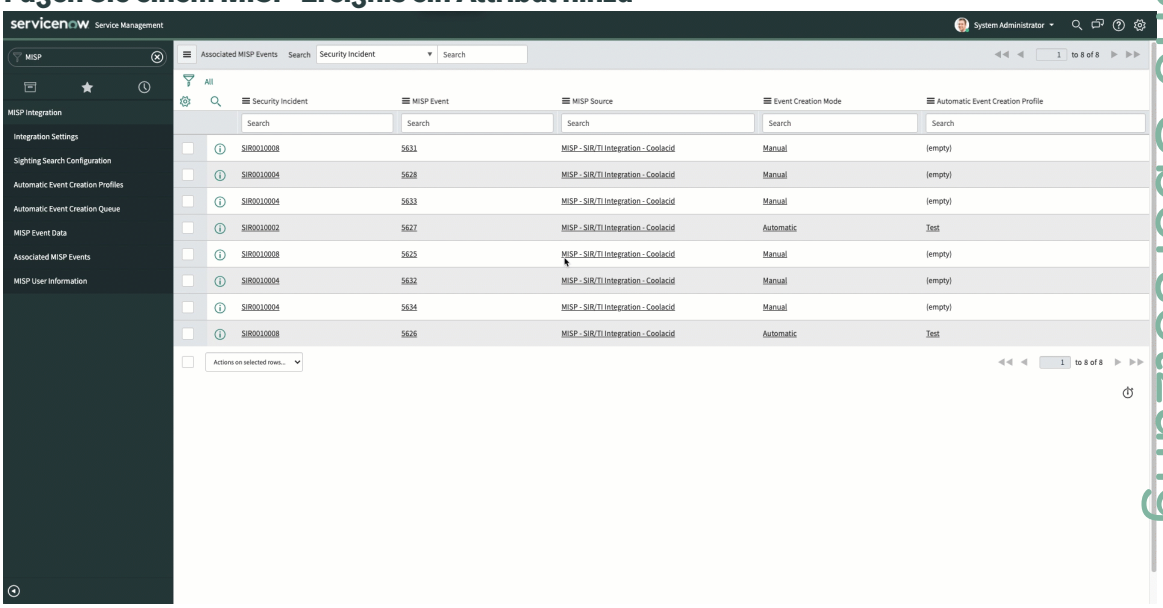
Feld	Beschreibung
Wert	Ist-Wert des Attributs. Geben Sie Daten zum Wert ein, die darauf basieren, was für den ausgewählten Attributtyp gültig ist. Beispiel: Für ein Attribut vom Typ ip-src (Quell-IP-Adresse) ist 11.11.11.11 ein gültiger Wert. **Hinweis:** Sie können nur Attribute oder erkennbare Elemente auswählen, die den Kontext mit dem Ereignis teilen. Die erkennbaren Elemente können in nicht bereits ein Attribut haben MISP.
Kategorie	Kategorie des Attributs. Die Kategorie beschreibt den Aspekt der Malware für dieses Attribut. Ein Beispiel wären die Persistenzmechanismen der Malware oder Netzwerkaktivität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typ	Typ, der die Kategorie erklärt. Wenn ein Angreifer beispielsweise eine IP-Adresse für einen Angriff verwendet, kann eine Quell-E-Mail-Adresse oder eine über einen Anhang gesendete Datei die Nutzlastbereitstellung einer Malware beschreiben. Diese Arten von Attributen haben die Kategorie „Nutzlastlieferung“.
Verteilung	Anwender, die dieses Attribut anzeigen können. Die Verteilung wird von Attributen geerbt. Die restriktivste Einstellung gewinnt.
Attribut als IDS-Signatur verwenden	Erkennbares Element, das in als schädlich markiert ist SIR. Das entsprechende Attribut in MISP Ist auch als „wahr“ markiert.
Kommentare	Kommentare, die Sie für die Attribute hinzufügen.

Das folgende Beispiel zeigt, dass Sie durch Navigieren aus der Liste der zugehörigen MISP-Ereignisse den Ereignisdatensatz 5627 anzeigen und dem Ereignis Attribute hinzufügen können. Die Attribute umfassen den Wert (testdomain.com), die Kategorie als externe Analyse und den Typ „Domäne“. Sie können auch IDS aktivieren. Die Erfolgsmeldung im Ereignisdatensatz zeigt an, dass das Attribut dem Ereignis hinzugefügt wird, wie im folgenden Beispiel gezeigt.

Fügen Sie einem MISP-Ereignis ein Attribut hinzu



5. Klicken Sie Auf **Fügen Sie dem MISP-Ereignis ein Attribut hinzu** .

Ergebnisse

Sie können das hinzugefügte Attribut im Abschnitt Attribute anzeigen.

Fügen Sie Tags zu hinzu MISP Ereignis

Fügen Sie Tags in hinzu ServiceNow AI Platform MISP Zum Klassifizieren von Ereignissen oder Attributen. Sie können das globale Tagging verwenden, um Ihre Klassifizierung zu aktivieren, oder Tags lokal verwenden, wenn Sie es nicht möchten MISP Ereignisse, die während Ihrer Klassifizierung geändert werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Zur Verwendung von MISP bidirektionale Funktionen.
- Stellen Sie sicher, dass das Ereignis, das Sie bearbeiten, zur selben Organisation gehört wie der MISP Anwender.
- Beachten Sie, dass die Tags und Galaxien, die Ihnen zur Verfügung stehen, auf basieren MISP Quelle und ihre Verteilungsberechtigungen.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, der das Ereignis enthält, für das Sie Tags hinzufügen möchten.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und die zugehörige Liste MISP-Anreicherungsergebnisse.
4. Klicken Sie in der Liste der Ergänzungsergebnisse auf die Ereignis-ID.
   Sie können auch von navigieren **MISP** > **Zugeordnete MISP-Ereignisse** Modul.
5. Überprüfen Sie den MISP-Ereignisdatensatz.

Formularansicht „MISP-Ereignis“

Feld	Beschreibung
Ereignis-ID	Ereignis-ID, die von zugewiesen wird MISP Wann das Ereignis zum ersten Mal erstellt oder in importiert wurde MISP Server.
UUID	ID, die Ereignisse und Attribute eindeutig identifiziert.
Organisation des Erstellers	Organisation, die das Ereignis in erstellt hat MISP Instanz.
Besitzerorganisation	Organisation, die das Ereignis auf der besitzt MISP Instanz. Dieses Feld ist nur für Administratoren sichtbar.
Erstelleranwender	Anwender, der das Ereignis in erstellt hat MISP.
Letzter Change	Datum, an dem das Ereignis zuletzt geändert wurde.
MISP-Quelle	MISP Quelle, in der das Ereignis erstellt wird.
Erstellungsdatum (in MISP)	Datum, an dem das Ereignis erstellt oder erstmals in importiert wurde MISP Server.
Bedrohungsstufe	Risikostufe des Ereignisses. Incidents können in drei verschiedene Bedrohungskategorien (niedrig, Mittel, hoch) kategorisiert werden. Dieses Feld kann als nicht definiert belassen werden. Die folgenden Optionen sind verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Niedrig: Allgemeine Massen-Malware ○ Mittel: Advanced Persistent Threats (APT) ○ Hoch: Ausgeklügelte APTs und 0-Tage-Angriffe
Analyse	Aktuelle Phase der Analyse für das Ereignis mit den folgenden möglichen Optionen: ○ Anfänglich: Die Analyse beginnt gerade erst ○ Laufend: Die Analyse wird ausgeführt ○ Abgeschlossen: Die Analyse ist abgeschlossen
Verteilung	Verteilung des einzelnen Attributs. Ein Attribut kann eine andere Verteilungsebene haben als das Ereignis.
Veröffentlicht	Status, der angibt, ob das Ereignis veröffentlicht wurde oder nicht. Durch die Veröffentlichung können die Attribute des Ereignisses für alle berechtigten Exporte verwendet werden, und Anwender, die die Ereigniswarnungen abonniert haben, werden benachrichtigt.
MISP-Ereignis-Hyperlink	Link zu MISP Ereignis, das auf gespeichert ist MISP Server.
Info	Kurzbeschreibung des Ereignisses.
Tags (lokal)	Tags, die in der Host-Organisation verfügbar sind MISP Instanz zum Aktivieren von Tagging für Synchronisierung und Exportfilterung. MISP Ereignisse werden nicht geändert, wenn Sie lokale Tags verwenden. Lokale Tags werden immer entfernt, bevor sie mit anderen synchronisiert werden MISP Instanzen und freigegebene Communities.
Tags (global)	Tags, die global verfügbar sind, um sie mit anderen freizugeben und zu synchronisieren MISP Instanzen und freigegebene Communities. Wenn Sie globale Tags zu hinzufügen MISP Instanzen können Sie Ereignisse ändern.
Galaxien (lokal)	Galaxien, die in der Host-Organisation verfügbar sind MISP Instanz für Synchronisierung und Exportfilterung. MISP Ereignisse werden nicht geändert, wenn Sie lokale Galaxien verwenden. Diese lokalen Galaxien werden immer entfernt, bevor sie mit anderen synchronisiert werden MISP Instanzen und freigegebene Communities.
Galaxien (global)	Galaxien, die global verfügbar sind, um mit anderen geteilt und synchronisiert zu werden MISP Instanzen und freigegebene Communities. Wenn Sie globale

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Galaxien hinzufügen, MISP Sie können Ereignisse ändern.

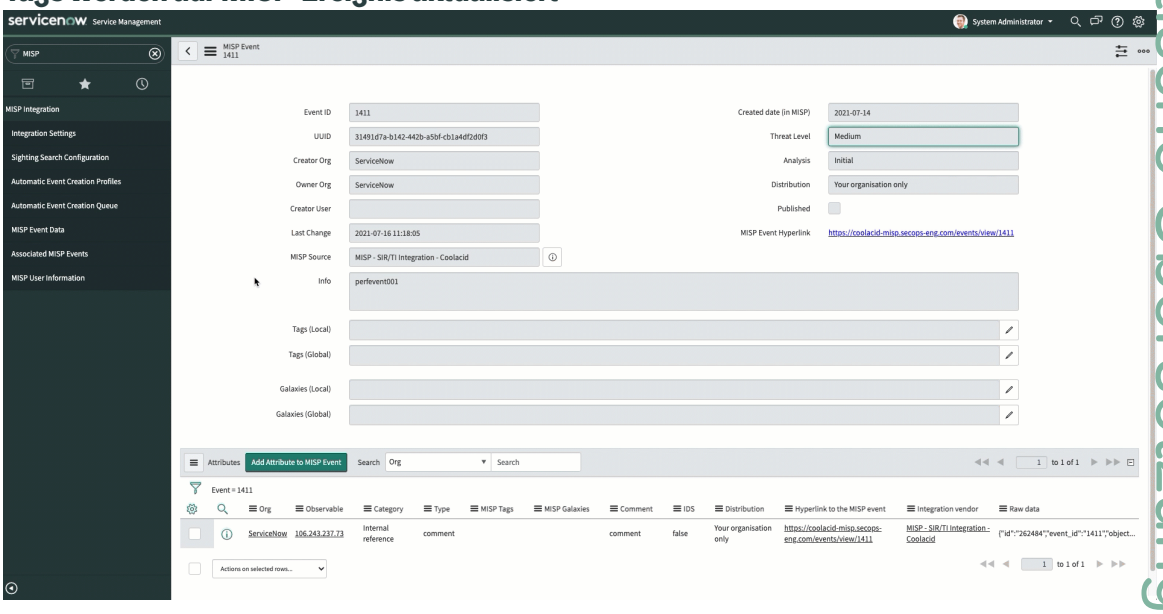
6. Klicken Sie auf das Bearbeitungssymbol, um entweder ein lokales oder ein globales Tag zu bearbeiten In einer der folgenden Optionen:

   - **Tags (lokal)**
   - **Tags (global)**

7. Geben Sie im Dialogfeld „MISP-Ereignis-Tags“ den Tag-Namen ein, nach dem die Tags gesucht und hinzugefügt werden sollen.
8. Klicken Sie Auf **Aktualisieren Sie Tags auf MISP-Ereignis** .

   Das folgende Beispiel zeigt, dass Sie durch Klicken auf das Bearbeitungssymbol für die lokalen Tags die Tags C3, Adware, C2 und Botnet 3101 suchen, hinzufügen und den MISP-Server mit den Tags aktualisieren können. Die Bestätigungsnachricht zeigt an, dass alle Tags in aktualisiert wurden MISP.

Tags werden auf MISP-Ereignis aktualisiert



9. Klicken Sie Auf **Formular Neu Laden** In der Erfolgsmeldung, um die Änderungen im Datensatz anzuzeigen.

Ergebnisse

Die Tags wurden erfolgreich in aktualisiert MISP Server.

Aktualisieren Sie Galaxien auf ein MISP Ereignis oder Attribut

Fügen Sie Galaxien in hinzu, oder entfernen Sie sie ServiceNow AI Platform MISP Damit Sie diese Objekte in als Cluster klassifizieren können MISP Instanz und Anhängen Sie sie an MISP Ereignisse oder Attribute.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Überprüfung des folgenden Elements: MISP Anwenderrolle und Berechtigungen Erforderlich für die Verwendung von MISP bidirektionale Funktionen.
- Um lokale Galaxien hinzuzufügen, muss der Anwender, der die Integration konfiguriert hat, der Host-Organisation des entsprechenden angehören MISP Server.
- Die Ihnen zur Verfügung stehenden Tags und Galaxien basieren auf MISP Quelle und ihre Verteilungsberechtigungen.
- Erforderliche Rolle: sn_sec_misp.write

Prozedur

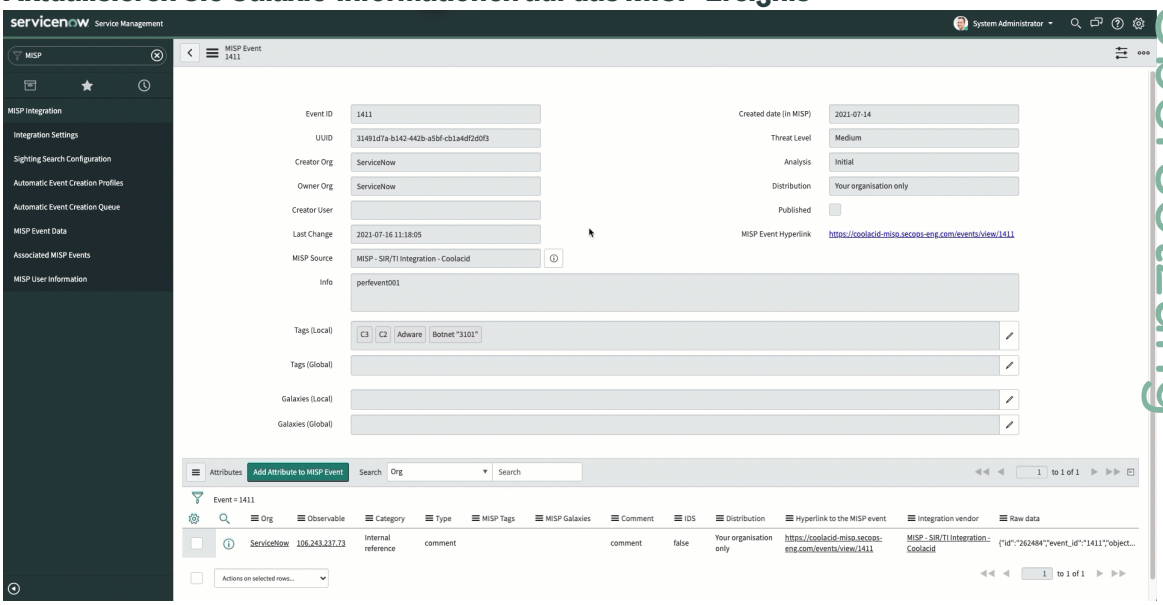
1. Klicken Sie auf das Bearbeitungssymbol In einer der folgenden Optionen.

   - **Galaxien (lokal)**
   - **Galaxien (global)**

2. Geben Sie im Dialogfeld „MISP-Ereignisgalaxien“ die Tags ein, und suchen Sie sie, um sie hinzuzufügen.
3. Klicken Sie Auf **Aktualisieren Sie Galaxien auf MISP-Ereignis** .

   Das folgende Beispiel zeigt, wie Sie auf das Bearbeitungssymbol für die lokalen Galaxien klicken, den veralteten Namespace auswählen, die Galaxie Enterprise Attack – Attack Pattern auswählen und Clusterinformationen hinzufügen. Nachdem die Galaxie-Informationen aktualisiert wurden, können Sie die Erfolgsmeldung anzeigen.

   Aktualisieren Sie Galaxie-Informationen auf das MISP-Ereignis

   Die Galaxien wurden erfolgreich in aktualisiert MISP Server.

4. Klicken Sie Auf **Formular Neu Laden** In der Erfolgsmeldung, um die Änderungen im Datensatz anzuzeigen.

Rollup durchführen MITRE-ATT&CK Informationen mit MISP Ergänzungsergebnisse

Führen Sie ein manuelles Rollup der MISP-Ergänzungsergebnisse durch, wenn Sie das automatische Rollup von nicht aktiviert haben MISP Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

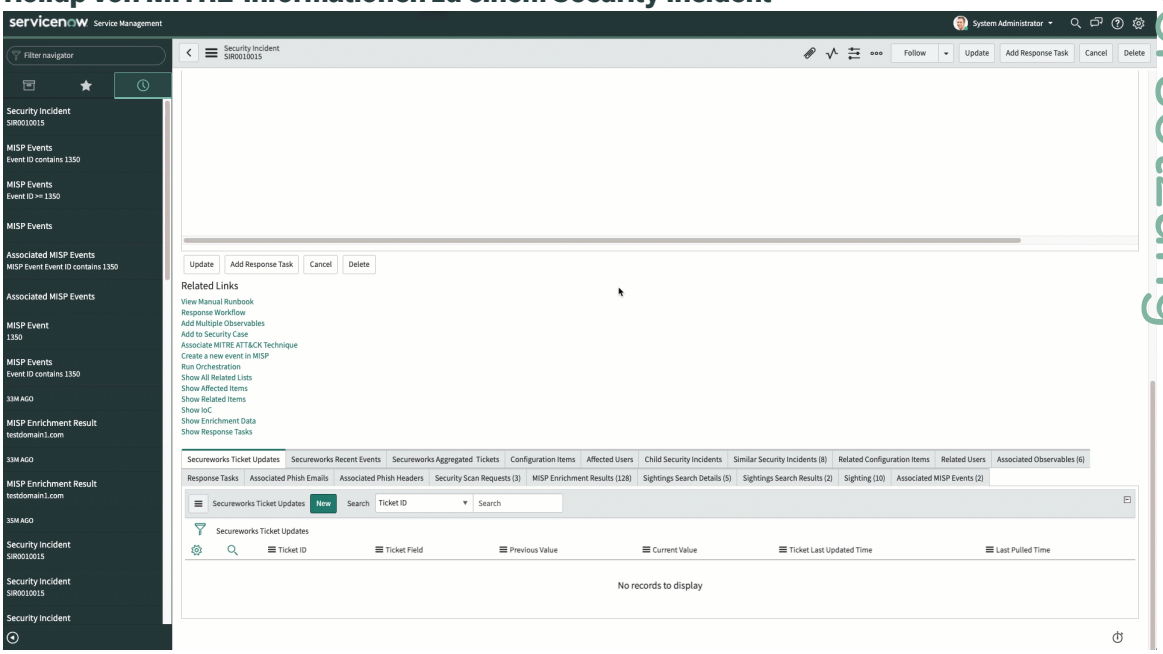
Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie die automatischen Extraktionsregeln des Basissystems, um zu importieren MITRE-ATT&CK Informationen aus dem MISP Integration. Die MISP integration for Security Operations Führt zwei Basissysteme ein MITRE-ATT&CK Extraktionsregeln für Technik für MISP– MISP Galaxien und MISP Tags. Weitere Informationen zu Regeln für automatische Extraktion finden Sie in MITRE-ATT&CK, Siehe Technische Regeln für den Import von MITRE-ATT&CK-Informationen automatisch extrahieren .

Wenn Sie aktiviert haben Automatischer Rollup von MITRE-ATT&CK Informationen mit MISP Ergänzungsergebnisse Für einen Security Incident werden die Informationen automatisch zusammengefasst. Wenn Sie das automatische Rollup nicht aktiviert haben, können Sie diese Aufgabe manuell ausführen.

Prozedur
1. Navigieren zu **Alle** > **Security Incidents** > **Alle Incidents anzeigen**an.
2. Wählen Sie den Security Incident aus, den Sie mit anreichern möchten MITRE-ATT&CK Informationen.
3. Klicken Sie Auf **Alle Zugehörigen Listen Anzeigen** Und **MISP-Anreicherungsergebnisse** Registerkarte.
4. Wählen Sie das erkennbare Element aus, und klicken Sie im Menü Aktionen auf **Rollup der MITRE ATT&CK-Informationen zu SI** .
   Sie können mehrere erkennbare Elemente auswählen und dann einen Rollup der Informationen durchführen.
5. Klicken Sie auf , um die Änderungen zu bestätigen **Neu Laden** .
   Das folgende Beispiel zeigt, wie ein erkennbares Element ausgewählt und ein Rollup durchgeführt wird MISP Ergänzungsergebnisse zum Security Incident.

Rollup von MITRE-Informationen zu einem Security Incident



Ergebnisse
Sie können anzeigen MITRE-ATT&CK Karte, um zu bestätigen, dass die MISP-Anreicherungsergebnisse für den Security Incident zusammengefasst wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OPSWAT-Metadefender-Integration

OPSWAT Metadefender Ermöglicht das Herunterladen von Bedrohungsdaten, die vom Metadefender-Scanner der Drittpartei erkannt wurden, in den Threat Intelligence Anwendung für Nachverfolgung, Priorisierung und Lösung.

Erkunden	Einrichtung
• Integrationsüberblick OPSWAT Metadefender • Threat Intelligence-Integrationen	Aktivieren und konfigurieren Sie OPSWAT Metadefender Integration
Verwenden	**Entwickeln**
Führen Sie Suchen nach erkennbaren Elementen durch	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie Komponenten, die mit einer Anwendung installiert sind
Problembehandlung und Hilfe	
• Problembehandlung bei der Integration • Stellen oder beantworten Sie Fragen in der Security Operations-Community • Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen • Kontakt Kundenservice und Support	

Integrationsüberblick OPSWAT Metadefender

OPSWAT Metadefender Ist eine Sicherheitslösung, die Zugriff auf mehrere Anti-Malware-Computer bietet und problemlos in integriert werden kann Security Operations.

Bevor Sie verwenden können OPSWAT Metadefender Integration müssen Sie das Plugin aktivieren und die Integration konfigurieren. Bei Bedarf können Sie auch Ihre X509-SSL-Zertifizierung aktualisieren.

Bedrohungssuche: OPSWAT-Metadefender-Flow

Der Flow „Bedrohungssuche – OPSWAT-Metadefender“ führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn die erkennbaren Elemente von einem Typ sind, der von OPSWAT Metadefender erkannt wird, werden die erkennbaren Elemente auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

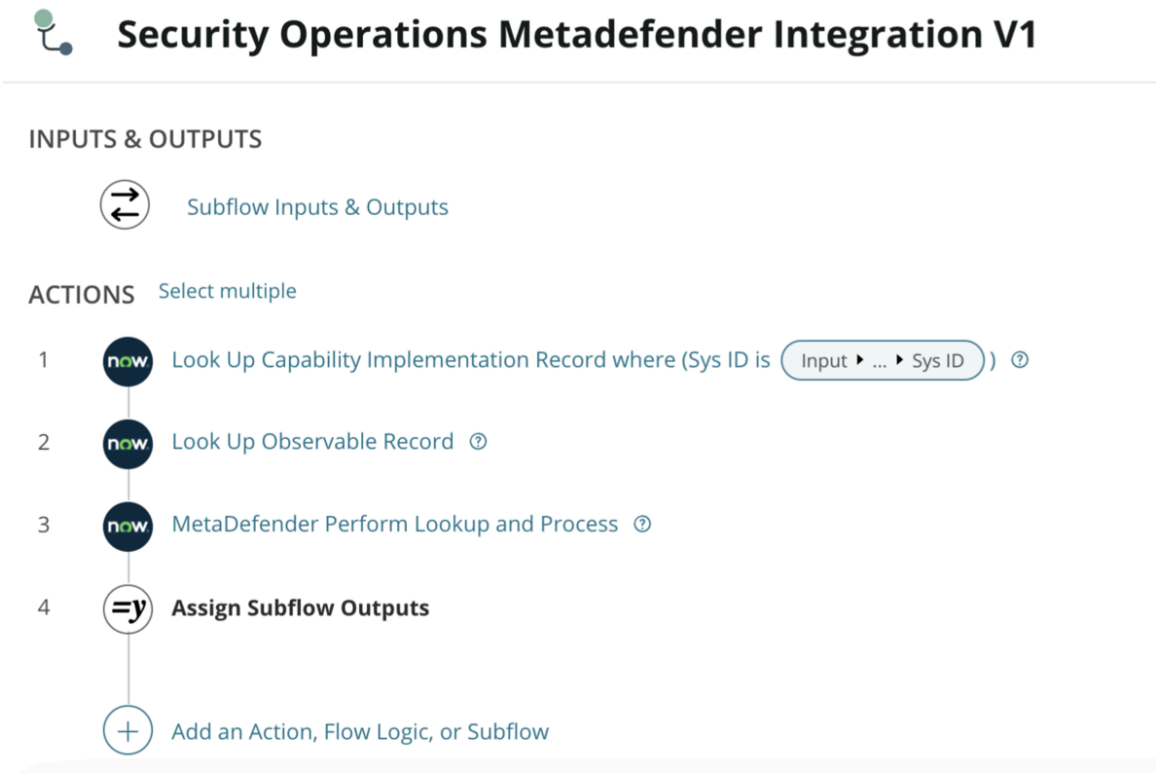
Dieser Flow wird durch ausgelöst Integration von Security Operations: Fähigkeit zur Bedrohungssuche Wenn Sie eine Bedrohungssuche für ein oder mehrere erkennbare Elemente durchführen und die OPSWAT-Metadefender-Implementierung ausgewählt ist. Weitere Informationen finden Sie unter Führen Sie Suchen nach erkennbaren Elementen durch.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_si.admin

Bedrohungssuche: OPSWAT-Metadefender-Flow



Informationen zu den von diesem Flow verwendeten Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Aktivieren und konfigurieren Sie OPSWAT Metadefender Integration

Bevor Sie verwenden können OPSWAT Metadefender Integration müssen Sie sie aus herunterladen ServiceNow Store.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Wenn die Integration abgeschlossen ist, greifen Sie auf das OPSWAT-Portal zu, und erhalten Sie den Metadefender Cloud API-Schlüssel
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationen** > **Integrationskonfiguration**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. Klicken Sie in der Karte OPSWAT-Metadefender auf **Konfigurieren** .
5. Geben Sie ein (oder fügen Sie ein) **API-Schlüssel** Sie haben über das OPSWAT-Portal erworben.
6. Klicken Sie auf **Absenden**.

Ergebnisse

Nach der Konfiguration kann OPSWAT-Metadefender ausgewählt werden, um Suchen nach erkennbaren Elementen in durchzuführen Threat Intelligence Und für erkennbare Elemente in Security Incidents.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Führen Sie Suchen nach erkennbaren Elementen durch

Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie eine SSL-Verbindung für die Integration benötigen, gibt es Umstände, in denen das vom Drittanbieter bereitgestellte Zertifikat entweder noch nicht vertrauenswürdig ist ServiceNow Oder ist abgelaufen. Diese Aufgabe ist optional.

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Erwerben Sie das SSL-Zertifikat vom Drittanbieter.
   Sie können beispielsweise ein X.509-Zertifikat (PEM) von einem SSL-Endpunkt im Firefox-Browser wie folgt importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/` .

   b. Klicken Sie auf das Schlosssymbol in der Adresszeile.

   c. Klicken Sie Auf **Weitere Informationen** Und klicken Sie auf **Sicherheit** Registerkarte.

   d. Klicken Sie Auf **Zeigen Sie Das Zertifikat An** Und klicken Sie auf **Detail** Registerkarte.

   e. Klicken Sie Auf **Exportieren** Um das PEM in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor-Tool, und kopieren Sie den Inhalt in die Zwischenablage.
   Sie muss mit beginnen `----- ZERTIFIKAT BEGINNEN------` Und enden mit `----- ENDZERTIFIKAT-----` .

2. Navigieren zu **Systemdefinition** > **Zertifikate**an.
3. Klicken Sie Auf **Neu** Und Erstellen Sie einen neuen Datensatz Für die Integration.
4. In **PEM-Zertifikat** , Fügen Sie das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.
   a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an.
   b. Wählen Sie den aktiven Standard-Identitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.
   c. Scrollen Sie nach unten zu **X.509-Zertifikate** Zugehörige Liste, und klicken Sie auf **Bearbeiten** .
   d. Verschieben Sie das neu erstellte Zertifikat in **Ausgewählt** Spalte.
6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

Hinweis:
Wenn Sie ein abgelaufenes Zertifikat haben, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 ersetzt ein ablaufendes SAML-Zertifikat .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integration mit VirusTotal

Die VirusTotal Mit der Integration können Sie die Analyse verdächtiger IP-Adressen, Dateien, Datei-Hashes und URL-Adressen anfordern, um Ihre Untersuchung zu unterstützen und festzustellen, ob sie böswillig sind.

Erkunden	Einrichten
Threat Intelligence-Integrationen	• VirusTotal Integrationen-Setup • Aktivieren und konfigurieren Sie die VirusTotal-Integration
Verwenden	**Entwickeln**
• Führen Sie Suchen nach erkennbaren Elementen durch • Bedrohungssuche: VirusTotal-Workflow	• ServiceNow Security Operations Richtlinien für die Integrationsentwicklung • Tipps zum Schreiben von Integrationen • Entwicklerschulungen • Entwicklerdokumentation • Suchen Sie Komponenten, die mit einer Anwendung installiert sind
Problembehandlung und Hilfe	
• Problembehandlung bei der Integration • Stellen oder beantworten Sie Fragen in der Security Operations-Community • Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen • Kontakt Kundenservice und Support	

VirusTotal Integrationen-Setup

VirusTotal Ist ein kostenloser Service, der verdächtige Dateien und URLs analysiert und die schnelle Erkennung von Viren, Würmern, Trojans und allen Arten von Malware erleichtert. Es lässt sich problemlos in integrieren Security Operations.

Bevor Sie verwenden können VirusTotal Integration müssen Sie das Plugin aktivieren und den entsprechenden API-Schlüssel hinzufügen. Bei Bedarf können Sie auch Ihre X509-SSL-Zertifizierung aktualisieren.

Wenn VirusTotal Die Suchquelle wird verwendet, und es wird Malware gefunden. Ein erkennbares Element wird erstellt. Für IP-Suchen wird eine zusätzliche Liste von URLs erstellt, die die IP-Adresse teilen, und erkennbare Elemente werden für jede der URLs erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Die Threat Intelligence Plugin ist für die Implementierung erforderlich VirusTotal Integration.
- Die VirusTotal Die Integration wurde auf APIs der Version 3 aktualisiert.

Aktivieren und konfigurieren Sie die VirusTotal-Integration

Bevor Sie die VirusTotal-Integration verwenden können, müssen Sie sie aus dem herunterladen ServiceNow Store.

Vorbereitungen

Erforderliche Rolle: Administrator

Threat Intelligence Muss installiert und aktiviert sein, bevor Sie VirusTotal verwenden können.
Die VirusTotal Die Integration wurde auf APIs der Version 3 aktualisiert.

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Wenn die Installation abgeschlossen ist, greifen Sie auf VirusTotal zu, und rufen Sie den API-Schlüssel unter Ihrem VirusTotal-Profil ab.
3. Navigieren Sie in Ihrer Instanz zu **Security Operations** > **Integrationskonfiguration**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
4. Klicken Sie in der Karte VirusTotal auf **Konfigurieren** .

Virustotal-Konfiguration

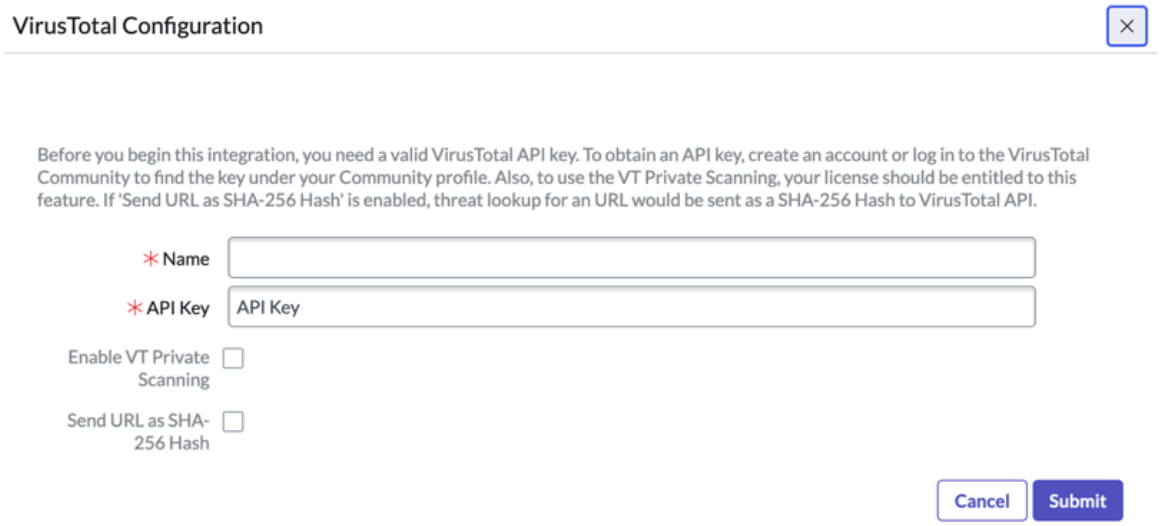
Feld	Beschreibung
Name	Name der Integration Beispiel: VirusTotal.
API-Schlüssel	Geben Sie ein (oder fügen Sie ein) **API-Schlüssel** Sie haben von der VirusTotal-Website erworben.
VT Private Scanning aktivieren	Aktivieren Sie dieses Kontrollkästchen, um Dateien mit VirusTotal datenschutzgeschützt zu analysieren. Die über dieses Angebot hochgeladenen Dateien werden für niemanden außerhalb Ihrer Organisation freigegeben und bleiben nur für einen kurzen Zeitraum in VirusTotal. Die resultierenden Analysen sind ebenfalls flüchtig und nur für Ihre VirusTotal-Gruppe sichtbar. **Wichtig:** Zur Verwendung des privaten VT-Scans sollte Ihre VirusTotal-Lizenz berechtigt sein, diese Funktion zu nutzen.
URL als SHA-256-Hash senden	Aktivieren Sie dieses Kontrollkästchen, um die URLs als Hashes für die Bedrohungssuche zu senden und die Privatsphäre der Anwender in der Integration zu schützen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn diese Option deaktiviert ist, wird die URL als Base64-Codierung an die VirusTotal-API gesendet.

5. Klicken Sie auf **Absenden**.



Ergebnisse

Nach der Konfiguration kann VirusTotal ausgewählt werden, um Suchen nach erkennbaren Elementen in durchzuführen Threat Intelligence Und für erkennbare Elemente in Security Incidents.

Zugehörige Informationen

Führen Sie Suchen nach erkennbaren Elementen durch

Bedrohungssuche: VirusTotal-Workflow

Die Bedrohungssuche – VirusTotal Der Workflow führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn die erkennbaren Elemente von einem Typ sind, der von erkannt wurde VirusTotal, Die erkennbaren Elemente werden auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

Vorbereitungen

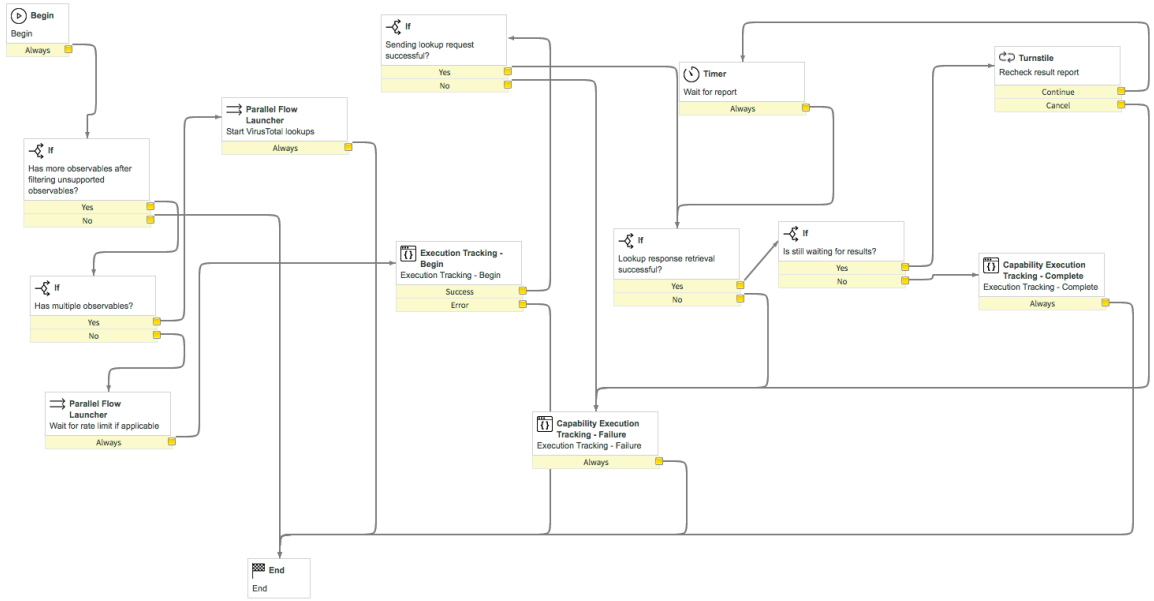
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Dieser Workflow wird durch ausgelöst Integration von Security Operations: Fähigkeit zur Bedrohungssuche Wenn Sie eine Bedrohungssuche für ein oder mehrere erkennbare Elemente durchführen, und VirusTotal Implementierung ist ausgewählt. Weitere Informationen finden Sie unter Führen Sie Suchen nach erkennbaren Elementen durch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungssuche: VirusTotal-Workflow



Informationen zu den von diesem Workflow verwendeten Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

WhoisXML-API-Integration

Mit der WhoisXML-API-Integration können Sie Whois-Suchen nach Domänennamen und URLs übermitteln, um Kontext zu erkennbaren URL-Elementen zu erhalten und Bedrohungen besser zu bestimmen.

Erkunden

Threat Intelligence-Integrationen

Einrichten

- Setup der WhoisXML-API-Integration
- Aktivieren und konfigurieren Sie die Integration von Security Operations Whois

---

Verwenden

Threat Intelligence – Workflow für IOC-Suche ausführen

Entwickeln

- ServiceNow Security Operations Richtlinien für die Integrationsentwicklung
- Tipps zum Schreiben von Integrationen
- Entwicklerschulungen
- Entwicklerdokumentation
- Suchen Sie Komponenten, die mit einer Anwendung installiert sind

---

Problembehandlung und Hilfe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Fortsetzung)

- Problembehandlung bei der Integration
- Stellen oder beantworten Sie Fragen in der Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Setup der WhoisXML-API-Integration

Bevor Sie die Whois-Integration verwenden können, müssen Sie das Plugin aktivieren und die Anmeldeinformationen hinzufügen. Bei Bedarf können Sie auch Ihre X509-SSL-Zertifizierung aktualisieren.

Die Threat Intelligence Und WhoisXML API Integration-Plugins sind erforderlich, um die WhoisXML API-Integration zu implementieren.

Aktivieren und konfigurieren Sie die Integration von Security Operations Whois

Mit der Integrationskonfigurationsfunktion können Sie Sicherheitsintegrationen von Drittparteien schnell aktivieren und einrichten, einschließlich der Integration von Security Operations Whois. Bevor Sie die Integration von Security Operations Whois verwenden können, müssen Sie sie aus dem herunterladen ServiceNow Store, Und Sie müssen über einen gültigen Account von der WhoisXML-API verfügen.

Vorbereitungen

Threat Intelligence Muss installiert und aktiviert sein, bevor Sie die Security Operations Whois-Integration verwenden können.

Erforderliche Rolle: Administrator

Prozedur

1. Laden Sie die Integration aus dem herunter ServiceNow Storean.
2. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Security Operations** > **Integrationskonfiguration**an.
   Die verfügbaren Sicherheitsintegrationen werden als Reihe von Karten angezeigt.
3. Klicken Sie in der Whois-API-Karte auf **Konfigurieren** .
4. Geben Sie den Anwendernamen und das Passwort aus Ihrem WhoisXML-API-Account ein.
5. Klicken Sie auf **Absenden**.

Aktualisieren Sie Ihr X.509-Zertifikat

Wenn Sie eine SSL-Verbindung für die Integration benötigen, gibt es Umstände, in denen das vom Drittanbieter bereitgestellte Zertifikat entweder noch nicht vertrauenswürdig ist ServiceNow Oder ist abgelaufen. Diese Aufgabe ist optional.

Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erwerben Sie das SSL-Zertifikat vom Drittanbieter.
   Sie können beispielsweise ein X.509-Zertifikat (PEM) von einem SSL-Endpunkt im Firefox-Browser wie folgt importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/` .

   b. Klicken Sie auf das Schlosssymbol in der Adresszeile.

   c. Klicken Sie Auf **Weitere Informationen** Und klicken Sie auf **Sicherheit** Registerkarte.

   d. Klicken Sie Auf **Zeigen Sie Das Zertifikat An** Und klicken Sie auf **Detail** Registerkarte.

   e. Klicken Sie Auf **Exportieren** Um das PEM in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor-Tool, und kopieren Sie den Inhalt in die Zwischenablage.
   Sie muss mit beginnen `----- ZERTIFIKAT BEGINNEN------` Und enden mit `-----ENDZERTIFIKAT-----` .

2. Navigieren zu **Systemdefinition** > **Zertifikate**an.
3. Klicken Sie Auf **Neu** Und Erstellen Sie einen neuen Datensatz Für die Integration.
4. In **PEM-Zertifikat** , Fügen Sie das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Fügen Sie das Zertifikat dem Identitätsanbieter-Datensatz hinzu.
   a. Navigieren zu **Mehrfachanbieter-SSO** > **Identity Provider**an.
   b. Wählen Sie den aktiven Standard-Identitätsanbieter aus, für den Sie das neue Zertifikat erstellt haben.
   c. Scrollen Sie nach unten zu **X.509-Zertifikate** Zugehörige Liste, und klicken Sie auf **Bearbeiten** .
   d. Verschieben Sie das neu erstellte Zertifikat in **Ausgewählt** Spalte.
6. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

Hinweis:
Wenn Sie ein abgelaufenes Zertifikat haben, müssen Sie es entfernen. Informationen zum Entfernen des abgelaufenen Zertifikats finden Sie unter KB0691439 ersetzt ein ablaufendes SAML-Zertifikat .

Bereichern Sie den WHOIS-Workflow erkennbarer Elemente

Die **Bereichern Sie WHOIS des erkennbaren Elements** Der Workflow führt eine Ergänzung für ausgewählte erkennbare Elemente durch. Wenn die erkennbaren Elemente vom Typ sind, der von erkannt wird WhoisXML-API-Integration, Die erkennbaren Elemente werden bereichert.

Vorbereitungen

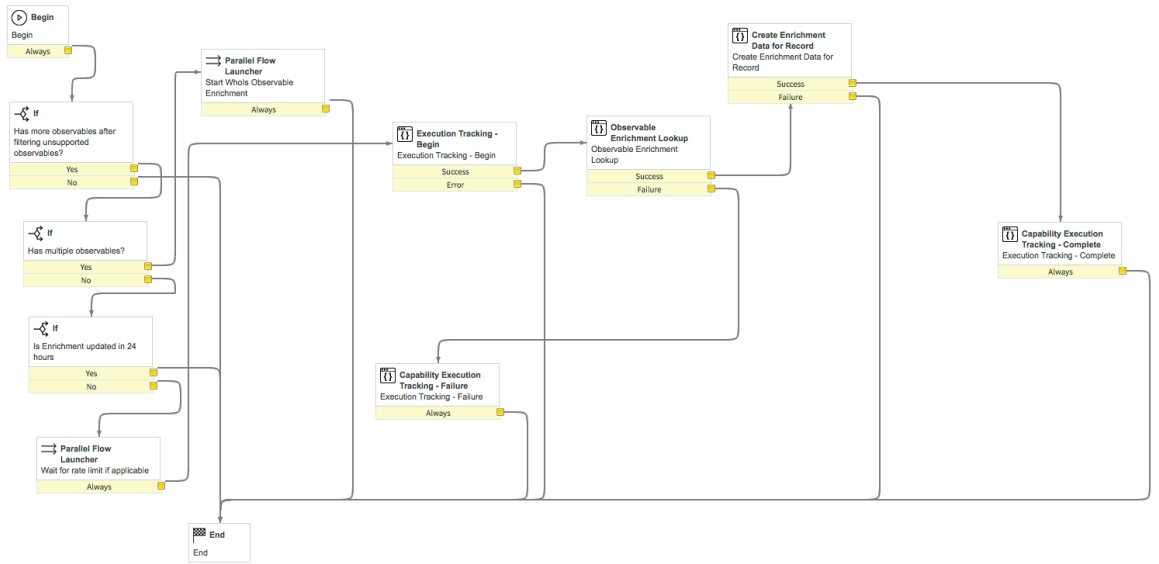
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Dieser Workflow wird durch ausgelöst Integration von Security Operations: Bereichern Sie die Fähigkeit erkennbarer Elemente Wenn Sie eine Ergänzung für ein oder mehrere erkennbare Elemente durchführen und die WHOIS-Implementierung ausgewählt ist.

Bereichern Sie den WHOIS-Workflow erkennbarer Elemente



Aktivitäten, die für diese Integration spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Suchaktivität für Ergänzung erkennbarer Elemente

Die **Suche Nach Ergänzung Erkennbarer Elemente** Workflow-Aktivität initiiert den Ergänzungsprozess erkennbarer Elemente.

Die **Suche Nach Ergänzung Erkennbarer Elemente** Die Aktivität kann mit jedem Workflow erkennbarer Elemente verwendet werden, um mit der Anreicherung zu beginnen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Die Suche ist erfolgreich.
Fehlgeschlagen	Beim Versuch, die Suche durchzuführen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
Implementierungs-ID	Systembezeichner der Implementierung, die zum Durchführen der Suche verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
domain_id	Der Domänenbezeichner für die Domäne, in der die Suche ausgeführt wird.
Erkennbare_IDs	Mindestens ein erkennbares Element, für das die gewünschte Aktion ausgeführt werden soll. Die IDs werden als Workflow-Eingabe verwendet.
CapabilityExcutionId	Systembezeichner der Fähigkeit, die den Implementierungs-Workflow gestartet hat. Nur erforderlich für Implementierungs-Workflows der Integrationsfähigkeit wie Splunk, Elasticsearch.
task_sys_id	Systembezeichner für jede Aufgabe, die dem Workflow zugeordnet ist.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Response_Data	Rohdaten, die vom API-Endpunkt der Implementierung für die angegebene Domäne zurückgegeben werden.
mapping_id	Der Bezeichner für die Ergänzungszuordnung. Beispielsweise gibt die WHOIS-Integration Daten in zwei verschiedenen Formaten zurück, IP und URL, mit jeweils einer Zuordnungs-ID.

Threat Intelligence Orchestration

Threat Intelligence Orchestration Mit Aktivitäten können Anwender mithilfe von Workflow-Orchestration bestimmen, ob eine Bedrohung bereits in anderen Security Incidents oder auf anderen Systemen erkannt wurde.

Für weitere Informationen zum Bearbeiten Security Incident Response Orchestration Workflows oder das Erstellen anwenderdefinierter Workflows finden Sie unter Erste Schritte mit Workflows Und Workflow-Editor Workflow-Editor .

Richten Sie Threat Intelligence Orchestration ein

Vor der Verwendung Threat Intelligence Orchestration, Führen Sie Schritte zum Einrichten verschiedener Teile des Systems aus, einschließlich Ausfüllen der CMDB, Konfigurieren des MID-Servers und Konfigurieren von Anmeldeinformationen.

Vorbereitungen

Erforderliche Rolle: Administrator

Zu verwenden Threat Intelligence Orchestration Sie benötigen eine vollständig ausgefüllte CMDB mit Domänennamen. Weitere Informationen finden Sie unter Discovery .

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Aktivieren Sie das Threat Intelligence Plugin.
2. Konfigurieren Sie den MID-Server
3. Konfigurieren Sie die Anmeldeinformationen für den MID-Server
   Sie sind jetzt bereit zur Verwendung Threat Intelligence Orchestration Aktivitäten in einem Workflow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence Orchestration-Workflows und -Aktivitäten

Das Basissystem enthält Workflows und Workflow-Aktivitäten, mit denen Sie Aktionen in Ihrer Instanz automatisieren können.

Threat Intelligence – Workflow für IOC-Suche ausführen

Die **Threat Intelligence – IOC-Suche ausführen** Der Workflow überprüft, ob ein nicht abgelaufenes erkennbares Element vorhanden ist. Wenn dies der Fall ist, wird die Suche auf festgelegt **Abgeschlossen** Und mit den Daten aus dem erkennbaren Element aktualisiert.

Vorbereitungen

Erforderliche Rolle: sn_si.Basic

Hinweis:

Dieser Workflow ersetzt Threat Intelligence Orchestration Business-Regeln (**Füllen Sie vorhandene IOC-Tabellen aus** , **Suche in Warteschlange stellen** , Und **Erkennbares Element aktualisieren**) Mit Aktivitäten.

Wenn eine Suche eingefügt oder aktualisiert wird und die Bedingungen erfüllt, löst die Business-Regel „Suchen“ diesen Workflow aus.

Warum und wann dieser Vorgang ausgeführt wird

Die **Threat Intelligence – IOC-Suche ausführen** Der Workflow überprüft, ob ein nicht abgelaufenes erkennbares Element vorhanden ist. Wenn dies der Fall ist, wird die Suche auf festgelegt **Abgeschlossen** Und mit den Daten aus dem erkennbaren Element aktualisiert. Alle Indikatoren, die dem erkennbaren Element zugeordnet sind, werden erneut aktiviert.

Wenn das erkennbare Element abgelaufen ist, führt der Workflow die Suchvorgänge aus und erhöht den **Sichtungsanzahl** Im vorhandenen abgelaufenen erkennbaren Element.

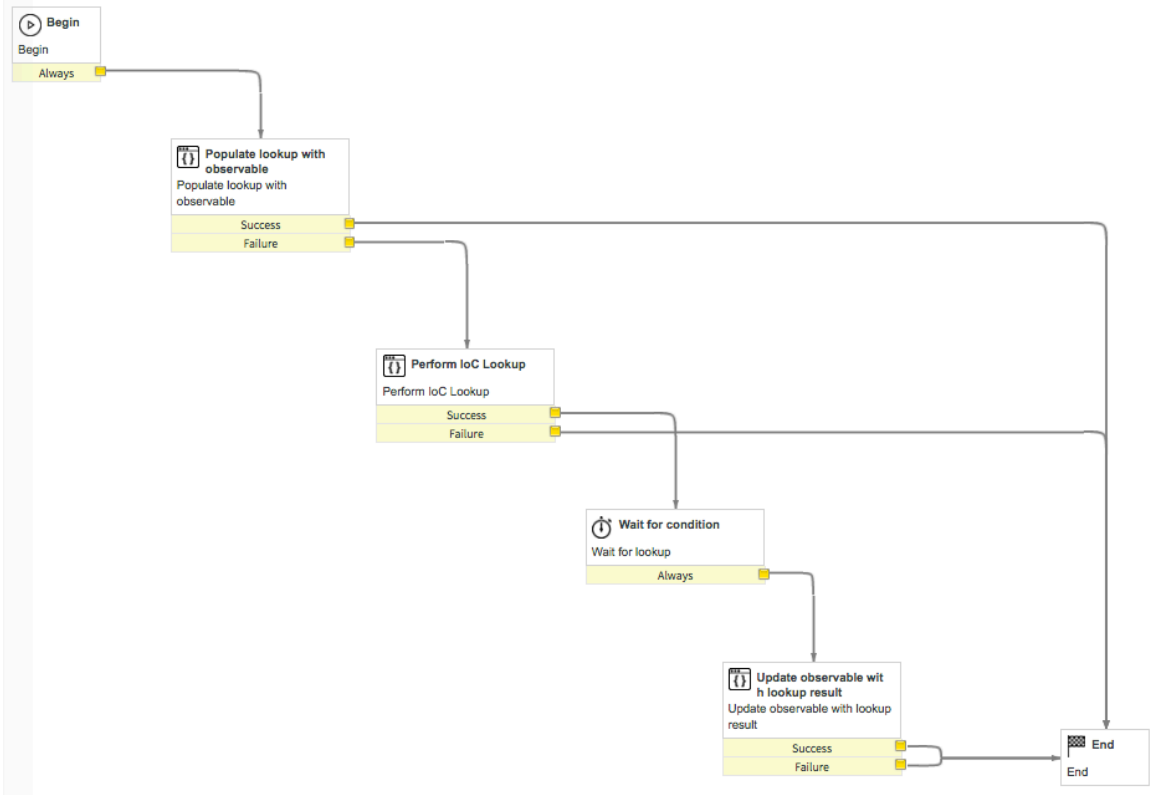
Wenn kein korrelierendes erkennbares Element vorhanden ist, wird ein neues erkennbares Element mit Indikator erstellt.

Workflow-Prozessaktivitäten umfassen:

- Füllen Sie die Suche mit Aktivität des erkennbaren Elements aus
- IOC-Suchaktivität durchführen
- Auf Suche warten (Kernaktivität)
- Aktualisieren Sie das erkennbare Element mit der Aktivität „Suchergebnis“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence: Führen Sie den IOC-Suchworkflow aus



Füllen Sie die Suche mit Aktivität des erkennbaren Elements aus

Wenn ein nicht abgelaufenes erkennbares Element gefunden wird, wird **Threat Intelligence Orchestration: Füllen Sie die Suche mit erkennbarem Element aus** Workflow-Aktivität stellt Daten aus einem vorhandenen erkennbaren Element für eine Suche bereit. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Wenn durch einen Workflow ausgelöst **Füllen Sie die Suche mit erkennbarem Element aus** Versucht, ein vorhandenes erkennbares Element für eine Suche zu finden, die mit übereinstimmt **Wert** Und **Typ** Der Suche, die für die Aktivität als Eingabe bereitgestellt wurde.

Wenn das erkennbare Element vorhanden ist und nicht abgelaufen ist, wird diese Aktivität:

- Aktualisiert die Suche mit den im erkennbaren Element gefundenen Informationen
- Reaktiviert einen Indikator, wenn er inaktiv ist, erhöht den **Aufgetretene Anzahl** , Und aktualisiert **Zuletzt gesehen** Datum
- Legt Fest **Status** Zum Abschließen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen	Beschreibung
Scan-ID[Zeichenfolge]	Suchbezeichner

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen	Beschreibung
True	Gültiges erkennbares Element gefunden und Suche aktualisiert.
Falsch	Es wurde kein gültiges erkennbares Element gefunden. Erkennbares Element fehlt oder ist abgelaufen.

IOC-Suchaktivität durchführen

Die **Threat Intelligence Orchestration: IOC-Suche durchführen** Die Workflow-Aktivität führt eine bestimmte Suche durch. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Wenn durch einen Workflow ausgelöst, **IOC-Suche durchführen** Verwendet eine Scan-ID, sucht nach dem Suchdatensatz und fügt die Suche der Warteschlange hinzu, indem ein Suchwarteschlangeneintrag erstellt wird.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Scan-ID[Zeichenfolge]	Suchbezeichner

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
True	Hat die Suche ausgelöst.
Falsch	Die Suche wurde nicht ausgelöst.

Aktualisieren Sie das erkennbare Element mit der Aktivität „Suchergebnis“

Die **Threat Intelligence Orchestration: Aktualisieren Sie das erkennbare Element mit dem Suchergebnis** Die Workflow-Aktivität aktualisiert den Datensatz des erkennbaren Elements. Wenn eines nicht vorhanden ist, wird ein neues erkennbares Element erstellt. Diese Aktivität ist nützlich für die Protokollierung von Informationen.

Wenn durch einen Workflow ausgelöst **Aktualisieren Sie das erkennbare Element mit dem Suchergebnis** Aktualisiert ein vorhandenes erkennbares Element, um das neue einzubeziehen **Sichtungsanzahl** , Fügt eine Notiz hinzu und aktiviert, falls inaktiv, alle Indikatoren erneut. Die **Aufgetretene Anzahl** Und **Zuletzt gesehen** Das Datum im Indikator wird ebenfalls aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn kein korrelierendes erkennbares Element vorhanden ist, erstellt der Workflow ein neues erkennbares Element mit Indikator wie folgt:

- Führt die IOC-Suchen aus
- Erstellt ein neues erkennbares Element
- Erstellt einen Indikator für das erkennbare Element
- Fügt ein hinzu **Sichtungsanzahl** Zum erkennbaren Element
- Fügt ein hinzu **Aufgetretene Anzahl** Und **Zuletzt gesehen** Datum für den Indikator
- Fügt eine Nachricht hinzu, die angibt, aus welcher Suche sie erstellt wurde

an.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Scan-ID[Zeichenfolge]	Suchbezeichner.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
True	Aktualisierung oder Erstellung des erkennbaren Elements ist erfolgreich.
Falsch	Fehler beim Aktualisieren oder Erstellen des erkennbaren Elements.

Führen Sie die Aktivität „Standard-IOC-Suchquellen“ aus

Wenn durch einen Workflow ausgelöst, Threat Intelligence– **Führen Sie Standard-IOC-Suchquellen aus** Nimmt eine Suchanforderungs-ID auf und erstellt je nach eingegebenen Datenwerten mehrere Suchvorgänge.

Für jeden Datentyp die **Include_in_Bulk-Scan** Die Spalte der unterstützten Suchtyptabelle jeder Suchquelle wird ausgewertet. Bei „wahr“ wird der Suchanforderung eine Suche hinzugefügt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Scan_Request_ID	Bezeichner des Suchanforderungssystems

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Anzahl der erstellten Scans	Ganzzahl

Security Case Management

Management von Sicherheitsfällen Bietet Sicherheitsanalysten, die an der Bedrohungssuche beteiligt sind, eine Möglichkeit, Informationen zu verdächtigen Aktivitäten in ihrer Umgebung zu sammeln. Fallbezogene Datensätze wie Security Incidents, erkennbare Elemente, Cls und betroffene Anwender können Fällen hinzugefügt werden, um umfassende und spezifische Analysen zu ermöglichen.

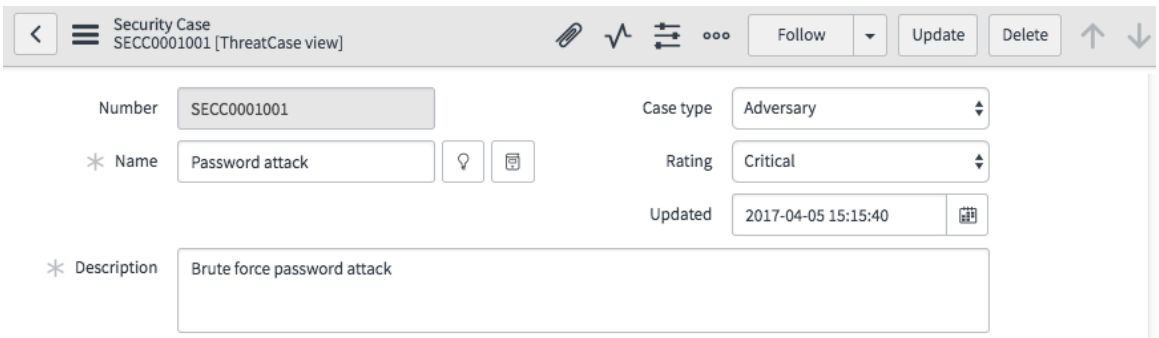
Mit der Möglichkeit, die Datensätze und zugehörigen Informationen einfach durchlaufen zu können, können Analysten bewerten, ob sie mit einer gezielten Kampagne, einer erweiterten persistenten Bedrohung usw. konfrontiert sind.

Sicherheitsfälle können aus verschiedenen Quellen in Ihrer Instanz erstellt werden, einschließlich Management von Sicherheitsfällen, Security Incident Response, Und Threat Intelligence. Sie können Fälle auch aus Konfigurationselementen und betroffenen Anwendern in den Tabellen Konfigurationselemente [cmdb.ci] und Anwender [sys.user] erstellen. Nachdem Fälle erstellt wurden, kann jede dieser Quellen auch verwendet werden, um vorhandenen Fällen wertvolle Analyseressourcen hinzuzufügen.

Jeder Sicherheitsfall besteht aus drei Hauptabschnitten, einem Header-Abschnitt, einem Abschnitt mit zusätzlichen Falldetails und einem Fallartefaktabschnitt, der eine Sammlung von Datensätzen enthält, die beim Erstellen eines Arguments für die Identifizierung und den Umgang mit bestimmten Bedrohungen helfen.

Fall-Header

Fall-Header-Abschnitt

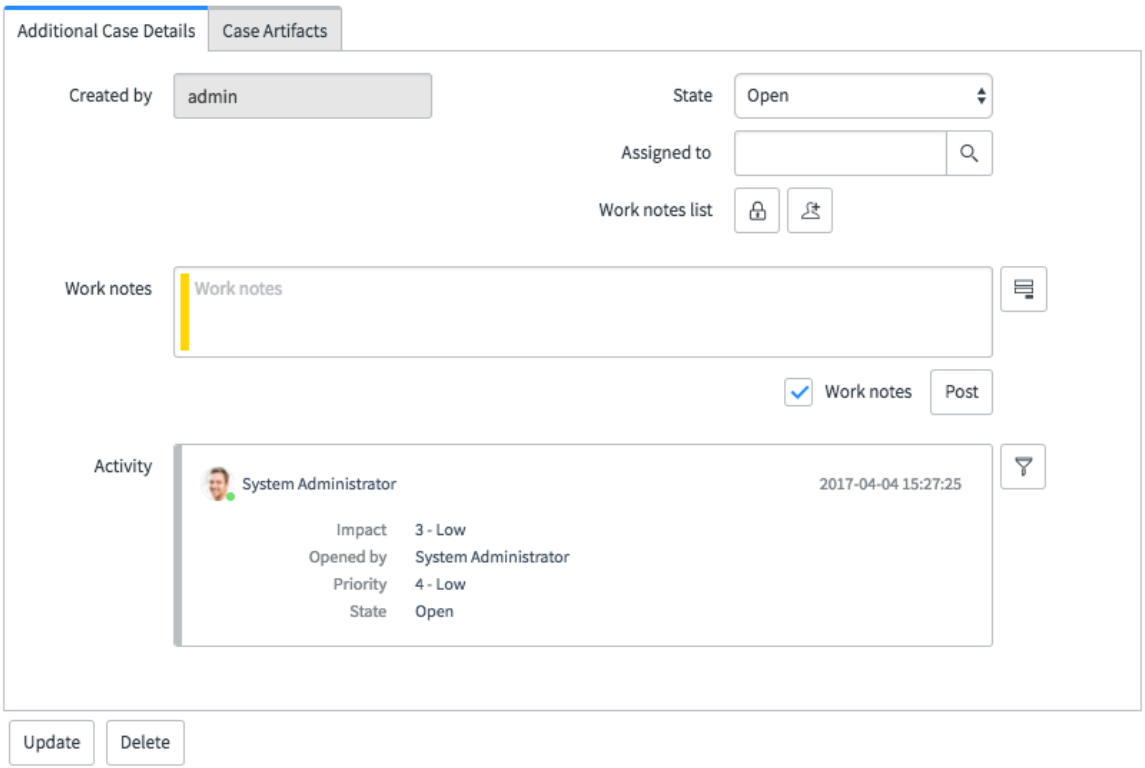


Der Fallheader enthält grundlegende Informationen, die zum Identifizieren und Klassifizieren des Sicherheitsfalls verwendet werden. Die Fallnummer verwendet das SECC-Präfix.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Falldetails

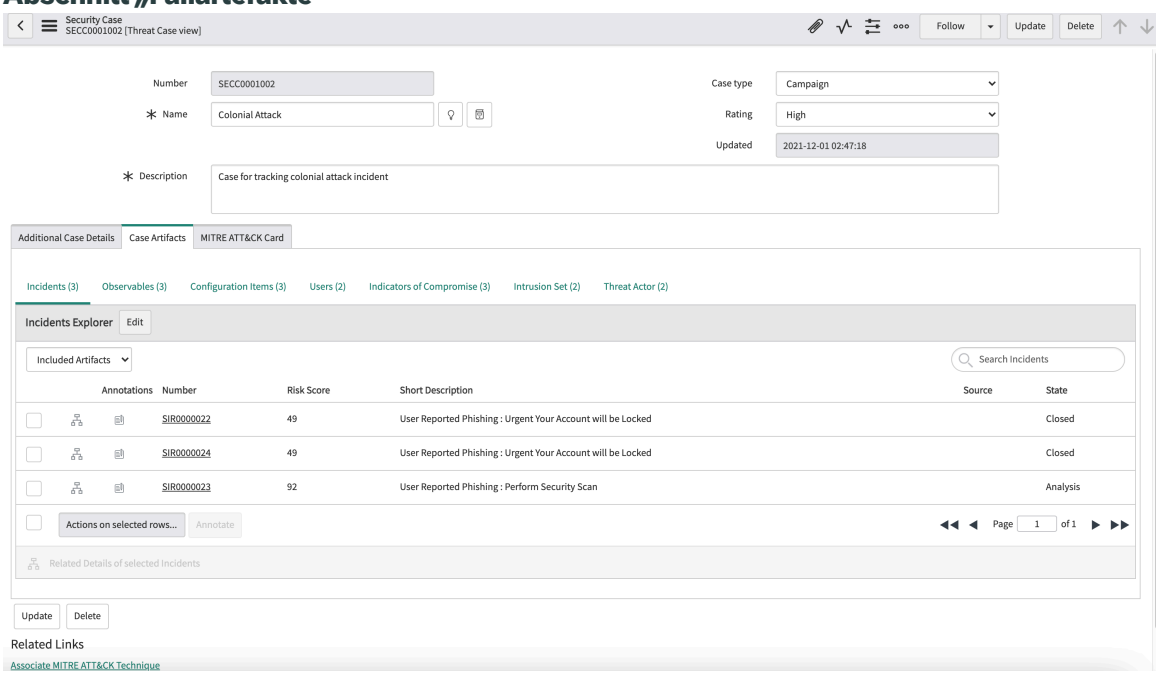
Abschnitt „zusätzliche Falldetails“



Die **Zusätzliche Falldetails** Abschnitt enthält spezifische Informationen für die Analyse, die bereits für den Fall durchgeführt wurde, einschließlich des aktuellen Status und der für den Fall aufgezeichneten Arbeitsnotizen und Aktivitäten.

Fallartefakte

Abschnitt „Fallartefakte“



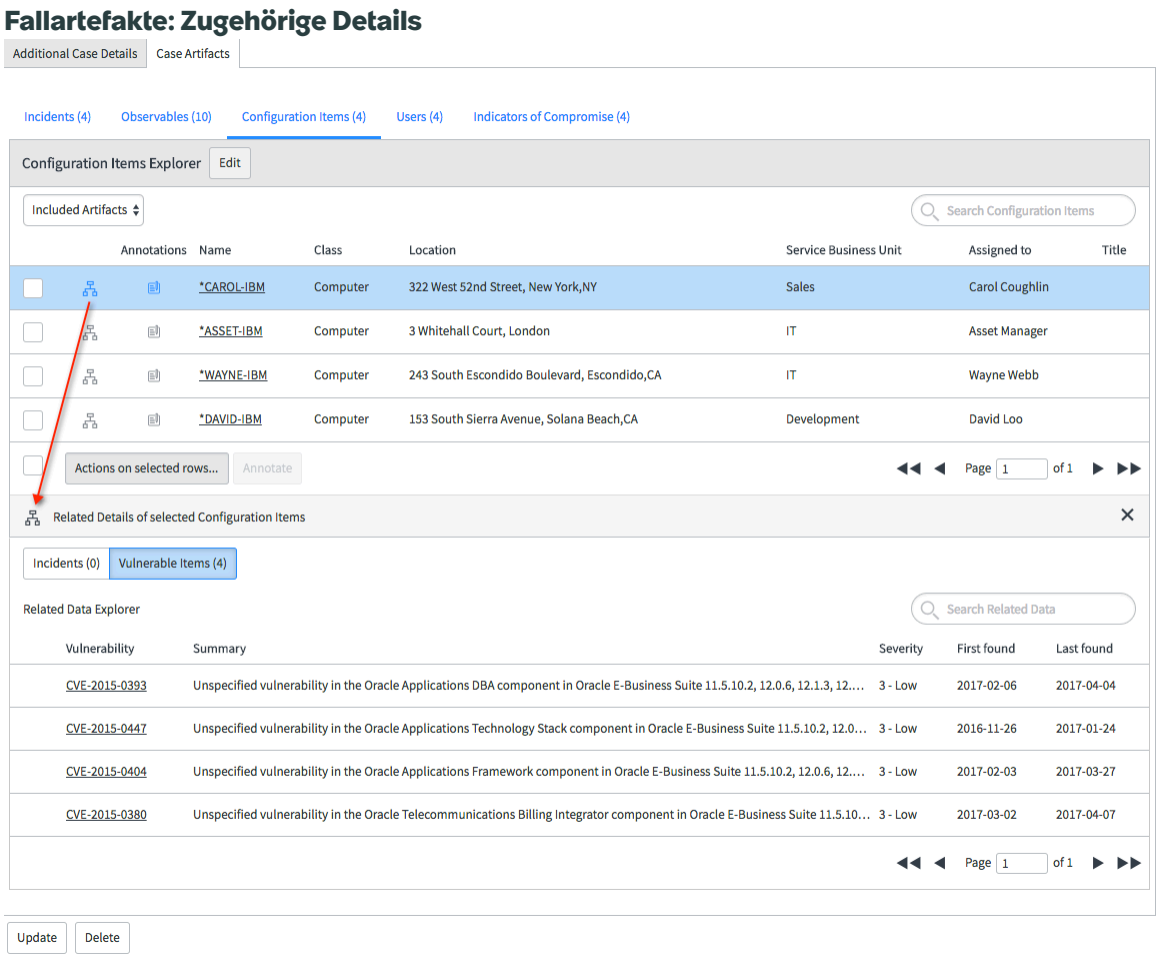
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die **Fallartefakte** Abschnitt enthält eine Reihe von Registerkarten mit Informationen, die im Sicherheitsfall enthalten sind.

Sie können Suchen innerhalb des Inhalts jeder Registerkarte durchführen. Sie können auch bestimmte Datensätze ausschließen, die Sie bereits als sicher bewertet haben oder die in Ihrer Untersuchung keinen Wert haben. Die ausgeschlossenen Datensätze werden nicht gelöscht, aber in der Ansicht ausgeblendet. Bei Bedarf können Sie ausgeschlossene Datensätze anzeigen und wieder hinzufügen.

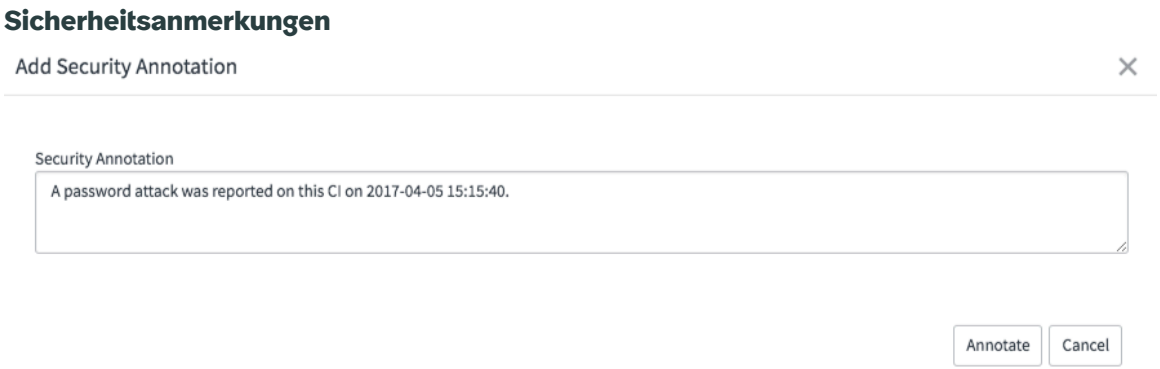
Auf jeder Registerkarte können Sie auf das Symbol „zusätzliche Details“ klicken, um zugehörige Informationen für den ausgewählten Datensatz anzuzeigen. Wenn Sie beispielsweise auf klicken **Konfigurationselemente** Registerkarte, um den Konfigurationselemente-Explorer anzuzeigen, und klicken Sie auf zusätzliche Details für ein bestimmtes CI. Sie können Incidents, angreifbare Elemente und Anmerkungen anzeigen, die diesem CI zugeordnet sind.



Sie können auch einen Datensatz auswählen und auf klicken **Anmerkungen Hinzufügen** Schaltfläche für ein fallbezogenes Artefakt, um dem Datensatz Anmerkungen hinzuzufügen. Anmerkungen sind einfach Notizen, die jeder Analyst zu einem bestimmten Artefakt machen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Andere Tools, die der Analyst für die Untersuchung von Fällen verwenden kann, sind:

- Führen Sie eine Sichtungssuche für erkennbare Elemente in einem Fall aus
- Suchen Sie nach Sicherheitsartefakten

Erstellen Sie Fälle in Security Case Management

Fälle werden verwendet, um Informationen über einen Kampagnen- oder Statusakteur nachzuverfolgen, der Ihre Organisation bedroht. Nachdem ein Fall erstellt wurde, können Sie Artefakte hinzufügen, mit denen Sie alle zugehörigen Informationen in einem einzelnen Falldatensatz überprüfen und analysieren können.

Vorbereitungen

Erforderliche Rolle: sn_ti.case_use

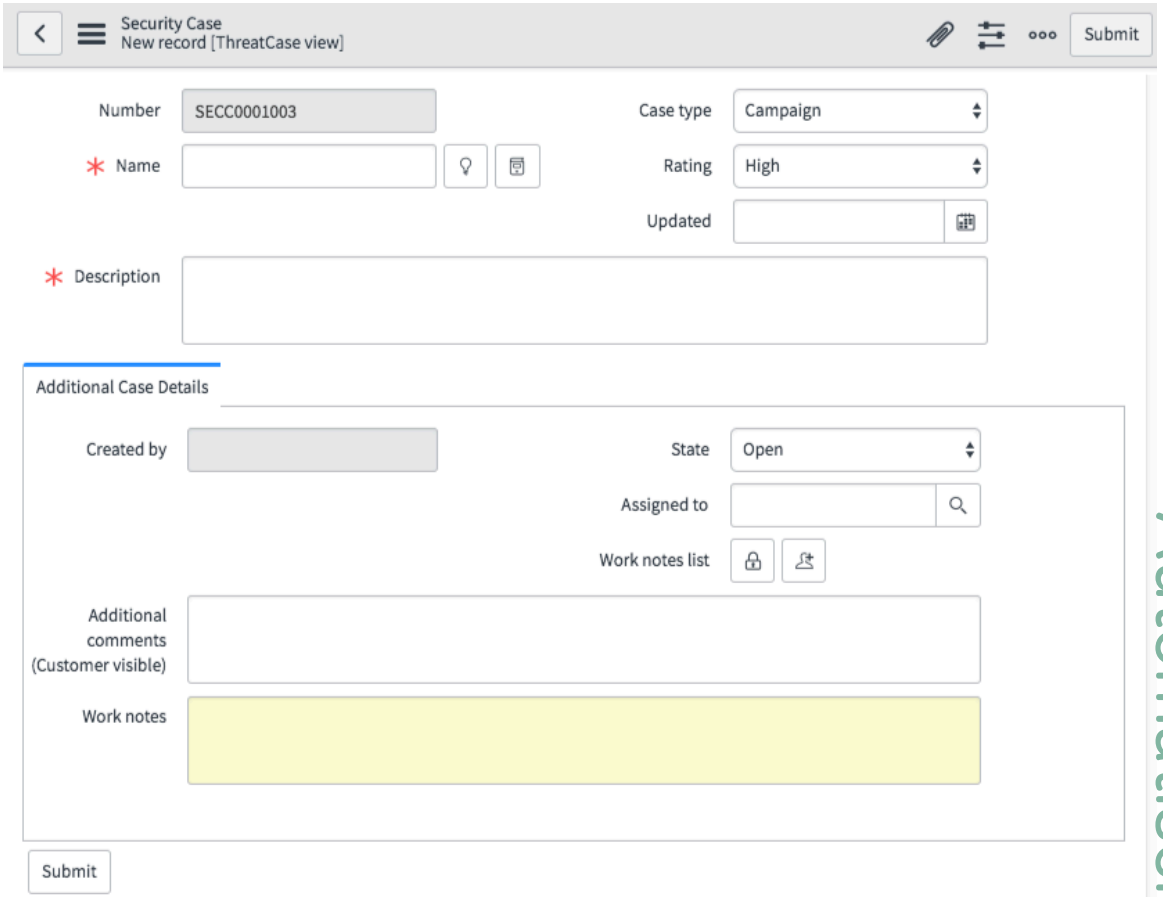
r

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallmanagement** > **Alle Fälle**an.
   Die Liste Sicherheitsfälle wird geöffnet.
2. Klicken Sie auf **Neu**.
   Der Bildschirm Sicherheitsfälle wird geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



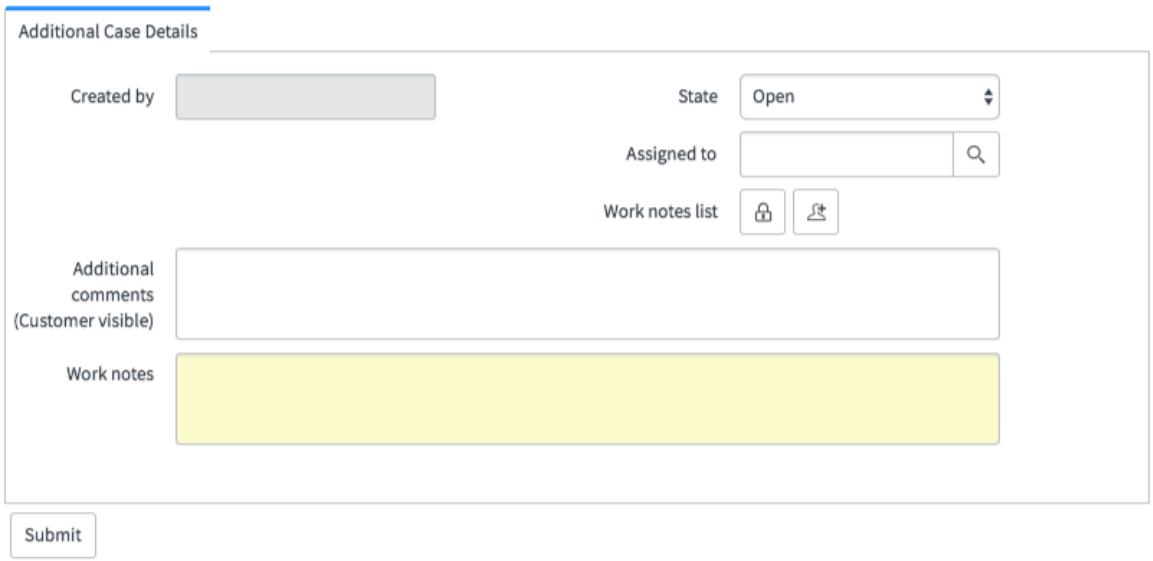
3. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Fallnummer	[Schreibgeschützt] die Fallnummer.
Fallname	Geben Sie einen beschreibenden Namen für den Fall ein.
Falltyp	Wählen Sie den Typ des untersuchten Falls aus.
Bewertung	Wählen Sie die Wichtigkeit dieses Falls aus (von Kritisch nach Niedrig).
Letztes Update	[Schreibgeschützt] Datum und Uhrzeit der letzten Aktualisierung des Falls.
Kurzbeschreibung	Eine kurze Beschreibung des Falls.

4. Klicken Sie auf **Zusätzliche Falldetails** Registerkarte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Erstellt von	[Schreibgeschützt] der Name des Anwenders, der diesen Fall erstellt hat.
Status	Aktueller Status des Falls. Bei der Fallerstellung wird der Status standardmäßig auf Entwurf festgelegt.
Zugewiesen an	Klicken Sie auf das Suchsymbol, und weisen Sie den Fall einem Analysten zu.
Arbeitsnotizenliste	Klicken Sie auf das Schlosssymbol, und fügen Sie interne Anwender hinzu, die Arbeitsnotizen anzeigen können.
Zusätzliche Anmerkungen	Geben Sie bei Bedarf Notizen zum Fall ein, die für den Kunden sichtbar sind.
Arbeitsnotizen	Geben Sie bei Bedarf eine Arbeitsnotiz für den Fall ein.

6. Klicken Sie auf **Absenden**.
   Nachdem der Datensatz gespeichert wurde, können Sie auf klicken **Fallartefakte** Registerkarte und Fügen Sie dem Fall Artefakte hinzu .

Fügen Sie einem Fall Artefakte hinzu

Nachdem Sie einen Fall erstellt haben, können Sie dem Fall Artefakte wie Security Incidents, CIs und Kompromittierungsindikatoren hinzufügen. Diese Artefakte dienen als Hinweise zur Lösung des Falls.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

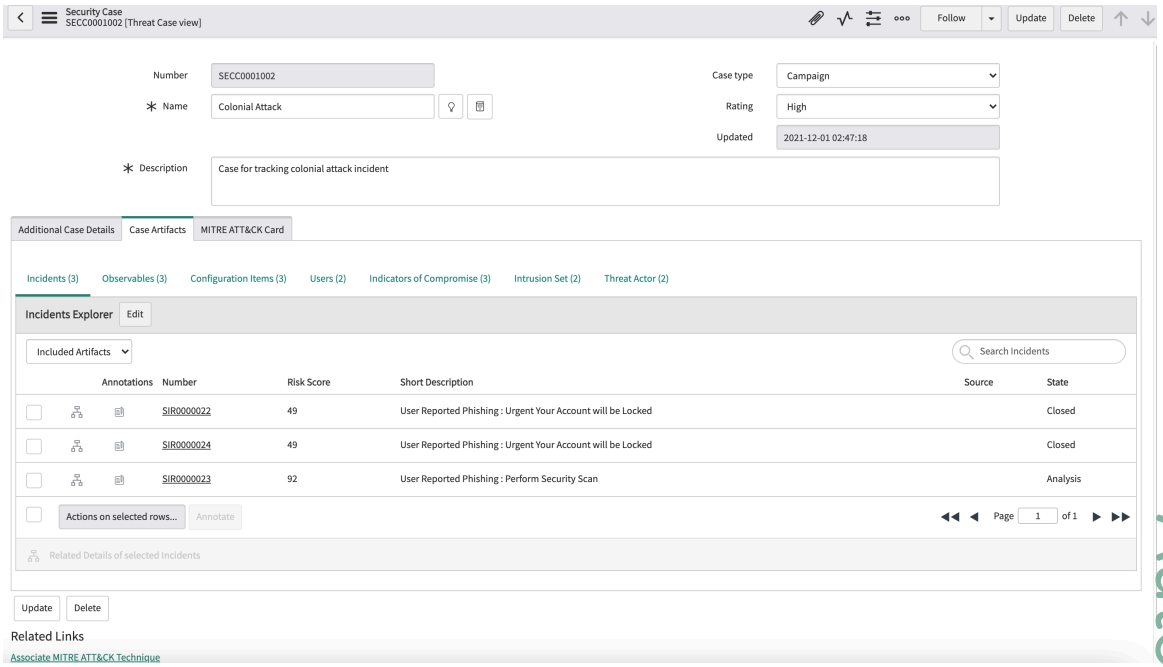
Erforderliche Rolle: sn_ti.case_user_write

Prozedur

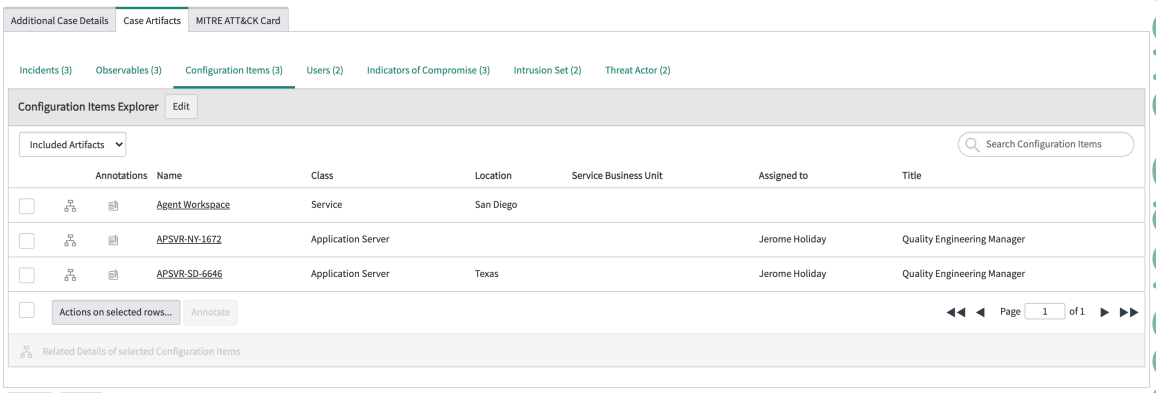
1. Öffnen Sie einen Fall, dem Sie Artefakte hinzufügen möchten.
2. Klicken Sie auf **Fallartefakte** Zugehörige Liste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



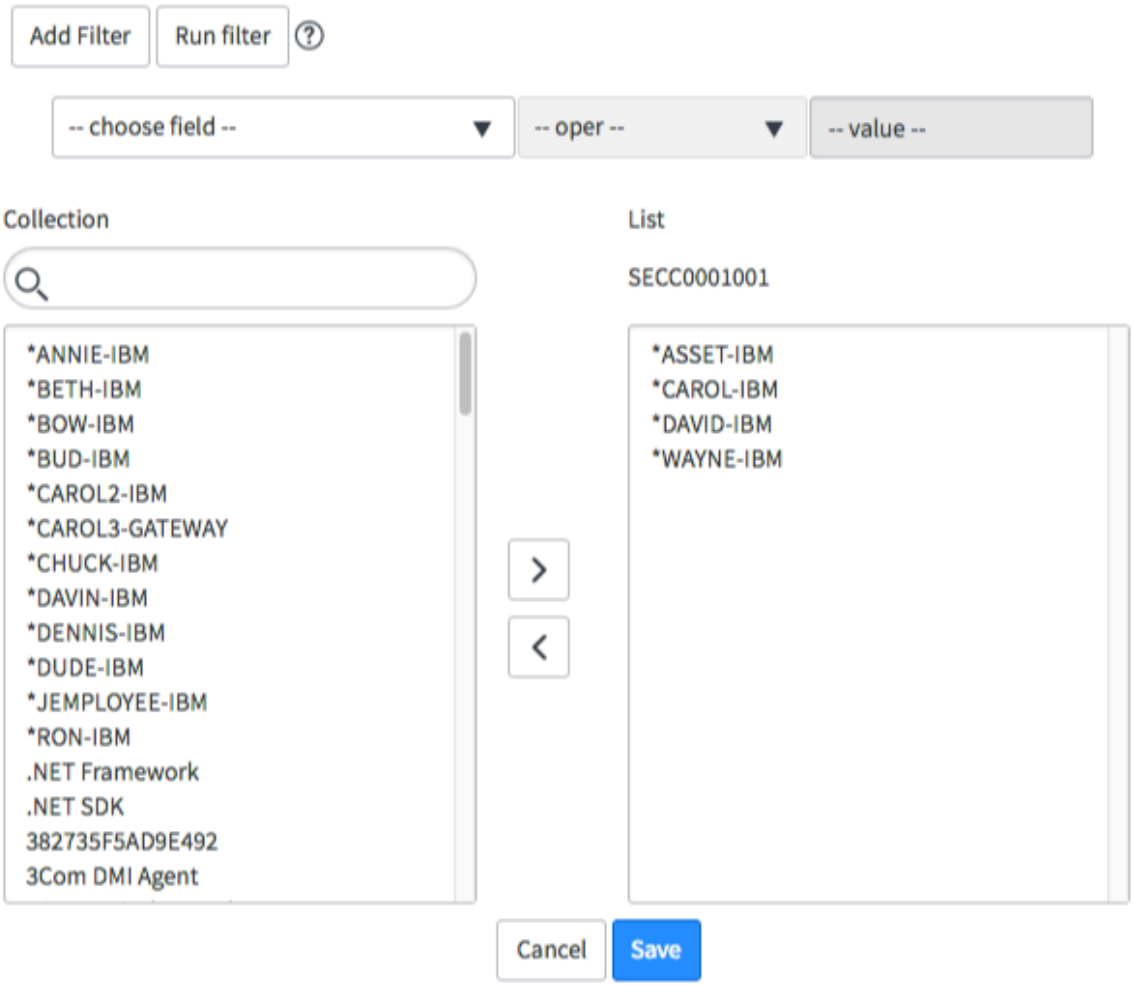
3. Klicken Sie auf die Registerkarte, die dem Artefakttyp zugeordnet ist, den Sie dem Fall hinzufügen möchten. Klicken Sie beispielsweise auf **Konfigurationselemente** Zum Hinzufügen eines oder mehrerer CIs zum Fall.



4. Klicken Sie auf **Bearbeiten**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Suchen Sie mit Slushbucket und Filtern die Artefaktdatensätze, die Sie dem Fall hinzufügen möchten, und verschieben Sie sie aus dem Sammlungs-Bucket in den Listen-Bucket, und klicken Sie auf **Speichern** . Die Liste wird auf der Registerkarte ausgewählt angezeigt, und die ausgewählten Artefakte werden der Liste hinzugefügt.

Zugehörige Informationen

Fügen Sie einem vorhandenen Fall IoCs und erkennbare Elemente hinzu

Fügen Sie einem vorhandenen Fall Security Incidents hinzu

Fügen Sie vorhandenen Fällen CIs hinzu

Fügen Sie betroffene Anwender zu vorhandenen Fällen hinzu

Zuordnen MITRE-ATT&CK Informationen mit Sicherheitsfall

Zuordnen MITRE-ATT&CK Taktiken und Techniken für einen Sicherheitsfall für ein besseres Management von Sicherheitsfällen und die Bedrohungsanalyse auf granularer Ebene.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallmanagement** > **Alle Fälle**an.
2. Wählen Sie den Sicherheitsfall aus, den Sie mit den MITRE-ATT&CK-Informationen anreichern möchten.

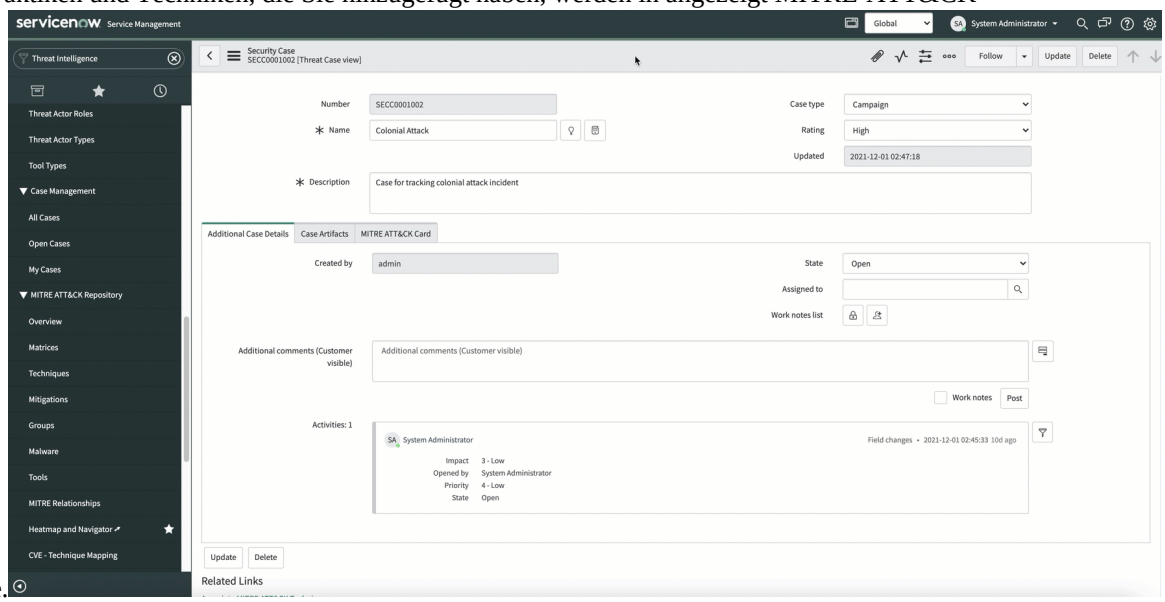
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie in der zugehörigen Liste auf **Ordnen Sie DIE MITRE ATT&CK-Technik zu** .

   In der folgenden Abbildung sehen Sie, wie Sie von der zugehörigen Liste zu navigieren **Ordnen Sie DIE MITRE ATT&CK-Technik zu** , Überprüfen Sie die Quelle, und fügen Sie eine Taktik und Technik hinzu.

4. Überprüfen Sie in den Quelllisten die **Quelle** .
5. Überprüfen Sie **Taktik** Und **Techniken** , Und fügen Sie sie basierend auf der Relevanz für den Fall hinzu oder entfernen Sie sie.
6. Klicken Sie auf **Speichern**.
   Die Taktiken und Techniken, die Sie hinzugefügt haben, werden in angezeigt MITRE-ATT&CK Karte.



Fallerstellung aus Sicherheitsartefakten

Zusätzlich zum manuellen Erstellen von Fällen aus Management von Sicherheitsfällen, Sie können Fälle auch aus Sicherheitsartefakten erstellen, z. B. Security Incidents, kompromittierte Indikatoren, betroffene Anwender und Konfigurationselemente.

IOCs und erkennbare Elemente in Fällen

In Threat Intelligence, Sie können Fälle aus IoCs und erkennbaren Elementen erstellen und IoCs und erkennbare Elemente zu vorhandenen Fällen hinzufügen. Sie können erkennbare Elemente auch direkt aus einem Fall erstellen.

Erstellen Sie einen Fall aus IoCs oder erkennbaren Elementen

In Threat Intelligence, Sie können einen Fall aus Artefakten (IoCs oder erkennbare Elemente) erstellen. Nachdem die IoCs oder erkennbaren Elemente zum Erstellen eines Falls verwendet wurden, können Sie verwenden Management von Sicherheitsfällen Um die Daten zu analysieren.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

Automatische Übersetzung

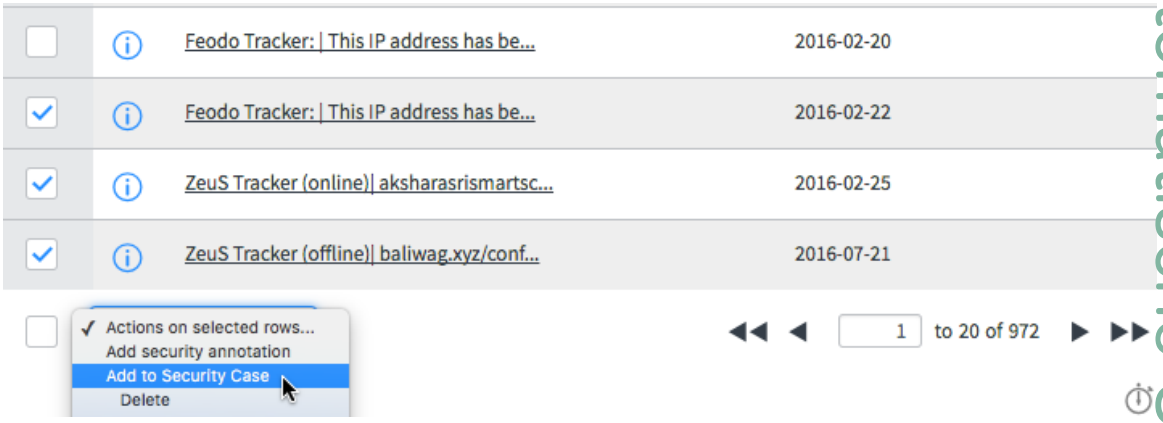
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

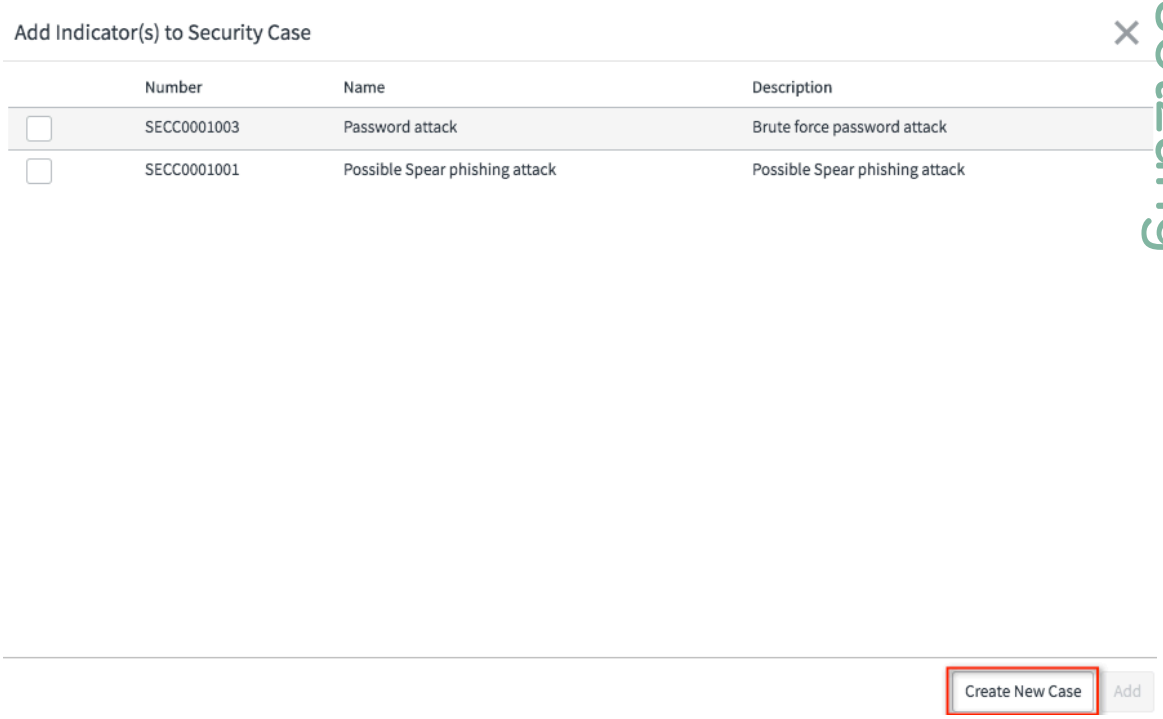
1. Navigieren Sie zu den Artefakten (IoCs oder erkennbare Elemente), die Sie zum Erstellen eines Falls verwenden möchten.
   - Um einen Fall aus IoCs zu erstellen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Indikatoren**an.
   - Um einen Fall aus erkennbaren Elementen zu erstellen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**an.
2. Wählen Sie in der Liste die Artefakte aus, die Sie einem neuen Fall hinzufügen möchten.

   Hinweis:
   Wenn Sie mehrere IoCs oder erkennbare Elemente auswählen, werden sie alle dem Fall hinzugefügt.

3. Von **Aktionen für ausgewählte Elemente** Dropdown-Liste auswählen **Dem Sicherheitsfall hinzufügen** .



Die **Dem Sicherheitsfall hinzufügen** Dialogfeld wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden sie in der Liste angezeigt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie Auf **Erstellen Sie Einen Neuen Fall** .
5. Füllen Sie die Felder aus.

Feld	Beschreibung
Fallname	Geben Sie einen Namen für diesen Fall ein.
Beschreibung	Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert wäre.

6. Klicken Sie auf **Absenden**.
   Eine Nachricht oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zum Fall in Management von Sicherheitsfällen.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

Fügen Sie einem vorhandenen Fall IoCs und erkennbare Elemente hinzu

Sie können IoCs und erkennbare Elemente zu vorhandenen Fällen hinzufügen. Nachdem Security Incidents zu Fällen hinzugefügt wurden, können Sie verwenden Management von Sicherheitsfällen Um die Daten zu analysieren.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

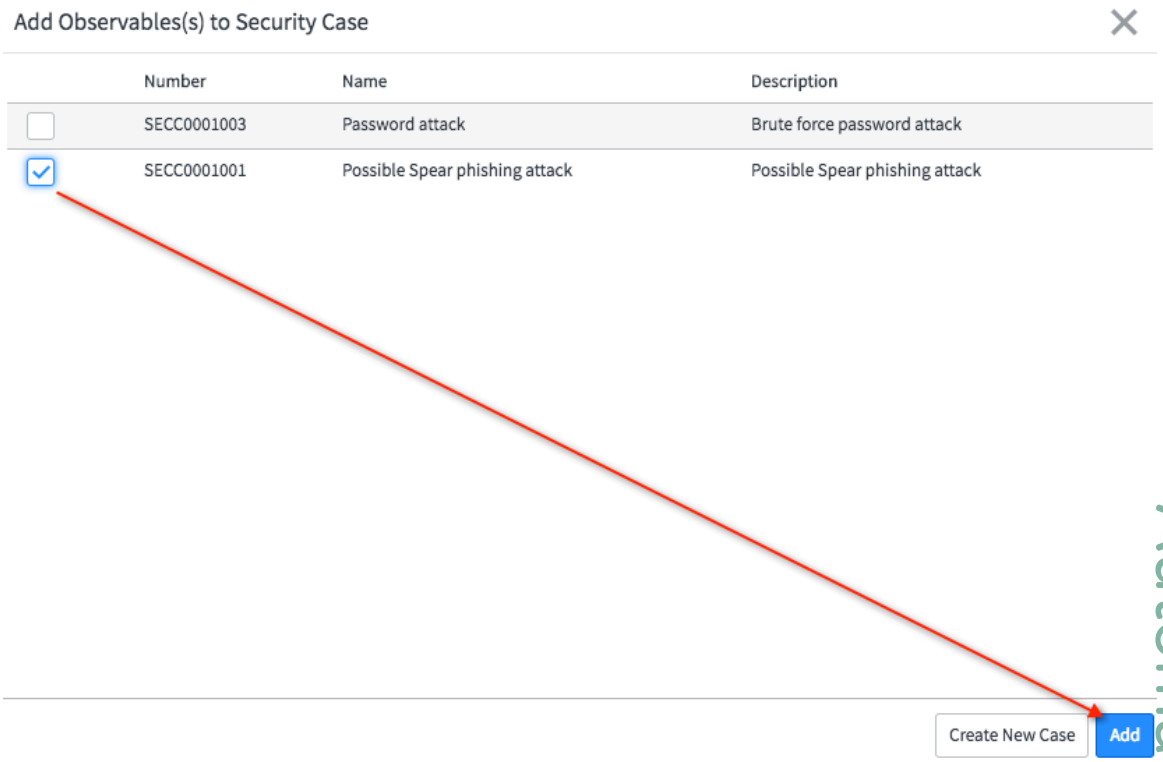
Prozedur

1. Navigieren Sie zu den Artefakten (IoCs oder erkennbare Elemente), die Sie vorhandenen Fällen hinzufügen möchten.
   - Um einem oder mehreren Fällen IoCs hinzuzufügen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Indikatoren**an.
   - Um einem oder mehreren Fällen erkennbare Elemente hinzuzufügen, navigieren Sie zu **Threat Intelligence** > **IoC-Repository** > **Erkennbare Elemente**an.
2. Wählen Sie in der Liste die Artefaktdatensätze aus, die Sie vorhandenen Fällen hinzufügen möchten.

   Hinweis:
   Wenn Sie mehrere Fälle auswählen, werden die ausgewählten IoCs oder erkennbaren Elemente jedem der ausgewählten Fälle hinzugefügt.

3. Von **Aktionen für ausgewählte Elemente** Dropdown-Liste auswählen **Dem Sicherheitsfall hinzufügen** .
   Die **Dem Sicherheitsfall hinzufügen** Dialogfeld wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden sie in der Liste angezeigt.
4. Wählen Sie die Fälle aus, denen Sie die ausgewählten IoCs oder erkennbaren Elemente hinzufügen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Hinzufügen**.
   Eine Nachricht gibt an, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Management von Sicherheitsfällen.

Erstellen Sie ein erkennbares Element aus einem Fall

Neue erkennbare Elemente können aus Fällen in erstellt werden Management von Sicherheitsfällen.

Vorbereitungen

Erforderliche Rolle: sn_ti.case_user

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallmanagement** > **Alle Fälle**an.
   Die Liste Sicherheitsfälle wird geöffnet.
2. Öffnen Sie entweder einen vorhandenen Fall, oder klicken Sie auf **Neu** Bis Erstellen Sie einen neuen Fall .
3. Klicken Sie auf **Fallartefakte** Zugehöriger Link, und klicken Sie auf **Erkennbare Elemente** Registerkarte.
4. Klicken Sie Auf **Neu** Und geben Sie die angeforderten Informationen ein.

Feld	Beschreibung
Wert	[Schreibgeschützt] die Fallnummer.
Typ des erkennbaren Elements	Geben Sie einen beschreibenden Namen für den Fall ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Typkategorie des erkennbaren Elements	Wählen Sie den Typ des untersuchten Falls aus.
Incident-Anzahl	Wählen Sie die Wichtigkeit dieses Falls aus (von Kritisch nach Niedrig).
Ergebnis	[Schreibgeschützt] Datum und Uhrzeit der letzten Aktualisierung des Falls.
Notizen	Eine kurze Beschreibung des Falls.

5. Klicken Sie auf **Zusätzliche Falldetails** Registerkarte.
6. Füllen Sie die Felder entsprechend aus.

Feld	Beschreibung
Erstellt von	[Schreibgeschützt] der Name des Anwenders, der diesen Fall erstellt hat.
Status	Aktueller Status des Falls. Bei der Fallerstellung wird der Status standardmäßig auf Entwurf festgelegt.
Arbeitsnotizenliste	Klicken Sie auf das Kontrollkästchen, um die Arbeitsnotizen im Abschnitt „zusätzliche Falldetails“ des Falldatensatzes anzuzeigen.
Arbeitsnotizen	Geben Sie bei Bedarf eine Arbeitsnotiz für den Fall ein. Wenn **Liste der Arbeitsnotizen** Ist ausgewählt, wird die Arbeitsnotiz im Abschnitt „zusätzliche Falldetails“ des Falldatensatzes angezeigt.

7. Klicken Sie auf **Absenden**.
   Nach Bedarf können Sie auf klicken **Fallartefakte** Registerkarte und Fügen Sie dem Fall Artefakte hinzu .

Führen Sie eine Sichtungssuche für erkennbare Elemente in einem Fall aus

Sie können mit der Sichtungssuchfunktion nach erkennbaren Elementen suchen, um zu bestimmen, wie oft sie auftreten. Jedes Vorkommen wird als betrachtet *Sichtung* . Sie können die Suche auf die Anzahl der Sichtungen innerhalb einer ausgewählten Anzahl von Tagen oder innerhalb eines Datumsbereichs beschränken.

Vorbereitungen

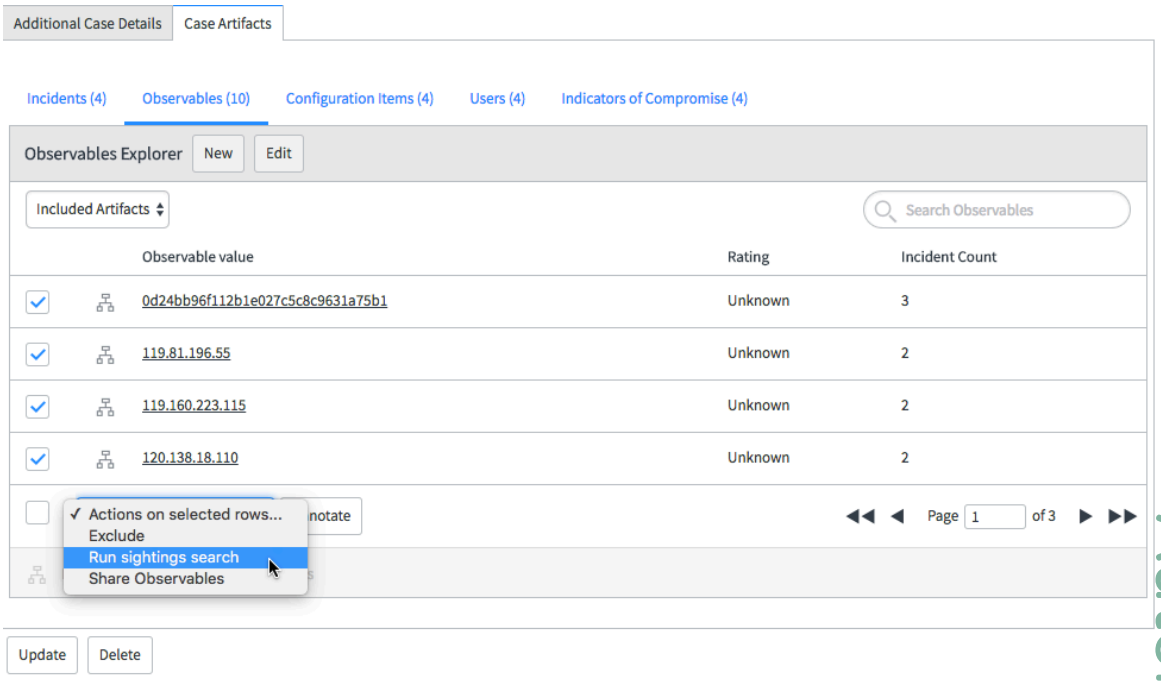
Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

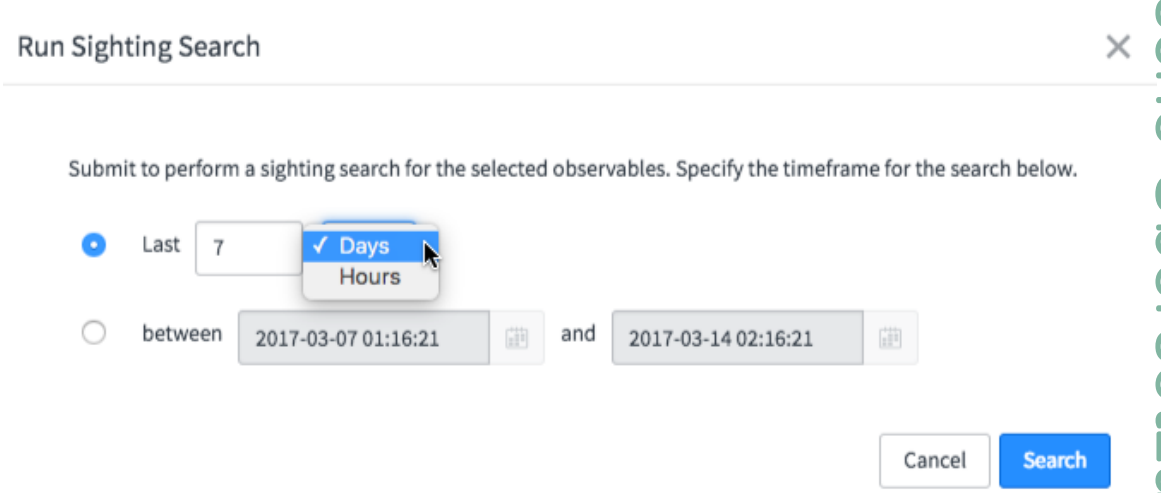
Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Fallmanagement** > **Alle Fälle**an.
2. Öffnen Sie den Fall, der erkennbare Elemente enthält, für die Sie eine Sichtungssuche ausführen möchten.
3. Klicken Sie auf **Fallartefakte** Zugehöriger Link.
4. Klicken Sie auf **Erkennbare Elemente** Registerkarte.
5. Wählen Sie ein oder mehrere erkennbare Elemente aus, nach denen Sie nach Sichtungen suchen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Von **Aktionen für ausgewählte Elemente** Dropdown-Liste auswählen **Sichtungssuche ausführen** . Die **Sichtungssuche Ausführen** Dialogfeld wird angezeigt.



7. Geben Sie entweder die Anzahl der Tage oder Stunden ein, die Sie nach Sichtungen der ausgewählten erkennbaren Elemente suchen möchten, oder wählen Sie einen Datumsbereich aus.
8. Klicken Sie auf **Suche**.

Security Incidents in Fällen

In Security Incident Response, Sie können Fälle aus Security Incidents, CIs und betroffenen Anwendern erstellen und diese Artefakte vorhandenen Fällen hinzufügen.

Erstellen Sie einen Fall aus Security Incidents

In Security Incident Response, Sie können Fälle aus Security Incidents erstellen. Nachdem die Security Incidents zum Erstellen eines neuen Falls verwendet wurden, können Sie verwenden Management von Sicherheitsfällen Um die Daten zu analysieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

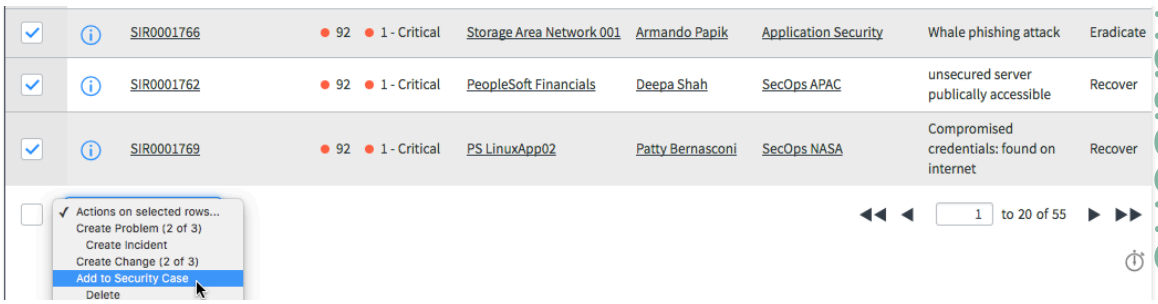
Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

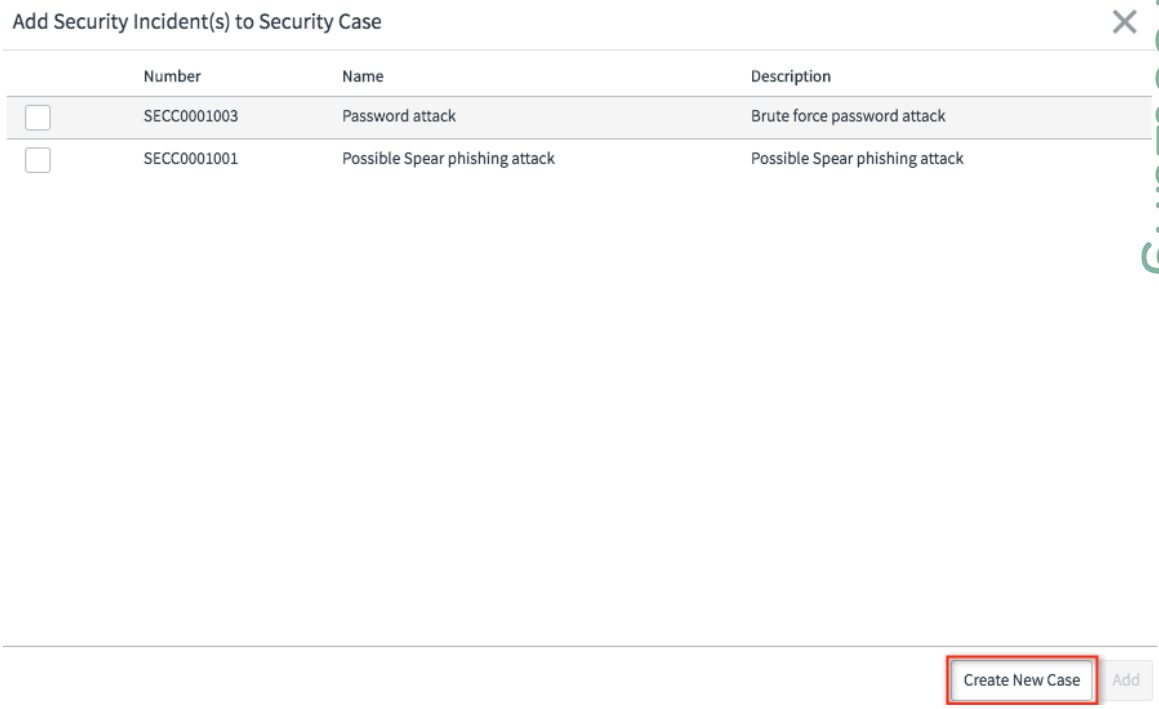
Sie müssen zu den Security Incidents navigieren, die Sie zum Erstellen von Fällen verwenden möchten.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Offene Incidents anzeigen**an.
   Die Liste Security Incidents wird geöffnet. In der Liste können Sie einen neuen Fall aus einem oder mehreren Security Incidents erstellen, oder Sie können einen bestimmten Security Incident auswählen und einen neuen Fall aus dem Formular erstellen.
2. Um einen Fall aus der Liste zu erstellen, wählen Sie die Artefakte aus, die Sie einem neuen Fall hinzufügen möchten.
3. Von **Aktionen für ausgewählte Elemente** Dropdown-Liste auswählen **Dem Sicherheitsfall hinzufügen** .



Die **Dem Sicherheitsfall hinzufügen** Dialogfeld wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden sie in der Liste angezeigt.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie Auf **Erstellen Sie Einen Neuen Fall** .
5. Füllen Sie die Felder aus.

Feld	Beschreibung
Fallname	Geben Sie einen Namen für diesen Fall ein.
Beschreibung	Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert wäre.

6. Klicken Sie auf **Absenden**.
   Eine Nachricht oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zum Fall in Management von Sicherheitsfällen.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

Fügen Sie einem vorhandenen Fall Security Incidents hinzu

Sie können Security Incidents zu einem oder mehreren vorhandenen Fällen hinzufügen. Nachdem Security Incidents zu Fällen hinzugefügt wurden, können Sie verwenden Management von Sicherheitsfällen Um die Daten zu analysieren.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den Security Incidents navigieren, die Sie vorhandenen Fällen hinzufügen möchten.

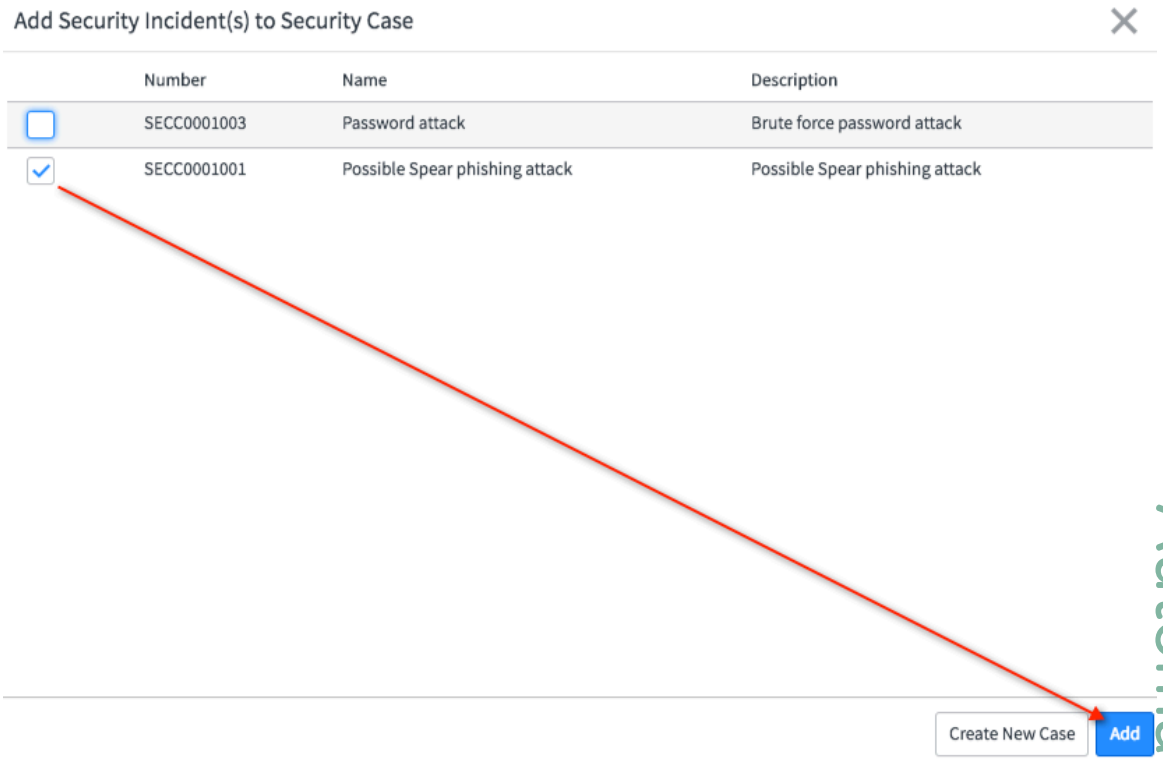
Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Offene Incidents anzeigen**an.
   Die Liste Security Incidents wird geöffnet.
2. Wählen Sie in der Liste einen oder mehrere Security Incidents aus, die Sie vorhandenen Fällen hinzufügen möchten.

   Hinweis:
   Wenn Sie mehrere Security Incidents auswählen, werden die ausgewählten Security Incidents jedem der ausgewählten Fälle hinzugefügt.

3. Von **Aktionen für ausgewählte Elemente** Dropdown-Liste auswählen **Dem Sicherheitsfall hinzufügen** .
   Die **Dem Sicherheitsfall hinzufügen** Dialogfeld wird geöffnet und zeigt die Ihnen zugewiesenen Fälle an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Fälle aus, denen Sie die ausgewählten Security Incidents hinzufügen möchten.
5. Klicken Sie auf **Hinzufügen**.
   Eine Nachricht gibt an, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Management von Sicherheitsfällen.

Konfigurationselemente in Fällen

Sie können einen neuen Fall aus einem oder mehreren Konfigurationselementen (CI) in der Tabelle „Konfigurationselement“ [cmdb_ci] erstellen. Sie können auch CIs zu vorhandenen Fällen hinzufügen.

Erstellen Sie einen Fall aus CIs

Sie können einen Sicherheitsfall aus Konfigurationselementen in der Tabelle „Konfigurationselement“ [cmdb_ci] erstellen. Nachdem die CIs zum Erstellen eines neuen Falls verwendet wurden, können Sie verwenden Management von Sicherheitsfällen Um die Daten zu analysieren.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

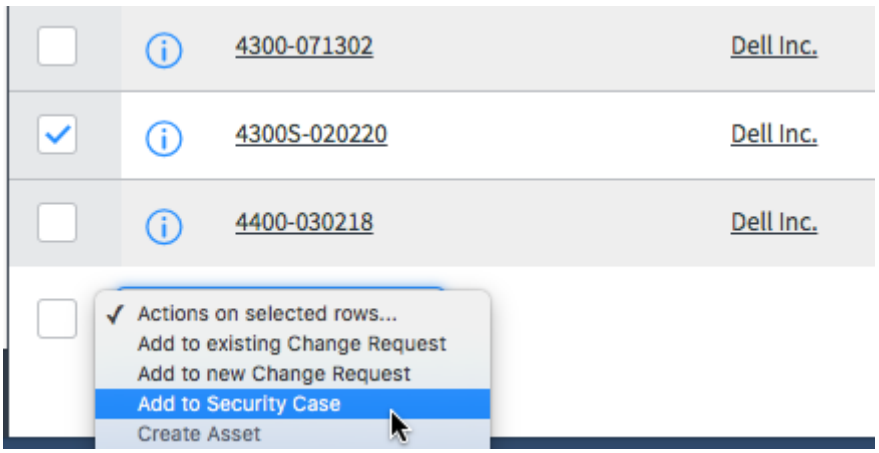
Sie müssen zu den Konfigurationselementen navigieren, die Sie zum Erstellen eines Falls verwenden möchten.

Automatische Übersetzung

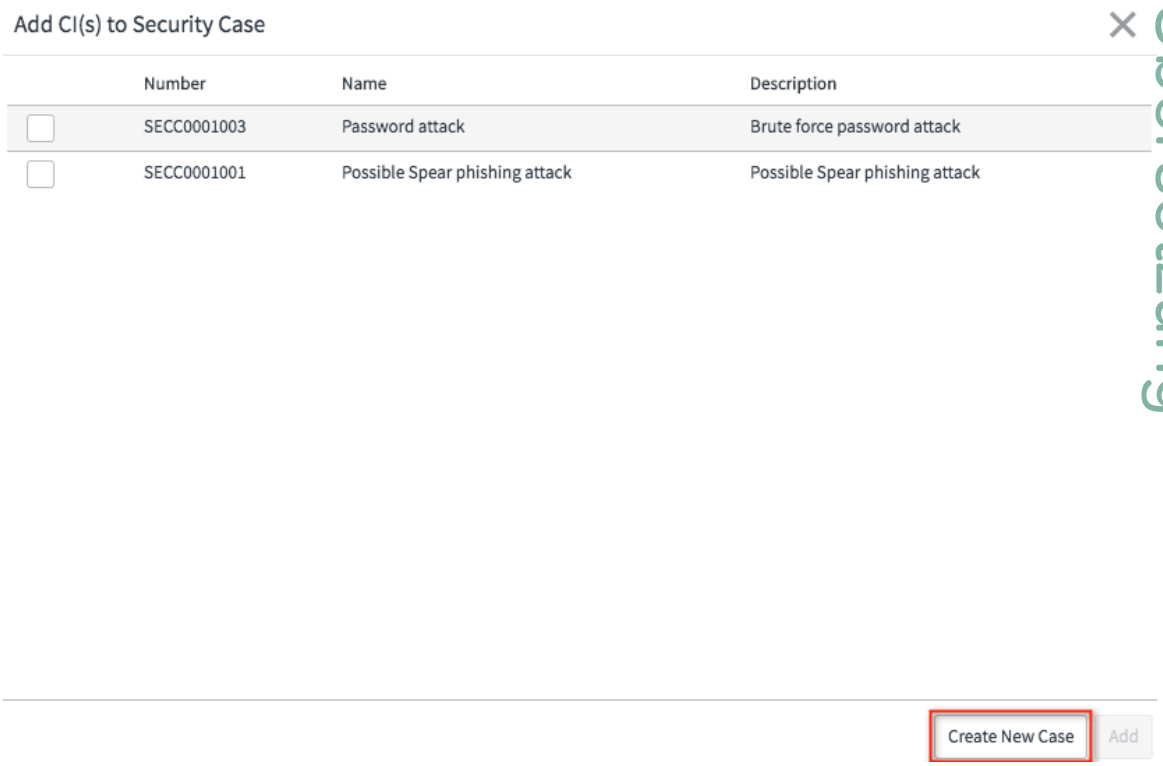
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **Basiselemente** > **Computer** Zum Anzeigen von CIs für Computer.
   Die Liste für den ausgewählten CI-Typ wird geöffnet. In der Liste können Sie einen neuen Fall aus einem oder mehreren CIs erstellen, oder Sie können ein bestimmtes CI auswählen und einen neuen Fall aus dem Formular erstellen.
2. Wählen Sie in der Liste die CIs aus, die Sie einem neuen Fall hinzufügen möchten.
3. Von **Aktionen für ausgewählte Elemente** Dropdown-Liste auswählen **Dem Sicherheitsfall hinzufügen** .



Die **Dem Sicherheitsfall hinzufügen** Dialogfeld wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden sie in der Liste angezeigt.



4. Klicken Sie Auf **Erstellen Sie Einen Neuen Fall** .
5. Füllen Sie die Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Fallname	Geben Sie einen Namen für diesen Fall ein.
Beschreibung	Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert wäre.

6. Klicken Sie auf **Absenden**.
   Eine Nachricht oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zum Fall in Management von Sicherheitsfällen.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

Fügen Sie vorhandenen Fällen CIs hinzu

Sie können einem oder mehreren vorhandenen Fällen Konfigurationselemente hinzufügen. Nachdem die CIs zu Fällen hinzugefügt wurden, können Sie verwenden Management von Sicherheitsfällen Um die Daten zu analysieren.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den CIs navigieren, die Sie den vorhandenen Fällen hinzufügen möchten.

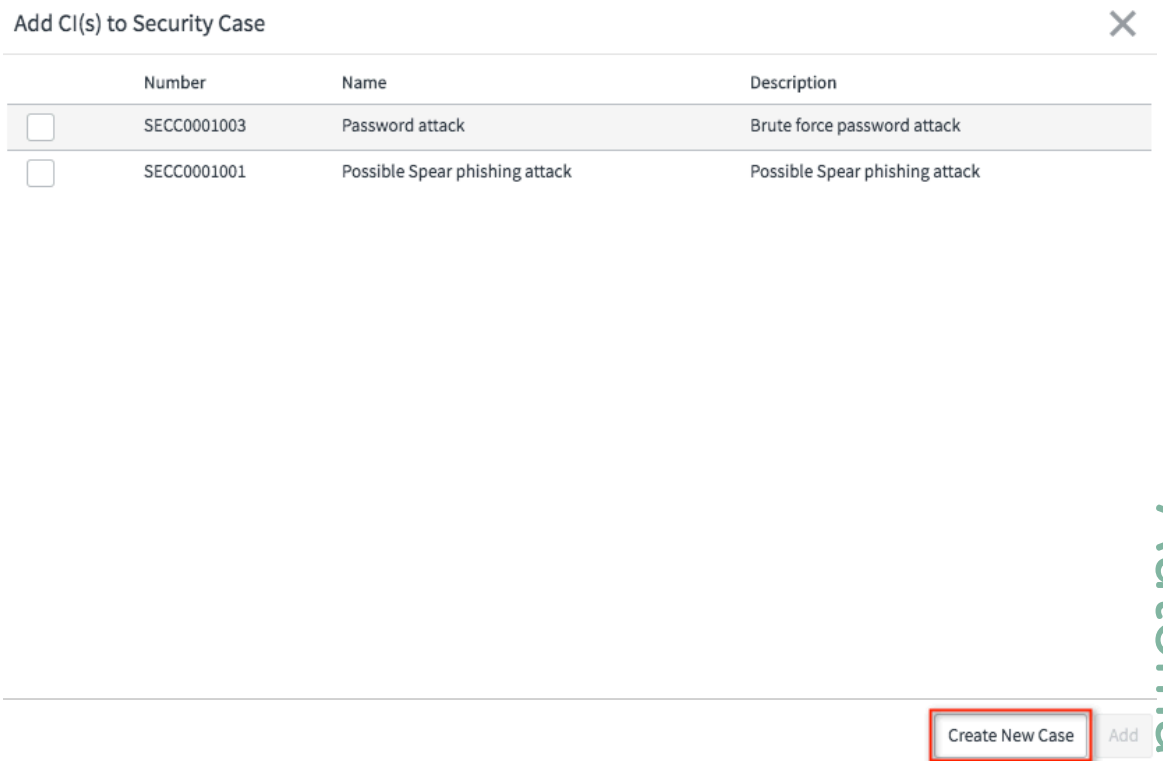
Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **Basiselemente** > **Computer** Zum Anzeigen von CIs für Computer.
   Die Liste der ausgewählten CIs wird geöffnet.
2. Wählen Sie in der Liste ein oder mehrere CIs aus, die Sie vorhandenen Fällen hinzufügen möchten.

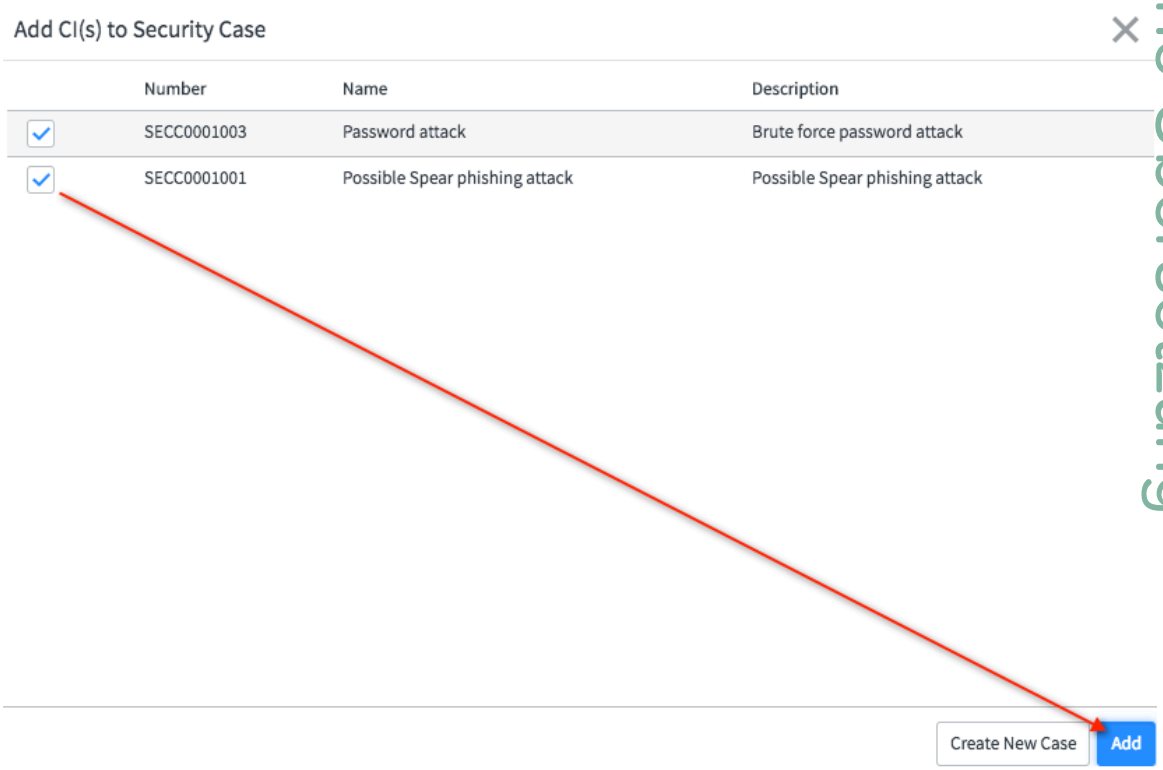
   Hinweis:
   Wenn Sie mehrere CIs auswählen, werden die ausgewählten CIs jedem der ausgewählten Fälle hinzugefügt.

3. Von **Aktionen für ausgewählte Elemente** Dropdown-Liste auswählen **Dem Sicherheitsfall hinzufügen** .
   Die **Dem Sicherheitsfall hinzufügen** Dialogfeld wird geöffnet und zeigt die Ihnen zugewiesenen Fälle an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Fälle aus, denen Sie die ausgewählten CIs hinzufügen möchten.



5. Klicken Sie auf **Hinzufügen**.
Eine Nachricht gibt an, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Management von Sicherheitsfällen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betroffene Anwender in Fällen

Sie können einen neuen Fall aus einem oder mehreren betroffenen Anwendern in der Anwendertabelle [sys_user] erstellen. Sie können vorhandene Fälle auch Anwender hinzufügen.

Erstellen Sie einen Fall von betroffenen Anwendern

Sie können einen Sicherheitsfall aus betroffenen Anwendern in der Anwendertabelle [sys_user] erstellen. Nachdem die betroffenen Anwender zum Erstellen eines neuen Falls verwendet wurden, können Sie verwenden Management von Sicherheitsfällen Um die Daten zu analysieren.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den Anwendern navigieren, die Sie zum Erstellen eines Falls verwenden möchten.

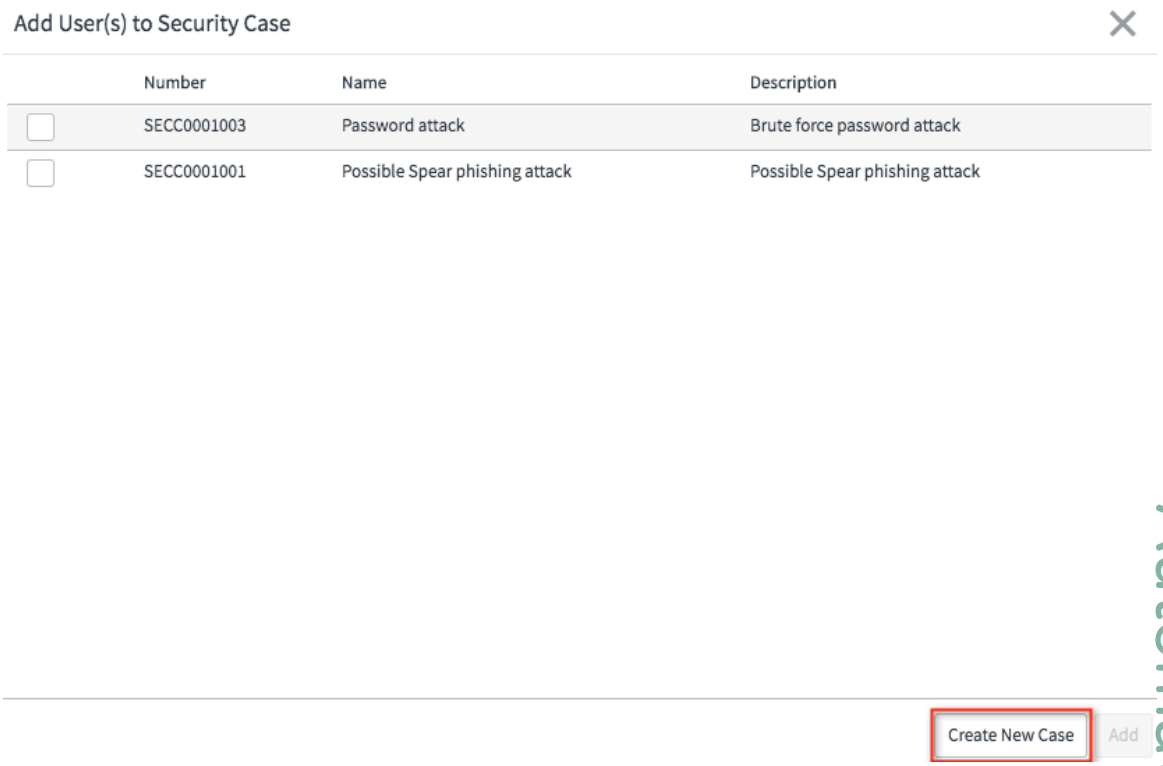
Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**an.
   Die Liste für die ausgewählten Anwender wird geöffnet. In der Liste können Sie einen neuen Fall aus einem oder mehreren Anwenderdatensätzen erstellen, oder Sie können einen bestimmten Anwenderdatensatz auswählen und einen neuen Fall aus dem Formular erstellen.
2. Wählen Sie in der Liste die Anwender aus, die Sie einem neuen Fall hinzufügen möchten.
3. Von **Aktionen für ausgewählte Elemente** Dropdown-Liste auswählen **Dem Sicherheitsfall hinzufügen** .

   Die **Dem Sicherheitsfall hinzufügen** Dialogfeld wird geöffnet. Wenn Ihnen bereits Fälle zugewiesen sind, werden sie in der Liste angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie Auf **Erstellen Sie Einen Neuen Fall** .
5. Füllen Sie die Felder aus.

Feld	Beschreibung
Fallname	Geben Sie einen Namen für diesen Fall ein.
Beschreibung	Geben Sie eine Beschreibung ein, die für den Fallanalysten von Wert wäre.

6. Klicken Sie auf **Absenden**.
   Eine Nachricht oben in der Liste gibt an, dass ein neuer Fall erstellt wurde, zusammen mit einem Link zum Fall in Management von Sicherheitsfällen.
7. Klicken Sie auf den Link, um den neuen Fall anzuzeigen.

Fügen Sie betroffene Anwender zu vorhandenen Fällen hinzu

Sie können betroffene Anwender einem oder mehreren vorhandenen Fällen hinzufügen. Nachdem die Anwenderdatensätze zu Fällen hinzugefügt wurden, können Sie verwenden Management von Sicherheitsfällen Um die Daten zu analysieren.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen zu den Anwenderdatensätzen navigieren, die Sie vorhandenen Fällen hinzufügen möchten.

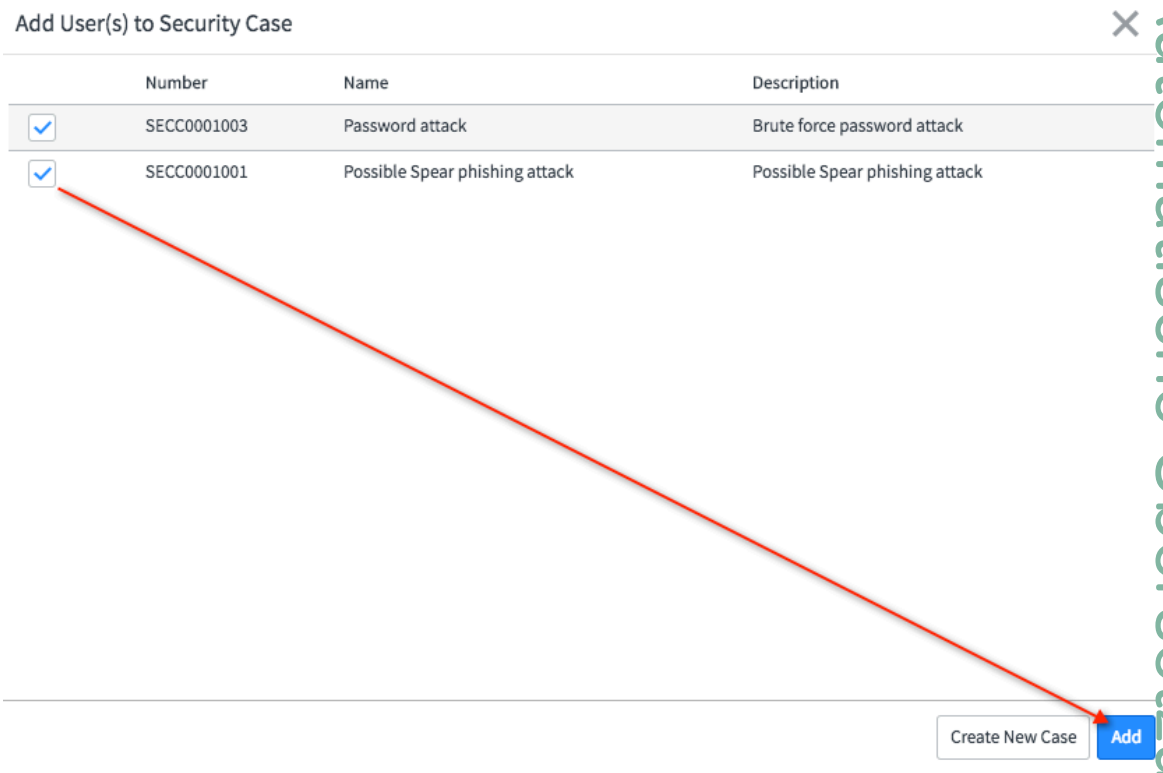
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**an.
   Die Liste der Anwenderdatensätze wird geöffnet.
2. Wählen Sie in der Liste einen oder mehrere Anwender aus, die Sie vorhandenen Fällen hinzufügen möchten.

   Hinweis:
   Wenn Sie mehrere Anwender auswählen, werden die ausgewählten Anwenderdatensätze jedem der ausgewählten Fälle hinzugefügt.

3. Von **Aktionen für ausgewählte Elemente** Dropdown-Liste auswählen **Dem Sicherheitsfall hinzufügen** .
   Die **Dem Sicherheitsfall hinzufügen** Dialogfeld wird geöffnet und zeigt die Ihnen zugewiesenen Fälle an.



4. Wählen Sie die Fälle aus, denen Sie die ausgewählten Anwender hinzufügen möchten.
5. Klicken Sie auf **Hinzufügen**.
   Eine Nachricht gibt an, dass die ausgewählten Datensätze den Fällen hinzugefügt wurden, zusammen mit einem Link zu den Fällen in Management von Sicherheitsfällen.

Analyse von Sicherheitsartefakten

Nachdem Sie Fälle erstellt haben, entweder mit Management von Sicherheitsfällen, Oder aus Artefakten wie IoCs, erkennbaren Elementen, Security Incidents usw. können Sie weiterhin Artefakte hinzufügen, um die Analyse der identifizierten Bedrohungen zu erleichtern.

Zugehörige Details für Fallartefakte

Wenn Sie einem Fall Artefakte hinzufügen, können auch zusätzliche zugehörige Details für jedes Artefakt automatisch hinzugefügt werden. Wenn Sie beispielsweise einen Security Incident hinzufügen, kann er betroffene CIs und Anwenderdatensätze enthalten. Sie können

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die zugehörigen Details für ein ausgewähltes Artefakt schnell anzeigen, ohne die Liste der Artefakte zu verlassen.

Zeigen Sie zugehörige Details für ein Security Incident-Artefakt an

Wenn Ihr Fall Security Incident-Artefakte enthält, können Sie alle zugehörigen Details anzeigen, die in jedem Security Incident enthalten sind, auf den der Fall verweist.

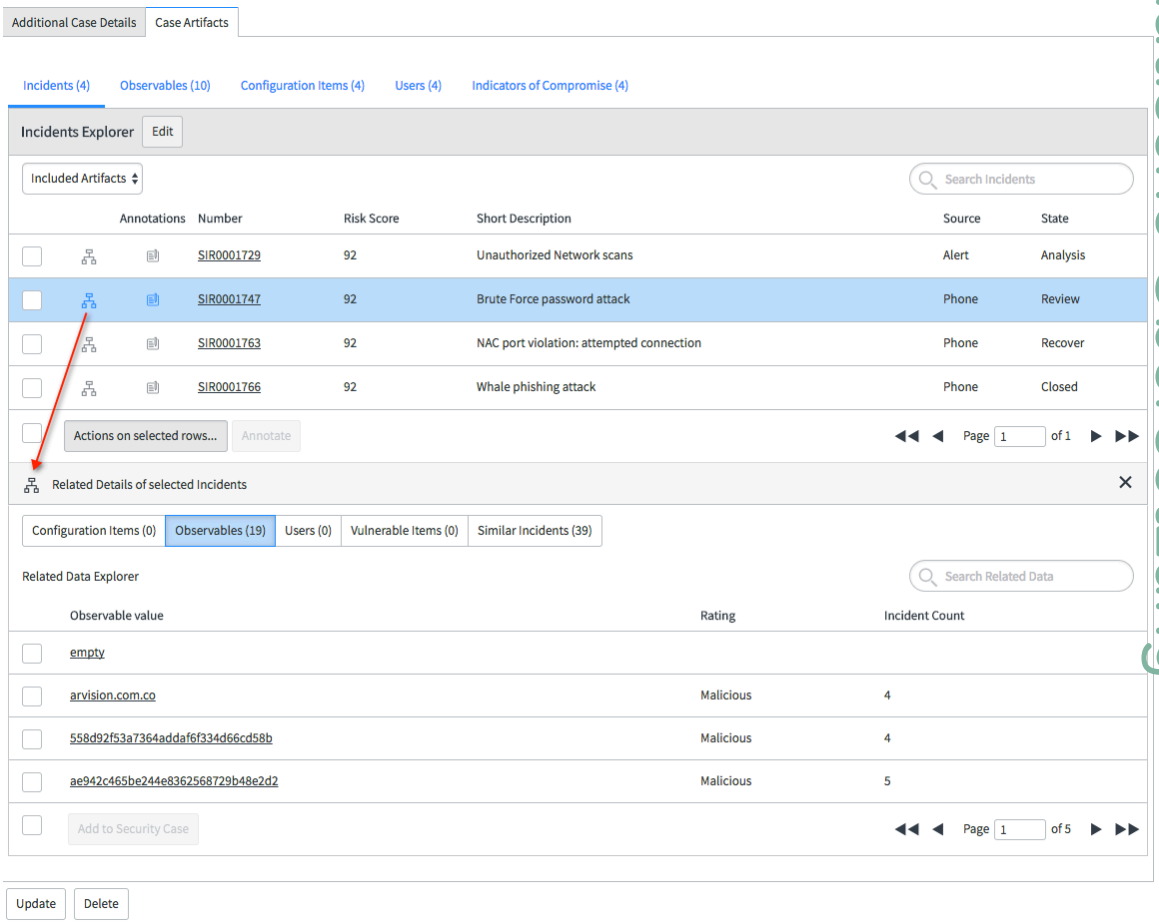
Vorbereitungen

- Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

Prozedur

1. Öffnen Sie einen Fall, der Security Incident-Artefakte enthält.
2. Klicken Sie auf **Incidents** Registerkarte.
3. Klicken Sie auf das Symbol „zusätzliche Details“ für den Security Incident, für den Sie zugehörige Details anzeigen möchten.



4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf klicken **Sicherheitsanmerkung** Registerkarte zum Anzeigen von Anmerkungen für das ausgewählte Artefakt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie zugehörige Details für ein Konfigurationselement-Artefakt an

Wenn Ihr Fall Konfigurationselementartefakte enthält, können Sie alle zugehörigen Details anzeigen, die in jedem CI enthalten sind, auf das der Fall verweist.

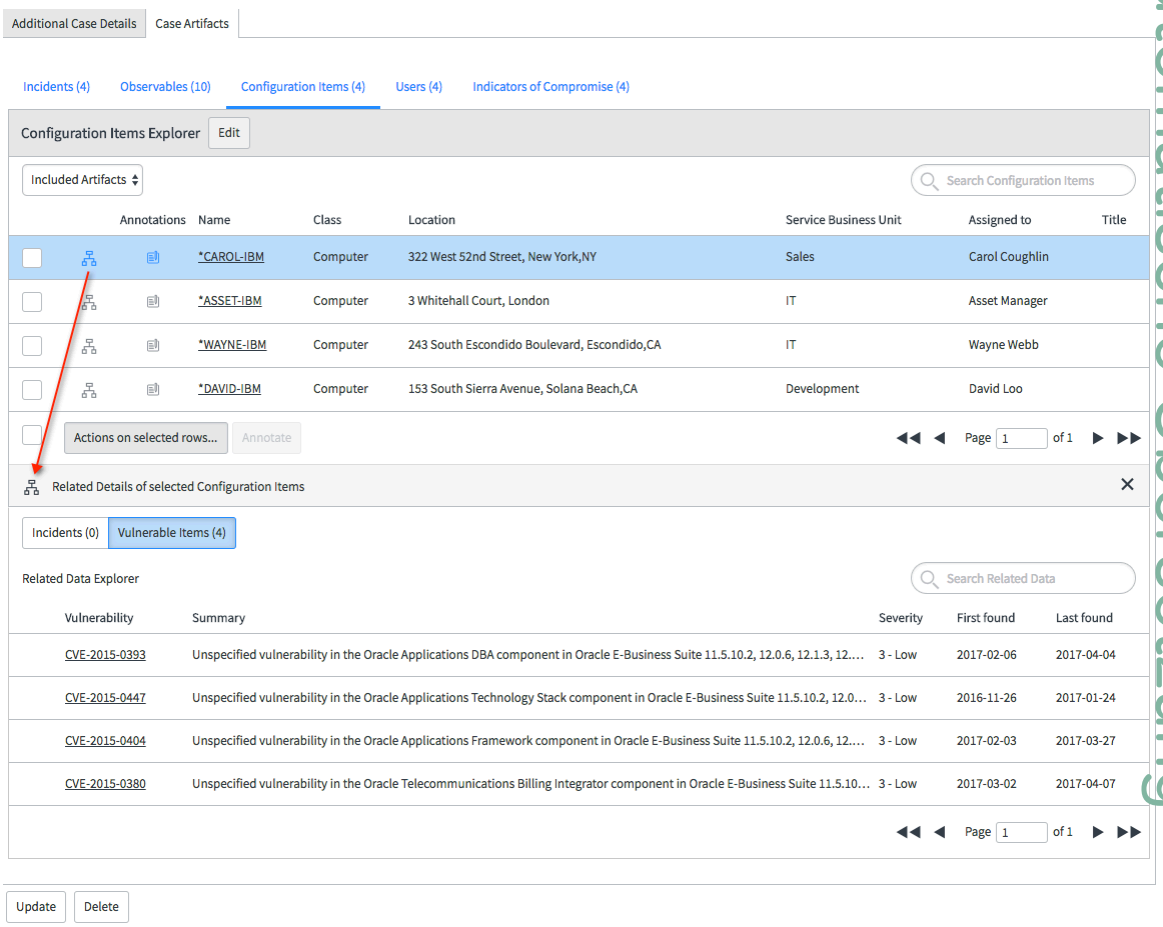
Vorbereitungen

- Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

Prozedur

1. Öffnen Sie einen Fall, der CI-Artefakte enthält.
2. Klicken Sie auf **Konfigurationselemente** Registerkarte.
3. Klicken Sie auf zusätzliche Details für das CI-Artefakt, für das Sie zugehörige Details anzeigen möchten.



4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf klicken **Sicherheitsanmerkung** Registerkarte zum Anzeigen von Anmerkungen für das ausgewählte Artefakt.

Zeigen Sie zugehörige Details für ein IOC-Artefakt an

Wenn Ihr Fall IOC-Artefakte (Indicators of Commitment) enthält, können Sie alle zugehörigen Details anzeigen, die in jedem IOC enthalten sind, auf das der Fall verweist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

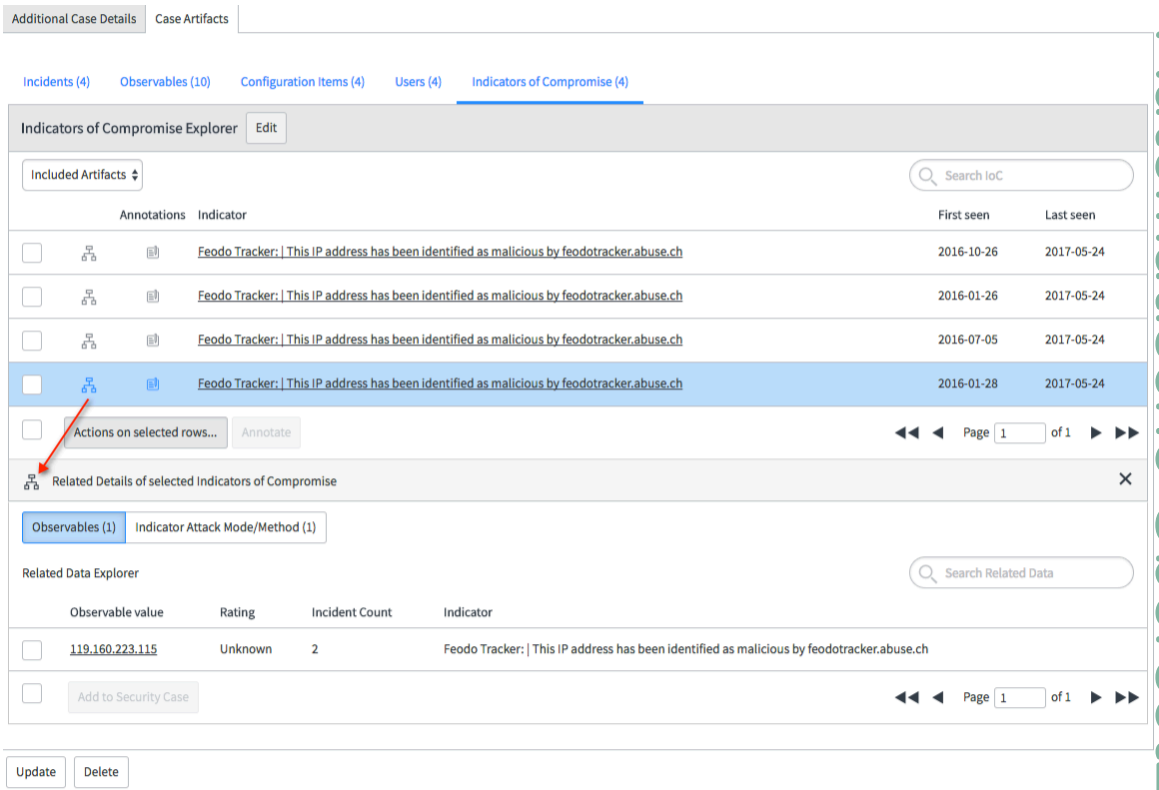
Vorbereitungen

- Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

Prozedur

1. Öffnen Sie einen Fall, der IOC-Artefakte enthält.
2. Klicken Sie auf **Kompromittierungsindikatoren** Registerkarte.
3. Klicken Sie auf das Symbol „zusätzliche Details“ für das IOC-Artefakt, für das Sie zugehörige Details anzeigen möchten.



4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf klicken **Sicherheitsanmerkung** Registerkarte zum Anzeigen von Anmerkungen für das ausgewählte Artefakt.

Zeigen Sie zugehörige Details für ein betroffenes Anwenderartefakt an

Wenn Ihr Fall Artefakte betroffener Anwender enthält, können Sie alle zugehörigen Details anzeigen, die in jedem betroffenen Anwender enthalten sind, auf den der Fall verweist.

Vorbereitungen

- Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

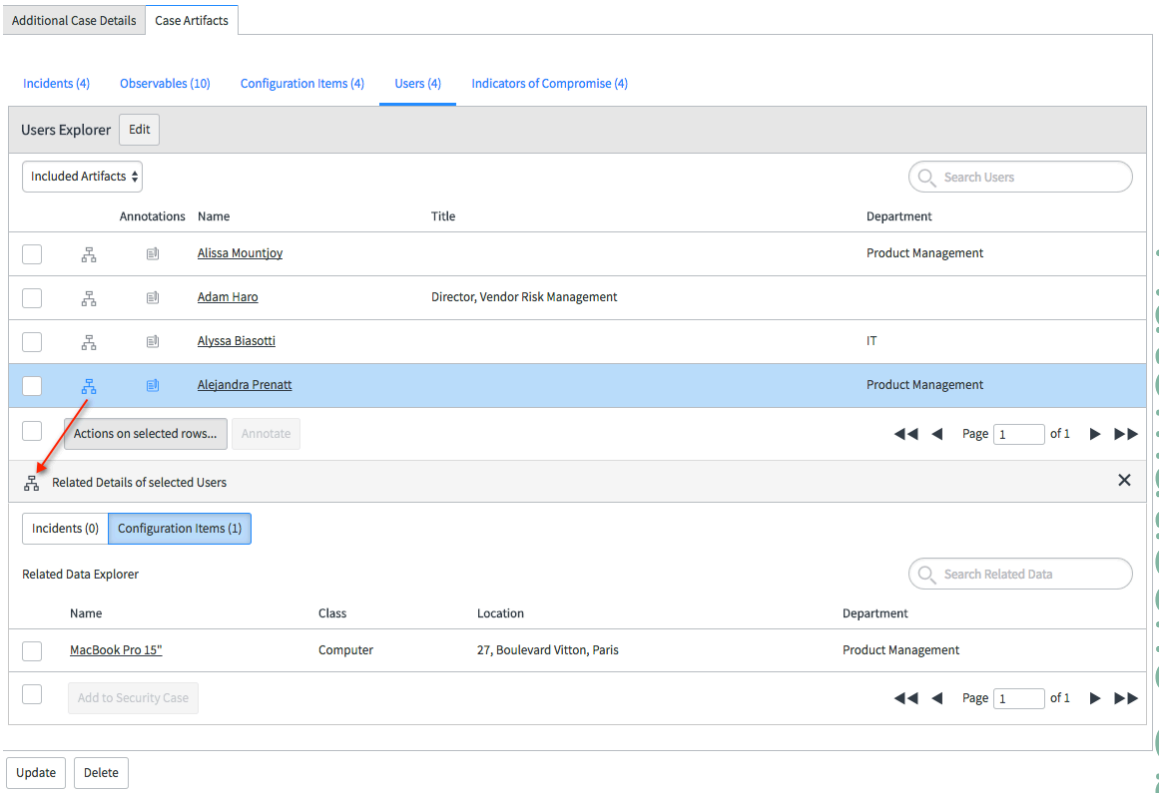
Erforderliche Rolle: sn_ti.case_user_write

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie einen Fall, der Artefakte betroffener Anwender enthält.
2. Klicken Sie auf **Anwender** Registerkarte.
3. Klicken Sie auf zugehörige Details für das betroffene Anwenderartefakt, für das Sie zugehörige Details anzeigen möchten.



4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf klicken **Sicherheitsanmerkung** Registerkarte zum Anzeigen von Anmerkungen für das ausgewählte Artefakt.

Zeigen Sie zugehörige Details für ein Artefakt erkennbarer Elemente an

Wenn Ihr Fall Artefakte erkennbarer Elemente enthält, können Sie alle zugehörigen Details anzeigen, die in jedem erkennbaren Element enthalten sind, auf das der Fall verweist.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

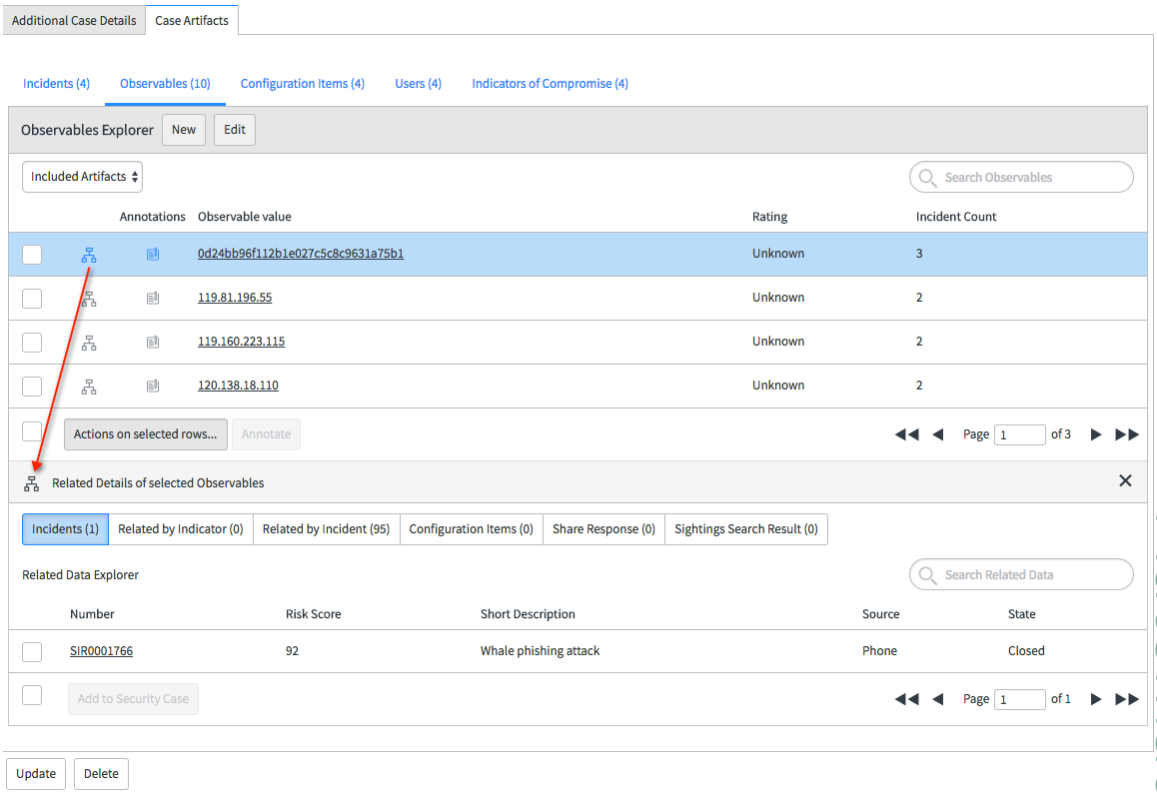
Erforderliche Rolle: sn_ti.case_user_write

Prozedur

1. Öffnen Sie einen Fall, der Artefakte erkennbarer Elemente enthält.
2. Klicken Sie auf **Erkennbare Elemente** Registerkarte.
3. Klicken Sie auf das Symbol „zusätzliche Details“ für das erkennbare Artefakt, für das Sie zugehörige Details anzeigen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf eine der Registerkarten, um bestimmte Arten von Details für das ausgewählte Artefakt anzuzeigen.
5. Sie können auch auf klicken **Sicherheitsanmerkung** Registerkarte zum Anzeigen von Anmerkungen für das ausgewählte Artefakt.

Ausschluss und Aufnahme von Sicherheitsartefakten

Die Listen der unterstützenden Artefakte, die einem Fall zugewiesen sind, können manchmal lang werden, und es kann Instanzen geben, in denen Sie bestimmte Artefakte aus einer Liste entfernen möchten. Anstatt die Artefakte dauerhaft zu entfernen, können Sie sie aus der Liste ausschließen und bei Bedarf zu einem späteren Zeitpunkt wieder in die Liste zurückgeben.

Schließen Sie Sicherheitsartefakte aus einem Fall aus

Sie können Artefakte aus den Listen der unterstützenden Artefakte entfernen. Sie werden nicht dauerhaft entfernt und können bei Bedarf an den Fall zurückgegeben werden.

Vorbereitungen

- Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

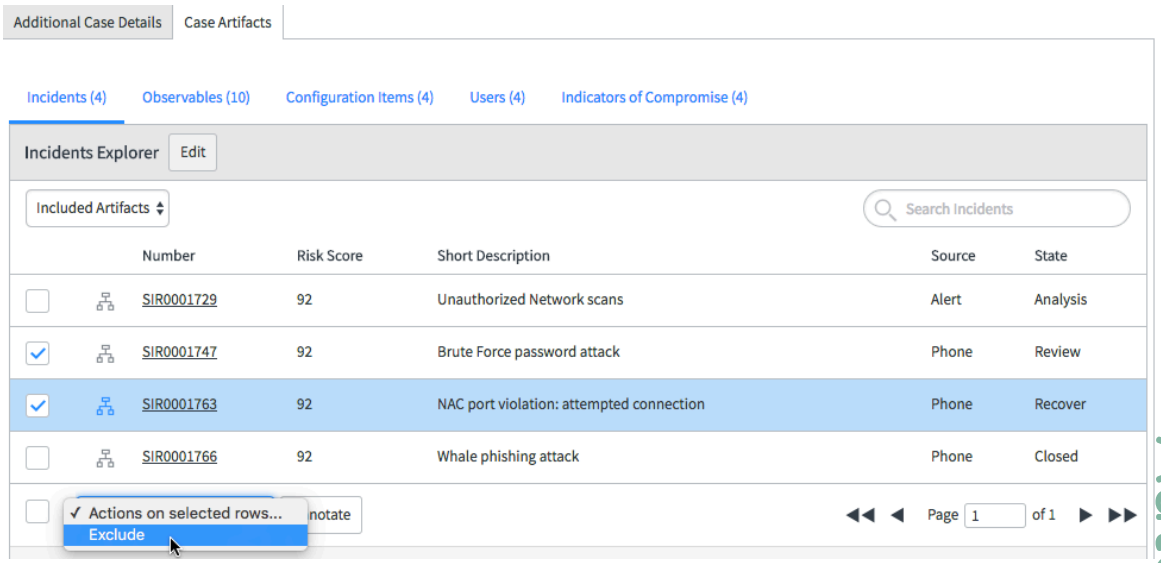
Prozedur

1. Öffnen Sie einen Fall, der Artefakte enthält, die Sie aus einer Liste ausschließen möchten.
2. Klicken Sie auf **Fallartefakte** Zugehörige Liste.
3. Klicken Sie auf die Registerkarte, die den Artefakten zugeordnet ist, die Sie ausschließen möchten. Klicken Sie beispielsweise auf **Incidents** Dient zum Ausschließen von Security Incidents aus der Liste.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie einen oder mehrere Artefaktdatensätze aus, die Sie ausschließen möchten.



5. Von **Aktionen für ausgewählte Elemente** Dropdown-Liste auswählen **Ausschließen** .
6. Klicken Sie Auf **Ausschließen** Im Bestätigungsfeld.
   Die ausgewählten Artefakte werden aus der Liste entfernt.

Ausgeschlossene Sicherheitsartefakte an einen Fall zurückgeben

Nachdem Sie Artefakte aus einer Liste in einem Fall ausgeschlossen haben, können Sie sie in den Fall zurückgeben. Sie können sie weiter bearbeiten.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

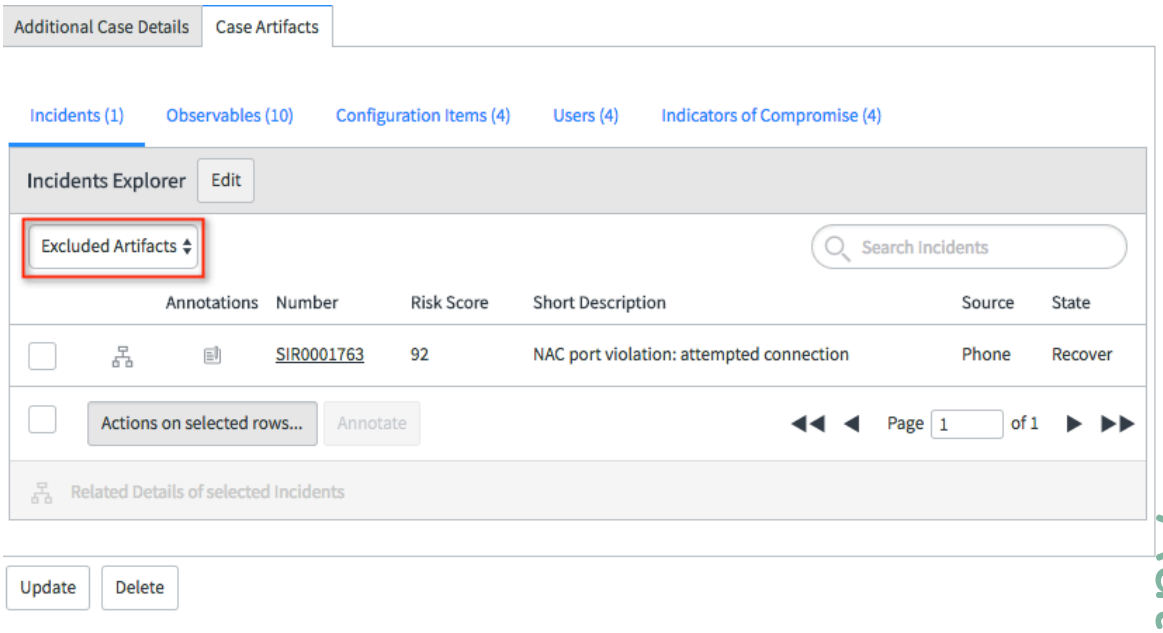
Erforderliche Rolle: sn_ti.case_user_write

Prozedur

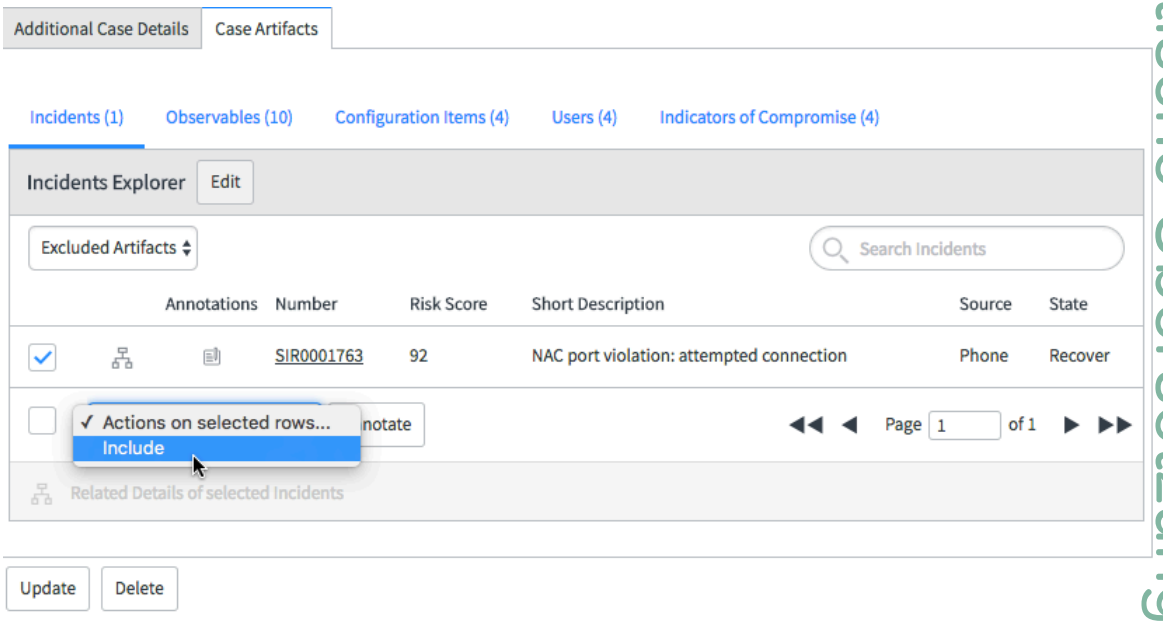
1. Öffnen Sie einen Fall, der Artefakte enthält, die Sie zuvor aus einer Liste ausgeschlossen haben, die Sie zur Liste zurückkehren möchten.
2. Klicken Sie auf **Fallartefakte** Zugehörige Liste.
3. Klicken Sie auf die Registerkarte, die den Artefakten zugeordnet ist, die Sie zur Liste zurückkehren möchten.
4. Klicken Sie auf die Dropdown-Liste Artefaktfilter, und wählen Sie aus **Ausgeschlossene Artefakte** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie einen oder mehrere Artefaktdatensätze aus, die Sie zur Einschlussliste zurückkehren möchten.
6. Von **Aktionen für ausgewählte Elemente** Dropdown-Liste auswählen **Einbeziehen** .



7. Klicken Sie Auf **Einbeziehen** Im Bestätigungsfeld.
   Die ausgewählten Artefakte werden aus der Liste der ausgeschlossenen Artefakte entfernt und an die Liste der im Fall enthaltenen Artefakte zurückgegeben.

Versehen Sie Sicherheitsartefakte mit Anmerkungen

Während Sie einen Fall analysieren, können Sie jedem Artefakt Anmerkungen hinzufügen.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

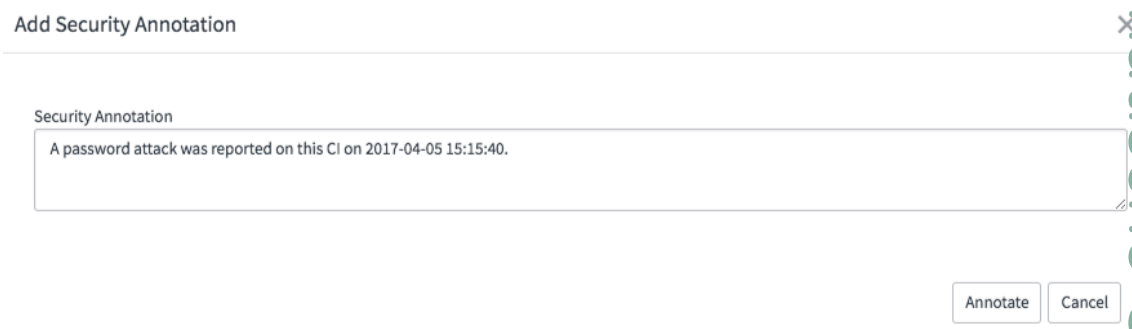
- sn_ti.case_user_write zum Hinzufügen von Anmerkungen
- sn_ti.case_user_read zum Anzeigen von Anmerkungen

Prozedur

1. Öffnen Sie einen Fall, der Artefakte enthält, die Sie kommentieren möchten.
2. Klicken Sie auf **Fallartefakte** Zugehörige Liste.
3. Klicken Sie auf die Registerkarte, die den Artefakten zugeordnet ist, die Sie mit Anmerkungen versehen möchten.
   Klicken Sie beispielsweise auf **Kompromittierungsindikatoren** Zum Hinzufügen von Anmerkungen zu IoCs.
4. Führen Sie die folgenden Schritte aus, um einem oder mehreren Artefakten eine Anmerkung hinzuzufügen:

   a. Wählen Sie die Artefakte aus, denen Sie eine Anmerkung hinzufügen möchten.

   b. Klicken Sie Auf **Anmerkungen Hinzufügen** .

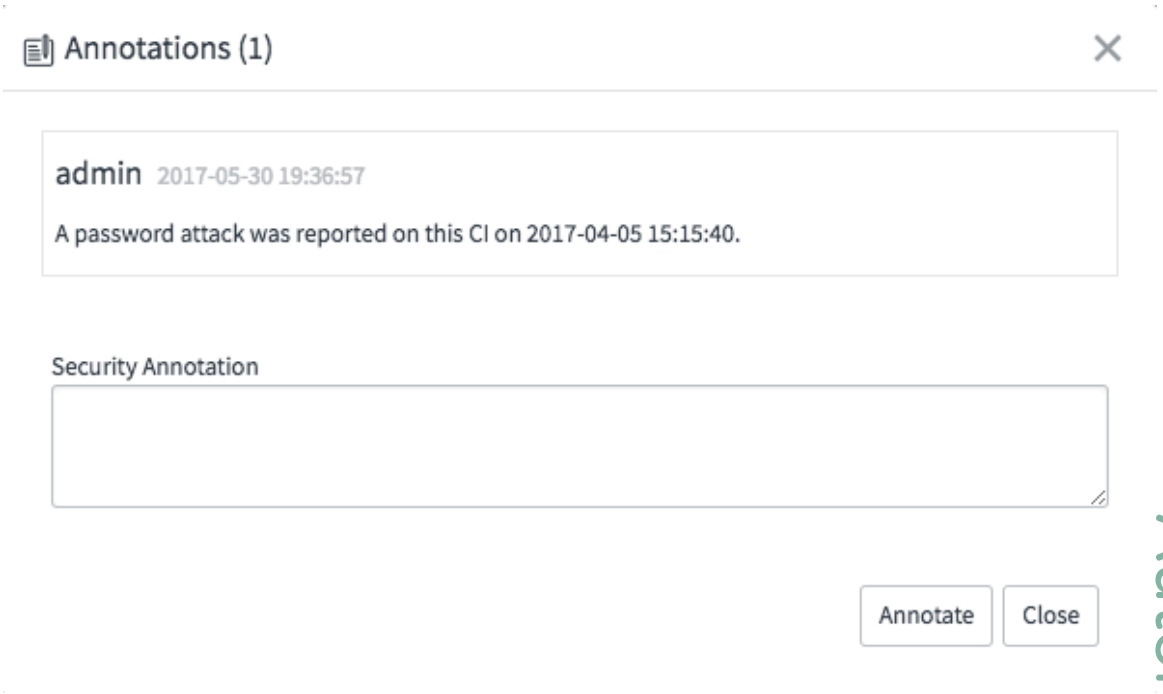


   c. Geben Sie die Anmerkung ein, und klicken Sie auf **Anmerkungen Hinzufügen** .
   Die Anmerkung wird den ausgewählten Artefakten hinzugefügt.

5. Um Anmerkungen für ein Artefakt anzuzeigen, klicken Sie auf Anmerkungen anzeigen ( )-Symbol.
   Die vorhandenen Anmerkungen werden im Dialogfeld Anmerkungen angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Sie können auch eine neue Anmerkung für das Artefakt in eingeben **Sicherheitsanmerkung** Feld, und klicken Sie auf **Anmerkungen Hinzufügen** .

Suchen Sie nach Sicherheitsartefakten

Sie können eine Stichwortsuche für jede Sicherheitsartefaktliste durchführen.

Vorbereitungen

Die Threat Intelligence Plugin muss zur Verwendung aktiviert sein Management von Sicherheitsfällen.

Erforderliche Rolle: sn_ti.case_user_write

Prozedur

1. Öffnen Sie einen Fall, der Sicherheitsartefakte enthält.
2. Klicken Sie auf die Registerkarte für die Sicherheitsartefakte, für die Sie eine Stichwortsuche durchführen möchten.
3. In **Stichwortsuche** Beginnen Sie mit der Eingabe des Namens des Artefakts, das Sie suchen möchten. Wenn Artefakte gefunden werden, die Ihrem Eintrag entsprechen, werden sie angezeigt.

Sicherheitsstatus-Überwachung

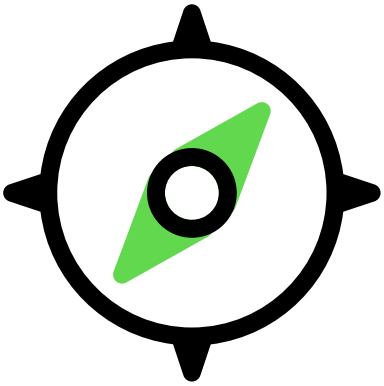
Verschaffen Sie sich Einblick in den Bestand Ihrer Enterprise-Assets und die Abdeckung von Sicherheitstools. Verwenden Sie mit dem Produkt bereitgestellte Richtlinien, oder erstellen Sie eigene, um Assets zu identifizieren, die wichtige Sicherheitstools wie Endpunktschutz, Konfigurationsmanagement und Schwachstellen-Scans fehlen. Überwachen Sie Assets für Sicherheitstoolkonfigurationen, die für Ihre Umgebung spezifisch sind, und automatisieren Sie den Korrekturworkflow für Sicherheitslücken in Konfigurations-Compliance Anwendung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

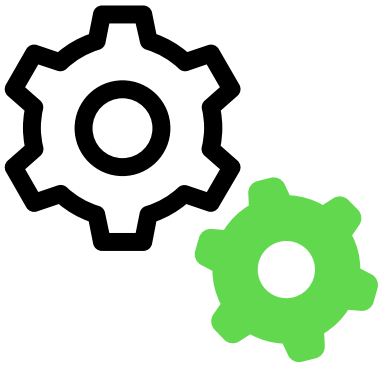
Erste Schritte

Untersuchen



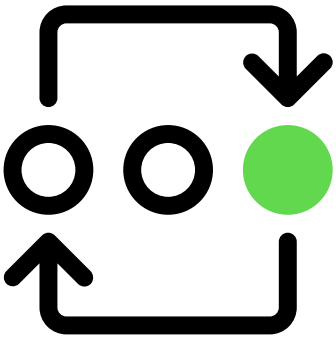
Erfahren Sie mehr über Konzepte und Funktionen der Sicherheitsstatus-Steuerung

Installieren



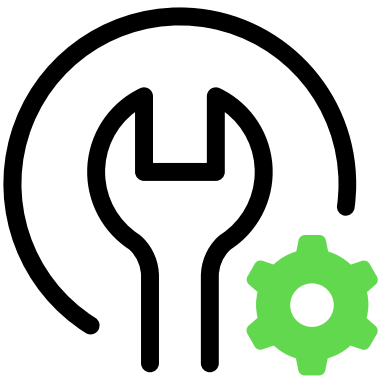
Installieren Sie Anwendungen zur Sicherheitsstatus-Steuerung

Integrieren



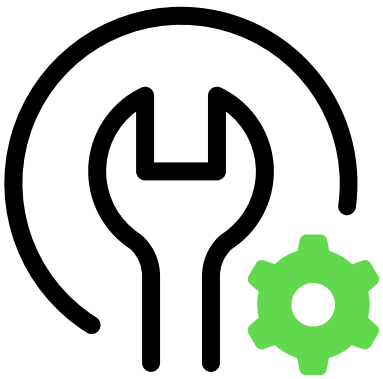
Integrieren Sie Service Graph Connectors mit der Sicherheitsstatus-Steuerung

Verwenden



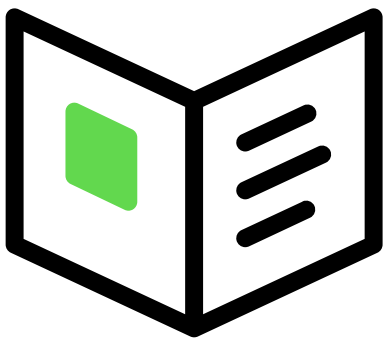
Erfahren Sie, wie Sie den Arbeitsbereich verwenden, um Ihre Assets zu durchsuchen und Sicherheitslücken zu identifizieren

Überwachung Von Minderungssteuerungen



Erhalten Sie Einblicke in die Bedrohungen für Ihre Assets durch verfügbare Minderungssteuerungen

Referenz



Rufen Sie Details zu Szenarien ab, mit denen Sie bestimmte Arten von Toolabdeckungslücken identifizieren können. Sehen Sie sich Beispiele für Basis-, untergeordnete und geklonte Richtlinien an, und sehen Sie sich eine Liste der unterstützten Hardware- und Software-Service Graph Connectors an.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Sicherheitsstatus-Überwachung erkunden

Sicherheitsstatus-Überwachung Ermöglicht Cybersicherheitsteams, Einblick in ihren gesamten Enterprise-Asset-Bestand zu erhalten und ihre allgemeine Sicherheitslage zu bestimmen.

Sicherheitsanalysten erhalten Einblicke darüber, wie gut Sicherheitstools bereitgestellt werden und ihre Assets abdecken, basierend auf ihrem Asset-Bestand und importierten Daten aus Service Graph Connectors und ServiceNow-Produkten wie Hardware Asset Management(HAM) und ITOM Discovery.

Sicherheitsanalysten können auch anwenderdefinierte Richtlinien erstellen und Einblicke konfigurieren, um die Compliance von Assets mit internen Sicherheitsstandards zu überwachen. Schwachstellenmanager können Einblicke aus verwenden Sicherheitsstatus-Überwachung(SSÜ), um die Behebung von Schwachstellen in Assets mit hohem Risiko zu priorisieren.

Das SPC-Produkt basiert auf Cloud Security Posture Management (CSPM) und Cyber Asset Hygiene Management (CAHM). Sicherheitsstatus-Überwachung Besteht aus zwei Anwendungen, die in einem separaten Abonnement von verfügbar sind ServiceNow® Store.

Freigabeversion	Release-Hinweise
Sicherheitsstatus-Steuerungskern: V6.2, v6.1, v6.0.	Informationen zur Kompatibilität finden Sie unter KB0856498 Vulnerability Response-Kompatibilitätsmatrix und Änderungen am Release-Schema Security Posture Control release notes
Sicherheitsstatus-Management für Assets: V5.3, v5.1, v5.0	
Überwachung der Minderungssteuerungen v4.0, v3.0, v2.0	

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

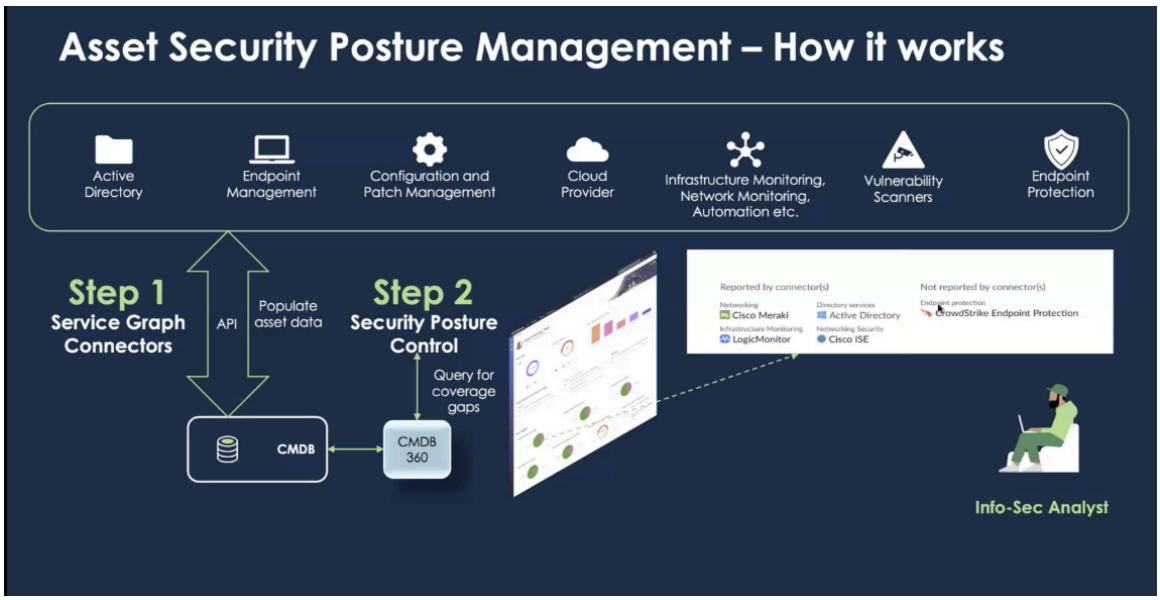
Mit SSÜ Produkt-, Info-Sec-Teams können die folgenden Aufgaben ausführen:

- Zeigen Sie Einblicke in die Sicherheitslage für Ihre lokalen und Cloud-Assets an. SSÜ Hilft Ihren Info-Sec-Teams, Assets zu identifizieren, denen Endpunktschutz fehlt, nicht verwaltete Assets, Assets, die dem Internet ausgesetzt sind, und alle Kombinationen mit hohem Risiko, die Schwachstellen enthalten.
- Überwachen Sie Ihre Assets auf Compliance mit internen Konfigurations-Standards für Sicherheitstools. Stellen Sie beispielsweise sicher, dass die neueste Version eines Endpunktschutzprodukts verwendet wird.
- Automatisieren Sie Ihren Korrektur-Workflow für die Sicherheitslücken, die Sie mit finden ServiceNow Konfigurations-Compliance-Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie anwenderdefinierte Richtlinien und Einblicke basierend auf Asset-Metadaten, Sicherheits-Tool-Abdeckungsdaten und Schwachstellendaten.
- Verschaffen Sie sich einen Einblick, welche Bedrohungen für Ihre Assets durch verfügbare Minderungssteuerungen gemindert werden, basierend auf der Konfiguration verschiedener Sicherheitstools mit Überwachung Der Minderungssteuerungen .

Funktionsweise von Sicherheitsstatus-Management für Assets



Asset Security Posture Management (ASPM) identifiziert Lücken in der Abdeckung von Sicherheitstools in Assets mithilfe von API-Integrationen mit verschiedenen Drittanbietertools (Service Graph Connectors) zusammen mit ServiceNow-Produkten.

ASPM basiert auf Daten, die in Ihrer CMDB zu Ihren Assets ausgefüllt sind. Die Asset-Daten werden von verschiedenen Kategorien von Überwachungstools importiert und verglichen, um potenzielle Sicherheitslücken zu identifizieren.

Angenommen, in der CMDB sind Asset-Daten ausgefüllt, die von Tools gemeldet werden, die Infrastrukturüberwachung und Netzwerktools abdecken. Diese Daten für dieselben Assets werden jedoch nicht von Endpunktschutztools ausgefüllt oder gemeldet. Wenn Sie die von diesen verschiedenen Tools gemeldeten Asset-Daten vergleichen, können Sie sehen, dass Assets ohne Endpunktschutz-Agent vorhanden sind.

Sicherheitsstatus-Management für Assets Identifiziert Sicherheitstool-Abdeckungslücken in Assets mithilfe von API-Integrationen mit verschiedenen Tools (Service Graph Connectors) und ServiceNow-Produkten. Zu den Kategorien gehören, sind jedoch nicht beschränkt auf:

- Digitale Mitarbeiter-Experience
- Discovery
- Endpunktverwaltung
- IT Asset Management
- Infrastrukturüberwachung
- Netzwerk
- Netzwerksicherheit
- Netzwerkleistungsüberwachung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfigurations- und Patch-Management
- Endpunktschutz
- Cloud-Provider
- Application Performance Monitoring
- Directory Services
- Schwachstellenbewertung

Die Sicherheitsstatus-Überwachung Workflow

Das Identifizieren von Lücken bei Sicherheitstools umfasst die folgenden Schritte:

1. Richten Sie API-Verbindungen mit einem der Tools ein, die Sie in verschiedenen Kategorien verwenden, und aktivieren Sie sie. Sie können Service Graph Connectors für Produkte verwenden, die im ServiceNow Store für die erforderlichen API-Verbindungen verfügbar sind. Weitere Informationen zu den unterstützten Service Graph Connectors finden Sie unter Service Graph Connectors . Unterstützte Service Graph Connectors sind über verfügbar ServiceNow® Store Mit separaten Abonnements.
2. Aktivieren Sie die mit gelieferten Richtlinien Sicherheitsstatus-Überwachung Anwendung. Die Sicherheitsstatus-Überwachung Das Produkt findet Lücken bei Sicherheitstools, indem es die folgenden Aufgaben ausführt:
   a. Gibt die Liste aller eindeutigen Assets an, die von verschiedenen Service Graph Connectors in der CMDB ausgefüllt werden.
   b. Identifiziert Assets, die nicht von bestimmten Kategorien aus diesem Asset-Pool gemeldet werden, z. B. Endpunktschutz. Assets werden basierend auf der aktiven Richtlinie identifiziert, die ausgewertet wird.
   c. Assets, die von bestimmten Kategorien als nicht gemeldet identifiziert wurden, werden als „Ergebnisse“ oder „Testergebnisse“ in gemeldet Konfigurations-Compliance Anwendung.
3. Weisen Sie „Ergebnisse“ automatisch verschiedenen Teams zur Korrektur mit der Configuration Compliance-Anwendung zu.

Kombinationen mit hohem Risiko

Mit Sicherheitsstatus-Management für Assets, Sie können auch Assets identifizieren, die Kombinationen mit hohem Risiko aufweisen. Ein Beispiel für eine Kombination mit hohem Risiko könnte Assets zeigen, denen Sicherheitstools fehlen, kritische Schwachstellen aufweisen und dem Internet ausgesetzt sind.

Einige der Richtlinien, die im Lieferumfang enthalten sind Sicherheitsstatus-Überwachung Anwendung sucht nach diesen risikoreichen Kombinationen aus kritischen Schwachstellen und Sicherheitstool-Abdeckungslücken. Damit diese Kombinationsrichtlinien funktionieren, müssen Sie jedoch über verfügen Vulnerability Response Anwendung und mindestens ein Integrationsprodukt für Schwachstellen-Scanner wie Qualys, Rapid7, Oder Tenable Vulnerability Integration Anwendung installiert. Diese Anwendungen sind mit separaten Abonnements aus dem ServiceNow Store verfügbar.

Überwachung von Risikominderungsmaßnahmen

Von innerhalb von in Sicherheitsstatus-Überwachung(SSÜ) Arbeitsbereich, erhalten Sie Einblicke darüber, welche Bedrohungen für Ihre Assets durch verfügbare Minderungssteuerungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

gemindert werden, basierend auf der Konfiguration verschiedener Sicherheitstools. Siehe Überwachung Der Minderungssteuerungen Weitere Informationen finden Sie unter .

Installieren Sie die unterstützten Anwendungen für die Sicherheitsstatus-Steuerung

Die für diese Integration erforderlichen Anwendungen sind im verfügbar ServiceNow Store. Einige Anwendungen haben Abhängigkeiten, die Sie separat herunterladen und installieren müssen.

Vorbereitungen

Erforderliche Rolle: administrator für Download, Installation und Aktivierung aller Anwendungen.

Prozedur

1. Laden Sie die erforderlichen Anwendungen aus dem herunter ServiceNow Store In Ihren ServiceNow Instanz.

   Die Sicherheitsstatus-Überwachung(SSÜ Core)-Anwendung stellt das Core-Framework bereit und ist für erforderlich Sicherheitsstatus-Management für Assets(ASPM). Die Konfigurations-Compliance Die Anwendung und ihre Abhängigkeiten ermöglichen es Ihnen, Korrekturaufgaben für die Sicherheitskontrolllücken zu erstellen, die Sie mit finden Sicherheitsstatus-Management für Assets.

Asset-Sicherheitsstatus-Management-Anwendungen

Anwendung	App-ID
Sicherheitsstatus-Management für Assets	(Plugin-ID: sn_sec_caasm)
ITOM Discovery-Lizenz	(Plugin-ID: com.snc.itom.discovery.license)
Sicherheitsstatus-Überwachung Core	(Plugin-ID: sn_sec_spc_Core)
Überwachung von Risikominderungsmaßnahmen	(Plugin-ID: sn_sec_mit_ctr)
Konfigurations-Compliance (enthält untergeordnete App secops_Shared_components)	(Plugin-ID: sn_vulc)
Vulnerability Response-Lizenzierung und -Nutzung	(Plugin-ID: sn_vul_Licensing)

Cloud-Sicherheitsstatus-Management-Anwendungen

Anwendung	App-ID
Discovery-Plugin	(Plugin-ID: Com.snc.Discovery)
Governance für Cloud-Konfigurationen	(Plugin-ID: sn_itom_ccg)
CCG-Inhaltspaket	(Plugin-ID: sn_itom_ccg_cp)
CMDB CI Class Models	(Plugin-ID: sn_cmdb_ci_class)
Cloud-Aktionsbibliothek	(Plugin-ID: com.sn.itom.cal)

Weitere Informationen zum Herunterladen und Aktivieren von Anwendungen finden Sie in den folgenden Themen:

- Laden Sie eine Anwendung aus dem herunter ServiceNow Store Zum ersten Mal.
- Aktivieren Sie einen ServiceNow Store Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Nachdem Sie die Anwendungen heruntergeladen haben, navigieren Sie zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
3. Suchen Sie die Anwendungen, die Sie heruntergeladen haben, und wählen Sie sie aus **Installieren** Um sie zusammen mit ihren Abhängigkeiten zu aktivieren.
   Alle Abhängigkeitsanwendungen, die ebenfalls automatisch zusammen mit einer Anwendung installiert werden, werden im Dialogfeld „Anwendungsinstallation“ angezeigt. Wenn Sie jedoch während der Installation aufgefordert werden, Abhängigkeits-Plugins zu installieren, befolgen Sie die angegebenen Anweisungen. Stellen Sie sicher, dass alle in der vorherigen Tabelle aufgeführten Anwendungen und Abhängigkeiten installiert und aktiviert sind.

   Ein Dialogfeld wird angezeigt, nachdem eine Anwendung erfolgreich aktiviert wurde.

   Weitere Informationen zum Herunterladen und Installieren von Anwendungen aus dem finden Sie ServiceNow Store:

   - Zum Aktivieren von ServiceNow-Produkte befolgen Sie die Schritte in Opt in to the ServiceNow Store products .
   - Zum Installieren einer Anwendung, die Sie über erworben haben ServiceNow Store, Befolgen Sie die Schritte in Install a ServiceNow Store application .
   - Alternativ, wenn Sie Ihre Berechtigung für die Anwendungen in anderen verwalten möchten ServiceNow AI Platform Führen Sie die Schritte in aus Manage entitlements from your ServiceNow instance .
4. Nachdem Sie die Anwendungen installiert und aktiviert haben, weisen Sie Anwender den folgenden Sicherheitsstatus-Steuerungsgruppen zu:

   Diese Gruppen erben alle Rollen, die zum Lesen und Bearbeiten von SPC-Datensätzen erforderlich sind.

   SPC-Administratorgruppe

   Anwender in dieser Gruppe haben vollständigen Lese- und Schreibzugriff auf alle Datensätze für das Produkt, einschließlich Lizenzierungsinformationen. Zu den granularen Rollen für diese Gruppe gehören: [sn_sec_caasm.Analyst, sn_sec_caasm.caasm_security_admin und sn_sec_spc_Core.configure].

   SPC-Analystengruppe

   Anwender in dieser Gruppe haben vollständigen Lese- und Schreibzugriff auf alle Datensätze für das Produkt, können jedoch keine Lizenzierungsinformationen anzeigen. Zu den granularen Rollen für diese Gruppe gehören [PA_Power_user und sn_sec_spc_Core.Analyst].

   Schreibgeschützte Gruppe des SPC-Analysten

   Anwender in dieser Gruppe haben vollen Lesezugriff auf alle Datensätze für das Produkt, können jedoch keine Lizenzierungsinformationen anzeigen. Zu den granularen Rollen für diese Gruppe gehören [PA_Power_user, sn_sec_spc_Core.Analyst_read, sn_sec_caasm.read und cmdb_ms_user].

   Unterstützende Anwendungsrollen

   Die folgenden Rollen sind für die in der vorangehenden Tabelle aufgeführten Anwendungen erforderlich, die unterstützen SSÜ Und Sicherheitsstatus-Management für Assets.

   - Konfigurations-Compliance Administrator [sn_vulc.admin]: Konfiguriert Konfigurations-Compliance Anwendung, hat Transparenz für alle Datensätze und kann Eigenschaften ändern. Weist Rollen in zu Konfigurations-Compliance Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vulnerability Response Administrator [sn_vulc.admin]: Konfiguriert die Vulnerability Response-Anwendung und die Schwachstellenrisikorechner.
- MID-Server [Mid_Server]: Konfiguriert einen MID-Server.

5. **Wahlweise:** Legen Sie fest **IgnorierCIClass** [sn_sec_cmn.ignoreCIClass] Systemeigenschaft zum Ignorieren einiger Konfigurationselementklassen (Configuration Item, CI) beim Ausführen von CI-Suchregeln.

   (Optional) Als SPC-Administrator und SPC-Analyst müssen Sie möglicherweise bestimmte Hardware- oder virtuelle Klassen ignorieren, damit Sie keine Informationen zu Assets erfassen, die Sie nicht steuern möchten. Siehe Erstellen Sie eine Vulnerability Response-CI-Suchregel und Ignorieren Sie CI-Klassen, um weitere Informationen zu erhalten.

6. Ändern Sie die Abstimmung, und berechnen Sie CMDB-Datenquellen neu, um die Wahrheitsquelle für Attributwerte festzulegen.

   Das CMDB 360-Dashboard bietet Zusammenfassungen und Analysen von CMDB 360-Daten. CMDB 360 erfasst Daten zu allen Discovery-Quellen, die Attributwerte für CIs melden. Verwenden Sie die CMDB 360-Ansicht im Configuration Management Database (CMDB)-Arbeitsbereich, um Aktivitäten nachzuverfolgen und potenzielle Probleme von Discovery-Quellen zu identifizieren. Weitere Informationen finden Sie unter CMDB 360 view in CMDB Workspace .

Service Graph Connectors für Sicherheitsstatus-Überwachung

Sicherheitsstatus-Überwachung Basiert auf API-Integrationen oder Service Graph Connectors als Schlüsselquelle für die Asset-Daten, die zur Identifizierung von Sicherheitslücken verwendet werden.

Sicherheitsstatus-Überwachung Unterstützt derzeit Service Graph Connectors (SGC), die Ihnen eine Vielzahl von Daten zu Ihren Assets bereitstellen können. Diese Integrationsanwendungen sind über verfügbar ServiceNow Store.

Wählen Sie die Connectors aus, die Sie verwenden möchten, laden Sie die Anwendungen herunter, und aktivieren Sie sie. Die Liste der unterstützten Connectors im Store wird als erweitert Sicherheitsstatus-Überwachung Unterstützt weitere Connectors.

Um die Vorteile von voll zu nutzen Sicherheitsstatus-Überwachung Funktionen, möchten Sie möglicherweise die folgenden Service Graph Connector-Produkte herunterladen und aktivieren, um die unten aufgeführten Kategorien zu unterstützen.

Service Graph Connectors unterstützt von Sicherheitsstatus-Überwachung Schließen Sie derzeit die folgenden Kategorien ein:

- Digitale Mitarbeiter-Experience
- Discovery
- Endpunktverwaltung: Microsoft Intune Oder Jamf-Geräte- und Endpunktverwaltung.
- IT Asset Management
- Infrastrukturüberwachung
- Netzwerk
- Netzwerksicherheit
- Netzwerkleistungsüberwachung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfigurations- und Patch-Management: Microsoft SCCM oder IBM Bigfix.
- Endpunktschutz: CrowdStrike Oder SentinelOne.
- Cloud-Provider: Amazon AWS Cloud, Microsoft Azure, GCP.

Hinweis:
Wenn Cloud-Discovery aktiviert ist, sind diese Service Graph Connector-Produkte nicht erforderlich.

- Application Performance Monitoring
- Verzeichnisservices (Active Directory) Microsoft Active Directory
- Schwachstellenbewertung: Qualys, Rapid7, Oder Tenable.

Nach der Installation können Sie die Connectors und ihre Kategorien in der Connector-Tabelle [sn_sec_spc_Core_Connector] in Ihrer Instanz anzeigen.

Sie können Asset-Typen und ihre Zuordnung zu CI-Klassen und Connectors in der Tabelle [sn_sec_spc_Core_Asset_type_Connector] anzeigen.

Siehe Unterstützte Hardware Service Graph Connectors für Sicherheitsstatus-Überwachung Und Unterstützte Software Service Graph Connectors für Sicherheitsstatus-Überwachung Für weitere Informationen und Beispiele zu diesen Tabellen. Obwohl keine umfangreichen Listen vorhanden sind, können Sie sehen, wie die unterstützten Connectors eine Vielzahl von Daten bereitstellen.

Sicherheitsstatus-Überwachung Unterstützt ServiceNow-Produkte wie Software Asset Management (SAM) und Hardware Asset Management(HAM) die Sie zusammen mit Service Graph Connectors verwenden können, um nach Diskrepanzen zu suchen, die zwischen der installierten Software, die von Ihren Schwachstellen-Scannerprodukten gemeldet wird, und der von Scannern gemeldeten Software bestehen, die bereits in SAM und anderen ServiceNow-Produkten berücksichtigt wird.

Weitere Informationen zum Herunterladen, Konfigurieren und Aktivieren unterstützter Anwendungen für Service Graph Connectors finden Sie in den folgenden Themen:

- Service Graph Connectors .
- Laden Sie eine Anwendung aus dem herunter ServiceNow Store Zum ersten Mal.
- Aktivieren Sie einen ServiceNow Store Anwendung.

Richtlinien für Sicherheitsstatus-Überwachung

Richtlinien auditieren Ihre Assets basierend auf Daten, die aus Ihren Service Graph Connectors importiert wurden, damit Sie potenzielle Verstöße finden können.

Richtlinien

Sicherheitsstatus-Überwachung Richtlinien basieren auf einem Datenmodell „Asset-Beziehungen-Eigenschaften“. Es gibt Richtlinien, die in der Anwendung enthalten sind, und Sie können eigene Richtlinien erstellen, um nach bestimmten Kriterien zu suchen.

Die Kriterien für Richtlinien können entweder in Form von Bedingungen für die Eigenschaften dieses Assets oder für die Eigenschaften einer zugehörigen Entität angegeben werden. Im Richtliniengenerator im Modul „Richtlinien und Ergebnisse“ im Arbeitsbereich können Sie Richtlinien definieren, um nach einem Asset-Typ (Hardware, Software) und einer Verbindung (gemeldet von, nicht gemeldet von) oder einer Entität (Asset-Quelle, Service Graph Connector-Produkt oder CMDB-Metadaten) zu suchen, oder Sie können andere Arten spezifischer Kriterien zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

So helfen Sie beim Ändern oder Erstellen von Richtlinien:

- Legen Sie Ihre Bedingungen im Asset-Suchmodul fest, und suchen Sie nach Assets anhand bestimmter Service Graph Connector-Produkte oder nach Assets, die bestimmte Daten enthalten, die von einem Connector gemeldet werden. Sie können Ihre Suchen als Richtlinien speichern.
- Klonen Sie die Richtlinien, die in der Anwendung enthalten sind, um umfassendere Richtlinien zu erstellen. Sie kopieren und verfeinern dann die Bedingungen einer vorhandenen Richtlinie, ohne sie erneut eingeben zu müssen.
- Erstellen Sie neue Richtlinien (untergeordnete Richtlinien) mit Basisrichtlinien, die Sie als Ausgangspunkt für neue Richtlinien auswählen.

Asset-Typen und -Richtlinien

Sie verwenden diese primären Asset-Typen oder Asset-Typen der obersten Ebene als Ausgangspunkt für die Definition von Richtlinien.

Hardware-Asset

Hardware-Asset ist eine Zusammenfassung, die jedes Gerät darstellt, das persönliche Computergeräte, Server, Netzwerkgeräte, virtuelle Cloud-Computer und andere Hardware umfasst. Richtlinien auditieren Ihre Assets basierend auf den importierten Daten aus Service Graph Connector-Produkten und auf potenzielle Verstöße ServiceNow® Produkte wie Software Asset Management (SAM) und ITOM Discovery.

Software Asset

Mit Software Asset können Sie nach Diskrepanzen suchen, die zwischen der installierten Software bestehen, die durch importierte Daten aus Service Graph Connectors gemeldet wird, Ihren Schwachstellen-Scannerprodukten und der von Scannern gemeldeten Software, die bereits in Software Asset Management (SAM) und anderen ServiceNow-Produkten berücksichtigt wird.

Entitäten und ihre Beziehungen zu sekundären Entitäten

Entität	Beziehung	Zielentität	Beschreibung
Hardware-Asset	Gemeldet von	Asset-Quelle	Stellt eine Quelle dar, die dieses Asset in CMDB gemeldet hat.
Hardware-Asset	Nur gemeldet von	Asset-Quelle	Stellt die einzige Quelle dar, die dieses Asset in CMDB meldet.
Hardware-Asset	Nicht gemeldet von	Asset-Quelle	Stellt eine Quelle dar, die dieses Asset nicht in CMDB gemeldet hat.
Hardware-Asset	Mit IRM-Ausnahme	IRM-Ausnahme	Stellt einen Ausnahmedatensatz im integrierten Risikomanagement dar.
Hardware-Asset	Mit Schwachstelle	Schwachstelle	Stellt eine Schwachstelle dar, die in diesem Asset gefunden wurde.
Hardware-Asset	Hat Konfigurationsergebnis	Konfiguration	Stellt ein Konfigurations- und Compliance-Problem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entitäten und ihre Beziehungen zu sekundären Entitäten (Fortsetzung)

Entität	Beziehung	Zielentität	Beschreibung
			dar, das für dieses Asset gefunden wurde.
Hardware-Asset	Mit CMDB-Metadaten	CMDB-Metadaten	Stellt die Sammlung von CMDB-CI-Eigenschaften für dieses Asset dar.
Hardware-Asset	Mit Connector-Daten	Service Graph Connector	Stellt eine Sammlung von Eigenschaften dar, die vom ausgewählten Service Graph Connector für dieses Asset gemeldet werden.
Hardware-Asset	Mit zusammengefassten Daten	Zusammengefasste Daten	Sammlung von Eigenschaften mit aggregierten Werten, die von verschiedenen Quellen für ein bestimmtes Asset gemeldet werden. Ein Beispiel ist das Betriebssystem.
Hardware-Asset	Von CI-Klasse	CMDB-CI-Klasse	Wird zum Definieren von Bedingungen für bestimmte CI-Klasseneigenschaften verwendet.
Hardware-Asset	Hat Cloud-Metadaten	Cloud-Metadaten	Stellt Cloud-Metadaten dar (gilt für Cloud-VMs).
Hardware-Asset	Hat einen Port, der dem Internet zugänglich ist	OpenPort	Stellt einen Port dar, der zum Internet geöffnet ist (gilt für Cloud-VMs).
Software	Gemeldet von	Asset-Quelle	Stellt eine Quelle dar, die diese Software gemeldet hat.
Software	Nur gemeldet von	Asset-Quelle	Stellt die einzige Quelle dar, die diese Software meldet.
Software	Nicht gemeldet von	Asset-Quelle	Stellt eine Quelle dar, die diese Software nicht gemeldet hat.
Software	Mit Softwaredetails	Software	Stellt die Sammlung von Softwareeigenschaften dar, z. B. Herausgeber und Version.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Richtlinien-Audit und Datenauffüllung: CI-Klassen in der CMDB

Wenn eine Richtlinie versucht, eine Asset-Klasse abzurufen, die von einem bestimmten Service Graph Connector gemeldet oder nicht gemeldet wird, ordnet die Sicherheitsstatus-Steuerung alle relevanten CI-Klassen (Configuration Item) zu, die sich auf diese Asset-Klasse in der CMDB beziehen, die von diesem Service Graph Connector oder dieser Connector-Kategorie ausgefüllt oder nicht ausgefüllt werden.

Beispiel: Eine Richtlinie sucht nach allen Hardware-Assets, die vom Service Graph Connector Jamf Pro gemeldet werden. Die folgende Logik gilt.

1. Die Sicherheitsstatus-Steuerung identifiziert, welche CI-Klassen in der CMDB der Klasse „Hardware-Asset“ für Jamf Pro zugeordnet sind.

   Hinweis:
   Verschiedene Service Graph Connectors füllen verschiedene CI-Klassen in der CMDB aus, und die Zuordnung zu CI-Klassen aus „Hardware Asset“ variiert von Service Graph Connector zu anderen.

2. Sicherheitsstatus-Überwachung Bestimmt, dass die CI-Klassen, Computer, Server und Drucker in der CMDB der Asset-Klasse „Hardware Asset“ für den Service Graph Connector Jamf Pro zugeordnet sind.
3. Sicherheitsstatus-Überwachung Fragt dann alle Asset-Datensätze ab, die in einer dieser drei CI-Klassen: Server, Computer und Drucker vom Jamf Pro Service Graph Connector in der CMDB ausgefüllt wurden, und gibt diese Assets zurück.

   Die Spalte „von SPC unterstützte CI-Klassen“ in der folgenden Tabelle gibt an, welche Klassen von CI-Datensätzen bei einer Abfrage vom Produkt „Sicherheitsstatus-Steuerung“ als Teil einer Richtlinienbewertung berücksichtigt werden. Diese Tabelle ist keine umfassende Liste, Sie können sie jedoch verwenden, um zu sehen, wie erfasste Daten aus verschiedenen Kategorien und Quellen im Allgemeinen zugeordnet und abgefragt werden.

In der Anwendung enthaltene Richtlinien

Aktivieren Sie die Asset-Profile und -Richtlinien in Sicherheitsstatus-Überwachung Arbeitsbereich, der ist In der Anwendung enthalten Damit Sie Lücken in der Konfiguration oder Abdeckung von Sicherheitstools identifizieren können.

Eigene Richtlinien werden erstellt

Siehe Erstellen Sie eigene Richtlinien in Sicherheitsstatus-Überwachung Anwendung Weitere Informationen zum Erstellen eigener Richtlinien.

Beispiele für Richtlinien finden Sie unter Beispiele für Basis-, untergeordnete und geklonte Richtlinien für Sicherheitsstatus-Überwachung.

Siehe Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung Weitere Informationen zu den Schritten, die zum Erstellen einer Richtlinie erforderlich sind.

Unterstützte SGCs

Eine Liste einiger der unterstützten Service Graph Connectors finden Sie unter Unterstützte Hardware Service Graph Connectors für Sicherheitsstatus-Überwachung Und Unterstützte Software Service Graph Connectors für Sicherheitsstatus-Überwachung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinien für Minderungssteuerungen

Von innerhalb von in Sicherheitsstatus-Überwachung(SSÜ) Arbeitsbereich, erhalten Sie Einblicke darüber, welche Bedrohungen für Ihre Assets durch verfügbare Minderungssteuerungen gemindert werden, basierend auf der Konfiguration verschiedener Sicherheitstools. Weitere Informationen finden Sie unter Richtlinien für Minderungssteuerungen.

Richtlinien, die in enthalten sind Sicherheitsstatus-Überwachung Anwendung

Es gibt einige Richtlinien, die im enthalten sind Sicherheitsstatus-Überwachung Anwendungen, die an wichtige Anwendungsfälle gebunden sind und letztendlich als wichtige Einblicke im Dashboard auf der Zielseite (Startmodul) in angezeigt werden SSÜ Arbeitsbereich.

Richtlinien werden angezeigt

Um diese Richtlinien anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Richtlinien und Ergebnisse** > **Alle**an.

Diese Richtlinien sind standardmäßig deaktiviert. Sie müssen sie aktivieren, bevor Sie zurückgegebene Ergebnisse (Ergebnisse) anzeigen können. Sie können diese Richtlinien nicht bearbeiten, aber Sie können sie verwenden, um andere Richtlinien zu erstellen, indem Sie ihre Bedingungen als Ausgangspunkt klonen. Weitere Informationen finden Sie unter Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung.

Sie können diese Richtlinien klonen, um eigene anwenderdefinierte Richtlinien zu erstellen. Beachten Sie jedoch, dass alle von Ihnen klonten Richtlinien nicht als wichtige Einblicke im Dashboard auf der Startseite mit den wichtigsten Einblicken angezeigt werden, die in der Anwendung enthalten sind. Sie können jedoch Ergebnisse für diese geklonten Richtlinien konfigurieren und die von diesen Richtlinien zurückgegebenen Ergebnisse anzeigen.

Sie können anwenderdefinierte Einblicke oder Berichte für die geklonten Richtlinien konfigurieren oder alternativ Ergebnisse für diese geklonten Richtlinien konfigurieren, um die Korrektur zu verwalten. Sie können auch eigene anwenderdefinierte Richtlinien erstellen, um die Abdeckung von Sicherheitskontrollen gemäß Ihren internen Anforderungen zu überwachen.

Die mit der Anwendung gelieferten Richtlinien umfassen die folgenden Kategorien:

- Richtlinien, die die Abdeckung von Sicherheitskontrollen überwachen (Endpunktschutz und Schwachstellenscanner).
- Richtlinien, die nicht verwaltete Geräte identifizieren.
- Richtlinien, die toxische Kombinationen überwachen, die kritische Kombinationen beinhalten, z. B. fehlende Sicherheitskontrollen, Internetrisiko usw.
- Richtlinien für SSÜ API-Integrationen für die Überwachung von Risikominderungssteuerungen.

Nachdem Sie alle von Ihnen erstellten Richtlinien geklont und aktiviert haben, müssen Sie Ihren eigenen anwenderdefinierten Einblickdatensatz im Modul „Generator für Anwenderdefinierte Einblicke“ im Arbeitsbereich (letztes Modul im Navigationsbereich) erstellen. Nur dann können Sie die Daten aus Ihren Richtlinien im Dashboard „Anwenderdefinierte Einblicke“ anzeigen (das zweite Symbol oben im Arbeitsbereich).

Richtlinien und Asset-Profile, die in der Anwendung enthalten sind

Erhalten Sie mithilfe der Richtlinien und Asset-Profile, die in der Anwendung enthalten sind, Einblicke in Ihre allgemeine Sicherheitslage und Konfigurationslücken in Ihren Sicherheitstools. Aktivieren Sie diese Asset-Profile und -Richtlinien in Sicherheitsstatus-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachung Arbeitsbereich, damit Sie Lücken in der Konfiguration oder Abdeckung der folgenden Tools identifizieren können:

- CrowdStrike
- Microsoft Intune, Defender und SCCM
- HCL Big Fix
- Qualys
- Rapid7

Eigene Richtlinien werden erstellt

Siehe Erstellen Sie eigene Richtlinien in Sicherheitsstatus-Überwachung Anwendung Weitere Informationen zum Erstellen eigener Richtlinien.

Beispiele für Richtlinien finden Sie unter Beispiele für Basis-, untergeordnete und geklonte Richtlinien für Sicherheitsstatus-Überwachung.

Siehe Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung Weitere Informationen zu den Schritten, die zum Erstellen einer Richtlinie erforderlich sind.

Siehe Richtlinien für Minderungssteuerungen Weitere Informationen zu Richtlinien, die für die Überwachung von Minderungssteuerungen verwendet werden.

Erstellen Sie eigene Richtlinien in Sicherheitsstatus-Überwachung Anwendung

Sie können eigene anwenderdefinierte Richtlinien erstellen, um Daten zu überwachen, die für die Assets in Ihrer Umgebung spezifisch sind. Diese Richtlinien basieren auf Daten, die Sie aus den verschiedenen Service Graph Connectors importieren, die Sie installiert und aktiviert haben.

So starten Sie

Sie können vorhandene Richtlinien klonen und ihnen weitere Bedingungen hinzufügen oder eine Richtlinie von Grund auf neu erstellen. Für Ihre anwenderdefinierten Richtlinien können Sie Kriterien für allgemeine CMDB-Eigenschaften einschließen, die von verschiedenen Service Graph Connectors ausgefüllt werden.

Alternativ können Sie eine Basisrichtlinie als Ausgangspunkt verwenden und Bedingungen für genehmigte Ausnahmen mit Richtlinien für die Anwendung Governance, Risk und Compliance (GRC) einschließen. Diese Ausnahmen gelten für Assets, die Sie nicht überwachen und in Ihre Asset-Anzahl einbeziehen möchten.

Für Ihre anwenderdefinierten Richtlinien können Sie Bedingungen für Metadaten wie Betriebssystem, Betriebssystemversion und FQDN einschließen, um beispielsweise Assets mit älterer Software zu überwachen. Beachten Sie, dass diese Eigenschaften allgemeine CMDB-Eigenschaften sind, die von verschiedenen Service Graph Connectors für ein bestimmtes Asset ausgefüllt werden.

Siehe Richtlinien, die in enthalten sind Sicherheitsstatus-Überwachung Anwendung Weitere Informationen zu Asset-Typen der obersten Ebene und ihren Beziehungen finden Sie im Richtlinienbedingungsgenerator für Ihre Richtlinien.

Beispiele für Richtlinien finden Sie unter Beispiele für Basis-, untergeordnete und geklonte Richtlinien für Sicherheitsstatus-Überwachung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Siehe Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung Weitere Informationen zu den Schritten, die zum Erstellen einer Richtlinie erforderlich sind.

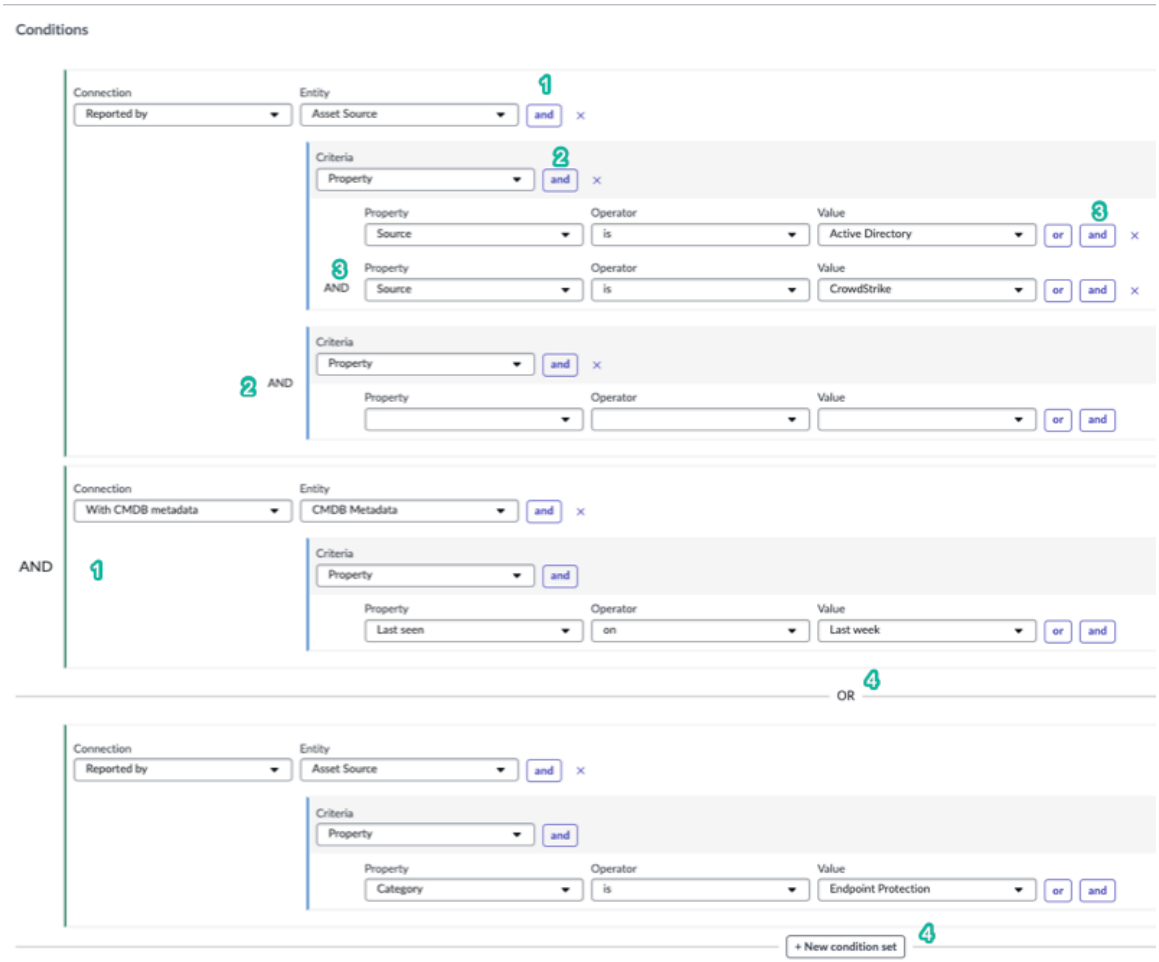
Verwenden der Decoratoren UND ODER im Bedingungsgenerator

Sie navigieren von den Asset-Typen der obersten Ebene für Hardware und Software zu ihren sekundären Entitäten, indem Sie den Bedingungsgenerator im Modul „Richtlinien und Ergebnisse“ im Arbeitsbereich verwenden. Je nach Auswahl werden Felder für Sie angezeigt, und Sie ändern oder fügen Kriterien hinzu.

Mit den Decoratoren UND ODER im Bedingungsgenerator können Sie die Logik für die zurückgegebenen Daten einrichten, die Sie für die Richtlinie zurückgeben möchten.

Decorator	Beschreibung	Nummer, auf die im Bild verwiesen wird
Wählen Sie Aus **UND** Neben den Feldern „Verbindung“ und „Entität“ oben für neue Bedingungen.	Fügt ein logisches UND zwischen den aktuellen Verbindungsentitätskriterien und neue Kriterien aus einer anderen Verbindungsentität hinzu.	1
Wählen Sie Aus **UND** Rechts neben einem Kriterien- oder Eigenschaftsfeld für neue Kriterien und Eigenschaftsbedingungen.	Fügt ein logisches UND zwischen den aktuellen Verbindungs-Entitätskriterien und ein neues Kriterium unter derselben Verbindungs-Entität hinzu.	2
Wählen Sie Aus **ODER/ UND** Rechts neben einem Eigenschaftsfeld für einen neuen Satz von Eigenschaftsbedingungen.	Fügt ein logisches ODER/UND zwischen der aktuellen Eigenschaft und einer neuen Eigenschaft aus denselben Verbindungs-Entitätskriterien hinzu.	3
Wählen Sie Aus **+ neuer Bedingungssatz** Für einen neuen Satz von Bedingungen.	Fügt ein logisches ODER zwischen dem Bedingungssatz aller aktuellen Kriterien und einem neuen Bedingungssatz hinzu.	4

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Verwenden Sie Basisrichtlinien, Klonen und untergeordnete Richtlinien

Sie können mehrere Richtlinien verwenden, um Ihre Assets zu bewerten und eigene anwenderdefinierte Einblicke zu erstellen. Sie haben die folgenden Optionen, mit denen Sie anwenderdefinierte Richtlinien schnell erstellen oder vorhandene Richtlinien bearbeiten können:

- Richtlinie klonen: Erstellt eine Kopie einer Richtlinie. Der Name der Richtlinie und ihre Bedingungen werden mit einer „Kopie“ im Titel angezeigt. Die Bedingungen werden angezeigt, und Sie können sie bearbeiten. Weitere Informationen finden Sie unter Bearbeiten Sie eine aktivierte Richtlinie in Sicherheitsstatus-Überwachung.
- Untergeordnete Richtlinie erstellen: Der Name der Richtlinie, mit der Sie begonnen haben, wird im neuen Datensatz als „Basisrichtlinie“ angezeigt. Bedingungen Ihrer Basisrichtlinie werden in die neue Richtlinie übernommen, und ein neuer, leerer Bedingungssatz wird angezeigt. Weitere Informationen finden Sie unter Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung.
- Ausschlussrichtlinien: Fügen Sie Ihren anwenderdefinierten Richtlinien Richtlinien Richtlinien hinzu, damit Asset-Ergebnisse aus den von Ihnen ausgewählten Richtlinien aus Ihren Ergebnissen ausgeschlossen werden. Weitere Informationen finden Sie unter Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung.

Metadaten- und CMDB-Filterung

Es kann für Ihre Sicherheitsteams wichtig sein, Assets mit älterer Software zu überwachen. Sie können Richtlinienkriterien beginnend mit der Verbindung „mit CMDB-Metadaten“ nach dem Hardware-Asset-Typ angeben, um die unten aufgeführten allgemeinen Eigenschaften

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einzubeziehen. Dies ist keine All-Inclusive-Liste. Um diese Metadaten zu erfassen, müssen die Eigenschaften über die CMDB-Metadatenverbindung verfügbar sein, die von Ihren Service Graph Connectors ausgefüllt wird.

- RAM
- Hostname
- Seriennummer
- BS-Domäne
- BS-Version
- Festplattenspeicher
- Zuletzt gesehen
- BS
- Zuerst gesehen
- CPU-Anzahl
- MAC-Hersteller
- NIC
- IP-Adresse
- Standort
- FQDN
- Netzmaske
- IP-Version
- Seriennummertyp
- BS-Service Pack

Beginnend mit v3.0 von Sicherheitsstatus-Überwachung:

Mit der Verbindung „mit CMDB-Metadaten“ können Sie die Eigenschaft „Hostname“ hinzufügen und den Operator für reguläre Ausdrücke für Übereinstimmungen verwenden, um reguläre Ausdrücke in Ihren Bedingungen für den Hardware-Asset-Typ einzugeben. Wenn Sie beispielsweise „lp“ eingeben, können Sie nach allen Laptops mit „lp“ als zweites und drittes Zeichen im Hostnamen suchen.

„Zuerst gesehen“: Assets, die von einer beliebigen Quelle innerhalb des von Ihnen mit der Zeitstempeleigenschaft „zuerst gesehen“ ausgewählten Zeitrahmens zum ersten Mal erkannt wurden.

„Zuletzt gesehen“: Assets, die von einer beliebigen Quelle „zuletzt gesehen innerhalb der letzten n Tage“ wurden. Geben Sie die Anzahl der Tage bis zu 30 als Wert ein. Geben Sie beispielsweise 3 als Wert ein, um Assets nach „Letzte Anmeldung“ aus Active Directory in den letzten drei Tagen zu überwachen.

Software-Asset-Typ: Suchen Sie nach Softwareherausgebern, oder verwenden Sie SGCs, die Sie installiert haben, die gewünschte Softwaredaten und Metadaten importieren, wenn Sie mit der Verbindung „mit Softwaredetails“ beginnen.

Für Hardware-Asset-Typen können Sie die Verbindung „hat Modellinformationen“ mit der Verbindung „mit CMDB-Metadaten“ für Geräte verwenden, die auf bestimmten Modellen und Modellinformationen basieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Hardware-Asset-Typen können Sie auch nach allen Assets suchen, die beispielsweise von einer Quelle, Qualys, gemeldet wurden, aber nicht von ServiceNow ITOM Discovery gemeldet werden.

Siehe Richtlinien für Sicherheitsstatus-Überwachung Weitere Informationen zu finden Sicherheitsstatus-Überwachung Richtlinienschema.

Ausnahmen mit der GRC-Anwendung (Governance, Risk and Compliance)

Eine Ausnahme für das integrierte Risikomanagement (IRM) ist ein Asset mit einer genehmigten Ausnahme vom GRC-Produkt (Governance, Risk and Compliance). Sie haben in einer Richtlinie die Möglichkeit, eine Bedingung für eine Ausnahme hinzuzufügen, damit Sie diese Assets nicht überwachen und in Ihre Anzahl aufnehmen können.

Beispielsweise können für einige Assets Ausnahmen für bestimmte Kontrollziele mit IRM genehmigt werden. Um Ihre zurückgegebenen Übereinstimmungen zu reduzieren, möchten Informationssicherheitsteams diese Assets möglicherweise von der Überwachung auf Sicherheitskontrollen mit IRM-Ausnahmen ausschließen, die bereits genehmigt wurden.

Wichtige Einblicke und konfigurierte Einblicke für Sicherheitsstatus-Überwachung

Wichtige und konfigurierte (anwenderdefinierte) Einblicke bieten Ihnen visuelle Berichte, die anhand der Bewertungskriterien erstellt und aktualisiert werden, die Ihren Assets entsprechen. Einblicke helfen Ihnen, die Metriken für Sicherheitskontrollen in einem Dashboard zu überwachen.

Wichtige Einblicke

Die für die Bewertungen Ihrer Assets verwendeten Kriterien werden von den Richtlinien bereitgestellt, die in der Anwendung enthalten sind.

- Wichtige Einblicke verwenden die Richtlinien, die in der Anwendung enthalten sind.
- Konfigurierte Einblicke können mithilfe der in der Anwendung enthaltenen Richtlinien, Ihrer eigenen anwenderdefinierten Richtlinien oder einer Kombination aus beidem erstellt werden.

Auf der Startseite (Zielseite) im Arbeitsbereich „Sicherheitsstatus-Steuerung“ werden im Abschnitt „wichtige Einblicke“ unter der Übersicht visuelle Berichte angezeigt, die durch die in der Anwendung enthaltenen Richtlinien erstellt und aktualisiert werden. Diese Einblicke sind auch in der Anwendung enthalten und zeigen die folgenden Informationen an:

- Endpunktschutz-Agent installiert: Gesamtzahl der Assets, die Endpunktschutz haben oder nicht haben.
- Abdeckung verwalteter Geräte: Anzahl der verwalteten Assets im Vergleich zu nicht verwalteten Assets.
- Abdeckung von Schwachstellen-Scans: Gesamtzahl der gescannten Assets im Vergleich zu denen, die nicht von einem Schwachstellen-Scanner einer Drittpartei auf bekannte Schwachstellen gescannt werden.
- Assets mit kritischen Schwachstellen: Anzahl der Assets von der Gesamtzahl der Assets mit kritischen Schwachstellen.
- Angreifbare Elemente nach Relevanz: Gesamtzahl der angreifbaren Elemente, aufgeschlüsselt nach Schweregrad. Eine bekannte Schwachstelle, die einem Asset in Ihrer CMDB entspricht, führt zu einem angreifbaren Element. Für diesen Einblick müssen Sie die Anwendung Vulnerability Response und mindestens eine Scannerintegration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

installieren: Qualys, Rapid7 oder Tenable Vulnerability Integration. Alle diese Anwendungen sind im verfügbar ServiceNow® Store.

- Top-3-Richtlinien nach Ergebnissen: Richtlinien, die die meisten Ergebnisse (Übereinstimmungen) für Ihre Assets zurückgeben.

Konfigurierte Einblicke

Sie können eigene Einblicke erstellen, wenn Sie möchten, dass weitere Informationen nicht in den wichtigsten Einblicken gefunden werden. Sie können diese konfigurierten Einblicke erstellen und vorhandene Richtlinien oder Ihre eigenen anwenderdefinierten Richtlinien für die Bewertung verwenden. Ihre konfigurierten Einblicke werden im Dashboard-Modul „konfigurierte Einblicke“ angezeigt, dem zweiten Symbol von oben im Arbeitsbereich.

Folgende Arten von Einblicken können konfiguriert werden.

- Vergleichsdiagramm: Vergleichen Sie Ergebnisse zwischen mehreren Richtlinien mit Balkendiagrammen.
- Widget „Anzahl der Richtlinienübereinstimmungen“: Zeigen Sie die Anzahl der Geräte an, die einer Richtlinie entsprechen.
- Prozentsatzdiagramm für Richtlinienübereinstimmung: Zeigen Sie den Prozentsatz der Geräte an, die einer Richtlinie in einem Kreisdiagramm entsprechen. Sie können den gesamten Asset-Pool entweder als alle von SPC überwachten Assets oder als Assets auswählen, die der Basisrichtlinie entsprechen, aus der die aktuell ausgewählte Richtlinie erstellt wird.
- Richtlinientrenddiagramm: Zeigen Sie die Trends von Assets an, die verschiedenen Richtlinien entsprechen.

Siehe Erstellen und aktivieren Sie einen konfigurierten Einblick für die Sicherheitsstatus-Steuerung Weitere Informationen zu den Schritten zum Erstellen eines konfigurierten Einblicks.

Gruppen

Sie müssen Gruppen erstellen oder Ihren konfigurierten Einblicken zuweisen, wenn Sie neue Datensätze im Modul „Generator für anwenderdefinierte Einblicke“ erstellen. Mit Gruppen können Sie Ihre Berichte im Dashboard „konfigurierte Einblicke“ organisieren.

Einblicke können in Gruppen organisiert werden. Jede Gruppe kann 21 Widgets oder Einblicke haben.

Mit Sicherheitsstatus-Überwachung Arbeitsbereich

Die Sicherheitsstatus-Überwachung Der Arbeitsbereich enthält die Module, die Sie zum Konfigurieren, Verwenden und Überwachen der importierten Daten zu Ihren Assets verwenden.

Rollen

SPC-Administratorgruppe

Anwender in dieser Gruppe haben vollständigen Lese- und Schreibzugriff auf alle Datensätze für das Produkt, einschließlich Lizenzierungsinformationen. Zu den granularen Rollen für diese Gruppe gehören: [sn_sec_caasm.Analyst, sn_sec_caasm.caasm_security_admin und sn_sec_spc_Core.configure].

SPC-Analystengruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender in dieser Gruppe haben vollständigen Lese- und Schreibzugriff auf alle Datensätze für das Produkt, können jedoch keine Lizenzierungsinformationen anzeigen. Zu den granularen Rollen für diese Gruppe gehören [PA_Power_user und sn_sec_spc_Core.Analyst].

Schreibgeschützte Gruppe des SPC-Analysten

Anwender in dieser Gruppe haben vollen Lesezugriff auf alle Datensätze für das Produkt, können jedoch keine Lizenzierungsinformationen anzeigen. Zu den granularen Rollen für diese Gruppe gehören [PA_Power_user, sn_sec_spc_Core.Analyst_read, sn_sec_caasm.read und cmdb_ms_user].

Unterstützende Anwendungsrollen

Die folgenden Rollen sind für die Anwendungen erforderlich, die unterstützen SSÜ Und Sicherheitsstatus-Management für Assets.

- Konfigurations-Compliance Administrator [sn_vulc.admin]: Konfiguriert Konfigurations-Compliance Anwendung, hat Transparenz für alle Datensätze und kann Eigenschaften ändern. Weist Rollen in zu Konfigurations-Compliance Anwendung.
- Vulnerability Response Administrator [sn_vulc.admin]: Konfiguriert die Vulnerability Response-Anwendung und die Schwachstellenrisikorechner.
- MID-Server [Mid_Server]: Konfiguriert einen MID-Server.

Die Module des Arbeitsbereichs

Um auf den Arbeitsbereich zuzugreifen, navigieren Sie zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** Die Startseite (Zielseite) wird angezeigt. Die Sicherheitsstatus-Überwachung Der Arbeitsbereich enthält die folgenden Module.

Module

Modul	Beschreibung
Startseite	Zeigen Sie Datenvisualisierungen und andere Informationen in den Abschnitten „Übersicht“, „wichtige Einblicke“ und „Abdeckung wichtiger Anwendungsfälle“ an, um Sie bei der Überwachung Ihrer Assets zu unterstützen. Mit den auf dieser Seite bereitgestellten Informationen können Sie IT, IT- und Sicherheitsmanagern und anderen wichtigen Stakeholdern über den Status Ihrer allgemeinen Sicherheitslage berichten. Siehe Wichtige Einblicke und konfigurierte Einblicke für Sicherheitsstatus-Überwachung und Richtlinien für Sicherheitsstatus-Überwachung.
Konfigurierte Einblicke	Zeigen Sie die Datenvisualisierungen zu Ihren Assets an, die Sie erstellen, konfigurieren und aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Module (Fortsetzung)

Modul	Beschreibung
	Weitere Informationen finden Sie unter Wichtige Einblicke und konfigurierte Einblicke für Sicherheitsstatus-Überwachung.
Asset-Suche	Suchen Sie schnell nach Assets in Ihrer Umgebung basierend auf von Ihnen festgelegten Bedingungen. Überprüfen Sie, ob Sie Assets mit einer Reihe von Bedingungen suchen können, bevor Sie diese Bedingungen für eine Richtlinie festlegen. Sie können diese Suchen verfeinern, um eine Vorschau der Assets zu erhalten, die Ihren Suchkriterien entsprechen. Wenn Sie bereit sind, können Sie Ihre Bedingungen als Richtlinie speichern. Weitere Informationen finden Sie unter Erstellen Sie eine Asset-Suche in der Sicherheitsstatus-Steuerung.
Asset-Profile	Erstellen und definieren Sie Asset-Profile, um verschiedene Gerätekategorien mit Ihren SPC-Richtlinien zu überwachen. Integrieren Sie Ihre Asset-Profile in Ihre Richtlinien, damit Sie Richtlinien für bestimmte Arten von Assets ausführen können. Filtern Sie die Einblicke im konfigurierten Dashboard „Einblicke“ so, dass sie auf Ihren Asset-Profilen basieren. Weitere Informationen finden Sie unter Erstellen Sie in ein Asset-Profil Sicherheitsstatus-Überwachung.
Richtlinien und Ergebnisse	Erstellen, klonen, bearbeiten und aktivieren Sie Richtlinien. Es gibt Richtlinien, die in der Anwendung enthalten sind, und Sie können eigene erstellen. Richtlinien auditieren Ihre Assets, um Übereinstimmungen für potenzielle Verstöße zu finden. Einblicke, Visualisierungen und Anwendungsfälle hängen von Richtlinien ab. Weitere Informationen finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung. Assets, die den Richtlinienbedingungen entsprechen, werden als Ergebnisse gemeldet und dem zugeordnet Konfigurations-Compliance Anwendung zur Korrektur. Weitere Informationen finden Sie unter Sicherheitsstatus-Steuerung: Konfigurieren und Anzeigen Ihrer Ergebnisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Module (Fortsetzung)

Modul	Beschreibung
Setup von Connectors und Anwendungsfällen	Aktivieren und zeigen Sie den Status installierter Service Graph Connectors (SGC) und API-Integrationen an. Service Graph Connectors und API-Integrationen sind Quellen, die Sie zum Importieren von Daten zu Ihren Assets verwenden. #Eine Vielzahl von (SGC)s wird unterstützt und ist über verfügbar ServiceNow® Store. Richten Sie wichtige Anwendungsfälle ein, und überwachen Sie sie. Anwendungsfälle sind verschiedene Szenarien, die Sie konfigurieren, um bestimmte Arten von Toolabdeckungslücken zu identifizieren. Jeder Anwendungsfall erfordert eine oder mehrere Richtlinien, um Ihre Assets auf potenzielle Verstöße zu überprüfen. Weitere Informationen finden Sie unter Anwendungsfälle, Richtlinienbeispiele und unterstützte Service Graph Connectors in Sicherheitsstatus-Überwachung.
Benutzerdefinierter Einblickgenerator	Erstellen Sie Ihre eigenen Datenvisualisierungen. Anwenderdefinierte Einblicke bieten Ihnen visuelle Berichte, die durch die Audit-Ergebnisse Ihrer Richtlinien und importierten Daten aktualisiert werden. Sobald Sie sie aktiviert haben, werden Ihre anwenderdefinierten Einblicke im Dashboard im Modul „konfigurierte Einblicke“ angezeigt. Mithilfe von Gruppen können Sie bestimmen, wo Daten für einen Einblick im Dashboard angezeigt werden. Weitere Informationen finden Sie unter Erstellen und aktivieren Sie einen konfigurierten Einblick für die Sicherheitsstatus-Steuerung.

Verwenden Sie die Module des Arbeitsbereichs, um Lücken in der Toolabdeckung zu identifizieren

Zur Identifizierung von Lücken bei Sicherheitstools müssen Sie die folgenden Schritte ausführen.

1. Richten Sie API-Verbindungen mit einem der Tools ein, die Sie in verschiedenen Kategorien verwenden, und aktivieren Sie sie. Sie können Service Graph Connectors für Produkte verwenden, die im ServiceNow Store für die erforderlichen API-Verbindungen verfügbar sind. Weitere Informationen zu den unterstützten Service Graph Connectors

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

finden Sie unter Service Graph Connectors für Sicherheitsstatus-Überwachung Und Service Graph Connectors . Unterstützte Service Graph Connectors sind über verfügbar ServiceNow® Store Mit separaten Abonnements.

2. Führen Sie eine oder mehrere Asset-Suchen basierend auf bestimmten Kriterien durch, um einen Bestand abzurufen.
3. Aktivieren Sie die mit der Anwendung „Sicherheitsstatus-Steuerung“ gelieferten Richtlinien. Sie können auch eigene Richtlinien erstellen und basierend auf den Ergebnissen Ihrer Asset-Suchen aktivieren.
4. Erstellen und aktivieren Sie eigene konfigurierte Einblicke, um Ihre Assets zu überwachen.
5. Informationen dazu, welche Bedrohungen für Ihre Assets durch verfügbare Minderungssteuerungen basierend auf der Konfiguration verschiedener Sicherheitstools gemindert werden, finden Sie unter Überwachung von Minderungssteuerungen mit verwenden Sicherheitsstatus-Überwachung.
6. Richten Sie Regeln ein, um den Korrektur-Workflow in der Anwendung Configuration Compliance zu automatisieren.

Das Identifizieren von Lücken bei Sicherheitstools umfasst die folgenden Schritte:

1. Aktivieren Sie die mit gelieferten Richtlinien Sicherheitsstatus-Überwachung Anwendung. Die Sicherheitsstatus-Überwachung Das Produkt findet Lücken bei Sicherheitstools, indem es die folgenden Aufgaben ausführt:
   a. Gibt die Liste aller eindeutigen Assets an, die von verschiedenen Service Graph Connectors in der CMDB ausgefüllt werden.
   b. Identifiziert Assets, die nicht von bestimmten Kategorien aus diesem Asset-Pool gemeldet werden, z. B. Endpunktschutz. Assets werden basierend auf der aktiven Richtlinie identifiziert, die ausgewertet wird.
   c. Assets, die von bestimmten Kategorien als nicht gemeldet identifiziert wurden, werden als „Ergebnisse“ oder „Testergebnisse“ in gemeldet Konfigurations-Compliance Anwendung.
2. Weisen Sie „Ergebnisse“ automatisch verschiedenen Teams zur Korrektur mit der Configuration Compliance-Anwendung zu.

Eigene Richtlinien werden erstellt

Siehe Erstellen Sie eigene Richtlinien in Sicherheitsstatus-Überwachung Anwendung Weitere Informationen zum Erstellen eigener Richtlinien.

Siehe Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung Weitere Informationen zu den Schritten, die zum Erstellen einer Richtlinie erforderlich sind.

Beispiele für Richtlinien finden Sie unter Beispiele für Basis-, untergeordnete und geklonte Richtlinien für Sicherheitsstatus-Überwachung.

Aktivieren Sie eine in enthaltene Richtlinie Sicherheitsstatus-Überwachung Anwendung

Richtlinien, die in der Anwendung enthalten sind, müssen vor aktiviert werden Sicherheitsstatus-Überwachung Kann die Assets überwachen, die dieser Richtlinie entsprechen. Standardmäßig ist keine der in der Anwendung enthaltenen Richtlinien aktiviert.

Vorbereitungen

Sie müssen sicherstellen, dass alle erforderlichen Voraussetzungen erfüllt sind, bevor Sie die in der Anwendung enthaltenen Richtlinien aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Überprüfen Sie, ob die erforderlichen Service Graph Connectors aktiviert sind.
- Überprüfen Sie, ob alle erforderlichen Anwendungen wie Vulnerability Response installiert und aktiviert sind, falls zutreffend.
- Weitere Informationen zu Richtlinien, die für die Überwachung von Minderungssteuerungen verwendet werden, finden Sie unter Richtlinien für Minderungssteuerungen.

Hinweis:

Sie können die Richtlinien, die in der Anwendung enthalten sind, nicht bearbeiten, aber Sie können neue Richtlinien basierend auf ihren Kriterien mit erstellen **Klonrichtlinie** Und **Erstellen Sie eine untergeordnete Richtlinie** Funktionen. Diese Funktionen sind im Menü „weitere Optionen“ (drei vertikale Punkte) verfügbar.

Erforderliche Rollen: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Richtlinien und Ergebnisse** > **Alle**an.

   Um festzustellen, ob eine Richtlinie aktiviert ist, bestätigen Sie ihren Status (Wahr Oder Falsch) In der Spalte aktiv.

2. Wählen Sie einen Richtliniendatensatz aus, um ihn zu öffnen.
3. Sie haben die folgenden Optionen für Richtliniendatensätze, die in der Anwendung enthalten sind:

Option	Beschreibung
Richtlinie aktivieren	Aktivieren Sie eine Richtlinie, wenn Sie Assets überwachen möchten, die den Richtlinienbedingungen entsprechen, und Ergebnisse generieren möchten. Wenn verfügbar, wählen Sie Richtlinie deaktivieren aus, um Asset-Auswertungen und Ergebnisgenerierung für diese Richtlinie zu stoppen.
Ergebnisse konfigurieren	Wählen Sie Aus **Ja** Im Modal zum Generieren von Ergebnissen für die Richtlinie. Wählen Sie aus **Konfigurieren Sie Zuweisungsregeln** Link zum Einrichten von Zuweisungsregeln in der Configuration Compliance-Anwendung, um Ergebnisse für Ihre Richtlinie zur Lösung zuzuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Hinweis: Für Richtlinien, die Sie mit „Software“ als Asset-Typ erstellen, können Sie die Richtlinie speichern und anwenderdefinierte Einblicke erstellen, Sie können jedoch keine Ergebnisse aus dem Richtliniendatensatz konfigurieren.
Richtlinie klonen	Erstellen Sie eine neue Richtlinie mit allen Bedingungen aus der angezeigten Richtlinie als Ausgangspunkt. Weitere Informationen finden Sie unter Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung.
Erstellen Sie eine untergeordnete Richtlinie	Erstellen Sie eine untergeordnete Richtlinie, die die Bedingungen der aktuellen Richtlinie erbt. Die aktuellen Richtlinienbedingungen werden im Feld „Basisrichtlinie“ im neuen Datensatz angezeigt, und Sie fügen weitere Bedingungen hinzu.
Richtlinie deaktivieren (wird nur für aktivierte Richtlinien angezeigt)	Deaktivieren Sie eine aktive Richtlinie, wenn keine Assets anhand dieser Richtlinie überwacht oder ausgewertet werden sollen. Diese Bearbeitungsoption ist nur in aktivierten Richtliniendatensätzen sichtbar.
Ergebnisse anzeigen	Öffnen Sie eine neue Registerkarte, und zeigen Sie die passenden Assets an, falls verfügbar. Ergebnisse werden auch auf CTRs oder Testergebnisdatensätze für die Richtlinie verwiesen.

Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung

Erstellen Sie eigene anwenderdefinierte Richtlinien, um Assets auf Toolabdeckung und andere Kombinationen mit hohem Risiko zu überwachen.

Vorbereitungen

Informationen zum Verständnis der Schritte, die zum Erstellen einer Richtlinie mit weiteren Details erforderlich sind, finden Sie unter Beispiele für Basis-, untergeordnete und geklonte Richtlinien für Sicherheitsstatus-Überwachung. Die Beispiele führen Sie durch die Schritte, die zum Erstellen einer Basisrichtlinie, zum Erstellen einer untergeordneten Richtlinie und zum Klonen einer Richtlinie erforderlich sind.

Beispiele für Richtlinien finden Sie unter Beispiele für Basis-, untergeordnete und geklonte Richtlinien für Sicherheitsstatus-Überwachung.

Erforderliche Rollen: SPC-Administratorgruppe oder SPC-Analystengruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Liste** > **Richtlinien** > **Alle**an.
2. Wählen Sie Aus **Neue Richtlinie** .
3. Wählen Sie das Bleistiftsymbol neben dem Namen oben aus, um die Metadaten zu ändern.

   Füllen Sie die Felder aus.

Feld	Beschreibung
Name	Ein eindeutiger Name für Ihre Richtlinie.
Relevanz	Wählen Sie einen aus der Liste aus.
Kurzbeschreibung	Eine eindeutige Beschreibung für Ihre Richtlinie.

4. Wählen Sie Aus **Speichern Sie Metadaten** .
5. Wählen Sie für Asset-Typ in der Liste ein aus.
6. **Wahlweise:** Wählen Sie keine, eine oder beide aus.

   (Optional) Die Felder Verbindung und Entität werden angezeigt.
7. Wählen Sie eine aus der Liste für das Feld Verbindung aus.
   Das Feld „Zielentität“ wird basierend auf Ihrer Auswahl automatisch ausgefüllt. Ein neues Kriterienfeld wird zusammen mit den Feldern „Eigenschaft“, „Operator“ und „Wert“ angezeigt. Weitere Informationen zu Asset-Typen und dem Schema für Beziehungen finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung.
8. Wählen Sie eine aus der Liste für Eigenschaft aus.
9. Wählen Sie Aus **Kategorie** Oder **Quelle** .
10. Wählen Sie einen Operator aus, und geben Sie eine Connector-Kategorie ein, z. B. Endpunktverwaltung oder einen Kategorienamen (Quelle).
11. **Wahlweise:** Verwenden Sie den Bedingungsgenerator, und fügen Sie weitere Bedingungen oder Bedingungssätze hinzu.

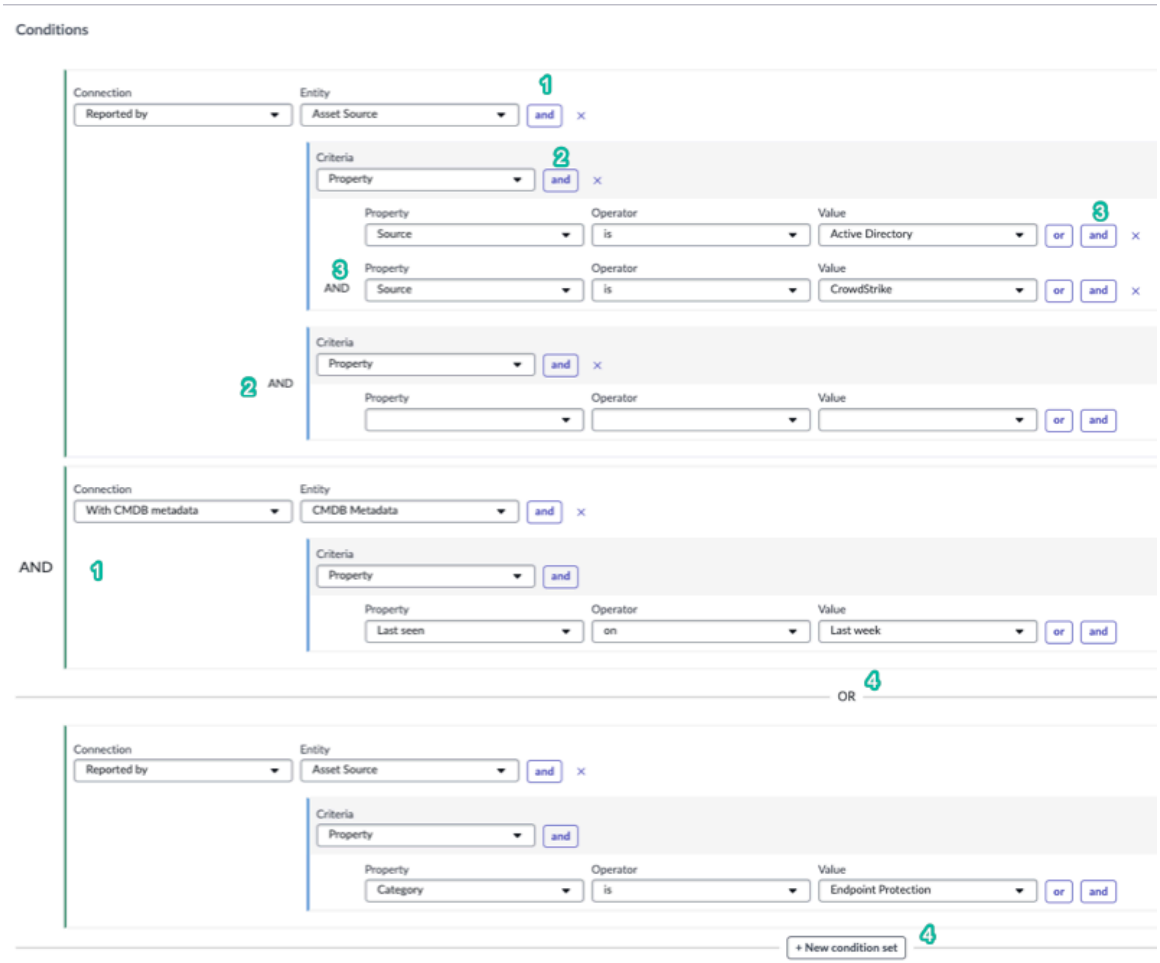
    (Optional) Sie navigieren von den Asset-Typen der obersten Ebene für Hardware und Software zu ihren sekundären Entitäten, indem Sie den Bedingungsgenerator verwenden. Je nach Auswahl werden Felder für Sie angezeigt, und Sie ändern oder fügen Kriterien hinzu.

    Mit den Decoratoren UND ODER im Bedingungsgenerator können Sie die Logik für die zurückgegebenen Daten einrichten, die Sie für die Richtlinie zurückgeben möchten. Weitere Informationen finden Sie in der folgenden Tabelle und Abbildung.

Decorator	Beschreibung	Nummer, auf die im Bild verwiesen wird
Wählen Sie Aus **UND** Neben den Feldern „Verbindung“	Fügt ein logisches UND zwischen den aktuellen Verbindungsentitätskriterien und	1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Decorator	Beschreibung	Nummer, auf die im Bild verwiesen wird
und „Entität“ oben für neue Bedingungen.	neue Kriterien aus einer anderen Verbindungsentität hinzu.	
Wählen Sie Aus **UND** Rechts neben einem Kriterien- oder Eigenschaftsfeld für neue Kriterien und Eigenschaftsbedingungen.	Fügt ein logisches UND zwischen den aktuellen Verbindungs-Entitätskriterien und ein neues Kriterium unter derselben Verbindungs-Entität hinzu.	2
Wählen Sie Aus **ODER/ UND** Rechts neben einem Eigenschaftsfeld für einen neuen Satz von Eigenschaftsbedingungen.	Fügt ein logisches ODER/ UND zwischen der aktuellen Eigenschaft und einer neuen Eigenschaft aus denselben Verbindungs-Entitätskriterien hinzu.	3
Wählen Sie Aus **+ neuer Bedingungssatz** Für einen neuen Satz von Bedingungen.	Fügt ein logisches ODER zwischen dem Bedingungssatz aller aktuellen Kriterien und einem neuen Bedingungssatz hinzu.	4



12. Wählen Sie Aus **Richtlinie speichern** Nachdem Sie mit der Bearbeitung fertig sind.
    Ihre Richtlinie wird gespeichert. Sie können es jetzt aktivieren oder später zurückkehren, um es zu aktivieren.
13. Im Menü „weitere Optionen“ neben **Richtlinie speichern** , Wählen Sie Ergebnisse konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

14. Füllen Sie die Felder aus.

Option	Beschreibung
Ergebnisse für diese Richtlinie generieren?	Wählen Sie Aus **Ja** Dient zum Generieren von Ergebnissen für übereinstimmende Assets. Nachdem Daten importiert wurden, wird die Option Suchen anzeigen im Richtliniendatensatz angezeigt. Wählen Sie Aus **Nein** Wenn Sie keine Ergebnisse generieren möchten.
Zuweisungsregeln konfigurieren	Wählen Sie den Link aus, um Zuweisungsregeln einzurichten, um Ergebnisse zur Korrektur in der Anwendung Configuration Compliance zuzuweisen. In der Tabelle [sn_vulc_assignment_rule_list] ist eine standardmäßige Zuweisungsregel vorhanden, die Sie in Configuration Compliance verwenden können.

15. Wählen Sie Aus **Speichern Sie die Konfiguration** .

Nachdem Sie eine Richtlinie gespeichert und aktiviert haben, werden die importierten Daten aus dem Service Graph Connector ausgewertet, der bei der nächsten Ausführung geplant ist. Wenn Sie die Daten im Dashboard „konfigurierte Einblicke“ im Arbeitsbereich anzeigen möchten, müssen Sie im Modul „Anwenderdefinierter Einblickgenerator“ einen neuen Einblick erstellen. Nachdem Sie den konfigurierten Einblick aktiviert haben, werden seine Daten im Dashboard „konfigurierte Einblicke“ im Arbeitsbereich angezeigt.

Bearbeiten Sie eine aktivierte Richtlinie in Sicherheitsstatus-Überwachung

Sie können aktivierte Richtlinien bearbeiten, damit Sie ihre Bedingungen besser an Ihre Assets anpassen können.

Vorbereitungen

Sie können die Richtlinien, die in der Anwendung enthalten sind, nicht bearbeiten, aber Sie können daraus untergeordnete Richtlinien klonen und erstellen. Weitere Informationen finden Sie unter Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung.

Wenn Sie Richtlinien bearbeiten und Ihre Änderungen veröffentlichen, werden Versionen nachverfolgt, und Versionsnummern werden im Richtliniendatensatz und den zugehörigen Testergebnissen angezeigt.

Bevor Sie eine aktivierte Richtlinie bearbeiten, sollten Sie sie möglicherweise deaktivieren, damit die Richtlinie Ihre Assets während der Bearbeitung nicht weiter auswertet.

Erforderliche Rollen: SPC-Administratorgruppe oder SPC-Analystengruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Liste** > **Richtlinien** > **Alle**an.
2. Wählen Sie einen Richtliniendatensatz aus, um ihn zu öffnen.
3. Wählen Sie Aus **Bearbeiten Sie die Richtlinie** .
   Wenn Sie zum ersten Mal bearbeiten, werden neben dem aktiven zwei deaktivierte Schaltflächen angezeigt **Bearbeitungsmodus beenden** Schaltfläche: **Speichern Sie die Änderungen** Und **Veröffentlichen Sie Changes** . Wenn Sie diese Richtlinie zuvor bearbeitet und als Entwurf gespeichert haben, wird die Benachrichtigung, Sie haben eine unveröffentlichte Bearbeitung Wird auch angezeigt.
4. Nehmen Sie Ihre Änderungen vor, und wählen Sie eine aus, um fortzufahren.

Option	Beschreibung
Änderungen speichern	Speichern Sie Ihre Änderungen als Entwurf, und kehren Sie zum Bearbeitungsmodus zurück. Ihre Änderungen werden zu diesem Zeitpunkt nicht veröffentlicht, und Sie können zur Richtlinie zurückkehren und später mit der Bearbeitung fortfahren.
Changes veröffentlichen	Veröffentlichen Sie Ihre Änderungen als neue Version der Richtlinie, und beenden Sie den Bearbeitungsmodus automatisch. Es kann einige Zeit dauern, bis Ergebnisse in Ihrer neuen Version der Richtlinie auf der Schaltfläche Ergebnisse anzeigen in der Richtlinie angezeigt werden. Wenn Sie eine neue Version einer Richtlinie veröffentlichen, haben Sie die Möglichkeit, alle vorhandenen Ergebnisse für die von Ihnen geänderte Richtlinie zu schließen. Möglicherweise möchten Sie alle vorhandenen Ergebnisse aus der ursprünglichen Richtlinie schließen, wenn Sie nur Ergebnisse für Ihre geänderte Richtlinie anzeigen möchten. Wenn Sie zu diesem Zeitpunkt abbrechen oder den Bearbeitungsmodus beenden, wird eine Meldung angezeigt, dass Sie eine unveröffentlichte Bearbeitung für diese Richtlinie haben. Wenn Sie die vorhandenen zugehörigen Testergebnisse (Ergebnisse) schließen, werden die statusübergänge für Testergebnisse und Korrekturaufgaben gemäß den Statusübergangsprozessen der Configuration Compliance-Anwendung abgeschlossen. Weitere Informationen finden Sie unter Statusübergänge von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Testergebnissen und Korrekturaufgaben in Sicherheitsstatus-Überwachung Anwendung.
Versionsverlauf anzeigen	Für veröffentlichte Changes werden Versionen nachverfolgt, und Versionsnummern werden im Richtliniendatensatz und den zugehörigen Testergebnissen angezeigt.
Bearbeitungsmodus beenden	Beenden Sie den Vorgang, ohne Ihre Änderungen zu speichern, oder speichern Sie Ihre Änderungen, und beenden Sie den Vorgang ohne Veröffentlichung. Wenn Sie Ihre Änderungen speichern und nicht veröffentlichen, müssen Sie Ihre neue Version veröffentlichen, bevor Ergebnisse erstellt werden können.
Richtlinie deaktivieren (wird nur für aktivierte Richtlinien angezeigt)	Deaktivieren Sie eine aktive Richtlinie, wenn keine Assets anhand dieser Richtlinie überwacht oder ausgewertet werden sollen. Diese Bearbeitungsoption ist nur in aktiven Richtliniendatensätzen sichtbar.
Ergebnisse anzeigen	Öffnen Sie eine neue Registerkarte, und zeigen Sie die passenden Assets an, falls verfügbar. Ergebnisse werden auch auf CTRs oder Testergebnisdatensätze für die Richtlinie verwiesen.

5. Nachdem Sie die Richtlinie als Entwurf gespeichert und den Bearbeitungsmodus beendet haben, wählen Sie aus den folgenden Optionen aus:

Option	Beschreibung
Richtlinie bearbeiten	Kehren Sie zum Bearbeitungsmodus zurück.
Richtlinie deaktivieren (wird nur für aktivierte Richtlinien angezeigt)	Deaktivieren Sie eine aktive Richtlinie, wenn keine Assets anhand dieser Richtlinie überwacht oder ausgewertet werden sollen. Diese Option ist nur in aktiven Richtliniendatensätzen sichtbar.
Menü „Weitere Optionen“	
Ergebnisse konfigurieren	Wählen Sie Aus **Ja** Im Modal zum Generieren von Ergebnissen für die Richtlinie. Weitere Informationen finden Sie unter Sicherheitsstatus-Steuerung: Konfigurieren und Anzeigen Ihrer Ergebnisse.
Richtlinie klonen	Erstellen Sie eine Kopie des Richtliniendatensatzes. Weitere Informationen finden Sie unter Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Untergeordnete Richtlinie erstellen	Erstellen Sie eine neue Richtlinie mit dieser Richtlinie als Basis. Weitere Informationen finden Sie unter Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung.
Richtlinie löschen	Entfernen Sie den Richtliniendatensatz aus der Richtlinienliste.
Ergebnisse anzeigen	Öffnen Sie eine neue Registerkarte, und zeigen Sie die passenden Assets an, falls verfügbar. Ergebnisse werden auch auf Testergebnisdatensätze (CTRs) für die Richtlinie verwiesen.
Zeigen Sie verknüpfte Datensätze an	Zeigen Sie für veröffentlichte Richtlinien anwenderdefinierte Einblicke an, falls verfügbar. Siehe Erstellen und aktivieren Sie einen konfigurierten Einblick für die Sicherheitsstatus-Steuerung

Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung

Klonen Sie eine vorhandene Richtlinie, und fügen Sie Bedingungen hinzu, um eine eigene anwenderdefinierte Richtlinie zu erstellen. Sie können auch untergeordnete Richtlinien aus vorhandenen Richtlinien erstellen.

Vorbereitungen

Sie können Richtlinien klonen, um eigene anwenderdefinierte Richtlinien zu erstellen. Sie können eine Richtlinie klonen oder eine untergeordnete Richtlinie mit einer beliebigen Richtlinie als Basis erstellen, um die vorhandenen Richtlinien zu erweitern, ohne die Bedingungen erneut eingeben zu müssen. Alle Bedingungen in der Basisrichtlinie werden auch in der untergeordneten Richtlinie geerbt. Weitere Informationen finden Sie unter Klonen Sie eine Richtlinie, oder erstellen Sie eine untergeordnete Richtlinie in Sicherheitsstatus-Überwachung.

Sie können alle Richtlinien klonen, die in der Anwendung enthalten sind, Richtlinienübereinstimmungen werden jedoch nicht als wichtige Einblicke im Dashboard auf der Startseite angezeigt. Nur wichtige Einblicke für Richtlinien, die in der Anwendung enthalten sind, werden auf der Startseite-Zielseite angezeigt.

Nachdem Sie alle von Ihnen erstellten Richtlinien geklont und aktiviert haben, müssen Sie im Modul „Anwenderdefinierter Einblickgenerator“ im Arbeitsbereich (letztes Modul im Navigationsbereich) einen eigenen konfigurierten Einblickdatensatz erstellen. Nur dann können Sie die Daten aus Ihren Richtlinien im Dashboard „konfigurierte Einblicke“ anzeigen (das zweite Symbol oben im Arbeitsbereich).

Erforderliche Rollen: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Liste** > **Richtlinien** > **Alle**an.
2. Wählen Sie den Richtliniendatensatz aus, den Sie klonen möchten.
3. Wählen Sie eine aus dem Menü „weitere Optionen“ neben aus **Aktivieren Sie die Richtlinie** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. **Wahlweise:** Wählen Sie Aus **Basisrichtlinie** Und wählen Sie eine Richtlinie als Basis für Ihre neue Richtlinie aus.

   (Optional) Sie können diese Option wählen, wenn Sie die Bedingungen einer vorhandenen Richtlinie als Ausgangspunkt für Ihre neue Richtlinie erben möchten.

5. **Wahlweise:** Wählen Sie Aus **Ausschlussrichtlinien** Und wählen Sie Richtlinien aus, die Sie aus den Ergebnissen dieser Richtlinie ausschließen möchten.
   Alle Ergebnisse in Ihrer neuen Richtlinie, die mit ausgeschlossenen Richtlinien übereinstimmen, werden nicht in Ihren Ergebnissen berücksichtigt.

6. Bearbeiten Sie für eine geklonte Richtlinie die Bedingungen.
   Weitere Informationen zu den Beziehungen Asset-connection-Entity im Bedingungsgenerator finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung. Weitere Informationen zu den Decorators im Bedingungsgenerator finden Sie unter Erstellen Sie eigene Richtlinien in Sicherheitsstatus-Überwachung Anwendung.

7. Bearbeiten und speichern Sie Ihre Richtlinie mit **Speichern Sie die Änderungen** .
   Ihre Richtlinie wird in der Liste alle im Listenmodul im Arbeitsbereich angezeigt.

8. Um eine Richtlinie zu aktivieren, führen Sie die unter beschriebenen Schritte aus Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung.

9. **Wahlweise:** Wählen Sie Richtlinie löschen aus, um eine Richtlinie zu löschen.
   Die Löschoption wird für Richtlinien, die im Lieferumfang der Anwendung enthalten sind, oder für Richtlinien, die Ergebnisse generiert haben, nicht unterstützt. Sie können nur Richtlinien mit Ergebnissen deaktivieren.

Erstellen und aktivieren Sie einen konfigurierten Einblick für die Sicherheitsstatus-Steuerung

Sie können eigene Einblicke erstellen. Konfigurierte Einblicke sind Einblicke, die Sie entweder mithilfe vorhandener Richtlinien oder Ihrer eigenen anwenderdefinierten Richtlinien erstellen können.

Vorbereitungen

Sie müssen einen Einblickdatensatz erstellen und aktivieren, bevor Sie Ihre Daten im Dashboard „konfigurierte Einblicke“ anzeigen können. Im konfigurierten Dashboard-Modul „Einblicke“ im Arbeitsbereich können Sie bis zu sechs Einblicke und 21 Diagramme anzeigen.

Alle Richtlinien, die Sie für einen anwenderdefinierten Einblick verwenden, müssen aktiviert sein.

Für Richtlinien, die Sie mit „Software“ als Asset-Typ erstellen, können Sie die Richtlinie speichern und anwenderdefinierte Einblicke erstellen, Sie können jedoch keine Ergebnisse aus dem Richtliniendatensatz konfigurieren.

Erforderliche Rollen: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Einblickgenerator**an.

   Auf dieser Zielseite gibt es drei Registerkarten:

   Aktiv

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihre aktivierten anwenderdefinierten Einblicke. Aktivierte anwenderdefinierte Einblicke werden auf der konfigurierten Zielseite „Einblicke“ angezeigt (zweites Symbol von oben im Arbeitsbereich).

Inaktiv

Ihre inaktiven anwenderdefinierten Einblicke. Deaktivierte Einblicke werden erst auf der konfigurierten Zielseite „Einblicke“ angezeigt, wenn die Einblicke und ihre unterstützenden Richtlinien aktiviert sind.

Alle

Alle Ihre aktiven und inaktiven konfigurierten Einblicke.

2. Wählen Sie Aus **Neuer Einblick** Rechts auf der Seite, um einen neuen Datensatz zu erstellen.
3. Wählen Sie im Feld Typ einen Einblick aus der Auswahlliste aus.

Option	Beschreibung
Vergleichsdiagramm	Vergleichen Sie die Anzahlen für übereinstimmende Assets für bis zu fünf Richtlinien.
Widget für die Anzahl der Richtlinienübereinstimmungen	Die Gesamtzahl Ihrer Assets, die einer oder mehreren Richtlinien entsprechen.
Diagramm für prozentuale Richtlinienübereinstimmung	Der Prozentsatz Ihrer gesamten Assets, die einer Richtlinie entsprechen oder nicht entsprechen.
Trenddiagramm für Richtlinienübereinstimmung	Historischer Trend von Assets, die einer Richtlinie oder einer Richtlinie entsprechen.

4. Wählen Sie eine Option aus.
   - Hardware-Asset oder virtuelle Cloud-Maschine
   - Software
5. Wählen Sie Gruppen für Ihren Einblick aus.
   Ein Einblick muss zu mindestens einer Gruppe gehören. Sie müssen Gruppen erstellen oder Ihren konfigurierten Einblicken zuweisen, wenn Sie neue Datensätze im Modul „Generator für anwenderdefinierte Einblicke“ erstellen. Mit Gruppen können Sie Ihre Berichte im Dashboard „konfigurierte Einblicke“ organisieren.
6. Wählen Sie die Richtlinien und die entsprechenden Bezeichnungen aus, die Sie für Ihre Einblickdaten benötigen.
7. Wählen Sie **Speichern**.
   Ihr Einblick wird auf der Registerkarte „inaktiver Einblick“ gespeichert.
8. Um Ihren neuen Einblick zu aktivieren, öffnen Sie den Datensatz in der Liste „Inaktiv“, und wählen Sie aus **Aktivieren** .
   Daten werden aus dem nächsten geplanten Import für die Service Graph Connectors gesammelt, die den Richtlinien des Einblicks zugeordnet sind, und Daten werden im Dashboard-Modul „Anwenderdefinierte Einblicke“ im Arbeitsbereich angezeigt.

Erstellen Sie in ein Asset-Profil Sicherheitsstatus-Überwachung

Erstellen Sie ein Asset-Profil mit Bedingungen, um Assets zu gruppieren. Sie können diese Asset-Profile in Ihren Richtlinien verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rollen: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereich Für Sicherheitsstatus-Steuerung** > **Asset-Profile**an.
2. Wählen Sie **Neu**.
   Der Bedingungsgenerator wird angezeigt. Beachten Sie, dass der Name das Datum und die Uhrzeit der Erstellung des Profils enthält.
3. Wählen Sie das Pen-Symbol aus, um den Profilnamen mit einem eindeutigen Namen zu bearbeiten.
4. Wählen Sie Aus **Speichern Sie Metadaten** .
5. Wählen Sie eine aus der Liste für Verbindung aus:

   Das Asset-Profil unterstützt drei Verbindungstypen.

   - **Mit CMDB-Metadaten** – Sammlung von CMDB-CI-Eigenschaften, z. B. Hostname, Betriebssystem, Betriebssystemversion, zuerst und zuletzt gesehen, oder Verbindungen, die Netzwerkadapter oder installierte Software haben.
   - **Mit zusammengefassten Daten** – Sammlung von Eigenschaften mit aggregierten Werten, die von verschiedenen Quellen für ein bestimmtes Asset gemeldet werden. Ein Beispiel sind die verschiedenen Möglichkeiten, wie Quellen eine Betriebssystemversion melden können: `Fenster11` , `Win11` , `Windows 11` , Und so weiter.
   - **Von CI-Klasse** – Sammlung von CI-Klassen, die Computer, Server, VM-Instanz und andere umfasst.

   Die Operatoren und Logik für diesen Asset-Profil-Richtliniengenerator ähneln denen, die in beschrieben werden Erstellen Sie eigene Richtlinien in Sicherheitsstatus-Überwachung Anwendung.
6. Wählen Sie **Erstellen** aus.
   Ihr Profil wird in der Liste Asset-Profile angezeigt.

   Sie können Asset-Profile beliebigen Richtlinien zuordnen.
7. Navigieren zu **Alle** > **Arbeitsbereich Für Sicherheitsstatus-Steuerung** > **Richtlinien und Ergebnisse**an.
8. Wählen Sie eine Richtlinie aus.
9. Wählen Sie im Abschnitt Richtlinien und Profile ein oder mehrere Asset-Profile aus.
10. Wählen Sie **Änderungen speichern**.
    Die Richtlinie auditiert Ihre Assets basierend auf Daten, die aus Ihren Service Graph Connectors importiert wurden, und enthält die Bedingungen der von Ihnen hinzugefügten Asset-Profile. Sie können Erstellen und aktivieren Sie einen konfigurierten Einblick für die Sicherheitsstatus-Steuerung Und fügen Sie Asset-Profile als Filter hinzu.
11. Navigieren zu **Alle** > **Arbeitsbereich Für Sicherheitsstatus-Steuerung** > **Konfigurierte Einblicke**an.
    Sie müssen Erstellen und aktivieren Sie einen konfigurierten Einblick für die Sicherheitsstatus-Steuerung Bevor Daten auf dieser Seite angezeigt werden.

    Da die Visualisierungen auf dieser Seite nach Richtlinien konfiguriert sind, können Sie sie mit Asset-Profilen filtern. Filtern Sie die Daten für die Visualisierungen, indem Sie die folgenden Schritte ausführen:
12. Wählen Sie das Filtersymbol aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Wählen Sie Aus **Wählen Sie Aus** .
14. Wählen Sie eines der Asset-Profile in der Spalte verfügbar aus, und verschieben Sie sie in die Spalte angewendet.
15. Wählen Sie **Übernehmen**.
    Die Visualisierungen anwenderdefinierter Einblicke werden gefiltert, um Daten für die Richtlinien anzuzeigen, die die von Ihnen ausgewählten Asset-Profile enthalten. Eine Nachricht im Bereich „Filter“ gibt an, wie viele konfigurierte Einblicke aufgrund der von Ihnen hinzugefügten Asset-Profile herausgefiltert werden. Es kann zu einer Verzögerung für Aktualisierungen von Trenddaten kommen, da die geplante Aufgabe „SPC-Richtlinie ausführen“ abgeschlossen sein muss, um Trenddaten zu aktualisieren.

Löschen Sie ein Asset-Profil in Sicherheitsstatus-Überwachung

Sie können Asset-Profile löschen. Sie löschen Asset-Profile, wenn sie Richtlinien zugeordnet sind, sodass die Bedingungen des Asset-Profils nicht im nächsten Richtlinien-Audit enthalten sind.

Vorbereitungen

Erforderliche Rollen: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereich Für Sicherheitsstatus-Steuerung** > **Asset-Profile**an.
2. Wählen Sie einen Profildatensatz aus.
3. Wählen Sie das Menüsymbol weitere Aktionen (⋮) Und wählen Sie aus **Löschen Sie das Asset-Profil** .
4. **Wahlweise:** Wählen Sie im Dialogfeld aus **Überprüfen Sie Richtlinien** Zum Anzeigen von Richtlinien, mit denen dieses Profil verknüpft ist.
   Richtlinien, die das Asset-Profil enthalten, werden auf der Registerkarte verknüpfte Richtlinien aufgelistet.
5. Wählen Sie die Registerkarte mit dem Asset-Profil aus, das Sie löschen möchten.
6. Wählen Sie das Menüsymbol weitere Aktionen aus, und wählen Sie aus **Löschen Sie das Asset-Profil** .
   Dies ist ein hartes Löschen. Die Bedingungen des Asset-Profils werden aus allen Richtlinien entfernt und nicht in die nächsten nächtlichen Richtlinien-Audits einbezogen, um die neuesten Ergebnisse zu erhalten.

Sicherheitsstatus-Steuerung: Konfigurieren und Anzeigen Ihrer Ergebnisse

Sie können die Ergebnisse, die durch die Auswertung von Richtlinien generiert wurden, in der Sicherheitsstatus-Steuerung im Arbeitsbereich „Sicherheitsstatus-Steuerung“ anzeigen.

Übersicht für Ergebnisse

Alle übereinstimmenden Assets werden als „Ergebnisse“ gemeldet. Sie können Ergebnisse konfigurieren, die aus der Ausführung von Richtlinien generiert werden, damit diese Ergebnisse verschiedenen Teams zur Korrektur zugewiesen oder für Berichte verwendet werden können. Die Sicherheitsstatus-Steuerung veröffentlicht diese Ergebnisse als „Testergebnisse“ im Modul „Konfigurations-Compliance“. Alle administrativen Steuerungen in der Configuration Compliance-Anwendung, die sich auf Zuweisung, Gruppierung (Generierung von Korrekturaufgaben), Korrekturziele und Ausnahmen beziehen, werden für Ergebnisse unterstützt, die von der Sicherheitsstatus-Steuerung generiert werden.

Die Arten der Ergebnisse:

Toolabdeckung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Typ stellt eine Abdeckungslücke des Sicherheitstools dar. Dieser Ergebnistyp gilt für Richtlinien, die Beziehungen „gemeldet von Connector“ und „nicht gemeldet von Connector“ verwenden.

Internet-Gefahrenpotenzial

Dieser Typ stellt das Internetrisiko eines Cloud-Assets dar. Dieser Ergebnistyp gilt für Richtlinien, die die Beziehung „hat-Internet-exponiert-Port“ in CloudVM verwenden.

Kombination mit hohem Risiko

Dieser Typ stellt ein Problem dar, dem mehrere Risikofaktoren zugeordnet sind, d. h. Assets mit kritischen Schwachstellen und ein fehlender Endpunktschutz-Agent.

Abhängig von den Beziehungen, die in den Richtlinien verwendet werden, sind die verfügbaren Suchtypen sichtbar, wenn Sie auswählen: **Konfigurieren Sie Ergebnisse** . Beispiel: Wenn Sie auswählen **Konfigurieren Sie Ergebnisse** Bei einer Richtlinie mit mehr als einem Risikofaktor wie „Cloud-Assets mit kritischen Schwachstellen, fehlendem Endpunktschutz und SSH-Port 22 offen für Internet“ werden die folgenden Optionen als Ergebnistypen angezeigt, die generiert werden können.

1. Kombination mit hohem Risiko
2. Toolabdeckung
3. Internet-Gefahrenpotenzial

Sie können Ergebnisse vom Typ „Kombination mit hohem Risiko“ generieren, wodurch pro Asset, das dieser Richtlinie entspricht, ein Ergebnis erstellt wird. Alternativ können Sie Ergebnisse vom Typ „Toolabdeckung“ und „Internetrisiko“ erstellen, was zu zwei Ergebnissen führt, die pro Asset erstellt werden, die der Richtlinie entsprechen: Einer vom Typ „Toolabdeckung“ und einer vom Typ „Internetrisiko“.

Mithilfe der Art der Ergebnisse oder des Testergebnisses können Sie Zuweisungsregeln in Configuration Compliance schreiben, um diese Probleme zur Behebung an die jeweiligen Teams weiterzuleiten. Sie können beispielsweise „Toolabdeckung“-Ergebnisse an das IT-Betriebsteam und „Internetrisiko“ an das Anwendungsteam senden.

Wenn jedoch einer der Korrekturbesitzer das Problem behebt, wird das andere Ergebnis automatisch geschlossen, da diese Ergebnisse aus einer Richtlinie generiert werden, die nach der Kombination sucht. Wenn das IT-OPS-Team beispielsweise das Ergebnis „Toolabdeckung“ durch die Installation des Endpunktschutz-Mitarbeiters schließt, wird das Ergebnis „Internetrisiko“, das aus dieser Richtlinie generiert wird, automatisch geschlossen, auch wenn das Asset mit Internetzugriff verbunden ist, da dieses Ergebnis aus einer Richtlinie generiert wird, die nach einer Kombination von Problemen sucht. Wenn Sie das Problem mit dem Internetrisiko für Assets nachverfolgen möchten, wird empfohlen, eine andere Richtlinie zu erstellen, die nur nach dem Internetrisiko für die Assets und nicht nach einem anderen Risikofaktor sucht.

Wo Ergebnisse angezeigt werden sollen

Sie haben diese Optionen, um die Ergebnisse anzuzeigen, die durch die Auswertung von Richtlinien generiert wurden.

- Navigieren zu **Arbeitsbereich Für Sicherheitsstatus-Steuerung** > **Listen** > **Ergebnisse** > **Alle.**
- Wählen Sie in einem Richtliniendatensatz aus **Zeigen Sie Ergebnisse an** .
- Wählen Sie in der Anwendung Konfigurations-Compliance die Option aus **Testergebnisse** Und filtern Sie die Datensätze nach **Quelle ist ServiceNow SPC** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Dashboard

Im Arbeitsbereich „Sicherheitsstatus-Steuerung“ werden auf der Startseite (Zielseite) die folgenden Visualisierungen angezeigt:

Übersicht

- Assets: Die Anzahl der Assets, die lokal und in der Cloud überwacht werden.
- Ergebnisse nach Relevanz: Die Anzahl der kritischen Ergebnisse aus Ihren gesamten Assets.
- Assets, die von den Top-5-Quellen überwacht werden: Die Top-fünf Service Graph Connectors, die Berichte zu Assets erstellen.
- Cloud-Accounts: Die Anzahl der Cloud-Accounts, die von AWS und Azure überwacht werden.
- Offene vs. Geschlossene Ergebnisse: Ein Vergleich von Datensätzen, die noch verarbeitet werden oder auf eine Lösung warten, und denen, die gelöst wurden.

Wichtige Einblicke

- Endpunktschutz-Agent installiert: Die Gesamtzahl der Assets mit Endpunktschutz oder nicht mit Endpunktschutz.
- Abdeckung verwalteter Geräte: Die Anzahl der verwalteten Assets im Vergleich zu nicht verwalteten Assets.
- Abdeckung von Schwachstellen-Scans: Die Gesamtzahl der gescannten Assets im Vergleich zur Anzahl, die nicht von einem Schwachstellen-Scanner einer Drittpartei auf bekannte Schwachstellen gescannt werden.
- Assets mit kritischen Schwachstellen: Die Anzahl der Assets aus der Gesamtzahl der Assets mit kritischen Schwachstellen.
- Angreifbare Elemente nach Relevanz: Die Gesamtzahl der angreifbaren Elemente, aufgeschlüsselt nach Schweregrad. Eine bekannte Schwachstelle, die einem Asset in Ihrer CMDB entspricht, führt zu einem angreifbaren Element.
- Top-3-Richtlinien nach Ergebnissen: Die Richtlinien, die die meisten Ergebnisse (Übereinstimmungen) für Ihre Assets zurückgeben.

Abdeckung wichtiger Anwendungsfälle

Wählen Sie eine Visualisierung und aus **Helfen Sie, sich zu verbessern** Um anzuzeigen, welche Service Graph Connectors und Richtlinien für die wichtigsten Anwendungsfälle aktiviert sind.

Statusübergänge von Testergebnissen und Korrekturaufgaben in Sicherheitsstatus-Überwachung Anwendung

Die status von Ergebnissen (Konfigurationstestdatensätze) und die zugehörigen Korrekturaufgaben sind betroffen, wenn Sie Ihre Richtlinien in der Anwendung „Sicherheitsstatus-Steuerung“ ändern.

Statusübergangsszenarien zwischen Testergebnissen und Korrekturaufgaben

Mit einigen Ausnahmen wechseln status im Allgemeinen zwischen Ihren Ergebnissen (Testergebnissen) und den zugehörigen Korrekturaufgaben in der Sicherheitsstatus-Steuerung auf die gleiche Weise zwischen Testergebnissen und Korrekturaufgaben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in der Konfigurations-Compliance Anwendung. Wenn Sie jedoch Ihre Richtlinien in der Sicherheitsstatus-Steuerung ändern, wirken sich Ihre Änderungen auf den statusübergang für Ihre Ergebnisse und die zugehörigen Korrekturaufgaben aus.

Die folgenden Tabellen veranschaulichen, wie status Ihrer Ergebnisse übergehen, wenn Sie eine neue Version bearbeiten und veröffentlichen (bearbeiten), Ihre Richtlinien deaktivieren oder löschen.

Für weitere Informationen zu Statusänderungen in Konfigurations-Compliance, Siehe Statusübergänge von Testergebnissen und Korrekturaufgaben in Konfigurations-Compliance Anwendung.

Hinweis:
Ab v14.9 von Konfigurations-Compliance, Die folgenden Begriffe wurden umbenannt:

Änderungen in der Terminologie

Terminologie vor v14.9	Terminologie v14.9 und höher
Testergebnisgruppe	Fehlerbehungsaufgabe
Gruppenregeln	Regeln für Korrekturaufgaben
Richtlinie	Testgruppe

Erweiterungen an Richtlinien-Audits stellen sicher, dass stillgelegte Assets nicht durch aktivierte Richtlinien bewertet werden. Wenn der Status eines Assets von übergeht **Stillgelegt** Zurück zu **Aktiv** , Ist in der nächsten Richtlinienbewertung enthalten.

Wenn eine Richtlinie...	Feldwerte in vorhandenen Ergebnisdatensätzen für...	Übergang zu...
Deaktiviert	Ergebnis	Ursprüngliche Werte beibehalten
	Status	Geschlossen
	Lösung	Veraltet

Wenn eine Richtlinie...	Feldwerte in vorhandenen Ergebnisdatensätzen für...	Übergang zu...
Wurde mit der Option zum Schließen vorhandener Ergebnisse bearbeitet	Ergebnis	Ursprüngliche Werte beibehalten
	Status	Geschlossen
	Lösung	Ergebnis ungültig

Wenn eine Richtlinie...	Feldwerte in vorhandenen Ergebnisdatensätzen für...	Übergang zu...
Wurde mit der Option bearbeitet, alle ausgewählten vorhandenen Ergebnisse beizubehalten	Ergebnis	Gültige (bestandene) Testfälle behalten die ursprünglichen Werte bei, und ungültige Testfälle (Fehlgeschlagen) werden geschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine Richtlinie...	Feldwerte in vorhandenen Ergebnisdatensätzen für...	Übergang zu...
	Status	Geschlossen
	Lösung	Ergebnis ungültig

Wenn eine Richtlinie...	Feldwerte in vorhandenen Ergebnisdatensätzen für...	Übergang zu...
Gelöscht	Ergebnisse	Ursprüngliche Werte beibehalten
	Status	Geschlossen
	Lösung	Ergebnis ungültig

Erstellen Sie eine Asset-Suche in der Sicherheitsstatus-Steuerung

Legen Sie Ihre Bedingungen fest, und suchen Sie nach Assets anhand bestimmter Service Graph Connector-Produkte oder nach Assets, die bestimmte Daten enthalten, die von einem Connector gemeldet werden.

Vorbereitungen

Angenommen, Sie möchten Ihre Assets mit Windows-Servern und einer bestimmten Version identifizieren, die in gefunden wurden CrowdStrike Metadatendetails.

Erforderliche Rollen: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Asset-Suche**an.
2. Wählen Sie eine aus.
   Wählen Sie für dieses Beispiel aus **Hardware-Asset** Für Asset-Typ.
3. **Wahlweise:** Wählen Sie Aus **Basisrichtlinie** Und **Ausschlussrichtlinien** Wenn Sie die Bedingungen einer vorhandenen Richtlinie als Start verwenden und Assets ausschließen möchten, die den vorhandenen Richtlinien entsprechen.
   Die von Ihnen ausgewählten Richtlinien werden angezeigt.
4. Wählen Sie Aus **Mit Connector-Daten** Für das Feld Verbindung.
5. Wählen Sie Aus **CrowdStrike-Gerätedetails** Für die Entität.
6. Wählen Sie für Eigenschaft, Operator und Wert die Option aus **[Agent-Version][ist]** Und geben Sie die Version ein, z. B. **6.26.14003.0** .
7. Wählen Sie den Operator und rechts neben dem Feld Entität mit aus CrowdStrike Gerätedetails als Wert für eine andere Bedingung.
8. Wählen Sie Aus **Mit CMDB-Metadaten** Für das Feld Verbindung.
   Das Feld Entität wird mit CMDB-Metadaten ausgefüllt.
9. Wählen Sie Aus **Eigenschaft** Für das Feld Kriterien.
10. Wählen Sie für Eigenschaft, Operator und Wert die Option aus **[BS][enthält]** Und geben Sie ein **Windows-Server** .
11. Wählen Sie Aus **Zeigen Sie Assets an** .
    Nach einigen Minuten werden die Ergebnisse auf der Registerkarte übereinstimmende Assets angezeigt.
    Wenn keine Übereinstimmungen angezeigt werden, können Sie Ihre Suche einschränken. Nachdem Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zufrieden sind, dass Sie die Bedingungen richtig festgelegt haben, können Sie die Suche als Richtlinie speichern und aktivieren. Wie andere Richtlinien durchsucht sie Ihre Assets kontinuierlich mit einem Hintergrundauftrag, nachdem Sie sie aktiviert haben.

Doppelte Konfigurationselemente in werden aufgelöst Sicherheitsstatus-Überwachung

Durch das Auflösen doppelter Einträge für Konfigurationselemente (Configuration Items, CIs) in Ihrer Konfigurationsmanagement-Datenbank wird sichergestellt, dass Sie genaue Audits mit erhalten SSÜ Richtlinien.

Übersicht über doppelte Konfigurationselemente

In bestimmten Fällen importieren Ihre Asset-Discovery-Quellen, d. h. Ihre Service Graph Connector-Produkte (SGCs), Asset-Daten, die möglicherweise doppelte Einträge in Ihrer Configuration Management Database (CMDB) für Assets (Konfigurationselemente) erstellen. Diese doppelten CI-Datensätze treten auf, wenn zwei oder mehr Assets in Ihrer CMDB mit denselben Namen aufgeführt sind, die CMDB-Referenzen jedoch unterschiedlich sind.

Ein Beispiel könnte ein Asset sein, das nach seiner IP-Adresse benannt wird. 10.0.2.11 , Die zweimal in der Tabelle „CMDB 360-Daten“ [cmdb_Multisource_Data] aufgeführt ist. Ein Eintrag für 10.0.2.11 Ist in der CMDB-Referenzspalte als aufgeführt 10.0.2.11 , Und eine weitere wird als aufgeführt 10.0.65.159 . Diese Assets können aus derselben Discovery-Quelle, einem SGC-Produkt, oder aus zwei oder mehr Discovery-Quellen stammen. Um in beiden Fällen Probleme mit SPC-Richtlinien und Ihren Asset-Beständen zu vermeiden, müssen Sie die doppelten CIs entfernen.

Identifizieren und Entfernen doppelter Konfigurationselemente

Sie können doppelte CIs identifizieren, indem Sie nach der Spalte Name in der Tabelle [sn_sec_spc_Core_Asset_Cache] filtern und notieren, welche Assets denselben Namen haben.

Wenn Sie Duplikate identifizieren, wird der CI-Deduplizierung Der Prozess enthält eine Deduplizierungsvorlage, die Sie veröffentlichen müssen, eine Systemeigenschaft, die Sie aktivieren, und eine geplante Aufgabe, die doppelte CIs in der Tabelle „zwischengespeicherte SPC-Assets“ [sn_sec_spc_Core_Asset_Cache] entfernt. Der Prozess entfernt Duplikate und behält den Master- oder kanonischen CI-Datensatz mit den am meisten zugehörigen Elementen bei.

Lösen Sie doppelte Konfigurationselemente in auf Sicherheitsstatus-Überwachung

Verwenden Sie diesen Prozess, um doppelte Konfigurationselemente in der Tabelle „zwischengespeicherte SPC-Assets“ [sn_sec_spc_Core_Asset_Cache] zu entfernen. Dieser Prozess entfernt doppelte Datensätze und behält den Master- oder kanonischen Asset-Datensatz mit den am meisten zugehörigen Elementen bei.

Vorbereitungen

Erforderliche Rollen: sn_cmdb_user für den Zugriff auf den CMDB-Arbeitsbereich und sn_sec_spc_Core.admin zum Initiieren der geplanten Aufgabe

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
2. Suchen Sie die Systemeigenschaft sn_sec_spc-Core.is_ci_Name_unique.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dies ist ein konfigurierbarer Wert in der Eigenschaft, der angibt, ob alle Konfigurationselemente, die in Ihrer CMDB- oder Asset-Cache-Tabelle aufgeführt sind, eindeutige Namen haben.

Siehe Doppelte Konfigurationselemente in werden aufgelöst Sicherheitsstatus-Überwachung Weitere Informationen zum Identifizieren doppelter CIs.

3. Wählen Sie den Datensatz aus, um ihn zu öffnen, und legen Sie das Wertfeld auf fest **Wahr** .
4. Aktualisieren Sie den Datensatz.
5. Navigieren zu **CMDB-Arbeitsbereich** > **Management** Und wählen Sie den Link Deduplizierungsvorlagenbibliothek unter Verwaltungstools auf der rechten Seite aus.

   Hinweis:
   Die Rolle sn_cmdb_user ist für den Zugriff auf den CMDB-Arbeitsbereich erforderlich.

6. Erweitern Sie im Bereich Deduplizierungsvorlagen **SPC-Deduplizierungsvorlagen** Und wählen Sie aus **Name Flip-Flop** Um es zu öffnen.
7. Wählen Sie **Veröffentlichen** aus.
8. Wählen Sie Aus **Veröffentlichen** Im Modal.

   Sie haben die Deduplizierungsvorlage veröffentlicht und die Systemeigenschaft sn_sec_spc-Core.is_ci_Name_unique aktiviert. Sie müssen die geplante Aufgabe „Deduplizierungsaufgabe generieren“ ausführen, um die Aufgaben zu generieren, die die duplizierten CIs lösen.

9. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben** > **Deduplizierungsaufgabe generieren** Und wählen Sie den Datensatz aus, um ihn zu öffnen.
10. Wählen Sie **Jetzt ausführen**.
    Stellen Sie sicher, dass der Hintergrundauftrag in die Warteschlange gestellt ist und verarbeitet wird.
11. Navigieren Sie zu **Hintergrundaufträge [sn_sec_cmn_background_Job]** Tabelle zur Überwachung der geplanten Aufgabe „Deduplizierungsaufgabe generieren“.
    Wenn die geplante Aufgabe erfolgreich abgeschlossen (abgeschlossen) wurde, können Sie die von Ihnen veröffentlichte Vorlage initiieren.
12. Navigieren zu **CMDB-Arbeitsbereich** > **Management** Und wählen Sie aus **Deduplizierungs-Dashboard anzeigen** .
13. Wählen Sie Aus **Wird Ausgeführt** Zum Laden der Vorlage.
14. Wählen Sie aus **Abgeschlossen** Registerkarte zum Anzeigen der abgeschlossenen Aufgaben.

    Sie müssen sicherstellen, dass die Deduplizierungsaufgaben abgeschlossen wurden, bevor Sie die Tabelle „zwischengespeicherte SPC-Assets“ [sn_sec_spc_Core_Asset_Cache] auf Duplikate überprüfen.

    Möglicherweise müssen Sie Ihren Bildschirm aktualisieren, um die abgeschlossenen Aufgaben anzuzeigen.

15. Wenn die geplante Aufgabe erfolgreich abgeschlossen wurde und Sie verifiziert haben, dass die Deduplizierungsaufgaben abgeschlossen sind, navigieren Sie zur Tabelle „zwischengespeicherte SPC-Assets“ [sn_sec_spc_Core_Asset_Cache], filtern Sie die Spalte Name, und überprüfen Sie auf Duplikate.
    Der Master oder kanonische ist der CI-Datensatz, der die am meisten zugehörigen Elemente enthält. Sie wird in der Tabelle beibehalten. Wenn keine Duplikate vorhanden sind, überprüfen Sie die Tabelle „CMDB 360-Daten“ [cmdb_Multisource_Data] auf Duplikate.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

16. Navigieren Sie zur Tabelle CMDB 360-Daten [cmdb_Multisource_Data].
17. Gruppieren Sie nach Spalte 0, und überprüfen Sie, ob andere CMDB-Referenzen für Assets vorhanden sind, die der Namensspalte der Tabelle „zwischengespeicherte SPC-Assets“ [sn_sec_spc_Core_Asset_Cache] entsprechen.
    Wenn Sie Duplikate finden, führen Sie die geplante Aufgabe Deduplizierungsaufgabe generieren erneut aus.

Überwachung von Minderungssteuerungen mit verwenden Sicherheitsstatus-Überwachung

Von innerhalb von in Sicherheitsstatus-Überwachung(SSÜ) Arbeitsbereich, erhalten Sie Einblicke darüber, welche Bedrohungen für Ihre Assets durch verfügbare Minderungssteuerungen gemindert werden, basierend auf der Konfiguration verschiedener Sicherheitstools.

Überwachung der Minderungssteuerungen

Für unterstützte Anwendungen für Sicherheitsstatus-Überwachung Und Überwachung der Risikominderungssteuerungen, siehe Sicherheitsstatus-Überwachung erkunden.

Die Sicherheitsstatus-Überwachung Die Anwendung konzentriert sich auf drei zentrale Problembereiche:

- Asset-Bestand: Identifizierung aller Ihrer Enterprise-Assets, die nicht verwaltete oder unbekannte Assets enthalten.
- Abdeckung und Integrität der Sicherheitskontrollen: Identifizierung von Abdeckungslücken mit Ihren Sicherheitskontrollen
- Sichtbarkeit von Schwachstellen und Bedrohungsminderung: Identifizierung, welche Bedrohungen oder Schwachstellen für Ihre Assets durch entsprechende Minderungssteuerungen gemindert werden.

Die Überwachung von Minderungssteuerungen beschreibt die Funktionen in Sicherheitsstatus-Überwachung Die unter die Transparenz von Schwachstellen und Bedrohungsminderung fallen.

Erforderliche Rollen:

- administrator: Installiert Anwendungen aus dem ServiceNow® Store Und aktiviert Plugins (ITOM Discovery).
- SSÜ Administratorgruppe und SSÜ Analystengruppe: Anwender in dieser Gruppe haben vollen Lese- und Schreibzugriff auf alle Datensätze für das Produkt und den Arbeitsbereich.
- SSÜ Schreibgeschützte Gruppe für Analysten: Anwender in dieser Gruppe haben vollen Lesezugriff auf alle Datensätze für das Produkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachung der Minderungssteuerungen Anwender und Vorteile

Anwender

Anwender	Beschreibung
Cybersicherheitsteams, Sicherheitsanalysten und Manager	• Verschaffen Sie sich Einblick in alle Ihre Enterprise-Assets, einschließlich nicht verwalteter oder unbekannter Assets. • Identifizieren Sie Abdeckungslücken mit Ihren Sicherheitskontrollen, giftige Kombinationen von Problemen wie kritische Schwachstellen und Internetrisiko für Ihre Assets und Abweichungen von Ihren internen Sicherheitsstandards.
Schwachstellenverwaltungsteams	Erhalten Sie Einblicke in die für Schwachstellen in den Assets verfügbaren Risikominderungen, und passen Sie die Risikopunktzahl für diese Schwachstellen dynamisch an.
Bedrohungsverteidigungsteams	Erhalten Sie Einblicke in Lücken in der Konfiguration von Risikominderungen oder Sicherheitssteuerungen gegenüber bestimmten Angriffstechniken.

Sicherheitsstatus-Überwachung Und die Überwachung der Minderungssteuerungen Workflow

Sicherheitsstatus-Überwachung Verwendet API-Integrationen mit Sicherheitstools wie Web-Anwendungs-Firewalls und Endpunktschutztools, um zusätzliche Konfigurationsdaten zu Ihren Assets zu importieren und zu analysieren, um die anwendbaren Minderungssteuerungen für ein bestimmtes Asset zu identifizieren. Diese API-Integrationen sind von den Service Graph Connector-Integrationen getrennt, die von unterstützt werden SSÜ Und importieren Sie verschiedene Daten. Sie konfigurieren diese API-Integrationen von innerhalb von SSÜ Arbeitsbereich.

Service Graph Connector-Integrationen oder ITOM Discovery sind für die Überwachung von Minderungssteuerungen weiterhin erforderlich. Beispiel: Beide CrowdStrike Service Graph Connector und CrowdStrike API-Integration unterstützt von SSÜ Muss aktiviert sein, um zusätzliche Einblicke darüber zu importieren, welche Minderungssteuerungen von aktiviert werden CrowdStrike Endpunktschutzkonfiguration.

Richtlinien für Minderungssteuerungen

Die Sicherheitsstatus-Überwachung Und die Anwendungen „Minderungssteuerungen“ sind erforderlich, um die Richtlinien für Minderungssteuerungen und Minderungssteuerungen in anzuzeigen SSÜ. Beide Anwendungen sind im ServiceNow Store verfügbar.

Weitere Informationen zum Herunterladen und Installieren von Anwendungen aus dem finden Sie in den folgenden Themen ServiceNow® Store.

- Laden Sie eine Anwendung aus dem herunter ServiceNow Store Zum ersten Mal
- Installieren Sie ein Security Operations Integration

Um die Richtlinien für Minderungssteuerungen anzuzeigen, können Anwender in der SPC-Administratorgruppe und der SPC-Analystengruppe zu navigieren **Arbeitsbereiche** >

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsstatus-Überwachung > **Richtlinien und Ergebnisse** > **Alle** In SSÜ Arbeitsbereich-Navigationsbereich.

Die folgenden Richtlinien für Minderungssteuerungen sind in der Anwendung enthalten und werden zusammen mit der anderen angezeigt SSÜ Richtlinien:

- Seh-Überschreiben
- Heap-Spray
- CrowdStrike NULL-Seitenzuteilung
- CrowdStrike DEP erzwingen
- CrowdStrike ASLR erzwingen
- Microsoft Flow Guard Für Defender-Steuerung
- Microsoft Defender Force ASLR
- Microsoft Defender – obligatorische ASLR und Bottom-up-ASLR
- SentinelOne-Anwendungssteuerung
- SentinelOne-Datendateien
- Ausführbare SentinelOne-Dateien
- SentinelOne-Exploits
- SentinelOne-IDR
- SentinelOne – interaktive Bedrohung erkennen
- SentinelOne erkennt seitliche Bewegungen
- SentinelOne statische KI
- SentinelOne statische KI – verdächtig
- Potenziell unerwünschte SentinelOne-Anwendungen
- SentinelOne Remote-Shell
- SentinelOne Reputation

Kategorien der Minderungssteuerungen

Die folgenden Kategorien von Minderungssteuerungen werden derzeit mit unterstützt SSÜ.

- Minderungssteuerungen und -Richtlinien, die für EDR-Minderungssteuerungen (Exploit Protection) erforderlich sind.
- Steuerungen zur Minderung von Exploit Protection (WAF). Sie müssen Richtlinien für AWS WAF erstellen. Weitere Informationen finden Sie unter Erstellen Sie eine Richtlinie für AWS WAF-Integration für die Überwachung von Minderungssteuerungen.

Minderungssteuerungen und -Richtlinien, die für EDR-Minderungssteuerungen (Exploit Protection) erforderlich sind

Diese Kategorie von Minderungssteuerungen deckt Minderungen ab, die für Ihre Assets in Form der Konfiguration des Endpunktschutz-Agents verfügbar sind. Dies gilt für Endpunktschutz-Agents wie CrowdStrike Und SentinelOne.

Einstellungen zur Exploit-Minderung wie „Randomisierung des Adressraumlayouts erzwingen“ und „DEP erzwingen“ können in Endpunktschutztools wie aktiviert werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CrowdStrike. SSÜ Erkennt diese Konfiguration automatisch auf Geräten mithilfe der in der Anwendung enthaltenen Richtlinien und der API-Integration mit Endpunktschutztools.

Erforderliche Rollen: SSÜ Administratorgruppe und SSÜ Analystengruppe.

Voraussetzungen für CrowdStrike Erkennung der Risikominderungssteuerung für Exploit Protection (EDR)

1. Überprüfen Sie, ob Sie aktiviert haben CrowdStrike Service Graph Connector. Diese Anwendung ist im ServiceNow Store verfügbar. Die Installations- und Konfigurationsinformationen sind in der App-Liste enthalten. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie CrowdStrike Integrationen für die Überwachung von Minderungssteuerungen.
2. Überprüfen Sie, ob CrowdStrike Die API-Integration ist in aktiviert Sicherheitsstatus-Überwachung Arbeitsbereich.

Voraussetzungen für Microsoft Erkennung der Risikominderungssteuerung für Exploit Protection (EDR)

Microsoft SCCM-Anmeldeinformationen, die die Rolle „Skriptautoren“ enthalten. Die Rolle „Skriptautoren“ bietet die erforderlichen Berechtigungen zum Erstellen eines Skripts, das zum Importieren von Minderungsinformationen auf den SCCM-Server erforderlich ist.

Sie müssen die SCCM-Integration aktivieren, um in Microsoft Defender konfigurierte Minderungssteuerungen zu identifizieren.

Weitere Informationen finden Sie unter Installieren und konfigurieren Sie Service Graph Connector für Microsoft SCCM und die Microsoft Defender Mitigation Control Integration.

- Defender – Exploit-Minderung – CFG

  Microsoft Flow Guard Für Defender-Steuerung.

- Defender – Exploit-Minderung – DEP

  Microsoft Defender-Datenausführungsverhinderung.

- Defender – Exploit-Minderung – obligatorische ASLR und Bottom-up-ASLR

  Microsoft Defender Force ASLR.

- MITRE Behandelte Taktiken: Anfänglicher Zugriff, Ausführung, Anmeldeinformationszugriff, Verteidigungsumgehung, Berechtigungseskalation, Laterale Bewegung.

1. Vergewissern Sie sich, dass Sie SentinelOne Service Graph Connector aktiviert haben.

   Diese Anwendung ist im ServiceNow Store verfügbar. Die Installations- und Konfigurationsinformationen sind in der App-Liste enthalten. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie Service Graph Connector für SentinelOne Und die SentinelOne Mitigation Control-Integration.

2. Überprüfen Sie, ob die SentinelOne-API-Integration im Arbeitsbereich der Sicherheitsstatus-Steuerung aktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren und konfigurieren Sie CrowdStrike Integrationen für die Überwachung von Minderungssteuerungen

Die CrowdStrike Service Graph Connector- und API-Integrationen erfordern separate Konfigurationsschritte. Sie konfigurieren CrowdStrike Service Graph Connector zum Importieren von Asset-Details. Sie konfigurieren CrowdStrike API-Integration zum Sammeln von Minderungsdaten zu den Assets, die von überwacht werden CrowdStrike.

Vorbereitungen

- Vergewissern Sie sich, dass Sie die Anwendungen Sicherheitsstatus-Steuerung und Überwachung der Risikominderungssteuerungen in Ihrer Instanz installiert und aktiviert haben. Diese Anwendungen sind im ServiceNow Store verfügbar.
- Die CrowdStrike Service Graph Connector muss installiert und konfiguriert werden, bevor Sie konfigurieren können CrowdStrike API-Integration.

Erforderliche Rollen: administrator für die Installation von Plugins und SPC-Administratorgruppe und SPC-Analystengruppe für die Konfiguration von Integrationen im Arbeitsbereich.

Prozedur

1. Zum Installieren und Konfigurieren von CrowdStrike Führen Sie die folgenden Schritte aus:

   Hinweis:
   Wenn Sie Service Graph Connector für installiert haben CrowdStrike, Fahren Sie mit Schritt 2 fort, um zu konfigurieren CrowdStrike API-Integration.

   a. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **Registerkarte „Service Graph Connectors“**an.

   b. Suchen Sie nach CrowdStrike Endpunkt-Schutz-Service Graph-Connector.

   c. Wählen Sie den Link aus, über den Sie die App-Liste für den Service Graph Connector für führen CrowdStrike In ServiceNow® Store.

   d. Befolgen Sie die Anweisungen, um die Anwendung zu installieren.

   e. Laden Sie die Installationsanleitung aus dem Abschnitt unterstützende Links und Dokumente in der App-Liste herunter, bevor Sie beenden, um Sie bei der Konfiguration und Aktivierung zu unterstützen.

   f. Navigieren zu **CrowdStrike** > **Setup** In Ihrer Instanz.

   g. Befolgen Sie die Anweisungen im geführten Setup, und lesen Sie die Dokumentation, um den SGC zu konfigurieren und zu aktivieren.

2. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen**an.

   Auf dieser Registerkarte werden die Quellen der Minderungssteuerungen aufgelistet (CrowdStrike, F5 Big IP und SCCM) und die Registerkarte wird im Arbeitsbereich nur angezeigt, wenn Sie die Anwendung Überwachung von Risikominderungssteuerungen installiert haben.

   Auf den Quellkarten können Sie den Status der Minderungsquelle anzeigen (Aktiv Oder Inaktiv) Und die Anzahl der Minderungssteuerungen und die zugehörigen Richtlinien, die von überwacht werden CrowdStrike(6). Sie können die Zahl auswählen, um die Liste anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beachten Sie, dass die Spalte aktiv in Quellen angezeigt wird. Aktiv . Dies gibt die Quelle an (CrowdStrike SGC) ist aktiv, Sie müssen jedoch konfigurieren CrowdStrike API-Integration, bevor Sie Minderungssteuerungen überwachen können.

3. Wählen Sie **Weiter**.
4. Wählen Sie Aus CrowdStrike In der Spalte Name.
5. Wählen Sie Bearbeiten, und füllen Sie die Felder aus.

Hinweis:
Geben Sie denselben ein CrowdStrike Account-Informationen und Serverdetails für die API-Integration, die Sie für bereitgestellt haben CrowdStrike Service Graph Connector. Diese Informationen stellen sicher, dass Sie Minderungsdaten importieren, die den Asset-Daten entsprechen, die Sie mit dem Service Graph Connector importiert haben.

Feld	Beschreibung
Name	Instanzname. Sie können diesen Namen ändern, damit Sie Anmeldeinformationen speichern können, ohne sie zu testen. Wenn Sie Felder im Feld Name ändern, müssen Sie die Verbindung testen, bevor Sie speichern und beenden.
Asset-Größenbeschränkung	Anzahl der überwachten Assets.
Client-ID	CrowdStrike – ID
Geheimer Clientschlüssel	CrowdStrike Geheimnis
API-URL	API-URL, z. B. https://api.crowdstrike.com

6. Wenn Sie bereit sind, wählen Sie aus **Verbindung testen** .
Wenn die Verbindung erfolgreich ist, wird eine Meldung angezeigt.
7. Wählen Sie Aus **Speichern und beenden** .
8. Wählen Sie Aus **Zeigen Sie Details an** Auf der CrowdStrike Karte auf der Registerkarte „SPC-API-Integrationen“, und beachten Sie, dass die Quelle und die API aktiviert sind, und der Konfigurationsfortschrittsbalken ist abgeschlossen.
9. **Wahlweise:** Wenn der Anmeldeinformationstest nicht erfolgreich ist, können Sie auswählen **Vorherige Anmeldeinformationen wiederherstellen** Zum Einfügen von Anmeldeinformationen, die Sie zuvor validiert haben.
10. Führen Sie die folgenden Schritte aus, um auszuführen CrowdStrike Integrationen.

a. Navigieren zu **CrowdStrike-Minderungssteuerung** > **Integrationen**an.
Es gibt drei Integrationen:

- CrowdStrike Integration Der Präventionsrichtlinie
- CrowdStrike Integration Der Gerätesteuerungsrichtlinie
- CrowdStrike Asset Insight-Integration

Die Integrationen sind verkettet und werden in einer bestimmten Reihenfolge ausgeführt. Erfolgreicher Abschluss einer Integration initiiert die nächste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Wählen Sie aus CrowdStrike Integration der Präventionsrichtlinie in der Spalte Name, um die Integrationsausführungen zu initiieren.

c. Wählen Sie im Datensatz die aus **Aktiv** Aktivieren Sie das Kontrollkästchen, und wählen Sie aus **Jetzt Ausführen** .

Sie können den Status der Integrationsausführung auf der Registerkarte Integrationsausführung aus den Integrationsdatensätzen anzeigen.

Die Integration ist standardmäßig so geplant, dass sie täglich ausgeführt wird.

Die CrowdStrike Asset Insight-Integration importiert nur Informationen zu Assets, die sich seit der letzten Integrationsausführung geändert haben. Die CrowdStrike Integration der Gerätesteuerungsrichtlinie und der CrowdStrike Integration der Präventionsrichtlinie importiert alle Daten für jede Ausführung.

Installieren und konfigurieren Sie Service Graph Connector für Microsoft SCCM und die Microsoft Defender Mitigation Control Integration

Der Service Graph Connector für SCCM und die Microsoft Defender Mitigation Control Integration erfordern separate Konfigurationsschritte.

Vorbereitungen

Sie müssen Service Graph Connector für SCCM installieren, aktivieren und konfigurieren, um Asset-Details zu importieren. Sie konfigurieren die Microsoft Defender Mitigation Control Integration, die auch SCCM verwendet, um zusätzliche Daten zu den Mitigation Controls zu sammeln, die für die Assets konfiguriert sind, die vom Service Graph Connector für SCCM überwacht werden.

Erforderliche Rollen:

- administrator für die Installation und Aktivierung von Plugins
- SPC-Administratorgruppe und SPC-Analystengruppe für die Konfiguration von Integrationen im Arbeitsbereich
- Microsoft SCCM-Anmeldeinformationen, die die Rolle Skriptautoren enthalten. Die Rolle „Skriptautoren“ bietet die erforderlichen Berechtigungen zum Erstellen eines Skripts, das zum Importieren von Minderungsinformationen auf den SCCM-Server erforderlich ist.

Hinweis:
Diese Rolle muss mit den folgenden Berechtigungen erstellt und zugewiesen werden:

Rolle der Skriptautoren

Kategorie	Berechtigung	Status
Sammlung	Skript ausführen	Nein
Site	Lesen	Ja
SMS-Skripts	Erstellen	Ja
SMS-Skripts	Lesen	Ja
SMS-Skripts	Löschen	Ja
SMS-Skripts	Ändern	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Microsoft SCCM-Anmeldeinformationen, die die Rolle „Skriptgenehmiger“ enthalten. Das Skript, das zum Importieren von Minderungsinformationen erstellt wurde, erfordert die Genehmigung in Ihrer Microsoft SCCM-Konsole durch einen Anwender mit der Rolle „Skriptgenehmiger“.

Hinweis:
Diese Rolle muss mit den folgenden Berechtigungen erstellt und zugewiesen werden:

Skriptgenehmiger

Kategorie	Berechtigung	Status
Sammlung	Skript ausführen	Nein
Site	Lesen	Ja
SMS-Skripts	Lesen	Ja
SMS-Skripts	Genehmigen	Ja
SMS-Skripts	Ändern	Ja

Prozedur

1. Führen Sie die folgenden Schritte aus, um die Integration von Service Graph Connector für Microsoft SCCM zu installieren und zu konfigurieren:

Hinweis:
Wenn Sie die Integration von Service Graph Connector für Microsoft SCCM installiert haben, fahren Sie mit Schritt 2 fort, um die Integration von Microsoft Defender Mitigation Control zu konfigurieren.

   a. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **Registerkarte „Service Graph Connectors“**an.
   b. Suchen Sie den Service Graph Connector für die Microsoft SCCM-Integration.
   c. Wählen Sie den Link aus, der Sie zur App-Liste für die Anwendung in führt ServiceNow® Store.
   d. Befolgen Sie die Anweisungen, um die Anwendung zu installieren.
   e. Laden Sie die Installationsanleitung aus dem Abschnitt unterstützende Links und Dokumente in der App-Liste herunter, bevor Sie beenden, um Sie bei der Konfiguration und Aktivierung zu unterstützen.
   f. Navigieren zu **Setup** In Ihrer Instanz.
   g. Befolgen Sie die Anweisungen im geführten Setup, und lesen Sie die Dokumentation, um den SGC zu konfigurieren und zu aktivieren.

2. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen** Dient zum Konfigurieren der Integration der Microsoft Defender-Minderungssteuerung.

   Auf dieser Registerkarte werden die Quellen der Minderungssteuerungen aufgelistet (CrowdStrike, F5 Big IP und Defender), und die Registerkarte wird im Arbeitsbereich nur angezeigt, wenn Sie die Anwendung Überwachung von Risikominderungssteuerungen installiert haben.

   Auf den Quellkarten können Sie den Status der Minderungsquelle anzeigen (Aktiv Oder Inaktiv).

   Beachten Sie, dass die Spalte aktiv in Quellen angezeigt wird. Aktiv . Dies gibt an, dass die Quelle (Service Graph Connector für Microsoft SCCM) aktiv ist, um Asset-Daten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

abzurufen. Sie müssen jedoch die Microsoft Defender Mitigation Control Integration konfigurieren, die mithilfe von SCCM zusätzliche Daten zu Defender-Konfigurationen für diese Assets abruft, bevor Sie Minderungssteuerungen überwachen können.

3. Wählen Sie **Weiter**.
   Die SCCM-Konfigurationsseite wird mit einem Instanzlink der Microsoft SCCM-Minderungssteuerung angezeigt.
4. Wählen Sie den Instanzlink aus, der in der Spalte Name bereitgestellt wird.
5. Füllen Sie die Felder für die Konfiguration der SCCM-Anmeldeinformationen für Microsoft SCCM-Steuerungsintegration aus.

Feld	Beschreibung
Name	Das Feld wird automatisch mit dem Instanznamen ausgefüllt.
Verbindung	Feld wird automatisch mit Verbindungsinformationen ausgefüllt.
Host	Hostname für den SCCM-Server in den im vorherigen Feld angegebenen Verbindungsinformationen.
Anwendername	Anwendername für den Zugriff auf den SCCM-Server.
Passwort	Passwort für den Zugriff auf den SCCM-Server.
MID-Server	Wählen Sie einen von ServiceNow verwalteten MID-Server aus der Liste aus.
Validierungsstatus	Feld, das nach dem Validierungsversuch ausgefüllt wurde. Wenn die Verbindung erfolgreich war, lautet der Status der Integrationsinstanz **Gültig** .
SG-Connector-Verbindung	Wählen Sie in der Liste für Service Graph Connector für Microsoft SCCM die Option Aliasse für Verbindungen und Anmeldeinformationen aus. Sie richten diese Verbindung während der Schritte des geführten Setups für Microsoft SCCM SGC ein.
Validierungsdetail	Details zum Validierungsversuch.

6. Wählen Sie Aus **Anmeldeinformationen speichern und testen** .
   A Gültig Eine Antwort für eine erfolgreiche Verbindung ist erforderlich, um mit dem nächsten Schritt fortzufahren.
7. Wählen Sie **Weiter**.
   Ein PowerShell-Skript wird automatisch erstellt, um Minderungsdetails abzurufen. Ein Modal mit der Option zum Validieren der Skriptgenehmigung wird angezeigt.
8. Um das Skript zu genehmigen, melden Sie sich mit der Rolle Skriptgenehmiger bei Ihrer Microsoft SCCM-Konsole an.

   In Ihrem SCCM-Konfigurationsmanager wurde ein PowerShell-Skript generiert, um Minderungsdetails abzurufen. Sie müssen sich mit den entsprechenden Anmeldeinformationen mit einer Anwenderrolle anmelden, die über die Berechtigung des Skriptgenehmigers verfügt, um das Skript zu genehmigen. Nach der Genehmigung können Sie sie in validieren ServiceNow AI Platform Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Suchen Sie in Ihrer -Konsole nach **[Servicenow Secops]: Systemminderungen Abrufen** Skript und genehmigen Sie es.

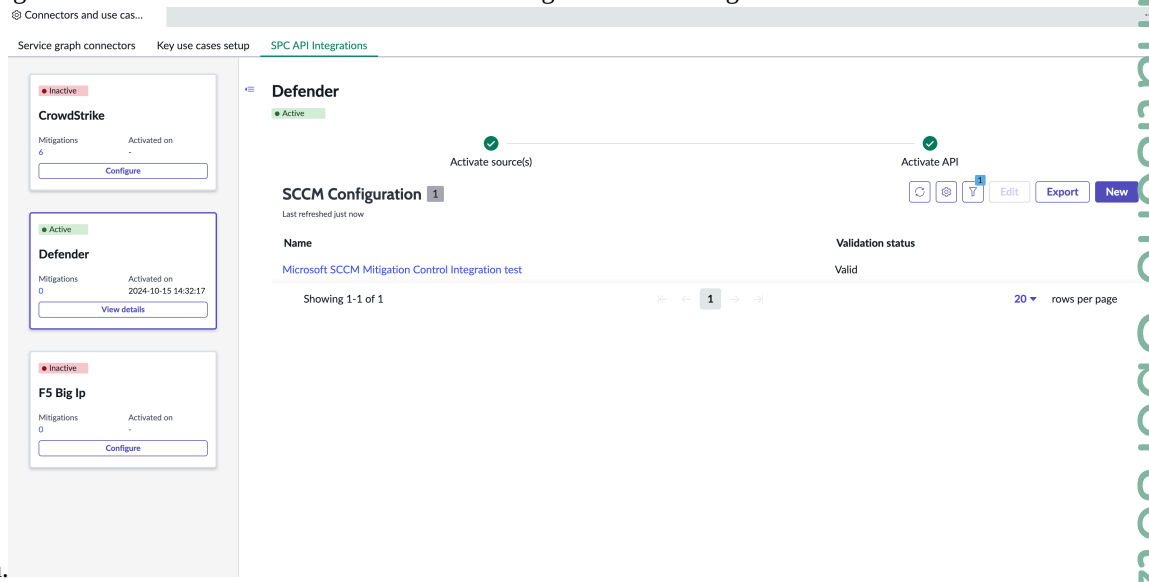
   Hinweis:
   In Ihrem SCCM-Konfigurationsmanager befindet sich der Abschnitt Skript unter der Softwarebibliothek. Suchen: [ServiceNow SecOps]: Skript zur Systemminderung abrufen, um es zu genehmigen.

   Dieses Skript verbleibt im **Warten auf Genehmigung** geben sie an, bis Sie es genehmigen.

   Sie können das Skript in validieren ServiceNow AI Platform Instanz, ohne sie wie oben beschrieben zu genehmigen, aber die Fehlermeldung, „Skript ist nicht genehmigt“ wird angezeigt .

10. Um die Genehmigung zu validieren, kehren Sie zu zurück ServiceNow AI Platform Instanz und wählen Sie im modalen Dialogfeld PowerShell-Skript genehmigen aus **Validiert die Skriptgenehmigung** .

11. Wählen Sie **Fertig**.
    Die Konfigurationsseite sollte wie der Bildschirm in der folgenden Abbildung aussehen.



Erstellen Sie mehrere Instanzen für die Microsoft Defender Mitigation Control Integration

Sie können mehrere Instanzen für die Integration der Microsoft Defender-Minderungssteuerung konfigurieren.

Vorbereitungen

Erforderliche Rollen:

- SPC-Administratorgruppe und SPC-Analystengruppe für die Konfiguration neuer Integrationsinstanzen im Arbeitsbereich
- Microsoft SCCM-Anmeldeinformationen, die die Rolle Skriptautoren enthalten. Die Rolle „Skriptautoren“ bietet die erforderlichen Berechtigungen zum Erstellen eines Skripts, das zum Importieren von Minderungsinformationen auf den SCCM-Server erforderlich ist.

  Hinweis:
  Diese Rolle muss mit den folgenden Berechtigungen erstellt und zugewiesen werden:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle der Skriptautoren

Kategorie	Berechtigung	Status
Sammlung	Skript ausführen	Nein
Site	Lesen	Ja
SMS-Skripts	Erstellen	Ja
SMS-Skripts	Lesen	Ja
SMS-Skripts	Löschen	Ja
SMS-Skripts	Ändern	Ja

- Microsoft SCCM-Anmeldeinformationen, die die Rolle „Skriptgenehmiger“ enthalten. Das Skript, das zum Importieren von Minderungsinformationen erstellt wurde, erfordert die Genehmigung in Ihrer Microsoft SCCM-Konsole durch einen Anwender mit der Rolle „Skriptgenehmiger“.

Hinweis:
Diese Rolle muss mit den folgenden Berechtigungen erstellt und zugewiesen werden:

Skriptgenehmiger

Kategorie	Berechtigung	Status
Sammlung	Skript ausführen	Nein
Site	Lesen	Ja
SMS-Skripts	Lesen	Ja
SMS-Skripts	Genehmigen	Ja
SMS-Skripts	Ändern	Ja

Prozedur

1. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen**an.
2. Wählen Sie **Neu**.
   Das modale Element „neue Defender-Instanz“ wird angezeigt.
3. Geben Sie einen Namen für Ihre neue Instanz ein, und wählen Sie aus **Erstellen Sie eine Instanz** .
   Die Seite „SPC-API-Integrationen“ wird mit der mit der Anwendung bereitgestellten Instanz und Ihrer neuen Instanz angezeigt.
4. Wählen Sie den Link für Ihre neue Instanz aus.
5. Füllen Sie die Felder im modalen Dialogfeld für die Konfiguration der SCCM-Anmeldeinformationen für Ihre neue Instanz aus.

Feld	Beschreibung
Name	Das Feld wird automatisch mit dem Instanznamen ausgefüllt.
Verbindung	Erstellen Sie eine neue Verbindung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	a. Wählen Sie Aus **Erstellen Sie eine Verbindung und einen Alias** Oben im Modal. **b.** Füllen Sie im Formular Aliasse für Verbindungen und Anmeldeinformationen die Pflichtfelder aus. ▪ **Name** – Eindeutiger Name ▪ **Typ** – Verbindung und Anmeldeinformationen ▪ **Verbindungstyp** – Standard **Hinweis:** Nicht auswählen **Übermitteln** Zu diesem Zeitpunkt. **c.** Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle in der grauen Kopfzeile, und wählen Sie aus **Speichern** . Die Seite wird aktualisiert, und zugehörige Links und Registerkarten werden nach dem Speichern unten auf der Seite angezeigt. **d.** Wählen Sie bei ausgewählter Registerkarte Verbindungen die Option aus **Neu** Rechts auf der Registerkarte. Das Verbindungsformular wird angezeigt. Füllen Sie die Felder aus. ▪ **Name** – Eindeutiger Name ▪ Anmeldeinformationen: Wählen Sie das Suchsymbol aus. Suchen Sie die Windows-Anmeldeinformationen, und wählen Sie den Link aus. Füllen Sie die Felder im Formular „Windows-Anmeldeinformationen“ aus. ▪ **Name** – Eindeutiger Name ▪ Anwendername: Anwendername für die Anmeldeinformationen. Dies ist der Anwendername, auf den für das Feld Anwendername im modalen Dialogfeld für die Konfiguration der SCCM-Anmeldeinformationen verwiesen wird, nachdem Sie ihn auf dieser Seite gespeichert haben. ▪ Passwort: Passwort für die Anmeldeinformationen. Dies ist das Passwort, auf das für das Passwortfeld im Modal für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	die Konfiguration der SCCM-Anmeldeinformationen verwiesen wird, nachdem Sie es auf dieser Seite gespeichert haben. ▪ Host: Dies ist der Host für den SCCM-Server, auf den im Feld Host im modalen Dialogfeld für die Konfiguration der SCCM-Anmeldeinformationen verwiesen wird, nachdem Sie ihn auf dieser Seite gespeichert haben. **e.** Wählen Sie aus **MID-Server verwenden** Kontrollkästchen. Wählen Sie bestimmten MID-Server für aus **MID-Auswahl** Und wählen Sie einen aus der Liste MID-Server aus. **f.** Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle in der grauen Kopfzeile, und wählen Sie aus **Speichern** . Dies sind die Anmeldeinformationen, die Sie im oben in Schritt d beschriebenen Verbindungsformular eingeben
Host	Dies ist der Host für den SCCM-Server, auf den im Feld Host verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Anwendername	Dies ist der Anwendername, auf den aus dem Feld Anwendername verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Passwort	Dies ist das Passwort, auf das im Feld Passwort verwiesen wird, nachdem Sie es auf der Verbindungsseite wie oben beschrieben gespeichert haben.
MID-Server	Dies ist der MID-Server, auf den aus den MID-Server-Feldern verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Validierungsstatus	Feld, das nach dem Validierungsversuch ausgefüllt wurde. Wenn die Verbindung erfolgreich war, lautet der Status der Integrationsinstanz **Gültig** .
SG-Connector-Verbindung	Wählen Sie in der Liste für Service Graph Connector für Microsoft SCCM die Option Aliasse für Verbindungen und Anmeldeinformationen aus. Sie richten diese Verbindung während der Schritte des geführten Setups für Microsoft SCCM SGC ein.
Validierungsdetail	Details zum Validierungsversuch.

6. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie den Link für Ihre neue Instanz aus.
8. Wählen Sie im modalen Dialogfeld für die Konfiguration der SCCM-Anmeldeinformationen die Verbindung aus der Liste aus, die Sie in Schritt 5 für das Feld Verbindung erstellt haben.

   Beachten Sie, dass die unten aufgeführten Felder basierend auf den Informationen, die Sie für Ihre neue Verbindung eingegeben haben, automatisch ausgefüllt werden.

Host	Dies ist der Host für den SCCM-Server, auf den im Feld Host verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Anwendername	Dies ist der Anwendername, auf den aus dem Feld Anwendername verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Passwort	Dies ist das Passwort, auf das im Feld Passwort verwiesen wird, nachdem Sie es auf der Verbindungsseite wie oben beschrieben gespeichert haben.
MID-Server	Dies ist der MID-Server, auf den aus den MID-Server-Feldern verwiesen wird, nachdem Sie ihn wie oben beschrieben auf der Verbindungsseite gespeichert haben.
Validierungsstatus	Feld, das nach dem Validierungsversuch ausgefüllt wurde. Wenn die Verbindung erfolgreich war, lautet der Status der Integrationsinstanz **Gültig** .
SG-Connector-Verbindung	Wählen Sie eine Option Aliasse für Verbindungen und Anmeldeinformationen aus der Liste aus.
Validierungsdetail	Details zum Validierungsversuch.

9. Wählen Sie Aus **Anmeldeinformationen speichern und testen** .
   A Gültig Eine Antwort für eine erfolgreiche Verbindung ist erforderlich, um mit dem nächsten Schritt fortzufahren.
10. Wählen Sie **Weiter**.
    Das PowerShell-Skript wird wie in beschrieben erstellt Installieren und konfigurieren Sie Service Graph Connector für Microsoft SCCM und die Microsoft Defender Mitigation Control Integration. Führen Sie die Schritte in diesem Thema aus, um die Skripts für Ihre neuen Instanzen zu genehmigen.

Installieren und konfigurieren Sie Service Graph Connector für SentinelOne Und die SentinelOne Mitigation Control-Integration

Die Service Graph Connector für SentinelOne Und die SentinelOne-Integration für die Integration der Risikominderungssteuerung erfordert separate Konfigurationsschritte. Sie installieren und konfigurieren Service Graph Connector für SentinelOne Dient zum Importieren von Asset-Details. Sie konfigurieren die SentinelOne Integration für die Integration der Minderungssteuerung, um Minderungsdaten zu den Assets zu sammeln, die von überwacht werden Service Graph Connector für SentinelOne.

Vorbereitungen

Erforderliche Rollen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- administrator für die Installation und Aktivierung von Plugins.
- SPC-Administratorgruppe und SPC-Analystengruppe für die Konfiguration von Integrationen im Arbeitsbereich.
- SentinelOne-Anmeldeinformationen.

Prozedur

1. Zum Installieren und Konfigurieren von Service Graph Connector für SentinelOne Integration führen Sie die folgenden Schritte aus:

   Hinweis:
   Wenn Sie Service Graph Connector für SentinelOne installiert haben, fahren Sie mit Schritt 2 fort, um die SentinelOne-Integration für die Integration der Minderungssteuerung zu konfigurieren.

   a. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **Registerkarte „Service Graph Connectors“**an.

   b. Suchen Sie nach Service Graph Connector für SentinelOne Integration.

   c. Wählen Sie den Link aus, der Sie zur App-Liste für die Anwendung in führt ServiceNow® Store.

   d. Befolgen Sie die Anweisungen, um die Anwendung zu installieren.

   e. Laden Sie die Installationsanleitung aus dem Abschnitt unterstützende Links und Dokumente in der App-Liste herunter, bevor Sie beenden, um Sie bei der Konfiguration und Aktivierung zu unterstützen.

   f. Navigieren zu **Setup** In Ihrer Instanz.

   g. Befolgen Sie die Anweisungen im geführten Setup, und lesen Sie die Dokumentation, um den SGC zu konfigurieren und zu aktivieren.

2. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen** Dient zum Konfigurieren der SentinelOne-Integration für die Integration der Minderungssteuerung.

   Auf dieser Registerkarte werden die Quellen der Minderungssteuerungen aufgelistet: CrowdStrike, F5 Big IP, Defender, SentinelOne. Die Registerkarte wird im Arbeitsbereich nur angezeigt, wenn Sie die Anwendung Überwachung der Risikominderungssteuerungen installiert haben.

   Auf den Quellkarten können Sie den Status der Minderungsquelle anzeigen (Aktiv Oder Inaktiv).

   Beachten Sie, dass die Spalte aktiv in Quellen angezeigt wird. Aktiv . Dies gibt die Quelle an, in diesem Fall die Service Graph Connector für SentinelOne, Ist aktiv, um Asset-Daten abzurufen, Sie müssen jedoch die SentinelOne-Integration für die Integration der Minderungssteuerung konfigurieren, bevor Sie Minderungssteuerungen für die importierten Assets überwachen können.

3. Wählen Sie **Weiter**.
   Die Seite „SentinelOne-Konfiguration“ wird mit einem Instanzlink „SentinelOne Integration for Mitigation Control“ angezeigt.

4. Wählen Sie den Instanzlink aus, der in der Spalte Name bereitgestellt wird.

5. Füllen Sie die Felder für die SentinelOne-Integration für die Integration der Minderungssteuerung aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Geben Sie die gleichen SentinelOne-Account-Informationen und Serverdetails für die SentinelOne-Integration für die Integration der Minderungssteuerung ein, die Sie für angegeben haben Service Graph Connector für SentinelOne. Diese Informationen stellen sicher, dass Sie Minderungsdaten importieren, die den Asset-Daten entsprechen, die Sie mit dem Service Graph Connector importiert haben.

Wählen Sie das Pen-Symbol aus, wenn Sie die Felder bearbeiten müssen.

Feld	Beschreibung
Instanzname	Das Feld wird automatisch mit dem Instanznamen ausgefüllt.
API-Schlüssel	Feld wird automatisch mit den API-Schlüsselinformationen ausgefüllt.
API-URL	Hostname für den SentinelOne-Server, z. B. https// usea1-na.sentinelone.net

6. Wählen Sie Aus **Anmeldeinformationen speichern und testen** .
   A Gültig Eine Antwort für eine erfolgreiche Verbindung ist erforderlich, um mit dem nächsten Schritt fortzufahren.
7. Wählen Sie Aus **Speichern und beenden** .
8. Wählen Sie Aus **Zeigen Sie Details an** Auf der Karte SentinelOne auf der Registerkarte SPC API-Integrationen.
   Beachten Sie, dass die Quelle und die API aktiviert sind und der Konfigurationsfortschrittsbalken abgeschlossen ist.
9. **Wahlweise:** Wählen Sie Aus **Vorherige Anmeldeinformationen wiederherstellen** Zum Einfügen von Anmeldeinformationen, die Sie zuvor validiert haben.
10. Führen Sie die folgenden Schritte aus, um die Integration des SentinelOne Asset-Imports auszuführen.

    a. Navigieren zu **Minderungssteuerung von SentinelOne** > **Integrationen**an.
    Es gibt eine Integration: SGC SentinelOne Asset-Import.

    b. Wählen Sie aus **Integration der SentinelOne-Präventionsrichtlinie** In der Spalte Name, um die Integration zu initiieren.

    c. Wählen Sie im Datensatz die aus **Aktiv** Aktivieren Sie das Kontrollkästchen, und wählen Sie aus **Jetzt Ausführen** .

    Sie können den Status der Integrationsausführung in anzeigen **Integrationsausführung** Registerkarte aus den Integrationsdatensätzen.

    Die Integration ist standardmäßig so geplant, dass sie täglich ausgeführt wird.

    Die SentinelOne Asset Import-Integration importiert nur Informationen zu Assets, die sich seit der letzten Integrationsausführung geändert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Steuerungen zur Minderung von Exploit Protection (WAF)

Diese Kategorie von Minderungssteuerungen deckt Minderungen ab, die in Form einer Webanwendungsfirewall verfügbar sind.

Exploit-Schutz (WAF)

Sicherheitsstatus-Überwachung Erkennt Server, die hinter der Web Application Firewall (WAF) ausgeführt werden, indem die API-Integration mit WAF-Tools wie verwendet wird F5 BIG-IP(F5) und Netzwerkverkehrsdaten aus ITOM IP-basierter Discovery, falls erforderlich.

Die Minderungssteuerung importiert die Web-ACL-Regeln und alle zugehörigen Lastenausgleichsmodule, um zu bestimmen, welche Regeln Ihre virtuellen Computer mithilfe von Discovery- und Service-Mapping-Mustern schützen.

Erforderliche Rollen: SSÜ Administratorgruppe und SSÜ Analystengruppe.

Voraussetzungen für Exploit Protection (WAF) mit F5 BIG-IP

1. Überprüfen Sie, ob Sie ITOM IP-basierte Discovery in der Umgebung aktiviert haben, in der sich befindet F5 BIG-IP F5 WAF und zugehörige Anwendungsserver sind eingerichtet.
2. Überprüfen Sie, ob die API-Integration für F5 BIG-IP F5 ist in aktiviert Sicherheitsstatus-Überwachung Arbeitsbereich.

Voraussetzungen für Exploit Protection (WAF) mit Amazon Web Services AWS

Daten für diese Integration werden von den Discovery- und Service-Mapping-Mustern [sn_itom_pattern] und der Anwendung „Überwachung der Risikominderungssteuerungen“ [sn_sec_mit_ctrl] importiert. Beide Anwendungen sind erforderlich. Führen Sie die folgenden Schritte in der Reihenfolge aus, in der sie aufgeführt sind, damit Sie alle Web-ACLs, die Web-ACL-Regeln und die Minderungsdaten importieren können, die erforderlich sind, um sicherzustellen, dass eine virtuelle Maschine geschützt ist. Siehe AWS discovery using patterns Weitere Informationen zu finden AWS Discovery-Muster.

1. Definieren Sie Web-ACLs und -Regeln in Ihrem AWS Service-Account, den Sie verwenden möchten. Siehe Verwenden von Web-ACLs in AWS WAF Weitere Informationen finden Sie unter .

   Hinweis:
   Sie können Ihre eigenen Web-ACL-Regeln erstellen, Sie können jedoch die verwenden AWS Verwaltete Regeln, die speziell für die Verwendung mit ihren Web-ACLs konzipiert sind. Wenn Sie eigene anwenderdefinierte Regeln für Web-ACLs erstellen möchten, beachten Sie, dass diese Integration mit durchgeführt wird AWS WAF unterstützt nur Angriffstypen, die mit SQL-Injection-Angriffen und XSS-Injection-Angriffen (Cross Site Scripting) übereinstimmen. Lastenausgleichsmodule sind die von dieser Integration unterstützten Assets (Ressourcen).

2. Installieren und aktivieren Sie die Anwendung „Muster für Discovery und Service-Mapping“ [sn_itom_pattern] in Ihrer Instanz, damit die Namen und Standardaktionen der in Schritt 1 definierten Web-ACLs erkannt werden können. Weitere Informationen finden Sie unter Installieren Sie die unterstützten Anwendungen für die Sicherheitsstatus-Steuerung.
3. Überprüfen Sie, ob die MID-Servereigenschaft sn_itom_pattern.Discover_aws_App_Pool_members auf festgelegt ist Wahr . Um diese Eigenschaft zu aktivieren, navigieren Sie zu **Alle** > **MID-Server** > **Eigenschaften**an.
4. Vergewissern Sie sich, dass Sie die Anwendung Überwachung der Risikominderungssteuerungen [sn_sec_mit_ctrl] installiert und aktiviert haben. Diese Anwendung enthält eine Mustererweiterung, Web-ACL-Regeln und zugehörige

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen. Mit dieser Mustererweiterung können Sie die tatsächlichen Web-ACL-Regeln und ihre Zuordnungen (Beziehungen) zu Ihren Ressourcen (Assets) in Ihre Instanz importieren.

Konfigurieren Sie F5 BIG-IP Integrationen für die Überwachung von Minderungssteuerungen

Die ITOM IP-basierte Discovery-Anwendung und die F5 BIG-IP API-Integrationen erfordern separate Konfigurationsschritte. Sie konfigurieren die ITOM IP-basierte Discovery-Anwendung, um Asset-Details zu importieren. Sie konfigurieren F5 BIG-IP API-Integration zum Sammeln von Minderungsdaten zu den Assets, die von ITOM IP-basierter Discovery überwacht werden.

Vorbereitungen

- Die IP-basierte ITOM-Discovery muss in der Umgebung ausgeführt werden, in der sie ausgeführt wird F5 BIG-IP Und alle zugehörigen Anwendungsserver werden eingerichtet.
- Für lokale Assets müssen Sie einen MID-Server bereitstellen.
- Aktivieren Sie die Quelle (ITOM), um Daten zu den überwachten Assets zu sammeln.
- Aktivieren Sie die API-Integration, um Minderungsdaten zu den Assets zu sammeln.

Erforderliche Rollen: administrator für die Installation von Plugins und das Erstellen von Systemeigenschaften, und SSÜ Administratorgruppe und SSÜ Analystengruppe für die Konfiguration von Integrationen im Arbeitsbereich.

Prozedur

1. Führen Sie die folgenden Schritte aus, um die Integration zu installieren und zu konfigurieren:

   Hinweis:
   Wenn Sie ITOM installiert und aktiviert haben, fahren Sie mit Schritt 2 fort, um zu konfigurieren F5 BIG-IP(F5) API-Integration.

   a. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **Registerkarte „Service Graph Connectors“**an.

   b. Wählen Sie aus F5 BIG-IP Karte.

   c. Wählen Sie aus **ITOM-Plugin** Link zum Aktivieren des ITOM-Plugins.

   d. Befolgen Sie die Anweisungen.

2. Navigieren zu **Setup von Connectors und Anwendungsfällen** > **SPC-API-Integrationen**an.

   Auf dieser Registerkarte werden die Quellen der Minderungssteuerungen aufgelistet (CrowdStrike Und F5 Big IP und SCCM), und die Registerkarte wird im Arbeitsbereich nur angezeigt, wenn Sie die Anwendung Überwachung von Risikominderungssteuerungen installiert haben.

   Auf den Quellkarten können Sie den Status der Minderungsquelle anzeigen (Aktiv Oder Inaktiv .

3. Wählen Sie **Weiter**.

   Beachten Sie, dass die Quelle (ITOM) aktiv ist, Sie jedoch konfigurieren und aktivieren müssen F5 BIG-IP API-Integration, bevor Sie Minderungssteuerungen überwachen können.

4. Wählen Sie Aus F5 BIG-IP In der Spalte Name.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie Bearbeiten, und füllen Sie die Felder aus.

Feld	Beschreibung
Name	Instanzname. Sie können diesen Namen ändern, damit Sie Anmeldeinformationen speichern können, ohne sie zu testen. Wenn Sie Felder im Feld Name ändern, müssen Sie die Verbindung testen, bevor Sie speichern und beenden.
Anwendername	F5 BIG-IP-Anwendername
Passwort	F5 BIG-IP Passwort.
MID-Server	Wählen Sie einen MID-Server aus der Liste aus.
API-URL	API-URL mit Port 8443, z. B. https://bigip.example.com:8443.

6. Wenn Sie bereit sind, wählen Sie aus **Verbindung testen** .
Wenn die Verbindung erfolgreich ist, wird eine Meldung angezeigt.

   Wenn der folgende Fehler beim Testen der Verbindung während der Konfigurationsschritte auftritt, Sitzung enthält keine Zertifikate – nicht vertrauenswürdig: Sitzung enthält keine Zertifikate – nicht vertrauenswürdig , Legen Sie die folgenden Systemeigenschaften auf fest Falsch :

   - com.glide.communications.httpclient.verify_hostname
   - com.glide.communications.httpclient.verify_revoked_certificate

   Ein Anwender mit der Administratorrolle muss diese Systemeigenschaften im globalen Bereich erstellen, wenn sie nicht in der Tabelle „Systemeigenschaft“ [sys_properties] aufgeführt sind. Die Systemeigenschaften sind Typ, wahr/falsch (boolescher Wert).

7. Wählen Sie Aus **Speichern und beenden** .
8. Auf der F5 BIG-IP Karte auf der Registerkarte „SPC-API-Integrationen“, und beachten Sie, dass die Quelle und die API aktiviert sind, und der Konfigurationsfortschrittsbalken ist abgeschlossen.
9. **Wahlweise:** Wenn der Anmeldeinformationstest nicht erfolgreich ist, können Sie auswählen **Vorherige Anmeldeinformationen wiederherstellen** Zum Einfügen von Anmeldeinformationen, die Sie zuvor validiert haben.
10. Führen Sie die folgenden Schritte aus, um die API-Integrationen auszuführen:

    a. Navigieren zu **F5-Steuerung zur Big IP-Minderung** > **Integrationen**

    Es gibt fünf Integrationen. Die Integrationen sind verkettet und werden in einer bestimmten Reihenfolge ausgeführt. Erfolgreicher Abschluss einer Integration initiiert die nächste:

    - F5 Big IP-Geräteintegration
    - F5 Big IP-Richtlinienintegration
    - F5 Big IP Attack Signature Integration
    - F5 Big IP Virtual Server-Integration
    - Integration von F5 Big-IP-Pool-Mitgliedern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Um die Integrationskette zu initiieren, wählen Sie aus **F5 Big IP-Geräteintegration** In der Spalte Name.

c. Wählen Sie im Datensatz die aus **Aktiv** Aktivieren Sie das Kontrollkästchen, und wählen Sie aus **Jetzt Ausführen** .

d. Zeigen Sie den Status der Integrationsausführungen auf der Registerkarte Integrationsausführung aus den Integrationsdatensätzen an.
Die Integration ist standardmäßig so geplant, dass sie täglich ausgeführt wird.

Konfigurieren Sie AWS WAF-Integration für die Überwachung von Minderungssteuerungen

Bestimmen Sie, ob Ihre virtuellen Computer mit geschützt sind AWS WAF-Integration für die Überwachung von Minderungssteuerungen.

Vorbereitungen

Daten werden von zwei separaten Anwendungen importiert:

- Die Anwendung „Muster für Discovery und Service-Mapping“ importiert die Namen und Standardaktionen „Zulassen“ oder „Blockieren“ der Web-ACLs, die Sie in definieren AWS Service-Account. Das Discovery-Muster Amazon AWS – Web-ACL (LP) Ist mit der Anwendung aktiviert.
- Die Anwendung „Überwachung von Risikominderungssteuerungen“ importiert die tatsächlichen Web-ACL-Regeln und die Beziehungen zwischen zugehörigen Ressourcen wie einem Anwendungslastausgleichsmodul. Diese Erweiterung ist als Teil der Anwendung „Überwachung von Risikominderungssteuerungen“ enthalten.

Vergewissern Sie sich, dass Sie die Schritte zum Definieren von Web-ACLs und -Regeln abgeschlossen und die erforderlichen Anwendungen für aktiviert haben AWS WAF-Integration beschrieben in Steuerungen zur Minderung von Exploit Protection (WAF) Vor der Aktivierung der Anwendungen.

Erforderliche Rollen:

- administrator für die Installation von Plugins in Ihrem ServiceNow AI Platform® Instanz.
- SSÜ Administratorgruppe für die Konfiguration von Integrationen im Arbeitsbereich.
- AWS Anmeldeinformationen für AWS Service-Account, den Sie verwenden möchten.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereich Für Sicherheitsstatus-Steuerung** > **Setup von Connectors und Anwendungsfällen** > **Registerkarte „SPC-API-Integrationen“**an.
2. Wählen Sie aus **AWS WAF** Kachel.
3. Wählen Sie eine Option aus.

Option	Beschreibung
Zeigen Sie Service-Accounts an	Zeigen Sie die verfügbaren an AWS Service-Accounts, die in Ihrer Instanz konfiguriert sind. So erstellen Sie einen neuen Account:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	a. Wählen Sie Aus **Zeigen Sie Service-Accounts an** . **b.** Wählen Sie **Neu**. **c.** Füllen Sie die Felder aus. ▪ Name: Name Ihres AWS Service-Account. Dies ist der Account, den Sie für Ihren Discovery-Zeitplan und Ihre Anmeldeinformationen verwenden. ▪ Account-ID: Account-ID für Ihren AWS Service-Account. ▪ Rechenzentrumstyp: Auswählen **AWS-Rechenzentrum [cmdb_ci_aws_Datacenter]** **d.** Wählen Sie **Absenden**.
Konfigurieren Sie den Service-Account	Konfigurieren Sie einen AWS Service-Account in Ihrer Instanz.

4. Erstellen Sie den Discovery-Zeitplan für AWS Service-Account, den Sie verwenden möchten.

a. Navigieren zu **Alle** > **Discovery** > **Startseite**an.

b. Wählen Sie Aus **Zeigen Sie Aktive Zeitpläne An** .

c. Wählen Sie Aus **Fügen Sie Zeitplan Hinzu** .

d. Wählen Sie Aus **Fügen Sie Cloud-Zeitplan Hinzu** Und füllen Sie die Felder aus.

Feld	Beschreibung
Anbieter	AWS
Zeitplanname	Geben Sie einen eindeutigen Namen für Ihren Zeitplan ein, damit Sie ihn von anderen unterscheiden können AWS Zeitpläne.
Account hinzufügen	Wählen Sie diese Option aus, um einen Service-Account zu erstellen.
Account auswählen	Wählen Sie diese Option aus, um einen vorhandenen Service-Account zu bearbeiten.
Account-ID	Account-ID für AWS Service-Account.
MID-Auswahltyp	Sie müssen einen MID-Server angeben. Wählen Sie eine Option aus: ▪ Wählen Sie automatisch MID-Server aus ▪ Spezifischer MID-Server-Cluster ▪ Spezifischer MID-Server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Um Regeldaten für einzelne virtuelle Maschinen mit Ihrem MID-Server zu importieren, müssen Sie eine MID-Server-Eigenschaft aktivieren. Um diese Eigenschaft zu überprüfen oder festzulegen, navigieren Sie zu **Alle** > **MID-Server** > **Eigenschaften** > **sn_itom_pattern.Discover_aws_App_Pool_members**an. Legen Sie den Wert auf fest Wahr .
Anmeldeinformationen	Dies sind die Discovery-Anmeldeinformationen für Ihren Service-Account.
URL	
Name der Zugriffsrolle	
Select account for access (Konto für Zugriff auswählen)	

e. Wählen Sie Aus **Test-Account** .
Sie müssen über eine erfolgreiche Validierung verfügen, bevor Sie fortfahren können.

f. Wählen Sie **Weiter**.

g. Wählen Sie die Rechenzentren aus, die Sie erkennen möchten.

h. Wählen Sie aus **Erkennen Sie VMs nach IP-Adresse** Schalten Sie den in Schritt d ausgewählten MID-Server aus der Liste um, und wählen Sie ihn aus.

i. Wählen Sie **Weiter**.

j. Wählen Sie aus, wie oft und wann Sie Ihre Discovery ausführen möchten.

k. Wählen Sie **Beenden und ausführen**.

Nachdem der von Ihnen festgelegte Discovery-Zeitplan ausgeführt wurde, wird das Discovery-Muster ausgeführt **Amazon AWS – Web-ACL (LP)** Wird ausgeführt, und die Daten aus beiden Anwendungen werden importiert.

Erstellen Sie eine Richtlinie für AWS WAF-Integration für die Überwachung von Minderungssteuerungen

Erstellen Sie eine Richtlinie, damit Sie Ihre Assets basierend auf Daten, die aus der Integration importiert wurden, auditieren können.

Vorbereitungen

Erforderliche Rollen: SPC-Administratorgruppe oder SPC-Analystengruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Richtlinien und Ergebnisse** > **Alle**an.
2. Wählen Sie Aus **Hardware-Asset** Für Asset-Typ.

   Eigenschaften funktionieren auch für die Asset-Suche und Asset-Profile.
3. Wählen Sie für Verbindung aus **Konfiguration der Sicherheitssteuerung** .
4. Wählen Sie für Entität aus **AWS-Einblick** .

   Ein Kriterienfeld wird automatisch mit ausgefüllt angezeigt Verbindung .
5. Wählen Sie für das Feld neue Verbindung die Option aus **Mit verwalteter AWS-Regel** .

   Das Feld Entität wird automatisch mit ausgefüllt Verwaltete Regel Und ein Kriterienfeld wird automatisch mit ausgefüllt angezeigt Eigenschaft . Leere Felder für Eigenschaft, Operator und Wert werden angezeigt.

   Wenn Sie eine anwenderdefinierte AWS-Regel erstellt haben, wählen Sie aus **Mit anwenderdefinierter Übereinstimmungsanweisung** . Das Feld Entität wird mit ausgefüllt Übereinstimmungsanweisung .
6. Wählen Sie Eigenschaften aus der Liste aus.

   Sie können mehrere hinzufügen.

   Für eine Web-ACL für SQL-Datenbank in Ihrem AWS-Service-Account werden beispielsweise die folgenden Regeln angezeigt:

   - SQLiExtendedPatterns_QUERYARGUMENTS
   - SQLiQUERYARGUMNETS
   - SQLi_BODY
   - SQLi_COOKIE
   - SQLi_URIPATH

   Im Richtliniengenerator wird diese Eigenschaft wie folgt angezeigt: SQLRuleSet-SQLi_BODY is allow. Sie können auswählen **Zulassen** Oder **Blockieren** Aus der Liste.
7. Wählen Sie Aus **Oder** Zum Hinzufügen von Eigenschaften.
   Siehe Erstellen und aktivieren Sie anwenderdefinierte Richtlinien für Sicherheitsstatus-Überwachung Weitere Informationen zur Verwendung des Richtliniengenerators zum Erstellen von Richtlinien.
8. Wählen Sie Aus **Speichern Sie die Änderungen** Wenn Sie Ihre Richtlinie abgeschlossen haben.
9. **Aktivieren** Die Richtlinie, wenn Sie Ergebnisse anzeigen möchten.
10. Siehe Sicherheitsstatus-Steuerung: Konfigurieren und Anzeigen Ihrer Ergebnisse Weitere Informationen zum Anzeigen der Ergebnisse aus Ihrer Richtlinie.
11. Öffnen Sie einen Datensatz in der Liste, und wählen Sie die Registerkarten „Risikominderungssteuerungen – geminderte angreifbare Elemente“ aus.

    Auf der Registerkarte „geminderte angreifbare Elemente“ werden alle geminderten angreifbaren Elemente aufgelistet, die Informationen zu den CVEs enthalten, die aufgrund der Minderungsregeln, die in Ihren Assets gefunden werden, gemindert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verifizierte Quelle(n) – AWS-APIs, ITOM-Discovery
- Geschützt durch Web Application Firewall (WAF) – Ja
- WAF-Typ: AWS
- Vollständig geminderte angreifbare Elemente: Anzahl der zugeordneten angreifbaren Elemente, die gemindert wurden.
- Teilweise geminderte angreifbare Elemente: Anzahl der zugeordneten angreifbaren Elemente, die verarbeitet werden.
- Verwaltete Regeln kategorisiert nach Aktionen: Verwaltete Regeln mit Aktionen „Block“ und „Allow“.

  Möglicherweise werden mehr Regeln angezeigt, als Sie für Ihre Richtlinie eingegeben haben. Diese Regeln werden mit identifiziert CommonRuleSet (CRS) in der Regel.
- Anwenderdefinierte Regeln: Eine Ihrer anwenderdefinierten Regeln, kategorisiert nach Aktionen „Blockieren“ und „Allow“.
- Im Dashboard „Homepage“ listet die Kachel „Assets mit Minderungen“ die Assets auf, die in der Visualisierung „Exploit Protection“ (WAF) durch WAF geschützt werden.

Zeigen Sie erkannte Minderungen an

Sie müssen Richtlinien aktivieren, bevor Sie anzeigen können, welche Bedrohungen für Ihre Assets durch verfügbare Minderungssteuerungen gemindert werden.

Vorbereitungen

Überprüfen Sie, ob Sie die in aufgeführten Anforderungen erfüllt haben Installieren und konfigurieren Sie CrowdStrike Integrationen für die Überwachung von Minderungssteuerungen, Installieren und konfigurieren Sie Service Graph Connector für Microsoft SCCM und die Microsoft Defender Mitigation Control Integration Und Konfigurieren Sie F5 BIG-IP Integrationen für die Überwachung von Minderungssteuerungen.

Erforderliche Rollen: SPC-Administratorgruppe und SPC-Analystengruppe.

Prozedur

Um Assets mit Minderungen anzuzeigen, die von der Sicherheitsstatus-Steuerung mit dem Widget „Assets mit MITRE-Minderungen“ im Dashboard erkannt wurden, führen Sie die folgenden Schritte aus.

a. Navigieren zu **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Startseite**an.

b. Überprüfen Sie im Abschnitt „wichtige Einblicke“ das Widget „Assets mit MITRE-Minderungen“.

c. Wählen Sie eine Minderungskategorie aus, **Exploit-Schutz (EDR)** Oder **Exploit-Schutz (WAF)** Im Widget.

d. Sie können die Liste der Assets mit erkannten Minderungen in dieser Minderungskategorie anzeigen.

e. Wählen Sie ein Asset aus.

f. Wählen Sie aus **Minderungssteuerungen** Registerkarte, um die Details der erkannten Minderungssteuerung anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

g. Wählen Sie aus **Geminderte angreifbare Elemente** Registerkarte, um die Liste der angreifbaren Elemente anzuzeigen, die durch diese Minderungssteuerung gemindert werden.

Hinweis:
Damit diese Registerkarte ausgefüllt werden soll, ist Vulnerability Response Die Anwendung muss installiert und aktiviert sein.

Zuordnung von Minderungssteuerungen zu angreifbaren Elementen

Daten der Minderungssteuerungen werden angreifbaren Elementen zugeordnet. Sie können eine Liste von Minderungssteuerungen anzeigen, die zur Minderung der Schwachstellen und zugrunde liegenden allgemeinen Schwachstellen und Risiken (Common Vulabilities and Exposures, CVEs) verwendet werden, die den angreifbaren Elementen zugeordnet sind.

Nachdem eine bestimmte Minderungssteuerung für ein Asset identifiziert wurde, identifiziert die Sicherheitsstatus-Steuerung automatisch alle angreifbaren Elemente, die durch diese Steuerung gemindert werden. Beispielsweise werden alle angreifbaren Elemente mit CVEs, die Teil von Signaturen in WAF-Richtlinien (Web Application Firewall) sind, als geminderte angreifbare Elemente markiert. Diese Identifizierung kann für Schwachstellenverwaltungsteams nützlich sein, um ihnen dabei zu helfen, die Risikopunktzahlen für angreifbare Elemente, die gemindert werden, automatisch zu reduzieren.

Tabelle für Steuerungen zur Verringerung angreifbarer Elemente

Die Tabelle „Steuerungen zur Minderung angreifbarer Elemente“ [sn_vul_vulnerable_item_Mitigation_Control] wurde erstellt, um Daten zur Minderungssteuerung zu mindernden angreifbaren Elementen (Vits) zuzuordnen. In dieser Tabelle werden geminderte Vits und die erkannten Minderungssteuerungen aufgelistet, die zur Minderung der Schwachstellen und der zugrunde liegenden CVEs verwendet wurden, die den angreifbaren Elementen zugeordnet sind. Die Datensätze für geminderte CVE enthalten Verweise auf die für die Assets verwendete Minderungssteuerung, z. B. Exploit Protection (EDR).

Beispieldaten werden in der folgenden Tabelle angezeigt.

Die Risikominderung für angreifbare Elemente steuert Daten

Minderungssteueru ist vorhanden	Effektivität der Minderungssteueru	Typ der Minderungssteueru erkannt	CVEs gemindert	Angreifbares Element
Ja/Nein	Mittel	Exploit-Schutz (EDR)	CVE-2009-3373	VIT0018323

Öffnen Sie einen Minderungssteuerungsdatensatz (erkannter Minderungssteuerungstyp) in der Tabelle, um Details darüber zu überprüfen, wie eine CVE und die zugehörige CWE-Schwachstelle (Common Schwachstellen Enumeration, Common Schwachstellen) durch die einem Asset zugeordnete Minderungssteuerung gemindert werden. Der Datensatz der Minderungssteuerung enthält Details zu den CWEs, die gemindert wurden, z. B. wie eine Minderungseinstellung die in einer CWE angegebenen Schwachstellen erfüllt.

Risikorechner- und Risikorechnerregeln

Minderungsinformationen können verwendet werden, um Ihnen beim Einrichten anwenderdefinierter Risikorechnerregeln zu helfen, die Risikopunktzahlen für Vits neu zu berechnen, denen bestimmte Arten von Schwachstellen und Minderungssteuerungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zugeordnet sind. Für diese Beispielregel, die auf der vorherigen Tabelle basiert, berechnet der Standardrisikorechner eine Risikopunktzahl von 60 für Vits, die den Minderungssteuerungstyp Exploit Protection (EDR) für erkannte Assets haben. Diese Berechnungspunktzahl ist auf das moderate Risiko zurückzuführen, das mit der Schwachstelle verbunden ist, die mit dieser Minderung verbunden ist.

Beispiel für eine Risikorechnerregel mit den folgenden Bedingungen:

[Details zur Minderungssteuerung] [ist nicht] [leer] UND [Details der Minderungssteuerung, erkannter Minderungssteuerungstyp] [ist] [Exploit-Schutz (EDR)] .

Werte:

[Risikopunktzahl] [Ist] [60]

Weitere Informationen finden Sie unter Definieren Sie Felder und Gewichtungen für die Risikoregel für Vulnerability Response-Risikorechner.

Anwendungsfälle, Richtlinienbeispiele und unterstützte Service Graph Connectors in Sicherheitsstatus-Überwachung

Anwendungsfälle sind verschiedene Szenarien, die Sie konfigurieren, um bestimmte Arten von Toolabdeckungslücken zu identifizieren. Jeder Anwendungsfall erfordert eine oder mehrere Richtlinien, um Ihre Assets auf potenzielle Verstöße zu überprüfen. Sie können auch eigene Richtlinien definieren, um die Anforderungen für Ihre spezifischen internen Sicherheitsstandards zu erfüllen.

Anwendungsfälle

Die Anwendung „Sicherheitsstatus-Steuerung“ unterstützt verschiedene Anwendungsfälle, die in der Anwendung enthalten sind. Anwendungsfälle helfen Ihnen, bestimmte Arten von Toolabdeckung-Lücken in Ihren Assets, das Internetrisiko von Cloud-Assets und Kombinationen mit Schwachstellen zu identifizieren. Die Richtlinien, die Sie für die unterstützten Anwendungsfälle benötigen, sind ebenfalls im Produkt enthalten.

Sie können den Abdeckungsstatus für einige der wichtigsten Anwendungsfälle auf der Startseite (Zielseite) im Arbeitsbereich „Sicherheitsstatus-Steuerung“ unter anzeigen **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Startseite** Im Startmodul (Zielseite).

Alternativ können Sie die unterstützten Service Graph Connectors und den Abdeckungsstatus für einige der wichtigsten Anwendungsfälle auf den Registerkarten „unterstützte Service Graph Connectors“ und „Setup des Schlüsselanwendungsfalls“ unter anzeigen **Alle** > **Arbeitsbereiche** > **Sicherheitsstatus-Überwachung** > **Setup von Connectors und Anwendungsfällen** (Zahnradsymbol).

Hinweis:

Auf der Registerkarte „Schlüsselanwendungsfälle“ auf den Zielseiten „Startseite“ werden nicht alle möglichen Anwendungsfälle aufgelistet. Sie erhalten einige wichtige Anwendungsfälle, die Sie aktivieren, um Ihnen den Einstieg in die Produktbereitstellung zur Sicherheitspositionssteuerung zu erleichtern.

Bevor Sie Richtlinien für die mit der Anwendung bereitgestellten unterstützten Anwendungsfälle aktivieren, stellen Sie sicher, dass Sie die folgenden Aufgaben abgeschlossen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie haben alle erforderlichen Anwendungen installiert und konfiguriert, die in beschrieben sind Installieren Sie die unterstützten Anwendungen für die Sicherheitsstatus-Steuerung.
- Sie haben mindestens eine der folgenden Voraussetzungen für jeden Anwendungsfall erfüllt.

1. Sie verwenden derzeit Service Graph Connectors für verschiedene Kategorien oder installieren und aktivieren sie sie.

   Zu den Kategorien für die Anwendungsfälle gehören Service Graph Connectors, die Sie aktivieren müssen, um erste Einblicke zu erhalten, und#Service Graph Connectors, die Sie aktivieren können, um die Abdeckung für die Assets zu verbessern,#die von der Sicherheitsstatus-Steuerung überwacht werden.

2. Sie verwenden derzeit oder installieren und aktivieren die Anwendung Vulnerability Response.
3. Sie verwenden derzeit den Cloud-Account-Scan für Ihre AWS- und Azure-Accounts oder konfigurieren ihn unter „Cloud-Sicherheitsstatus-Management“.

Spezifische Anforderungen für jeden unterstützten Anwendungsfall werden in den folgenden Abschnitten beschrieben. Darüber hinaus müssen Sie mindestens eine der mit der Sicherheitsstatus-Steuerung gelieferten Richtlinien für einen Anwendungsfall aktivieren. Dieses Konzept wird auch in den folgenden Abschnitten behandelt.

Beispiele für Basis-, untergeordnete und geklonte Richtlinien

Siehe Beispiele für Basis-, untergeordnete und geklonte Richtlinien für Sicherheitsstatus-Überwachung Und wie Sie die Bedingungen einer Basisrichtlinie wiederverwenden können, wenn Sie andere Richtlinien erstellen. Erstellen Sie in diesen Beispielen Basis-, untergeordnete Richtlinien und Klonen vorhandener Richtlinien. Diese Beispiele helfen Ihnen auch, zu sehen, wie der Richtliniengenerator im Modul „Richtlinien und Ergebnisse“ funktioniert.

Unterstützte Service Graph Connectors

Sehen Sie sich Tabellen der unterstützten Service Graph Connectors, ihre Toolkategorien und die Arten der Daten an, in die sie importiert werden Unterstützte Hardware Service Graph Connectors für Sicherheitsstatus-Überwachung Und Unterstützte Software Service Graph Connectors für Sicherheitsstatus-Überwachung.

Sicherheitsstatus-Überwachung Anwendungsfall: Assets mit fehlendem Endpunktschutz werden erkannt

Um Assets zu erkennen, für die kein Endpunktschutz-Agent fehlt, sind die folgenden Voraussetzungen erforderlich.

Je nach Anwendungsfall können Sie nur die erforderlichen Connectors aktivieren.

1. Aktivieren Sie mindestens einen Service Graph Connector aus der Kategorie „Endpunktschutz“.
2. Aktivieren Sie mindestens einen Service Graph Connector für EINE der folgenden Kategorien.
   a. Verzeichnisservices (Microsoft Active Directory).
   b. Endpunktverwaltung: Microsoft Intune Oder Jamf-Geräte- und Endpunktverwaltung.
   c. Konfigurations- und Patch-Management: Microsoft SCCM oder IBM Bigfix.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Cloud-Provider: Amazon AWS Cloud, Microsoft Azure, GCP.

> **Hinweis:**
> Wenn Cloud-Discovery aktiviert ist, sind diese Service Graph Connector-Produkte nicht erforderlich.

3. [Optional] Sie können Service Graph Connectors für eine der folgenden Kategorien aktivieren, um die Gesamtabdeckung zu verbessern, d. h. die Anzahl der Assets, die von der Sicherheitsstatus-Steuerung gemeldet und überwacht werden.
   a. Netzwerksicherheit
   b. Infrastrukturüberwachung
   c. Netzwerk
   d. Überwachung Der Anwendungsleistung#.

Nachdem Sie überprüft haben, dass Sie diese Voraussetzungen erfüllt haben, müssen Sie die folgende Richtlinie aktivieren: Assets ohne Endpunktschutz###. #Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung.

Sicherheitsstatus-Überwachung Anwendungsfall: Erkennung von Assets, die von Schwachstellenbewertungstools verpasst wurden

Um Assets zu erkennen, die von Schwachstellenbewertungstools verpasst wurden, sind die folgenden Voraussetzungen erforderlich.

Für jeden Service Graph Connector in der Liste können Sie sehen, ob dieser Connector für die Überwachung von lokalen Assets oder Cloud-Assets erforderlich ist. Je nach Anwendungsfall können Sie nur die erforderlichen Connectors aktivieren.

1. Aktivieren Sie mindestens einen Service Graph Connector aus der Kategorie Schwachstellenbewertung.
2. Aktivieren Sie mindestens einen Service Graph Connector für EINE der folgenden Kategorien.
   a. Verzeichnisservices (Microsoft Active Directory).
   b. Endpunktverwaltung: Microsoft Intune Oder Jamf-Geräte- und Endpunktverwaltung.
   c. Konfigurations- und Patch-Management: Microsoft SCCM oder IBM Bigfix.
   d. Cloud-Provider: Amazon AWS Cloud, Microsoft Azure, GCP.

> **Hinweis:**
> Wenn Cloud-Discovery aktiviert ist, sind diese Service Graph Connector-Produkte nicht erforderlich.

3. [Optional] Sie können Service Graph Connectors für eine der folgenden Kategorien aktivieren, um die Gesamtabdeckung zu verbessern, d. h. die Anzahl der Assets, die von der Sicherheitsstatus-Steuerung gemeldet und überwacht werden.
   a. Netzwerksicherheit#.
   b. Netzwerk.
   c. Infrastrukturüberwachung.
   d. Überwachung Der Anwendungsleistung#.

Nachdem Sie überprüft haben, dass Sie diese Voraussetzungen erfüllt haben, müssen Sie die folgende Richtlinie aktivieren: Assets, die nicht auf Schwachstellen gescannt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wurden. Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung.

Sicherheitsstatus-Überwachung Anwendungsfall: Nicht verwaltete Assets werden erkannt

Dieser Anwendungsfall umfasst zwei Teile: Die Erkennung von Assets, denen eine Konfiguration fehlt, und Patch-Management-Agents.

Um Assets mit fehlenden Konfigurations- und Patch-Management-Tools zu erkennen, sind die folgenden Voraussetzungen erforderlich.

Für jeden Service Graph Connector in der Liste können Sie sehen, ob dieser Connector für die Überwachung von lokalen Assets oder Cloud-Assets erforderlich ist.

Je nach Anwendungsfall können Sie nur die erforderlichen Connectors aktivieren.

1. Aktivieren Sie mindestens einen Service Graph Connector aus den Kategorien Konfigurations- und Patch-Management.
2. Mindestens ein Service Graph Connector muss für EINE der folgenden Kategorien aktiviert sein.
   a. Verzeichnisservices (Microsoft Active Directory).
   b. Endpunktschutz: CrowdStrike Oder SentinelOne.
   c. Schwachstellenbewertung: Qualys, Rapid7, Oder Tenable.
   d. Konfigurations- und Patch-Management: Microsoft SCCM oder IBM Bigfix.
3. [Optional] Sie können Service Graph Connectors für eine der folgenden Kategorien aktivieren, um die Gesamtabdeckung zu verbessern, d. h. die Anzahl der Assets, die von der Sicherheitsstatus-Steuerung gemeldet und überwacht werden.
   a. Netzwerk.
   b. Infrastrukturüberwachung
   c. Netzwerksicherheit
   d. Überwachung Der Anwendungsleistung#.

Nachdem Sie überprüft haben, dass Sie diese Voraussetzungen erfüllt haben, müssen Sie mindestens eine der folgenden Richtlinien aktivieren. #Für jede Richtlinie, die mit „Cloud-Assets“ beginnt, müssen Service Graph Connectors in der Kategorie „Cloud-Provider“ aktiviert sein. ##Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung.

- Für Assets fehlt Konfiguration und Patch-Management.
- Cloud-Assets fehlen Konfiguration und Patch-Management.

Sicherheitsstatus-Überwachung Anwendungsfall: Erkennung von Assets ohne Endpunktverwaltungslösung

Um Assets zu erkennen, für die keine Endpunktverwaltungslösung fehlt, sind die folgenden Voraussetzungen erforderlich.

Je nach Anwendungsfall können Sie nur die erforderlichen Connectors aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Aktivieren Sie mindestens einen Service Graph Connector aus der Kategorie „Endpunktmanagement“.
2. Mindestens ein Service Graph Connector muss für EINE der folgenden Kategorien aktiviert sein.
   a. Verzeichnisservices (Microsoft Active Directory).
   b. Endpunktschutz: CrowdStrike Oder SentinelOne.
   c. Schwachstellenbewertung: Qualys, Rapid7, Oder Tenable.
   d. Konfigurations- und Patch-Management: Microsoft SCCM oder IBM Bigfix.

Nachdem Sie überprüft haben, dass Sie diese Voraussetzungen erfüllt haben, müssen Sie die folgende Richtlinie aktivieren: Assets fehlende Endpunktverwaltungslösung. Weitere Informationen zu Richtlinien finden Sie unter Richtlinien für Sicherheitsstatus-Überwachung.

Sicherheitsstatus-Überwachung Anwendungsfall: Erkennung von Assets mit Schwachstellen und Sicherheitstool-Abdeckungslücken

Sie können Assets mit kritischen Schwachstellen und fehlenden kritischen Sicherheitstools wie Endpunktschutz identifizieren, um diese Assets für die Korrektur zu priorisieren. Die Sicherheitsstatus-Steuerung liefert einige Richtlinien, die im Produkt enthalten sind, um diesen Anwendungsfall zu unterstützen.

Für diesen Anwendungsfall müssen Sie die Anwendung Vulnerability Response und eine Integration mit mindestens einem Schwachstellenbewertungsprodukt wie installieren Qualys, Rapid7, Oder Tenable.

Die folgenden Richtlinien sind im Produkt „Sicherheitsstatus-Steuerung“ enthalten, um diesen Anwendungsfall für Assets mit kritischen Schwachstellen zu unterstützen, für die auch die Abdeckung von Sicherheitstools fehlt.

1. Assets mit kritischen Schwachstellen und fehlendem Endpunktschutz.
2. Assets mit kritischen Schwachstellen und fehlender Konfigurations- und Patch-Verwaltung.
3. Assets mit kritischen Schwachstellen und fehlender Endpunktverwaltung.

Sicherheitsstatus-Überwachung Anwendungsfall: Erkennung des Internetrisikos von Cloud-Assets#und Kombinationen mit hohem Risiko

Es ist wichtig, das potenzielle Internetrisiko von Cloud-Assets (virtuellen Maschinen) auf verschiedenen Ports zu überwachen, um sicherzustellen, dass Schwachstellen in diesen Assets nicht Remote ausgenutzt werden. Dieser Anwendungsfall hilft Ihnen, diese Assets zu identifizieren.

Mit der Sicherheitsstatus-Steuerung können Sie die Konfiguration von Cloud-Assets bewerten, um die Assets mit Internetzugriff zu identifizieren, d. h. welche Assets von überall im Internet erreichbar sind und über welche Ports sie zugänglich sind.

Die Sicherheitsstatus-Steuerung kombiniert diese Einblicke mit Abdeckungslücken von Sicherheitstools und Schwachstellendaten von Drittanbieterscannern wie Qualys, Rapid7, Oder Tenable, um Kombinationen mit hohem Risiko zu identifizieren.

Derzeit unterstützt dieser Anwendungsfall AWS und erfordert die folgenden Voraussetzungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Service Graph Connector für AWS wird für dieselben AWS-Accounts aktiviert, die Sie konfiguriert haben.
2. Sie haben eine oder mehrere der Richtlinien aktiviert, die im Produkt in der Sicherheitsstatus-Steuerung enthalten sind.
   - Cloud-Assets mit SSH-Port 22, offen für Internet.
   - Cloud-Assets mit SSH-Port 22, die für das Internet geöffnet sind und keinen Endpunktschutz aufweisen.
   - Cloud-Assets mit HTTP-Port 80, die für das Internet geöffnet sind und keinen Endpunktschutz aufweisen.
   - Cloud-Assets mit kritischen Schwachstellen und SSH-Port 22 offen für das Internet (erfordert Vulnerability Response).
   - Cloud-Assets mit kritischen Schwachstellen, fehlendem Endpunktschutz und SSH-Port 22 offen für das Internet (erfordert Vulnerability Response).
   - Cloud-Assets mit HTTP-Ports, die für das Internet geöffnet sind, kritischen Schwachstellen und fehlendem Endpunktschutz (erfordert Vulnerability Response).

Unterstützte Hardware Service Graph Connectors für Sicherheitsstatus-Überwachung

Unterstützte Hardware Service Graph Connectors mit CI-Klasse, Quelle (Produkt) und Toolkategorien. Diese Liste ist nicht vollständig und kann sich durch Hinzufügen weiterer Produkte ändern.

Für die Discovery-Quelle für einen aufgelisteten Connector steht „SG“, „SGO“ oder „SGC“ vor dem Produktnamen für Drittparteiprodukte, z. B. „SG-AWS“, „SGO-Datadog“ oder „SGC-AD“ (Active Directory). Bei ServiceNow-Produkten steht „SN“ oder „ServiceNow“ vor dem Produktnamen, z. B. „SNAssetManagement für ServiceNow Hardware Asset Management“.

Nach der Installation können Sie die Connectors und ihre Kategorien in der Connector-Tabelle [sn_sec_spc_Core_Connector] in Ihrer Instanz anzeigen.

Sie können Asset-Typen und ihre Zuordnung zu CI-Klassen und Connectors in der Tabelle [sn_sec_spc_Core_Asset_type_Connector] anzeigen.

Hardware Service Graph Connectors

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Hardware-Asset	cmdb_ci_computer	Active Directory	Directory Services
Hardware-Asset	cmdb_ci_server	AppDynamics	Application Performance Monitoring
Hardware-Asset	cmdb_ci_server	Automox	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_computer	Automox	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_computer	BigFix	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_server	BigFix	Konfigurations- und Patchverwaltung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardware Service Graph Connectors (Fortsetzung)

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Hardware-Asset	cmdb_ci_printer	Cisco Meraki	Netzwerk
Hardware-Asset	cmdb_ci_server	Cisco Meraki	Netzwerk
Hardware-Asset	cmdb_ci_iot	Cisco Meraki	Netzwerk
Hardware-Asset	cmdb_ci_hc_device	Cisco Meraki	Netzwerk
Hardware-Asset	cmdb_ci_netgear	Cisco Meraki	Netzwerk
Hardware-Asset	cmdb_ci_computer	Cisco Meraki	Netzwerk
Hardware-Asset	cmdb_ci_server	CrowdStrike	Endpunktschutz
Hardware-Asset	cmdb_ci_server	Datadog	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_server	Dynatrace	Application Performance Monitoring
Hardware-Asset	cmdb_ci_computer	Dynatrace	Application Performance Monitoring
Hardware-Asset	cmdb_ci_computer	ExtraHop-Enthüllung(x)	Netzwerksicherheit
Hardware-Asset	cmdb_ci_hc_device	ExtraHop-Enthüllung(x)	Netzwerksicherheit
Hardware-Asset	cmdb_ci_server	ExtraHop-Enthüllung(x)	Netzwerksicherheit
Hardware-Asset	cmdb_ci_iot	ExtraHop-Enthüllung(x)	Netzwerksicherheit
Hardware-Asset	cmdb_ci_printer	ExtraHop-Enthüllung(x)	Netzwerksicherheit
Hardware-Asset	cmdb_ci_iot	Forescout	Netzwerksicherheit
Hardware-Asset	cmdb_ci_hc_device	Forescout	Netzwerksicherheit
Hardware-Asset	cmdb_ci_computer	Forescout	Netzwerksicherheit
Hardware-Asset	cmdb_ci_server	Forescout	Netzwerksicherheit
Hardware-Asset	cmdb_ci_printer	Forescout	Netzwerksicherheit
Hardware-Asset	cmdb_ci_server	Intune	Endpunktverwaltung
Hardware-Asset	cmdb_ci_computer	Intune	Endpunktverwaltung
Hardware-Asset	cmdb_ci_printer	Jamf Pro	Endpunktverwaltung
Hardware-Asset	cmdb_ci_server	Jamf Pro	Endpunktverwaltung
Hardware-Asset	cmdb_ci_computer	Jamf Pro	Endpunktverwaltung
Hardware-Asset	cmdb_ci_server	Lansweeper	IT Asset Management
Hardware-Asset	cmdb_ci_computer	Lansweeper	IT Asset Management
Hardware-Asset	cmdb_ci_printer	Lansweeper	IT Asset Management
Hardware-Asset	cmdb_ci_hc_device	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_printer	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_server	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_vm_instance	LogicMonitor	Infrastrukturüberwachung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardware Service Graph Connectors (Fortsetzung)

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Hardware-Asset	cmdb_ci_iot	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_computer	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_netgear	LogicMonitor	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_server	Microsoft Defender	Endpunktschutz
Hardware-Asset	cmdb_ci_server	New Relic	Application Performance Monitoring
Hardware-Asset	cmdb_ci_computer	Nexthink	Digitale Mitarbeiter-Experience
Hardware-Asset	cmdb_ci_computer	Netskope	Vermeidung Von Datenverlust
Hardware-Asset	cmdb_hardware_product_model	Netskope	Vermeidung Von Datenverlust
Hardware-Asset	cmdb_ci_network_adapter	Netskope	Vermeidung Von Datenverlust
Hardware-Asset	cmdb_software_instance	Netskope	Vermeidung Von Datenverlust
Hardware-Asset	cmdb_sam_sw_install	Netskope	Vermeidung Von Datenverlust
Hardware-Asset	sn_sec_sgc_netskop_Client_Attribute	Netskope	Vermeidung Von Datenverlust
Hardware-Asset	cmdb_ci_server	Öffnen Sie Telemetrie	Application Performance Monitoring
Hardware-Asset	cmdb_ci_computer	Puppet	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_server	Puppet	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_computer	Qualys-IDs	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_server	Qualys-IDs	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_vm_instance	Qualys-ServiceNow	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_server	Qualys-ServiceNow	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_hardware	Rapid7	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_computer	SCCM	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_server	SCCM	Konfigurations- und Patchverwaltung
Hardware-Asset	cmdb_ci_printer	ScienceLogic	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_iot	ScienceLogic	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_server	ScienceLogic	Infrastrukturüberwachung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardware Service Graph Connectors (Fortsetzung)

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Hardware-Asset	cmdb_ci_computer	ScienceLogic	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_hc_device	ScienceLogic	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_vm_instance	ScienceLogic	Infrastrukturüberwachung
Hardware-Asset	cmdb_ci_hardware	ServiceNow HAM	Hardware Asset Management
Hardware-Asset	cmdb_ci_hardware	ServiceNow ITOM-Discovery	Discovery
Hardware-Asset	cmdb_ci_aws_datacenter	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_azure_datacenter	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_availability_zone	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_google_datacenter	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_cloud_service_account	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_cloud_subnet	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_compute_template	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_network	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_vm_instance	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_key_value	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_os_template	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_server	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_computer	SentinelOne	Endpunktschutz
Hardware-Asset	sn_sec_sgc_sntlone_Asset_Tags	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_ip_address	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_network_adapter	SentinelOne	Endpunktschutz
Hardware-Asset	sn_sec_sgc_sntlone_additional_attributes	SentinelOne	Endpunktschutz
Hardware-Asset	cmdb_ci_server	Tanium-Asset	Endpunktverwaltung
Hardware-Asset	cmdb_ci_computer	Tanium-Asset	Endpunktverwaltung
Hardware-Asset	cmdb_ci_ups	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_Industrial_Sensor	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_cnc	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_hardware	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_netgear	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_Industrial_actuator	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ip_switch	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_Hub_Network	Tenable	Schwachstellenbewertung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardware Service Graph Connectors (Fortsetzung)

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Hardware-Asset	cmdb_ci_Security	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_server	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_rtu	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_ews	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_plc	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_Control	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_dcs	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_storage_server	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_hmi	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_Control_Module	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_Industrial_Router	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_Historian	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_Industrial_Drive	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_iot	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_ip_Firewall	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_computer	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_Unclassed_Hardware	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_IDs_Netzwerk	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_OT_ied	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_printer	Tenable	Schwachstellenbewertung
Hardware-Asset	cmdb_ci_computer	VMware Workspace ONE UEM	Endpunktverwaltung
Hardware-Asset	cmdb_ci_server	VMware Workspace ONE UEM	Endpunktverwaltung
Hardware-Asset	cmdb_ci_printer	VMware Workspace ONE UEM	Endpunktverwaltung
Hardware-Asset	cmdb_ci_vm_instance	Assistent	Cloud-Native Anwendungsschutzplattform
Hardware-Asset	cmdb_ci_server	Assistent	Cloud-Native Anwendungsschutzplattform
Hardware-Asset	cmdb_ci_linux_server	Assistent	Cloud-Native Anwendungsschutzplattform
Hardware-Asset	cmdb_ci_win_server	Assistent	Cloud-Native Anwendungsschutzplattform

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Software Service Graph Connectors für Sicherheitsstatus-Überwachung

Unterstützte Software Service Graph Connectors mit CI-Klasse, Quelle (Produkt) und Toolkategorien. Diese Liste ist nicht vollständig und kann sich durch Hinzufügen weiterer Produkte ändern.

Nach der Installation können Sie die Connectors und ihre Kategorien in der Connector-Tabelle [sn_sec_spc_Core_Connector] in Ihrer Instanz anzeigen.

Sie können Asset-Typen und ihre Zuordnung zu CI-Klassen und Connectors in der Tabelle [sn_sec_spc_Core_Asset_type_Connector] anzeigen.

Software Service Graph Connectors

Asset-Typ	CI-Klasse	Asset-Quelle	Connector-Kategorie
Software	cmdb_ci_spkg	BigFix	Konfigurations- und Patchverwaltung
Software	cmdb_ci_spkg	Dynatrace	Application Performance Monitoring
Software	cmdb_ci_spkg	Forescout	Netzwerksicherheit
Software	cmdb_ci_spkg	Intune	Endpunktverwaltung
Software	cmdb_ci_spkg	Jamf Pro	Endpunktverwaltung
Software	cmdb_ci_spkg	New Relic	Application Performance Monitoring
Software	cmdb_ci_spkg	Nexthink	Digitale Mitarbeiter-Experience
Software	cmdb_ci_spkg	Netskope	Vermeidung Von Datenverlust
Software	cmdb_ci_spkg	Qualys-ServiceNow	Schwachstellenbewertung
Software	cmdb_ci_spkg	SCCM	Konfigurations- und Patchverwaltung
Software	cmdb_ci_spkg	ServiceNow ITOM-Discovery	Discovery
Software	cmdb_ci_spkg	Tanium-Asset	Endpunktverwaltung
Software	cmdb_ci_spkg	VMware Workspace ONE UEM	Endpunktverwaltung

Beispiele für Basis-, untergeordnete und geklonte Richtlinien für Sicherheitsstatus-Überwachung

Sie können eigene Basisrichtlinien erstellen, die über breite Sätze von Bedingungen verfügen, die Sie als Ausgangspunkte für komplexere Richtlinien verwenden können.

Beispiele

Die folgenden Beispiele helfen Ihnen zu sehen, wie Sie die Bedingungen einer Basisrichtlinie wiederverwenden können, wenn Sie andere Richtlinien erstellen, indem Sie untergeordnete

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinien erstellen oder vorhandene Richtlinien klonen. Diese Beispiele helfen Ihnen auch, zu sehen, wie der Richtliniengenerator im Modul „Richtlinien und Ergebnisse“ funktioniert.

Beginnen Sie mit dem ersten Beispiel, der Basisrichtlinie. Die anderen Beispiele verwenden die Basisrichtlinie als Ausgangspunkt.

Hinweis:
Der CrowdStrike Service Graph Connector wird in diesen Beispielen als Service Graph Connector verwendet, Sie können jedoch jeden von Ihnen installierten Connector verwenden. In diesen Beispielen können Sie Richtlinien erstellen und aktivieren, um nach Asset-Übereinstimmungen zu suchen. Sie können diese Richtlinien jederzeit aus dem Modul „Richtlinien und Ergebnisse“ entfernen, nachdem Sie sie aktiviert haben.

Erstellen Sie eine Basisrichtlinie für Sicherheitsstatus-Überwachung(Beispiel)

Ein Beispiel für die Erstellung einer Basisrichtlinie, die Sie zum Erstellen anderer Richtlinien verwenden können.

Vorbereitungen
Erforderliche Rollen: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereich Für Sicherheitsstatus-Steuerung** > **Richtlinien und Ergebnisse**an.
2. Wählen Sie Aus **Neue Richtlinie** .
3. Wählen Sie das Pen-Symbol oben links aus, und füllen Sie die Felder im Modal „Metadaten bearbeiten“ aus.
4. Wählen Sie Aus **Speichern Sie Metadaten** .
5. Wählen Sie im Bedingungsgenerator die Option aus **Hardware-Asset** Für Asset-Typ.

   Belassen Sie für diese Richtlinie die Optionen Basisrichtlinie und Ausschlussrichtlinien in ihren Standardeinstellungen (aus).
6. Wählen Sie für Verbindung aus **Mit zusammengefassten Daten** .

   Für diese Richtlinie helfen aggregierte Daten Ihnen, Assets in Ihrer CMDB zu finden, auf denen Windows 10 installiert ist. Zum Beispiel können einige Datensätze geringfügige Variationen darüber aufweisen, wie verschiedene Scanner „Windows 10“ melden. Zusammengefasste Daten stellen sicher, dass alle diese geringfügigen Variationen von „Windows 10“ dieser Richtlinie entsprechen.

   Die Felder Entität und Kriterien werden basierend auf Ihrer Auswahl im Feld Verbindung automatisch ausgefüllt.
7. Wählen Sie für Eigenschaft aus **BETRIEBSSYSTEM** .
8. Für Wert geben Sie in ein `Windows 10` .
9. Wählen Sie **Änderungen speichern**.
   Ihre Basisrichtlinie wird in der Liste alle des Moduls „Richtlinien und Ergebnisse“ angezeigt, ist jedoch nicht aktiviert.
10. Wählen Sie Aus **Aktivieren Sie die Richtlinie** Daher überwacht Ihre Basisrichtlinie alle Assets, die den Bedingungen der Richtlinie entsprechen, und generiert Ergebnisse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine untergeordnete Richtlinie aus einer Basisrichtlinie für Sicherheitsstatus-Überwachung(Beispiel)

Ein Beispiel für das Erstellen einer untergeordneten Richtlinie mit den Bedingungen einer Basisrichtlinie.

Vorbereitungen

Diese untergeordnete Richtlinie erbt die Bedingungen einer Basisrichtlinie, und Sie fügen Ihrer untergeordneten Richtlinie weitere Bedingungen hinzu, damit Sie sich auf spezifischere Asset-Details konzentrieren können. Sie möchten eine neue Richtlinie zur Überwachung aller Ihrer Geräte, auf denen Windows 10 installiert ist und die von gemeldet werden CrowdStrike Service Graph Connector, und Sie möchten alle Geräte ausschließen, die einer anderen Richtlinie entsprechen. In diesem Beispiel schließen Sie Assets aus, die für Ausnahmen des integrierten Risikomanagements (IRM) genehmigt wurden.

Hinweis:
Wenn Sie nicht haben CrowdStrike Service Graph Connector installiert. Sie können einen verwenden, der installiert ist.

Erforderliche Rollen: SPC-Administratorgruppe oder SPC-Analystengruppe

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereich Für Sicherheitsstatus-Steuerung** > **Richtlinien und Ergebnisse**an.
2. Suchen Sie in der Liste aktiv nach der Basisrichtlinie – Windows 10-Geräte, die Sie im ersten Beispiel erstellt haben, und wählen Sie sie aus, um den Datensatz zu öffnen.
3. Wählen Sie das Menü weitere Optionen (drei vertikale Punkte), und wählen Sie aus **Erstellen Sie eine untergeordnete Richtlinie** .
   Eine neue Registerkarte wird geöffnet und mit einem neuen Datensatz und der Basisrichtlinie – Windows 10-Geräte wird im Feld Basisrichtlinie angezeigt.
4. Wählen Sie oben links das Pen-Symbol aus, und füllen Sie im Modal „Metadaten bearbeiten“ die Felder aus.
5. Wählen Sie Aus **Speichern Sie Metadaten** .
6. Wählen Sie im Bedingungsgenerator die Option aus **Hardware-Asset** Für Asset-Typ.
7. Wählen Sie den Umschalter Basisrichtlinie aus.
8. Wählen Sie die von Ihnen erstellte Richtlinie aus, z. B. 1, **Basisrichtlinie: Windows 10-Geräte** Aus der Liste.

   Diese untergeordnete Richtlinie erbt automatisch die Bedingungen der Basisrichtlinie.
9. Wählen Sie den Umschalter für Ausschlussrichtlinien aus.
10. Wählen Sie Assets mit IRM-Ausnahme genehmigt aus der Liste aus.

Hinweis:
Wenn Sie diese Richtlinie nicht haben, können Sie eine andere Richtlinie aus der Liste auswählen, die Sie von dieser Richtlinie ausschließen möchten.

Die Assets, die dieser Richtlinie entsprechen, werden aus Ihrer untergeordneten Richtlinie ausgeschlossen. Beachten Sie, dass Sie weitere Richtlinien hinzufügen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

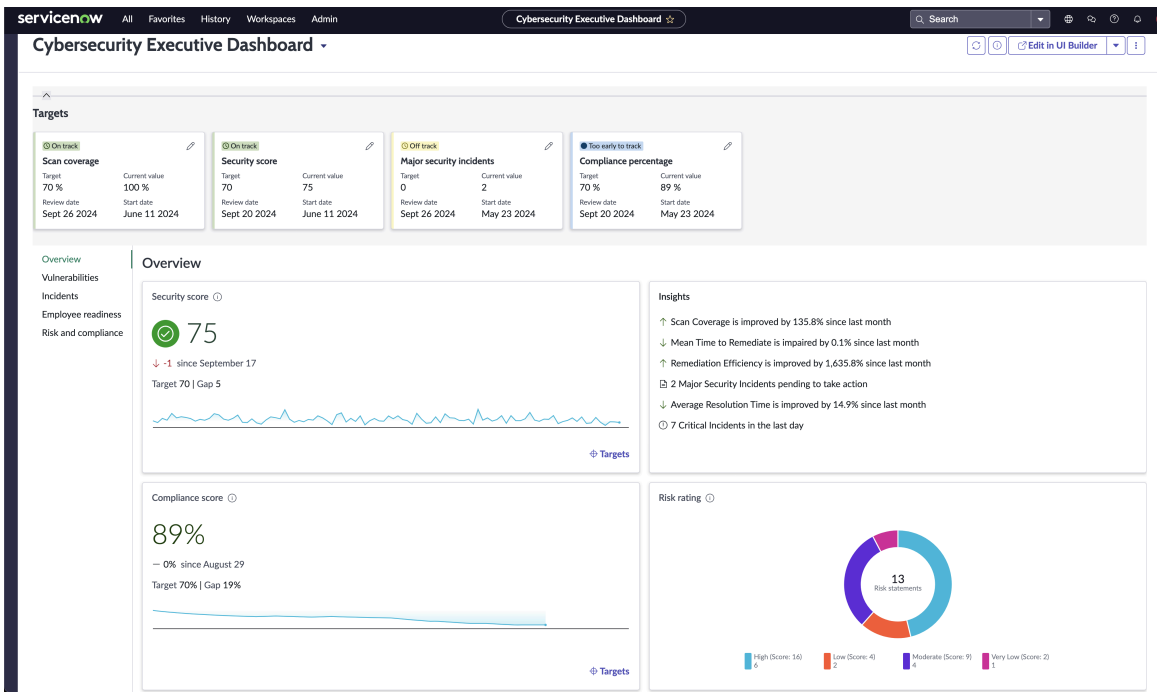
11. Wählen Sie Aus **Gemeldet von** .
12. Wählen Sie Aus **CrowdStrike** Aus der Liste.
13. Wählen Sie **Änderungen speichern**.
    Ihre neue Richtlinie wird in der Liste alle des Moduls „Richtlinien und Ergebnisse“ angezeigt, ist jedoch nicht aktiviert.
14. Wählen Sie Aus **Aktivieren Sie die Richtlinie** Daher überwacht Ihre Basisrichtlinie alle Assets, die den Bedingungen der Richtlinie entsprechen, und generiert Ergebnisse.

Cybersicherheits-Dashboard

Das Cybersicherheits-Dashboard ist eine umfassende Lösung, die Chief Information Security Officers (CISOs) und CyberSecurity Executives Einblick in die Sicherheitslage und -Initiativen der Organisation ermöglicht. Das -Dashboard konsolidiert Daten aus verschiedenen Produkten innerhalb von ServiceNow Security Operations-Suite und Governance, Risk and Compliance (GRC).

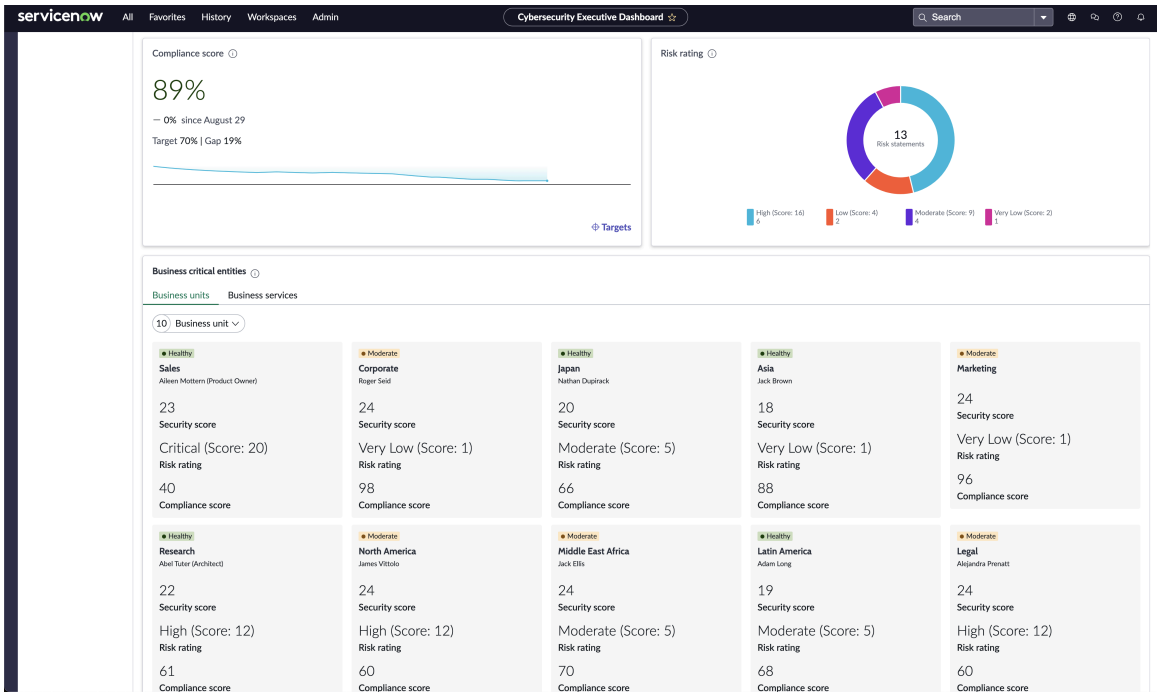
Das Dashboard bietet die folgenden Funktionen:

- Organisationsweite Bewertung der Sicherheitslage
- Sicherheits-, Risiko- und Compliance-Punktzahlen nach Geschäftsbereich
- Anpassbare Überwachung
- Einheitliche Ansicht der Sicherheitslandschaft einer Organisation
- Benchmarking
- Anwenderfreundliche Oberfläche
- Einblick in Phishing-Simulationsmetriken aus KnowBe4 und Microsoft Defender for Office 365



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Funktionen ermöglichen eine proaktive Entscheidungsfindung, indem sie schnellen Zugriff auf kritische Sicherheitsmetriken bieten. Somit ist es ein unverzichtbares Tool zur Verbesserung der allgemeinen Sicherheitsresilienz und -Bereitschaft.



Erforderliche ServiceNow AI Platform-Rollen

- CISO (sn_Bod.ciso) zum Anzeigen und Freigeben des Dashboards.
- sn_Bod.ciso_admin zum Anzeigen, Freigeben des Dashboards und Konfigurieren von Gewichtungen für die Bewertung der Sicherheitslage.
- GRC CISO-Anwender (sn_grc_dashboards.grc_ciso_user) zum Anzeigen von Risiko- und Compliance-Berichten.

Greifen Sie auf das Dashboard für Cybersicherheit-Führungskräfte zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Cybersicherheits-Dashboard** > **Cybersicherheits-Dashboard**an.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
Chief Information Security Officers (CISOs)	CISOs erhalten Einblicke in Schwachstellenmanagement, Incident-Management, Sicherheitslage der Organisation, Phishing-Simulationsmetriken usw. für ihre Organisationen.

Datenvisualisierung

Hinweis:

Um mehr über ein Widget zu erfahren, wählen Sie das Informationssymbol ⓘ.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ziele

Metriken	Typ	Beschreibung
Ziele	Prozentsatz	Zeigt das festgelegte Ziel an, das für eine Metrik abgedeckt werden soll. Der Status der Ziele wird durch Farbcodierung angezeigt. Zeigt alle Ziele an, deren Überprüfungsdatum entweder innerhalb der letzten 30 Tage oder in Kürze liegt. Sie können die Anzahl der Tage für die Anzeige von Zielen mit festlegen `sn_bod.show_targets_from`Systemeigensch Darüber hinaus können diese Ziele bearbeitet werden. Weitere Informationen finden Sie unter Legen Sie Ziele fest.

Metriken	Typ	Beschreibung
Sicherheitspunktzahl	Einzelne Punktzahl	Gesamtpunktzahl der Sicherheitslage der Organisation unter Berücksichtigung angreifbarer Elemente, Security Incidents, schwerwiegender Security Incidents und Fehlkonfigurationen.
Einblicke	Hervorhebungen	Highlights des gesamten Dashboards.
Compliance-Bewertung	Einzelne Punktzahl	Stellt die Compliance-Situation der Organisation mithilfe der Compliance-Punktzahl bereit, die basierend auf dem Prozentsatz der konformen Steuerungen aus der Gesamtzahl der Steuerungen berechnet wird.
Risikopunktzahl	Einzelne Punktzahl	Stellt die Anzahl der Risikobeschreibungen basierend auf den Risikobewertungen bereit. Es hilft Unternehmen, die potenziellen Auswirkungen und die Wahrscheinlichkeit verschiedener Risiken zu verstehen, sodass sie diese Risiken priorisieren und verwalten können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken	Typ	Beschreibung
Geschäftskritische Entitäten		
Geschäftsbereiche	Einzelne Punktzahl	Gesamtsicherheitspunktzahl der Geschäftsbereiche unter Berücksichtigung des Risikos im Zusammenhang mit Schwachstellen, Fehlkonfigurationen, Schwachstellen der operativen Technologie (OT), Security Incidents und schwerwiegenden Security Incidents. Die Integritätsbezeichnung der Geschäftsbereiche basiert nur auf der Sicherheitspunktzahl. Um zu sehen, wie diese Bezeichnungen zugewiesen werden, navigieren Sie zur Tabelle Risikopunktzahlgewichtungen [sn_sec_cmn_Risk_Score_weight_list.do], und suchen Sie nach einer Geschäftsentität. Bezeichnungen wie „fehlerfrei“ werden basierend auf vordefinierten Wertbereichen zugewiesen. Beispielsweise wird eine Sicherheitspunktzahl zwischen 0 und 39 als fehlerfrei gekennzeichnet. Die Farbcodierung für diese Bezeichnungen ist in angegeben UnifiedCISOUtils Skripteinbindung. Sie können sowohl den Wertebereich als auch die Farben für die Bezeichnungen konfigurieren. Um zu sehen, wie die Geschäftsbereichs- und Geschäftsbereichsobernamen zugewiesen werden, wechseln Sie zu **Alle** > **Organisation** > **Geschäftsbereiche**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken	Typ	Beschreibung
		Hinweis: Je nachdem, welche Plugins Sie aktiviert haben, können Sie auf die Compliance-Punktzahl, die Risikopunktzahl und die Sicherheitspunktzahl zugreifen. Um die Compliance- und Risikopunktzahl anzuzeigen, müssen Sie die GRC-Plugins aktivieren. Um die Sicherheitspunktzahl anzuzeigen, müssen Sie die Plugins im Zusammenhang mit Security Operations aktivieren. Weitere Informationen finden Sie im Abschnitt „Anwendungen zu aktiv“.
Geschäftsservices	Einzelne Punktzahl	Gesamtsicherheitspunktzahl der Business-Services unter Berücksichtigung des Risikos im Zusammenhang mit Schwachstellen, Fehlkonfigurationen, Schwachstellen der operativen Technologie (OT), Security Incidents und schwerwiegenden Security Incidents. Um zu sehen, wie diese Bezeichnungen zugewiesen werden, navigieren Sie zur Tabelle Risikopunktzahlgewichtungen [sn_sec_cmn_Risk_Score_weight_list.do], und suchen Sie nach einer Geschäftsentität. Bezeichnungen wie „fehlerfrei“, „Mittel“ und „Kritisch“ werden basierend auf vordefinierten Wertbereichen zugewiesen. Beispielsweise wird eine Sicherheitspunktzahl zwischen 0 und 39 als fehlerfrei gekennzeichnet. Die Farbcodierung für diese Bezeichnungen ist in angegeben UnifiedCISOUtils Skripteinbindung. Sie können sowohl den Wertebereich

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken	Typ	Beschreibung
		als auch die Farben für die Bezeichnungen konfigurieren. Um zu sehen, wie der Geschäftsbereich und der Geschäftsbereichskopf zugewiesen werden, wechseln Sie zu **Alle** > **Organisation** > **Geschäftsbereiche**an. **Hinweis:** Je nachdem, welche Plugins Sie aktiviert haben, können Sie auf die Compliance-Punktzahl, die Risikopunktzahl und die Sicherheitspunktzahl zugreifen. Um die Compliance- und Risikopunktzahl anzuzeigen, müssen Sie die GRC-Plugins aktivieren. Um die Sicherheitspunktzahl anzuzeigen, müssen Sie die Plugins im Zusammenhang mit Security Operations aktivieren. Weitere Informationen finden Sie im Abschnitt „Anwendungen zu aktiv“.

Schwachstellen

Metriken	Typ	Beschreibung
Durchschnittliche Zeit bis zur Fehlerkorrektur (monatlich)	Liniendiagramm	Durchschnittliche Zeit, die in einem Monat zum Schließen von Schwachstellen und fehlgeschlagenen Testergebnissen für alle Assets (Hosts, Container und Anwendungen) benötigt wurde. Außerdem werden die folgenden Metriken bereitgestellt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

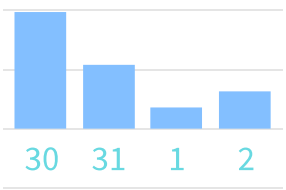
Schwachstellen (Fortsetzung)

Metriken	Typ	Beschreibung
		• Ziel: Ziel in Tagen zur Behebung der Schwachstellen. • Lücke: Differenz in Tagen zwischen dem Ziel und der tatsächlichen Zeit, die zur Behebung der Schwachstellen benötigt wird. • Branchen-Benchmark: Durchschnitt der Metriken von Peers in derselben Branche. • Globale Benchmark: Durchschnitt der Metriken der Peers auf dem globalen Markt Siehe Aktivieren Sie Benchmark-Punktzahlen Wie die Benchmark-Punktzahlen angezeigt werden.
Durchschnittliches Alter aktiver Schwachstellen (monatlich)	Einzelne Punktzahl	Monatliches Durchschnittsalter aller drei Arten von angreifbaren Elementen. Außerdem bietet es einen Vergleich des aktuellen Monatsalters mit dem vorherigen Monat. Außerdem werden die folgenden Metriken bereitgestellt: • Branchen-Benchmark: Durchschnitt der Metriken von Peers in derselben Branche. • Globale Benchmark: Durchschnitt der Metriken der Peers auf dem globalen Markt • Ziel: Ziel in Tagen zur Behebung der Schwachstellen.
Effizienz der Fehlerbehebung (monatlich)	Einzelne Punktzahl	Prozentsatz der monatlichen geschlossenen angreifbaren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

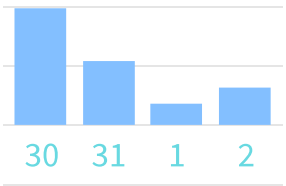
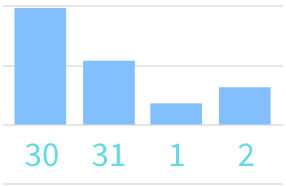
Schwachstellen (Fortsetzung)

Metriken	Typ	Beschreibung
		Elemente zu monatlichen aktiven angreifbaren Elementen. Außerdem werden die folgenden Metriken bereitgestellt: • Prozentuale Änderung gegenüber dem vorherigen Monat. • Ziel: Ziel in Prozent zur Behebung der Schwachstellen. • Lücke: Die Lücke zwischen Ziel- und aktueller Punktzahl. • Branchen-Benchmark: Durchschnitt der Metriken von Peers in derselben Branche. • Globale Benchmark: Durchschnitt der Metriken der Peers auf dem globalen Markt
Durchschnittliches aktiver Schwachstellen nach Zuweisungsgruppe.	Mehrere Zeilen	Durchschnittliches Alter der aktiven Schwachstellen für jede Zuweisungsgruppe.
Schwachstellen nach Risikobewertung und Alter	Heatmap	Aufgliederung der aktiven Schwachstellen auf Hosts, Containern und Anwendungen nach Risikobewertung und Alter.
Einhaltung des Korrekturziels nach Zuweisungsgruppe	Vertikaler Balken  	Verhältnis der Anzahl der Schwachstellen und Fehlkonfigurationen, die innerhalb des Korrekturziels geschlossen wurden, zur Gesamtzahl der geschlossenen Schwachstellen und Fehlkonfigurationen.
Scan-Abdeckung	Prozentsatz	Prozentsatz der in den letzten 90 Tagen gescannten Assets aller Assets in CMDB.
Assets gescannt im Vergleich zu ungescannt	Horizontale Leiste	Aufgliederung der in den letzten 90 Tagen gescannten Assets und der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellen (Fortsetzung)

Metriken	Typ	Beschreibung
		gesamten Assets in CMDB Nach CI-Klasse
Assets gescannt	Horizontale Leiste	Assets, die in den letzten 90 Tagen auf Schwachstellen im Vergleich zur Konfigurations-Compliance gescannt wurden.
Trend für aktive Funde der Stufen kritisch und hoch	Mehrere Zeilen	Täglicher Trend der Schwachstellen und Fehlkonfigurationen mit kritischer und hoher Risikobewertung.
Schwachstellen nach Asset-Kategorie und Risikobewertung	Vertikaler Balken 	Aufgliederung der aktiven Schwachstellen und Fehlkonfigurationen nach Asset-Kategorie und Risikobewertung (Kritisch, hoch und Mittel).
Nach Grund und Zuweisungsgruppe zurückgestellte Funde	Vertikaler Balken 	Aufgliederung der zurückgestellten aktiven Schwachstellen und Fehlkonfigurationen nach Zurückstellungsgrund und Zuweisungsgruppe.
Operative Technologien (OT)		
Trend für aktive kritische und Schwachstellen mit hoher Anfälligkeit	Position	Täglicher Trend der aktiven OT-Schwachstellen mit kritischer und hoher Risikobewertung.
Durchschnittliche Zeit bis zur Fehlerkorrektur (monatlich)	Einzelne Punktzahl	Durchschnittliche Zeit zum Schließen von OT-Schwachstellen. Verhältnis des Gesamtalters der geschlossenen OT-Schwachstellen zur Gesamtzahl der OT-Schwachstellen. Außerdem werden die folgenden Metriken bereitgestellt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schwachstellen (Fortsetzung)

Metriken	Typ	Beschreibung
		• Prozentuale Änderung gegenüber dem vorherigen Monat. • Ziel: Ziel in Tagen zur Behebung der Schwachstellen. • Branchen-Benchmark: Durchschnitt der Metriken von Peers in derselben Branche. • Globale Benchmark: Durchschnitt der Metriken der Peers auf dem globalen Markt Siehe Aktivieren Sie Benchmark-Punktzahlen Wie die Benchmark-Punktzahlen angezeigt werden.
Schwachstellen nach Risikobewertung und Alter	Heatmap	Aufgliederung der aktiven OT-Schwachstellen nach Risikobewertung und Alter.
Durchschnittliches Alter aktiver Schwachstellen (monatlich)	Liniendiagramm	Monatliches Durchschnittsalter angreifbarer OT-Elemente. Außerdem bietet es einen Vergleich des aktuellen Monatsalters mit dem vorherigen Monat.
Schwachstellen nach Status und Alter	Heatmap	Aufgliederung der aktiven OT-Schwachstellen nach Status und Alter.

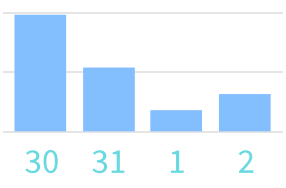
Incidents

Metriken	Typ	Beschreibung
Schwerwiegende Security Incidents	Einzelne Punktzahl	Anzahl der derzeit aktiven schwerwiegenden Security Incidents
Durchschnittliche Lösungszeit für Security Incidents (monatlich)	Einzelne Punktzahl	Monatliche durchschnittliche Lösungszeit geschlossener Security Incidents in Tagen. Außerdem werden die folgenden Metriken bereitgestellt:

Automatische Übersetzung

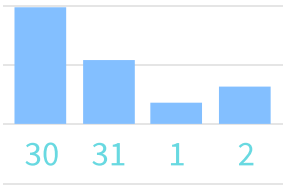
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incidents (Fortsetzung)

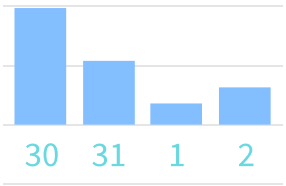
Metriken	Typ	Beschreibung
		• Prozentuale Änderung gegenüber dem vorherigen Monat. • Ziel: Ziel in Tagen zur Behebung der Security Incidents. • Lücke: Die Lücke zwischen den tatsächlichen Tagen, die für die Lösung benötigt wurden, und dem Ziel, das behoben werden soll. • Branchen-Benchmark: Durchschnitt der Metriken von Peers in derselben Branche. • Globale Benchmark: Durchschnitt der Metriken der Peers auf dem globalen Markt
Durchschnittliche Zeit bis Beseitigung (monatlich)	Liniendiagramm	Monatliche durchschnittliche Lösung in Tagen zur Beseitigung von Security Incidents.
Durchschnittliche Zeit für Identifizierung (monatlich)	Einzelne Punktzahl	Monatliche durchschnittliche Lösung in Tagen zur Identifizierung der Security Incidents.
Durchschnittliche Zeit bis zur Eindämmung (monatlich)	Einzelne Punktzahl	Monatliche durchschnittliche Lösung in Tagen zur Eindämmung von Security Incidents.
Aktive Incidents nach Priorität und Kategorie	Heatmap	Anzahl der aktiven Security Incidents, die nach Priorität und Kategorie kategorisiert sind.
Trend geschlossener und offener Incidents	Vertikaler Balken 	Aufgliederung der geschlossenen und offenen Incidents.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incidents (Fortsetzung)

Metriken	Typ	Beschreibung
Aktive Incidents nach Status	Vertikaler Balken 	Aufgliederung der aktiven Incidents basierend auf ihren status.

Mitarbeiterbereitschaft

Metriken	Typ	Beschreibung
Übersicht über die monatliche Phishing-Simulation	Vertikaler Balken 	Summe der Anwender, die die Aktionen wie „geöffnet“, „angeklickt“ und „gemeldet“ in der Phishing-Simulation ausgeführt haben, zusammen mit der Summe der Gesamtzahl der Anwender jeder Simulation in den letzten sechs Monaten.

Risiko und Compliance

Zum Anzeigen von Risiko- und Compliance-Widgets müssen Sie die GRC-Plugins aktivieren. Informationen zu GRC-Plugins finden Sie im Abschnitt zu aktivierende Anwendungen. Informationen zu GRC-Widgets finden Sie unter Risiko- und Compliance-Dashboard für GRC: Metrics.

Indikatoren

Host-SLA: Geschlossen

Dieser Indikator wird täglich berechnet. Berücksichtigt das Gesamtalter aller Host-Schwachstellen, die am Vortag zum Zeitpunkt der Berechnung geschlossen wurden.

Container-SLA: Geschlossen

Dieser Indikator wird täglich berechnet. Berücksichtigt alle Container-Schwachstellen, die am Vortag zum Zeitpunkt der Berechnung geschlossen wurden.

Anwendungs-SLA: Geschlossen

Dieser Indikator wird täglich berechnet. Berücksichtigt das Gesamtalter aller Anwendungsschwachstellen, die am Vortag zum Zeitpunkt der Berechnung geschlossen wurden.

Testergebnis-SLA: Bestanden

Dieser Indikator wird täglich berechnet. Berücksichtigt alle Schwachstellen des Testergebnisses, die am Vortag zum Zeitpunkt der Berechnung bestanden wurden.

Host-SLA – Anzahl geschlossener

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl aller Host-Schwachstellen, die am Vortag zum Zeitpunkt der Berechnung geschlossen wurden.

Container-SLA – Anzahl geschlossener

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl aller Container-Schwachstellen, die am Vortag zum Zeitpunkt der Berechnung geschlossen wurden.

Anwendungs-SLA – Anzahl geschlossener

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl aller Anwendungsschwachstellen, die am Vortag zum Zeitpunkt der Berechnung geschlossen wurden.

Testergebnis-SLA: Anzahl der bestandenen Tests

Dieser Indikator wird täglich gemessen. Berücksichtigt die Anzahl aller Testergebnis-Schwachstellen, die zuletzt am Vortag zum Zeitpunkt der Berechnung übergeben wurden.

Gescannte Assets

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der gescannten CIs aus der Tabelle „sn_vul_Analytics_Scan_Coverage_config“, die die zuletzt innerhalb der letzten 90 Tage gescannten CIs für alle CMDB-CI-Klassen enthält.

Scannbare Assets

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der CIs insgesamt aus der Tabelle „sn_vul_Analytics_Scan_Coverage_config“ für alle vorhandenen CMDB-CI-Klassen.

Angreifbare Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl der aktiven angreifbaren Elemente zum Zeitpunkt der Berechnung.

Angreifbares Anwendungselement

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl der aktiven angreifbaren Anwendungselemente zum Zeitpunkt der Berechnung.

Angreifbares Container-Element

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl der aktiven angreifbaren Container-Elemente zum Zeitpunkt der Berechnung.

Summiertes Alter der angreifbaren Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt das summierte Alter der aktiven angreifbaren Elemente zum Zeitpunkt der Berechnung.

Summiertes Alter der angreifbaren Anwendungselemente

Dieser Indikator wird täglich berechnet. Berücksichtigt das summierte Alter der aktiven angreifbaren Anwendungselemente zum Zeitpunkt der Berechnung.

Offene angreifbare Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt die offenen angreifbaren Elemente zum Zeitpunkt der Berechnung.

Offene angreifbare Container-Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt die offenen angreifbaren Container-Elemente zum Zeitpunkt der Berechnung.

Offene angreifbare Anwendungselemente

Dieser Indikator wird täglich berechnet. Berücksichtigt die offenen angreifbaren Anwendungselemente zum Zeitpunkt der Berechnung.

Aktive Testergebnisse

Dieser Indikator wird täglich berechnet. Berücksichtigt die offenen Testergebnisse zum Zeitpunkt der Berechnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zurückgestellte VITs

Dieser Indikator wird täglich berechnet. Es hat eine Indikatorquelle als angreifbares Host-Element.

Zurückgestellte AVITs

Dieser Indikator wird täglich berechnet. Sie hat eine Indikatorquelle als angreifbares Anwendungselement.

Zurückgestellte CVITs

Dieser Indikator wird täglich berechnet. Es hat eine Indikatorquelle als angreifbares Container-Element.

Zurückgestellte Testergebnisse

Dieser Indikator wird täglich berechnet. Berücksichtigt die Testergebnisse, die sich in einem zurückgestellten Status befanden.

Offene Konfigurationsprobleme – Testergebnisse

Dieser Indikator wird täglich berechnet. Es hat eine Indikatorquelle als Testergebnis für das Dashboard „einheitliche Schwachstellenantwort“.

SI – Durchschnittliche Zeit bis zur Identifizierung

Dieser Indikator wird täglich berechnet. Berücksichtigt den Security Incident, bei dem die Definition zum Zeitpunkt der Berechnung an der Zeit für die Identifizierung ist.

SI – Durchschnittliche Dauer

Dieser Indikator wird täglich berechnet. Berücksichtigt den Security Incident, bei dem die Definition zum Zeitpunkt der Berechnung eine Incident-Statusdauer ist.

Anzahl der offenen schwerwiegenden Security Incidents

Dieser Indikator wird täglich berechnet. Berücksichtigt offene schwerwiegende Security Incidents zum Zeitpunkt der Berechnung.

Anzahl der geschlossenen Security Incidents

Dieser Indikator wird täglich berechnet. Berücksichtigt geschlossene Security Incidents zum Zeitpunkt der Berechnung.

Geschlossene angreifbare Anwendungselemente

Dieser Indikator wird täglich berechnet. Berücksichtigt geschlossene angreifbare Anwendungselemente zum Zeitpunkt der Berechnung.

Geschlossene angreifbare Container-Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt geschlossene angreifbare Container-Elemente zum Zeitpunkt der Berechnung.

Geschlossene angreifbare Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt geschlossene angreifbare Elemente zum Zeitpunkt der Berechnung.

Maximale Risikopunktzahl für angreifbares Elemente abrufen

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximale Risikopunktzahl für angreifbare Elemente zum Zeitpunkt der Berechnung.

Maximale Risikopunktzahl für angreifbares Container-Element abrufen

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximale Risikopunktzahl für angreifbare Container-Elemente zum Zeitpunkt der Berechnung.

Maximale Risikopunktzahl für angreifbare Anwendungselemente abrufen

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximale Risikopunktzahl für angreifbare Anwendungselemente zum Zeitpunkt der Berechnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Summierte Risikopunktzahl von VITs

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der Risikopunktzahlen angreifbarer Elemente zum Zeitpunkt der Berechnung.

Summierte Risikopunktzahl von AVIs

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der Risikopunktzahlen von angreifbaren Anwendungselementen zum Zeitpunkt der Berechnung.

Summierte Risikopunktzahl von CVIs

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der Risikopunktzahlen angreifbarer Container-Elemente zum Zeitpunkt der Berechnung.

Summierte Risikopunktzahl der Fehlkonfigurationen

Dieser Indikator wird täglich berechnet. Berücksichtigt die Summe der Risikopunktzahlen der Testergebnisse zum Zeitpunkt der Berechnung.

Maximale Risikopunktzahl für SI-Incidents abrufen

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximalen Risikopunktzahlen von Security Incidents zum Zeitpunkt der Berechnung.

Max. Risikopunktzahl für Fehlkonfigurations-Testergebnisse abrufen

Dieser Indikator wird täglich berechnet. Berücksichtigt die maximalen Risikopunktzahlen für Fehlkonfiguration von Testergebnissen zum Zeitpunkt der Berechnung.

Durchschn. Risikopunktzahl für Fehlkonfigurationstestergebnisse abrufen

Dieser Indikator wird täglich berechnet. Berücksichtigt die durchschnittlichen Risikopunktzahlen für Fehlkonfiguration von Testergebnissen zum Zeitpunkt der Berechnung.

Anzahl der offenen Security Incidents

Dieser Indikator wird täglich berechnet. Berücksichtigt offene Security Incidents zum Zeitpunkt der Berechnung.

Phishing-Übersicht

Dieser Indikator wird täglich berechnet. Berücksichtigt die Anzahl der Sicherheitssimulationsmetriken zum Zeitpunkt der Berechnung.

Aggregierte MTTR

Berechnet die durchschnittliche Zeit zum Schließen von Schwachstellen (Hosts, Container und Anwendungen) und die Zeit zum Schließen der Testergebnisse in Tagen. [[Host-SLA – Geschlossen]] + [[Anwendungs-SLA – Geschlossen]] + [[Container-SLA – Geschlossen]] + [[Testergebnis-SLA – Bestanden]]) / ([[Host-SLA – Anzahl geschlossener]] + [[Anwendungs-SLA – Anzahl geschlossener]] + [[Testergebnis-SLA – Anzahl bestanden]] + [[Container-SLA – Anzahl geschlossener])

Aktuelle Scan-Abdeckung

Berechnet den Prozentsatz anhand des Verhältnisses zwischen der Anzahl der gescannten Elemente und der Gesamtzahl der Elemente, die während desselben Zeitraums für das Scannen in Frage kommen. VAR scannedItems =[[gescannte Assets]];VAR scannableItems = [[scannbare Assets]];VAR res;if (scannedItems == 0)res = 0;elseres = scannedItems / scannableItems * 100;if (res > 100)res = 100;res;

Durchschnittliches Alter aktiver angreifbarer Elemente

Berechnet das durchschnittliche Alter aller aktiven angreifbaren Elemente (Hosts, Container und Anwendungen) in Tagen. ([[summiertes Alter der angreifbaren Elemente]] + [[summiertes Alter der angreifbaren Anwendungselemente]] + [[summiertes Alter der angreifbaren Container-Elemente]]) / ([[angreifbare Elemente]] + [[angreifbare Anwendungselemente]] + [[angreifbare Container-Elemente]])

Aktive Vits nach Alter und Risikobewertung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechnet die Gesamtanzahl aller aktiven angreifbaren Elemente (Hosts, Container und Anwendungen), kategorisiert nach Alter und Risikobewertungsgrad. [[Offene Angreifbare Elemente]] + [[Offene Angreifbare Container-Elemente]] + [[Offene Angreifbare Anwendungselemente]]

Zurückgestellte Probleme

Berechnet die Gesamtanzahl aller angreifbaren Elemente (Hosts, Container, Anwendungen und Testergebnisse) mit dem Status „zurückgestellt“. [[zurückgestellte Vits]] + [[zurückgestellte AVITs]] + [[zurückgestellte Testergebnisse]] + [[zurückgestellte CVITs]]

Durchschnittliche Lösungszeit der geschlossenen Security Incidents

Berechnet die durchschnittliche Zeit, die zum Schließen der Security Incidents in Tagen benötigt wird. ([[summierte Dauer geschlossener Security Incidents]] / [[Anzahl geschlossener Security Incidents]]) /24

Sicherheitspunktzahl

Berechnet täglich die allgemeinen Sicherheitsbewertungen. Sie wird basierend auf der Rollup-Risikopunktzahl berechnet. VAR secPostureRating = 100 - [[Sicherheitspunktzahl]]; secPostureRating;

Sicherheitspunktzahl (Geschäftsbereiche)

Berechnet die endgültige Rollup-Risikopunktzahl, bei der die Rollup-Risikopunktzahl von angreifbaren Elementen, Fehlkonfigurationen, Security Incidents und schwerwiegenden Security Incidents mit den jeweiligen Gewichtungen multipliziert wird, die aus der Rollup-Tabelle für die Sicherheitslage abgerufen werden. VAR – schwerwiegende Incidents = [[Anzahl offener schwerwiegender Security Incidents]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0) majorSIRiskScore = 100; else majorSIRiskScore = 0; rollUpRiskScore = ([[Rollup-Risikopunktzahl für Schwachstellen und Fehlkonfiguration]] * 20 + [[OT-Schwachstellen-Risikopunktzahl für Rollup-40 Score]]] RisCore + 100]]

Sicherheitspunktzahl (Business-Services)

Berechnet die endgültige Rollup-Risikopunktzahl, bei der die Rollup-Risikopunktzahl von angreifbaren Elementen, Fehlkonfigurationen, Security Incidents und schwerwiegenden Security Incidents mit den jeweiligen Gewichtungen multipliziert wird, die aus der Rollup-Tabelle für die Sicherheitslage abgerufen werden. VAR MajorIncidents = [[Anzahl offener schwerwiegender Security Incidents – Services]], majorSIRiskScore, rollUpRiskScore; if(numMajorIncidents > 0) majorSIRiskScore = 100; else majorSIRiskScore = 0; rollUpRiskScore = ([[Rollup-Risikopunktzahl für Schwachstellen und Fehlkonfiguration – Services] * 20 + [[OT-Schwachstellen-100 Score-Risikopunktzahl für Rollup-Score] * 20] * 40]

Schwachstellen-Rollup-Risikopunktzahl

Berechnet die Rollup-Risikopunktzahl für Schwachstellen, wobei die maximale Risikopunktzahl, die durchschnittliche Risikopunktzahl angreifbarer Elemente und die Anzahl der angreifbaren Elemente mit ihren jeweiligen Gewichtungen multipliziert werden. VAR maxRiskScore = 100; VAR-Anzahl = [[aktive Vits nach Alter und Risikobewertung]]; VAR-CountRiskScore; if (0 == count) CountRiskScore = 0; else if (count > 10000) CountRiskScore = maxRiskScore 0,60; else if (count > 1000) CountRiskScore = (maxRiskScore 0,40 * 0,80) 0,20; else if (count > 100) VAR vulRiskScore = ([[Max. Punktzahl aus allen angreifbaren Elementen abrufen]] * 0 + [[Durchschnittliche Risikopunktzahl aller angreifbaren Elemente]] * 100 + CountRiskScore * 0)/100; vulRiskScore;

Maximale Risikopunktzahl von allen angreifbaren Elementen abrufen

Berechnet die Rollup-Risikopunktzahl für Schwachstellen, wobei die maximale Risikopunktzahl, die durchschnittliche Risikopunktzahl angreifbarer Elemente und die Anzahl der angreifbaren Elemente mit ihren jeweiligen Gewichtungen multipliziert werden. VAR = [[Max. Risikopunktzahl für angreifbare Anwendungselemente abrufen], maxScoreForCVI = [[Max. Risikopunktzahl für angreifbares Container-Element abrufen], maxScoreForAVI = [[Max. Risikopunktzahl für angreifbare Anwendungselemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

abrufen]], maxScore; if (maxScoreForVI >= maxScoreForCVI &&&& maxScoreForVI >= maxScoreForAVI) ScoreForAVI) ScoreScoreScoreScoreScoreScoreForAVI) ScoreScoreScoreScoreScoreScoreScoreScoreScoreScoreScore = Score = Score = SmaxForxFormaxForxForxFormaxForAVI; Score>

Durchschnittliche Risikopunktzahlen aller angreifbaren Elemente

Berechnet die durchschnittliche Risikopunktzahl aus allen angreifbaren Elementen (Hosts, Container und Anwendungen). VAR summedRiskScore = [[summierte Risikopunktzahl von Vits]] + [[summierte Risikopunktzahl von Avis]] + [[summierte Risikopunktzahl von CVIS]], avgRiskScore; var totalVulCount = [[offene angreifbare Elemente]] + [[offene angreifbare Anwendungselemente]]] + [[offene angreifbare Container-Elemente]]]]]]; if(summedRiskScore == 0) VulgRiscore = 0; Anzahl = 0; VulgRiscore = 0; VulgRiscore = 0

Fehlkonfiguration – Rollup-Risikopunktzahl

Berechnet die Rollup-Risikopunktzahl für Fehlkonfigurationen anhand der Testergebnisse, die als Fehlgeschlagen, Fehler oder Unbekannt kategorisiert sind. VAR maxRiskScore = 100; VAR-Anzahl = [[offene Konfigurationsprobleme – Testergebnisse]; VAR CountRiskScore; if (0 == count) CountRiskScore = 0; else if (count > 10000) CountRiskScore = maxRiskScore 0,40; else if (count > 1000) CountRiskScore = (maxRiskScore * 0,80) 0,20; else if (count > 100); else if (count > 0,60) VAR misRiskScore = ([[Max. Risikopunktzahl für Fehlkonfigurationstestergebnisse abrufen]] * 0 + [[Durchschn. Risikopunktzahl für Fehlkonfigurationstestergebnisse abrufen]] * 100 + CountRiskScore * 0)/100; misRiskScore;

Durchschnittliche Zeit bis Beseitigung

Berechnet die durchschnittliche Zeit bis zur Beseitigung von Security Incidents in Tagen [[SI – Durchschnittliche Dauer > Security Incident-Status = Beseitigung]] / 1440

Durchschnittliche Zeit für Identifizierung

Berechnet die durchschnittliche Zeit, die zur Identifizierung von Security Incidents in Tagen benötigt wird. [[SI – Durchschnittliche Zeit bis zur Identifizierung]] / 1440

Durchschnittliche Zeit bis zur Eindämmung

Berechnet die durchschnittliche Zeit, die zur Eindämmung von Security Incidents in Tagen benötigt wird. [[SI – Durchschnittliche Dauer > Status des Security Incidents = Einhalten]] / 1440

Einhaltung des Korrekturziels

Berechnet den monatlichen Prozentsatz der Einhaltung des Korrekturziels aus Testergebnissen, angreifbaren Elementen, angreifbaren Containerelementen und angreifbaren Anwendungselementen. Die Zieleinhaltung wird durch die Anzahl der Elemente bestimmt, die das festgelegte Ziel erfüllt haben. ([[Testergebnis-SLA – Anzahl bestanden > Korrekturstatus (einheitlich) = Ziel erfüllt]] + [[Container-SLA – Anzahl geschlossen > Korrekturstatus (einheitlich) = Ziel erfüllt]] + [[Anwendungs-SLA – Anzahl geschlossener SLA > Korrekturstatus (einheitlich) = Ziel erfüllt]] + [[Host-SLA – Anzahl geschlossener SLA > Korrekturstatus (einheitlich) = Ziel erfüllt]]) / ([[Test-SLA – Anzahl geschlossener SLA – Anzahl] + [[Anzahl geschlossener SLA – Anzahl] + [[Anzahl geschlossener Anwendungen] + [[Anzahl geschlossener SLA – Anzahl] + [] 100]

Effizienz der monatlichen Fehlerbehebung (alle angreifbaren Elemente)

Berechnet den monatlichen Prozentsatz geschlossener angreifbarer Elemente, angreifbarer Container-Elemente und angreifbarer Anwendungselemente im Gegensatz zu neu identifizierten Elementen. VAR closedItems = [[Host-SLA – Anzahl geschlossener Elemente]] + [[Container-SLA – Anzahl geschlossener Elemente]] + [[Anwendungs-SLA – Anzahl geschlossener Elemente]] + [[Testergebnis-SLA – Anzahl bestanden]];

VAR newItems = [[Host-Vits, die gestern geöffnet/erneut geöffnet wurden]] + [[Container-Vits, die gestern geöffnet/erneut geöffnet wurden]] + [[Anwendungs-Vits, die gestern geöffnet/erneut geöffnet wurden]] + [[Testergebnisse, die gestern geöffnet/erneut geöffnet wurden]];

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VAR res = 0;if (closedItems == 0) re = 0;Else if (newItems .=0)re = closedItems / newItems * 100;if (res > 1000) re = 1000; re;

Host-VITs, die gestern geöffnet/erneut geöffnet wurden

Dieser Indikator wird täglich berechnet. Berücksichtigt die angreifbaren Host-Elemente, die zuletzt am Vortag zum Zeitpunkt der Berechnung geöffnet wurden.

Anwendungs-VITs, die gestern geöffnet/erneut geöffnet wurden

Dieser Indikator wird täglich berechnet. Berücksichtigt die angreifbaren Anwendungselemente, die zuletzt am Vortag zum Zeitpunkt der Berechnung geöffnet wurden.

Container-VITs, die gestern geöffnet/erneut geöffnet wurden

Dieser Indikator wird täglich berechnet. Berücksichtigt die angreifbaren Container-Elemente, die zuletzt am Vortag zum Zeitpunkt der Berechnung geöffnet wurden.

Testergebnisse, die gestern geöffnet/erneut geöffnet wurden

Dieser Indikator wird täglich berechnet. Berücksichtigt die Testergebnisse, die zuletzt am Vortag zum Zeitpunkt der Berechnung angezeigt wurden.

Angreifbare OT-Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt aktive angreifbare OT-Elemente, die zum Zeitpunkt der Berechnung vorhanden sind.

Summierte OT-Dauer der geschlossenen angreifbaren Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt das Gesamtalter aller OT-Schwachstellen, die am Tag der Berechnung geschlossen wurden.

Geschlossene angreifbare OT-Elemente

Dieser Indikator wird täglich berechnet. Berücksichtigt die angreifbaren OT-Elemente, die am Tag der Berechnung geschlossen wurden.

Durchschnittliches Alter der aktiven angreifbaren OT-Elemente

Berechnet das durchschnittliche Alter der angreifbaren OT-Elemente ([[summiertes Alter der angreifbaren OT-Elemente]] / [[angreifbare OT-Elemente]])

Aufgliederungen

- Geschäftsbereich
- Business-Services
- Risikobewertung
- Altersbereich
- Zuweisungsgruppe (einheitlich)
- Nachbesserungszielstatus (geschlossen)
- Assetklasse
- Asset-Kategorie
- Risikobewertung (einheitlich)
- Grund für Zurückstellung (einheitlich)
- Status des Security Incidents
- Priorität von Security Incident
- Kategorie von Security Incident

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Phishing-Ereignis
- Grund für Zurückstellung nicht geschlossen (einheitlich)

Zu aktivierende Anwendungen

Sie müssen die folgenden Anwendungen aktivieren, um die Punktzahl in den Widgets auszufüllen. Basierend auf der von Ihnen verwendeten Anwendung müssen Sie die abhängigen Anwendungen aktivieren.

Wenn Sie verwenden	Aktivieren
Vulnerability Response	• Performance Analytics for Vulnerability Response • Gemeinsame Vulnerability Response-Komponenten • Vulnerability Response • Vulnerability Response und Konfigurations-Compliance für Container • Konfigurations-Compliance
Operative Technologien	Vulnerability Response für operative Technologie
Phishing-Integrationen	• Integration von Sicherheitssimulationen und -Schulungen für SecOps • KnowBe4-Integration für SecOps • Microsoft Defender for Office365 Integration für SecOps
Security Incident Response	• Performance Analytics für Security Incident Response • Security Incident Response • Management schwerwiegender Sicherheits-Incidents
Governance, Risk und Compliance	• GRC: Allgemeine Dashboard-Elemente • GRC: Risikomanagement-Arbeitsbereich • GRC: Erweitertes Risikomanagement • GRC: Compliance-Management-Arbeitsbereich

Geplante Aufgaben für die Datensammlung

Die folgenden geplanten Aufgaben werden ausgeführt, um Punktzahlen für neue Daten automatisch zu erfassen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Häufigkeit	Beschreibung
Benchmark-Punktzahlen hochladen	Bei Bedarf	Sammelt Punktzahlen aus der Instanz und postet in der zentralen Instanz. Die Benchmark-Algorithmen berechnen die besten Punktzahlen der Branche.
Benchmark-Punktzahlen herunterladen	Bei Bedarf	Lädt die Benchmark-Punktzahlen herunter. Sie ist in der Tabelle Benchmark-Punktzahlen [sn_bm_Client_Score_list] verfügbar.

Aktivieren Sie Benchmark-Punktzahlen

Rufen Sie Benchmark-Punktzahlen ab, indem Sie Ihre Instanz bei registrieren ServiceNow Zentrale Instanz. Letzteres verwaltet Informationen mehrerer Branchen, um die Benchmark-Punktzahl bereitzustellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Benchmarking finden Sie unter Exploring Benchmarks .

Prozedur

1. Führen Sie die folgenden Schritte aus, um Ihre Instanz bei der zentralen Instanz zu registrieren:
   a. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**an.
   b. Wählen Sie Aus *`sn_bm_client.central_instance_url`*Systemeigenschaft.
   c. In **Wert** Geben Sie die URL der zentralen Benchmark-Instanz ein.

      Hinweis:
      Wenn die Instanz bereitgestellt wird, werden Ihre Details automatisch an die zentrale Instanz übertragen.

   d. Wählen Sie Aus **Aktivieren** Aus dem Widget, um eine Verbindung mit der zentralen Instanz zu validieren und herzustellen.
2. Führen Sie die folgenden Schritte aus, um Ihre Punktzahl in die zentrale Instanz hochzuladen:
   a. Navigieren zu **Alle** > **Systemzeitplaner** > **Geplante Aufgaben**
   b. Wählen Sie aus *`Upload the benchmark scores`*Geplante Aufgabe.
   c. Wählen Sie **Aktualisieren**.
      Die Punktzahlen werden in die zentrale Instanz hochgeladen. Die geplanten Aufgaben der zentralen Instanz werden jedoch einmal im Monat ausgeführt, um die Punktzahlen in den Dashboard-Widgets zu aktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Um die Punktzahl aus der zentralen Instanz herunterzuladen, gehen Sie wie folgt vor:

   a. Navigieren zu **Alle** > **Systemzeitplaner** > **Geplante Aufgaben**

   b. Wählen Sie aus `Download the benchmark scores`Geplante Aufgabe.

   c. Wählen Sie **Jetzt ausführen**.
   Die Punktzahlen sind in der Tabelle „Benchmark-Punktzahlen“ [sn_bm_Client_Score_list] verfügbar, die in den Dashboard-Widgets angezeigt wird.

Legen Sie Ziele fest

Legen Sie Ziele in Tagen fest, um zu definieren, wie schnell Schwachstellen, Security Incidents und Konfigurationsfehler behoben werden sollen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Wählen Sie Aus **Ziele** Wählen Sie im Widget aus, oder wählen Sie aus **Ziele** Symbol auf der Seite „KPI-Details“.
2. Wählen Sie aus **Für alle** Schaltfläche.
3. In **Neuer Wert** Geben Sie die Anzahl der Tage ein, in denen Sie das Ziel erreichen möchten.
4. Wählen Sie das Zielstartdatum aus.
5. Wählen Sie das Zielüberprüfungsdatum aus.
6. Wählen Sie **Aktualisieren**.

Integration von Sicherheitssimulationen und -Schulungen für Security Operations

Stärken Sie die Abwehr Ihrer Organisation vor prominenten Cybersicherheitsbedrohungen, indem Sie Phishing-Integrationen in das Cybersecurity Executive Dashboard integrieren. Die Phishing-Integrationen verbessern das Cybersicherheits-Dashboard, indem Daten aus Phishing-Simulationstools von Drittanbietern wie KnowBe4 und Microsoft Defender for Office 365 nahtlos integriert werden.

Die folgenden Integrationen verbessern die Fähigkeiten des Cybersicherheits-Executive-Dashboards und bieten einen einheitlichen Überblick über die Sicherheitslage Ihrer Organisation, die Bereitschaft der Mitarbeiter und die Anfälligkeit für Phishing-Angriffe:

- KnowBe4-Integration
- Integration von Microsoft Defender for Office 365

Konfigurieren Sie die Knowbe4-Integration

Erhalten Sie durch die Integration mit KnowBe4, einer führenden Trainingsplattform für Cybersicherheitsbewusstsein, sofortige Einblicke in die Schwachstelle Ihrer Mitarbeiter gegenüber Phishing-Angriffen. Identifizieren Sie durch die KnowBe4-Integration Trends und Verbesserungsbereiche in Ihren Cybersicherheits-Schulungsprogrammen, überwachen Sie die allgemeine Phishing-Resilienz und stärken Sie proaktiv die Sicherheitsmaßnahmen Ihrer Organisation.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_phish.admin und sn_sec_phish_kb4.kb4_admin

Prozedur

1. Navigieren zu **Alle** > **KnowBe4-Integration** > **KnowBe4-Konfigurationen**an.
2. Wählen Sie **Neu**.
3. Geben Sie im Formular die Details ein:

Formular „KnowBe4-Konfiguration“

Feld	Beschreibung
Integrationsinstanz	Name der Integrationsinstanz. Wählen Sie die Integrationsinstanz über das Suchsymbol aus.
Basis-URL	URL zur Integration mit KnowBe4.
API-Schlüssel	API-Schlüssel, der vom KnowBe4-Account erworben wurde.
Seite	Seitenzahl, von der Simulationen abgerufen werden sollen.
Seitengröße	Anzahl der Simulationen, die einbezogen werden sollen.

   a. Wählen Sie Aus **Neu** Wenn keine Integrationsinstanz verfügbar ist.

   b. Geben Sie im Formular die Details ein:

Formular „Integrationsinstanz“

Feld	Beschreibung
Name	Name für die Integrationsinstanz.
Anwendung	Name der Anwendung (KnowBe4-Integration für SecOps).
Integration	KnowBe4 ist der Standard.
Aktiv	Standard ist aktiviert (ausgewählt). Wenn diese Option deaktiviert ist, ist die Instanz nicht aktiv.
Beschreibung	Kurzbeschreibung der Integrationsinstanz.

4. Wählen Sie **Absenden**.
5. Navigieren zu **Alle** > **Sicherheitssimulation und -training** > **Integrationen**an.
6. Wählen Sie Knowbe4-Integration aus.
7. Wählen Sie Aus **Jetzt Ausführen** Zum Ausführen und Erfassen von Daten aus KnowBe4.

Konfigurieren Sie die Integration von Microsoft Defender for Office 365

Erhalten Sie durch die nahtlose Integration mit Microsoft Defender for Office 365 wertvolle Einblicke in Phishing-Simulationsmetriken direkt im Cybersicherheits-Dashboard.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_phish_msatk.ms_admin

Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen zum Simulieren eines Phishing-Angriffs und zum Einrichten eines Mandanten finden Sie unter:

- Simulieren Sie einen Phishing-Angriff mit dem Angriffssimulationstraining
- Erste Schritte mit dem Angriffssimulationstraining
- Richten Sie einen Mandanten ein

Prozedur
1. Navigieren zu **Alle** > **Microsoft Attack-Integration** > **Microsoft Attack-Konfigurationen**an.
2. Wählen Sie **Neu**.
3. Geben Sie im Formular die Details ein:

Formular „Microsoft Attack Configuration“

Feld	Beschreibung
Integrationsinstanz	Name der Integrationsinstanz. Wählen Sie die Integrationsinstanz über das Suchsymbol aus.
Mandanten-ID	Mandanten-ID der Anwendung, die im Microsoft Azure-Portal erstellt wurde.
Client-ID	Client-ID der Anwendung, die im Microsoft Azure-Portal erstellt wurde.
Geheimer Clientschlüssel	Geheimer Clientschlüssel der Anwendung, die im Microsoft Azure-Portal erstellt wurde.
Lesezeichen	Datum, ab dem die Simulationen abgerufen werden müssen.
Token-URL	Basis-URL, von der aus das Token erstellt wird, um auf die Microsoft Simulations-API zuzugreifen.
Gesamte Simulations-URL	Basis-URL der Microsoft Simulations-API.

   a. Wählen Sie Aus **Neu** Wenn keine Integrationsinstanz verfügbar ist.

   b. Geben Sie im Formular die Details ein:

Formular „Integrationsinstanz“

Feld	Beschreibung
Name	Name der Integrationsinstanz.
Anwendung	Name der Anwendung (Microsoft Defender for Office 365).
Integration	Referenz für Drittpartei-Integration (Microsoft Attack Integration).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Standard ist aktiviert (ausgewählt). Wenn diese Option deaktiviert ist, ist die Instanz nicht aktiv.
Beschreibung	Kurzbeschreibung der Integrationsinstanz.

4. Wählen Sie **Absenden**.
5. Navigieren zu **Alle** > **Sicherheitssimulation und -training** > **Integrationen**an.
6. Wählen Sie Microsoft Attack Integration aus.
7. Wählen Sie Aus **Jetzt Ausführen** Zum Ausführen und Erfassen von Daten von Microsoft.

Risiko- und Compliance-Dashboard für GRC: Metrics

Das Risiko- und Compliance-Dashboard bietet Compliance- und Risiko-Anwendern einen umfassenden Überblick über Risiko- und Compliance-Informationen in einem einzigen Dashboard, das bei wichtigen Entscheidungen hilft.

Sie können über eine zentrale Konsole zum Risiko- und Compliance-Dashboard navigieren Cybersicherheits-Dashboard Dient zum Anzeigen der Risiko- und Compliance-Metriken von Governance, Risk und Compliance Anwendungen.

Das Dashboard bietet Funktionen wie:

- Compliance-Übersicht
- Risikoübersicht
- Datenschutzübersicht
- Geschäftskontinuitätsübersicht
- Drittpartei-Risiko
- Audit-Übersicht

Voraussetzungen für den Zugriff auf das Risiko- und Compliance-Dashboard

Wichtig:
Sie müssen primären Zugriff auf haben Cybersicherheits-Dashboard Zum Aktivieren des funktionalen Plugins Cybersicherheit und Risiko, mit dem Sie auf das Risiko- und Compliance-Dashboard zugreifen können.

Eine neue funktionale Domäne wird eingeführt, um Cybersicherheits- und risikobezogene Daten zu trennen. Sie können das Plugin „Cybersicherheit und Risiko“ aktivieren, indem Sie auswählen **Aktivieren** UI-Aktionsschaltfläche. Standardmäßig ist diese funktionale Domäne inaktiv.

Erforderliche ServiceNow AI Platform-Rollen

Die Hauptansicht GRC Die Anwenderrolle ist sn_grc_dashboards.grc_ciso_user, die die Berichte im Risiko- und Compliance-Dashboard anzeigen kann. Diese Rolle enthält:

- sn_Compliance.Reader
- sn_risk.reader

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie müssen jedoch über die Rolle sn_Bod.ciso verfügen, um sich anzumelden, das Cybersicherheits-Führungskräfte-Dashboard anzuzeigen und freizugeben, von dem aus Sie zum Risiko- und Compliance-Dashboard navigieren können.

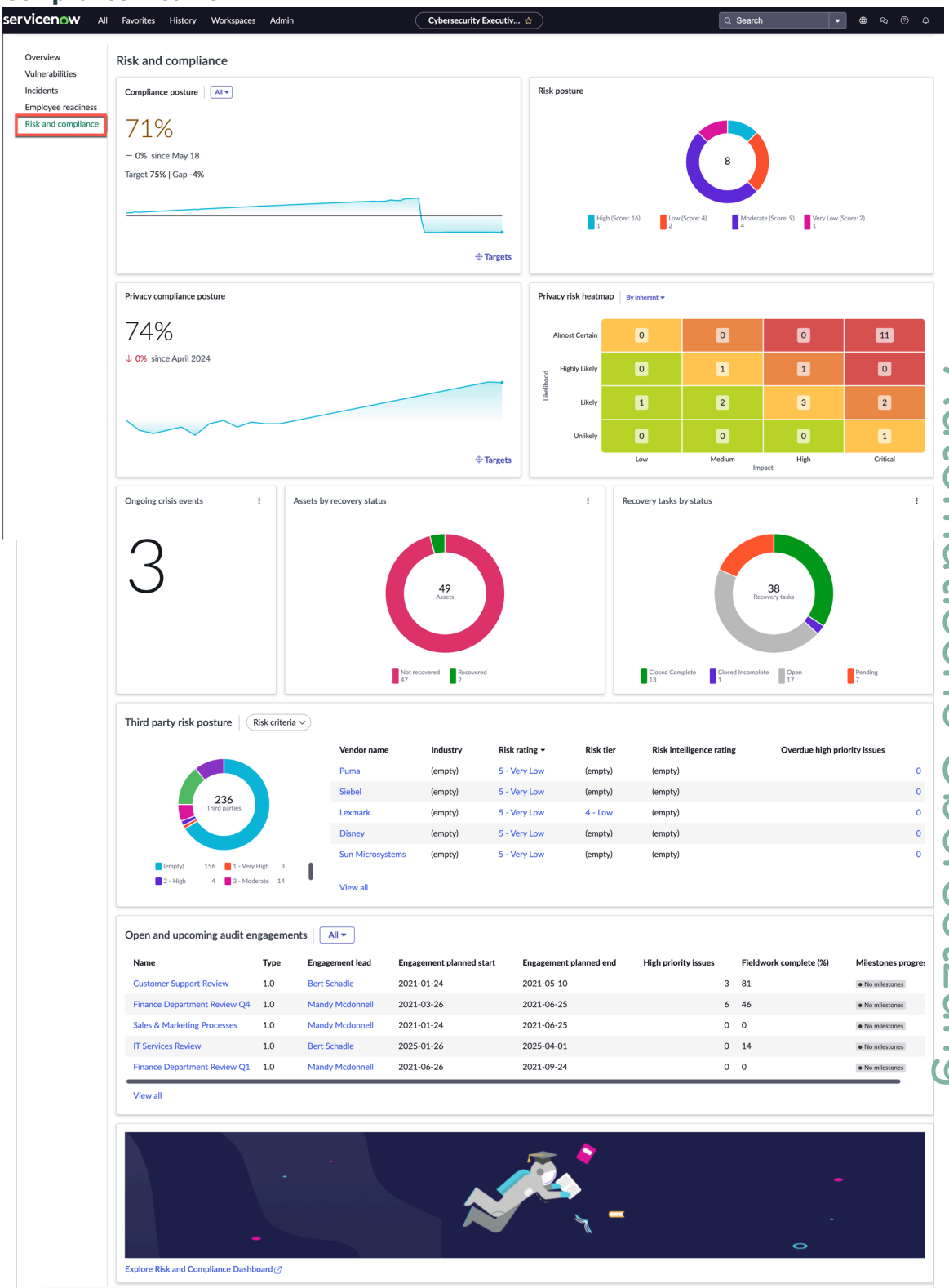
Greifen Sie auf das Risiko- und Compliance-Dashboard zu

1. Um auf das Dashboard „Risiko und Compliance“ zuzugreifen, navigieren Sie zu **Alle** > **Cybersicherheits-Dashboard** > **Cybersicherheits-Dashboard**an.
2. Wählen Sie Aus **Risiko und Compliance** Bezeichnung aus der Liste auf der linken Seite des Dashboards.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einheitliches Dashboard für Cybersicherheits-Führungskräfte für Risiko- und Compliance-Metriken



Automatische Übersetzung

3. Um Ihre Daten zu visualisieren und die Berichte und Lösungen anzuzeigen, die im für den Anwender konzipierten Dashboard verfügbar sind, wählen Sie aus Bezeichnung für „Risiko- und Compliance-Dashboard erkunden“ .

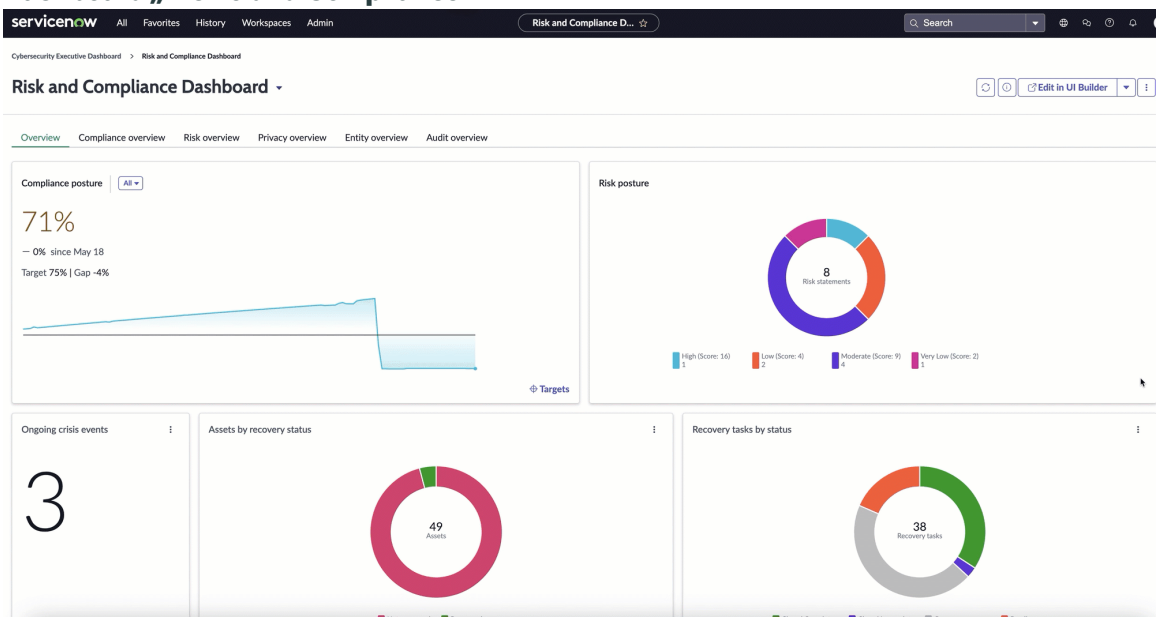
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Risiko und Compliance Dashboard-Berichte und -Lösungen

Das Risiko- und Compliance-Dashboard ist ein einheitliches Dashboard, das umfassende analytische Daten zu Berichten bietet, die aus den wichtigsten GRC-Anwendungen verfügbar sind, damit der Chief Information Security Officer die Compliance- und Risikosituation der Organisation versteht. Das -Dashboard konsolidiert Daten aus verschiedenen Produkten innerhalb von ServiceNow GRC suite von Anwendungen.

Hinweis:
Alle Berichte sind nur verfügbar, wenn die entsprechenden Arbeitsbereiche installiert sind.

Dashboard „Risiko und Compliance“



Erforderliche ServiceNow AI Platform-Rollen

Für Compliance-bezogene Berichte

Der Anwender muss über die Rolle „sn_grc_dashboards.grc_ciso_user und die Rolle „sn_bod.ciso“ verfügen.

Für risikobezogene Berichte

Der Anwender muss über die Rolle „sn_grc_dashboards.grc_ciso_user und die Rolle „sn_bod.ciso“ verfügen.

Für Berichte im Zusammenhang mit Geschäftskontinuitätsmanagement

Anwender muss die Rolle „sn_bcm.Viewer“ und „sn_Bod.ciso“ haben.

Für risikobezogene Berichte von Drittparteien

Anwender muss die Rolle sn_vdr_Risk_asmt.Vendor_assessment_Reviewer und sn_Bod.ciso haben.

Für datenschutzbezogene Berichte

Der Anwender muss über die Rolle „sn_privacy.Analyst“ und „sn_bod.ciso“ verfügen.

Für Audit-bezogene Berichte

Der Anwender muss über die Rolle „sn_audit_ws.auditor und die Rolle „sn_bod.ciso“ verfügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Greifen Sie auf das Risiko- und Compliance-Dashboard zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Cybersicherheits-Dashboard** > **Cybersicherheits-Dashboard**an.

Indikatoren

Compliance-Situation

- Compliance-Prozentsatz: Formelindikator, der die Compliance-Situation darstellt.
- Alle Steuerungen: Automatisierter Indikator, der den Formelindikator unterstützt.
- Konforme Steuerungen: Automatisierter Indikator, der den Formelindikator unterstützt.

Compliance-Situation für Datenschutz

PA-Indikator: Prozentsatz der Compliance-Punktzahl der Verarbeitungsaktivität.

Aufgliederungen

Funktionale Domäne.

Berichte

Hinweis:
Alle Berichte sind nur verfügbar, wenn die entsprechenden Arbeitsbereiche installiert sind.

Registerkarte „Übersicht“

Titel	Typ	Quelltabelle	Beschreibung
Compliance-Situation	Liniendiagramm	Steuerung [sn_Compliance_Control]	Bietet Cybersicherheit und -Risiken sowie IT-Risiko und -Compliance basierend auf einer Datenanalyse für Compliance-Manager.
Risikosituation	Ringdiagramm	Die Quelltabellen lauten wie folgt: • Risiko [sn_risk_risk] • Detailliertes aggregiertes Risiko [sn_Risk_Advanced_Risk_assessment_result] (wenn Erweitertes Risikomanagement Die Anwendung ist installiert, und die erweiterte Risikobewertung ist aktiviert	Stellt die Risikoanzahl basierend auf den Risikobewertungen bereit.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Übersicht“ (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
Laufende Krisenereignisse	Einzelne Punktzahl	Wiederherstellungsereignis [sn_Recovery_event], bei dem der Ereignistyp „ist“ ist	Zeigt die Gesamtzahl der laufenden Krisenereignisse an, die weder genehmigt noch geschlossen wurden.
Assets nach Wiederherstellungsstatus	Ringdiagramm	Assets [sn_Recovery_event_Asset]	Stellt die Gesamtzahl der Assets für laufende Krisenereignisse gruppiert nach ihrem Wiederherstellungsstatus bereit, einschließlich wiederhergestellter und nicht hergestellter Assets.
Wiederherstellungsaufgaben nach Status	Ringdiagramm	Wiederherstellungsaufgaben [sn_Recovery_event_Task]	Stellt den Status von Wiederherstellungsaufgaben in verschiedenen status für laufende Krisenereignisse bereit.

Registerkarte „Compliance-Übersicht“

Titel	Typ	Quelltabelle	Beschreibung
Regulatorische Dokumente	Ringdiagramm	Regulatorisches Dokument [sn_Compliance_Authority_document]	Stellt Daten von konformen und nicht konformen regulatorischen Dokumenten im Diagramm bereit. Die Liste enthält Details zu den regulatorischen Dokumenten, ihre individuelle Compliance-Punktzahl in Prozent, die Anzahl der Probleme mit hoher Priorität und Ausnahmen mit hohem Risiko in den regulatorischen Dokumenten sowie die Anzahl der konformen Fälle.
Richtlinien	Ringdiagramm	Richtlinie [sn_Compliance_Policy]	Gibt die Anzahl der konformen und nicht konformen Richtlinien im Diagramm an. Die Liste enthält Details zu den Richtlinien, ihre individuelle Compliance-Punktzahl in Prozent, die Anzahl der Probleme

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Compliance-Übersicht“ (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			mit hoher Priorität und Risikoausnahmen, die für jede Richtlinie ausgelöst wurden, sowie die Anzahl der konformen Fälle.

Registerkarte „Risikoübersicht“

Titel	Typ	Quelltabelle	Beschreibung
Risikosituation	Ringdiagramm	Die Quelltabellen lauten wie folgt: • Risiko [sn_risk_risk] • Detailliertes aggregiertes Risiko [sn_Risk_Advanced_Risk_assessment_result] (wenn Erweitertes Risikomanagement Anwendung ist installiert, und erweiterte Risikobewertung ist aktiviert.)	Stellt die Risikoanzahl basierend auf den Risikobewertungen bereit.
Risikosituation	Liste	GRC-Inhaltsstatus [sn_grc_content_reports]	Stellt die Risikobewertung für jedes Organisationsrisiko bereit, um die Ergebnisse der Gesamtrisikobewertung zu verstehen. Diese Bewertungen helfen Unternehmen, die potenziellen Auswirkungen und die Wahrscheinlichkeit verschiedener Risiken zu verstehen, sodass sie diese Risiken priorisieren und verwalten können. Die Karte „Risikolage“ hebt auch die folgenden Informationen für jedes Risiko hervor: • **Risikobereitschaft** : Wert der Risikobereitschaft definiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Risikoübersicht“ (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			• **Probleme mit hoher Priorität** : Die Anzahl der Probleme mit Priorität ist als hoch definiert. • **Überfällige Risikoantwortaufgaben** : Anzahl der überfälligen Risikoantwortaufgaben. • **KRI-Verstoß %** : Prozentsatz der Key Risk Indicators (Kris), die ihre vordefinierten Schwellenwerte oder Grenzwerte überschritten haben.
Drittpartei-Risikosituation	Ringdiagramm	Drittparteirisiken [sn_grc_Dashboards_third_Party_Risk]	Stellt die Risikobewertung für jede Drittpartei bereit. Die Risikobewertung ist die Gesamtbewertungsbewertung, die die Punktzahlen und Bewertungen aller Bewertungen berücksichtigt, die für eine Drittpartei oder einen Lieferanten durchgeführt wurden. Die Drittpartei-Risikokarte hebt auch die folgenden Informationen für jede Drittpartei oder jeden Lieferanten hervor: • **Risikokriterien** : Gruppe von Risikodomänen (in anderen Plattformfunktionen manchmal als Risikobereiche bezeichnet), die für einen bestimmten Typ von Drittparteien gilt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Risikoübersicht“ (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			• **Risikostufe** : Wert, der basierend auf den Antworten bestimmt wird, die nach Abschluss einer Bewertung des inhärenten Risikos (IRQ) erfasst wurden. • **Risk Intelligence-Bewertung** : Aggregat aller Punktzahlen, die von Risk Intelligence-Anbietern erfasst wurden. • **Überfällige Risikoantwortaufgaben** : Anzahl der überfälligen Risikoantwortaufgaben.

Registerkarte „Datenschutzübersicht“

Titel	Typ	Quelltabelle	Beschreibung
Compliance-Situation für Datenschutz	Linie	PA-Indikator: Prozentsatz der Compliance-Punktzahl für Verarbeitungsaktivität [PA_indicators]	Stellt die Compliance-Situation nach Monat bereit und wird unter Bezugnahme auf die Compliance-Gesamtpunktzahl für alle Verarbeitungsaktivitäten dargestellt.
Überfällige Probleme hoher Priorität	Einzelne Punktzahl	Probleme [sn_grc_issue]	Bietet einen fokussierten Überblick über alle überfälligen datenschutzbezogenen Probleme mit hoher Priorität, sodass kritische Aufgaben schnell identifiziert und gelöst werden können, um Compliance und Datenschutz sicherzustellen.
Heatmap für Datenschutzrisiken	Heatmap	Risikobewertungsmethode [sn_Risk_Advanced_Risk_Assessment_method]	Stellt die Daten zur Datenschutzrisikobewertung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Datenschutzübersicht“ (Fortsetzung)

Titel	Typ	Quelltabelle	Beschreibung
			in Form einer Heatmap bereit. Datenschutzrisikobewertungen sind detaillierte Bewertungen, die durchgeführt werden, wenn die Kritikalitätspunktzahl hoch ist. Bewerten Sie jedes Risiko, das der Verarbeitungsaktivität zugeordnet ist, und kennen Sie die zusammengefasste Risikopunktzahl für die Verarbeitungsaktivität. Nachdem Sie die Datenschutzrisiken bewertet haben, können Sie die Situation des Datenschutzrisikos auf der Risiko-Heatmap anzeigen.

Registerkarte „Entitätsübersicht“

Titel	Typ	Quelltabelle	Beschreibung
Entitäten	Liste	Entitäts-Compliance-Status [sn_Compliance_Entities_report]	Stellt die Zusammenfassung der Risiken bereit, die direkt mit der Entität verknüpft sind und zur Gesamtrisikobewertung der Entität beitragen. Die Liste zeigt auch die Compliance-Punktzahl von Entitäten sowie Probleme und Risikoausnahmen mit hoher Priorität an, die aufgrund der nicht konformen Steuerungen ausgelöst werden, die der Entität zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Audit-Übersicht“

Titel	Typ	Quelltabelle	Beschreibung
Offene und bevorstehende Audit-Interaktionen	Liste	Interaktion [sn_Audit_Engagement]	Stellt eine Liste offener und bevorstehender Audit-Interaktionen bereit. Die Liste enthält auch Details zum Interaktionsleiter für jedes regulatorische Dokument, die geplanten Start- und Enddaten jeder Interaktion, Probleme mit hoher Priorität, den Prozentsatz der abgeschlossenen Feldarbeit und die in Bearbeitung befindlichen Meilensteine.

Filter

Name	Typ	Beschreibung
Risikokriterium	Bericht	Je nachdem, welche Risikokriterien Sie auswählen, werden im Ringdiagramm und in der Liste die Drittparteien oder Lieferanten angezeigt, die sich in diesen Risikobereichen befinden.

Threat Intelligence-Sicherheitszentrum

Die Threat Intelligence-Sicherheitszentrum(TISC) Die Plattform bietet eine Technologielösung für die Zusammenfassung, Verwaltung und Operationalisierung von Threat Intelligence.

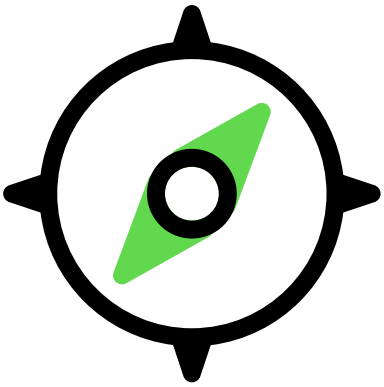
Erste Schritte

Klicken Sie auf eine Kachel, um zu beginnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

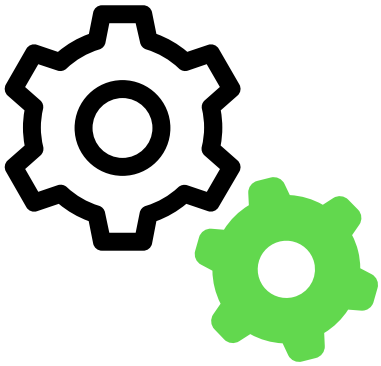
Automatische Übersetzung

Untersuchen



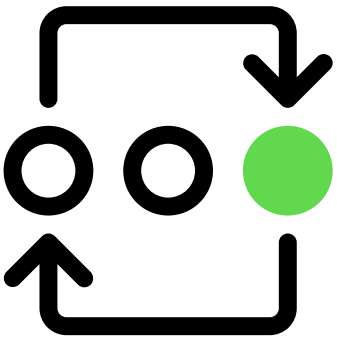
Erfahren Sie, wie das Threat Intelligence-Sicherheitszentrum Ihnen mit seinen wichtigsten Funktionen und Vorteilen helfen kann.

Konfigurieren



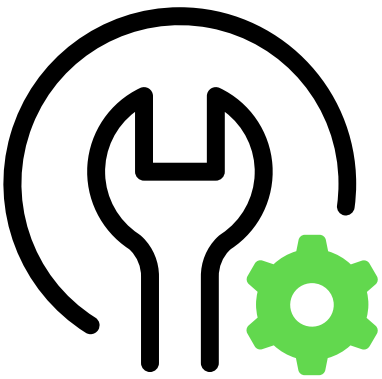
Richten Sie das Threat Intelligence Security Center ein, und konfigurieren Sie es entsprechend Ihren spezifischen Anforderungen.

Integrieren



Integration mit Threat Intelligence Security Center

Verwalten



Verwalten und passen Sie Ihr Threat Intelligence Security Center an.

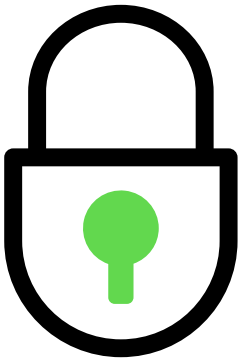
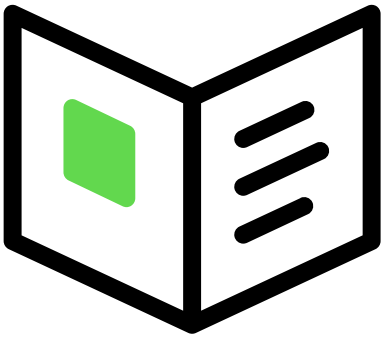
Verwenden

Verwalten Sie Ihre Threat Intelligence Security Center-Bibliothek und -Objekte.

Berichtsvorlagen

Verwalten und passen Sie Ihre Fallmanagementberichte an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MITRE ATT&CK-Repository	TISC Datenarchivierung Archivieren	Referenz
		
Verwalten Sie MITRE ATT&CK-Repository-Daten.	Verwalten Sie Datenarchivierungs- und Vernichtungsregeln.	Rufen Sie zusätzliche Informationen zum Threat Intelligence-Sicherheitszentrum ab.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Wird Installiert Threat Intelligence-Sicherheitszentrum(sn_sec_tisc) installiert automatisch alle abhängigen Anwendungen von ServiceNow Store.

Weitere Ressourcen

Besuchen Sie Security Incident Response-forum auf der ServiceNow Community.

Problembehandlung und Hilfe

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Threat Intelligence-Sicherheitszentrum erkunden

Threat Intelligence-Sicherheitszentrum(TISC) Ermöglicht Ihnen die Zusammenarbeit mit den Threat Intelligence-Teams und verfügt über mehrere Fähigkeiten zum Sammeln und Verarbeiten verschiedener Threat Intelligence-Feeds sowie einen Arbeitsbereich zum Analysieren, Zusammenarbeiten, Aktionen und Freigeben der erforderlichen Informationen.

Sehen Sie sich einen Überblick über an Threat Intelligence-Sicherheitszentrum Anwendung.

https://player.vimeo.com/video/1020328039?h=33e58d6e14&badge=0&autopause=0&player_id=0&app_id=58479

Das Threat Intelligence-Sicherheitszentrum wird durch Funktionen zur Verwaltung der Datenerfassung, Datenverarbeitung wie DEDUPLIZIERUNG, Normalisierung und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusammenfassung, Analyse von Threat Intelligence, Verbreitung von Threat Intelligence und auch Arbeitsbereich erweitert, der Verwaltungsaufgaben bereitstellt.

Schlüsselfunktionen

Threat Intelligence-Sicherheitszentrum Bietet eine umfassende und robuste Suite von Funktionen, die zur Verbesserung der Threat Intelligence-Fähigkeiten für Sicherheitsteams entwickelt wurden:

- **Kuratierter Katalog von OSINT-Bedrohungsfeeds** : Bietet Zugriff auf eine breite Auswahl beliebter Open Source Threat Intelligence-Feeds, um eine breite Abdeckung sicherzustellen.
- **Premium-Feed-Integration** : Verbessert die Qualität von Threat Intelligence, indem Premium-Quellen neben OSINT-Daten integriert werden.
- **Automatisierte Extraktion Erkennbarer Elemente** : Identifiziert und extrahiert automatisch alle relevanten erkennbaren Elemente aus hochgeladenen Dateien, um die Datenerfassung zu optimieren.
- **Zusammenfassung Verschiedener Daten** : Unterstützt mehrere Datenformate, einschließlich STIX, MISP, JSON und andere, und ermöglicht eine nahtlose Feed-Konsolidierung.
- **Ergänzung Und Validierung** : Entfernt falsch positive Ergebnisse, weist Konfidenzpunktzahlen zu, validiert Indikatoren und fügt wertvolle kontextbezogene Informationen hinzu, um die Datenqualität zu verbessern.
- **Korrelationsregeln-Engine** : Stellt automatisch Beziehungen zwischen erkennbaren Elementen her, um tiefere Einblicke in Bedrohungsmuster zu ermöglichen.
- **Anpassbare Bedrohungsbewertung** : Ermöglicht die Feinabstimmung von Bedrohungspunktzahlen für eine nuanciertere und genauere Bedrohungsbewertung.
- **Integration Von Internal Intelligence** : Kombiniert externe Feeds mit internen Daten aus Vulnerability Reports (VR), Security Incident Response (SIR), Assets, Services und CMDB.
- **Anwenderspezifische Dashboards** : Passt Visualisierungen und Datenansichten an Threat Intelligence-Personas an, wodurch die Anwender-Experience und Relevanz verbessert werden.
- **Grafische Visualisierungstools** : Erleichtert das Verständnis komplexer Threat Intelligence-Daten durch intuitive grafische Darstellung.
- **Dedizierter Arbeitsbereich Für Analysten** : Stellt ein dediziertes, optimiertes bereit Threat Intelligence Arbeitsbereich für Analysten, mit dem Analysten von Threat Intelligence sich mit minimalen Ablenkungen auf Untersuchungen und Analysen konzentrieren können.
- **Bedrohungssuche mit Fallmanagement** : Unterstützt Untersuchungs-Workflows mit Aufgabenverfolgung und Fallbearbeitung.
- **MITRE ATT&CK-INTEGRATION** : Ermöglicht Anwendern das Verknüpfen von Falldatensätzen mit MITRE ATT&CK-Framework-Daten für eine erweiterte kontextbezogene Analyse.
- **Nahtlose SIR-Integration** : Stellt eine reibungslose Datenmigration und Interoperabilität zwischen sicher Threat Intelligence Und Security Incident Response-Anwendungen für Threat Intelligence-Sicherheitszentrum.
- **Benachrichtigungs- Und Warnungsregeln** : Richtet Auslöserwarnungen ein, um Teams basierend auf der Entwicklung von Threat Intelligence zu benachrichtigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Richtlinien Zur Datenaufbewahrung Und -Bereinigung** : Ermöglicht Organisationen das Definieren von Datenverwaltungsregeln, um die Leistung und Compliance von Anwendungen aufrechtzuerhalten.
- **Berichterstellung Und Zusammenarbeit** : Generiert umfassende Statusberichte und Untersuchungszusammenfassungen mit Rich-Text-Editoren und anpassbaren Vorlagen.
- **Domänentrennung für MSSPs** : Unterstützt Umgebungen mit mehreren Mandanten, sodass Managed Security Service Provider (MSSPs) Kundendaten sicher trennen können.
- **Umfassende API-Integration** : Bietet TISC-API für nahtlose Konnektivität mit anderen Sicherheitstools und -Plattformen.

TISC-Schlüsselterminologie

Die unten definierten Begriffe werden im Threat Intelligence Security Center (TISC) verwendet.

Terminologiedefinitionen

Terminologie	Definition
Datenverarbeitung	Eine Threat Intelligence Platform (TIP) ist eine Technologielösung, die Threat Intelligence-Daten aus verschiedenen Quellen und Mustern sammelt, aggregiert und organisiert. Threat Intelligence sind die Daten, die erfasst, verarbeitet und analysiert werden, um die Ziele und das Angriffsverhalten von Bedrohungsakteuren zu verstehen.
Erkennbare Elemente	Erkennbare Elemente stellen statusbehaftete Eigenschaften (z. B. den MD5-Hash einer Datei oder den Wert eines Registrierungsschlüssels) oder messbare Ereignisse (z. B. die Erstellung eines Registrierungsschlüssels oder das Löschen einer Datei) dar, die für den Betrieb von Computern und Netzwerken relevant sind. Weitere Informationen finden Sie unter Erkennbare Elemente.
Indikatoren	Indikatoren enthalten ein Muster, das verwendet werden kann, um verdächtige oder böswillige Cyberaktivitäten zu erkennen. Beispielsweise kann ein Indikator verwendet werden, um eine Reihe schädlicher Domänen darzustellen, und die STIX-Mustersprache zur Angabe dieser Domänen verwenden. Das Indikator-SDO enthält eine einfache Textbeschreibung, die Kill Chain-Phasen, in denen das Verhalten erkannt wird, ein Zeitfenster, in dem der Indikator gültig oder nützlich ist, und ein erforderliches **Muster** Eigenschaft zum Erfassen eines strukturierten Erkennungsmusters. Weitere Informationen finden Sie unter Indikatoren.
Objekte	Definiert den Satz von STIX-Domänenobjekten (SDOs), von denen jedes einem eindeutigen Konzept

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Terminologiedefinitionen (Fortsetzung)

Terminologie	Definition
	entspricht, das üblicherweise in Cyber Threat Intelligence (CTI) dargestellt wird. Mithilfe von SDOs und STIX-Beziehungsobjekten (SROs) als Bausteine können Einzelpersonen umfassende und umfassende Cyberbedrohungsinformationen erstellen und teilen. Weitere Informationen finden Sie unter TISC-Bibliotheks-Repository.
Beziehungen	Eine Beziehung ist eine Verknüpfung zwischen zwei erkennbaren Elementen oder zwei SDOs oder erkennbarem Element und SDO, die die Art und Weise beschreibt, in der die Objekte zusammenhängen. Beziehungen können mithilfe eines externen STIX-Beziehungsobjekts (SRO) oder in einigen Fällen durch bestimmte Eigenschaften dargestellt werden, die eine Bezeichnerreferenz speichern, die eine eingebettete Beziehung umfasst. Weitere Informationen finden Sie unter Beziehungsobjekte.

Anzeigen TISC Homepage

Verwenden Sie TISC Homepage, die die Zielseite ist, um die Daten im Zusammenhang mit Threat Intelligence zu visualisieren.

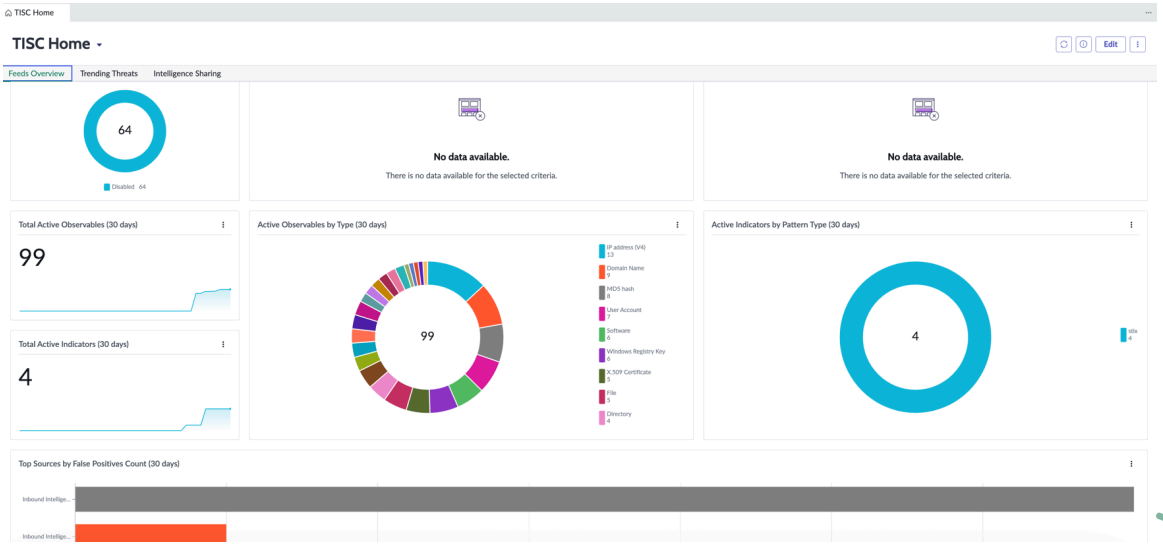
Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
   Die TISC Homepage wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Zeigen Sie an TISC Homepage mit verschiedenen Widgets-Daten.
Die Homepage-Ansicht besteht aus drei verschiedenen Registerkarten: **Feeds-Übersicht** , **Bedrohungen Im Trend** , Und **Intelligenzfreigabe** . Der Inhalt auf der Homepage stammt aus verschiedenen Quellen, z. B. erkennbare Elemente, Indikatoren und Daten-Feeds.

a. Feeds-Übersicht : Diese Registerkarte bietet eine allgemeine Übersicht über verschiedene Quellen, in denen die Daten erfasst werden, und Quellen, die für die Datenerfassung konfiguriert sind.

Feeds-Übersicht

Widget-Name	Beschreibung	Aktion
Anzahl der Quellen	Zeigt die Anzahl der Quellen nach Status an, z. B. Entwurf, aktiviert und deaktiviert im System.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Aktive Quellen nach Quelltyp	Zeigt die Verteilung aktiver Quellen nach Quelltyp an.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Aktive Quellen nach Feed-Format	Zeigt die Anzahl der aktivierten Quellen nach Feed-Typ an.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Aktive erkennbare Elemente insgesamt (30 Tage)	Zeigt die Top 10 Quellen nach Volumen von Intelligence-Datensätzen an, die in den letzten 30 Tagen erstellt wurden.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter auf einer neuen Registerkarte geöffnet.
Aktive erkennbare Elemente nach Typ	Zeigt das oberste Gesamtvolumen der Aggregate erkennbarer Elemente an, die in den letzten 30 Tagen erstellt wurden.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter auf einer neuen Registerkarte geöffnet.
Aktive Indikatoren nach Mustertyp	Zeigt das Gesamtvolumen der Indikatoraggregate nach	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Widget-Name	Beschreibung	Aktion
	Mustertyp an, die in den letzten 30 Tagen erstellt wurden.	ausgewählten Filter auf einer neuen Registerkarte geöffnet.
Aktive Indikatoren insgesamt (30 Tage)	Zeigt das Gesamtvolumen der Indikatoraggregate an, die in den letzten 30 Tagen erstellt wurden.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter auf einer neuen Registerkarte geöffnet.
Häufigste Quellen nach Anzahl falsch positiver Ergebnisse (30 Tage)	Zeigt das Gesamtvolumen von falsch positiven erkennbaren Elementen an, die in den letzten 30 Tagen erstellt wurden.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.

b. Bedrohungen Im Trend : Diese Registerkarte bietet eine allgemeine Übersicht über die Bedrohungen im Trend.

Bedrohungen im Trend

Widget-Name	Beschreibung	Aktion
Aktuelle Berichte (Top 10)	Zeigt die Liste der Berichte und Links an – Top-10-Reihenfolge nach Veröffentlichungsdatum.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Neueste RSS-Feeds (Top 10)	Zeigt die Liste der RSS-Feeds und Links an – Top-10-Reihenfolge nach Veröffentlichungsdatum.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Aktive erkennbare Elemente nach Bedrohungsbewertungsbereich (30 Tage)	Zeigt die Anzahl erkennbarer Elemente an, die in den letzten 30 Tagen erstellt wurden, verteilt nach Bedrohungsbewertungsbereichen.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter auf einer neuen Registerkarte geöffnet.
Aktive erkennbare Elemente nach Reputation (30 Tage)	Zeigt die Anzahl erkennbarer Elemente an, die in den letzten 30 Tagen erstellt wurden, verteilt nach Reputation.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter auf einer neuen Registerkarte geöffnet.
Top-Tags (30 Tage)	Zeigt die Top-Tags in den in den letzten 30 Tagen erstellten Datensätzen basierend auf der Häufigkeit der Nutzung an.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter auf einer neuen Registerkarte geöffnet.
Am meisten anvisierte Sektoren (30 Tage)	Zeigt die Top-10-Sektoren nach gemeldeten Aktivitäten an, die in den letzten 30 Tagen erstellt wurden.	Wenn auf dieses Widget geklickt wird, wird die KPI-Detailseite des Widgets für den ausgewählten Filter auf einer neuen Registerkarte geöffnet.

c. Intelligenzfreigabe : Diese Registerkarte bietet einen allgemeinen Überblick über die gemeinsame Nutzung von Intelligenzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Intelligenzfreigabe

Widget-Name	Beschreibung	Aktion
Eingehende Intel – Datensatzanzahl (30 Tage)	Zeigt die Anzahl der in den letzten 30 Tagen empfangenen eingehenden intel-Datensätze an, kategorisiert nach Typ (erkennbares Element, Objekt, Indikator).	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Ausgehende Intel – Datensatzanzahl (30 Tage)	Zeigt die Anzahl der ausgehenden intel-Datensätze an, die in den letzten 30 Tagen freigegeben wurden, kategorisiert nach Typ (erkennbares Element, Objekt, Indikator).	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Eingehende Intel – Verteilung nach Status (30 Tage)	Zeigt die Verteilung der eingehenden Intelligence-Datensätze nach Status über die letzten 30 Tage an.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Ausgehende Intel – Verteilung nach Status (30 Tage)	Zeigt die Verteilung ausgehender Intelligence-Datensätze nach Status über die letzten 30 Tage an.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Eingehende Intel – am häufigsten freigebendes Profil (30 Tage)	Zeigt die Top-Profile basierend auf eingehenden informationen an, die in den letzten 30 Tagen empfangen wurden.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Ausgehende Intel – am häufigsten freigegebenes Profil (30 Tage)	Zeigt die Top-Profile basierend auf ausgehenden intel an, die in den letzten 30 Tagen freigegeben wurden.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Eingehende Intel – am häufigsten freigegebene Typen (30 Tage)	Zeigt die am häufigsten empfangenen intel-Typen (Objekt, Indikator, erkennbares Element) in den letzten 30 Tagen an.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Ausgehende Intel – am häufigsten freigegebene Typen (30 Tage)	Zeigt die am häufigsten freigegebenen intel-Typen (Objekt, Indikator, erkennbares Element) in den letzten 30 Tagen an.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Eingehende Intel – Verteilung nach Format (30 Tage)	Zeigt die Formatverteilung (z. B. MISP, STEX) eingehender intel in den letzten 30 Tagen an.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.
Ausgehende Intel – Verteilung nach Format (30 Tage)	Zeigt die Formatverteilung (z. B. MISP, STEX) ausgehender intel in den letzten 30 Tagen an.	Wenn auf dieses Widget geklickt wird, wird die Listenseite mit den gefilterten Datensätzen geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence-Sicherheitszentrum konfigurieren

Richten Sie die Funktionen, Komponenten und Integrationen ein, die Sie benötigen, um Ihren Kunden Service und Support bereitzustellen.

Laden Sie die TISC-Anwendung aus dem ServiceNow Store herunter

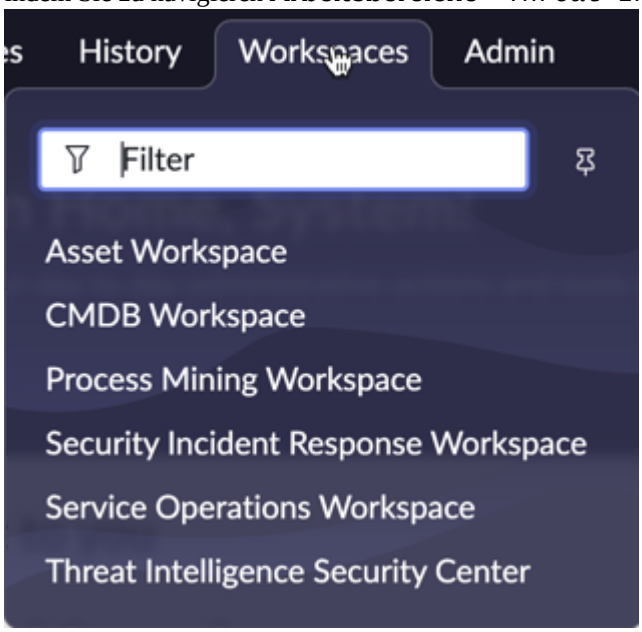
Bevor Sie ausführen Threat Intelligence-Sicherheitszentrum Anwendung in Ihrer Instanz müssen Sie sie aus herunterladen ServiceNow® Store Und installieren Sie es.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Befolgen Sie die Anweisungen für Lädt eine Anwendung aus dem herunter ServiceNow Store Und installieren Sie **Security Operations Des Threat Intelligence-Sicherheitszentrums** Anwendung.
2. Nach Abschluss der Installation können Sie öffnen Threat Intelligence-Sicherheitszentrum Arbeitsbereich, indem Sie zu navigieren **Arbeitsbereiche** > *`Threat Intelligence-Sicherheitszentrum`*



Nächste Maßnahme

Nachdem Sie die Anwendung erfolgreich heruntergeladen haben, stellen Sie sicher, dass Sie alle hier in diesem Abschnitt genannten Aufgaben abgeschlossen haben. Richten Sie das Threat Intelligence-Sicherheitszentrum ein Für eine reibungslose Integration.

Richten Sie das Threat Intelligence-Sicherheitszentrum ein

Bevor Sie verwenden Threat Intelligence-Sicherheitszentrum, Sie müssen es aus herunterladen ServiceNow Speichern.

Installierte Rollen

Überprüfen Sie die folgenden Informationen, und stellen Sie sicher, dass Sie alle Aufgaben für eine reibungslose Integration abgeschlossen haben. Nachfolgend finden Sie die Liste der verschiedenen Anwenderpersona, die für den Zugriff auf die Anwendung und die Arbeit mit der Anwendung definiert sind:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Threat Intelligence-Analyst (sn_sec_tisc.Analyst)
- Threat Intelligence-Administrator (sn_sec_tisc.admin)

Berechtigungen, die für TISC-Rollen gelten

Setup	Beschreibung
Weisen Sie die erforderlichen zu, und verifizieren Sie sie ServiceNow AI Platform Und Threat Intelligence Security Center-Rollen.	Die folgenden Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich: • Als Administrator müssen Sie die TISC-Anwendung aus dem installieren ServiceNow Speichern Sie die Rolle sn_sec_tisc.admin, und weisen Sie sie zu. • Diese Rolle „sn_sec_tisc.admin“ führt die folgenden Aufgaben aus: ◦ Konfiguriert die Datenquellen zum Erfassen der Daten. Weitere Informationen finden Sie unter Threat Intelligence-Feeds. ◦ Hat die Integrationen konfiguriert, die zum Anreichern von Daten erkennbarer Elemente in TISC erforderlich sind. Weitere Informationen finden Sie unter TISC-Anreicherungsintegrationen. ◦ Konfiguriert Genehmigungsrollen für Datenimport für den Datenimport zum Importieren von Daten mit dem Importassistenten. Weitere Informationen finden Sie unter Mit Datenimporten arbeiten. ◦ Konfiguriert den Rechner für die Bedrohungsbewertung anhand der erforderlichen Kriterien für die automatische Berechnung der Bedrohungsbewertung erkennbarer Elemente. Weitere Informationen finden Sie unter Definieren Sie Den Rechner Für Die Bedrohungsbewertung. ◦ Konfiguriert erforderliche Taxonomien und Taxonomiewerte. Weitere Informationen finden Sie unter Taxonomien Werden Erstellt. ◦ Konfigurieren Sie das für Ihre Organisation relevante MITRE ATT&CK-Repository. Weitere Informationen finden Sie unter MITRE-ATT&CK Repository.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigungen, die für TISC-Rollen gelten (Fortsetzung)

Setup	Beschreibung
	Hinweis: Als sn_sec_tisc.admin können Sie auch die Rolle sn_sec_tisc.Analyst zuweisen. • Die Rolle sn_sec_tisc.Analyst führt die folgenden Aufgaben aus: ○ Zeigt die Übersicht der Daten im System mithilfe der Anwendungs-Homepage an. Weitere Informationen finden Sie unter Anzeigen TISC Homepage. ○ Importieren Sie Daten über die Schaltfläche „Intelligenz importieren“ auf der Seite „Bedrohungsbibliothek“ in das System. Weitere Informationen finden Sie unter Threat Intelligence-Sicherheitszentrum Bibliothek. ○ ▪ Durchsucht die in der Anwendung vorhandenen Daten mithilfe der Suche, die auf der Seite „Bedrohungsbibliothek“ bereitgestellt wird. ▪ Verwaltet die Daten, die aus verschiedenen Quellen in der Bedrohungsbibliothek erfasst wurden. ▪ Führt verschiedene Anreicherungsaktionen für erkennbare Elemente aus. ▪ Erstellt und verwaltet Fälle. Weitere Informationen finden Sie unter Erstellen von Fällen mit der Workbench für Bedrohungsanalysen.

Abhängigkeits-Plugins

Plugin	Beschreibung
Die folgenden Anwendungen sind für die Installation dieser Anwendung erforderlich: • Allgemeine Sicherheitsfallmanagement-Arbeitsbereichskomponenten [com.snc.escm.ws_commons] • Threat Intelligence-Support – Allgemein [com.snc.Threat] • Verschlüsselung auf Spaltenebene (com.Glide.Encryption)	Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung der Integration erforderlich sind, werden installiert und aktiviert, bevor Sie diese Integration konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugin	Beschreibung
• Große API für JSON- und XML-Nutzlastgenerator (com.Glide.Streaming_Builder) • Sicherheitssupport Core (com.snc.security_support.core) • Experience-Komponente der Knotenzuordnung (sn_node_Map) • UI-Komponente für Berichterstellung für Arbeitsbereich (sn_sec_Reporting) • Rich-Text-Editor-Komponente für Security Operations (sn_escm_rte) • Sicherheitsintegrations-Framework (sn_sec_int) • Sicherheitssupport allgemein (sn_sec_cmn) • Orchestration für Sicherheitssupport (sn_sec_cmn_orch)	

Integration Threat Intelligence-Sicherheitszentrum

Verwenden Sie diesen Abschnitt, um zu verstehen Threat Intelligence-Sicherheitszentrum Integrationen.

Die **Integrationen** Abschnitt enthält die folgenden Untermodule.

Integrationen

Modulname	Beschreibung
Katalog	Alle verfügbaren Threat Intelligence-Feeds und Ergänzungsintegrationen werden hier als Kacheln/Karten angezeigt. Die Anwender haben keine Möglichkeit, einen neuen Feed oder eine neue Integration aus diesem Abschnitt zu erstellen.
Bedrohungs-Feeds	Dieser Abschnitt enthält nur die Details zu Threat Intelligence-Feeds, und die Anwender können neue Threat Intelligence-Feeds aus diesem Abschnitt konfigurieren.
Ergänzungsintegrationen	Dieser Abschnitt enthält nur die Details zu Ergänzungsintegrationen, und die Anwender können verfügbare Ergänzungsintegrationen in diesem Abschnitt konfigurieren. **Hinweis:** Der Abschnitt „Ergänzungsintegrationen“ ist nur sichtbar, wenn mindestens ein Ergänzungsintegrations-Plugin installiert ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

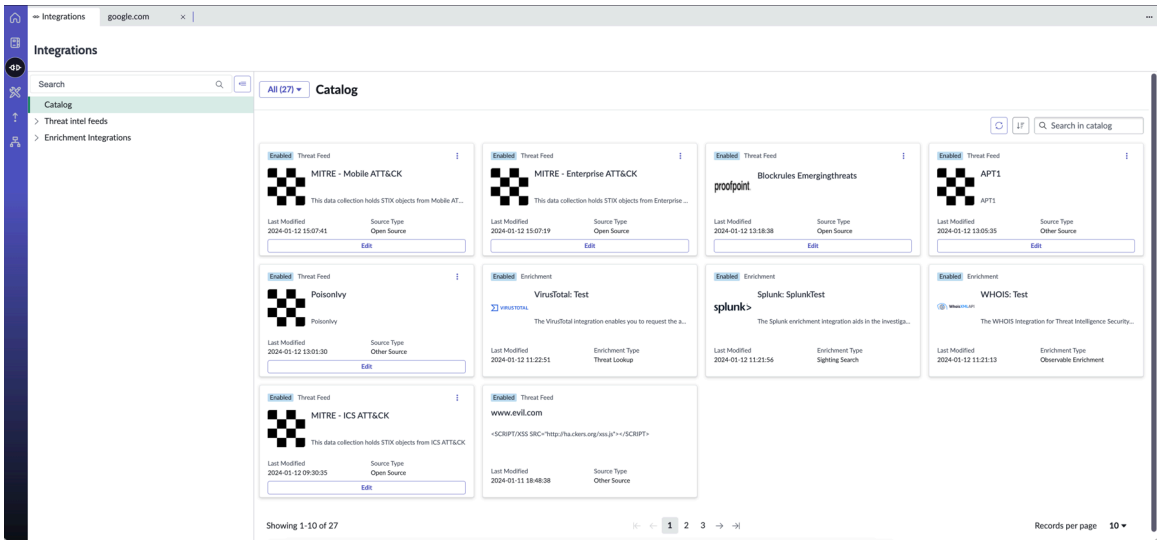
Threat Intelligence-Sicherheitszentrum Katalog

Die Threat Intelligence-Sicherheitszentrum Katalog ist eine kuratierte Liste von Threat Intelligence-Feeds und Ergänzungsintegrationen, die in der Anwendung verfügbar sind, damit Sie sie nach dem Hinzufügen der erforderlichen Informationen aktivieren und den Feed so planen können, dass Threat Intelligence-Daten automatisch mit einer festgelegten Häufigkeit erfasst werden.

Als sn_sec_tisc.admin können Sie auch die vorhandenen Quellkonfigurationen durchsuchen und bearbeiten, aktivieren oder deaktivieren und die Konfigurationen aus dem Katalog löschen. Jede neue Datenquelle wird dem Katalog hinzugefügt, die als neue Konfigurationskarte im Katalog angezeigt wird.

Erforderliche Rolle:

- sn_sec_tisc.admin (erstellen/aktualisieren)
- sn_sec_tisc.Analyst (lesen)



Hinweis:
Die Karten im Katalog unterscheiden sich durch ihre Bezeichnung, die oben auf der Karte vorhanden ist Bedrohungs-Feed/-Anreicherung .

Aktionen in der Katalogansicht

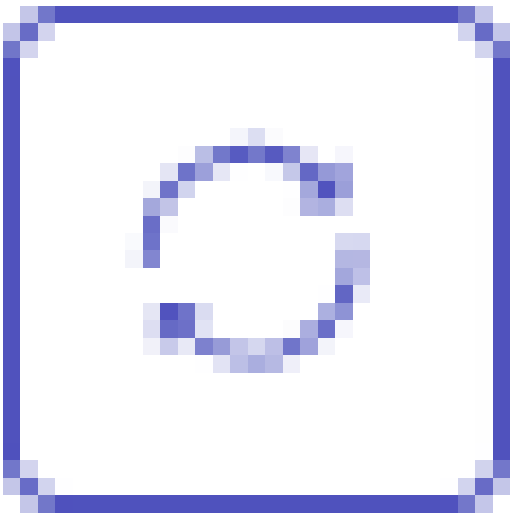
In der Katalogansicht können Sie die folgenden Aktionen ausführen.

Aktionen in der Katalogansicht

Aktion	Beschreibung
Alle	Verwenden Sie dieses Dropdown-Menü, um Feeds und Integrationen basierend auf ihrem aktuellen Status zu filtern. Sie können basierend auf den folgenden status filtern:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen in der Katalogansicht (Fortsetzung)

Aktion	Beschreibung
	• **Alle** : Zeigt alle Feeds und Integrationen auf der Seite an. Dies ist die Standardoption. • **Aktiviert** : Zeigt alle Feeds und Integrationen an, die sich in einem aktivierten Status befinden. • **Deaktiviert** : Zeigt alle Feeds und Integrationen an, die sich in einem deaktivierten Status befinden. • **Entwurf** : Zeigt alle Feeds und Integrationen an, die sich im Entwurfsstatus befinden.
	Verwenden Sie diese Aktion, um den Katalog zu aktualisieren.
	Verwenden Sie diese Aktion, um alle Feeds und Integrationen nach folgenden Kriterien zu sortieren: • **Zuletzt geändert (aktuell)** • **Zuletzt geändert (am ältesten)** • **Name A–Z** • **Name (Z–A)**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen in der Katalogansicht (Fortsetzung)

Aktion	Beschreibung
In Katalog suchen	Verwenden Sie diese Aktion, um basierend auf dem Namen und der Beschreibung im Katalog nach Feeds/ Integrationen zu suchen.

Threat Intelligence-Feeds

Verwenden Sie Threat Intelligence-Feeds, um die Datenquelle des Threat Intelligence-Feeds hinzuzufügen, zu bearbeiten oder zu entfernen.

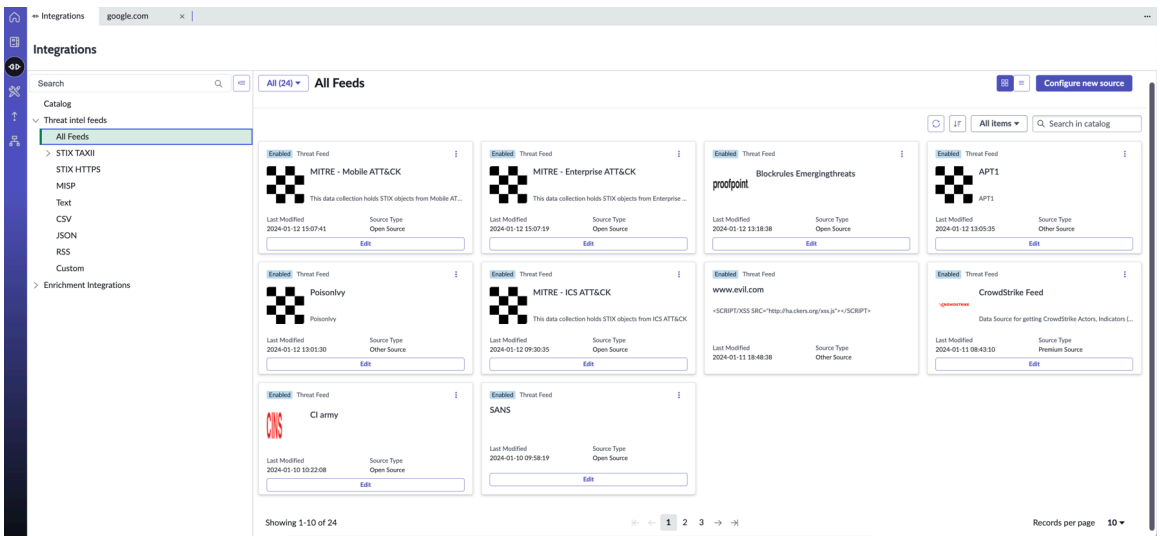
Die Datenquellen-Feeds sind im Abschnitt „Integrationen“ im Threat Intel-Katalog verfügbar.

Der Katalog für Threat Intelligence-Feeds wurde erstellt, um die verfügbaren Feed-Datenquellen in Form von Kacheln anzuzeigen. Er hat die Möglichkeit, die Details der Quellkonfiguration zu filtern, zu durchsuchen und zu navigieren und verschiedene Aktionen auszuführen.

Alle Feeds

Das Basissystem enthält eine Reihe von Karten für jeden der Feeds, die Sie aktivieren und verwenden können.

Die Feeds können angezeigt werden, indem Sie zu navigieren **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen** > **Bedrohungsinformationsfeeds** > **Alle Feeds**an.



Aktionen in der Ansicht „alle Feeds“

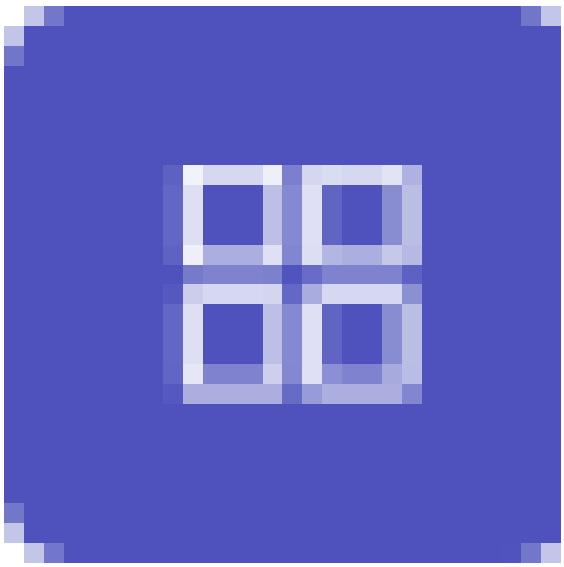
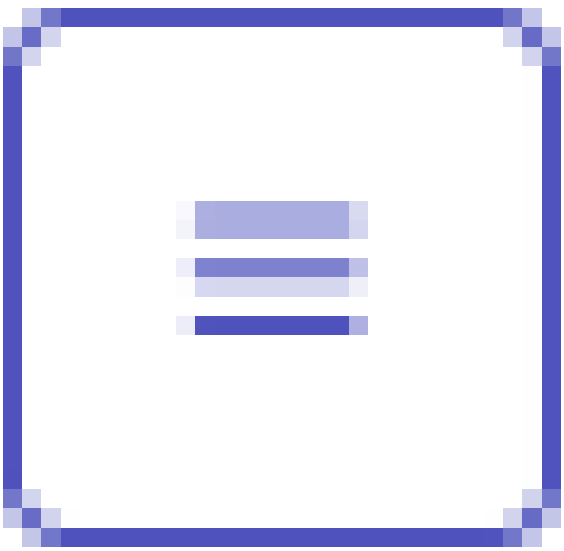
Im Abschnitt alle Feeds können Sie die folgenden Aktionen ausführen.

Aktionen in der Ansicht „alle Integrationen“

Aktion	Beschreibung
Alle	Verwenden Sie dieses Dropdown-Menü, um Feeds basierend auf ihrem aktuellen Status zu filtern. Sie können basierend auf den folgenden status filtern:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

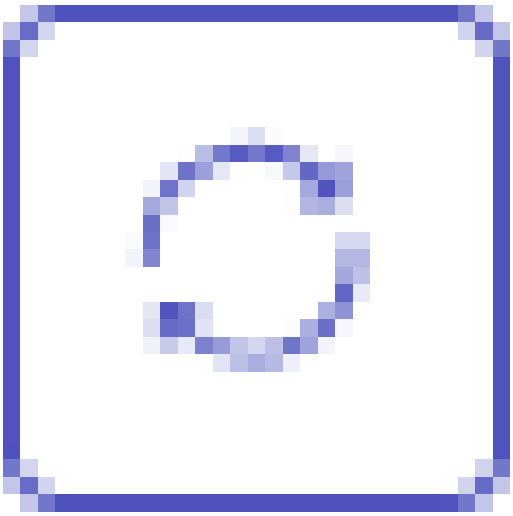
Aktionen in der Ansicht „alle Integrationen“ (Fortsetzung)

Aktion	Beschreibung
	• **Alle** : Zeigt alle Feeds auf der Seite an. Dies ist die Standardoption. • **Aktiviert** : Zeigt alle Feeds an, die sich in einem aktivierten Status befinden. • **Deaktiviert** : Zeigt alle Feeds an, die sich in einem deaktivierten Status befinden. • **Entwurf** : Zeigt alle Feeds an, die sich im Entwurfsstatus befinden.
	Verwenden Sie diese Aktion, um alle Feeds in Form von Karten anzuzeigen.
	Verwenden Sie diese Aktion, um alle Feeds in Form einer Listenansicht anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen in der Ansicht „alle Integrationen“ (Fortsetzung)

Aktion	Beschreibung
	Verwenden Sie diese Aktion, um die Seite zu aktualisieren.
	Verwenden Sie diese Aktion, um alle Integrationen nach folgenden Kriterien zu sortieren: • **Zuletzt geändert (aktuell)** • **Zuletzt geändert (am ältesten)** • **Name A–Z** • **Name (Z–A)**
Alle Elemente	Verwenden Sie diese Aktion, um die Threat Intelligence-Feed-Kacheln nach Quelltyp oder Feed-Typ zu filtern und aufzulisten. **Quelltyp** : • Open Source • Andere Quelle • Premium-Quelle **Feed-Typ** : • CSV • Anwenderdefinierter Feed • JSON

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen in der Ansicht „alle Integrationen“ (Fortsetzung)

Aktion	Beschreibung
	• MISP • RSS • STIX-HTTPS • Text
In Katalog suchen	Verwenden Sie diese Aktion, um basierend auf dem Namen und der Beschreibung im Katalog nach Feeds zu suchen.

Arten von Bedrohungsinformationen-Feeds

Im Folgenden sind die Arten von Threat Intelligence-Feeds aufgeführt, die konfiguriert und aktiviert werden können:

Threat Intelligence-Feeds

Typ	Beschreibung
TAXII-Feeds	Feeds, die als STIX-/TAXII-Sammlungsformat verfügbar sind.
STIX HTTPS	Threat Intelligence-Feeds im STIX-Format, auf die über REST APIs im HTTPS-Protokoll zugegriffen werden kann.
MISP	Feeds, die sich im MISP-Format-Feeds befinden.
Text	Feeds, die als gehostete Dateien im Textformat verfügbar sind. **Hinweis:** Das System analysiert die Dateien auf URL, Domäne, Dateiname, Hashes und IP-Adresse. Es werden nur extrahiert, und es werden keine anderen erkennbaren Elemente extrahiert.
CSV	Feeds, die als gehostete Dateien im CSV-Format verfügbar sind. **Hinweis:** Das System analysiert die Dateien auf URL, Domäne, Dateiname, Hashes und IP-Adresse. Es werden nur extrahiert, und es werden keine anderen erkennbaren Elemente extrahiert.
JSON	Feeds, die als gehostete Dateien im JSON-Format verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence-Feeds (Fortsetzung)

Typ	Beschreibung
	Hinweis: Das System analysiert die Dateien auf URL, Domäne, Dateiname, Hashes und IP-Adresse. Es werden nur extrahiert, und es werden keine anderen erkennbaren Elemente extrahiert.
RSS	Feeds, die im RSS-Format verfügbar sind. Die Anwendung speichert die Daten als RSS-Feed-Datensätze.
Anwenderdefiniert	Feeds, die mit anwenderdefinierten Parsern konfiguriert werden. **Hinweis:** Das System analysiert die Dateien auf URL, Domäne, Dateiname, Hashes und IP-Adresse. Es werden nur extrahiert, und es werden keine anderen erkennbaren Elemente extrahiert.

Die nächsten Schritte des Verfahrens finden Sie im entsprechenden Abschnitt zum Konfigurieren eines bestimmten Feed-Typs unter Threat Intelligence-Feeds.

Konfigurieren Sie einen neuen Threat Intelligence-Feed

Konfigurieren Sie den neuen Threat Intelligence-Feed.

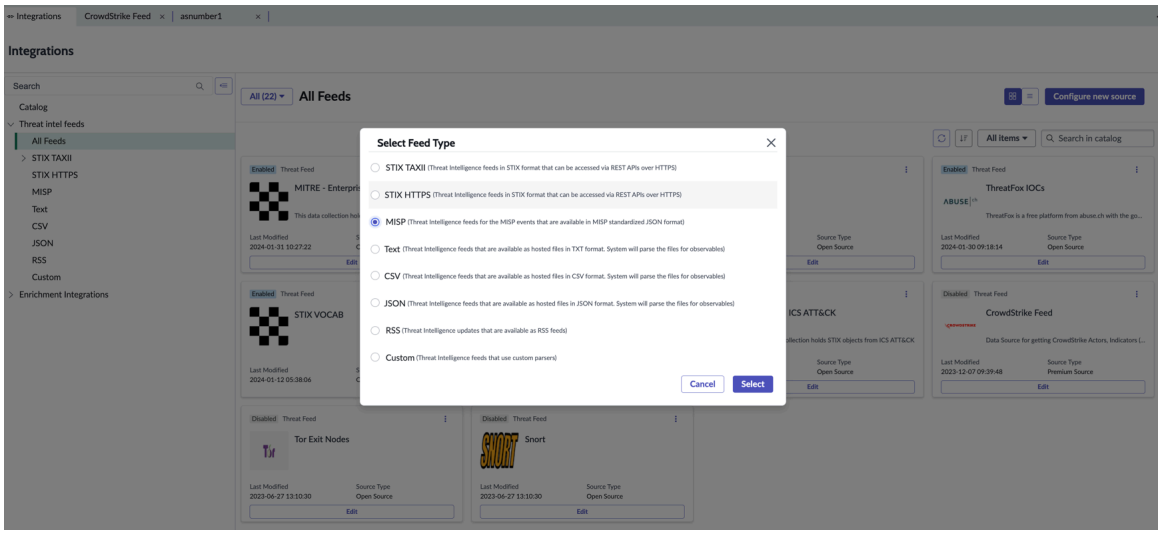
Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Um einen neuen Threat Intelligence-Feed zu konfigurieren, gehen Sie wie folgt vor:

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** Symbol.
3. Auswahlvorgang **Bedrohungsinformationsfeeds** > **Alle Feeds**an.
4. Klicken Sie Auf **Konfigurieren Sie eine neue Quelle** .
   Die verschiedenen Feed-Typen werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie den entsprechenden Feed-Typ aus.
6. Füllen Sie im Formular die Felder aus.

Neue Quelle konfigurieren

Feld	Beschreibung
Name	Geben Sie einen Namen für den Feed ein.
Beschreibung	Beschreibung des Feeds.
Feed-Typ	Der Feed-Typ. Beispiel: MISP. Standardmäßig wird dieser Wert basierend auf dem Feed-Typ angezeigt, den Sie im Katalog ausgewählt haben.
Logo	Hängen Sie das Logo des Quell-Feeds an. **Hinweis:** Die Größe muss 72 px/72 px betragen.
Branche	Wählen Sie die Branchenkategorie aus, z. B. Luft- und Raumfahrt, Landwirtschaft usw., für die der Feed gilt.
Quelltyp	Wählen Sie den Typ der Quelle aus der Liste der verfügbaren Quelltypen aus. Liste der verfügbaren Quellen: ○ Regierung ○ ISACs ○ Open Source ○ Premium-Quelle ○ Andere Quelle

7. Klicken Sie auf **Auswählen**.
8. Füllen Sie die Felder im Abschnitt Konfiguration entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration

Feld	Beschreibung
Ablaufzeitraum (in Tagen)	Geben Sie den Ablaufzeitraum für den Feed in Tagen ein. Beispiel: 180 Tage. **Hinweis:** Alle Daten, die aus der Quelle erfasst werden, laufen 180 Tage nach der Erfassung ab.
REST-Nachricht verwenden	Wählen Sie Aus **REST-Nachricht verwenden** Kontrollkästchen, wenn Sie die Funktionalität „REST-Nachricht/REST-Methode“ verwenden müssen, die von bereitgestellt wird ServiceNow AI Platform. Wenn dieses Kontrollkästchen nicht aktiviert ist, verwendet die Anwendung den in angegebenen Endpunkt **REST-Endpunkt-URL** Zum Abrufen der Daten aus dem Feed. Weitere Informationen finden Sie unter Ausgehender REST-Webservice Ein ServiceNow AI Platform Dokumentation. **Hinweis:** Die Felder „REST-Nachricht“ und „REST-Methode“ sind obligatorisch, wenn Sie die REST-Nachricht auswählen.
REST-Nachricht	Wählen Sie den REST-Nachrichtendatensatz aus der Liste der REST-Nachrichtendatensätze aus, die bereits in der Instanz konfiguriert sind. Weitere Informationen finden Sie unter Ausgehender REST-Webservice Auf der ServiceNow AI Platform Dokumentation. **Hinweis:** Wählen Sie diesen Wert aus, wenn Sie bestimmte Header anzeigen und die REST-bezogenen Datensätze mit der REST-Nachrichtenoption definieren müssen.
REST-Methode	Wählen Sie REST-Methode aus der Liste der verfügbaren REST-Methoden aus, die für die ausgewählte REST-Nachricht konfiguriert sind. Weitere Informationen finden Sie unter Ausgehender REST-Webservice Auf der ServiceNow AI Platform Dokumentation.
Vertrauen	Legen Sie die Konfidenz für alle zutreffenden Datensätze fest, die über diesen spezifischen Feed erfasst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Legen Sie die Konfidenz für diese Quelle zwischen 0-100 fest.
Datenanalysemechanismus	Wählen Sie die entsprechende Option für den Datenanalysemechanismus aus. Verfügbare Optionen: ○ **Automatisierte IOC-Extraktion** : Diese Option ist standardmäßig ausgewählt, wenn Text-, CSV- oder JSON-Feeds konfiguriert werden. ○ **Anwenderdefinierte Feldzuordnung** : Wählen Sie diese Option aus, wenn Sie definieren möchten, wie die spezifischen Felder in Ihren Feed-Daten den Attributen des erkennbaren Elements zugeordnet werden sollen. Nach der Auswahl können Sie die Zuordnungen in konfigurieren **Feldzuordnung** Abschnitt. Weitere Informationen zur anwenderdefinierten Feldzuordnung finden Sie unter Konfigurieren Sie Die Anwenderdefinierte Feldzuordnung. **Hinweis:** Die Option „Datenanalysemechanismus“ ist nur für Text-, CSV- und JSON-Feeds verfügbar, in denen Feeds verwendet werden **Berichtsprozessor** Ist auf festgelegt `SimpleFeedDatasourceResponseProcessor` .
REST-Endpunkt-URL	Geben Sie die REST-Endpunkt-URL ein, unter der die Daten vom Threat Intelligence-Feed gehostet werden. **Hinweis:** Für MISP-Feed-Typen die REST-Endpunkt-URLs, die mit enden `/Manifest.JSON` Werden unterstützt.
Authentifizierung erforderlich	Aktivieren Sie dieses Kontrollkästchen, wenn für Ihren neuen Threat Intelligence-Feed eine Authentifizierung erforderlich ist. **Hinweis:** Dies gilt nur, wenn die REST-Endpunkt-URL zum Abrufen der Daten verwendet wird.
Authentifizierungstyp	Der Authentifizierungstyp für den Quell-Feed. Im Folgenden sind die Authentifizierungstypen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	aufgeführt, die im Basissystem für die Anwender konfiguriert und bereitgestellt werden: ○ API-ID/API-SCHLÜSSEL ○ API-ID/API-GEHEIMNIS ○ API-Schlüssel ○ API-Schlüssel/API-Geheimnis ○ API-Anwendername/API-Passwort/API-Schlüssel ○ Standardauthentifizierung
Header, die mit der Anforderung übergeben werden sollen	Alle Header, die mit den Anforderungen übergeben werden sollen, können in der Anforderungs-Header-Zuordnung angegeben werden. ○ Header muss als Schlüssel-Wert-Paar angegeben werden, das durch einen Doppelpunkt („:“) getrennt ist. ○ Jedes Header-Schlüssel-Wert-Paar muss in einer neuen Zeile angegeben werden. ○ Um Authentifizierungsparameter als Header-Werte anzugeben, schließen Sie die erforderliche Authentifizierungsbezeichnung mit „${“ und „}$“ ein. Beispiel: X-api-key:${API Key}$.
Erweitert	Aktivieren Sie dieses Kontrollkästchen, um ein anwenderdefiniertes Integrationsskript und ein Berichtsprozessorskript zu definieren. **Hinweis:** Wenn Sie dieses Kontrollkästchen aktivieren, wird die **Integrationsskript** Und **Berichtsprozessor** Felder werden angezeigt, damit Sie die anwenderdefinierten Skripts auswählen können.
Integrationsskript	Das Integrationsskript ruft einen Aufruf der REST-Endpunkt-URL mithilfe der Authentifizierungsparameter und der im Feed konfigurierten Header auf, und das Skript ruft dann die Daten ab, die aus dem spezifischen Feed verfügbar sind. Im Basissystem sind die folgenden anwenderdefinierten Skripteinbindungen verfügbar, die innerhalb der Anwendung für die Integrationsskripts bereitgestellt werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ MITRESourceIntegration: Wird zum Abrufen der Daten aus MITRE-Feeds verwendet. ○ RSSFeedDatasourceIntegration: Wird zum Abrufen der Daten aus RSS-Feeds verwendet. ○ SimpleFeedDatasourceIntegration: Wird zum Abrufen der Daten aus einfachen Feeds ohne Authentifizierung oder Standardauthentifizierung verwendet. ○ SimpleMISPFeedDatasourceIntegration: Wird zum Abrufen der Daten aus gehosteten MISP-Feeds verwendet. Das Standardintegrationsskript basiert auf dem von Ihnen ausgewählten Feed-Typ. Wenn Sie beispielsweise den MISP-Feed-Typ auswählen, bei dem es sich um ein Standardformat zum Verarbeiten und Abrufen der Daten handelt, lautet das Integrationsskript **SimpleMISPFeedDatasourceIntegration** . **Hinweis:** Für die anwenderdefinierten Integrationsskripts können Sie eine Skripteinbindung erstellen, indem Sie erweitern **FeedDatasourceIntegrationBase** Und überschreiben die erforderlichen Methoden.
Berichtsprozessor-Skript	Das Berichtsprozessorskript verarbeitet Daten, die aus dem Feed mithilfe des Integrationsskripts abgerufen wurden. Das Basissystem enthält die folgenden anwenderdefinierten Skripts, die innerhalb der Anwendung zur Unterstützung des Berichtsprozessorskripts bereitgestellt werden: ○ AtomFeedDatasourceResponseProcessor: Wird für die Verarbeitung von RSS-Feeds im Atom-Format verwendet. ○ MITRECollectionDataProcessor: Wird für die Verarbeitung von MITRE-Feeds verwendet. ○ RSSFeedDatasourceResponseProcessor: Wird für die Verarbeitung von RSS-Feeds verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ SimpleDataplaneFeedResponseProcessor: Wird für die Verarbeitung von Dataplane-Feeds verwendet. ○ SimpleFeedDatasourceResponseProcessor: Wird für die Verarbeitung einfacher Feeds mithilfe der Extraktion von erkennbaren Elementen mit regulären Ausdrücken verwendet. ○ SimpleFeodotrackerFeedResponseProcessor: Wird zur Verarbeitung von Feodotracker-Feeds verwendet. ○ SimpleMISPFeedDatasourceResponseProcessor: Wird für die Verarbeitung gehosteter MISP-Feeds verwendet. ○ TAXIIV2CollectionDataProcessor: Wird für die Verarbeitung von TAXII-Sammlungsdaten verwendet. Der standardmäßige Berichtsprozessor für MISP-Feeds ist SimpleMISPFeedDatasourceResponseProcessor. Dieser Prozessor ist von der Anwendung vorkonfiguriert und kann nicht geändert oder ersetzt werden.

9. Füllen Sie die Felder im Abschnitt „Zeitplanung“ entsprechend aus.

Zeitplanung

Feld	Beschreibung
Ausführen	Legen Sie die Häufigkeit fest, mit der Sie die Datensätze erfassen möchten. Der Feed wird basierend auf dem Zeitplanungsauftragsintervall ausgeführt und ausgeführt. Die verfügbaren Auftragsintervalle sind: ○ Täglich ○ Wöchentlich ○ Monatlich ○ In regelmäßigen Abständen ○ Einmal ○ Bei Bedarf ○ Geschäftskalender: Eintragsbeginn ○ Geschäftskalender: Eintragsende **Hinweis:** Standardmäßig ist die Häufigkeit auf „bei Bedarf“ festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Weitere Informationen finden Sie unter Geplante Aufgaben und wie ein Skript Ihrer Wahl automatisch ausgeführt wird .
Daten abrufen von	Das Startdatum, ab dem die Daten abgerufen werden mussten. Dieses Feld sollte mit der Zeit festgelegt werden, ab der die Daten aus der entsprechenden Quelle erfasst werden müssen. Sobald dieses Feld festgelegt ist, ruft die nächste Erfassungsausführung die Daten aus der konfigurierten Zeit ab, und aufeinanderfolgende Erfassungsausführungen rufen inkrementelle Daten ab. Beispielsweise ist „Quelle“ so geplant, dass die Daten stündlich erfasst werden. Der Anwender legt fest **Daten Von Abrufen** Bis zum 12. Januar 6:00 Uhr am 12. Januar 9:00 Uhr ruft die am 12. Januar 30 ausgelöste Erfassung die Daten vom 12. Januar 6:00 UHR bis 12. Januar 10:00 Uhr ab. Die nächste Erfassung, die um 11:00 Uhr ausgelöst wird, ruft nur die inkrementellen Daten vom 12. Januar 10:00 UHR bis 12. Januar 11:00 Uhr ab. **Hinweis:** Dies bedeutet, dass die geplanten Ausführungen ab dem angegebenen Datum inkrementell Daten abrufen. **Wichtig:** Dies gilt auch nicht für Text-, CSV- und JSON-Feeds.

Tags

Feld	Beschreibung
Tags auswählen	Verwenden Sie die Tags, um Anmerkungen oder Ohrmarkendatensätze zu versehen, die aus dieser Quelle in das System aufgenommen werden. Beginnen Sie mit der Eingabe des Tag-Namens in **Suchen** Leiste, um die verfügbaren Tags in der Anwendung auszuwählen, oder geben Sie einen neuen Tag-Namen ein, und klicken Sie auf **Hinzufügen** Um es der Quelle zuzuweisen.

10. Klicken Sie auf **Speichern** Aktion zum Speichern und Erstellen des Feeds.
    Die angegebenen Details werden validiert, und standardmäßig ist der Feeds-Status deaktiviert.
11. **Wahlweise:** Klicken Sie auf **Als Entwurf speichern** Aktion, um die Feed-Konfigurationen nur als Entwurf zu speichern.
    Anwender können einen Feed nicht aktivieren, wenn er im Entwurf gespeichert wird. Wenn Sie sich bei den Konfigurationsdetails nicht sicher sind, können Sie verwenden **Als Entwurf speichern** Option.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie die Konfigurationsdetails erhalten haben, können Sie die verbleibenden Informationen in die Entwurfsversion eingeben und erstellen.

12. Klicken Sie Auf **Aktivieren** Zum Aktivieren des Datensatzes.

    Sobald der Threat Intelligence-Feed-Datensatz aktiviert ist, können Sie den Datensatz ausführen, um die Integration auszuführen.

    Hinweis:

    - Der Threat Intelligence-Feed-Datensatz ist gekennzeichnet und als angegeben **Aktiviert** . Ebenso können Sie den Threat Intelligence-Feed deaktivieren, indem Sie auf klicken **Deaktivieren** Schaltfläche.
    - Sie können einen bestimmten Feed auch aktivieren, deaktivieren oder löschen, indem Sie verwenden **Aktionen** Menü der erforderlichen Feed-Kachel auf der **Katalog** Oder **Bedrohungsinformationen-Feeds** Seite.

13. Klicken Sie Auf **Löschen** Um den Threat Intelligence-Feed-Datensatz zu löschen.
14. Wählen Sie Aus **Integrationen Werden Ausgeführt** Abschnitt zum Überprüfen der Ausführungsdetails.

Hinweis:
Das oben genannte Konfigurationsverfahren für Threat Intelligence-Feed ist für alle anderen Threat Intelligence-Feed-Typen identisch, mit Ausnahme von STIX TAXII. Weitere Informationen zur Konfiguration VON STIX TAXII finden Sie unter Konfigurieren Sie einen neuen TAXII-Feed.

Konfigurieren Sie Die Anwenderdefinierte Feldzuordnung

Mit der Feldzuordnung können Sie konfigurieren, wie jedes Feld in einem Daten-Feed wie Text, CSV oder JSON interpretiert und dem entsprechenden erkennbaren Element zugewiesen wird.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

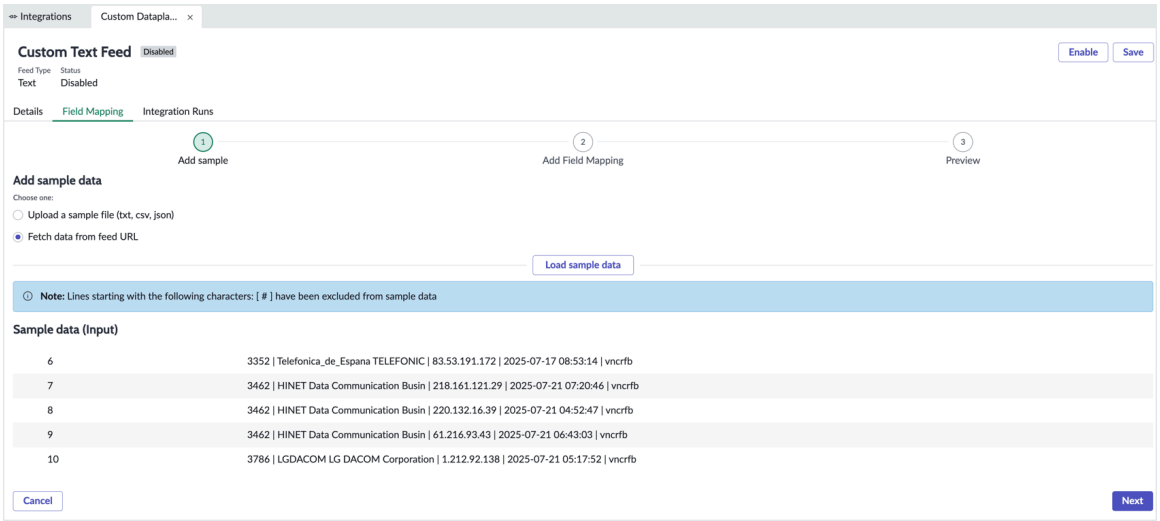
1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen**an.
2. Auswahlvorgang **Bedrohungsinformationsfeeds** > **Alle Feeds** > **Text**an.
3. Wählen Sie Aus **Konfigurieren Sie eine neue Quelle** .
4. Füllen Sie die Details des Text-Feed-Formulars nach Bedarf aus.
   Weitere Informationen finden Sie unter Konfigurieren Sie einen neuen Threat Intelligence-Feed.
5. Führen Sie in der neuen Formularansicht einen Drilldown zu **Datenanalysemechanismus** Feld unter **Konfiguration** Abschnitt.
   Weitere Informationen zum Datenanalysemechanismus finden Sie unter Konfigurieren Sie einen neuen Threat Intelligence-Feed.
6. Wählen Sie Aus **Anwenderdefinierte Feldzuordnung** Option.
7. Navigieren Sie zu **Feldzuordnung** Abschnitt.
8. Wählen Sie Aus **Konfigurieren** Zum Hinzufügen der Feldzuordnung für die neue Datenquelle.
   Dieser Abschnitt umfasst drei Schritte, z. B. das Hinzufügen von Beispieldaten, die Feldzuordnung und die Vorschau der zugeordneten Beispieldatensätze.
9. Um die Beispieldaten hinzuzufügen, wählen Sie aus **Beispieldaten Laden** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dadurch werden die Beispieldaten aus der ausgewählten Option angezeigt. Die Anwendung zeigt nur die relevanten Datenzeilen und -Zeilen an, die mit beginnen # Sind aus den Beispieldaten ausgeschlossen. Die Kommentarbezeichner können mit der Systemeigenschaft geändert werden: sn_sec_tisc.Feed_comment_Identifiers .

Die Anwendung ruft ein Beispiel der eingehenden Daten entweder aus einer Beispieldatei (z. B. .txt, .csv oder .JSON) oder direkt aus der konfigurierten Feed-URL (die Feed-URL und die Anmeldeinformationen, die in eingegeben wurden) ab **Details** Abschnitt). Auf diese Weise können Sie eine Vorschau der Struktur und des Inhalts der Daten anzeigen, bevor Sie Feldzuordnungen definieren.

10. Wählen Sie entweder aus **Laden Sie eine Beispieldatei hoch** Oder **Feed-Daten aus Feed-URL** .
Diese Beispieldaten rufen standardmäßig die ersten zehn Datensätze ab. Diese Gesamtzahl der abzurufenden Datensätze kann mit der Systemeigenschaft geändert werden sn_sec_tisc.Feed_field_Mapping_sample_count .



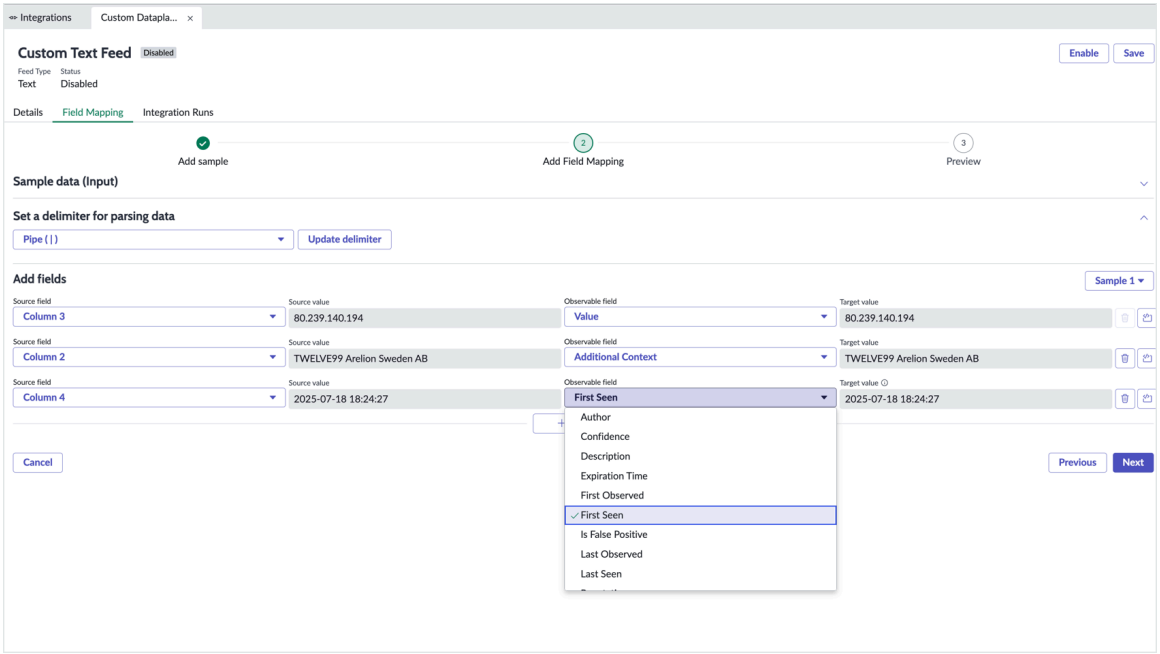
11. Wählen Sie Aus **Als Nächstes** Zum Konfigurieren der Feldzuordnung.
12. Wählen Sie Aus **Legen Sie ein Trennzeichen für die Analyse von Daten fest** Option aus der Dropdown-Liste.
Bei der Arbeit mit Textfeeds ist das Trennzeichen für die korrekte Analyse der Daten in einzelnen Feldern wichtig.

    In diesem Szenario verwendet der Text-Feed den Pipe-Operator (|) als Trennzeichen, das jeden Wert in den Beispieltextdaten in unterschiedliche Spalten trennt. Die korrekte Identifizierung und Anwendung dieses Trennzeichens ist wichtig, um eine genaue Feldzuordnung und eine erfolgreiche Datenerfassung sicherzustellen.

    Hinweis:
    Für CSV-Feeds ist das Komma (,) das Standardtrennzeichen, und für JSON-Feeds ist kein Trennzeichen erforderlich.

13. Wählen Sie Aus **Trennzeichen aktualisieren** .
Die Optionen zum Hinzufügen von Feldern für die Feldzuordnung werden angezeigt.
14. Fahren Sie mit dem Hinzufügen der Feldzuordnung fort, indem Sie die entsprechenden Werte aus der Dropdown-Liste auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



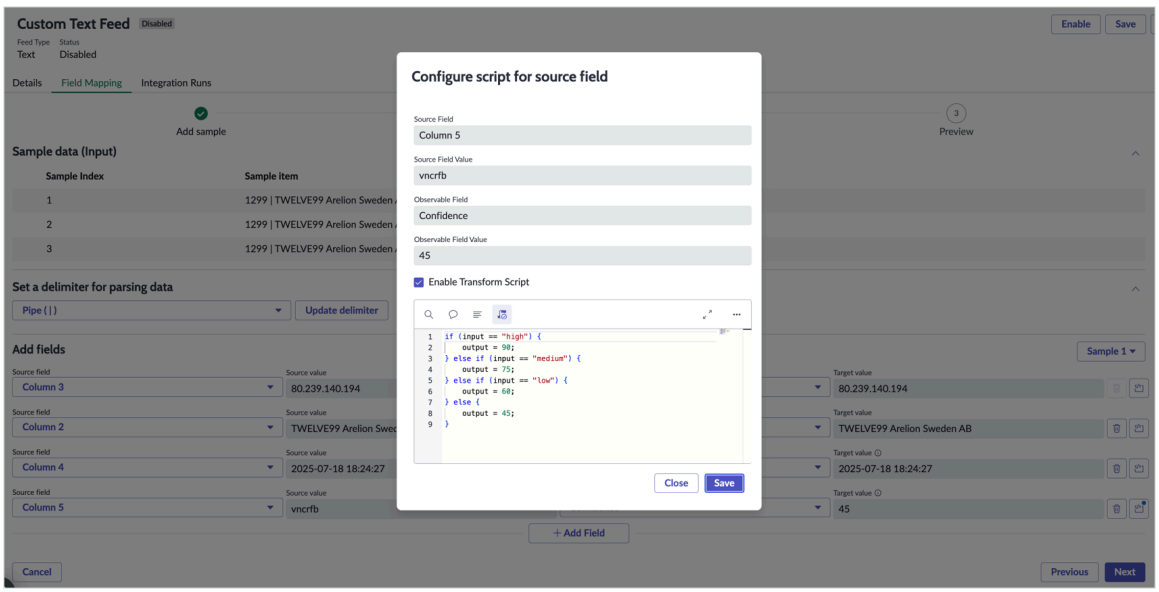
15. Verwenden Sie **Transformationsskript** Um die Eingabewerte zu transformieren und zu normalisieren, bevor sie erkennbaren Elementen zugeordnet werden.

a. Wählen Sie Aus **Transformationsskript aktivieren/deaktivieren** Symbol zum Konfigurieren des Skripts.
Das Dialogfeld Skript für Quellfeld konfigurieren wird angezeigt.

b. Wählen Sie Aus **Aktivieren Sie Das Transformationsskript** Kontrollkästchen auf der **Konfigurieren Sie das Skript für das Quellfeld** Dialogfeld.

c. Fügen Sie das Skript hinzu, oder ändern Sie es.

Wenn Ihr Eingabefeld beispielsweise Werte wie Niedrig, Mittel oder hoch enthält und Sie diese Werte numerischen Konfidenzniveaus (zwischen 0 und 100) zuordnen möchten, können Sie den Eingabewert mithilfe des Transformationsskripts konvertieren und dem zuordnen **Vertrauen** Feld des erkennbaren Elements.



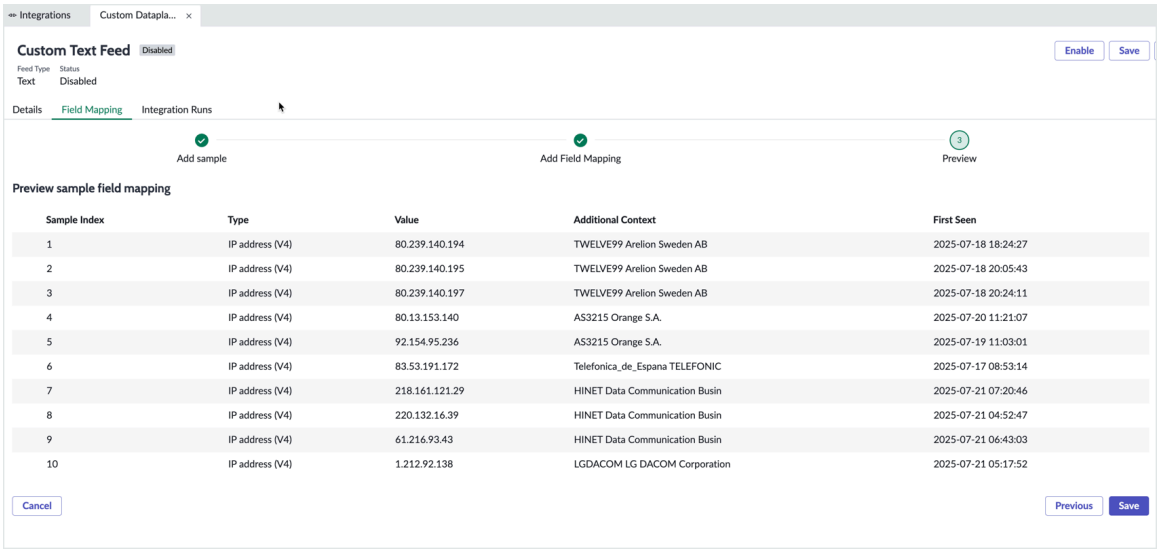
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wählen Sie Aus **Speichern** Zum Speichern des Skripts, um den aktualisierten Zielwert abzurufen.

e. Schließen **Konfigurieren Sie das Skript für das Quellfeld** Dialogfeld, und fahren Sie mit dem nächsten Schritt fort.

16. Wählen Sie Aus **Als Nächstes** Um mit der Vorschau der Feldzuordnungen in der fortzufahren **Vorschau** Abschnitt.



17. Zeigen Sie eine Vorschau der Beispielfeldzuordnung an, und wählen Sie aus **Speichern** .
Eine Bestätigungsnachricht wird angezeigt, die angibt, dass die Feldzuordnung erfolgreich gespeichert wurde.

Im Rahmen der Beispielfeldzuordnung identifiziert die Anwendung automatisch den Typ des erkennbaren Elements (z. B. IP-Adresse v4 usw.), den der Anwender aus den Beispieldaten zugeordnet hat. Dieser Mechanismus optimiert den Zuordnungsprozess und stellt sicher, dass die entsprechenden erkennbaren Typen basierend auf der Eingabe zugewiesen werden.

Wichtig:
Feldzuordnungs-Integrationsausführung: Jede Integrationsausführung, die für diesen Feed-Typ ausgeführt wird, verwendet die gespeicherte Feldzuordnungskonfiguration. Dadurch wird sichergestellt, dass eingehende Daten konsistent analysiert und den richtigen Attributen erkennbarer Elemente basierend auf der während der Konfiguration definierten Struktur zugeordnet werden.

Hinweis:
Wählen Sie Aus **Bearbeiten Sie Die Feldzuordnung** Dient zum Bearbeiten und Vornehmen der erforderlichen Änderungen an der Feldzuordnung, falls erforderlich. Eine Warnmeldung wird angezeigt, um zu bestätigen, ob Sie mit der Bearbeitung fortfahren möchten. Bestätigen Sie die Eingabeaufforderung, und wählen Sie aus **Ja** Um fortzufahren. Nehmen Sie die erforderlichen Änderungen an den Feldzuordnungen anhand der aktualisierten Beispieldaten vor, und speichern Sie die Änderungen.

Alle an der Feldzuordnung vorgenommenen Änderungen werden auf die zukünftigen Integrationsausführungen für diesen Feed angewendet.

Überprüfen Sie die Beispieldaten nach Änderungen immer, um eine korrekte Analyse sicherzustellen, bevor Sie die Integration ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intel-Feeds Anzeigen

Dieser Abschnitt enthält die bedrohungsinformationen-Feeds, die im Basissystem konfiguriert sind.

Zeigen Sie STIX TAXII-Feeds an

Zeigen Sie die konfigurierten STIX TAXII-Feeds im Basissystem an.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** Symbol.
3. Wählen Sie Aus **STIX-TAXII** .
   Die MISP-Feeds im Basissystem sind in der folgenden Tabelle beschrieben.

Bedrohungs-Feed	Beschreibung	URL
Cyware-TAXII	Cyware Threat Intelligence Exchange (CTIX) ist eine Plattform, die die gemeinsame Nutzung von Cyberbedrohungsinformationen zwischen Organisationen erleichtert.	https://threatfeed.cyware.com/ctixapi/ctix21/
RecordedFuture-TAXII	„Recorded Future“ ist eine unabhängige Threat Intelligence-Cloud-Plattform, die es Unternehmen ermöglicht, Bedrohungen in Cyber-, Lieferketten-, physischen und Betrugsdomänen zu identifizieren und zu mindern.	https://api.recordedfuture.com/taxii2
Pulsedive-TAXII	Pulsedive ist eine Threat Intelligence-Plattform, die eine breite Palette von Cyberbedrohungsservices und -Tools für Organisationen bereitstellt.	https://pulsedive.com/taxii2/api/

4. Klicken Sie Auf **Bearbeiten** Zum Bearbeiten des Feeds.

Zeigen Sie STIX HTTPS-Feeds an

Zeigen Sie die konfigurierten STIX HTTPS-Feeds im Basissystem an.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** Symbol.
3. Wählen Sie Aus **STIX-HTTPS** .
   Die folgende Tabelle beschreibt die STIX HTTPS-Feeds im Basissystem.

ThreatFeed	Beschreibung	URL
MITRE: MOBILE ATT&CK	Diese Datensammlung enthält STIX-Objekte aus Mobile ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/mobile-attack/mobile-attack.json
MITRE: ICS ATT&CK	Diese Datensammlung enthält STIX-Objekte aus ICs ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/ics-attack/ics-attack.json
MITRE: ENTERPRISE ATT&CK	Diese Datensammlung enthält STIX-Objekte aus Enterprise ATT&CK.	https://raw.githubusercontent.com/mitre/cti/master/enterprise-attack/enterprise-attack.json

4. Klicken Sie Auf **Bearbeiten** Um den Feed zu bearbeiten und die erforderlichen Aktualisierungen vorzunehmen.

Zeigen Sie MISP-Feeds an

Zeigen Sie die MISP-Feeds an, die im Basissystem konfiguriert sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** Symbol.
3. Wählen Sie Aus **MISP** .
   Die MISP-Feeds im Basissystem sind in der folgenden Tabelle beschrieben.

Bedrohungs-Feed	Beschreibung	URL
DigitalSide Threat Intel OSINT-Feed	Datenquelle zum Abrufen von Open Source Cyber Threat Intelligence-Informationen aus dem DigitalSide Threat-Intel OSINT-Feed, der hauptsächlich auf Malware-Analysen und gefährdeten URLs, IPs und Domänen basiert.	https://osint.digitalside.it/Threat-Intel/digitalside-misp-feed/manifest.json
URLhaus-IOCs	URLhaus ist ein Projekt aus dem Jahr abuse.ch mit dem Ziel, schädliche URLs freizugeben, die für die Malware-Verteilung verwendet werden.	https://urlhaus.abuse.ch/downloads/misp/manifest.json

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungs-Feed	Beschreibung	URL
Malware-Basar	MalwareBazaar ist ein Projekt aus dem Jahr abuse.ch mit dem Ziel, Malware-Beispiele für die Infosec-Community, AV-Lieferanten und Threat Intelligence-Anbieter freizugeben.	https://bazaar.abuse.ch/downloads/misp/manifest.json
ThreatFox-IOCs	ThreatFox ist eine kostenlose Plattform von abuse.ch mit dem Ziel, Indikatoren der Gefährdung (IOCs) im Zusammenhang mit Malware für die Infosec-Community, AV-Lieferanten und Threat Intelligence-Anbieter freizugeben.	https://threatfox.abuse.ch/downloads/misp/manifest.json

Hinweis:
Für MISP-Feed-Typen die REST-Endpunkt-URLs, die mit enden `/Manifest.JSON` Werden unterstützt.

4. Klicken Sie Auf **Bearbeiten** Zum Bearbeiten des Feeds.

Zeigen Sie Textfeeds An

Zeigen Sie die Textfeeds an, die im Basissystem konfiguriert sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** Symbol.
3. Wählen Sie Aus **Text** Option.
   Im Folgenden werden die konfigurierten Text-Feeds im Basissystem aufgelistet.

Bedrohungs-Feed	Beschreibung	URL
Haley's Brute Force-IPs	Stellt eine Liste der IP-Adressen des Angreifers in den letzten 2 Jahren bereit, sortiert nach IP-Adresse	http://charles.the-haleys.org/ssh_dico_attack_hdeny_format.php/hostsdeny.txt
Blockrules-Auslösebedrohungen	Emerging Threat Intelligence (ET) bietet umsetzbare bedrohungsinformationen-Feeds, um IPs zu identifizieren, die an verdächtigen und böswilligen Aktivitäten beteiligt sind.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Nuug Pop3 Groper Web	Liste der Hosts, die versucht haben, sich bei dem pop3-Service unter bsdly.net anzumelden.	https://home.nuug.no/%7Epeter/pop3gropers.txt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungs-Feed	Beschreibung	URL
Tor-Austrittsknoten	Tor-Austrittsknoten können verwendet werden, um Datenverkehr zu erkennen, der aus dem Tor-Netzwerk kommt.	https://www.dan.me.uk/torlist/?exit
Schwarze Liste für Talos Intelligence-IP	Talos wurde durch die Kombination des Vulnerability Research-Teams von Sourcefire, der Cisco Threat Research and Communications-Gruppe und der Cisco Secure Applications-Gruppe gegründet. Das kombinierte Know-how wird durch eine ausgeklügelte Infrastruktur und die konkurrenzlose Datentelemetrie von Cisco unterstützt, die sich über Netzwerke, Endpunkte, Cloud-Umgebungen, virtuelle Systeme sowie den täglichen Web- und E-Mail-Datenverkehr erstreckt.	https://www.talosintelligence.com/documents/ip-blacklist
SANS	ISC bietet Tausenden von Internetanwendern und -Organisationen einen kostenlosen Analyse- und Warnungsservice.	https://isc.sans.edu/feeds/topips.txt
Schnaubend	Snort ist das weltweit führende Open Source Intrusion Prevention System (IPS). Snort-IPS verwendet eine Reihe von Regeln, mit denen schädliche Netzwerkaktivitäten definiert werden können.	https://snort.org/downloads/ip-block-list
CI-Armee	Die Liste der CINS-Armee ist eine Teilmenge des CINS Active Threat Intelligence-Regelsatzes und besteht aus IP-Adressen, die eines von zwei grundlegenden Kriterien erfüllen: 1) der Punktzahlfaktor für aktuelle Rogue-Pakete der IP ist sehr schlecht, oder 2) die IP hat eine bestimmte Anzahl von „vertrauenswürdigen“ Warnungen für eine bestimmte Anzahl ihrer weltweit bereitgestellten Sentinels ausgelöst.	https://cinsscore.com/list/ci-badguys.txt
Proofpoint	Roh-IPs für die Firewall-Blocklisten. Diese stammen von: Von Spamhaus identifizierte Spam-Netze (www.spamhaus.org), Top-Angreifer gelistet von DShield (www.dshield.org) und Abuse.ch	https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungs-Feed	Beschreibung	URL
Blockliste Greensnow	GreenSnow ist ein Team, das aus den besten Spezialisten für Computersicherheit besteht. GreenSnow sammelt eine große Anzahl von IPs von verschiedenen Computern auf der ganzen Welt.GreenSnow ist für Angriffe jeglicher Art mit Ausnahme von Spam vergleichbar mit SpamHaus.org.	https://blocklist.greensnow.co/greensnow.txt
CI-Armee	Die Liste der CINS-Armee ist eine Teilmenge des CINS Active Threat Intelligence-Regelsatzes und besteht aus IP-Adressen, die eines von zwei grundlegenden Kriterien erfüllen: 1) der Punktzahlfaktor für aktuelle Rogue-Pakete der IP ist sehr schlecht, oder 2) die IP hat eine bestimmte Anzahl von „vertrauenswürdigen“ Warnungen für eine bestimmte Anzahl ihrer weltweit bereitgestellten Sentinels ausgelöst.	https://cinsscore.com/list/ci-badguys.txt
Blockliste	www.blocklist.de ist ein kostenloser und freiwilliger Service, der von einem Betrugs-/Missbrauchsspezialisten bereitgestellt wird, dessen Server häufig über SSH-, Mail-Login-, FTP-, Webserver- und andere Services angegriffen werden.	https://lists.blocklist.de/lists/all.txt
Tor-Austrittsknoten	Tor-Austrittsknoten können verwendet werden, um Datenverkehr zu erkennen, der aus dem Tor-Netzwerk kommt.	https://www.dan.me.uk/torlist/?exit
Botscout-BOT-IPs	BotScout hilft, zu verhindern, dass automatisierte Webskripts, sogenannte „Bots“, sich in Foren registrieren, Datenbanken verschmutzen, Spam verbreiten und Formulare auf Websites missbrauchen.	http://botscout.com/last_caught_cache.txt
Dataplane-VNC RFB	IP-Adressen, die als Initiierung von VNC-Remote-Frame-Puffersitzungen identifiziert wurden.	https://dataplane.org/signals/vncrfb.txt
Dataplane-TELNET-Anmeldung	IP-Adressen, die als Anmeldeversuch über TELNET-Passwortauthentifizierung identifiziert wurden.	https://dataplane.org/signals/telnetlogin.txt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungs-Feed	Beschreibung	URL
SSH-Passwortauthentifizierung für Dataplane	IP-Adressen, die als Anmeldeversuch über SSH-Passwortauthentifizierung identifiziert wurden.	https://dataplane.org/signals/sshpwauth.txt
Dataplane-SSH-Clientverbindung	IP-Adressen, die als Durchführen von SSH-Clientprotokollverhandlungen identifiziert wurden.	https://dataplane.org/signals/sshclient.txt
Blockrules-Auslösebedrohungen	Emerging Threat Intelligence (ET) bietet umsetzbare bedrohungsinformationen-Feeds, um IPs zu identifizieren, die an verdächtigen und böswilligen Aktivitäten beteiligt sind.	https://rules.emergingthreats.net/blockrules/compromised-ips.txt
Dataplane-SMTP-Begrüßung	IP-Adressen, die als SMTP-Clients identifiziert werden, die nicht angeforderte HELO- oder EHLO-Befehle ausgeben.	https://dataplane.org/signals/smtpgreet.txt
Dataplane-SIP-Abfrage	IP-Adressen, die als SIP-OPTIONSABFRAGEN gesendet werden.	https://dataplane.org/signals/sipquery.txt
Dataplane-IP-Protokoll 41	IP-Adressen, die als Relais „offenes IPv4-Protokoll 41 identifiziert wurden (z. B. IPv6 über IPv4).	https://dataplane.org/signals/proto41.txt
Dataplane-SIP-Einladung	IP-Adressen, die als Vorgänge zum Senden von SIP-EINLADUNGEN identifiziert wurden.	https://dataplane.org/signals/sipinvitation.txt
Dataplane-DNS CH TXT Version.Bind	IP-Adressen, die als sendende DNS CH TXT-VERSION.BIND-Abfragen identifiziert werden.	https://dataplane.org/signals/dnsversion.txt
Dataplane-DNS-TCP	IP-Adressen, die als DNS-Abfragen über TCP-Port 53 gesendet werden.	https://dataplane.org/signals/dnstcp.txt
Dataplane-DNS-Rekursion IN BELIEBIGER erwünscht	IP-Adressen, die IN ALLEN Abfragen als rekursives DNS gesendet werden.	https://dataplane.org/signals/dnsrdany.txt
Dataplane-DNS-Rekursion gewünscht	IP-Adressen, die als rekursive DNS-Abfragen gesendet werden.	https://dataplane.org/signals/dnsrd.txt
Phishing-Datenbank aus GitHub Active Phishing Links	Datenquelle zum Abrufen aktiver Phishing-Links aus der Phishing-Datenbank, die auf Github verfügbar ist.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-links-ACTIVE.txt
Phishing-Datenbank aus aktiven GitHub-Domänen	Datenquelle zum Abrufen aktiver Domänen aus der Phishing-Datenbank, die in Github verfügbar ist.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-domains-ACTIVE.txt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungs-Feed	Beschreibung	URL
Phishing-Datenbank aus GitHub Active IPs	Datenquelle zum Abrufen aktiver IPs aus der Phishing-Datenbank, die auf Github verfügbar ist.	https://raw.githubusercontent.com/mitchellkrogza/Phishing.Database/master/phishing-IPs-ACTIVE.txt
Blocklisten-Bots	Alle IP-Adressen, die in den letzten 48 Stunden als Angriffe auf die RFI-Angriffe, REG-Bots, IRC-Bots oder BadBots gemeldet wurden.	https://lists.blocklist.de/lists/bots.txt
Apache-Angriffe Blockieren	Alle IP-Adressen, die in den letzten 48 Stunden als Angriffe auf den Service Apache, Apache-DDOS, RFI-Angriffe gemeldet wurden.	https://lists.blocklist.de/lists/apache.txt
Voip-Blacklist Von Scopserv	Ruft die Liste der blockierten ips aus der schwarzen VoIP-Liste ab.	http://voipbl.org/update/?dm=bl
Threatview Domain Blocklist (Domänenblockliste Anzeigen)	Schädliche Domänen, die für Phishing/Bereitstellung von Malware/Befehlen und Steuerung identifiziert wurden.	https://threatview.io/Downloads/DOMAIN-High-Confidence-Feed.txt
MD5-Hash-Blockliste anzeigen	MD5-Hashes von schädlichen Dateien oder in Verbindung mit Malware, Ransomware, Hack-Tools, Bots usw.	https://threatview.io/Downloads/MD5-HASH-ALL.txt
Threatview-URL-Blockliste	Schädliche URLs, die Malware, Phishing, Botnets und C2 bereitstellen.	https://threatview.io/Downloads/URL-High-Confidence-Feed.txt
ThreatView SHA-Datei-Hash-Blockliste	SHA-Hashes von Dateien, die bekannt sind oder mit der Malware-Ausführung verknüpft sind.	https://threatview.io/Downloads/SHA-HASH-FEED.txt
ThreatView-IP-Blockliste	Schädliche IP-Blockliste für bekannte fehlerhafte IP-Adressen.	https://threatview.io/Downloads/IP-High-Confidence-Feed.txt
ThreatView C2 Hunt Feed	Infrastruktur-Hosting von Befehls- und Steuerungsservern, die während der proaktiven Jagd von Threatview.io gefunden wurden	https://threatview.io/Downloads/High-Confidence-CobaltStrike-C2%20-Feeds.txt
ThreatView OSINT Threat Feed	Böswillige Kompromittierungsindikatoren, die aus der OSINT-Quelle – Twitter und Pastebin erfasst wurden.	https://threatview.io/Downloads/Experimental-IOC-Tweets.txt

4. Klicken Sie Auf **Bearbeiten** Zum Bearbeiten des Feeds.

Zeigen Sie CSV-Feeds an

Zeigen Sie die CSV-Feeds an, die im Basissystem konfiguriert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** Symbol.
3. Wählen Sie Aus **CSV** .
   Die CSV-Feeds im Basissystem werden in der folgenden Tabelle erläutert.

ThreatFeed	Beschreibung	URL
Phishstatistiken	Phishing-URLs aus den letzten 30 Tagen aus PhishStats.	https://phishstats.info/phish_score.csv
Schwarze Liste des SSL-Zertifikats für Abuse.ch	Die SSL Certificate Blacklist (CSV) ist eine CSV, die SHA1-Fingerabdrücke aller SSL-Zertifikate enthält, die auf SSLBL auf die schwarze Liste gesetzt sind.	https://sslbl.abuse.ch/blacklist/sslblacklist.csv
Schwarze Botnet-C2-IP-Liste	Ein SSL-Zertifikat kann einem oder mehreren Servern zugeordnet werden (IP-Adresse:Port-Kombination). SSLBL erfasst IP-Adressen, die mit einem SSL-Zertifikat auf der schwarzen Liste in SSLBL ausgeführt werden. Dies sind normalerweise Botnet Command&Control-Server (C&C). SSLBL veröffentlicht daher eine schwarze Liste mit diesen IPs, die verwendet werden kann, um Botnet C2-Datenverkehr von infizierten Computern in Richtung Internet zu erkennen und Ihr Netzwerk zu verlassen.	https://sslbl.abuse.ch/blacklist/sslipblacklist.csv
PhishTank online	NA	https://data.phishtank.com/data/online-valid.csv

4. Klicken Sie Auf **Bearbeiten** Zum Bearbeiten des Feeds.

Zeigen Sie JSON-Feeds an

Zeigen Sie die im Basissystem konfigurierten JSON-Feeds an.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** Symbol.
3. Wählen Sie Aus **JSON** Option.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Folgenden werden die konfigurierten JSON-Feeds im Basissystem aufgelistet.

Bedrohungs-Feed	Beschreibung	URL
Feodotracker-C&C-Hosts	Datenquelle zum Abrufen der Botnet C2-IP-Blockliste aus Feodotracker	https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.json
Feodotracker	Datenquelle zum Abrufen der Botnet C2-IP-Blockliste aus Feodotracker	https://feodotracker.abuse.ch/downloads/ipblocklist.json

4. Klicken Sie Auf **Bearbeiten** Zum Bearbeiten des Feeds.

Zeigen Sie RSS-Feeds an

Zeigen Sie die im Basissystem konfigurierten RSS-Feeds an.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** Symbol.
3. Wählen Sie Aus **RSS** Option.
   Im Folgenden werden die konfigurierten RSS-Feeds im Basissystem aufgelistet.

Bedrohungs-Feed	Beschreibung	URL
CISO2CISO.COM RSS-Feed	RSS-Feed-Daten aus CISO2CISO.com	https://ciso2ciso.com/feed/
Schneier im Sicherheits-RSS-Feed	RSS-Feed-Daten aus Schneier für Sicherheit	https://www.schneier.com/feed/atom/
Krebs im Sicherheits-RSS-Feed	RSS-Feed-Daten aus KerbsonSecurity	https://krebsonsecurity.com/feed/
Wir Live-Sicherheits-RSS-Feed	RSS-Feed-Daten aus welivesecurity	http://feeds.feedburner.com/eset/blog
JISA-Softech-RSS-Feed	RSS-Feed-Daten aus JISA	https://www.jisasoftech.com/feed/
Cisco Newsroom Security RSS-Feed	Aktuelle Sicherheitsnachrichten von cisco.	https://newsroom.cisco.com/c/services/i/servlets/newsroom/rssfeed.json?feed=security
HelpNet-Sicherheit	Informationssicherheitsnachrichten mit Schwerpunkt auf Unternehmenssicherheit.	https://www.helpnetsecurity.com/feed/
Sicherheitsangelegenheiten	Informationen zur digitalen Forensik aus erstklassigen Medien.	https://securityaffairs.com/feed

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungs-Feed	Beschreibung	URL
Volexity-RSS-Feed	RSS-Feed-Daten von Informationssicherheits-Blogs aus Volexity.	https://www.volexity.com/blog/feed/
Hacker-Nachrichten-RSS-Feed	RSS-Feed-Daten aus „The Hacker News	https://feeds.feedburner.com/TheHackersNews?format=xml
Graham-Cluley-RSS-Feed	RSS-Feed-Daten aus Graham Cluley	https://grahamcluley.com/feed/

4. Klicken Sie Auf **Bearbeiten** Zum Bearbeiten des Feeds.

Zeigen Sie Anwenderdefinierten Feed An

Zeigen Sie den anwenderdefinierten Feed an, der im Basissystem geliefert wird.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** Symbol.
3. Wählen Sie Aus **Anwenderdefiniert** .
   In der folgenden Tabelle ist der vordefinierte anwenderdefinierte Feed aufgeführt.

ThreatFeed	Beschreibung	URL
CrowdStrike-Feed	Quelle zum Abrufen von Daten zu CrowdStrike-Akteuren, erkennbaren Elementen und Berichten.	https://api.crowdstrike.com

4. Klicken Sie Auf **Bearbeiten** Zum Bearbeiten des Feeds.

Premium-Bedrohungs-Feed für CrowdStrike anzeigen

Mit dem CrowdStrike-Feed können Anwender Indikatoren, Akteure, Berichte und den zugehörigen Kontext aus dem CrowdStrike Falcon Intelligence-Feed in erfassen TISC.

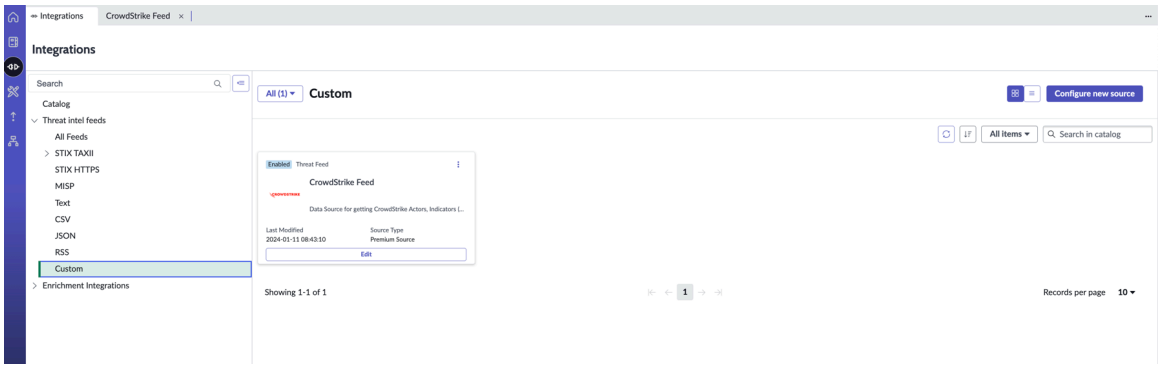
Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen**an.
2. Wählen Sie Aus **Anwenderdefiniert** .
3. Klicken Sie auf **Bearbeiten** Schaltfläche von *`CrowdStrike`***Feed** Formularseite.

Hinweis:
Standardmäßig ist der CrowdStrike-Feed deaktiviert. Sie müssen die Konfigurationen bearbeiten, um den Feed zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Führen Sie einen Drilldown zu **Konfigurationsdetails** Abschnitt.
5. Geben Sie ein **Client-ID** , Und **Geheimer Client-Schlüssel** .

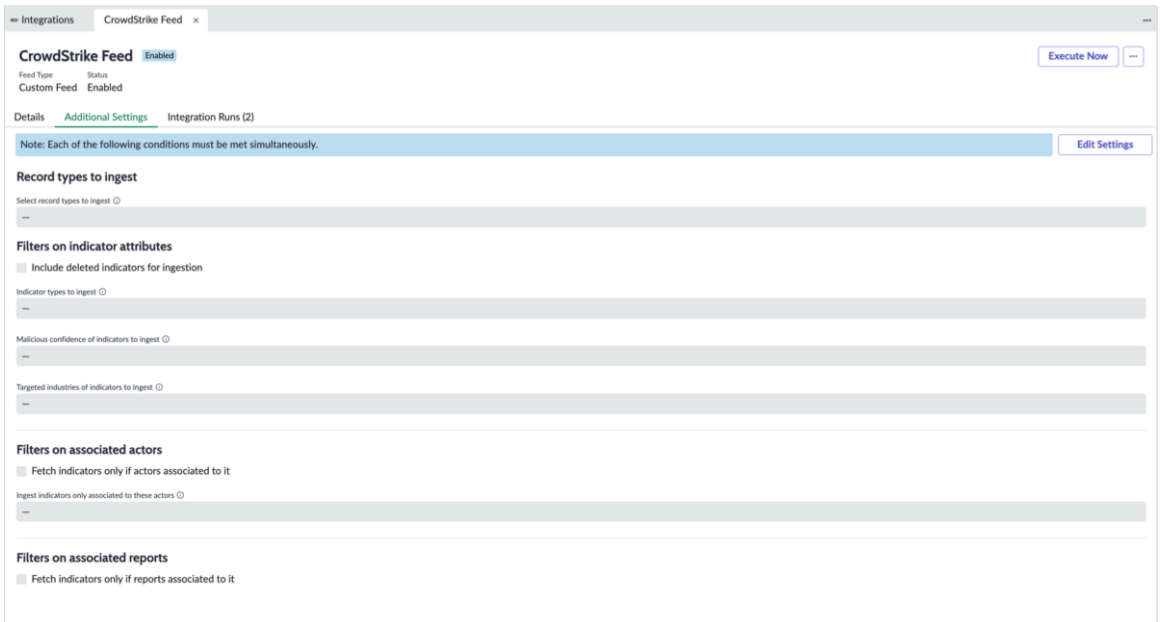
Hinweis:

a. Sie müssen Ihre Client-ID und das geheime Clientgeheimnis generieren, falls Sie es nicht haben. Weitere Informationen zur Client-ID und zum geheimen Client finden Sie unter Definieren Sie Ihren ersten API-Client Abschnitt.

b. Client-ID und geheimer Client-Schlüssel von abrufen `CrowdStrike`Für erforderliche Bereiche. Nachfolgend finden Sie die Bereiche, die für die Client-ID und das geheime Clientgeheimnis von erforderlich sind `CrowdStrike`:

- Indikatoren (Falcon Intelligence)
- Akteure (Falcon Intelligence)
- Berichte (Falcon Intelligence)

6. Navigieren Sie zu **Zusätzliche Einstellungen** Zum Konfigurieren der Filter, die beim Erfassen von Indikatoren aus angewendet werden CrowdStrike.



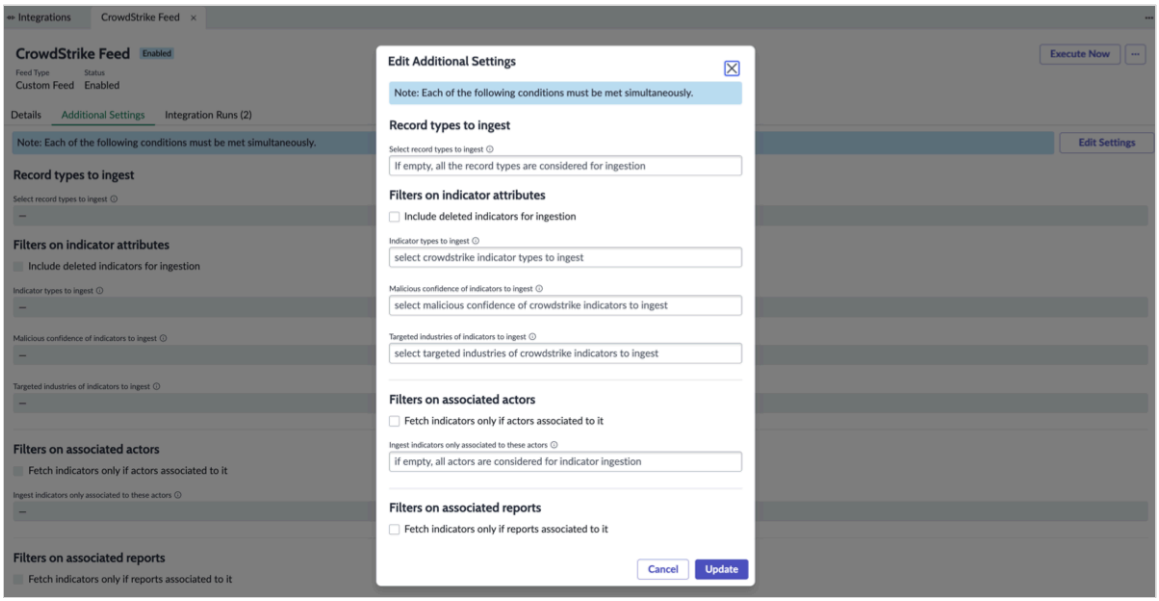
Die **Zusätzliche Einstellungen** Die Registerkarte wird hauptsächlich verwendet, um die Filter zu konfigurieren, die steuern, wie Daten in die Anwendung aufgenommen werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit diesen Filtern können Sie den Datenintegrationsprozess an Ihre spezifischen Anforderungen anpassen und sicherstellen, dass nur die relevantesten Informationen enthalten sind.

7. Klicken Sie Auf **Bearbeiten Sie Die Einstellungen** .



8. Wählen Sie die erforderlichen Filter aus.

> **Hinweis:**
> Alle konfigurierten Filter werden beim Erfassen von Indikatoren aus in Verbindung angewendet CrowdStrike.

Der folgende Abschnitt enthält eine detaillierte Erklärung der einzelnen verfügbaren Optionen. Überprüfen Sie jede Option in der folgenden Tabelle, um zu verstehen, wie die Filter angewendet werden können, um die in die Anwendung erfassten Daten zu optimieren.

9. Wählen Sie die erforderlichen Werte aus den folgenden verfügbaren Filtern aus.

Zusätzliche Einstellungen bearbeiten

Feld	Beschreibung
Zu erfassende Datensatztypen	
Wählen Sie Datensatztypen aus, die erfasst werden sollen	Wählen Sie die Datensatztypen aus, die Sie erfassen möchten. Die verfügbaren Datensatztypen sind Indikatoren, Berichte und Akteure.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn Sie nur auswählen **Indikatoren** Als Datensatztyp, der erfasst werden soll, werden die zugehörigen Berichte und Akteure, die diesen Indikatoren zugeordnet sind, nicht automatisch erfasst. Um die zugehörigen Berichte und Akteure zu erfassen, müssen Sie alle drei Datensatztypen auswählen: Indikatoren, Berichte und Akteure.
Filtert nach Indikatorattributen	
Gelöschte Indikatoren für die Erfassung einschließen	Aktivieren Sie dieses Kontrollkästchen, um die Erfassung von Indikatoren zu ermöglichen, die gelöscht wurden. **Hinweis:** Gelöschte Indikatoren werden nur dann als erkennbare Elemente erstellt, wenn sie zuvor erfasst wurden. A **In CrowdStrike gelöscht** Das Tag wird Indikatoren hinzugefügt, die aus entfernt werden CrowdStrike.
Zu erfassende Indikatortypen	Wählen Sie die spezifische aus CrowdStrike Indikatortypen, die Sie erfassen möchten. Wenn keine ausgewählt ist, werden standardmäßig alle verfügbaren Indikatoren abgerufen.
Böswillige Konfidenz der zu erfassenden Indikatoren	Wählen Sie die böswillige Vertrauensstufe von aus CrowdStrike Zu erfassende Indikatoren. Wenn leer gelassen, werden alle Indikatoren aus abgerufen CrowdStrike Unabhängig von ihrem böswilligen Vertrauen.
Zielbranchen von zu erfassenden Indikatoren	Wählen Sie die Zielbranchen aus, die zugeordnet sind CrowdStrike Zu erfassende Indikatoren. Wenn keine ausgewählt ist, werden alle Indikatoren aus abgerufen CrowdStrike Unabhängig von der Zielbranche.
Filtert nach zugeordneten Akteuren	
Indikatoren nur abrufen, wenn Akteure ihm zugeordnet sind	Aktivieren Sie dieses Kontrollkästchen, um Indikatoren nur abzurufen, wenn sie Akteuren zugeordnet sind.
Erfassen Sie nur Indikatoren, die diesen Akteuren zugeordnet sind	Geben Sie kommagetrennte Akteurnamen für die Indikatoren für die Erfassung an. Wenn nicht angegeben, werden alle Indikatoren aus abgerufen CrowdStrike Unabhängig von zugeordneten Akteuren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Filtert zugeordnete Berichte	
Indikatoren nur abrufen, wenn ihnen Berichte zugeordnet sind	Aktivieren Sie dieses Kontrollkästchen, um Indikatoren nur abzurufen, wenn sie Berichten zugeordnet sind.
Erfassen Sie nur Indikatoren, die diesen Berichten zugeordnet sind	Geben Sie kommagetrennte Berichtsnamen ein, die den Indikatoren für die Erfassung zugeordnet sind. Wenn leer gelassen, werden alle Berichte in den Erfassungsprozess einbezogen. Wenn nicht angegeben, werden alle Indikatoren aus abgerufen CrowdStrike Unabhängig von zugeordneten Berichten.
Filtert nach zugehörigen Malware-Familien	
Rufen Sie Indikatoren nur ab, wenn Malware-Familien damit verknüpft sind	Aktivieren Sie dieses Kontrollkästchen, um Indikatoren nur abzurufen, wenn sie Malware-Familien zugeordnet sind.
Erfasst nur Indikatoren, die diesen Malware-Familien zugeordnet sind	Geben Sie kommagetrennte Malware-Familiennamen ein, die den Indikatoren für die Erfassung zugeordnet sind. Wenn leer gelassen, werden alle Malware-Familien in den Erfassungsprozess einbezogen. Wenn nicht angegeben, werden alle Indikatoren aus abgerufen CrowdStrike Unabhängig von Malware-Familien.
Zuordnung der böswilligen Konfidenz des Indikators zu TISC-Konfidenz **Hinweis:** Die Werte „hoch“, „Mittel“ und „Niedrig“ sind der Quellwert oder das schädliche Vertrauen, das von empfangen wurde CrowdStrike.	
Hoch	Geben Sie einen Konfidenzwert (0–100) für Indikatoren mit hoher böswilliger Konfidenz ein. **Hinweis:** Wenn eine übereinstimmende schädliche Konfidenzzuordnung in gefunden wird **Zusätzliche Einstellungen** , Überschreibt den in angegebenen Wert **Details** Abschnitt, auch wenn ein Konfidenzwert manuell eingegeben wird.
Mittel	Geben Sie einen Konfidenzwert (0–100) für Indikatoren mit mittlerer böswilliger Konfidenz ein.
Niedrig	Geben Sie einen Konfidenzwert (0–100) für Indikatoren mit geringer böswilliger Konfidenz ein.
Nicht verifiziert	Geben Sie einen Konfidenzwert (0–100) für Indikatoren mit nicht verifizierter böswilliger Konfidenz ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Mit denselben zusätzlichen Einstellungen, die Sie oben definiert haben, können Sie den Feed beim Erstellen eines neuen Feeds duplizieren.

10. Klicken Sie Auf **Aktualisieren** Auf der **Zusätzliche Einstellungen** Dialogfeld zum Speichern der geänderten zusätzlichen Einstellungen.
11. Klicken Sie Auf **Aktivieren** Zum Aktivieren CrowdStrike Feed für Erfassung.

Hinweis:
Der Premium-Feed ist mit anderen Feeds identisch, mit Ausnahme der Antwort, die während der Konfiguration analysiert wird. Eine bestimmte Antwort wird analysiert CrowdStrike Durch Hinzufügen der Client-ID und des geheimen Clientschlüssels.

Welche Art von Daten abgerufen werden `CrowdStrike`:

a. Indikatoren von CrowdStrike Die nach der konfigurierten Erfassungszeit aktualisiert werden und den Filtern entsprechen, die als Teil zusätzlicher Einstellungen konfiguriert sind. Diese Indikatoren von CrowdStrike Wird dann erkennbaren Elementen in zugeordnet TISC. Nachfolgend finden Sie die Indikatortypen, die in erfasst werden TISC:
   - SHA256-Hash
   - MD5-Hash
   - SHA1-Hash
   - URL
   - Domäne
   - IP-Adresse
   - Mutex-Name
   - Dateiname
   - E-Mail-Adresse
   - Anwendername
   - IP-Adressblock

b. Bedrohungsakteure von CrowdStrike Die nach der konfigurierten Erfassungszeit aktualisiert werden, werden Bedrohungsakteuren in zugeordnet TISC.

c. Berichte von CrowdStrike Die nach der konfigurierten Erfassungszeit aktualisiert werden, werden Bedrohungsberichten in zugeordnet TISC Basierend auf den übereinstimmenden Attributen.

d. Zusätzlich zu den oben genannten Entitäten werden auch die folgenden zugehörigen Daten abgerufen:
   i. Bedrohungsakteure, Berichte und Indikatoren im Zusammenhang mit den zuvor erfassten Indikatoren.
   ii. Bedrohungsakteure und -Indikatoren, die allen während des aktuellen Erfassungsprozesses erfassten Berichten zugeordnet sind.

Hinweis:
In konfigurierte Filter **Zusätzliche Einstellungen** Wird auch angewendet, wenn die Indikatoren erfasst werden, die den zuvor erfassten Indikatoren, Berichten oder Akteuren zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. **Wahlweise:** Klicken Sie Auf **Duplikat** Um den Feed zu duplizieren.
    Weitere Informationen finden Sie unter Doppelte Threat Intelligence-Feeds.

Systemeigenschaften für CrowdStrike

Im Folgenden werden die Systemeigenschaften für CrowdStrike beschrieben.

1. sn_sec_tisc.crowdstrike_actor_Batch_size: Gibt die Anzahl der Akteure an, die in einem einzelnen API-Aufruf abgerufen werden sollen. Hinweis: Gilt nur, wenn die Integration die erforderlichen nicht im System findet.
   - Typ: Ganzzahl
   - Wert: 250
2. sn_sec_tisc.crowdstrike_api_limit: Anzahl der Datensätze, die gleichzeitig von CrowdStrike abgerufen werden sollen. Je höher die Zahl, desto mehr Arbeitsspeicher würde für die Verarbeitung der Nutzlast verbraucht.
   - Typ: Ganzzahl
   - Wert: 1000
3. sn_sec_tisc.crowdstrike_indicator_Batch_size: Gibt die Anzahl der Indikatoren an, die in einem einzelnen API-Aufruf abgerufen werden sollen. Hinweis: Gilt nur, wenn die Integration die erforderlichen nicht im System findet.
   - Typ: Ganzzahl
   - Wert: 150
4. sn_sec_tisc.crowdstrike_Offset_limit_total: Die zulässige Summe von Offset und Grenzwert aus der CrowdStrike-API.
   - Typ: Ganzzahl
   - Wert: 50000
5. sn_sec_tisc.crowdstrike_Report_Batch_size: Gibt die Anzahl der Berichte an, die in einem einzelnen API-Aufruf abgerufen werden sollen. Hinweis: Gilt nur, wenn die Integration die erforderlichen nicht im System findet.
   - Typ: Ganzzahl
   - Wert: 50

STIX TAXII verstehen

Structured Threat Information Expression (STEX) ist eine Sprache und ein Serialisierungsformat, die zum Austausch von Cyberbedrohungsinformationen (Cyber Threat Intelligence, CTI) verwendet werden. Trusted Automated Exchange of Intelligence Information (TAXII) ist ein Protokoll, das zum Austausch von Cyber Threat Intelligence (CTI) über HTTPS verwendet wird.

Mit STIX werden alle Aspekte von Verdacht, Kompromittierung und Zuschreibung als Objekte und beschreibende Beziehungen dargestellt. STIX-Informationen können für einen Analysten visuell dargestellt oder als JSON gespeichert werden, um schnell maschinell lesbar zu sein.

Cyber Threat Intelligence (CTI) wurde beauftragt, eine Reihe von Informationsdarstellungen und Protokollen zu definieren, um die Notwendigkeit zu erfüllen, Cyberbedrohungsinformationen zu modellieren, zu analysieren und freizugeben. Der CTI konzentriert sich in erster Linie auf die Entwicklung und Standardisierung von STEX (Structured Threat Information Expression) und TAXII (Trusted Automated Exchange of Indicator Information).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie einen neuen TAXII-Feed

Sie können TAXII-Feeds verwalten, um STIX-formatierte Informationen freizugeben. Jeder TAXII-Feed enthält eine oder mehrere TAXII-Sammlungen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** Symbol.
3. Auswahlvorgang **Bedrohungsinformationsfeeds** > **STIX-TAXII** > **TAXII-Feeds**an.

> **Hinweis:**
> Konfigurieren Sie den TAXII-Feed so, dass er als Profil für alle TAXII-Sammlungen in dient.

4. Klicken Sie Auf **Konfigurieren Sie eine neue Quelle** .
   Die Seite Neuen TAXII-Feed konfigurieren wird angezeigt.
5. Füllen Sie im Formular die Felder aus.

Neue Datenquelle erstellen

Feld	Beschreibung
Name	Geben Sie einen Namen für den Feed ein.
Beschreibung	Beschreibung des Feeds.
Quelltyp	Der Typ der Quelle, z. B. Open Source, Premium Source usw., die für den Feed bereitgestellt wird. Die verfügbaren Quelltypen sind: ○ Regierung ○ ISACs ○ Open Source ○ Premium-Quelle ○ Andere Quelle
Logo	Hängen Sie das Logo des Quell-Feeds an.
Branche	Wählen Sie die Branchenkategorie aus, z. B. Luft- und Raumfahrt, Landwirtschaft usw., für die die Feed-Datenquelle gilt.

Füllen Sie die Felder im Abschnitt Konfiguration entsprechend aus.

Konfiguration

Feld	Beschreibung
TAXII-Version	Wählen Sie die TAXII-Version des TAXII-Servers aus, die konfiguriert werden muss. Unterstützte Versionen sind 2,0 und 2,1.
Konfigurationstyp	Geben Sie einen Konfigurationstyp an, um TAXII-Sammlungen abzurufen. Verfügbare Werte sind:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Discovery-Service-URL** : Wählen Sie die Discovery-Service-URL aus, um Sammlungen aus allen verfügbaren API-Stämmen im Discovery-Service des TAXII-Servers abzurufen. ○ **API-Stamm-URL** : Wählen Sie die API-Stamm-URL aus, um Sammlungen aus dem spezifischen API-Stamm des TAXII-Servers abzurufen.
Authentifizierung	Wählen Sie die erforderliche Option aus der Dropdown-Liste aus, wenn die Authentifizierung erforderlich ist. Verfügbare Optionen: ○ **Keine** : Wählen Sie diese Option aus, wenn keine Authentifizierung erforderlich ist. ○ **Standard** : Wählen Sie diese Option aus, um Anwendername und Passwort anzugeben. ○ **API-Schlüssel** : Wählen Sie diese Option aus, um einen API-Schlüssel bereitzustellen. ○ **Wählen Sie eine REST-Nachricht aus** : Wählen Sie diese Option für einen anderen Authentifizierungstyp aus. Die REST-Nachrichtenoptionen sind: ▪ **REST-Nachricht verwenden** : Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine REST-Nachricht zum Erstellen einer vor-Build-REST-Nachricht benötigen. Wenn Sie nicht auswählen, wird der Wert im Feld „Endpunkt“ verwendet. Klicken Sie auf das Suchsymbol, und wählen Sie die REST-Nachricht aus der Liste aus. ▪ **REST-Methode** : Aktivieren Sie dieses Kontrollkästchen, wenn Sie eine REST-Methode benötigen. Klicken Sie auf das Suchsymbol, und wählen Sie die REST-Methode aus der Liste aus. **Hinweis:** Die Felder REST-Nachricht und REST-Methode werden verfügbar, wenn die Option REST-Nachricht ausgewählt ist.
URL	Geben Sie entweder die URL des TAXII-Server-Discovery-Service oder die spezifische API-Stamm-URL basierend auf dem ausgewählten Konfigurationstyp ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erweiterter Abschnitt	
Erweitert	Aktivieren Sie das Kontrollkästchen, um ein anderes Integrationsskript und einen anderen Berichtsprozessor auszuwählen. Stellen Sie sicher, dass die ausgewählten Skripts mit der ausgewählten TAXII-Version kompatibel sind. Basierend auf der TAXII-Version und -Authentifizierung werden diese Skripts standardmäßig automatisch ausgefüllt.
Integrationsskript	Ruft einen Aufruf der REST-Endpunkt-URL-API mithilfe der Authentifizierungsparameter wie Authentifizierungstyp auf: Anwendername/Passwort/API-Schlüssel und die mit der Anforderung zu übergebenden Header. Dann ruft das Skript die STEX-Daten erkennbarer Elemente oder Indikatoren ab, die für den spezifischen Feed verfügbar sind. **Hinweis:** Die abgerufenen Daten sind nur die Rohdaten (es werden keine Datensätze erstellt), die an den Integrationsprozess angehängt und dann unter angezeigt werden können **Integrationsausführung** Abschnitt. Im Basissystem finden Sie die folgenden anwenderdefinierten Skripteinbindungen, die innerhalb der Anwendung für die Integrationsskripts bereitgestellt werden: ○ TAXIIV2_0QueryParamAPIKeyIntegrationScript ○ TAXIIV2_0BasicAuthIntegrationScript ○ TAXIIV2_1QueryParamAPIKeyIntegrationScript ○ TAXIIV2_1BasicAuthIntegrationScript Das Standardintegrationsskript basiert auf dem von Ihnen ausgewählten Feed-Typ. Das Skript enthält führt einen einfachen REST-Aufruf aus, speichert die Antwort als Anhang und gibt den Anhang dann an den Prozessor zurück.
Berichtsprozessor-Skript	Der Berichtsprozessor ruft einen Aufruf der REST-Endpunkt-URL auf. Im Basissystem finden Sie unten die anwenderdefinierten Skripteinbindungen, die in der Anwendung für die Integrationsskripts bereitgestellt werden. **TAXIIV2CollectionDataProcessor** .

Füllen Sie die Felder im Abschnitt „Zeitplanung“ entsprechend aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeitplanung

Feld	Beschreibung
Ausführungshäufigkeit von Sammlungen	Das Zeitplanungsintervall, das auf die TAXII-Sammlungsdatensätze angewendet wird. Die Ausführungshäufigkeit für eine TAXII-Sammlung kann bei Bedarf in der Formularansicht der TAXII-Sammlung geändert werden. **Hinweis:** Diese Einstellung wird standardmäßig auf alle abgerufenen TAXII-Sammlungen angewendet. Es gibt eine Option, die Einstellung in TAXII-Sammlungen bei Bedarf zu überschreiben. Weitere Informationen finden Sie unter Geplante Aufgaben und wie ein Skript Ihrer Wahl automatisch ausgeführt wird .
Daten abrufen von	Das Startdatum, ab dem die Daten abgerufen werden mussten. Dieses Feld sollte mit der Zeit festgelegt werden, ab der die Daten aus der entsprechenden Quelle erfasst werden müssen. Sobald dieses Feld festgelegt ist, ruft die nächste Erfassungsausführung die Daten aus der konfigurierten Zeit ab, und aufeinanderfolgende Erfassungsausführungen rufen inkrementelle Daten ab. Beispielsweise ist „Quelle“ so geplant, dass die Daten stündlich erfasst werden. Der Anwender legt fest **Daten Von Abrufen** Bis zum 12. Januar 6:00 Uhr am 12. Januar 9:00 Uhr ruft die am 12. Januar 30 ausgelöste Erfassung die Daten vom 12. Januar 6:00 UHR bis 12. Januar 10:00 Uhr ab. Die nächste Erfassung, die um 11:00 Uhr ausgelöst wird, ruft nur die inkrementellen Daten vom 12. Januar 10:00 UHR bis 12. Januar 11:00 Uhr ab. **Hinweis:** Dies bedeutet, dass die geplanten Ausführungen ab dem angegebenen Datum inkrementell Daten abrufen.

6. Klicken Sie Auf **Validieren Sie Die Verbindung**
   Es wird eine Informationsnachricht angezeigt, dass die TAXII-Feed-Verbindung erfolgreich ist. Um die Sammlungen abzurufen, fahren Sie mit dem nächsten Schritt fort.
7. Klicken Sie Auf **TAXII-Sammlungen abrufen** .

Hinweis:
Wenn Fehler auftreten, wird eine Fehlermeldung angezeigt, dass beim Abrufen von TAXII-Sammlungen ein Fehler aufgetreten ist, und überprüfen Sie die Protokolle auf weitere Details.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die TAXII-Sammlungen werden im Abschnitt „TAXII-Sammlungen“ angezeigt und sind standardmäßig deaktiviert.

8. Aktivieren Sie die TAXII-Sammlungen, um die in diesen TAXII-Sammlungen verfügbaren STIX-Objekte abzurufen.

Doppelte Threat Intelligence-Feeds

Durch das Duplizieren eines Bedrohungs-Feeds können Sie eine genaue Kopie eines vorhandenen Feeds erstellen, einschließlich aller zugehörigen erkennbaren Elemente, Indikatoren, Akteure usw.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** Symbol.
3. Wählen Sie die gewünschte Integration aus der aus **Katalog** Anzeigen.
   Wählen Sie beispielsweise aus CrowdStrike
4. Klicken Sie Auf **Bearbeiten** Schaltfläche für CrowdStrike Feed-Karte zum Öffnen des Konfigurationsformulars.
5. Klicken Sie auf **Weitere Aktionen** Menü und wählen Sie aus **Duplikat** .
   Es wird eine Bestätigung angezeigt, dass die aktuelle Feed-Konfiguration dupliziert und einen neuen Feed mit dem Namen [integrationname Feed-copy] mit einem Link zum neuen duplizierten Feed erstellt hat. Beispiel: CrowdStrike-Feed-copy.

TISC-Anreicherungsintegrationen

Die Threat Intelligence-Sicherheitszentrum Das Basissystem enthält keine vorkonfigurierten Integrationen. Dieser Abschnitt enthält Anweisungen zum Konfigurieren beider Elemente ServiceNow Und Drittpartei-Integrationen.

Wichtig:

Stellen Sie sicher, dass Sie die erforderlichen Drittanbieter-App-Integrationen installiert haben. Sie können die Details der erkennbaren Elemente, der Sichtungssuche und der Bedrohungssuche nur für die installierten Drittanbieter-Apps anzeigen.

Alle Integrationskonfigurationen

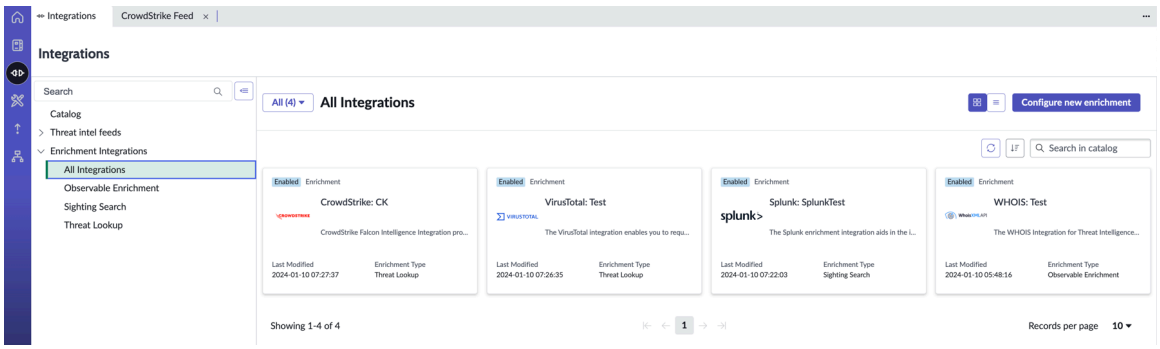
Alle Integrationen sind separate Anwendungen, die installiert werden müssen. TISC unterstützt Integrationen mit Drittparteien. Alle installierten Integrationen können hier konfiguriert werden.

In diesem Abschnitt werden Karten für jede der konfigurierten Integrationsimplementierungen angezeigt, die Sie aktivieren und verwenden können.

Der Abschnitt jedes Ergänzungstyps ist nur sichtbar, wenn mindestens eine der entsprechenden Integrationen für diesen Ergänzungstyp installiert ist. Zum Beispiel die **Bedrohungssuche** Abschnitt wäre unter sichtbar **Ergänzungsintegrationen** Nur, wenn mindestens eine Integration der Bedrohungssuche installiert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die konfigurierten Integrationskarten können angezeigt werden, indem Sie zu navigieren **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**an.



Aktionen in der Ansicht alle Integrationen

In der Ansicht „alle Integration“ können Sie die folgenden Aktionen ausführen.

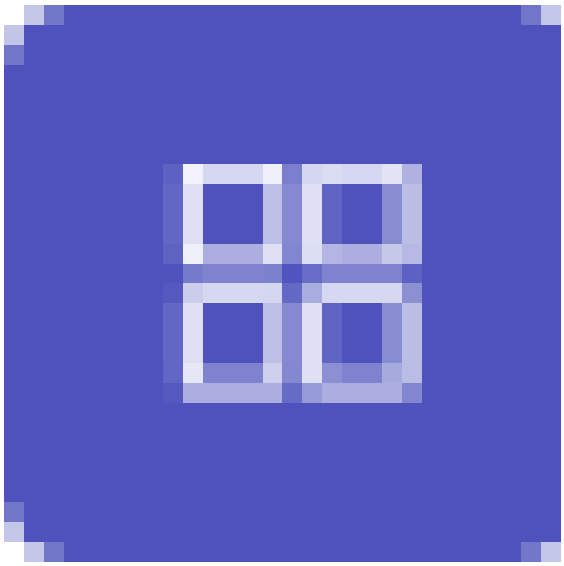
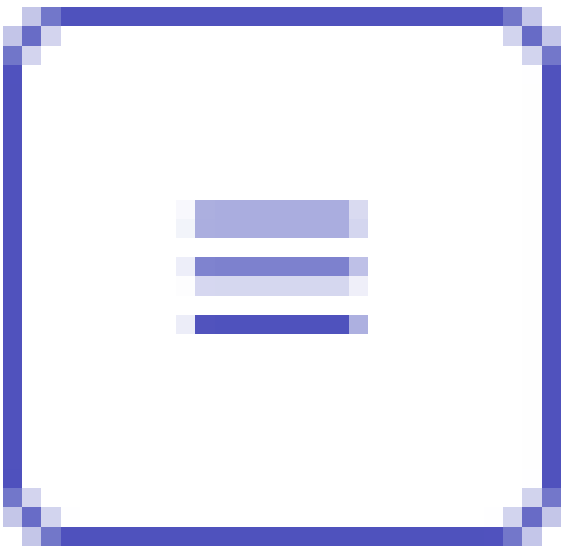
Aktionen in der Ansicht „alle Integrationen“

Aktion	Beschreibung
Alle	Verwenden Sie dieses Dropdown-Menü, um Integrationen basierend auf ihrem aktuellen Status zu filtern. Sie können basierend auf den folgenden status filtern: • **Alle** : Zeigt alle Integrationen auf der Seite an. Dies ist die Standardoption. • **Aktiviert** : Zeigt alle Integrationen an, die sich in einem aktivierten Status befinden. • **Deaktiviert** : Zeigt alle Integrationen an, die sich in einem deaktivierten Status befinden. • **Entwurf** : Zeigt alle Integrationen an, die sich im Entwurfsstatus befinden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

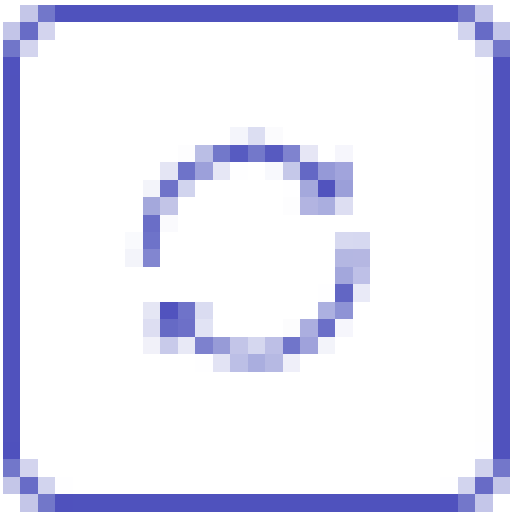
Aktionen in der Ansicht „alle Integrationen“ (Fortsetzung)

Aktion	Beschreibung
	Verwenden Sie diese Aktion, um alle Integrationen in Form von Karten anzuzeigen.
	Verwenden Sie diese Aktion, um alle Integrationen in Form von Listen anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen in der Ansicht „alle Integrationen“ (Fortsetzung)

Aktion	Beschreibung
	Verwenden Sie diese Aktion, um die Seite „alle Integrationen“ zu aktualisieren.
	Verwenden Sie diese Aktion, um alle Integrationen nach folgenden Kriterien zu sortieren: • **Zuletzt geändert (aktuell)** • **Zuletzt geändert (am ältesten)** • **Name A–Z** • **Name (Z–A)**
In Katalog suchen	Verwenden Sie diese Aktion, um basierend auf Name und Beschreibung im Katalog nach konfigurierten Integrationen zu suchen.

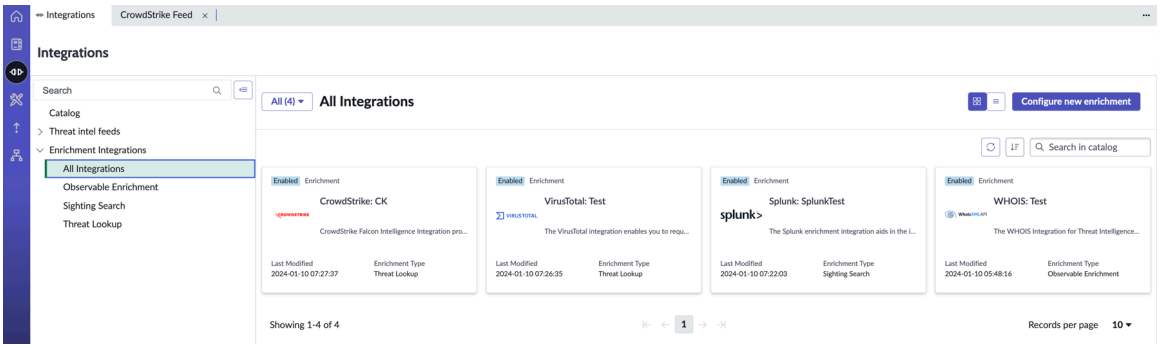
Konfigurieren Sie neue Ergänzungen in der Ansicht „alle Integrationen“

Sie können neue Ergänzungen in der Ansicht „alle Integrationen“ oder direkt in den Abschnitten „Anreicherung erkennbarer Elemente“, „Sichtungssuche“ oder „Bedrohungssuche“ konfigurieren. Führen Sie die folgenden Schritte aus, um die neue Ergänzung in der gesamten Ansicht alle Integrationen zu konfigurieren.

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** -Symbol, und wählen Sie aus **Alle Integrationen** Abschnitt.

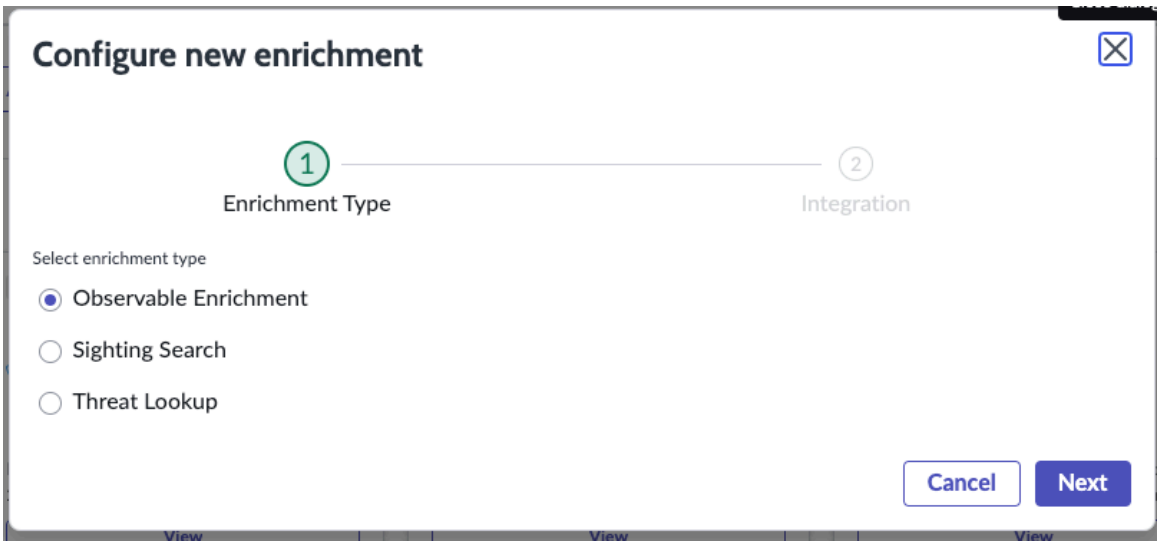
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **Konfigurieren Sie eine neue Ergänzung** Aktion.

   Das Popup „neue Ergänzung konfigurieren“ wird mit drei Ergänzungstypen angezeigt: Anreicherung erkennbarer Elemente, Sichtungssuche oder Bedrohungssuche. Sie müssen auswählen, welche Art der Ergänzung Sie konfigurieren möchten.



4. Wählen Sie einen Ergänzungstyp aus, und klicken Sie auf **Als Nächstes** .

   Dadurch gelangen Sie zum Popup, in dem die verfügbaren Integrationen angezeigt werden. Sie müssen die Integration auswählen, die Sie konfigurieren möchten.

5. Wählen Sie eine Integration aus der Liste der verfügbaren Integrationen aus, und klicken Sie auf **Wählen Sie Aus** .

   Dadurch gelangen Sie zur Seite „neue Anreicherungsintegration erstellen“ der ausgewählten Integration. Diese Seite ist standardmäßig mit Details der ausgewählten Integration vorab ausgefüllt. Beispiel: WHOIS-Integration.

6. Füllen Sie die Felder im Formular „neue Integration erstellen“ aus.

Konfigurieren Sie das neue Ergänzungsintegrationsformular

Feld	Beschreibung
Name	Geben Sie einen Namen für die neue Ergänzungsintegration ein. Beispiel: `WHOIS1` .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten sind standardmäßig vorab ausgefüllt. Beispiel: WHOIS .
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Anreicherung erkennbarer Elemente. Die Details des ausgewählten Integrationstyps sind standardmäßig vorab ausgefüllt. Die folgenden Integrationstypen werden unterstützt: ○ Ergänzung erkennbarer Elemente ○ Sichtungssuche ○ Bedrohungssuche
Beschreibung	Geben Sie eine eindeutige Beschreibung für die neue Ergänzungsintegration ein.

7. Konfigurieren Sie im Abschnitt „Integrationskonfiguration“ die Integrationsdetails basierend auf Ihren Anforderungen.

   Der Abschnitt „Integrationskonfiguration“ enthält Konfigurationsdetails wie API-Schlüssel, API-Client-ID oder -Geheimnis, Anwendername, Passwort usw., die Sie ausfüllen müssen. Diese Konfigurationsdetails variieren für verschiedene Integrationen.

8. Klicken Sie auf **Speichern** Aktion zum Speichern und Erstellen der Konfiguration der Ergänzungsintegration.

   Die angegebenen Details werden validiert, und standardmäßig ist der Status der Ergänzungsintegration deaktiviert.

9. (Optional) Klicken Sie auf **Als Entwurf speichern** Aktion zum Speichern der Integrationskonfigurationen nur als Entwurf. Anwender können eine Integration nicht aktivieren, wenn sie im Entwurf gespeichert ist

   Wenn Sie sich bei den Konfigurationsdetails nicht sicher sind, können Sie verwenden **Als Entwurf speichern** Option. Nachdem Sie die Konfigurationsdetails erhalten haben, können Sie die verbleibenden Informationen in die Entwurfsversion eingeben und erstellen.

10. Um die Ergänzungsintegration zu aktivieren, klicken Sie auf **Aktivieren** .

    Die Ergänzungsintegration wurde erfolgreich aktiviert.

11. Sie können auch eine bestimmte Ergänzungsintegration aktivieren, deaktivieren oder löschen, indem Sie das Menü Aktionen der erforderlichen Integrationskachel auf der Seite Katalog oder Ergänzungsintegrationen verwenden.

Konfigurieren Sie Die Anreicherung Erkennbarer Elemente

Sie können Threat Intelligence-Ergänzungen für ein oder mehrere erkennbare Elemente durchführen, um zu bestimmen, ob sie bekannten Sicherheitsbedrohungen zugeordnet sind. Welche Implementierungen ausgeführt werden, hängt von denen ab, die Sie aktiviert haben.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Threat Intelligence-Sicherheitszentrum Unterstützt die Anreicherung erkennbarer Elemente ab jetzt nur für die WHOIS-Integration. Weitere Informationen finden Sie unter Konfigurieren und aktivieren Sie die Whois-Integration.

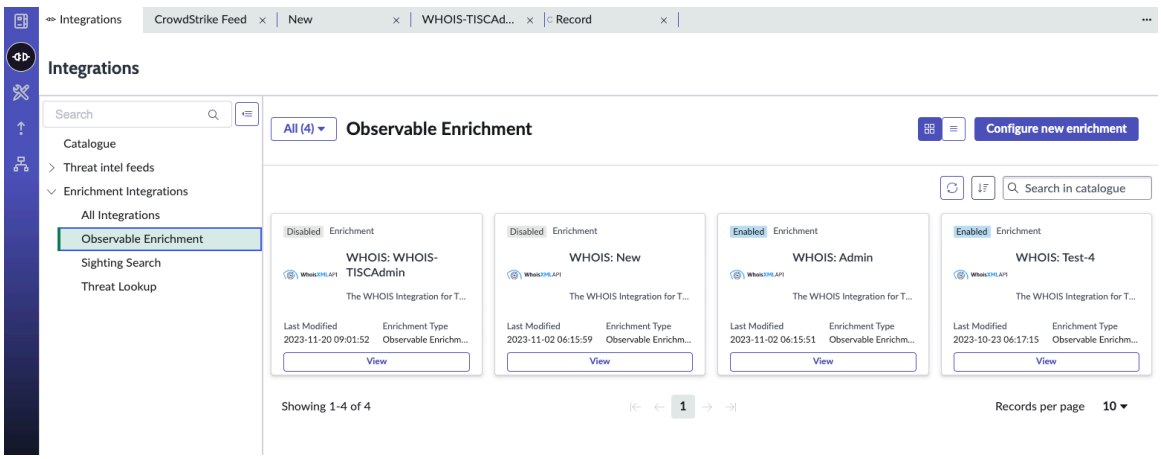
Hinweis:
Das Modul „Ergänzungsintegrationen“ wird nur angezeigt, wenn mindestens eine der Integrationen, die eine der Fähigkeiten unterstützen, in der Anwendung installiert ist.

Warum und wann dieser Vorgang ausgeführt wird

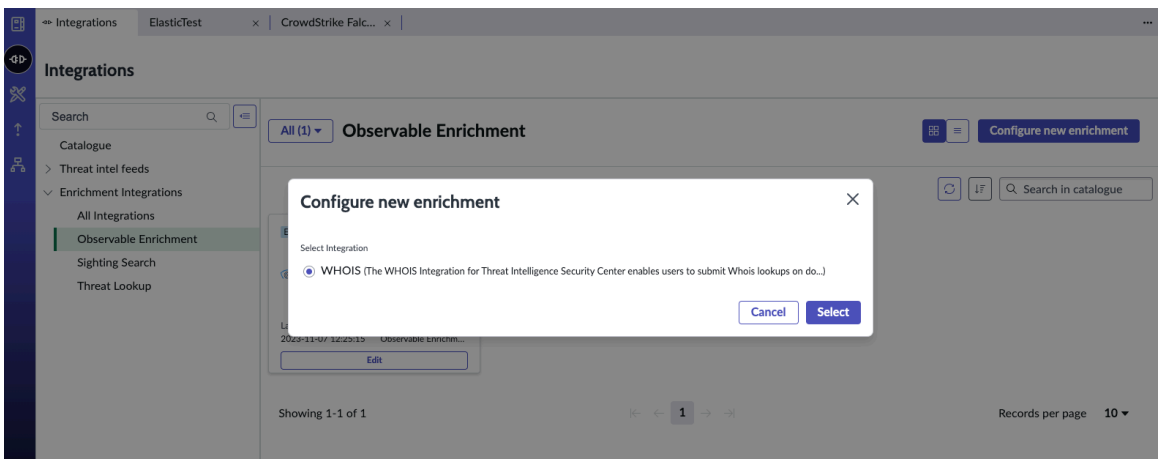
Der Abschnitt „Anreicherung erkennbarer Elemente“ enthält nur die Integrationen mit dem Integrationstyp „Anreicherung erkennbarer Elemente“. In diesem Abschnitt werden Karten für jede der konfigurierten Integrationsimplementierungen angezeigt, die Sie aktivieren und verwenden können.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** -Symbol, und wählen Sie aus **Anreicherung Erkennbarer Elemente** Abschnitt.



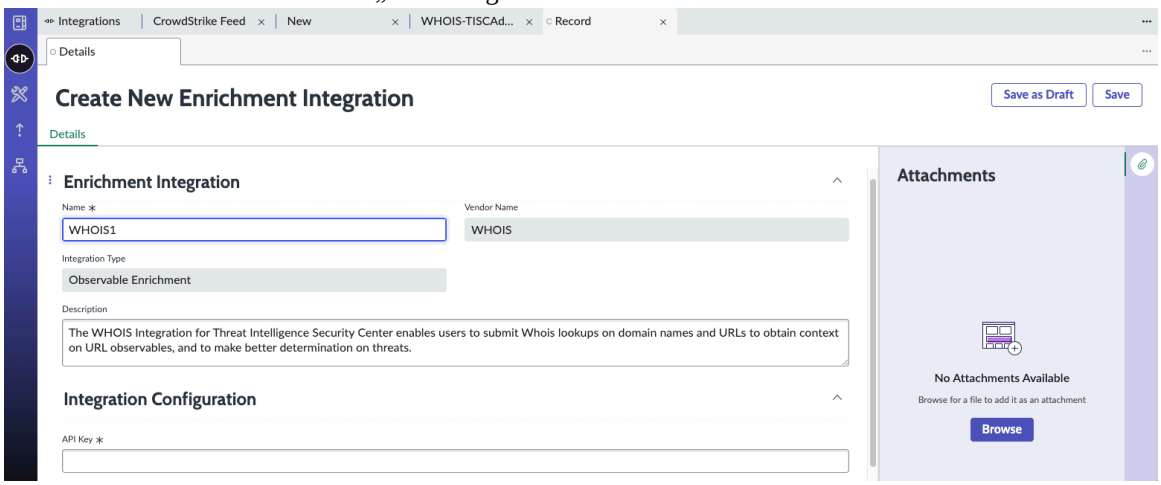
3. Klicken Sie auf **Konfigurieren Sie eine neue Ergänzung** Aktion.
   Dadurch gelangen Sie zum Popup, in dem die verfügbaren Integrationen angezeigt werden. Sie müssen die Integration auswählen, die Sie konfigurieren müssen.
4. Wählen Sie eine Integration aus der Liste der verfügbaren Integrationen aus, und klicken Sie auf **Wählen Sie Aus** .
   Dadurch gelangen Sie zur Seite „neue Anreicherungsintegration erstellen“ der ausgewählten Integration. Diese Seite ist standardmäßig mit Details der ausgewählten Integration vorab ausgefüllt. Beispiel: WHOIS-Integration.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Füllen Sie die Felder im Formular „neue Integration erstellen“ aus.



6. Konfigurieren Sie im Abschnitt „Integrationskonfiguration“ die Integrationsdetails basierend auf Ihren Anforderungen.
   Der Abschnitt „Integrationskonfiguration“ enthält Konfigurationsdetails wie API-Schlüssel, API-Client-ID oder -Geheimnis, Anwendername, Passwort usw., die Sie ausfüllen müssen. Diese Konfigurationsdetails variieren für verschiedene Apps.
7. Klicken Sie auf **Speichern** Aktion zum Speichern und Erstellen der neuen Konfiguration der Ergänzungsintegration.
   Nachdem Sie auf geklickt haben **Speichern** Oder **Aktivieren** Aktion, die Integration wird mit den angegebenen Integrationskonfigurationen validiert. Standardmäßig ist der Status der Ergänzungsintegration auf deaktiviert festgelegt.
8. Klicken Sie Auf **Als Entwurf speichern** Aktion, um nur die an der Ergänzungskonfiguration vorgenommenen Aktualisierungen zu speichern und nicht zu erstellen.
   Wenn Sie sich bei den Konfigurationsdetails nicht sicher sind, können Sie verwenden **Als Entwurf speichern** Option. Nachdem Sie die Konfigurationsdetails erhalten haben, können Sie die verbleibenden Informationen in die Entwurfsversion eingeben und erstellen.
9. Um die Ergänzungsintegration zu aktivieren, klicken Sie auf **Aktivieren** .
   Die Ergänzungsintegration wurde erfolgreich aktiviert. Sie können auch eine bestimmte Ergänzungsintegration aktivieren, deaktivieren oder löschen, indem Sie das Menü Aktionen der erforderlichen Integrationskachel auf der Seite Katalog oder Ergänzungsintegrationen verwenden.

Konfigurieren Sie Die Sichtungssuche

Sie können Sichtungssuche für ein oder mehrere erkennbare Elemente durchführen, um zu bestimmen, wie oft die erkennbaren Elemente in Ihren Organisationsprotokollen gesehen werden. Sie können innerhalb einer ausgewählten Anzahl von Tagen oder innerhalb eines Datumsbereichs eine Sichtungssuche für erkennbare Elemente durchführen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Hinweis:
Das Modul „Ergänzungsintegrationen“ wird nur angezeigt, wenn mindestens eine der Integrationen, die eine der Fähigkeiten unterstützen, in der Anwendung installiert ist.

Die Threat Intelligence-Sicherheitszentrum Unterstützt Sichtungssuche nur für die folgenden Integrationen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Splunk-Suche
- ElasticSearch

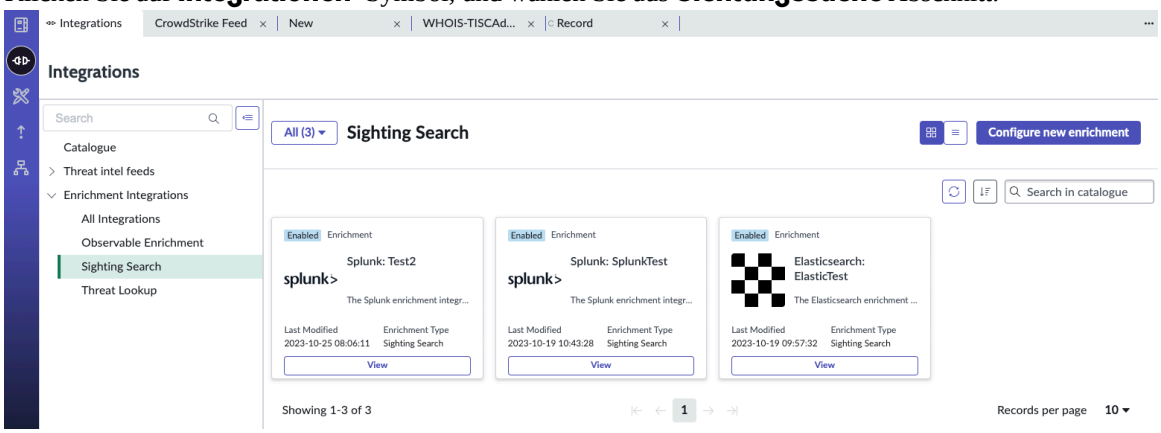
Warum und wann dieser Vorgang ausgeführt wird

Der Abschnitt „Sichtungssuche“ enthält nur die Integrationen mit dem Integrationstyp „Sichtungssuche“.

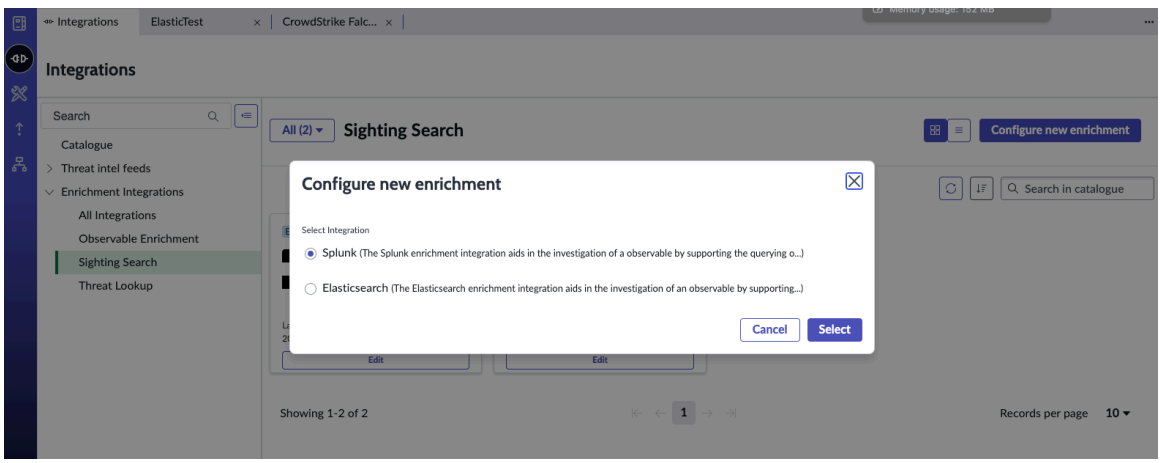
In diesem Abschnitt werden Karten für jede der konfigurierten Integrationsimplementierungen angezeigt, die Sie aktivieren und verwenden können.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** -Symbol, und wählen Sie aus **Sichtungssuche** Abschnitt.

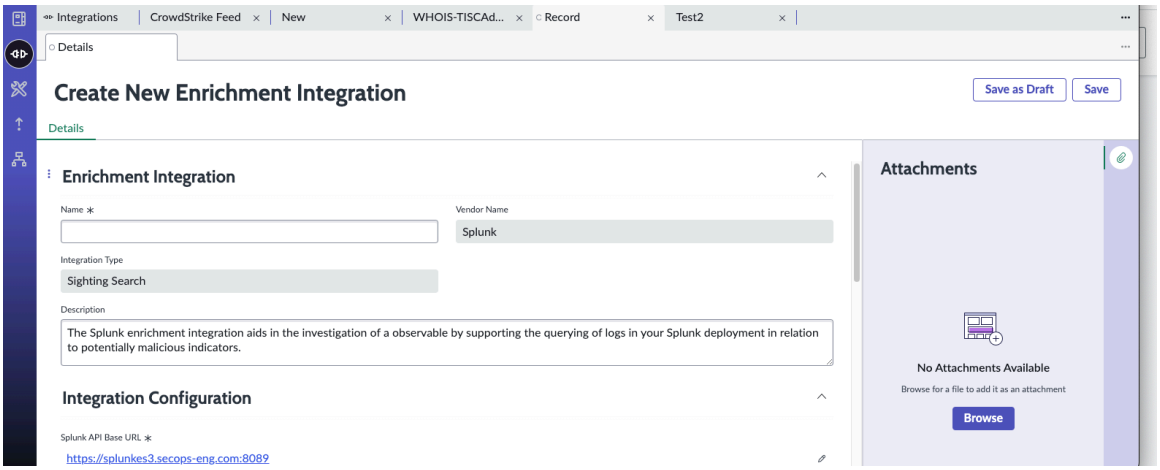


3. Klicken Sie auf **Konfigurieren Sie eine neue Ergänzung** Aktion.
   Dadurch gelangen Sie zum Popup, in dem die verfügbaren Integrationen angezeigt werden. Sie müssen die Integration auswählen, die Sie konfigurieren müssen.
4. Wählen Sie eine Integration aus der Liste der verfügbaren Integrationen aus, und klicken Sie auf **Wählen Sie Aus** .
   Dadurch gelangen Sie zur Seite „neue Anreicherungsintegration erstellen“ der ausgewählten Integration. Diese Seite ist standardmäßig mit Details der ausgewählten Integration vorab ausgefüllt. Beispiel: Splunk-Integration.



5. Füllen Sie die Felder im Formular „neue Integration erstellen“ aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Konfigurieren Sie im Abschnitt „Integrationskonfiguration“ die Integrationsdetails basierend auf Ihren Anforderungen.
   Der Abschnitt „Integrationskonfiguration“ enthält Konfigurationsdetails wie API-Schlüssel, API-Client-ID oder -Geheimnis, Anwendername, Passwort usw., die Sie ausfüllen müssen. Diese Konfigurationsdetails variieren für verschiedene Apps.
7. Klicken Sie auf **Speichern** Aktion zum Speichern und Erstellen der neuen Konfiguration der Ergänzungsintegration.
   Die angegebenen Details werden validiert, und standardmäßig ist der Status der Ergänzungsintegration deaktiviert.
8. Klicken Sie Auf **Als Entwurf speichern** Aktion, um nur die an der Ergänzungskonfiguration vorgenommenen Aktualisierungen zu speichern und nicht zu erstellen.
   Wenn Sie sich bei den Konfigurationsdetails nicht sicher sind, können Sie verwenden **Als Entwurf speichern** Option. Nachdem Sie die Konfigurationsdetails erhalten haben, können Sie die verbleibenden Informationen in die Entwurfsversion eingeben und erstellen.
9. Um die Ergänzungsintegration zu aktivieren, klicken Sie auf **Aktivieren** .
   Die Ergänzungsintegration wurde erfolgreich aktiviert. Sie können auch eine bestimmte Ergänzungsintegration aktivieren, indem Sie das Menü Aktionen der erforderlichen Integrationskachel auf der Seite „Katalog“ oder auf der Seite „alle Integration“ verwenden.

Definieren Sie Abfragen für die Sichtungssuche

Sie können Sichtungssuchkonfigurationen verwenden, um die Abfragen zu definieren, die verwendet werden, um die Verbreitung erkennbarer Elemente in Ihrer Umgebung im Rahmen der Untersuchung erkennbarer Elemente zu finden.

Zeigen Sie Abfragen für die Sichtungssuche an

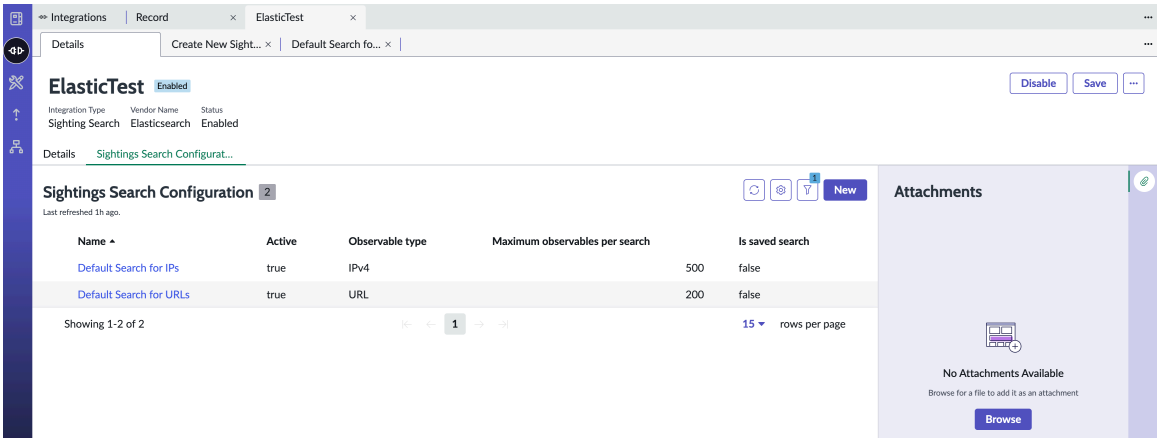
Erforderliche Rolle: sn_sec_tisc.admin

Um die Konfigurationen der Sichtungssuche anzuzeigen, führen Sie die folgenden Schritte aus:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen**an.
2. Navigieren Sie auf der Seite Integrationen zu **Ergänzungsintegrationen** > **Sichtungssuche**an.
3. Suchen Sie nach der Integration, für die Sie die Sichtungssuchkonfiguration anzeigen möchten, und klicken Sie auf **Bearbeiten** .
4. Wählen Sie aus **Sichtungssuchkonfigurationen** Registerkarte.

   Sie können die Liste der Sichtungssuchkonfigurationen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf die erforderliche Sichtungssuchkonfiguration, um die Details der Konfiguration anzuzeigen.
6. Klicken Sie auf , um eine Testsichtungssuchabfrage zu generieren **Testsichtungssuchabfrage Generieren** Aktion.

> **Hinweis:**
> Die **Testsichtungssuchabfrage Generieren** Die Aktion funktioniert nur, wenn Sie Abfrageparameter für die Sichtungssuche konfiguriert haben. Weitere Informationen finden Sie unter Sichtungssuchparameter Verwenden.

7. Geben Sie im Popup-Fenster „Testsichtungssuchabfrage generieren“ mehrere erkennbare Elemente ein, oder fügen Sie sie mithilfe von Kommas, neuen Zeilen-, Registerkarten- oder Pipe-Trennzeichen ein, um eine Testabfrage zu generieren.
8. Klicken Sie Auf **Generieren** Dient zum Generieren der Testsichtungssuchabfrage.
9. Sie können auch die folgenden Aktionen auf der Registerkarte „Konfigurationen der Sichtungssuche“ ausführen:
   a. Um die Liste der Sichtungssuchkonfigurationen zu aktualisieren, klicken Sie auf Symbol.
   b. Um eine Listenaktion für die Sichtungssuchkonfigurationen auszuführen, klicken Sie auf Symbol.

      Sie können die folgenden zwei Listenaktionen ausführen:

      - **Bearbeiten Sie Spalten** : Mit dieser Aktion können Sie vorhandene Spalten hinzufügen oder entfernen und die Reihenfolge entsprechend Ihren Anforderungen ändern.
      - **Breiten zurücksetzen** : Mit dieser Aktion können Sie die Breiten der Spalten zurücksetzen.

   c. Klicken Sie auf , um Konfigurationen der Sichtungssuche basierend auf Bedingungen zu filtern Symbol.

      Der Wert 1 gibt an, dass eine Bedingung für die Filterung verwendet wird.

Erstellen Sie Konfigurationen Für Die Seufzersuche

Erforderliche Rolle: sn_sec_tisc.admin

Maximum observables per search = "maximum number of observables that can be substituted in a single search query"

Automatische Übersetzung

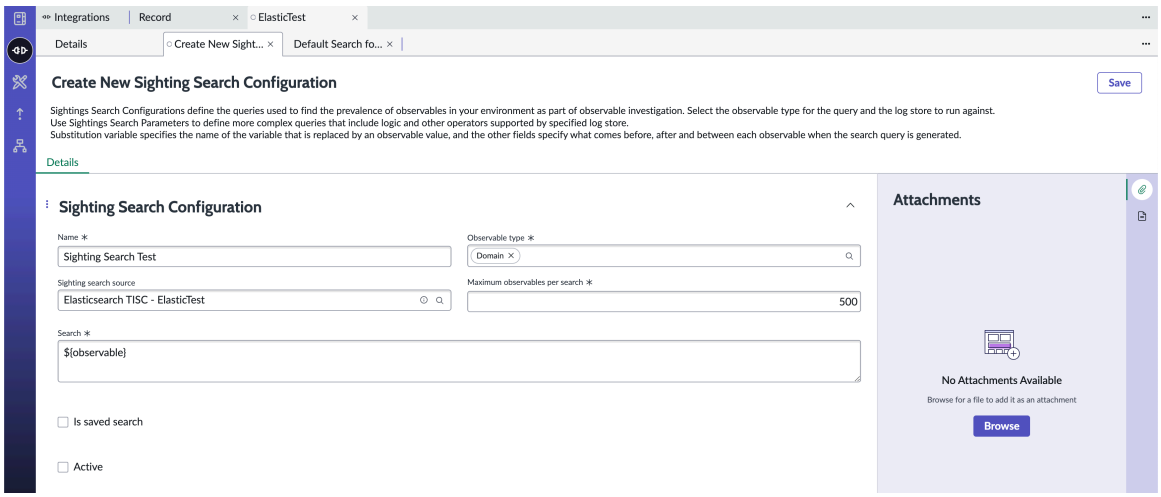
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
Search = "Search query that should be executed in sighting search source.
Search query can contain substitution variables that would be substituted with observables
 of specific type as configured in sighting search parameters when sighting search query is
 formed"
```

Führen Sie die folgenden Schritte aus, um eine Sichtungssuchkonfiguration zu erstellen:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen**an.
2. Navigieren Sie auf der Seite Integrationen zu **Ergänzungsintegrationen** > **Sichtungssuche**an.
3. Suchen Sie nach der Integration, für die Sie die Sichtungssuchkonfiguration anzeigen möchten, und klicken Sie auf **Bearbeiten** .
4. Wählen Sie aus **Sichtungssuchkonfigurationen** Registerkarte.

   Sie können die Liste der Sichtungssuchkonfigurationen anzeigen.
5. Um eine Sichtungssuchkonfiguration zu erstellen, klicken Sie auf **Neu** .



6. Füllen Sie die Felder im Formular aus.

Erstellen Sie eine Sichtungssuchkonfiguration

Feld	Beschreibung
Name	Name für die Sichtungssuchkonfiguration.
Typ des erkennbaren Elements	Definiert den Typ der Kategorie erkennbarer Elemente.
Sichtungssuchquelle	Definiert die für die Integration konfigurierte Quelle.
Maximale erkennbare Elemente pro Suche	Die Anzahl der erkennbaren Elemente bevor die Suchabfrage in mehrere Abfragen aufgeteilt wird. Legen Sie diesen Wert auf fest `500` Für diese Integration.
Suchen	Fügen Sie eine native Suchzeichenfolge hinzu, um eine Abfrage zu erstellen. Beispiel: `${erkennbares Element}` .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ist gespeicherte Suche	Führt eine gespeicherte Suche aus, d. h. das Feld Name muss mit dem Namen der gespeicherten Suche übereinstimmen.
Aktiv	Abfrage wird nur ausgeführt, wenn die Option „aktiv“ ausgewählt ist.

7. Klicken Sie auf **Speichern**.

Sichtungssuchparameter Verwenden

Sie können Sichtungssuchparameter verwenden, die komplexere Abfragen definieren, darunter Logik und andere Operatoren, die vom angegebenen Protokollspeicher unterstützt werden.

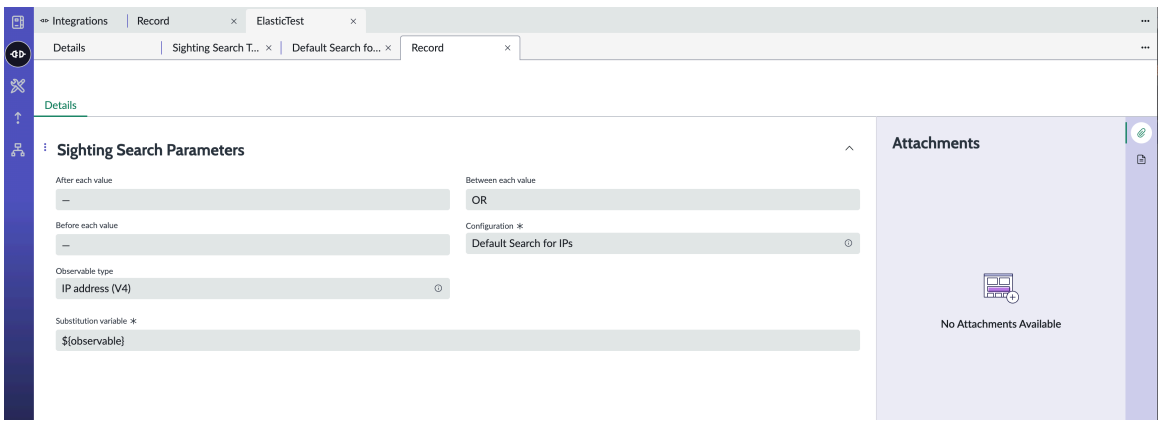
Sichtungssuchparameter Anzeigen

Erforderliche Rolle: sn_sec_tisc.admin

Führen Sie die folgenden Schritte aus, um die Sichtungssuchparameter anzuzeigen:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen**an.
2. Navigieren Sie auf der Seite Integrationen zu **Ergänzungsintegrationen** > **Sichtungssuche**an.
3. Suchen Sie nach der Integration, für die Sie die Sichtungssuchkonfiguration anzeigen möchten, und klicken Sie auf **Bearbeiten** .
4. Wählen Sie aus **Sichtungssuchkonfigurationen** Registerkarte.

   Sie können die Liste der Sichtungssuchkonfigurationen anzeigen.
5. Klicken Sie auf die erforderliche Sichtungssuchkonfiguration, um die Details der Konfiguration anzuzeigen.



6. Wählen Sie aus **Sichtungssuchparameter** Registerkarte.

   Sie können die Liste der Sichtungssuchparameter anzeigen.
7. Klicken Sie auf den erforderlichen Sichtungssuchparameter, um die Details des Parameters anzuzeigen.
8. Sie können auch die folgenden Aktionen auf der Registerkarte Sichtungssuchparameter ausführen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Um die Liste der Sichtungssuchparameter zu aktualisieren, klicken Sie auf Symbol.

b. Um eine Listenaktion für die Sichtungssuchparameter auszuführen, klicken Sie auf Symbol.

Bearbeiten Sie Spalten : Mit dieser Aktion können Sie vorhandene Spalten hinzufügen oder entfernen und die Reihenfolge entsprechend Ihren Anforderungen ändern.

c. Um Sichtungssuchparameter basierend auf Bedingungen zu filtern, klicken Sie auf Symbol.

Der Wert 1 gibt an, dass eine Bedingung für die Filterung verwendet wird.

Erstellen Sie Einen Sichtungssuchparameter

Beispiel für die Abfragegenerierung

```
Configured Query: ${Observable}

Observables Substitutes for Sightings search: Obs1 , Obs2

Query: {Before each Value}Obs1{After each Value}{Between each value}{Before each Value}Obs2{After each Value}


Let observables are: 172.32.31.41 & 192.168.10.12

Query Formed with below configuration will be: “ip_address = 172.32.31.41 OR ip_address = 192.168.10.12”
```

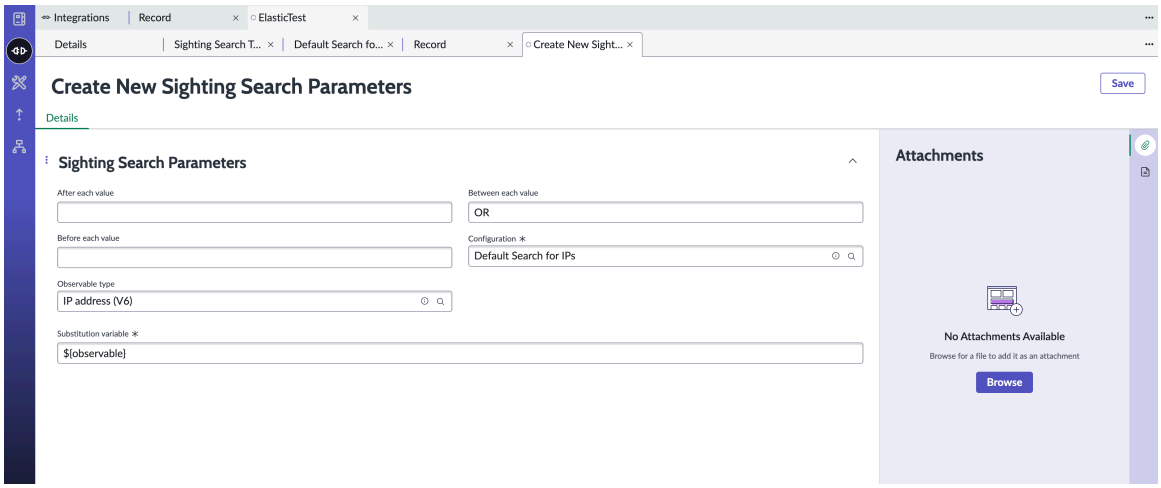
Führen Sie die folgenden Schritte aus, um einen Sichtungssuchparameter zu erstellen:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Integrationen**an.
2. Navigieren Sie auf der Seite Integrationen zu **Ergänzungsintegrationen** > **Sichtungssuche**an.
3. Suchen Sie nach der Integration, für die Sie die Sichtungssuchkonfiguration anzeigen möchten, und klicken Sie auf **Bearbeiten** .
4. Wählen Sie aus **Sichtungssuchkonfigurationen** Registerkarte.

   Sie können die Liste der Sichtungssuchkonfigurationen anzeigen.
5. Klicken Sie auf die erforderliche Sichtungssuchkonfiguration, um die Details der Konfiguration anzuzeigen.
6. Wählen Sie aus **Sichtungssuchparameter** Registerkarte.

   Sie können die Liste der Sichtungssuchparameter anzeigen.
7. Um einen Sichtungssuchparameter zu erstellen, klicken Sie auf **Neu** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Füllen Sie die Felder im Formular aus.

Erstellen Sie einen Sichtungssuchparameter

Feld	Beschreibung
Nach jedem Wert	Der Sichtungssuchparameter nach jedem erkennbaren Element, wenn die Suchabfrage generiert wird.
Zwischen jedem Wert	Der Sichtungssuchparameter zwischen jedem erkennbaren Element, wenn die Suchabfrage generiert wird. Zum Beispiel ODER.
Vor jedem Wert	Der Sichtungssuchparameter vor jedem erkennbaren Element, wenn die Suchabfrage generiert wird.
Konfiguration	Die Konfigurationsdetails des Suchparameters.
Typ des erkennbaren Elements	Definiert den Typ der Kategorie erkennbarer Elemente.
Ersetzungsvariable	Gibt den Namen der Variable an, die durch einen erkennbaren Wert ersetzt wird.

9. Klicken Sie auf **Speichern**.

Konfigurieren Sie Die Bedrohungssuche

Sie können die Bedrohungssuche konfigurieren, um eine Suche nach ausgewählten erkennbaren Elementen durchzuführen. Wenn die erkennbaren Elemente von einem von Threat Intelligence erkannten Typ sind, werden die erkennbaren Elemente auf Malware gescannt, und die Ergebnisse werden zurückgegeben. Sie können eine Bedrohungssuche für ein oder mehrere erkennbare Elemente durchführen, um die Böswilligkeit eines erkennbaren Elements zu bestimmen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Hinweis:
Das Modul „Ergänzungsintegrationen“ wird nur angezeigt, wenn mindestens eine der Integrationen, die eine der Fähigkeiten unterstützen, in der Anwendung installiert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Threat Intelligence-Sicherheitszentrum Unterstützt die Bedrohungssuche nur für die folgenden Integrationen:

- VirusTotal
- CrowdStrike Intelligence

Weitere Informationen finden Sie unter Bedrohungssuche.

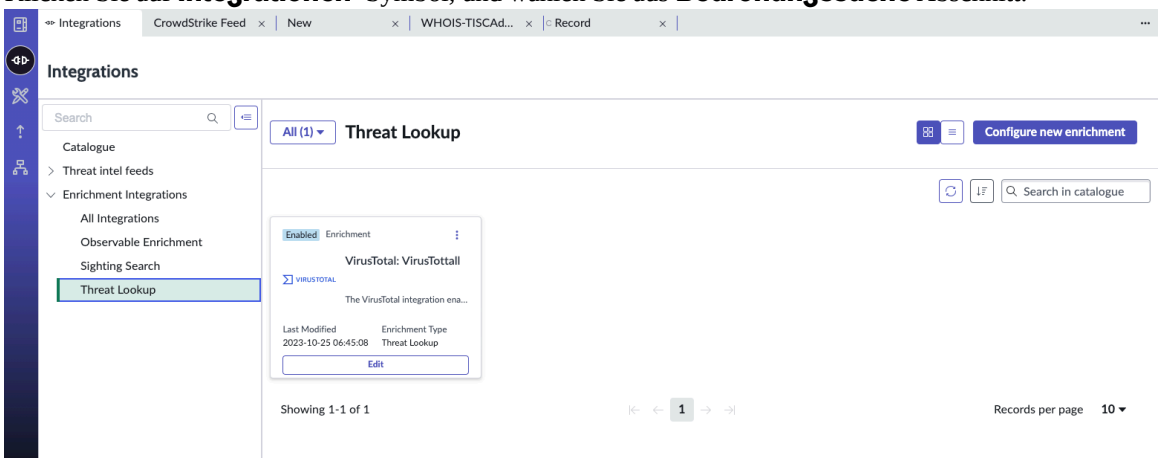
Warum und wann dieser Vorgang ausgeführt wird

Der Abschnitt „Bedrohungssuche“ enthält nur die Integrationen mit dem Integrationstyp „Bedrohungssuche“.

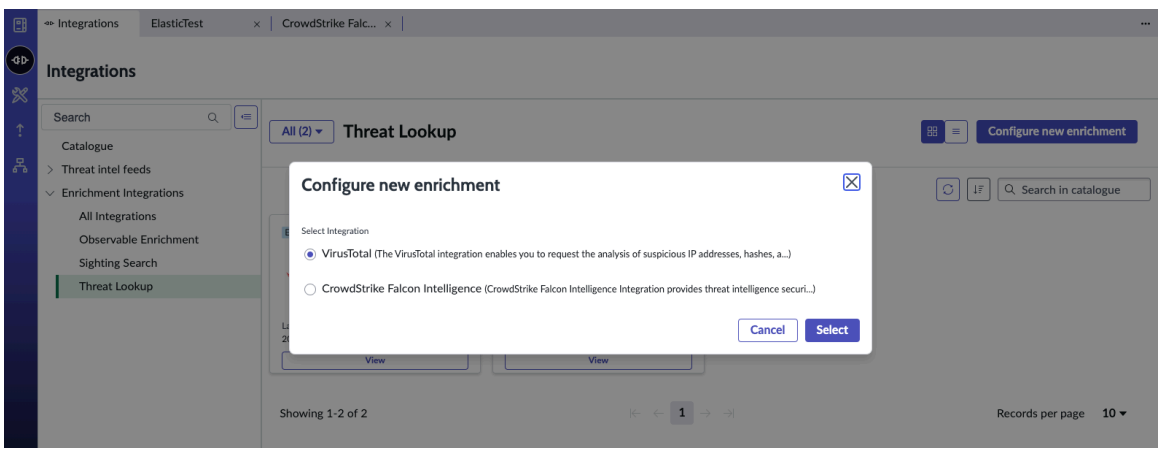
In diesem Abschnitt werden Karten für jede der konfigurierten Integrationsimplementierungen angezeigt, die Sie aktivieren und verwenden können.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Integrationen** -Symbol, und wählen Sie aus **Bedrohungssuche** Abschnitt.



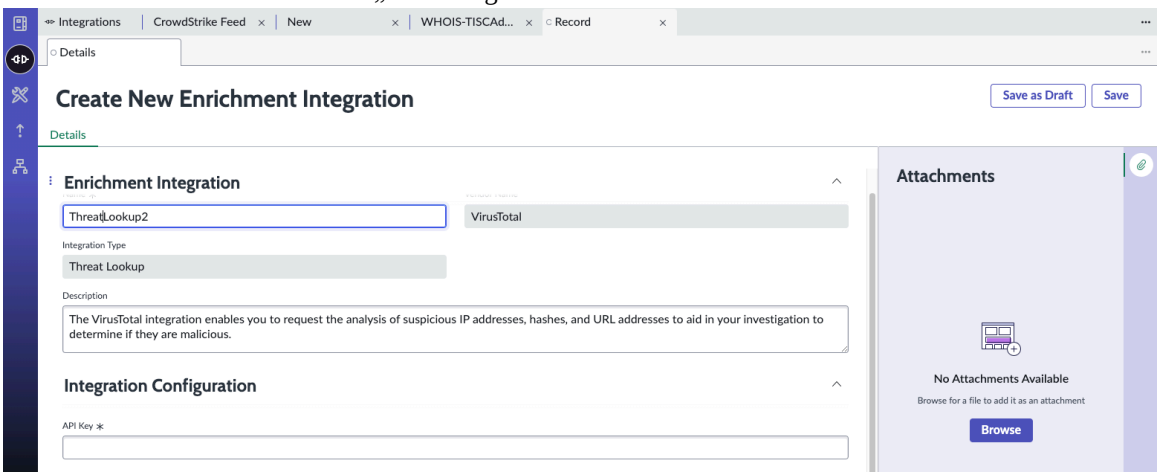
3. Klicken Sie auf **Konfigurieren Sie eine neue Ergänzung** Aktion.
   Dadurch gelangen Sie zum Popup, in dem die verfügbaren Integrationen angezeigt werden. Sie müssen die Integration auswählen, die Sie konfigurieren müssen.
4. Wählen Sie und Integration aus der Liste der verfügbaren Integrationen aus, und klicken Sie auf **Wählen Sie Aus** .
   Dadurch gelangen Sie zur Seite „neue Anreicherungsintegration erstellen“ der ausgewählten Integration. Diese Seite ist standardmäßig mit Details der ausgewählten Integration vorab ausgefüllt. Beispiel: VirusTotal-Integration.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Füllen Sie die Felder im Formular „neue Integration erstellen“ aus.



6. Konfigurieren Sie im Abschnitt „Integrationskonfiguration“ die Integrationsdetails basierend auf Ihren Anforderungen.
   Der Abschnitt „Integrationskonfiguration“ enthält Konfigurationsdetails wie API-Schlüssel, API-Client-ID oder -Geheimnis, Anwendername, Passwort usw., die Sie ausfüllen müssen. Diese Konfigurationsdetails variieren für verschiedene Apps.
7. Klicken Sie auf **Speichern** Aktion zum Speichern und Erstellen der neuen Konfiguration der Ergänzungsintegration.
   Die angegebenen Details werden validiert, und standardmäßig ist der Status der Ergänzungsintegration deaktiviert.
8. Klicken Sie Auf **Als Entwurf speichern** Aktion, um nur die an der Ergänzungskonfiguration vorgenommenen Aktualisierungen zu speichern und nicht zu erstellen.
   Wenn Sie sich bei den Konfigurationsdetails nicht sicher sind, können Sie verwenden **Als Entwurf speichern** Option. Nachdem Sie die Konfigurationsdetails erhalten haben, können Sie die verbleibenden Informationen in die Entwurfsversion eingeben und erstellen.
9. Um die Ergänzungsintegration zu aktivieren, klicken Sie auf **Aktivieren** .
   Die Ergänzungsintegration wurde erfolgreich aktiviert. Sie können auch eine bestimmte Ergänzungsintegration aktivieren, deaktivieren oder löschen, indem Sie das Menü Aktionen der erforderlichen Integrationskachel auf der Seite Katalog oder Ergänzungsintegrationen verwenden.

Reputationsrechner Für Bedrohungssuche Anzeigen

Sie können den Ergebnisrechner für Bedrohungssuche anzeigen, um die Ergebnisse erkennbarer Elemente für Ihre Integration zu berechnen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

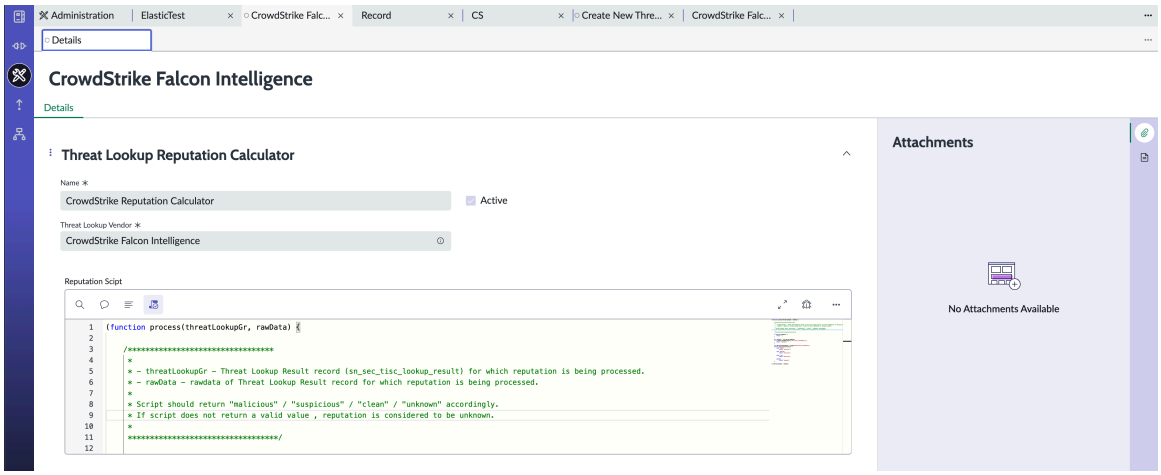
Weitere Informationen zu den Reputationsrechnern für Bedrohungssuche finden Sie unter Reputationsrechner für Bedrohungssuche verwalten.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Wählen Sie aus **Reputationsrechner Für Bedrohungssuche** Abschnitt.
   Sie können die Liste der Reputationsrechner für die Bedrohungssuche anzeigen.
3. Klicken Sie auf den erforderlichen Reputationsrechner für Bedrohungssuche, um die Details des Rechners anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Sie können auch die folgenden Aktionen im Abschnitt „Reputationsrechner für Bedrohungssuche“ ausführen:

   a. Um die Liste der Reputationsrechner für Bedrohungssuche zu aktualisieren, klicken Sie auf Symbol.

   b. Um eine Listenaktion für die Reputationsrechner der Bedrohungssuche auszuführen, klicken Sie auf Symbol.

      Sie können die folgenden zwei Listenaktionen ausführen:

      - **Bearbeiten Sie Spalten** : Mit dieser Aktion können Sie vorhandene Spalten hinzufügen oder entfernen und die Reihenfolge entsprechend Ihren Anforderungen ändern.
      - **Breiten zurücksetzen** : Mit dieser Aktion können Sie die Breiten der Spalten zurücksetzen.

   c. Um Reputationsrechner für Bedrohungssuche basierend auf Bedingungen zu filtern, klicken Sie auf Symbol.

      Der Wert 1 gibt an, dass eine Bedingung für die Filterung verwendet wird.

TISC-API-Referenzen

Die folgende Tabelle enthält die API-Endpunktreferenzen, die bei Ergänzungen helfen.

TISC-APIs

API	Beschreibung
TISC-API – POST /sn_sec_tisc/Threat_intel_Data/observables	Diese API ruft die Daten erkennbarer Elemente ab, einschließlich der Beziehungen zwischen erkennbaren Elementen und anderen zugehörigen Threat Intelligence-Daten.
TISC-API – POST /sn_sec_tisc/Threat_intel_Data/add_observables	Diese API fügt der Anwendung Threat Intelligence Security Center (TISC) gültige erkennbare Elemente hinzu, indem Quelldatensätze für erkennbare Elemente erstellt werden.

Weitere Informationen zu den TISC-API-Endpunkten finden Sie unter TISC-API im REST-API-Referenzabschnitt zu API-Implementierung und -Referenz Auf servicenow.com/docs.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TISC-Integrationen

Dieser Abschnitt enthält Anweisungen zum Konfigurieren und Aktivieren der Threat Intelligence-Integrationen.

Ergänzung erkennbarer Elemente

Der WHOIS-Workflow „erkennbares Element anreichern“ führt eine Ergänzung für ausgewählte erkennbare Elemente durch. Wenn die erkennbaren Elemente von einem Typ sind, der von der WhoisXML-API-Integration erkannt wird, werden die erkennbaren Elemente angereichert.

Hinweis:
Das Threat Intelligence-Sicherheitszentrum unterstützt die Anreicherung erkennbarer Elemente nur für die WHOIS-Integration.

WHOIS-Integration

Mit der Whois-Integration können Sie Whois-Suchen nach Domänennamen und URLs übermitteln, um Kontext zu erkennbaren URL-Elementen zu erhalten und Bedrohungen besser zu bestimmen.

Konfigurieren und aktivieren Sie die Whois-Integration

Bevor Sie die Whois-Integration verwenden, müssen Sie sie aus dem ServiceNow Store herunterladen und über einen gültigen Account von Whois verfügen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Die Plugins „Threat Intelligence Security Center“ und „Whois erkennbares Element“ sind erforderlich.

Prozedur

1. Greifen Sie mit Ihrer Instanz auf zu **Threat Intelligence-Sicherheitszentrum** .
2. Laden Sie die Integration aus dem herunter ServiceNow Storean.
3. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
4. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**an.
5. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Ergänzung erkennbarer Elemente**an.
6. In **WHOIS** Karte, klicken Sie auf **Konfigurieren Sie Neue Anreicherung** Zum Konfigurieren **WHOIS** Integration.
7. Füllen Sie die Felder im Formular „neue Anreicherung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die neue Ergänzungsintegration ein. Beispiel: WHOIS.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: WHOIS.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Bedrohungssuche.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Geben Sie die Beschreibung für die neue Ergänzungsintegration ein. Die Beschreibung für die WHOIS-Integration lautet beispielsweise: WHOIS Integration for Threat Intelligence Security Center ermöglicht Anwendern die Übermittlung von Whois-Suchen zu Domänennamen und URLs, um Kontext zu erkennbaren URL-Elementen zu erhalten und Bedrohungen besser zu bestimmen.

8. Drilldown zu **Integrationskonfiguration** Abschnitt.
9. Geben Sie ein (oder fügen Sie ein) **API-Schlüssel** Sie haben von der WHOIS-Website erworben.
10. Klicken Sie auf **Speichern**.
    Die Integrationsdetails werden validiert, und standardmäßig ist der Status der WHOIS-Integration deaktiviert.
11. Klicken Sie Auf **Aktivieren** Zum Aktivieren der WHOIS-Integration.

Ergebnisse

Nach der Konfiguration kann WHOIS ausgewählt werden, um Ergänzungen für erkennbare Elemente im Threat Intelligence-Sicherheitszentrum durchzuführen.

SHODAN-Integration

SHODAN ist eine Suchmaschine, die Servicebannerinformationen von verbundenen Geräten auf der ganzen Welt analysiert.

Die Shodan-Integration führt eine Ergänzung für die folgenden erkennbaren Elemente durch:

- IP-Adressen
- URLs
- Domänen

Konfigurieren und aktivieren Sie die Shodan-Integration

Bevor Sie die Shodan-Integration verwenden, müssen Sie sie aus dem herunterladen ServiceNow Speichern.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Greifen Sie mit Ihrer Instanz auf zu **Threat Intelligence-Sicherheitszentrum** .
2. Laden Sie die Integration aus dem herunter ServiceNow Storean.
3. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
4. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**an.
5. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Ergänzung erkennbarer Elemente**an.
6. In **Shodan** Karte, klicken Sie auf **Konfigurieren Sie Neue Anreicherung** Zum Konfigurieren der Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Füllen Sie die Felder im Formular „neue Anreicherung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die neue Ergänzungsintegration ein. Beispiel: Shodan.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden automatisch ausgefüllt, und standardmäßig ist dieses Feld schreibgeschützt. Beispiel: Shodan.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Anreicherung erkennbarer Elemente.
Beschreibung	Geben Sie die Beschreibung für die neue Ergänzungsintegration ein. Die Beschreibung für die Shodan-Integration lautet beispielsweise „Shodan hilft Ihnen, Bannerinformationen von verbundenen Geräten auf der ganzen Welt zu analysieren.

8. Drilldown zu **Integrationskonfiguration** Abschnitt.
9. Geben Sie ein (oder fügen Sie ein) **API-Schlüssel** Sie haben über das Shodan-Portal erworben.
10. Klicken Sie auf **Speichern**.
    Die Integrationsdetails werden validiert, und standardmäßig ist der Status deaktiviert.
11. Klicken Sie Auf **Aktivieren** Zum Aktivieren der Integration.

Sichtungssuche

In diesem Abschnitt werden die Integrationen TISC-Sichtungssuche und Elastic Search beschrieben.

Erste Schritte mit der Elasticsearch-Integration

Die Elasticsearch-Ergänzungsintegration durchsucht Ihre Protokolle und fügt Ihren erkennbaren Elementen relevante Sichtungsinformationen hinzu.

Konfigurieren und aktivieren Sie die Elasticsearch-Integration

Elasticsearch ist eine verteilte RESTful-Such- und Analytics-Engine, die sich problemlos in Security Operations integrieren lässt.

Vorbereitungen

Bevor Sie Elasticsearch verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen.

Erforderliche Rolle: sn_sec_tisc.admin

- Das Plugin „Threat Intelligence Security Center“ muss installiert und aktiviert sein, bevor Sie die Elasticsearch-Integration verwenden können.
- Rufen Sie die Elasticsearch-API-Basis-URL, die Kibana-Basis-URL, den Anwendernamen und das Passwort unter Ihrem Elasticsearch-Profil ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Greifen Sie mit Ihrer Instanz auf zu **Threat Intelligence-Sicherheitszentrum** .
2. Laden Sie die Integration aus dem herunter ServiceNow Storean.
3. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
4. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**an.
5. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Sichtungssuche**

Hinweis:
Die konfigurierten Integrationen werden als Reihe von Karten angezeigt.

6. In **Elasticsearch** Karte, klicken Sie auf **Konfigurieren Sie Neue Anreicherung** Zum Konfigurieren **Elasticsearch** Integration.
7. Füllen Sie die Felder im Formular „neue Anreicherung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die Sichtungssuchkonfiguration ein.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: Elasticsearch.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Bedrohungssuche.
Beschreibung	Geben Sie die Beschreibung für die Elasticsearch-Integration ein. Beispielsweise hilft die Elasticsearch-Ergänzungsintegration bei der Untersuchung eines erkennbaren Elements, indem sie die Abfrage von Protokollen in Ihrer Elasticsearch-Bereitstellung unterstützt.
Integrationskonfiguration	
Basis-URL der Elasticsearch-API	Die Basis-URL, die Sie von der Elasticsearch-Website erworben haben.
Kibana-Basis-URL	Die Kibana-Basis-URL. [Optional] Links zu einer Kibana-Instanz, falls verfügbar.
Anwendername	Ihr Intel Elasticsearch-Anwendername.
Passwort	Ihr Intel Elasticsearch-Passwort.
Elasticsearch-Index	Der Elasticsearch-Index. Diese wiederum enthalten Dokumente, die für jeden Index eindeutig sind. Indizes werden durch Kleinbuchstabennamen identifiziert, die sich auf Aktionen beziehen, bei denen es sich um ausgeführte Aktionen handelt (z. B. Suchen und Löschen).
Feld „Datumsbereich“	Der Zeitstempel der Konfiguration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie in Tagen anzeigen möchten.
Rohdatenmuster in Suchergebnissen berücksichtigen	Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung für die Anzahl der Zeilen der Rohdateneigenschaft in ab Eigenschaften von Security Incident Response .
MID-Server	Wählen Sie beliebig aus, um einen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum Workflow-Editor.

8. Klicken Sie auf **Speichern**.
   Die Integrationsdetails werden validiert, und standardmäßig ist der Status der Elasticsearch-Integration deaktiviert.
9. Klicken Sie Auf **Aktivieren** Zum Aktivieren der Elasticsearch-Integration.

Ergebnisse
Nach der Konfiguration kann Elasticsearch ausgewählt werden, um eine Sichtungssuche für erkennbare Elemente im Threat Intelligence-Sicherheitszentrum durchzuführen.

Erste Schritte mit der Splunk Search-Integration

Splunk-Software sucht, überwacht und analysiert maschinell generierte Big Data und lässt sich problemlos in Security Operations integrieren. Bevor Sie die Splunk-Sichtungssuche-Integration verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen.

Konfigurieren und aktivieren Sie die Splunk-Integration

Die Splunk-Anreicherungsintegration durchsucht Ihre Protokolle und fügt relevante Sichtungsinformationen hinzu.

Vorbereitungen
Bevor Sie die Splunk-Suche verwenden können, müssen Sie sie aus dem ServiceNow Store herunterladen.

Erforderliche Rolle: sn_sec_tisc.admin

- Das Plugin „Threat Intelligence Security Center“ muss installiert und aktiviert sein, bevor Sie die Splunk Search-Integration verwenden können.
- Rufen Sie den Splunk ab, erhalten Sie die Splunk-Suche, und erhalten Sie die API-Basis-URL, die Link-URL, den Anwendernamen und das Passwort von Ihrer Splunk-Instanz.

Prozedur

1. Greifen Sie mit Ihrer Instanz auf zu **Threat Intelligence-Sicherheitszentrum** .
2. Laden Sie die Integration aus dem herunter ServiceNow Storean.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wenn die Installation abgeschlossen ist, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
4. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**an.
5. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Sichtungssuche**
   Die konfigurierten Integrationen werden als Reihe von Karten angezeigt.
6. In **Splunk-Suche** Karte, klicken Sie auf **Konfigurieren Sie Neue Anreicherung** Zum Konfigurieren **Splunk-Suche** Integration.
7. Füllen Sie die Felder im Formular „neue Anreicherung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die Sichtungssuchkonfiguration ein.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: Splunk.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Bedrohungssuche.
Beschreibung	Geben Sie die Beschreibung für die Splunk-Integration ein. Beispielsweise hilft die Splunk-Ergänzungsintegration bei der Untersuchung eines erkennbaren Elements, indem sie die Abfrage von Protokollen in Ihrer Splunk-Bereitstellung in Bezug auf potenziell schädliche Indikatoren unterstützt.
Integrationskonfiguration	
Basis-URL der Splunk-API	Die Basis-URL, die Sie von der Splunk-Website erworben haben.
Link-URL	[Optional] die Link-URL, die mit der Splunk-Webschnittstelle verknüpft ist, falls verfügbar.
Anwendername	Ihr Intel Elasticsearch-Anwendername.
Passwort	Ihr Intel Elasticsearch-Passwort.
Max. Zeilen	Die maximale Anzahl von Zeilen, die Sie durchsuchen möchten.
Erstes Ergebnis (Tage)	Die frühesten Ergebnisse, die Sie in Tagen anzeigen möchten.
Rohdatenmuster in Suchergebnissen berücksichtigen	Wählen Sie diese Option aus, um Beispiele von Rohdaten in Ihre Sichtungssuchergebnisse aufzunehmen. Die Menge der zurückgegebenen Daten hängt von Ihrer Einstellung für die Anzahl der Zeilen der Rohdateneigenschaft in ab Eigenschaften von Security Incident Response .
Lokale Bereitstellung	Die lokal bereitgestellte Umgebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID-Server	Wählen Sie beliebig aus, um einen aktiven MID-Server zu verwenden, oder wählen Sie einen bestimmten MID-Server-Namen aus.

Hinweis:
Durch die Konfiguration dieser Integration werden Workflows aktiviert. Um die Workflows zu verwalten, navigieren Sie zum Workflow-Editor.

8. Klicken Sie auf **Speichern**.
   Die Integrationsdetails werden validiert, und standardmäßig ist der Status der Splunk-Integration deaktiviert.
9. Klicken Sie Auf **Aktivieren** Zum Aktivieren der Splunk-Integration.

Ergebnisse
Nach der Konfiguration kann Splunk ausgewählt werden, um eine Sichtungssuche für erkennbare Elemente im Threat Intelligence-Sicherheitszentrum durchzuführen.

Bedrohungssuche

Der Workflow „Bedrohungssuche – VirusTotal und CrowdStrike Falcon Intelligence“ führt eine Suche nach ausgewählten erkennbaren Elementen durch. Wenn die erkennbaren Elemente von einem Typ sind, der von VirusTotal und sowie CrowdStrike erkannt wird, werden die erkennbaren Elemente auf Malware gescannt, und die Ergebnisse werden zurückgegeben.

TISC VirusTotal-Integration

Mit der TISC VirusTotal-Integration können Sie die Analyse verdächtiger IP-Adressen, Datei-Hashes und URL-Adressen anfordern, um Ihre Untersuchung zu unterstützen und festzustellen, ob sie böswillig sind.

Konfigurieren und aktivieren Sie die VirusTotal-Integration

Bevor Sie die VirusTotal-Integration verwenden können, müssen Sie sie aus dem herunterladen ServiceNow Store.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Das Plugin „Threat Intelligence Security Center“ ist erforderlich, um die VirusTotal-Integration zu aktivieren.

Prozedur

1. Greifen Sie mit Ihrer Instanz auf zu **Threat Intelligence-Sicherheitszentrum** .
2. Laden Sie die Integration aus dem herunter ServiceNow Storean.
3. Wenn die Installation abgeschlossen ist, greifen Sie auf VirusTotal zu, und rufen Sie den API-Schlüssel unter Ihrem VirusTotal-Profil ab.
4. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
5. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**an.
6. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Bedrohungssuche**
7. Klicken Sie Auf **Konfigurieren Sie Neue Anreicherung** Zum Konfigurieren **Virustotal** Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Füllen Sie die Felder im Formular „neue Anreicherung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die neue Ergänzungsintegration ein. Beispiel: VirusTotal.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: VirusTotal.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Bedrohungssuche.
Beschreibung	Geben Sie die Beschreibung für die neue Ergänzungsintegration ein.

9. Drilldown zu **Integrationskonfiguration** Abschnitt.
10. Geben Sie ein (oder fügen Sie ein) **API-Schlüssel** Sie haben von der VirusTotal-Website erworben.
11. Klicken Sie auf **Speichern**.
    Die Integrationsdetails werden validiert, und standardmäßig ist der Status der VirusTotal-Integration deaktiviert.
12. Klicken Sie Auf **Aktivieren** Zum Aktivieren der VirusTotal-Integration.

Ergebnisse
Nach der Konfiguration kann VirusTotal ausgewählt werden, um im Threat Intelligence-Sicherheitszentrum nach erkennbaren Elementen zu suchen.

TISC CrowdStrike Falcon Intelligence-Integration

CrowdStrike Falcon Intelligence bietet Cybersicherheits-Intelligence, die sich einfach in Security Operations integrieren lässt.

Hinweis:

Das Plugin Threat Intelligence Security Center ist erforderlich, um die CrowdStrike Falcon Intelligence-Integration zu implementieren.

Konfigurieren und aktivieren Sie die CrowdStrike Falcon Intelligence-Integration

Bevor Sie CrowdStrike Falcon Intelligence verwenden können, müssen Sie es aus dem ServiceNow Store herunterladen und die entsprechende Client-ID und das Clientgeheimnis hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

- Die Anwendung Threat Intelligence Security Center muss installiert und aktiviert sein.
- Rufen Sie die API-Client-ID und das API-Client-Geheimnis unter Ihrem CrowdStrike Falcon Intelligence-Profil ab.
- Aktivieren Sie in den Bereichen der CrowdStrike Falcon Intelligence-Portal-API die Einstellung Lesen für Indikatoren (Falcon Intelligence).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Greifen Sie mit Ihrer Instanz auf zu **Threat Intelligence-Sicherheitszentrum** .
2. Laden Sie die Integration aus dem herunter ServiceNow Storean.
3. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
4. Auswahlvorgang **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen**an.
5. Alternativ können Sie zu navigieren **Integrationen** > **Ergänzungsintegrationen** > **Alle Integrationen** > **Bedrohungssuche**an.
6. Klicken Sie Auf **Konfigurieren Sie Neue Anreicherung** Zum Konfigurieren **CrowdStrike Falcon Intelligence** Integration.
7. Füllen Sie die Felder im Formular „neue Anreicherung konfigurieren“ aus.

Ergänzungsintegration

Feld	Beschreibung
Name	Geben Sie einen Namen für die neue Ergänzungsintegration ein. Beispiel: CrowdStrike Falcon Intelligence.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: CrowdStrike Falcon Intelligence.
Integrationstyp	Typ der von Ihnen ausgewählten Integration. Beispiel: Bedrohungssuche.
Beschreibung	Geben Sie die Beschreibung für die neue Ergänzungsintegration ein.
Integrationskonfiguration	
Client-ID	Die Client-ID, die Sie von CrowdStrike erhalten haben.
Geheimer Clientschlüssel	Der geheime Clientschlüssel, den Sie von CrowdStrike erhalten haben.

8. Klicken Sie auf **Speichern**.
   Die Integrationsdetails werden validiert, und standardmäßig ist der Status der CrowdStrike Falcon Intelligence-Integration deaktiviert.
9. Klicken Sie Auf **Aktivieren** Zum Aktivieren der CrowdStrike Falcon Intelligence-Integration.

Ergebnisse

Nach der Konfiguration kann CrowdStrike Falcon Intelligence ausgewählt werden, um im Threat Intelligence-Sicherheitszentrum nach erkennbaren Elementen zu suchen.

TISC-Sicherheitstools – EDR

TISC Endpoint Detection and Response (EDR)-Integrationen konzentrieren sich auf die Identifizierung und Bekämpfung von Sicherheitsbedrohungen auf Endpunktebene.

EDR-Netzwerklösungen prognostizieren und verhindern neu auftretende Bedrohungen und helfen bei der Verbesserung der Sicherheitslage der gesamten Organisation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch die Integration mit anderen Sicherheitstools wie EDR ermöglicht TISC eine proaktive Bedrohungsüberwachung an Endpunkten und verbessert dadurch die allgemeine Sicherheitslage und Resilienz gegenüber sich entwickelnden Bedrohungen.

Zugehörige Informationen

CrowdStrike Falcon EDR-Integration

CrowdStrike Falcon EDR-Integration

Integration mit CrowdStrike Falcon EDR ermöglicht kontinuierliche Überwachung und Echtzeitwarnungen basierend auf Informationen von TISC.

Diese Integration kann dazu beitragen, den Sicherheitsbetrieb zu optimieren und potenzielle Risiken für das Geschäft der Organisation zu reduzieren.

Konfigurieren Sie die CrowdStrike Falcon EDR-Integration

Bevor Sie verwenden können CrowdStrike Falcon EDR-Integration, Sie müssen sie aus herunterladen ServiceNow Store Speichern und fügen Sie die entsprechende Client-ID und das geheime Client-Geheimnis hinzu.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

- Die Anwendung Threat Intelligence Security Center muss installiert und aktiviert sein.
- Rufen Sie die API-Client-ID und das API-Client-Geheimnis von ab CrowdStrike Falcon-Konsole.
- In CrowdStrike Falcon Portal-API-Umfänge aktivieren **IOC-Management: Lese- und Schreibzugriff** .

Prozedur

1. Greifen Sie mit Ihrer Instanz auf zu **Threat Intelligence-Sicherheitszentrum** .
2. Laden Sie die Integration aus dem herunter ServiceNow Storean.
3. Auswahlvorgang **Integrationen** > **Sicherheitstools** > **EDR**an.
4. Klicken Sie Auf **Konfigurieren Sie Das Neue Sicherheitstool** Zum Konfigurieren CrowdStrike Falcon EDR-Integration.
5. Wählen Sie Aus **CrowdStrike Falcon EDR** Option.
6. Füllen Sie die Felder im Formular Neues Sicherheitstool konfigurieren aus.

Neue Ergänzungsintegration erstellen

Feld	Beschreibung
Name	Geben Sie einen Namen für die Integration des neuen Sicherheitstools ein. Beispiel: CrowdStrike Falcon EDR.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt. Beispiel: CrowdStrike Falcon EDR.
Beschreibung	Geben Sie die Beschreibung für die Integration des neuen Sicherheitstools ein.
Integrationstyp	Option, die den Integrationstyp anzeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Integrationskategorie	Option, die die Integrationskategorie anzeigt.
Integrationskonfiguration	
Basis-URL	Die Basis-URL ist die Basis-URL der CrowdStrike-API. Der Standardwert ist https://api.crowdstrike.com . Weitere Informationen finden Sie unter https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis#k9578c40
Client-ID	Die Client-ID, die Sie von erhalten haben CrowdStrike. Weitere Informationen finden Sie unter https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis .
Geheimer Clientschlüssel	Der geheime Clientschlüssel, von dem Sie abgerufen haben CrowdStrike. Weitere Informationen finden Sie unter https://falcon.crowdstrike.com/documentation/page/a2a7fc0e/crowdstrike-oauth2-based-apis .
Ablaufzeitraum in Tagen für jede Art von erkennbaren Elementen	Der Ablaufzeitraum in Tagen, der für eine beliebige Art von erkennbaren Elementen angewendet wird, wenn sie an gesendet werden CrowdStrike EDR. **Hinweis:** Diese Option ist ein Fallback-Ablaufzeitraum, wenn die Ablaufzeit für keinen bestimmten erkennbaren Typ festgelegt ist.
Ablaufzeit des erkennbaren IP-Elements	Der Ablaufzeitraum in Tagen, der für den IP-Typ des erkennbaren Elements angewendet wird, wenn sie an gesendet werden CrowdStrike EDR.
Ablaufzeit Des Erkennbaren Domänenelements	Der Ablaufzeitraum in Tagen, der für den Domänentyp des erkennbaren Elements angewendet wird, wenn sie an gesendet werden CrowdStrike EDR.
Ablaufzeit Des Erkennbaren Hash-Elements	Der Ablaufzeitraum in Tagen, der für den Hash-Typ des erkennbaren Elements angewendet wird, wenn sie an gesendet werden CrowdStrike EDR.

7. Klicken Sie auf **Speichern**.
   Die Integrationsdetails werden validiert, und standardmäßig die CrowdStrike Der Status der EDR-Integration ist deaktiviert.
8. Klicken Sie Auf **Aktivieren** Zum Aktivieren von CrowdStrike EDR-Integration.

Hinweis:
Mehrere Konfigurationen sind für zulässig CrowdStrike Falcon EDR-Integration.

Erkennbare Elemente an EDR senden

Senden Sie erkennbare Elemente an das EDR-Sicherheitstool.

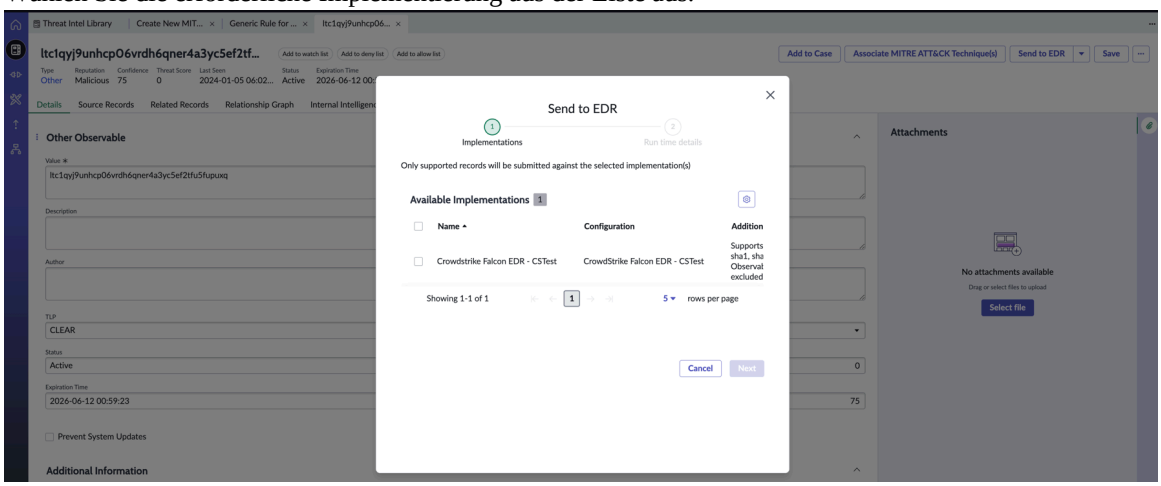
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

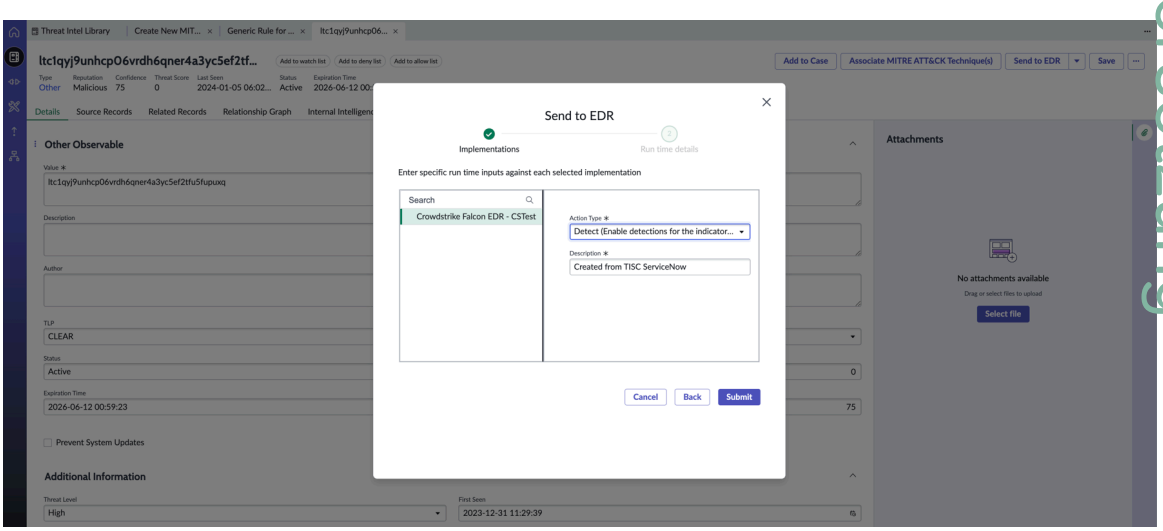
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
4. Öffnen Sie einen beliebigen Datensatz erkennbarer Elemente.
5. Wählen Sie Aus **An EDR senden** .
   An EDR senden **Implementierungen** Der modale Bildschirm wird angezeigt.
6. Wählen Sie die erforderliche Implementierung aus der Liste aus.



7. Klicken Sie auf **Next (Weiter)**.
8. Wählen Sie die Laufzeitdetails aus, z. B. **Aktionstyp** Und **Beschreibung** Der Implementierung.



Die verfügbaren Optionen für CrowdStrike Während der Implementierungslaufzeit sind Details:

- **Keine Aktion (Indikator für zukünftige Verwendung speichern, aber keine Aktion ausführen)** : In der Formularansicht des erkennbaren Elements ist der Bedrohungsschweregrad des erkennbaren Elements für optional CrowdStrike Falcon EDR.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Erkennen (Erkennungen für den Indikator beim Bedrohungsschweregrad des Datensatzes aktivieren)** : In der Formularansicht des erkennbaren Elements ist der Bedrohungsschweregrad für obligatorisch CrowdStrike Falcon EDR. Der Bedrohungsschweregrad des erkennbaren Elements darf für dieses ausgewählte erkennbare Element nicht leer sein.

9. Klicken Sie auf **Absenden**.
   Die ausgewählte Aktion wird ausgeführt, und es wird eine Informationsnachricht angezeigt, die angezeigt wird Die Ausführung „an EDR senden“ des erkennbaren Elements wurde gestartet.

Hinweis:

- Sobald die Ausführung initiiert oder abgeschlossen ist, werden Arbeitsnotizen im Aktivitätenstrom der Formularansicht veröffentlicht.
- **An EDR senden** Die Aktion ist auch in der Liste erkennbarer Elemente unter verfügbar **Artefakte** Registerkarte für einen Falldatensatz. Weitere Informationen finden Sie unter Artefakte zu Fällen oder Fallaufgaben hinzufügen.

Microsoft Defender for EDR-Integration

Die Integration mit Microsoft Defender for EDR ermöglicht es Analysten von Cyber Threat Intelligence (CTI), schädliche oder verdächtige IP-Adressen, Domänen, Datei-Hashes und URLs zur kontinuierlichen Überwachung und Echtzeitwarnung automatisch an Microsoft Defender zu senden.

Registrieren und konfigurieren Sie Microsoft Defender in Microsoft Azure Portal

Registrieren Sie den Microsoft Defender EDR im Microsoft Azure Portal und gewähren Sie Lese- und Schreibzugriff auf die Anwendung.

Vorbereitungen

Erforderliche Rolle: Anwendungsentwickler, Mandantenadministrator.

Prozedur

1. Melden Sie sich beim Microsoft Azure-Portal an.
2. Geben Sie Ein App-Registrierungen Klicken Sie im Suchfeld auf **Klicken Sie auf neue Registrierung** .
3. Geben Sie einen Namen für Ihre Anwendung und den Umleitungs-URI ein, und klicken Sie auf **Registrieren** .
   Ein Beispielname ist Microsoft Defender für Endpunkt . Der Umleitungs-URI wird verwendet, wenn der Administrator die Zustimmung für die Anwendung erteilt.
4. In **App-Registrierungen** Wählen Sie die Anwendung aus, die Sie in Schritt 3 registriert haben.
5. Wählen Sie unter Verwalten die Option aus **Zertifikate und Geheimnisse** .
6. Um ein geheimes Clientgeheimnis zu erstellen, wählen Sie aus **Neues geheimes Clientgeheimnis** .
7. Kopieren Sie das geheime Clientgeheimnis, und speichern Sie es.

   Wenn Sie das geheime Clientgeheimnis vergessen haben, können Sie ein neues geheimes Clientgeheimnis generieren.

8. Navigieren zu **Verwalten** > **API-Berechtigungen**an.
9. Klicken Sie auf **Add a permission (Berechtigung hinzufügen)**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Klicken Sie im Fenster „API-Berechtigungen anfordern“ auf **APIs, die meine Organisation verwendet** Registerkarte.
11. Suchen und wählen Sie aus **WindowsDefenderATP** .
12. Wählen Sie in den WindowsDefenderATP-Berechtigungen die Option aus **Anwendungsberechtigungen** .
    Durch Aktivieren dieser Berechtigung wird sichergestellt, dass die Anwendung als Hintergrundservice oder Daemon ohne angemeldeten Anwender ausgeführt wird.
13. Fügen Sie die folgende Berechtigung auf Anwendungsebene hinzu, und gewähren Sie dem Administrator die Zustimmung für die neu hinzugefügte API-Berechtigung.

Berechtigung	Anzeigename Der Berechtigung
TI.Lesen.Schreiben.alle	Lese- und Schreibindikatoren

Installieren und konfigurieren Sie die Microsoft Defender for EDR-Integration

Installieren und konfigurieren Sie die Microsoft Defender for EDR-Integration aus dem ServiceNow Store.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

- Threat Intelligence-Sicherheitszentrum Die Anwendung muss im ServiceNow Store installiert und aktiviert werden.
- Rufen Sie die API-Mandanten-ID, die Client-ID und das Client-Geheimnis von der Microsoft Defender for EDR-Konsole ab.

Prozedur

1. Laden Sie die Microsoft Defender for EDR-Integration aus dem ServiceNow Store herunter, und installieren Sie sie.
2. Greifen Sie mit Ihrer Instanz auf zu *`Threat Intelligence-Sicherheitszentrum`*.
3. Laden Sie die Integration aus dem herunter ServiceNow Storean.
4. Auswahlvorgang **Integrationen** > **Sicherheitstools** > **EDR**an.
5. Klicken Sie Auf **Konfigurieren Sie die Integration neuer Quelltools** .
6. Wählen Sie Aus **Microsoft Defender für EDR** Option.
7. Klicken Sie auf **Auswählen**.
8. Füllen Sie die folgenden Felder des Formulars aus.

Konfigurieren Sie die Microsoft Defender for EDR-Integration

Feld	Beschreibung
Name	Name für die neue Integrationskonfiguration des Sicherheitstools. Beispiel: Microsoft Defender for EDR-Integration.
Integrationskategorie	Option, die die Integrationskategorie anzeigt.
Lieferantenname	Name des Lieferanten. Die Details des ausgewählten Lieferanten werden standardmäßig ausgefüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Integrationstyp	Option, die den Integrationstyp anzeigt.
Beschreibung	Geben Sie die Beschreibung für die neue Integrationskonfiguration des Sicherheitstools ein.
Integrationskonfiguration	
Basis-URL	Die Basis-URL ist die Basis-URL der Microsoft Defender for EDR-API. Der Standardwert ist https://api.securitycenter.microsoft.com/ .
Mandanten-ID	Die Mandanten-ID, die Sie von Microsoft Defender erhalten haben.
Client-ID	Die Client-ID, die Sie von Microsoft Defender erhalten haben.
Geheimer Clientschlüssel	Der geheime Clientschlüssel, den Sie von Microsoft Defender erhalten haben.
Vorab ausgefüllter Titel (während der Übermittlung verwendet)	Der vorab ausgefüllte Titel definiert den Standardtitel, der während der Übermittlung erkennbarer Elemente an Microsoft Defender verwendet wird. Diese Details werden standardmäßig angezeigt, sodass Sie sie nicht jedes Mal während der Übermittlung an EDR erneut eingeben müssen.
Vorab ausgefüllte Beschreibung (während der Übermittlung verwendet)	Die vorab ausgefüllte Beschreibung definiert den Standardtitel, der während der Übermittlung erkennbarer Elemente an Microsoft Defender verwendet wird. Diese Details werden standardmäßig angezeigt, sodass Sie sie nicht jedes Mal während der Übermittlung an EDR erneut eingeben müssen.
Ablaufzeitraum in Tagen für jede Art von erkennbaren Elementen	Der Ablaufzeitraum in Tagen, der für erkennbare Elemente angewendet wird, wenn sie an Microsoft Defender EDR gesendet werden. **Hinweis:** Diese Option ist ein Fallback-Ablaufzeitraum, wenn die Ablaufzeit für keinen bestimmten erkennbaren Typ festgelegt ist.
Ablaufzeitraum in Tagen für den IP-Typ erkennbarer Elemente	Der Ablaufzeitraum in Tagen, der für den IP-Typ des erkennbaren Elements angewendet wird, wenn sie an Microsoft Defender EDR gesendet werden.
Ablaufzeitraum in Tagen für den Domänentyp erkennbarer Elemente	Der Ablaufzeitraum in Tagen, der für den Domänentyp des erkennbaren Elements angewendet wird, wenn sie an Microsoft Defender EDR gesendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ablaufzeitraum in Tagen für den Hash-Typ erkennbarer Elemente	Der Ablaufzeitraum in Tagen, der für den Hash-Typ des erkennbaren Elements angewendet wird, wenn sie an Microsoft Defender EDR gesendet werden.

9. Klicken Sie Auf **Speichern** Nachdem Sie die erforderlichen Konfigurationsinformationen hinzugefügt haben.
10. Klicken Sie Auf **Aktivieren** Um die Konfiguration zu aktivieren, nachdem Sie die neue Microsoft Defender EDR-Integration gespeichert haben.
    Es wird eine Bestätigungsnachricht angezeigt, dass die Ergänzungsintegration erfolgreich aktiviert wurde.

Ergebnisse

Nachdem die Integration konfiguriert wurde, können Sie in der Threat Intel Library einen beliebigen Typ von erkennbaren Elementen auswählen, die Microsoft Defender EDR unterstützen. Sie können dann erkennbare Elemente an EDR senden. Weitere Informationen finden Sie unter Erkennbare Elemente an EDR senden.

Systemeigenschaften für Microsoft Defender EDR

Im Folgenden werden die Systemeigenschaften für Microsoft Defender EDR beschrieben.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Alle** > **Glide-Eigenschaftenkatalog** > **Glide-Eigenschaften**an.
2. Suchen Sie nach Microsoft Defender-Eigenschaften.

Eigenschaft	Beschreibung
sn_tisc_Defender.rate_Limiter.Minute	Dadurch können Anwender die Rate des Sendens von EDR an MS Defender minutengenau begrenzen. ○ Typ: Ganzzahl ○ Wert: 100
sn_tisc_Defender.rate_Limiter.Hour	Auf diese Weise können Anwender die Rate der Übertragung von EDR an MS Defender stündlich begrenzen. ○ Typ: Ganzzahl ○ Wert: 1500

Erkennbare Elemente an EDR senden

Senden Sie erkennbare Elemente an das EDR-Sicherheitstool.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
4. Öffnen Sie einen beliebigen Datensatz erkennbarer Elemente.
5. Wählen Sie Aus **An EDR senden** .
   An EDR senden **Implementierungen** Der modale Bildschirm wird angezeigt.
6. Wählen Sie die erforderliche Implementierung aus der Liste aus.
   Wählen Sie beispielsweise die Implementierung aus, die Microsoft Defender EDR zugeordnet ist.
7. Klicken Sie auf **Next (Weiter)**.
8. Wählen Sie die Laufzeitdetails aus, z. B. **Titel** Und **Beschreibung** Der Implementierung.
9. Klicken Sie auf **Absenden**.
   Die ausgewählte Aktion wird ausgeführt, und es wird eine Informationsnachricht angezeigt, die angezeigt wird Die Ausführung „an EDR senden“ des erkennbaren Elements wurde gestartet, und die Ergebnisse dieser Ausführung sind nach Abschluss der Ausführung im Aktivitätenstrom verfügbar.

Hinweis:
Sobald die Ausführung initiiert oder abgeschlossen wurde, werden Arbeitsnotizen im Aktivitätenstrom der Formularansicht veröffentlicht, und Sie können den Ausführungsfortschritt entsprechend überprüfen.

TISC-Sicherheitstools: Firewall

TISC-Sicherheitstools: Firewall verhindert nicht autorisierten Zugriff auf das Netzwerk. Die Integration von Palo Alto mit TISC hilft beim Blockieren schädlicher IP-Adressen, URLs und Domänen mithilfe von EDL-Funktionen (External Dynamic List) mit ServiceNow Threat Intelligence-Daten.

Innerhalb von TISC durch Integration mit anderen Sicherheitstools wie Palo Alto Networks Verbessert die Netzwerksicherheit der gesamten Organisation.

Integration von Palo Alto Networks

Die Integration von Palo Alto Networks nach der Konfiguration ermöglicht es dem Bedrohungsanalyst, schädliche IP-Adressen, URLs und Domänen zur externen dynamischen Liste (EDL) hinzuzufügen oder diese Einträge aus der EDL zu entfernen, sobald sie als nicht schädlich oder bereinigt bestätigt wurden.

Eine EDL ist eine Textdatei, die auf einem externen Webserver gehostet wird. Für diese Integration ist dieser Webserver Ihr ServiceNow AI Platform Instanz, die es der Palo Alto Networks-Firewall ermöglicht, Objekte zu importieren, die in der Liste, IP-Adressen, URLs und Domänen enthalten sind.

Erstellen Sie eine neue EDL für Palo Alto Networks

Erstellen Sie eine neue externe dynamische Liste (EDLs) für Palo Alto Networks. Sobald Sie EDLs erstellt haben, können Sie mit der Erstellung von Einträgen für diese EDLs beginnen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Nachdem Sie die neu konfigurierte Palo Alto NGFW-Konfiguration gespeichert haben, navigieren Sie zu **EDLs** Abschnitt.
2. Klicken Sie Auf **Neu** Dient zum Erstellen einer neuen externen dynamischen Liste (EDLs).
3. Füllen Sie im Formular die Felder aus.

Formular „externe dynamische Liste der Palo Alto Networks-Firewall“

Feld	Beschreibung
Name	Name der dynamischen Liste der Palo Alto Networks-Firewall.
Erkennbarer Typ	Wählen Sie einen Typ des erkennbaren Elements aus der Auswahlliste aus, den diese EDL akzeptiert: IP (einschließlich CIDR), URL oder Domäne.
Ablaufzeitraum (in Tagen)	Ablaufzeitraum der EDL. 0 (Standard) gibt an, dass der EDL-Eintrag nie abläuft. Wenn Sie diesen Wert ändern, ist dieser Eintrag für die von Ihnen eingegebene Anzahl von Tagen aktiv. Sie können einen Mindestwert von 1 eingeben, und es gibt keinen Höchstwert. Beispiel: Wenn Sie eingeben 30 Tage um 14:01 Uhr am 1. November läuft die EDL am 30. November um 14:01 Uhr ab. Alle Einträge in dieser EDL erben diesen Wert standardmäßig, es sei denn, Sie überschreiben den Wert für einzelne Einträge.
Change-Anforderung erstellen	Dieses Kontrollkästchen ist standardmäßig aktiviert, um automatisch eine Change-Anforderung und Change-Aufgaben in zu erstellen ServiceNow AI Platform Instanz, die an den EDL-Datensatz angehängt sind. Die Change-Anforderung wird verwendet, um die EDL-Listenabruf-URL im Palo Alto Networks Next-Generation Firewall-Server zu konfigurieren. Diese Option wird empfohlen, wenn Ihr Firewall-Administrator auch verwendet ServiceNow AI Platform Für Firewall-Richtlinien- oder -Regeländerungen. Wenn Sie eine Anforderung erstellen, wird die EDL-Liste automatisch aktiviert, sobald sie geschlossen wurde.
Beschreibung	Beschreibung der dynamischen Liste der Palo Alto Networks-Firewall. Der Name enthält im Allgemeinen die Typen von Sites und erkennbaren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Elementen, die Sie in dieser EDL erwarten, und Sie können dieses Feld für weitere Details verwenden.
Change-Anforderung	Wenn das Kontrollkästchen Change-Anforderung erstellen aktiviert ist, wird die Change-Anforderungsnummer auf angezeigt ServiceNow AI Platform Instanz, sobald die EDL gespeichert wurde. Wenn das Kontrollkästchen für **Erstellen Sie eine Change-Anforderung** Ist gelöscht, wird dieses Feld nicht angezeigt.
IP-Adressen und Subnetzadressen in einem einzigen Eintrag zusammenfassen	Option zum Kombinieren von IP-Adressen und Subnetzadressen in einem einzigen Eintrag. Wenn Sie dieses Kontrollkästchen aktivieren und die IP des CIDR-Typs hinzugefügt wird, werden die vorhandenen Einträge, die in den CIDR-Bereich fallen, automatisch entfernt. Beispiel: Wenn in EDL ein Eintrag mit dem Wert 192.168.1,1 vorhanden ist und der gleiche EDL ein CIDR-Wert von 192.168.1.0/24 hinzugefügt wird, wird der ursprüngliche IP-Adresseintrag entfernt, da er in den CIDR-Bereich des neuen Eintrags fällt. **Hinweis:** Diese Option wird nur angezeigt, wenn Sie auswählen **Typ Des Erkennbaren Elements** Als IP.
EDL-Abruf-URL	Der URL-Link, den der Palo Alto Networks-Firewall-Administrator für die Konfiguration in der Palo Alto Networks-Firewall verwendet, wird automatisch generiert und angezeigt.

4. Erstellen Sie nach Bedarf weitere EDLs, und fügen Sie sie hinzu.
   Die EDLs werden in der Liste „externe dynamische Listen von Palo Alto Networks“ angezeigt.

Zugehörige Informationen

Palo Alto EDL-Genehmigungsregeln

Palo Alto EDL-Genehmigungsregeln

Mit Genehmigungsregeln können Anwender den Genehmigungs-Workflow aktivieren, der zum Genehmigen oder Ablehnen der EDL-Einträge erforderlich ist.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Der TISC-Administrator definiert diese Genehmigungsregeln, um die Zustimmung zu den Genehmigungsanforderungen zu erteilen. Als TISC-Administrator können Sie hier auch mehrere Genehmigungsebenen definieren.

Prozedur

1. Nachdem Sie die neu konfigurierte Palo Alto NGFW-Konfiguration gespeichert haben, navigieren Sie zu **EDL-Genehmigungsregeln** Abschnitt.
2. Klicken Sie Auf **Neu** Dient zum Erstellen einer neuen Genehmigungsregel.
   Die folgenden Regeln sind die vorkonfigurierten Regeln im Basissystem für die Palo Alto NGFW-Integration.

Vorkonfigurierte EDL-Genehmigungsregeln

Name	Beschreibung	EDL-Aktion
Genehmigungsregel zum Hinzufügen zu EDL	Mit dieser Genehmigungsregel können Anwender den Genehmigungs-Workflow zum Hinzufügen von Einträgen zu EDL aktivieren.	Zu EDL hinzufügen
Genehmigungsregel zum Entfernen aus EDL	Mit dieser Genehmigungsregel können Anwender den Genehmigungs-Workflow zum Entfernen von Einträgen aus EDL aktivieren.	Aus EDL entfernen

3. Füllen Sie die Felder im Formular entsprechend aus.

Erstellen Sie neue EDL-Genehmigungsregeln

Feld	Beschreibung
Name	Name der Genehmigungsregel.
EDL-Aktion	Option zum Hinzufügen oder Entfernen des EDL-Eintrags.
EDLs	Wählen Sie die EDLs aus, die eine Genehmigung erfordern. Wenn Sie dieses Feld leer lassen, werden alle EDLs eingeschlossen.
Beschreibung	Geben Sie die Beschreibung für die Genehmigungsregel ein.
Anwender oder Gruppen mit erforderlicher Genehmigung auswählen	
Anwender	Wählen Sie die Anwender aus, die eine Genehmigung erfordern.
Gruppe(n)	Wählen Sie die Gruppe(n) aus, die eine Genehmigung erfordert.
Den/die Genehmiger auswählen	
Anwender	Wählen Sie die Anwender zur Genehmigung aus.
Gruppe(n)	Wählen Sie die Gruppe(n) für die Genehmigung aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Benachrichtigungen	
Anfordernde Person über Genehmigung benachrichtigen	Aktivieren Sie dieses Kontrollkästchen, um die anfordernde Person über die Genehmigung von EDLs zu benachrichtigen.
Anfordernde Person über Ablehnung benachrichtigen	Aktivieren Sie dieses Kontrollkästchen, um die anfordernde Person über die Ablehnung von EDLs zu benachrichtigen.

4. Klicken Sie Auf **Speichern** Dient zum Validieren und Speichern der Genehmigungsregel.
5. Klicken Sie Auf **Aktivieren** Zum Aktivieren der Genehmigungsregel.

Fügen Sie der EDL erkennbare Elemente hinzu

Fügen Sie der externen dynamischen Liste (EDLs) erkennbare Elemente wie IPs, Domänen und Hashes hinzu.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
4. Öffnen Sie einen beliebigen Datensatz erkennbarer Elemente.
5. Klicken Sie Auf **Zu EDL hinzufügen** .
   Der modale Bildschirm „zu EDL hinzufügen“ wird angezeigt.

Entfernen Sie erkennbare Elemente aus EDL

Entfernen Sie erkennbare Elemente aus EDL.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
4. Öffnen Sie einen beliebigen Datensatz erkennbarer Elemente.
5. Klicken Sie Auf **Aus EDL entfernen** .
   Der modale Bildschirm aus EDL entfernen wird angezeigt.

Genehmigen Sie EDL-Einträge für Palo Alto Networks

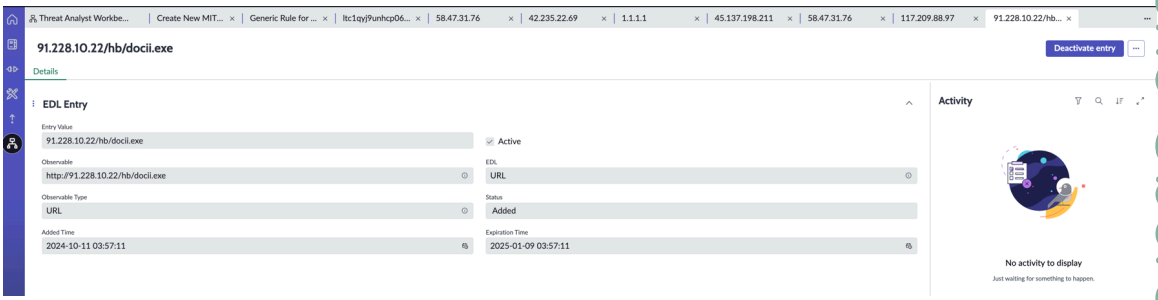
Die Genehmigung von EDL-Einträgen (External Dynamic List) ist Teil der Vorkonfiguration. Sie müssen die EDL-Einträge genehmigen, bevor die Einträge in EDLs für die Firewall aktiviert werden, um den Eintrag abzurufen und die Sicherheitsrichtlinie anzuwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn der Genehmigungsprozess aktiviert ist, wird ein EDL-Eintrag erst dann in der EDL aktiviert oder deaktiviert, wenn er genehmigt wurde.

Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Analyst Workbench für Bedrohungen**an.
2. Drilldown zu **NGFW SCHWENKEN** Abschnitt und wählen Sie den EDL-Datensatz zur Genehmigung aus.
3. Wechseln Sie zu **Meine Genehmigungen** .
4. Wählen Sie die EDL-Datensätze zur Genehmigung aus.
5. Klicken Sie auf **Genehmigen**.
6. Unter **Meine Genehmigung** Anforderungen, klicken Sie auf ein Element in **Status** Spalte zum Öffnen.
7. Wählen Sie die Option zum Genehmigen des EDL-Eintrags aus.
   Nachdem Sie den EDL-Eintrag genehmigt und aktiviert haben, ruft Palo Alto Networks den EDL-Eintrag nach dem nächsten Abrufintervall ab. Nachdem der Eintrag abgerufen wurde, wird das erkennbare Element von diesem Punkt an blockiert. Beachten Sie in der folgenden Abbildung, dass **Aktiv** Das Kontrollkästchen ist aktiviert, der Status wird hinzugefügt, und die Arbeitsnotizen geben an, dass die Anforderung genehmigt wurde.



TISC-Add-on für Splunk-Übersicht

Das Threat Intelligence Security Center (TISC) für Splunk Die App bietet die Integration zwischen TISC und Splunk Damit können Anwender die neuesten Bedrohungsinformationen nahtlos aus TISC in importieren Splunk Zur Überwachung und Ergänzung von Warnungen. Benutzer können Indikatorsammlungen konfigurieren, Suchen durchführen und Dashboards verwenden, um Suchergebnisse und Indikatorsammlungen effektiv zu analysieren.

TISC-Integration mit Splunk

Die Integration zwischen Threat Intelligence-Sicherheitszentrum(TISC) Und Splunk Ermöglicht Anwendern das Filtern und Abrufen relevanter Daten erkennbarer Threat Intelligence-Elemente in Splunk. Innerhalb von Splunk, Die Anwender können diese Daten verwenden, um Sicherheitswarnungen zu generieren.

Erforderliche Rolle: Splunk Administrator

Mit TISC Mit der Add-on-Anwendung können Sie das Intervall konfigurieren, in dem Sie erkennbare Elemente abrufen können ServiceNow TISC Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieses Intervall bestimmt, wie häufig die Anwendung Anforderungen an stellen kann ServiceNow Und rufen Sie die Daten erkennbarer Elemente ab. Außerdem können Sie Filter definieren und anwenden, um die erkennbaren Elemente anzugeben, die Sie aus abrufen möchten ServiceNow TISC Instanz.

Sobald die erkennbaren Elemente aus abgerufen wurden ServiceNow, Die Daten erkennbarer Elemente werden in gespeichert Splunk KV Store (Key-Value Store) und Sie können die Korrelationsregeln weiter über den Satz der erkennbaren Elemente schreiben, die abgerufen wurden.

Erstellen von Anwendern in ServiceNow TISC Instanz

Sie können Anwender in erstellen ServiceNow TISC Instanz mit einer gültigen Anwenderrolle: sn_sec_tisc.api_obs_read_Access.

Installieren TISC Add-on-App auf Splunk

Weitere Informationen finden Sie unter Weisen Sie einem Anwender eine Rolle zu .

Erforderliche Rolle: Splunk admin.

1. Melden Sie sich bei an *Splunk*.
2. Navigieren zu **Apps** > **Apps verwalten** Oder klicken Sie auf **Verwalten** Zahnradsymbol.
3. Suchen Sie nach *Threat Intelligence-Sicherheitszentrum***Für** *Splunk*App und installieren Sie sie.
4. Nach der Installation ist die Anwendung unter der Liste der Apps sichtbar.

Wird Konfiguriert TISC Add-on in Splunk

Gehen Sie wie folgt vor, um die Anwendung zu konfigurieren.

Vorbereitungen
Erforderliche Rolle: Splunk Administrator

Warum und wann dieser Vorgang ausgeführt wird
Im folgenden Verfahren wird die Konfiguration des TISC-Add-ons in beschrieben Splunk.

Prozedur

1. Suchen Sie nach **Threat Intelligence-Sicherheitszentrum für Splunk** App aus der linken Navigation.
2. Klicken Sie auf **Einrichten** Unter **Aktionen** Spalte.
   Die **Konfiguration** Seite wird angezeigt, und Sie können einrichten ServiceNow TISC Account.
3. Wählen Sie **Hinzufügen**.
4. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Konten hinzufügen	
Name	Ein eindeutiger Name für den Account.
Anwendername	Geben Sie an ServiceNow Account-Anwendername. Sie können denselben Anwendernamen verwenden, der für die Anwender verwendet wird, der während der Rollenerstellung erstellt wird

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	`sn_sec_tisc.api_obs_read_Access` Im obigen Schritt.
Passwort	Geben Sie An ServiceNow Account-Passwort.
Instanz-URL	Geben Sie an ServiceNow Instanz-URL-Adresse.

5. Klicken Sie auf **Hinzufügen**.
   Die ServiceNow Instanzaccount wird zu hinzugefügt Splunk.
6. Navigieren Sie zu **Eingaben** Seite zum Erstellen von Sammlungen verwalten Sie Ihre Dateneingaben für ServiceNow Account.
7. Klicken Sie Auf **Neue Eingabe Erstellen** .
   Die **Eingabe Hinzufügen** Das Dialogfeld wird angezeigt, in dem Sie die Eingaben zu hinzufügen können ServiceNow Account.

   Sobald der Eingabesatz definiert ist, sendet die Anwendung die Informationen an den TISC Instanz zum Abrufen einer bestimmten Anzahl erkennbarer Elemente, die die Kriterien erfüllen.
8. Geben Sie die Eingabedetails entsprechend ein.

Feld	Beschreibung
Name	Ein eindeutiger Name für Ihre Eingabe. Beispiel: Liste schädlicher IP-Adressen.
Account	Geben Sie an ServiceNow Account-Anwendername. Sie können denselben Anwendernamen verwenden, der für die Anwender verwendet wird, die mit der Rolle erstellt werden `sn_sec_tisc.api_obs_read_Access` Im obigen Schritt.
Intervall	Legen Sie das Zeitintervall in Sekunden fest, aus dem die Daten abgerufen werden sollen TISC.
Ablaufzeitraum (in Tagen)	Option zum Festlegen des Ablaufzeitraums in Tagen. **Hinweis:** Der Ablauf des Beispiels ist auf 30 Tage festgelegt. Wenn beispielsweise Daten an einem bestimmten Datum abgerufen werden, kann ein Satz von 10.000 Datensätzen abgerufen werden. Diese Datensätze werden im KV-Speicher (Key-value) in gespeichert Splunk. Ab dem Erfassungsdatum werden die Datensätze 30 Tage lang aufbewahrt. Am 31. Tag werden sie automatisch aus dem KV-Store gelöscht.
Läuft Nie Ab	Wählen Sie diese Option aus, wenn Sie die erfassten Datensätze nicht ablaufen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zusätzliche Attribute	Ermöglicht Ihnen das Hinzufügen zusätzlicher Attribute aus der Liste der empfohlenen Optionen, die in den KV-Store aufgenommen werden sollen. Attribute müssen durch Kommas getrennt werden. Eine Liste der zulässigen Attribute wird in der Tabelle nach der Tabelle mit obligatorischen Attributen bereitgestellt.
Filter	Definieren Sie die Bedingungen, anhand derer Daten importiert werden sollen, gefiltert werden. Um die Filterbedingungen festzulegen, können Sie die Kriterien basierend auf den Feldern wie Bedrohungspunktzahl, Konfidenzniveau und Typ definieren. Für einfache Filterbedingungen können Sie diese Filteroption verwenden. Wenn die Filterbedingungen jedoch komplexer sind und Sie erweiterte Filterung durchführen, können Sie JSON-Filter hinzufügen. ○ Die zulässigen Ganzzahloperatoren sind: "=", "!=", ">", "<", ">=", "<=" ○ Die zulässigen Zeichenfolgenoperatoren sind: „=“, „!=“, „IN“ **Unten finden Sie ein Beispiel für einen einfachen Filter** : {Sample filter format: Allowed Tokens: "threat_score", "confidence", "reputation", "type", "value". Allowed Integer Operators: "=", "!=", ">", "<", ">=", "<=". Allowed String Operators: "=", "!=", "IN". Example: reputation IN ("clean","suspicious","malicious") AND threat_score > 90 AND confidence > 90 AND type = "ip_v4_address"}
JSON	Mit JSON-basierten Filtern können Sie kompliziertere Bedingungen definieren. Der Status des JSON-Objekts muss „aktiv“ sein. Wählen Sie Aus **JSON** Kontrollkästchen „Filter“, um zu erweiterten Filtern zu wechseln, bei denen eine JSON zum Anwenden der Filterbedingung verwendet werden kann.

Beispiel für erweiterten Filter :

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

{"boolean_operator":"AND","filters":[{"field_name":"reputation","operator":"IN","field_value":"clean,suspicious,malicious"},{"field_name":"threat_score","operator":">","field_value":"90"},{"field_name":"confidence","operator":">","field_value":"90"},{"field_name":"type","operator":"=","field_value":"ip_v4_address"}]}

Hinweis:
Accounts sind standardmäßig aktiv, Eingaben sind jedoch standardmäßig inaktiv. Sie müssen sie aktivieren, um mit dem Importieren der Daten zu beginnen. Mögliche Filter finden Sie im Abschnitt „Observable_Filters“ in Fügt dem Threat Intelligence Security Center (TISC) Quelldatensätze erkennbarer Elemente hinzu Anwendung.

9. Klicken Sie Auf **Hinzufügen** Zum Hinzufügen der Eingaben.
10. Klicken Sie Auf **Klon** Oder kopieren, um einen neuen Account basierend auf dem vorhandenen Account zu kopieren und zu erstellen.
    Stellen Sie sicher, dass die Eingabe vor dem Klonen deaktiviert ist, um zu vermeiden, dass beim Importieren von Daten mit denselben Kriterien doppelte Einträge erstellt werden.
11. Sobald die Daten abgerufen wurden, werden die folgenden Informationen abgerufen und im KV-Speicher in gespeichert Splunk Zusammen mit den aus TISC abgerufenen Datensätzen:

Feld	Beschreibung
confidence	Gibt das Konfidenzniveau an, das der Genauigkeit der Bedrohungspunktzahl zugeordnet ist.
Kvlookup_created_time	Gibt die Datensatzerstellungszeit im Schlüssel-Wert-Speicher an.
Kvlookup_days_to_expiry	Gibt die Anzahl der Tage an, nach denen der Datensatz aus dem KV-Store gelöscht wird.
instance_url	Gibt an ServiceNow Instanz-URL-Adresse.
Reputation	Gibt die Reputation der beteiligten Entität an.
Source_reports_score	Die gemeldete Quellpunktzahl von TISC.
sys_id	SYS-ID des Datensatzes, der durchgeht TISC.
Threat_level	Gibt den Schweregrad der Bedrohung an.
Threat_Score	Die Punktzahl, die das Ausmaß der Bedrohung angibt, die einem Datensatz zugeordnet ist.
Threat_severity	Gibt den Bedrohungsschweregrad des erkennbaren Elements an.
type	Gibt den Typ der erkennbaren Elemente an.
Aktualisiert_von	Stellt Informationen dazu bereit, wer den Datensatz zuletzt aktualisiert hat.
Kvlookup_updated_time	Gibt den Zeitstempel an, zu dem der Datensatz zuletzt im Schlüsselwertspeicher aktualisiert wurde.
Wert	Wert des Datensatzes. Beispiel: IP, Hash usw.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Attribute

Feld	Beschreibung
additional_context	Geben Sie bei Bedarf zusätzlichen Kontext an.
Attack_Phases	Gibt Angriffsphasen in einer Kill Chain an, z. B. LM, MITRE ATT&CK.
Autor	Geben Sie den Autorennamen an.
Kommentare	Fügen Sie nach Bedarf zusätzliche Kommentare hinzu.
erstellt	Gibt an, wann das erkennbare Element erstellt wurde.
Beschreibung	Geben Sie die Beschreibung an.
Ablaufzeit	Gibt die Ablaufzeit des Datensatzes des erkennbaren Elements an.
Erweiterungen	Gibt die Erweiterungen eines erkennbaren Elements an.
First_Observed	Das erste Mal, dass die Daten beobachtet wurden.
first_seen	Das erste Mal, dass dieser Datensatz schädliche Aktivitäten ausgeführt hat.
Historisch_signifikant	Gibt an, ob das erkennbare Element als historisch signifikant betrachtet wird. Diese TISC-Systemkennzeichnung wird verwendet, um das erkennbare Element von der Archivierung auszuschließen.
id	Eindeutiger Bezeichner, der dem erkennbaren Element vom TISC-System zugewiesen ist.
Is_defanged	Kennzeichnung, die angibt, ob der Wert des erkennbaren Elements geändert wurde.
Ist_falsch_positiv	Eine boolesche Kennzeichnung, die angibt, ob das erkennbare Element als falsch positiv identifiziert wird.
language	Gibt die Sprache des Textinhalts in diesem Objekt an.
Last_Observed	Der Zeitpunkt, zu dem die Daten zuletzt beobachtet wurden.
last_seen	Die Zeit, zu der dieses Objekt zuletzt schädliche Aktivitäten ausgeführt hat.
Notizen	Fügen Sie zusätzliche Notizen für einen Datensatz erkennbarer Elemente hinzu.
Nummer	Vom System generierte Nummer, die dem erkennbaren Element von TISC zugewiesen wurde.
Security_type	Gibt an, ob das erkennbare Element zur Allowlist oder Denylist gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
No_of_sources	Stellt die Anzahl der eindeutigen Quellen dar, die zum erkennbaren Element beigetragen haben.
Quellen	Gibt die Bedrohungsquelle an, aus der dieser Datensatz erstellt wird.
status	Geben Sie den Status des erkennbaren Elements ein, ob aktiv oder inaktiv.
tisc_Tags	Wählen Sie die TISC-Tags aus, die einem erkennbaren Element zugeordnet sind.
Taxonomien	Wählen Sie die Taxonomie aus, die einem erkennbaren Element zugeordnet ist.
tlp	Eindeutiger Wert, der die Einstellung für die Datensensibilität pro TLP angibt.
aktualisiert	Gibt an, wann der Datensatz des erkennbaren Elements zuletzt aktualisiert wurde
Usage_Categories	Kategorien, unter die das erkennbare Element fällt, z. B. Botnet oder Phishing.
Watch_list	Kennzeichnung, die angibt, ob das erkennbare Element in der Beobachtungsliste enthalten ist.

Diese Felder sowie alle anderen, die durch Ihre Kriterien definiert sind, sind in verfügbar Splunk Und können über die Registerkarte „Suche“ angezeigt, durchsucht und analysiert werden.

Datenspeicher in Splunk

In diesem Abschnitt wird erläutert, wie TISC Verwendet Suchvorgänge während der Integration im Splunk-Schlüssel-Wert-Speicher für die Datenspeicherung. Es wird beschrieben, wie diese Suchvorgänge in konfiguriert und abgerufen werden Splunk.

Nachschlagen	Suchbeschreibung
`tisc_store_lookup`	Name der KV-Suche, die zum Durchsuchen der eingehenden Datensätze verwendet werden soll.
`tisc_kv_store`	Name des KV-Speichers, in dem sich die Daten befinden.
`inputlookup <lookup_name>" example : | inputlookup tisc_store_lookup`	Abfrage zum Suchen von Datensätzen im KV-Store.

TISC – Microsoft Sentinel-Integration

Threat Intelligence-Sicherheitszentrum Für Microsoft bietet Sentinel mehrere Funktionen, einschließlich des Imports erkennbarer Elemente aus TISC In Sentinel, um Sentinel-Incidents mit Details zu zugehörigen erkennbaren Elementen zu ergänzen und auch den Export erkennbarer Elemente von Sentinel nach zu ermöglichen TISC.

Hinweis:
In Microsoft Sentinel werden erkennbare Elemente als Entitäten bezeichnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Abhängigkeiten

Die **Threat Intelligence** Lösung aus Microsoft Sentinel Content Hub muss installiert sein.

Rollen und Berechtigungen

Anwendung	Rollen und Berechtigungen	Beschreibung
Microsoft Sentinel-spezifische Rollen	1. Beitragender Der Logic-App 2. Microsoft Sentinel-Beitragender	1. Zum Installieren der erforderlichen Playbooks auf Ressourcengruppenebene. 2. Interagieren Sie mit Microsoft Sentinel-Playbooks. Weitere Informationen finden Sie unter Rollen und Berechtigungen In Microsoft Sentinel.
Threat Intelligence-Sicherheitszentrum	sn_sec_tisc.api_Azure_sentinel_Solution	Der im anwenderdefinierten TISC-Connector konfigurierte Anwender muss über diese Rolle verfügen, um den Zugriff auf TISC-APIs zu ermöglichen.

TISC-Playbook-Vorlagen

In diesem Abschnitt werden die Playbook-Vorlagen beschrieben, die im Lieferumfang der TISC Sentinel-Lösung enthalten sind.

Playbook-Anwendungsfälle

In der folgenden Tabelle werden die verschiedenen Playbook-Anwendungsfälle beschrieben.

Anwendungsfall	Playbook	Beschreibung
Erkennbare Elemente werden aus TISC nach Sentinel importiert	Batch_Indicator_Uploader	Stellt einen Batching-Mechanismus für den Export erkennbarer Elemente aus TISC mithilfe der Upload-Indikatoren-API bereit, die von Microsoft Sentinel bereitgestellt wird.
	Import_Observables_Batch	Aktiviert den geplanten Export erkennbarer Elemente aus TISC.
Exportieren Sie Entitäten aus Sentinel nach TISC	Export_Incident_Entitäten	Exportieren Sie alle Entitäten eines Sentinel-Incidents.
	Export_Hash_Entity	Exportieren Sie Datei-Hash-Entitäten des Sentinel-Incidents.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook-Anwendungsfälle

In der folgenden Tabelle werden die verschiedenen Playbook-Anwendungsfälle beschrieben.

(Fortsetzung)

Anwendungsfall	Playbook	Beschreibung
	Export_Domain_Entity-Entitäten	Exportieren Sie Domänenentitäten des Sentinel-Incidents.
	Export_IP_Entity	Exportieren Sie IP-Entitäten des Sentinel-Incidents.
	Export_URL_Entity	Export-URL-Entitäten des Sentinel-Incidents.
Bereichern Sie Sentinel-Incidents	Incident_Enrichment	Ermöglicht die Ergänzung von Sentinel-Incidents, indem Details zu Entitäten abgerufen werden, die ihm zugeordnet sind, und Informationen in Form von Kommentaren zum Incident veröffentlicht werden.

Hinweis:
Alle Playbooks verwenden intern TISC Custom Connector, um TISC-APIs zu verwenden.

Erstellen Sie Playbooks aus Vorlagen

1. Navigieren Sie zu T **ISC-Lösung** Inhaltsseite aus dem **Content Hub im Sentinel-Arbeitsbereich** .
2. Gehen Sie für jedes Playbook, das auf der Inhaltsseite angezeigt wird, wie folgt vor:
   a. Wählen Sie die Playbook-Vorlage aus. Auf der rechten Seite des Bildschirms wird ein Kontextbereich angezeigt **Konfiguration** .
   b. Lesen Sie die Beschreibung der Playbook-Vorlage, und gehen Sie durch **Voraussetzungen** Und **Nach der Bereitstellung** Schritte, die in der Beschreibung erwähnt werden.
   c. Klicken Sie auf **Anwenderdefinierten Connector bereitstellen** (Wenn Sie den anwenderdefinierten Connector noch nicht bereitgestellt haben).

      Fügen Sie hinzu **ServiceNow-Instanz-URL** Auf der **Bereitstellungskonfiguration** Seite.

   d. Klicken Sie Auf **Erstellen Sie Ein Playbook** , Werden Sie zum Bildschirm „Bereitstellungskonfiguration“ weitergeleitet
   e. Auf dem Bildschirm Playbook-Konfiguration erstellen:
      - Wählen Sie die entsprechende Ressourcengruppe aus.
      - Ändern Sie den Playbook-Namen, oder verwenden Sie den Standardnamen.
      - Geben Sie an **Anwenderdefinierter Connector-name** E (stellen Sie sicher, dass dies mit dem Namen des Connectors übereinstimmt, den Sie im vorherigen Schritt bereitgestellt haben) im Abschnitt „Parameter“.
      - Klicken Sie Auf **Überprüfen und erstellen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie das Playbook „Import_observables_Batch“

Stellen Sie sicher, dass Sie das Playbook „Batch_Indicator_Uploader“ erstellen, bevor das Playbook „Import_observables_Batch“ erstellt wird.

1. Navigieren zu **Logik-App-Designer** Zum Bearbeiten des Playbooks.
2. Aktualisieren Sie die Wiederholungszeit (in Stunden) nach Bedarf.
3. Aktualisieren Sie in der Komponente „Anwenderdefinierter TISC-Connector“ im Playbook die Parameter, die an die TISC-API gesendet werden.

Parametername	Beschreibung
Erkennbarer Typ	Im Folgenden sind die unterstützten Typen aufgeführt. Wählen Sie mindestens einen aus: ○ IP ○ Datei-Hash ○ Domäne ○ URL
Bedrohungsbewertung	Geben Sie die Bedrohungspunktzahl für erkennbare Elemente ein. Der Bedrohungspunktzahlwert MUSS eine Zahl im Bereich von 0 bis 100 sein.
Vertrauen	Geben Sie die Konfidenz für erkennbare Elemente ein. Der Konfidenzwert MUSS eine Zahl im Bereich von 0–100 sein.
Reputation	Im Folgenden sind die unterstützten Werte aufgeführt. Wählen Sie mindestens einen aus: ○ Clean ○ Böswillig ○ Verdächtig ○ Unbekannt
Bedrohungsschweregrad	Im Folgenden sind die unterstützten Schweregradstufen aufgeführt. Wählen Sie mindestens einen aus: ○ Kritisch ○ Hoch ○ Mittel ○ Niedrig
Bedrohungsstufe	Im Folgenden sind die unterstützten Bedrohungsstufen aufgeführt. Wählen Sie mindestens eine aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Beschreibung
	○ Hoch ○ Mittel ○ Niedrig
Zuletzt aktualisiertes Delta in Stunden	Die letzte Aktualisierungszeit (in Stunden) für erkennbare Elemente.

Konfigurieren Sie das Playbook „Export_Incident_Entities“

Dieses Playbook verwendet die TISC-API „erkennbare Elemente hinzufügen“. Mit dem Logic-App-Designer können Sie die Parameter bearbeiten, die aus dem Playbook an die API gesendet werden. Weitere Informationen finden Sie unter TISC-API – POST /sn_sec_tisc/Threat_intel_Data/add_observables .

Sie können das gleiche Verfahren für alle unten aufgeführten Playbooks ausführen, die verschiedene Arten von Entitäten exportieren:

- Export_Hash_Entity
- Export_Domain_Entity
- Export_IP_Entity
- Export_URL_Entity

Konfigurieren Sie das Playbook „Incident_Enrichment“

Dieses Playbook verwendet die TISC-API erkennbarer Elemente. Mit dem Logic-App-Designer können Sie die Parameter bearbeiten, die aus dem Playbook an die API gesendet werden. Weitere Informationen finden Sie unter TISC-API – POST /sn_sec_tisc/Threat_intel_Data/observables .

Führen Sie Playbooks aus

In der folgenden Tabelle wird beschrieben, wie Sie die folgenden Playbooks ausführen können.

Playbook	Aktion
Import_Observables_Batch	Dieses Playbook wird automatisch basierend auf der geplanten Zeit ausgeführt, die im Wiederholungsauslöser erwähnt wird.
Export_Incident_Entitäten	Wählen Sie für einen Sentinel-Incident die Option aus **Incident-Aktionen** > **Playbook Ausführen** Zur Ausführung.
Export_Hash_Entity	Wählen Sie für einen Sentinel-Incident die Option aus **Datei-Hash-Entität** > **Playbook Ausführen** Zur Ausführung.
Export_Domain_Entity	Wählen Sie für einen Sentinel-Incident die Option aus **Domänenentität** > **Playbook Ausführen** Zur Ausführung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook	Aktion
Export_IP_Entity	Wählen Sie für einen Sentinel-Incident die Option aus **IP-Entität** > **Playbook Ausführen** Zur Ausführung.
Export_URL_Entity	Wählen Sie für einen Sentinel-Incident die Option aus **URL-Entität** > **Playbook Ausführen** Zur Ausführung.
Incident_Enrichment	Wählen Sie für einen Sentinel-Incident die Option aus **Incident-Aktionen** > **Playbook Ausführen** Zur Ausführung.

Threat Intelligence-Sicherheitszentrum verwalten

Verwenden Sie die linke Navigation, um in zum Modul Administration zu navigieren Threat Intelligence-Sicherheitszentrum Und zeigen Sie die folgenden Module von an TISC Datenverwaltung, um Filterregeln und Genehmigungsregeln weiter festzulegen, Bedrohungspunktzahl zu definieren und Benachrichtigungen zu verwalten.

Datenverwaltung

Modul	Beschreibung
Regel-Engine	Dieser Abschnitt enthält die folgenden Regeln, die während der Datenverwaltung erforderlich sind: 1. **Genehmigungsregeln Für Datenimporte** : Definieren Sie die Genehmigungsregeln, und integrieren Sie den Genehmigungs-Flow in den Abschnitt „Intelligence importieren“, nachdem Sie den Datenimport übermittelt haben. 2. **Eingehende Filterregeln** : Erstellen Sie Filterregeln, um die Daten der eingehenden Quelldatensätze zu filtern. 3. **Bedrohungsbewertungsregel** : Passt den Rechner für Bedrohungsbewertung an, der den erkennbaren Elementen die Bedrohungsbewertung zuweist.
Sicherheitskontrolllisten	Dieses Modul hilft Ihnen bei den Sicherheitskontrollen: 1. **AllowList** 2. **DenyList** 3. **Beobachtungsliste**
Taxonomien	Dieses Modul hilft Ihnen beim Erstellen von Taxonomien für die Datenquellendatensätze.
Benachrichtigungen	Dieses Modul definiert, wie E-Mail-Benachrichtigungen verwaltet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenverwaltung (Fortsetzung)

Modul	Beschreibung
Vorlagen	In diesem Modul wird beschrieben, wie Berichtsvorlagen sowohl in der Designzeit als auch in der Laufzeit-Experience erstellt werden.

Definieren Von Genehmigungsregeln Für Datenimporte

Verwenden Sie diesen Abschnitt, um die Genehmigungsregeln zu definieren und den Genehmigungs-Flow nach dem Senden des Datenimports in den Abschnitt „Intelligence importieren“ zu integrieren.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Verwaltung** Symbol im Arbeitsbereich.
3. Gehe zu **Regel-Engine** > **Genehmigungsregeln für Datenimporte**an.
4. Wählen Sie Aus **Genehmigungsregel für Datenimporte** .

   Innerhalb des Basissystems **Genehmigungsregel für Datenimporte** Ist die standardmäßige Genehmigungsregel bereitgestellt, damit Anwender den Genehmigungs-Workflow aktivieren können.

5. Geben Sie mindestens einen Anwendernamen oder eine Anwendergruppe für jeden von ein **Wählen Sie Anwender oder Gruppen aus, die eine Genehmigung erfordern** Und **Genehmiger auswählen** Abschnitt.
6. Klicken Sie auf **Aktivieren** Schaltfläche zum Aktivieren des Genehmigungs-Flows für die Datenimporte.

   Wenn diese Option aktiviert ist, befinden sich die Datenimporte in der Genehmigungswarteschlange, damit der Genehmiger die Datenverarbeitung genehmigen oder ablehnen kann. Der Genehmiger überprüft die vom Analyst vorgenommenen Änderungen und genehmigt dann die Datenimportanforderung oder lehnt sie ab.

Hinweis:
Eine E-Mail-Benachrichtigung wird an die Anwender oder Anwendergruppen gesendet, dass der Importauftrag verarbeitet und genehmigt oder abgelehnt wird.

Ablaufregeln Werden Definiert

Definieren Sie Ablaufregeln für verschiedene erkennbare Elemente oder eine Kombination verschiedener Quellobjekte oder Indikatorquellen, die in TISC erstellt werden.

Vorbereitungen

Jede Quelle, die in der Anwendung erstellt wird, hat einen Ablaufzeitraum. Die Daten-Feeds verwenden Techniken wie einen zeitbasierten Ablaufzeitraum, um die Datenerfassung zu beschleunigen. In TISC definieren die Ablaufregeln die Ablaufzeit für einen bestimmten Satz von Datenquellen oder eine Reihe von Objekttypen oder Typen erkennbarer Elemente.

Erforderliche Rolle: sn_sec_tisc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Ablaufregeln**an.
   Die Seite Ablaufregeln wird angezeigt.
3. Klicken Sie auf **Neu**.
4. Klicken Sie Auf **Aktivieren** Um die Ablaufregel zu aktivieren, nachdem Sie eine neue Regel erstellt haben. Wenn Sie die Ablaufregel nicht aktivieren, wird die Regel nicht auf den Quelldatensatz angewendet.

   Hinweis:

   - Immer wenn Sie eine Ablaufregel aktivieren, wird im Hintergrund eine Duplikationsprüfung durchgeführt, um zu überprüfen, ob im System eine doppelte Regel mit derselben Kombination aus Datenquellen und Datensatztyp vorhanden ist. Wenn dies der Fall ist, wird von der Anwendung eine Informationsnachricht ausgegeben, dass die Regel bereits dieselbe Kombination aus Datenquelle und Objektkategorie enthält. Sie müssen die vorhandene Kombination ändern, um die Regel zu aktivieren.
   - Eine Beispielablaufregel wird für die Anwender im Basissystem bereitgestellt und dies **Beispiel Für Ablaufregel** Für erkennbares Element befindet sich standardmäßig im deaktivierten Status, und Sie müssen die Regel aktivieren und aktivieren.

5. Klicken Sie auf **Speichern**.
6. Klicken Sie Auf **Löschen** Wenn Sie eine Ablaufregel löschen möchten.

Ablaufregeln für Quelldatensätze

Ablaufregeln sind grundsätzlich hilfreich, um die Ablaufzeit für die Quelldatensätze festzulegen. Der Aggregatdatensatz erbt die höchste Ablaufzeit aus den entsprechenden Quelldatensätzen.

Wie die Regeln angewendet werden

Example: Der Datensatztyp der eingehenden Quelle ist Malware vom Datenquellentyp CrowdStrike

Regelauswertungsprozess basierend auf den Regeln, die für die Anwendung von Ablaufzeiten auf Quelldatensätze bereitgestellt werden:

1. **Alle aktivierten Regeln abrufen:** Die Anwendung überprüft zunächst alle derzeit aktivierten Regeln.
2. Auf bestimmte Regelkombination prüfen:

   Suchen Sie nach einer Regel, die speziell der Kombination von entspricht:

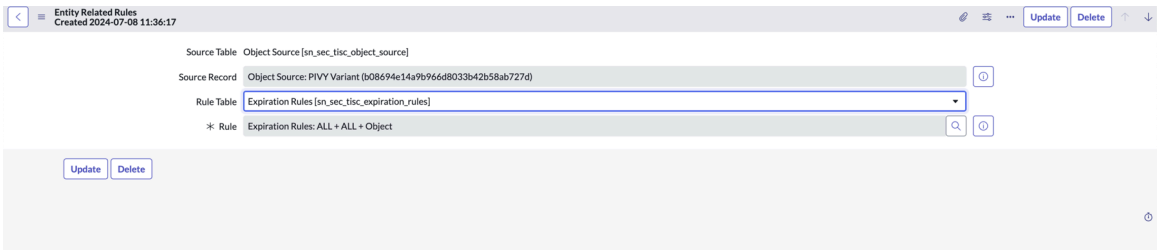
   - **Datenquellentyp** : CrowdStrike
   - **Typ der Datensätze** : Malware

3. **Priorität basierend auf den Übereinstimmungsregelkombinationen:**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn eine Regel vorhanden ist, bei der der Datenquelltyp lautet **CrowdStrike** Und der Datensatztyp ist **Malware** , Diese Regel hat Vorrang. Die in dieser Regel angegebene Ablaufzeit wird angewendet.

4. **Fallback-Regeln:**
   a. Wenn keine Regel mit übereinstimmt **CrowdStrike und Malware** Kombination, sucht das System nach einer Regel, bei der der Datenquelltyp lautet **CrowdStrike** Und der Datensatztyp ist **Alle** .
   b. Wenn immer noch keine Regel gefunden wird, wird nach einer Regel gesucht, bei der der Datenquelltyp lautet **Alle** Und der Datensatztyp ist **Malware** .
   c. Wenn keine der obigen Regeln vorhanden ist, wird standardmäßig eine Regel verwendet, bei der sowohl Datenquellentyp als auch Datensatztyp sind **Alle** .
5. Wenn keine dieser Regeln im System vorhanden ist, wird keine Ablaufregel auf die Quelldatensätze angewendet. Navigieren Sie in diesem Fall zur folgenden Tabelle (im Screenshot angezeigt), um die Kombination der Regeln zu überprüfen, die auf die Objekte angewendet wurden.



6. **Löschen von Datenquellen:**

   Angenommen, wenn eine Datenquelle, der die Ablaufregeln zugeordnet sind, gelöscht wird, kann die Löschung eingeschränkt oder nicht zulässig sein, bis diese Regeln behandelt wurden. Dadurch wird sichergestellt, dass keine Inkonsistenzen bei der Anwendung von Ablaufrichtlinien auftreten.

Erstellen Sie Ausschlussregeln Für Eingehende Daten

Erstellen Sie Ausschlussregeln für eingehende Daten, um beliebige Datentypen oder eingehende Quelldatensatzdaten zu filtern.

Vorbereitungen

Die Anwendung unterstützt die Integration mehrerer Threat Intelligence-Feeds, einschließlich STIX-Datenquellen. Um sicherzustellen, dass nur relevante Daten erfasst werden, müssen anpassbare Ausschlussregeln angewendet werden.

Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird

Ausschlussregeln werden erstellt und auf einen Quelldatensatz angewendet, um weitere Schritte zu verarbeiten. Das -Basissystem stellt bereit **Beispiel Für Filterregel** Für Anwender mit einer vordefinierten Regel zum Filtern der erfassten erkennbaren Elemente, Indikatordaten oder Entitäten/Objekte.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Drilldown zu **Regel-Engine** > **Ausschlussregeln für eingehende Daten**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie Auf **Neu** Zum Definieren von Ausschlussregeln.
   Die Seite neue Ausschlussregeln für eingehende Daten erstellen wird angezeigt.
4. Füllen Sie im Formular die Felder aus.

Definieren Sie Ausschlussregeln

Feld	Beschreibung
Name	Name der neuen Ausschlussregel.
Beschreibung	Kurzbeschreibung der Ausschlussregel.
Reihenfolge	Die Priorität der Ausschlussregel. Dieses Feld gibt die Reihenfolge an, in der die Ausschlussregeln ausgeführt werden, wenn zwei oder mehr Regeln die auslösenden Bedingungen gemeinsam haben. Die Ausschlussregel mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Beispiel: 100, 200, 300 usw. Der Standardwert für die Ausschlussregel des Basissystems ist 100.
Datenquellen	Wählen Sie die Feeds aus, für die die Ausschlussregel angewendet werden soll.
Tabelle	Wählen Sie den Typ der Tabelle aus, für die Sie den Filter anwenden möchten. Beispiel: Quelle des erkennbaren Elements, Indikatorquelle und Objektquelle.
Filtertyp (nur wenn die ausgewählte Tabelle Quelle erkennbarer Elemente ist)	Filtertypen enthalten zwei Optionen, auf denen Sie den Filter anwenden können. ○ Basierend auf Bedingung filtern ○ Basierend auf Liste filtern
Filtertyp (Filter basierend auf Bedingung)	Filterbedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der Quelltabelle. Beispielsweise haben Indikatorquelle und Objektquelle nur den Filtertyp: Filter basierend auf Bedingung. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER** . Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neuer Bedingungssatz** .
Filtertyp (Filter basierend auf Liste)	Wenn die eingehenden erkennbaren Elemente mit den Einträgen in der ausgewählten Liste übereinstimmen, werden sie gefiltert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Diese Ausschlussregeln gelten nicht für Datenimporte mit Import Intelligence, und die verfügbaren Optionen sind Allow-Liste, Deny-Liste und Beobachtungsliste.

Die von der Ausschlussregel ausgeschlossenen Datensätze können in den folgenden Abschnitten angezeigt werden.

a. **Gefilterte Datensätze Erkennbarer Elemente** : Filtert und listet die Datensätze erkennbarer Elemente auf.

b. **Datensätze Gefilterter Indikatoren** : Filtert und listet die Indikatordatensätze auf.

c. **Gefilterte Objektdatensätze** : Filtert und listet die Objektdatensätze auf.

Hinweis:
Um die Ausschlussregeln basierend auf Tags anzuwenden, die den Quelldatensätzen hinzugefügt werden, wählen Sie dann aus *TISC***Tags** Option im Generator für Filterbedingungen.

Anwenderdefinierter Rechner für Bedrohungsbewertung in TISC

Mit dem anwenderdefinierten Bedrohungsbewertungsrechner können Sie eine Punktzahl des Bedrohungsschweregrads eines erkennbaren Elements basierend auf den anwenderdefinierten Kriterien definieren und berechnen, was eine transparente Intelligenzbewertung erkennbarer Elemente bietet. Die Bedrohungspunktzahl wird für Datensätze erkennbarer Elemente automatisch berechnet.

Definieren Sie Den Rechner Für Die Bedrohungsbewertung

Definieren Sie die Bedrohungspunktzahl für die Datensätze erkennbarer Elemente, die basierend auf den anwenderdefinierten Parametern generiert werden. Das Basissystem wird mit einer Bedrohungsbewertungsregel bereitgestellt, die angepasst und entsprechend aktiviert werden kann.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Hinweis:
Standardmäßig ist die Bedrohungsbewertungsregel inaktiv. Sie müssen die Regel aktivieren, um die Bewertung erkennbarer Elemente anzuzeigen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Gehe zu **Regel der Bedrohungsbewertung**an.
   Die Seite „Rechner der Bedrohungsbewertung“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

- In der Anwendung gibt es innerhalb des Basissystems eine Bewertungsregel, die den Anwendern zum Anzeigen, Bearbeiten oder Ändern der Bedrohungsbewertung zur Verfügung steht. Der Anwender kann jedoch weder eine neue Regel erstellen noch die vordefinierte Bedrohungsbewertungsregel löschen.
- Die Änderungen gelten ab diesem Zeitpunkt für alle neuen erkennbaren Elemente oder Aktualisierungen der erkennbaren Elemente. Um historische Punktzahlen neu anzugeben, sollten sie die Option „Neu berechnen“ verwenden.

3. Im Formular enthalten die folgenden Felder die vordefinierten Werte.

Bedrohungsbewertungsrechner

Feld	Beschreibung
Name	Name des Bedrohungsbewertungswerts. Beispiel: Bedrohungsbewertungsrechner.
Beschreibung	Beschreibung des Bedrohungsbewertungsdatensatzes. Beispielsweise berechnet die Bedrohungspunktzahl basierend auf der gewichteten Summe vordefinierter Kriterienpunktzahlen.
Gesamtgewichtung (gilt für den Kriteriengenerator)	Dieses Feld kann nicht bearbeitet werden und zeigt die Gesamtgewichtung an, die vom System basierend auf der Gewichtung berechnet wird, die den aktivierten Kriterien entspricht.
Bewertungskriterien	Gibt die Bewertungskriterien für ein erkennbares Element an. Im Folgenden finden Sie die zwei verfügbaren Optionen zum Definieren der Bedrohungsbewertungskriterien: ○ **Kriteriengenerator** : Verwenden Sie diese Option, um Kriterien hinzuzufügen, zu bearbeiten oder zu entfernen, zu aktivieren und zu deaktivieren, die zur Berechnung der Bedrohungsbewertung beitragen, und sicherzustellen, dass die aggregierte Gesamtgewichtung 100 % beträgt. ○ **Skript Verwenden (Erweitert)** : Die Skriptfunktion ist eine erweiterte Funktion zum Erstellen eines anwenderdefinierten Skripts, das die Bedrohungspunktzahl im Bereich von 0 bis 100 zurückgeben soll.

Nachfolgend finden Sie die verfügbaren Optionen zum Definieren von **Bewertungskriterien** :

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Kriteriengenerator
- Skript verwenden (erweitert)

Im Folgenden finden Sie das Verfahren für den Kriteriengenerator:

Hinweis:
Sie können die vorhandenen Kriterien bearbeiten oder ändern oder neue Kriterien hinzufügen.

a. Wählen Sie den Typ der Kriterien aus.
Beispiel: Fügen Sie ein neues Kriterium hinzu.

b. Wählen Sie aus **Tabelle** Für die die Kriterien konfiguriert sind.
Die Liste der Werte in der Dropdown-Liste ist erkennbare Elemente, Bedrohungsakteur, Kampagne, Standort, Identität, Schwachstelle, Bedrohungsereignis, Security Incident und Aggregate. Wenn Sie eine dieser Optionen aus der Dropdown-Liste auswählen, wird eine Bedingung angewendet. Diese Bedingung stellt sicher, dass nur Datensätze angezeigt oder berechnet werden, die sich auf den ausgewählten Wert beziehen.

Hinweis:

- Wenn das ausgewählte erkennbare Element ausgewählt ist, wird die Bedingung auf den Datensatz des erkennbaren Elements angewendet, für den die Bedrohungsbewertung berechnet wird. Wenn die ausgewählte Tabelle nicht erkennbar ist, wird die Bedingung nur angewendet, wenn sich die Datensätze auf das erkennbare Element beziehen, für das die Bedrohungspunktzahl berechnet wird.
- Eine zusätzliche Aggregattabelle wird hinzugefügt, um die Punktzahlen basierend auf der Anzahl der Beziehungen zu definieren, die den erkennbaren Elementen zugeordnet sind. Wählen Sie beispielsweise die Tabelle: Aggregate und den Feldwert: Bedrohungsakteure aus. Wenn es mehr als zwei Bedrohungsakteure gibt, legen Sie dann für ein erkennbares Element die Punktzahl fest, und wenden Sie die Bedingungen an.
- Wenn Sie beispielsweise eine Punktzahl für einen oder mehrere Bedrohungsakteure festlegen möchten, die einem erkennbaren Element zugeordnet sind, wählen Sie das Feld Anzahl der Bedrohungsakteure aus, legen Sie die gewünschte Punktzahl fest, und wenden Sie die entsprechenden Bedingungen an.

c. Wählen Sie aus **Feld** Aus der oben ausgewählten Tabelle.

d. Geben Sie ein **Gewichtung** Der Kriterien zwischen 0 und 100.
Die Gesamtgewichtung aller Kriterien muss 100 % betragen.

e. Geben Sie den Namen und die Kurzbeschreibung der Kriterien ein.

f. Wählen Sie aus **Aktivieren Sie Bewertungskriterien** Kontrollkästchen zum Aktivieren der Bewertungskriterien.

g. Definieren Sie **Bedingungen** Und legen Sie die Punktzahl für die Bedingungen fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Sie können auch mit neue Bedingungen hinzufügen **Neue Bedingung** Und löschen Sie die Bedingung mit **Löschen Sie Kriterien** Symbol.

i. Klicken Sie Auf **Hinzufügen** Um die konfigurierten Kriterien hinzuzufügen.

Hier ist ein Beispiel für die Definition einer Bedingung für eine Bedrohungsbewertung:

```
Table: Vulnerability

Field: CVSS2.0

Weightage: 30%

Condition-1: CVSS2.0 > 7, Score = 80

Condition-2: CVSS2.0 > 4 AND CVSS2.0 < 7, Score = 50

Condition-3: CVSS2.0 < 4, Score = 10
```

4. Klicken Sie Auf **Verlauf Neu Berechnen** Schaltfläche zum erneuten Koppeln der Bedrohungspunktzahl. Wenn die Bedrohungsbewertungsregel geändert wird, müssen Sie die Bewertungsregel erneut auf die erkennbaren Elemente anwenden, deren Bedrohungspunktzahl bereits in der Vergangenheit berechnet wurde. Verwenden Sie **Verlauf neu berechnen** Schaltfläche zum Auslösen des Neuberechnungsauftrags.

Hinweis:

- Eine Bestätigungsnachricht wird angezeigt, damit Sie die Aktion ausführen können. Dies ist ein Prozess mit langer Ausführung, der im Hintergrund ausgeführt wird. Sie können erst Änderungen vornehmen, wenn der Prozess abgeschlossen ist. Möchten Sie diese Aktion wirklich ausführen?
- Für alle Aktualisierungsereignisse, die für erkennbare Elemente als Teil von generiert werden **Verlauf neu berechnen** , Die Verarbeitung von Webhooks ist deaktiviert, und wenn Sie aktivieren möchten, ändern Sie diese Systemeigenschaft `Webhook_ignore_Threat_Score_reapply` .

5. Klicken Sie auf **OK**.

Wichtig:
Diese Aktion löst einen Auftrag mit langer Ausführungszeit aus, und das System erlaubt Ihnen erst, weitere Änderungen an der Bedrohungsbewertungsregel vorzunehmen, wenn der Auftrag abgeschlossen ist. Weitere Informationen zur Konfiguration der Hintergrundauftragskonfiguration finden Sie unter Framework-Konfiguration des Vulnerability Response-Hintergrundauftrags .

Im Folgenden finden Sie die **Skript Verwenden (Erweitert)** Skript: Verwenden Sie dieses Skript, um ein anwenderdefiniertes Skript zu erstellen, das die Bedrohungspunktzahl im Bereich von 0 bis 100 zurückgeben soll.

Das Feld „Erweitertes Skript“ wird automatisch mit einer Funktion ausgefüllt, die die Parameter übernimmt **Aktuell** Und **Aggregate** Und diese Funktion sollte die Bedrohungspunktzahl im Bereich von 0 bis 100 zurückgeben.

Hier ist der aktuelle Parameter das GlideRecord-Objekt der Entität (erkennbares Element), für die die Bedrohungspunktzahl berechnet wird. Für die erkennbaren Elemente entspricht er dem GlideRecord für die Tabelle „sn_sec_tisc_observable“. Der Parameter „Aggregate“ ist ein GlideRecord-Objekt von sn_sec_tisc_Aggregates Tabellendatensatz,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der verwendet wird, um auf die Datensatzanzahlen der verschiedenen zugehörigen Datensatztypen (z. B. Kampagnen oder Identitäten) der Hauptentität (erkennbares Element) zuzugreifen.

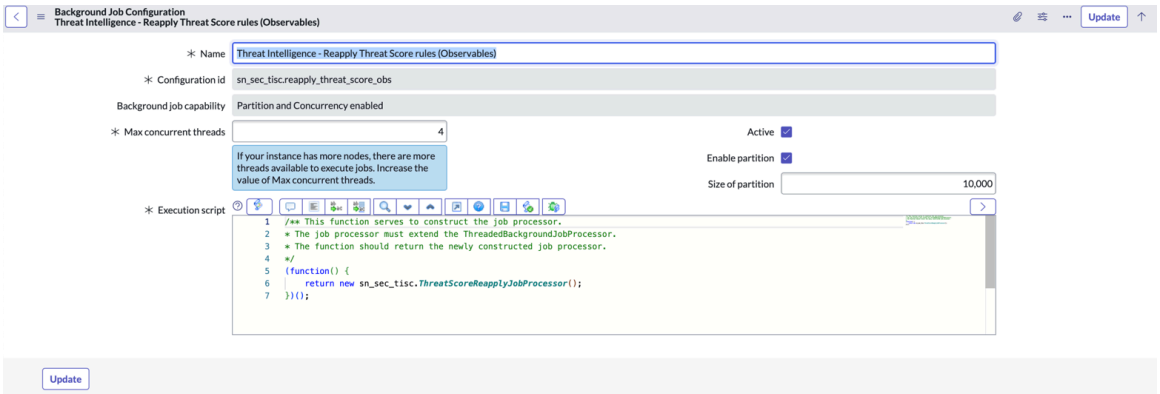
Beispielbeispiel für das Skript in der erweiterten Option:

```
answer = (function threatScoreCalculator(current, aggregates) {

   // return the threat score in the range of 0-100
   var threatSeverity = current.getValue("threat_severity");
   if(threatSeverity == "high")
    return 80;
   else {
      let associatedCampaigns = aggregates.getValue("num_of_campaigns");
      if(associatedCampaigns > 0)
         return 50;
   }
   return 0;

})(current, aggregates);
```

Zu Ihrer Referenz finden Sie unten der Screenshot, der den Konfigurationsprozess des Hintergrundauftrags für die Bedrohungsbewertung zeigt.



Extraktionsregeln für MITRE ATT&CK-Technik

Extrahieren Sie MITRE-Techniken automatisch aus erkennbaren Elementen oder Objekten, die aus verschiedenen Datenquellen erfasst wurden, und extrahieren Sie auch MITRE-Techniken aus Ergebnissen der Bedrohungssuche im Datensatz erkennbarer Elemente.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Hinweis:
Stellen Sie sicher, dass die MITRE ATT&CK-Repository-Daten in der von Ihnen verwendeten Instanz verfügbar sind. Wenn die Daten nicht verfügbar sind, führt die Anwendung die Extraktion nicht durch.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Gehe zu **Regel-Engine** > **Extraktionsregeln für MITRE ATT&CK-Technik**an.
   Die Seite „Extraktionsregeln für MITRE ATT&CK-Technik“ wird angezeigt.
3. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie Auf **Aktivieren** Zum Aktivieren der Extraktionsregel für die MITRE ATT&CK-Technik, nachdem Sie eine neue Regel erstellt haben.
   Wenn Sie die Extraktionsregel der MITRE ATT&CK-Technik nicht aktivieren, wird die Regel nicht auf den Datensatz angewendet.

   Hinweis:

   a. Datenquellen: Wenn Sie die Extraktionsregel aktivieren, darf die Kombination aus Datenquellen und Integrationstyp keiner der vorhandenen aktivierten Extraktionsregeln entsprechen. Wenn dies der Fall ist, zeigt die Anwendung eine Fehlermeldung an, mit der Sie die vorhandenen Kombinationen ändern und die Regel erneut aktivieren können.

   b. Bedrohungssuche: Wenn Sie die Extraktionsregel aktivieren, darf der Lieferantenname mit keiner der vorhandenen aktivierten Extraktionsregeln übereinstimmen. Wenn dies der Fall ist, zeigt die Anwendung eine Fehlermeldung an, in der Sie den Lieferantennamen ändern und die Regel erneut aktivieren können.

   c. Für die Anwender im Basissystem werden Beispielextraktionsregeln für die MITRE ATT&CK-Technik bereitgestellt. Diese Regeln befinden sich standardmäßig im deaktivierten Status, und Sie müssen die Regel aktivieren und aktivieren.

Feld	Beschreibung
Generische Regel für Datenquellenerfassung	Dies ist eine generische Regel für die Erfassung aus allen Arten von Datenquellen, einschließlich Import Intelligence und manueller Erstellung.
Generische Regel für Bedrohungssuche	Dies ist eine generische Regel für alle Integrationen der Bedrohungssuche.
Generische Regel für Integrationen zur Anreicherung erkennbarer Elemente	Dies ist eine generische Regel für alle Ergänzungsintegrationen erkennbarer Elemente.

5. Klicken Sie Auf **Duplikat** Dient zum Erstellen einer Kopie der Extraktionsregel.
6. Klicken Sie Auf **Deaktivieren** Zum Deaktivieren der Extraktionsregel.

   Hinweis:
   Sobald sie deaktiviert ist, wird die Regel für die Extraktion von MITRE-Daten nicht mehr berücksichtigt.

7. Klicken Sie auf **Speichern**.
8. Klicken Sie Auf **Löschen** Wenn Sie eine Extraktionsregel für MITRE ATT&CK-Technik löschen möchten.

Extraktionsmethode der MITRE ATT&CK-Technik

Die Extraktionsmethode der MITRE ATT&CK-Technik beschreibt, wie die Extraktionsmethoden durchgeführt und die zugehörigen Techniken verifiziert werden.

1. Die Extraktionsregeln für Datenquellen (Bedrohungssuchen sind nicht anwendbar) werden immer dann verarbeitet, wenn ein Quelldatensatz einer Entität (z. B. Quelle eines erkennbaren Elements oder einer Objektquelle) erstellt wird.
2. Die Regeln gelten für alle Felder im Entitätsquelldatensatz (mit Ausnahme von Datums-, Zahlenfeldern, Nutzungskategorie und Angriffsphasen).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Die extrahierten MITRE-Techniken sind dem entsprechenden Entitätsdatensatz zugeordnet, und Sie zeigen die Datensätze in der zugehörigen Liste „MITRE-Techniken“ in an **Zugehörige Datensätze** Registerkarte.

Hinweis:
Die MITRE-Techniken werden zuerst extrahiert und dem Entitätsquelldatensatz zugeordnet. Anschließend werden die Zuordnungen der Techniken dedupliziert und zum Datensatz der übergeordneten Entität aggregiert.

Zeigen Sie MITRE-Techniken an

1. Navigieren zu **Threat Intel-Bibliothek**Jeder Entitätsdatensatz (erkennbares Element oder Objekt), der den verwendet.
2. Klicken Sie auf **Zugehörige Datensätze** Registerkarte.
3. Wählen Sie Aus **MITRE-Techniken** Und zeigen Sie die zugehörigen Techniken an, die extrahiert werden.
4. Klicken Sie auf die MITRE-Technik-ID, um den Zuordnungsdatensatz der MITRE-Technik anzuzeigen und darauf zuzugreifen. Die **Quellen** In der Spalte werden alle Quellen angezeigt (auch durch Kommas getrennt, wenn eine oder mehrere Quellen vorhanden sind), die dem Entitätsquelldatensatz zugeordnet sind, für den die MITRE-Extraktion durchgeführt wird.

Hinweis:
Wenn dieselben Taktik- und Technik-IDs aus mehreren Quellen extrahiert werden, wird nur ein Datensatz der Taktik- und Technikzuordnung und der angezeigt **Quellen** In der Spalte werden alle extrahierten Quellen angezeigt.

5. Zur Fehlerbehebung können Sie die MITRE-Extraktionsregel anzeigen, die für die Extraktion der Taktik- und Technikzuordnungen verantwortlich war, indem Sie zu navigieren **Technikquellenbeziehungen** .

Hinweis:
Stellen Sie sicher, dass Sie hinzufügen **Extraktionsregel** Spalte mit **Listenaktionen** Symbol, falls die Spalte „Extraktionsregel“ nicht angezeigt wird.

Die Extraktionsregeln für Bedrohungssuchen werden immer dann verarbeitet, wenn der Ergebnisdatensatz der Bedrohungssuche für ein erkennbares Element erstellt wird, für das **Bedrohungssuche ausführen** Die Aktion wird ausgelöst, und die Extraktion wird nur für die Rohdaten-Nutzlast (Feld „Rohdaten“) ausgeführt, die im Ergebnisdatensatz der Bedrohungssuche verfügbar ist.

Hinweis:

- Wenn in der extrahierten Entitätsquelle (erkennbares Element oder Objekt) oder dem Bedrohungssuchergebnis für eine MITRE ATT&CK-Technik keine Taktik-ID vorhanden ist, werden die Technikzuordnungen für alle Taktiken erstellt, die der entsprechenden Technik im MITRE-Repository zugeordnet sind.
- Wenn in der extrahierten Entitätsquelle (erkennbares Element oder Objekt) oder dem Bedrohungssuchergebnis für eine MITRE ATT&CK-Technik eine Taktik-ID vorhanden ist, werden die Technikzuordnungen nur für alle extrahierten Taktiken erstellt, die der entsprechenden Technik im MITRE-Repository zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Von Sicherheitssteuerungslisten

Verwenden Sie diese Funktion, um erkennbare Elemente in einem Massenvorgang hinzuzufügen oder zu entfernen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Gehe zu **Sicherheitskontrolllisten**an.
   Beispiel: Fügen Sie erkennbare Elemente zur Allow-Liste hinzu, und wechseln Sie dann zur Option Allow-Liste.
3. Wählen Sie Aus **Allow-Liste** .
4. Wählen Sie den Typ der erkennbaren Elemente aus, z. B. IP-Adresse, Datei usw., um sie der Allow-Liste hinzuzufügen.
5. Klicken Sie auf **Hinzufügen**.
   Die **Wählen Sie erkennbare Elemente für die Allow-Liste aus** Wird angezeigt.
6. Wählen Sie alle erkennbaren Elemente aus, die der Allow-Liste hinzugefügt werden müssen.
7. Klicken Sie Auf **Der Allow-Liste hinzufügen** .
   Die ausgewählten erkennbaren Elemente werden hinzugefügt.
8. Wählen Sie ebenfalls aus **Der Deny-Liste hinzufügen** Um die erkennbaren Elemente zur Liste entfernt hinzuzufügen.
9. Wählen Sie Aus **Der Beobachtungsliste hinzufügen** Um die erkennbaren Elemente zur Beobachtungsliste hinzuzufügen.

   Hinweis:
   Sie können die erkennbaren Elemente direkt auf der Formularansichtsseite „erkennbare Elemente“ hinzufügen, die über dem Formularbanner verfügbar ist, um Listen, Deny-Listen oder Beobachtungslisten zuzulassen.

10. Navigieren Sie zum Überprüfen zu **Threat Intel-Bibliothek** .
11. Wählen Sie den Typ des erkennbaren Elements aus, das der Allow-Liste hinzugefügt wurde.
    Das erkennbare Element wird als „hinzugefügt, um die Liste zulassen“ angegeben.

    Hinweis:
    Allow-Liste und Deny-Liste schließen sich gegenseitig aus, und das System stellt automatisch sicher, dass ein erkennbares Element in der Allow-Liste nicht Teil der Deny-Liste ist und umgekehrt.

Taxonomien Werden Erstellt

Erstellen Sie Taxonomien für die Datenquellendatensätze.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Taxonomien**an.
2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Geben Sie ein **Name** .
4. Aktivieren oder deaktivieren Sie die Taxonomie **Status** Mithilfe der Formularaktionen aktivieren oder deaktivieren.

   Hinweis:
   Deaktivierte Taxonomien sind nicht für die Auswahl von Datensätzen verfügbar, für die Taxonomien gelten.

5. Wechseln Sie zu **Taxonomiewerte** Abschnitt zum Hinzufügen von Taxonomiewerten.
6. Klicken Sie Auf **Neu** Um einen neuen Taxonomiewert zu öffnen, und geben Sie ein **Taxonomie** Und **Wert** .
7. Klicken Sie auf **Speichern**.
8. Navigieren Sie beispielsweise zu **Threat Intel-Bibliothek** > **Erkennbare Elemente** Dient zum Überprüfen der Taxonomien für den Datensatz erkennbarer Elemente.
9. Navigieren Sie zu **Tags und Taxonomien** Abschnitt auf einer beliebigen Formularseite für erkennbare Elemente, und wählen Sie die neu erstellte Taxonomie aus.

   Hinweis:
   Sie können Tags und Taxonomien auch aus der Listenansicht der Threat Intel-Bibliothek hinzufügen.

Massenimport von Taxonomien

Importieren Sie die Taxonomiedatensätze.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Taxonomien mithilfe der Daten aus der Tabelle importieren. Auf diese Weise können Sie mehrere Datensätze in einem Massenimport importieren.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Taxonomien**an.
2. Wählen Sie Aus **Importieren** Schaltfläche.
   Mit dieser Aktion wird eine Aktion zum Importieren der Datendatei im XLSX- oder CSV-Format geöffnet. Sie können auch die Beispieldatei herunterladen, um das zu importierende Format zu verstehen. Das Dateiformat enthält zwei Werte, die Taxonomie und Taxonomiewert enthalten.
3. Klicken Sie Auf **Fügen Sie eine Datei hinzu** Link.
4. Wählen Sie die Datei und aus **Hochladen** .
5. Klicken Sie auf **Erledigt**.
   Eine Bestätigungsmeldung zeigt an, dass die Daten aus der angehängten Datei erfolgreich importiert wurden. Sie können auf den Link klicken, um die Importzusammenfassung anzuzeigen. Durch Klicken auf den Link wird der Datensatz in einer neuen Registerkarte geöffnet. Sie können die Anzahl der erstellten Taxonomien und Taxonomiewerte anzeigen. Wenn Fehler protokolliert werden, werden sie im Abschnitt „Importfehler“ protokolliert.

   Hinweis:
   Standardmäßig werden alle diese Taxonomien und Taxonomiewerte mit dem Status „aktiviert“ erstellt. Wenn Sie deaktivieren möchten, können Sie dies jederzeit über die Listenansicht tun.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Auf der **Taxonomien** Auf der Seite können Sie auf einen beliebigen Datensatz klicken. Diese Aktion zeigt die Taxonomiewerte als separate Registerkarte an, und Sie können die beiden Taxonomiewerte anzeigen, die erfolgreich importiert wurden, und diese Taxonomiewerte befinden sich im Status aktiviert.
7. Um einen der Taxonomieimporte anzuzeigen, können Sie auch jederzeit zu navigieren **Importe** Abschnitt, in dem die importierten Taxonomien angezeigt werden **Taxonomie-Importe** Abschnitt.
8. Klicken Sie Auf **Alle Importe** Zum Anzeigen aller Taxonomieimporte, die von verschiedenen Anwendern in der Anwendung erstellt wurden.
9. Klicken Sie Auf **Meine Importe** Um die Taxonomieimporte für den aktuell angemeldeten Anwender anzuzeigen.

Reputationsrechner für Bedrohungssuche verwalten

Sie können den Ergebnisrechner für Bedrohungssuche verwenden, um die Ergebnisse erkennbarer Elemente basierend auf den Antworten des Lieferanten für Bedrohungssuche zu berechnen.

Sie können einen Ergebnisrechner für die Bedrohungssuche für Ihre Integration erstellen und mithilfe eines Skripts bestimmen, wie Sie die verschiedenen Ergebnisse erkennbarer Elemente identifizieren möchten. Der Ergebnisrechner für die Bedrohungssuche enthält ein Beispielskript, das im Basissystem enthalten ist, mit dem Sie die Ergebnisse erkennbarer Elemente identifizieren oder dieses Skript entsprechend Ihren Anforderungen ändern können.

Bei Integrationen von Drittparteien, die die berechneten Ergebnisse liefern, ordnet der Ergebnisrechner der Bedrohungssuche die Ergebnisse den unterstützten Ergebnissen im Basissystem zu.

Rollup-Ergebnisse Der Bedrohungssuche

Wenn Sie mehrere Bedrohungssuchergebnisse für ein erkennbares Element von den verschiedenen Integrationsanbietern haben, werden die aktuellen Bedrohungssuchergebnisse aller Lieferanten berücksichtigt, und die allgemeinen Ergebnisse erkennbarer Elemente werden wie folgt markiert:

Rollup-Ergebnisse Der Bedrohungssuche

Letztes Ergebnis Erkennbarer Elemente	Gesamtergebnis Erkennbarer Elemente
Böswillig	Wenn einer der Integrationsanbieter das erkennbare Element als böswillig meldet, wird das Gesamtergebnis des erkennbaren Elements als böswillig markiert.
Verdächtig	Wenn keiner der Integrationsanbieter das erkennbare Element als böswillig meldet, meldet es einer von ihnen als verdächtig, und dann wird das allgemeine Ergebnis erkennbarer Elemente als verdächtig markiert.
Clean	Wenn alle Integrationslieferanten das erkennbare Element als bereinigt melden, wird das Gesamtergebnis des erkennbaren Elements als bereinigt markiert.
Unbekannt	Wenn keiner der Integrationsanbieter das erkennbare Element als böswillig oder verdächtig meldet und einer von ihnen es als Unbekannt meldet, wird das allgemeine Ergebnis erkennbarer Elemente als Unbekannt markiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Reputationsrechner Für Bedrohungssuche Anzeigen

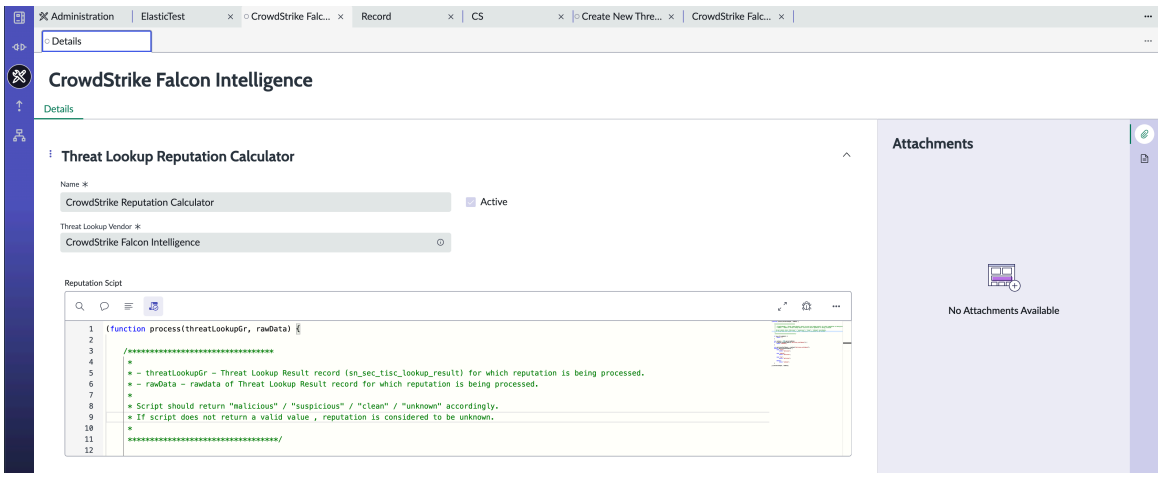
Sie können den Ergebnisrechner für Bedrohungssuche anzeigen, um zu bestimmen, wie die Reputation des erkennbaren Elements basierend auf der Antwort eines bestimmten Lieferanten für Bedrohungssuche berechnet wird.

Erforderliche Rolle: sn_sec_tisc.admin

Führen Sie die folgenden Schritte aus, um den Reputationsrechner für die Bedrohungssuche anzuzeigen:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Wählen Sie aus **Reputationsrechner Für Bedrohungssuche** Abschnitt.

   Sie können die Liste der Reputationsrechner für die Bedrohungssuche anzeigen.
3. Klicken Sie auf den erforderlichen Reputationsrechner für Bedrohungssuche, um die Details des Rechners anzuzeigen.



Reputationsrechner Für Bedrohungssuche Erstellen

Erforderliche Rolle: sn_sec_tisc.admin

Hinweis:
Pro Bedrohungssuche-Lieferant kann zu jedem Zeitpunkt nur ein Rechner für Bedrohungssuche aktiv sein.

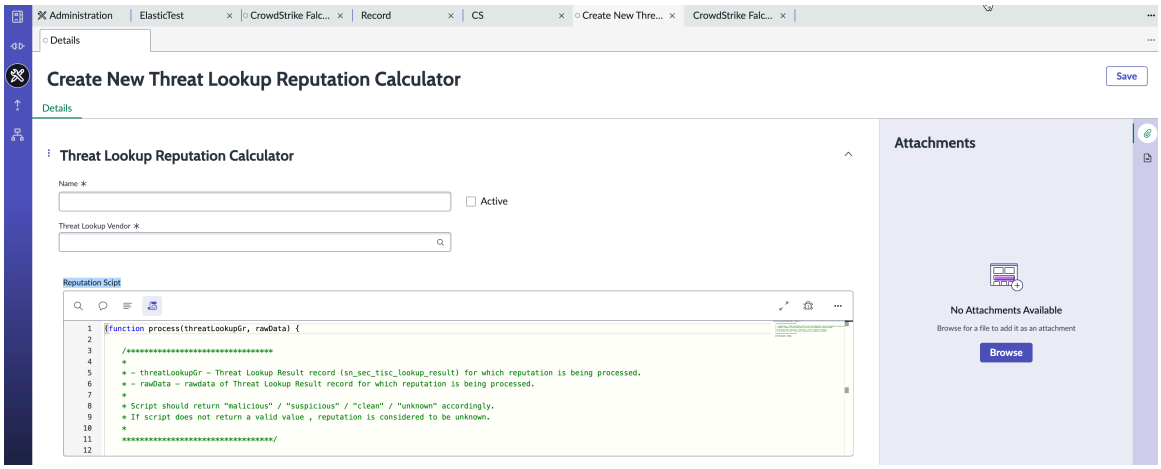
Führen Sie die folgenden Schritte aus, um einen Reputationsrechner für die Bedrohungssuche zu erstellen:

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Wählen Sie aus **Reputationsrechner Für Bedrohungssuche** Abschnitt.

   Sie können die Liste der Reputationsrechner für die Bedrohungssuche anzeigen.
3. Klicken Sie auf, um einen Reputationsrechner für die Bedrohungssuche zu erstellen **Neu** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie die Felder im Formular aus.

Erstellen Sie einen Reputationsrechner für die Threat-Suche

Feld	Beschreibung
Name	Name für den Reputationsrechner für die Bedrohungssuche.
Aktiv	Die Berechnung der Bedrohungssuche wird nur ausgeführt, wenn die Option aktiv ausgewählt ist.
Bedrohungssuche-Anbieter	Name des Lieferanten der Bedrohungssuche. Beispiel: CrowdStrike Falcon Intelligence .
Reputationsskript	Skripteditor, um zu bestimmen, wie Sie die verschiedenen Ergebnisse erkennbarer Elemente identifizieren möchten. Jede Integration der Bedrohungssuche enthält ein Basisskript zur Berechnung der Reputation der Bedrohungssuche.

5. Klicken Sie auf **Speichern**.

Verwalten Sie E-Mail-Benachrichtigungen

Verwenden ServiceNow Benachrichtigungen zum Erstellen und Verwalten von System-E-Mail-Benachrichtigungen und zum Anzeigen von E-Mail-Protokollen.

E-Mail-Benachrichtigungen

Verwenden Sie E-Mail-Benachrichtigungen, um ausgewählten Anwendern E-Mail-Benachrichtigungen zu bestimmten Aufgaben innerhalb der Anwendung zu senden, z. B. Aktualisierungen von erkennbaren Elementen/Indikatoren/verschiedenen anderen Objekten.

Erforderliche Rolle: Administrator

Hinweis:
Als Systemadministrator können Sie die Details der E-Mail-Benachrichtigungsregel in der klassischen Ansicht der Anwendung anzeigen, erstellen oder bearbeiten.

Threat Intelligence-Sicherheitszentrum Stellt regelgesteuerte E-Mail-Benachrichtigungen bereit, die an einzelne E-Mail-Adressen oder eine Liste von E-Mail-Adressen gesendet werden. Normalerweise wird die Verbreitung von Informationen zu Bedrohungsinformationen an

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

interne Anwender normalerweise in Form einer E-Mail gesendet. Der Prozess umfasst die Bereitstellung der Threat Intelligence-Daten an Anwender gemäß dem angegebenen Format und den angegebenen Zeitlinien.

Mit E-Mail-Benachrichtigungen können Administratoren Folgendes angeben:

- Wann die Benachrichtigung gesendet wird
- Wer die Benachrichtigung erhält
- Welchen Inhalt die Benachrichtigung hat

Hinweis:
Wenn Sie Änderungen vornehmen möchten, müssen Sie konfigurieren, wer die E-Mail gesendet werden soll, indem Sie die Basissystemregeln entsprechend Ihren Anforderungen ändern.

Weitere Informationen finden Sie unter Erstellen Sie eine E-Mail-Benachrichtigung Abschnitt auf Verwaltung der ServiceNow AI Platform Dokumentation.

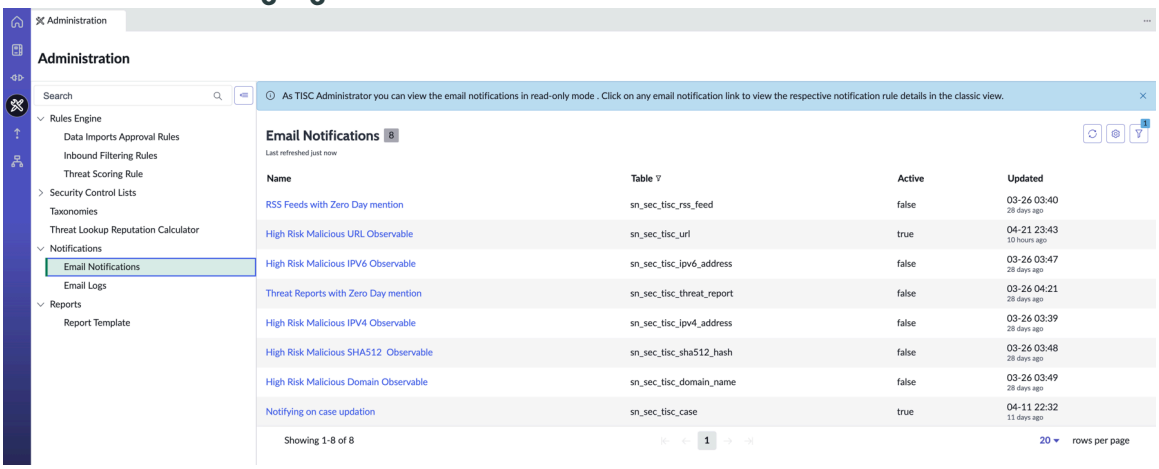
In der folgenden Tabelle werden die E-Mail-Benachrichtigungsregeln aufgeführt, die im Basissystem bereitgestellt werden.

E-Mail-Benachrichtigungen

Name	Tabelle
RSS-Feeds mit Zero Day-Erwähnung	sn_sec_tisc_rss_Feed
Erkennbares Element für schädliche URL mit hohem Risiko	sn_sec_tisc_url
Erkennbares schädliches IPV6-Element mit hohem Risiko	sn_sec_tisc_ipv6_address
Bedrohungsberichte mit Zero Day-Erwähnung	sn_sec_tisc_Threat_Report
Erkennbares schädliches IPV4-Element mit hohem Risiko	sn_sec_tisc_ipv4_address
Erkennbares schädliches SHA512-Element mit hohem Risiko	sn_sec_tisc_sha512_hash
Erkennbares Element Für Schädliche Domäne Mit Hohem Risiko	sn_sec_tisc_Domain_Name
Benachrichtigung über Fallaktualisierung	sn_sec_tisc_Case

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Benachrichtigungen



Hinweis:
Wenn Sie auf jede E-Mail-Benachrichtigung klicken, gelangen Sie zur klassischen Anwenderoberfläche, sodass Sie die erforderlichen Aktionen ausführen können, z. B. zum Anzeigen, Bearbeiten oder Erstellen der Benachrichtigungen.

E-Mail-Protokolle

Dieser Abschnitt bietet den TISC-Administratoren eine klare Sichtbarkeit der E-Mails, die mithilfe der konfigurierten E-Mail-Benachrichtigungsregeln gesendet werden.

E-Mail-Benachrichtigungen und Protokolle

TISC bietet verschiedene Möglichkeiten, um auf E-Mail-Benachrichtigungen und -Protokolle basierend auf verschiedenen Persona zuzugreifen, anzuzeigen oder zu ändern.

Hinweis:

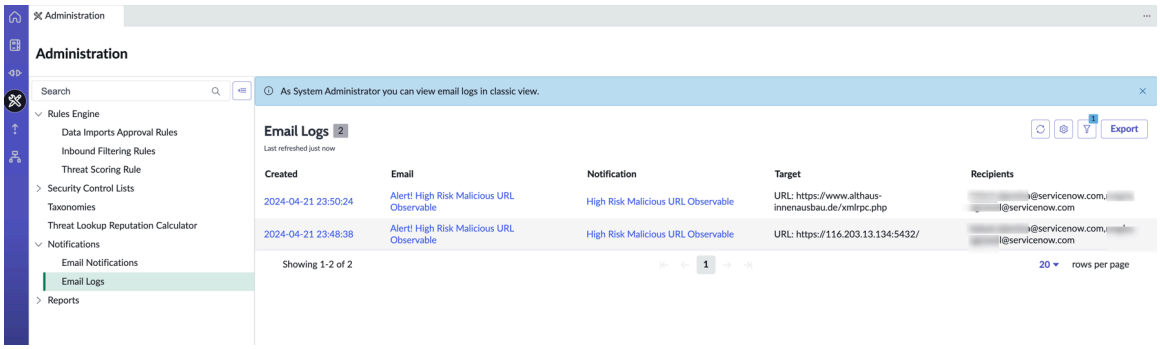
Persona	Zugriffsebenen
TISC-Administrator (sn_sec_tisc.admin)	Als sn_sec_tisc.admin können Sie nur die E-Mail-Benachrichtigungen anzeigen, die für TISC konfiguriert sind. **Hinweis:** Klicken Sie auf die Hyperlinks für E-Mail-Protokolle, um zur klassischen Anwenderoberfläche zu navigieren und diese Benachrichtigungen anzuzeigen.
Systemadministrator (admin)	Als Administrator können Sie die Benachrichtigungen in der klassischen Anwenderoberfläche erstellen, anzeigen und bearbeiten. **Hinweis:** Klicken Sie auf die Hyperlinks für E-Mail-Protokolle, um zur klassischen Anwenderoberfläche zu navigieren, um diese Benachrichtigungen anzuzeigen und zu erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sowohl der TISC-Administrator als auch der Systemadministrator können die Filter verwenden und nach den E-Mail-Protokollen suchen.

E-Mail-Protokolle



Berichtsvorlagen

Definiert die Möglichkeit, die Berichtsvorlagen wiederzuverwenden, die innerhalb der Anwendergruppe freigegeben werden können, um schnell und konsistent Berichte zu generieren.

Verwenden Sie diese Funktion, um verschiedene Arten von Berichtsvorlagen zu erstellen, die auf Fälle angewendet werden können, die den Status laufender Untersuchungen in Relevanz zu jeder Bedrohung für Ihre Organisation bereitstellen und bei der Generierung von Berichten derselben helfen.

In diesem Abschnitt wird erläutert, wie CTI-Berichterstellung auf Fallebene implementiert wird, und es werden sowohl Administrator- (Vorlagendesign) als auch Analyst-Experiences (Laufzeit) bereitgestellt.

Sie können der Berichtsvorlage anwenderdefinierte Fallaufgaben-Formularfelder oder zugehörige Listen hinzufügen, die Dot-Walking-fähig sind. Darüber hinaus können Sie den Bericht basierend auf Ihren Anforderungen mithilfe verschiedener Berichtselemente formatieren und konfigurieren.

Erforderliche Rolle: sn_sec_tisc.admin

In der folgenden Tabelle werden einige Berichtsvorlagen erläutert, die im Basissystem bereitgestellt werden.

Berichtsvorlage

Name	Beschreibung
Fallstatusbericht – Profil des Bedrohungsakteurs	Der Bericht soll einen Status über die laufende Falluntersuchung im Zusammenhang mit einem Bedrohungsakteur bereitstellen, der versucht, den Kontext und die Relevanz der Bedrohung für die Organisation, das Verhalten der Angreifer und potenzielle Ziele, die IOC-Ergänzung, die zugehörige Malware und Tools, die beobachteten TTPs, den Unterschied zu vorhandenen TTPs zu verstehen – Netto-neue Fähigkeiten, leichte Änderungen usw.
Kurzübersicht	Der Bericht soll leitende Entscheidungsträger über ein bestimmtes Risiko informieren. Der Schwerpunkt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berichtsvorlage (Fortsetzung)

Name	Beschreibung
	liegt auf den Zielgruppen von Führungskräften und der Unterstützung strategischer Probleme, die erklären, warum und wie, und nicht was und wann. Technische Details und Anhänge zur Unterstützung von Langform- und Textbeschreibungen werden nicht in diesen Bericht aufgenommen.
Zusammenfassung nach Untersuchung – Profil des Bedrohungsakteurs	Der Bericht soll Kontext und Relevanz der Bedrohung für die Organisation bereitstellen; Verhalten und potenzielle Ziele der Angreifer; IOC-Ergänzung; zugehörige Malware und Tools; beobachtete TTPs; Unterschiede zu vorhandenen TTPs – Netto-neue Fähigkeiten, geringfügige Änderungen usw.

Hinweis:
Standardmäßig befinden sich diese Berichte im Status „veröffentlicht“ und befinden sich im schreibgeschützten Modus. Da sich die Berichtsvorlagen im schreibgeschützten Modus befinden, können die Anwender keine Änderungen an den Vorlagen vornehmen, und die Analysten können die Berichte nicht generieren, da die Berichtsvorlagen deaktiviert werden.

Erstellen Sie eine neue Berichtsvorlage

Erstellen Sie eine neue Fallberichtsvorlage entsprechend Ihren Geschäftsanforderungen Ihrer Organisation.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Berichte** > **Berichtsvorlage**an.
   In diesem Abschnitt werden die im Basissystem verfügbaren Vorlagen sowie die veröffentlichten Vorlagen angezeigt. Sie können eine beliebige Vorlage für die Arbeit mit den Berichten auswählen.

   Hinweis:
   In diesem Abschnitt können Sie bei Bedarf auch die Vorlagen löschen.

3. Klicken Sie auf **Neu**.
4. Geben Sie den Namen und die Beschreibung der Vorlage ein.
5. Klicken Sie auf **Speichern**.
   Der Abschnitt Vorlageninhalt wird angezeigt.

   Hinweis:
   Jedes Mal, wenn Sie eine neue Berichtsvorlage erstellen, befindet sich die Vorlage im Entwurfsstatus, was bedeutet, dass die Vorlagenerstellung in Bearbeitung ist und andere Anwender die Berichtsvorlage erst anzeigen können, wenn sie abgeschlossen ist.

6. Erweitern Sie **Vorlageninhalte** Zum Einfügen der gewünschten Felder in den Vorlagentext.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Mit der Vorlage, die Sie bearbeiten, können Sie den Vorlagentext definieren und die erforderlichen Variablen auswählen, die dem Vorlageneditor-Abschnitt hinzugefügt werden sollen. Die Vorlagen werden mit dem Rich-Text-Editor (RTE) unterstützt, sodass Sie verschiedene verfügbare Funktionen wie Einrücken, Schriftgröße, Erstellen von Tabellen, Hinzufügen von Bildern und verschiedene andere Formatierungsfunktionen steuern können.
- Sie können auch Bilder in Ihre Berichtsvorlagen einfügen. Dazu müssen Sie das Bild kopieren und direkt in die Vorlage einfügen. Wenn Sie ein Bild hinzufügen, wird dieses Bild als Anhang hochgeladen.
- Sie können ein Bild mit bis zu 698 Pixeln hochladen oder anhängen. Wenn das Bild über der definierten Größe liegt, wird es automatisch an die ursprüngliche Größe angepasst. Diese Einschränkung der Pixelgröße hilft der PDF-Berichterstellung, im richtigen Format anzuzeigen, und die Bilder werden im Bericht nicht gekürzt.

7. Fügen Sie die erforderlichen Elemente des Falls hinzu.
8. Klicken Sie Auf **Inhalt Speichern** Um den Inhalt Ihrer neuen Berichtsvorlage zu speichern.
9. Klicken Sie Auf **Vorschau** Um eine Vorschau Ihres Berichtsformats anzuzeigen und zu sehen, wie ein Bericht generiert wird, wenn Sie einen Fallbericht generieren.

Hinweis:

- **Fallfelder** : Wenn Sie Ihre Berichtsvorlage(n) ändern, zeigen Sie eine Vorschau der Inhalte an, die der Vorlage hinzugefügt wurden. Wenn Sie beispielsweise einen Fallbericht generieren und ein Feld mit der Bezeichnung Kurzbeschreibung hinzufügen möchten, können Sie dieses Feld aus den Fallfeldern auswählen. Dann wird dieses Feld als Variable in der Berichtsvorlage hinzugefügt. Wenn ein Bericht für den Analysten generiert wird, wird die Kurzbeschreibung des Falls im Bericht angezeigt.
- **Datensätze** : Innerhalb der Berichtsvorlage können Sie auch die zugehörigen Datensätze dieses bestimmten Falls hinzufügen, die als Artefakte des Falls angezeigt werden. Wenn Sie beispielsweise schädliche erkennbare Elemente im Bericht aus den zugehörigen Listen erkennbarer Elemente sehen möchten, können Sie sie Ihrer Berichtsvorlage hinzufügen. Diese zugehörigen Datensätze werden im Tabellenformat angezeigt
- **Skripts** : Immer wenn Sie Datum und Uhrzeit des Berichts anzeigen möchten, können Sie hinzufügen **Aktuelles Datum/Uhrzeit** Skripts zu Ihrer Berichtsvorlage, und dadurch werden Datum und Uhrzeit der Berichterstellung hinzugefügt.
- **MITRE ATT&CK** : Zeigt die mit der MITRE-Karte verknüpften Techniken in Ihrem Bericht an.

Nachdem Sie Ihrer Berichtsvorlage alle erforderlichen fallbezogenen Felder hinzugefügt haben, müssen Sie Ihre Berichtsvorlage veröffentlichen.

10. Klicken Sie Auf **Veröffentlichen** Um die Vorlage zu veröffentlichen.
Es wird eine Bestätigungsnachricht angezeigt, ob Sie die Berichtsvorlage veröffentlichen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie eine Berichtsvorlage veröffentlichen, ist diese Vorlage für alle Anwender aktiviert. Wenn er veraltet ist und Sie die Berichtsansicht für die Anwender einschränken möchten, können Sie den veröffentlichten Bericht deaktivieren, was bedeutet, dass die Berichtsvorlage für die Anwender ausgeblendet wird. Sie müssen den veröffentlichten Bericht erneut aktivieren, damit die Anwender ihn anzeigen und verwenden können, bis er dann für die Anzeige ausgeblendet wird.

11. Klicken Sie Auf **Löschen** Dient zum Löschen der Berichtsvorlage, falls Sie diese Berichtsvorlage nicht möchten.
Wenn Sie Ihre Berichtsvorlage umbenennen möchten, klicken Sie auf **Bearbeiten** Und ändern Sie die gewünschten Felder.

Systemeigenschaften für Berichte

Die Systemeigenschaften für Berichte werden unten erläutert.

Eigenschaft	Beschreibung	Wert
sn_sec_Reporting.max_list_columns_allowed	Beschränken Sie die Anzahl der Spalten, die beim Rendern von Listen in Berichts-pdfs hinzugefügt werden können. Dadurch werden die Spalten vom Anfang der Ansicht bis zum zulässigen Grenzwert verwendet.	5
sn_sec_Reporting.Report_default_style_object	Verwenden Sie diese Eigenschaft, um die CSS von freien Formfeldern, dem linken Bereich und der Berichtslisten zu steuern.	(JSON-Objekt)
sn_sec_Reporting.load_all_Records	Lädt alle Datensätze für die Listen im Bericht, die aus einer Vorlage erstellt wurden. „true“ – lädt alle Datensätze; und „false“ – lädt eine bestimmte Anzahl von Datensätzen, die durch die Eigenschaft „sn_sec_reporting.reporting_list_records_count“ definiert sind.	Falsch
sn_sec_Reporting.Reporting_list_Records_count	Lädt eine bestimmte Anzahl von Datensätzen im Berichtseditor.	20
sn_sec_tisc.sn_sec_tisc_case.defang_second_url	Steuert, ob URLs aus Listen definiert werden oder nicht.	True
sn_sec_tisc.Show_all_tactics_Reporting	Bei „true“ werden alle Taktiken (einschließlich der Taktiken, denen keine Techniken mit dem Fall zugeordnet sind) für die im Bericht gerenderten MITRE-Listen angezeigt.	Falsch
sn_sec_tisc.Reporting_email_template_sn_sec_tisc_case	Sys_ID der E-Mail-Client-Vorlage für die Falltabelle	B55e22c54324021060eeee0ea78b8f2df

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung	Wert
	(sn_sec_tisc_case), die in der Berichtfreigabe verwendet wird.	
sn_sec_tisc.sn_sec_tisc_Case.excluded_fields	Ausgeschlossene Felder des Falls in den Menüoptionen für Berichte/ Vorlagen zum Ersetzen eines Felds.	(Liste aller ausgeschlossenen Fallfelder
sn_sec_tisc.sn_sec_tisc_Case.ctx_menu_field_Header	Diese Eigenschaft wird verwendet, um den entsprechenden UI-Nachrichtendatensatz für die Bezeichnung der Fallfelder in den Menüoptionen für Berichte/ Vorlagen abzurufen.	sn_sec_tisc_Case_Reporting_ctx_menu_field_Header

Bearbeiten Sie eine veröffentlichte Berichtsvorlage

Verwenden Sie diesen Abschnitt, um eine veröffentlichte Berichtsvorlage zu bearbeiten.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Berichte** > **Berichtsvorlage**an.
3. Wählen Sie die erforderliche Berichtsvorlage aus.
4. Wählen Sie Aus **Bearbeiten** Schaltfläche, die in der Berichtsvorlage angezeigt wird.

   Hinweis:

   Eine Bestätigungsnachricht wird angezeigt, die angibt, dass Sie eine veröffentlichte Vorlage bearbeiten und die Vorlage erneut veröffentlichen müssen, um sie unter Fallberichten verfügbar zu machen. Möchten Sie mit der Bearbeitung fortfahren? Dies bedeutet, dass Sie die bearbeitete Vorlage erneut veröffentlichen müssen, nachdem Sie die erforderlichen Änderungen vorgenommen haben.

5. Wählen Sie Aus **Bearbeiten** Im Bestätigungsdialogfeld.
6. Nehmen Sie die erforderlichen Änderungen vor, indem Sie die erforderlichen Inhaltsfelder oder die zugehörige Liste hinzufügen.
7. Wählen Sie Aus **Inhalt Speichern** .
8. Wählen Sie Aus **Veröffentlichen** Schaltfläche zum Veröffentlichen der Änderungen.
   Sobald Sie die Berichtsvorlage veröffentlicht haben, wird eine Bestätigungsmeldung angezeigt, die angibt, dass die Berichtsvorlage erfolgreich veröffentlicht wurde.

   Hinweis:

   - Sie können auch eine Vorschau des Inhalts der Berichtsvorlage anzeigen, bevor Sie die Berichtsvorlage veröffentlichen.
   - Wenn Sie die Berichtsvorlage löschen möchten, können Sie auswählen **Löschen** Zum Löschen der Berichtsvorlage.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Duplizieren Sie eine Berichtsvorlage

Duplizieren Sie eine Berichtsvorlage. Wenn Sie inkrementelle Updates hinzufügen möchten, können Sie eine Kopie der Berichtsvorlage erstellen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > > **Administration**an.
2. Auswahlvorgang **Berichte** > **Berichtsvorlage**an.
3. Wählen Sie die Vorlage aus.
4. Klicken Sie Auf **Duplikat** .
   Der Inhalt der ausgewählten Vorlage wird dupliziert, und eine Kopie dieser Vorlage wird angezeigt. Die Vorlage befindet sich erneut im Status Entwurf. Sie können den Inhalt anpassen und die Vorlage dann nach Bedarf umbenennen.
5. Bearbeiten oder ändern Sie den Inhalt der kopierten Vorlage.

Hinweis:
Sie können die Berichtsvorlagen auch löschen, wenn Sie sie nicht mehr benötigen, und neue Vorlagen erstellen.

Arbeiten mit Webhooks

Ein Webhook ist eine HTTP-Anforderung, die durch ein Ereignis im Quellsystem (TISC) ausgelöst und an ein Zielsystem gesendet wird (wo die Endpunkt-URL vorhanden ist), mit einer Nutzlast von Ereignisdaten.

Diese Webhooks in Threat Intelligence-Sicherheitszentrum Sind nützlich, um die Zielanwendung zu benachrichtigen, wenn Ereignisse auftreten.

In TISC können Sie Folgendes tun:

- Konfigurieren Sie Webhooks
- Auslöser Verwalten
- Wiederholungsmechanismus
- Führen Sie eine Validierung durch
- Abonnements verwalten

Systemeigenschaften für Webhooks

Die Systemeigenschaften für Webhooks werden unten erläutert.

Eigenschaftsname	Beschreibung	Typ	Wert
sn_sec_tisc.Webhook_ignore_Threat_Sie_Webhook	Ignorieren Sie Webhook-Ereignisse, die durch die Neuberechnung der Bedrohungsbewertung ausgelöst wurden.	Wahr/falsch	True
sn_sec_tisc.Webhook_max_Maximale Anzahl	Maximale Anzahl von Ereignissen, die als Teil einer Webhook-	Ganzzahl	1000

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftsname	Beschreibung	Typ	Wert
	Anforderung gesendet werden sollen. Die Batchgröße ist auf 2000 beschränkt, auch wenn in dieser Eigenschaft ein höherer Wert festgelegt ist.		
sn_sec_tisc.Webhook_retry_count	Gibt an, wie oft eine fehlgeschlagene Anforderung wiederholt werden soll, bevor sie als Fehler markiert und mit dem nächsten Ereignisbatch fortgefahren wird. Die Anzahl der Wiederholungen ist auf 10 beschränkt, auch wenn in dieser Eigenschaft eine höhere Zahl festgelegt ist.	Ganzzahl	5
sn_sec_tisc.Webhook_retry_interval	Anzahl der Sekunden, die gewartet werden soll, bevor ein fehlgeschlagener Batch erneut versucht wird. Dies erhöht sich exponentiell basierend auf der Anzahl der Wiederholungen. Wenn beispielsweise retry_count 3 und retry_interval 30 ist, werden Wiederholungen nach 30, 60 und 120s ausgelöst Das anfängliche Wiederholungsintervall ist auf 300 Sekunden beschränkt, auch wenn in dieser Eigenschaft ein höherer Wert festgelegt ist.	Ganzzahl	30

Konfigurieren Sie Webhooks

Konfigurieren Sie einen Webhook zum Abonnieren von Ereignissen im Threat Intelligence-Sicherheitszentrum.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird
TISC-Webhooks bieten die Möglichkeit zur Integration in Sicherheitstools wie SIEM. Benutzer können dann verschiedene Ereignisse im Zusammenhang mit verschiedenen Artefakten abonnieren, z. B. erkennbare Elemente oder Indikatoren oder Malware- oder Bedrohungsakteure. TISC benachrichtigt Sicherheitstools (z. B. SIEM), wenn eine neue Threat Intelligence verfügbar ist oder vorhandene Threat Intelligence-Daten in TISC aktualisiert oder gelöscht werden.

Wenn beispielsweise ein neues erkennbares Element in Threat Intelligence hinzugefügt wird, wird eine Nutzlastanforderung an die Webhook-URL-Konfiguration gesendet. Diese Nutzlastanforderung erfasst normalerweise die Informationen erkennbarer Elemente und stellt sie als zusätzliche Informationen für Sicherheitstools (z. B. SIEM) bereit.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Webhooks-Konfigurationen** > **Webhooks**an.
   Die Seite „Webhooks“ wird angezeigt.
3. Klicken Sie auf **Neu**.
4. Klicken Sie Auf **Validieren und speichern** .
   Wenn Ihre Konfigurationsdetails falsch sind, validiert das System die Verbindung automatisch, wenn Konfigurationsdetails geändert werden, und die Anwendung fordert eine Warnmeldung auf, dass die Validierung des Webhooks fehlgeschlagen ist und Sie die Konfigurationsdetails überprüfen und entsprechend ändern müssen.

Hinweis:

- Zur Validierung des Webhooks wird eine leere Anforderungsnutzlast an den Endpunkt gesendet, und der Anwender muss sicherstellen, dass der Endpunkt einen erfolgreichen Antwortcode (200) sendet, wenn die leere Anforderung an den konfigurierten Webhook-Endpunkt übergeben wird.
- Standardmäßig befindet sich jeder erstellte Webhook im deaktivierten Status. Sie müssen den Webhook aktivieren und aktivieren. Ein Beispiel für einen Webhook wird im Basissystem als Verweis auf die Anwender bereitgestellt.

Auslöser Abonnieren

Zeigen Sie die Liste aller abonnierten Webhook-Auslöser für den aktuellen Webhook an.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Webhooks-Konfigurationen** > **Webhooks**an.
   Die Seite „Webhooks“ wird angezeigt.
3. Wählen Sie den Webhook aus.
   Der Abschnitt abonnierte Auslöser wird angezeigt.
4. Klicken Sie Auf **Abonnieren** Schaltfläche im Abschnitt „abonnierter Auslöser“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Listenansicht werden alle aktivierten Webhook-Auslöser in der Instanz angezeigt.

5. Wählen Sie die gewünschten Webhook-Auslöser aus, und klicken Sie auf **Abonnieren** Im Dialogfeld Webhook-Auslöser.
   Es wird eine Bestätigungsnachricht angezeigt, dass der Webhook die ausgewählten Auslöser erfolgreich abonniert hat. Von hier aus können Sie auch direkt einen neuen Auslöser erstellen und den Webhook abonnieren.

Hinweis:
Sie können auch **Abonnement Kündigen** Der Webhook aus den ausgewählten Auslösern.

Zeigen Sie Webhook-Fehlerprotokolle an

Verwenden Sie diesen Abschnitt „Fehlerprotokolle“, um alle Audit-Einträge anzuzeigen, die im Status für einen bestimmten Webhook als Fehler markiert sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird
Die Audit-Protokolle ermöglichen es Anwendern, die Ausführung weiter zu untersuchen, zu debuggen und die Ursache des Ausführungsfehlers zu identifizieren.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Webhooks-Konfigurationen** > **Webhooks**an.
   Die Seite „Webhooks“ wird angezeigt.
3. Wählen Sie den Webhook aus.
4. Wechseln Sie zu **Fehlerprotokolle** .
5. Zeigen Sie die Fehlerprotokolle an.
   In der Listenansicht werden alle Fehlerprotokolle aus einem bestimmten Webhook angezeigt.
6. Wechseln Sie zu **Batch** Spalte.
7. Klicken Sie auf eine beliebige Option **Batch-ID** .

Hinweis:
Jedes Fehlerprotokoll ist einem Batch zugeordnet. Mithilfe der Batch-ID (in der Spalte „Batch“) können Sie den zugehörigen Batch-Datensatz anzeigen. Klicken Sie auf eine beliebige Batch-ID, und diese wird in einer separaten Registerkarte geöffnet. Jede Batch-ID enthält die Webhook-Batchnummer, die Fehlermeldung, den Antwortstatuscode, die Anzahl der Wiederholungen, die tatsächliche Nutzlast, und die Liste der Ereignisse, die an den Webhook gesendet werden.

8. Klicken Sie Auf **Batch wiederholen** Um die fehlgeschlagenen Batches zu wiederholen.
   Wenn Sie auf diese Schaltfläche klicken, wird eine Anforderungsnutzlast (dieser bestimmten Batch-Informationen) an den konfigurierten Webhook-Endpunkt gesendet.

Hinweis:
Diese Aktion ist nur für die Batch-Datensätze verfügbar, die Ausführungsfehler aufweisen oder erfolgreich abgeschlossen wurden, und die Datensätze, die sich im Wiederholungsstatus befinden, werden automatisch wiederholt.

Zeigen Sie Webhook-Batches an

Für jede Webhook-Ausführung wird ein Webhook-Batch-Datensatz erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Um die Anzahl der API-Aufrufe zu reduzieren, die an die Webhook-Endpunkte gesendet werden, wird das Batching von Ereignissen in Webhooks implementiert. Wenn für jeden Webhook mehrere Ereignisse fast gleichzeitig ausgelöst werden, werden alle diese Ereignisse als Teil derselben Anforderung an den Webhook-Endpunkt gesendet.

Prozedur
1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Webhooks-Konfigurationen** > **Webhooks**an.
   Die Seite „Webhooks“ wird angezeigt.
3. Wählen Sie den Webhook aus.
4. Wechseln Sie zu **Fehlerprotokolle** .
5. Zeigen Sie die Fehlerprotokolle an.
   In der Listenansicht werden alle Fehlerprotokolle aus einem bestimmten Webhook angezeigt.
6. Wechseln Sie zu **Batch** Spalte.
7. Klicken Sie auf eine beliebige Option **Batch-ID** .
   Die Seite „Webhook-Batch“ wird angezeigt.

Hinweis:
Alle Batches werden in der Tabelle gespeichert `sn_sec_tisc_Webhook_Batch` .

Nachfolgend finden Sie das Beispielnutzlastformat, das der Webhook-Endpunkt empfängt:


```
{
  "batch_id": "06eeb3693b6bca10f6f82a60c5e45a7b",
  "events": [
    {
      "record": "Observable",
      "record_fields": {
        "is_false_positive": "false",
        "reputation": "malicious",
        "sys_updated_on": "2024-07-22T14:31:26.000Z",
        "type": "url",
        "sys_updated_by": "admin",
        "sys_created_on": "2024-07-04T06:45:20.000Z",
        "id": "url--1e77adb7eb8b06107750fa86cad0cd70",
        "is_defanged": "false",
        "sys_created_by": "SecCommon.System",
        "tags": "Enriched",
        "taxonomies": "T1: V1",
        "domain": "urlhaus.abuse.ch",
        "status": "active",
        "source_count": "1",
        "threat_score": "20",
        "sys_id": "da77adb7eb8b06107750fa86cad0cd70",
        "value": "https://urlhaus.abuse.ch/url/2578255/",
        "confidence": "89",
        "expiration_time": "2025-10-07T07:13:18.000Z",
        "tlp": "CLEAR"
      },
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        "trigger": {
          "name": "Observable Update",
          "type": "UPDATE",
          "trigger_time": "2024-07-22T14:31:26.000Z",
          "trigger_fields": [
            {
              "field_name": "reputation",
              "previous_value": null,
              "current_value": "malicious"
            }
          ]
        }
      },
      {
        "record": "Observable",
        "record_fields": {
          "is_false_positive": "false",
          "reputation": "malicious",
          "sys_updated_on": "2024-07-22T14:31:19.000Z",
          "type": "url",
          "sys_updated_by": "admin",
          "sys_created_on": "2024-07-04T06:45:20.000Z",
          "id": "url--9a77adb7eb8b06107750fa86cad0cd6f",
          "is_defanged": "false",
          "sys_created_by": "SecCommon.System",
          "tags": "Enriched",
          "taxonomies": "T1: V1",
          "domain": "urlhaus.abuse.ch",
          "status": "active",
          "source_count": "1",
          "threat_score": "20",
          "sys_id": "5a77adb7eb8b06107750fa86cad0cd6f",
          "value": "https://urlhaus.abuse.ch/url/2578264/",
          "confidence": "89",
          "expiration_time": "2025-10-07T07:13:18.000Z",
          "tlp": "CLEAR"
        },
        "trigger": {
          "name": "Observable Update",
          "type": "UPDATE",
          "trigger_time": "2024-07-22T14:31:19.000Z",
          "trigger_fields": [
            {
              "field_name": "reputation",
              "previous_value": null,
              "current_value": "malicious"
            }
          ]
        }
      }
    ]
}
```


Die folgende Tabelle listet die Batch-Nutzlaststruktur und ihre Attribute auf, die als Webhook-Nutzlast an die Anwender gesendet werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter in Batch-Nutzlast	Typ	Beschreibung
batch_id	Zeichenfolge	Gibt einen eindeutigen Bezeichner für einen Batch an.
Ereignisse	Array von Objekten	Enthält ein Array von Ereignissen, die als Teil dieses Webhooks ausgelöst werden. Jedes Ereignis enthält den Snapshot der Feldwerte zum Zeitpunkt der Ereignisgenerierung und enthält auch die Auslöserinformationen. **Hinweis:** Weitere Informationen zum Anzeigen der Parameter im Ereignisobjekt finden Sie unter Webhook-Auslöser.

Hinweis:

8. Klicken Sie Auf **Batch wiederholen** Schaltfläche zum erneuten Versuch des fehlgeschlagenen Batches.

Hinweis:
Sie können auch den Wiederholungs-Batch für die abgeschlossenen Batches auslösen.

Webhook-Auslöser

Webhook-Auslöser werden verwendet, um die Threat Intelligence-Entitäten zu filtern, die nach Ereignisänderungen wie Erstellen, Aktualisieren und Löschen nachverfolgt werden müssen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Webhooks-Konfigurationen** > **Wiederholungen**an.
   Die Seite Webhooks-Auslöser wird angezeigt.
3. Klicken Sie auf **Neu**.
4. Klicken Sie auf **Speichern**.
   Standardmäßig wird der Auslöser im deaktivierten Status erstellt.
5. Klicken Sie Auf **Aktivieren** Um den Auslöser zu aktivieren, ist dieser Auslöser für die Webhooks zum Abonnieren verfügbar.

Hinweis:
Klicken Sie Auf **Deaktivieren** Zum Deaktivieren des aktivierten Auslösers und der Deaktivierung werden alle zugehörigen Webhooks von diesem Auslöser abbestellt.

6. Klicken Sie Auf **Zeigen Sie Die Beispielnutzlast An** Zum Auswählen des Datensatzes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie die Beispielnutzlast dieses bestimmten Webhook-Auslösers an. Basierend auf der ausgewählten Tabelle werden diese Datensätze aus der angegebenen Tabelle in ausgefüllt **Wählen Sie Datensatz Aus** Dropdown-Liste. Wählen Sie den Datensatz aus, um die Beispielnutzlast anzuzeigen. Die Beispielnutzlast wird im JSON-Format angezeigt. Die Felder in der Nutzlast sind unten aufgeführt.

7. Wählen Sie den Typ des Datensatzes aus der Dropdown-Liste aus.
Die Nutzlast wird automatisch basierend auf dem ausgewählten Datensatz geändert.


```
{
   "record": "Observable",
   "record_fields": {
      "additional_context": "This could be a potential malicious IP. ",
      "attack_phases": "Lockheed Martin: Command and Control",
      "author": "Anomali",
      "confidence": "50",
      "description": "This could be a potential malicious IP. ",
      "expiration_time": "2024-12-01T00:00:00.000Z",
      "first_observed": "2024-01-01T00:00:00.000Z",
      "first_seen": "2024-01-01T00:00:00.000Z",
      "id": "ipv4-addr--70526b0a436a02102164e0ea78b8f210",
      "is_defanged": "false",
      "is_false_positive": "false",
      "last_observed": "2024-01-01T00:00:00.000Z",
      "last_seen": "2024-01-01T00:00:00.000Z",
      "reputation": "suspicious",
      "source_count": "1",
      "status": "active",
      "sys_created_by": "SecCommon.System",
      "sys_created_on": "2024-06-04T00:00:00.000Z",
      "sys_id": "30526b0a436a02102164e0ea78b8f210",
      "sys_updated_by": "system",
      "sys_updated_on": "2024-06-15T00:00:00.000Z",
      "tags": "critical",
      "taxonomies": "MITRE: T121",
      "threat_level": "medium",
      "threat_score": "24",
      "threat_severity": "medium",
      "tlp": "CLEAR",
      "type": "ip_v4_address",
      "usage_categories": "APT",
      "value": "116.98.170.70"
   },
   "trigger": {
      "name": "Observable Update",
      "type": "UPDATE",
      "trigger_time": "2024-07-26T07:27:29.000Z",
      "trigger_fields": [
         {
            "field_name": "confidence",
            "previous_value": "30",
            "current_value": "50"
         }
      ]
   }
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste der Parameter in der Auslösernutzlast

Parameter in Auslösernutzlast	Typ	Beschreibung
record	Zeichenfolge	Gibt den Datensatztyp an, z. B. erkennbares Element oder Indikator.
Record_fields	Objekt	Gibt den Snapshot der Datensatzfelder an, wenn das Ereignis generiert wird. Eine Liste der unterstützten Felder finden Sie in der Tabelle im folgenden Abschnitt.
Auslöser	Objekt	Gibt die übereinstimmenden Auslöserinformationen an.
trigger.name	Zeichenfolge	Gibt den Namen des Auslösers an
Auslöser.Typ	Zeichenfolge	Gibt den Typ des Auslösers an. Gültige Werte sind „CREATE“, „UPDATE“, „DELETE“.
Auslöser.Auslöser_Zeit	Datum (im ISO-Format mit UTC-Zeitzone)	Gibt die Zeit an, zu der das Ereignis im Datensatz aufgetreten ist.
Trigger_fields	Array von Objekten	Dies ist nur für den AKTUALISIERUNGSAUSLÖSERTYP verfügbar. Gibt die Liste der Auslöserfelder an, die im Zuge des Ereignisses geändert wurden. Die Parameter in **Trigger_fields** Sind: ○ **Feldname** : Gibt den Feldnamen an, der geändert wurde ○ **Vorheriger_Wert** : Gibt den vorherigen Wert des Felds an. ○ **Current_value** : Gibt den aktuellen Wert des Felds an.

Liste der unterstützten Felder für „Auslöser erstellen und aktualisieren“

Tabelle	Spaltenname	Spaltenbezeichnung
Kampagne	Aliasse	Aliasse
Kampagne	Beschreibung	Beschreibung
Kampagne	first_seen	Erstmals aufgetreten
Kampagne	last_seen	Zuletzt aufgetreten
Kampagne	name	Name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Spaltenname	Spaltenbezeichnung
Kampagne	Ziel	Ziel
Indikator	additional_context	Zusätzlicher Kontext
Indikator	Attack_Phases	Angriffsphasen
Indikator	Autor	Autor
Indikator	confidence	Vertrauen
Indikator	Beschreibung	Beschreibung
Indikator	Ablaufzeit	Ablaufzeit
Indikator	First_detected	Zuerst erkannt
Indikator	First_Observed	Zuerst beobachtet
Indikator	first_seen	Erstmals aufgetreten
Indikator	id	ID
Indikator	Indikatortypen	Indikatortypen
Indikator	ioc_classification	IoC-Klassifizierung
Indikator	Last_Observed	Zuletzt beobachtet
Indikator	last_seen	Zuletzt aufgetreten
Indikator	name	Name
Indikator	pattern	Muster
Indikator	Muster_Typ	Mustertyp
Indikator	Pattern_Version	Musterversion
Indikator	Plattformen	Plattformen
Indikator	widerrufen	Widerrufen
Indikator	Source_count	Anzahl der Quellen
Indikator	SPEC_Version	Spezifikationsversion
Indikator	status	Status
Indikator	tags	TISC-Tags
Indikator	Taxonomien	Taxonomien
Indikator	Threat_level	Bedrohungsstufe
Indikator	Threat_severity	Bedrohungsschweregrad
Indikator	tlp	TLP
Indikator	Usage_Categories	Nutzungskategorien
Indikator	Valid_from	Gültig ab
Indikator	Valid_until	Gültig bis
Malware	Aliasse	Aliasse
Malware	Attack_Phases	Angriffsphasen
Malware	Beschreibung	Beschreibung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Spaltenname	Spaltenbezeichnung
Malware	Executable_Process_Architectures	Prozessarchitekturen
Malware	first_seen	Erstmals aufgetreten
Malware	Implementation_Languages	Implementierungssprachen
Malware	Is_family	Ist Familie
Malware	last_seen	Zuletzt aufgetreten
Malware	Malware_Capabilities	Malware-Fähigkeiten
Malware	Malware_types	Schadsoftwaretypen
Malware	name	Name
Objekt (Allgemeine Objektfelder)	additional_context	Zusätzlicher Kontext
Objekt (Allgemeine Objektfelder)	confidence	Vertrauen
Objekt (Allgemeine Objektfelder)	Ablaufzeit	Ablaufzeit
Objekt (Allgemeine Objektfelder)	id	ID
Objekt (Allgemeine Objektfelder)	widerrufen	Widerrufen
Objekt (Allgemeine Objektfelder)	Source_count	Anzahl der Quellen
Objekt (Allgemeine Objektfelder)	SPEC_Version	Spezifikationsversion
Objekt (Allgemeine Objektfelder)	status	Status
Objekt (Allgemeine Objektfelder)	tags	TISC-Tags
Objekt (Allgemeine Objektfelder)	Taxonomien	Taxonomien
Objekt (Allgemeine Objektfelder)	Threat_level	Bedrohungsstufe
Objekt (Allgemeine Objektfelder)	Threat_severity	Bedrohungsschweregrad
Objekt (Allgemeine Objektfelder)	tlp	TLP
Erkennbares Element	additional_context	Zusätzlicher Kontext
Erkennbares Element	Attack_Phases	Angriffsphasen
Erkennbares Element	Autor	Autor
Erkennbares Element	confidence	Vertrauen
Erkennbares Element	Beschreibung	Beschreibung
Erkennbares Element	Ablaufzeit	Ablaufzeit
Erkennbares Element	First_Observed	Zuerst beobachtet
Erkennbares Element	first_seen	Erstmals aufgetreten
Erkennbares Element	id	ID
Erkennbares Element	Is_defanged	Ist entsperrt
Erkennbares Element	Ist_falsch_positiv	Ist falsch positiv
Erkennbares Element	Last_Observed	Zuletzt beobachtet
Erkennbares Element	last_seen	Zuletzt aufgetreten
Erkennbares Element	Reputation	Reputation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Spaltenname	Spaltenbezeichnung
Erkennbares Element	Source_count	Anzahl der Quellen
Erkennbares Element	status	Status
Erkennbares Element	tags	TISC-Tags
Erkennbares Element	Taxonomien	Taxonomien
Erkennbares Element	Threat_level	Bedrohungsstufe
Erkennbares Element	Threat_Score	Bedrohungsbewertung
Erkennbares Element	Threat_severity	Bedrohungsschweregrad
Erkennbares Element	tlp	TLP
Erkennbares Element	type	Typ
Erkennbares Element	Usage_Categories	Nutzungskategorien
Erkennbares Element	Wert	Wert
Bedrohungsakteur	Aliasse	Aliasse
Bedrohungsakteur	Beschreibung	Beschreibung
Bedrohungsakteur	first_seen	Erstmals aufgetreten
Bedrohungsakteur	goals	Ziele
Bedrohungsakteur	last_seen	Zuletzt aufgetreten
Bedrohungsakteur	name	Name
Bedrohungsakteur	Personal_Motivations	Persönliche Motivationen
Bedrohungsakteur	Primary_Motivation	Primäre Motivation
Bedrohungsakteur	Resource_level	Ressourcenebene
Bedrohungsakteur	Secondary_Motivations	Sekundäre Motivationen
Bedrohungsakteur	Raffinesse	Ausgereiftheit
Bedrohungsakteur	Threat_actor_roles	Bedrohungsakteurrollen
Bedrohungsakteur	Threat_actor_types	Bedrohungsakteurtypen
Bedrohungsbericht	Beschreibung	Beschreibung
Bedrohungsbericht	name	Name
Bedrohungsbericht	Veröffentlicht	Veröffentlicht
Bedrohungsbericht	Report_types	Berichtstypen
Schwachstelle	Betroffene_Software	Betroffene Software
Schwachstelle	Beschreibung	Beschreibung
Schwachstelle	Exploitation_Status	Nutzungsstatus
Schwachstelle	Exploit_exists	Exploit vorhanden
Schwachstelle	name	Name
Schwachstelle	Veröffentlicht	Veröffentlicht
Schwachstelle	Record_Last_modified	Datensatz zuletzt geändert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Spaltenname	Spaltenbezeichnung
Schwachstelle	severity	Schweregrad

Unten finden Sie die Liste der anwendbaren Systemfelder, die für jede Entität gemeinsam sind. Diese werden in der Webhook-Auslöser-Nutzlast für Erstellungs- und Update-Auslöser unterstützt.

- sys_ID (SYS-ID)
- sys_created_on (erstellt)
- sys_created_by (erstellt von)
- sys_updated_on (aktualisiert)
- sys_updated_by (aktualisiert von)

Hinweis:
Beim Löschen wird nur sys_ID (SYS-ID) als Teil der Nutzlast an die Webhook-Endpunkt-URL gesendet, und andere Systemfelder werden nicht unterstützt.

Liste der unterstützten Felder für Löschauslöser

Tabelle	Spaltenname	Spaltenbezeichnung
Erkennbares Element	type	Typ
Erkennbares Element	Wert	Wert
Indikator	name	Name
Indikator	pattern	Muster
Indikator	Muster_Typ	Mustertyp
Indikator	Valid_from	Gültig ab
Kampagne	name	Name
Malware	Is_family	Ist Familie
Malware	name	Name
Bedrohungsakteur	name	Name
Bedrohungsbericht	name	Name
Bedrohungsbericht	Veröffentlicht	Veröffentlicht
Schwachstelle	name	Name
Schwachstelle	severity	Schweregrad

Konfigurieren Sie Tooltips für Nodemaps

Verwenden Sie diesen Abschnitt, um Tooltips für Knotenzuordnungsbeziehungen im Untersuchungs-Canvas zu konfigurieren.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Nodemap-Steuerungen** > **Tooltip-Konfiguration**an.
2. Wählen Sie das gewünschte Objekt aus der Liste aus.
   Standardmäßig werden die folgenden drei Datensätze im Basissystem bereitgestellt.
   a. Erkennbare Elemente
   b. Indikatoren
   c. Objekte
3. Wählen Sie Aus **Erkennbares Element** Als Beispieldatensatz.
4. Fügen Sie dem Datensatz des erkennbaren Elements bei Bedarf einen oder mehrere Werte hinzu.
   Fügen Sie Indikatoren und anderen Objekten gleichermaßen Werte hinzu.

   Hinweis:
   Jedes Objekt unterstützt maximal sechs Werte.

5. Wählen Sie Aus **Speichern** Zum Anwenden der Änderungen.
6. Wechseln Sie zu **Untersuchungs-Canvas** Abschnitt und wählen Sie aus **Aktualisieren** Symbol.
   Dieselben Werte sind auf konfiguriert **Tooltip-Konfiguration** Seite wird auf jeder Knotenzuordnung angezeigt.

Arbeiten mit automatisierten Flows

Verwenden Sie diese definierten Schritte, um zu erfahren, wie Sie die automatisierten Flows in TISC und seine Fähigkeiten verwenden können.

Erstellen Sie Flows, die mit TISC-Rollen ausgeführt werden. In TISC werden die Flows für Folgendes erstellt:

- Automatisierte IOC-Anreicherung
- Analysieren, bewerten und verbreiten Sie die IOC im Zusammenhang mit der Bedrohung
- Analysieren, bewerten Sie die IOC im Zusammenhang mit der Bedrohung, und erstellen Sie einen Incident.
- Schwachstellenmanagement-Support.
- Zero-Day-Schwachstellennachverfolgung.

Hinweis:
Alle Flows sind Vorlagen, die im Entwurfsstatus geliefert werden, damit Anwender sie an ihre eigenen Anforderungen anpassen oder kopieren können.

Wiederverwendbare Aktionen

Flow-Aktion	Beschreibung
Fügen Sie Der Entität Ein Tag Hinzu	Hinzufügen eines Tags zu einer Entität, die es unterstützt (erkennbares Element/Indikator/Objekt).
Tag aus Entität entfernen	Tag wird in einer Entität entfernt, die es unterstützt (erkennbares Element/Indikator/Objekt).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flow-Aktion	Beschreibung
Überprüfen, ob die IP-Adresse im CIDR-Bereich vorhanden ist	Überprüft, ob sich eine IP-Adresse in einem CIDR-Bereich befindet.
Überprüfen, ob die IP-Adresse im Bereich vorhanden ist	Überprüft, ob sich eine IP-Adresse im Bereich von und bis befindet.

Automatisierte IOC-Anreicherung

Erfahren Sie, wie Sie die Anreicherung von IOC mithilfe von Flows automatisieren, wenn sie einem bestimmten Kriterium entsprechen.

Vorbereitungen

Erforderliche Rolle:

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

Ergänzung der IOC-Auslöser nur dann automatisieren, wenn:

- Der Typ des erkennbaren Elements ist ein Domänenname, eine IPv4-Adresse oder eine IPv6-Adresse.
- Das erkennbare Element befindet sich im Status „verarbeitet“.
- Für das erkennbare Element sind die Tags nicht angereichert oder Anreicherung überspringen.

Prozedur

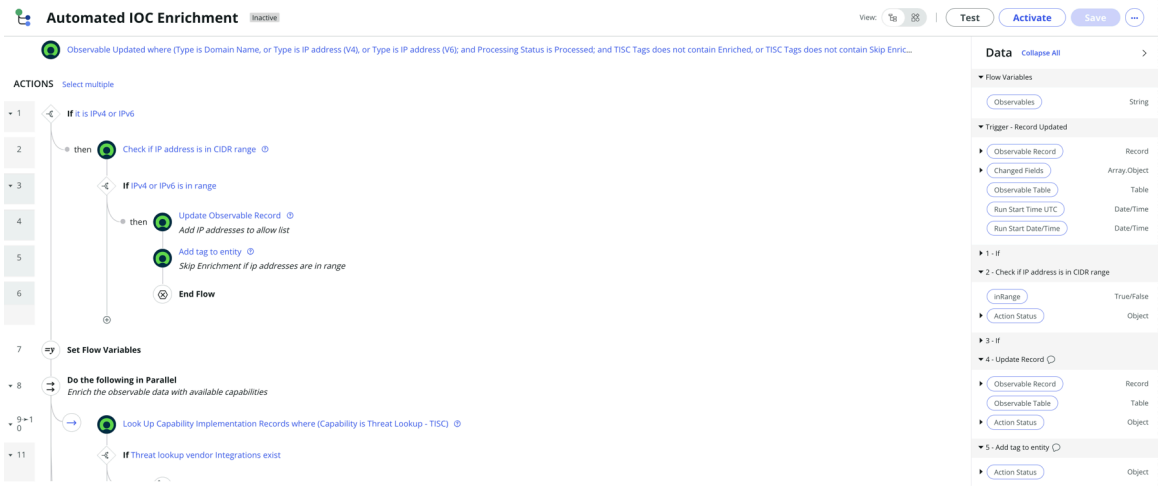
1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Automatisierte Flows**an.
3. Wählen Sie Aus **Automatisierte IOC-Anreicherung** Aktionslink zum Anzeigen der jeweiligen Regeldetails im Flow Designer.
4. Zeigen Sie die Flow Designer-Aktion für den folgenden Auslöser an:

   Observable Updated where (Type is Domain Name, or Type is IP address (V4), or Type is IP address (V6); and Processing Status is Processed; and TISC Tags does not contain Enriched, or TISC Tags does not contain Skip Enrichment, or TISC Tags does not contain Potential New Threat)

5. **Wenn das erkennbare Element eine IPv4- oder IPv6-Adresse ist und in einen zulässigen CIDR-Bereich fällt, gilt Folgendes:**
   a. Fügen Sie das erkennbare Element der Allow-Liste hinzu.
   b. Aktualisieren Sie die Tags erkennbarer Elemente auf „Anreicherung überspringen“.
   c. Beenden Sie den Flow für dieses erkennbare Element.
6. **Andernfalls ergänzen Sie die Daten erkennbarer Elemente mit verfügbaren Fähigkeiten:**
   a. Führen Sie eine Bedrohungssuche und eine Sichtungssuche durch, um zusätzliche Informationen zum erkennbaren Element zu sammeln.
   b. Aktualisieren Sie das erkennbare Element mit angereicherten Daten.
   c. Fügen Sie ein Tag hinzu **Angereichert** Gibt an, dass das IOC verarbeitet wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. **Wenn die Reputation erkennbarer Elemente sauber ist, gilt Folgendes:**
   a. Kennzeichnen Sie das erkennbare Element als falsch positiv, und deaktivieren Sie es.
8. **Andernfalls, wenn die Reputation erkennbarer Elemente unbekannt ist**
   a. Tag hinzufügen **Keine Potenzielle Bedrohung Und Angereichert** Um anzugeben, dass es sich nicht um eine Bedrohung handelt.



Automatisierte Freigabe von IOC mit hohem Risiko für vertrauenswürdige Partner

Erfahren Sie, wie Sie die Freigabe von IOC mit hohem Risiko für vertrauenswürdige Partner automatisieren können.

Vorbereitungen

Erforderliche Rolle:

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

Die automatisierte Freigabe von IOC mit hohem Risiko für vertrauenswürdige Partner wird nur ausgelöst, wenn:

- Der Typ des erkennbaren Elements ist ein Domänenname, eine IPv4-Adresse oder eine IPv6-Adresse.
- Das erkennbare Element befindet sich im Status „verarbeitet“.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Automatisierte Flows**an.
3. Wählen Sie Aus **Automatisierte Freigabe von IOC mit hohem Risiko für vertrauenswürdige Partner** Aktionslink zum Anzeigen der jeweiligen Regeldetails im Flow Designer.
4. Zeigen Sie die Flow Designer-Aktion für die folgenden Auslöser an:

Daily at 12.00.00 Run every day once

5. **Aktionen** :

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Suchen Sie nach dem Systemeigenschaftsdatensatz, und durchsuchen Sie den Schwellenwert für ausgehende Intelligenz:

```
Look Up System Property Record where (Name is
sn_sec_tisc.shared_intelligence_entity_threshold).
```

b. IOC-Typ = IP, Domäne, Hash; Reputation = böswillig; Konfidenz >= 80 oder Bedrohungspunktzahl >=80.

```
Look Up Observable Records where (Type is IP address (V4), or Type is IP address (V6),
or Type is Domain Name, or Type is MD5 hash; and Confidence greater than 80, and
Reputation is Malicious, and Processing Status is Processed, and Updated on Yesterday)
IOC type = IP, Domain, Hash; Reputation = Malicious ; confidence >= 80 or Threat Score
>=80.
```

6. **Wenn der Schwellenwert von Datensätzen, die dem ausgehenden Intelligence-Datensatz hinzugefügt werden können, erfüllt ist, gehen Sie folgendermaßen vor:**

   a. Das System übergibt die Datensätze automatisch zur Verarbeitung an die Aktion Automated Outbound Intelligence.

   b. Beenden Sie den Flow für diese Freigabe von IOCs mit hohem Risiko für vertrauenswürdige Partner.

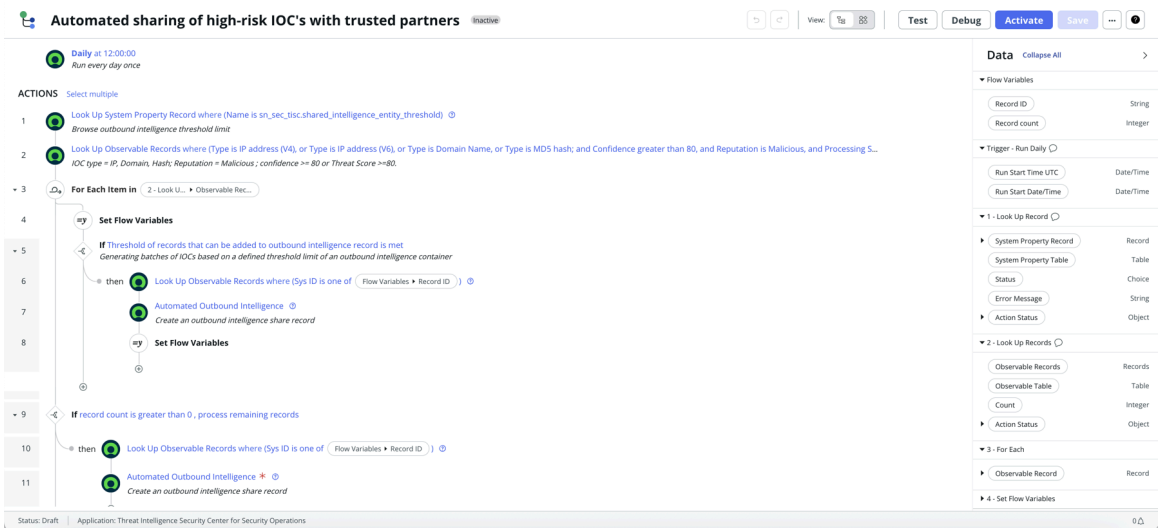
7. **Wenn die Datensatzanzahl größer als 0 ist, verarbeitet das System die verbleibenden Datensätze.**
   Beispiel:

   Wenn der definierte Schwellenwert 1000 ist und insgesamt 2030 Datensätze verarbeitet werden sollen:

   - Ausgehender Intelligence-Datensatz Nr. 1 wird mit den ersten 1000 Datensätzen erstellt.
   - Ausgehender Intelligence-Datensatz Nr. 2 wird mit den nächsten 1000 Datensätzen erstellt.
   - Ausgehender Intelligence-Datensatz Nr. 3 wird mit den verbleibenden 30 Datensätzen erstellt.

   Dieser Batching-Prozess stellt sicher, dass der Schwellenwert eingehalten wird und gleichzeitig alle Intelligence-Datensätze effizient verarbeitet werden.

8. Beenden Sie den Flow für diese Freigabe von IOCs mit hohem Risiko für vertrauenswürdige Partner.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Automatisierte Freigabe ausgehender Intelligence-Datensätze

Freigabe ausgehender Intelligence-Datensätze aus der GUI

Fügen Sie einer TAXII-Sammlung automatisch Threat Intelligence hinzu

Erfahren Sie, wie Sie einer TAXII-Serversammlung automatisch Threat Intelligence hinzufügen.

Vorbereitungen

Erforderliche Rolle:

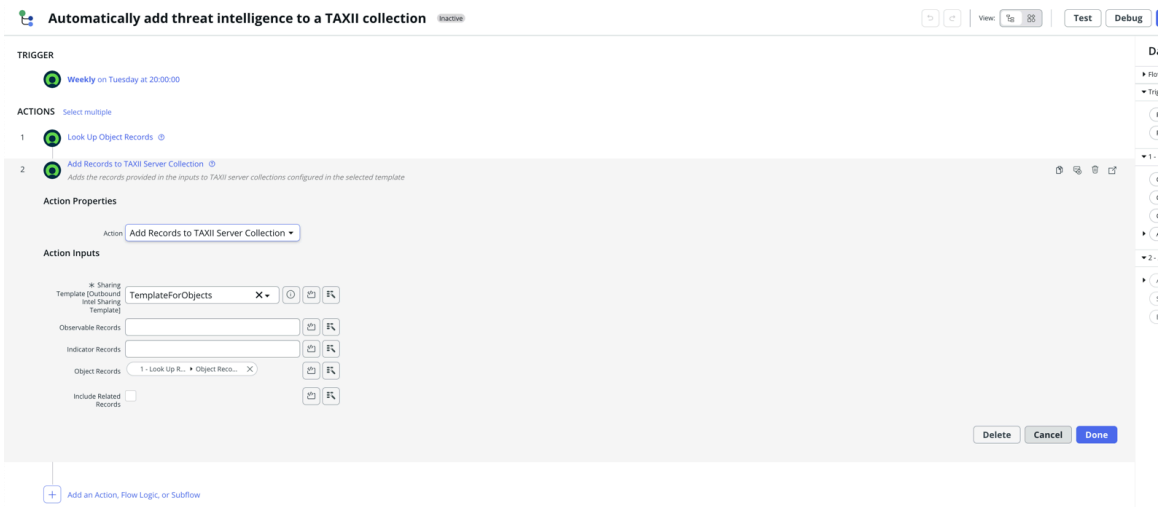
- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Automatisierte Flows**an.
3. Wählen Sie Aus **Fügen Sie einer TAXII-Sammlung automatisch Threat Intelligence hinzu** Aktionslink zum Anzeigen der jeweiligen Regeldetails im Flow Designer.
4. Zeigen Sie die Flow Designer-Aktion für die folgenden Auslöser an:

Observable Created or Updated where (Type is IP address (V4), or Type is IP address (V6), or Type is Domain Name; and TISC Tags contains Add to: Sample Collection, and Reputation is Malicious, and Threat Score greater than or is 60

5. **Aktionen**
   Fügt den in den Eingaben bereitgestellten Datensatz zu TAXII-Serversammlungen hinzu, die in der ausgewählten Vorlage konfiguriert sind
   a. **Fügen Sie der TAXII-Serversammlung einen Datensatz hinzu**
   b. **Fügen Sie der TAXII-Serversammlung Datensätze hinzu**
6. Beenden Sie den Flow zum Hinzufügen von Threat Intelligence zu einer TAXII-Sammlung.



Analysieren, bewerten und verbreiten Sie erkennbare Elemente

Erfahren Sie, wie Sie erkennbare Elemente analysieren und verbreiten, die sich auf Bedrohungen beziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

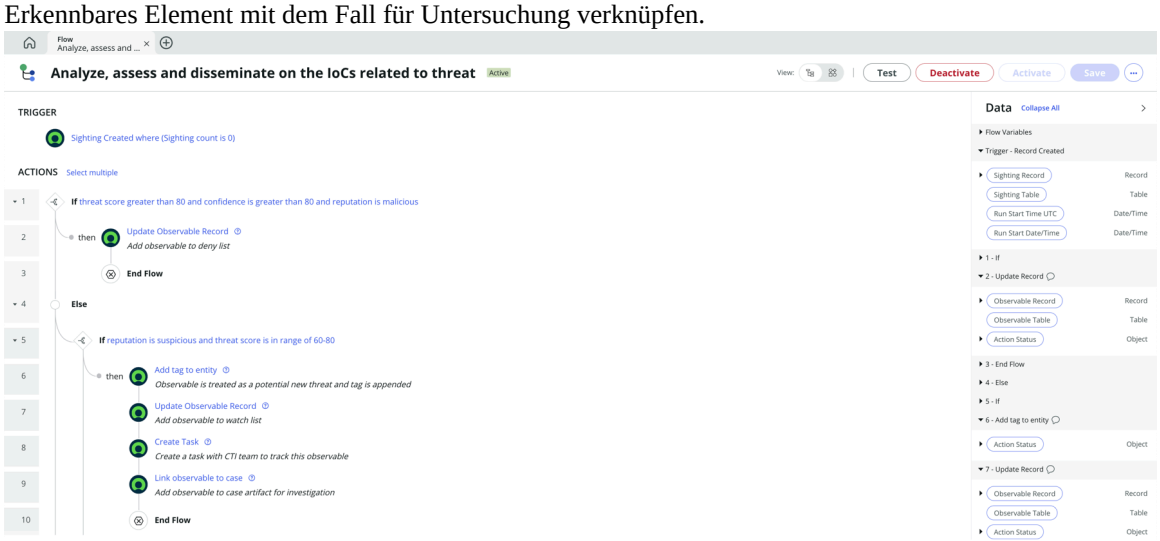
Wenn eine Ergänzung der Sichtungssuche angefordert wird, wird sie ohne Sichtungen zurückgegeben.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Automatisierte Flows**an.
3. Wählen Sie Aus **Analysieren, bewerten und verbreiten Sie die IoCs im Zusammenhang mit der Bedrohung** Aktionslink zum Anzeigen der jeweiligen Regeldetails im Flow Designer.
4. Zeigen Sie die Flow Designer-Aktion für den folgenden Auslöser an:

   Sighting Created where (Sighting count is 0)

5. **Das erkennbare Element hat eine Bedrohungspunktzahl von mehr als 80, eine Konfidenz von mehr als 80 und eine böswillige Reputation:**
   a. Fügen Sie das erkennbare Element zur Verweigerungsliste hinzu.
   b. Beenden Sie den Flow für dieses erkennbare Element.
6. **Andernfalls ist die Reputation des erkennbaren Elements verdächtig, und die Bedrohungspunktzahl liegt im Bereich von 60 bis 80:**
   a. Fügen Sie ein Tag mit der Bezeichnung potenzielle neue Bedrohung hinzu.
   b. Fügen Sie das erkennbare Element der Beobachtungsliste hinzu.
   c. Erstellen Sie eine Fallaufgabe mit dem CTI-Team, um dieses erkennbare Element nachzuverfolgen und weiter zu analysieren.
   d. Erkennbares Element mit dem Fall für Untersuchung verknüpfen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Analysieren und bewerten Sie Bedrohungs-IOCs

Erfahren Sie, wie Sie IOC analysieren, die eine Bedrohung darstellen, und das Security Incident-Team benachrichtigen.

Vorbereitungen

Erforderliche Rolle:

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

Wann immer eine Ergänzung der Sichtungssuche angefordert wird:

- Wenn das erkennbare Element gesehen wird (Anzahl > 0) und
- Reputation erkennbarer Elemente ist böswillig und
- Die Bedrohungspunktzahl des erkennbaren Elements ist > 80 und
- Konfidenz Erkennbarer Elemente > 80

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Automatisierte Flows**an.
3. Wählen Sie Aus **Analysieren Sie die IoCs im Zusammenhang mit der Bedrohung, bewerten Sie sie, und erstellen Sie einen Incident** Aktionslink zum Anzeigen der jeweiligen Regeldetails im Flow Designer.
4. Zeigen Sie die Flow Designer-Aktion für den folgenden Auslöser an:

   Sighting Created where (Sighting count greater than 0, and Observable. Reputation is Malicious, and Observable. Threat Score greater than 80, and Observable. Confidence greater than 80)

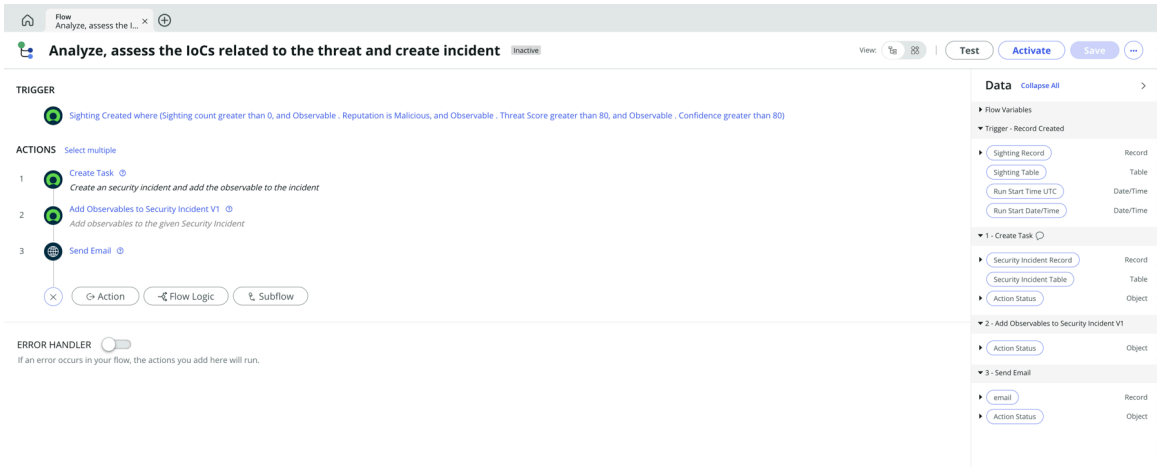
5. **Wenn eine Sichtung erstellt wurde, wo (Sichtungsanzahl größer als 0 und erkennbares Element. Reputation ist böswillig und erkennbar. Bedrohungspunktzahl größer als 80 und erkennbares Element. Konfidenz größer als 80), dann:**

   a. Erstellen Sie einen Security Incident, und fügen Sie dem Incident das erkennbare Element hinzu.

   b. Fügen Sie dem Security Incident V1 erkennbare Elemente hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Senden Sie eine E-Mail-Kommunikation.



Schwachstellenmanagement-Support

Erfahren Sie, wie in TISC eine neue Schwachstelle mit einer zugehörigen Schwachstelle in VR erstellt wird.

Vorbereitungen

Erforderliche Rolle:

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

Wenn in TISC eine neue Schwachstelle erstellt wird und eine zugehörige Schwachstelle in VR vorhanden ist.

- Wenn die Punktzahl der VR-Schwachstelle (v2) > 8 ist ODER die Punktzahl der VR-Schwachstelle (v3) > 8 ist.
- Die Gesamtanzahl der ihm zugeordneten VI ist größer als 0.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Automatisierte Flows**an.
3. Wählen Sie Aus **Schwachstellenmanagement-Support** Aktionslink zum Anzeigen der jeweiligen Regeldetails im Flow Designer.
4. Zeigen Sie die Flow Designer-Aktion für den folgenden Auslöser an:

   When new vulnerability is created in TISC and there is a related vulnerability in VR.

5. **Wenn der Prozentsatz der insgesamt korrigierten VIS, die dieser Schwachstelle zugeordnet sind, 100 % beträgt, dann:**

   a. Fügen Sie dem erkennbaren Element ein Tag namens „korrigiert“ hinzu.

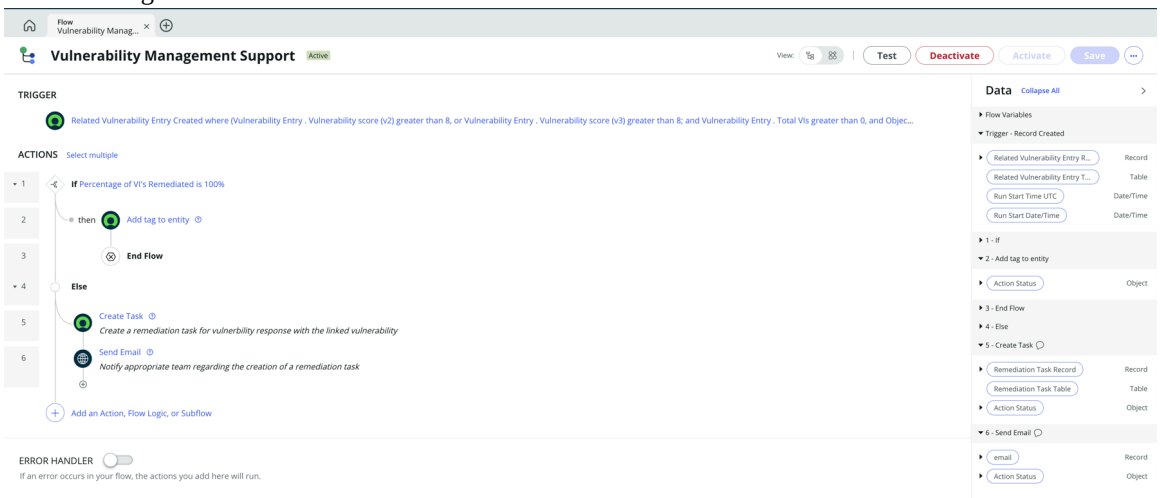
6. **Andernfalls ergänzen Sie die Daten erkennbarer Elemente mit verfügbaren Fähigkeiten:**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Erstellen Sie eine Korrekturaufgabe für VR.

b. Benachrichtigen Sie die betroffenen VR-Teams darüber.



Zero-Day-Schwachstellennachverfolgung

Erfahren Sie, wie Sie RSS-Feeds analysieren, die in das System eingehen.

Vorbereitungen

Erforderliche Rolle:

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

Jedes Mal, wenn ein neuer RSS-Feed im System erstellt wird und im Titel oder in der Beschreibung „Zero Day“ erwähnt wird.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Automatisierte Flows**an.
3. Wählen Sie Aus **Zero-Day-Schwachstellennachverfolgung** Link zum Anzeigen der entsprechenden Regeldetails im Flow Designer.
4. Zeigen Sie die Flow Designer-Aktion für den folgenden Auslöser an:

   RSS Feed Created where (Title contains zero day, or Description contains zero day, or Title contains zero_day, or Description contains zero_day, or Title contains zero-day, or Description contains zero-day)

5. **Wenn das erkennbare Element eine IPv4- oder IPv6-Adresse ist und in einen zulässigen CIDR-Bereich fällt, gilt Folgendes:**

   a. Erstellen Sie einen Fall für das TISC-Team zusammen mit einer Korrekturaufgabe für das VR-Team.

   b. Benachrichtigen Sie die betroffenen TISC-Teams und VR-Teams.

Automatisierte Flows-Tabellen

Die folgenden Tabellen helfen Ihnen, die Beziehungstabellen zwischen Entitäten und Ergänzungstabellen zu verstehen, die in automatisierten Flows verwendet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehungstabellen zwischen Entitäten

Tabelle	Entität
Zugehöriges erkennbares Element des Indikators	sn_sec_tisc_m2m_indicator_observable
Zugehöriger Indikator	sn_sec_tisc_m2m_indicator
Zugehöriges erkennbares Element	sn_sec_tisc_m2m_Observable
Objekt-Objekt-Beziehung	sn_sec_tisc_m2m_object
Zugehöriges Indikatorobjekt	sn_sec_tisc_m2m_object_indicator
Beziehung von Objekt und erkennbarem Element	sn_sec_tisc_m2m_object_observable

Ergänzungstabelle

Tabelle	Entität
Bedrohungssuche – Ergebnisse	sn_sec_tisc_Lookup_result
Sichtungen	sn_sec_tisc_Sighting
Ergänzung eines erkennbaren Elements – Ergebnisse	sn_sec_tisc_observable_Enrichment_result

Threat Intelligence-Sicherheitszentrum – Referenz

Referenzthemen enthalten zusätzliche Informationen zum Threat Intelligence-Sicherheitszentrum.

Referenzinformationen	Links zu Themen
Domänentrennung und Threat Intelligence-Sicherheitszentrum	Domain Separation and Threat Intelligence Security Center
Mit installierte Komponenten Threat Intelligence-Sicherheitszentrum Anwendung	Mit Threat Intelligence Security Center installierte Komponenten

Domain Separation and Threat Intelligence Security Center

Domänentrennung wird für Threat Intelligence-Sicherheitszentrum unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Standard

- Enthält alle Aspekte von **Standard** Level-Support.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

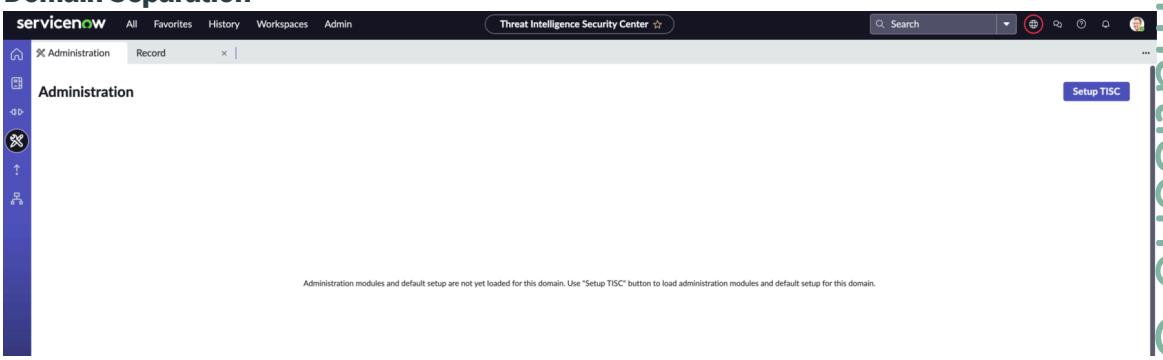
Übersicht

Domänentrennung ist für alle Funktionen von aktiviert Threat Intelligence-Sicherheitszentrum.

So funktioniert Domain Separation in Threat Intelligence-Sicherheitszentrum

- Alle konfigurationsbezogenen Datensätze, die im Basissystem bereitgestellt werden, werden in der globalen Domäne versendet. Wenn die Instanz domänengetrennt ist, sehen Anwender eine explizite Schaltfläche **TISC einrichten** Unter **Verwaltung** Modul des TISC-Arbeitsbereichs. Klicken Sie auf diese Schaltfläche, um die vom Basissystem bereitgestellten globalen Domänenkonfigurationen in die jeweiligen Domänen zu klonen.

Domain Separation



Hinweis:
Anwender sollten nur domänenspezifische Konfigurationsdatensätze aktivieren oder ändern und keine Konfigurationsdatensätze in der globalen Domäne aktivieren oder ändern.

- Im Basissystem sind einige Plattformbenachrichtigungsregeln (sysevent_email_action) bereitgestellt. Diese Benachrichtigungsregeln sollten in erforderliche Domänen geklont werden, und nur domänenspezifische Benachrichtigungsregeln müssen aktiviert werden.

Hinweis:
Weitere Informationen zu den Regelbenachrichtigungen finden Sie unter **Systembenachrichtigung** > **Benachrichtigungen** Und Filter für alle globalen Domänenbenachrichtigungsregeln, die in den Tabellen definiert sind, beginnend mit dem Namen `sn_sec_tisc` Um zu verstehen, wie Anwender die Basisbenachrichtigungsregeln identifizieren können, die im Basissystem bereitgestellt werden.

- Alle erfassten Konfigurationen und Daten sind für jede Domäne spezifisch, was bedeutet, dass Anwender aus einer Domäne nicht auf Daten aus einer anderen Domäne zugreifen können.
- Konfigurieren Sie eine domänengetrennte Umgebung mit dieser Anwendung, indem Sie installieren Domänensupport: Installationsprogramm Für Domänenerweiterungen Plugin.
- Es werden Domänenspalten für alle Tabellen der Basissystemanwendung hinzugefügt.
- Mit der von der Plattform bereitgestellten Funktionalität verwalten die Mandantendomänen ihre eigenen Anwendungsdaten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Geschäftslogik und -Prozesse, die vom Instanzbesitzer domänengetrennt werden können, sind identisch mit den von der Plattform unterstützten Prozessen.
- Die Geschäftslogik und -Prozesse, die von der Mandantendomäne verwaltet werden können, entsprechen der von der Plattform unterstützten.
- Sie können über den Abschnitt Administration auf die Seite Setup zugreifen. Klicken Sie auf den Link, der im Abschnitt Administration bereitgestellt wird, um die Domänentrennungsansicht anzuzeigen.
- Informationen zur Unterstützung der Domänentrennung für Widgets mit Performance Analytics (PA)-Indikatoren im TISC-Startseite-Dashboard finden Sie im KB-artikel KB1647990 Für detailliertes Verfahren.

Domänengetrennte Tabellen

Alle Tabellen sind domänengetrennt.

Anwendungsfälle

Alle Funktionen dieser Anwendung sind domänengetrennt.

Zugehörige Informationen

Domänentrennung für Service Provider

Mit Threat Intelligence Security Center installierte Komponenten

Beim Herunterladen und Aktivieren von werden verschiedene Arten von Komponenten installiert Threat Intelligence-Sicherheitszentrum Anwendung, einschließlich Anwenderrollen und -Eigenschaften.

Installierte Eigenschaften

Erforderliche Rolle: sn_sec_tisc.admin

Benutzer mit der Rolle „Sicherheitsadministrator“ [sn_sec_tisc.admin] können sie ändern.

Eigenschaft	Monatlich
Eigenschaften für Threat Intelligence-Sicherheitszentrum	
Dadurch werden alle Korrelationsregeln deaktiviert. Wenn wir nur ausgewählte Korrelationsregeln deaktivieren müssen, verwenden Sie stattdessen das Feld „aktiv“ in der Korrelationsregel. sn_sec_tisc.disable_correlation_rules	• **Typ**: true | false • **Standardwert**: false
Diese Eigenschaft wird verwendet, um die Verarbeitung von Aggregaten in der Funktion zur Berechnung der Bedrohungsbewertung zu aktivieren/deaktivieren. sn_sec_tisc.aggregates_for_Calculator	• **Typ**: true | false • **Standardwert**: true
Die Anzahl der Zeilen mit Rohdaten, die gespeichert werden, wenn eine Sichtungssuche durchgeführt wird. Bereich 0 Bis 100 sn_sec_tisc.Sighting_search_RAW_Data_rows	• **Typ**: Ganzzahl • **Standardwert**: 50

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Monatlich
Ordnen Sie die Ergebnisse der Sichtungssuche den CIs in der CMDB zu. sn_sec_tisc.Associate_ci_with_Sighting_search	• **Typ**: true | false • **Standardwert**: true
Dadurch wird gesteuert, ob URLs aus Listen entsperrt werden oder nicht sn_sec_tisc.sn_sec_tisc_case.defang_record_list_urls	• **Typ**: true | false • **Standardwert**: false
Diese Eigenschaft ermöglicht es, dass für die MITRE-Techniken automatisch ein Rollup zu Fällen aus den zugeordneten Objekten oder Security Incidents durchgeführt wird. sn_sec_tisc.auto_rollup_mitre_data	• **Typ**: true | false • **Standardwert**: true
Bei „true“ werden alle Taktiken (einschließlich der Taktiken, denen keine Techniken mit dem Fall zugeordnet sind) für die im Bericht gerenderten MITRE-Listen angezeigt. sn_sec_tisc.Show_all_tactics_Reporting	• **Typ**: true | false • **Standardwert**: true
Sys-ID der E-Mail-Client-Vorlage für die Falltabelle (sn_sec_tisc_case), die in der Berichtfreigabe verwendet wird. sn_sec_tisc.Reporting_email_template_sn_sec_tisc_Case	• **Typ**: Zeichenfolge • **Standardwert** : B55e22c54324021060eee0ea78b8f2df
Die Standard-TLP-Ebene wird beim Erstellen eines neuen Datensatzes angewendet. Wenn im Formular nicht manuell festgelegt, wird dieser Wert verwendet. sn_sec_tisc.tlp_default_value	• **Typ**: Auswahlliste • **Standardwert** : 955c9e5543d35110baf06e434ab8f2cb
Protokollierungsebene – Debug, Info, Warnung, Fehler sn_sec_tisc.Logging.verbosity	• **Typ**: Auswahlliste • **Standardwert**: Info
Eigenschaften für Threat Intelligence-Feeds	
Maximale Zeit in Sekunden, die eine ausgehende HTTP-Verbindung wartet, um TAXII-Sammlungsdaten abzurufen sn_sec_tisc.Taxii.http.max_timeout	• **Typ**: Ganzzahl • **Standardwert**: 300
Maximale Anzahl von Objekten, die in einem REST-Aufruf von einem TAXII-Server abgerufen werden (gilt nur für TAXII-Versionen 2.0 und 2.1) sn_sec_tisc.Taxii.max_page_size	• **Typ**: Ganzzahl • **Standardwert**: 5.000
Maximale Anzahl von Wiederholungen für einen fehlgeschlagenen TAXII2. X-REST-Aufruf sn_sec_tisc.taxii2.retry_count	• **Typ**: Ganzzahl • **Standardwert**: 3

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Monatlich
Maximale Anzahl von Objekten, die in einem REST-Aufruf vom Cyware TAXII-Server abgerufen werden sn_sec_tisc.Cyware_Taxii.max_page_size	• **Typ**: Ganzzahl • **Standardwert**: 1.000 **Hinweis:** Gibt die Seitengröße an, die beim Abrufen von Daten aus TAXII-Sammlungen im Zusammenhang mit dem Cyware-TAXII-Feed verwendet wird. Für alle anderen TAXII-Sammlungen wird die aus der TAXII-Sammlung abgerufene Seitengröße standardmäßig auf den Wert festgelegt, der in der entsprechenden Eigenschaft definiert ist: sn_sec_tisc.Taxii.max_page_size .
Anzahl der Datensätze, die gleichzeitig von CrowdStrike abgerufen werden sollen. Je höher die Zahl, desto mehr Arbeitsspeicher würde für die Verarbeitung der Nutzlast verbraucht. sn_sec_tisc.crowdstrike_api_limit	• **Typ**: Ganzzahl • **Standardwert**: 1.000
Gibt die Anzahl der Indikatoren an, die in einem einzelnen API-Aufruf abgerufen werden sollen. **Hinweis:** Dies gilt nur, wenn die Integration die erforderlichen nicht im System findet. sn_sec_tisc.crowdstrike_indicator_Batch_size	• **Typ**: Ganzzahl • **Standardwert**: 1.000
Gibt die Anzahl der Akteure an, die in einem einzelnen API-Aufruf abgerufen werden sollen. **Hinweis:** Dies gilt nur, wenn die Integration die erforderlichen nicht im System findet. sn_sec_tisc.crowdstrike_actor_Batch_size	• **Typ**: Ganzzahl • **Standardwert**: 1.000
Gibt die Anzahl der Berichte an, die in einem einzelnen API-Aufruf abgerufen werden sollen. **Hinweis:** Dies gilt nur, wenn die Integration die erforderlichen nicht im System findet. sn_sec_tisc.crowdstrike_Report_Batch_size	• **Typ**: Ganzzahl • **Standardwert**: 50

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Monatlich
Die zulässige Summe aus Offset und Grenzwert aus der CrowdStrike-API. sn_sec_tisc.crowdstrike_Offset_limit_total	• **Typ**: Ganzzahl • **Standardwert** : 50000
Eigenschaften für REST APIs	
Definiert die maximale Seitengröße (maximale Anzahl von erkennbaren Elementen, die als Teil der Antwort zurückgegeben werden) für die API zum Abrufen erkennbarer Elemente. Es wird nicht empfohlen, den Wert auf einen hohen Wert zu erhöhen, da dies sich auf die API-Antwortzeit auswirken kann. sn_sec_tisc.api_Maximum_page_size_limit	• **Typ**: Ganzzahl • **Standardwert**: 1.000
Definiert die maximale Anzahl von erkennbaren Elementen, die im Anforderungstext für die API zum Hinzufügen erkennbarer Elemente gesendet werden können. Es wird nicht empfohlen, den Wert auf einen hohen Wert zu erhöhen, da dies sich auf die API-Antwortzeit auswirken kann. sn_sec_tisc.add_obs_api_max_Records	• **Typ**: Ganzzahl • **Standardwert**: 100
Eigenschaften für Webhooks	
Maximale Anzahl von Ereignissen, die als Teil einer Webhook-Anforderung gesendet werden sollen. Die Batchgröße ist auf 2000 beschränkt, auch wenn in dieser Eigenschaft ein höherer Wert festgelegt ist. sn_sec_tisc.Webhook_max_event_Batch_size	• **Typ**: Ganzzahl • **Standardwert**: 100
Gibt an, wie oft eine fehlgeschlagene Anforderung wiederholt werden soll, bevor sie als Fehler markiert und mit dem nächsten Ereignisbatch fortgefahren wird. Die Anzahl der Wiederholungen ist auf 10 beschränkt, auch wenn in dieser Eigenschaft eine höhere Zahl festgelegt ist. sn_sec_tisc.Webhook_retry_count	• **Typ**: Ganzzahl • **Standardwert**: 100
Anzahl der Sekunden, die gewartet werden soll, bevor ein fehlgeschlagener Batch erneut versucht wird. Dies erhöht sich exponentiell basierend auf der Anzahl der Wiederholungen. Beispiel: Wenn „retry_count“ 3 und „retry_interval“ 30 ist, werden Wiederholungen nach 30, 60 und 120 Sekunden ausgelöst Das anfängliche Wiederholungsintervall ist auf 300 Sekunden beschränkt, auch wenn in dieser Eigenschaft ein höherer Wert festgelegt ist. sn_sec_tisc.Webhook_retry_interval	• **Typ**: Ganzzahl • **Standardwert**: 30
Durch erneute Anwendung der Bedrohungsbewertung ausgelöste Webhook-Ereignisse ignorieren sn_sec_tisc.Webhook_ignore_Threat_Score_reapply	• **Typ**: true | false • **Standardwert**: true
Eigenschaften für Untersuchungs-Canvas	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Monatlich
Wenn Sie den Wert auf „true“ festlegen, werden neue Knoten in der linken oberen Ecke hinzugefügt. Bei „false“ fügt sie der Mitte des Canvas hinzu. sn_sec_tisc.canvas_suspend_reLayout	• **Typ**: true | false • **Standardwert**: true
Eigenschaften für Export in CTI-Formaten	
Maximale Anzahl der Zeilen, die in eine STIX 2.1-Datei exportiert werden können. sn_sec_tisc.stix_Export_limit	• **Typ**: Ganzzahl • **Standardwert**: 10.000
Schließen Sie Felder vom Typ „Journal“ in die Exportdatei ein. sn_sec_tisc.Export_Journal_fields	• **Typ**: true | false • **Standardwert**: true

Geplante Aufgaben

In der folgenden Tabelle werden die geplanten Aufgaben beschrieben:

Auftrag	Beschreibung
Datensätze Der Aggregatindikatorquelle	Fasst Indikatorquelldatensätze zusammen.
Aggregatobjektquelldatensätze	Fasst Objektquelldatensätze zusammen.
Fassen Sie Quelldatensätze Erkennbarer Elemente Zusammen	Fasst Quelldatensätze erkennbarer Elemente zusammen.
Bereinigung veralteter Importe	Bereinigt veraltete Importauftragsdatensätze.
Bereinigung nicht verwendeter neuer Knoten von Canvas	Bereinigt nicht verwendete neue Knoten von Canvas.
Bereinigen Sie Datensätze Für Sicheren Dateidownload	Bereinigt sichere Dateidownload-Datensätze.
Deduplizieren Sie Indikatorquelldatensätze	Dedupliziert Indikatorquelldatensätze.
Deduplizieren Sie Objektquelldatensätze	Dedupliziert Objektquelldatensätze.
Deduplizieren Sie Quelldatensätze erkennbarer Elemente	Dedupliziert Quelldatensätze erkennbarer Elemente.
Deaktivieren Sie Abgelaufene Indikatoren	Deaktiviert abgelaufene Indikatordatensätze.
Deaktivieren Sie Abgelaufene Objekte	Deaktiviert abgelaufene Objektdatensätze.
Deaktivieren Sie Abgelaufene Erkennbare Elemente	Deaktiviert abgelaufene Datensätze erkennbarer Elemente
Migrieren Sie Daten von TI zu TISC	Verarbeitet ausstehende Datensätze zur Ausführung des Migrationsauftrags
Füllen Sie zusammengefasste Datensätze für Indikatorquelldatensätze aus	Gibt den übergeordneten zusammengefassten Datensatz für neu erstellte Indikatorquelldatensätze an
Füllen Sie zusammengefasste Datensätze für Objektquelldatensätze aus	Gibt den übergeordneten zusammengefassten Datensatz für neu erstellte Objektquelldatensätze an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auftrag	Beschreibung
Füllen Sie zusammengefasste Datensätze für Quelldatensätze erkennbarer Elemente aus	Gibt den übergeordneten zusammengefassten Datensatz für neu erstellte Quelldatensätze erkennbarer Elemente an.
Füllen Sie die TISC-Referenz in TI aus	Füllt die Referenz des aggregierten erkennbaren TISC-Elements im Datensatz des erkennbaren TI-Elements aus.
Genehmigte Importe Verarbeiten	Verarbeitet genehmigte Importaufträge.
Verarbeitet importierte MISP DSM-Warteschlangendatensätze	Datensätze der bereitgestellten MISP-Feed-Erfassungswarteschlange verarbeitet.
Importierte MISP-Indikatorimport-Warteschlangendatensätze verarbeiten	Verarbeitet bereitgestellte MISP-Daten, die aus Import Intelligence erfasst wurden
Verarbeitet importierte STIX-Importwarteschlangendatensätze	Verarbeitet bereitgestellte STIX-Daten, die aus Import Intelligence erfasst wurden
Importierte STIX-Importwarteschlangendatensätze verarbeiten – Erfassung	Verarbeitet bereitgestellte STIX-Daten, die aus Bedrohungs-Feeds erfasst wurden.
Verarbeiten Sie Die Migration Ausstehender Fallartefakte	Migriert Fallartefakte aus der Threat Intelligence-Anwendung zum Threat Intelligence-Sicherheitszentrum.
Verarbeiten Sie Datensätze der Warteschlange für ausstehende Bedrohungsquellen	Verarbeitet Datensätze der ausstehenden Quellerfassungswarteschlange.
Verarbeiten Sie Entitäten In Der Warteschlange Für Den Rechner Der Bedrohungsbewertung	Verarbeitet ausstehende Bedrohungsrechner-Warteschlangeneinträge
Verarbeiten Sie MISP DSM-Warteschlangendatensätze in der Warteschlange	Verarbeitet MISP-Daten in der Warteschlange, die aus dem Bedrohungs-Feed erfasst wurden
Importwarteschlangendatensätze für MISP-Indikator in Warteschlange verarbeiten	Verarbeitet MISP-Daten in der Warteschlange, die aus Import Intelligence erfasst wurden
STEX-Importwarteschlangendatensätze in Warteschlange verarbeiten – Erfassung	Verarbeitet STIX-Daten in Warteschlange, die aus Bedrohungs-Feeds erfasst wurden.
Importwarteschlangendatensätze des STEX-Indikators in der Warteschlange verarbeiten	Verarbeitet STIX-Daten in Warteschlange, die aus Import Intelligence erfasst wurden
Webhook-Warteschlange Verarbeiten	Verarbeitet ausstehende Webhook-Warteschlangendatensätze.
Fassen Sie Quelldatensätze Erneut Zusammen	Fasst Quelldatensätze neu zusammen, für die zusammengefasste Datensätze gelöscht werden.
Entfernen Sie den gefilterten Quelldatensatz	Bereinigt gefilterte Quelldatensätze
CrowdStrike-Integration – Prozessüberprüfung fortsetzen/CrowdStrike-Quelldatensätze erneut verarbeiten	Setzt die CrowdStrike-Feed-Integrationsausführungen fort, die auf Quotenlimit-/Reporussquelldatensätze für die Zusammenfassung von Beziehungen warten
Anzahl Der Falsch Positiven Erkennbaren Elemente Synchronisieren	Synchronisiert die Anzahl der falsch positiven erkennbaren Elemente mit der Anzahl der Flase-positiven Elemente pro Quelle
TISC – Webhook-Batches erstellen	Batches für Webhook-Warteschlangeneinträge in der Warteschlange zur Verarbeitung erstellt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auftrag	Beschreibung
TISC löst Webhooks aus	Führt ausstehende Webhook-Batches aus
Archivierte Beziehungsspalte Wird Aktualisiert	Aktualisiert den Archivstatus der Beziehungsquellen- und Zieldatensätze

Threat Intelligence-Sicherheitszentrum verwenden

Verwenden Threat Intelligence-Sicherheitszentrum Um Datensätze der Threat Intelligence-Bibliothek zu verwalten, importieren Sie externe Bedrohungsdaten, und optimieren Sie die Fallverwaltung. Es hilft Sicherheitsteams, Intelligence-Daten zu zentralisieren, die Analyse zu verbessern und effektiver auf Bedrohungen zu reagieren, indem die relevanten Informationen in laufende Untersuchungen integriert werden.

TISC-Integration mit SIR Workspace

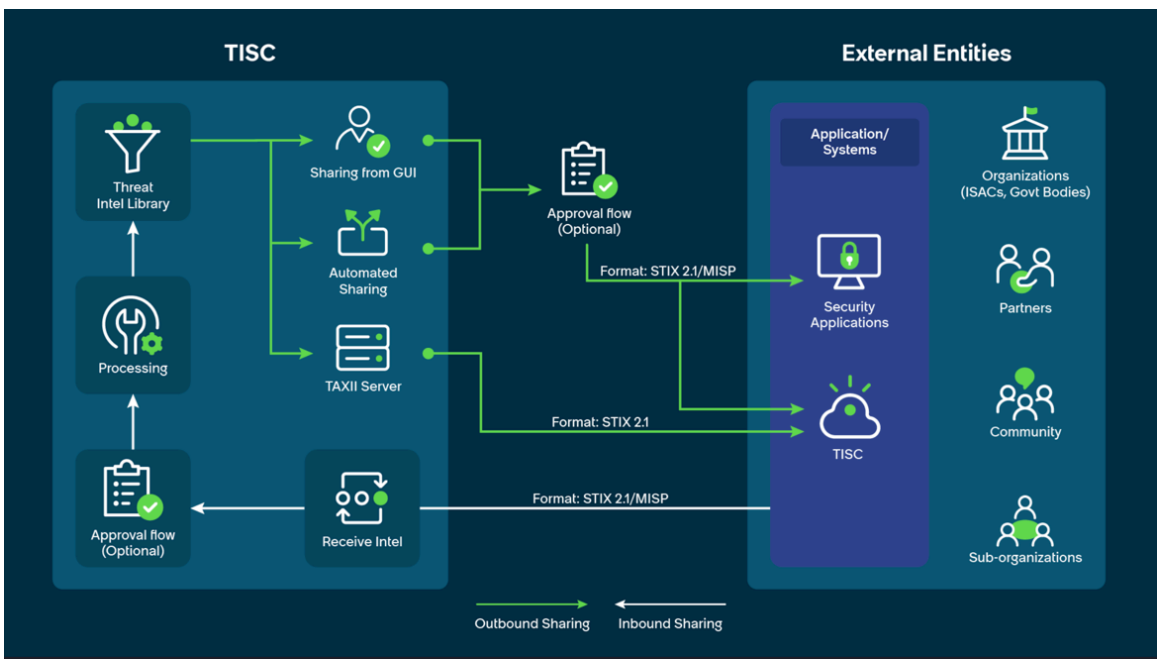
Durch die TISC-Integration mit SIR wird der Kontext automatisch an die erkennbaren Elemente im Security Incident-Arbeitsbereich für die Sicherheitsanalysten angehängt. Alle neuen erkennbaren Elemente von SIR können zur weiteren Analyse durch das CTI-Team mithilfe der UI-Aktionen auf den Bildschirmen an TISC gesendet werden.

Darüber hinaus können alle Ergänzungsergebnisse, die aus Integrationen erstellt werden, die nur in SIR verfügbar sind, auch mithilfe der im Arbeitsbereich bereitgestellten UI-Aktionen bereitgestellt werden.

Konfigurieren Sie Die Externe Freigabe Von Threat Intelligence

Externe Freigabe von Threat Intelligence in TISC Beschreibt die Richtlinien und Funktionalitäten für die Automatisierung und Freigabe von Threat Intelligence in und über die GUI hinweg. Diese Funktion konzentriert sich auf Schlüsselbereiche wie Freigabeausschlussregeln, Genehmigungen, Datenaufbewahrung und Auditing, um die sichere, konforme und effiziente Freigabe von Intelligenzen zu bestätigen.

Externe Freigabe von Threat Intelligence mit Threat Intelligence Security Center (TISC)



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtige Funktionen der externen Freigabe von Threat Intelligence für TISC

- **Vorlagen Werden Freigegeben** : Vorlagen ermöglichen die Kontrolle darüber, welche Entitäten und Felder in Shared Intelligence enthalten sind, wodurch sichergestellt wird, dass nur relevante Daten verbreitet werden.
- **Genehmigungsregeln für die Freigabe** : Administratoren können Genehmigungsregeln für ausgehende und eingehende Intelligenz konfigurieren, um eine robuste Verwaltung von Genehmigungs-Workflows zu ermöglichen.
- **Schwärzungsfähigkeiten** : Analysten haben die Möglichkeit, vertrauliche Informationen aus gemeinsam genutzter Intelligenz zu schwärzen, mit einfachen Optionen zum Aktivieren oder Deaktivieren der Schwärzung.
- **Audit-Fähigkeiten** : Jede Aktion zur Freigabe von Intelligenzen wird auditiert. Dabei werden Details erfasst, einschließlich Absender, Empfänger, Zeitstempel und freigegebener Inhalte, um vollständige Compliance und Nachverfolgbarkeit sicherzustellen.
- **Datenaufbewahrungsrichtlinien** : Gemeinsam genutzte Intelligenz und zugehörige Audit-Protokolle werden gemäß Compliance-Anforderungen mit definierten Regeln für die Archivierung und Vernichtung verschiedener Datensatztypen aufbewahrt.
- **TISC zu TISC Exchange** : Mechanismen für einen effizienten, bidirektionalen Austausch von Intelligenzen zwischen Threat Intelligence-Sicherheitszentrum(TISC) Instanzen.
- **Anwender- und Gruppenverwaltung für TAXII** : Definiert TAXII-Anwender und -Gruppen, indem ihr Zugriff auf Sammlungen verwaltet und sichere Datenaustauschprotokolle verwaltet werden.

Erkunden Sie Die Ausgehende Intel-Freigabe

Mit der Intelligenz für ausgehende Freigabe können Sie definieren und freigeben, welche Threat Intelligence-Entitäten und -Attribute, Ausschlussregeln, Profile und Gruppen sowie Genehmigungsregeln extern und intern freigegeben werden können.

Konfigurieren Von Steuerungen Für Die Freigabe Ausgehender Intel

Verwenden Sie diesen Abschnitt, um Steuerungen für die ausgehende Freigabe zu konfigurieren, die die Entitäten bestimmen, die für die Freigabe von Intelligenzen von aktiviert sind TISC An externe Systeme.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Ausgehende Intel-Freigabe**an.
2. Wählen Sie Aus **Steuerungen Für Ausgehende Intel-Freigabe** .
   Ausgehende Intel-Freigabesteuerungen sind die standardmäßige Freigabesteuerung, die im Basissystem bereitgestellt wird. Standardmäßig ist diese Steuerung auf festgelegt **Veröffentlicht** status.

Hinweis:

- Dies sind die allgemeinen Freigabesteuerungen, die später in Vorlagen für die gemeinsame Nutzung von Intelligenzen verwendet werden können.
- Jede Aktion, die für die ausgehenden Freigabesteuerungen ausgeführt wird, wird aufgezeichnet, und eine Arbeitsnotiz wird im Aktivitätenstrom für jede Entität veröffentlicht, die erstellt, geändert oder gelöscht wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Freigabesteuerungen Werden Bearbeitet:

3. Wählen Sie Aus **Bearbeiten** Dient zum Ändern der Pflichtfelder, wenn Sie den Standarddatensatz für die Freigabesteuerung ändern möchten.

   Wenn Sie den Datensatz der Freigabesteuerung bearbeiten, wird eine Validierungsnachricht angezeigt, die Sie angibt, alle Vorlagen zu deaktivieren und zu bestätigen, dass keine ausgehenden Datensätze zur Freigabe von Intelligenzen vorhanden sind, bevor Sie fortfahren.

   Wenn die obigen Validierungen erfolgreich sind, wird eine weitere Warnmeldung angezeigt, die darauf hinweist, dass Automatisierungs-Flows basierend auf diesen Einstellungen fehlschlagen können, wenn Sie fortfahren, ohne sie zuerst zu deaktivieren.

   > ⚠ **Warnung:**
   > Das Bearbeiten dieser Einstellungen, ohne die zugehörigen Automatisierungs-Flows zuerst zu deaktivieren, kann zu Fehlern führen. Möchten Sie fortfahren?

   Wenn Sie dieses Risiko bestätigen und fortfahren möchten, können Sie die Freigabesteuerung ändern.

Verwalten Von Freigabesteuerungen Auf Entitätsebene:

4. Wechseln Sie zu **Freigabesteuerungen** Abschnitt zum Anzeigen aller für die Entitäten verfügbaren Freigabesteuerungen.
   Standardmäßig sind alle Entitäten der Threat Intelligence-Bibliothek in der Anwendung enthalten, einschließlich der erkennbaren Elemente, des Indikators und der Objekte.
5. Wählen Sie eine beliebige Entität aus, um die erforderlichen und optionalen Attribute anzuzeigen.
   Die **Bearbeiten Sie Entität und Attribute** Dialogfeld wird angezeigt.

Hinzufügen oder Entfernen von Entitäten:

6. Wählen Sie Aus **Entfernen Sie Die Entität** Wenn Sie eine Entität entfernen möchten.
   Diese Aktion **Entfernen Sie Die Entität** Entfernt die Entität und schließt sie automatisch von der Freigabe ausgehender Informationen aus. Nach dem Entfernen kann die Entität nicht für die Freigabe in verwendet werden TISC Und das Entfernen entfernt die Entität automatisch aus allen Vorlagen, die diese Entität als Teil der Freigabesteuerungen haben.

   Wählen Sie außerdem aus **Entfernen Sie alle Attribute** (Papierkorbsymbol unten im Dialogfeld verfügbar), um alle optionalen Attribute zu entfernen. Das Entfernen eines dieser Attribute wirkt sich direkt auf die entsprechenden Vorlagen für die gemeinsame Nutzung von Intelligenzen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn Vorlagen für ausgehende Freigaben vorhanden sind, die die ausgewählte Entität enthalten, wird eine Warnmeldung auf angezeigt **Bearbeiten Sie Entität und Attribute** Dialogfeld, das angibt, dass das Entfernen der ausgewählten Entität oder eines ihrer Attribute sie automatisch von der {#total number of Templates} ausgehenden Vorlagen für die gemeinsame Nutzung von Informationen ausschließt, in denen sie derzeit enthalten sind. Die betroffenen Vorlagen werden im aufgeführt **Bearbeiten Sie Entität und Attribute** Dialogfeld selbst.
- Eine Liste betroffener Vorlagen, z. B. IOC-Freigabevorlage, wird zur Überprüfung angezeigt.
- Wenn bestimmte Entitäten nicht für externe Systeme freigegeben werden sollen, können Sie sie aus den Freigabesteuerungen entfernen.
- Nur die innerhalb der Freigabesteuerungen konfigurierten Entitäten können beim Erstellen oder Ändern von Vorlagen für ausgehende intelligente Freigabe ausgewählt werden.

7. Wählen Sie Aus **Fügen Sie alle optionalen Attribute hinzu** Um alle optionalen Attribute der ausgewählten Entität in die ausgehende Intelligence-Freigabe einzubeziehen.
8. Nachdem Sie die erforderlichen Änderungen an den Freigabesteuerungen vorgenommen haben, wählen Sie aus **Veröffentlichen** Um die Freigabesteuerungen zu veröffentlichen.
   Sobald die Freigabesteuerungen veröffentlicht wurden, können sie in Vorlagen für ausgehende Freigabe von Intelligenz verwendet werden. Weitere Informationen finden Sie unter Konfigurieren Von Vorlagen Für Ausgehende Intel-Freigabe.

Nächste Maßnahme

In den folgenden Abschnitten finden Sie Anleitungen zur Freigabe externer Intelligenz mit der GUI und automatisierten Verfahren.

- Freigabe ausgehender Intelligence-Datensätze aus der GUI
- Automatisierte Freigabe von IOC mit hohem Risiko für vertrauenswürdige PartnerKonfigurieren Von Vorlagen Für Ausgehende Intel-Freigabe

Konfigurieren Der Ausschlussregel Für Ausgehende Intel-Daten

Verwenden Sie diesen Abschnitt, um Ausschlussregeln zu erstellen, die von konfiguriert werden können TISC administrator, um die Freigabe von Datensätzen einzuschränken, die den definierten Kriterien entsprechen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können bestimmte Entitäten freigeben, während Sie bestimmte Datensätze innerhalb dieser Entitäten ausschließen. Sie können bestimmte Entitätstypen freigeben, während Sie bestimmte Datensätze basierend auf ihrer Vertraulichkeit ausschließen. Beispielsweise möchten Sie Domänennamen freigeben, aber solche mit einer TLP-Bewertung (Traffic Light Protocol) ausschließen, die die Freigabe einschränkt. Dieser Ansatz trägt dazu bei, zu verhindern, dass vertrauliche Domänennamen innerhalb der Organisation oder für externe Organisationen freigegeben werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Ausgehende Intel-Freigabe**an.
2. Wählen Sie Aus **Ausgehende Intel-Datenausschlussregeln** .
   Die **Datenausschlussregel** Ist die standardmäßige Ausschlussregel für ausgehende Intel-Daten für die ausgehende Freigabe, die im Basissystem bereitgestellt wird.

Ausgehende Intel-Datenausschlussregeln Bearbeiten:

3. Wählen Sie Aus **Bearbeiten** Schaltfläche zum Ändern der Ausschlussregeln, die für jede Tabelle unter definiert sind **Ausschlussregeln** Registerkarte.
   Eine Warnmeldung wird angezeigt, die darauf hinweist, dass Automatisierungs-Flows basierend auf diesen Einstellungen fehlschlagen können, wenn Sie fortfahren, ohne sie zuerst zu deaktivieren.

   Wenn Sie dieses Risiko bestätigen und fortfahren möchten, können Sie die Ausschlussregeln ändern, indem Sie auswählen **Bearbeiten** Schaltfläche.

Ausschlussregeln Für Ausgehende Intel-Daten Ändern:

4. Wechseln Sie zu **Ausschlussregeln** Abschnitt.
   Die **Ausschlussregeln** Listen zeigen alle Regeln an, die im Basissystem bereitgestellt werden.
   Die Liste enthält die Details jeder Ausschlussregel, einschließlich Entität, Entitätstyp und spezifische Ausschlussbedingungen.

   Wenn die Bedingungen erfüllt sind, werden die Datensätze, die diese angegebenen Kriterien erfüllen, nicht freigegeben.

5. Wählen Sie eine beliebige Ausschlussregel aus, die Sie ändern oder zusätzliche Bedingungen hinzufügen möchten, und **Speichern** Die Regel.
6. Nachdem Sie die erforderlichen Änderungen an der globalen Datenausschlussregel vorgenommen haben, wählen Sie aus **Veröffentlichen** Schaltfläche zum Anwenden der aktualisierten Ausschlussregel.

   Jede Aktion, die für die Ausschlussregeln ausgeführt wird, wird aufgezeichnet, und im Aktivitätenstrom wird eine Arbeitsnotiz mit den vorherigen und aktuellen Werten für jede Bedingung veröffentlicht.

Hinweis:

- Das Aktivieren von Vorlagen oder die Freigabe über die GUI ist nicht zulässig, solange sich die Ausschlussregel für ausgehende Intelligence-Daten im Bearbeitungsmodus befindet.
- Die automatisierte Freigabe und das automatische Hinzufügen von Datensätzen zu TAXII-Sammlungen schlägt ebenfalls fehl, während die Ausschlussregel im Bearbeitungsmodus verbleibt.

Konfigurieren Von Ausgehenden Intel-Freigabeprofilen

Verwenden Sie diesen Abschnitt, um neue Profile für ausgehende Intelligenz zu erstellen. Die Profile für ausgehende Intelligenz geben die Endpunktdetails an, an die Threat Intelligence-Daten gesendet werden.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Ausgehende Intel-Freigabe**an.
2. Wählen Sie Aus **Ausgehende Intel-Freigabeprofile** .
3. Wählen Sie Aus **Neu** Dient zum Erstellen eines Profils für ausgehende Intelligenz.
4. Füllen Sie im Formular die Felder aus.

Erstellen Sie Ein Neues Profil Für Ausgehende Intelligenz

Feld	Beschreibung
Name	Name des Profils für ausgehende Intelligenz.
Branche	Wählen Sie die Branchenkategorie aus, z. B. Luft- und Raumfahrt, für die das Profil der ausgehenden Intelligenz gilt.
Beschreibung	Beschreibung des Profils für ausgehende Intelligenz.
Einstellungen Für Ausgehende Intelligenz	
Datenformat	Unterstützte Datenformate für das Freigabeprofil für ausgehende Intelligenz. Derzeit werden die folgenden zwei Datenformate für die Freigabe ausgehender Intelligenz unterstützt: ○ **STIX 2,1** : Unterstützt verschiedene Endpunkttypen, einschließlich Endpunkte der Standardauthentifizierung und Open Source-Endpunkte. Um dies zu berücksichtigen, sind für STIX 2,1 zwei Authentifizierungstypen verfügbar. ○ **MISP** : Für MISP wird die Authentifizierung ausschließlich über einen API-Schlüssel verarbeitet. ▪ Wenn MISP als Format ausgewählt ist, wird die Option Authentifizierung erforderlich automatisch aktiviert. ▪ Der Authentifizierungstyp ist als API-Schlüssel festgelegt, und Anwender müssen einen gültigen API-Schlüssel angeben, um eine Verbindung zur MISP-Instanz herzustellen.
API-Endpunkt-URL	Geben Sie die API-Endpunkt-URL ein, an die die Daten gesendet werden müssen.
Authentifizierung erforderlich	Aktivieren Sie dieses Kontrollkästchen, wenn die Authentifizierung erforderlich ist.
Authentifizierungstyp	Wählen Sie die erforderliche Option aus der Dropdown-Liste aus, wenn die Authentifizierung erforderlich ist. Die verfügbare Option ist:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Standard : Wählen Sie diese Option aus, um Anwendername und Passwort anzugeben.
Header, die mit der Anforderung übergeben werden sollen	Alle Header, die mit den Anforderungen übergeben werden sollen, können für das Profil der ausgehenden Intelligenz angegeben werden. Header muss als Schlüssel-Wert-Paar angegeben werden, das durch einen Doppelpunkt („:“) getrennt ist. Jedes Header-Schlüssel-Wert-Paar muss in einer neuen Zeile angegeben werden. Um Authentifizierungsparameter als Headerwerte bereitzustellen, schließen Sie die erforderliche Authentifizierung mit „${“ und „}$“ ein. (Beispiel: Username: ${Username}$)

5. Sobald die Profil- und Authentifizierungsdetails angegeben sind, klicken Sie auf **Speichern** .
6. Wählen Sie Aus **Validieren Sie Die Verbindung** Dient zum Bestätigen des Setups durch Testen der Endpunkt-URL, die unter „ausgehende Freigabe von Intelligence“ konfiguriert ist.

   Mit dieser Option können Sie einen Anforderungstext angeben, um den im Profilabschnitt definierten spezifischen Endpunkt zu validieren.

   Hinweis:
   Ein Beispielanforderungstext wird basierend auf dem ausgewählten Format angezeigt, und Sie können ihn nach Bedarf ändern.

   Nehmen Sie die erforderlichen Änderungen am Anforderungstext vor, und klicken Sie auf **Speichern und validieren** Schaltfläche. Wenn Sie auf den ursprünglichen Beispielanforderungstext zurücksetzen möchten, können Sie auswählen **Zurücksetzen** Schaltfläche zum Zurücksetzen auf den ursprünglichen Anforderungstext.

   Eine Bestätigungsnachricht wird angezeigt, die angibt, dass die Verbindung zum Endpunkt erfolgreich ist.

   Wenn die Verbindung zum Endpunkt nicht erfolgreich ist, überprüfen Sie die Fehlerprotokolle, und beheben Sie alle Probleme, bevor Sie es erneut versuchen.
7. Wählen Sie aus **Aktivieren** Schaltfläche zum Aktivieren des Freigabeprofils für ausgehende Intelligenz.

   Hinweis:
   Wenn Sie auswählen **Aktivieren** Schaltfläche, dann erfolgt die Validierung bis zum Endpunkt automatisch.

   Wenn Sie ein Freigabeprofil erstellen, **Aktivieren** Die Schaltfläche wird nur angezeigt, wenn die Verbindung erfolgreich validiert wurde. Andernfalls ist diese Schaltfläche erst sichtbar, wenn die Verbindung zum Endpunkt erfolgreich ist.
   Eine Bestätigungsnachricht wird angezeigt, die angibt, dass das Freigabeprofil erfolgreich aktiviert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie müssen das Freigabeprofil aktivieren, um es für die Freigabe von Informationen zu verwenden.

8. Wählen Sie außerdem aus **Deaktivieren** Zum Deaktivieren des Profils, wenn es nicht für die Freigabe von Informationen benötigt wird.

Konfigurieren Ausgehender Intel-Freigabegruppen

Mit ausgehenden Intel-Freigabegruppen können Sie mehrere Profile kombinieren und sie beim Freigeben von Daten gemeinsam verwenden.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Ausgehende Intel-Freigabe**an.
2. Wählen Sie Aus **Ausgehende Intel-Freigabegruppen** .
3. Wählen Sie Aus **Neu** Dient zum Erstellen einer ausgehenden Intelligence-Freigabegruppen.
4. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Name	Name der ausgehenden Intel-Freigabegruppe.
Beschreibung	Beschreibung der ausgehenden Intel-Freigabegruppe.
Typ	Gibt an, ob die Gruppe zu einer internen oder externen Organisation gehört.

5. Klicken Sie Auf **Speichern** Zum Speichern der intel-Freigabegruppe.

Hinzufügen Von Gruppenmitgliedern:

In diesem Abschnitt können Sie mehrere Profile an eine Gruppe anhängen.

6. Navigieren Sie zu **Gruppenmitglieder** Abschnitt.
7. Klicken Sie auf **Hinzufügen**.
   Das Dialogfeld Outbound Intelligence-Profile hinzufügen wird angezeigt. Listet alle aktivierten Profile für die Freigabe ausgehender Informationen auf.
8. Wählen Sie mindestens ein Profil aus.
9. Klicken Sie auf **Hinzufügen**.
10. Klicken Sie außerdem auf **Entfernen** Zum Entfernen der Profile aus der Gruppe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie die erforderlichen Änderungen an der Gruppe vorgenommen haben, können Sie aktivieren, um sie bei der Freigabe von Intelligenzen aktiv und nutzbar zu machen. Andernfalls können Sie sie deaktivieren, wenn sie nicht mehr verwendet werden soll.

Hinweis:
Eine Informationsnachricht wird angezeigt, die angibt, dass die ausgewählten ausgehenden Intelligenzprofile dieser Gruppe hinzugefügt oder entfernt wurden. Diese Nachricht wird in Bezug auf die von Ihnen ausgewählte Aktion „Hinzufügen“ oder „Entfernen“ angezeigt.

Definieren der Genehmigungsregel für ausgehende Intel

Definieren Sie Genehmigungsregeln, um zu steuern, ob bestimmte Anwender eine Genehmigung benötigen, bevor sie die gemeinsam genutzte Intelligenz freigeben.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Sie können Genehmigungsregeln für den Datensatz „ausgehende Intel“ konfigurieren. Diese Regeln bestimmen, ob eine Freigabe basierend auf den Anwenderrollen oder anderen Kriterien genehmigt werden muss.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Verwaltung** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Ausgehende Intel-Freigabe** .
4. Wählen Sie Aus **Genehmigungsregel für ausgehende Intel** .

   Hinweis:
   Innerhalb des Basissystems die **Genehmigungsregel für ausgehende Intelligenz** Ist die im Basissystem bereitgestellte Standardregel, um den Genehmigungs-Workflow zu aktivieren.

   Die Genehmigungsregel gilt nur für die Freigabe ausgehender Intelligenz bei Bedarf. Weitere Informationen zu Outbound Intelligence bei Bedarf finden Sie unter . Konfigurieren Von Vorlagen Für Ausgehende Intel-Freigabe.

5. Geben Sie im Formular „Genehmigungsregel“ in jedem der folgenden Abschnitte mindestens einen Anwender oder eine Anwendergruppe ein:
   a. **Anwender oder Gruppen mit erforderlicher Genehmigung auswählen**
   b. **Den/die Genehmiger auswählen**
6. Klicken Sie auf **Aktivieren** Schaltfläche zum Aktivieren des Genehmigungs-Flows für eingehende Intel.

Hinweis:

- Nach der Aktivierung wird jeder zutreffende ausgehende Intel-Datensatz an die Genehmigungswarteschlange weitergeleitet.
- Die zugewiesenen Genehmiger überprüfen die vom Analysten vorgenommenen Änderungen und entscheiden sich, die Anforderung zu genehmigen oder abzulehnen.
- Nachdem eine Entscheidung getroffen wurde, wird eine E-Mail-Benachrichtigung an die Anwender oder Anwendergruppen gesendet, die angibt, ob der Datensatz genehmigt oder abgelehnt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Von Vorlagen Für Ausgehende Intel-Freigabe

Mit Vorlagen für ausgehende Intel-Freigabe können Sie die extern von freigegebenen Daten definieren und steuern Threat Intelligence-Sicherheitszentrum(TISC).

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird

Der primäre Zweck der Freigabevorlagen besteht darin, die Details des Freigabedatensatzes wie den Namen des Freigabedatensatzes, die Beschreibung, das Profil der ausgehenden Intelligenz oder die Gruppen vorab auszufüllen. Weitere Informationen finden Sie unter Freigabe ausgehender Intelligence-Datensätze aus der GUI.

Diese Vorlagen geben an, welche Entitäten und Attribute enthalten sind, sowie die Systemeinstellungen für die Freigabe.

Durch die Konfiguration dieser Vorlagen können Organisationen bestätigen, dass nur relevante und genehmigte Intelligence-Daten freigegeben werden, indem die Sicherheit und Compliance für interne und externe Zusammenarbeitsbemühungen aufrechterhalten wird.

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Wählen Sie Aus **Verwaltung** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Ausgehende Intel-Freigabe** .
4. Wählen Sie Aus **Vorlagen Für Ausgehende Intel-Freigabe** .
5. Wählen Sie **Neu**.
6. Füllen Sie im Formular die Felder aus.

Neue Vorlage Für Ausgehende Intel-Freigabe Erstellen

Feld	Beschreibung
Vorlagenname	Name der Vorlage für die Freigabe ausgehender Intelligenz.
Vorlagenbeschreibung	Beschreibung der Vorlage für die Freigabe ausgehender Intelligenz.
Nutzungsmodus	Gibt an, wie eine Freigabevorlage verwendet werden soll. Vorlagen im Modul „Freigabe ausgehender Intelligenz“ sind vielseitig und können je nach Anforderungen auf mehrere Freigabeszenarien angewendet werden. Die verfügbaren Freigabeoptionen sind: **a. Freigabe Bei Bedarf** : Wird zum Freigeben von Daten aus der GUI verwendet. **b. Automatisierte Freigabe** : Aktiviert die geplante oder Auslöserbasierte Freigabe über Automatisierungs-Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	c. **Sowohl bei Bedarf als auch bei automatisierter Freigabe** : Ermöglicht die Verwendung der Vorlage in der On-Demand- oder automatisierten Freigabe und bietet maximale Flexibilität. d. **Automatisiertes Hinzufügen zu TAXII-Sammlungen** : Fügt TAXII-Sammlungen automatisch freigegebene Daten zur Verteilung an vertrauenswürdige externe Partner hinzu.
Schwärzung aktivieren (gilt nur für automatisierte Modi)	Aktivieren Sie dieses Kontrollkästchen, um es zu aktivieren **Schwärzung** , Bei dem sensible Informationen aus freigegebenen Daten ersetzt werden, um die Vertraulichkeit während der Freigabe von Informationen zu schützen. **Hinweis:** Diese Option gilt für **Automatisierte Freigabe** , Sowie für beide **Freigabe bei Bedarf und automatisierte Freigabe** Option, und **Automatisiertes Hinzufügen zu TAXII-Sammlungen** Und nicht zutreffend für **Freigabe Bei Bedarf** .
Zugriffssteuerungen für die Freigabe bei Bedarf	
Wichtig: Da diese Vorlagen in einem verwalteten Freigabemodell verwendet werden, z. B. beim Freigeben der Intelligenz für bestimmte Objekte oder erkennbare Elemente, möchten Sie möglicherweise steuern, welche Anwender oder Gruppen darauf zugreifen können. Um dies zu verwalten, gibt es einen dedizierten Abschnitt namens **Gewähren Sie allen Anwendern oder Gruppen mit Berechtigungen für die Freigabe ausgehender Intelligenz Zugriff** Wo Sie die Anwender und Gruppen angeben können, die für eine bestimmte Vorlage sichtbar sein sollen. Sie können den Zugriff einschränken, indem Sie die einzelnen Anwender oder Gruppen angeben und überprüfen, ob die Vorlage nur von ausgewählten Anwendern oder Gruppen verwendet werden kann.	
Gewähren Sie allen Anwendern oder Gruppen mit Berechtigungen für ausgehende intel-Freigaben Zugriff	Aktivieren Sie dieses Kontrollkästchen, um allen Anwendern oder Gruppen Zugriff zu gewähren, die über Berechtigungen für ausgehende Intel-Freigabe verfügen.
Anwender (sollte die Rolle „sn_sec_tisc.int_exch_write' haben)	Wählen Sie die Anwender aus, die auf Vorlagen für die Freigabe von Intelligenz zugreifen sollen. Sie müssen haben sn_sec_tisc.int_exch_write Rolle zum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Durchführen der Freigabe ausgehender Intelligenz.
Gruppen (sollte die Rolle „sn_sec_tisc.int_exch_write' haben)	Wählen Sie die Gruppen für den Zugriff auf Vorlagen für die Freigabe von Intelligenzen aus. Gruppen müssen über verfügen `sn_sec_tisc.int_exch_write` Rolle zum Durchführen der Freigabe ausgehender Intelligenz.
Vorab Ausgefüllte Eingaben	
Name (Name Des Freigabedatensatzes)	Name des freigegebenen Datensatzes. Dieser Wert ist im Datensatz der ausgehenden intelligenten Freigabe vorab ausgefüllt.
Beschreibung (Beschreibung Des Freigabedatensatzes)	Beschreibung des Freigabedatensatzes. Dieser Wert ist im Datensatz der ausgehenden intelligenten Freigabe vorab ausgefüllt.
Ausgehende Intel-Freigabeprofile	Gibt die ausgehenden Intel-Freigabeprofile an. Dieser Wert ist im Datensatz der ausgehenden intelligenten Freigabe vorab ausgefüllt. Weitere Informationen finden Sie unter Konfigurieren Von Ausgehenden Intel-Freigabeprofilen.
Ausgehende Intel-Freigabegruppen	Gibt die ausgehenden Intel-Freigabegruppen an. Dieser Wert ist im Datensatz der ausgehenden intelligenten Freigabe vorab ausgefüllt. Weitere Informationen finden Sie unter Konfigurieren Ausgehender Intel-Freigabegruppen.
TAXII-Sammlungen	Gibt die TAXII-Sammlungen an. Diese Option ist nur sichtbar, wenn Sie den Nutzungsmodus als auswählen **Automatisiertes Hinzufügen zu TAXII-Sammlungen** .
Standardkonfidenz (0–100)	Gibt den Standardkonfidenzwert an, der nur angewendet wird, wenn die Intelligenzdatensätze im Freigabedatensatz keinen Konfidenzwert angeben. Dieser Wert ist im Datensatz der ausgehenden intelligenten Freigabe vorab ausgefüllt.
TLP überschreiben	Aktivieren Sie dieses Kontrollkästchen, um das TLP (Traffic Light Protocol) zu überschreiben, indem eine bestimmte TLP auf alle Datensätze innerhalb der Freigabesteuerung angewendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dieser TLP wird während der Nutzlastgenerierung verwendet und überschreibt den auf der Ebene der einzelnen Datensätze zugewiesenen TLP. Dieser Wert ist im Datensatz der ausgehenden intelligenten Freigabe vorab ausgefüllt.
TLP	Gibt das Traffic Light Protocol (TLP) der Freigabevorlage an. Diese Option ist nur sichtbar, wenn Sie auswählen **TLP überschreiben** Kontrollkästchen.
Systemeinstellungen für Freigabe	
Steuerungen Für Ausgehende Intelligence-Freigabe	Gibt die Steuerungen für die Freigabe ausgehender Intelligence an. Standardmäßig ist der Wert in diesem Feld **Steuerungen Für Ausgehende Intel-Freigabe** Da dies die einzige Freigabesteuerung ist, die im Basissystem bereitgestellt wird.
Ausschlussregeln Für Ausgehende Intelligenz	Gibt die Ausschlussregeln für ausgehende Intelligenz an. Standardmäßig ist der Wert in diesem Feld **Ausgehende Datenausschlussregel** Da dies die einzige Ausschlussregel ist, die im Basissystem bereitgestellt wird.

7. Wählen Sie Aus **Speichern** Um die Freigabevorlage zu speichern.
   Eine Bestätigungsnachricht wird angezeigt, die angibt, dass alle Steuerungen für die ausgehende Freigabe von Intelligenzen automatisch in diese Vorlage kopiert und in sichtbar sind **Steuerungen Für Vorlagenfreigabe** Abschnitt innerhalb weniger Sekunden.

Steuerungen Für Vorlagenfreigabe:

8. Navigieren Sie zu **Steuerungen Für Vorlagenfreigabe** Abschnitt.
   Vorlagenfreigabesteuerungen zeigen alle Freigabesteuerungen an, die für die ausgewählte Vorlage definiert sind. Diese Freigabesteuerungen hängen von den Freigabesteuerungen auf Hauptebene ab, die als ausgehende Steuerungen für die gemeinsame Nutzung von Intelligenzen bezeichnet werden. Weitere Informationen finden Sie unter Konfigurieren Von Steuerungen Für Die Freigabe Ausgehender Intel.
9. Wählen Sie Aus **Hinzufügen** Innerhalb von **Steuerungen Für Vorlagenfreigabe** Abschnitt.
   Das Dialogfeld Entitäten und Attribute hinzufügen wird angezeigt.

   Sie sehen nur die Entitäten, die in den Hauptfreigabesteuerungen definiert sind. Standardmäßig sind alle Entitäten im Basissystem enthalten und bereitgestellt, sodass Sie zunächst alle Freigabesteuerungen sehen. Wenn Sie jedoch eine Entität aus der Hauptfreigabesteuerung entfernen, ist diese Entität nicht mehr für die Auswahl in den Freigabesteuerungen der Vorlage verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:
Diese Vorlagen werden auch in STIX verwendet, daher werden die Validierungsregeln für STIX eingeführt. Ein Verstoß gegen diese Regeln kann zu einem Fehler beim Generieren der Nutzlast führen. Wenn die definierten STIX-Compliance-Regeln nicht erfüllt werden, wird die Nutzlast möglicherweise nicht an den konfigurierten Endpunkt gesendet, und der Freigabeprozess könnte vollständig gestoppt werden.

Eine Fehlermeldung wird angezeigt, die eine STIX-Validierungswarnung angibt: Sie müssen mindestens eines der erforderlichen Attribute für diese Entität einschließen.

10. Wählen Sie Aus **Fügen Sie alle optionalen Attribute hinzu** Um die optionalen Attribute in die Freigabevorlagen einzubeziehen.
11. Klicken Sie außerdem auf **Entfernen Sie alle Attribute** (Papierkorbsymbol unten im Dialogfeld verfügbar), um alle optionalen Attribute zu entfernen oder auszuwählen **Entfernen Sie Die Entität** Schaltfläche im Dialogfeld „Entität und Attribute bearbeiten“, um die Entität vollständig aus der Vorlage zu entfernen.
12. Nachdem Sie die erforderlichen Änderungen an der Freigabesteuerung vorgenommen haben, klicken Sie auf **Veröffentlichen** Um die Steuerungen für die Vorlagenfreigabe zu veröffentlichen.
Sobald die Steuerungen für die Vorlagenfreigabe veröffentlicht wurden, werden sie für die Verwendung in Vorlagen für ausgehende Freigabe von Intelligenz verfügbar.

Wichtig:
Diese Vorlagen gelten auch während der Freigabe von Daten aus dem GUI-Setup und können über die Threat Intelligence-Bibliothek aufgerufen werden. Weitere Informationen finden Sie unter Freigabe ausgehender Intelligence-Datensätze aus der GUI.

13. **Wahlweise:** Wählen Sie Aus **Bearbeiten** Schaltfläche, um die erforderlichen Änderungen an der Vorlage vorzunehmen.

Hinweis:
Wenn Sie Änderungen an der Vorlage vornehmen, wird eine Warnmeldung angezeigt, die darauf hinweist, dass ausgehende Datensätze für die gemeinsame Nutzung von Informationen vorhanden sind, die von der Freigabevorlage abhängig sind. Stellen Sie sicher, dass keine ausstehenden ausgehenden Intelligence-Freigabedatensätze vorhanden sind, bevor Sie diese Vorlage bearbeiten.

(Optional) Während Sie die Freigabevorlage bearbeiten, wird eine Bestätigungsnachricht angezeigt, die angibt, dass das Bearbeiten dieser Vorlage, ohne die abhängigen Automatisierungs-Flows zuerst zu deaktivieren, zu Fehlern führen kann, und möchten Sie trotzdem fortfahren. Wenn Sie fortfahren möchten, wählen Sie aus **Bearbeiten** Schaltfläche zum Vornehmen der Änderungen.

14. Wählen Sie außerdem aus **Duplikat** Schaltfläche wenn Sie ein Duplikat der Vorlage erstellen möchten, klonen Sie die aktuelle Vorlage.
Mit dieser Aktion wird die gesamte Konfiguration einschließlich aller zugehörigen Freigabesteuerungen repliziert.

Validierung zum Aktivieren der Freigabevorlage:

Die Anwendung prüft auf verschiedene Validierungen, bevor die Vorlagen für die Freigabe ausgehender Informationen aktiviert werden. Sie werden aktiviert, wenn alle erforderlichen Konfigurationen abgeschlossen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. **Fehlende Freigabesteuerungen** : Wenn der Vorlage keine Freigabesteuerungen hinzugefügt wurden und der Anwender versucht, zu veröffentlichen, lässt die Anwendung zu, dass die Vorlage gespeichert und veröffentlicht, aber nicht aktiviert wird.

   Eine Validierungsnachricht wird angezeigt, um zu verhindern, dass die Vorlage aktiv verwendet wird.

b. **Entwurfsfreigabesteuerungen auf Hauptebene** : Wenn sich die Hauptsteuerelemente für ausgehende Intel-Freigabe noch in befinden **Bearbeitungsmodus (Entwurf)** , Kann die Vorlage nicht aktiviert werden. In diesem Fall wird eine Warnmeldung angezeigt, die darauf hinweist, dass sich die Freigabesteuerungen im Entwurfsstatus befinden und veröffentlicht werden müssen, bevor fortgefahren wird.

   Diese Validierungen werden erzwungen, um zu bestätigen, dass Vorlagen nur für die Freigabe aktiviert werden, wenn sich alle zugehörigen Komponenten in befinden **Veröffentlicht** Und Status aktiviert. Dies hilft, zu verhindern, dass unvollständige oder ungültige Konfigurationen in betrieblichen Freigabeprozessen verwendet werden.

Hinweis:

- Wenn Sie auswählen **Veröffentlichen** Und wenn eines der genannten Kriterien nicht erfüllt ist, wird die Vorlage trotzdem veröffentlicht, aber nicht aktiviert.
- Wenn Sie auswählen **Aktivieren** Und wenn eines der genannten Kriterien nicht erfüllt ist, wird die Vorlage nicht aktiviert.
- **Aktivieren** Und **Deaktivieren** Schaltflächen werden nur für veröffentlichte Vorlagen angezeigt.

15. **Wahlweise:** Wählen Sie Aus **Deaktivieren** Von **Vorlagen Für Ausgehende Intel-Freigabe** Seite direkt, wenn Sie eine Freigabevorlage deaktivieren möchten.

Hinweis:
Auf der **Vorlagen Für Ausgehende Intel-Freigabe** Seitenlistenansicht können Sie auch verschiedene Aktionen ausführen, z. B. **Duplikat** , **Aktivieren** , Oder **Deaktivieren** Indem Sie eine oder mehrere Vorlagen auswählen.

Zugehörige Informationen

Freigabe ausgehender Intelligence-Datensätze aus der GUI

Automatisierte Freigabe ausgehender Intelligence-Datensätze

Automatisierte Freigabe von TAXII-Sammlungen

Bearbeitung der Schwärzungsbibliothek

Schwärzung ist der Prozess zum Ersetzen vertraulicher Informationen aus freigegebenen Daten, um die Vertraulichkeit während der Freigabe von Informationen zu schützen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird
Mit dieser Funktion können Sie vertrauliche oder personalisierte Informationen durch bestimmte Werte schwärzen oder ersetzen.

Innerhalb des Datensatzes für die ausgehende Freigabe von Intelligenzen können Sie die Schwärzungsbibliothek anwenden, um bestimmte Attribute oder Inhalte automatisch herauszufiltern, bevor die Nutzlast generiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei der Freigabe von Threat Intelligence werden die vertraulichen Informationen, die als Schwärzkategoriewerte definiert sind, durch die entsprechende Schwärzungskategorie ersetzt.

Dies ist besonders nützlich, wenn Daten für externe Organisationen freigegeben werden, in denen nur die relevanten und nicht vertraulichen Informationen offengelegt werden sollen.

Durch die Nutzung der Funktion „Schwärzungsbibliothek“ können TISC-Administratoren und -Analysten wiederverwendbare Schwärzungskonfigurationen definieren und einheitlich auf mehrere Freigabevorlagen anwenden.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Wählen Sie Aus **Verwaltung** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Ausgehende Intel-Freigabe** .
4. Wählen Sie Aus **Schwärzungsbibliothek** .
   Die Listenansicht „Schwärzungsbibliothek“ wird angezeigt.
5. Wählen Sie **Neu**.
6. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Schwärzungskategorie	Geben Sie die Schwärzungskategorie für den Datensatz der ausgehenden intelligenten Freigabe an.
Status	Der Status der Schwärzungskategorie. Standardmäßig sind alle Schwärzungskategorien aktiviert. Sie können jedoch eine bestimmte Schwärzungskategorie deaktivieren.

7. Klicken Sie auf **Speichern**.
8. Wechseln Sie zu **Schwärzungskategoriewerte** Abschnitt.
9. Wählen Sie Aus **Neu** Dient zum Erstellen eines Wertsatzes für die Schwärzkategorie.

Systemeigenschaft für Schwärzungsbibliothek :

Name	Beschreibung
sn_sec_tisc.case_sensitive_for_redaction	Diese Eigenschaft aktiviert oder deaktiviert die Groß-/Kleinschreibung beim Anwenden von Schwärzung auf gemeinsam genutzte Intelligenz. Standard: Deaktiviert (`Falsch`), was bedeutet, dass bei der Schwärzung die Groß-/Kleinschreibung standardmäßig nicht beachtet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	Hinweis: Standardmäßig ist diese Eigenschaft deaktiviert, sodass bei der Schwärzung die Groß-/Kleinschreibung nicht beachtet wird. Beispielsweise würden Service_now und Service_now gleichermaßen schwärzt. Aktivieren (Wahr) Bedeutet, dass die Schwärzung nur angewendet wird, wenn der Fall genau übereinstimmt.

10. Wählen Sie **Speichern**.

Massenimport von Schwärzungskategorien und -Werten

Schwärzungskategorien importieren. Massenimport von Schwärzungskategorien und ihren zugehörigen Werten.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Beispieldatei entweder im CSV- oder XLSX-Format herunterladen, sie mit Schwärzungskategorien und entsprechenden Werten ausfüllen und sie dann zurück in die Anwendung importieren. Diese Massenimport-Funktion optimiert das effiziente Hinzufügen mehrerer Schwärzungsregeln.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Wählen Sie Aus **Verwaltung** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Ausgehende Intel-Freigabe** .
4. Wählen Sie Aus **Schwärzungsbibliothek** .
5. Klicken Sie auf **Importieren**.
6. Laden Sie eine Beispieldatei herunter.
   Die Importdatei enthält zwei Spalten:
   - Schwärzungskategorie
   - Wert

   Stellen Sie sicher, dass Sie die Header in der Beispieldatei nicht ändern, da dies zu Importfehlern führen kann.
7. Laden Sie die Datei hoch, und klicken Sie auf **Fertig** .
   Eine Bestätigungsnachricht wird angezeigt, dass die Schwärzungszeilen erfolgreich importiert wurden. Sie können auch auf den Link klicken, um die Importzusammenfassung anzuzeigen.

   Hinweis:
   Die Dateigröße darf 5 MB nicht überschreiten, und die Anzahl der Zeilen darf 1000 nicht überschreiten.

   Validierungsregeln:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Stellen Sie sicher, dass alle Schwärzungskategorien und ihre Kategoriewerte eindeutig sind.

b. Ein Schwärzungskategoriewert kann nicht mit mehr als einer Schwärzungskategorie verknüpft werden. Wenn beispielsweise ein Kategoriewert bereits einer Schwärzungskategorie zugeordnet ist, kann er keiner anderen Kategorie zugewiesen werden.

Systemeigenschaften für den Massenimport von Schwärzungskategorien und -Werten :

Name	Beschreibung
sn_sec_tisc.max_redaction_rows_Import	Diese Eigenschaft legt die maximale Anzahl von Zeilen fest, die beim Massenimport von Daten in die Schwärzungsbibliothek zulässig sind. Der Standardwert für den Höchstwert ist 1000.

Eingehende Intel-Freigabe Erkunden

Freigabe eingehender Intelligenz in TISC Ermöglicht Ihnen das Erstellen von Profilen externer Systeme oder Geräte, die Informationen an die IT übermitteln können.

Eingehende Intel-Freigabeprofile Konfigurieren

In diesem Abschnitt werden die Profile für die gemeinsame Nutzung eingehender Informationen beschrieben, die zum Empfangen von Informationen von externen Organisationen in verwendet werden TISC.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Hinweis:

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Eingehende Intel-Freigabe**an.
2. Wählen Sie Aus **Eingehende Intel-Freigabeprofile** .
3. Wählen Sie Aus **Neu** Dient zum Erstellen eines Profils für eingehende Intelligenz.
4. Füllen Sie im Formular die Felder aus.

Erstellen Sie Ein Neues Eingehendes Intelligence-Profil

Feld	Beschreibung
Name	Name des eingehenden Intelligence-Profils.
Branche	Wählen Sie die Branchenkategorie aus, z. B. Luft- und Raumfahrt, für die das Profil für eingehende Intelligenz gilt.
Beschreibung	Beschreibung des Profils für eingehende Intelligenz.
Einstellungen Für Eingehende Intelligenz	
Datenformat	Unterstützte Datenformate für das Profil für die Freigabe eingehender Intelligenz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Derzeit werden zwei Datenformate für die Freigabe eingehender Informationen unterstützt: ○ STIX 2,1 ○ MISP Weitere Informationen zur Beschreibung der Datenformate finden Sie unter Konfigurieren Von Ausgehenden Intel-Freigabeprofilen.
Anwender für Authentifizierung (muss die Rolle „sn_sec_tisc.api_post_intel“ haben)	Wählen Sie den Anwender aus, dessen Anmeldeinformationen für die Authentifizierung verwendet werden sollen, wenn ein externes System Intelligenz für freigibt TISC Für dieses Profil. **Hinweis:** Anwender mit der Rolle „sn_sec_tisc.api_post_intel“ sind nur in der Dropdown-Liste verfügbar.
Standardkonfidenz	Gibt das Standardkonfidenzniveau an, das auf alle von diesem Profil empfangenen Intelligence-Datensätze angewendet wird, wenn die Quelle keinen Konfidenzwert bereitstellt.
Ablaufzeitraum (in Tagen)	Gibt die Anzahl der Tage an, nach denen die vom Freigabeprofil empfangenen Intelligence-Datensätze ablaufen. Nach Ablauf sind die Intelligence-Datensätze möglicherweise nicht mehr sichtbar, freigegeben oder gelten als gültig.
Standard-TLP	Gibt den Standard-TLP an, der auf alle von diesem Profil empfangenen Intelligence-Datensätze angewendet wird, wenn die Quelle keinen TLP-Wert bereitstellt.
Aktivieren Sie Die Benachrichtigung	Wählen Sie diese Prüfung aus, um eine Benachrichtigung an den Absender zu senden, wenn der eingehende Intelligence-Datensatz genehmigt oder abgelehnt wird.
Benachrichtigen am	Verwenden Sie diese Option, um auszuwählen, wann die konfigurierten E-Mail-Empfänger benachrichtigt werden sollen (z. B. bei Genehmigung oder Ablehnung oder beides eines Datensatzes). **Hinweis:** Diese Option wird nur angezeigt, wenn **Aktivieren Sie Die Benachrichtigung** Ist ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
E-Mail-Empfänger	Geben Sie die E-Mail-Adressen der Anwender ein, die basierend auf den in konfigurierten Kriterien benachrichtigt werden sollen **Benachrichtigen Am** Feld. **Hinweis:** Dieses Feld ist nur sichtbar, wenn **Aktivieren Sie Die Benachrichtigung** Ist aktiviert. Mehrere E-Mail-Adressen können durch Kommas getrennt eingegeben werden.
TISC-Tags	Gibt die Tags an, die allen eingehenden Informationen hinzugefügt werden sollen, die vom externen System empfangen werden.

5. Wählen Sie **Speichern**.

Profil-ID kopieren :

Die externen Organisationen benötigen diese Profil-ID, um die Informationen freizugeben.

6. Wählen Sie Aus **Profil-ID kopieren** Schaltfläche zum Kopieren Ihrer Profil-ID zur Freigabe.
7. Wählen Sie außerdem aus **E-Mail-Profil-ID** Zum E-Mail der Details zum Freigabeprofil.
   Wenn Sie diese Option auswählen, wird ein Dialogfeld zum E-Mail-Editor angezeigt. Geben Sie die E-Mail-Details ein, für die Sie das Profil freigeben möchten.
8. Wählen Sie Aus **Senden** Um die Details an den externen Anwender zu senden.

Zugehörige Informationen

Eingehende Intel-Freigabegruppen Konfigurieren

Definieren der Genehmigungsregel für eingehende Intel

Eingehende Intel-Freigabegruppen Konfigurieren

Eingehende Intel-Freigabegruppen ermöglichen Administratoren die Gruppierung ähnlicher Profile für eingehende Intelligenz. Diese Gruppen können verwendet werden, um Genehmigungsregeln zu definieren, die für alle Profile innerhalb der Gruppe gelten.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Eingehende Intel-Freigabe**an.
2. Wählen Sie Aus **Eingehende Intel-Freigabegruppen** .
3. Wählen Sie Aus **Neu** Dient zum Erstellen einer eingehenden Intelligence-Gruppe.
4. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name der eingehenden Intel-Freigabegruppe.
Beschreibung	Beschreibung der eingehenden Intel-Freigabegruppe.
Typ	Gibt an, ob die Gruppe zu einer internen oder externen Organisation gehört.

5. Wählen Sie Aus **Speichern** Zum Speichern der Intelligence-Freigabegruppe.
   Außerdem können Sie die Gruppe basierend auf der Anforderung aktivieren oder deaktivieren.

Hinzufügen Von Gruppenmitgliedern:

In diesem Abschnitt können Sie mehrere Profile an eine Gruppe anhängen.

6. Navigieren Sie zu **Gruppenmitglieder** Abschnitt.
7. Wählen Sie **Hinzufügen**.
   Das Dialogfeld eingehende Intelligence-Profile hinzufügen wird angezeigt. Hier werden alle aktivierten Profile für die Freigabe eingehender Informationen aufgelistet.
8. Wählen Sie mindestens ein Profil aus.
9. **Wahlweise:** Geben Sie einen Grund für das Hinzufügen der ausgewählten Profile für eingehende Intelligenz zu den Gruppen an.
10. Wählen Sie **Hinzufügen**.
    Die ausgewählten Profile werden den Gruppen hinzugefügt.
11. Wählen Sie außerdem aus **Entfernen** Zum Entfernen der Profile aus der Gruppe.

> **Hinweis:**
> Sie müssen einen Grund für die Entfernung hinzufügen.

Zugehörige Informationen

Eingehende Intel-Freigabeprofile Konfigurieren

Definieren der Genehmigungsregel für eingehende Intel

Definieren der Genehmigungsregel für eingehende Intel

Definieren Sie Genehmigungsregeln, um zu steuern, ob bestimmte Profile oder Gruppen vor der Verarbeitung der eingehenden Intelligenz genehmigt werden müssen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Wählen Sie Aus **Verwaltung** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Eingehende Intel-Freigabe** .
4. Wählen Sie Aus **Genehmigungsregel für eingehende Intelligenz** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Innerhalb des Basissystems die **Genehmigungsregel für eingehende Intelligenz** Ist die zum Aktivieren des Genehmigungs-Workflows bereitgestellte Standardregel.

5. Geben Sie im Formular „Genehmigungsregel“ in jedem der folgenden Abschnitte mindestens einen Anwender oder eine Anwendergruppe ein:
   a. **Wählen Sie ein Profil oder eine Gruppe für die Genehmigung aus** : Wählen Sie in diesem Abschnitt die Freigabeprofile für eingehende Intel oder die Freigabegruppen für eingehende Intelligenz aus, die eine Genehmigung für die Verarbeitung der eingehenden Intelligenzdaten erfordern.
   b. **Genehmiger auswählen** : Wählen Sie in diesem Abschnitt die Anwender oder Gruppen aus, die zum Genehmigen der eingehenden Intelligence-Datensätze erforderlich sind, die von den zuvor konfigurierten Profilen/Gruppen empfangen wurden.
6. Wählen Sie Aus **Aktivieren** Schaltfläche zum Aktivieren der Genehmigungsregel für eingehende Intel.

Hinweis:
- Nach der Aktivierung wird jeder zutreffende Datensatz für eingehende Intel an die Genehmigungswarteschlange weitergeleitet.
- Mindestens ein zugewiesener Genehmiger überprüft die vom Analysten vorgenommenen Änderungen und entscheidet sich, die Anforderung zu genehmigen oder abzulehnen.
- Nachdem eine Entscheidung getroffen wurde, wird eine E-Mail-Benachrichtigung an E-Mail-Adressen gesendet, wie im entsprechenden Profil für die Freigabe eingehender Informationen konfiguriert, die angibt, ob der Datensatz genehmigt oder abgelehnt wurde.

TAXII-ausgehender Server erkunden

TAXII-Sammlungen sind logische Gruppierungen von Threat Intelligence-Daten.

Erstellen Sie eine TAXII-Sammlung

In diesem Abschnitt erfahren Sie, wie Sie TAXII-Sammlungen für die Freigabe von Intelligenz konfigurieren und definieren.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Ausgehender TAXII-Server**an.
2. Wählen Sie Aus **TAXII-Sammlungen** .
3. Wählen Sie Aus **Neu** Dient zum Erstellen einer TAXII-Sammlung.
4. Füllen Sie im Formular die Felder aus.

Erstellen Sie Ein Neues Eingehendes Intelligence-Profil

Feld	Beschreibung
Name	Name der TAXII-Sammlung.
Beschreibung	Beschreibung der TAXII-Sammlung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Spezifikationsversion	Gibt die Version der TAXII an, die für die Datenformatierung und den Datenaustausch verwendet wird. **Hinweis:** Die einzige unterstützte Spezifikationsversion für die Datenformatierung ist 2,1.
Ablaufzeitraum (in Tagen)	Gibt die Anzahl der Tage an, nach denen die der TAXII-Sammlung hinzugefügten Datensätze ablaufen. **Hinweis:** Nach Ablauf werden die Datensätze als inaktiv markiert und anschließend aus der Sammlung entfernt.
Versionsverwaltung aktivieren	Aktivieren Sie dieses Kontrollkästchen, um die Versionsverwaltung für die Datensätze zu aktivieren, die der TAXII-Sammlung hinzugefügt werden. **Hinweis:** Wenn ein Datensatz einer TAXII-Sammlung hinzugefügt wird und sich von seiner vorherigen Version unterscheidet, fügt die Anwendung die neue Version nur hinzu, wenn die Versionsverwaltung aktiviert ist. Wenn die Versionsverwaltung nicht aktiviert ist, wird der vorhandene Datensatz mit den aktualisierten Daten überschrieben.
Zugriff auf alle TAXII-API-Anwender	Gibt den Zugriff für TAXII-Anwender an. Wenn diese Option ausgewählt ist, erhalten alle Anwender, denen die Rolle „TAXII-Server-API“ zugewiesen ist, die Berechtigung zum Abrufen von Daten aus dieser Sammlung. **Hinweis:** Wenn **Zugriff auf alle TAXII-API-Anwender** Feld ist nicht ausgewählt. Nur die in diesem Feld angegebenen Anwender haben Zugriff auf die TAXII-Sammlungsdatensätze.
Lesezugriff	Wenn **Zugriff auf alle TAXII-API-Anwender** Feld ist nicht ausgewählt, dann können nur die in diesem Feld angegebenen Anwender auf die TAXII-Sammlungsdatensätze zugreifen.

5. Wählen Sie **Speichern**.

Systemeigenschaft zum Hinzufügen von Datensätzen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Systemeigenschaft für TAXII-Sammlungen begrenzt die Anzahl der Datensätze, die einer TAXII-Sammlung hinzugefügt werden können.

Die folgende Systemeigenschaft ist für die Konfiguration der TAXII-Sammlung:

Name	Beschreibung
sn_sec_tisc.Taxii_Server_Collection_Record_limit	Maximale Anzahl von Datensätzen, die einer ausgehenden TAXII-Serversammlung hinzugefügt werden können. Der Standardwert ist 10000.

6. Zeigen Sie die Systemeigenschaftsinformationen zum Hinzufügen von Datensätzen zur TAXII-Sammlung an.
7. Navigieren Sie zu **Flow Designer** > **Flows**an.
   Diese Navigation zeigt den Vorlagen-Flow zum Hinzufügen von TAXII-Sammlungen an.
8. Wählen Sie aus **Fügen Sie einer TAXII-Sammlung automatisch Threat Intelligence hinzu** Flow.
9. Navigieren Sie zu **Flow Designer** > **Aktionen**an.

Hinzufügen von Datensätzen zur TAXII-Sammlung

Derzeit ist die einzige Methode zum Hinzufügen von Datensätzen zur TAXII-Serversammlung über einen automatisierten Prozess. Im folgenden sind die beiden Aktionen aufgeführt, die im Basissystem bereitgestellt werden:

a. **Fügen Sie der TAXII-Serversammlung einen Datensatz hinzu**
b. **Fügen Sie der TAXII-Serversammlung Datensätze hinzu**

10. Zeigen Sie die jeweilige TAXII-Serversammlungsaktion an.

Zugehörige Informationen

Automatisierte Freigabe von TAXII-Sammlungen

Konfigurieren Von Vorlagen Für Ausgehende Intel-Freigabe

Automatisierte Freigabe von TAXII-Sammlungen

Automatisierte TAXII-Sammlungen fügen TAXII-Serversammlungen automatisch Intelligenzdatensätze hinzu, um sie nahtlos an vertrauenswürdige externe Partner zu verteilen.

Vorbereitungen

Erforderliche Rolle:

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

Die automatisierte Flow-Aktion fügt den in den Eingaben bereitgestellten Datensatz zu TAXII-Serversammlungen hinzu, die in der ausgewählten Vorlage konfiguriert sind. Weitere Informationen finden Sie unter Konfigurieren Von Vorlagen Für Ausgehende Intel-Freigabe.

Fügen Sie der TAXII-Serversammlung einen Datensatz über einen automatisierten Prozess hinzu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Automatisierte Flows**an.
3. Wählen Sie Aus **Fügen Sie einer TAXII-Sammlung automatisch Threat Intelligence hinzu** Aktionslink zum Anzeigen der jeweiligen Regeldetails im Flow Designer.
4. Zeigen Sie die Flow Designer-Aktion für die folgenden Auslöser an:

   Observable Created or Updated where (Type is IP address (V4), or Type is IP address (V6), or Type is Domain Name; and TISC Tags contains Add to: Sample Collection, and Reputation is Malicious, and Threat Score greater than or is 60) Actions Select multiple

5. Wechseln Sie zu **Aktionen**
6. Wählen Sie **Fertig**.

Nächste Maßnahme

Aktivieren Sie den Flow.

Zugehörige Informationen

Erstellen Sie eine TAXII-Sammlung

Konfigurieren Von Steuerungen Für Die Freigabe Ausgehender Intel

Konfigurieren Von Vorlagen Für Ausgehende Intel-Freigabe

TAXII-Sammlungsdatensätze anzeigen

Zeigen Sie die Datensätze an, die den TAXII-Sammlungen hinzugefügt werden.

Vorbereitungen

Erforderliche Rolle:

- sn_sec_tisc.admin
- sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Administration** > **Ausgehender TAXII-Server**an.
2. Wählen Sie Aus **TAXII-Sammlungen** .
3. Wechseln Sie zu **TAXII-Sammlungsdatensätze** Abschnitt, nachdem Sie die neue TAXII-Sammlung gespeichert haben.
   Alle der TAXII-Sammlung hinzugefügten Datensätze werden in diesem Abschnitt angezeigt.
4. Wählen Sie Aus **Entfernen** Schaltfläche zum Entfernen von Datensätzen aus der TAXII-Sammlung.
   Ein Anwender mit der Rolle „sn_sec_tisc.Analyst“ kann nur Datensätze aus der TAXII-Sammlung entfernen.
5. Wählen Sie die zu entfernenden Datensätze aus, und wählen Sie sie aus **Entfernen** .

Zeigen Sie Die Externe Freigabe Von Threat Intelligence An

Die Freigabe von Threat Intelligence bietet eine zentrale Ansicht verschiedener Quellen für die Freigabe von Bedrohungsdaten. Mit der Funktion können Sie die Bedrohungsdatensätze überwachen, die für die Freigabe von Intelligenzen verarbeitet werden, und die Genehmigungs-Workflows für verschiedene Arten von Intelligence-Daten verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Abschnitt wird Folgendes beschrieben:

1. Ausgehende Intelligenz
2. Eingehende Intelligenz
3. TAXII-Sammlungen

Ausgehende Intelligenz

Ausgehende Intelligenz bezieht sich auf Threat Intelligence-Daten, die Ihre Organisation für externe Entitäten freigibt.

Als TISC-Analyst können Sie die zugehörigen Details überprüfen, z. B. Vorlagen, Profile, Gruppen, Freigabe von Entitätsattributen, Ausschlussregeln, und genehmigen oder lehnen Sie sie ab, bevor Sie sie in den Intelligence-Systemen der Organisation verwenden. Weitere Informationen finden Sie unter Erkunden Sie Die Ausgehende Intel-Freigabe.

Eingehende Intelligenz

Eingehende Intelligenz bezieht sich auf Bedrohungsdaten, die von externen Quellen empfangen werden. In diesem Abschnitt können Sie eingehende Intelligence-Daten verwalten, die von externen Systemen empfangen wurden.

Eingehende Intelligenz ist eine Gruppe von Sammlungen, die erkennbare Bedrohungsinformationen, Indikatoren und andere Bedrohungsobjekte enthalten, die als eingehende Intelligence-Datensätze bezeichnet werden.

Als TISC-Analyst können Sie sie überprüfen und genehmigen oder ablehnen, bevor sie in die Intelligence-Systeme der Organisation aufgenommen werden. Weitere Informationen finden Sie unter Eingehende Intel-Freigabe Erkunden.

TAXII-Sammlungen

Trusted Automated Exchange of Intelligence Information (TAXII) ist ein Protokoll, das für die Freigabe von Threat Intelligence verwendet wird. Weitere Informationen finden Sie unter TAXII-ausgehender Server erkunden.

Ausgehende Intelligence Anzeigen

Verwenden Sie diesen Abschnitt, um alle Datensätze für die Freigabe ausgehender Intelligenz anzuzeigen. Überprüfen Sie die Intelligence-Daten, und ergreifen Sie die erforderlichen Aktionen, um sie zu genehmigen oder abzulehnen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intelligence-Freigaben**an.
   Die Seite Threat Intelligence-Freigabe wird mit den folgenden Abschnitten zur Freigabe von Intelligenzen angezeigt, die die entsprechende Aktion erfordern.
   - Ausgehende Intelligenz
   - Eingehende Intelligenz
   - Ausgehender TAXII-Server
2. Auswahlvorgang **Ausgehende Intelligenz** > **Alle**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf der Seite „ausgehende Intelligenz“ werden die Datensätze angezeigt, die derzeit für die Freigabe von Intelligenzen verwendet werden. Es werden die folgenden Unterabschnitte angezeigt:

- **Alle** : Zeigt alle ausgehenden Datensätze zur gemeinsamen Nutzung von Intelligenzen an.
- **Von Mir Erstellt** : Zeigt die von Ihnen erstellten Datensätze für die ausgehende gemeinsame Nutzung von Intelligenzen an.
- **Ausstehende Genehmigungen** : Zeigt die ausgehenden Intelligence-Datensätze an, für die Genehmigungen ausstehen.
- **Meine Genehmigungen** : Zeigt die ausgehenden Intelligence-Datensätze an, die auf Ihre Genehmigung warten.

3. Öffnen Sie einen beliebigen Datensatz, um den Status des freigegebenen Datensatzes anzuzeigen.
   Überprüfen Sie die Datensätze für die Freigabe von Intelligence, die auf Genehmigung oder Ablehnung warten.
4. Wählen Sie Aus **Überprüfen** Abschnitt zum Überprüfen der ausgehenden Intelligence-Daten.
5. Verifiziert die veröffentlichten Aufträge, die den ausgehenden Intelligence-Daten zugeordnet sind.
6. Wählen Sie Aus **Genehmigen** Um den Freigabedatensatz zu genehmigen.
   Die Option ausgehende Intelligenz genehmigen wird angezeigt.
7. Fügen Sie bei Bedarf Kommentare hinzu.
8. Wählen Sie Aus **Genehmigen** Schaltfläche zum Genehmigen des Datensatzes für die Freigabe von Informationen.
   Eine Bestätigungsnachricht wird angezeigt, die angibt, dass der ausgehende Intelligence-Datensatz genehmigt wurde.
9. Wählen Sie außerdem aus **Ablehnen** Schaltfläche, wenn Sie die ausgehende Freigabeinformation ablehnen müssen.

Eingehende Intelligence Anzeigen

Verwenden Sie diesen Abschnitt, um alle eingehenden Datensätze für die gemeinsame Nutzung von Intelligenzen anzuzeigen. Überprüfen Sie die Intelligence-Daten, und ergreifen Sie die erforderlichen Aktionen, um sie zu genehmigen oder abzulehnen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intelligence-Freigaben**an.
2. Auswahlvorgang **Eingehende Intelligenz** > **Alle**
   Auf der Seite „eingehende Intelligenz“ werden die eingehenden Intelligence-Datensätze angezeigt, die von den Systemen von den externen Parteien empfangen werden, die derzeit für die Freigabe von Informationen zuständig sind. Es werden die folgenden Unterabschnitte angezeigt:
   - **Alle** : Zeigt alle eingehenden Datensätze für die gemeinsame Nutzung von Intelligenzen an, die vom System über mehrere Profile hinweg empfangen wurden.
   - **Ausstehende Genehmigungen** : Zeigt die eingehenden Intelligence-Datensätze an, für die Genehmigungen ausstehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Meine Genehmigungen** : Zeigt die eingehenden Intelligence-Datensätze an, die auf Ihre Genehmigung warten.

  Hinweis:
  Sie können direkt **Genehmigen** Oder **Ablehnen** In der Listenansicht des Abschnitts „meine Genehmigungen“. Wählen Sie die gewünschte Option in der geteilten Schaltflächenansicht aus, und genehmigen oder lehnen Sie sie ab, indem Sie einen Grund angeben.

Wählen Sie den entsprechenden Abschnitt aus, und erwägen Sie, die erforderliche Aktion für jeden eingehenden Intelligence-Datensatz zu ergreifen.

3. Wählen Sie einen beliebigen eingehenden Intelligence-Datensatz aus, um die Details anzuzeigen.
   Alle Datensätze, die als Teil des Intelligence-Datensatzes empfangen werden, sind unter verfügbar **Eingehende Intelligence-Datensätze** Abschnitt.
4. Wählen Sie Aus **Genehmigen** Um den Freigabedatensatz zu genehmigen.
   Das Dialogfeld eingehende Intelligence genehmigen wird angezeigt.
5. Fügen Sie bei Bedarf Kommentare hinzu.
6. Öffnen Sie einen beliebigen Datensatz, der auf Ihre Überprüfung wartet.

   a. Wählen Sie Aus **Genehmigen** Schaltfläche zum Genehmigen des eingehenden Intelligence-Datensatzes.
   Eine Bestätigungsnachricht wird angezeigt, die angibt, dass der eingehende Intelligence-Datensatz genehmigt wurde.

   Hinweis:

   Benachrichtigungen werden basierend auf den Regeln ausgelöst, die in jedem Profil konfiguriert sind. Sobald Sie einen Freigabedatensatz genehmigt oder abgelehnt haben, wird eine E-Mail gesendet, wenn E-Mail-Benachrichtigungen für das Profil aktiviert sind. Wenn keine E-Mail konfiguriert ist, wird keine Benachrichtigung gesendet.

7. Wählen Sie außerdem aus **Ablehnen** Schaltfläche, wenn Sie den eingehenden Intelligence-Datensatz ablehnen möchten.

   Hinweis:

   E-Mail-Beispiele für die Genehmigung und Ablehnung eines Freigabedatensatzes:

   - **E-Mail-Benachrichtigung bei Genehmigung** : Ihre Anforderung für eingehende Intelligence-Daten wird genehmigt.
   - **E-Mail-Benachrichtigung bei Ablehnung** : Ihre Anforderung für eingehende Intelligence-Daten {sharing Record number} wurde abgelehnt. Sie können den abgelehnten Freigabedatensatz über den angegebenen Link anzeigen.

TAXII-Sammlungen anzeigen

Verwenden Sie diesen Abschnitt, um die TAXII-Sammlungen anzuzeigen, die als Teil des ausgehenden TAXII-Servers konfiguriert sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intelligence-Freigaben**an.
2. Auswahlvorgang **Ausgehender TAXII-Server** > **TAXII-Sammlungen**an.
3. Wählen Sie einen beliebigen gewünschten TAXII-Sammlungsdatensatz aus, um die Datensätze anzuzeigen, die den TAXII-Sammlungen hinzugefügt wurden.
4. Wechseln Sie zu **TAXII-Sammlungsdatensätze** Abschnitt.
   Alle der TAXII-Sammlung hinzugefügten Datensätze werden im Abschnitt „TAXII-Sammlungsdatensätze“ angezeigt.
5. Wählen Sie Aus **Entfernen** Schaltfläche zum Entfernen von Datensätzen aus der TAXII-Sammlung.
   Ein Anwender mit der Rolle „sn_sec_tisc.Analyst“ kann nur Datensätze aus der TAXII-Sammlung entfernen.
6. Wählen Sie die zu entfernenden Datensätze aus, und wählen Sie sie aus **Entfernen** .
   Wenn Sie die Entfernung von TAXII-Sammlungsdatensätzen initiieren, wird eine Bestätigungsnachricht angezeigt, die Sie auffordert, zu bestätigen, ob ein oder mehrere Datensätze aus der Intelligence-Freigabe entfernt werden können. Nach der Bestätigung werden die Datensätze entfernt, und im Aktivitätenstrom wird automatisch eine Arbeitsnotizaktivität veröffentlicht, die die Details der entfernten Datensätze enthält.

Schwärzungsimporte Anzeigen

Mit Schwärzungsimporten können Sie alle Datensätze anzeigen, die derzeit in Importaufträgen verarbeitet werden, sowie alle Importaufträge, für die die Genehmigung aussteht.

Zeigen Sie alle Schwärzungsimporte an

Verwenden Sie diesen Abschnitt, um alle mit Schwärzung importierten Datensätze anzuzeigen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Importe**an.
2. Auswahlvorgang **Schwärzungsimporte** > **Alle Importe**
   Auf dieser Seite werden alle Datensätze angezeigt, die für den Importauftrag verarbeitet werden.
3. Öffnen Sie einen beliebigen Datensatz, um den Status des Importprozesses anzuzeigen.

Hinweis:
Sie können auch auf klicken **Neuer Import** Dient zum Erstellen eines neuen Importdatensatzes. Nachdem Sie auf diese Schaltfläche geklickt haben, leitet die Anwendung Sie zu **Importieren Sie Intelligence** Seite. Weitere Informationen zum Erstellen neuer Datensätze finden Sie unter Importieren Sie Intelligence in TISC Abschnitt und fahren Sie mit dem jeweiligen Importtyp fort.

Zeigen Sie meine Schwärzungsimporte an

Verwenden Sie diesen Abschnitt, um Importdatensätze anzuzeigen, die vom derzeit angemeldeten Anwender erstellt wurden.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Importe**an.
2. Auswahlvorgang **Schwärzungsimporte** > **Meine Importe**
   Auf dieser Seite werden alle Datensätze dieser Importdatensätze angezeigt, die für den weiteren Prozess für den Importauftrag kategorisiert sind.
3. Öffnen Sie einen beliebigen Datensatz, um den Status des Importprozesses anzuzeigen.
4. Zeigen Sie die Zusammenfassung der Importdatensätze an, die vom angemeldeten Anwender importiert werden.

Freigabe ausgehender Intelligence-Datensätze aus der GUI

In diesem Abschnitt wird die Funktionalität beschrieben, mit der Anwender Intelligence-Datensätze direkt aus der Threat Intelligence-Bibliothek (TI) in freigeben können TISC Anwendung.

Vorbereitungen

Erforderliche Rolle:

- sn_sec_tisc.Analyst
- sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird

Der Zugriff auf die Freigabevorlagen unterliegt mehreren Einschränkungen, die in jeder Vorlage definiert sind. Diese Einschränkungen geben an, ob eine Vorlage für alle Anwender verfügbar oder auf bestimmte Anwender oder Anwendergruppen beschränkt ist. Dementsprechend sind nur die in diesen Einstellungen zulässigen Vorlagen sichtbar, wenn Anwender initiieren **Intelligence Freigeben** Prozess.

Nur Anwender mit einer Analystenrolle können die Intelligence-Daten aus der GUI für externe Systeme freigeben. Die Funktion „Intelligenz freigeben“ gilt auch für die verschiedenen anderen Entitäten der Threat Intelligence-Bibliothek, einschließlich erkennbarer Elemente, Indikatoren und Objekte wie Angriffsmuster, Bedrohungsakteure usw.

Im Folgenden finden Sie das Verfahren zum Freigeben von Informationen aus der Formularansicht von Datensätzen erkennbarer Elemente.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
2. Öffnen Sie einen Datensatz für erkennbare Elemente.
3. Klicken Sie auf **Intelligence Freigeben** Schaltfläche.
   Das Dialogfeld Vorlage für ausgehende Intelligenz auswählen wird angezeigt.
4. Wählen Sie die erforderliche Vorlage für ausgehende Intelligenz aus der Suche aus.

Hinweis:
Mit dem Hyperlink „Standardvorlageneinbindungen anzeigen“ (Tabellen und Attribute) können Sie alle enthaltenen Attribute anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Aktivieren Sie das Kontrollkästchen **Verknüpfen Sie automatisch auch zugehörige Datensätze der ausgewählten Intelligenz** Um die zugehörigen Datensätze automatisch mit dem Freigabedatensatz zu verknüpfen und die Details zu speichern.
6. Wählen Sie **Absenden**.
   Nachdem Sie die Datensätze zur Freigabe von Intelligenzen übermittelt haben, werden nur die zugänglichen Vorlagen angezeigt.
   a. **Konfigurationen von Datenausschlussregeln** : Datensätze werden ausgeschlossen, wenn sie den in Ihren Datenausschlussregeln definierten Kriterien entsprechen. Weitere Informationen finden Sie unter Konfigurieren Der Ausschlussregel Für Ausgehende Intel-Daten.
   b. **Ausgewählte Steuerungen für Freigabevorlagen** : Datensätze werden gemäß den Steuerungen gefiltert, die in den ausgewählten Freigabevorlagen definiert sind. Weitere Informationen finden Sie unter Konfigurieren Von Vorlagen Für Ausgehende Intel-Freigabe.

   Basierend auf diesen Konfigurationskriterien werden die relevanten Datensätze von der Freigabe ausgeschlossen.
7. Klicken Sie Auf **Wählen Sie Aus** Dient zum Erstellen eines Datensatzes für ausgehende Intelligence-Freigabe.
   Nehmen Sie bei Bedarf die erforderlichen Änderungen vor.
8. Klicken Sie Auf **Speichern** Zum Speichern der geänderten Werte in **Ausgehende Intelligence-Daten** Formular.
9. Wählen Sie Aus **Übermitteln** Um den Freigabedatensatz zur Übermittlung zu übermitteln.
   In **Details** Abschnitt des Freigabedatensatzes füllt die Anwendung automatisch die Werte aus, die in konfiguriert sind **Vorab Ausgefüllte Eingaben** Der Seite „Vorlagen für ausgehende Intel-Freigabe“. Weitere Informationen finden Sie unter Konfigurieren Von Vorlagen Für Ausgehende Intel-Freigabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Im Folgenden sind die Systemeigenschaften für den ausgehenden Intelligence-Datensatz aufgeführt.

Name	Beschreibung
Shared_Intelligence_Entity_threshold	Schwellenwert für Datensatz: Diese Eigenschaft steuert die maximale Anzahl einzelner Datensätze, die in einem einzelnen ausgehenden Intelligence-Datensatz enthalten sein können. ○ Der Standardwert beträgt 1000 Datensätze. ○ Der Höchstwert beträgt 10000 Datensätze.
Shared_Intelligence_Exclusion_work_Notes_count	Grenzwert für ausgeschlossene Datensätze: Diese Eigenschaft steuert, wie viele Zeilen pro Arbeitsnotiz im Aktivitätenstrom angezeigt werden. ○ Standard: 10 Zeilen pro Arbeitsnotiz. ○ Maximal: 100 Zeilen pro Arbeitsnotiz. Wenn die Anzahl der Zeilen den angegebenen Grenzwert überschreitet, werden die Datensätze auf mehrere Arbeitsnotizen aufgeteilt, um die Lesbarkeit und die Anwender-Experience sicherzustellen.

10. Wechseln Sie zu **Intelligence-Datensätze** Abschnitt.
In diesem Abschnitt werden alle Intelligence-Datensätze angezeigt, die Teil des ausgewählten Freigabedatensatzes sind.

Abschnitt „Intelligence-Datensätze“ anzeigen:

Hinweis:
Der Abschnitt „Datensätze zur intelligenten Freigabe“ ist nur sichtbar, wenn sich der Freigabedatensatz im befindet **Entwurf** status und nicht sichtbar, wenn sich der Freigabedatensatz in einem anderen status befindet, z. B. **Verarbeitet** , **Warten Auf Genehmigung** Und so weiter.

Sie können die vollständige Liste der erkennbaren Elemente, Objekte und zugehörigen Entitäten anzeigen, die als Teil des Datensatzes gruppiert und gemeinsam genutzt werden.

Wenn Sie auf zugreifen **Datensätze Zur Intelligenten Freigabe** Abschnitt sehen Sie eine strukturierte Ansicht aller mit diesem Datensatz verknüpften Intelligence-Entitäten, die im linken Seitenbereich der Seite angezeigt werden.

- **Vorlagenkonfiguration** : Die in dieser Ansicht angezeigten Entitätstabellen basieren auf den Freigabesteuerungen, die in der Freigabevorlage definiert sind, die dem Freigabedatensatz zugeordnet ist.
- **Entitätsgruppierung** : Die erste Gruppierung auf hoher Ebene ist erkennbare Elemente. Außerdem werden erkennbare Elemente auf untergeordneter Ebene wie Datei, IP-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Adresse und andere relevante Typen angezeigt. Indikatoren und Objekte werden auch nach erkennbaren Elementen aufgelistet.

- **Beziehungen** : Zeigt Beziehungen zwischen den freigegebenen Entitäten an. Es werden sechs verschiedene Arten von Beziehungen dargestellt, die jeweils in der entsprechenden Beziehungstabelle organisiert sind, um Klarheit und Struktur zu gewährleisten.

Hinweis:
Listen mit mindestens einem Datensatz anzeigen Ist ein Umschalter verfügbar, um schnell nur die Entitätstabellen zu filtern und anzuzeigen, die Daten enthalten.

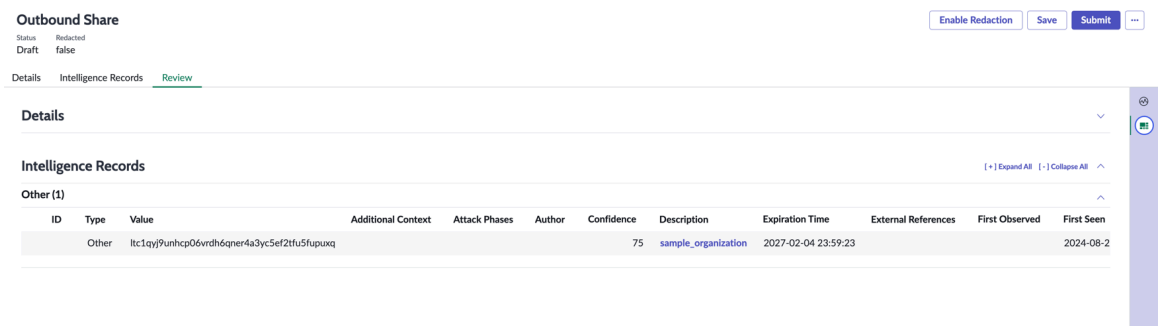
11. Klicken Sie Auf **Bearbeiten Sie Spalten** Zum Ändern der Listenansichtsspalten.
Die **Wählen Sie Spalten Aus** Das Dialogfeld wird angezeigt, mit dem Sie konfigurieren können, welche Spalten in der Listenansicht angezeigt werden.
12. Wenn Sie außerdem die Details der Datensätze ändern möchten, wählen Sie aus **Datensätze Ändern** . Wenn Sie diese Aktion auswählen, können Sie einen oder mehrere Datensätze ändern. Angenommen, Sie können nur die optionalen Felder des Datensatzes ändern, wenn Sie einen oder mehrere Datensätze ändern oder eine Massenbearbeitung durchführen. Wenn eine Massenbearbeitungsoption ausgewählt ist, werden alle Werte in den Feldern gelöscht, und wenn Sie einen Wert und angeben **Speichern** Dann gelten diese Werte für alle ausgewählten Datensätze.

Hinweis:
Alle Änderungen, die an den Entitätsdatensätzen vorgenommen werden, die im Abschnitt „Intelligenzdatensätze“ vorhanden sind, werden nicht auf die entsprechenden Bibliotheksdatensätze angewendet. Wenn Sie beispielsweise die Beschreibung für ein Angriffsmuster ändern, hätte diese Änderung Auswirkungen auf das entsprechende Angriffsmuster in der Threat Intelligence-Bibliothek.

13. Klicken Sie Auf **Hinzufügen** Um dem Freigabedatensatz Datensätze hinzuzufügen, wird eine Bestätigung angezeigt, dass die ausgewählten Datensätze erfolgreich hinzugefügt wurden.

Hinweis:
Wenn Ausschlussregeln für die Freigabe von Datensätzen konfiguriert sind, werden alle ausgewählten Datensätze, die die Kriterien für Ausschlussregeln erfüllen, automatisch übersprungen. Diese Datensätze werden den Intelligence-Datensätzen nicht hinzugefügt. Eine entsprechende Fehlermeldung wird angezeigt, um den Anwender zu benachrichtigen, und detaillierte Informationen zu den ausgeschlossenen Datensätzen werden im Aktivitätenstrom aufgezeichnet.

14. Klicken Sie Auf **Entfernen** Um die Datensätze aus dem Freigabedatensatz zu entfernen.
15. Wählen Sie Aus **Aktivieren Sie Die Schwärzung** Schaltfläche zum Aktivieren der Schwärzung für die freigegebenen Datensätze.



Hinweis:
Um die Schwärzungsbibliothek zu aktivieren, müssen Sie die Schwärzungsbibliothek konfigurieren. Weitere Informationen finden Sie unter Bearbeitung der Schwärzungsbibliothek.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

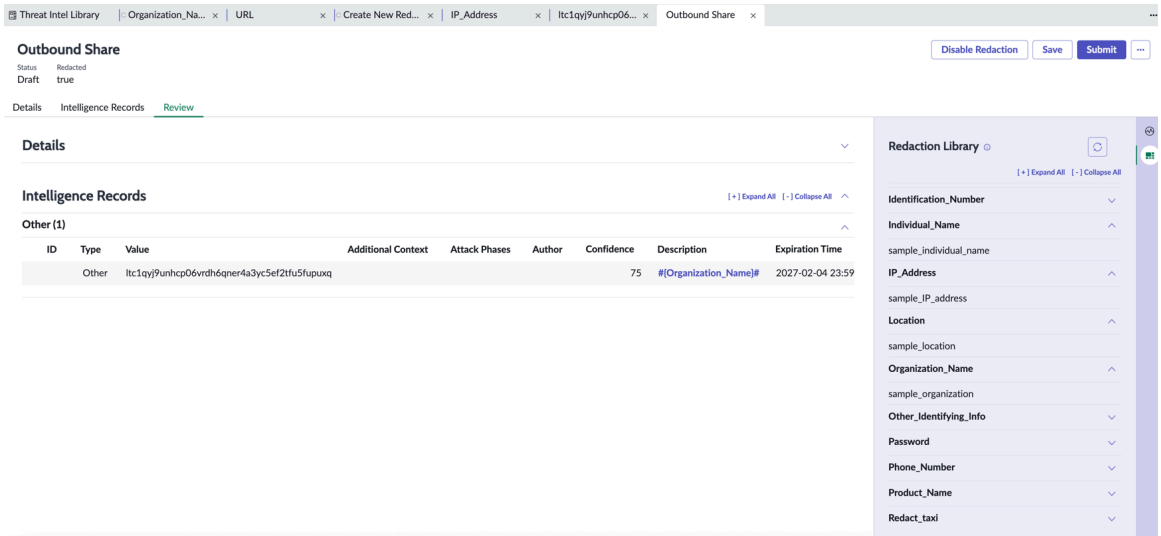
Aktivieren Sie Die Schwärzung Mit der Option können Sie vertrauliche Informationen automatisch entfernen oder maskieren, indem Sie vertrauliche Inhalte schwärzen, bevor Sie Intelligence-Datensätze freigeben. Durch Aktivieren der Schwärzung wird sichergestellt, dass vertrauliche Daten während der Freigabe von Intelligenzen geschützt und nicht zugänglich gemacht werden.

Sobald Sie diese Option aktiviert haben, wird die **Schwärzungsbibliothek** Das Symbol wird im rechten Kontextmenü angezeigt und bietet Zugriff auf eine Liste aller verfügbaren Schwärzkategorien und Schwärzkategoriewerte, die in der Schwärzungsbibliothek in definiert sind **Verwaltung** Abschnitt.

Beispiel: Wenn Sie einen Organisationsnamen schwärzen, z. B. **Service_Now** , Und **Service_Now** Wird als Schwärzkategoriewert unter hinzugefügt **Organization_Name** Kategorie, dann alle Vorkommen von **Service_Now** Wird mit dem folgenden Format ersetzt:

`#{Organization_Name}#` .

Durch Aktivieren der Option „Schwärzen“ schwärzt das System den Organisationsnamen vor der Freigabe automatisch. Der folgende Screenshot zeigt den geschwärzten Kategoriewert.



16. Wechseln Sie zu **Überprüfen** Abschnitt zum Überprüfen des Intelligence-Datensatzes des ausgewählten Freigabedatensatzes.
17. **Wahlweise:** Wählen Sie Aus **Deaktivieren Sie Die Schwärzung** Zum Deaktivieren der Schwärzung für die freigegebenen Datensätze bei Bedarf.

Überprüfen Sie Intelligence-Datensätze

18. Navigieren Sie zu **Überprüfen** Abschnitt zum Überprüfen der Datensätze im Freigabedatensatz.
    Die **Überprüfen** Abschnitte bieten eine Snapshot-Ansicht, die alle Entitäten zusammenfasst, die in der Intelligence-Freigabe enthalten sind. Die Datensätze zeigen die schnelle Zusammenfassung der folgenden Elemente:
    - **Details** : Zeigt die Details des freigegebenen Datensatzes im schreibgeschützten Modus an.
    - **Entitätsattribute Freigeben** : Zeigt die Freigabesteuerungen an, die in der Freigabevorlage definiert sind, die einem Freigabedatensatz zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Ausschlussregeln** : Zeigt die konfigurierten Ausschlussregeln an.
- **Schwärzungsbibliothek** : Zeigt die Schwärzungsbibliothek an, die in konfiguriert ist **Verwaltung** Abschnitt. Weitere Informationen finden Sie unter Bearbeitung der Schwärzungsbibliothek.

19. Nehmen Sie die erforderlichen Änderungen unter vor **Überprüfen** Abschnitt und klicken Sie auf **Übermitteln** Zur Übermittlung.
Eine Bestätigungsnachricht wird angezeigt, die Sie auffordert, den Datensatz zur Verarbeitung zu übermitteln. Wenn Sie fortfahren möchten, wählen Sie aus **Übermitteln** .

    Sobald Sie die Übermittlung abgeschlossen haben, werden die Datensätze der ausgehenden Freigabe von Intelligenzen verwendet **Status** Ändert sich von **Entwurf** Bis **Warten Auf Genehmigung** . Die **Status** Wird in geändert **Warten Auf Genehmigung** Nur, wenn die Genehmigungsregeln für die ausgehende Intelligenz konfiguriert sind. Weitere Informationen finden Sie unter Definieren der Genehmigungsregel für ausgehende Intel.

20. Wählen Sie Aus **Genehmigen** Schaltfläche zum Genehmigen des ausgehenden Intelligence-Datensatzes.
21. Fügen Sie bei Bedarf Kommentare hinzu, und wählen Sie aus **Genehmigen** Auf der **Genehmigen Sie Ausgehende Intelligence** Dialogfeld.
22. Wählen Sie auch aus **Ablehnen** Schaltfläche zum Ablehnen des ausgehenden Intelligence-Datensatzes.
23. Geben Sie einen Grund an, und wählen Sie aus **Ablehnen** Auf der **Lehnt Ausgehende Intelligence Ab** Dialogfeld.

    Sobald Sie die Ablehnung vorgenommen haben, werden die Datensätze der ausgehenden Intelligence-Freigabe angezeigt **Status** Ändert sich in **Abgelehnt** .

    Hinweis:
    Wählen Sie Aus **Bearbeiten** Schaltfläche und nehmen Sie die erforderlichen Änderungen basierend auf den Ablehnungskommentaren vor. Die **Status** Wird zurück zu verschoben **Entwurf** Wenn Sie die Datensätze bearbeiten und erneut übermitteln möchten.

    Wenn keine Genehmigungsregel definiert ist oder der Datensatz bereits genehmigt ist, wird der Datensatz für die ausgehende gemeinsame Nutzung von Intelligenzen in verschoben **Warten Auf Verarbeitung** status. In dieser Phase werden die Intelligence-Daten extern freigegeben, danach wird der Status auf aktualisiert **Verarbeitet** . Weitere Informationen finden Sie unter Definieren der Genehmigungsregel für ausgehende Intel.

24. Navigieren Sie zu **Veröffentlichte Aufträge** Zum Anzeigen der veröffentlichten Aufträge für den Freigabedatensatz.
Für jedes Profil für ausgehende Intelligenz gibt es einen veröffentlichten Auftrag und den **Status** Kann durch diese veröffentlichten Aufträge nachverfolgt werden.

    Wenn Sie auf einen der veröffentlichten Aufträge klicken, werden die Details des Auftrags angezeigt, z. B. **Nutzlast** , **Status** , Und so weiter.

    Wenn beim Senden von Daten an den entsprechenden Endpunkt auf der Empfängerseite ein Problem auftritt, versucht die Anwendung standardmäßig bis zu 5 Mal automatisch erneut. Um die Anzahl der Wiederholungsversuche zu ändern, können Sie den Wert mit der folgenden Systemeigenschaft ändern:

    `sn_sec_tisc.Shared_Intelligence_retry_count`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

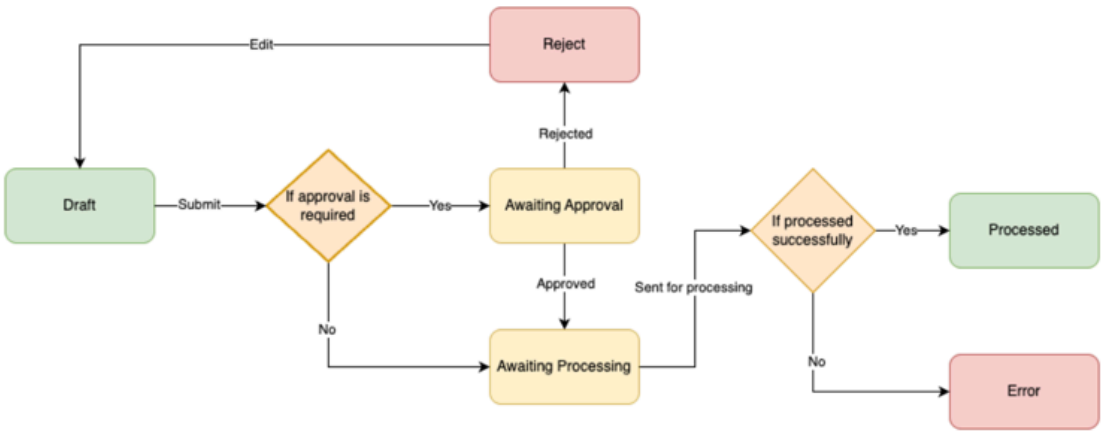
Konfigurieren Von Steuerungen Für Die Freigabe Ausgehender Intel

Automatisierte Freigabe ausgehender Intelligence-Datensätze

Genehmigungs-Workflow Für Threat Intelligence-Freigabe

In diesem Abschnitt werden die verschiedenen Genehmigungsebenen beschrieben, die für die Freigabe von Intelligence-Daten für externe Organisationen erforderlich sind.

Der folgende Workflow veranschaulicht die verschiedenen Genehmigungsebenen, die für die externe Freigabe von Daten erforderlich sind. Weitere Informationen zu den Genehmigungsebenen finden Sie unter Freigabe ausgehender Intelligence-Datensätze aus der GUI.



Automatisierte Freigabe ausgehender Intelligence-Datensätze

Die automatisierte Freigabe ausgehender Informationen ermöglicht die nahtlose und automatische Verteilung von Intelligence-Datensätzen an externe Systeme.

Vorbereitungen

Erforderliche Rolle:

- Systemadministrator (anzeigen, erstellen oder bearbeiten)
- sn_sec_tisc.admin (Ansicht)

Warum und wann dieser Vorgang ausgeführt wird

Die automatisierte Flow-Aktion erstellt einen ausgehenden Datensatz für die gemeinsame Nutzung von Intelligenzen mit den angegebenen Datensätzen und verarbeitet sie entsprechend.

Erstellen eines Datensatzes für ausgehende Intelligence-Freigabe über einen automatisierten Prozess:

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Administration**an.
2. Auswahlvorgang **Automatisierte Flows**an.
3. Wählen Sie Aus **Automatisierte Freigabe von IOC mit hohem Risiko für vertrauenswürdige Partner** Aktionslink zum Anzeigen der jeweiligen Regeldetails im Flow Designer.
4. Zeigen Sie die Flow Designer-Aktion für die folgenden Auslöser an:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daily at 12.00.00
Run every day once

5. Wechseln Sie zu **Aktionen**

6. Wählen Sie **Fertig**.

Nächste Maßnahme
Aktivieren Sie den Flow. Weitere Informationen zu automatisierten Flows finden Sie unter Automatisierte Freigabe von IOC mit hohem Risiko für vertrauenswürdige Partner.

Zugehörige Informationen

Konfigurieren Von Steuerungen Für Die Freigabe Ausgehender Intel

Freigabe ausgehender Intelligence-Datensätze aus der GUI

Mit Datenimporten arbeiten

Mit Datenimporten können Sie alle Datensätze anzeigen, die für den Importauftrag verarbeitet werden, und auch die Importaufträge auflisten, die auf Genehmigungen warten.

Alle Importe werden angezeigt

Verwenden Sie diesen Abschnitt, um alle importierten Datensätze anzuzeigen, die in der Listenansicht für alle Anwender angezeigt werden.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Importe**an.
2. Auswahlvorgang **Datenimporte** > **Alle Importe**
   Auf dieser Seite werden alle Datensätze angezeigt, die für den Importauftrag verarbeitet werden.
3. Öffnen Sie einen beliebigen Datensatz, um den Status des Importprozesses anzuzeigen.

Hinweis:
Sie können auch auf klicken **Neuer Import** Dient zum Erstellen eines neuen Importdatensatzes. Nachdem Sie auf diese Schaltfläche geklickt haben, leitet die Anwendung Sie zu **Importieren Sie Intelligence** Seite. Weitere Informationen zum Erstellen neuer Datensätze finden Sie unter Importieren Sie Intelligence in TISC Abschnitt und fahren Sie mit dem jeweiligen Importtyp fort.

Meine Importe werden angezeigt

Verwenden Sie diesen Abschnitt, um die Importdatensätze anzuzeigen, die vom angemeldeten Anwender erstellt wurden.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Importe**an.
2. Auswahlvorgang **Datenimporte** > **Meine Importe**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf dieser Seite werden alle Datensätze dieser Importdatensätze angezeigt, die für den weiteren Prozess für den Importauftrag kategorisiert sind.

3. Öffnen Sie einen beliebigen Datensatz, um den Status des Importprozesses anzuzeigen.

Hinweis:
Sie können auch auf klicken **Neuer Import** Dient zum Erstellen eines neuen Importdatensatzes. Nachdem Sie auf diese Schaltfläche geklickt haben, leitet die Anwendung Sie zu **Importieren Sie Intelligence** Seite. Weitere Informationen zum Erstellen neuer Datensätze finden Sie unter Importieren Sie Intelligence in TISC Abschnitt und fahren Sie mit dem jeweiligen Importtyp fort.

4. Zeigen Sie die Zusammenfassung der Importdatensätze an.

Hinweis:
Falls einer der Importaufträge nicht übermittelt wird, können Sie dies tun **Übermitteln** Die Datensätze zur weiteren Verarbeitung und senden sie zur Genehmigung. Wenn für diesen bestimmten Importauftrag keine Genehmigung erforderlich ist, werden diese Datensätze automatisch verarbeitet.

Meine Genehmigungen werden angezeigt

Verwenden Sie diesen Abschnitt, um die Importauftragsdatensätze zu überprüfen und zu genehmigen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Importe**an.
2. Auswahlvorgang **Datenimporte** > **Meine Genehmigungen**
   Auf dieser Seite werden alle Importdatensätze angezeigt, die auf die Genehmigung durch den angemeldeten Anwender warten.
3. Öffnen Sie einen beliebigen Datensatz, um den Importdatensatz zu genehmigen oder abzulehnen.
4. Klicken Sie Auf **Genehmigen** Zum Genehmigen des Importauftragsdatensatzes.
   Die **Import Genehmigen** Das Dialogfeld wird angezeigt, und es wird eine Bestätigungsmeldung angezeigt, ob die ausgewählten Importe genehmigt werden sollen.

Hinweis:
Eine E-Mail-Benachrichtigung wird an die jeweiligen Anwender gesendet, dass der Importauftrag, der in Bearbeitung war, jetzt genehmigt wurde. Weitere Informationen zum Genehmigen von Regeln finden Sie unter Definieren Von Genehmigungsregeln Für Datenimporte.

5. Wählen Sie Aus **Genehmigen** Über das Dialogfeld.
   Eine E-Mail-Benachrichtigung wird an den Anwender gesendet, der den Importauftrag erstellt hat, und der Importauftrag, der in Bearbeitung war, wird jetzt genehmigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie Auf **Ablehnen** Zum Ablehnen eines Datensatzes.

Hinweis:

- Sie können den abgelehnten Importauftrag überprüfen und erneut übermitteln. Stellen Sie sicher, dass Sie Kommentare zur Ablehnung hinzufügen.
- Eine E-Mail-Benachrichtigung wird an den Anwender gesendet, der den Importauftrag für den Importauftrag erstellt hat, wenn der Importauftrag, der gerade verarbeitet wurde, abgelehnt wird.
- Eine E-Mail-Benachrichtigung wird an die Genehmiger gesendet, die die Genehmigung anfordern.

Importieren Sie Intelligence in TISC

Verwenden Sie diese Funktion, um Threat Intelligence-Daten manuell in das Repository zu importieren, sodass Analysten nach Bedarf die relevanten Informationen aus externen Quellen erfassen können.

Die folgenden Formate werden für den Import von Threat Intelligence-Daten unterstützt:

Importformat	Beschreibung	Datensätze Unterstützt
Aus strukturierter Datei importieren	Laden Sie die Beispieldatei über den Link Vorschau herunter, und laden Sie Ihre strukturierten Daten in einem kompatiblen Format wie CSV, XLS oder XLSX hoch.	• Erkennbare Elemente • Indikatoren
Import aus Standardformat	Unterstützte Dateitypen sind die Formate STIX 2.x JSON und MISP JSON.	• **STIX 2,1** : Erkennbare Elemente, Indikatoren • **MISP** : Erkennbare Elemente
Import aus Rohtext	Analysieren Sie die Eingabe als Rohtext, um erkennbare Elemente zu importieren. Die maximale Zeichenbeschränkung für die Eingabe beträgt 10.000 Zeichen.	Erkennbare Elemente
Aus Datei (unstrukturiert) importieren	Die Anwendung analysiert die hochgeladene Datei automatisch, um erkennbare Elemente zu extrahieren. Unterstützte Dateitypen: TXT, CSV, JSON, XLS und XLSX.	Erkennbare Elemente

Ein besseres Verständnis der einzelnen Importformate und der unterstützten Datensatztypen finden Sie im Abschnitt zugehörige Informationen.

Zugehörige Informationen

Importieren Sie Daten mit einer strukturierten Datei

Importieren Sie Daten im Standardformat

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importieren Sie Daten mit Rohtext

Importieren Sie Daten im unstrukturierten Dateiformat

Importieren Sie Daten mit einer strukturierten Datei

Laden Sie die strukturierten Daten in den unterstützten Dateiformaten wie CSV, XLSX oder XLS hoch.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
   Die Seite „Threat Intel Library“ wird angezeigt.
2. Klicken Sie Auf **Importieren Sie Intelligence** .
3. Klicken Sie Auf **Aus strukturierter Datei importieren** Karte.

> **Wichtig:**
> Beim Importieren der Threat Intelligence-Daten in die unterstützten Dateiformate wie TXT, CSV, STIX 2.x JSON, MISP JSON oder strukturierte Datei die Dateigröße ist auf 5 MB beschränkt. Die Zeichenbeschränkung für Rohtext ist auf 000 begrenzt.

4. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Option wählen	Wählen Sie die erforderliche Option aus der Dropdown-Liste aus, z. B. erkennbare Elemente oder Indikatoren. ○ **Erkennbare Elemente** : Wählen Sie die zu importierenden Daten erkennbarer Elemente aus. **Hinweis:** Wählen Sie diese Option aus, wenn Sie Daten erkennbarer Elemente importieren. Ändern Sie auch die Spaltenüberschriften in der Datei nicht. Die Pflichtfelder sind Wert und Typ, andere sind optional. Geben Sie außerdem Datum/Uhrzeit im Format JJJJ-MM-TTThh:mm:SSZ ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Indikatoren** : Wählen Sie die zu importierenden Indikatordaten aus. **Hinweis:** Wählen Sie diese Option aus, wenn Sie Indikatordaten importieren. Ändern Sie auch die Spaltenüberschriften in der Datei nicht. Die Pflichtfelder für Indikatoren sind Muster, Mustertyp und gültig ab, andere sind optional. Geben Sie außerdem Datum/Uhrzeit im Format JJJJ-MM-TTThh:mm:SSZ ein.
Beispieldatei für Indikatoren in der Vorschau anzeigen und herunterladen	Verwenden Sie diesen Link, um die Beispieldatei über den Link Vorschau herunterzuladen und die strukturierten Daten in einem kompatiblen Dateiformat wie CSV, XLS oder XLSX hochzuladen. **Hinweis:** Die Spalten-Header müssen genau mit den Header übereinstimmen. Werte- und Typfelder sind für jedes erkennbare Element in der Datei erforderlich. Die verbleibenden Felder sind optional, wobei „zuletzt gesehen“ als Zahlen angegeben und die Epochenzeit in Millisekunden angegeben werden muss.
Datei hochladen	Klicken Sie auf diesen Link, um die Dateidaten im empfohlenen Strukturdateiformat hochzuladen. **Hinweis:** Sie können jeweils nur eine Datei hochladen. Um eine neue Datei hinzuzufügen, müssen Sie die vorhandene entfernen und eine neue Datei hinzufügen.
Legen Sie Definitionen fest	
TLP	Wählen Sie den Indikator „Traffic Light Protocol“ (TLP) aus der Dropdown-Liste aus, der auf die importierten Datensätze angewendet werden soll. TLP befindet sich in TISC ist mit verschiedenen Farben gekennzeichnet, um sicherzustellen, dass die sensiblen Daten für die beabsichtigten Anwender freigegeben werden. ○ KLAR: Informationen können ohne Einschränkung freigegeben werden. ○ ROT ○ GELB+STRIKT

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ GELB ○ GRÜN
Konfidenz (0-100)	Legen Sie den Konfidenzwert für die importierten Datensätze auf 0-100 fest.
Ablaufzeitraum (in Tagen)	Geben Sie den Ablaufzeitraum für die importierten Datensätze ein. **Hinweis:** Das ist ein Pflichtfeld.
Fügen Sie der Sicherheitssteuerungsliste erkennbare Elemente hinzu	Wählen Sie diese Option aus, um der entsprechenden Sicherheitssteuerungsliste erkennbare Elemente hinzuzufügen. Mit dieser Option können Sie die erkennbaren Elemente beim Importieren direkt einer Sicherheitssteuerungsliste hinzufügen. Die verfügbaren Optionen in der Dropdown-Liste sind: ○ Allow-Liste ○ Sperrliste ○ Keine Die Standardoption ist **Keine** .
Tags	
Tags hinzufügen	Verwenden Sie die Tags, um Anmerkungen oder Ohrmarkendatensätze zu versehen, die aus dieser Quelle in das System aufgenommen wurden. Beginnen Sie mit der Eingabe des Tag-Namens in **Suchen** Leiste, um die verfügbaren Tags im System auszuwählen oder einen neuen Tag-Namen einzugeben, und klicken Sie auf **Hinzufügen** Um es der Quelle zuzuweisen.
Taxonomie	
Eine Taxonomie auswählen	Wählen Sie die Taxonomie für die importierten Daten aus. Definieren Sie mithilfe von Taxonomien Wörterbücher, die als Taxonomien verwendet werden können, die Threat Intelligence-Datensätzen zugewiesen sind. Beispiel: CAPEC-Nomenklatur. Weitere Informationen finden Sie unter Taxonomien Werden Erstellt. **Hinweis:** Die Optionen für den Taxonomiewert ändern sich basierend auf der ausgewählten Taxonomie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quellwert überschreiben	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Quellwerte für TLP, Konfidenz, Ablauf, Tags und Taxonomien mit den konfigurierten Werten überschreiben möchten. Wenn Sie dieses Kontrollkästchen nicht aktivieren, werden die konfigurierten Werte angewendet, wenn sie nicht leer sind.

5. Klicken Sie auf **Next (Weiter)**.
6. Überprüfen Sie die Daten vor der Übermittlung zur Verarbeitung.

Hinweis:
Die Überprüfung importierter Datensätze wird für die STIX-Option nicht unterstützt.

Nachdem Sie auf geklickt haben **Als Nächstes** , Sie können die Zusammenfassung aller Informationen sehen, die der Anwender im obigen Abschnitt angegeben hat, und der folgende Abschnitt enthält alle Datensätze, die importiert werden müssen.

Der Anwender kann jede Art von Aktivitäten ausführen, und mehrere Anwender können über den Kommentarabschnitt zusammenarbeiten, der im rechten Kontextmenü verfügbar ist. Die Liste der importierten Datensätze wird gerendert, sobald die gesamte Datei oder der Rohtext verarbeitet wurde. Die Importverarbeitung für große Dateien dauert mehr Zeit. Während der Verarbeitung können Sie den Status überprüfen, überprüfen und übermitteln auch über die Importdatensatzseite.

Hinweis:
Alle Datensätze, die die Validierungen nicht bestehen, werden aus dem Importprozess übersprungen, und diese Datensätze werden nicht auf der Seite „Überprüfen und übermitteln“ zur weiteren Verarbeitung angezeigt.

7. Klicken Sie Auf **Aktualisierungstyp** Und wählen Sie den Typ aus, um einen beliebigen Typ der importierten Datensätze zu aktualisieren.
8. Klicken Sie Auf **Löschen** Zum Löschen eines beliebigen Typs der importierten Datensätze.
9. Klicken Sie auf **Absenden**.

Hinweis:
Nachdem Sie den Importdatensatz übermittelt haben, wird der Anwender an den Genehmiger weitergeleitet, um den entsprechenden Importdatensatz basierend auf den konfigurierten Genehmigungsregeln zu genehmigen. Wenn der aktuelle Anwender, der den Datensatz erstellt, den Genehmigungsprozess nicht erfordert, durchläuft der Datensatz den automatischen Genehmigungsprozess. Der Importauftrag wird beim Senden der Anforderung automatisch genehmigt.

10. Klicken Sie Auf **Status Anzeigen** Um den Status des Importdatensatzes anzuzeigen, oder klicken Sie auf **Fertig** .
Der Datensatz zeigt den Status „verarbeitet“ an, sobald die Daten zur Verarbeitung importiert wurden.
11. Klicken Sie Auf **Abbrechen** Um den Importprozess abzubrechen.
12. Klicken Sie Auf **Zurück** Um zur vorherigen Seite zurückzukehren und den Datensatz bei Bedarf zu überprüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Importieren Sie Daten im Standardformat

Laden Sie die Standarddaten in den unterstützten Dateiformaten wie STIX 2.x JSON, MISP JSON hoch.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
   Die Seite „Threat Intel Library“ wird angezeigt.
2. Klicken Sie Auf **Importieren Sie Intelligence** .
3. Klicken Sie Auf **Aus Standarddatei importieren** Karte.

> **Wichtig:**
> Beim Importieren der Threat Intelligence-Daten in die unterstützten Dateiformate wie TXT, CSV, STIX 2.x JSON, MISP JSON oder strukturierte Datei die Dateigröße ist auf 5 MB beschränkt. Die Zeichenbeschränkung für Rohtext ist auf 000 begrenzt.

4. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Dateiformat	Wählen Sie die erforderliche Option aus der Dropdown-Liste aus, z. B. STIX 2.x JSON oder MISP JSON. ○ **STIX 2.x JSON** : Wählen Sie das Format in STIX 2.x JSON aus, das importiert werden soll. **Hinweis:** Nur erkennbare Elemente und Indikatoren werden aus der hochgeladenen STIX-Datei importiert. Alle anderen Objekttypen werden während des Importprozesses ignoriert. ○ **MISP-JSON** : Wählen Sie das Format im MISP-JSON-Format aus, das importiert werden soll.
Datei hochladen	Klicken Sie auf diesen Link, um die Daten im Standarddateiformat hochzuladen.
Legen Sie Definitionen fest	
TLP	Wählen Sie den TLP-Indikator aus der Dropdown-Liste aus, der auf die importierten Datensätze angewendet werden soll.
Konfidenz (0-100)	Definieren Sie den Konfidenzwert.
Ablaufzeitraum (in Tagen)	Geben Sie den Ablaufzeitraum für die importierten Datensätze ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Das ist ein Pflichtfeld.
Tags hinzufügen	Verwenden Sie die Tags, um Anmerkungen oder Ohrmarkendatensätze zu versehen, die aus dieser Quelle in das System aufgenommen wurden. Beginnen Sie mit der Eingabe des Tag-Namens in der Suchleiste, um die verfügbaren Tags im System auszuwählen, oder geben Sie einen neuen Tag-Namen ein, und klicken Sie auf Hinzufügen, um ihn der Quelle zuzuweisen.
Fügen Sie der Sicherheitssteuerungsliste erkennbare Elemente hinzu	Wählen Sie diese Option aus, um der entsprechenden Sicherheitssteuerungsliste erkennbare Elemente hinzuzufügen. Mit dieser Option können Sie die erkennbaren Elemente beim Importieren direkt einer Sicherheitssteuerungsliste hinzufügen. Die verfügbaren Optionen in der Dropdown-Liste sind: ○ Allow-Liste ○ Sperrliste ○ Keine Die Standardoption ist **Keine** .
Taxonomie	
Eine Taxonomie auswählen	Wählen Sie die Taxonomie für die importierten Daten aus. Definieren Sie mithilfe von Taxonomien Wörterbücher, die als Taxonomien verwendet werden können, die Threat Intelligence-Datensätzen zugewiesen sind. Beispiel: CAPEC-Nomenklatur. Weitere Informationen finden Sie unter Taxonomien Werden Erstellt.
Wählen Sie Taxonomiewerte aus	Gibt die Taxonomiewerte an, die der Taxonomie zugeordnet sind.
Quellwert überschreiben	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Quellwerte für TLP, Konfidenz, Ablauf, Tags und Taxonomien aus den konfigurierten Werten überschreiben möchten. Wenn Sie dieses Kontrollkästchen nicht aktivieren, werden die Standardwerte angewendet.

5. Klicken Sie auf **Next (Weiter)**.
6. Überprüfen Sie die Daten vor der Übermittlung zur Verarbeitung.

Hinweis:
Die Überprüfung importierter Datensätze wird für die STIX-Option nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie auf geklickt haben **Als Nächstes** , Sie können die Zusammenfassung aller Informationen sehen, die der Anwender im obigen Abschnitt angegeben hat, und der folgende Abschnitt enthält alle Datensätze, die importiert werden müssen.

Der Anwender kann jede Art von Aktivitäten ausführen, und mehrere Anwender können über den Kommentarabschnitt zusammenarbeiten, der im rechten Kontextmenü verfügbar ist.

Hinweis:
Alle Datensätze, die die Validierungen nicht bestehen, werden aus dem Importprozess übersprungen, und diese Datensätze werden nicht auf der Seite „Überprüfen und übermitteln“ zur weiteren Verarbeitung angezeigt.

7. Klicken Sie Auf **Aktualisierungstyp** Und wählen Sie den Typ aus, um einen beliebigen Typ der importierten Datensätze zu aktualisieren.
8. Klicken Sie Auf **Löschen** Zum Löschen eines beliebigen Typs der importierten Datensätze.
9. Klicken Sie auf **Absenden**.

Hinweis:

Nachdem Sie den Importdatensatz übermittelt haben, wird der Anwender an den Genehmiger weitergeleitet, um den entsprechenden Importdatensatz basierend auf den konfigurierten Genehmigungsregeln zu genehmigen. Wenn der aktuelle Anwender, der den Datensatz erstellt, den Genehmigungsprozess nicht erfordert, durchläuft der Datensatz den automatischen Genehmigungsprozess. Der Importauftrag wird beim Senden der Anforderung automatisch genehmigt.

10. Klicken Sie Auf **Status Anzeigen** Um den Status des Datensatzes anzuzeigen, oder klicken Sie auf **Fertig** .
    Der Datensatz zeigt den Status „verarbeitet“ an, sobald er verarbeitet wurde.
11. Klicken Sie Auf **Abbrechen** Um den Importprozess abzubrechen.
12. Klicken Sie Auf **Zurück** Um zur vorherigen Seite zurückzukehren und den Datensatz bei Bedarf zu überprüfen.

Importieren Sie Daten mit Rohtext

Importieren Sie die Daten erkennbarer Elemente, indem Sie Rohtext kopieren und einfügen oder den Freitext eingeben.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
   Die Seite „Threat Intel Library“ wird angezeigt.
2. Klicken Sie Auf **Importieren Sie Intelligence** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig:

- Alle freistellenden Zeichen werden als Teil der Analyse und Extraktion erkennbarer Elemente bereinigt.
- Für diese eingefügte Textoption werden nur URL, Domäne, Dateiname, Hashes und IP-Adresse extrahiert, und keine anderen erkennbaren Typen werden für den Datenimport extrahiert. Im Falle eines solchen Typs von erkennbaren Elementen wie Registrierung, Verzeichnistypen werden diese vom Import übersprungen.

3. Klicken Sie Auf **Import aus Rohtext** Karte.

Wichtig:
Beim Importieren der Threat Intelligence-Daten im Rohtextformat sind die Zeichen auf 000 beschränkt. Die Rohtextoption kann als Problemumgehung verwendet werden, um die erkennbaren Elemente aus der PDF-Datei zu extrahieren.

4. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Textfeld für Rohdaten	Geben Sie den Rohtext ein, oder kopieren Sie ihn, und fügen Sie ihn hier in dieses Textfeld ein. **Hinweis:** Sie können den Rohtext nur in 10.000 Zeichen eingeben oder einfügen.
Legen Sie Definitionen fest	
TLP	Wählen Sie den TLP-Indikator aus der Dropdown-Liste aus, der auf die importierten Datensätze angewendet werden soll.
Konfidenz (0-100)	Definieren Sie den Konfidenzwert.
Ablaufzeitraum (in Tagen)	Geben Sie den Ablaufzeitraum für die importierten Datensätze ein. **Hinweis:** Das ist ein Pflichtfeld.
Fügen Sie der Sicherheitssteuerungsliste erkennbare Elemente hinzu	Wählen Sie diese Option aus, um der entsprechenden Sicherheitssteuerungsliste erkennbare Elemente hinzuzufügen. Mit dieser Option können Sie die erkennbaren Elemente beim Importieren direkt einer Sicherheitssteuerungsliste hinzufügen. Die verfügbaren Optionen in der Dropdown-Liste sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Allow-Liste ○ Sperrliste ○ Keine Die Standardoption ist **Keine** .
Tags hinzufügen	Verwenden Sie die Tags, um Anmerkungen oder Ohrmarkendatensätze zu versehen, die aus dieser Quelle in das System aufgenommen wurden. Geben Sie den Tag-Namen in die Suchleiste ein, um die verfügbaren Tags im System auszuwählen, oder geben Sie einen neuen Tag-Namen ein, und klicken Sie auf Hinzufügen, um ihn der Quelle zuzuweisen.
Taxonomie	
Eine Taxonomie auswählen	Wählen Sie die Taxonomie für die importierten Daten aus. Definieren Sie mithilfe von Taxonomien Wörterbücher, die als Taxonomien verwendet werden können, die Threat intel-Datensätzen zugewiesen sind. Beispiel: CAPEC-Nomenklatur. Weitere Informationen finden Sie unter Taxonomien Werden Erstellt.

5. Klicken Sie auf **Next (Weiter)**.
6. Überprüfen Sie die Daten vor der Übermittlung zur Verarbeitung.

   Nachdem Sie auf geklickt haben **Als Nächstes** , Sie können die Zusammenfassung aller Informationen sehen, die der Anwender im obigen Abschnitt angegeben hat, und der folgende Abschnitt enthält alle Datensätze, die importiert werden müssen.

   Der Anwender kann jede Art von Aktivitäten ausführen, und mehrere Anwender können über den Kommentarabschnitt zusammenarbeiten, der im rechten Kontextmenü verfügbar ist.

   Hinweis:
   Alle Datensätze, die die Validierungen nicht bestehen, werden aus dem Importprozess übersprungen, und diese Datensätze werden nicht auf der Seite „Überprüfen und übermitteln“ zur weiteren Verarbeitung angezeigt.

7. Klicken Sie Auf **Aktualisierungstyp** Und wählen Sie den Typ aus, um einen beliebigen Typ der importierten Datensätze zu aktualisieren.
8. Klicken Sie Auf **Löschen** Zum Löschen eines beliebigen Typs der importierten Datensätze.
9. Klicken Sie auf **Absenden**.

   Hinweis:
   Nachdem Sie den Importdatensatz übermittelt haben, wird der Anwender an den Genehmiger weitergeleitet, um den entsprechenden Importdatensatz basierend auf den konfigurierten Genehmigungsregeln zu genehmigen. Wenn der aktuelle Anwender, der den Datensatz erstellt, den Genehmigungsprozess nicht erfordert, durchläuft der Datensatz den automatischen Genehmigungsprozess. Der Importauftrag wird beim Senden der Anforderung automatisch genehmigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Klicken Sie Auf **Status Anzeigen** Um den Status des Datensatzes anzuzeigen, oder klicken Sie auf **Fertig** .
    Der Datensatz zeigt den Status „verarbeitet“ an, sobald er verarbeitet wurde.
11. Klicken Sie Auf **Abbrechen** Um den Importprozess abzubrechen.
12. Klicken Sie Auf **Zurück** Um zur vorherigen Seite zurückzukehren und den Datensatz bei Bedarf zu überprüfen.

Importieren Sie Daten im unstrukturierten Dateiformat

Laden Sie die Daten in einem unstrukturierten Format hoch, das mithilfe von Dateiformaten wie TXT, CSV, JSON, XLS, XLSX unterstützt wird.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
   Die Seite „Threat Intel Library“ wird angezeigt.
2. Klicken Sie Auf **Importieren Sie Intelligence** .

Wichtig:

- Alle freistellenden Zeichen werden als Teil der Analyse und Extraktion erkennbarer Elemente bereinigt.
- Für diese unstrukturierte Dateiformatoption werden nur URL, Domäne, Dateiname, Hashes und IP-Adresse extrahiert, und keine anderen erkennbaren Typen werden für den Datenimport extrahiert. Im Falle eines solchen Typs von erkennbaren Elementen wie Registrierung, Verzeichnistypen werden diese vom Import übersprungen.

3. Klicken Sie Auf **Aus Datei importieren (unstrukturiert)** Karte.

Hinweis:
Beim Importieren der Threat Intelligence-Daten in die unterstützten Dateiformate wie TXT, CSV, STIX 2.x JSON, MISP JSON oder strukturierte Datei die Dateigröße ist auf 5 MB beschränkt.

4. Füllen Sie im Formular die Felder aus.

Feld	Beschreibung
Datei hochladen	Klicken Sie auf diesen Link, um die Daten im Standarddateiformat hochzuladen.
Legen Sie Definitionen fest	
TLP	Wählen Sie den TLP-Indikator aus der Dropdown-Liste aus, der auf die importierten Datensätze angewendet werden soll.
Konfidenz (0-100)	Definieren Sie den Konfidenzwert.
Ablaufzeitraum (in Tagen)	Geben Sie den Ablaufzeitraum der zugehörigen erkennbaren Elemente ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Das ist ein Pflichtfeld.
Fügen Sie der Sicherheitssteuerungsliste erkennbare Elemente hinzu	Wählen Sie diese Option aus, um der entsprechenden Sicherheitssteuerungsliste erkennbare Elemente hinzuzufügen. Mit dieser Option können Sie die erkennbaren Elemente beim Importieren direkt einer Sicherheitssteuerungsliste hinzufügen. Die verfügbaren Optionen in der Dropdown-Liste sind: ○ Allow-Liste ○ Sperrliste ○ Keine Die Standardoption ist **Keine** .
Tags hinzufügen	Verwenden Sie die Tags, um Anmerkungen oder Ohrmarkendatensätze zu versehen, die aus dieser Quelle in das System aufgenommen wurden. Beginnen Sie mit der Eingabe des Tag-Namens in der Suchleiste, um die verfügbaren Tags im System auszuwählen, oder geben Sie einen neuen Tag-Namen ein, und klicken Sie auf **Hinzufügen** Um es der Quelle zuzuweisen.
Taxonomie	
Eine Taxonomie auswählen	Wählen Sie die Taxonomie für die importierten Daten aus. Definieren Sie mithilfe von Taxonomien Wörterbücher, die als Taxonomien verwendet werden können, die Threat Intelligence-Datensätzen zugewiesen sind. Beispiel: CAPEC-Nomenklatur. Weitere Informationen finden Sie unter Taxonomien Werden Erstellt.

5. Überprüfen Sie die Daten vor der Übermittlung zur Verarbeitung.

Nachdem Sie auf geklickt haben **Als Nächstes** , Sie können die Zusammenfassung aller Informationen sehen, die der Anwender im obigen Abschnitt angegeben hat, und der folgende Abschnitt enthält alle Datensätze, die importiert werden müssen.

Der Anwender kann jede Art von Aktivitäten ausführen, und mehrere Anwender können über den Kommentarabschnitt zusammenarbeiten, der im rechten Kontextmenü verfügbar ist.

Hinweis:
Die unterstützten Formate zum Importieren der Daten sind TXT, CSV, JSON, XLS, und alle Datensätze, die die Validierungen fehlschlagen, werden aus dem Importprozess übersprungen, und diese Datensätze werden nicht auf der Seite „Überprüfen und übermitteln“ zur Verarbeitung angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie Auf **Aktualisierungstyp** Und wählen Sie den Typ aus, um einen beliebigen Typ der importierten Datensätze zu aktualisieren.
7. Klicken Sie Auf **Löschen** Zum Löschen eines beliebigen Typs der importierten Datensätze.
8. Klicken Sie auf **Absenden**.

Hinweis:
Nachdem Sie den Importdatensatz übermittelt haben, wird der Anwender an den Genehmiger weitergeleitet, um den entsprechenden Importdatensatz basierend auf den konfigurierten Genehmigungsregeln zu genehmigen. Wenn der aktuelle Anwender, der den Datensatz erstellt, den Genehmigungsprozess nicht erfordert, durchläuft der Datensatz den automatischen Genehmigungsprozess. Der Importauftrag wird beim Senden der Anforderung automatisch genehmigt.

9. Klicken Sie Auf **Status Anzeigen** Um den Status des Datensatzes anzuzeigen, oder klicken Sie auf **Fertig** .
   Der Datensatz zeigt den Status „verarbeitet“ an, sobald die Übermittlung erfolgreich war.
10. Klicken Sie Auf **Abbrechen** Um den Importprozess abzubrechen.
11. Klicken Sie Auf **Zurück** Um zur vorherigen Seite zurückzukehren und den Datensatz bei Bedarf zu überprüfen.

Analyst Workbench für Bedrohungen

Die Seite „Workbench für Bedrohungsanalysen“ besteht aus Fällen und Fallaufgaben, die Bedrohungsanalysten und deren Team unterstehen.

Verwenden Sie **Fallmanagement** Funktion zum Erstellen und Nachverfolgen von Bedrohungsuntersuchungen und -Analyseaktivitäten.

Während der Bedrohungsuntersuchungen erfassen die Analysten die Daten aus internen Intelligence-Datensätzen wie erkennbaren Elementen, Bedrohungsakteuren, Kampagnen usw.

Workbench – Übersicht

Die Seite „Workbench-Übersicht“ besteht aus den Fallaufgaben und Fällen, die Analysten der Bedrohung ausgesetzt sind, und ihrem Team.

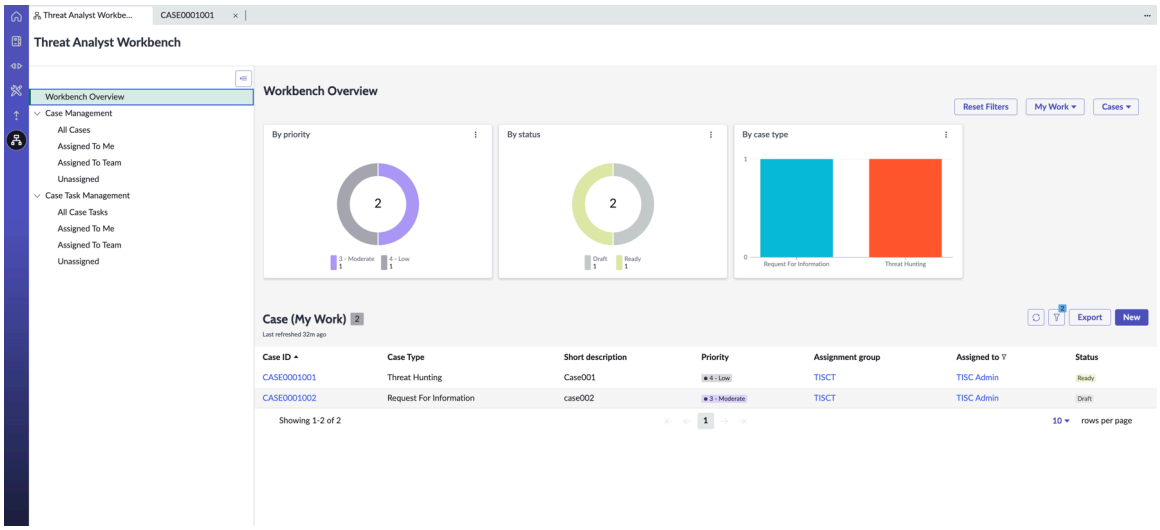
Die Übersicht listet alle offenen Fälle und ihren Status auf, was den Analysten hilft, ihre Arbeitsauslastung zu verwalten und ihre Untersuchungen zu priorisieren.

Erforderliche Rolle: sn_sec_tisc.Analyst, sn_sec_tisc.admin

Nachdem der Fall erstellt wurde, weisen die Analysten die Fallaufgaben dann anderen Analysten oder Teams zu, um weitere Untersuchungen durchzuführen, und arbeiten auch mit ihnen zusammen, um Informationen und Einblicke zu teilen.

Unter jedem Filter sind verschiedene Widgets vorhanden, gruppiert nach Priorität, Status und Falltyp, die sich in den Warteschlangen der Bedrohungsanalysten und des Bedrohungsanalystenteams befinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Filter auf die Widgets angewendet werden, wird die untere Hälfte der Übersichtsseite mit den entsprechenden Fällen oder Fallaufgaben als Listenelemente gefüllt. Klicken Sie auf , um die angewendeten Filter zu entfernen **Filter Zurücksetzen** Um sie auf die ursprüngliche Ansicht zurückzusetzen.

Auf dieser Seite können die Bedrohungsanalysten und Administratoren ihre Arbeit, ihre Teamarbeit und alle nicht zugewiesenen Arbeiten anzeigen. Sie können zur Dropdown-Liste navigieren. Verfügbare Optionen:

- Meine Arbeit: Wählen Sie diese Option aus, um die Ihnen zugewiesene Arbeit anzuzeigen.
- Arbeit meines Teams: Wählen Sie diese Option aus, um die Arbeit Ihres Teams anzuzeigen, die allen Gruppen zugewiesen ist, denen Sie angehören.
- Nicht zugewiesene Arbeit: Wählen Sie diese Option aus, um den Fall oder die Fallaufgabe anzuzeigen, die nicht zugewiesen sind. Um den Fall oder die Fallaufgabe zuzuweisen, müssen Sie zur Formularansicht wechseln und den/die Anwender oder Anwendergruppen dem Fall und der Fallaufgabe(n) zuweisen.

Sie können auch Fälle und Fallaufgaben direkt aus der Workbench-Übersicht anzeigen, die Ihnen zugewiesen sind. Standardmäßig wird die Fallansicht angezeigt. Sie können die Dropdown-Liste verwenden und die Fallaufgaben auswählen, wenn Sie die Fallaufgaben nach Priorität und Status anzeigen möchten.

Erstellen von Fällen mit der Workbench für Bedrohungsanalysen

Fälle werden verwendet, um Informationen zu einer Kampagne oder einem Bedrohungsakteur nachzuverfolgen, der Ihre Organisation bedroht. Nachdem ein Fall erstellt wurde, können Sie Artefakte hinzufügen, mit denen Sie alle zugehörigen Informationen aus einem einzelnen Fall oder einer Fallaufgabe überprüfen und analysieren können.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst, sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Alle Fälle werden angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder entsprechend aus.

Neuen Fall erstellen

Feld	Beschreibung
Fall-ID	Ein eindeutiger Bezeichner für den Fall. Dies ist eine vom System generierte ID.
Kurzbeschreibung	Zusammenfassung der Anforderung oder des Problems, die bzw. das untersucht wird, oder eine kurze Beschreibung.
Beschreibung	Eine detaillierte Beschreibung mit allen relevanten Informationen zum Fall, z. B. Hintergrund, erforderliche Analyse, erwartete Ergebnisse.
Falltyp	Wählen Sie den Typ des untersuchten Falls aus. Die möglichen Optionen für die Untersuchung sind: ○ Bedrohungssuche ○ Informationsanforderung ○ Schwachstellenmanagement-Fall ○ Compliance-Fall ○ Fall vom Typ „Reaktion auf Incidents“ ○ Zusammenarbeitsfall ○ Andere
Priorität	Eine Bewertung des Schweregrads der Anforderung oder des Problems.
Zuweisungsgruppe	Die zugewiesene Gruppe, die für die Bearbeitung des Falls verantwortlich ist.
Status	Der aktuelle Status des Falls.
Zugewiesen an	Der Analyst, der für die Bearbeitung eines Falls verantwortlich ist.
Fälligkeitsdatum	Datum und Uhrzeit, zu der die Aufgabe abgeschlossen oder geschlossen werden soll.
Beitragende	Die Liste der Beauftragten, die aus Aufgaben zusammengefasst werden und darüber hinzugefügt werden können.
TLP	Eindeutiger Wert, der die Einstellung für die Datensensibilität pro TLP angibt.
Beobachtungsliste	Wenn ein Anwender der Beobachtungsliste hinzugefügt wird, erhält die Person E-Mail-Benachrichtigungen über Änderungen an Status und Priorität.
Beschränkung erzwingen	Aktivieren Sie dieses Kontrollkästchen, um Mitglieder der zulässigen Gruppe und der zulässigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Mitglieder zu ändern. Weitere Informationen finden Sie unter Erzwungene Einschränkungen für Fälle.

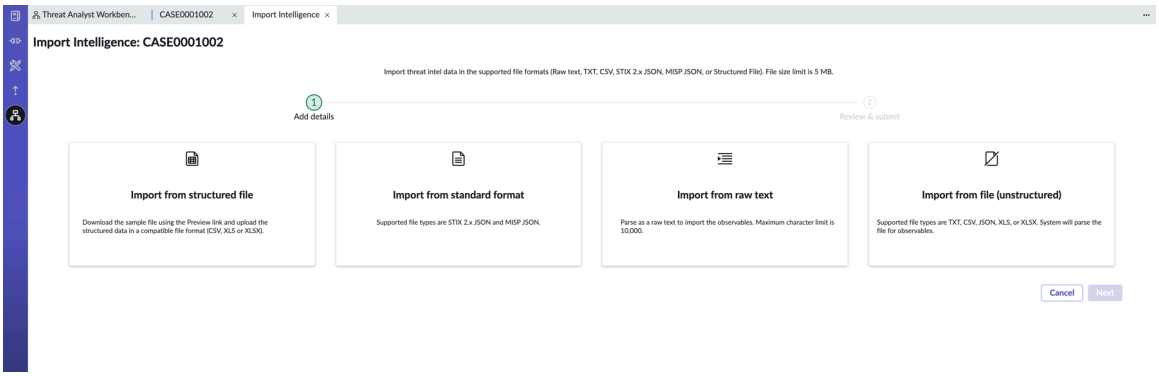
6. Füllen Sie die Felder im Abschnitt „Einblicke“ entsprechend aus.

Einblicke

Feld	Beschreibung
Notizen	Alle zusätzlichen Notizen im Zusammenhang mit der Bedrohungsuntersuchung.
Empfehlungen oder Aktionen	Alle Empfehlungen oder Aktionen im Zusammenhang mit der Bedrohungsuntersuchung.
Analyse und Ergebnisse	Geben Sie die Analyse und Ergebnisse im Zusammenhang mit der Bedrohungsuntersuchung ein.
Abschlusszusammenfassung	Fügen Sie die Abschlusszusammenfassung der Ergebnisse hinzu.

7. Klicken Sie auf **Speichern**.
Nachdem der Datensatz gespeichert wurde, können Sie auf klicken **Importieren Sie Intelligence** Registerkarte zum Importieren der Threat Intelligence-Daten mit **Importieren Sie Intelligence** Funktion.

Hinweis:
Wenn Sie Daten aus Fallmanagement importieren und verarbeiten, wird dem Importdatensatz ein eindeutiges Element zugeordnet.



Erzwungene Einschränkungen für Fälle

Verwenden Sie diese Funktion, um einen Fall einzuschränken und eine Liste der Gruppen und Anwender bereitzustellen, die darauf zugreifen können.

Erforderliche Rolle:

- sn_sec_tisc.Analyst
- sn_sec_tisc_admin
- sn_sec_tisc.Restriction_Access_Manager

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtige Überlegungen

1. Schränken Sie einen Fall ein, und geben Sie eine Liste der Gruppen/Anwender an, die darauf zugreifen können.
2. Aktivieren Sie das Feld „Einschränkung erzwingen“ auf der Fallformularseite.
3. Ändern Sie Mitglieder der zulässigen Gruppe und der zulässigen Mitglieder.
4. Sobald ein Fall als eingeschränkt markiert wurde, können nur Mitglieder zulässiger Gruppen, Mitglieder der Liste zulässiger Anwender und Anwender mit der Rolle „sn_sec_tisc.admin“ auf diesen Fall zugreifen.
5. Gewähren Sie dem Analysten (sn_sec_tisc.restriction_Access_Manager mit dieser Rolle) Zugriff, der Zugriff auf das Feld „Einschränkung erzwingen“ benötigt.
6. Vorhandene Assigned_to-Analysten und -Analysten, die sie als eingeschränkt markiert haben, verlieren auch den Zugriff, wenn sie nicht den zulässigen Gruppen oder Mitgliedern hinzugefügt werden.
7. Die Einschränkung des Falls innerhalb des CTI-Teams wird pro Fall implementiert. Zulässige Mitglieder können auf eingeschränkte Fälle zugreifen, wenn sie sich in der zulässigen Liste befinden. Wenn Sie sie in eine der zulässigen Fälle setzen, bedeutet dies nicht, dass sie auf alle anderen eingeschränkten Fälle zugreifen können.
8. Wenn der Fall als eingeschränkt markiert ist und zulässige Mitglieder oder zulässige Gruppe leer gelassen werden, kann nur sn_sec_tisc.admin auf diese eingeschränkten Fälle zugreifen.
9. Nur die Gruppen, denen die Rolle „Analyst“ (sn_sec_tisc.Analyst) zugewiesen ist, sind in der Liste „zulässige Mitglieder“ und „zulässige Gruppen“ zulässig.

Hinweis:
Eine Arbeitsnotiz wird veröffentlicht, wenn ein Fall als eingeschränkt markiert ist.

Zugriffssteuerungen für einen Fall

Zugriffssteuerungen zulassen, die für einen Fall spezifisch sind.

In der folgenden Tabelle werden die Rollen und Zugriffssteuerungen beschrieben.

Rolle	Zugriff	Beschreibung
sn_sec_tisc.Restriction_Access_Manager	Lesezugriff	Externe Anwender, die hier hinzugefügt werden, erhalten Zugriff zum Anzeigen des Fallformulars, können jedoch kein Feld im Fall bearbeiten oder Aktionen ausführen.
	Privilegierter Zugriff	Externe Anwender, die hier hinzugefügt werden, erhalten Zugriff zum Bearbeiten eines Felds im Fallformular, dürfen jedoch keine Orchestrationen ausführen.
sn_sec_tisc.special_Access_read_Manager	Lesezugriff	Externe Anwender, die hier hinzugefügt werden, erhalten Zugriff zum Anzeigen des Fallformulars, können jedoch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Zugriff	Beschreibung
		kein Feld im Fall bearbeiten oder Aktionen ausführen.
sn_sec_tisc.special_Access_write_Manager	Privilegierter Zugriff	Externe Anwender, die hier hinzugefügt werden, erhalten Zugriff zum Bearbeiten eines Felds im Fallformular, dürfen jedoch keine Orchestrationen ausführen.

Externer Anwenderzugriff für Fallaufgaben

In diesem Abschnitt wird der externe Anwenderzugriff für Fallaufgaben beschrieben.

Zuweisung von Fallaufgaben an externe Anwender

Fallaufgaben werden den Anwendern mit der externen Rolle zugewiesen, auch wenn sie keinen Zugriff auf die Rolle „sn_sec_tisc.Analyst“ haben.

1. Jeder externe Anwender, der einer Fallaufgabe zugewiesen ist, kann nur das Fallaufgabenmodul anzeigen und hat die Berechtigung zum Bearbeiten der Fallaufgabe.
2. Der externe Anwender kann nur die Fallaufgaben anzeigen, die diesem bestimmten Anwender oder den Gruppen zugewiesen sind, denen der Anwender angehört.
3. Der externe Anwender sollte die Aufgabe innerhalb der Gruppe, der der Anwender angehört, neu zuweisen können.

Ordnen Sie einem Fall MITRE-Techniken zu

Ordnen Sie einem Fall eine oder mehrere MITRE-Techniken zu.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen beliebigen Fall aus.
5. Klicken Sie Auf **MITRE-Technik zuordnen** Schaltfläche.
6. Klicken Sie Auf **Fügen Sie Matrix Hinzu** Zum Zuordnen der MITRE-Technik.
   Die **MITRE-Technik dem Fall zuordnen** Dialogfeld wird angezeigt.
7. Wählen Sie aus **Matrix** .
   Alle aktivierten Matrizen werden angezeigt, damit Sie die Matrix auswählen können.
8. Wählen Sie die Taktik aus den Dropdown-Listen aus.
   Alle Taktiken, die einer Matrix zugeordnet sind, werden angezeigt.

Hinweis:
Wenn Sie weitere Taktiken hinzufügen möchten, klicken Sie auf **Fügen Sie Taktik Hinzu** . Die zuvor ausgewählten Taktiken werden nicht mehr in der Dropdown-Liste angezeigt, wenn Sie eine neue Taktik hinzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Wählen Sie aus **Technik** .
   Alle Techniken, die Ihrer ausgewählten Taktik zugeordnet sind, werden angezeigt. Wenn Sie weitere Taktiken hinzufügen, können Sie die zugehörigen Techniken für diese ausgewählten Taktiken auswählen.
10. Klicken Sie auf **Speichern**.
    Wenn Sie die gesamten zugeordneten Matrixdaten löschen möchten, klicken Sie auf **Löschen Sie Die Matrix** , Diese Aktion entfernt nur die zugehörigen Matrixdaten, die Matrix verbleibt jedoch im MITRE ATT&CK-Repository.

    Der zugehörige Matrixdatensatz wird im Abschnitt „MITRE ATT&CK-Karte“ angezeigt. In der Kartenansicht:

    Hinweis:
    Sie können in der Dropdown-Liste Matrix zwischen mehreren Matrizen wechseln.

    a. In der ersten Zeile der Kartenansicht werden alle Taktiken angezeigt, die der aktuell ausgewählten Matrix zugeordnet sind.
    b. Jede Taktikkarte zeigt den Taktiknamen und die Anzahl der Techniken dieser Taktik an, die dem aktuellen Falldatensatz zugeordnet sind.
    c. Alle diesem Fall zugeordneten Techniken werden unter jeder Taktik vertikal angezeigt. Sie können auf eine beliebige Technik klicken, um die Formularansicht Technik anzuzeigen.
11. Klicken Sie Auf **ID anzeigen** Zeigt die IDs für alle zugehörigen Techniken an.

    Hinweis:
    Jede Technikkarte zeigt den Techniknamen und die Technik-ID nur dann an, wenn **ID anzeigen** Ist aktiviert.

12. Klicken Sie Auf **Aktualisieren** Zum Aktualisieren der Kartenansicht.
    Sie können den Zeitstempel der letzten Aktualisierung für die ausgewählte Matrix anzeigen.

    Hinweis:
    Klicken Sie auf das Popout-Symbol, um die zugehörige Matrixkarte auszublenden, um sie auf einer neuen Registerkarte anzuzeigen.

Rollup von MITRE-Technikzuordnungen

Rollup von MITRE-Technikzuordnungen aus erkennbaren Elementen, Indikatoren, Objekten und Security Incidents, die mit einem Falldatensatz verknüpft oder nicht verknüpft sind.

Vorbereitungen

Hinweis:

- Ein Rollup von MITRE-Technikzuordnungen für Security Incidents führt ein Rollup der MITRE-Technik zugeordneten Daten aus Security Incidents zum Fallmanagement in TISC durch.
- Standardmäßig ist diese Eigenschaft sn_sec_tisc.auto_rollup_mitre_data aktiviert, damit die MITRE-Technik(en) automatisch zu Fällen aus den zugehörigen Objekten oder Security Incidents zusammengefasst wird.
- Wenn Sie bei Bedarf ein Rollup von MITRE-Technikzuordnungen durchführen möchten, navigieren Sie zu den weiteren Aktionen in **Fallformularansicht** Und wählen Sie aus **Rollup der MITRE-Techniken** Option. Dieser Vorgang wird asynchron ausgeführt, und Sie können überprüfen **Aktivitätenstrom** Abschnitt für die Updates der Rollup-Aktivität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_sec_tisc.Analyst

Warum und wann dieser Vorgang ausgeführt wird

- Immer wenn eine Entität wie ein erkennbares Element oder ein Indikator mit einem Fall verknüpft ist, werden alle Zuordnungen der MITRE-Technik, die für diese Entität vorhanden sind, automatisch für den Fall zusammengefasst.
- Wenn eine Entität wie ein erkennbares Element oder ein Indikator getrennt und aus dem Fall entfernt wird, werden alle Zuordnungen der MITRE-Technik, die aus dem Fall zusammengefasst werden und für diese Entität vorhanden sind, automatisch entfernt und für den Fall zusammengefasst.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Alle Fälle werden angezeigt.
4. Öffnen Sie einen beliebigen Fall.
5. Wechseln Sie zu **Artefakte** Registerkarte.
6. Wählen Sie Aus **Erkennbare Elemente** Aus der zugehörigen Liste Artefakte.
7. Wählen Sie aus **Link** Schaltfläche.
8. Wählen Sie die erkennbaren Elemente aus, die Sie mit dem Fall verknüpfen möchten.
9. Klicken Sie Auf **Link** Zum Verknüpfen der erkennbaren Elemente.
   Nachdem Sie die erkennbaren Elemente mit einem Fall verknüpft haben, werden die für dieses bestimmte erkennbare Element zugeordneten MITRE-Techniken automatisch zusammengefasst, und die Listenanzahl der MITRE-Techniken im Abschnitt „Artefakte“ wird automatisch aktualisiert.
10. Klicken Sie Auf **Verknüpfung Aufheben** Um die Verknüpfung der erkennbaren Elemente mit dem Fall aufzuheben.
    Nachdem Sie die Verknüpfung der erkennbaren Elemente mit einem Fall aufgehoben haben, werden die für dieses bestimmte erkennbare Element zugeordneten MITRE-Techniken automatisch entfernt, und die Listenanzahl der MITRE-Techniken im Abschnitt „Artefakte“ wird automatisch aktualisiert.

Erstellen einer Fallaufgabe mit der Workbench für Bedrohungsanalysen

Erstellen Sie Fallaufgaben, die mit Fällen verknüpft werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst, sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallaufgabenmanagement** > **Alle Fallaufgaben**an.
   Alle Fallaufgaben werden angezeigt.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Eine Neue Fallaufgabe

Feld	Beschreibung
Aufgaben-ID	Ein eindeutiger Bezeichner für die Fallaufgabe. Dies ist eine vom System generierte ID.
Kurzbeschreibung	Zusammenfassung der Anforderung oder des Problems, die bzw. das untersucht wird, oder eine kurze Beschreibung.
Beschreibung	Eine detaillierte Beschreibung mit allen relevanten Informationen zur Fallaufgabe, z. B. Hintergrund, erforderliche Analyse, erwartete Ergebnisse.
ID des übergeordneten Falls	Wählen Sie die ID des übergeordneten Falls aus der Suche aus.
Priorität	Eine Bewertung des Schweregrads der Anforderung oder des Problems.
Zuweisungsgruppe	Die zugewiesene Gruppe, die für die Bearbeitung der Fallaufgabe verantwortlich ist.
Status	Der aktuelle Status der Fallaufgabe.
Zugewiesen an	Der Analyst, der für die Arbeit an einer Fallaufgabe verantwortlich ist.
Fälligkeitsdatum	Datum und Uhrzeit, zu der die Fallaufgabe abgeschlossen oder geschlossen werden soll.
TLP	Eindeutiger Wert, der die Einstellung für die Datensensibilität pro TLP angibt.
Beschränkung erzwingen	Aktivieren Sie als sn_sec_tisc_admin dieses Kontrollkästchen, um Mitglieder der zulässigen Gruppe und der zulässigen Mitglieder zu ändern. Weitere Informationen finden Sie unter Erzwungene Einschränkungen für Fälle.

6. Füllen Sie die Felder im Abschnitt „Einblicke“ entsprechend aus.

Einblicke

Feld	Beschreibung
Notizen	Alle zusätzlichen Notizen im Zusammenhang mit der Bedrohungsuntersuchung.
Abschluss	Fügen Sie die Abschlusszusammenfassung der Ergebnisse hinzu.

7. Klicken Sie auf **Speichern**.
   Ihre Fallaufgabe wird Ihrem Fall zugeordnet.

Hinweis:
Nach dem Speichern der Fallaufgabe können Sie der Aufgabe Tags und Taxonomien hinzufügen. Weitere Informationen finden Sie unter Taxonomien Werden Erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeiten mit Untersuchungs-Canvas

Die Untersuchungs-Canvas ist eine wichtige Funktion, die den Analysten von Threat Intelligence (TI) wertvolle Informationen bereitstellt. Es bietet ein strukturiertes Framework, indem eine zu einer oder eine zu viele Beziehungen zugeordnet und Informationen im Zusammenhang mit erkennbaren Elementen, Indikatoren der Kompromittierung (Indicators of Commitment, IOCs) oder Entitäten visualisiert werden.

Mithilfe der Untersuchungs-Canvas können Bedrohungsanalysten effektiv:

- **Beziehungen Zuordnen** : Visualisieren Sie Knotenverbindungen zwischen verschiedenen Entitäten wie erkennbaren Elementen, Indikatoren der Gefährdung (IOCs), Bedrohungsakteuren, Angriffsmustern, betroffenen Assets und mehr. Jedes Objekt in der Untersuchungs-Canvas wird zusammen mit Objekttyp, Knotentyp und Status durch eine bestimmte Farbe dargestellt. Der Status spiegelt die Reputation des Objekts wider, z. B. **Verdächtig** , **Niedrig** , Oder **Kritisch** Für erkennbare Elemente und andere Objekttypen. Indikatoren werden mit dem zugehörigen Bedrohungsschweregrad angezeigt, um die Analyse zu priorisieren.
- **Verknüpfen Sie Fälle oder Canvase** : Verknüpfen Sie einen Fall oder eine Canvas, um die Analyse zu verbessern und einen umfassenderen Überblick über die Bedrohungslandschaft im Fallmanagement zu erhalten.
  - Mit der Verknüpfungsfunktion können Analysten Knoten dynamisch hinzufügen oder entfernen. Dadurch werden auch die vorhandenen Beziehungen zwischen den Knoten zum Canvas ausgefüllt.
  - Temporäre Beziehungsdiagramme, indem Beziehungen separat im Kontext der Untersuchungs-Canvas gespeichert werden.
- **MITRE-Technikzuordnungen** : Zuordnen oder Entfernen Sie MITRE-Techniken zu Knoten direkt auf der Canvas, und stellen Sie eine Analyse auf der MITRE-Kill Chain-Karte bereit.

Einstiegspunkte für die Untersuchungs-Canvas

1. **Erster Einstiegspunkt: Neuer leerer Canvas** : Dieser Einstiegspunkt sollte es den Analysten ermöglichen, eine neue und leere Canvas ohne Knoten oder Links zu öffnen.
2. **Zweiter Einstiegspunkt: Öffnen Sie Canvas in der Falluntersuchung** :
   a. Dieser Einstiegspunkt öffnet einen vorhandenen Untersuchungsfall und ermöglicht das Bearbeiten, Ändern und Umbenennen des Canvas.
   b. Eine neue Canvas mit vorhandenen Artefakten als Knoten.

Arbeiten mit Aktionen im Untersuchungs-Canvas

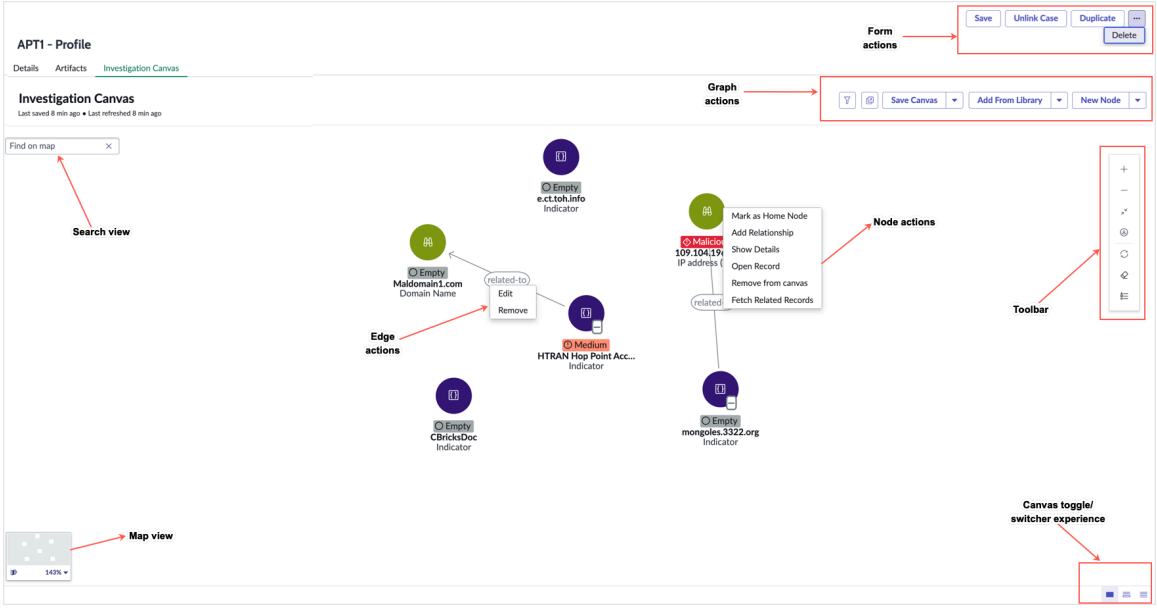
In diesem Abschnitt werden die verschiedenen Aktionen beschrieben, die Sie im Untersuchungs-Canvas ausführen können.

Untersuchungs-Canvas enthält:

1. Formularaktionen
2. Diagrammaktionen
3. Knotenaktionen
4. Edge-Aktionen
5. Symbolleistenaktionen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchungs-Canvas



Aktionen des Untersuchungs-Canvas-Formulars

Aktion	Vorgang
Fall verknüpfen	Ermöglicht das Verknüpfen von Fällen im Untersuchungs-Canvas.
Verknüpfung mit Fall aufheben	Ermöglicht Ihnen, die Verknüpfung des Falls im Untersuchungs-Canvas aufzuheben.
Speichern	Option zum Speichern des Falldatensatzes.
Duplikat	Option zum Duplizieren der Knoten im Untersuchungs-Canvas.
Löschen	Option zum Löschen des Canvas.

Aktionen des Untersuchungs-Canvas-Diagramms

Aktion	Vorgang
Auf Karte suchen	Ermöglicht Ihnen die Suche durch verschiedene Knoten und Edges.
Canvas-Filter	Die **Filter** Die Funktionalität hilft Ihnen, Ihre Ansicht im Untersuchungs-Canvas zu verfeinern. Wenn Sie beispielsweise einen Datensatztyp wie Kampagne herausfiltern, wird er vorübergehend aus der Canvas-Anzeige entfernt. Durch Anwenden von Filtern können Sie steuern, welche Arten von Entitäten oder Datensätzen auf der Karte angezeigt werden, was eine bereinigte und fokussiertere Untersuchungs-Experience ermöglicht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen des Untersuchungs-Canvas-Diagramms (Fortsetzung)

Aktion	Vorgang
	Hinweis: Verwenden Sie Filter, um nur die relevantesten Knoten wie erkennbare Elemente oder Bedrohungsakteure hervorzuheben und gleichzeitig weniger kritische Informationen im Canvas vorübergehend auszublenden.
Canvas speichern	Ermöglicht das Speichern des Untersuchungs-Canvas.
Fügen Sie der Bibliothek Daten hinzu	Mit dieser Option können Sie eine neue Beziehung zwischen zwei verschiedenen Knoten im Untersuchungs-Canvas herstellen. Alle am Canvas vorgenommenen Änderungen, einschließlich der neuen Knoten, neuen Links zwischen Knoten und allen bearbeiteten oder geänderten Edge-Bezeichnungen, werden in der Bibliothek gespeichert. Alle derzeit im Canvas vorhandenen Knoten werden dem verknüpften Fall als Artefakte hinzugefügt. Eine Bestätigungsnachricht wird angezeigt, sobald die Daten erfolgreich in der Bibliothek gespeichert wurden.
Aus Bibliothek hinzufügen	Mit dieser Aktion werden die Daten der Threat Intelligence-Bibliothek hinzugefügt und auch die Beziehung zwischen dem neuen Knoten hergestellt, der aus der Threat Intelligence-Bibliothek importiert wurde, und den vorhandenen Knoten im Untersuchungs-Canvas.
Aus Fallartefakten hinzufügen	Ermöglicht Ihnen das Hinzufügen von Daten aus entsprechenden Fallartefakten, die mit dem Canvas verknüpft sind.

Aktionen des Untersuchungs-Canvas-Knotens

Aktion	Vorgang
Als Startknoten markieren	Mit dieser Option können Sie einen bestimmten Knoten als Startknoten im Untersuchungs-Canvas markieren. Beim Drehen während der Analyse hebt die Anwendung den Startknoten automatisch hervor und zentriert ihn, sodass er in der Mitte des Canvas fokussiert wird. Der fokussierte Knoten wird visuell hervorgehoben durch:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen des Untersuchungs-Canvas-Knotens (Fortsetzung)

Aktion	Vorgang
	• Ein eindeutiger Rahmen • Hervorhebung • Eine subtile kreisförmige Bewegungsanimation Dies erleichtert die Identifizierung und Untersuchung der Canvas-Daten im Zusammenhang mit dem primären Fokus Ihrer Untersuchung.
Beziehung hinzufügen	Mit dieser Option können Sie anwenderdefinierte Beziehungen zwischen Knoten im Untersuchungs-Canvas hinzufügen. Sie können Beziehungstypen definieren, z. B.: • Eins-zu-viele • N:1 • Viele-zu-viele Dies hilft bei der Darstellung komplexer Zuordnungen zwischen Entitäten.
Details anzeigen	Mit dieser Option können Sie detaillierte Informationen zum ausgewählten Knoten im Untersuchungs-Canvas anzeigen, einschließlich seiner Attribute und aller zugehörigen erkennbaren Elemente oder Beziehungen.
Datensatz öffnen	Mit dieser Option können Sie den ausgewählten Datensatz in einer neuen Browserregisterkarte öffnen, um das Referenz- und Multitasking zu erleichtern.
Aus Canvas entfernen	Mit dieser Option können Sie den ausgewählten Knoten aus der Untersuchungs-Canvas entfernen und ihn effektiv aus der aktuellen Ansicht löschen.
Rufen Sie Zugehörige Datensätze Ab	Mit dieser Option können Sie zugehörige Datensätze für einen bestimmten Knoten abrufen und sie direkt dem Untersuchungs-Canvas mit hinzufügen **Wählen Sie Entitätstypen Aus** Dialogfeld. Wählen Sie Aus **Alle Hinzufügen** Option zum automatischen Einbeziehen aller objektbezogenen Datensatztypen in das angegebene Auswahlfeld. Wenn es beispielsweise 5 bis 10 verschiedene Arten zugehöriger Datensätze gibt, müssen Sie jeden Objekttyp manuell auswählen. Die **Alle Hinzufügen** Die Funktion optimiert diesen Prozess, indem alle relevanten Datensätze gleichzeitig ausgefüllt werden, was die Anwender-Experience

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen des Untersuchungs-Canvas-Knotens (Fortsetzung)

Aktion	Vorgang
	verbessert. Nachdem Sie Datensätze hinzugefügt haben, können Sie sie entfernen oder auswählen **Erweitern Sie** Option zum Anzeigen der zugehörigen Knoten. Um die Anwenderfreundlichkeit zu verbessern, können Sie jetzt auswählen **Erweitern Sie Alle** Um alle zugehörigen Datensätze, die mit einem Knoten verknüpft sind, sofort zu erweitern, anstatt die Datensätze manuell hinzuzufügen oder zu erweitern.

Canvas Edge-Aktionen für Untersuchung

Aktion	Vorgang
Bearbeiten	Mit dieser Option können Sie die Bezeichnung eines Edge auf der Untersuchungs-Canvas bearbeiten und ändern, um eine klarere Darstellung von Beziehungen zwischen Knoten zu ermöglichen.
Entfernen	Mit dieser Option können Sie einen Edge aus der Untersuchungs-Canvas entfernen und die visuelle Verbindung zwischen zwei Knoten effektiv löschen.

Symbole der Symbolleiste „Untersuchungs-Canvas“

Aktion	Vorgang
Vergrößern	Option zum Vergrößern der Untersuchungs-Canvas, um sich leicht auf bestimmte Bereiche der Canvas zu konzentrieren.
Verkleinern	Option zum Verkleinern der Untersuchungs-Canvas, um sich leicht auf bestimmte Bereiche der Canvas zu konzentrieren.
An Bildschirm anpassen	Option zum Anpassen der Untersuchungs-Canvas an die Bildschirmgröße.
Karte exportieren	Option zum Exportieren der Untersuchungs-Canvas als PDF zur besseren Anzeige.
Neu laden	Die **Aktualisieren** Mit der Option können Sie die Daten aus der Bibliothek aktualisieren und neu in die Untersuchungs-Canvas laden.

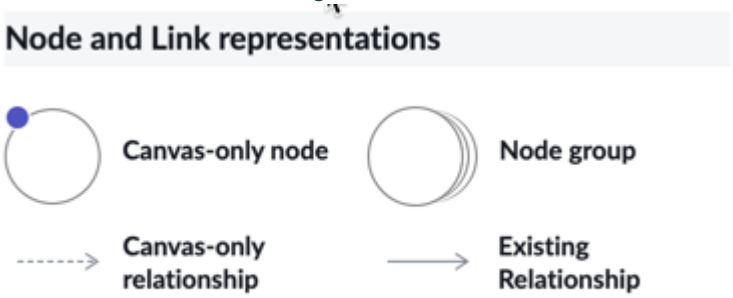
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symbole der Symbolleiste „Untersuchungs-Canvas“ (Fortsetzung)

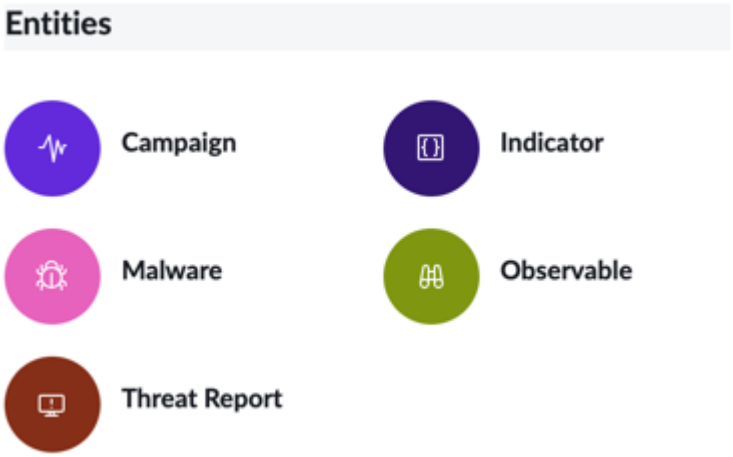
Aktion	Vorgang
	Hinweis: Alle nicht gespeicherten Änderungen im Canvas gehen verloren, wenn Sie aktualisieren, ohne zu speichern. Es wird empfohlen, Ihren Canvas vor der Aktualisierung zu speichern, um Datenverlust zu vermeiden.
Canvas löschen	Ermöglicht das Löschen der Canvas. Mit dieser Auswahl werden die Knoten vorübergehend aus dem Untersuchungs-Canvas entfernt. Eine Bestätigungsnachricht wird angezeigt, die Sie auffordert, zu bestätigen, ob Sie den Canvas löschen möchten. Bestätigen Sie die Nachricht, um fortzufahren. **Hinweis:** Nachdem Sie Änderungen am Untersuchungs-Canvas vorgenommen haben, müssen Sie dies tun **Speichern** Die Canvas. Wenn die Änderungen nicht gespeichert werden und Sie den Canvas aktualisieren, wird er in den vorherigen Status zurückgesetzt, und alle nicht gespeicherten Knoten oder Änderungen gehen verloren.
Legende	Diese Option bietet eine visuelle Darstellung der Knoten und Entitäten, die derzeit im Untersuchungs-Canvas angezeigt werden. Die Legende enthält zwei wichtige Ansichten: • **Knoten- und Linkdarstellung** : Zeigt an, wie verschiedene Knotentypen auf dem Canvas angezeigt werden und wie sie über Edges verbunden sind. Dies hilft Ihnen, die Struktur und die Beziehung zwischen verschiedenen Elementen in der Untersuchung schnell zu verstehen. • **Entitätsdarstellung** : Zeigt die Typen von Entitäten an, die derzeit im Canvas vorhanden sind (erkennbare Elemente, Indikatoren und Objekte). Im Folgenden werden die Legenden für Knoten-, Link- und Entitätsdarstellungen veranschaulicht:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Knoten- und Linkdarstellung



Entitätsdarstellung



Gruppieren oder Aufheben der Gruppierung von Datensätzen aus Untersuchungs-Canvas

Mit der Gruppenfunktion können Sie Knoten gruppieren, um die Analyse zu erleichtern. Eine Gruppierungsschaltfläche wurde neben Knoten hinzugefügt, die gruppiert werden können. Standardmäßig zeigt diese Schaltfläche ein Minus-Symbol (–) auf der Canvas an, das angibt, dass der verbundene Knoten reduziert oder gruppiert werden kann.

Jeder Outgrade-Knoten wird für eine Gruppe berücksichtigt.

Hinweis:
Das Gruppensymbol wird eingeführt, um Unordnung auf der Canvas zu reduzieren und die Navigation bei kritischen Untersuchungen zu vereinfachen. Für Knoten ohne zusätzliche Edges (Verbindungen) wird die Gruppierungsschaltfläche nicht angezeigt, da keine zugehörigen Knoten für die Gruppe verfügbar sind.

In der folgenden Tabelle werden die Richtlinien beim Gruppieren oder Aufheben der Gruppierung der Knoten erläutert:

Aktion	Ergebnis
Gruppieren eines Knotens	• Alle untergeordneten Knoten mit nur einem übergeordneten Knoten (auch auf mehreren Ebenen) werden innerhalb der Gruppe ausgeblendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Ergebnis
	• Knoten mit mehreren übergeordneten Elementen bleiben sichtbar, Verbindungen von der Gruppe zu ihnen werden jedoch ausgeblendet.
Gruppierung eines Knotens aufheben	• Zeigt alle zuvor ausgeblendeten Knoten mit einem übergeordneten Element und ihren Verbindungen an. • Wenn Knoten mit mehreren übergeordneten Elementen bereits sichtbar waren, werden auch ihre ausgeblendeten Verbindungen wiederhergestellt.
Knoten wird importiert/zugehörige Datensätze abrufen	Erweitert automatisch eine reduzierte Gruppe, wenn der neue Knoten eine Verbindung zu einem ausgeblendeten Knoten in ihm herstellt.
Zulässige Aktionen	Gruppierte Knoten unterstützen nur **Details Anzeigen** Aktion, die Details des übergeordneten Knotens anzeigt. Andere Aktionen sind deaktiviert.
Filter	Filterung **Nicht gruppierte Knoten** Folgt dem standardmäßigen Filterverhalten und respektiert dennoch Gruppierungsregeln. Filtern von **Gruppierter Knoten** Blendet die gesamte Gruppe und ihren untergeordneten Knoten aus.
Andere Aktionen	Aktionen wie das Entfernen eines Knotens oder das Ändern von Edges folgen allen Gruppierungsregeln und -Verhaltensweisen.

Verknüpfen eines vorhandenen Falls aus Untersuchungs-Canvas

Verwenden Sie diesen Abschnitt, um einen vorhandenen Fall aus dem Untersuchungs-Canvas zu verknüpfen.

Vorbereitungen

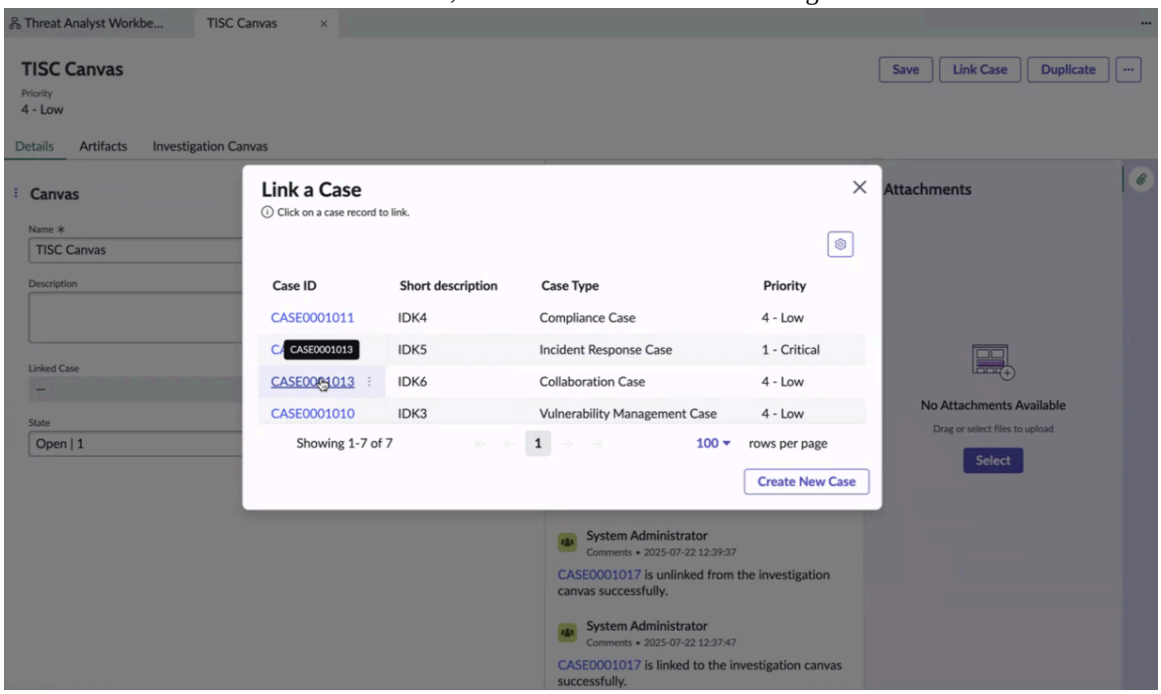
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Wählen Sie Aus **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Dadurch werden alle Fälle angezeigt.
4. Auswahlvorgang **Fallmanagement** > **Alle Fälle**
5. Öffnen Sie einen beliebigen Falldatensatz in der Listenansicht.
6. Wählen Sie Aus **Fall Verknüpfen** Von **Details** Abschnitt.
   Das Dialogfeld „Fall verknüpfen“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie eine Fall-ID aus der Liste aus, um den Fall einem Untersuchungs-Canvas zuzuordnen.



Eine Bestätigungsnachricht wird angezeigt, die bestätigt, dass der Fall erfolgreich verknüpft wurde.

Hinweis:
Wenn kein Fall für die Verknüpfung mit dem Untersuchungs-Canvas verfügbar ist, können Sie einen neuen Fall erstellen, um Ihren Untersuchungskontext zu initiieren und zu organisieren. Weitere Informationen zum Erstellen eines neuen Falls finden Sie unter Erstellen eines Falls und Verknüpfen aus Untersuchungs-Canvas

an.

8. Um einen verknüpften Fall zu entfernen, wählen Sie aus **Verknüpfung Aufheben** Schaltfläche.

Zugehörige Informationen

Untersuchungs-Canvas wird erstellt

Erstellen eines Falls und Verknüpfen aus Untersuchungs-Canvas

Verwenden Sie diesen Abschnitt, um einen Fall aus einem Untersuchungs-Canvas zu erstellen und zu verknüpfen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Wählen Sie Aus **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Dadurch werden alle Fälle angezeigt.
4. Öffnen Sie einen beliebigen Falldatensatz aus der Liste.
5. Wählen Sie Aus **Fall Verknüpfen** Von **Details** Abschnitt.
   Das Dialogfeld Fall erstellen und verknüpfen wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wählen Sie einen Fall aus der Liste aus, um den Fall einem Untersuchungs-Canvas zuzuordnen.
7. Wählen Sie Aus **Erstellen Sie Eine Neue Canvas** .
   Das Dialogfeld Neuen Fall erstellen wird angezeigt.
8. Füllen Sie die Formularfelder entsprechend aus.

Feld	Beschreibung
Fall-ID	Ein eindeutiger Bezeichner für den Fall. Dies ist eine vom System generierte ID.
Kurzbeschreibung	Zusammenfassung der Anforderung oder des Problems, die bzw. das untersucht wird, oder eine kurze Beschreibung.
Falltyp	Wählen Sie den Typ des untersuchten Falls aus. Die möglichen Optionen für die Untersuchung sind: ○ Bedrohungssuche ○ Informationsanforderung ○ Schwachstellenmanagement-Fall ○ Compliance-Fall ○ Fall vom Typ „Reaktion auf Incidents“ ○ Zusammenarbeitsfall ○ Andere
Priorität	Gibt die Priorität eines Falls an.
Zuweisungsgruppe	Die zugewiesene Gruppe, die für die Bearbeitung des Falls verantwortlich ist.
Status	Der aktuelle Status des Falls.
Zugewiesen an	Der Analyst, der für die Bearbeitung eines Falls verantwortlich ist.

9. Wählen Sie Aus **Erstellen und verknüpfen** Um einen neuen Fall zu erstellen und direkt mit dem Untersuchungs-Canvas zu verknüpfen.

   Eine Bestätigung wird angezeigt, die bestätigt, dass der Fall erfolgreich erstellt und mit dem Untersuchungs-Canvas verknüpft wurde.

   Hinweis:
   Diese Option ist nützlich, wenn dem Untersuchungs-Canvas kein vorhandener Fall zugeordnet ist.

10. Um einen verknüpften Fall zu entfernen, wählen Sie aus **Verknüpfung Aufheben** Schaltfläche.
    Weitere Informationen zum direkten Verknüpfen eines vorhandenen Falls mit dem Untersuchungs-Canvas finden Sie unter Verknüpfen eines vorhandenen Falls aus Untersuchungs-Canvas.

Zugehörige Informationen

Untersuchungs-Canvas wird erstellt

Canvas wird aus einem Fall verknüpft

Verwenden Sie diesen Abschnitt, um eine Canvas aus einem Fall zu verknüpfen.

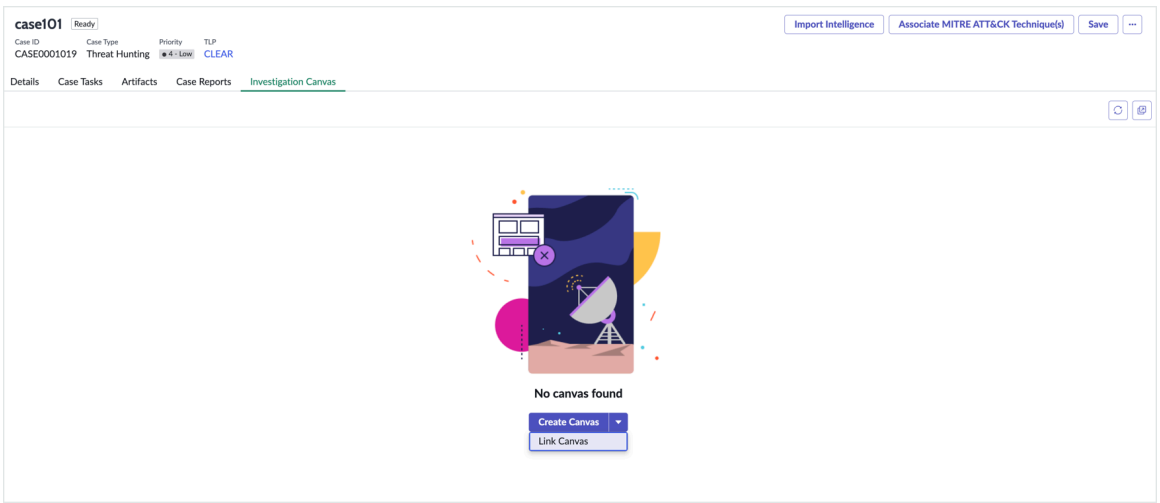
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Untersuchungs-Canvase** > **Alle Canvase**an.
4. Von **Alle Fälle** Listenansicht wählen Sie einen Fall aus, der nicht mit dem Canvas verknüpft ist.
5. Wechseln Sie zu **Untersuchungs-Canvas** Abschnitt.
6. Wählen Sie Aus **Fall Verknüpfen** Aus der Dropdown-Liste auf der leeren Canvas-Seite (die Option wird im folgenden Screenshot angezeigt).



7. Wählen Sie die Canvas aus.
8. Wählen Sie aus **Link** Schaltfläche zum Verknüpfen des Canvas mit einem Fall.

   Eine Informationsmeldung wird angezeigt, die angibt, dass die Canvas-Daten erfolgreich aktualisiert wurden.

Untersuchungs-Canvas wird erstellt

Erstellen Sie einen Canvas, um erkennbare Elemente aus der Threat Intelligence-Bibliothek hinzuzufügen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Untersuchungs-Canvase** > **Alle Canvase**an.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Eine Neue Canvas

Feld	Beschreibung
Name	Geben Sie den Namen der Canvas ein.
Beschreibung	Fügen Sie die Beschreibung des Canvas hinzu.
Verknüpfter Fall	Mit dieser Option wird eine Liste von Fällen angezeigt, denen keine Canvase zugeordnet sind. Das Feld wird dynamisch ausgefüllt, je nachdem, ob für jeden Fall kein verknüpfter Canvas vorhanden ist, sodass Anwender Fälle leicht identifizieren können, für die möglicherweise Untersuchungskontexte erstellt oder verknüpft werden müssen.
Priorität	Wählen Sie die Priorität des Canvas aus.
Status	Wählen Sie den Status des Canvas aus.

6. Klicken Sie auf **Speichern**.
   Die beiden neuen Abschnitte werden angezeigt **Artefakte** Und **Untersuchungs-Canvas** . Wenn Sie eine neue Canvas erstellen, enthält die Canvas keine Knoten. Sie müssen Knoten aus der Threat Intelligence-Bibliothek oder Artefakten über die Option „aus Bibliothek hinzufügen“ hinzufügen.
7. Wechseln Sie zu **Untersuchungs-Canvas** .
8. Klicken Sie Auf **Aus Bibliothek hinzufügen** .

   Hinweis:
   Es sind zwei Optionen zum Hinzufügen der Knoten verfügbar. Sie können entweder auswählen **Importieren** Um alle erkennbaren Elemente zu importieren oder auszuwählen **Aus Bibliothek hinzufügen** Option zum Hinzufügen der erkennbaren Elemente aus der Threat Intelligence-Bibliothek.

   Die **Importieren Sie den Knoten aus der Bibliothek** Das Dialogfeld wird angezeigt.
9. Wählen Sie aus **Typ des Knotens** Aus der Dropdown-Liste.
   Wählen Sie beispielsweise den Typ erkennbare Elemente aus, wenn Sie der Untersuchungs-Canvas erkennbare Elemente hinzufügen.
10. Wählen Sie die erforderliche Anzahl erkennbarer Elemente aus.
11. Klicken Sie auf **Importieren**.
    Nachdem Sie erkennbare Elemente importiert haben, werden die Knoten dem Untersuchungs-Canvas hinzugefügt. Alle Knoten, die dem Canvas hinzugefügt werden, werden derzeit vorübergehend dem Canvas hinzugefügt, und es wird nicht im Canvas beibehalten.
12. Wählen Sie Aus **Speichern Sie Canvas** .
    Wenn Sie die Knotendaten im Canvas verarbeiten möchten, müssen Sie die Daten speichern, um sie dauerhaft zu behalten.

    Hinweis:
    Wenn Sie nicht ausführen **Speichern Sie Canvas** Option dann können Sie die Daten verlieren, wenn Sie den Canvas aktualisieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Wählen Sie Aus **Fügen Sie der Bibliothek Daten hinzu** Um eine neue Beziehung zwischen zwei verschiedenen Knoten zu erstellen.
    Die Beziehung zwischen den beiden Knoten wird durch die gepunktete Linie angezeigt, was bedeutet, dass die Knoten temporär sind. Wenn Sie die Knotendaten in die Beziehungen verschieben möchten, wählen Sie aus **Speichern Sie Daten in der Bibliothek** Und fügen Sie der Bibliothek Daten hinzu. Nachdem Sie diesen Vorgang ausgeführt haben, wird die gepunktete Linie in eine durchgehende Kantenlinie umgewandelt, die anzeigt, dass der Knoten jetzt Teil der Bibliothek ist.
14. Verwenden Sie **Filter** Symbol, um den Typ der erkennbaren Elemente und Objekte anzuzeigen, die im Canvas vorhanden sind, und Sie können selektiv den Typ der Daten auswählen, die im Untersuchungs-Canvas angezeigt werden sollen.
15. Wählen Sie auch das Popout-Symbol aus, um Vorgänge für die Untersuchungs-Canvas-Knoten auf einem größeren Bereich anzuzeigen oder auszuführen.
16. Wählen Sie Aus **Fall Verknüpfen** Zum Verknüpfen des Falls mit dem Untersuchungs-Canvas.
    a. Wählen Sie aus **Fall-ID** .
    b. Klicken Sie auf **Link** Schaltfläche.
17. Klicken Sie Auf **Duplikat** Zum Duplizieren der Canvas-Daten und -Knoten innerhalb des Canvas.

Zugehörige Informationen

Arbeiten mit Aktionen im Untersuchungs-Canvas

Canvas wird aus einem Fall verknüpft

Erstellen eines Falls und Verknüpfen aus Untersuchungs-Canvas

Dem Canvas wird ein neuer Knoten hinzugefügt

Verwenden Sie diesen Abschnitt, um neue Entitäten, einschließlich erkennbarer Elemente oder Objekte, direkt aus dem Untersuchungs-Canvas zu erstellen und hinzuzufügen.

Vorbereitungen

Diese Funktion ermöglicht eine schnelle Ergänzung des Canvas, ohne von der aktuellen Ansicht wegnavigieren zu müssen.

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Wählen Sie aus **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
4. Öffnen Sie einen beliebigen Falldatensatz.

> **Hinweis:**
> Beim Erstellen eines Falls müssen Sie entweder eine Canvas erstellen oder eine vorhandene verknüpfen. Nach der Verknüpfung sind die Canvas-Aktionen, einschließlich der Option zum Hinzufügen neuer Knoten, automatisch in der Anwenderoberfläche verfügbar.

5. Auswahlvorgang **Untersuchungs-Canvas** > **Neuer Knoten**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

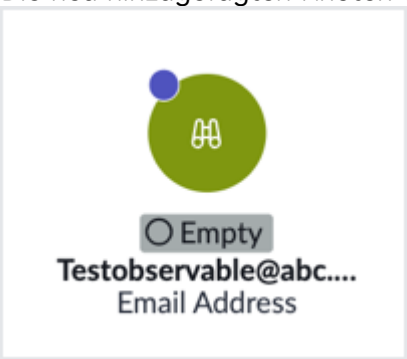
- Sie können auch anzeigen **Neuer Knoten** Funktionalität aus der Dropdown-Liste der leeren **Untersuchungs-Canvas** Abschnitt des Falls.
- Eine weitere Option zum Anzeigen von **Neuer Knoten** Die Funktionalität besteht darin, direkt über die Seite „Untersuchungs-Canvas“ anzuzeigen.

6. Um einen Knoten zu erstellen, wählen Sie den entsprechenden aus **Entitätskategorie** Und **Entitätstyp** .

7. Geben Sie die erforderlichen Objektdetails wie Name, Beschreibung ein.

8. Wählen Sie Aus **Hinzufügen** Um den neuen Knoten hinzuzufügen.
   Dieser Prozess fügt den Knoten automatisch dem Untersuchungs-Canvas hinzu.

   Die neu hinzugefügten Knoten werden visuell durch einen Punkt unterschieden



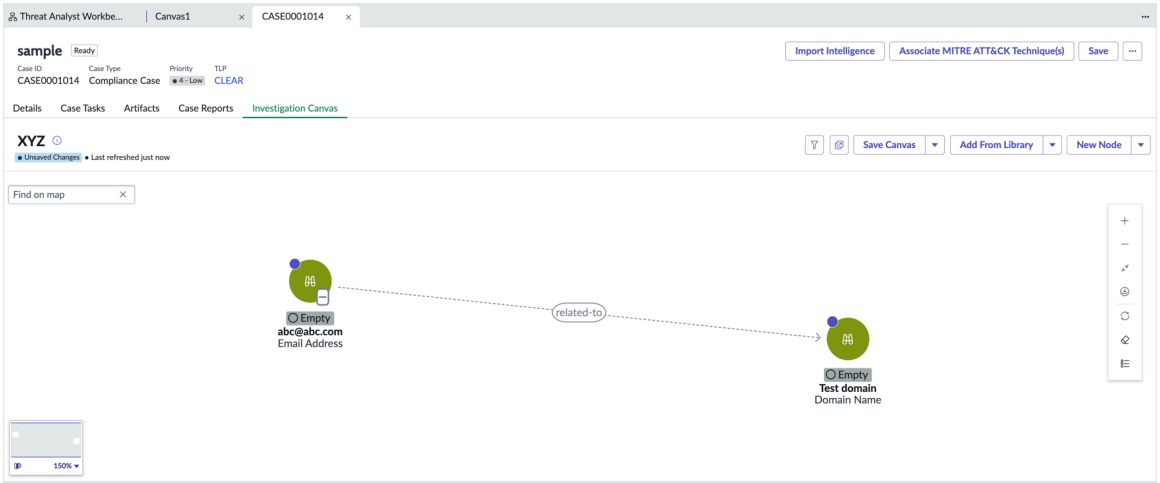
   Auf dem Knoten aus Knoten, die über die Bibliothek oder Fallartefakte importiert werden.

> **Wichtig:**
> Neu hinzugefügte Knoten sind temporär und werden nicht in der Threat Intelligence-Bibliothek oder im Canvas gespeichert. Wenn Sie den Canvas vor dem Speichern aktualisieren, gehen diese Knoten verloren. Stellen Sie sicher, dass Sie den Canvas speichern, nachdem Sie neue Knoten hinzugefügt haben, um Ihre Änderungen beizubehalten.

9. Klicken Sie mit der rechten Maustaste auf den neuen Knoten, und wählen Sie aus **Fügen Sie Eine Beziehung Hinzu** Option zum Erstellen von Beziehungen zwischen den Knoten.

> **Hinweis:**
> - Beim Erstellen neuer Beziehungen werden die Edges als gestrichelte Linien angezeigt, was darauf hinweist, dass sie temporäre Knoten sind und nicht in der Threat Intelligence-Bibliothek gespeichert sind.
> - Neu hinzugefügte Edges sind temporär und werden nicht in der Threat Intelligence-Bibliothek oder im Canvas gespeichert. Wenn Sie den Canvas vor dem Speichern aktualisieren, gehen diese Edges verloren. Stellen Sie sicher, dass Sie den Canvas speichern, nachdem Sie neue Edges hinzugefügt haben, um Ihre Änderungen beizubehalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Rechtsklicken Sie, und wählen Sie aus **Details Anzeigen** Zum Anzeigen der Details im Zusammenhang mit der ausgewählten Entität.

> **Hinweis:**
> Zum Hinzufügen von Daten können Sie entweder auf den Hyperlink im Detailbereich klicken oder auswählen **Öffnen Sie Den Datensatz** Option und fügen Sie die erforderlichen knotenbezogenen Daten hinzu.

11. Wählen Sie Aus **Fügen Sie der Bibliothek Daten hinzu** Option zum Speichern aller Knoten und Edges, die während Ihrer Untersuchung vorübergehend hinzugefügt wurden.
Durch Ausführen dieser Aktion werden die temporären Datensätze in dauerhaft zusammengefasste Datensätze in der Threat Intelligence-Bibliothek konvertiert.

Untersuchungs-Canvas und MITRE ATT&CK

Im Untersuchungs-Canvas können Sie die MITRE ATT&CK-Techniken und -Untertechniken anzeigen, die allen derzeit auf dem Canvas vorhandenen Knoten zugeordnet sind.

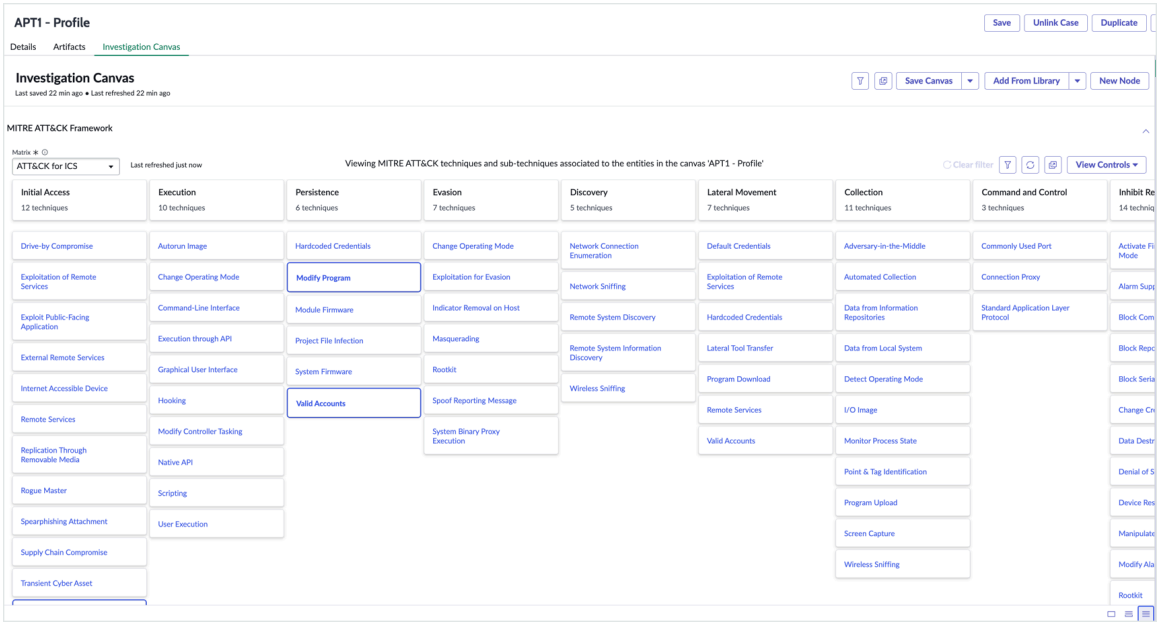
Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Wählen Sie aus **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
4. Öffnen Sie einen beliebigen Fall.
5. Wechseln Sie zu **Untersuchungs-Canvas** Registerkarte.
6. Verwenden Sie im Untersuchungs-Canvas **Handle der Trennlinie für skalierbare Bereiche** Zum Ziehen, um das MITRE ATT&CK-Framework anzuzeigen.
7. Wählen Sie die erforderliche MITRE ATT&CK-Matrix aus der aus **Matrix** Dropdown-Liste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das MITRE ATT&CK-Framework zeigt verschiedene Ebenen der Zuordnung von Taktiken und Techniken an.

a. In der oberen Zeile werden alle Taktiken angezeigt, die in der ausgewählten MITRE ATT&CK-Matrix vorhanden sind.

b. Standardmäßig zeigt jede Taktik die Anzahl der insgesamt zugehörigen Techniken und Untertechniken an.

c. Verwenden Sie **Aktualisieren** Symbol, um das MITRE ATT&CK-Framework neu zu laden und die neuesten Zuordnungen von Technik und Taktik anzuzeigen.

d. Zeigen Sie die MITRE ATT&CK-Techniken und -Subtechniken an, die sich auf alle Knoten (Entitäten) im Canvas beziehen.

e. Klicken Sie auf einen oder mehrere Knoten, um die zugehörigen MITRE ATT&CK-Techniken und -Untertechniken im Zusammenhang mit diesen ausgewählten Knoten im Canvas anzuzeigen.

> **Wichtig:**
> Im Framework werden die Techniken und Untertechniken hervorgehoben, die den Knoten im Canvas zugeordnet sind.

8. Wählen Sie Aus **Filter** Damit Sie Filter für TTPs erstellen und speichern können, die bestimmten Gegnern und anderen MITRE-Technikattributen zugeordnet sind.
   Weitere Informationen zu den MITRE-Filteroptionen finden Sie unter MITRE-Filter für Untersuchungs-Canvas.
9. Verwenden **Steuerungen Anzeigen** Für erweiterte Filteroptionen.
   Sobald Sie den entsprechenden Filter ausgewählt haben, werden nur die MITRE ATT&CK-Techniken und -Untertechniken angezeigt, die den ausgewählten Knoten zugeordnet sind. Die Optionen in **Steuerungen Anzeigen** Listen sind:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **ID anzeigen** : Zeigt die eindeutige Technik-ID an (z. B. `T1059`) Auf jeder Karte zur einfachen Referenz.
- **Untertechniken Anzeigen** : Zeigt die Untertechniken an. Mit dieser Option werden die übergeordneten Technikkarten automatisch erweitert, um ihre Untertechniken anzuzeigen, ohne dass eine manuelle Erweiterung erforderlich ist.
- Wählen Sie Aus **Nur Zugeordnete Techniken Anzeigen** : Zeigt nur die Techniken an, die derzeit mit Knoten im Untersuchungs-Canvas verknüpft sind, und blendet alle irrelevanten Techniken aus, auch wenn sie die Filterkriterien erfüllen. Wenn diese Option ausgewählt ist, zeigt jede Taktik die Gesamtanzahl der zugeordneten Techniken und Untertechniken an, die derzeit mit dem Canvas verknüpft sind.

10. Klicken Sie auf das Popout-Symbol, um das MITRE ATT&CK Framework auf einem größeren Platz anzuzeigen.

Wichtig:

- Jedes Mal, wenn Sie einen Knoten hinzufügen oder entfernen, wird das MITRE ATT&CK-Framework automatisch aktualisiert. Sie können auch das Aktualisierungssymbol verwenden, um jederzeit eine manuelle Aktualisierung durchzuführen.
- Wenn Sie bestimmte Knotentypen filtern, wird das MITRE ATT&CK-Framework automatisch aktualisiert, um die Änderungen widerzuspiegeln.

MITRE-Filter für Untersuchungs-Canvas

Mit MITRE-Filtern können Sie Filter für Taktiken, Techniken und Verfahren (TTPs) erstellen und speichern, die bestimmten Gegnern und anderen MITRE-Technikattributen zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Analysten können die auf der MITRE-Karte verfügbaren Filter verwenden, um bestimmte Akteur-TTPs zu filtern, die für an der Untersuchung beteiligte Angreifer relevant sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Wählen Sie aus **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
4. Öffnen Sie einen beliebigen Fall.
5. Wechseln Sie zu **Untersuchungs-Canvas** Registerkarte.
6. Wählen Sie Aus **Filter** Zum Erstellen von Filtern für Taktiken, Techniken und Verfahren (TTPs), die bestimmten Gegnern und anderen MITRE-Technikattributen zugeordnet sind.
7. Geben Sie die erforderlichen Werte im Filterbereich ein, um die gewünschten Filter anzuwenden.
   Im MITRE-Filterbereich können Sie MITRE ATT&CK-Techniken basierend auf ausgewählten Kriterien wie Gruppen, Malware, Tools, Tags und Priorität filtern und visualisieren.

Feld	Beschreibung
Gespeicherte Filter	Analysten können bestimmte Kriterien als speichern **Gespeicherte Filter** Zur Wiederverwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

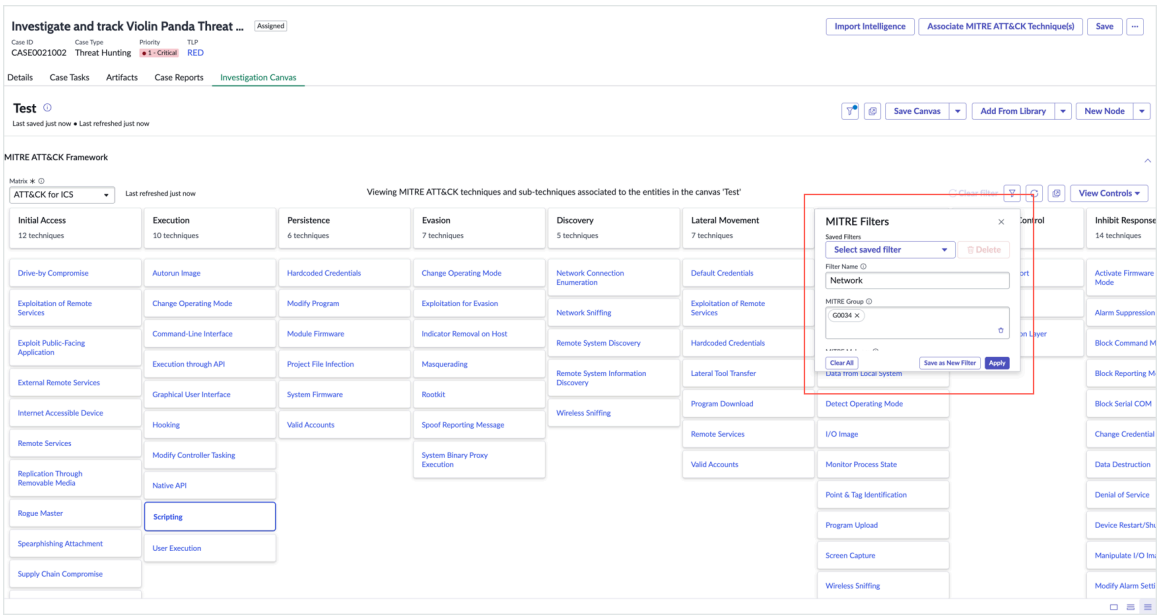
Feld	Beschreibung
	Von einem Analysten gespeicherte Filter sind anwenderspezifisch. **Hinweis:** Wenn Analyst X beispielsweise eine Filterkonfiguration speichert, ist sie nur für Analyst X sichtbar. Wenn sich ein anderer Analyst anmeldet und die Filter-Dropdown-Liste anzeigt, werden die von anderen gespeicherten Filter nicht angezeigt. Dadurch wird sichergestellt, dass jeder Anwender personalisierte Ansichten erstellen und verwalten kann, ohne die Filtereinstellungen anderer Anwender zu beeinträchtigen oder davon betroffen zu sein.
Filtername	Name des Filters.
MITRE-Gruppe	Gibt die MITRE-Gruppe an. Wählen Sie eine oder mehrere Gruppen aus, um die ihnen zugeordneten Techniken zu filtern.
MITRE-Malware	Gibt die MITRE-Malware an. Wählen Sie ein oder mehrere Malware-Elemente aus, um die ihnen zugeordneten Techniken zu filtern.
MITRE-Tools	Gibt die MITRE-Tools an. Wählen Sie ein oder mehrere Tools aus, um die ihnen zugeordneten Techniken zu filtern.
TISC-Tags	Gibt an TISC Tags. Wählen Sie ein oder mehrere Tags aus, um Techniken basierend auf ihrer Klassifizierung zu filtern.
Priorität von Techniken	Gibt die Prioritätsstufe von Techniken an. Sie können eine oder mehrere Optionen auswählen, um Techniken basierend auf ihrer zugewiesenen Priorität zu filtern.
Alles löschen	Ermöglicht Ihnen das Löschen der im Filterbereich eingegebenen Eingaben.
Als neuen Filter speichern	Speichert die im Filterbereich eingegebenen Kriterien als neuen gespeicherten Filter. **Hinweis:** Gespeicherter Filtername muss eindeutig sein.
Aktuellen Filter speichern	Speichert Änderungen an den Kriterien im aktuell ausgewählten gespeicherten Filter. Mit dieser Option können Sie einen Filter auch umbenennen. **Hinweis:** Gespeicherter Filtername muss eindeutig sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übernehmen	Mit dieser Option können Sie die Änderungen auf Ihre Filter auf der MITRE-Karte anwenden.
Löschen	Wählen Sie diese Option aus, um einen ausgewählten gespeicherten Filter zu entfernen. Wenn Sie auf klicken **Löschen** Schaltfläche neben einem gespeicherten Filter wird eine Bestätigungsnachricht angezeigt, wenn Sie diesen Filter wirklich löschen möchten. Wenn Sie diese Aktion bestätigen, wird der gespeicherte Filter dauerhaft entfernt. Klicken Sie auf , um einen einzelnen Feldwert im Filterbereich zu entfernen **Löschen (Papierkorb)** Symbol neben diesem spezifischen Feld.

Durch Anwenden von Filtern mit diesen Werten wird die MITRE-Matrix dynamisch aktualisiert, um nur die Techniken anzuzeigen, die den ausgewählten Attributen zugeordnet sind. Diese fokussierte Ansicht ermöglicht es Analysten, sich während Untersuchungen stärker auf die relevantesten Taktiken, Techniken und Verfahren (TTPs) zu konzentrieren.

Darüber hinaus können Analysten TTPs mithilfe von Filtern für Malware, Tools, Tags und Prioritätsstufen weiter eingrenzen.



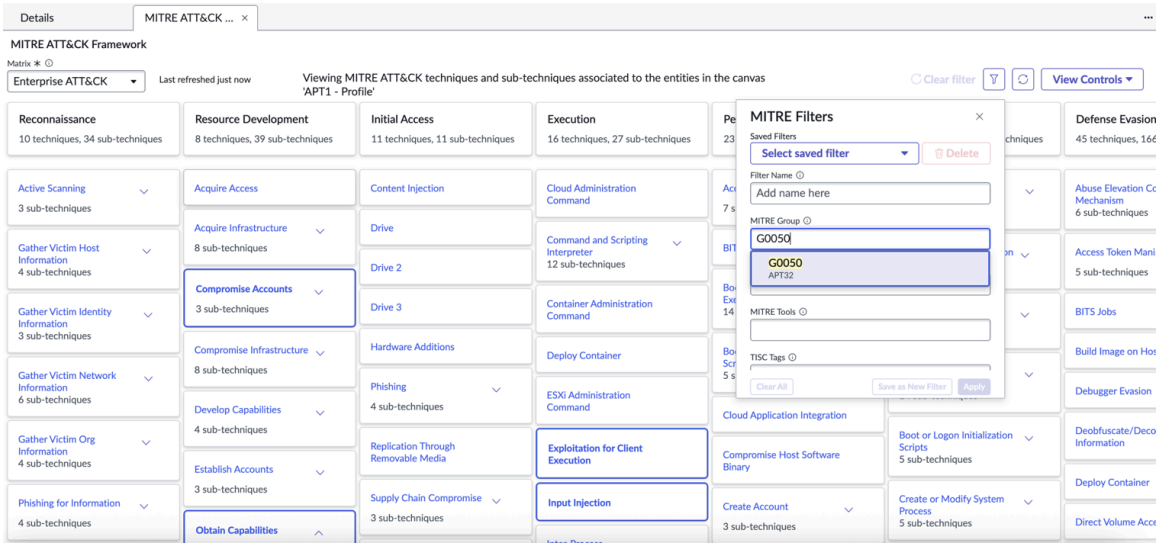
8. **Wahlweise:** Wählen Sie Aus **Als neuer Filter speichern** Um Ihre Filterkriterien zu speichern.
9. Wählen Sie Aus **Anwenden** Zum Anwenden der Änderungen.

Example: Filterung nach MITRE-Gruppe

Wählen Sie eine MITRE-Gruppe als APT32 (G1001, siehe folgenden Screenshot) aus. Wenn Sie diesen Filter anwenden, wird die MITRE-Matrix aktualisiert, um nur die Techniken anzuzeigen, die direkt mit der ausgewählten Gruppe verknüpft sind.

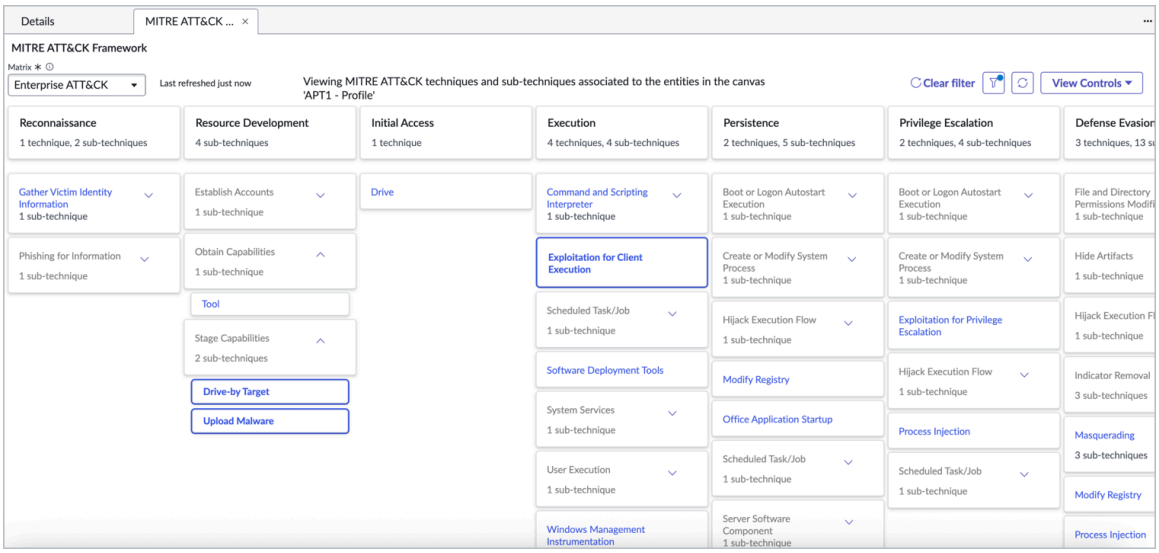
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung



Diese fokussierte Ansicht hilft Analysten, sich insbesondere auf die Taktiken, Techniken und Verfahren (TTPs) zu konzentrieren, die der ausgewählten Bedrohungsgruppe zugeordnet sind.

Wenn Sie den Filter anwenden, werden einige Techniken in der Matrix in blauem Text angezeigt, während andere Techniken in grau angezeigt werden.



Die visuelle Darstellung im MITRE-Framework zeigt an, wie Techniken und Untertechniken sich auf die angewendeten Filter und den Untersuchungskontext beziehen.

- **Blauer Text:** Techniken oder Untertechniken, die in blauem Text angezeigt werden, geben diejenigen an, die den Filterkriterien entsprechen.
- **Blauer Text in Fettdruck mit blauem Rahmen:** Techniken oder Untertechniken, die in fett gedrucktem blauem Text mit blauem Rahmen angezeigt werden, geben diejenigen an, die den Filterkriterien entsprechen und einem oder mehreren Knoten auf der Canvas zugeordnet sind.
- **Graue Karte:** Übergeordnete Techniken werden grau angezeigt, wenn sie nicht direkt den Filterkriterien entsprechen (d. h. sie sind nicht mit der ausgewählten Gruppe verknüpft), sie werden jedoch angezeigt, um die Elternbeziehung zu verknüpften Untertechniken darzustellen, die den Filterkriterien entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Artefakte zu Fällen oder Fallaufgaben hinzufügen

Nachdem Sie einen Fall erstellt haben, können Sie dem Fall Artefakte wie Security Incidents, CIs und kompromittierte Indikatoren anzeigen oder hinzufügen. Diese Artefakte dienen als Hinweise zur Lösung des Falls.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis:
Artefakte sind nur für die vorhandenen Fälle verfügbar. Bei erkennbaren Elementen und Indikatoren können die Artefakte auch aus dem Importauftrag über die Schaltfläche „Intelligenz importieren“ einem Fall hinzugefügt oder zugeordnet werden. Weitere Informationen zum Importieren finden Sie unter . Importieren Sie Intelligence in TISC

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen Fall oder eine Fallaufgabe aus.
5. Wechseln Sie zu **Artefakte** Registerkarte.
   Die zugeordneten Artefakte werden als zugehörige Listen für diesen bestimmten Fall oder diese Fallaufgabe angezeigt.
6. Verknüpfen oder heben Sie die Verknüpfung der Datensätze mit dem Fall oder der Fallaufgabe auf.

Hinweis:
Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze

In der folgenden Tabelle sind die zugehörigen Listen zu Artefakten im Zusammenhang mit den Fällen oder Fallaufgaben aufgeführt:

Zugehörige Datensätze

Zugehörige Liste	Beschreibung
MITRE-Techniken	Listen Sie die MITRE-Techniken auf, die sich auf die Fälle beziehen. MITRE-Techniken zeigt auch alle zugehörigen Techniken in einem Fall an.
Erkennbares Element	Liste der erkennbaren Elemente im Zusammenhang mit diesen Fällen oder Fallaufgaben.
Indikatoren	Liste der Indikatoren im Zusammenhang mit diesen Fällen oder Fallaufgaben.
Angriffsmuster	Liste der Angriffsmuster, die sich auf diese Fälle oder Fallaufgaben beziehen.
Kampagnen	Listen Sie die Kampagnen auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Vorgehensweisen	Listet die Aktionen auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Datenkomponenten	Liste der Datenkomponenten, die sich auf diese Fälle oder Fallaufgaben beziehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Beschreibung
Bedrohungsgruppierungen	Listen Sie die Bedrohungsgruppierungen auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Identitäten	Listen Sie die Identitäten auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Infrastruktur	Listen Sie die Infrastruktur auf, z. B. Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen, die sich auf diese Fälle oder Fallaufgaben beziehen.
Angriffssätze	Listen Sie die Angriffssätze auf, z. B. eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften, die sich auf diese Fälle oder Fallaufgaben beziehen.
Standorte	Listen Sie die Standortdatensätze auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Malware	Listen Sie die Malware-Quelldatensätze auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Markierungsdefinitionen	Listen Sie die Markierungsdefinitionsdatensätze auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Bedrohungshinweise	Listen Sie die Markierungsdefinitionsdatensätze auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Beobachtete Daten	Listen Sie die beobachteten Daten auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Bedrohungsmeinungen	Listen Sie die Bedrohungsmeinungen auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Bedrohungsberichte	Listen Sie die Bedrohungsberichte auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Sichtungen	Liste der Sichtungen, die sich auf diese Fälle oder Fallaufgaben beziehen.
Bedrohungsakteure	Listen Sie die Bedrohungsakteure auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Tools	Listen Sie die Tools auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Schwachstellen	Wenn das erkennbare Element eine IP-Adresse ist, zeigt diese Liste alle Ressourcen (Konfigurationselemente) an, die eine übereinstimmende IP-Adresse haben, die sich auf diese Fälle oder Fallaufgaben beziehen.
Verwandte Fälle	Listet die zugehörigen Fälle auf.
Zugehöriger Fall – Aufgaben	Listet die zugehörigen Fallaufgaben auf.
Security Incidents	Listet die Security Incidents auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Betroffene Konfigurationselemente	Listen Sie die betroffenen Konfigurationselemente auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Betroffene Services	Listen Sie die betroffenen Services auf, die sich auf diese Fälle oder Fallaufgaben beziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Liste	Beschreibung
Betroffene Assets	Listen Sie die betroffenen Assets auf, die sich auf diese Fälle oder Fallaufgaben beziehen.
Schwachstelleneinträge	Listen Sie die Schwachstelleneinträge auf, die sich auf diese Fälle oder Fallaufgaben beziehen.

Rollup von MITRE-Techniken von Artefakten zu Fall

Wenn einem Fall Intelligenzdatensätze hinzugefügt werden, werden alle zugehörigen MITRE-Techniken automatisch auf Fallebene zusammengefasst.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen beliebigen Fall aus.
5. Wechseln Sie zu **Artefakte** Registerkarte.
   Die zugeordneten Artefakte werden als zugehörige Listen für diesen spezifischen Fall angezeigt.

MITRE ATT&CK-Framework für einen Fall anzeigen

Zeigt alle zugeordneten Techniken eines Falls im MITRE ATT&CK-Framework an.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Wählen Sie die erforderliche MITRE ATT&CK-Matrix aus der aus **Matrix** Dropdown-Liste. Das MITRE ATT&CK-Framework zeigt verschiedene Ebenen der Zuordnung von Taktiken und Techniken an.

1. In der oberen Zeile werden alle Taktiken angezeigt, die in der ausgewählten vorhanden sind **Matrix** . Standardmäßig zeigen alle Taktiken die Anzahl der insgesamt vorhandenen Techniken und Untertechniken für die entsprechende Taktik an. Sie können verwenden **Aktualisieren** Symbol, um das MITRE ATT&CK-Framework neu zu laden und die neuesten Zuordnungen anzuzeigen.
2. Unter jeder Taktik zeigt das Framework alle Techniken an, die als Beziehung zur entsprechenden Taktik vorhanden sind.
3. Das Framework zeigt die Untertechniken an, die unter jeder Technik vorhanden sind. Erweitern Sie jede Technik, um die Untertechniken anzuzeigen.

Wichtig:
Im Framework werden die Techniken und Untertechniken hervorgehoben, die einem Fall zugeordnet sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Workbench Für Bedrohungsanalysen** Symbol.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen beliebigen Fall aus.
5. Wechseln Sie zu **Artefakte** Registerkarte.
   Die zugeordneten Artefakte werden als zugehörige Listen für diesen spezifischen Fall angezeigt.
6. Wählen Sie Aus **MITRE ATT&CK-Framework anzeigen** Schaltfläche
   Wenn Sie diese Schaltfläche auswählen, zeigt das Framework alle zugehörigen Techniken eines Falls und Artefakte auf der MITRE ATT&CK an.
7. Zeigen Sie MITRE ATT&CK-Techniken und -Untertechniken im Zusammenhang mit dem Fall aus den MITRE-Techniken an, die Sie zum Anzeigen ausgewählt haben.
8. Wählen Sie einen beliebigen Datensatz aus, um die MITRE ATT&CK-Techniken und -Untertechniken im Zusammenhang mit dem Fall anzuzeigen.
9. Verwenden **Steuerungen Anzeigen** Um die MITRE ATT&CK-Techniken und -Untertechniken nach Bedarf anzuzeigen.
   In den Steuerungslisten:
   - Wählen Sie Aus **ID anzeigen** Zum Anzeigen der MITRE-IDs für Techniken und Untertechniken.
   - Wählen Sie Aus **Untertechniken Anzeigen** Zum Anzeigen aller Untertechniken. Wenn Sie diese Option auswählen, werden alle Techniken in der erweiterten Ansicht angezeigt. Die erweiterte Ansicht der Technik zeigt alle Untertechniken an, die für die entsprechende Technik vorhanden sind.
   - Wählen Sie Aus **Nur Zugeordnete Techniken Anzeigen** Um nur MITRE-Techniken anzuzeigen, die einem Fall zugeordnet sind. Wenn Sie diese Option auswählen, zeigt jede Taktik die Gesamtzahl der zugehörigen Techniken und Untertechniken an.

Führen Sie Anreicherungsaktionen in einem Fall aus

In diesem Abschnitt erfahren Sie, wie Ergänzungsaktionen für Fälle ausgeführt werden.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

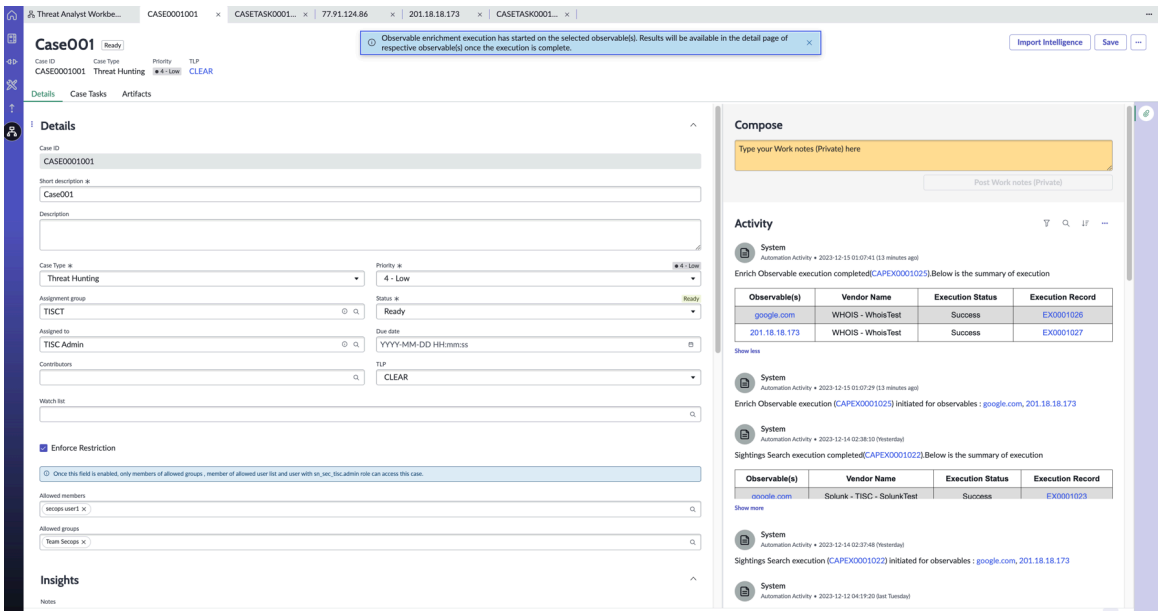
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen Fall oder eine Fallaufgabe aus.
5. Wechseln Sie zu **Artefakte** Registerkarte.
6. Wählen Sie die zugehörige Liste erkennbarer Elemente aus.
7. Wählen Sie mindestens ein erkennbares Element aus.
8. Klicken Sie in der Dropdown-Liste auf eine beliebige Anreicherungsaktion.
9. Wählen Sie die verfügbaren Implementierungen aus.
10. Klicken Sie auf **Absenden**.
    Beispiel: Bedrohungssuche ausführen. Die ausgewählte Ergänzungsaktion wird ausgeführt, und es wird eine Informationsnachricht angezeigt, die angezeigt wird Die Ausführung der Ergänzung erkennbarer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elemente wurde für die ausgewählten erkennbaren Elemente gestartet. Ergebnisse sind auf der Detailseite der jeweiligen erkennbaren Elemente verfügbar, sobald die Ausführung abgeschlossen ist .

Hinweis:
Sobald die Ausführung initiiert oder abgeschlossen ist, werden Arbeitsnotizen im Aktivitätenstrom der Formularansicht veröffentlicht.



Zeigen Sie Fallberichte An

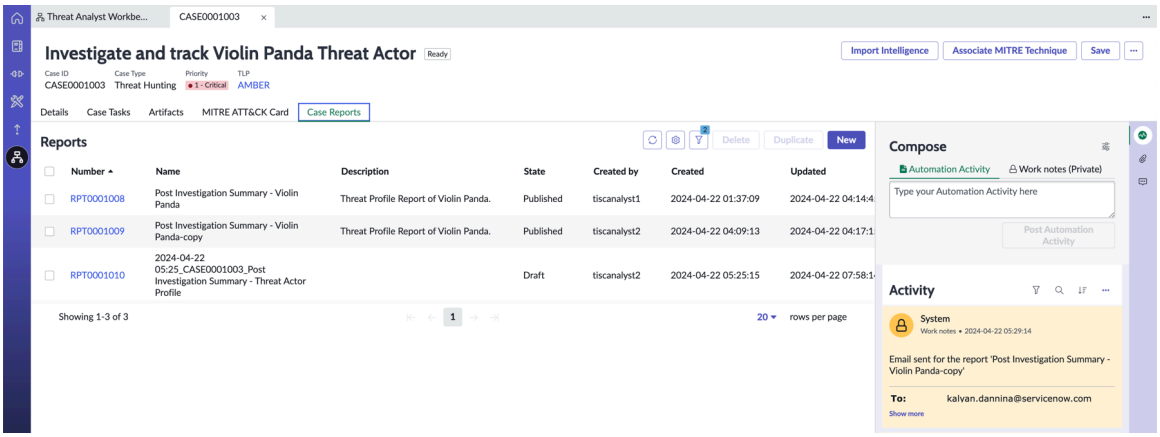
Verwenden Sie die Funktion „Fallberichte“, um Berichte zu den Fällen zu generieren. Diese Berichte umfassen einen Bericht nach der Untersuchung oder einen Zusammenfassungsbericht.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

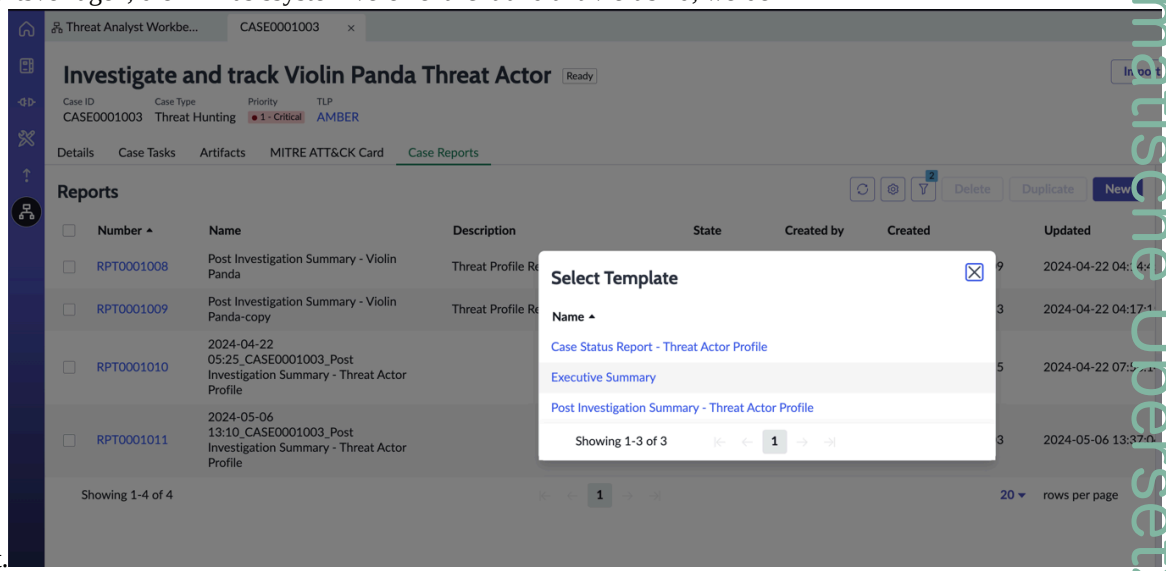
1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen beliebigen Fall aus.
5. Wechseln Sie zu **Fallberichte** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Sie können die Berichte aus der Liste löschen, eine doppelte Kopie der vorhandenen Berichte erstellen und Ihren eigenen Bericht anpassen.

6. Klicken Sie auf **Neu**.
   Die Berichtsvorlagen, die im Basissystem veröffentlicht und aktiviert sind, werden angezeigt.



7. Wählen Sie die gewünschte Berichtsvorlage aus.
   Die ausgewählte Berichtsvorlage für den Berichtstyp wird generiert. Außerdem bedeutet dies, dass hier, sobald der Bericht veröffentlicht wurde, eine größere Gruppe von Anwendern ihn anzeigen kann. Wenn sich der Bericht jedoch im Entwurfsstatus befindet, wird dieser Bericht für die Anwender ausgeblendet. Als Analyst können Sie nur die veröffentlichten Berichte anzeigen, aber nicht die Berichte im Entwurfsstatus.

Hinweis:

- Wenn Sie weitere Felder hinzufügen möchten, wählen Sie die Felder aus, und fügen Sie sie direkt in Ihrem Fallbericht hinzu.
- Wenn Sie eine zugehörige Liste hinzufügen möchten, z. B. eine Liste erkennbarer Elemente, wählen Sie erkennbare Elemente aus. Alle erkennbaren Elemente, die diesem bestimmten Fall zugeordnet sind, werden aufgelistet. Wählen Sie mindestens ein erkennbares Element aus, und klicken Sie auf **Hinzufügen** . Sie können das erforderliche erkennbare Element auch herausfiltern und Ihrem Fall hinzufügen.

8. Klicken Sie Auf **Inhalt Speichern** Um den Inhalt Ihres Berichts zu speichern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Klicken Sie Auf **Vorschau** Um eine Vorschau des Berichts anzuzeigen.

Hinweis:
Sie können dann wie folgt vorgehen:

- **Maximieren** Das Berichtsfenster.
- **Herunterladen** Der Bericht mit **Herunterladen** Symbol.
- Klappen Sie den Bericht auf einer neuen Registerkarte aus, falls die Höhe oder Größe des Berichts eine bessere Anzeige ermöglichen soll.
- **Bearbeiten** Der Berichtsname und die Berichtsbeschreibung.
- **Veröffentlichen** Der Bericht.

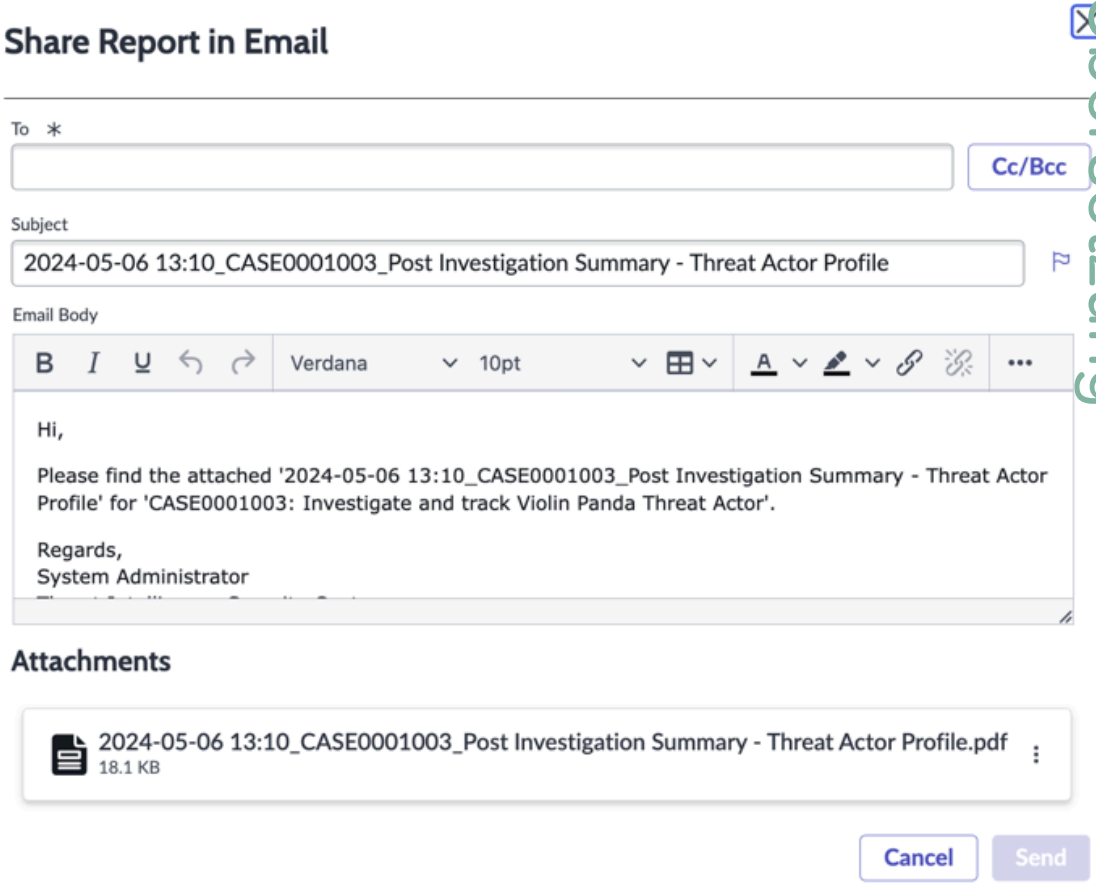
10. Klicken Sie Auf **Bearbeiten Sie Den Inhalt** Schaltfläche zum erneuten Veröffentlichen des Berichts.

Hinweis:
Eine Warnmeldung wird angezeigt, damit Sie den Bericht freigeben können:

Sie müssen den Bericht erneut veröffentlichen, nachdem Sie Änderungen vorgenommen haben, damit Sie den Bericht herunterladen oder freigeben können. Möchten Sie die Bearbeitung trotzdem fortsetzen?

11. Klicken Sie auf **Bearbeiten**.
Wenn Sie den Bericht bearbeiten möchten, können Sie den Bericht wie erläutert weiter bearbeiten oder den Bericht veröffentlichen. Sobald er veröffentlicht wurde, ist der Bericht schreibgeschützt.

12. Klicken Sie auf **Bericht in E-Mail freigeben** Um den Bericht freizugeben.
Beim Freigeben des Berichts wird der generierte PDF-Bericht als Anhang an die E-Mail



angehängt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Fügen Sie die erforderlichen E-Mail-Felder hinzu, z. B. für (für wen Sie den Bericht freigeben möchten), CC und BCC
14. Markieren Sie die E-Mail bei Bedarf als wichtig.
15. Klicken Sie auf **Senden**.
    Der Bericht wird für die größere Gruppe von Anwendern freigegeben.

Erstellen Sie einen Security Incident aus einem TISC Fall

Erstellen Sie Security Incidents, und ordnen Sie den Security Incidents erkennbare Elemente aus einem zu TISC Fall.

Vorbereitungen

Erforderliche Rolle: sn_si_Basic

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Alle Fälle werden angezeigt.
4. Öffnen Sie einen beliebigen Fall.
5. Klicken Sie Auf **Erstellen Sie Einen Security Incident** Schaltfläche.

   Hinweis:
   Auf der **Fallmanagement-Workbench** Die **Erstellen Sie Einen Security Incident** Die Schaltfläche ist nur für die Datensätze offener Fälle aktiviert und für die Datensätze geschlossener Fälle deaktiviert.

   Das Dialogfeld Security Incident erstellen wird angezeigt.
6. Füllen Sie das Formular mit den entsprechenden Incident-Details aus:

Details hinzufügen

Feld	Beschreibung
Kurzbeschreibung	Geben Sie eine Kurzbeschreibung des Security Incidents ein.
Beschreibung	Geben Sie eine Beschreibung des Security Incidents ein.
Kategorie	Definiert die Klassifizierung des Security Incidents.
Priorität	Definiert die Priorität des Security Incidents.
Unterkategorie	Definiert die Unterklassifizierung des Security Incidents basierend auf seiner Kategorie.
Zuweisungsgruppe	Gibt die Zuweisungsgruppe an, der der Security Incident zugewiesen werden soll.
Übergeordnet	Gibt den übergeordneten Security Incident an, der ein ist TISC Fall, aus dem diese Aktion ausgelöst wird.

7. Klicken Sie Auf **Als Nächstes** Um fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Sie müssen alle Pflichtfelder eingeben, die **Als Nächstes** Die Schaltfläche bleibt deaktiviert, bis Sie alle Pflichtfelder eingeben.

8. Wählen Sie die erkennbaren Elemente aus, die dem zugeordnet sind TISC Fall, um sie mit einem Security Incident zu verknüpfen, und klicken Sie dann auf **Als Nächstes** Um fortzufahren
9. Überprüfen Sie die Security Incident-Details und das erkennbare Element, das dem neu erstellten Security Incident zugeordnet wird, und klicken Sie dann auf **Erstellen** Um fortzufahren und den Security Incident zu erstellen.

Hinweis:
Eine Bestätigungsnachricht wird angezeigt, die angibt, dass der Security Incident erstellt wurde. Wenn Sie auf den Link klicken, gelangen Sie zum Security Incident in Arbeitsbereich für Security Incident Response.

Nachdem der Security Incident erstellt wurde, werden Sie zu weitergeleitet TISC **Artefakte** Registerkarte des Falls.

10. Wechseln Sie zu **Security Incidents** Abschnitt unter TISC **Artefakte** Registerkarte zum Anzeigen der Incidents.

Hinweis:
Arbeitsnotizen werden auch im veröffentlicht TISC Fallaktivitätenstrom, der angibt, dass der Security Incident (Security Incident-Nummer) mit erstellt wird, der zugeordnet ist TISC Erkennbare Elemente. Diese Arbeitsnotizen enthalten Details wie den Typ des erkennbaren Elements und den Wert des erkennbaren Elements.

Auf der Arbeitsbereich für Security Incident Response, Security Incident-Formular:

- Im Aktivitätenstrom werden Arbeitsnotizen veröffentlicht, die angeben, dass der Security Incident erfolgreich aus erstellt wurde TISC Fall. Diese Arbeitsnotizen enthalten auch einen Link zu TISC Fall, der bestätigt, dass die ausgewählten erkennbaren Elemente dem Security Incident zugeordnet wurden.
- Darüber hinaus können Sie dies auch überprüfen, indem Sie auf zugreifen **Zugehörige Datensätze** Registerkarte von Arbeitsbereich für Security Incident Response Und überprüfen Sie die Einträge erkennbarer Elemente unter **Bedrohungsinformationen** > **Zugehörige erkennbare Elemente**an. Von dort aus können Sie auch die zugehörigen erkennbaren Elemente unter anzeigen **TISC-Kontext** Abschnitt. Möglicherweise wurden diese erkennbaren Elemente direkt mit verknüpft TISC.

Laden Sie Sichere Dateianhänge Hoch

In diesem Abschnitt erfahren Sie, wie Sie die sicheren Dateianhänge in den Fall(e) hochladen.

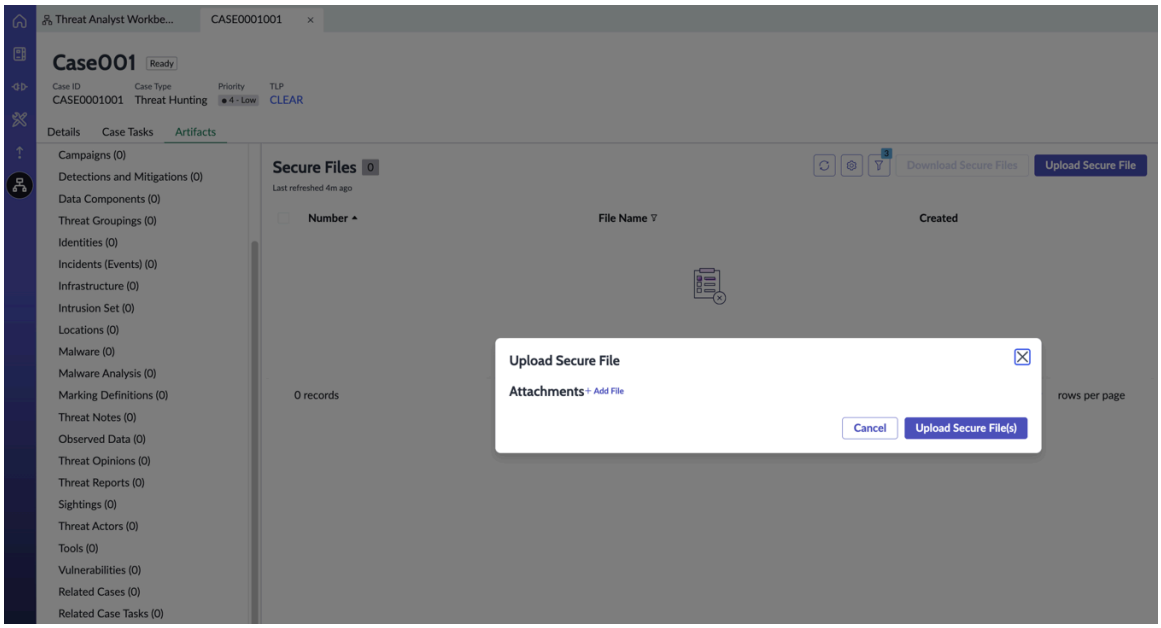
Vorbereitungen
Erforderliche Rolle: sn_sec_tisc_Secure_file_Access, sn_sec_tiscadmin

Hinweis:
Zugehörige Listen für sichere Dateien werden nur angezeigt, wenn Sie die Anwenderrolle sn_sec_tisc.secure_file_access innehaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Fallmanagement** > **Alle Fälle**an.
   Alle Fälle werden angezeigt.
4. Wählen Sie einen beliebigen Fall aus.
5. Gehe zu **Artefakte** > **Sichere Dateien** Zugehörige Listen.
6. Klicken Sie Auf **Sichere Datei Hochladen** Schaltfläche.
7. Klicken Sie Auf **Datei Hinzufügen** Zum Hinzufügen der Anhänge.
8. Wählen Sie die Dateien aus, und klicken Sie auf **Sichere Datei(en) hochladen** Schaltfläche.
   Die Dateianhänge werden hochgeladen.



9. Klicken Sie Auf **Sichere Dateien Herunterladen** Zum Herunterladen der Anhänge.
   Die Anhänge sind im ZIP-Format verfügbar.
10. Alternativ können Sie die Datei herunterladen, indem Sie zur Detailseite des sicheren Dateidatensatzes navigieren.

Hinweis:

- Alle sicheren Anhänge werden mithilfe des Key Management Framework (KMF) verschlüsselt und im System gespeichert. Weitere Informationen finden Sie unter Anhangsverschlüsselung .
- Wenn Anwender ein Abonnement für haben *ServiceNow IntegrationHub***Professionelles Paket-Installationsprogramm** , Sichere Dateien werden im ZIP-Format komprimiert und ebenfalls verschlüsselt und gespeichert

Threat Intelligence-Sicherheitszentrum Bibliothek

Eine Bedrohungsbibliothek ist definiert als eine Gruppe organisierter Objekte und Entitäten, die den Organisationen strukturierte und unstrukturierte Sicherheitsbedrohungsinformationen zur Verfügung stellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Bedrohungsinformationen sind in Form von Feeds verfügbar. Die Feeds bieten Ihnen wertvolle Bedrohungsdaten aus Quellen wie STIX, MISP usw., die Threat Intelligence-Entitäten auflisten.

Die Bibliothek des Threat Intelligence-Sicherheitszentrums erklärt, wie Sie die Daten durchsuchen, indem Sie grundlegende und erweiterte Suchvorgänge durchführen und Regeln filtern, den Importassistenten aufrufen, Threat Intelligence-Datensätze manuell hinzufügen und die erforderlichen Aktionen wie Hinzufügen von „Allow-Liste“, „Deny-Liste“ und „Beobachtungsliste“ ausführen.

Die Detailansicht bietet Einblicke in die Intelligence-Datensätze, und in Listenansichten können Sie schnelle Aktionen für einen oder mehrere Datensätze ausführen.

Verständnis des Datenmodells

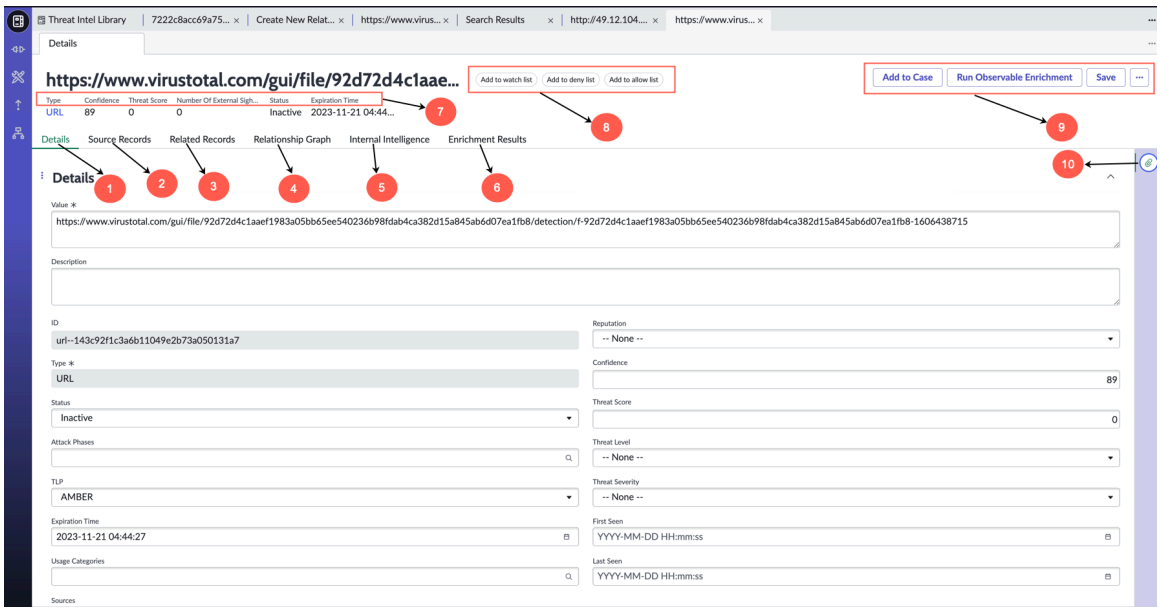
Das Datenmodell und die Architektur des Security Center-Moduls von Threat Intelligence unterstützen die Funktionen der Threat Intelligence-Plattform und verschiedene Sicherheitsansichten, die detaillierte Daten für Bedrohungsanalysten bereitstellen.

Das Datenmodell verfügt über die Datenstrukturen, die im Threat Intelligence-Repository als Objekte dargestellt werden.

TISC Formularansicht „Bibliotheksobjekte“

Die Threat Intelligence-Sicherheitszentrum Die Homepage von Objekten besteht aus den folgenden Funktionen.

Verwenden oder navigieren Sie zu diesen folgenden Abschnitten, um mehr über die einzelnen SDOs zu erfahren.



TISC Formularansicht „Bibliotheksobjekte“

Reihenfolge	Menü/Registerkarte	Beschreibung
1	Registerkarte **Details**	Verwenden Sie diesen Abschnitt, um die SDOs in der Formularansicht anzuzeigen oder zu bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TISC Formularansicht „Bibliotheksobjekte“ (Fortsetzung)

Reihenfolge	Menü/Registerkarte	Beschreibung
2	**Quelldatensätze** Registerkarte	Quelldatensätze tragen zu einem aggregierten Datensatz bei, wie in der Formularansicht angezeigt. Diese Quelldatensätze werden automatisch aus Feeds erstellt oder vom Anwender manuell erstellt.
3	Registerkarte **Zugehörige Datensätze**	Listet alle zugehörigen Datensätze auf, die dem SDO zugeordnet sind.
4	**Beziehungsdiagramm** Registerkarte	Visuelle Darstellung der zugehörigen Objekte.
5	**Interne Intelligenz** Registerkarte	Listet die internen Intelligence-Datensätze der zugeordneten Objekte auf.
6	**Ergänzungsergebnisse** Registerkarte	Listet die Ergänzungsintegrationen auf, die den Objekten zugeordnet sind.
7	**Formularbanner**	Dies ist ein schreibgeschützter Abschnitt, der die Schlüsselfelder wie Typ, Konfidenz, Bedrohungspunktzahl, Anzahl der Sichtungen, Status und Ablaufzeit enthält.
8	**UI-Aktionen des Formularbanners**	Dies sind die Sicherheitssteuerungslisten, auf die Sie klicken können, wenn sie der Allow-Liste hinzugefügt, aus der Allow-Liste entfernt (Deny-Liste) oder der Beobachtungsliste basierend auf den erkennbaren Elementen hinzugefügt werden müssen. Klicken Sie, um: • Zur Beobachtungsliste hinzufügen • Der Deny-Liste hinzufügen • Zur Allow-Liste hinzufügen **Hinweis:** Die Formularaktionen gelten nur für erkennbare Elemente.
9	**Formular-UI-Aktionen**	Die verfügbaren Formular-UI-Aktionen sind: 1. **Zu Fall hinzufügen** : Fügt dem Fall die Objekte hinzu. 2. **Ergänzung Erkennbarer Elemente Ausführen**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TISC Formularansicht „Bibliotheksobjekte“ (Fortsetzung)

Reihenfolge	Menü/Registerkarte	Beschreibung
		: Ergänzungen für die ausgewählten Objekte ausführen. 3. **Speichern** : Speichern Sie den Datensatz. 4. **Löschen** : Löschen Sie den Datensatz.
10	**Rechtes Kontextmenü**	Bietet einfachen Zugriff auf die Schnellsteuerungen wie Anhänge, Notizen usw. basierend auf den Aufgaben, die diesem Objekt zugeordnet sind. Diese Option ist auf den verbleibenden beiden Registerkarten verfügbar, auf die der Bedrohungsanalyst bei Bedarf zugreifen kann. Das Kontextmenü bietet eine einfache Navigation zu: 1. **Anhänge** : Anhängen Sie eine beliebige Datei an, die sich auf die Objekte bezieht. **Hinweis:** Wenn Sie entweder ein neues erkennbares Element, Indikatoren oder ein Objekt erstellen oder die vorhandenen Objekte anzeigen, wird das angezeigt **Anhänge** Der Bereich wird standardmäßig in der jeweiligen Formularansicht angezeigt. Sie können entweder auf klicken **Anhänge** Symbol im rechten Kontextmenü oder gehe zu **Einstellungen** > **Arbeitsbereiche** Und deaktivieren Sie **Sidebar anzeigen** . Weitere Informationen finden Sie unter Konfigurieren Sie die Einstellungen des Next Experience-Arbeitsbereichs .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TISC Formularansicht „Bibliotheksobjekte“ (Fortsetzung)

Reihenfolge	Menü/Registerkarte	Beschreibung
		2. Einblicke : Fügen Sie zusätzliche Informationen zu den erkennbaren Elementen oder Indikatoren hinzu, die diesem Objekt zugeordnet sind.
NA	**Suchen Sie im Navigator**	Verwenden Sie diese Suchfunktion, um in der Threat Intel (TI)-Bibliothek nach verschiedenen Objekten zu suchen. Sie können beispielsweise nach allen Datensätzen erkennbarer Elemente im TI-Bibliotheksmodul suchen.
NA	**In Bedrohungsinformationenbibliothek suchen**	Verwenden Sie diese Suchfunktion, um basierend auf Ihren Suchkriterien in mehreren Quellen nach den Quelldatensätzen zu suchen. Die Ergebnisse werden separat angezeigt **Suchergebnisse** Registerkarte. Wenn Sie beispielsweise für eine IP-Adresse 104.227.137.35 die Datensätze durchsuchen müssen, indem Sie 104.* eingeben, werden die Datensätze durch die Suche eingegrenzt und die Datensätze angezeigt, die die IP-Adresse beginnend mit 104 enthalten **Suchergebnisse** Registerkarte. • Sie können auch die vorhandenen Suchstichwörter in den Suchkriterien auf derselben Seite mit Suchergebnissen ändern, ohne zur Seite „Bedrohungsbibliothek“ zurückzukehren. • Ebenso können Sie auch basierend auf dem Namen und der Beschreibung eines bestimmten Datensatzes suchen. • Sobald die Datensätze gefiltert und aufgelistet wurden, können Sie auf die Listenansicht klicken, die Sie auf einer

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TISC Formularansicht „Bibliotheksobjekte“ (Fortsetzung)

Reihenfolge	Menü/Registerkarte	Beschreibung
		neuen Registerkarte zum entsprechenden Datensatz führt.

TISC-Bibliotheks-Repository

IOC-Repository enthält STIX-Objekte, jedes dieser Objekte enthält eine bestimmte Information.

Erkennbare Elemente

Erkennbare Elemente stellen statusbehaftete Eigenschaften (z. B. den MD5-Hash einer Datei oder den Wert eines Registrierungsschlüssels) oder messbare Ereignisse (z. B. die Erstellung eines Registrierungsschlüssels oder das Löschen einer Datei) dar, die für den Betrieb von Computern und Netzwerken relevant sind.

Im Folgenden finden Sie den Typ der in der Anwendung verfügbaren erkennbaren Elemente:

- Artefakt
- AS-Nummer
- Verzeichnis
- Domänenname
- E-Mail-Adresse
- E-Mail-Nachricht
- E-Mail-Betreff
- Datei
- IPv4-Adresse
- IPv4-CIDR
- IPv6-Adresse
- IPv6-CIDR
- MAC-Adresse
- MD5-Hash
- Mutex-Name
- Netzwerk
- Sonstiges erkennbares Element
- Prozess
- SHA1-Hash
- SHA256-Hash
- SHA512-Hash
- Software
- URL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwenderaccount
- Windows-Registrierungsschlüssel
- X.509-Zertifikat

Definieren Sie ein erkennbares Element

Erkennbare Elemente können aus der geplanten Feed-Erfassung oder aus dem Importassistenten abgerufen werden. Sie können jedoch erkennbare Elemente nach Bedarf erstellen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
2. Klicken Sie auf **Neu**.
3. Wählen Sie aus **Typ Des Erkennbaren Elements** .
   Das Formular „Neuen Datensatz erkennbarer Elemente erstellen“ wird angezeigt.

   Hinweis:
   Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

4. Füllen Sie im Formular die Felder aus.

   Hinweis:
   Wenn Sie entweder ein neues erkennbares Element erstellen oder die vorhandenen erkennbaren Elemente anzeigen, wird das angezeigt **Anhänge** Der Bereich wird standardmäßig in der Formularansicht angezeigt. Sie können entweder im rechten Kontextmenü auf das Symbol Anhänge klicken oder zu wechseln **Einstellungen** > **Arbeitsbereiche** Und deaktivieren Sie **Sidebar anzeigen** . Weitere Informationen finden Sie unter Konfigurieren Sie die Einstellungen des Next Experience-Arbeitsbereichs .

Abschnitt „Details“

Feld	Beschreibung
Wert	Der Wert (z. B. IP-Adresse oder Hash), der dem erkennbaren Element zugeordnet ist.
Beschreibung	Beschreibung des Datensatzes des erkennbaren Elements.
Autor	Geben Sie den Namen ein.
Typ	Der Klassifizierungstyp des erkennbaren Elements, z. B. IP-Adresse, Domänenname, Artefakt, Verzeichnis, Datei, oder Hash. Standardmäßig wird dies angezeigt, wenn Sie den neuen Datensatz ausgewählt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Der aktive oder inaktive Status des erkennbaren Elements.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
TLP	Eindeutiger Wert, der die Einstellung für die Datensensibilität pro TLP angibt.
Reputation	Gibt die schädliche Reputation des erkennbaren Elements an.
Status	Geben Sie den Status des erkennbaren Elements ein, ob aktiv oder inaktiv.
Bedrohungsbewertung	Gibt die Bedrohungspunktzahl für dieses erkennbare Element an.
Ablaufzeit	Gibt die Ablaufzeit des Datensatzes des erkennbaren Elements an.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Datensatz erstellt wird.
Vertrauen	Geben Sie die Konfidenz für diesen Datensatz des erkennbaren Elements ein. Die Konfidenzeigenschaft gibt die Konfidenz an, die der Ersteller in der Richtigkeit seiner Daten hat. Der Konfidenzwert MUSS eine Zahl im Bereich von 0–100 sein.
Systemupdates verhindern	Wenn Sie diese Kennzeichnung auf „wahr“ festlegen, wird verhindert, dass das System Werte von Feldern im Datensatz überschreibt.
Ist falsch positiv	Eine boolesche Kennzeichnung, die angibt, ob das erkennbare Element als falsch positiv identifiziert wird.

Attribute

Feld	Beschreibung
Auflösung	Gibt eine Liste von Verweisen auf eine oder mehrere IP-Adressen oder Domänennamen an, in die der Domänenname aufgelöst wird.
Ist FQDN	Ein vollqualifizierter Domänenname (FQDN) ist die vollständige Adresse eines Internethosts oder Computers. Es stellt seinen genauen Speicherort innerhalb des Domänennamenssystems (DNS) durch Angabe des Hostnamens, des Domänennamens und der Domäne der obersten Ebene (TLD) bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Informationen

Feld	Beschreibung
Bedrohungsstufe	Gibt die Bedrohungsstufe des Datensatzes des erkennbaren Elements an.
Erstmals aufgetreten	Der Zeitpunkt, zu dem dieser Datensatz des erkennbaren Elements erstmals schädliche Aktivitäten ausgeführt hat.
Bedrohungsschweregrad	Gibt den Bedrohungsschweregrad des Datensatzes des erkennbaren Elements an.
Zuletzt aufgetreten	Die Zeit, zu der dieser Datensatz des erkennbaren Elements zuletzt schädliche Aktivitäten ausgeführt hat.
Nutzungskategorien	Kategorien, unter die das erkennbare Element fällt, z. B. Botnet oder Phishing.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext hinzu.
Quellen	Gibt die Bedrohungsquelle an, aus der dieser Datensatz erstellt wird.

Wichtig:
Von Quelle Gemeldete Punktzahl : Dieses Feld enthält den aggregierten Wert der Bedrohungspunktzahlen, die von den Quellen gemeldet werden, aus denen das erkennbare Element erfasst wird. Um dieses Feld im Datensatzformular für erkennbare Elemente anzuzeigen, müssen Sie es manuell hinzufügen, da es standardmäßig nicht verfügbar ist.

Attribute

Feld	Beschreibung
Auflösung	Gibt eine Liste von Verweisen auf eine oder mehrere IP-Adressen oder Domänennamen an, in die der Domänenname aufgelöst wird.
Ist FQDN	Ein vollqualifizierter Domänenname (FQDN) ist die vollständige Adresse eines Internethosts oder Computers. Es stellt seinen genauen Speicherort innerhalb des Domänennamenssystems (DNS) durch Angabe des Hostnamens, des Domänennamens und der Domäne der obersten Ebene (TLD) bereit.

Hinweis:
Löst Auf Und **Ist FQDN** Attribute gelten nur für **Domänenname** Typ der erkennbaren Elemente.

Typattribute Des Erkennbaren Elements

Attributname	Attributtypen
Artefakt	○ Entschlüsselungsschlüssel ○ Verschlüsselungsalgorithmus

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attributname	Attributtypen
	○ MD5-Hash ○ MIME-Typ ○ SHA1-Hash ○ SHA256-Hash ○ SHA512-Hash ○ URL
AS-Nummer	○ Name ○ RIR
Verzeichnis	○ Verzeichniserstellungszeit ○ Zeit des letzten Zugriffs auf das Verzeichnis ○ Zeit der letzten Bearbeitung des Verzeichnisses ○ Codierter Pfad
Domänenname	○ Ist FQDN ○ Auflösung
E-Mail-Adresse	○ Anzeigename ○ E-Mail-Text ○ E-Mail-Empfänger Bcc ○ E-Mail-Empfänger CC ○ E-Mail-Empfänger an ○ E-Mail-Absender ○ E-Mail-Betreff ○ Sendedatum
Datei	○ Zusätzliche Informationen ○ Codierter Dateiname ○ Zeitpunkt der Dateierstellung ○ Zeitpunkt des letzten Dateizugriffs ○ Zeitpunkt der letzten Änderung ○ Magische Nummer Des Dateinamens ○ MD5-Hash ○ MIME-Typ ○ SHA1-Hash ○ SHA256-Hash ○ SHA512-Hash

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attributname	Attributtypen
IPv4-Adresse	○ AS-Nummer ○ MAC-Adresse
IPv4-CIDR	○ AS-Nummer ○ MAC-Adresse
IPv6-Adresse	○ AS-Nummer ○ MAC-Adresse
IPv6-CIDR	○ AS-Nummer ○ MAC-Adresse
Netzwerk	○ Zielbytes ○ Anzahl Der Zielpakete ○ Ziel-Port ○ Endzeit ○ Länge des HTTP-Nachrichtentexts ○ HTTP-Anforderungsheader ○ HTTP-Anforderungsmethode ○ HTTP-Anforderungswert ○ HTTP-Anforderungsversion ○ ICMP-Code-Byte ○ ICMP-Typ-Byte ○ Ist Netzwerk aktiv ○ Socket-Blockierung ○ Socket-Zuhörvorgang ○ Netzwerkprotokolle ○ Socket-Adressenfamilie ○ Socket-Deskriptor ○ Socket-Handle ○ Socket-Optionen ○ Anzahl Der Socket-Typ-Quellbytes ○ Anzahl der Quellpakete ○ Quell-Port ○ Startzeit ○ TCP-Ziel-Kennzeichnungen ○ TCP-Quell-Kennzeichnungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attributname	Attributtypen
Prozess	○ ASLR aktiviert ○ Befehlszeile ○ Aktuelles Arbeitsverzeichnis (Current Working Directory, CWD) ○ DEP aktiviert ○ Umgebungsvariablen ○ Ausgeblendet ○ Besitzer-SID ○ Prozess-ID ○ Priorität ○ Verarbeitungszeit des Prozesses ○ Servicebeschreibungen ○ Anzeigename für Service ○ Name der Servicegruppe ○ Servicename ○ Servicestarttyp ○ Servicestatus Servicetyp ○ Startinformation ○ Windows-Integritätsstufe ○ Fenstertitel
Software	○ Common Platform Enumeration (CPE) ○ Unterstützte Sprachen ○ Softwareidentifizierung (SWID) ○ Lieferantenversion
Anwenderaccount	○ Account-Erstellungszeit ○ Account-Ablaufzeit ○ Account-Anmeldung ○ Kontotyp ○ Zusätzliche Informationen ○ Kann Berechtigungen eskalieren ○ Zeit der letzten Änderung der Anmeldeinformationen ○ Anzeigename ○ Zeit der ersten Anmeldung ○ Ist Account deaktiviert ○ Ist berechtigt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attributname	Attributtypen
	○ Ist Serviceaccount ○ Zeitpunkt der letzten Anmeldung ○ Anwender-ID
Windows-Registrierungsschlüssel	○ Schlüssel Geändert ○ Zeitregistrierungswert ○ Anzahl der Unterschlüssel
X.509-Zertifikat	○ Zusätzliche Informationen ○ Bezeichner des regulatorischen Schlüssels ○ Grundlegende Einschränkungen ○ Zertifizierungsrichtlinien ○ CRL-Verteilungspunkte ○ Erweiterte Schlüsselnutzung ○ Beliebige Richtlinie sperren ○ Bearbeiter ○ Alternativer Ausstellername ○ Ist selbstsigniert ○ Schlüsselnutzung ○ Nameneinschränkungen ○ Richtlinieneinschränkungen ○ Richtlinienzuordnungen ○ Nutzung des privaten Schlüssels gültig ab ○ Nutzung des privaten Schlüssels gültig bis ○ Signaturalgorithmus ○ Betreff ○ Alternativer Antragstellername ○ Attribute des Betreffverzeichnisses ○ Antragstellerschlüssel-Bezeichner ○ Algorithmus des Antragstellers des öffentlichen Schlüssels ○ Exponent des Antragstellers des öffentlichen Schlüssels ○ Modulo des öffentlichen Schlüssels des Antragstellers ○ Gültig ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attributname	Attributtypen
	○ Gültig bis ○ Version

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für einen Datensatz erkennbarer Elemente hinzu.

5. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
6. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die einem erkennbaren Element zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie die Taxonomie aus, die einem erkennbaren Element zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie die Taxonomiewerte hinzu, die einem erkennbaren Element zugeordnet sind.

Quelldatensätze

Feld	Beschreibung
Die Quelldatensatzdetails für ein erkennbares Element werden angezeigt, falls vorhanden.	

Nächste Maßnahme

Die folgende Tabelle listet die zugehörigen Datensätze auf, die sich auf die erkennbaren Elemente beziehen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze

Zugehörige Liste	Beschreibung
Erkennbares Element	Liste der erkennbaren Elemente, die sich auf dieses erkennbare Element beziehen. **Hinweis:** Dieser Abschnitt enthält auch die potenziellen Beziehungen zwischen zwei erkennbaren Elementen. Weitere Informationen finden Sie unter Bestätigen Sie die potenzielle Beziehung zwischen erkennbarem Element und erkennbarem Element Und siehe Definieren Sie Beziehungen zwischen erkennbarem Element und erkennbarem Element Für die bestätigten Beziehungen zwischen den beiden erkennbaren Elementen.
Indikatoren	Liste der Indikatoren, die sich auf dieses erkennbare Element beziehen.
Angriffsmuster	Liste der Angriffsmuster, die sich auf dieses erkennbare Element beziehen.
Kampagnen	Listen Sie die Kampagnen auf, die sich auf dieses erkennbare Element beziehen.
Infrastruktur	Listen Sie die Infrastruktur auf, z. B. Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen, die sich auf dieses erkennbare Element beziehen.
Angriffssätze	Listen Sie die Angriffssätze auf, z. B. eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften, die sich auf dieses erkennbare Element beziehen.
Malware	Listen Sie die Malware-Quelldatensätze auf, die sich auf dieses erkennbare Element beziehen.
Bedrohungsakteure	Listen Sie die Bedrohungsakteure auf, die sich auf dieses erkennbare Element beziehen.
Bedrohungsereignisse	Listen Sie die Bedrohungsereignisse auf, die sich auf dieses erkennbare Element beziehen.
Schwachstellen	Wenn das erkennbare Element eine IP-Adresse ist, zeigt diese Liste alle Ressourcen (Konfigurationselemente) an, die eine übereinstimmende IP-Adresse haben, die sich auf dieses erkennbare Element beziehen.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Auch aus dem **Zugehörige Datensätze** Abschnitt können Sie die Beziehungen zwischen zwei erkennbaren Elementen mit bestätigen **Potenzielle Beziehungen** Abschnitt verfügbar auf **Erkennbare Elemente** Formularansicht. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
3. Sie können Fälle erkennbare Elemente hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.
4. Sie können auch Ergänzungsaktionen für erkennbare Elemente ausführen. Weitere Informationen finden Sie unter Führen Sie Anreicherungsaktionen in einem Fall aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quelldatensätze erkennbarer Elemente

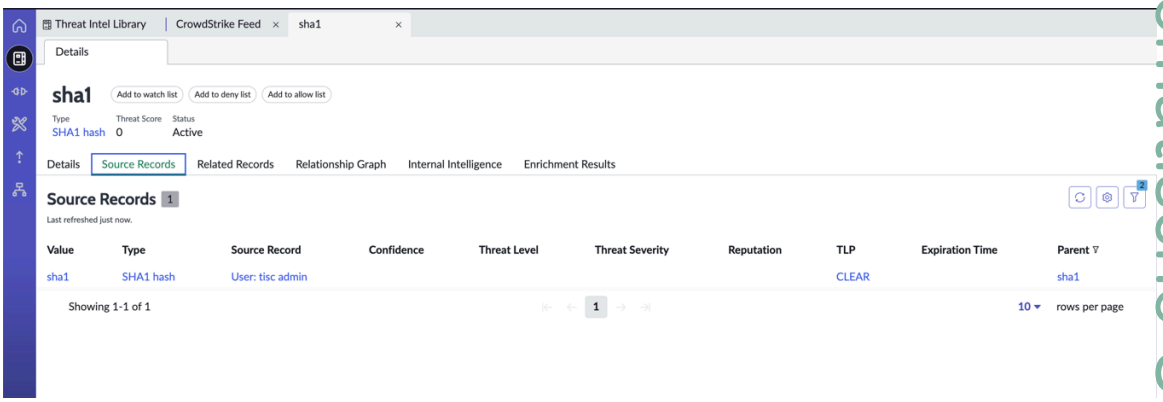
Die Quelldatensätze tragen zu einem aggregierten Datensatz bei, wie in der Formularansicht angezeigt. Diese Quelldatensätze werden automatisch aus Feeds erstellt oder vom Anwender manuell erstellt.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
4. Wählen Sie ein oder mehrere erkennbare Elemente aus.
5. Wechseln Sie zu **Quelldatensätze** .
   Die Quelldatensätze eines aggregierten Datensatzes werden angezeigt.



6. Zeigen Sie die Datensätze an.

Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze

Verknüpfen Sie die Datensätze, die sich auf die entsprechenden Threat Intelligence-Objekte beziehen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
2. Wählen Sie als Beispiel einen beliebigen Datensatz erkennbarer Elemente aus.
3. Wechseln Sie zu **Zugehörige Datensätze** Abschnitt.
4. Wählen Sie einen beliebigen zugehörigen Datensatz aus.
5. Klicken Sie Auf **Link** .
   Das Dialogfeld Objekte verknüpfen wird angezeigt.
6. Wählen Sie die Objekte aus der Liste aus, und klicken Sie auf **Link** Schaltfläche.
   Die Objekte, die einem Datensatz eines erkennbaren Elements zugeordnet sind, werden verknüpft und in der Listenansicht zugehörige Datensätze angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Speichern**.
   Klicken Sie Auf **Verknüpfung Aufheben** Schaltfläche zum Aufheben der Verknüpfung der Objekte

Rufen Sie Daten Erkennbarer Elemente Ab

Rufen Sie die zugehörigen Datensatzdaten erkennbarer Elemente ab.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Erkennbare Elemente** .
   Die zugehörigen erkennbaren Elemente, die diesem ausgewählten Objekt zugeordnet sind, werden angezeigt.
4. Wählen Sie einen beliebigen Datensatz erkennbarer Elemente aus.
   Wenn den angegebenen erkennbaren Elementen CVEs zugeordnet sind, können Sie die zugehörigen angreifbaren Daten automatisch über die angegebene Schaltfläche abrufen, und diese zugehörigen Datensätze werden im Abschnitt „Geschäftskontext“ der Schwachstellen angezeigt.
5. Gehe zu **Interne Intelligenz** > **Einträge für angreifbare Elemente**an.
   Die zugehörigen CVEs-Datensätze für die erkennbaren Elemente werden angezeigt.
6. Wählen Sie ein beliebiges CVE aus, und klicken Sie auf **Rufen Sie schwachstellenbezogene Daten ab** Schaltfläche.

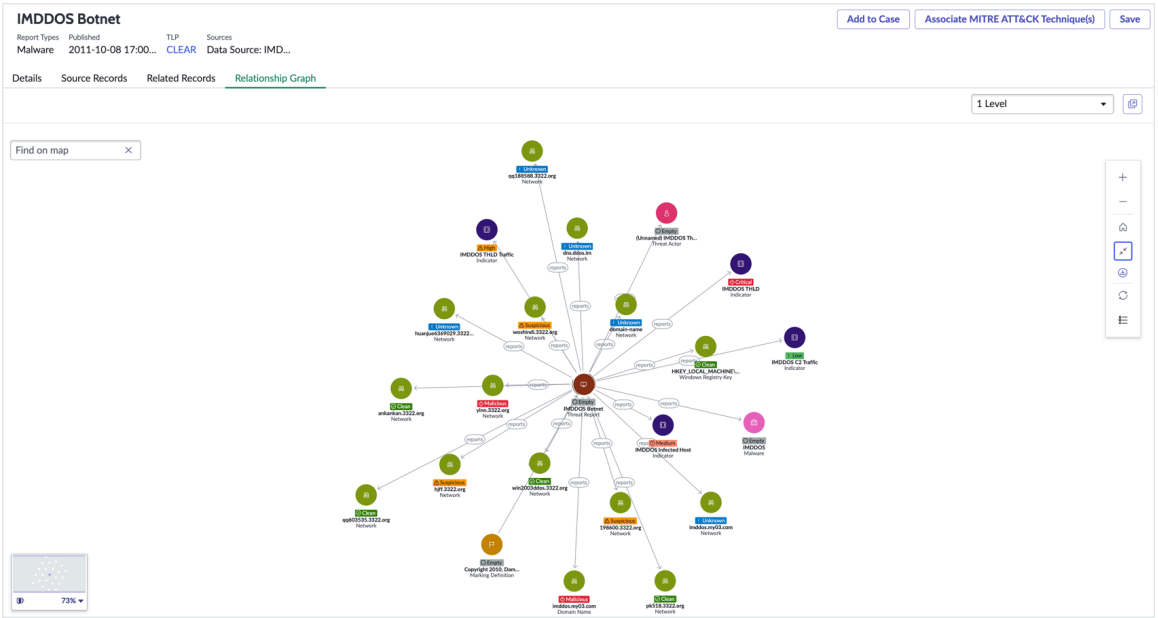
Hinweis:

- Eine Informationsnachricht zeigt an, dass diesem spezifischen Schwachstellenobjekt keine Einträge für angreifbare Elemente zugeordnet sind. Sie müssen die Objekte den angreifbaren Einträgen zuordnen, um die Daten abzurufen. Weitere Informationen finden Sie unter . Rufen Sie Schwachstellendaten Ab Informationen zum Verknüpfen der Datensätze und zum Ausführen der geplanten Aufgabe zum Abrufen der Daten. Weitere Informationen zu geplanten Aufgaben finden Sie unter Geplante Aufgaben .
- Diese Schaltfläche löst eine geplante Hintergrundaufgabe aus, und die Details zur Auftragsinitiierung und -Ausführung werden im Abschnitt „Aktivitätenstrom“ angezeigt. Wenn der Auftrag beispielsweise ausgelöst wird, zeigt der Aktivitätenstrom eine Aktivität an, die mit dem Abrufen zugeordneter Daten mit den Einträgen für angreifbare Elemente begonnen hat. Die geplante Hintergrundaufgabe überprüft kontinuierlich nach erkennbaren Elementen, denen angreifbare Einträge zugeordnet sind, und wird automatisch ausgeführt. Diese geplante Aufgabe wird alle eine Stunde ausgeführt. Wenn die Datensätze nicht abgerufen werden, können Sie die Datensätze manuell verknüpfen und die Daten abrufen.

Zeigen Sie Details in Visualizer an

Mit der Visualisierung können Sie die Beziehungen zwischen Objekten, erkennbaren Elementen und Indikatoren anzeigen, die Ihnen Kontext zur weiteren Untersuchung bieten. Die Visualisierung verwendet Farben und Symbole, um verschiedene Informationen zu den Objekten zu veranschaulichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können dann wie folgt vorgehen:

- Vergrößern Sie ein beliebiges Objekt, passen Sie es in den Bildschirm ein, ziehen Sie die Knoten, oder heften Sie sie an, um sich auf eine bestimmte Beziehung zu konzentrieren.
- Klicken Sie auf ein beliebiges Objekt, um den Detailbereich zu öffnen. Im Detailbereich finden Sie weitere Informationen, die dem Objekt zugeordnet sind. Sie können die Knoteneigenschaften wie Objekt, Objektname, Beschreibung und Quellen anzeigen. Standardmäßig wird der Detailabschnitt jedes Diagrammknotens nicht angezeigt, und Sie müssen auf jeden Knoten im Diagramm klicken, um die Details des ausgewählten Knotens anzuzeigen.

  Hinweis:
  Die Visualisierung ist für alle STIX Domain Objects (SDOs) mit Ausnahme der beobachteten Datenobjekte verfügbar. Klicken Sie Auf **Aktualisieren** Schaltfläche zum Aktualisieren der Visualisierung.

- Sie können auch auf das Popout-Symbol klicken, um das Diagramm in einem viel größeren Fenster anzuzeigen.

Verknüpfen Sie Knotenaktionen im Beziehungsdiagramm

Fügen Sie neue zugehörige Datensätze hinzu, um die Knoten zu verknüpfen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

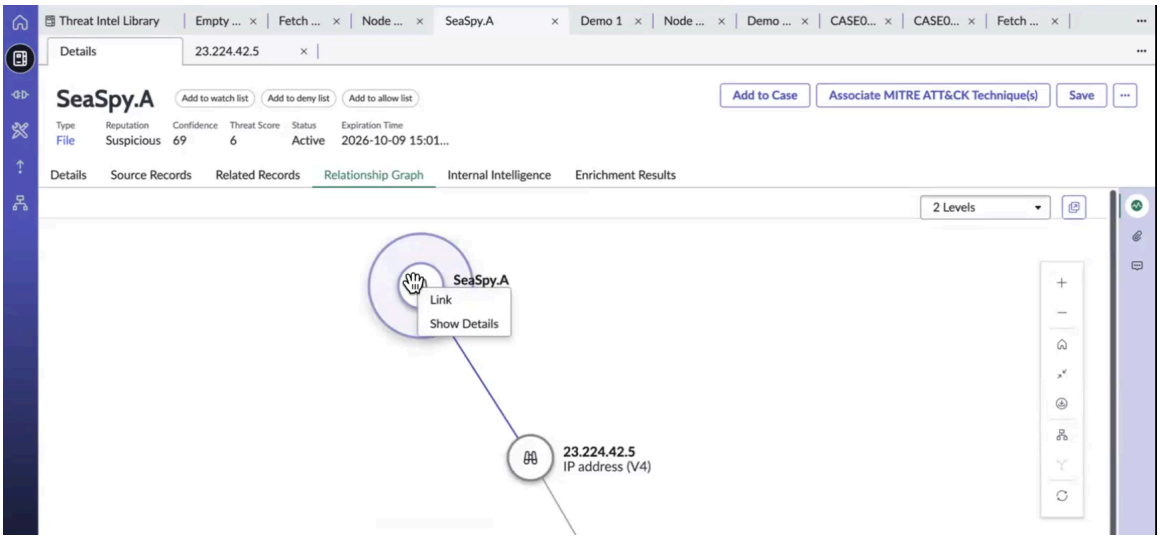
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
2. Wählen Sie als Beispiel einen beliebigen Datensatz erkennbarer Elemente aus.
3. Wechseln Sie zu **Beziehungsdiagramme** Abschnitt.
4. Klicken Sie auf den Knoten.
5. Klicken Sie Auf **Link** .

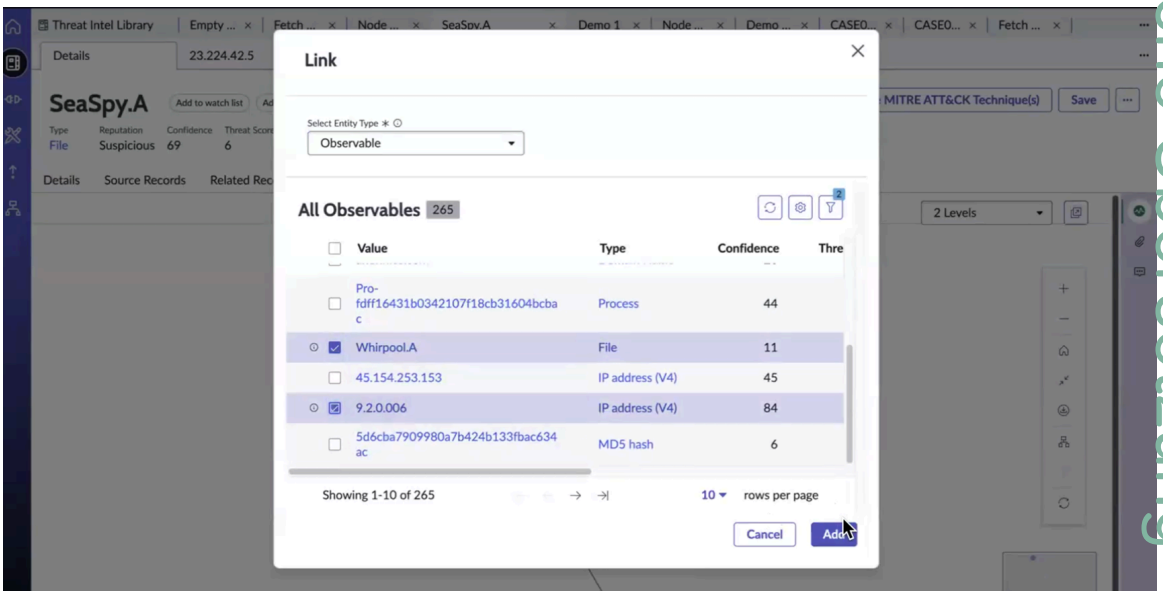
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Diese Aktion ist nur auf Startknotenebene verfügbar.



6. Wählen Sie den Entitätstyp aus, z. B. erkennbares Element.
7. Wählen Sie mindestens ein erkennbares Element für den übergeordneten Knoten aus.
8. Klicken Sie auf **Hinzufügen**.
   Die erkennbaren Elemente werden dem übergeordneten Knoten hinzugefügt.



9. Wählen Sie Aus **Verknüpfung Aufheben** Um die Verknüpfung der zugehörigen Datensätze mit den Knoten aufzuheben.

Hinweis:
Die zugehörigen Datensatzdaten werden nicht verknüpft, aber diese Beziehungen zwischen dem Startknoten und dem erkennbaren Element sind weiterhin in der Threat Intelligence-Bibliothek vorhanden.

10. Wählen Sie Aus **Details anzeigen** Um die zugehörigen Daten erkennbarer Elemente anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeiten mit internen Intelligence-Datensätzen

Verwenden Sie diese Funktion, um mit den internen Intelligenzdaten zu arbeiten, die aus dem Configuration Database Management System (CMDB) im Threat Intelligence-Sicherheitszentrum erfasst werden.

Interne Intelligence-Datensätze Anzeigen

Zeigen Sie die internen Intelligence-Datensätze an, die von CMDB, Security Incident Response (SIR), Vulnerability Response (VR) dieser Datensätze erfasst wurden.

Vorbereitungen

Der Abschnitt „interne Intelligenz“ stellt den Kontext aus anderen Anwendungen auf der Plattform bereit, z. B. SIR, VR und CMDB, um Analysten eine breitere Perspektive der Bedrohung zu bieten.

Erforderliche Rolle: sn_sec_tisc.Analyst

Hinweis:
Die Registerkarte „interne Intelligenz“ ist nur für erkennbare Elemente und Schwachstellenobjekte sichtbar.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
2. Wählen Sie einen Datensatz für erkennbare Elemente aus.
3. Wechseln Sie zu **Interne Intelligenz** Registerkarte.
   Der Abschnitt „interne Intelligenz“ umfasst drei Unterabschnitte wie Security Incident Response, Business Context, Vulnerability Response.

   Hinweis:
   Sie müssen die entsprechenden Anwendungen auf Ihrer Instanz installiert haben, damit diese Abschnitte in aufgelistet werden **Interne Intelligenz** Registerkarte.

   a. **Security Incident Response** : Zeigt alle Incidents an, die mit den zugehörigen erkennbaren Elementen und Schwachstellenelementen verknüpft sind.

   Hinweis:
   Der Wert des erkennbaren Elements/der erkennbaren Elemente muss zwischen dem SIR-Incident und auch innerhalb der TISC übereinstimmen. Dann werden die zugehörigen erkennbaren Elemente oder Indikatoren im Abschnitt „Security Incident Response“ aufgeführt. Sie können die Datensätze auch verknüpfen und deren Verknüpfung aufheben, indem Sie die Datensätze in den Quellsystemen durchsuchen. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.

   - Wählen Sie einen beliebigen Datensatz aus, um im Quellsystem zu navigieren und die Details anzuzeigen. Zum Beispiel zugeordnete erkennbare Elemente in Security Incident Response, um die zugehörigen Datensätze erkennbarer Elemente abzurufen.
   - Als Teil des aktuellen Release finden Sie im Folgenden die Intelligence-Daten, die Sie aus den Quelldatensätzen (SIR) abrufen können:
     - Zugehörige erkennbare Elemente
     - Schwachstellenelemente

   b. **Geschäftskontext** : Zeigt die betroffenen Anwender und alle anderen Konfigurationselemente an. Als Teil des aktuellen Release finden Sie im Folgenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Intelligence-Daten, die Sie aus den Quelldatensätzen (Geschäftskontext) abrufen können:

- Konfigurationselemente
- Betroffene Services
- Betroffene Assets

c. **Vulnerability Response** : Zeigt die Schwachstellen Intelligence-Daten an.

Schwachstelleneinträge: Diese Option stimmt mit den Schwachstellen überein und ruft die zugehörigen Datensätze ab.

Führen Sie Anreicherungsaktionen aus einem erkennbaren Element aus

In diesem Abschnitt erfahren Sie, wie Ergänzungsaktionen für erkennbare Elemente und andere Objekte ausgeführt werden.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
4. Klicken Sie über die Schaltfläche „Teilen“ auf eine beliebige Anreicherungsaktion.
5. Wählen Sie die verfügbaren Implementierungen aus.
6. Klicken Sie auf **Absenden**.
   Beispiel: Bedrohungssuche ausführen. Die ausgewählte Ergänzungsaktion wird ausgeführt, und es wird eine Informationsnachricht angezeigt, die angezeigt wird Die Ausführung der Ergänzung erkennbarer Elemente wurde für die ausgewählten erkennbaren Elemente gestartet. Ergebnisse sind auf der Detailseite der jeweiligen erkennbaren Elemente verfügbar, sobald die Ausführung abgeschlossen ist .

Hinweis:
Sobald die Ausführung initiiert oder abgeschlossen ist, werden Arbeitsnotizen im Aktivitätenstrom der Formularansicht veröffentlicht.

Dem Fall hinzufügen

Fügen Sie dem Fall erkennbare Elemente, Indikatoren oder andere Objekte hinzu.

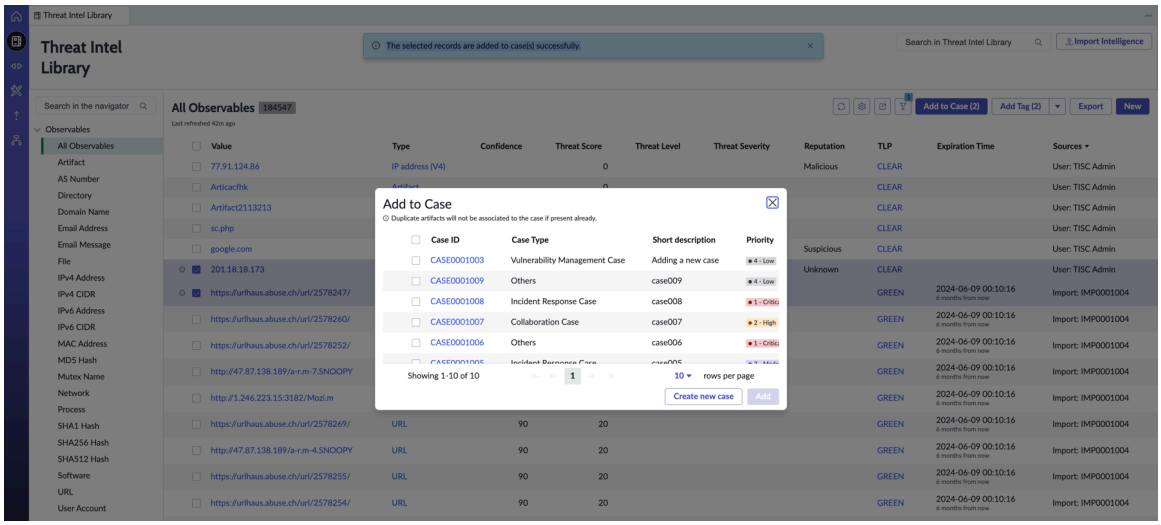
Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Im Folgenden finden Sie das Verfahren, das zeigt, wie ein Fall zu einem Datensatz eines erkennbaren Elements hinzugefügt wird.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
2. Wählen Sie die erkennbaren Elemente aus.
3. Klicken Sie Auf **Zu Fall hinzufügen** Schaltfläche.
   Dadurch werden nur die Fälle angezeigt, in denen der Datensatz noch nicht zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Überprüfen Sie, ob Sie den Datensatz den vorhandenen Fällen hinzufügen möchten, und wählen Sie dann den ausgehenden Fall aus, andernfalls klicken Sie auf **Erstellen Sie Einen Neuen Fall** .
Erstellen Sie einen neuen Fall, indem Sie die folgenden Informationen eingeben.

Neuen Fall erstellen

Feld	Beschreibung
Fall-ID	Ein eindeutiger Bezeichner für den Fall. Dies ist eine vom System generierte ID.
Kurzbeschreibung	Zusammenfassung der Anforderung oder des Problems, die bzw. das untersucht wird, oder eine kurze Beschreibung.
Falltyp	Wählen Sie den Typ des untersuchten Falls aus. Die möglichen Optionen für die Untersuchung sind: ○ Bedrohungssuche ○ Informationsanforderung ○ Schwachstellenmanagement-Fall ○ Compliance-Fall ○ Fall vom Typ „Reaktion auf Incidents“ ○ Zusammenarbeitsfall ○ Andere
Priorität	Eine Bewertung des Schweregrads der Anforderung oder des Problems.
Zuweisungsgruppe	Die zugewiesene Gruppe, die für die Bearbeitung des Falls verantwortlich ist.
Zugewiesen an	Der Analyst, der für die Bearbeitung eines Falls verantwortlich ist.

5. Klicken Sie Auf **Erstellen** Wenn Sie einen neuen Fall erstellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Der neue Fall wird der vorhandenen Fallliste hinzugefügt.

6. Wählen Sie die neu hinzugefügten Fälle aus.
7. Klicken Sie auf **Hinzufügen**.
   Es wird eine Informationsnachricht angezeigt, dass die ausgewählten Datensätze erfolgreich zu Fällen hinzugefügt wurden.

Führen Sie Anreicherungsvorgänge in TISC aus

Die folgende Tabelle beschreibt die Interaktionen, die bei der Ausführung verschiedener Ergänzungsvorgänge von TISC beteiligt sind.

Modale TISC-Bildschirme

Fähigkeit	UX-Frameworks-Interaktionen	Integrationen unterstützt
Bedrohungssuche durchführen	Auf Bildschirm 1: Wählen Sie die Implementierung(en) aus, und übermitteln Sie sie. Es gibt keine allgemeinen Eingaben oder implementierungsspezifischen Eingaben, die für die Ausführung der Bedrohungssuche gelten.	• Viren insgesamt • Crowd Strike Falcon Intelligence
Sichtungssuche ausführen	Bildschirm 1 – Implementierungen auswählen und Bildschirm 2 – Allgemeine Eingaben sind anwendbar. Die Sichtungssuche verwendet die Datums- und Uhrzeithäufigkeit als allgemeine Eingaben für mehrere Implementierungen von Splunk und anderen Integrationen.	• Elastische Suche • Splunk-Sichtung
Anreicherung erkennbarer Elemente durchführen	Nur Bildschirm 1: Implementierungen Auswählen. Es gibt keine allgemeinen Eingaben oder implementierungsspezifischen Eingaben, die für die Ausführung der Anreicherung erkennbarer Elemente gelten.	• WHOIS • Shodan

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedrohungssuche durchführen

Wählen Sie eine oder mehrere Implementierungen aus, um die Bedrohungssuche für erkennbare Elemente auszuführen.

Vorbereitungen

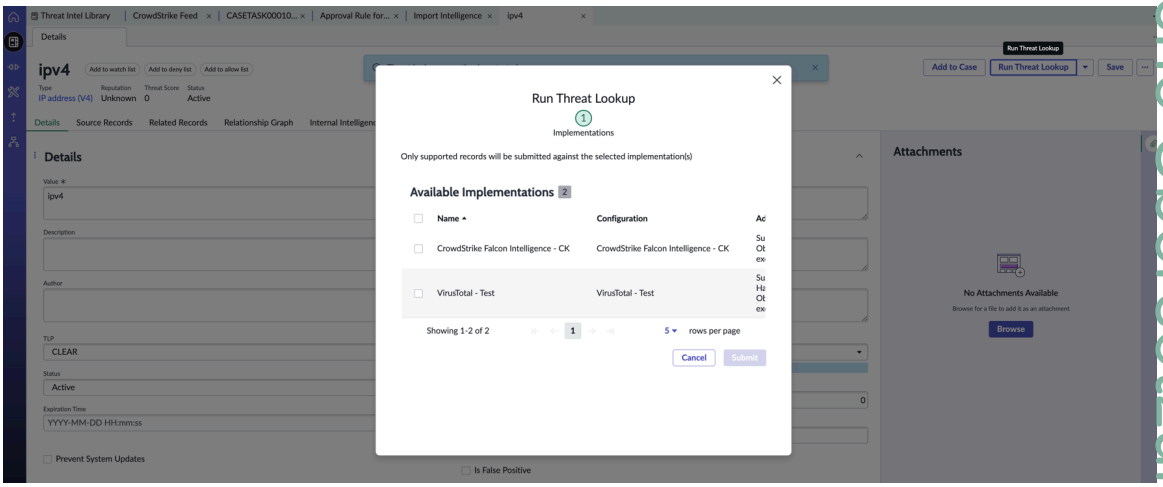
Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
4. Öffnen Sie einen beliebigen Datensatz erkennbarer Elemente.
5. Klicken Sie Auf **Bedrohungssuche Ausführen** .
   Die Bedrohungssuche Ausführen **Wählen Sie Implementierungen Aus** Der modale Bildschirm wird angezeigt.

   Hinweis:
   Die Bedrohungssuche ausführen führt die Threat Intelligence-Suchen durch, um zu bestimmen, ob die erkennbaren Elemente bekannten Bedrohungen zugeordnet sind.

6. Wählen Sie die erforderliche(n) Implementierung(en) aus der Liste aus.



7. Klicken Sie auf **Absenden**.
   Die ausgewählte Ergänzungsaktion wird ausgeführt, und es wird eine Informationsnachricht angezeigt, die angezeigt wird Ausführung der Bedrohungssuche wurde gestartet.

   Hinweis:

   - Sobald die Ausführung initiiert oder abgeschlossen ist, werden Arbeitsnotizen im Aktivitätenstrom der Formularansicht veröffentlicht.
   - Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse finden Sie in **Ergänzungsergebnisse** Registerkarte der entsprechenden Detailseite für erkennbare Elemente im TISC-Arbeitsbereich.
   - Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse können mit identifiziert werden **Quelle** Feld der Ergänzungsergebnistabelle.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichtungssuche ausführen

Führen Sie die zugehörige Integration „Sichtungssuche ausführen“ durch.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

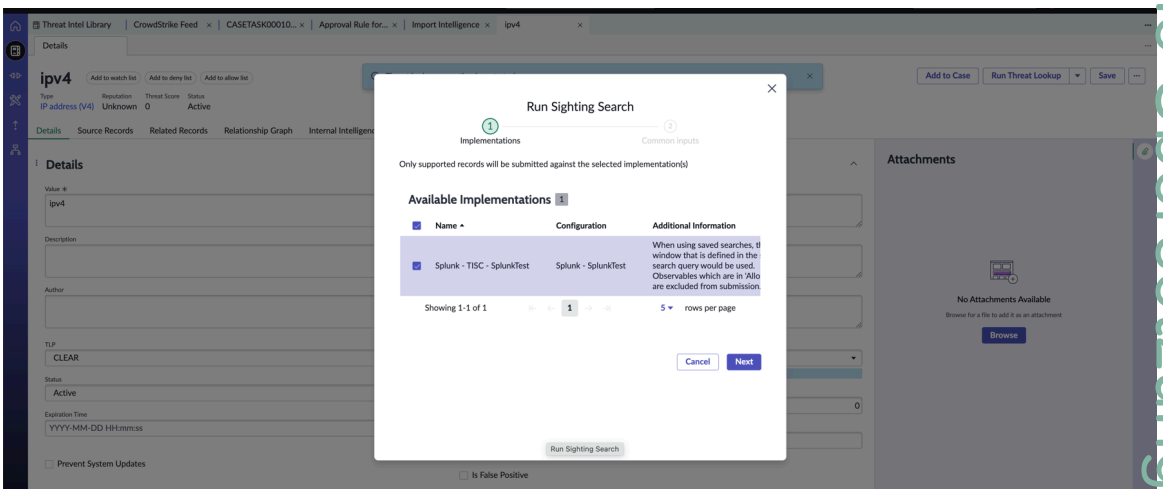
Um diese Aktion auszuführen, wählen Sie die Implementierung aus, und fügen Sie allgemeine Laufzeiteingaben hinzu, die für alle ausgewählten Implementierungen gelten.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
4. Öffnen Sie einen beliebigen Datensatz erkennbarer Elemente.
5. Klicken Sie Auf **Sichtungssuche Ausführen** .
   Die Sichtungssuche Ausführen **Wählen Sie Implementierungen Aus** Der modale Bildschirm wird angezeigt.

   Hinweis:
   Die Sichtungssuche ausführen führt die Threat Intelligence-Suchen durch, um zu bestimmen, ob die erkennbaren Elemente bekannten Bedrohungen zugeordnet sind.

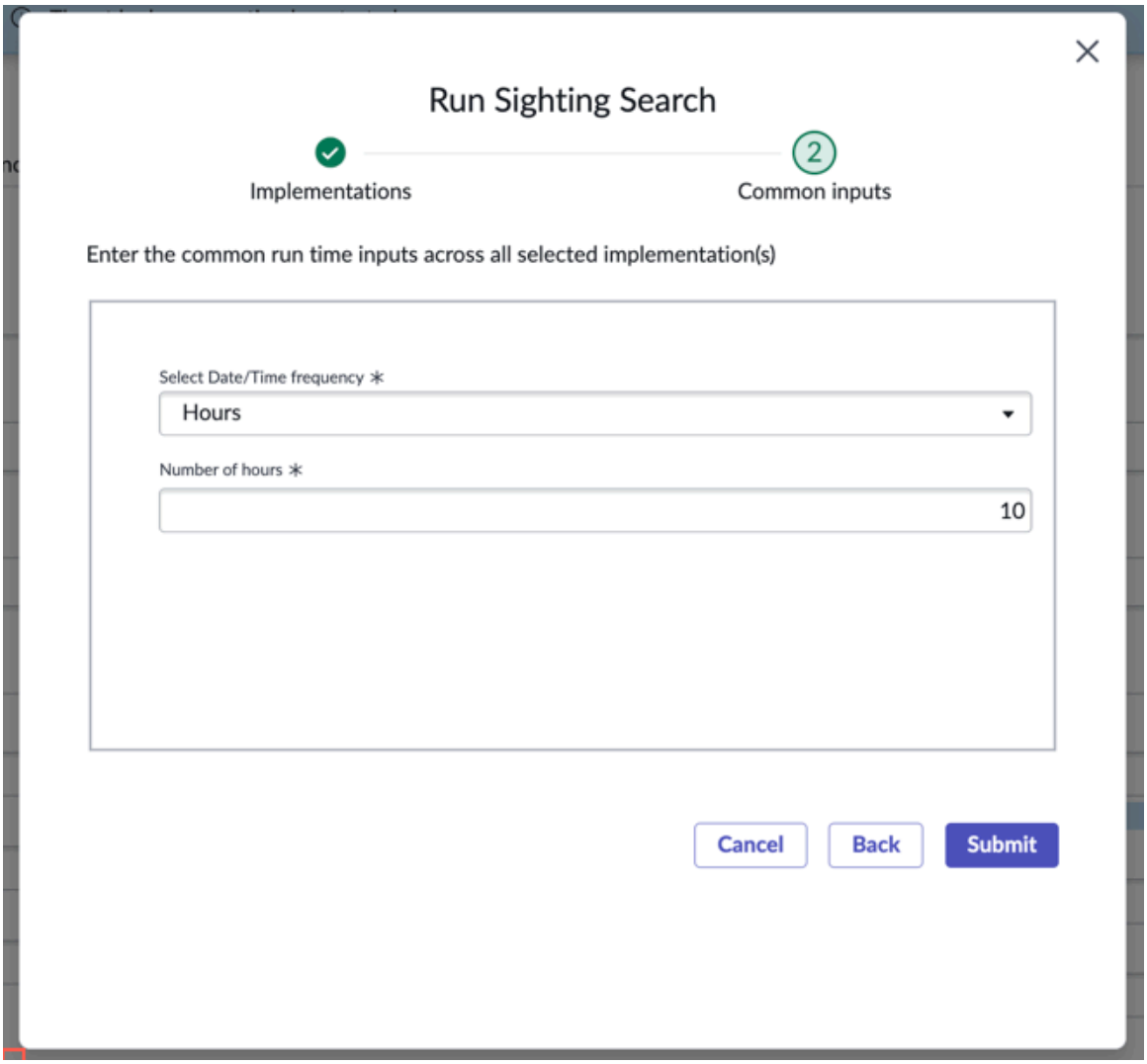
6. Wählen Sie die erforderliche(n) Implementierung(en) aus der Liste aus.



7. Klicken Sie auf **Next (Weiter)**.
8. Wählen Sie den allgemeinen Eingabewert für die Laufzeit aus, z. B. Häufigkeit für Datum/Uhrzeit auswählen und Anzahl der Stunden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Klicken Sie auf **Absenden**.
   Die ausgewählte Ergänzungsaktion wird ausgeführt, und es wird eine Informationsnachricht angezeigt, die angezeigt wird Die Ausführung der Sichtungssuche wurde gestartet.

Hinweis:

- Sobald die Ausführung initiiert oder abgeschlossen ist, werden Arbeitsnotizen im Aktivitätenstrom der Formularansicht veröffentlicht.
- Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse finden Sie in **Ergänzungsergebnisse** Registerkarte der entsprechenden Detailseite für erkennbare Elemente im TISC-Arbeitsbereich.
- Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse können mit identifiziert werden **Quelle** Feld der Ergänzungsergebnistabelle.

Anreicherung erkennbarer Elemente durchführen

Wählen Sie eine oder mehrere Implementierungen aus, um die Bedrohungssuche für erkennbare Elemente auszuführen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Automatische Übersetzung

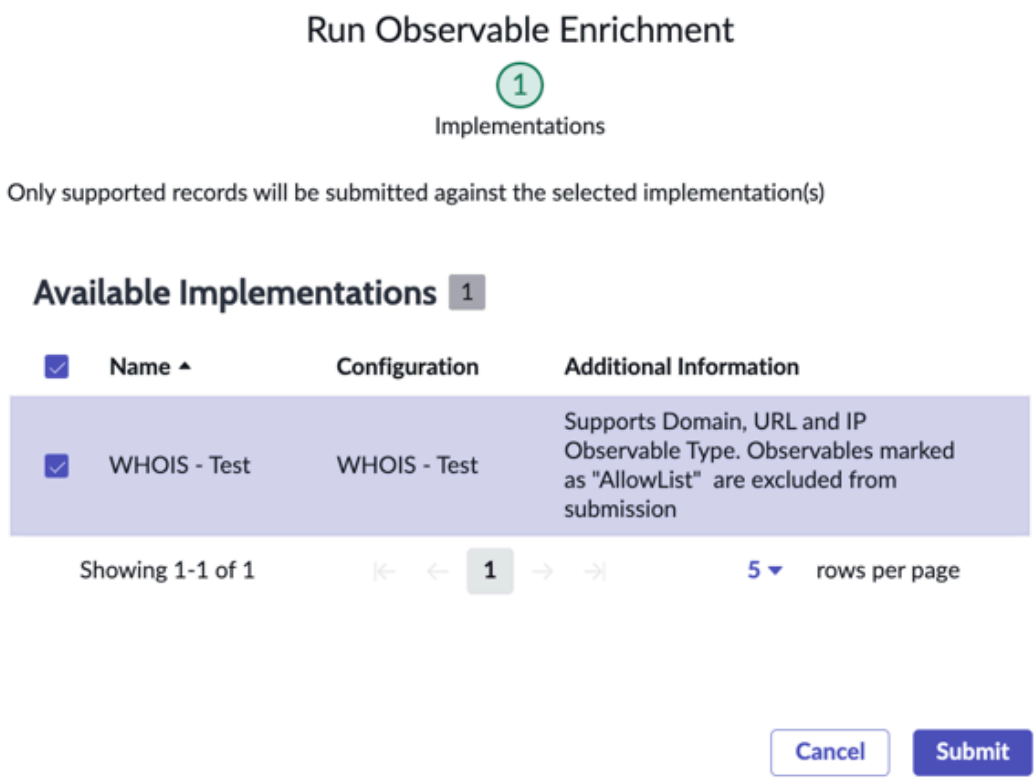
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Workbench Für Bedrohungsanalysen** Symbol.
3. Gehe zu **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
4. Öffnen Sie einen beliebigen Datensatz erkennbarer Elemente.
5. Klicken Sie Auf **Ergänzung Erkennbarer Elemente Ausführen** .
   Die Ergänzung Erkennbarer Elemente Ausführen **Wählen Sie Implementierungen Aus** Der modale Bildschirm wird angezeigt.

   Hinweis:
   Nur unterstützte Datensätze werden für die ausgewählte(n) Implementierung(en) übermittelt.

6. Wählen Sie die erforderliche(n) Implementierung(en) (z. B. WHOIS) aus der Liste aus.



7. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die ausgewählte Ergänzungsaktion wird ausgeführt, und es wird eine Informationsnachricht angezeigt, die angezeigt wird Ausführung der Bedrohungssuche wurde gestartet.

Hinweis:

- Sobald die Ausführung initiiert oder abgeschlossen ist, werden Arbeitsnotizen im Aktivitätenstrom der Formularansicht veröffentlicht.
- Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse finden Sie in **Ergänzungsergebnisse** Registerkarte der entsprechenden Detailseite für erkennbare Elemente im TISC-Arbeitsbereich.
- Die aus dem SIR-Arbeitsbereich übertragenen Ergänzungsergebnisse können mit identifiziert werden **Quelle** Feld der Ergänzungsergebnistabelle.

Datenanreicherungs-Ergebnisse anzeigen

Zeigen Sie die Ergebnisse der Ergänzung erkennbarer Elemente, Indikatoren und verschiedener Objekte an.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
2. Wählen Sie einen Datensatz für erkennbare Elemente aus.
3. Wechseln Sie zu **Ergänzungsergebnisse** Registerkarte.
   Die Anreicherungsergebnisse zeigen die Ergänzungsergebnisse der TISC-Integrationen an.

Ergänzungsname	Beschreibung
Bedrohungssuche – Ergebnisse	Listet alle zugehörigen Bedrohungssuchergebnisse für ein erkennbares Element auf.
Sichtungen	Listet alle zugeordneten Sichtungen für ein erkennbares Element auf.
Erkennbare Elemente – Datenanreicherungs-Ergebnisse	Listet alle zugehörigen Ergänzungsergebnisse erkennbarer Elemente für ein erkennbares Element auf.

Indikatoren

Indikatoren sind Artefakte, die in einem Netzwerk oder Betriebssystem beobachtet werden und wahrscheinlich auf einen Angriff hinweisen. Typische IoCs sind Virensignaturen und IP-Adressen, MD5-Hashes von Malware-Dateien oder URLs oder Domänennamen.

Definieren Sie einen Indikator

Definieren Sie einen Indikator.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Indikatoren**an.
2. Wählen Sie Aus **Indikator** .
3. Klicken Sie auf **Neu**.

Hinweis:
Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

4. Füllen Sie im Formular die Felder aus.

Abschnitt „Details“

Feld	Beschreibung
ID	Eindeutige ID des Indikators.
Beschreibung	Beschreibung des Indikators.
Name	Name des Indikators.
Muster	Das Erkennungsmuster für diesen Indikator kann als STIX-Muster ausgedrückt werden.
Mustertyp	Die in diesem Indikator verwendete Mustersprache.
Musterversion	Die Version der Mustersprache, die für die Daten in der Mustereigenschaft verwendet wird und dem Typ der Musterdaten entsprechen muss, die in der Mustereigenschaft enthalten sind.
Gültig ab	Der Zeitpunkt, ab dem dieser Indikator als gültiger Indikator für das Verhalten betrachtet wird, das er zugehörig ist oder darstellt.
Gültig bis	Die Zeit, nach der dieser Indikator nicht mehr als gültiger Indikator für das Verhalten betrachtet werden soll, das er darstellt oder mit dem er verknüpft ist.
IoC-Klassifizierung	Die IOC-Klassifizierung der Indikatoren.
Indikatortypen	Gibt die verschiedenen Kategorien des Indikators an.
Status	Gibt den Status der Indikatoren an.
Plattformen	Definiert die Plattformen, für die dieser Indikator gilt.
TLP	Eindeutiger Wert, der die Einstellung für die Datensensibilität pro TLP angibt.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Vertrauen	Geben Sie die Konfidenz für diesen Indikatordatensatz ein. Die Konfidenzeigenschaft gibt die Konfidenz an, die der Ersteller in der Richtigkeit seiner Daten hat. Der Konfidenzwert MUSS eine Zahl im Bereich von 0–100 sein.
Bedrohungsstufe	Gibt die Bedrohungsstufe des Indikatordatensatzes an.
Ablaufzeit	Gibt die Ablaufzeit des Indikatordatensatzes an.
Bedrohungsschweregrad	Gibt den Bedrohungsschweregrad des Indikatordatensatzes an.
Nutzungskategorien	Kategorien, unter die das erkennbare Element fällt, z. B. Botnet oder Phishing.
Erstmals aufgetreten	Die Zeit, zu der dieser Indikatordatensatz erstmals schädliche Aktivitäten ausgeführt hat.
Zuletzt aufgetreten	Die Zeit, zu der dieser Indikatordatensatz zuletzt schädliche Aktivitäten ausgeführt hat.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Datensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für einen Indikator hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Indikator hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung des Indikators verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellt	Gibt die Zeit an, zu der der Indikator im System erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktualisiert	Gibt die Zeit an, zu der der Indikator im System aktualisiert wird.
Erweiterungen	Gibt die Erweiterungen des Indikators an.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Indikators dar.

5. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
6. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die einem Indikator zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie die Taxonomie aus, die einem Indikator zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie die Taxonomiewerte hinzu, die einem Indikator zugeordnet sind.

Quelldatensätze

Feld	Beschreibung
Die Quelldatensatzdetails für einen Indikator werden angezeigt, falls vorhanden.	

Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die den Indikatoren zugeordnet sind.

Zugehörige Datensätze

Zugehörige Liste	Beschreibung
MITRE-Techniken	Listet die MITRE-Techniken auf, die sich auf diesen Indikator beziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Zugehörige Liste	Beschreibung
Angriffsmuster	Listet die Quelle der Angriffsmuster auf, die die Methoden beschreiben, mit denen Angreifer versuchen, Ziele zu gefährden, die sich auf diesen Indikator beziehen.
Kampagnen	Listet die Kampagnenquelle auf, die eine Reihe böswilliger Aktivitäten oder Angriffe beschreibt, die im Laufe der Zeit gegen eine bestimmte Gruppe von Zielen auftreten, die sich auf diesen Indikator beziehen.
Vorgehensweisen	Listet die Aktionen im Zusammenhang mit diesem Indikator auf.
Datenquellen	Listet die Datenquellen auf, die sich auf diesen Indikator beziehen.
Datenkomponenten	Listet die Datenkomponenten auf, die sich auf diesen Indikator beziehen.
Identitäten	Listet die Identitäten auf, die sich auf diesen Indikator beziehen.
Indikatoren	Listet die Indikatoren auf, die sich auf diesen Indikator beziehen. **Hinweis:** Dieser Abschnitt enthält auch die potenziellen Beziehungen zwischen zwei Indikatoren. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Beziehungen zwischen Indikator und Indikator Und siehe Definieren Sie Indikator-Indikator-Beziehungen Für die bestätigten Beziehungen zwischen den beiden erkennbaren Elementen.
Infrastruktur	Listet die Infrastrukturquelle auf, die alle Systeme, Softwareservices und zugehörigen physischen oder virtuellen Ressourcen beschreibt, die einen bestimmten Zweck eines Angriffs unterstützen sollen, die sich auf diesen Indikator beziehen.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die sich auf diesen Indikator beziehen.
Standorte	Listet die geografischen Standorte auf, die dem Objekt zugeordnet sind.
Malware	Listet Malware-Quelldatensätze auf, die sich auf diesen Indikator beziehen.
Markierungsdefinitionen	Listet die Markierungsdefinitionen auf, die diesem Objekt zugeordnet sind.
Malware-Analyse	Listet die Metadaten und Ergebnisse einer bestimmten statischen oder dynamischen Analyse auf, die für eine Malware-Instanz durchgeführt wird, die diesem Indikator zugeordnet ist.
Erkennbare Elemente	Listet die zugehörigen Datensätze erkennbarer Elemente auf, die sich auf diesen Indikator beziehen.
Beobachtete Daten	Listet die beobachteten Daten auf, bei denen es sich um Cyber-sicherheitsbezogene Entitäten wie Dateien, Systeme und Netzwerke handelt und die diesem Indikator zugeordnet sind.
Sichtungen	Listet Sichtungsquelldatensätze auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet Changes auf, die dem erkennbaren Element zugeordnet sind.
Bedrohungsereignisse	Listet das Ereignis oder die Situation auf, das/die das Potenzial hat, unerwünschte Konsequenzen oder Auswirkungen zu verursachen, die dem Indikator zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Zugehörige Liste	Beschreibung
Bedrohungsgruppierungen	Listet die Bedrohungsgruppierungen als Objekte mit einem gemeinsam genutzten Kontext auf.
Bedrohungshinweise	Listet die Bedrohungshinweise auf, die Informationen enthalten, um weiteren Kontext oder Analysen bereitzustellen, die dem Indikator zugeordnet sind.
Bedrohungsmeinungen	Listet die Bedrohungsmeinungen als Bewertung der Genauigkeit der Informationen auf, die dem Indikator zugeordnet sind.
Bedrohungsberichte	Listet die Bedrohungsberichte auf, die diesem Indikator zugeordnet sind.
Tools	Listet das diesem Objekt zugeordnete Tool auf.
Schwachstellen	Wenn das erkennbare Element eine IP-Adresse ist, werden in dieser Liste alle Ressourcen (Konfigurationselemente) angezeigt, die eine übereinstimmende IP-Adresse haben.
Verwandte Fälle	Listet die zugehörigen Fälle auf, die diesem Indikator zugeordnet sind.
Zugehöriger Fall – Aufgaben	Listet die zugehörigen Fallaufgaben auf, die diesem Indikator zugeordnet sind.
Zugehörige Canvase	Listet die zugehörigen Canvases auf, die diesem Indikator zugeordnet sind.
Indikatorreferenzen	Liste der externen Referenzen, die diesen Indikator beschreiben.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Auch aus dem **Zugehörige Datensätze** Abschnitt können Sie die Beziehungen zwischen zwei erkennbaren Elementen mit bestätigen **Potenzielle Beziehungen** Abschnitt verfügbar auf **Indikatoren** Formularansicht. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
3. Sie können Indikatoren zu Fällen hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Angriffsmuster

Angriffsmuster sind eine Art von Taktiken, Techniken und Verfahren (TTPs), die die Methoden beschreiben, mit denen Angreifer versuchen, Ziele zu gefährden.

Angriffsmuster werden verwendet, um Angriffe zu kategorisieren. Sie verallgemeinern bestimmte Angriffe auf die Muster, denen sie folgen, und stellen detaillierte Informationen zur Durchführung von Angriffen bereit.

Beispielsweise ist Spear-Phishing eine gängige Art von Angriff, bei dem ein Angreifer eine sorgfältig gestaltete E-Mail-Nachricht an eine Partei sendet, mit der Absicht, sie dazu zu bringen, auf einen Link zu klicken oder einen Anhang zu öffnen, um Malware bereitzustellen. Angriffsmuster sind spezifischer, z. B. Spear-Phishing durch einen bestimmten Bedrohungsakteur (z. B. dass das Ziel einen Wettbewerb gewonnen hat), kann auch ein Angriffsmuster sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie ein Angriffsmuster

Definieren Sie ein Angriffsmuster, damit Bedrohungsanalysten die Angriffe kategorisieren können.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Angriffsmuster** .
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Detailansicht des Angriffsmusters

Feld	Beschreibung
ID	Eindeutige ID für ein Angriffsmuster.
Name	Geben Sie einen Namen für dieses Angriffsmuster ein.
Beschreibung	Geben Sie eine Beschreibung für ein Angriffsmuster ein.
Aliasse	Alternative Namen zur Identifizierung dieses Angriffsmusters. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf **Fügen Sie Neue Aliasse Hinzu** Symbol, das im Feld „Alias“ selbst verfügbar ist.
Angriffsphase	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
Berechtigungen erforderlich	Wählen Sie die erforderlichen Berechtigungen für dieses Angriffsmuster aus.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Vertrauen	Geben Sie die Konfidenz für diesen Angriffsmustermodus ein. Die Konfidenzeigenschaft gibt die Konfidenz an, die der Ersteller in der Richtigkeit seiner Daten hat. Der Konfidenzwert MUSS eine Zahl im Bereich von 0–100 sein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.
Systemupdates verhindern	Wenn Sie diese Kennzeichnung auf „wahr“ festlegen, wird verhindert, dass das System Werte von Feldern im Datensatz überschreibt.

Wichtig:
Nachdem Sie einen neuen Objektdatensatz erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für ein Angriffsmuster hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts, des Angriffsmusters, verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellt	Gibt die Zeit an, zu der der Datensatz im System erstellt wird.
Aktualisiert	Gibt die Zeit an, zu der der Datensatz im System geändert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Angriffsmuster.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die einem erkennbaren Element zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die einem Angriffsmuster zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die einem Angriffsmuster zugeordnet sind.

Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Angriffsmuster zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet Kampagnen auf, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Kampagne

„Kampagne“ ist definiert als Gruppierung von konversationswidrigen Verhaltensweisen, die eine Reihe böswilliger Aktivitäten oder Angriffe beschreibt, manchmal als Wellen bezeichnet, die über einen bestimmten Zeitraum für eine bestimmte Gruppe von Zielen auftreten.

Kampagne Definieren

Definieren Sie eine Kampagne, um konversationswidriges Verhalten zu gruppieren.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Kampagne** Objekt.
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Kampagnenansicht

Feld	Beschreibung
ID	Eindeutige ID für ein konversariales Verhalten.
Name	Geben Sie einen Namen für ein gegnerisches Verhalten ein.
Beschreibung	Geben Sie eine Beschreibung für diese Kampagne ein.
Ziel	Primäres Ziel, Ziel, gewünschtes Ergebnis oder beabsichtigte Auswirkung der Kampagne. Was der Bedrohungsakteur oder der Angreifer mit dieser Kampagne erreichen möchte.
Aliasse	Alternative Namen, die für diese Kampagne identifiziert werden sollen. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf **Fügen Sie Neue Aliasse Hinzu** Symbol, das im Feld „Alias“ selbst verfügbar ist.
TLP	Traffic Light Protocol (TLP) gibt die vertraulichen Informationen an, die an die richtige Zielgruppe weitergegeben werden. Es verwendet vier Farben (weiß, Grün, Gelb und Rot), um unterschiedliche Empfindlichkeitsgrade für dieses Angriffsmuster anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für diese Kampagne ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für eine Kampagne hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Kampagne hinzu.
Erstmals aufgetreten	Die Zeit, zu der dieses Objekt erstmals konversarisches Verhalten gezeigt hat.
Zuletzt aufgetreten	Die Zeit, zu der dieses Objekt zuletzt ein konversarisches Verhalten ausgeführt hat.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wurde.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts, der Kampagne dar.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die einer Kampagne zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die einer Kampagne zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die der Kampagne zugeordnet sind.

Nächste Maßnahme

Sie können jetzt auf eine der folgenden zugehörigen Listen klicken, um zusätzliche Informationen zu Objekten anzuzeigen, die der Kampagne zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssatz	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Vorgehensweisen

Handlungsweisen sind Aktionen, die entweder ausgeführt werden, um einen Angriff zu verhindern oder auf einen laufenden Angriff zu reagieren.

In Aktionskursen werden technische oder automatisierte Antworten beschrieben, z. B. das Anwenden von Patches und die Neukonfiguration von Firewalls. Es kann auch Aktionen auf höherer Ebene wie Mitarbeiterschulungen oder Richtlinienänderungen beschreiben.

Beispielsweise könnten Aktionskurse zur Minderung einer Schwachstelle beschreiben, wie der Patch angewendet wird, der sie behebt.

Definieren Sie Handlungskurse

Definieren Sie Handlungsweisen, um einen Angriff zu verhindern oder auf einen laufenden Angriff zu reagieren.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wechseln Sie zu **Handlungskurse** Objekt.
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Detailansicht für Aktionskurse

Feld	Beschreibung
ID	Eindeutige ID für Aktionen zur Verhinderung eines Angriffs.
Name	Geben Sie einen beschreibenden Namen für diese Aktionskurse ein.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zu den Handlungskursen enthält, möglicherweise einschließlich ihres Zwecks und ihrer wichtigsten Merkmale.
Aktion	Zum Erfassen strukturierter oder automatisierter Handlungskurse.
TLP	Traffic Light Protocol (TLP) gibt die vertraulichen Informationen an, die an die richtige Zielgruppe weitergegeben werden. Es verwendet vier Farben (weiß, Grün, Gelb und Rot), um unterschiedliche Empfindlichkeitsgrade für dieses Angriffsmuster anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für diese Handlungsweisen ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für einen Aktionskurs hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Aktionskurse.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die einem erkennbaren Element zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die einem Angriffsmuster zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die einem Angriffsmuster zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den Aktionskursen zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Identität

Identitäten stellen tatsächliche Einzelpersonen, Organisationen oder Gruppen und Klassen von Einzelpersonen, Systemen oder Gruppen dar. Identitäten gelten für STIX 2.x.

Ein Identitäts-SDO kann grundlegende Identifizierungsinformationen, Kontaktinformationen und die Sektoren erfassen, zu denen die Identität gehört. Identität stellt Ziele von Angriffen, Informationsquellen, Objekterstellern und Identitäten von Bedrohungsakteuren dar.

Definieren Sie Identitäten

Definieren Sie Identitäten, die tatsächliche Einzelpersonen, Organisationen oder Gruppen darstellen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Identität** Objekt.
4. Klicken Sie auf **Neu**.

Hinweis:

Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Ansicht „Identitätsdetails“

Feld	Beschreibung
ID	Eindeutige ID für eine Identität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen für diese Identität ein. Bei Verweis auf eine bestimmte Entität (eine Einzelperson oder Organisation) muss diese Eigenschaft den kanonischen Namen der spezifischen Entität enthalten.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Vorgehensweise enthält, möglicherweise einschließlich ihres Zwecks und ihrer wichtigsten Merkmale.
Rollen	Die Liste der Rollen, die diese Identität ausführt.
Identitätsklasse	Der Typ der Entität, die diese Identität beschreibt. Zum Beispiel Einzelperson oder Organisation.
Sektoren	Die Liste der Branchen, zu denen diese Identität gehört.
Kontaktinformationen	Die Kontaktinformationen wie E-Mail-Adresse und Telefonnummer für diese Identität.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden.es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um unterschiedliche Vertraulichkeitsgrade anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für diese Identität ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für die Identität hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext im Zusammenhang mit dieser Identität hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Identität zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die der Identität zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die der Identität zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Identität zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet externe Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Infrastruktur

Das Infrastruktur-SDO stellt eine Art von Taktiken, Techniken und Verfahren (TTPs) dar. Sie beschreiben alle Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen, die einen bestimmten Zweck eines Angriffs unterstützen sollen. Infrastruktur gilt für STIX 2.x.

Die Elemente eines Angriffs werden von anderen SDOs oder SCOs dargestellt. Das Infrastruktur-SDO stellt jedoch eine benannte Gruppe von Daten dar, die die Infrastruktur ausmachen.

Beispiele für Infrastruktur sind C2-Server, die bei einem Angriff verwendet werden, ein Gerät oder ein Server, der Teil einer Verteidigung ist, oder Datenbankserver, die von einem Angriff angegriffen werden sollen.

Definieren Sie die Infrastruktur

Definieren Sie eine Infrastruktur, bei der es sich um alle Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen handelt, die einen Zweck eines Angriffs unterstützen sollen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Infrastruktur** Objekt.
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Ansicht „Infrastrukturdetails“

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zur Verhinderung eines Angriffs.
Name	Geben Sie einen beschreibenden Namen für diese Vorgehensweise ein. Bei Verweis auf eine bestimmte Entität (eine Einzelperson oder Organisation) muss diese Eigenschaft den kanonischen Namen der spezifischen Entität enthalten.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Infrastruktur enthält, möglicherweise einschließlich ihres Zwecks, ihrer Verwendung, ihrer Beziehung zu anderen in zugehörigen Objekten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	erfassten Intelligence-Aktivitäten und ihren wichtigsten Merkmalen.
Infrastrukturtypen	Beschreibt die Kategorisierung der Infrastruktur.
Aliasse	Alternative Namen zur Identifizierung dieser Infrastruktur. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf **Fügen Sie Neue Aliasse Hinzu** Symbol, das im Feld „Alias“ selbst verfügbar ist.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Erstmals aufgetreten	Die Zeit, zu der diese Infrastruktur erstmals schädliche Aktivitäten ausgeführt hat.
Zuletzt aufgetreten	Die Zeit, zu der diese Infrastruktur zuletzt schädliche Aktivitäten ausgeführt hat.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diese Infrastruktur hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Infrastruktur hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt die Zeit an, zu der der Datensatz in der Quelle erstellt wird.
Aktualisiert	Gibt die Zeit an, zu der der Datensatz in der Quelle geändert wird.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Infrastruktur zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Infrastruktur zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Infrastruktur zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Identität zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Angriffssatz

Ein Angriffssatz ist ein gruppierter Satz von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften. Ein Angriffssatz umfasst normalerweise eine einzelne Organisation. Angriffssatz gilt für STIX 2.x.

Ein Angriffssatz kann mehrere Kampagnen oder andere Aktivitäten erfassen. Diese Aktivitäten teilen Attribute, die auf einen allgemein bekannten oder unbekannten Bedrohungsakteur hinweisen.

Neue Aktivität kann einem Angriffssatz zugeordnet werden, auch wenn die Bedrohungsakteure hinter dem Angriff nicht bekannt sind. Bedrohungsakteure können von der Unterstützung eines Angriffssatzes zur Unterstützung eines anderen wechseln oder mehrere Angriffssätze unterstützen.

Ein Angriffssatz ist das gesamte Angriffspaket und kann über einen langen Zeitraum in mehreren Kampagnen verwendet werden, um potenziell mehrere Zwecke zu erreichen.

Definieren Sie Den Angriffssatz

Definieren Sie einen Angriffssatz, der ein gruppiertes Set von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften ist.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Angriffssatz** .
4. Klicken Sie auf **Neu**.

Hinweis:

Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Füllen Sie im Formular die Felder aus.

Detailansicht des Angriffssatzes

Feld	Beschreibung
ID	Eindeutige ID für einen Angriffssatz.
Name	Geben Sie einen beschreibenden Namen für diesen Angriffssatz ein. Bei Verweis auf eine bestimmte Entität (eine Einzelperson oder Organisation) muss diese Eigenschaft den kanonischen Namen der spezifischen Entität enthalten.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Angriffssatz enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Aliasse	Alternative Namen zur Identifizierung dieses Angriffssatzes. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf **Fügen Sie Neue Aliasse Hinzu** Symbol, das im Feld „Alias“ selbst verfügbar ist.
Ziele	Die allgemeinen Ziele dieses Angriffssatzes, nämlich, was versucht wird. Beispielsweise können sie durch persönlichen Gewinn motiviert sein, ihr Ziel besteht jedoch darin, Kreditkartennummern zu stehlen. Dazu können sie bestimmte Kampagnen ausführen, die detaillierte Ziele haben, z. B. kompromittierende Point-of-Sale-Systeme bei einem großen Einzelhändler.
Erstmals aufgetreten	Die Zeit, zu der dieser Angriffssatz erstmals bei der Ausführung schädlicher Aktivitäten beobachtet wurde.
Zuletzt aufgetreten	Die Zeit, zu der dieser Angriffssatz zuletzt schädliche Aktivitäten ausgeführt hat.
Primäre Motivation	Der primäre Grund, die Motivation oder der Zweck dieses Angriffssatzes. Die Motivation ist, warum der Angriffssatz das Ziel erreichen möchte (was er erreichen möchte).
Sekundäre Motivationen	Die sekundären Gründe, Motivationen oder Zwecke hinter diesem Angriffssatz. Diese Motivationen können als gleiche oder nahezu gleiche Ursache der primären Motivation vorhanden sein. Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	ersetzt die primäre Motivation jedoch nicht oder erhöht sie notwendigerweise nicht, kann jedoch auf zusätzlichen Kontext hinweisen. Die Position in der Liste hat keine Bedeutung.
Ressourcenebene	Diese Eigenschaft gibt die Organisationsebene an, auf der dieser Angriffssatz normalerweise funktioniert, was wiederum die Ressourcen bestimmt, die diesem Angriffssatz zur Verwendung bei einem Angriff zur Verfügung stehen.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für diesen Angriffssatz ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diesen Angriffssatz hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Angriffssatz hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der der Datensatz in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erstellt	Gibt die Zeit an, zu der der Datensatz in der Quelle erstellt wird.
Aktualisiert	Gibt die Zeit an, zu der der Datensatz in der Quelle geändert wird.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die dem Angriffssatz zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die diesem Angriffssatz zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die diesem Angriffssatz zugeordnet sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Angriffssatz zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Standort

Ein Standort stellt einen geografischen Standort dar. Standorte werden hauptsächlich verwendet, um anderen SDOs Kontext zu geben. Standorte gelten für STIX 2.x.

Der Standort kann einige oder alle der folgenden Elemente enthalten: Region (Nordamerika), Bürgeranschrift (New York, USA), Breitengrad und Längengrad.

Das Standort-SDO kann sich auf eine Identität oder einen Angriffssatz beziehen, um anzuzeigen, dass sich die Identität oder der Angriffssatz an diesem Standort befindet. Sie kann sich auch auf eine Malware oder ein Angriffsmuster beziehen, um anzuzeigen, dass sich das Zielopfer an einem bestimmten Standort befindet.

Beispielsweise könnte ein Standort in einer Beziehung verwendet werden, um zu beschreiben, dass der Bourgeois Swallow-Intrusion Set aus Osteuropa stammt.

Mindestens eine der folgenden Eigenschaften oder Eigenschaftensätze muss angegeben werden:

- region
- country
- Breitengrad und Längengrad

Definieren Sie Den Standort

Definieren Sie einen geografischen Standort, um anderen SDOs mehr Kontext bereitzustellen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Standort** Objekt.
4. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie die Felder im Formular aus

Ansicht „Identitätsdetails“

Feld	Beschreibung
ID	Eindeutige ID für den Standort.
Name	Geben Sie einen beschreibenden Namen ein, um den Standort zu identifizieren.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Angriffssatz enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Breitengrad	Der Breitengrad des Standorts in Dezimalgraden. Positive Zahlen beschreiben Breitengrade nördlich des Äquators, negative Zahlen beschreiben Breitengrade südlich des Äquators. Der Wert dieser Eigenschaft muss zwischen -90,0 und 90,0 liegen.
Längengrad	Der Längengrad des Standorts in Dezimalgraden. Positive Zahlen beschreiben Längengrade östlich des Primmeridians, negative Zahlen beschreiben Längengrade westlich des Primmeridians. Der Wert dieser Eigenschaft muss zwischen -180,0 und 180 liegen (einschließlich).
Genauigkeit	Definiert die Genauigkeit der Koordinaten, die durch die Eigenschaften für Breitengrad und Längengrad angegeben werden. Dies wird in Metern gemessen. Der tatsächliche Standort kann sich an einem beliebigen Ort bis zu Genauigkeitsmessgeräten vom definierten Punkt befinden. Wenn diese Eigenschaft nicht vorhanden ist, ist die Genauigkeit nicht angegeben. Wenn diese Eigenschaft vorhanden ist, müssen die Eigenschaften für Breitengrad und Längengrad vorhanden sein.
Region	Die Region, in der sich dieser Standort befindet.
Land	Das Land, in dem sich dieser Standort befindet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Verwaltungsgebiet	Das Bundesland, die Provinz oder ein anderes subnationales Verwaltungsgebiet, in dem sich dieser Standort befindet.
Stadt	Die Stadt, in der sich dieser Standort befindet.
Straße und Hausnummer	Die Straße, die dieser Standort beschreibt. Diese Eigenschaft enthält alle Aspekte oder Teile der Straße.
Postleitzahl	Die Postleitzahl, in der sich dieser Standort befindet.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diesen Standort hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Standort hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen für diesen Standort an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt die Zeit an, zu der der Datensatz in der Quelle erstellt wird.
Aktualisiert	Gibt die Zeit an, zu der der Datensatz in der Quelle geändert wird.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die dem Standort zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die diesem Standort zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die diesem Standort zugeordnet sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Standort zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Malware

Malware ist eine Art von TTP, die schädlichen Code darstellt. Bezieht sich auf ein Programm, das verdeckt in ein System eingefügt wird. Malware gilt für STIX 2.x.

Die Absicht einer Malware besteht darin, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder des Betriebssystems des Opfers zu gefährden.

Das Malware-SDO charakterisiert, identifiziert und kategorisiert Malware-Instanzen und -Familien aus Daten, die aus der Analyse abgeleitet wurden. Dieses SDO erfasst detaillierte Informationen darüber, wie die Malware funktioniert und was sie tut.

Definieren Sie Malware

Definieren Sie eine Malware, die schädlichen Code darstellt.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Malware** Threat Intel-Objekt.
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Ansicht „Malware-Details“

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung der Malware-Instanz.
Name	Geben Sie einen Namen ein, um die Malware-Instanz oder -Familie zu identifizieren, wie vom Ersteller des SDO angegeben. Für eine Malware-Familie muss der Name definiert werden.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Malware-Instanz oder -Familie enthält, möglicherweise einschließlich ihres Zwecks und ihrer wichtigsten Merkmale.
Schadsoftwaretypen	Gibt die verschiedenen Kategorien der Malware an.
Ist Familie	Aktivieren Sie dieses Kontrollkästchen, um anzugeben, ob das Objekt eine Malware-Familie oder eine Malware-Instanz darstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aliasse	Die alternativen Namen, die zur Identifizierung dieser Malware oder Malware-Familie verwendet werden. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf **Fügen Sie Neue Aliasse Hinzu** Symbol, das im Feld „Alias“ selbst verfügbar ist.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
Erstmals aufgetreten	Der Zeitpunkt, zu dem diese Malware-Instanz oder -Familie erstmals schädliche Aktivitäten ausgeführt hat.
Zuletzt aufgetreten	Die Zeit, zu der diese Malware-Instanz oder -Familie zuletzt schädliche Aktivitäten ausgeführt hat
Prozessarchitekturen	Gibt die Prozessarchitekturen für diese Malware an.
Implementierungssprachen	Gibt die Implementierungssprachen für diese Malware an.
Malware-Fähigkeiten	Die Fähigkeiten, die von einer Malware-Instanz oder -Familie bereitgestellt werden können.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für diese Malware ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für den Malware-Datensatz hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Malware-Datensatz hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Malware.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Malware zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die der Malware zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die der Malware zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Malware zugeordnet sind.

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Erkennungen und Verringerungen	Listet die Erkennungen und Minderungen auf, die sich auf diese Malware beziehen.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Indikatoren	Listet zugehörige Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware-Analyse	Listet Malware-Analysedatensätze auf, die diesem Objekt zugeordnet sind.
Malware	Listet Malware-Datensätze auf, die diesem Objekt zugeordnet sind.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Malware-Analyse

Malware-Analyse erfasst die Metadaten und Ergebnisse einer Malware. Malware-Analyse gilt für STIX 2.x.

Malware-Analyse umfasst statische oder dynamische Analysen, die für eine Malware-Instanz oder -Familie durchgeführt werden.

Definieren Sie Die Malware-Analyse

Definieren Sie eine Malware-Analyse, die die Metadaten und Ergebnisse einer bestimmten statischen oder dynamischen Analyse erfasst, die für eine Malware-Instanz oder -Familie durchgeführt wird.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Malware-Analyse** Objekt.
4. Klicken Sie auf **Neu**.

Hinweis:

Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Detailansicht der Malware-Analyse

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung der Malware-Analyse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Produkt	Der Name der verwendeten Analyse-Engine oder des verwendeten Produkts. Produktnamen MÜSSEN in Kleinbuchstaben mit Wörtern angegeben werden, die durch einen Bindestrich „-“ getrennt sind. In Fällen, in denen der Name eines Produkts nicht angegeben werden kann, muss der Wert anonymisiert verwendet werden.
Version	Die Version des Analyseprodukts, das zur Durchführung der Analyse verwendet wurde.
Host-VM	Eine Beschreibung der VM-Umgebung, die zum Hosten des Gastbetriebssystems verwendet wurde (falls zutreffend), die für die dynamische Analyse der Malware-Instanz oder -Familie verwendet wurde. Wenn dieser Wert nicht in Verbindung mit der Eigenschaft „Operating_System_ref“ enthalten ist, bedeutet dies, dass die dynamische Analyse möglicherweise für Bare Metal (d. h. ohne Virtualisierung) durchgeführt wurde oder die Informationen geschwärzt wurden. Der Wert dieser Eigenschaft MUSS der Bezeichner für ein SCO-Softwareobjekt sein.
Betriebssystem	Das Betriebssystem, das für die dynamische Analyse der Malware-Instanz oder -Familie verwendet wird. Dies gilt für virtualisierte Betriebssysteme sowie für solche, die auf Bare Metal ausgeführt werden. Der Wert dieser Eigenschaft MUSS der Bezeichner für ein SCO-Softwareobjekt sein.
Konfigurationsversion	Die alternativen Namen, die zur Identifizierung dieser Malware oder Malware-Familie verwendet werden.
Module	Die spezifischen Analysemodule, die während dieser Analyseausführung im Produkt verwendet und konfiguriert wurden.
Analyse-Engine-Version	Die Version der Analyse-Engine oder des Produkts (einschließlich AV-Engines), die zur Durchführung der Analyse verwendet wurde.
Analysedefinitionsversion	Die Version der Analysedefinitionen, die vom Analysetool einschließlich AV-Tools verwendet werden.
Analyse gestartet	Datum und Uhrzeit der Initiierung der Malware-Analyse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Analyse beendet	Datum und Uhrzeit des Beendens der Malware-Analyse.
Ergebnis	Das Klassifizierungsergebnis, wie durch den Scanner- oder Toolanalyseprozess bestimmt.
Ergebnisname	Das Klassifizierungsergebnis oder der Name, das bzw. der der Malware-Instanz vom Scanner-Tool zugewiesen wurde.
Eingereicht	Datum und Uhrzeit der ersten Übermittlung der Malware zum Scannen oder Analysieren. Dieser Wert bleibt konstant, solange sich das gescannte Datum ändern kann. Zum Beispiel, wenn Malware an ein Virenanalysetool übermittelt wurde.
Analysiertes erkennbares Element	Wählen Sie das analysierte erkennbare Element aus.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für diese Malware-Analyse ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für den Datensatz der Malware-Familie hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Malware-Datensatz hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Malware.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Malware zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die der Malware zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die der Malware zugeordnet sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Malware zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Relatd-Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Malware	Listet Malware-Datensätze auf, die diesem Objekt zugeordnet sind.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Objektsichtung

Sichtungen geben an, dass ein Objekt gesehen wurde. Objekte können Malware, Tool, Bedrohungsakteur usw. sein.

Sichtungen verfolgen, wer und was das Ziel ist, wie Angriffe ausgeführt werden, und um Trends im Angriffsverhalten nachzuverfolgen.

Das Sichtungsbeziehungsobjekt enthält zusätzliche Eigenschaften, die nicht in den generischen Beziehungsobjekten vorhanden sind. Diese zusätzlichen Eigenschaften stellen Daten dar, die für Sichtungsbeziehungen spezifisch sind.

Objektsichtung Definieren

Definieren Sie die Objektsichtung, die beschreibt, dass ein Objekt (Malware, Tool, Bedrohungsakteur usw.) gesehen wurde.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Objektsichtung** Objekt.
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Wählen Sie Entität&Wert

Feld	Beschreibung
Entität	Wählen Sie den Entitätsobjekt-Sichtungsdatensatz aus. **Hinweis:** Während der Erstellung eines neuen Objektsichtungsdatensatzes ist ein zugeordneter Beziehungsdatensatz für die Zusammenfassung erforderlich.
Sichtung von	Gibt an, dass eine bestimmte Entität oder ein bestimmter Indikator in einer Umgebung beobachtet wurde, was ein Hinweis auf eine potenzielle Bedrohung sein kann. **Hinweis:** Wählen Sie den zu Sichtungen gehörigen Datensatz aus, der dem im Feld Entität ausgewählten Objekt zugeordnet ist, damit jetzt zugehörige Datensätze erstellt und die Sichtungsdatensätze aggregiert werden können.

Detailansicht der Objektsichtung

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zur Verhinderung eines Angriffs.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Sichtung enthält.
Erstmals aufgetreten	Der Beginn des Zeitfensters, in dem das SDO referenziert wurde, von dem die Eigenschaft gesehen wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zuletzt aufgetreten	Das Ende des Zeitfensters, in dem das SDO referenziert wurde, von dem die Eigenschaft gesehen wurde.
Anzahl	Falls vorhanden, muss dies eine Ganzzahl zwischen 0 und 999.999.999 einschließlich sein und die Anzahl der Male darstellen, mit denen das SDO referenziert wurde, von dem die Eigenschaft gesehen wurde.
Ist Zusammenfassung	Gibt an, ob die Sichtung als Zusammenfassungsdaten betrachtet werden soll. Zusammenfassungsdaten sind eine Zusammenfassung vorheriger Sichtungsberichte und sollten nicht als primäre Quelldaten betrachtet werden.
Ist intern	Gibt an, ob die Sichtung intern ist.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diesen Angriffssatz hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Identität zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Infrastruktur zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Infrastruktur zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Objektsichtung zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Objekte	Listet die Objekte auf, die den Sichtungen zugeordnet sind.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Beobachtete Daten

Beobachtete Daten übermitteln Informationen über Entitäten im Zusammenhang mit der Cybersicherheit, z. B. Dateien, Systeme und Netzwerke, die STIX Cyber-Observable Objects (SCOs) verwenden. Beobachtete Daten gelten für STIX 2.x.

Beobachtete Daten erfassen sowohl eine einzelne Beobachtung einer einzelnen Entität (Datei, Netzwerkverbindung) als auch die Zusammenfassung mehrerer Beobachtungen einer Entität.

Sie können beobachtete Daten selbst (ohne Beziehungen) verwenden, um Rohdaten zu übermitteln, die aus einer beliebigen Quelle erfasst wurden. Quellen umfassen Analystenberichte, Sandboxen sowie Netzwerk- und hostbasierte Erkennungstools.

Beispielsweise können beobachtete Daten Informationen zu einer IP-Adresse, einer Netzwerkverbindung, einer Datei oder einem Registrierungsschlüssel erfassen. Beobachtete Daten sind keine Intelligence Assertion, es handelt sich einfach um Rohinformationen ohne Kontext für das, was sie bedeuten.

Beobachtete Daten Definieren

Übermittelt Informationen über Entitäten im Zusammenhang mit der Cybersicherheit, z. B. Dateien, Systeme und Netzwerke, die STIX Cyber-Observable Objects (SCOs) verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Beobachtete Daten** Objekt.
4. Klicken Sie auf **Neu**.

Hinweis:
Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Detailansicht der beobachteten Daten

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung der beobachteten Daten.
Zuerst beobachtet	Die anfängliche Zeit, zu der die Daten angezeigt wurden.
Zuletzt beobachtet	Der Zeitpunkt, zu dem die Daten zuletzt angezeigt wurden.
Beobachtete Anzahl	Die Anzahl der Aufrufe jedes Cyber-erkennbaren Objekts. Der Wert muss eine Ganzzahl von 1 bis 999,999,999 sein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für die beobachteten Daten ein
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diese beobachteten Daten hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese beobachteten Daten hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die den beobachteten Daten zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die diesen beobachteten Daten zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die diesen beobachteten Daten zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den beobachteten Daten zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungsakteur

Bedrohungsakteure sind Einzelpersonen, Gruppen oder Organisationen, die mit böswilliger Absicht handeln. Bedrohungsakteure gelten für STIX 2.x.

Ein Bedrohungsakteur ist kein Angriffssatz, kann jedoch im Laufe der Zeit verschiedene Angriffssätze, Gruppen oder Organisationen unterstützen oder ihnen zugeordnet sein.

Bedrohungsakteure verwenden ihre Ressourcen und die Ressourcen eines Angriffssatzes, um Angriffe durchzuführen und Kampagnen für Ziele auszuführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Bedrohungsakteure anhand ihrer Motive, Fähigkeiten, Ziele, Raffinesse-Ebene, vergangener Aktivitäten, Ressourcen, auf die sie Zugriff haben, und ihre Rolle in der Organisation.

Definieren Sie Den Bedrohungsakteur

Definieren Sie Bedrohungsakteure, die Einzelpersonen, Gruppen oder Organisationen sind, die mit böswilliger Absicht handeln.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Bedrohungsakteur** Objekt.
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Detailansicht des Bedrohungsakteurs

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zur Verhinderung eines Angriffs.
Name	Geben Sie einen beschreibenden Namen ein, um den Standort zu identifizieren.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Angriffssatz enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Aliasse	Eine Liste anderer Namen zur Identifizierung dieses Bedrohungsakteurs. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf **Fügen Sie Neue Aliasse Hinzu** Symbol, das im Feld „Alias“ selbst verfügbar ist.
Ziele	Die allgemeinen Ziele dieses Bedrohungsakteurs, d. h., was versucht er zu tun. Beispielsweise können sie durch persönlichen Gewinn motiviert sein, ihr Ziel besteht jedoch darin, Kreditkartennummern zu stehlen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bedrohungsakteurtypen	Die Typen dieses Bedrohungsakteurs.
Bedrohungsakteurrollen	Die verschiedenen Bedrohungsakteurrollen für dieses Objekt.
Erstmals aufgetreten	Die Zeit, zu der dieser Bedrohungsakteur erstmals gesehen wurde. Diese Eigenschaft ist eine Zusammenfassungseigenschaft von Daten aus Sichtungen und anderen Daten, die in STIX verfügbar sein können oder nicht. Wenn neue Sichtungen empfangen werden, die vor dem Zeitstempel des ersten Auftretens liegen, kann das Objekt aktualisiert werden, um die neuen Daten zu berücksichtigen.
Zuletzt aufgetreten	Die Zeit, zu der dieser Bedrohungsakteur zuletzt gesehen wurde.
Primäre Motivation	Der primäre Grund, die Motivation oder der Zweck dieses Bedrohungsakteurs. Die Motivation ist, warum der Bedrohungsakteur das Ziel erreichen möchte (was er erreichen möchte). Beispielsweise könnte ein Bedrohungsakteur mit dem Ziel, den Finanzsektor in einem Land zu stören, durch ideologischen Hass auf den Kapitalismus motiviert werden.
Ausgereiftheit	Die Kompetenz, das spezifische Wissen, die spezielle Schulung oder das Fachwissen, das ein Bedrohungsakteur haben muss, um den Angriff auszuführen.
Sekundäre Motivationen	Diese Eigenschaft gibt die sekundären Gründe, Motivationen oder Zwecke für diesen Bedrohungsakteur an. Diese Motivationen können als gleiche oder nahezu gleiche Ursache der primären Motivation vorhanden sein. Sie ersetzt die primäre Motivation jedoch nicht oder erhöht sie notwendigerweise nicht, kann jedoch auf zusätzlichen Kontext hinweisen. Die Position in der Liste hat keine Bedeutung.
Ressourcenebene	Die Organisationsebene, auf der dieser Bedrohungsakteur normalerweise arbeitet, was wiederum die Ressourcen bestimmt, die diesem Bedrohungsakteur zur Verwendung bei einem Angriff zur Verfügung stehen. Dieses Attribut ist mit der Raffinesse-Eigenschaft verknüpft. Eine bestimmte Ressourcenebene bedeutet, dass der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Bedrohungsakteur Zugriff auf mindestens eine bestimmte Raffinesse hat.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diesen Bedrohungsakteur hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die dem Bedrohungsakteur zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die diesem Bedrohungsakteur zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die diesem Bedrohungsakteur zugeordnet sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Bedrohungsakteur zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, mit denen Angriffe kategorisiert werden können, die diesem Objekt zugeordnet sind.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Identitäten	Liste der Identitäten, die diesem Objekt zugeordnet sind.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Liste der Standorte, die diesem Objekt zugeordnet sind.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungsereignis

Ein Ereignis oder eine Situation, das/die das Potenzial hat, unerwünschte Konsequenzen oder Auswirkungen zu verursachen.

Ein Hacker, der eine Website angreift, ist ein Bedrohungsereignis. Wenn die Hacker eine Website beschädigen oder Informationen stehlen können, wird dies als Bedrohungsereignis definiert.

Definieren Sie Das Bedrohungsereignis

Definieren Sie ein Bedrohungsereignis, wenn ein Ereignis zu einem nicht autorisierten Zugriff auf und zur Beschaffung nicht öffentlicher Informationen oder zur Störung oder zum Missbrauch eines Informationssystems führt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Bedrohungsereignis** Objekt.
4. Klicken Sie auf **Neu**.

Hinweis:
Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Detailansicht des Bedrohungsakteurs

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zur Verhinderung eines Bedrohungsereignisses.
Name	Geben Sie einen beschreibenden Namen ein, um das Bedrohungsereignis zu identifizieren.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Bedrohungsereignis enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diesen Bedrohungsakteur hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die dem Bedrohungsereignis zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die diesem Bedrohungsereignis zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die diesem Bedrohungsereignis zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die dem Bedrohungsereignis zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungsgruppierung

Ein Bedrohungsgruppierungsobjekt bestätigt explizit, dass die referenzierten STIX-Objekte einen gemeinsam genutzten Kontext haben. Bedrohungsgruppierungen gelten für STIX 2.x.

Ein Bedrohungsgruppierungsobjekt stellt einen Satz von Daten dar, die bei ausreichender Analyse ausgereift sind, um einen Incident oder Bedrohungsbericht als STIX-Berichtsobjekt zu übermitteln. Beispielsweise kann eine Gruppierung verwendet werden, um eine laufende Untersuchung eines Sicherheitsereignisses oder Incidents zu charakterisieren.

Ein Bedrohungsgruppierungsobjekt kann auch verwendet werden, um zu bestätigen, dass die referenzierten STIX-Objekte mit einem laufenden Analyseprozess verknüpft sind. Beispielsweise kann ein Bedrohungsanalyst mit anderen in seiner Vertrauensgemeinschaft zusammenarbeiten, um eine Reihe von Kampagnen und Indikatoren zu untersuchen.

Das Bedrohungsgruppierungs-SDO enthält eine Liste von Verweisen auf SDOs, SCOs und SROs, zusammen mit einer expliziten Angabe des vom Inhalt freigegebenen Kontexts, einer Textbeschreibung und dem Namen der Gruppierung.

Definieren Sie Die Bedrohungsgruppierung

Definieren Sie Bedrohungsgruppierungen als Objekte mit einem gemeinsam genutzten Kontext.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Bedrohungsgruppierung** Objekt.
4. Klicken Sie auf **Neu**.

Hinweis:
Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Detailansicht der Bedrohungsgruppierung

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zur Verhinderung eines Angriffs vom Typ „Bedrohungsgruppe“.
Name	Geben Sie einen beschreibenden Namen ein, um die Bedrohungsgruppe zu identifizieren.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Bedrohungsereignis enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diese Bedrohungsgruppierung hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Bedrohungsgruppierung zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Bedrohungsgruppierung zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Bedrohungsgruppierung zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Bedrohungsgruppierung zugeordnet sind.

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bedrohungsereignisse	Listet die diesem Objekt zugeordneten Bedrohungsereignisse auf.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungshinweis

Eine Bedrohungshinweis übermittelt informativen Text, um zusätzliche Analysen bereitzustellen, die nicht in den STIX-Objekten, Markierungsdefinitionsobjekten oder Sprachinhaltsobjekten enthalten sind, auf die sich der Hinweis bezieht. Bedrohungshinweise gelten für STIX 2.x.

Beispielsweise kann ein Analyst einem Kampagnenobjekt, das von einer anderen Organisation erstellt wurde, eine Notiz hinzufügen. Der Hinweis kann darauf hinweisen, dass er Posts im Zusammenhang mit dieser Kampagne in einem Hacker-Forum gesehen hat.

Notizen werden normalerweise von menschlichen Analysten erstellt und bestehen aus menschlichem Text. Sie enthalten eine zusätzliche Eigenschaft, um den Autor zu erfassen, der die Notiz erstellt hat.

Bedrohungshinweis Definieren

Definieren Sie Bedrohungshinweise, die Informationen übermitteln, um weiteren Kontext oder Analysen bereitzustellen, die in vorhandenen Objekten nicht verfügbar sind.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Bedrohungshinweis** .
4. Klicken Sie auf **Neu**.

> **Hinweis:**
> Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Detailansicht der Bedrohungshinweise

Feld	Beschreibung
ID	Eindeutige ID für eine Bedrohungsnotiz.
Zusammenfassung	Geben Sie eine kurze Zusammenfassung des Notizinhalts an.
Inhalt	Gibt den Inhalt der Notiz an.
Autoren	Gibt den Namen des Autors an (z. B. ein Analyst).
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diese Bedrohungshinweis hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Bedrohungsgruppierung zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Bedrohungsgruppierung zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Bedrohungsgruppierung zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Bedrohungshinweis zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Bedrohungsereignisse	Listet die diesem Objekt zugeordneten Bedrohungsereignisse auf.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungsmeinung

Eine Meinung ist eine Bewertung der Genauigkeit der Informationen in einem STIX-Objekt, das von einer anderen Entität erstellt wurde. Bedrohungsmeinungen gelten für STIX 2.x.

Die Eigenschaft „Meinung“ erfasst die Ebene der Zustimmung oder Meinungsverschiedenheit mithilfe einer festen Skala. Die feste Skala unterstützt auch eine numerische Zuordnung, um konsistente statistische Vorgänge über Meinungen hinweg zu ermöglichen.

Beispielsweise kann ein Analyst aus einer verbrauchenden Organisation sagen, dass er einem Kampagnenobjekt „überhaupt nicht zustimmt“, und eine Erklärung dazu geben.

Meinungen sind subjektiv, und in der Spezifikation wird nicht angegeben, wie sie am besten zu interpretieren sind.

Menschliche Analysten erstellen Meinungen und bestehen aus menschlich orientiertem Text. Sie enthalten eine zusätzliche Eigenschaft, um den Autor zu erfassen, der die Meinung erstellt hat.

Definieren Sie Die Bedrohungsmeinung

Definieren Sie Bedrohungsmeinungen als Bewertung der Genauigkeit der Informationen in einem STIX-Objekt.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Bedrohungsmeinung** Objekt.
4. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Detailansicht der Bedrohungsmeinung

Feld	Beschreibung
ID	Eindeutige ID für eine Bedrohungsmeinung.
Meinung	Die Meinung des Herstellers zum STIX-Objekt.
Erklärung	Gibt den Inhalt der Meinung an.
Autoren	Gibt den Namen des Autors an (z. B. ein Analyst).
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für diese Vorgehensweise ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diese Bedrohungsmeinung hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Bedrohungsmeinung hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt die Zeit an, zu der der Datensatz in der Quelle erstellt wird.
Aktualisiert	Gibt die Zeit an, zu der der Datensatz in der Quelle geändert wird.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Bedrohungsmeinung zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Bedrohungsmeinung zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Bedrohungsmeinung zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Bedrohungsmeinung zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Bedrohungsereignisse	Listet die diesem Objekt zugeordneten Bedrohungsereignisse auf.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Bedrohungsbericht

Bedrohungsberichte sind Sammlungen von Threat Intelligence, die sich auf ein oder mehrere Themen konzentrieren. Bedrohungsberichte gelten für STIX 2.x.

Bedrohungsberichte enthalten eine Beschreibung eines Bedrohungsakteurs, Malware und Angriffstechnik, einschließlich Kontext und zugehörigen Details. Sie werden verwendet, um zugehörige Bedrohungsinformationen zusammenzufassen, damit sie als umfassende Cyberbedrohungsstory veröffentlicht werden können.

Das Bedrohungsbericht-SDO enthält eine Liste von Verweisen auf STIX-Objekte zusammen mit einer Textbeschreibung und dem Namen des Berichts.

Definieren Sie Den Bedrohungsbericht

Definieren Sie Bedrohungsberichte, die einen Bedrohungsakteur, Malware und Angriffstechnik beschreiben, einschließlich Kontext und zugehörige Details.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Bedrohungsbericht** Objekt.
4. Klicken Sie auf **Neu**.

   Hinweis:
   Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Detailansicht des Bedrohungsberichts

Feld	Beschreibung
ID	Geben Sie einen Namen an, um den Bedrohungsbericht zu identifizieren.
Name	Geben Sie eine kurze Zusammenfassung des Notizinhalts an.
Beschreibung	Eine Beschreibung, die zusätzlichen Einblick und Kontext zum Bericht bietet.
Berichtstypen	Gibt den Namen des Autors an (z. B. ein Analyst).
Veröffentlicht	Das Datum, an dem dieser Bericht vom Berichtautor offiziell veröffentlicht wurde.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diese Bedrohungshinweis hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Angriffsmuster hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Bedrohungsgruppierung zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Bedrohungsgruppierung zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Bedrohungsgruppierung zugeordnet sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den Bedrohungsberichten zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Bedrohungsereignisse	Listet die diesem Objekt zugeordneten Bedrohungsereignisse auf.
Bedrohungsgruppierungen	Listet die Bedrohungsgruppierungen auf, die diesem Objekt zugeordnet sind.
Bedrohungsberichte	Listet die diesem Objekt zugeordneten Bedrohungsberichte auf.
Tools	Listet legitime Software auf, die von Bedrohungsakteuren verwendet wird, um Angriffe auszuführen, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Tool

Tools sind legitime Software, die von Bedrohungsakteuren zum Ausführen von Angriffen verwendet wird. Tools gelten für STIX 2.x.

Mit Tools können Sie wissen, wie und wann Bedrohungsakteure sie für die Ausführung von Kampagnen verwenden. Im Gegensatz zu Malware werden diese Tools oder Softwarepakete häufig auf einem System gefunden und haben legitime Zwecke für Poweruser, Administratoren, Netzwerkadministratoren oder sogar normale Anwender.

Beispielsweise sind Remote Access Tools (RDP) und Network Scan Tools (Nmap) Tools, die ein Bedrohungsakteur während eines Angriffs verwendet.

Definieren Sie Tools

Definieren Sie Tools als legitime Software, die zum Ausführen von Angriffen verwendet wird.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Tool** Objekt.
4. Klicken Sie auf **Neu**.

Hinweis:
Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Detailansicht „Tools“

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung eines Tools.
Name	Geben Sie einen beschreibenden Namen ein, um das Tool zu identifizieren.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Tool enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Tooltypen	Die Art(en) der beschriebenen Tools.
Aliasse	Ein alternativer Name, der zur Identifizierung dieses Tools verwendet wird. **Hinweis:** Um einen neuen Alias hinzuzufügen, der in der Anwendung nicht vorhanden ist, klicken Sie auf **Fügen Sie Neue Aliasse Hinzu** Symbol, das im Feld „Alias“ selbst verfügbar ist.
Toolversion	Der dem Tool zugeordnete Versionsbezeichner.
Angriffsphasen	Stellt die Angriffsphase in einer Kill Chain wie LM, MITRE ATT&CK dar.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für dieses Tool hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Tool hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Bedrohungsgruppierung zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Bedrohungsgruppierung zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Bedrohungsgruppierung zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die den Tools zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Erkennungen und Verringerungen	Listet die Erkennungen und Minderungen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Schwachstelle

Eine Schwachstelle ist eine Schwachstelle oder ein Fehler in einer Software- oder Hardwarekomponente, die Angreifer ausnutzen. Schwachstellen gelten für STIX 2.x.

Die Schwachstelle oder der Fehler liegt in den Anforderungen, Designs oder Implementierungen des Codes in einer Software- oder Hardwarekomponente. Diese Schwachstelle wird direkt ausgenutzt, um die Vertraulichkeit, Integrität oder Verfügbarkeit dieses Systems negativ zu beeinflussen.

CVE ist eine Liste von Informationssicherheitsschwachstellen und -Risiken, die allgemeine Namen für öffentlich bekannte Probleme [CVE] bereitstellt.

Wenn beispielsweise eine Malware CVE-2015-12345 ausnutzt, kann ein Malware-Objekt mit einem Schwachstellenobjekt verknüpft werden, das auf CVE-2015-12345 verweist.

Definieren Sie Schwachstelle

Definieren Sie Schwachstelle als Schwachstelle oder Fehler in einer Software- oder Hardwarekomponente, die Angreifer ausnutzen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Schwachstelle** Objekt.
4. Klicken Sie auf **Neu**.

   Hinweis:
   Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Detailansicht der Schwachstellen

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung einer Schwachstelle.
Name	Ein Name, der zur Identifizierung der Schwachstelle verwendet wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Schwachstelle enthält, möglicherweise einschließlich ihres Zwecks und ihrer wichtigsten Merkmale.
Schweregrad	Gibt den normalisierten Schweregrad dieser Schwachstelle an
CVSS3.0	Gibt das CVSS v3 für diese Schwachstelle an.
CVSS2.0	Gibt das CVSS v2 für diese Schwachstelle an.
Nutzungsstatus	Gibt den Exploit-Status an, der dieser Schwachstelle zugeordnet ist
Veröffentlicht	Gibt an, wann die Schwachstelle veröffentlicht wird.
Datensatz zuletzt geändert	Gibt an, wann der Datensatz zuletzt geändert wurde.
Betroffene Software	Listet die betroffene Software auf, die der Schwachstelle zugeordnet ist.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diese Schwachstelle hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Schwachstelle hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Schwachstelle zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Schwachstelle zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Schwachstelle zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Schwachstelle zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Erkennungen und Verringerungen	Listet die Erkennungen und Minderungen auf, die diesem Objekt zugeordnet sind.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Marketingdefinitionen	Listet die Marketingdefinitionen auf, die diesem Objekt zugeordnet sind.
Sichtungen	Listet die Sichtungen auf, die diesem Objekt zugeordnet sind.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet eine Schwachstelle oder einen Fehler in einer Software oder Hardware auf, die Angreifer ausnutzen, die diesem Objekt zugeordnet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Rufen Sie Schwachstellendaten Ab

Rufen Sie angreifbare Daten ab, z. B. Konfigurationselemente, Einträge angreifbarer Elemente und Geschäftskontext.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Schwachstelle** Objekt.
   Die zugehörigen Schwachstellen, die diesem Objekt zugeordnet sind, werden angezeigt.
4. Wählen Sie den entsprechenden Schwachstellendatensatz aus.
   Wenn ihm CVEs zugeordnet sind, können Sie die zugehörigen angreifbaren Daten automatisch über die angegebene Schaltfläche abrufen, und diese zugehörigen Datensätze werden im Abschnitt „Geschäftskontext“ der Schwachstellen angezeigt.
5. Gehe zu **Interne Intelligenz** > **Einträge für angreifbare Elemente**an.
   Die zugehörigen CVEs-Datensätze werden angezeigt.
6. Wählen Sie ein beliebiges CVE aus, und klicken Sie auf **Rufen Sie schwachstellenbezogene Daten ab** Schaltfläche.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Dieser Link ordnet die Datensätze automatisch zu und ruft diesen bestimmten Geschäftskontext von Datensätzen ab.
- Wenn keine Datensätze zugeordnet sind, wird eine Informationsnachricht angezeigt, dass diesem spezifischen Schwachstellenobjekt keine angreifbaren Einträge zugeordnet sind. Sie müssen die Objekte manuell den angreifbaren Einträgen zuordnen, um die Daten abzurufen.
- Diese Schaltfläche löst eine geplante Hintergrundaufgabe aus, und die Details zur Auftragsinitiierung und -Ausführung werden in angezeigt **Aktivitätenstrom** Abschnitt. Wenn der Auftrag beispielsweise ausgelöst wird, zeigt der Aktivitätenstrom eine Aktivität an, die mit dem Abrufen zugeordneter Daten mit den Einträgen für angreifbare Elemente begonnen hat. Weitere Informationen zur Ausführung der geplanten Aufgaben zum Abrufen der Daten finden Sie unter Geplante Aufgaben .

7. Klicken Sie Auf **Link** Um die Objekte manuell zu verknüpfen.
8. Wählen Sie die zu verknüpfenden Datensätze aus, und rufen Sie die angreifbaren Daten mit ab **Rufen Sie schwachstellenbezogene Daten ab** Schaltfläche.
   Sobald Sie auf diese Schaltfläche klicken, wird der Hintergrundauftrag ausgelöst, und die Daten werden automatisch in den entsprechenden Abschnitt abgerufen. Eine Meldung zeigt an, dass der Auftrag zum Abrufen von Daten, die den Einträgen angreifbarer Elemente zugeordnet sind, gestartet wurde. Sie können den Status im Aktivitätenstrom nachverfolgen und die Liste aktualisieren, sobald der Auftrag abgeschlossen ist, um die Ergebnisse zu überprüfen. Wenn sich die Daten beispielsweise auf die Konfigurationselemente beziehen, überprüfen Sie die Ergebnisse im Abschnitt Konfigurationselemente. Weitere Informationen zum Hinzufügen von CVEs finden Sie unter Fügen Sie CVEs zu Drittparteieinträgen hinzu .

   Hinweis:
   Ebenso können Sie die Datensatzdaten erkennbarer Elemente abrufen. Weitere Informationen finden Sie unter Rufen Sie Schwachstellendaten Ab.

Markierungsdefinition

Das Markierungsdefinitionsobjekt stellt eine bestimmte Markierung dar. Datenmarkierungen stellen normalerweise Anforderungen an die Verarbeitung oder Freigabe von Daten dar.

Definieren Sie Die Markierungsdefinition

Definieren Sie Markierungsdefinitionen, um die Anforderungen für die Daten zu verarbeiten und freizugeben.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Markierungsdefinition** Objekt.
4. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Detailansicht der Markierungsdefinitionsquelle

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung einer Markierungsdefinition.
Name	Ein Name, der zur Identifizierung der Markierungsdefinition verwendet wird.
Definitionstyp	Die Typeigenschaft identifiziert den Typ des Objekts. Die Eigenschaft „Definition_type“ gibt den Typ der Markierungsdefinition an.
Definition	Die Definitionseigenschaft enthält das Markierungsobjekt selbst, z. B. TLP.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Vertrauen	Geben Sie die Konfidenz für dieses Objekt ein. Die Konfidenzeigenschaft gibt die Konfidenz an, die der Ersteller in der Richtigkeit seiner Daten hat. Der Konfidenzwert MUSS eine Zahl im Bereich von 0–100 sein.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Hinweise für diese Markierungsdefinition hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Markierungsdefinition hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Schwachstelle zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Schwachstelle zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Schwachstelle zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Schwachstelle zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.
Angriffsmuster	Listet die Angriffsmuster auf, die diesem Objekt zugeordnet sind.
Kampagnen	Listet die diesem Objekt zugeordneten Kampagnen auf.
Erkennungen und Verringerungen	Listet die Erkennungen und Minderungen auf, die diesem Objekt zugeordnet sind.
Identitäten	Listet die diesem Objekt zugeordneten Identitäten auf.
Indikatoren	Listet die zugehörigen Indikatoren für Kompromittierung (IOC) auf, die von der diesem Objekt zugeordneten Bedrohungsquelle identifiziert wurden.
Infrastruktur	Listet Systeme, Softwareservices und alle zugehörigen physischen oder virtuellen Ressourcen auf, die diesem Objekt zugeordnet sind.
Angriffssätze	Listet eine Reihe von konversären Verhaltensweisen und Ressourcen mit allgemeinen Eigenschaften auf, die diesem Objekt zugeordnet sind.
Standorte	Listet die Standorte auf, die diesem Objekt einen geografischen Kontext bereitstellen.
Malware	Listet den schädlichen Code auf, der diesem Objekt zugeordnet ist.
Malware-Analyse	Listet die schädliche Analyse auf, die diesem Objekt zugeordnet ist.
Erkennbare Elemente	Listet die diesem Objekt zugeordneten erkennbaren Elemente auf.
Beobachtete Daten	Listet die beobachteten Daten auf, die diesem Objekt zugeordnet sind.
Bedrohungsakteure	Listet die Einzelpersonen, Gruppen oder Organisationen auf, die mit böswilligen Absichten handeln, die diesem Objekt zugeordnet sind.
Bedrohungsereignisse	Listet die diesem Objekt zugeordneten Bedrohungsereignisse auf.
Bedrohungsgruppierungen	Listet die Bedrohungsgruppierungen auf, die diesem Objekt zugeordnet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze (Fortsetzung)

Feld	Beschreibung
Bedrohungshinweise	Listet die diesem Objekt zugeordneten Bedrohungshinweise auf.
Bedrohungsmeinungen	Listet die Bedrohungsmeinungen auf, die diesem Objekt zugeordnet sind.
Tools	Listet die Tools auf, die diesem Objekt zugeordnet sind.
Schwachstellen	Listet die diesem Objekt zugeordneten Schwachstellen auf.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Datenkomponente

Datenkomponenten werden verwendet, um bestimmte Eigenschaften oder Werte einer Datenquelle zu identifizieren.

Definieren Sie Die Datenkomponente

Definieren Sie eine Datenkomponente, um die Eigenschaften oder Werte einer Datenquelle zu identifizieren

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Datenkomponente** Objekt.
4. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

5. Füllen Sie im Formular die Felder aus.

Detailansicht der Datenkomponente

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung einer Datenkomponente.
Name	Ein Name, der zur Identifizierung der Datenkomponente verwendet wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Schwachstelle enthält, möglicherweise einschließlich ihres Zwecks und ihrer wichtigsten Merkmale.
Datenquelle	Gibt den normalisierten Schweregrad dieser Schwachstelle an
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Vertrauen	Gibt die Konfidenz für dieses Objekt an. Die Konfidenz muss zwischen 0 und 100 liegen.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diese Datenkomponente hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Datenkomponente hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen der Datenkomponente an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Schwachstelle zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Schwachstelle zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Schwachstelle zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Datenkomponente zugeordnet sind.

Zugehörige Datensätze

Feld	Beschreibung
Angriffsmuster	Listet die Angriffsmuster auf, die diesem Objekt zugeordnet sind.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Datenquellen

Datenquellen stellen die verschiedenen Themen/Themen von Informationen dar, die von Sensoren/Protokollen erfasst werden können. Datenquellen enthalten auch Datenkomponenten, die bestimmte Eigenschaften/Werte einer Datenquelle identifizieren.

Definieren Sie Datenquellen

Definieren Sie eine Datenquelle, um die verschiedenen Themen oder Themen von Informationen darzustellen.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Datenquellen** Objekt.
4. Klicken Sie auf **Neu**.

Hinweis:

Immer wenn Sie neue Objektdatensätze für erkennbare Elemente, Indikatoren, Entitäten oder Objekte erstellen, wird ein Quelldatensatz erstellt, und es wird eine Eingabeaufforderung angezeigt, dass der neue Objektdatensatz erstellt wird und der Anwender dann zum zusammengefassten Datensatz weitergeleitet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Füllen Sie im Formular die Felder aus.

Detailansicht der Schwachstellen

Feld	Beschreibung
ID	Eindeutige ID zur Identifizierung der Datenquelle.
Name	Ein Name, der zur Identifizierung der Datenquelle verwendet wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zur Datenquelle enthält, möglicherweise einschließlich ihres Zwecks und ihrer wichtigsten Merkmale.
Sammlungsebenen	Gibt die Beschreibung an, wo die Datenquelle physisch erfasst werden kann, z. B. Host, Netzwerk, Cloud-Steuerungsebene usw.
Plattformen	Gibt an, dass das System, in dem ein Angreifer arbeitet, ein Betriebssystem oder eine Anwendung sein kann.
Beitragende	Gibt die Beitragenden für diese Datenquelle an.
TLP	TLP wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die entsprechende Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diese Datenquelle hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diese Datenquelle hinzu.
Spezifikationsversion	Die Version der STIX-Spezifikation, die zur Darstellung dieses Objekts verwendet wird. Der Wert dieser Eigenschaft muss für STIX-Objekte, die gemäß dieser Spezifikation definiert sind, 2,1 betragen.
Lang	Diese Eigenschaft gibt die Sprache des Textinhalts in diesem Objekt an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Erweiterungen	Gibt die Erweiterungen des Angriffsmusters an.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Verarbeitungsstatus	Stellt den Verarbeitungsstatus dieses Objekts dar, Vorgehensweise.
Erstellt	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle erstellt wird.
Aktualisiert	Gibt das Datum und die Uhrzeit an, zu der das Objekt in der Quelle aktualisiert wurde.
Erstellt von Ref	Diese Eigenschaft gibt an, dass das Identitätsobjekt, das die Entität beschreibt, dieses Objekt erstellt hat.

6. Klicken Sie auf **Speichern**.
   Nach dem Speichern wird eine Eingabeaufforderung angezeigt, die darauf hinweist Ein neuer Datensatz für erkennbare Elemente wird erstellt. Klicken Sie Auf **Fahren Sie Fort** Dient zum Bearbeiten des Datensatzes und zum Erstellen neuer Beziehungen.
7. Klicken Sie auf **Fortsetzen**.

Wichtig:
Nachdem Sie einen neuen Datensatz für erkennbare Elemente erstellt haben, **Verhindern Sie Systemupdates** Das Kontrollkästchen wird angezeigt.

Aktivieren Sie dieses Kontrollkästchen, um Aktualisierungen vom System zu verhindern, nachdem die Datensätze für erkennbare Elemente, Indikatoren oder STIX-Objekte erstellt wurden.

Tags&Taxonomien

Feld	Beschreibung
Tags	
Tags auswählen	Wählen Sie die Tags aus, die der Datenquelle zugeordnet sind.
Tags hinzufügen	Fügen Sie neue Tags hinzu.
Taxonomien	
Taxonomie auswählen	Wählen Sie eine Taxonomie aus, die dieser Datenquelle zugeordnet ist.
Taxonomiewerte hinzufügen	Fügen Sie Taxonomiewerte hinzu, die dieser Datenquelle zugeordnet sind.

Nächste Maßnahme

Klicken Sie auf eine der folgenden zugehörigen Listen, um zusätzliche Informationen zu Objekten anzuzeigen, die der Datenquelle zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Datensätze

Feld	Beschreibung
Externe Referenzen	Listet die externen Referenzen auf, die auf nicht-STIX-Informationen verweisen. Diese Eigenschaft wird verwendet, um einen oder mehrere externe Objektbezeichner bereitzustellen.

Hinweis:

1. Sie können die zugehörigen Datensätze verknüpfen und die Verknüpfung aufheben, die diesem Objekt zugeordnet sind. Weitere Informationen finden Sie unter Verknüpfen Sie Mit Bedrohungsinformationen Verbundene Datensätze.
2. Die verschiedenen SDOs in der TI-Bibliothek enthalten auch die potenziellen Beziehungen. Um Beziehungen zwischen zwei beliebigen Objekten herzustellen, verwenden Sie **Potenzielle Beziehungen** Link von **Threat Intel-Bibliothek** Zum Bestätigen der Beziehungen zwischen den Objekten. Weitere Informationen finden Sie unter Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen.
3. Verwenden Sie auch **Zugehörige Datensätze** Abschnitt aus der Objektansicht, um die Beziehungen zwischen zwei Objekten mit zu bestätigen **Potenzielle Beziehungen** Abschnitt, der in der Formularansicht verfügbar ist. Weitere Informationen zu finden Sie unter . Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen.
4. Sie können Fälle Objekte hinzufügen. Weitere Informationen finden Sie unter Dem Fall hinzufügen.

Definieren Sie RSS-Feeds

Ein Threat Intelligence-Feed ist ein kontinuierlicher Echtzeit-Datenstrom, der Informationen im Zusammenhang mit Cyberrisiken oder -Bedrohungen sammelt. RSS-Feeds bieten eine einfache Möglichkeit, mit Ihren bevorzugten Websites wie Blogs oder aktuellen Cybersicherheitsnachrichten auf dem Laufenden zu bleiben.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **RSS-Feeds** Objekt.

Hinweis:
Die erfassten Feeds können in diesem Abschnitt durchsucht werden, Sie können jedoch keine neuen Datensätze erstellen.

4. Im Formular werden die folgenden Felder automatisch ausgefüllt.

RSS-Feeds-Detailansicht

Feld	Beschreibung
Titel	Titel des RSS-Feeds.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zu den RSS-Feeds enthält, möglicherweise einschließlich ihres Zwecks und ihrer wichtigsten Merkmale.
Verknüpfung	Gibt den Link an, der den RSS-Feeds hinzugefügt wurde.
Quelle	Gibt die RSS-Feed-Quelle an, aus der dieser Objektdatensatz erstellt wird.
Veröffentlichungsdatum	Gibt an, wann der RSS-Feed veröffentlicht wird.
Autor	Gibt den Autor für den RSS-Feed an.

5. Klicken Sie auf **Speichern**.

Einblicke

Feld	Beschreibung
Notizen	Fügen Sie zusätzliche Notizen für diesen Feed hinzu.

Zusätzliche Informationen

Feld	Beschreibung
Medien-URL	Gibt die Medien-URL an.
Feedback-Kommentare	Alle zusätzlichen Feedback-Kommentare zum Feedback.

Beziehungsobjekte

Verwenden Sie die Beziehungsobjekte, um zwei erkennbare Elemente oder ein erkennbares Element und SDO miteinander zu verknüpfen, um zu erklären, wie sie zueinander in Beziehung stehen.

STIX-Beziehungsobjekte (SROs) stellen Arten von Beziehungen zwischen verschiedenen STIX-Objekten dar. Die folgenden Beziehungsobjekte sind verfügbar:

- **Beziehung Zwischen Erkennbarem Element Und Erkennbarem Element** : Dieses Objekt definiert Beziehungen zwischen erkennbaren Elementen.
- **Objekt-Objekt-Beziehung** : Dieses Objekt definiert Beziehungen zwischen SDOs mit Ausnahme des Indikatorobjekts. Ein Beispiel für eine von Objekt zu Objekt definierte Beziehung ist, dass ein Angriffsmuster eine Malware bereitstellt.
- **Beziehung Zwischen Objekt Und Erkennbarem Element** : Dieses Objekt definiert Beziehungen zwischen SDOs und dem erkennbaren Objekt (SCO). Ein Beispiel für eine definierte Beziehung zwischen Objekt und erkennbarem Element ist, dass eine Infrastruktur aus Cyber-Objekten besteht, die Informationen zu einem potenziellen Angriff bereitstellen.
- **Objekt-Indikator-Beziehung** : Dieses Objekt definiert Beziehungen zwischen SDOs und dem Indikatorobjekt.
- **Indikator-Indikator-Beziehungen** : Dieses Objekt definiert Beziehungen zwischen Indikatorobjekten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Beziehung Zwischen Indikator Und Erkennbarem Element** : Dieses Objekt definiert Beziehungen zwischen dem Indikatorobjekt und anderen SDOs. Ein Beispiel für eine definierte Objekt-Indikator-Beziehung besteht darin, dass ein Indikator Beweise für eine Kampagne erkennt.

Objektbeziehungen

Beziehungsobjekt	Beispielquelle	Beispielziel	Beispielbeschreibung
Beziehungen Zwischen Erkennbarem Element Und Erkennbarem Element	IP-Adresse, Domänenname		Diese Beziehung beschreibt zwischen den erkennbaren Elementen.
Objekt-Objekt-Beziehungen	Angriffsmuster	Malware	Diese Beziehung beschreibt, dass dieses Angriffsmuster zur Bereitstellung dieser Malware-Instanz (oder -Familie) verwendet wird.
Objekt-Erkennbares Element-Beziehungen			Diese Beziehung beschreibt zwischen den Objekten und erkennbaren Elementen.
Objekt-Indikator-Beziehungen	Indikator	Angriffsmuster, Kampagne, Infrastruktur, Angriffssatz, Malware, Bedrohungsakteur, Tool	Diese Beziehung beschreibt, dass der Indikator Nachweise für das zugehörige Angriffsmuster, die Kampagne, die Infrastruktur, den Angriffssatz, die Malware erkennen kann, Bedrohungsakteur oder Tool. Der Nachweis ist möglicherweise nicht direkt. Beispielsweise kann der Indikator sekundäre Nachweise der Kampagne erkennen, z. B. Malware, die häufig von dieser bestimmten Kampagne verwendet wird.
Indikator: Indikatorbeziehungen	Infrastruktur	Beobachtete Daten	Diese Beziehung beschreibt, dass der Indikator basierend auf Informationen aus einem beobachteten Datenobjekt erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Objektbeziehungen (Fortsetzung)

Beziehungsobjekt	Beispielquelle	Beispielziel	Beispielbeschreibung
			Ein Beispiel für eine definierte Beziehung zwischen Objekt und erkennbarem Element ist, dass eine Infrastruktur aus Cyber-Objekten besteht, die Informationen zu einem potenziellen Angriff bereitstellen.
Indikator – Erkennbares Element			Diese Beziehung beschreibt zwischen den Indikatoren und erkennbaren Elementen.

Definieren Sie Beziehungen zwischen erkennbarem Element und erkennbarem Element

Definieren Sie Beziehungen zwischen erkennbaren Elementen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Gehe zu **Beziehungen** > **Erkennbares Element: Erkennbares Element**an.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder im Formular entsprechend aus.
6. Klicken Sie auf **Absenden**.

Definieren Sie Objekt-Objekt-Beziehungen

Definieren Sie Beziehungen zwischen SDOs mit Ausnahme des Indikatorobjekts.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Gehe zu **Beziehungen** > **Objekt: Objekt**an.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder im Formular entsprechend aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Absenden**.

Definieren Sie Beziehungen zwischen Objekt und erkennbaren Elementen

Definieren Sie Beziehungen zwischen SDOs und dem erkennbaren Objekt (SCO).

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Gehe zu **Beziehungen** > **Objekt – Erkennbares Element**an.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder im Formular entsprechend aus.

6. Klicken Sie auf **Absenden**.

Definieren Sie Objekt-Indikator-Beziehungen

Definieren Sie Beziehungen zwischen dem Indikatorobjekt und anderen SDOs.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Gehe zu **Beziehungen** > **Objektindikator**an.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder im Formular entsprechend aus.

6. Klicken Sie auf **Absenden**.

Definieren Sie Indikator-Indikator-Beziehungen

Definieren Sie Beziehungen zwischen dem Indikatorobjekt und anderen Verwenden Sie die Beziehungsobjekte, um zwei erkennbare Elemente oder ein erkennbares Element und SDO miteinander zu verknüpfen, um zu erklären, wie sie zueinander in Beziehung stehen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Gehe zu **Beziehungen** > **Indikator: Indikator**an.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder im Formular entsprechend aus.
6. Klicken Sie auf **Absenden**.

Definieren Sie Beziehungen zwischen Indikator und erkennbarem Element

Definieren Sie Beziehungen zwischen dem Indikatorobjekt und anderen SDOs.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Gehe zu **Beziehungen** > **Indikator – Erkennbares Element**an.
4. Klicken Sie auf **Neu**.
5. Füllen Sie die Felder im Formular entsprechend aus.
6. Klicken Sie auf **Absenden**.

Potenzielle Beziehungen

Die Anwendung verwendet automatisierte Korrelation, um potenziell mögliche Beziehungen zwischen zwei SDOs, zwei erkennbaren Elementen oder einem erkennbaren Element und SDO herzustellen.

1. Wählen Sie einen oder mehrere potenziell zugehörige Datensätze aus, und wenden Sie diese Aktion auf die Anwenderoberfläche an. Dadurch werden die Datensätze weiter in den Abschnitt „bestätigte Beziehungen“ geändert und im Abschnitt „zugehörige Datensätze“ sichtbar.
2. Alle bestätigten Korrelationen, die von einem Analysten erfasst oder manuell erstellt wurden, überschreiben die durch die automatische Korrelation erstellten potenziellen Beziehungen.

Bestätigen Sie die potenzielle Beziehung zwischen erkennbarem Element und erkennbarem Element

Verwenden Sie diesen Abschnitt, um die Beziehungen zwischen den erkennbaren Elementen zu bestätigen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Gehe zu **Potenzielle Beziehungen** > **Erkennbares Element: Erkennbares Element**an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie den Datensatz des erkennbaren Elements aus.
5. Klicken Sie Auf **Beziehung Bestätigen** .
   Idealerweise wird ein Datensatz für eine potenzielle Beziehung erstellt, der basierend auf seinen Korrelationsregeln identifiziert wird. Sobald Sie die Beziehung bestätigt haben, wird der Datensatz der erkennbaren Elemente in den Abschnitt „Beziehungen“ verschoben, was bedeutet, dass die Beziehung zwischen den erkennbaren Elementen zu erkennbaren Elementen bestätigt wird. Der Datensatz zeigt eine bestätigte Beziehung nur an, wenn die Korrelationsregeln übereinstimmen. Beispielsweise kann eine potenzielle Beziehung erstellt werden, wenn zwei erkennbare Elemente vom Typ URLs denselben Domänennamen haben.

   Alternativ können Sie auch einen neuen Datensatz erkennbarer Elemente erstellen, indem Sie die erkennbaren Elemente aus der Liste der erkennbaren Elemente verknüpfen und die Beziehungen auf der Registerkarte zugehörige Datensätze jedes erkennbaren Elements bestätigen.

   a. Öffnen Sie einen beliebigen Datensatz erkennbarer Elemente.
   b. Wechseln Sie zu **Zugehörige Datensätze** Registerkarte.
   c. Klicken Sie auf **Link** Schaltfläche.
   d. Wählen Sie ein oder mehrere erkennbare Elemente aus.
   e. Klicken Sie Auf **Link** .
      Dadurch wird eine neue Beziehung zwischen dem ausgewählten Datensatz erkennbarer Elemente und den neu verknüpften erkennbaren Elementen erstellt.
6. Klicken Sie Auf **Löschen** Um die Beziehungen zu löschen.

Bestätigen Sie potenzielle Objekt-Objekt-Beziehungen

Definieren Sie die potenziellen Beziehungen zwischen den Objekten.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Gehe zu **Potenzielle Beziehungen** > **Objekt: Objekt**an.
4. Wählen Sie den Datensatz des erkennbaren Elements aus.
5. Klicken Sie Auf **Beziehung Bestätigen** .
   Idealerweise wird ein Datensatz für eine potenzielle Beziehung erstellt, der basierend auf seinen Korrelationsregeln identifiziert wird. Sobald Sie die Beziehung in diesem Abschnitt bestätigt haben, wird der Datensatz der erkennbaren Elemente in den Abschnitt „Beziehungen“ verschoben, was bedeutet, dass die Beziehung zwischen den erkennbaren Elementen und erkennbaren Elementen bestätigt wird. Der Datensatz zeigt eine bestätigte Beziehung nur an, wenn die Korrelationsregeln übereinstimmen. Beispielsweise kann eine potenzielle Beziehung erstellt werden, wenn zwei erkennbare Elemente vom Typ URLs denselben Domänennamen haben.

   Alternativ können Sie auch einen neuen Datensatz erkennbarer Elemente erstellen, indem Sie die erkennbaren Elemente aus der Liste der erkennbaren Elemente verknüpfen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und die Beziehungen auf der Registerkarte zugehörige Datensätze jedes erkennbaren Elements bestätigen.

a. Öffnen Sie einen beliebigen Datensatz erkennbarer Elemente.

b. Wechseln Sie zu **Zugehörige Datensätze** Registerkarte.

c. Klicken Sie auf **Link** Schaltfläche.

d. Wählen Sie ein oder mehrere erkennbare Elemente aus.

e. Klicken Sie Auf **Link** .
Dadurch wird eine neue Beziehung zwischen dem ausgewählten Datensatz erkennbarer Elemente und den neu verknüpften erkennbaren Elementen erstellt.

6. Klicken Sie Auf **Löschen** Um die Beziehungen zu löschen.

Bestätigen Sie potenzielle Beziehungen zwischen Indikator und Indikator

Definieren Sie die potenziellen Beziehungen zwischen den Objekten.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Gehe zu **Potenzielle Beziehungen** > **Indikator: Indikator**an.
4. Wählen Sie den Datensatz des erkennbaren Elements aus.
5. Klicken Sie Auf **Beziehung Bestätigen** .
   Ein Datensatz für eine potenzielle Beziehung wird idealerweise basierend auf automatisierten Korrelationsregeln bestätigt. Sobald Sie die Beziehung bestätigt haben, wird der Datensatz der erkennbaren Elemente in den Abschnitt „Beziehungen“ verschoben, was bedeutet, dass die Beziehung zwischen den erkennbaren Elementen zu erkennbaren Elementen bestätigt wird.

   Der Datensatz zeigt eine bestätigte Beziehung nur an, wenn die Korrelationsregeln übereinstimmen. Beispielsweise wird eine potenzielle Beziehung bestätigt, wenn zwei erkennbare Elemente vom Typ URLs denselben Domänennamen haben.

   Alternativ können Sie auch einen neuen Datensatz erkennbarer Elemente erstellen, indem Sie die erkennbaren Elemente aus der Liste der erkennbaren Elemente verknüpfen und die Beziehungen auf der Registerkarte zugehörige Datensätze jedes erkennbaren Elements bestätigen.

   a. Öffnen Sie einen beliebigen Datensatz erkennbarer Elemente.

   b. Wechseln Sie zu **Zugehörige Datensätze** Registerkarte.

   c. Klicken Sie auf **Link** Schaltfläche.

   d. Wählen Sie ein oder mehrere erkennbare Elemente aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Klicken Sie Auf **Link** .
Dadurch wird eine neue Beziehung zwischen dem ausgewählten Datensatz erkennbarer Elemente und den neu verknüpften erkennbaren Elementen erstellt.

6. Klicken Sie Auf **Löschen** Um die Beziehungen zu löschen.

Exportieren Sie Intelligence-Daten

Verwenden Sie die Exportfunktion, um die Intelligence-Daten manuell in verschiedenen Formaten zu exportieren.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Derzeit ist die Exportfunktion auf erkennbare Elemente, Indikatoren und Fallmanagement beschränkt. Im folgenden Verfahren wird beschrieben, wie Sie die Daten erkennbarer Elemente exportieren können, und wie Sie die Indikatordaten exportieren können.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **Erkennbare Elemente** > **Alle erkennbaren Elemente**an.
2. Wählen Sie ein oder mehrere erkennbare Elemente aus.
3. Klicken Sie Auf **Exportieren** Schaltfläche.

   Hinweis:
   Die **Exportieren** Die Schaltfläche ist nur aktiviert, wenn erkennbare Elemente für den Export ausgewählt sind. Wenn keine erkennbaren Elemente ausgewählt sind, bleibt die Schaltfläche deaktiviert.

4. Wählen Sie den gewünschten Dateityp für den Export aus.
   Derzeit werden Excel, CSV und STIX 2,1 JSON unterstützt. Angenommen, wenn Ihr Exporttyp Excel ist, ist die Anzahl der Datensätze, die gleichzeitig exportiert werden können, unabhängig vom ausgewählten Formattyp auf 000 beschränkt.

   Wenn die Auswahl 10.000 Datensätze überschreitet, wird eine Fehlermeldung angezeigt, die angibt, dass die maximale Grenze für den ausgewählten Formattyp überschritten wurde, und nur die ersten 10000 Datensätze werden exportiert.

   Wenn das Exportformat CSV ist und die Datensatzgrenze überschritten wird, wird eine Warnmeldung angezeigt, die angibt, dass der Export erfolgt **In Bearbeitung** status zusammen mit einem Link zum Anzeigen des Exportstatus. Sie können auf den Link klicken, um den Status anzuzeigen, den Datensatz zu aktualisieren und zu wechseln **Verarbeitet** status nach der Aktualisierung können Sie den Anhang herunterladen.

5. Klicken Sie auf **Exportieren**.

   Hinweis:
   Sie können Exportdaten auch aus anzeigen **Importe/Exporte** Modul.

   Eine Bestätigungsnachricht, die angibt, dass der Export erfolgreich ist und Ihr Download abgeschlossen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bestätigen Sie potenzielle Beziehungen aus zugehörigen Datensätzen

Bestätigen Sie die Beziehungen zwischen den beiden SDOs.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

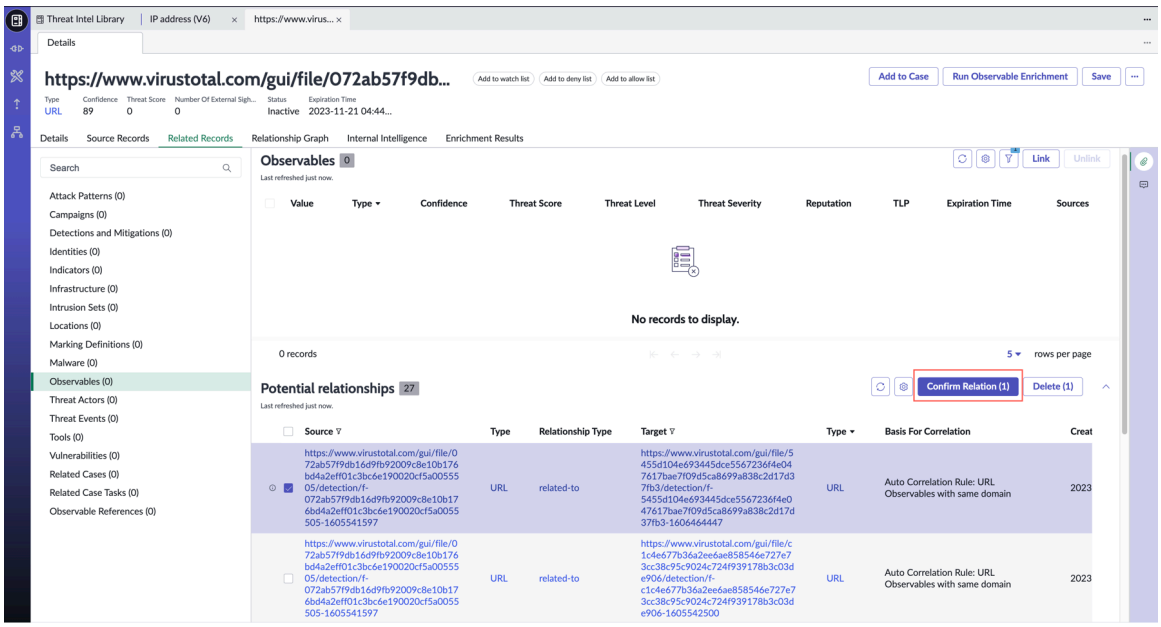
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Wechseln Sie zu **Zugehörige Datensätze** Abschnitt.
4. Erweitern Sie **Potenzielle Beziehungen** .
5. Öffnen Sie einen beliebigen Datensatz wie erkennbare Elemente, Indikatoren oder andere Objekte, die Sie bestätigen möchten, dass die Beziehungen zwischen zwei SDOs bestätigt werden.
6. Wählen Sie hier beispielsweise aus **Erkennbare Elemente** Über die linke Navigation.
7. Wählen Sie aus **Erkennbares Element(e)** Datensätze aus der Liste.

Hinweis:
Im Listenabschnitt werden alle verknüpften Datensätze erkennbarer Elemente des zugehörigen erkennbaren Elements angezeigt.

8. Klicken Sie Auf **Bestätigen Sie Beziehungen** Schaltfläche zum Bestätigen der Beziehungen zwischen den Objekten.

Hinweis:
Weitere Informationen finden Sie unter Beziehungsobjekte Und Potenzielle Beziehungen.



9. Klicken Sie Auf **Löschen** Zum Löschen der zugeordneten erkennbaren Elemente.
Informationen dazu, wie potenzielle Beziehungen und Beziehungen zwischen den SDOs hergestellt werden, finden Sie unter Potenzielle Beziehungen Und Beziehungsobjekte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatisierte Korrelation

Automatisierte Korrelation hilft Ihnen, die Beziehungen zwischen erkennbaren Elementen, Indikatoren und Objekten zu identifizieren.

Mit dem Korrelationsprozess stellt die Anwendung automatisch die Korrelation zwischen Threat Intelligence-Datensätzen basierend auf den vordefinierten Regeln her. Basierend auf dem Typ der angewendeten Regel kann die Beziehung eine bestätigte Beziehung oder eine potenzielle Beziehung sein. Wenn die Beziehungen zwischen den Objekten bestätigt werden, werden diese Objekte automatisch in der Detailansicht dieses Objekts unter angezeigt **Zugehörige Datensätze** Abschnitt.

Im Folgenden werden die Beziehungen und potenziellen Beziehungen beschrieben:

- **Beziehungen** : Verwenden Sie die Beziehungsobjekte, um zwei erkennbare Elemente oder ein erkennbares Element miteinander zu verknüpfen, und SDO, um zu erklären, wie sie zueinander in Beziehung stehen.
- **Potenzielle Beziehungen** : Verwenden Sie die potenziellen Beziehungen, um potenziell mögliche Beziehungen zwischen zwei SDOs, zwei erkennbaren Elementen oder einem erkennbaren Element und SDO mithilfe der automatisierten Korrelation herzustellen.

Im Folgenden finden Sie die vordefinierten Korrelationsregeln, die im Basissystem bereitgestellt werden:

Korrelationsregeln

Regelname	Regelbeschreibung	Regeldefinition	Regelaktion
Erkennbare Elemente mit demselben Datei-Hash	Die Regel vergleicht die Hash-Werte der erkennbaren Elemente (desselben Typs) und gibt an, ob sie denselben Hash verwenden.	Die Regel vergleicht die Hash-Werte (desselben Typs) der Indikatoren und gibt an, ob sie denselben Hash verwenden.	Erstellt eine Beziehung
Erkennbare URL-Elemente mit derselben Domäne	Die Regel untersucht die Gemeinsamkeiten in der Struktur von URLs, um festzustellen, ob sie dieselbe Basisdomäne teilen.	Die Regel untersucht die Gemeinsamkeiten in der Struktur von URLs – gibt an, ob sie dieselbe Basisdomäne teilen und eine ähnliche Unterverzeichnisstruktur haben.	Erstellt eine potenzielle Beziehung
Erkennbares Element als Quellen im Netzwerkobjekt gefunden	Die Regel stimmt den Wert des Netzwerkquellenattributs mit erkennbaren Elementen IPV4, IPV6 oder Domänenname im System und Links als Quelle des Datenverkehrs überein.	Die Regel stimmt den Wert des Quellattributs mit erkennbaren IPV4-, IPV6- oder Domänennamen-Elementen im System überein und verknüpft als Quelle des Datenverkehrs.	Erstellt eine Beziehung
Erkennbares Element als Ziel im Netzwerkobjekt gefunden	Die Regel stimmt den Wert des Netzwerkzielattributs mit erkennbaren IPV4-, IPV6- oder	Die Regel stimmt den Wert des Quellattributs mit erkennbaren IPV4-, IPV6- oder Domänennamen-	Erstellt eine Beziehung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrelationsregeln (Fortsetzung)

Regelname	Regelbeschreibung	Regeldefinition	Regelaktion
	Domänennamen-Elementen im System und in Links als Ziel des Datenverkehrs überein.	Elementen im System und Links als Ziel des Datenverkehrs überein.	
Verknüpfen Sie erkennbare Elemente basierend auf der Kommunikation	Basierend auf Netzwerkobjekten identifiziert die Regel alle erkennbaren Elemente (IPV4, IPV6 und Domänenname), die mit demselben Ziel (IPV4, IPV6 oder Domänenname) kommuniziert haben, und stellt eine Beziehung zwischen diesen erkennbaren Elementen her. Auch zugehörige erkennbare Elemente (IPV4, IPV6 und Domänenname), wenn sie sich auf dasselbe Netzwerkobjekt beziehen wie die mit dem Ziel kommunizierende Quelle.	Auf der Basis von Netzwerkobjekten identifiziert die Regel alle Indikatoren, die mit demselben Ziel kommuniziert haben (IPV4, IPV6, mac-addr oder Domänenname), und stellt eine Beziehung zwischen diesen Indikatoren her, die mit derselben C2-Infrastruktur verbunden sind.	Erstellt eine Beziehung
Zugehörige erkennbare Stammdomänen zu Unterdomänen	Die Regel bindet eine Stammdomäne mit Unterdomänen zusammen und umgekehrt für den Domänentyp erkennbarer Elemente.	Die Regel bindet eine Stammdomäne mit Unterdomänen zusammen.	Erstellt eine Beziehung
Zugehörige Domänen zu IPs basierend auf DNS-Auflösungen	Mithilfe von Domänen-ipv4- oder Domänen-ipv6-Attributen erkennbarer Domänenelemente stellt die Regel Beziehungen zwischen den Domänen und IPs her.	Verwenden Sie die Attribute Domain-ipv4 oder Domain-ipv6. Die Regel identifiziert alle Domänen oder Subdomänen, die in dieselbe IP-Adresse aufgelöst werden, und stellt Beziehungen zwischen den Indikatoren her, die ihre Verbindung mit derselben C2-Infrastruktur angeben.	Erstellt eine Beziehung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrelationsregeln (Fortsetzung)

Regelname	Regelbeschreibung	Regeldefinition	Regelaktion
Übereinstimmende Domänen mit SSL-Zertifikaten	Die Regel analysiert die SSL-Zertifikatinformationen, die den erkennbaren Domänenelementen zugeordnet sind, und stellt eine Beziehung zwischen ihnen her.	Die Regel analysiert die SSL-Zertifikatinformationen, die den Indikatoren zugeordnet sind, und identifiziert, dass beide Zertifikate von derselben Zertifizierungsstelle ausgestellt werden und dasselbe Ablaufdatum haben, und stellt Beziehungen zwischen den Indikatoren her, die ihre Verbindung mit derselben C2-Infrastruktur oder Bedrohungskampagne angeben.	Erstellt eine Beziehung
Verknüpfen Sie Entitäten basierend auf allgemeinen erkennbaren Elementen	Die Regel vergleicht, ob dasselbe erkennbare Element mit zwei verschiedenen Entitäten verknüpft ist, und bezieht sie zueinander.	Die Regel vergleicht, ob dasselbe erkennbare Element mit zwei verschiedenen Entitäten verknüpft ist, und identifiziert sie als zueinander verwandt.	Erstellt eine potenzielle Beziehung
Verknüpfen Sie Indikatoren basierend auf allgemeinen erkennbaren Elementen	Die Regel vergleicht, ob dasselbe erkennbare Element mit zwei verschiedenen Indikatoren verknüpft ist, und bezieht sie zueinander.	Die Regel vergleicht, ob dasselbe erkennbare Element mit zwei verschiedenen Indikatoren verknüpft ist, und identifiziert sie als zueinander verwandt.	Erstellt eine potenzielle Beziehung
Verknüpfen Sie Indikatoren mit Objekten basierend auf allgemeinen erkennbaren Elementen	Die Regel vergleicht, ob dasselbe erkennbare Element mit Indikatoren und Objekten zusammenhängt, und bezieht sie zueinander.	Die Regel vergleicht, ob dasselbe erkennbare Element mit zwei verschiedenen Indikatoren und Objekten verknüpft ist, und identifiziert sie als zueinander verwandt.	Erstellt eine potenzielle Beziehung

Mit Datenexporten arbeiten

Threat Intelligence-Sicherheitszentrum Unterstützt den manuellen Export von erkennbaren Elementen, Indikatoren und Fällen in den empfohlenen Formaten.

Mit dieser Funktionalität können Sie die Daten einfach für weitere Analysen extrahieren. Dies sind die wichtigsten Funktionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Exportieren Sie erkennbare Elemente, Indikatoren und Fälle einzeln oder als Massenexport.
- Ausgabe in empfohlenen Formaten wie CSV, STIX 2,1 für eine nahtlose Integration.

Hinweis:
Die Funktionalität „Datenexporte“ wird derzeit nur für erkennbare Elemente, Indikatoren und das Fallmanagement unterstützt. Innerhalb des Fallmanagements sind Exporte auf die Listen erkennbarer Elemente und Indikatoren unter Fallartefakte beschränkt.

Zeigen Sie alle Exporte an

Verwenden Sie diesen Abschnitt, um alle manuell exportierten Datensätze anzuzeigen.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Export

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Importe/Exporte**an.
2. Auswahlvorgang **Exporte** > **Alle Exporte**
   Auf dieser Seite werden die Exportdatensätze angezeigt.
3. Öffnen Sie einen beliebigen Datensatz, um den Status des Exportprozesses anzuzeigen.

Zeigen Sie meine Exporte an

Zeigen Sie die Exporte an, für die Sie berechtigt sind, und laden Sie sie herunter.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Export

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Importe/Exporte**an.
2. Auswahlvorgang **Exporte** > **Meine Exporte**
   Auf dieser Seite werden die Exportdatensätze angezeigt.
3. Öffnen Sie einen beliebigen Datensatz, um den Status des Exportprozesses anzuzeigen.

Exportieren Sie Intelligence-Systemeigenschaften

In diesem Abschnitt werden die Datensatzbeschränkungen und ihre Eigenschaften beim Exportieren von Daten beschrieben.

Hinweis:
TISC Stellt den folgenden Grenzwert für Datenexporte bereit. Um die folgenden Eigenschaften festzulegen, navigieren Sie zu **Systemeigenschaften** > **Import Export**an.

Erforderliche Rolle: sn_sec_tisc.Export

Format	Eigenschaft	Beschreibung
STIX 2.1 JSON	sn_sec_tisc.stix_Export_limit	Maximale Anzahl von Zeilen, die in eine STIX 2,1-Datei exportiert werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Format	Eigenschaft	Beschreibung
		Der Standardwert e ist 10000.
STIX 2.1 JSON	sn_sec_tisc.stix_Export_Payload_Streaming_attachment_objects_size	Wenn die Anzahl der Objekte im Array „Objekte“ der STIX-Exportnutzlast größer ist als die in dieser Eigenschaft angegebene Anzahl, wird JSONStreamingAPI zum Erstellen eines Anhangs verwendet. Die standardmäßige Exportbeschränkung ist 4000.
STIX 2.1 JSON	sn_sec_tisc.stix_JSON_from_JSON_Streaming_api_trigger_timeout	Zeitüberschreitung (in Sekunden), die beim Auslösen der Flow Designer-Aktion zum Generieren DES STIX-JSON-Anhangs mit der JSON-Streaming-API verwendet wird. Die standardmäßige Exportbeschränkung ist 900.

Hinweis:
Ein besseres Verständnis der Exportbeschränkung für andere Formattypen finden Sie unter Exportlimits .

MITRE-ATT&CK™ Repository

Die MITRE-ATT&CK Das Repository ist unter der Intelligence Library verfügbar, in der die Daten aus den MITRE-Quellen erfasst werden.

Die MITRE-Daten, die in das Repository kommen, werden in einem separaten MITRE-Repository von den Daten der Bedrohungsbibliothek gespeichert, in dem MITRE-Daten nicht für den Zusammenfassungs- oder Deduplizierungsflow zusammengefasst werden und unabhängig sind.

Die verfügbaren Datenquellen in der Anwendung sind:

1. MITRE: ENTERPRISE ATT&CK
2. MITRE: MOBILE ATT&CK
3. MITRE: ICS ATT&CK

Die Daten für diese Quellen werden in einem separaten MITRE-Repository unter der TI-Bibliothek im Basissystem gespeichert. Wenn Sie eine neue MITRE-Quelle erstellen möchten, konfigurieren Sie eine anwenderdefinierte Quelle. Weitere Informationen finden Sie unter Zeigen Sie Anwenderdefinierten Feed An Und klicken Sie in der Formularansicht auf **Erweitert** Aktivieren Sie das Kontrollkästchen, und aktivieren Sie das **Berichtsprozessor** Als: **MITRECollectionDataProcessor** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Matrizen Verwalten

Verwalten Sie die Matrizen, die aus den MITRE TAXII-Sammlungen importiert werden. Matrizen sind eine Sammlung von Taktiken und Techniken. Sie können die Matrizen anzeigen, um zu überprüfen, ob Ihre Sammlungen im MITRE-ATT&CK-Repository verfügbar sind.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Nachdem Sie die MITRE ATT&CK-bezogenen Feed-Datenquellen aktiviert haben, die im Basissystem verfügbar sind, klicken Sie auf **Jetzt Ausführen** Um die Integrationen auszuführen und die MITRE-bezogenen Informationen abzurufen.
   Weitere Informationen zum Aktivieren der Integrationen
2. Um die MITRE ATT&CK-Repository-Daten anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK**an.
   Die zugehörigen MITRE ATT&CK-Datensätze werden angezeigt. Standardmäßig befinden sich alle Datensätze im Status „aktiviert“.

   Hinweis:
   Sie können nur die Matrizen aktivieren, die für Ihre Organisation relevant sind.

3. Wählen Sie einen Matrixdatensatz aus, und klicken Sie auf **Deaktivieren** Wenn Sie einen bestimmten Datensatz deaktivieren möchten.
4. Alternativ können Sie einen neuen Matrizen-Datensatz erstellen, indem Sie auf klicken **Neu** Zum manuellen Erstellen der MITRE ATT&CK-Matrizen.
5. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Minderung erstellen – Details

Feld	Beschreibung
Name	Geben Sie den Namen der Matrix ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Datensatz erstellt wird.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um den Matrixdatensatz zu aktivieren.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Angriffssatz enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Einblicke	
Notizen	Alle zusätzlichen Informationen im Zusammenhang mit der Minderung.
Zusätzliche Informationen	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Objekttyp hinzu.
Kommentare	Fügen Sie alle Kommentare hinzu, die Sie zusätzlich haben könnten.

Techniken Verwalten

Verwalten Sie die Techniken, die aus den MITRE TAXII-Sammlungen importiert werden. Die Techniken enthalten verschiedene Methoden, die Angreifer entwickelt haben, um eine bestimmte Taktik anzuwenden. Sie können Techniken überprüfen und deaktivieren, die für Ihre Organisation nicht relevant sind. In STIX werden Techniken als Angriffsmuster bezeichnet.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Techniken stellen dar, wie ein Angreifer ein taktisches Ziel erreicht, indem er eine Aktion ausführt.

Prozedur

1. Nachdem Sie die MITRE ATT&CK-bezogenen Feed-Datenquellen aktiviert haben, die im Basissystem verfügbar sind, klicken Sie auf **Jetzt Ausführen** Um die Integrationen auszuführen und die MITRE-bezogenen Informationen abzurufen.
   Weitere Informationen zum Aktivieren der Integrationen
2. Um die MITRE ATT&CK-Repository-Daten anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Techniken**an. Die Datensätze der MITRE ATT&CK-Techniken werden angezeigt. Standardmäßig befinden sich alle Datensätze im Status „aktiviert“.
3. Wählen Sie einen beliebigen Technikdatensatz aus, und klicken Sie auf **Deaktivieren** Wenn Sie einen bestimmten Datensatz deaktivieren möchten.
4. Alternativ können Sie neue Technikdatensätze erstellen, indem Sie auf klicken **Neu** Zum manuellen Erstellen der MITRE ATT&CK-Techniken.
5. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Minderung erstellen – Details

Feld	Beschreibung
ID	Eindeutige ID für eine Technik.
Name	Geben Sie den Namen der Technik ein.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Datensatz erstellt wird.
Plattformen	Fügen Sie die erforderlichen Plattformen hinzu.
Berechtigungen erforderlich	Fügen Sie die erforderlichen Berechtigungen hinzu.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Priorität	Gibt die der MITRE-Technik zugewiesene Prioritätsstufe an, z. B. Niedrig, Mittel, hoch oder Kritisch. **Hinweis:** Prioritäten können Techniken zugewiesen werden, um Ihrer Organisation Relevanz zu verleihen.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Angriffssatz enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Erkennung	Die Erkennungstechnik wird verwendet, um den Zugriff von Angreifern auf oder nicht autorisierte Aktivitäten in Computernetzwerken zu identifizieren.
Einblicke	
Notizen	Alle zusätzlichen Informationen im Zusammenhang mit der Minderung.
Zusätzliche Informationen	
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für diesen Objekttyp hinzu.
Kommentare	Fügen Sie alle Kommentare hinzu, die Sie zusätzlich haben könnten.
TISC-Tags	
TISC-Tags auswählen	Wählen Sie Tags aus, um Datensätze, die aus dieser Quelle in das System aufgenommen wurden, mit Anmerkungen zu versehen oder zu markieren. **Hinweis:** Tags können Techniken zugewiesen werden, um Ihrer Organisation Relevanz zu verleihen.

Verwalten Sie Risikominderungen

Verwalten Sie die Minderungen, die aus den MITRE TAXII-Sammlungen importiert werden. Mit Minderungen können Sie verhindern, dass Angreifer Techniken oder Untertechniken erfolgreich für Ihre Organisation ausführen. In STIX werden Minderungen als Handlungsverlauf bezeichnet.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Nachdem Sie die MITRE ATT&CK-bezogenen Feed-Datenquellen aktiviert haben, die im Basissystem verfügbar sind, klicken Sie auf **Jetzt Ausführen** Um die Integrationen auszuführen und die MITRE-bezogenen Informationen abzurufen.
   Weitere Informationen zum Aktivieren der Integrationen.
2. Um die MITRE ATT&CK-Repository-Daten anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Mitigationen**an.
   Klicken Sie auf eine Minderung, um alle zugehörigen Informationen anzuzeigen.
3. Klicken Sie Auf **Neu** Dient zum manuellen Erstellen der MITRE ATT&CK-Minderungen.
4. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Tools erstellen – Details

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zur Verhinderung eines Angriffs.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.
Name	Geben Sie einen beschreibenden Namen ein, um das Objekt zu identifizieren.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Aliasse	Eine Liste anderer Namen zur Identifizierung dieses Objekts.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Objekt enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Beitragende	Gibt die Beitragenden an.
Einblicke	
Notizen	Alle zusätzlichen Informationen im Zusammenhang mit der Minderung.
Zusätzliche Informationen	
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Objekt hinzu.
Kommentare	Fügen Sie Kommentare für dieses Objekt hinzu.

5. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppen verwalten

Verwalten Sie die Gruppen, die aus den MITRE TAXII-Sammlungen importiert werden. Gruppen sind Sätze zugehöriger Angriffsaktivitäten, die von einem allgemeinen Namen in der Sicherheits-Community nachverfolgt werden. Analysten verfolgen Aktivitätencluster mithilfe verschiedener Begriffe wie Bedrohungsgruppen, Aktivitätsgruppen, Bedrohungsakteure, Angriffssätze und Kampagnen. In STIX werden Gruppen als Angriffssätze bezeichnet.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Um die MITRE ATT&CK-Repository-Daten anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Gruppen**an. Sie können die aufgelisteten Gruppen anzeigen.
2. Klicken Sie Auf **Neu** Zum manuellen Erstellen der MITRE ATT&CK-Gruppen.
3. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Gruppen erstellen – Details

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zur Verhinderung eines Angriffs.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.
Name	Geben Sie einen beschreibenden Namen ein, um das Objekt zu identifizieren.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Aliasse	Eine Liste anderer Namen zur Identifizierung dieses Objekts.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Objekt enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Einblicke	
Notizen	Alle zusätzlichen Informationen im Zusammenhang mit der Minderung.
Zusätzliche Informationen	
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Objekt hinzu.
Kommentare	Fügen Sie Kommentare für dieses Objekt hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Speichern**.
5. Um anzuzeigen, wie diese Objekte zusammenhängen, klicken Sie auf **Beziehungen** .

Malware Verwalten

Verwalten Sie die Malware-Informationen, die Sie aus den MITRE TAXII-Sammlungen importiert haben. Es handelt sich um eine Art von TTP, die schädlichen Code darstellt.

Vorbereitungen

Bezieht sich auf ein Programm, das verdeckt in ein System eingefügt wird. Die Absicht einer Malware besteht darin, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder des Betriebssystems des Opfers zu gefährden.

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Um die MITRE ATT&CK-Repository-Daten anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Gruppen**an. Sie können die aufgelistete Malware anzeigen.
2. Klicken Sie auf eine Malware, um alle zugehörigen Informationen anzuzeigen.
3. Klicken Sie Auf **Neu** Zum manuellen Erstellen der MITRE ATT&CK-Malware.
4. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Malware erstellen – Details

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zur Verhinderung eines Angriffs.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.
Name	Geben Sie einen beschreibenden Namen ein, um das Objekt zu identifizieren.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Aliasse	Eine Liste anderer Namen zur Identifizierung dieses Objekts.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Objekt enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Beitragende	Gibt die Beitragenden an.
Einblicke	
Notizen	Alle zusätzlichen Informationen im Zusammenhang mit der Minderung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zusätzliche Informationen	
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Objekt hinzu.
Kommentare	Fügen Sie Kommentare für dieses Objekt hinzu.

5. Klicken Sie auf **Speichern**.
6. Um anzuzeigen, wie diese Objekte zusammenhängen, klicken Sie auf **Beziehungen** .

Tools Verwalten

Verwalten Sie die Toolinformationen, die Sie aus den MITRE TAXII-Sammlungen importiert haben. Tools sind legitime Software, die von Bedrohungsakteuren zum Ausführen von Angriffen verwendet wird.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Mit Tools können Sie wissen, wie und wann Bedrohungsakteure sie für die Ausführung von Kampagnen verwenden. Im Gegensatz zu Malware werden diese Tools oder Softwarepakete häufig auf einem System gefunden und haben legitime Zwecke für Poweruser, Administratoren, Netzwerkadministratoren oder sogar normale Anwender.

Prozedur
1. Um die MITRE ATT&CK-Repository-Daten anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Tools**an.
   Sie können die aufgeführten Tools anzeigen.
2. Klicken Sie auf ein Tool, um alle zugehörigen Informationen anzuzeigen.
3. Klicken Sie Auf **Neu** Zum manuellen Erstellen der MITRE ATT&CK-Tools.
4. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Tools erstellen – Details

Feld	Beschreibung
ID	Eindeutige ID für eine Vorgehensweise zur Verhinderung eines Angriffs.
Widerrufen	Gibt an, dass die widerrufenen Objekte vom Objektersteller nicht mehr als gültig gelten.
Name	Geben Sie einen beschreibenden Namen ein, um das Objekt zu identifizieren.
Quelle	Gibt die Bedrohungsquelle an, aus der dieser Objektdatensatz erstellt wird.
Aliasse	Eine Liste anderer Namen zur Identifizierung dieses Objekts.
Erstellungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle erstellt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Änderungszeit in Quelle	Gibt die Zeit an, zu der das Objekt in der Quelle geändert wird.
Beschreibung	Eine Beschreibung, die weitere Details und Kontext zum Objekt enthält, möglicherweise einschließlich seines Zwecks und seiner wichtigsten Merkmale.
Beitragende	Gibt die Beitragenden an.
Einblicke	
Notizen	Alle zusätzlichen Informationen im Zusammenhang mit der Minderung.
Zusätzliche Informationen	
Zusätzlicher Kontext	Fügen Sie zusätzlichen Kontext für dieses Objekt hinzu.
Kommentare	Fügen Sie Kommentare für dieses Objekt hinzu.

5. Klicken Sie auf **Speichern**.
6. Um anzuzeigen, wie diese Objekte zusammenhängen, klicken Sie auf **Beziehungen** .

Verwalten Sie MITRE-Beziehungen

Verwalten Sie die MITRE-Beziehungsinformationen, die Sie aus den MITRE TAXII-Sammlungen importiert haben.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.Analyst

Prozedur

1. Um die MITRE ATT&CK-Repository-Daten anzuzeigen, navigieren Sie zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum** > **Threat Intel-Bibliothek** > **MITRE ATT&CK** > **Beziehungen**an.
   Sie können die aufgelisteten Beziehungen anzeigen.
2. Klicken Sie auf ein beliebiges Quellobjekt, um alle zugehörigen Informationen anzuzeigen.
3. Klicken Sie Auf **Neu** Zum manuellen Erstellen der MITRE ATT&CK-Beziehungen.
4. Füllen Sie die Felder entsprechend aus.

Neue MITRE-Tools erstellen – Details

Feld	Beschreibung
MITRE-Quellobjekt	Fügen Sie das MITRE-Quell-Objekt hinzu.
MITRE-Zielobjekt	Fügen Sie das MITRE-Zielobjekt hinzu.
MITRE-Quelltyp	Geben Sie den MITRE-Quelltyp ein.
MITRE-Zieltyp	Geben Sie den MITRE-Zieltyp ein.
Beziehungstyp	Definieren Sie Beziehungen zwischen Objekten. Eine Beschreibung, die weitere Details und Kontext zum Beziehungstyp enthält. Verfügbare Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Definieren Sie die Beziehungsrichtung, ob sie direkt oder umgekehrt ist. ○ Umgekehrt: Dies ist der Typ der Beziehung zwischen dem erkennbaren Element und dem Objekt. ○ Direkt: Dies ist der Typ der Beziehung zwischen dem Objekt und dem erkennbaren Element.
Quelle	Wählen Sie das Quellobjekt aus, und definieren Sie es.
Beziehungs-ID	Definieren Sie die Beziehungs-ID.

5. Klicken Sie auf **Speichern**.
6. Um anzuzeigen, wie diese Objekte zusammenhängen, klicken Sie auf **Beziehungen** .

Datenmigration in TISC

Die Datenmigration ist ein Prozess, bei dem Sie alle Ihre Daten von einer klassischen Anwenderoberfläche nach verschieben TISC.

Der Zweck dieser Migration besteht darin, Anwendern die Daten aus vorhandenen Threat Intelligence-Daten zu migrieren TISC. Zur Ausführung dieses Prozesses wird in ein neues Framework eingeführt TISC Was im weiteren Abschnitt erläutert wird.

Datenmigration von SIR TI nach TISC

Konfiguration des Datenmigrationsauftrags in TISC Ermöglicht Ihnen das Verschieben der vorhandenen Threat Intelligence-Plugin-Daten nach TISC Plugin-Daten direkt.

Vorbereitungen
Erforderliche Rolle: sn_sec_tisc.admin

Warum und wann dieser Vorgang ausgeführt wird

- **Selektive Datensatzmigration** : Nur Datensätze aus der ausgewählten Tabelle, die die angegebenen Bedingungen erfüllen, werden migriert.
- **Beziehungen Einschließen** : Zugehörige Datensätze werden nur migriert, wenn **Beziehungen Einschließen** Das Kontrollkästchen ist aktiviert.
- **Entitätsmigrationsstatus** : Sobald eine Entität (erkennbares Element oder Objekt) migriert wurde, wird sie nicht in weitere Migrationen einbezogen, es sei denn, sie wird als zugehöriger Datensatz migriert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Datensatzausschlusskriterien für das Migrationsdienstprogramm

Das Migrationsdienstprogramm schließt bestimmte Datensätze basierend auf den folgenden Kriterien aus:

- **Erkennbare Elemente** : Erkennbare Elemente vom Typ **Datei** Die sichere Dateianhänge enthalten, werden nicht migriert.
- **Indikatoren** : Indikatoren mit leeren Werten in den Feldern „Muster“ oder „Mustertyp“ werden nicht migriert.
- **Objekte** : Objekte, die aus dem MITRE TAXII-Profil in Threat Intelligence-Daten erfasst werden, werden nicht zum Threat Intelligence-Sicherheitszentrum migriert.

- **Falldatensätze** : Standardmäßig werden nur aktive Datensätze migriert, es sei denn **Schließen Sie Geschlossene Fälle Ein** Das Kontrollkästchen ist aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence-Sicherheitszentrum** > **Konfiguration des Datenmigrationsauftrags**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus.

Konfiguration des Datenmigrationsauftrags

Feld	Beschreibung
Name	Name der Datenmigration.
Tabelle	Wählen Sie die Tabelle aus, aus der die Datensätze migriert werden sollen TISC. Die TISC Tabellenoptionen für die Migration sind: ○ Erkennbares Element (sn_ti_observable) ○ Indikator der Gefährdung (sn_ti_indicator) ○ Sicherheitsfall (sn_ti_Case) ○ STIX V2-Objekte (sn_ti_stix2_object) (Optionen wie Angriffsmuster, Kampagnen, Vorgehensweise)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ○ Wenn Sie die Option STIX V2 auswählen, werden alle STIX-Objekte mit Ausnahme des MITRE ATT&CK migriert, da TISC ein anderes Framework zum Migrieren von MITRE ATT&CK hat. ○ Wenn Sie auswählen, den Sicherheitsfall zu migrieren, werden die geschlossenen Fälle nicht migriert, sondern nur die aktiven Fälle werden migriert. Wählen Sie beispielsweise aus **Erkennbares Element** Migrationstabelle.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, wenn der Datenmigrationsprozess aktiv ist.
Beziehungen einbeziehen	Aktivieren Sie das Kontrollkästchen, um die Beziehungen von Threat Intelligence-Datensätzen zu migrieren TISC Datensätze. **Hinweis:** Wenn Sie dieses Kontrollkästchen aktivieren, werden alle zugehörigen Entitäten zusammen mit dem erkennbaren Element migriert. Wenn das Kontrollkästchen nicht aktiviert ist, wird nur das einzelne erkennbare Element ohne zugehörige Entitäten migriert.
Geschlossene Fälle einbeziehen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die geschlossenen Fälle als Teil der Migration von Falldatensätzen einschließen möchten.
Nur dem Security Incident zugeordnete erkennbare Elemente migrieren	Aktivieren Sie das Kontrollkästchen zum Migrieren der erkennbaren Elemente, die den Security Incidents zugeordnet sind. Wenn das Kontrollkästchen nicht aktiviert ist, werden alle erkennbaren Elemente migriert, unabhängig von ihrer Zuordnung zu Security Incidents.
Bedingungen	Option zum Auswählen der Bedingungen, die zum Filtern der migrierten Daten verwendet werden können.
Zusätzliche Konfigurationen	
Vertrauen	Geben Sie die Konfidenz für die migrierten TISC-Entitäten (erkennbare Elemente oder Objekte oder Indikatoren) ein. Die Konfidenz muss im Bereich von 0-100 liegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ablaufzeitraum (in Tagen)	Der Ablaufzeitraum für migrierte TISC Entitäten.

Hinweis:
Das System ignoriert die Datensätze, die bereits zu migriert wurden, oder überspringt sie TISC Wenn erneut abgerufen.

4. Klicken Sie auf **Absenden**.
5. Klicken Sie Auf **Jetzt Ausführen** Zum Ausführen der Datenmigration.
   Wenn Sie die Datenmigration ausführen, wird ein Hintergrundauftrag ausgeführt, und der Migrationsauftrag wird erstellt. Dieser Auftrag erstellt einen Migrationsprozess, und die Batchgröße dieser Migrationsdatensätze beträgt 5000.
6. Überprüfen Sie den Status des Migrationsauftrags unter **Migrationsauftrag Wird Ausgeführt** Abschnitt.
   Der Auftragsstatus wird in die Warteschlange gestellt, und der maximale Grenzwert für die Batchgröße darf 5000 Datensätze nicht überschreiten. Klicken Sie auf den Datensatz, um die Objekte anzuzeigen, die alle für diese bestimmte Entität migriert wurden.
7. Überprüfen Sie den Status des Migrationsauftrags unter **Migrationsauftrag Wird Ausgeführt** Zugehörige Liste.
8. Klicken Sie auf den Datensatz, um den Verarbeitungsstatus anzuzeigen.
9. Überprüfen Sie den Batch-Migrationsstatus unter **Warteschlange Für Migrationsverarbeitung** Abschnitt der zugehörigen Liste „Datensätze“ im Ausführungsdatensatz des Migrationsauftrags.
   Die Batchgröße für die Migration von Datensätzen beträgt 5000.
10. Überprüfen Sie die TISC-Entitäten, die als Teil der Batch-Migration unter den entsprechenden zugehörigen Listen in erstellt wurden **Warteschlange Für Migrationsverarbeitung** Datensatz.

Funktionaler Flow für TISC-Datenverarbeitung

Das Threat Intelligence Security Center (TISC) bietet eine Lösung, die die Datensammlung und -Verarbeitung automatisiert und dabei hilft, die Belastung für Analysten von Threat Intel zu reduzieren, indem manuelle Schritte vermieden werden.

Threat Intelligence Security Center (TISC) erfasst Intelligenz mit einer der folgenden Methoden:

1. Erfassung aus Datenquellen, die vorkonfiguriert sind und nach einem Zeitplan ausgeführt werden.
2. Threat Intel-Analysten, die Daten mit der Funktion „Intelligence importieren“ importieren.
3. Einzelne Datensätze in der Anwendung werden manuell erstellt.

Hinweis:
Die in der Anwendung erfassten Daten werden verarbeitet, um die Informationen zu normalisieren, zu deduplizieren und zusammenzufassen, bevor sie in die Threat Intel-Bibliothek geladen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

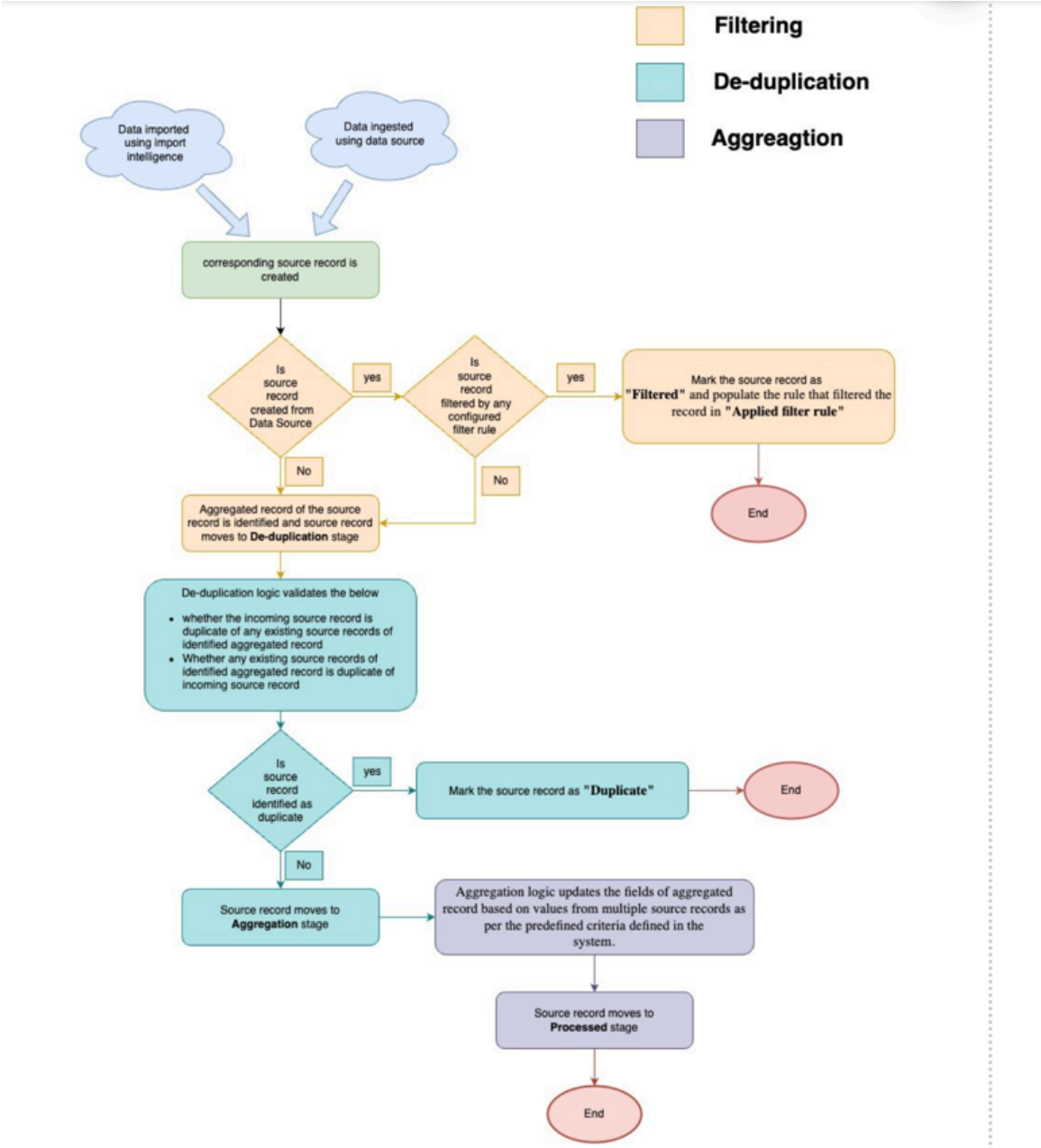
In der Datenverarbeitung verwendete grundlegende Terminologie

1. Quelltabellen : Die Quelltabellen enthalten die Daten im Zusammenhang mit den Entitäten, die aus mehreren Quellen abgerufen werden, und dann werden die Datensätze von jeder Quelle erstellt.
2. Zusammengefasste Datensätze : Die Tabellen der aggregierten Datensätze enthalten die Daten im Zusammenhang mit einer bestimmten Entität, indem die Daten aus allen Quelldatensätzen einer bestimmten Entität zusammengefasst werden.

TISC-Daten-Flow

1. Bei einer erfolgreichen Ausführung des Imports von Intelligenz/Datenquelle werden die Datensätze in den entsprechenden Quelltabellen erstellt.
2. Sobald die Daten in die Quelltabelle gelangen, durchlaufen die Daten die Filterlogik, um zu validieren, ob der Datensatz basierend auf der konfigurierten gefiltert werden soll **Eingehende Filterregeln** . (Betrachten wir SourceRecord1 als Quelldatensatz für unsere Erklärung).
3. Wenn der Datensatz nach einer der konfigurierten Regeln für eingehende Filterung gefiltert wird, wird der entsprechende Quelldatensatz (SourceRecord1) als markiert **Gefiltert** Und-Regel, die den Datensatz gefiltert hat, finden Sie in der angewendeten Filterregel.
4. Nehmen wir an, dass der Quelldatensatz (SourceRecord1) zu AggregateRecord1 aggregiert wird.
5. Wenn der Datensatz nicht gefiltert ist, wird der Datensatz für die Deduplizierung markiert, indem der Verarbeitungsstatus auf „bereit für Deduplizierung“ festgelegt wird.
6. Die Deduplizierungslogik validiert Folgendes:
   a. Gibt an, ob der eingehende Quelldatensatz (SourceRecord1) ein Duplikat vorhandener Quelldatensätze für AggregateRecord1 ist.
   b. Jeder der vorhandenen Quelldatensätze für AggregateRecord1 ist ein Duplikat des eingehenden Quelldatensatzes (SourceRecord1).
7. Jede Entität verfügt über bestimmte Felder und Beziehungen, basierend auf denen der Quelldatensatz auf Duplizierung validiert wird.
8. Wenn der eingehende Quelldatensatz (SourceRecord1) ein Duplikat eines vorhandenen Quelldatensatzes von AggregateRecord1 ist, wird der eingehende Quelldatensatz (SourceRecord1) als Duplikat markiert.
9. Wenn einer der vorhandenen Quelldatensätze (vorhandener Quelldatensatz 1) von AggregateRecord1 als Duplikat des eingehenden Quelldatensatzes (SourceRecord1) identifiziert wird, wird der vorhandene Quelldatensatz (vorhandener Quelldatensatz 1) als Duplikat markiert, und der eingehende Quelldatensatz (SourceRecord1) wird für die Zusammenfassung markiert, indem der Verarbeitungsstatus auf „bereit für Zusammenfassung“ festgelegt wird.
10. Im Rahmen der Zusammenfassung werden Felder des aggregierten Datensatzes „AggregateRecord1“ basierend auf Werten aus mehreren Quelldatensätzen gemäß den im System definierten vordefinierten Kriterien zusammengefasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



TISC Datenarchivierung

Daten wachsen in Tabellen mit zunehmender Akzeptanz der Plattform schnell an. Einige Tabellen befinden sich im Basissystem mit verschiedenen Datenverwaltungsrichtlinien, andere Anwender müssen jedoch selbst implementieren.

Datenverwaltung in TISC

Daten werden in gespeichert und verwaltet TISC Instanz gemäß TISC Bibliotheksobjektstruktur, die Administratoren je nach Bedarf ihrer Organisation anzeigen und konfigurieren können.

Datenarchivierung und -Wiederherstellung ist eine der wichtigsten Funktionen zum Schutz der Datensätze für ihre zukünftige Verwendung. Im folgenden Abschnitt wird beschrieben TISC Archivierungsprozess und Datensatzaufbewahrung als Threat Intelligence Enthält große Mengen von Daten und Datensätzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es gibt eine Reihe verschiedener Methoden, mit denen Anwender ihre Daten in Tabellen verwalten können:

- Archivieren Sie die Daten
- Löschen Sie die Daten

Hinweis:
Wenn die Anwender keine der Methoden anwenden, um ihre Daten effektiv zu verwalten, steigt die Nutzung im Laufe der Zeit, und die Daten werden tendenziell viel größer, was große Auswirkungen auf die Leistung der Anwendungsinstanz und den Speicher hat.

TISC-Datenarchivierung

Die Threat Intelligence-Sicherheitszentrum Wird mit Archivierungsregeln im Basissystem für bereitgestellt TISC Tabelle. Die zugehörigen Datensätze werden auch im Basissystem zu hinzugefügt TISC Archivregel.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivierungsregeln**an.
   Die Liste der Archivierungsregeln, die für gelten TISC Werden angezeigt. Diese Archivierungsregeln unterscheiden sich für jeden Objekttyp und gelten unabhängig voneinander.
2. Filter der Tabellennamen beginnt mit sn_sec_tisc.
3. Zeigen Sie an TISC Zugehörige Datensätze.

Threat Intelligence-Datensatz	Referenztabelle
Angriffsmuster Archivieren	sn_sec_tisc_Attack_pattern
Kampagne Archivieren	sn_sec_tisc_campaign
Archivieren Sie die Vorgehensweise	sn_sec_tisc_Course_of_action
Datenkomponente Archivieren	sn_sec_tisc_aggregated_Data_component
Datenquelle Archivieren	sn_sec_tisc_aggregated_Data_Source
Identität Archivieren	sn_sec_tisc_Identity
Archivieren Sie Die Infrastruktur	sn_sec_tisc_Infrastructure
Archivangriffssatz	sn_sec_tisc_Intrusion_Set
Malware Archivieren	sn_sec_tisc_Malware
Malware-Analyse Archivieren	sn_sec_tisc_Malware_Analysis
Markierungsdefinition Archivieren	sn_sec_tisc_Marking_Definition
Objektsichtung Archivieren	sn_sec_tisc_object_Sighting
Beobachtete Daten Archivieren	sn_sec_tisc_observed_Data
Bedrohungsakteur Archivieren	sn_sec_tisc_Threat_actor
Bedrohungsereignis Archivieren	sn_sec_tisc_Threat_event
Bedrohungsgruppierung Archivieren	sn_sec_tisc_Threat_grouping

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Threat Intelligence-Datensatz	Referenztabelle
Bedrohungshinweis Archivieren	sn_sec_tisc_Threat_note
Bedrohungsmeinung Archivieren	sn_sec_tisc_Threat_opinion
Bedrohungsbericht Archivieren	sn_sec_tisc_Threat_Report
Archivierungstool	sn_sec_tisc_Tool
Schwachstelle Archivieren	sn_sec_tisc_Vulnerability
Artefakt	sn_sec_tisc_Artefakt
AS-Nummer	sn_sec_tisc_AS_number
Verzeichnis	sn_sec_tisc_Directory
E-Mail-Adresse	sn_sec_tisc_email_address
E-Mail-Nachricht	sn_sec_tisc_email_message
E-Mail-Betreff	sn_sec_tisc_email_subject
Datei	sn_sec_tisc_file
Indikatorarchivierungsregel	sn_sec_tisc_indicator
IPv4-Adresse	sn_sec_tisc_ipv4_address
IPv4-CIDR	sn_sec_tisc_ipv4_cidr
IPv6-Adresse	sn_sec_tisc_ipv6_address
Standort	sn_sec_tisc_location
MAC-Adresse	sn_sec_tisc_mac_address
MD5-Hash	sn_sec_tisc_md5_hash
Mutex-Name	sn_sec_tisc_Mutex_Name
Sonstiges erkennbares Element	sn_sec_tisc_Other_Observable
Prozess	sn_sec_tisc_Process
SHA1-Hash	sn_sec_tisc_sha1_hash
SHA256-Hash	sn_sec_tisc_sha256_hash
SHA512-Hash	sn_sec_tisc_sha512_hash
URL	sn_sec_tisc_url
Anwenderaccount	sn_sec_tisc_user_Account
Windows-Registrierungsschlüssel	sn_sec_tisc_Windows_Registry_key
X.509-Zertifikat	sn_sec_tisc_x_509_certificate
Objekt-Objekt-Beziehungsarchivierungsregel	sn_sec_tisc_m2m_object
Archivregel Für Objekt-Erkennbare Beziehung	sn_sec_tisc_m2m_object_observable
Archivregel Für Zugehörigen Indikator	sn_sec_tisc_m2m_indicator
RSS-Feed-Archivregel	sn_sec_tisc_m2m_object_indicator
Importiert Archivregeln	sn_sec_tisc_m2m_indicator_observable

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Informationen zum Erstellen der Archivierungsregeln finden Sie unter Create an archive rule .

4. Wählen Sie eine Archivierungsregel aus.
   Wählen Sie beispielsweise Datensatz des erkennbaren Verzeichnisses aus, um die Archivierungsregel des Basissystems anzuzeigen.
5. Aktualisieren Sie die Regel bei Bedarf.

Archivieren TISC Zugehörige Datensätze

Verwenden Sie die zugehörige Liste zugehörige Datensätze archivieren für TISC Zum Hinzufügen der zugehörigen Datensätze zur Archivregel.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivregeln**an.
2. Filter der Tabellennamen beginnt mit sn_sec_tisc.
3. Wechseln Sie zu **Zugehörige Datensätze Archivieren** Zugehöriger Listenabschnitt zum Anzeigen von TISC Zugehörige Datensätze.

Vernichtungsregeln in TISC

Zeigen Sie die Vernichtungsregeln an, die im Basissystem bereitgestellt werden.

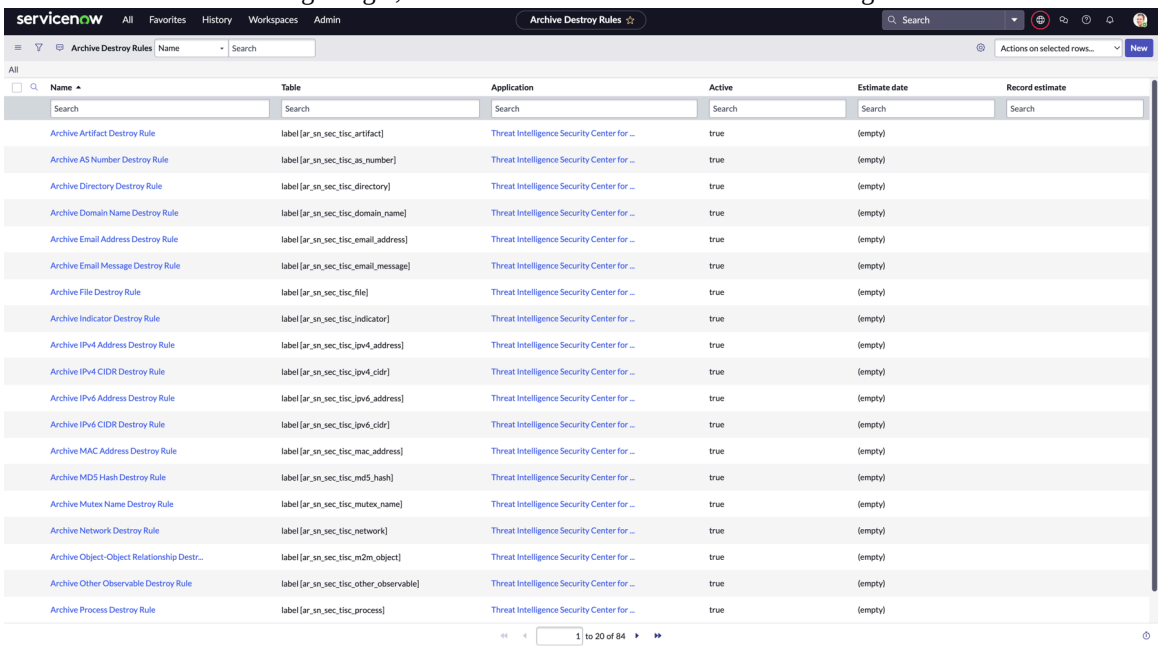
Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivlöschregeln**an.
   Die Liste der Vernichtungsregeln, die für gelten TISC Werden angezeigt. Diese Vernichtungsregeln unterscheiden sich für jeden Objekttyp und gelten unabhängig voneinander.
2. Zeigen Sie die anwendbaren Vernichtungsregeln für an TISC.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf eine beliebige Regel, um den Zeitraum der Archivdauer anzuzeigen.



Löschen Sie Intelligence-Datensätze

Löschen Sie Datensätze aus Threat Intelligence Bibliothek.

Vorbereitungen

Erforderliche Rolle: sn_sec_tisc.admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Threat Intelligence-Sicherheitszentrum**an.
2. Klicken Sie Auf **Threat Intel-Bibliothek** Symbol im Arbeitsbereich.
3. Öffnen Sie einen beliebigen Datensatz.
4. Wechseln Sie zu **Quelldatensätze** Abschnitt.
5. Wählen Sie Aus **Löschen** Zum Löschen der Quelldatensätze.
6. Löschen Sie den Bibliotheksdatensatz.

Hinweis:

a. Wenn ein Bibliotheksdatensatz mit zugeordneten Quelldatensätzen gelöscht wird, werden die Quelldatensätze erneut verarbeitet, und ein neuer Bibliotheksdatensatz wird erstellt, indem die Feldwerte aus den Quelldatensätzen zusammengefasst werden.

b. Um die Daten dauerhaft aus der Threat Intelligence-Bibliothek zu löschen, verwenden Sie Archivierungsregeln, anstatt die Bibliotheksdatensätze zu löschen. Weitere Informationen finden Sie unter TISC Datenarchivierung.

Data Loss Prevention Incident Response

Die Data Loss Prevention Incident Response Mit der Anwendung (DLP IR) können Sie den Korrektur-Workflow von DLP-Incidents aus mehreren Quellen überprüfen und verwalten, z. B. Endpunkt, Netzwerk, E-Mail und Cloud.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Data Loss Prevention Incident Response

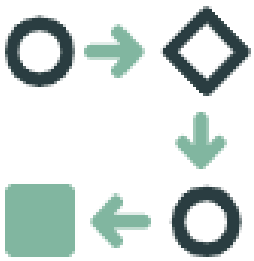
Untersuchen

Erfahren Sie, wie Analysten und Administratoren DLP Incident Response verwenden

Installieren und konfigurieren

Installation und Konfiguration der DLP Incident Response-Anwendung

Verwalten



Administrationsaufgaben zur Verwaltung der DLP-Incidents im ServiceNow AI Platform

Verwenden

Aktualisieren und verwalten Sie Incidents, indem Sie das DLP-Endanwenderportal, das DLP-Ops-Portal und das DLP-Dashboard nutzen.

Integrieren

Erweitern Sie DLP-Fähigkeiten durch Integration mit Drittanbieteranwendungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- Security Operations-Ressourcenbibliothek
- Security Operations-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Data Loss Prevention Incident Response erkunden

Erkunden Data Loss Prevention Incident Response Anwendung, um zu erfahren, wie Sie vertrauliche Informationen für Ihre Kunden verwalten, z. B. finanzielle und proprietäre Daten, Gesundheitsdatensätze oder Sozialversicherungsnummern.

Datenverlust tritt auf, wenn vertrauliche oder vertrauliche Informationen aufgrund nicht autorisierter Kommunikation das Unternehmensnetzwerk verlassen. Mit der DLP-Anwendung können Sie Ihre Datenverlustkanäle identifizieren, reagieren und schützen.

Mithilfe von Data Loss Prevention Incident Response Anwendung hat Ihre Organisation die folgenden wesentlichen Vorteile:

- Integrieren Sie mehrere DLP-Lösungen von Drittanbietern, um einen einheitlichen Überblick über die Incidents in zu erhalten ServiceNow AI Platform.
- Überwachen Sie Incidents, und weisen Sie sie den Endanwendern zu, damit Sie das DLP-Incident-Management optimieren können.
- Coachen Sie Ihre Mitarbeiter durch die anwenderdefinierten E-Mail-Vorlagen und Benachrichtigungen, die für jeden Incident sowie in Form eines Digest gesendet werden.
- Eskalieren Sie die überfälligen DLP-Incidents von den Endanwendern an die Manager.
- Zeigen Sie Zusammenfassungsberichte offener Incidents nach Richtlinie, Schweregrad, häufigsten Tätern usw. an.
- Verfolgen Sie DLP-Incident-Trends, falsch positive Trends und Nachbesserungstrends.

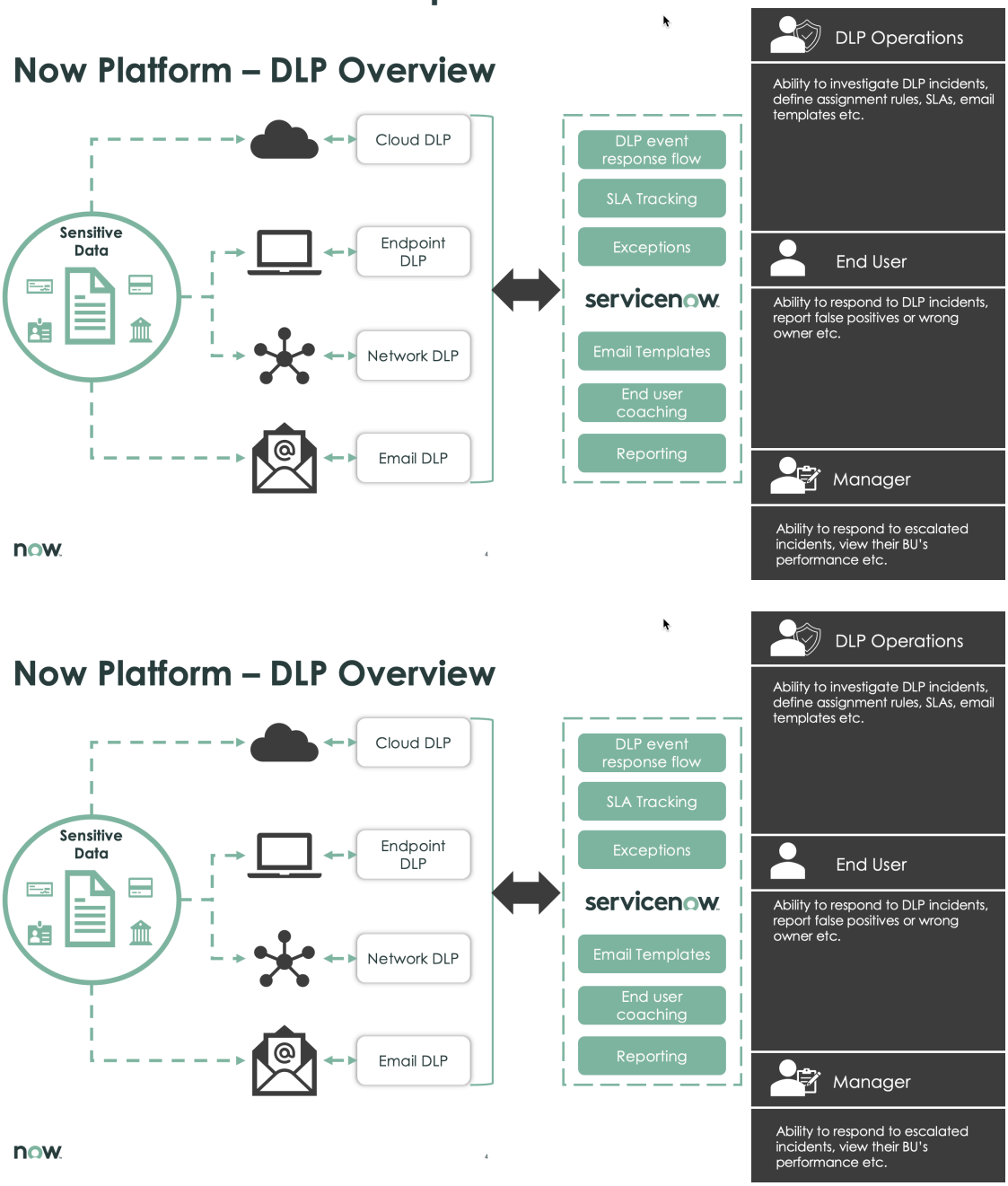
In diesem Abschnitt erfahren Sie mehr über die wichtigsten Funktionen und verschiedenen Rollen, die bei der Arbeit mit DLP-Incidents beteiligt sind.

DLP-Incident-Antwort – Übersicht

Erfahren Sie, wie Sie den verwenden können ServiceNow AI Platform Und Data Loss Prevention Incident Response(DLP IR)-Anwendung. Verwalten Sie vertrauliche Informationen für Ihre Kunden, z. B. finanzielle und proprietäre Daten, Gesundheitsdatensätze oder Sozialversicherungsnummern. Automatisieren Sie die Korrektur-Workflows mit der DLP Incident Response-Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Data Loss Prevention Incident Response Und ServiceNow AI Platform



1. Dies ist ein anklickbares Bild. Sie können also versuchen, auf die verschiedenen Abschnitte zu klicken, um mehr über DLP zu erfahren
2. DLP-Administratoraufgaben: Dies ist ein anklickbares Bild. Sie können also versuchen, auf die verschiedenen Abschnitte zu klicken, um mehr über DLP zu erfahren
3. Verwenden des DLP-Endanwenderportals: Dies ist ein anklickbares Bild, sodass Sie versuchen können, auf die verschiedenen Abschnitte zu klicken, um mehr über DLP zu erfahren
4. DLP-Ops-Portal verwenden: Dies ist ein anklickbares Bild. Sie können also versuchen, auf die verschiedenen Abschnitte zu klicken, um mehr über DLP zu erfahren
5. DLP-Dashboard verwenden: Dies ist ein anklickbares Bild. Sie können also versuchen, auf die verschiedenen Abschnitte zu klicken, um mehr über DLP zu erfahren

Die Data Loss Prevention Incident Response Die Anwendung enthält die folgenden Fähigkeiten:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ein Endanwender-Arbeitsbereich, in dem Ihre Endanwender oder Mitarbeiter die zugewiesenen DLP-Incidents überprüfen und darauf reagieren können.
- Ein Manager-Arbeitsbereich, in dem ein Manager die eskalierten DLP-Incidents überprüfen und entsprechend reagieren kann.
- Ein einheitlicher Arbeitsbereich, in dem Ihr DLP-Betriebsteam die Trends der offenen Incidents, der häufigsten Straftäter und Incidents nach Scan-Quelle nachverfolgen und die DLP-Incidents über mehrere Quellen (Endpunkte, Netzwerke und E-Mail) hinweg anzeigen, bearbeiten, zuweisen und schließen kann.
- Administrative Steuerungen, die die E-Mail-Vorlagen für Endanwender-Coaching und -Kommunikation, Zuweisungsregeln für die automatische Zuweisung von Incidents, automatische Eskalationsregeln und Delegierung für Incident-Antworten definieren.

Erste Schritte mit DLP Incident Response

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihres beginnen Data Loss Prevention Incident Response(DLP IR)-Anwendung.

Prüfliste

Setupaufgabe	Beschreibung
Überprüfen Sie, ob Sie die erforderliche zugewiesen haben ServiceNow AI Platform Und DLP-Rollen.	DLP Incident Response unterstützt die folgenden Rollen: • Der Administrator (Administrator) installiert die -Anwendungen aus dem ServiceNow Store Und weist den DLP-Administrator (sn_dlir.admin) zu. • sn_dlir.admin • sn_dlir.Analyst
Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung von erforderlich sind Data Loss Prevention Incident Response Die Anwendung wird installiert und aktiviert.	Die Data Loss Prevention Incident Response Plugin (com.snc.Data_loss_Incident) ist zur Unterstützung von erforderlich Data Loss Prevention Incident Response Produkt. Überprüfen Sie Folgendes Security Operations Anwendungen werden über installiert und aktiviert ServiceNow Store. Wenn nicht installiert, installieren und aktivieren Sie jeweils eine Anwendung in der folgenden Reihenfolge, um eine reibungslose Installation sicherzustellen: • Reaktion auf Incidents zur Vermeidung von Datenverlust (com.snc.Data_loss_Incident) • Security Support Common Weitere Informationen zum Einrichten von finden Sie ServiceNow AI Platform Instanz für die Integration finden Sie unter Rufen Sie die Berechtigung für ein Security Operations-Produkt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung
	oder eine Anwendung ab Oder Aktivieren Sie eine ServiceNow Store-Anwendung .
Domänentrennung	Verifizieren Sie Domänentrennung und DLP-Incident-Antwort Thema, wenn Sie Daten, Prozesse und Verwaltungsaufgaben trennen möchten.

Installation und Konfiguration DLP IR Incident-Antwort

Laden Sie herunter Data Loss Prevention Incident Response(DLP IR)-Anwendung aus dem ServiceNow Store Und installieren Sie es auf Ihrer Instanz.

Bevor Sie die -Workflows für die -Integration aufrufen, installieren und konfigurieren Sie Data Loss Prevention Incident Response Anwendung aus dem ServiceNow Store Auf Ihrem ServiceNow AI Platform Instanz.

Installieren und konfigurieren Sie die DLP Incident Response-Anwendung

Verwalten Sie vertrauliche Informationen, und automatisieren Sie die Korrektur-Workflows, indem Sie verwenden Data Loss Prevention Incident Response(DLP IR)-Anwendung in Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen

Bevor Sie die Konfigurationsschritte abschließen können, müssen Sie die Anwendung aus dem herunterladen ServiceNow Store Und installieren Sie es auf Ihrer Instanz.

Erforderliche Rollen: admin und sn_dlir.admin

Prozedur

1. Befolgen Sie die Anweisungen für Lädt eine Anwendung aus dem ServiceNow Store herunter .
2. Nachdem Sie heruntergeladen haben **DLP-Incident-Antwort** Navigieren Sie zu Anwendung und allen zugehörigen Abhängigkeitsanwendungen **Alle** > **DLP-Administration** > **Standardkonfiguration** Um den Rest von abzuschließen Anwendungskonfiguration .

Domänentrennung und DLP-Incident-Antwort

Sie können die Domänentrennung mit DLP Incident Response verwenden, um die Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen zu trennen, die als Domänen bezeichnet werden. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Support-Stufe: Standard

- Enthält alle Aspekte von **Standard** Level-Support.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Funktionsweise der Domänentrennung mit DLP Incident Response

- Erstellen Sie einen Anwender mit den erforderlichen Rollen sn_dlir.admin und sn_dlir.Analyst in der jeweiligen Domäne.
- Führen Sie die DLP-Incident-Response-Konfigurationen in der entsprechenden Domäne durch.

Verwaltung der DLP-Incident-Reaktion

Sie können Regeln einrichten und zuweisen, Fälligkeitsdatumsregeln konfigurieren, E-Mail-Vorlagen verwenden, Endanwenderantwortaktionen konfigurieren und vieles mehr, um zu verwalten Data Loss Prevention Incident Response(DLP IR) Incidents auf dem ServiceNow AI Platform.

Die Data Loss Prevention Incident Response Mit der Anwendung können Sie die folgenden Konfigurationen ausführen.

DLP-Standardkonfigurationseinstellungen

Definieren Sie die Standardkonfigurationseinstellungen für Data Loss Prevention Incident Response(DLP IR) Incidents zum Identifizieren und Einrichten der Einstellungen für Incident-Benachrichtigungen und Incident-Zuweisungen für Endanwender.

Vorbereitungen
Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird
Sie können dieses Modul verwenden, um die Standardkonfigurationseinstellungen zu definieren, wenn die Core-Zuweisungsregeln und Bezeichnerregeln erschöpft sind und nicht mit einer Bedingung oder einem Anwender übereinstimmen können. Sie können auch Suchregeln und Zuweisungsregeln für Endanwender definieren und erneut auf vorhandene aktive DLP-Incidents anwenden.

Mit der Incident-Benachrichtigung für Endanwender können Sie die Häufigkeit angeben, mit der E-Mail-Benachrichtigungen an Endanwender gesendet werden. Sie können beispielsweise Benachrichtigungseinstellungen einrichten, um Incidents zu akkumulieren und einmal pro Woche einen E-Mail-Digest zu senden. Indem Sie einen Incident zuweisen, können Sie angeben, welcher Gruppe Sie die DLP-Incidents anfänglich zuweisen. Sie können auch angeben, wie die Endanwender vom DLP-Betriebsteam weiter identifiziert werden.

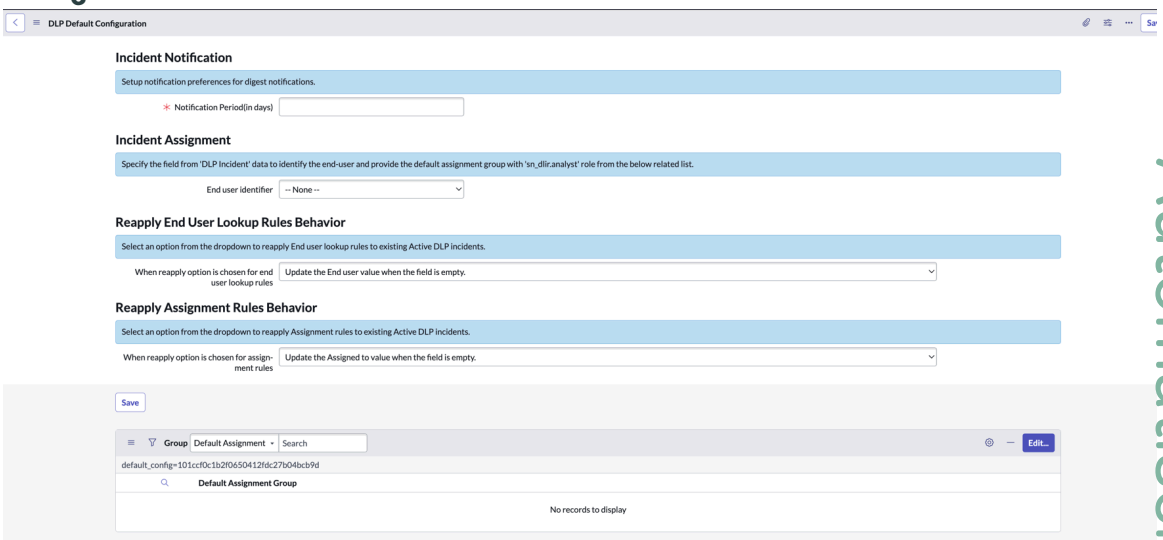
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Angenommen, ein Anwender hat Kreditkarteninformationen in einer Datei in einem Netzwerk gespeichert. Wenn das DLP-Integrationsprodukt einer Drittpartei einen Incident für einen Verstoß gegen die Richtlinie zu vertraulichen Daten erstellt, die Incident-Daten, die von erstellt werden ServiceNow AI Platform DLP-Erfassungen enthalten Informationen zum Endanwender. Sie können den Incident dann dem rechten Endanwender zuweisen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Standardkonfiguration**an.

Konfigurieren Sie DLP-Richtlinien



2. Füllen Sie im Formular die Felder aus.

Formular „DLP-Standardkonfiguration“

Konfigurationsname	Feld	Beschreibung
Endanwender-Incident-Benachrichtigung	Benachrichtigungszeitraum (Tage)	Definieren Sie die Anzahl der Tage, nach denen eine E-Mail-Benachrichtigung an den Endanwender gesendet werden soll. Die Anzahl der Tage muss zwischen 1 und 60 Tagen liegen.
	Übergeordneten Status automatisch basierend auf geklonten/untergeordneten Incidents aktualisieren	Option zum automatischen Aktualisieren des übergeordneten Status-Incidents basierend auf den geklonten oder untergeordneten Incidents.
Incident-Zuweisung	Endanwenderbezeichner	Geben Sie das Feld an, das aus Incident-Daten verwendet werden soll, um den Endanwender zu identifizieren. Mögliche Werte sind die folgenden: ○ **E-Mail des Datenbesitzers** ○ **Ziel** ○ **Datei erstellt von** ○ **Datei geändert von** ○ **Dateibesitzer**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsname	Feld	Beschreibung
		○ **FTP-Anwendername** ○ **Absender**
Verhalten der Endanwender-Suchregeln erneut anwenden	Wenn die Option „Erneut anwenden“ für Suchregeln für Endanwender ausgewählt ist	Option zum erneuten Anwenden von Endanwendersuchregeln auf vorhandene aktive DLP-Incidents. Sie können eine der folgenden Optionen zum erneuten Anwenden auswählen: ○ **Aktualisieren Sie den Endanwenderwert, wenn das Feld leer ist** : Aktualisiert den Endanwenderwert der vorhandenen aktiven DLP-Incidents, wenn dieses Feld leer ist. ○ **Aktualisieren Sie den Endanwenderwert** : Aktualisiert den Endanwenderwert der vorhandenen aktiven DLP-Incidents. ○ **Aktualisieren Sie die Werte Endanwender und Zugewiesen an, wenn beide Felder leer sind** : Aktualisiert den Endanwender der vorhandenen aktiven DLP-Incidents und die Werte „Zugewiesen an“, wenn beide Felder leer sind. **Hinweis:** Wenn diese Option ausgewählt ist, wird **Aktualisieren Sie den Wert „Zugewiesen an“, wenn das Feld leer ist** Die Option wird im Abschnitt „Zuweisungsregeln erneut anwenden“ automatisch deaktiviert, da sie für beide gilt. ○ **Aktualisieren Sie die Werte Endanwender und Zugewiesen an für alle aktiven DLP-Incidents** : Aktualisiert die Werte für Endanwender und Zugewiesen an für alle aktiven DLP-Incidents. **Hinweis:** Wenn diese Option ausgewählt ist, wird **Aktualisieren Sie den Wert Zugewiesen an für alle aktiven DLP-Incidents** Die Option wird im Abschnitt „Zuweisungsregeln erneut anwenden“ automatisch deaktiviert, da sie für beide gilt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsname	Feld	Beschreibung
Verhalten von Zuweisungsregeln erneut anwenden	Wenn die Option „Erneut anwenden“ für Zuweisungsregeln ausgewählt ist	Option zum erneuten Anwenden von Zuweisungsregeln auf vorhandene aktive DLP-Incidents. Sie können eine der folgenden Optionen zum erneuten Anwenden auswählen: ○ **Aktualisieren Sie den Wert „Zugewiesen an“, wenn das Feld leer ist.** ○ **Aktualisieren Sie den Wert Zugewiesen an für alle aktiven DLP-Incidents.**

3. Wählen Sie aus **Standardmäßige Zuweisungsgruppe** Aus dem Abschnitt der zugehörigen Liste, in dem alle DLP-Incidents zugewiesen sind.
   Klicken Sie Auf **Bearbeiten** Um die Anwendergruppe hinzuzufügen. Wenn Sie auf klicken **Bearbeiten** Wählen Sie im Abschnitt „zugehörige Liste“ ein Element aus **Sammlungen** Spalten und fügen Sie dann den ausgewählten Beauftragten den Gruppenspalten in hinzu **Bearbeiten Sie Mitglieder** Seite, und speichern Sie die Liste.

   Hinweis:
   Sie können nur Gruppen anzeigen und auswählen, denen die Rolle „sn_dlir.Analyst“ aus der zugehörigen Liste zugewiesen wurde. Sie können nur eine Gruppe auswählen.

4. Klicken Sie auf **Speichern**.

Erstellen Sie Suchregeln für Endanwender

Sie können Suchregeln für Endanwender erstellen und konfigurieren und die DLP-Incidents den jeweiligen Endanwendern basierend auf diesen Regeln zuweisen.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Der DLP-Administrator definiert diese Endanwendersuchregeln, um die Endanwender automatisch DLP-Incidents zuzuweisen, wobei nur das Endanwenderfeld verwendet wird. Mit der DLP-Endanwendersuchregel können Sie dem Endanwender DLP-Incidents basierend auf Endanwenderbezeichner, anwenderdefinierten Attributen oder Skript zuweisen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **DLP-Endanwender-Suchregeln**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „DLP-Endanwender-Suchregel“

Feld	Beschreibung
Name	Name für die Endanwender-Suchregel.
Aktiv	Option, um anzugeben, ob die Suchregel für Endanwender aktiv ist.
Ausführungsreihenfolge	Die Priorität der Endanwender-Suchregel. Dieses Feld gibt die Reihenfolge an, in der die Suchregeln des Endanwenders ausgeführt werden, wenn zwei oder mehr Regeln die auslösenden Bedingungen gemeinsam haben. Die Suchregel für Endanwender mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Beispiel: 100, 200, 300 usw. Der Standardwert ist 100.
Beschreibung	Eindeutige Beschreibung für die Endanwender-Suchregel.
Bedingung	Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Endanwender-Suchregel zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER** . ○ Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien** . Sie können beispielsweise die Bedingungen für diese Endanwender-Suchregel festlegen, indem Sie die Bedingung als auswählen **Integrationsquelle** , **Enthält** , **Symantec** . **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

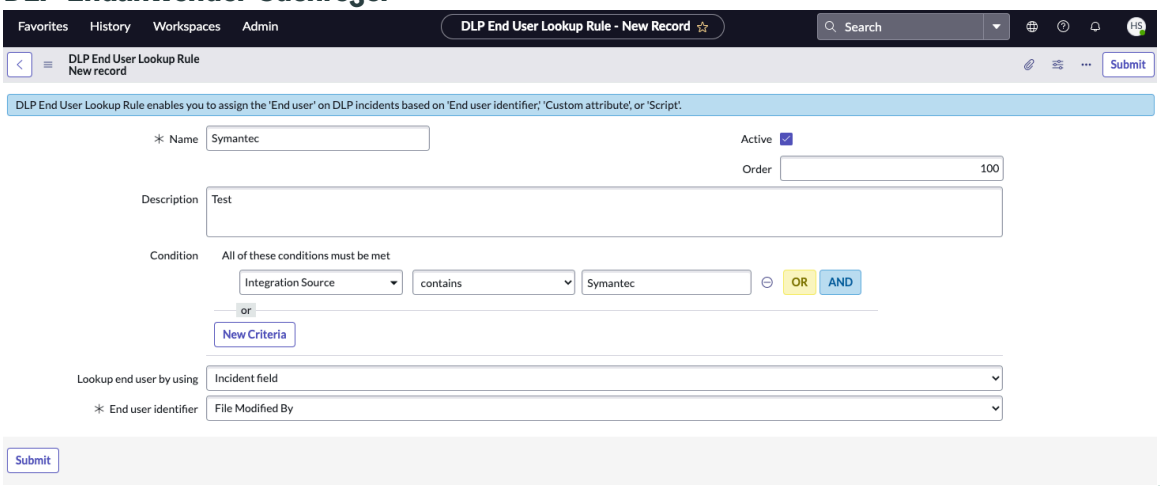
Feld	Beschreibung
Endanwender suchen mithilfe von	Option zum Suchen von Endanwendern mithilfe von **Incident-Feld** Oder **Skript** .
Endanwenderbezeichner	Der Endanwender-Bezeichner des DLP-Incidents. Dieses Feld wird angezeigt, wenn **Incident-Feld** Ist aus ausgewählt **Suchen Sie mit Endanwender** Feld. Sie können einen Endanwenderbezeichner aus den folgenden Optionen auswählen: ○ **E-Mail des Datenbesitzers** ○ **Ziel** ○ **Datei erstellt von** ○ **Datei geändert von** ○ **Dateibesitzer** ○ **FTP-Anwendername** ○ **Absender** **Hinweis:** Die oben aufgeführten Endanwenderbezeichner können mithilfe der Systemeigenschaft konfiguriert werden `sn_dlir.assignment.fields` . Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren. ○ **Anwenderdefinierter Anwender aus Incident**
Anwenderdefiniertes Attribut	Option zum Angeben eines anwenderdefinierten Attributs aus dem Incident, das den Verweis auf einen Anwender hat. Dieses Feld wird nur angezeigt, wenn **Das A** Ist aus ausgewählt **Endanwenderbezeichner** Feld.
Skript	Sie können den Skripteditor verwenden, um die Feldwerte während der Erstellung der Endanwender-Suchregel anzupassen und zu formatieren. Sie können beispielsweise das Feld „E-Mail-Adresse“ verwenden, um den Endanwender zu identifizieren.

Example

Das folgende Beispiel zeigt eine Endanwender-Suchregel mit dem Namen „Symantec“. Der Bedingungsgenerator erfordert „Integrationsquelle“ als „Symantec“. Die **Suchen Sie mit Endanwender** Option ist auf „Incident-Feld“ und festgelegt **Endanwenderbezeichner** Option ist auf „Datei geändert von“ festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DLP-Endanwender-Suchregel



4. Klicken Sie auf **Absenden**.
   Sie haben auch die Möglichkeit, eine oder mehrere Endanwendersuchregeln auszuwählen und sie auf alle vorhandenen DLP-Incidents erneut anzuwenden.
5. Um eine Endanwender-Suchregel auf alle vorhandenen DLP-Incidents erneut anzuwenden, klicken Sie auf **Erneut Anwenden** .

Erstellen Sie Zuweisungsregeln

Verwenden Sie diesen Abschnitt, um Zuweisungsregeln zu erstellen. Weisen Sie dann zu Data Loss Prevention Incident Response(DLP IR) Incidents für Anwendergruppen, Endanwender, Manager oder Anwender aus Incident.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Sie können Zuweisungsregeln verwenden, um Anwendergruppen, Endanwendern oder Managern DLP-IR-Incidents zuzuweisen. Die Zuweisung der DLP-Incidents erfolgt, wenn die Bedingungen in der Zuweisungsregel erfüllt sind.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Zuweisungsregeln**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „DLP-Zuweisungsregel“

Feld	Beschreibung
Name	Name für die Zuweisungsregel.
Aktiv	Option, um anzugeben, ob die Zuweisungsregel aktiv ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ausführungsreihenfolge	Die Zuweisungsregelpriorität. Dieses Feld gibt die Reihenfolge an, in der die Zuweisungsregeln ausgeführt werden, wenn zwei oder mehr Regeln die auslösenden Bedingungen gemeinsam haben. Die Zuweisungsregel mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Beispiel: 100, 200, 300 usw. Der Standardwert ist 100.
Beschreibung	Eindeutige Beschreibung für diese Zuweisungsregel.
Bedingung	Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Zuweisungsregel zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER**. ○ Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. Angenommen, Sie erstellen eine DLP-Zuweisungsregel für einen Endpunkt. Sie können angeben, dass die Bedingungsscanquelle ein Endpunkt-Dateisystem ist, das vor dem Zuweisen eines Incident erfüllt werden muss. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Zuweisen an	Zuweisung zu einer der folgenden Elemente: ○ Anwendergruppe ○ Endanwender ○ Manager ○ Anwender aus Incident Die Zuweisung erfolgt, wenn die Bedingungen im Bedingungsgenerator erfüllt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwendergruppe	Option zum Suchen und Auswählen einer Anwendergruppe, der die DLP-Incidents zugewiesen werden sollen. Dieses Feld wird angezeigt, wenn **Anwendergruppe** Ist aus ausgewählt **Zuweisen an** Feld. **Hinweis:** Sie können nur Gruppen anzeigen und auswählen, denen die Rolle „sn_dlir.Analyst“ zugewiesen wurde.
Endanwender	Option zum Zuweisen des DLP-Incidents an den Endanwender. Die Zuweisung erfolgt, wenn die Bedingungen im Bedingungsgenerator erfüllt sind.
Zuweisen mithilfe von Manager-Feldern	Manager des Endanwenders. Dieses Feld wird angezeigt, wenn **Manager** Ist aus ausgewählt **Zuweisen an** Feld. Sie können die DLP-Incidents einem bestimmten Manager zuweisen, indem Sie eines der Manager-Felder auswählen, z. B. Nachname, E-Mail-Adresse, Stadt, Mitarbeiternummer.
Anwenderbezeichner	Der Anwenderbezeichner des Incident. Dieses Feld wird angezeigt, wenn **Anwender aus Incident** Ist aus ausgewählt **Zuweisen an** Feld. Sie können einen Anwenderbezeichner aus den folgenden Optionen auswählen: ○ **E-Mail des Datenbesitzers** ○ **Ziel** ○ **Datei erstellt von** ○ **Datei geändert von** ○ **Dateibesitzer** ○ **FTP-Anwendername** ○ **Absender** ○ **Anwenderdefinierter Anwender aus Incident**
Anwenderdefiniertes Attribut	Option zum Angeben eines anwenderdefinierten Attributs aus dem Incident, das den Verweis auf einen Anwender hat. Dieses Feld wird nur angezeigt, wenn **Anwenderdefinierter Anwender aus Incident** Ist aus ausgewählt **Anwenderbezeichner** Feld.
Bewertung anhängen	Option, um anzugeben, ob Sie dem Incident eine Bewertung anhängen möchten.
Antwortstatus vor der Bewertung	Option zum Auswählen des Status, in dem sich der Incident befinden soll, bevor der Endanwender

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

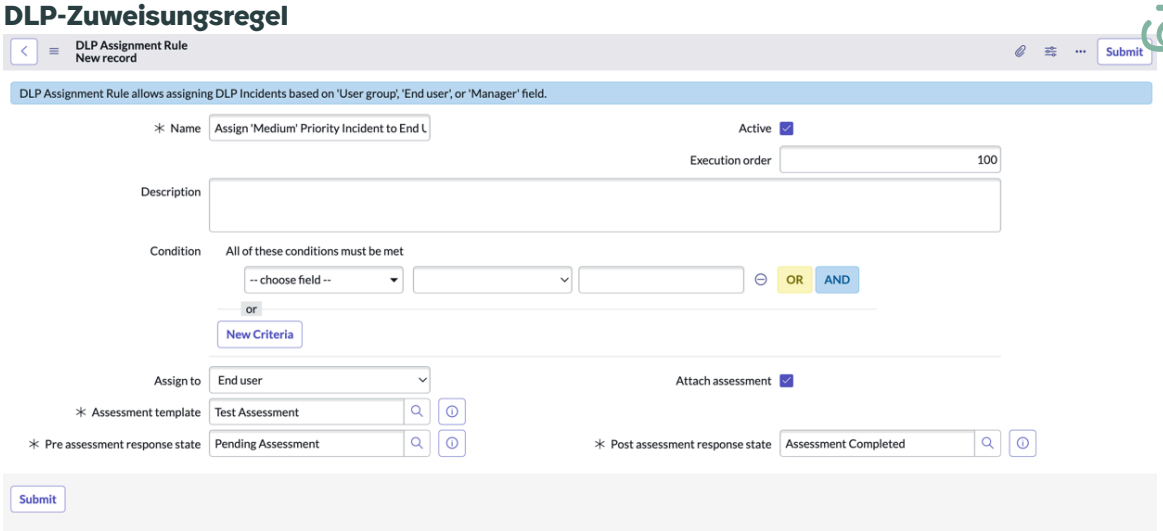
Feld	Beschreibung
	antwortet. Es kann auch ein anwenderdefinierter Status sein. Der Standardwert ist „Bewertung ausstehend“.
Antwortstatus nach der Bewertung	Option zum Auswählen des Status, in dem sich der DLP-Incident befinden soll, nachdem der Anwender geantwortet hat. Der Standardwert ist „Bewertung abgeschlossen“.
Erweitert	Erweiterte Option zur Identifizierung des Endanwenders. Dieses Feld wird nur angezeigt, wenn **Anwenderdefinierter Anwender aus Incident** Ist aus ausgewählt **Anwenderbezeichner** Feld. Sie können den Skript-Editor verwenden, um die Feldwerte während der Erstellung der Zuweisungsregel anzupassen und zu formatieren, um den Endanwender zu identifizieren. Dann wählen Sie aus, wem Sie den DLP-Incident zuweisen möchten, z. B. ein Endanwender oder der Manager des Endanwenders. Sie können beispielsweise das Feld „E-Mail-Adresse“ verwenden, um den Endanwender zu identifizieren.

Automatische Übersetzung

Example

Das folgende Beispiel zeigt eine Zuweisungsregel mit dem Namen Weisen Sie dem Endanwender einen Incident mit Priorität „Mittel“ zu . Der Bedingungsgenerator erfordert, dass die Scan-Quelle ist Weisen Sie dem Endanwender einen Incident mit Priorität „Mittel“ zu , Und Zuweisen an Feld ist auf festgelegt Endanwender . Anschließend können Sie nach der E-Mail-Adresse des Endanwenders suchen.

DLP-Zuweisungsregel



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie aus **Zuweisen an** Feld aus dem Abschnitt der zugehörigen Liste, dem alle DLP-Incidents zugewiesen sind.
   Klicken Sie Auf **Bearbeiten** Um die Anwendergruppe hinzuzufügen. Wenn Sie auf klicken **Bearbeiten** Wählen Sie im Abschnitt „zugehörige Liste“ ein Element aus **Sammlungen** Spalten und fügen Sie dann den ausgewählten Beauftragten den Gruppenspalten in hinzu **Bearbeiten Sie Mitglieder** Seite, und speichern Sie die Liste.

   Hinweis:
   Sie können nur Gruppen anzeigen und auswählen, denen die Rolle „sn_dlir.Analyst“ aus der zugehörigen Liste zugewiesen wurde. Sie können nur eine Gruppe auswählen.

5. Klicken Sie auf **Absenden**.
   Sie haben auch die Möglichkeit, eine oder mehrere Zuweisungsregeln auszuwählen und auf alle vorhandenen DLP-Incidents erneut anzuwenden.
6. Um eine Zuweisungsregel erneut auf alle vorhandenen DLP-Incidents anzuwenden, klicken Sie auf **Erneut Anwenden** .

Erstellen Sie Incident-Konsolidierungsregeln

Erstellen Sie eine Incident-Konsolidierungsregel, um mehrere Incidents ähnlicher Art unter einem übergeordneten Incident zu konsolidieren.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt)

Warum und wann dieser Vorgang ausgeführt wird

Der DLP-Administrator definiert diese Incident-Konsolidierungsregeln, um DLP-Incidents derselben Art automatisch unter einem übergeordneten Incident zu konsolidieren. Mit der DLP-Incident-Konsolidierungsregel können Sie DLP-Incidents basierend auf der Konfiguration konsolidieren, die für die Konsolidierungsdauer und die Konsolidierungsidentifizierung bereitgestellt wird.

Hinweis:

Wenn ein konsolidierter Incident erstellt wird, wird er dem übergeordneten DLP-Incident untergeordnet. Wenn der Schweregrad des konsolidierten Incident höher ist als der des übergeordneten Incident, wird der Schweregrad des übergeordneten Incidents so aktualisiert, dass er mit dem untergeordneten Incident übereinstimmt.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Konsolidierungsregeln für DLP-Incidents**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „DLP-Zuweisungsregel“

Feld	Beschreibung
Name	Name für die Incident-Konsolidierungsregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Option, um anzugeben, ob die Incident-Konsolidierungsregel aktiv ist.
Ausführungsreihenfolge	Die Priorität der Incident-Konsolidierungsregel. Dieses Feld gibt die Reihenfolge an, in der die Incident-Konsolidierungsregeln ausgeführt werden, wenn zwei oder mehr Regeln die auslösenden Bedingungen gemeinsam haben. Die Incident-Konsolidierungsregel mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Beispiel: 100, 200, 300 usw. Der Standardwert ist 100.
Beschreibung	Eindeutige Beschreibung für die Incident-Konsolidierungsregel.
Bedingung	Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Incident-Konsolidierungsregel zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER** . ○ Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien** . Sie können beispielsweise die Bedingungen für diese Incident-Konsolidierungsregel festlegen, indem Sie die Bedingung als auswählen **Integrationsquelle** , **Enthält** , **Symantec** . **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Konsolidierungsdauer	Option zum Festlegen der Dauer für die Incident-Konsolidierung. Incidents in diesem Zeitraum mit denselben Werten für die ausgewählten Felder werden unter dem ersten Incident konsolidiert. Der erste Incident, der dieser Regel entspricht, ist der übergeordnete Incident, und der Rest der Incidents sind untergeordnete Incidents.
Incidents konsolidieren nach	Wählen Sie das Feld „DLP-Incident“ aus, um die Incidents zu konsolidieren, wenn im Feld „ausgewählt“ für verschiedene Incidents der gleiche Wert vorhanden ist. Wählen Sie mindestens ein Feld aus. Wählen Sie mindestens ein Feld aus.

Das folgende Beispiel zeigt eine Incident-Konsolidierungsregel mit dem Namen Incidents für Symantec-Integration konsolidieren. Der Bedingungsgenerator erfordert die Integrationsquelle Symantec. Die **Bedingungsdauer** Option ist auf 1 Stunde festgelegt, und die Option Richtlinienname ist für ausgewählt **Incident konsolidieren bis** .

Zum Zeitpunkt der Symantec DLP-Incident-Erfassung wird diese Regel ausgeführt, und wenn mehrere Incidents denselben Richtliniennamen haben, wird der Incident unter dem ersten erfassten Incident konsolidiert, der dieser Regel entspricht.

4. Klicken Sie auf **Absenden**.
   Incidents, die basierend auf der Konsolidierungsregel konsolidiert wurden, sind unter der Liste untergeordnete Incidents im DLP-Arbeitsbereich verfügbar.

Erstellen Sie Regeln für das Fälligkeitsdatum der Antwort

Richten Sie die Regeln für das Fälligkeitsdatum der Antwort ein, um zu bestimmen, wann Sie Ihren Endanwendern geben möchten, um auf die zugewiesenen zu antworten Data Loss Prevention Incident Response(DLP IR) Incidents.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Sie können dieses Modul verwenden, um die Regeln für das Fälligkeitsdatum der Antwort für die verschiedenen Typen von DLP-Incidents und die Regeln für den Start der Zählung des Fälligkeitsdatums zu definieren. Nachdem das Fälligkeitsdatum abgelaufen ist, werden die Anwender über den überfälligen Incident benachrichtigt. Sie haben auch die Möglichkeit, den überfälligen Incident an einen der folgenden Personen zu eskalieren:

- Manager
- Anwenderdefinierter Anwender aus Incident
- Anwendergruppe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Wenn Sie den überfälligen Incident an einen Manager eskalieren und maximal drei Eskalationsstufen angegeben haben. Die erste Managerebene wird zuerst benachrichtigt. Wenn der Incident erneut überfällig ist, wird die zweite Managerebene benachrichtigt, gefolgt von der dritten Ebene, wenn der Incident noch überfällig ist. Wenn der Manager einen Delegierten hat, hat der Manager die Möglichkeit, dem Delegierten den Eskalations- oder überfälligen Incident zuzuweisen.

Sie haben auch die Möglichkeit, mehrere Regeln für das Fälligkeitsdatum von Antworten zu erstellen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Regeln für Fälligkeitsdatum der Antwort**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „Regel für Fälligkeitsdatum der Antwort“

Feld	Beschreibung
Name	Name der Regel für das Fälligkeitsdatum der Antwort.
Aktiv	Option, um anzugeben, ob die Regel für das Fälligkeitsdatum der Antwort aktiv ist.
Fällig in (Tagen)	Anzahl der Fälligkeitstage.
Fälligkeitsdatum gezählt von	Startdatum, das zur Berechnung des Fälligkeitsdatums verwendet wird. Das Fälligkeitsdatum kann entweder vom ersten Zeitpunkt der Benachrichtigung des Anwenders über den Incident oder vom Zuweisungsdatum des Incidents berechnet werden.
Vor dem Fälligkeitsdatum benachrichtigen	Option, den Endanwender vor dem Fälligkeitsdatum über den DLP-Incident zu benachrichtigen.
Benachrichtigen am (Tage vor Fälligkeitsdatum)	Anzahl der Tage vor dem Fälligkeitsdatum, in denen die Regel eine Benachrichtigung an den Endanwender auslöst.
Beschreibung	Eindeutige Beschreibung für diese Regel für das Fälligkeitsdatum der Antwort.
Bedingung	Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Regel für das Fälligkeitsdatum der Antwort zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien** . **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Eskalation	Option, den DLP-Incident an jemanden zu eskalieren, wenn das Fälligkeitsdatum der Antwort verletzt wurde. Weitere Informationen finden Sie unter Fügen Sie mehrere Anwender hinzu, um auf DLP-Incidents zuzugreifen
Überfälligen Incident eskalieren an	Option zum Festlegen, ob der Incident an einen Manager, einen anwenderdefinierten Anwender oder eine Anwendergruppe eskaliert werden soll. Dieses Feld wird nur angezeigt, wenn **Eskalieren** Option ist aktiviert.
Zuweisen mit	Geben Sie an, wie ein Manager identifiziert werden soll. Dieses Feld wird nur angezeigt, wenn **Manager** Ist aus ausgewählt **Eskalieren Sie überfälligen Incident an** Feld.
Maximale Eskalationsebenen	Option zum Definieren der maximalen Anzahl von Eskalationsebenen für einen Manager und einen anwenderdefinierten Anwender. Als Manager oder anwenderdefinierter Anwender können Sie eine beliebige Anzahl von Eskalationsebenen definieren. Standardmäßig werden drei Eskalationsstufen bereitgestellt. ○ Als Manager können Sie eine beliebige Anzahl von Eskalationsebenen definieren, indem Sie den Wert in diesem Feld aktualisieren. ○ Als anwenderdefinierter Anwender können Sie das +-Symbol verwenden, um eine beliebige Anzahl von Eskalationsebenen zu definieren.
Anwenderdefiniertes Attribut	Option zum Angeben eines anwenderdefinierten Attributs aus dem Incident, das den Verweis auf einen Anwender hat.

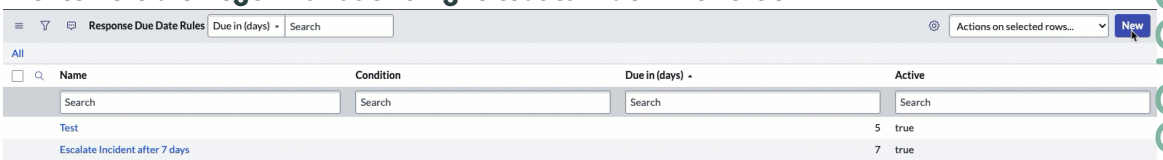
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dieses Feld wird nur angezeigt, wenn **Anwenderdefinierter Anwender aus Incident** Ist aus ausgewählt **Eskalieren Sie überfälligen Incident an** Feld.
Anwendergruppe	Option zum Suchen und Auswählen einer Anwendergruppe, an die DLP-Incidents eskaliert werden sollen. Dieses Feld wird nur angezeigt, wenn **Anwendergruppe** Ist aus ausgewählt **Eskalieren Sie überfälligen Incident an** Feld. **Hinweis:** Sie können nur Gruppen anzeigen und auswählen, denen die Rolle „sn_dlir.Analyst“ zugewiesen wurde.

Example

Das folgende Beispiel zeigt die Regel für das Fälligkeitsdatum der Antwort, um zu bestimmen, wie viel Zeit Sie Ihren Endanwendern geben möchten, um auf die zugewiesene zu antworten Data Loss Prevention Incident Response(DLP) Incidents. Nachdem der Endanwender erstmals benachrichtigt wurde, liegt das Fälligkeitsdatum der Antwort in zwei Tagen. Der Bedingungsgenerator zeigt an, dass die Scanquelle mit dem Endpunktdateisystem übereinstimmen muss, um mit der Erstellung des Fälligkeitsdatums der Antwort fortzufahren. Die Eskalationsoption ist ausgewählt. Der Incident wird an den Manager eskaliert, wenn das Fälligkeitsdatum der Antwort verletzt wird.

Richten Sie die Regeln für das Fälligkeitsdatum der Antwort ein



4. Klicken Sie auf **Absenden**.

Fügen Sie mehrere Anwender hinzu, um auf DLP-Incidents zuzugreifen

Verwenden Sie die Funktion „Eskalationskette“, damit alle jeweiligen Anwender, die an dem Incident beteiligt sind, über die Listenansicht auf die DLP-Incidents zugreifen können, obwohl der Incident einem anderen Anwender zugewiesen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

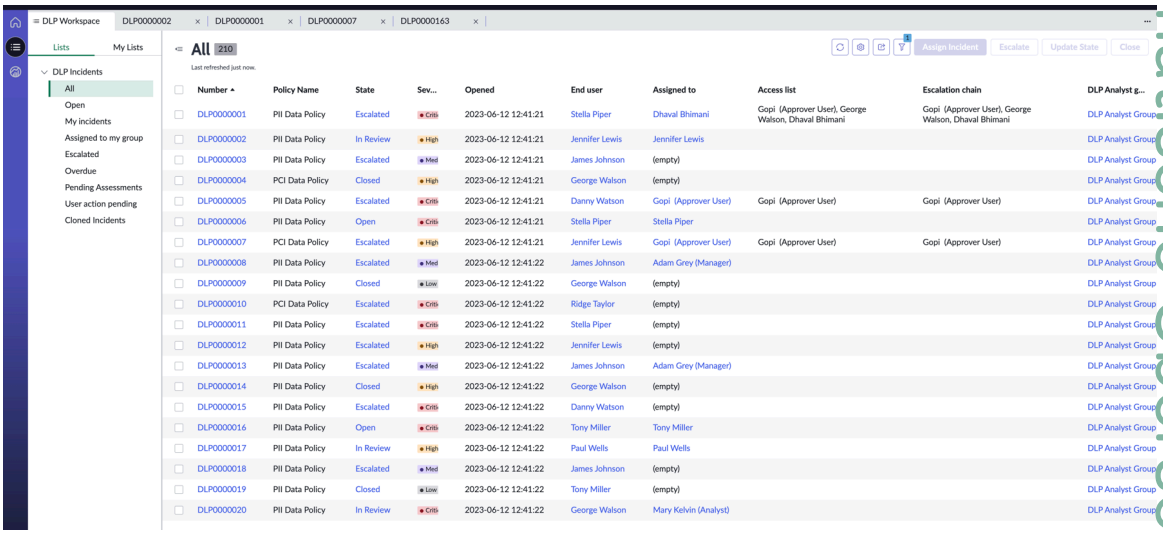
Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.read, sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Prozedur

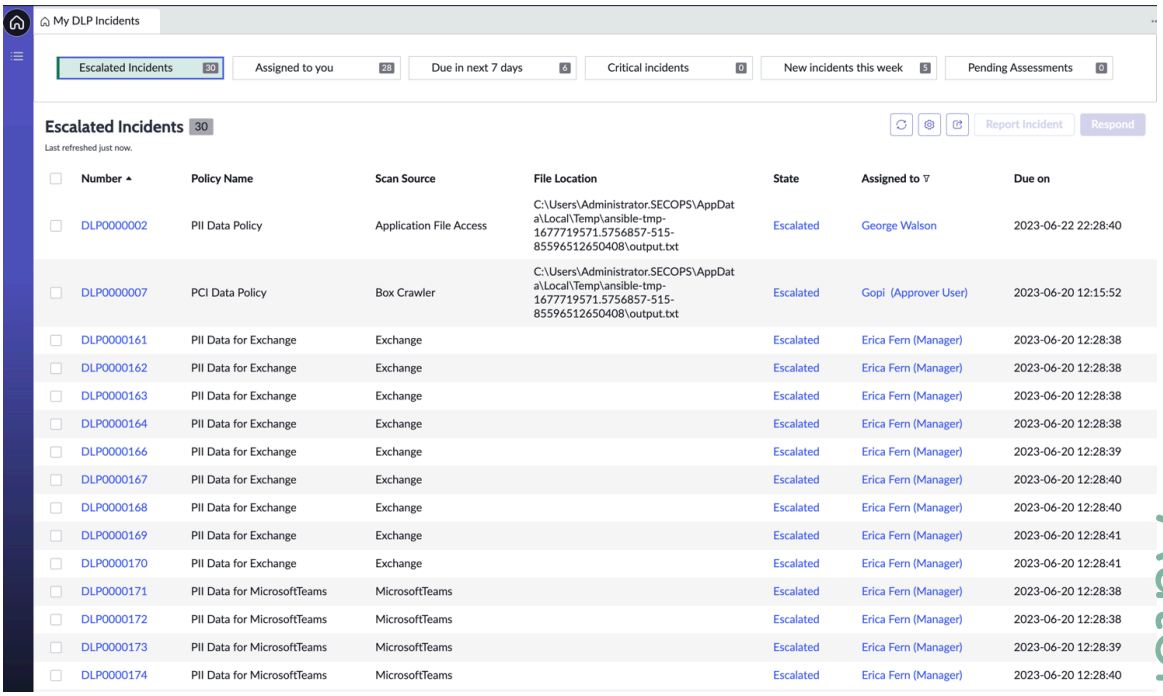
1. Navigieren zu **DLP** > **DLP-Arbeitsbereich für Analysten**an.
   In der Listenansicht sollten Anwender und ihre Delegierten den DLP-Incident unter anzeigen können **Eskaliert** Registerkarte „Incidents“ im Endanwenderportal.
2. Öffnen Sie einen beliebigen Incident.
3. Klicken Sie Auf **Eskalieren** Schaltfläche zum Eskalation eines Incident.
4. Wählen Sie den Anwender oder die Anwendergruppe aus der Dropdown-Liste aus.
   Sie können der Eskalationskette mehrere Anwender hinzufügen. Alle Anwender, die Zugriff haben, werden im Abschnitt „Details“ der Formularansicht und auch unter aufgeführt **Alle** Registerkarte „Incidents“. Die Eskalationskette wird basierend auf den Konfigurationseinstellungen angezeigt. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren



5. Klicken Sie auf **Absenden**.
   Nach der Übermittlung wird der Incident einem Manager zugewiesen, der Endanwender kann den Incident jedoch weiterhin anzeigen.
6. Um dies zu überprüfen, navigieren Sie zu **DLP-Anwenderarbeitsbereich** Als Endanwender.
   Alle Incidents, die dem Endanwender zugewiesen sind, werden angezeigt.
7. Zeigen Sie die Liste der eskalierten Incidents unter an **Eskalierte Incidents** Abschnitt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können die Anwenderzugriffsliste auch unter anzeigen **Eskalationskette** Spalte in der Listenansicht.

8. Öffnen Sie einen beliebigen Incident.
9. Klicken Sie Auf **Antworten Sie** Schaltfläche zum Senden der Incident-Antwort.
10. Wählen Sie die Antwort aus der Dropdown-Liste aus.
11. Klicken Sie auf **Absenden**.

Erstellen Sie Genehmigungsregeln

Erstellen Sie Genehmigungsregeln, um Genehmigungen von verschiedenen Ebenen von Genehmigeranwendern zu erhalten, wenn eine erweiterte Antwortoption ausgewählt wird.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Der DLP-Administrator definiert diese Genehmigungsregeln, um die Zustimmung zu Anforderungen zu erteilen, die von Endanwendern zur Genehmigung der erweiterten Antwortoption gestellt werden. Der DLP-Administrator kann hier auch mehrere Genehmigungsebenen definieren.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **DLP-Genehmigungsregeln**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „DLP-Zuweisungsregel“

Feld	Beschreibung
Name	Name für die Genehmigungsregel.
Aktiv	Option, um anzugeben, ob die Genehmigungsregel aktiv ist.
Ausführungsreihenfolge	Die Genehmigungsregelpriorität. Dieses Feld gibt die Reihenfolge an, in der die Genehmigungsregeln ausgeführt werden, wenn zwei oder mehr Regeln die auslösenden Bedingungen gemeinsam haben. Die Genehmigungsregel mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Beispiel: 100, 200, 300 usw. Der Standardwert ist 100.
Beschreibung	Eindeutige Beschreibung für die Genehmigungsregel.
Bedingung	Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Genehmigungsregel zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER**. ○ Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. Sie können beispielsweise die Bedingungen für diese Incident-Konsolidierungsregel festlegen, indem Sie die Bedingung als auswählen **Integrationsquelle**, **Enthält**, **Microsoft**.
Gilt für Antwortoptionen	Option zum Auswählen der Antwortoption vom Typ „Erweitert“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie können mehrere Antwortoptionen auswählen.
Genehmigende Person	Wählen Sie aus, welche Art von Genehmigeranwender Sie festlegen möchten. ○ **Anwendertabelle** : Wählen Sie diese Option aus, wenn Sie den Genehmigeranwender aus der Tabelle Anwender (sys_user) auswählen möchten. ○ **Anwenderdefinierte Genehmigungsliste** : Wählen Sie diese Option aus, wenn Sie mehrere Ebenen von anwenderdefinierten Genehmigern für eine einzelne Anforderung konfigurieren möchten
Bezeichner des Genehmigers	Dieses Feld wird angezeigt, wenn **Anwendertabelle** Ist für ausgewählt **Genehmiger** Option. Wählen Sie das Feld aus, um den Genehmiger aus der Tabelle „Anwender“ (sys_user) zu bezeichnen.
Anzahl der Ebenen	Dieses Feld wird angezeigt, wenn **Anwendertabelle** Ist für ausgewählt **Genehmiger** Option. Endnummer in diesem Feld, um die Genehmigungsebenen zu definieren. Wenn beispielsweise 3 im Feld Anzahl der Ebenen hinzugefügt wird und Manager im Feld Genehmigerbezeichner ausgewählt ist, wird die Genehmigungsanforderung auf drei Genehmigungsebenen durchlaufen.

Das folgende Beispiel zeigt die Genehmigungsregel, die für eine der erweiterten Antwortoptionen erstellt wurde. Die Bedingung erfordert, dass der Name der Integrationsquelle das Microsoft-Stichwort enthält, das diese Konfiguration auslöst.

4. Für **Genehmiger** Option, wählen Sie aus **Anwenderdefinierte Genehmigungsliste** .
5. Klicken Sie auf **Absenden**.
6. **Genehmigungsebenen** Zugehörige Liste wird in der Formularansicht ausgefüllt.
7. In **Genehmigungsebenen** Klicken Sie auf Abschnitt **Neu** .
8. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Genehmigungsebene“

Feld	Beschreibung
Name	Name für die Genehmigungsebene.
Aktiv	Option, um anzugeben, ob die Genehmigungsebene aktiv ist.
level	Die Ebene für die Genehmigungsregel. Dieses Feld gibt die Reihenfolge an, in der die Genehmigungsebenen ausgeführt werden, wenn zwei oder mehr Ebenen konfiguriert sind. Die Genehmigungsebene mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Betriebsebene festzulegen. Beispiel: 100, 200, 300 usw. Der Standardwert ist 100.
Genehmigungsregel	Genehmigungsregel, für die Sie diese Konfiguration definieren möchten. Dieses Feld ist schreibgeschützt.
Beschreibung	Eindeutige Beschreibung für die Genehmigungsregel.
Genehmigungen erforderlich	Wählen Sie die Option aus, um zu definieren, ob die Genehmigung aller konfigurierten Anwender/ Gruppen erforderlich ist oder nur von einem Anwender erforderlich ist.
Verantwortliche Vertragsgenehmigung	Option zum Auswählen der Genehmiger. **a.** Anwender und Gruppen: **i. Anwender** : Klicken Sie auf Symbol zum Hinzufügen eines bestimmten Anwenders aus der Liste. Sie können einen Anwender auch mithilfe seiner E-Mail-Adresse oder der Suchoption hinzufügen. Um sich selbst als Anwender hinzuzufügen, für den die DLP-Bedingungen gelten, klicken Sie auf . **ii. Gruppen** : Klicken Sie auf das <add_icon>-Symbol, um eine bestimmte Gruppe aus der Liste hinzuzufügen. Sie können auch eine Gruppe mithilfe der Suchoption hinzufügen. **b. Suchen Sie mithilfe eines Skripts** : Sie können den Skript-Editor verwenden,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	um die Feldwerte während der Erstellung der Genehmigungsebene anzupassen und zu formatieren. Sie können beispielsweise das Feld „E-Mail-Adresse“ verwenden, um den Genehmigeranwender zu identifizieren.

9. Klicken Sie auf **Absenden**.

Erstellen Sie Vorlagen für Anwenderanweisungen

Erstellen und verwalten Sie eine Vorlage für Anwenderanweisungen für DLP-Incidents, um den Anwendern zu helfen, die Anweisungen für die Incident-Lösung und die nächsten Schritte im Lösungsprozess zu verstehen.

Vorbereitungen

Die Kartenvorlage „Anwenderanweisungen“ zeigt zwei verschiedene Header an, die Ihnen weitere Informationen zu einem bestimmten Incident in der Formularansicht bieten.

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Wenn dem Endanwender ein Incident zugewiesen wird, muss der Anwender möglicherweise die zusätzlichen Anweisungen zur Reaktion auf Incidents kennen, den Anwendern die Terminologie vorstellen und zusätzliche Informationen zum Incident bereitstellen. Diese Vorlagen können die Anwender dabei unterstützen, die genaue Antwort auf DLP-Incidents bereitzustellen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Vorlagen für Anwenderanweisungen**an.

2. Klicken Sie auf **Neu**.

3. Füllen Sie im Formular die Felder aus.

DLP-Incident-Bewertung

Feld	Beschreibung
Name	Name der Anwenderanweisungsvorlage.
Kurzbeschreibung	Eindeutige Beschreibung dieser Anwenderanweisungsvorlage.
Aktiv	Option, um anzugeben, ob die Anwenderanweisungsvorlage aktiv ist.
Ausführungsbefehl	Priorität der Vorlage für Incident-Anwenderanweisungen. Dieses Feld gibt die Reihenfolge an, in der die Reihenfolge ausgeführt wird, um die Anwenderanweisungsvorlage bei der Erstellung eines Incident auszuwerten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Die Option mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Zum Beispiel 100, 200 oder eine andere Nummer. Der Standardwert ist 100.
Incidents, die der Bedingung entsprechen	Incidents, die den definierten Bedingungen im Bedingungsgenerator entsprechen, werden angezeigt. Diese Bedingungen basieren auf den DLP-Incident-Daten. Um eine Bedingung für eine Anwenderanweisung zu erstellen, wählen Sie eines der Incident-Felder aus. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf UND oder oder: Wenn UND ausgewählt ist, müssen alle Bedingungen erfüllt werden. Wenn ODER ausgewählt ist, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien** . **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Betrifft	Wählen Sie den Anwender oder die Anwendergruppen aus, für die die Vorlage gilt. Die anderen verfügbaren Optionen sind: ○ **Alle Endanwender** : Aktivieren Sie dieses Kontrollkästchen, wenn die Anweisungsvorlage für alle Anwender gilt. ○ **Alle Prüfer eskalierter Incidents** : Aktivieren Sie dieses Kontrollkästchen, wenn die Vorlage für alle Prüfer der eskalierten Incidents gilt. ○ **Bestimmte Anwender** : Klicken Sie auf das Symbol, um einen bestimmten Anwender aus der Liste hinzuzufügen, für den die DLP-Incident-Bedingungen gelten. Sie können einen Anwender auch mithilfe seiner E-Mail-Adresse oder der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Suchoption hinzufügen. Beispiel: Legal Manager. Um sich selbst als Anwender hinzuzufügen, für den die DLP-Bedingungen gelten, klicken Sie auf **Fügen Sie mich hinzu** Symbol. ○ **Bestimmte Anwendergruppen** : Klicken Sie auf das Symbol, um eine bestimmte Gruppe aus der Liste hinzuzufügen, für die die DLP-Incident-Bedingungen gelten. Sie können auch eine Gruppe mithilfe der Suchoption hinzufügen. Zum Beispiel Umfrageersteller.
Anweisungsvorlage: Anweisungen	Fügen Sie im Rich-Text-Editor Anweisungen mit Variablen hinzu, die auf Incident-Ebene verfügbar sind.

4. Führen Sie einen Drilldown zu **Anweisungsvorlage** Geben Sie die Vorlagenanweisung ein, und fügen Sie unter diesem Abschnitt bei Bedarf Informationen auf Incident-Ebene hinzu.
5. Ziehen Sie die erforderlichen Variablen per Drag-and-Drop, um bestimmte Felder dynamisch anzuzeigen.
6. Klicken Sie auf **Absenden**.
   Die Vorlagen für Anwenderanweisungen werden jetzt erstellt, und Sie können auf einen beliebigen Header für Anwenderanweisungen klicken, um die zusätzlichen Details eines DLP-Incidents zu erfahren.

   Weitere Informationen finden Sie unter Data Loss Prevention Incident Response Anwenderarbeitsbereich.

Konfigurieren Sie DLP-UI-Anwenderanweisungen

Konfigurieren Sie die System-UI-Nachrichten, um detaillierte Header für Anwenderanweisungen nach Bedarf hinzuzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **System-UI** > **Nachrichten**an.
2. Suchen Sie nach **User_Instructions_Card_heading** .

   Standardmäßig User_Instructions_Card_heading Und User_Instructions_Modal_window_heading Werden die beiden UI-Nachrichtenkonfigurationen für die Anwender bereitgestellt?
3. Klicken Sie auf eine der Anwenderanweisungen, um sie zu aktualisieren oder zu ändern.

Erstellen Sie E-Mail-Vorlagen

Erstellen und verwalten Sie die vorkonfigurierten E-Mail-Vorlagen zum Senden von Benachrichtigungen an Endanwender, Anwendergruppen oder Manager. Mit diesen Vorlagen können Sie Coaching und Kommunikation mit Ihren Endanwendern über durchführen Data Loss Prevention Incident Response(DLP IR) Incidents.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

> **Wichtig:**
> Damit Analysten die E-Mail-Kommunikation eines DLP-Incidents im Aktivitätenstrom anzeigen können, sollten Sie die Rolle „sn_dlir.Analyst“ in der globalen Systemeigenschaft hinzufügen oder anhängen `Glide.ui.Activity.email_roles` .

Warum und wann dieser Vorgang ausgeführt wird

E-Mail-Benachrichtigungen werden nach den Incident-Benachrichtigungen kategorisiert, die an die Endanwender gesendet werden, den Eskalationsbenachrichtigungen, die an die Manager gesendet werden, oder den Benachrichtigungen zum Fälligkeitsdatum. Sie können E-Mail-Benachrichtigungen über die Fälligkeitsdaten von DLP-Incidents senden oder die Endanwender sogar darüber coachen, was zu tun ist, wenn bestimmte Bedingungen im E-Mail-Bedingungsfilter erfüllt sind.

Mit DLP-E-Mail-Vorlagen können Sie die E-Mail-Benachrichtigung an Endanwender, Manager und Analysten senden. Sie können die Vorlagen konfigurieren, die pro Incident oder als Digest gesendet werden sollen. Ihr E-Mail-Betreff und -Text können Variablen enthalten, damit Sie Ihren vorhandenen Inhalt wiederverwenden können.

DLP stellt die folgenden vorkonfigurierten E-Mail-Vorlagen basierend auf den Kategorien bereit:

- **DLP-E-Mail-Vorlage – Genehmigungsbenachrichtigung pro Incident:** Benachrichtigen Sie Anwender über die Genehmigung ihrer Anforderungen.
- **DLP-E-Mail-Vorlage – Eskalationsbenachrichtigung:** Senden Sie Eskalationsbenachrichtigungen in Form von Digests an Manager.
- **DLP-E-Mail-Vorlage – Benachrichtigung über ausstehende Genehmigung:** Benachrichtigen Sie Genehmiger über ausstehende Elemente.
- **DLP-E-Mail-Vorlage – Benachrichtigung über Abbruch der Genehmigungsanforderung pro Incident:** Benachrichtigen Sie Anwender über eine Genehmigungsanforderung, die vom DLP-Analystenteam abgebrochen wurde.
- **DLP-E-Mail-Vorlage – Benachrichtigung über Abschluss der Anwenderantwort:** Benachrichtigen Sie das DLP-Analystenteam über die von Anwendern übermittelte Antwort.
- **DLP-E-Mail-Vorlage – Benachrichtigung über Anwender-Incidents:** Dies ist eine Standardvorlage für die Anwender-Digest-Benachrichtigung. Senden Sie alle paar Tage Incident-Benachrichtigungen in Form von Digests an die Endanwender, auch wenn keine neuen Incidents vorhanden sind, um die Anwender über die Gesamtzahl der Incidents für den Namen des jeweiligen Anwenders zu informieren. Sie können auch Digest-Benachrichtigungen senden, um die Anwender über die nächsten bevorstehenden Fälligkeitsdaten von DLP-Incidents mit dem Schweregrad „Kritisch“, „hoch“, „Mittel“ oder „Niedrig“ zu benachrichtigen.
- **DLP-E-Mail-Vorlage: Benachrichtigung über ausstehende Genehmigung pro Incident** : Benachrichtigen Sie Genehmiger über ausstehende Genehmigungen.
- **DLP-E-Mail-Vorlage – Ablehnungsbenachrichtigung:** Senden Sie eine Benachrichtigung über die Ablehnung an die anfordernde Person.
- **DLP-E-Mail-Vorlage – Benachrichtigung über Fälligkeitsdatum:** Benachrichtigung über Fälligkeitsdatum des Incidents senden. Wenn dem Endanwender ein DLP-Incident zugewiesen wird und der Endanwender vor dem Fälligkeitsdatum keine Maßnahmen ergriffen hat, wird eine E-Mail-Benachrichtigung an den Endanwender

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

gesendet. Sie haben auch die Möglichkeit, den DLP-Incident an einen Manager, einen anwenderdefinierten Anwender oder eine Anwendergruppe zu eskalieren, wenn das Fälligkeitsdatum der Antwort überschritten wurde.

Hinweis:
Benachrichtigungen zu Fälligkeitsdatum müssen in Form von Digests vorliegen.

- **DLP-E-Mail-Vorlage – Anwenderantwortbenachrichtigung pro Incident:** Benachrichtigen Sie Analysten über die übermittelten Anwender pro Incident.
- **DLP-E-Mail-Vorlage – Eskalationsbenachrichtigung pro Incident:** Benachrichtigen Sie Manager über Eskalationen pro Incident.
- **DLP-E-Mail-Vorlage – Anwenderbenachrichtigung pro Incident:** Benachrichtigen Sie Anwender über die Zuweisung pro Incident.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **E-Mail-Vorlagen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „DLP-E-Mail-Vorlage“

Feld	Beschreibung
Name	Name der E-Mail-Vorlage.
Aktiv	Option, um anzugeben, ob die DLP-E-Mail-Vorlage aktiv ist. Wenn diese Option nicht aktiviert ist, werden für diese E-Mail-Vorlage keine Benachrichtigungen gesendet.
Kategorie	E-Mail-Benachrichtigungskategorie. DLP unterstützt die folgenden Optionen: ○ **Incident-Benachrichtigung an Endanwender** : Wird gesendet, wenn die Incidents Endanwendern zugewiesen werden. ○ **Eskalationsbenachrichtigung an Manager** : Wird gesendet, wenn das Fälligkeitsdatum der Antwort überschritten oder dem Manager manuell über das DLP-Ops-Portal zugewiesen wird. ○ **Benachrichtigung über Fälligkeitsdatum** : Wird gesendet, wenn das Fälligkeitsdatum der Antwort überschritten wird. ○ **Anwenderantwortbenachrichtigung an Analysten** : Wird gesendet, wenn der Endanwender eine Aktion für den DLP-Incident ausführt. ○ **Benachrichtigung über ausstehende Genehmigungen** : Benachrichtigen Sie Genehmiger über ausstehende Elemente. ○ **Genehmigungsbenachrichtigung an die anfordernde Person** : Benachrichtigen Sie Anwender über die Genehmigung ihrer Anforderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Lehnen Sie die Benachrichtigung an die anfordernde Person ab** : Benachrichtigen Sie Anwender über die Ablehnung ihrer Anforderungen. ○ **Benachrichtigung an die anfordernde Person abbrechen** : Benachrichtigen Sie Anwender über den Abbruch ihrer Anforderungen.
Typ	Option, um anzugeben, ob die E-Mail pro Incident oder als Digest gesendet wird. **Hinweis:** Wenn Sie ausgewählt haben **Benachrichtigung über Fälligkeitsdatum** Von **Kategorie** Dann können Sie nur Digests verwenden. Wählen Sie diese Option aus.
Beschreibung	Eindeutige Beschreibung für diese E-Mail-Vorlage.
Ausführungsbefehl	E-Mail-Vorlagenpriorität Dieses Feld gibt die Reihenfolge an, in der die E-Mail-Vorlagen ausgeführt werden, wenn zwei oder mehr E-Mail-Vorlagen die auslösenden Bedingungen gemeinsam haben. Die E-Mail-Vorlage mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Zum Beispiel 100, 200 oder eine andere Nummer. Der Standardwert ist 100.
Vorlagenbedingung	Optionen in den Vorlagenbedingungen, die auf der DLP-Incident-Tabelle basieren. Sie können jedes der Incident-Felder auswählen, um die Auslöserbedingung für die E-Mail-Vorlage zu erstellen. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER** . ○ Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien** . **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Zielanwender	Zielanwender für die Vorlage, wenn die Bedingungen erfüllt sind. Die Zielanwender können einer der folgenden sein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Alle Empfänger** : Senden Sie die E-Mail an Zielanwender. ○ **Empfänger in der Gruppe:** Senden Sie die E-Mail nur an Empfänger innerhalb einer bestimmten Gruppe, indem Sie die Filteroption verwenden. ○ **Empfänger, die den Kriterien entsprechen** : Senden Sie die E-Mail an Zielanwender, die den Kriterien entsprechen. Sie können den Filter verwenden, um Zielanwender basierend auf den Bedingungen anzuzeigen. Beispiel: Stadt.

E-Mail-Vorlage	E-Mail-Vorlage, die Sie auswählen können. Sie können die Variablen definieren, um vorhandene Inhalte wiederzuverwenden, um sie der E-Mail-Benachrichtigung hinzuzufügen.
	Die **Kategorie** Und **Typ** Felder bestimmen die Variablen, die zur Auswahl verfügbar sind. Nehmen wir beispielsweise an, dass die E-Mail-Kategorie auf Incident-Benachrichtigung festgelegt ist und der E-Mail-Typ ein Digest ist, dann sind die zur Auswahl stehenden Variablen Digest-Felder, um die Akkumulation mehrerer DLP-Incidents zu berücksichtigen.
	Hier ist ein Beispiel für E-Mail-Text-HTML jeder E-Mail-Vorlage:
	○ **Standardvorlage für Genehmigungsbenachrichtigungen pro Incident** :
	`Dear ${respondent.first_name},`
	`Your request "${end_user_response}" on the incident ${number} has been approved.`
	`- Date protection team`
	○ **Benachrichtigung über Abbruch der Anforderung für die Genehmigung eines Incidents**
	`Dear ${respondent.first_name},`
	`Your request "${end_user_response}" on the DLP incident ${number} has been cancelled.`
	`No action is required from you at this point. Data protection team will contact you for any further information required.`
	`- Data protection team`
	○ **Standardvorlage für Benachrichtigung über Fälligkeitsdatum** :

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dear ${target_user.name}, Following incidents require your response. ${due_days_table} - Data protection team ○ **Standardvorlage für Anwenderbenachrichtigung pro Incident** : Dear ${assigned_to.name}, DLP Incident ${number} is assigned to you. Please review and submit your response. - Data protection team ○ **Standardvorlage für Anwender-Incident-Benachrichtigung** : Hello ${target_user.name}, You have ${total_number_of_incidents} incidents assigned to you currently that require your response. ${new_incidents_in_period} new incidents got assigned to you since the last email communication. Nearest upcoming due date for responding to a critical incident is ${nearest_due_date_for_critical_severity_incidents}. Please log in to the ${link_to_dlp_portal} and submit your response. - Data protection team ○ **Standardvorlage für Eskalation – Digest** : Hi ${target_user.name}, The following data security incidents have been escalated to you due to lack of response from the assignees. Please login to the incident response workspace to review the incidents and submit your response. ${overdue_table} - Data protection team ○ **Standardvorlage für Eskalation – Pro Incident** :

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dear ${assigned_to.name}, Data security incident ${number} has been escalated to you. Please review and submit your response or assign the incident back to the user. - Data protection team
	○ **Standardvorlage für Benachrichtigung über ausstehende Genehmigung** : Dear ${approver.first_name}, Your approval is required for a few requests on data security incidents. Please login to the workspace here and review the requests. - Data protection team
	○ **Standardvorlage für Benachrichtigung über ausstehende Genehmigung pro Incident** : Dear ${Approver}, Your approval is required for the incident ${number} requested by the user ${respondent.first_name} ${respondent.last_name}. Please visit this here to approve or reject the request. - Data Protection Team
	○ **Standardvorlage für die Benachrichtigung über die Ablehnung pro Incident** : Dear ${respondent.first_name} ${respondent.last_name}, This is to inform you that your request "${end_user_response}" for the DLP incident ${number} has been rejected. Please review the incident here. - Data protection team
	○ **Standardvorlage für Anwenderantwortbenachrichtigung für „Pro Incident“** :

Automatische Übersetzung

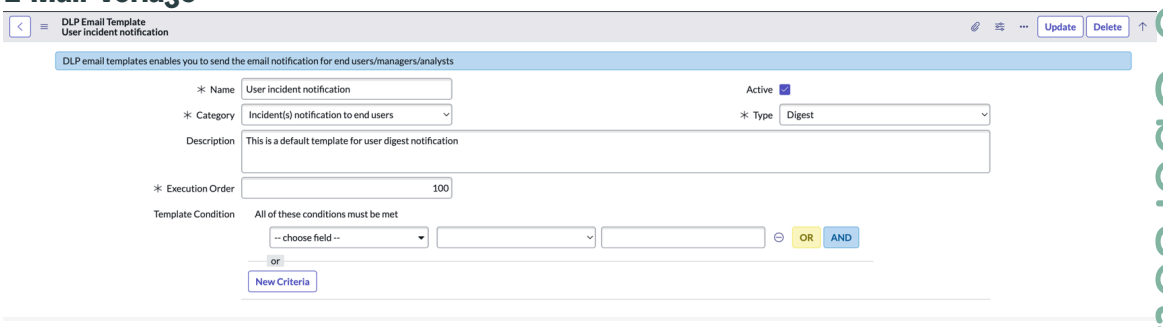
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hi ${assigned_to.name}, This is to inform you that a response has been submitted for the DLP Incident ${number}. ○ **Standardvorlage für Benachrichtigung über Abschluss der Anwenderantwort** : Hello ${target_user.name}, This email is to inform you that users have submitted their response for ${new_incidents_in_period_user_response_completed} new incidents since the last email communication. Please review the response for these incidents ${link_to_incidents_in_period_user_response_completed}.

Example

Das folgende Beispiel zeigt die DLP-E-Mail-Vorlage mit den Zielanwendern, die als alle Empfänger definiert sind.

E-Mail-Vorlage

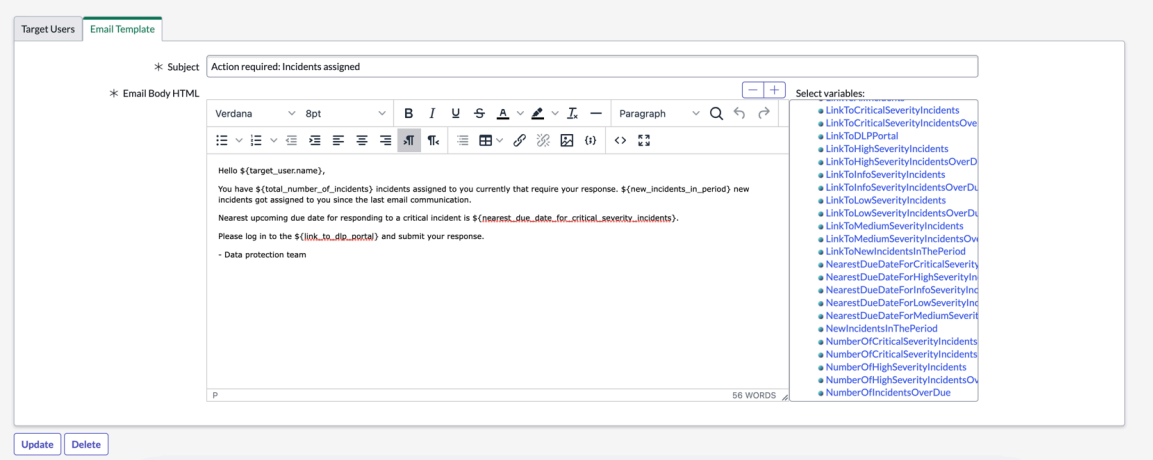


Das folgende Beispiel zeigt eine E-Mail-Vorlage mit dem Betreff „User Incident Notification“ und einer Variable `New_Incidents_in_period` . Der E-Mail-Text enthält mehrere Variablen, die aus der Spalte Variablen auswählen hinzugefügt werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Vorlagenvariablen



4. Klicken Sie auf **Absenden**.

Ergebnisse

Der Endanwender erhält eine Digest-Benachrichtigungs-E-Mail mit allen ausgewählten Variablenfeldern in der Vorlage.

Erstellen Sie einen Data Loss Prevention Incident Response SLA-Auslöser

Erstellen Sie einen Data Loss Prevention Incident Response SLA-Auslöserbedingung, die eine Eingabeaufforderung und effiziente Antwort auf einen Incident ermöglicht, wenn er ausgelöst wird.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – DLP-SLA-Auslöser erstellen, aktualisieren und löschen
- sn_dlir.Analyst.read: Auslösertabelle lesen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **SLA-Auslöser**an.
2. Wählen Sie Aus **Neu** Zum Erstellen des SLA-Auslösers.

Feld	Beschreibung
Name	Name des Auslösers
Reihenfolge	Reihenfolge, in der der Auslöser berücksichtigt wird.
Aktiv	Option zum Auswerten des SLA-Auslösers.
Auslöser, wenn ein DLP-Incident aktualisiert wird	Option zum Auswerten der Auslöserbedingung bei jeder Aktualisierung des DLP-Incidents.

3. Konfigurieren Sie eine Bedingung, indem Sie den Regeldatensatz auswählen und Bedingungen in definieren **Auslöserbedingung** Feld.
   Beispielsweise wäre die Auslöserbedingung zum Festlegen von SLAs für DLP-Incidents aus einer E-Mail-Scan-Quelle **[Scanquelle][ist][E-Mail-SMTP]** .
4. Wählen Sie **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Einmal ein Aufgaben-SLA-Datensatz für einen Data Loss Prevention Incident Response Incident erstellt wird, wird die Registerkarte „SLA-Datensätze“ für diesen bestimmten Incident im Arbeitsbereich sichtbar. Auf dieser Registerkarte können Sie ein SLA-System für die Aufgabe Ihrer Organisation verwenden.

Erstellen Sie einen Data Loss Prevention Incident Response SLA-Definition

Erstellen Sie einen Data Loss Prevention Incident Response SLA-Definition, die die Bedingungen und die Dauer für die Reaktion auf Datenschutzverletzungen beschreibt. Die Festlegung klarer Erwartungen und Protokolle trägt dazu bei, eine schnelle Reaktion auf Incidents zu gewährleisten, potenzielle Schäden zu minimieren und allgemeine Datenschutzstrategien zu verbessern.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin – DLP-SLA-Definitionen erstellen, aktualisieren und löschen.
- sn_dlir.Analyst.read: DLP-SLA-Definitionen lesen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **SLA-Definitionen**an.
2. Erstellen Sie eine SLA-Definition.
   Eine Beschreibung der Feldwerte finden Sie unter Formular „DLP-SLA-Definition“.
3. Wählen Sie **Absenden**.

> **Hinweis:**
> Fälligkeitsdatumsregeln, Eskalationen und SLA-Definitionen schließen sich gegenseitig aus. Eine SLA-Definition bestimmt in erster Linie, wann ein bestimmtes SLA wirksam wird, angehalten, angehalten oder ausgelöst wird.

Bewertungen erstellen

Erstellen und verwalten Sie Bewertungen, damit Endanwender auf DLP-Incidents reagieren können. Sie können die Bewertungen verwenden, um Informationen zu den vertraulichen Daten zu sammeln, die aus den DLP-Incidents verfügbar gemacht oder weitergegeben werden.

Erstellen und verwalten Sie Bewertungen für DLP-Incidents

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

DLP-Incident-Bewertungen helfen Ihnen, potenzielle Bedrohungen und Schwachstellen für Ihre Daten basierend auf der Endanwenderantwort zu identifizieren. Sie können diese Informationen verwenden, um die vorhandenen Lücken, Bedenken und Erwartungen Ihrer Endanwender zu bestimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Bewertungen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

DLP-Incident-Bewertung

Feld	Beschreibung
Name	Name der DLP-Incident-Bewertung.
Aktiv	Option, um anzugeben, ob die DLP-Incident-Bewertung aktiv ist.
Beschreibung	Eindeutige Beschreibung für diese DLP-Incident-Bewertung.
Einführung in die Bewertung	Geben Sie eine Einführung oder einen Kontext für Ihre Bewertung an. Sie können auch Variablen aus dem Abschnitt Variablen auswählen verwenden, um bestimmte Felder dynamisch anzuzeigen.

4. Klicken Sie auf **Absenden**.
5. Öffnen Sie nach dem Erstellen einer Bewertung die Bewertung, und klicken Sie auf **Bewertungsdesigner** .
6. Wählen Sie im Abschnitt „neue Bewertung“ im Abschnitt „Steuerungen“ eine Art von Bewertungsfrage aus.
7. Ziehen Sie den erforderlichen Bewertungsfragetyp per Drag-and-Drop im Abschnitt „neue Bewertung“. Sie können beispielsweise Drag-and-Drop verwenden **Auswahl** Steuerung im Abschnitt „neue Bewertung“ oder „neue Kategorie“.
8. Klicken Sie auf , um weitere Kategorien für die Bewertung hinzuzufügen Symbol.
9. Klicken Sie auf , um eine vorhandene Kategorie zu ändern Symbol.
10. Nachdem Sie die verschiedenen Bewertungsfragen zum ersten Mal erstellt haben, klicken Sie auf **Speichern** , Und dann **Veröffentlichen** .

Erstellen Sie Optionsregeln für die Reaktion auf Incidents

Erstellen Sie die Optionsregeln für die Reaktion auf Incidents, die Endanwender oder Analyst bei der Reaktion auf einen Incident verwenden können.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Art der Antwort konfigurieren, die ein Endanwender basierend auf dem Typ des DLP-Incidents ausführen soll. Die DLP Incident Response-Basissystem-Anwendung bietet Anwendern die folgenden Antwortoptionen:

- Bewertung Abgeschlossen
- Inhalt Gelöscht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Datei löschen
- Verschlüsselte Datei
- Maskierter Inhalt
- Falsch positiv melden
- Falschen Besitzer melden
- Erforderlich für Geschäftsprozess
- Berechtigungen Überprüft

Angenommen, ein Endanwender meldet einen DLP-Incident als falsch positiv. Der Status für diesen Incident wird dann automatisch als „Geschlossen“ markiert, da der von Ihnen konfigurierte Zielstatus „Geschlossen“ ist.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Optionsregeln für die Reaktion auf Incidents**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „Optionsregeln für Incident-Reaktion“

Feld	Beschreibung
Name	Name der Option für die Reaktion auf Incidents.
Aktiv	Option, um anzugeben, ob die Option für die Reaktion auf Incidents aktiv ist.
Ausführungsreihenfolge	Priorität der Option für die Reaktion auf Incidents. Dieses Feld gibt die Reihenfolge an, in der die Antwortoptionen für Incidents ausgeführt werden, wenn zwei oder mehr Antwortoptionen für Incidents die auslösenden Bedingungen teilen. Die Option „Reaktion auf Incidents“ mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Zum Beispiel 100, 200 oder eine andere Nummer. Der Standardwert ist 100.
Beschreibung	Eindeutige Beschreibung für diese Option für die Reaktion auf Incidents.
Standardzielstatus	Der von Ihnen konfigurierte Standardzielstatus.
Bedingung	Bedingungen im Bedingungsgenerator. Diese Bedingungen basieren auf der DLP-Incident-Tabelle. Um eine Bedingung für die Optionen für die Reaktion auf Incidents zu erstellen, wählen Sie eines der Incident-Felder aus.

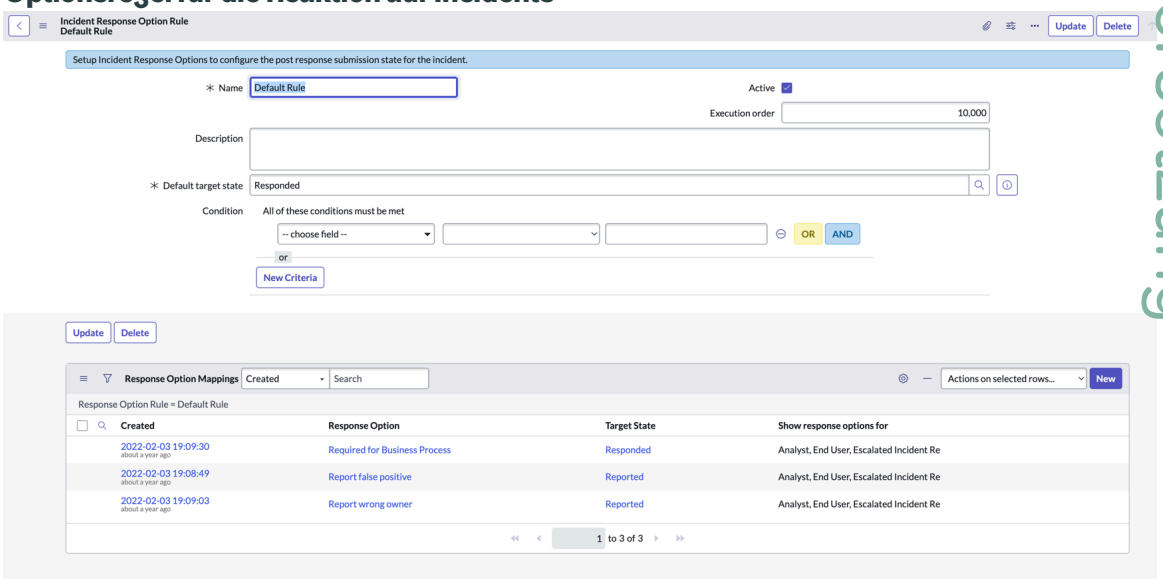
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER**: ○ Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.

Example

Das folgende Beispiel zeigt die Konfiguration der Endanwenderaktion für einen Endpunkt. Die Bedingung erfordert, dass die Scanquelle ein Endpunkt-Dateisystem ist, das dann diese Konfiguration der Endanwenderaktion auslöst. Die Zuordnung zeigt, dass der falsche Besitzer melden, falsch positive Berichte melden und die gelöschte Datei die Antwortoptionen sind, die für verfügbar sind Endanwender .

Optionsregel für die Reaktion auf Incidents



4. In **Antwortoptionszuordnungen** Klicken Sie auf Abschnitt **Neu**.
5. Füllen Sie im Formular die Felder aus.

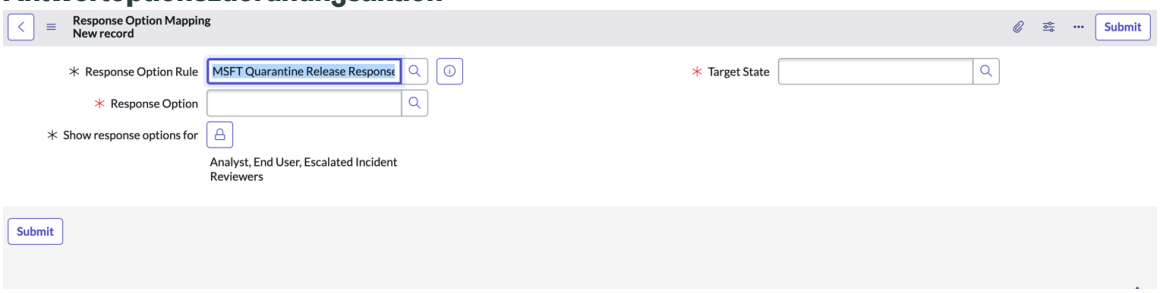
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Antwortoptionszuordnung“

Regel für Antwortoption	Name der Optionsregel für die Reaktion auf Incidents. Beispiel: SharePoint Impliziert, dass die Scanquelle SharePoint ist. Sie können entweder den Namen der Incident-Antwort eingeben oder mithilfe der Suche suchen.
Antwortoption	Option zum Auswählen der Antwortoption. Sie können entweder die Antwortoption eingeben oder mithilfe der Suche suchen.
Zielstatus	Der Zielstatus des DLP-Incidents, nachdem der Endanwender die entsprechende Aktion ausgewählt hat. **Hinweis:** **a.** Die **Zielstatus** Feld wird nur angezeigt, wenn Sie auswählen **Antwortoption** Welche von ist **Typ: Standard** . Weitere Informationen zur Konfiguration der Zielstatustypen finden Sie unter Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents. **b.** Wenn eine Antwortoption von ist **Typ: Erweitert** Ist ausgewählt, können Sie den Zielstatus nicht festlegen und werden ausgeblendet. Der Zielstatus wird basierend auf dem anwenderdefinierten Status zugewiesen, der im Flow Designer-Subflow konfiguriert ist.
Antwortoptionen anzeigen für	Option zum Bestimmen der Anwenderrollen, für die die Antwortoptionen angezeigt werden sollen. Sie können aus wählen **Analyst** , **Endanwender** , Und **Eskalierte Prüfer Von Analysten** Durch Verwenden der Option Entsperren. Sie können eine oder alle Rollen auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwortoptionszuordnungsaktion



6. Klicken Sie auf **Absenden**.

Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents

Verwenden Sie diese Funktion, um den Typ der Antwort zu konfigurieren, die ein Endanwender oder Analyst ausführen soll.

Vorbereitungen

Die DLP Incident Response-Basissystem-Anwendung bietet die folgenden Antwortoptionen:

1. Bewertung Abgeschlossen
2. Inhalt Gelöscht
3. Datei löschen
4. Verschlüsselte Datei
5. Maskierter Inhalt
6. Falsch positiv melden
7. Falschen Besitzer melden
8. E-Mail-Freigabe aus Quarantäne anfordern

   Hinweis:
   Diese Option ist für die DLP Microsoft Exchange-Datensätze verfügbar.

9. Erforderlich für Geschäftsprozess
10. Berechtigungen Überprüft

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Antwortoptionen**an.

   Standardmäßig bietet das Basissystem zwei Arten von Antwortoptionen:

   a. **Standard** : Eine vom Anwender übermittelte manuelle Antwortoption.

   b. **Erweitert** : Eine automatisierte Antwortoption löst einen Flow Designer-Subflow aus, wenn der Anwender die Antwortoption übermittelt.

2. Klicken Sie auf **Neu**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Füllen Sie im Formular die Felder aus.

Antwortoptionsformular vom Typ: Standard

Feld	Beschreibung
Name	Geben Sie den Namen der Option für die Reaktion auf Incidents ein.
Typ	Option zum Auswählen des Antwortoptionstyps.

Antwortoptionsformular vom Typ: Erweitert

Feld	Beschreibung
Name	Geben Sie den Namen der Option für die Reaktion auf Incidents ein.
Typ	Option zum Auswählen der Antwortoption. Standardmäßig zeigt dieses Feld die folgenden zwei Arten von Optionen an: ○ **Standard** : Wenn Sie diese Option beim Erstellen einer neuen Antwortoption auswählen, müssen Sie möglicherweise einen Antwortoptionsnamen und den Typ hinzufügen. ○ **Erweitert** : Wenn Sie diese Option auswählen, stehen Ihnen die folgenden Felder zur Auswahl: ▪ **Flow** : Wählen Sie den Flow Designer-Subflow aus. ▪ **MID-Server erforderlich** : Aktivieren Sie dieses Kontrollkästchen, wenn der ausgewählte Flow den MID-Server verwendet.
Flow	Wählen Sie den erforderlichen Flow Designer-Flow aus, um die MID-Anwendung und die MID-Fähigkeit zu aktivieren. Wenn Sie einen Subflow für die Antwortoption erstellen, fügen Sie die folgenden Subflow-Eingaben hinzu: **a. Name** : ▪ dlp_Incident ▪ Mid_Server_Capability ▪ Mid_Server_Application **b. Typ**: ▪ Referenz (zur DLP-Incident-Tabelle) ▪ SYS-ID für die MID-Server-Anwendung und die MID-Server-Fähigkeit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

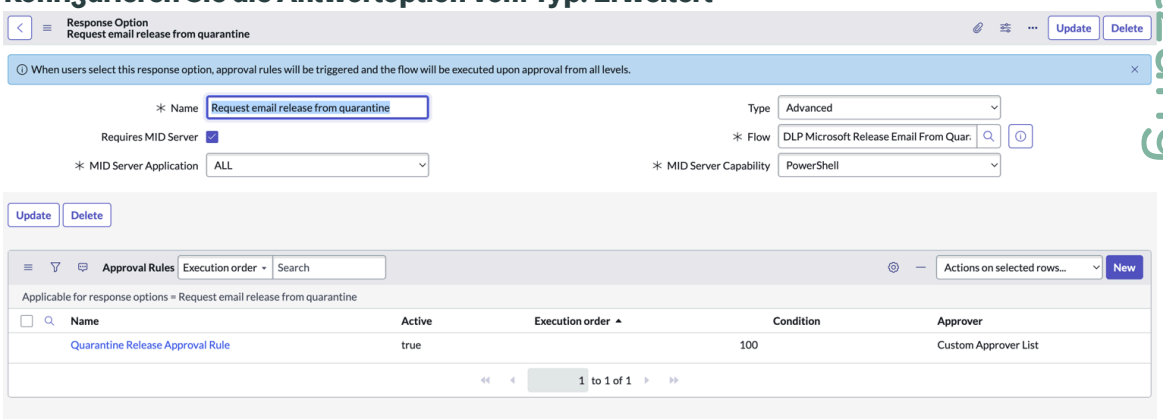
Feld	Beschreibung
MID-Server erforderlich	Option zum Bestimmen dieser MID-Server-Konfiguration. Durch Aktivieren von **MID-Server erforderlich** Kontrollkästchen **MID-Server-Anwendung** Und **MID-Server-Fähigkeit** Felder Sie können die MID-Anwendung und DIE MID-Fähigkeit konfigurieren. **Hinweis:** Basierend auf der Konfiguration der MID-Serveranwendung und der MID-Server-Fähigkeit und wenn ein MID aktiv ist und ausgeführt wird, ist nur die Antwortoption im Arbeitsbereich sichtbar.
MID-Server-Anwendung	Wählen Sie die erforderliche MID-Server-Anwendung aus der Dropdown-Liste aus.
MID-Server-Fähigkeit	Wählen Sie die erforderliche MID-Server-Fähigkeit aus der Dropdown-Liste aus.

Hinweis:
Wenn für die ausgewählte MID-Server-Fähigkeit kein MID-Server verfügbar ist, ist die Antwortoption nicht sichtbar. Wenn Sie einen bestimmten MID-Server aus der Liste haben möchten, müssen Sie die MID-App konfigurieren und in der Liste sichtbar machen. Dann sollte mindestens ein konfigurierter MID-Server aus den ausgewählten MID-Anwendungen ausgeführt werden und über die ausgewählte MID-Server-Fähigkeit verfügen.

4. Klicken Sie auf **Absenden**.

Hinweis:
Wenn Sie einen erstellen **Erweitert** Typ der Antwortoption, dann die **Genehmigungsregeln** Die zugehörige Liste wird ausgefüllt, damit Sie die Genehmigungsregel für diese neue Antwortoption konfigurieren können. Weitere Informationen finden Sie unter Erstellen Sie Genehmigungsregeln.

Konfigurieren Sie die Antwortoption vom Typ: Erweitert



Erstellen Sie Altersdiagrammkonfigurationen

Konfigurieren Sie das Altersdiagramm, das in angezeigt wird Data Loss Prevention Incident Response(DLP IR) Ops-Portal. Dieses Diagramm zeigt die Anzahl der offenen Incidents nach Anzahl der Tage.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Konfiguration des Altersdiagramms**an.
2. Überprüfen Sie die Einträge des Altersdiagramms in der folgenden Tabelle, und passen Sie die Einträge für Ihre Umgebung an.

Formular „DLP-Altersdiagrammkonfigurationen“

Name	Bedingung
0–30 Tage	Alter des offenen Incidents, das zwischen 0 und 30 Tagen liegt.
31–60 Tage	Alter des offenen Incidents, das zwischen 31 und 60 Tagen liegt.
61–90 Tage	Alter des offenen Incidents, das zwischen 61 und 90 Tagen liegt.
Über 90 Tage	Alter des offenen Incidents, das über 90 Tage beträgt.

3. Fügen Sie eine neue Altersdiagrammkonfiguration hinzu, indem Sie auf klicken **Neu** .
4. Geben Sie im Feld Name einen ein **Name** Für die DLP-Altersdiagrammkonfiguration.
5. Legen Sie die Bedingungen für die DLP-Altersdiagrammkonfiguration fest.

   a. Um Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER** .
      - Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
      - Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden.

      Hinweis:
      Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.

   b. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien** .

6. Klicken Sie auf **Absenden**.

Erstellen Sie Anwenderdelegiertenkonfigurationen

Verhindern Sie, dass bestimmte Führungskräfte in der Organisation Benachrichtigungen über die ihnen zugewiesenen oder eskalierten Incidents erhalten.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Betrachten Sie ein Szenario, in dem die Führungskraft ein Anwender ist, der einer Führungskraft oder Führungsgruppe angehört. Die Führungskraft darf keine E-Mails über die Zuweisung oder Eskalation von Incidents erhalten. Ein delegierter Anwender kann dann im Namen der Führungskraft die erforderliche Aktion ergreifen.

Sobald ein Anwender eine bestimmte Person, Henry, als Delegierten zugewiesen hat, kann ein anderer Anwender Henry nicht mehr als Delegierten zuweisen. Ebenso kann ein Delegierter keinen anderen Anwender als Delegierten zuweisen.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Delegierten-Konfiguration**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „Konfiguration delegieren"

Feld	Beschreibung
Anwender	Name des Anwenders, der einen Delegierten für DLP-Incidents benötigt.
Delegierter	Name des Anwenders, der im Namen des ursprünglichen Endanwenders auf den DLP-Incident reagieren kann.

4. Klicken Sie auf **Absenden**.

Erstellen Sie Identifizierungsregeln für Wiederholungsdelikte

Erstellen Sie Regeln zur Identifizierung von Wiederholungsverletzern, um Anwender zu identifizieren, die dasselbe Problem mehrmals wiederholen.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Sie können wiederholte Straftäter anhand bestimmter Regeln oder Kriterien identifizieren. Data Loss Prevention Incident Response Stellt Felder bereit, mit denen Sie wiederholte Straftäter identifizieren können.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Regeln zur Identifizierung von Straftätern wiederholen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Regeln zur Identifizierung von Straftätern wiederholen“

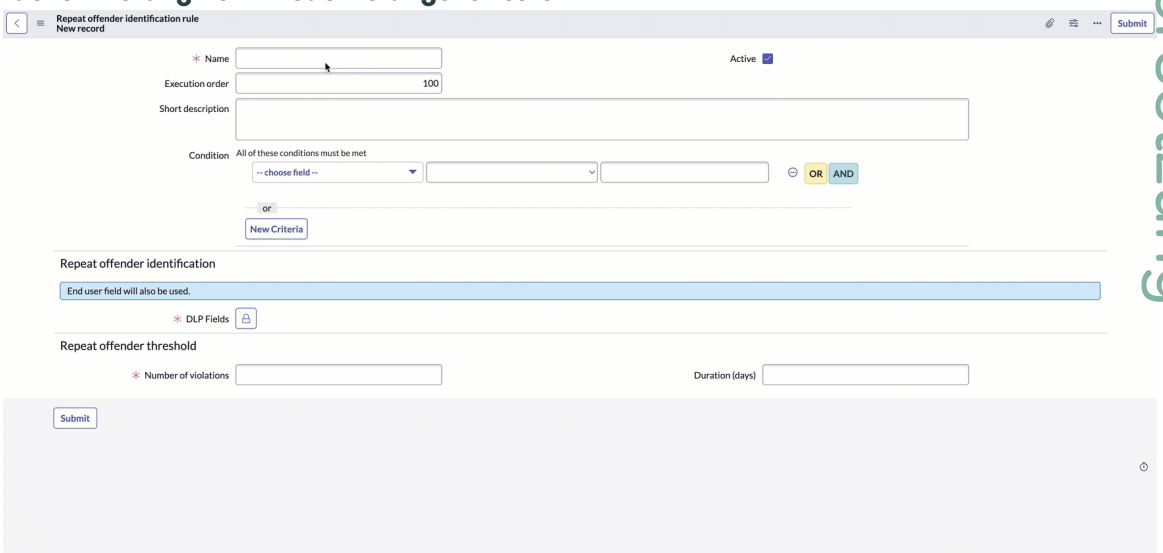
Feld	Beschreibung
Name	Name der Identifizierungsregel für wiederholte Straftäter.
Ausführungsreihenfolge	Priorität der Identifizierungsregeln für Wiederholungsdelikte. Dieses Feld gibt die Reihenfolge an, in der die Identifizierungsregeln für wiederholte Straftäter ausgeführt werden, wenn zwei oder mehr Regeln die auslösenden Bedingungen gemeinsam haben. Die Regel zur Identifizierung von Wiederholungstätern mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Zum Beispiel 100, 200 oder eine andere Nummer. Der Standardwert ist 100.
Kurzbeschreibung	Eindeutige Beschreibung für diese Regel zur Identifizierung wiederholter Straftäter.
Bedingung	Bedingungen im Bedingungsgenerator, die auf der DLP-Incident-Tabelle basieren. Sie können jedes der Incident-Felder auswählen, um die Auslöserbedingung für die Identifizierungsregel für Wiederholungsdelikte zu erstellen. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER**: ○ Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
DLP-Felder	Identifizieren Sie wiederholte Straftäter basierend auf den erforderlichen DLP-Feldern. Klicken Sie auf Symbol neben den DLP-Feldern, um die Liste der verfügbaren DLP-Felder anzuzeigen. Wählen Sie die DLP-Felder, die Sie verwenden möchten, aus der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Spalte verfügbar aus, und verschieben Sie sie in die Spalte ausgewählt. Sie können beispielsweise auswählen **Dateiname** Und **Dateibesitzer** Felder aus der Spalte verfügbar und verschieben sie in die Spalte ausgewählt. Dann können Sie die Wiederholungsvergehen basierend auf identifizieren **Dateiname** Und **Dateibesitzer** Felder. Wenn ein Anwender den Schwellenwert für Wiederholungsverstöße (Anzahl der Verstöße und Dauer) verletzt und derselbe Anwender mit den DLP-Feldern übereinstimmt, wird dieser Anwender als Wiederholungsverstößer identifiziert.
Anzahl der Verstöße	Definieren Sie den Schwellenwert für wiederholte Straftäter. Nachdem der Anwender die gleichen Aktionen wiederholt und die angegebene Anzahl von Verstößen verletzt hat, wird der Anwender als wiederholter Straftäter identifiziert.
Dauer (in Tagen)	Definieren Sie den Schwellenwert für Wiederholungsvergehen in Form von Tagen. Nachdem der Anwender die gleichen Aktionen wiederholt und die Dauer des Schwellenwerts nicht eingehalten hat, wird er als wiederholter Täter identifiziert.

Identifizierung Von Wiederholungsverletzern



4. Klicken Sie auf **Absenden**.

Erstellen Sie Zusätzliche Incident-Datenfelder

Erstellen Sie Ihre zusätzlichen Incident-Datenfelder für die DLP-Incidents. Sie können verschiedene Arten zusätzlicher Incident-Datenfelder erstellen, z. B. Zeichenfolge, Zahl,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontrollkästchen, Auswahl, Datum und Uhrzeit, und verwenden Sie sie in den DLP-Incident-Formularen.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Wichtig:
Zusätzliche Incident-Datenfelder für DLP-Incidents werden nur in der San Diego-Version oder höher unterstützt.

Warum und wann dieser Vorgang ausgeführt wird

Zusätzliche Incident-Datenfelder sind Einschränkungen auf Feldebene zugeordnet. Wenn also Einschränkungen auf Feldebene bestehen, gelten sie für zusätzliche Incident-Datenfelder im DLP-Ops-Portal und im Endanwenderportal.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Zusätzliche Incident-Datenfelder**an.
2. Erstellen Sie zusätzliche Incident-Datenfelder, indem Sie auf klicken **Neu** .
3. Füllen Sie im Formular die Felder aus.

Formular „zusätzliche DLP-Incident-Datenfelder“

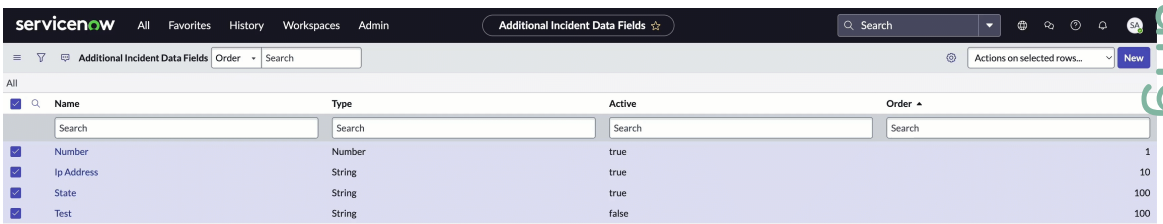
Feld	Beschreibung
Name	Name der zusätzlichen Incident-Datenfelder.
Typ	Option zum Auswählen des Typs zusätzlicher Incident-Datenfelder. Sie können einen der folgenden Typen auswählen: ○ **Zeichenfolge** ○ **Nummer** ○ **Checkbox** ○ **Auswahl** Wenn Sie die Felder zusätzliche Incident-Daten auswählen, geben Sie als ein **Auswahl** , Können Sie nach dem Erstellen der Felder „zusätzliche Incident-Daten“ die Auswahloptionen für zusätzliche Incident-Datenfelder definieren. So erstellen Sie eine zusätzliche Auswahloption für Incident-Datenfelder: **a.** Öffnen Sie die erforderlichen Felder „zusätzliche Incident-Daten“. **b.** Klicken Sie im Abschnitt „Feldoptionen für anwenderdefinierte Auswahl“ auf **Neu** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	c. Definieren Sie im Feld Optionsname den erforderlichen Optionsnamen. **d.** Klicken Sie auf **Absenden**. ○ **Datum** ○ **Datum/Uhrzeit** **Hinweis:** Nachdem Sie einen Typ für Ihre neuen Felder „zusätzliche Incident-Daten“ ausgewählt haben, dürfen Sie ihn nicht ändern. Wenn Sie den Typ ändern möchten, müssen Sie erneut neue Felder für zusätzliche Incident-Daten mit dem erforderlichen Typ erstellen.
Reihenfolge	Option zum Auswählen der Reihenfolge, in der die Felder „zusätzliche Incident-Daten“ angezeigt werden sollen. Sie können den Reihenfolgewert für jedes zusätzliche Incident-Datenfeld definieren. Die Felder „zusätzliche Incident-Daten“ werden basierend auf den von Ihnen definierten Reihenfolgenwerten sortiert. Standardmäßig werden die Felder „zusätzliche Incident-Daten“ in aufsteigender Reihenfolge sortiert. Sie können die Felder „zusätzliche Incident-Daten“ in absteigender Reihenfolge sortieren, indem Sie auf klicken **Reihenfolge** Spalte.
Aktiv	Option, um anzugeben, ob die Felder „zusätzliche Incident-Daten“ aktiv sind.
Beschreibung	Beschreibung für die von Ihnen erstellten zusätzlichen Incident-Datenfelder.

Zusätzliche DLP-Incident-Datenfelder



4. Klicken Sie auf **Absenden**.

Formular „DLP-SLA-Definition“

Feldbeschreibungen für das DLP-SLA-Definitionsformular, das zum Erstellen eines SLA-Datensatzes verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name der Definition.
Typ	Typ der Vereinbarung, in diesem Fall SLA.
Zielvorgabe	Ziel, das zum Filtern, Suchen und Reporting der zu definierenden Vereinbarung verwendet wird. Verfügbare Optionen: • Keine • Antwort • Lösung
Tabelle	Tabelle, die die vom SLA nachverfolgten Datensätze bestimmt, wobei es sich um die DLP-SLA-Aufgabe [sn_dlir_Incident_sla_Task] handeln sollte.
Flow	Flow, der ausgeführt werden soll, wenn die SLA-Definition an einen Aufgabendatensatz angehängt wird, der Standard-SLA-Flow sein sollte.
Dauertyp	Methode zur Berechnung der Dauer des SLA. Verfügbare Optionen: • Anwenderdefinierte Dauer • 2 Werktage bis 16:00 Uhr • 3 Werktage bis 16:00 Uhr • Verstoß am Fälligkeitsdatum • Ende des nächsten Geschäftstags • Nächster Geschäftstag bis 16:00 Uhr
Dauer	Dauer, die das SLA ausgeführt wird, bevor es als nicht eingehalten markiert wird. Dieses Feld ist nur verfügbar, wenn „Anwenderdefinierte Dauer“ aus ausgewählt ist **Dauertyp** .
Zeitplanquelle	Zeitplan, der beim Erstellen der Aufgaben-SLAs verwendet werden soll.
Zeitplan	Stunden, in denen der SLA-Timer ausgeführt wird. Dieser Satz von Zeitplänen ist in der Core-Konfiguration definiert.
Zeit Zonenquelle	Zeit Zonenquelle, die beim Erstellen von Aufgaben-SLAs verwendet werden soll. Verfügbare Optionen: • Die Zeitzone des Anrufers • Die Zeitzone der SLA-Definition • Die Zeitzone des CI-Standorts • Die Zeitzone des Aufgabenorts • Die Zeitzone des Anruferstandorts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Option, um den Auslöser wirksam zu machen, wenn die Startbedingung erfüllt ist.
Registerkarten	
Startbedingung	Bedingung, die den SLA-Timer initiiert und das SLA aktiviert.
Anhaltebedingung	Bedingungen, unter denen das SLA ausgesetzt wird, wodurch die insgesamt verstrichene Zeit erhöht wird.
Abbruchbedingung	Bedingungen, unter denen das SLA abgebrochen wird.
Rücksetzbedingung	Bedingungen, unter denen das aktive SLA abgeschlossen wird und ein neues SLA eingerichtet wird, wenn sich der Wert eines Felds im Aufgabendatensatz ändert oder in einen bestimmten Wert im Datensatz ändert. Sagen Sie zum Beispiel den Wert von **Standort** Das Feld im Aufgabendatensatz ist 101 Broadway East, Seattle, WA. Wenn Sie die SLA-Rücksetzbedingung auf festlegen **[Standort][Änderungen von][101 Broadway East, Seattle, WA]** , Jede Änderung des Werts von **Standort** Feld setzt das SLA des Aufgabendatensatzes zurück.

Zugehörige Informationen

Erstellen Sie einen Data Loss Prevention Incident Response SLA-Definition

Erweiterte Einstellungen konfigurieren

Konfigurieren Sie die erweiterten Einstellungen, damit Sie unter anderem die Felder im Incident zur Identifizierung der Endanwender bestimmen können.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Erweiterte Einstellungen für konfigurieren Data Loss Prevention Incident Response Ist optional. Einige erweiterte Einstellungen umfassen:

- Definieren Sie die maximale Anzahl von Incidents, die in einer Digest-E-Mail gesendet werden können.
- Aktivieren Sie den Schnellmodus, um E-Mails schneller zu senden.
- Bestimmen Sie die Protokollausführlichkeit der Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Erweiterte Einstellungen**an.
2. Füllen Sie im Formular die Felder aus.

Formular „Erweiterte Einstellungen“

Feld	Beschreibung
Sollen die vertraulichen Daten, die den Verstoß verursacht haben, im Incident angezeigt werden?	Option zum Auswählen, ob Sie die vertraulichen Daten anzeigen möchten, die den Verstoß für den DLP-Incident verursacht haben. Standardmäßig ist diese Option aktiviert.
Sollen die vertraulichen Daten, die den Verstoß verursacht haben, auch in den untergeordneten Incidents angezeigt werden?	Option zum Auswählen, ob Sie die vertraulichen Daten, die den Verstoß verursacht haben, auch für den untergeordneten DLP-Incident anzeigen möchten. Standardmäßig ist diese Option deaktiviert.
Liste der Felder im Incident, die zur Identifizierung des Endanwenders verwendet werden	Die Liste der Felder im Incident des Zuweisungsregel-Moduls, die zur Identifizierung des Endanwenders verwendet werden. Sie können auch eigene anwenderdefinierte Attribute angeben, um den Endanwender zu identifizieren.
Maximale Anzahl von Incidents in einer Digest-E-Mail	Die maximale Anzahl von Incidents, die in einer Digest-E-Mail gesendet werden können. Standardmäßig ist der Wert 100.
Maximale Dauer von Wiederholungsvergehen (in Tagen)	Die maximale Dauer zum Identifizieren eines Wiederholungsverbrechers. Standardmäßig beträgt der Wert 90 Tage.
Schnellmodus zum Senden von E-Mails	Option zum Validieren von E-Mails und Identifizieren von Problemen. Sie können die Validierung durchführen, indem Sie aktivieren **Ja** Option. Standardmäßig ist diese Option aktiviert.
Diese Eigenschaft wird verwendet, um die Protokollausführlichkeit der Anwendung festzulegen	Die Protokollausführlichkeitsstufe der Anwendung, d. h. der Name des Informationstyps. Sie können den Wert auch auf die folgenden Optionen aktualisieren: ○ **Fehler** ○ **warnen** ○ **Info** ○ **debuggen** Standardmäßig ist der Wert **Info** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Geklonte und untergeordnete Incidents aus Berichten ausschließen	Option zum Ausschließen der geklonten und untergeordneten Incidents aus den Berichten. Standardmäßig ist diese Option **Ja**.
Tage, die auf das Löschen von Übereinstimmungsinhalten im Cloud-Speicher gewartet werden, nachdem der Incident geschlossen wurde	Option zum Auswählen der Anzahl der Wartetage zum Bereinigen des Übereinstimmungsinhalts der Incidents, die für eine bestimmte Zeit inaktiv sind. Standardmäßig ist der Wert 90. Wenn der DLP-Incident nach 90 Tagen inaktiv ist, wird der Übereinstimmungsinhalt aus dem Cloud-Speicher bereinigt.
Incident nach der letzten Eskalationsstufe der DLP-Analystengruppe zuweisen	Aktivieren Sie dieses Kontrollkästchen, um den Incident nach der letzten Eskalationsstufe dem Analysten zuzuweisen.
Anwendern den Zugriff auf Incidents nach der Eskalation ermöglichen	Aktivieren Sie dieses Kontrollkästchen, damit die zugewiesenen Anwender nach der Eskalation auf die Incidents zugreifen können. Wenn Sie diese Option auswählen, können alle Anwender, die der Liste der Eskalationsketten hinzugefügt wurden, auf die Incidents zugreifen.
Zulassen, dass Analysten abgeschlossene Bewertungen bearbeiten	Aktivieren Sie dieses Kontrollkästchen, damit der Analyst die abgeschlossene Bewertung bearbeiten kann. Wenn Sie diese Option auswählen, können die Analysten die Bewertungen bearbeiten. Wenn diese Option deaktiviert ist, können Sie die Bewertungen im schreibgeschützten Modus anzeigen.
Vorschaueigenschaften für Nachweisdateien	
Durch Aktivieren dieser Systemeigenschaft wird die Vorschaufunktion für Nachweisdateien im DLP-Analystenarbeitsbereich aktiviert. sn_dlir.enable_evidence_file_preview	Option, um auszuwählen, ob Sie eine Vorschau der Nachweisdateien direkt im Arbeitsbereich anzeigen möchten. Standardmäßig ist diese Option **Ja**.
Dadurch können DLP-Anwender die in der Vorschau angezeigten Nachweisdateien herunterladen. Sobald diese Eigenschaft aktiviert ist, sehen Anwender im Dokument-Viewer eine Download-Schaltfläche, um die Nachweisdatei herunterzuladen. sn_dlir.enable_Download in_preview	Option zum Auswählen, ob die Schaltfläche „Herunterladen“ im Dokument-Viewer angezeigt werden soll, mit der Sie die in der Vorschau angezeigten Nachweisdateien herunterladen können. Standardmäßig ist diese Option **Ja**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Diese Eigenschaft bestimmt die Dauer, für die Dateien vorübergehend für Vorschauzwecke von Nachweisdateien aufbewahrt werden. (In Minuten) sn_dlir.preview_temp_files_cleanup_interval	Die maximale Dauer, für die Dateien vorübergehend für die Vorschau der Nachweisdatei gespeichert werden. Standardmäßig ist der Wert 10. Wenn der DLP-Incident nach 10 Minuten inaktiv ist, wird die Nachweisdatei aus dem Arbeitsbereich des Analysten bereinigt.
Durch Aktivieren dieser Eigenschaft wird das Bereinigungsintervall verlängert, wenn Nachweisdateien verwendet werden. Dadurch kann das System die Ablaufzeit von Nachweisdateien basierend auf dem in der Systemeigenschaft „sn_dlir.preview_temp_files_cleanup_interval“ festgelegten Wert verlängern. sn_dlir.extend_Cleanup_interval_on_usage	Option zum verlängern der Zeit vor dem Löschen von Nachweisdateien, wenn sie verwendet werden. Standardmäßig ist diese Option **Ja** .
Die maximale Dauer für die Verlängerung des Bereinigungsintervalls von Nachweisdateien (in Minuten). sn_dlir.max_Extension_duration_for_cleanup	Option zum Auswählen, wie lange das System Ihre Nachweisdateien in Minuten speichert, bevor sie bereinigt werden. Standardmäßig ist der Wert 60.

3. Klicken Sie auf **Speichern**.

Überwachen Sie den DLP-Integrationsausführungsprozess

Verfolgen und überwachen Sie die laufende Erfassung oder den Integrationsausführungsprozess. Die Integrationsausführungsprozesse enthalten die Statistiken darüber, wie viel die Daten verarbeitet wurden, und den Integrationsstatus.

Erforderliche Rolle: sn_dlir.admin.

Der Integrationsausführungsprozess listet die Details dazu auf, wie viele Datensätze erfasst werden. Zum Beispiel:

1. In der Symantec-Integration enthält der Prozess sowohl untergeordnete als auch übergeordnete Integrationsausführungen. Der übergeordnete Datensatz gibt die Erfassungsdaten an, und der untergeordnete Datensatz gibt die Ergänzungsaufrufe und anwenderdefinierten Attributdatensätze an.
2. In der Microsoft-Integration kann nur der übergeordnete Datensatzerfassungsprozess ausgeführt werden.

DLP-Integrationsausführungsprozesse : Zeigt die Warteschlangeneinträge, den Status von Warteschlangeneinträgen und abgerufene Datensätze an.

Die Integrationsausführung enthält die Quelle, für die das Integrationsprofil und der Integrationsausführungsdatensatz erstellt werden, Profilabfrageintervalle, erfassungsstatus und -Substatus, die Incident-Anzahl, die die Anzahl der erfassten Datensätze angibt.

1. Navigieren zu **DLP-Administration** > **Integrationsausführungen**an.
2. Wählen Sie die Integrationsausführung aus der Liste aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Navigieren Sie zu **DLP-Integrationsausführungsprozess** .
4. Zeigen Sie den Status des Warteschlangeneintrags des Datensatzes an.

Zugriffsbeschränkungen für DLP-Incidents

Verwalten Sie die Sichtbarkeit eines bestimmten DLP-Incidents, der vertrauliche Informationen enthält. Sie können Zugriffsbeschränkungen für Incidents verwenden, um zu definieren, wer auf einen bestimmten DLP-Incident zugreifen kann, und um den Zugriff bestimmter Anwender oder Gruppen auf diesen Incident zu beschränken.

Erstellen Sie Einschränkungen auf Feldebene

Legen Sie Einschränkungen auf Feldebene in DLP-Incidents fest, um vertrauliche Informationen vor Offenlegung zu schützen. Sie können Einschränkungen auf Feldebene verwenden, um die Anwender oder Gruppen zu steuern, die auf bestimmte Felder in DLP-Incidents zugreifen können.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Einschränkungen auf Feldebene ermöglichen es Ihnen, nur bestimmte Felder für bestimmte Anwender oder Gruppen anzuzeigen, was eine detailliertere Möglichkeit zur Steuerung der Daten bietet, auf die ein Anwender zugreifen kann. Sie können eine Einschränkung auf Feldebene erstellen, indem Sie die entsprechenden Bedingungen für DLP-Incidents definieren, die Anwender oder Gruppen auswählen, für die diese Bedingungen gelten, und dann die DLP-Felder auswählen, die diese Anwender oder Gruppen anzeigen können.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Incident-Zugriffsbeschränkungen** > **Einschränkungen auf Feldebene**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „Einschränkung auf DLP-Feldebene“

Feld	Beschreibung
Name	Name der Einschränkung auf Feldebene.
Aktiv	Option, um anzugeben, ob die Einschränkung auf Feldebene aktiv ist.
Ausführungsreihenfolge	Priorität der Einschränkungen auf Feldebene. Dieses Feld gibt die Reihenfolge an, in der die Einschränkungen auf Feldebene ausgeführt werden, wenn zwei oder mehr Einschränkungen auf Feldebene die auslösenden Bedingungen teilen. Die Einschränkung auf Feldebene mit der niedrigsten Zahl hat die höchste Priorität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

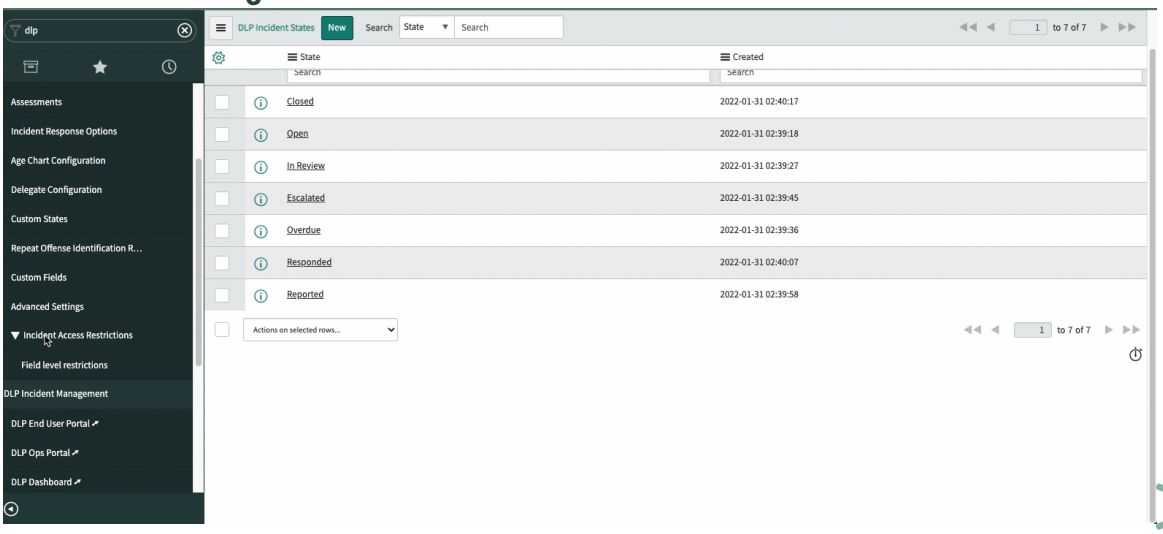
Feld	Beschreibung
	Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Zum Beispiel 100, 200 oder eine andere Nummer. Der Standardwert ist 100.
Kurzbeschreibung	Eindeutige Beschreibung für diese Einschränkung auf Feldebene.
Incident-Übereinstimmungsbedingung	Optionen im Incident, die den definierten Bedingungen entsprechen. Sie können jedes der Incident-Felder auswählen, um die Auslöserbedingung für die Einschränkungen auf Feldebene zu definieren. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER**: ○ Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. Sie können das Feld beispielsweise als auswählen `Richtlinienname` Und legen Sie die Bedingung als fest `In`, Und `Name der Richtlinie`. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden.
Betrifft	Option zum Anwenden der Incident-Übereinstimmungsbedingungen auf bestimmte Anwender oder Gruppen. Sie können die Bedingungen auf Folgendes anwenden: ○ **Alle Endanwender**: Option zum Auswählen aller Endanwender, für die die DLP-Incident-Bedingungen gelten. ○ **Alle Prüfer eskalierter Incidents**: Option zum Auswählen aller Überprüfer von eskalierten Incidents, für die die DLP-Incident-Bedingungen gelten. Dies bezieht sich auf alle DLP-Incidents, die an den Manager eskaliert wurden. ○ **Anwender**: Klicken Sie auf Symbol zum Hinzufügen eines bestimmten Anwenders aus der Liste, für den die DLP-Incident-Bedingungen gelten. Sie können einen Anwender auch mithilfe seiner E-Mail-Adresse oder der Suchoption hinzufügen. Beispiel: Legal Manager. Um sich selbst als Anwender hinzuzufügen, für den die DLP-Bedingungen gelten, klicken Sie auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Gruppen** : Klicken Sie auf Symbol zum Hinzufügen einer bestimmten Gruppe aus der Liste, für die die DLP-Incident-Bedingungen gelten. Sie können auch eine Gruppe mithilfe der Suchoption hinzufügen. Zum Beispiel Umfrageersteller.
Nur Zugriff auf folgende Felder zulassen	○ **DLP-Felder** : Option zum Definieren der DLP-Felder, die den Zugriff auf die ausgewählten Anwender oder Gruppen zulassen sollen. Wählen Sie die DLP-Felder aus, auf die Sie Zugriff zulassen möchten, aus der Spalte verfügbar aus, und verschieben Sie sie in die Spalte ausgewählt. **Hinweis:** Die ausgewählten Anwender oder Gruppen können nur auf die ausgewählten DLP-Felder zugreifen. Sie können beispielsweise auswählen **Zugewiesen an** Und **Geöffnet** Felder aus der Spalte verfügbar und verschieben sie in die Spalte ausgewählt. Dann haben die ausgewählten Anwender oder Gruppen nur Zugriff auf die Felder Zugewiesen an und geöffnet. ○ **Anhänge hochladen** : Option, um anzugeben, ob Sie den ausgewählten Anwendern oder Gruppen das Hochladen von Anhängen erlauben möchten. ○ **Anwenderdefinierte Felder** : Option zum Definieren der anwenderdefinierten Felder, die den Zugriff auf die ausgewählten Anwender oder Gruppen zulassen sollen. Sie können die anwenderdefinierten Felder anzeigen, die Sie in der Spalte verfügbar erstellt haben. Wählen Sie die anwenderdefinierten Felder aus, auf die Sie Zugriff zulassen möchten, aus der Spalte verfügbar aus, und verschieben Sie sie in die Spalte ausgewählt. **Wichtig:** ▪ Anwenderdefinierte Felder für DLP-Incidents werden nur in der San Diego-Version oder höher unterstützt. ▪ Die ausgewählten Anwender oder Gruppen können nur auf die ausgewählten anwenderdefinierten Felder zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DLP-Einschränkung auf Feldebene



4. Klicken Sie auf **Absenden**.

Erstellen Sie Einschränkungen auf Datensatzebene

Legen Sie Einschränkungen auf Datensatzebene in DLP-Incidents fest, um vertrauliche Datensätze vor der Offenlegung zu schützen. Sie können Einschränkungen auf Datensatzebene verwenden, um die Anwender oder Gruppen zu steuern, die auf bestimmte Datensätze in den DLP-Incidents zugreifen können.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin: Erstellen, bearbeiten und löschen.
- sn_dlir.Analyst und sn_dlir.Analyst_read – Ansicht (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Einschränkungen auf Datensatzebene ermöglichen es Ihnen, nur für bestimmte Anwender oder Gruppen Zugriff auf Datensätze zu gewähren und so die Datensätze, auf die ein Anwender zugreifen kann, genauer zu steuern. Sie können eine Einschränkung auf Datensatzebene erstellen, indem Sie die Bedingungen für den DLP-Incident definieren, die Anwender oder Gruppen auswählen, für die diese Bedingungen gelten, und dann die DLP-Datensätze auswählen, die diese Anwender oder Gruppen anzeigen können.

Prozedur

1. Navigieren zu **Alle** > **DLP-Administration** > **Incident-Zugriffsbeschränkungen** > **Einschränkungen auf Datensatzebene**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Formular „Einschränkung auf DLP-Datensatzebene“

Feld	Beschreibung
Name	Name der Einschränkung auf Datensatzebene.
Kurzbeschreibung	Eindeutige Beschreibung für diese Einschränkung auf Datensatzebene.

Automatische Übersetzung

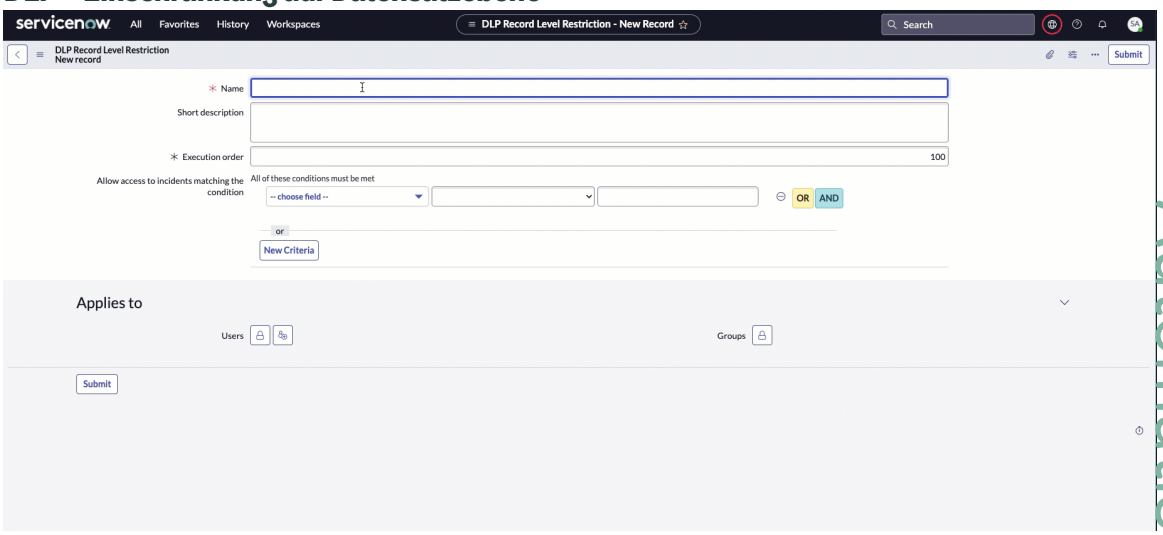
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ausführungsreihenfolge	Priorität der Einschränkungen auf Datensatzebene. Dieses Feld gibt die Reihenfolge an, in der die Einschränkungen auf Datensatzebene ausgeführt werden, wenn zwei oder mehr Einschränkungen auf Datensatzebene die auslösenden Bedingungen teilen. Die Einschränkung auf Datensatzebene mit der niedrigsten Zahl hat die höchste Priorität. Geben Sie einen Wert ein, um die Reihenfolge des Vorgangs festzulegen. Zum Beispiel 100, 200 oder eine andere Nummer. Der Standardwert ist 100.
Gewähren Sie Zugriff auf Incidents, die der Bedingung entsprechen	Optionen ermöglichen den Zugriff auf die Incidents, die den definierten Bedingungen entsprechen. Sie können eines der Incident-Felder auswählen, um die Auslöserbedingung für die Einschränkungen auf Datensatzebene zu definieren. Verwenden Sie die Listen und Felder des Bedingungsgenerators, um die Filter für die erste Zeile festzulegen. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER**: ○ Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. ○ Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. Um eine zweite Filterbedingung festzulegen, klicken Sie auf **Neue Kriterien**. **Hinweis:** Bei den Bedingungen im Bedingungsgenerator wird zwischen Groß- und Kleinschreibung unterschieden. Sie können das Feld beispielsweise als auswählen `Aktiv` Und legen Sie die Bedingung als fest `Ist`, Und `Wahr`.
Betrifft	Option zum Anwenden von Einschränkungen auf Datensatzebene auf bestimmte Anwender oder Gruppen. Sie können die Bedingungen wie folgt anwenden: ○ **Anwender**: Klicken Sie auf Symbol zum Hinzufügen eines bestimmten Anwenders aus der Liste, für den der ausgewählte Datensatz gilt. Sie können einen Anwender auch mithilfe seiner E-Mail-Adresse oder der Suchoption hinzufügen. Beispiel: Legal Manager. Um sich selbst als Anwender hinzuzufügen, für den der Datensatz gilt, klicken Sie auf . Beispiel: Systemadministrator.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ **Gruppen** : Klicken Sie auf Symbol zum Hinzufügen einer bestimmten Gruppe aus der Liste, für die der ausgewählte Datensatz gilt. Sie können auch eine Gruppe mithilfe der Suchoption hinzufügen. Zum Beispiel Umfrageersteller.

DLP – Einschränkung auf Datensatzebene



4. Klicken Sie auf **Absenden**.

Archivierung von DLP-Incidents

Die Data Loss Prevention Incident Response Wird mit einer Archivierungsregel im Basissystem für die DLP-Incident-Tabelle bereitgestellt. Die zugehörigen Datensätze werden auch im Basissystem der DLP-Incident-Archivregel hinzugefügt.

Vorbereitungen

Erforderliche Rolle: Administrator

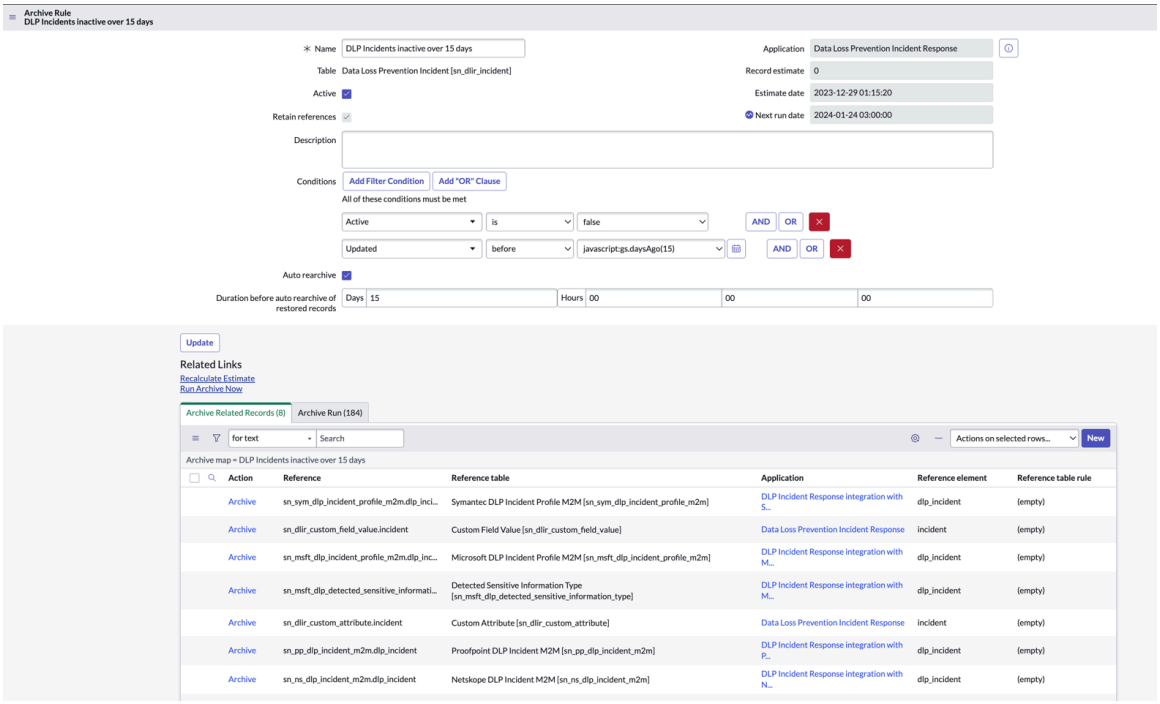
Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivregeln**an.
   Die Systemarchivierungsregeln im Basissystem werden angezeigt.
2. Zeigen Sie die DLP-Archivierungsregel an.

Hinweis:
DLP-Incidents, die über 15 Tage inaktiv sind Ist die standardmäßige Basissystemarchivierungsregel für DLP-Incidents, können Sie die Archivierungsregel bei Bedarf ändern. Diese Regel bedeutet, dass Incidents, die länger als 15 Tage inaktiv sind, automatisch archiviert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Informationen zum Erstellen der Archivierungsregeln finden Sie unter Erstellen Sie eine Archivregel .

3. **Aktualisieren** Die Regel, falls erforderlich.

Archivieren Sie DLP-bezogene Datensätze

Verwenden Sie die zugehörige Liste zugehörige Datensätze archivieren für DLP-Incidents, um die zugehörigen Datensätze der Archivregel hinzuzufügen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemarchivierung** > **Archivregeln**an.
2. Wählen Sie Aus **DLP-Incidents, die über 15 Tage inaktiv sind** Archivierungsregel.
3. Wechseln Sie zu **Zugehörige Datensätze Archivieren** Zugehörige Liste.
4. Zeigen Sie die zugehörigen DLP-Datensätze an.

Anwendung	Referenztabelle
Integration von DLP Incident Response mit Symantec	Symantec DLP-Incident-Profil M2M [sn_sym_dlp_Incident_Profile_m2m]
Reaktion auf Incident zur Vermeidung von Datenverlust	Anwenderdefinierter Feldwert [sn_dlir_custom_field_value]
Integration von DLP Incident Response mit Microsoft	Microsoft DLP-Incident-Profil M2M [sn_msft_dlp_Incident_Profile_m2m]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung	Referenztabelle
Integration von DLP Incident Response mit Microsoft	Typ der erkannten sensiblen Informationen [sn_msft_dlp_detected_sensitive_Information_type]
Reaktion auf Incident zur Vermeidung von Datenverlust	Anwenderdefiniertes Attribut [sn_dlir_custom_Attribute]
Integration von DLP Incident Response mit Proofpoint	Proofpoint-DLP-Incident M2M [sn_PP_dlp_Incident_m2m]
DLP Incident Response integration with Netskope	Netskope-DLP-Incident M2M [sn_ns_dlp_Incident_m2m]
Integration von DLP Incident Response mit Symantec	Typ der erkannten sensiblen Informationen [sn_sym_dlp_detected_sensitive_Information_type]

Hinweis:
Alle Systemtabellen wie E-Mails, Bewertungen, Anhänge werden automatisch an den archivierten DLP-Datensatz weitergeleitet.

5. Wählen Sie die Archivbezogene Datensatzregel aus, die Sie archivieren möchten.

Hinweis:
Weitere Informationen zum Hinzufügen weiterer zugehöriger Datensätze finden Sie unter Archivieren Sie DLP-bezogene Datensätze Ein ServiceNow AI Platform.

Data Loss Prevention Incident Response Incident-Management

Verwenden Sie Data Loss Prevention Incident Response Incident-Management zum Aktualisieren und Verwalten von Incidents durch Nutzung des DLP-Anwenderarbeitsbereichs, des DLP-Analystenarbeitsbereichs und des DLP-Dashboards.

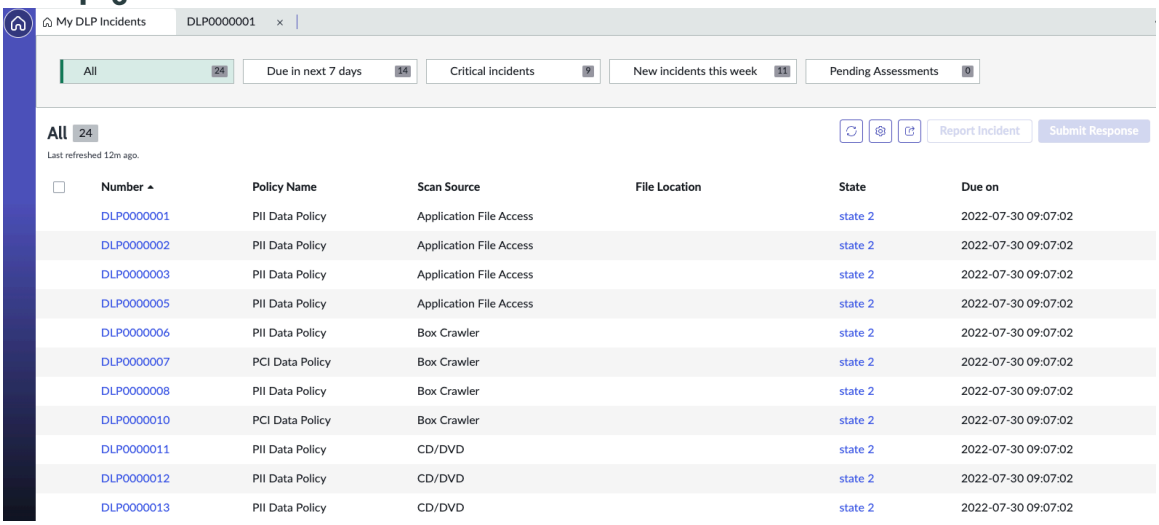
Data Loss Prevention Incident Response Anwenderarbeitsbereich

Die Data Loss Prevention Incident Response(DLP IR) Anwenderarbeitsbereich ist ein Arbeitsbereich, in dem Endanwender, Manager und Genehmiger auf die zugewiesenen DLP-Incidents reagieren können. Endanwender, Manager und Genehmiger können dann auf die Incidents reagieren, indem sie die richtigen Aktionen angeben.

Sie können auch Bewertungen erstellen und verwalten, damit Endanwender auf DLP-Incidents reagieren können. Der Arbeitsbereich besteht aus einer Zielseite und Listenansichten, in denen Sie die zugewiesenen DLP-Incidents anzeigen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Homepage des DLP-Anwenderarbeitsbereichs



Melden Sie DLP-Incidents, oder reagieren Sie darauf

Greifen Sie auf zu Data Loss Prevention Incident Response(DLP) Anwenderarbeitsbereich, überprüfen Sie die zugewiesenen DLP-Incidents, und melden Sie die Incidents, oder reagieren Sie darauf.

Vorbereitungen

Erforderliche Rolle:

- Jeder gültige Anwender/Mitarbeiter

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Anwenderarbeitsbereich**an.
   Die Seite meine DLP-Incidents wird in einer neuen Registerkarte geöffnet.
2. Klicken Sie auf eine Listenansicht, um die Ihnen zugewiesenen Incidents zu überprüfen.

Listenansicht	Beschreibung
Alle	Zeigen Sie alle zugewiesenen Incidents an.
In den nächsten 7 Tagen fällig	Zeigen Sie alle Incidents an, die in den nächsten 7 Tagen fällig sind.
Kritische Incidents	Zeigen Sie alle Incidents mit der Schweregradbezeichnung Kritisch an.
Neue Incidents diese Woche	Zeigen Sie alle Incidents an, die diese Woche zugewiesen wurden.
Ausstehende Bewertungen	Zeigen Sie alle Bewertungen an, die noch ausstehen.

3. Sie können die DLP-Incidents auf zwei Arten überprüfen:

   a. Die erste Möglichkeit besteht darin, einen oder mehrere DLP-Incidents zu suchen und auszuwählen, die Sie überprüfen möchten, und klicken Sie auf das Kontrollkästchen neben den Incidents.

   b. Wählen Sie die Option aus, die für Sie geeignet ist.

Automatische Übersetzung

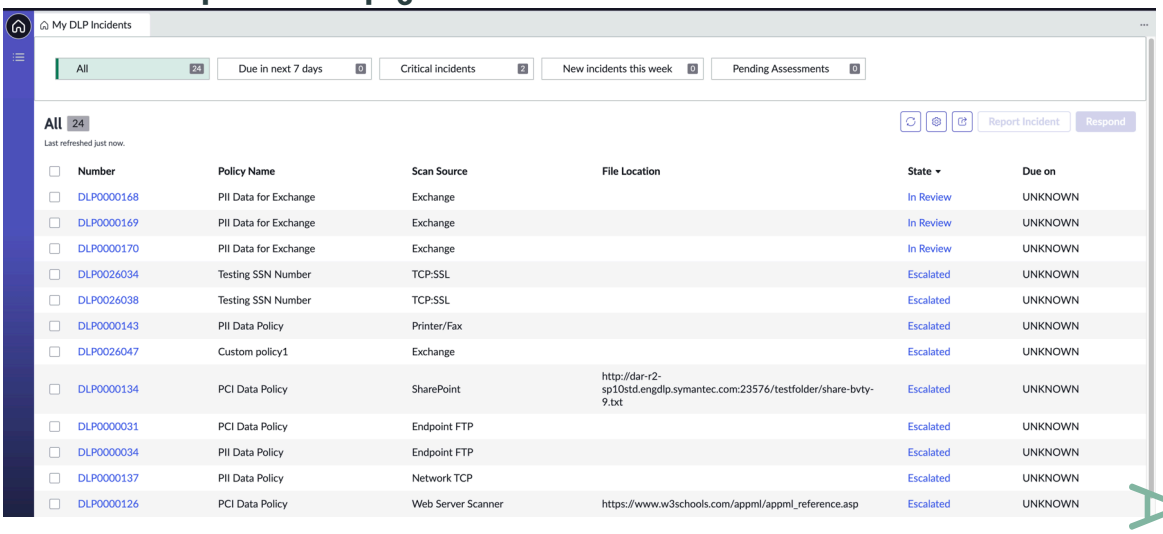
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Homepage des DLP-Endanwenderportals

Option	Beschreibung
Liste neu laden	Option zum Aktualisieren der Liste der DLP-Incidents, wenn Sie eine Aktualisierung vorgenommen haben.
Listenaktionen	Liste der Aktionen, die Sie ausführen können. Die Auswahlmöglichkeiten lauten wie folgt: ▪ **Speichern unter** ▪ **Spalten bearbeiten** ▪ **Breiten zurücksetzen** **Hinweis:** Wenn Sie über eine eigene anwenderdefinierte Liste verfügen, die unter erstellt wird **Meine Listen** Für Ihren Arbeitsbereich konfigurierter Abschnitt können Sie auch die folgenden zusätzlichen Listenaktionen ausführen: ▪ **Umbenennen** ▪ **Speichern** ▪ **Löschen**
URL für alle kopieren	Option zum Kopieren der URLs aller DLP-Incidents.
Incident melden	Aktion zum Melden des Incident als falsch positiv oder falsch Besitzer. Sie können beispielsweise einen falschen Besitzer melden und einen anderen Besitzer vorschlagen oder den Incident als falsch positiv melden.
Beantworten	Reagieren Sie auf einen Incident, indem Sie eine Option für die Reaktion auf Incidents auswählen. Wenn der Anwender beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann er die Option auswählen **Datei Gelöscht** Um eine manuelle Bestätigung zu übermitteln, dass die Datei gelöscht wurde, und Kommentare einzugeben. Hier können Sie auch erweiterte Antwortoptionen auswählen. Beispiel: **E-Mail-Freigabe aus Quarantäne anfordern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DLP-Anwenderportal-Homepage



c. Die zweite Möglichkeit besteht darin, auf einen bestimmten DLP-Incident zu klicken, um ihn zu öffnen. Die **Details** Auf der Registerkarte werden die folgenden Abschnitte angezeigt:

- Details : Sie können die Details des DLP-Incidents anzeigen, z. B. Incident-Nummer, Schweregrad, Dateiname.
- Verfassen : Um Kommentare zum DLP-Incident hinzuzufügen, der für alle sichtbar ist, geben Sie die Kommentare auf der Registerkarte Kommentare ein. Um Kommentare hinzuzufügen, die für bestimmte Personen sichtbar sind, geben Sie die Kommentare auf der Registerkarte Arbeitsnotizen (privat) ein.
- Aktivität : Sie können die Details der verschiedenen Aktivitäten für den DLP-Incident anzeigen.
- Anhänge : Wenn Sie Anhänge im Zusammenhang mit dem DLP-Incident haben, klicken Sie auf **Durchsuchen** Und wählen Sie den Anhang auf Ihrem lokalen Laufwerk aus.

  Die **Zusätzliche Details** Auf der Registerkarte werden alle zusätzlichen Informationen zum DLP-Incident einschließlich anwenderdefinierter Felder angezeigt.

  Wichtig:

  - Anwenderdefinierte Felder für DLP-Incidents werden nur in der San Diego-Version oder höher unterstützt.
  - Wenn für einen bestimmten DLP-Incident Daten anwenderdefinierter Felder verfügbar sind, können Sie sie unter anzeigen **Zusätzliche Details** Registerkarte. Wenn für den DLP-Incident keine anwenderdefinierten Felder vorhanden sind, wird eine leere Seite angezeigt.

- **Typ Der Erkannten Sensiblen Informationen** : Zeigt die erkannten vertraulichen Informationen des Incidents an.

  Hinweis:
  Diese zugehörige Liste ist nur für DLP-Incidents sichtbar, die für Microsoft- oder Symantec-Integrationen erstellt wurden. Wenn der Anwender im Microsoft- oder Symantec-Incident-Datensatz auf den erkannten Datensatz vom Typ „vertrauliche Informationen“ zugreift, wird der hervorgehobene Übereinstimmungsinhalt in Bezug auf diese Integration angezeigt.

d. Wählen Sie die Option aus, die für Sie geeignet ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

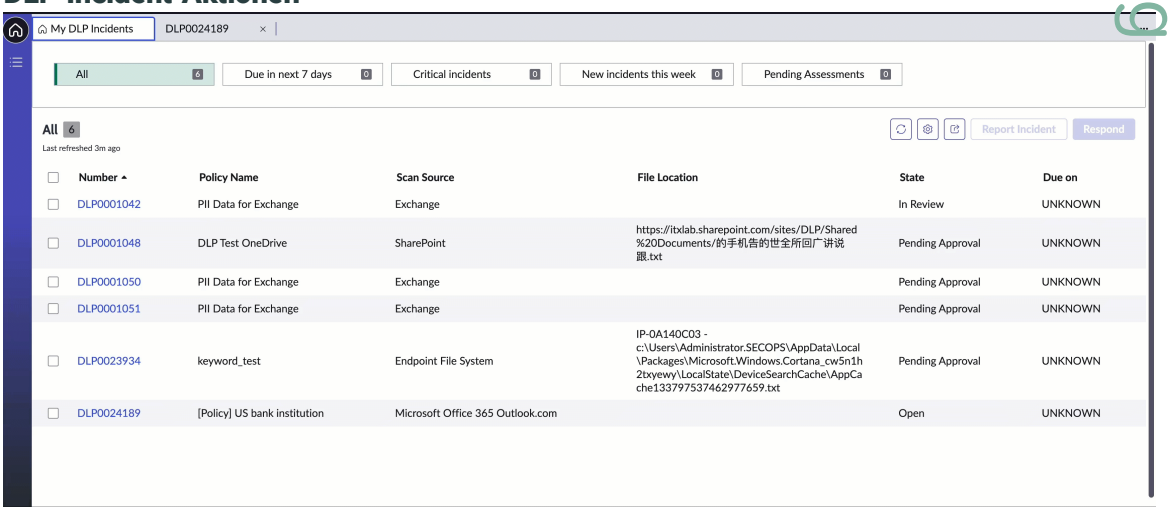
Option	Beschreibung
Falsch positives Ergebnis melden	Aktion, um zu melden, dass der DLP-Incident falsch ausgelöst oder erstellt wurde. Sie können im Feld Kommentare die Details dazu angeben, warum Sie den Incident als falsch positiv markiert haben.
Falschen Besitzer melden	Aktion zum Melden, dass der DLP-Incident dem falschen Anwender zugewiesen wurde. Wenn Sie den richtigen Besitzer für den Incident kennen, können Sie den Namen des Besitzers im Feld Vorschlagen des Besitzers auswählen. Um zusätzliche Details hinzuzufügen, verwenden Sie das Feld Kommentare.
Beantworten	Reagieren Sie auf einen Incident, indem Sie eine Option für die Reaktion auf Incidents auswählen. Wenn der Anwender beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann er die Option auswählen **Datei Gelöscht** Um eine manuelle Bestätigung zu übermitteln, dass die Datei gelöscht wurde, und Kommentare einzugeben. Hier können Sie auch erweiterte Antwortoptionen auswählen. Beispiel: **E-Mail-Freigabe aus Quarantäne anfordern** .

e. Wählen Sie aus **Antworten Sie** Schaltfläche nach Beantwortung der Analystenabfrage.
Ein Popup-Fenster zum Senden einer Incident-Antwort wird angezeigt. Wählen Sie die Antwort aus dem Dropdown-Menü aus, und fügen Sie Kommentare hinzu.

f. Wählen Sie **Absenden**.
Ein Banner wird angezeigt, das bestätigt, dass Ihre Antwort erfolgreich übermittelt wurde.

Hinweis:
Der Incident wird dem entsprechenden Genehmiger oder Analysten zugewiesen, und der Endanwender verliert den Zugriff auf den Incident.

DLP-Incident-Aktionen



Automatische Übersetzung

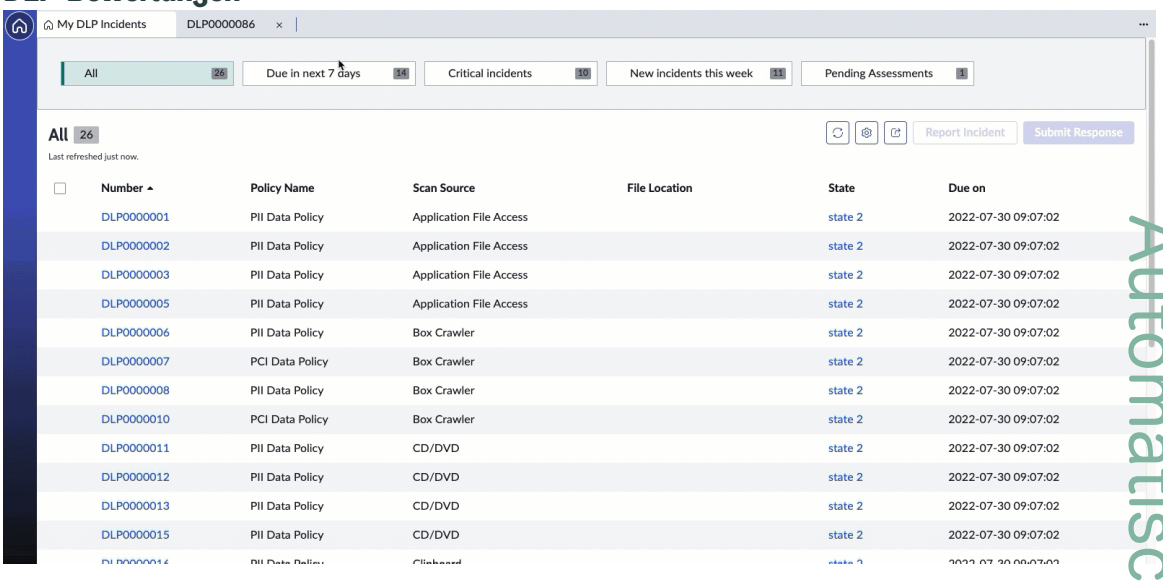
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Um Bewertungen vorzunehmen, wählen Sie aus **Ausstehende Bewertungen** Listenansicht.

   a. Klicken Sie auf eine bestimmte Bewertungsnummer, um sie zu öffnen.

   b. Beantworten Sie die Bewertungsfragen, und klicken Sie auf **Speichern** Oder **Übermitteln** Basierend auf Ihren Anforderungen.

DLP-Bewertungen



5. Klicken Sie auf **Anweisungen** Kartenabschnitt, der über allen Feldern in der Formularansicht „DLP-Incident“ angezeigt wird, um zusätzliche Informationen zu einem bestimmten Incident anzuzeigen.

Hinweis:
Dieser Abschnitt im Arbeitsbereich führt die Anwender zu den Incident-Informationen, die helfen, die nächsten Schritte der Incident-Lösung zu verstehen.

Die Karte „Anwenderanweisungen“ zeigt zwei verschiedene Header an, die Ihnen weitere Informationen zu einem bestimmten Incident in der Formularansicht bieten. Klicken Sie auf einen beliebigen Header für Anwenderanweisungen, um die zusätzlichen Details anzuzeigen.

Weitere Informationen finden Sie unter Erstellen Sie Vorlagen für Anwenderanweisungen und Konfigurieren Sie DLP-UI-Anwenderanweisungen.

Mit Modul „meine Genehmigungen“ arbeiten

Das Modul „meine Genehmigungen“ ist für angemeldete Anwender im DLP-Anwenderarbeitsbereich verfügbar. Anwender können die Genehmigungsanforderungen von hier aus genehmigen oder ablehnen.

Vorbereitungen

Erforderliche Rolle:

- Endanwender
- Manager
- Genehmigende Person

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Anwenderarbeitsbereich**an.
   Die **Meine DLP-Incidents** Seite wird auf einer neuen Registerkarte angezeigt.
2. Klicken Sie auf **Meine Genehmigungen** Modul unter vorhanden **Meine DLP-Incidents** Modul.
   Die Listenansicht „meine Genehmigungen“ wird angezeigt.

   Der Genehmiger kann die Anforderungen in der Listenansicht von genehmigen oder ablehnen **Meine Genehmigungen** Seite. In der Listenansicht können Sie mehrere Anforderungen genehmigen oder ablehnen.

   Genehmiger können die Details der zugewiesenen Anforderung in der Formularansicht anzeigen. Indem Sie auf klicken **Genehmigen** Oder **Ablehnen** Aktion in der Formularansicht kann die einzelne Anforderung genehmigt oder abgelehnt werden.

Hinweis:

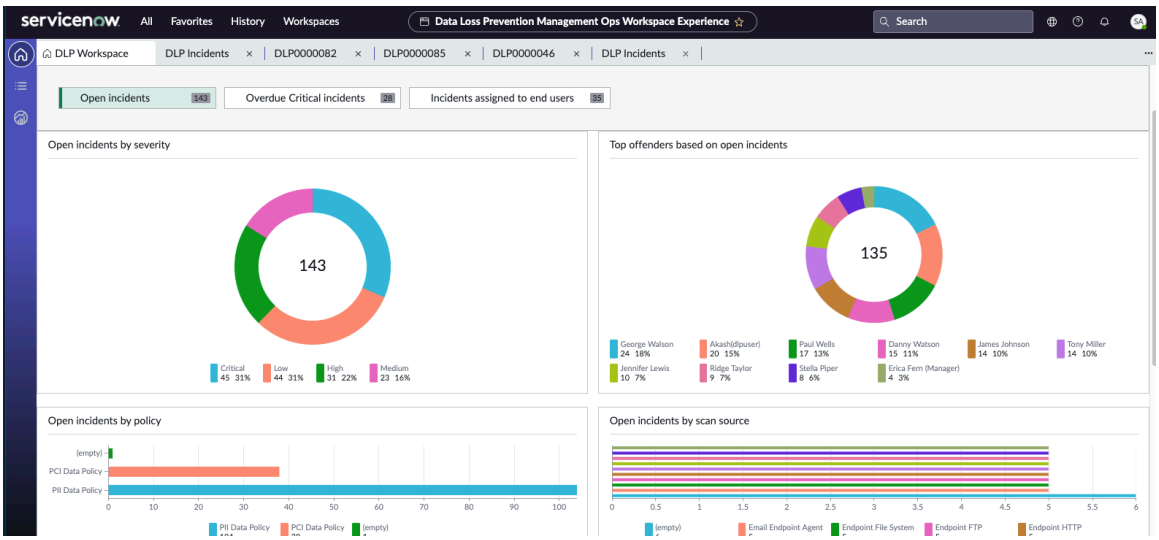
Klicken Sie auf , um die DLP-Incident-Details anzuzeigen Info-Symbol im verfügbar **Genehmigen** Feld.

Data Loss Prevention Incident Response Arbeitsbereich Für Analysten

Verwenden Sie Data Loss Prevention Incident Response(DLP IR) Arbeitsbereich für Analysten zum Anzeigen der DLP-Incidents. Weisen Sie die Incidents Endanwendern zur Lösung und mehr zu.

Der DLP-Arbeitsbereich besteht aus einer Homepage mit Dashboards, Listenansichten und Formularansichten, auf denen Sie DLP-Incidents überwachen können.

DLP-Arbeitsbereich – Übersichtsseite



Überprüfen und weisen Sie Ihre DLP-Incidents zu

Greifen Sie auf zu Data Loss Prevention Incident Response(DLP IR) Arbeitsbereich für Analysten, damit Sie die DLP-Incidents überprüfen und zuweisen oder lösen können. Sie können Trends bei Incidents nach Schweregrad, häufigsten Tätern, Incidents nach Scan-Quelle und Incidents nach Richtlinie nachverfolgen.

Homepage des DLP-Arbeitsbereichs

DLP-Arbeitsbereichsübersicht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.Analyst: Bearbeiten und zeigen Sie DLP-Incidents an.
- sn_dlir.Analyst_read und sn_dlir.read: Zeigen Sie DLP-Incidents an.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
   Die Listenseite „DLP-Arbeitsbereich – meine Incidents – Vorgänge“ wird in einer neuen Registerkarte geöffnet.
2. Klicken Sie auf **DLP-Arbeitsbereich** Startsymbol zum Anzeigen der Homepage-Ansicht des Arbeitsbereichs.
3. Überprüfen Sie die Dashboard-Widgets, um Trends nach Incidents nach Schweregrad, häufigste Täter, Incidents nach Scan-Quelle und Incidents nach Richtlinie zu identifizieren.
4. Klicken Sie auf der Homepage auf die entsprechenden Filter, um die Widgets nach ihren verschiedenen Kategorien anzuzeigen.

Filter	Beschreibung
Offene Incidents	Zeigen Sie alle offenen Incidents an.
Überfällige kritische Incidents	Zeigen Sie die Incidents mit der Schweregradbezeichnung „Kritisch“ an, die überfällig sind.
Endanwendern zugewiesene Incidents	Zeigen Sie die Incidents an, die Endanwendern zugewiesen sind.

5. Sie können die DLP-Incidents auf zwei Arten überprüfen und zuweisen:

   a. Die erste Möglichkeit besteht darin, einen oder mehrere DLP-Incidents zu suchen und auszuwählen, die Sie überprüfen möchten, und klicken Sie auf das Kontrollkästchen neben den Incidents.

   b. Wählen Sie die Option aus, die für Sie geeignet ist.

Option	Beschreibung
Liste neu laden	Option zum Aktualisieren der Liste der DLP-Incidents, wenn Sie eine Aktualisierung vornehmen.
Listenaktionen	Liste der Aktionen, die Sie ausführen können. Die Auswahlmöglichkeiten lauten wie folgt: ▪ **Speichern unter** ▪ **Spalten bearbeiten** ▪ **Breiten zurücksetzen**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Hinweis: Wenn Sie über eine eigene anwenderdefinierte Liste verfügen, die unter erstellt wird **Meine Listen** Für Ihren Arbeitsbereich konfigurierter Abschnitt können Sie auch die folgenden zusätzlichen Listenaktionen ausführen: ▪ **Umbenennen** ▪ **Speichern** ▪ **Löschen**
URL für alle kopieren	Option zum Kopieren der URLs aller DLP-Incidents.
Filterbereich anzeigen	Option zum Drilldown der erforderlichen Incidents mithilfe der Filteroption. **i.** Klicken Sie auf den Filter oben links auf der Seite, und wählen Sie aus **Erweiterte Ansicht** . **ii.** Verwenden Sie einen vorhandenen Filter, oder erstellen Sie einen eigenen, indem Sie Bedingungen hinzufügen, die ein Feld, einen Operator und Werte enthalten. **iii.** Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** Oder **ODER** : ▪ Wenn **UND** Ist ausgewählt, müssen alle Bedingungen erfüllt sein. ▪ Wenn **ODER** Ist ausgewählt, kann eine der Bedingungen erfüllt werden. **iv.** Klicken Sie auf **Aktualisieren**.
Incident zuweisen	Aktion, um zu bestimmen, wem der DLP-Incident zugewiesen werden soll. Die Auswahlmöglichkeiten lauten wie folgt: ▪ **Incident zuweisen zu** : Option zum Zuweisen des Incident an einen Analyst, Endanwender oder eine andere Person. ▪ **Anwender** : Option, um zu bestimmen, welchem Anwender der Incident zugewiesen werden soll. ▪ **Voranwenderantwort für Incident-Status** : Option, um zu bestimmen, in welchem Status sich der Incident befinden soll, bevor der Anwender antwortet. Es kann auch ein anwenderdefinierter Status sein. ▪ **Bewertung anhängen** : Option, um anzugeben, ob Sie dem Incident eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Bewertung anhängen möchten. Wenn diese Option aktiviert ist, sind die folgenden Optionen verfügbar: ▪ **Bewertungsvorlage** : Option zum Auswählen einer Bewertungsvorlage für den DLP-Incident. ▪ **Incident-Status nach Anwenderantwort** Option zum Auswählen des Status, in dem sich der DLP-Incident befinden soll, nachdem der Anwender geantwortet hat.
Beantworten	Reagieren Sie auf einen Incident, indem Sie eine Option für die Reaktion auf Incidents auswählen. Wenn der Anwender beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann er die Option auswählen **Datei Gelöscht** Um eine manuelle Bestätigung zu übermitteln, dass die Datei gelöscht wurde, und Kommentare einzugeben. Hier können Sie auch erweiterte Antwortoptionen auswählen. Beispiel: **E-Mail-Freigabe aus Quarantäne anfordern** .
Eskalation	Aktion zur Eskalation des Incident. Sie können den Incident eskalieren, indem Sie den Anwender auswählen, an den Sie ihn eskalieren möchten. Sie können auch zusätzliche Informationen im Feld Kommentare anzeigen.
Status aktualisieren	Aktion zum Aktualisieren des Status des Incident. Sie können den Status des Incident aktualisieren, indem Sie einen der status aus den Dropdown-Optionen auswählen. Es kann auch ein anwenderdefinierter Status sein.
Schließen	Aktion zum Schließen der Incidents. Wählen Sie die entsprechende aus **Abschlusscode** Aus der Dropdown-Liste und fügen Sie Abschlusskommentare hinzu. Die **Schließen** Funktion in Data Loss Prevention Incident Response Wird sowohl asynchron als auch synchron in der Listenansicht ausgeführt. **i.** Synchroner Abschluss: Wenn Incidents synchron geschlossen werden, bedeutet dies, dass die Abschlussaktion sofort ausgeführt wird. Wenn Sie mehrere Incidents zum Abschluss auswählen und die Incident-Anzahl kleiner oder gleich 100 ist, werden die Incidents in der Listenansicht „DLP-Incidents“ im

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Vordergrund geschlossen. Hier ist 100 der Standardwert. **ii.** Asynchroner Abschluss: Dies bedeutet, dass die Abschlussanforderung übermittelt wird und die Anwendung die Anforderung im Hintergrund ausführt, wenn die Anzahl der ausgewählten Incidents größer als 100 ist. Sie müssen die Listenansicht „DLP-Incidents“ aktualisieren, um den Status der aktualisierten Incidents anzuzeigen. **Hinweis:** ▪ Die Anzahl der ausgewählten Incidents für den asynchronen oder synchronen Abschluss wird mit der Systemeigenschaft konfiguriert `sn_dlir.closure_Sync_count_limit` . ▪ Standardmäßig ist die Incident-Anzahl auf 100 festgelegt.

c. Die zweite Möglichkeit besteht darin, auf einen bestimmten DLP-Incident zu klicken, um ihn zu öffnen.

- **Details** Registerkarte: Zeigt die folgenden Abschnitte an:
  - **Details** : Sie können die Details des DLP-Incidents anzeigen, z. B. Incident-Nummer, Schweregrad, Dateiname usw. Sie haben auch die Möglichkeit, die Felder Schweregrad, Status, Endanwender und DLP-Analystengruppe zu ändern und zu speichern.
  - **Verfassen** : Um Kommentare zum DLP-Incident hinzuzufügen, der für alle sichtbar ist, geben Sie die Kommentare auf der Registerkarte Kommentare ein. Um Kommentare hinzuzufügen, die für bestimmte Personen sichtbar sind, geben Sie die Kommentare auf der Registerkarte Arbeitsnotizen (privat) ein.
  - **Aktivität** : Sie können die Details der verschiedenen Aktivitäten für den DLP-Incident anzeigen.
  - **Anhänge** : Wenn Sie Anhänge im Zusammenhang mit dem DLP-Incident haben, klicken Sie auf **Durchsuchen** Und wählen Sie den Anhang auf Ihrem lokalen Laufwerk aus.
- **Zusätzliche Details** Registerkarte: Zeigt alle zusätzlichen Informationen zum DLP-Incident an, einschließlich anwenderdefinierter Felder.

Wichtig:

- Anwenderdefinierte Felder für DLP-Incidents werden nur in der San Diego-Version oder höher unterstützt.
- Sie können verwenden **Zusätzliche Details** Registerkarte, um zu sehen, ob anwenderdefinierte Felder für einen bestimmten DLP-Incident erstellt wurden oder nicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Anwenderdefinierte Attribute** Registerkarte: Zeigt die Liste der anwenderdefinierten Attribute im Zusammenhang mit dem DLP-Incident an.
- **Andere Incidents vom Endanwender** : Zeigt den Incident desselben Endanwenders an. Sie können Incidents konsolidieren, indem Sie ausführen **Als untergeordneten Incident hinzufügen** Aktion aus dieser zugehörigen Liste.
- **Typ der erkannten sensiblen Informationen** : Zeigt die erkannten vertraulichen Informationen des Incidents an.

> **Hinweis:**
> Diese zugehörige Liste ist nur für DLP-Incidents sichtbar, die für Microsoft- oder Symantec-Integrationen erstellt wurden. Wenn der Anwender im Microsoft- oder Symantec-Incident-Datensatz auf den erkannten Datensatz vom Typ „vertrauliche Informationen“ zugreift, wird der hervorgehobene Übereinstimmungsinhalt in Bezug auf diese Integration angezeigt.

- **Untergeordnete Incidents** : Zeigt die untergeordneten Incidents an, die manuell (durch Ausführen der Aktion „als untergeordneten Incident hinzufügen“) oder über die DLP-Konsolidierungsregeln erstellt wurden. Sie können die Verknüpfung des untergeordneten Incidents aufheben, indem Sie in dieser zugehörigen Liste „Verknüpfung des untergeordneten Incidents aufheben“ ausführen.
- **Geklonte Incidents** : Zeigt die geklonten Incidents aus dem übergeordneten Incident an. Indem Sie auf klicken **Incident klonen** Aktion der Formularansicht können Sie einen neuen geklonten Incident erstellen.
- **Bewertungen** Registerkarte: Zeigt die Liste der Bewertungen an, die dem DLP-Incident zugewiesen sind.

d. Wählen Sie die Option aus, die für Sie geeignet ist.

Option	Beschreibung
Incident zuweisen	Aktion, um zu bestimmen, wem der DLP-Incident zugewiesen werden soll. Die Auswahlmöglichkeiten lauten wie folgt: ▪ **Incident zuweisen zu** : Option zum Zuweisen des Incident an einen Analyst, Endanwender oder eine andere Person. ▪ **Anwender** : Option zum Auswählen, welchem Anwender der Incident zugewiesen werden soll. ▪ **Voranwenderantwort für Incident-Status** : Option zum Auswählen des Status, in dem sich der Incident befinden soll, bevor der Anwender antwortet. Es kann auch ein anwenderdefinierter Status sein. ▪ **Bewertung anhängen** : Option, um anzugeben, ob Sie dem Incident eine Bewertung anhängen möchten. Wenn diese Option aktiviert ist, sind die folgenden Optionen verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	▪ **Bewertungsvorlage** : Option zum Auswählen einer Bewertungsvorlage für den DLP-Incident. ▪ **Incident-Status nach Anwenderantwort** : Option zum Auswählen des Status, in dem sich der DLP-Incident befinden soll, nachdem der Anwender geantwortet hat.
Genehmigung abbrechen	Aktion zum Abbrechen der Genehmigungsanforderung. Diese Aktion ist für Analysten in der Formularansicht nur sichtbar, wenn sich der DLP-Incident in befindet **Genehmigung Ausstehend** status. Verfügbare Optionen: ▪ **Incident zuweisen zu** : Option, den Incident niemandem, einem Analysten oder einer anderen Person zuzuweisen. ▪ **Anwender** : Option zum Auswählen, welchem Anwender der Incident zugewiesen werden soll. ▪ **Incident-Status nach Abbruch** : Option zum Auswählen des Status, in dem sich der Incident nach dem Abbrechen der Anforderung befinden soll. ▪ **Kommentare** : Zur Angabe zusätzlicher Details für die Stornierung.
Bewertung zuweisen	Aktion zum Anhängen einer Bewertung beim Zuweisen des Incident. Auswahlmöglichkeiten: ▪ **Bewertungsvorlage** : Option zum Auswählen einer Bewertungsvorlage für den DLP-Incident. ▪ **Incident-Status nach Anwenderantwort** : Option zum Auswählen des Status, in dem sich der DLP-Incident befinden soll, nachdem der Anwender geantwortet hat.
Datei herunterladen	Aktion zum Herunterladen der Datei oder E-Mail mit dem verstoßenden Inhalt. Diese Aktion kann für Incidents ausgeführt werden, die für Microsoft OneDrive, SharePoint Online oder Exchange Online erstellt wurden.
Speichern	Aktion zum Speichern aller von Ihnen vorgenommenen Änderungen. Sie haben die Möglichkeit, die Felder Schweregrad, Status und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Endanwender des DLP-Incidents zu ändern und zu speichern.
Beantworten	Reagieren Sie auf einen Incident, indem Sie eine Option für die Reaktion auf Incidents auswählen. Wenn der Anwender beispielsweise eine Datei löscht, die gegen eine DLP-Richtlinie verstößt, kann er die Option auswählen **Datei Gelöscht** Um eine manuelle Bestätigung zu übermitteln, dass die Datei gelöscht wurde, und Kommentare einzugeben. Hier können Sie auch die erweiterten Antwortoptionen auswählen. **Beispiel: E-Mail-Freigabe aus Quarantäne anfordern** .
Eskalation	Aktion zur Eskalation des Incident. Sie können den Incident eskalieren, indem Sie den Anwender auswählen, an den Sie ihn eskalieren möchten. Sie können auch zusätzliche Informationen im Feld Kommentare anzeigen.
Incident klonen	Aktion zum Erstellen eines Klon-Incidents, wenn sich der Incident-Datensatz auf mehrere Anwender auswirkt. Sie können die geklonten Incidents mehreren Stakeholdern wie der Rechtsabteilung/IT zuweisen. Nachdem Sie einen Klon-Incident-Datensatz erstellt haben, einen neuen **Geklonte Incidents** Die Registerkarte wird unter dem übergeordneten DLP-Incident erstellt, und alle geklonten Incidents werden in dieser Ansicht aufgelistet.

Automatische Übersetzung

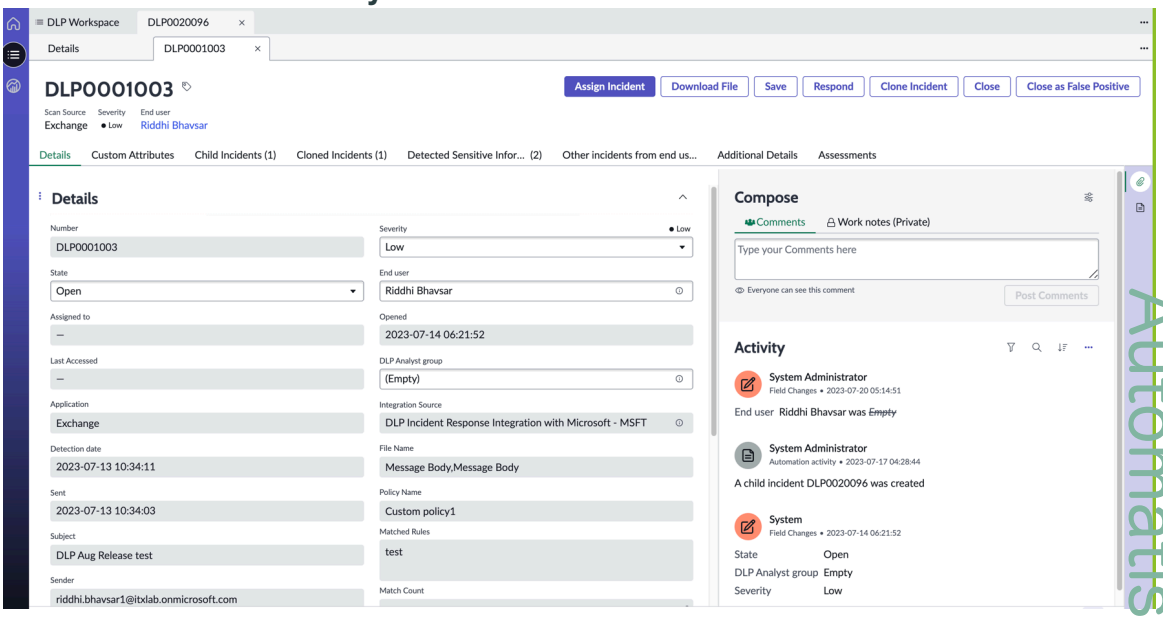
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Hinweis: ▪ Wenn der übergeordnete DLP-Incident-Datensatz geschlossen wird, werden alle geklonten Incident-Datensätze automatisch geschlossen. ▪ Wenn ein DLP-Incident-Datensatz einen geklonten Incident enthält, kann er Endanwendern nicht zugewiesen werden. Die übergeordneten DLP-Incident-Datensätze können nur von Anwendern mit der Rolle „Analyst“ verwaltet werden. ▪ Sie haben auch die Möglichkeit, den übergeordneten Status basierend auf dem Status der geklonten Incidents im Modul „Standardkonfiguration“ automatisch zu aktualisieren. Wenn beispielsweise alle geklonten Incidents in den Status „eskaliert“ verschoben werden, wird der übergeordnete Incident auch in den Status „eskaliert“ verschoben.
Schließen	Aktion zum Schließen des Incident. Sie müssen die entsprechende auswählen **Abschlusscode** Aus der Dropdown-Liste, und fügen Sie bei Bedarf Abschlusskommentare hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
Als falsch positiv schließen	Aktion zum Schließen des Incident als falsch positiv. Sie können auch zusätzliche Kommentare hinzufügen, bevor Sie den Incident schließen.

DLP-Arbeitsbereich für Analysten



6. Sie können die Listenansicht auf der Homepage anzeigen, indem Sie oben links auf der Seite wechseln und auf klicken **Listen** Registerkarte.
   Die Kategorie Listen besteht aus den standardmäßigen und anwenderdefinierten Listenseiten für DLP-Incidents.
   - **Listen** Registerkarte : Standardlisten für DLP-Incidents. Im Folgenden finden Sie die Standardlisten:
     - Alle
     - Öffnen
     - Meine Incidents
     - Meiner Gruppe zugewiesen
     - Eskaliert
     - Überfällig
     - Ausstehende Bewertungen
     - Anwenderaktion ausstehend
     - Geklonte Incidents
     - Archivierte Incidents
   - **Meine Listen** Registerkarte : Zeigt alle Listen an, die Sie umbenannt haben, und alle von Ihnen erstellten Listen.

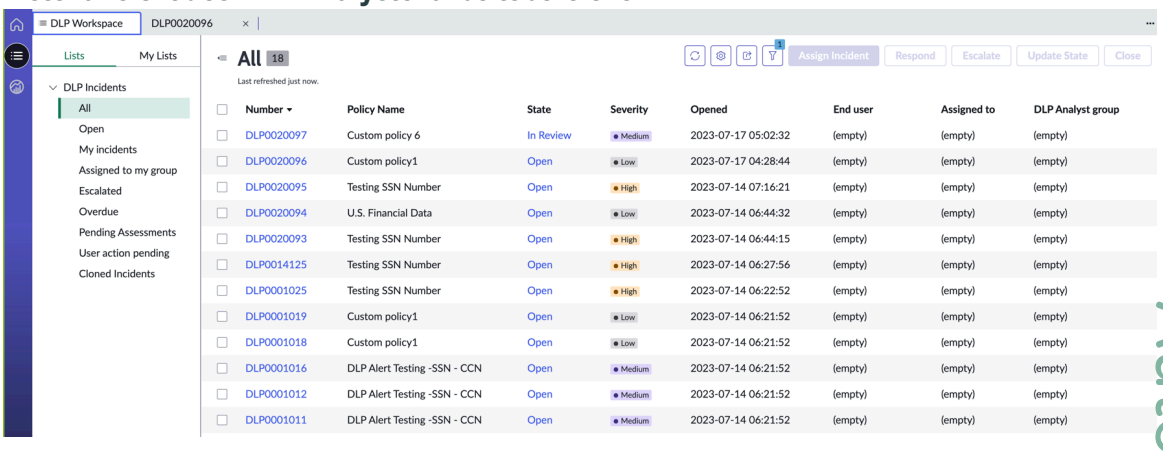
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example

Das folgende Beispiel zeigt den DLP-Arbeitsbereich mit den Listenansichtskategorien. Die **Alle** Listenansichtsoption ist ausgewählt.

Listenansicht des DLP-Analystenarbeitsbereichs



Vorschau der Nachweisdateien anzeigen

Vorschau Data Loss Prevention Incident Response Nachweisdateien im DLP-IR-Analyst-Arbeitsbereich.

Vorbereitungen

Wichtig:
Bei der Verwendung der Aktion „Nachweisdateien“ im DLP-Analysten-Arbeitsbereich werden die Nachweisdateien vorübergehend in der ServiceNow-Datenbank in einem unverschlüsselten Format gespeichert. Wenn Sie die Nachweisdateien nicht speichern möchten, deaktivieren Sie die Vorschaufunktion für Nachweisdateien. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Erforderliche Rolle: sn_dlir.Analyst

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
2. Öffnen Sie einen DLP-Incident-Datensatz.
3. Wählen Sie in der kontextbezogenen Sidebar das Symbol für Nachweisdateien ( ).
4. Auf der **Nachweisdateien** Wählen Sie die Registerkarte aus **Nachweisdatei** Karte zur Vorschau der Nachweisdateien im Dokument-Viewer.

   Die Vorschaufunktion unterscheidet sich für jeden Dateityp, wie in der folgenden Tabelle aufgeführt.

Dateiformat	Dateierweiterung
Bild	.Bmp, .gif, .ico, .JPEG, .jpg, .png, .svg und .webp. Bilddateien werden im Dokument-Viewer-Modus geöffnet.
Microsoft Office-Dateien	.Doc, .docx, .ppt, .pptx, .xls, und .xlsx

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateiformat	Dateierweiterung
	Office-Dateien werden im Dokument-Viewer-Modus geöffnet.
Textdateien	.txt Textdateien werden im Texteditor-Modus geöffnet.
E-Mail-Dateien	.Eml **Hinweis:** Die Dateigröße muss weniger als 5 MB betragen. Sie müssen zuerst die Datei herunterladen, um eine Vorschau des Inhalts anzuzeigen.
PDF-Dateien	.PDF ○ Geben Sie ein Stichwort ein, um das Dokument zu durchsuchen. ○ Zoom- und Verkleinerungsfunktionen, um die Ansicht für eine bessere Lesbarkeit anzupassen. ○ Drehen Sie die Seite im Uhrzeigersinn oder gegen den Uhrzeigersinn, um den Inhalt klarer anzuzeigen.

Hinweis:

Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion „Vorschaunachweisdatei“ funktioniert auch für archivierte Incidents.

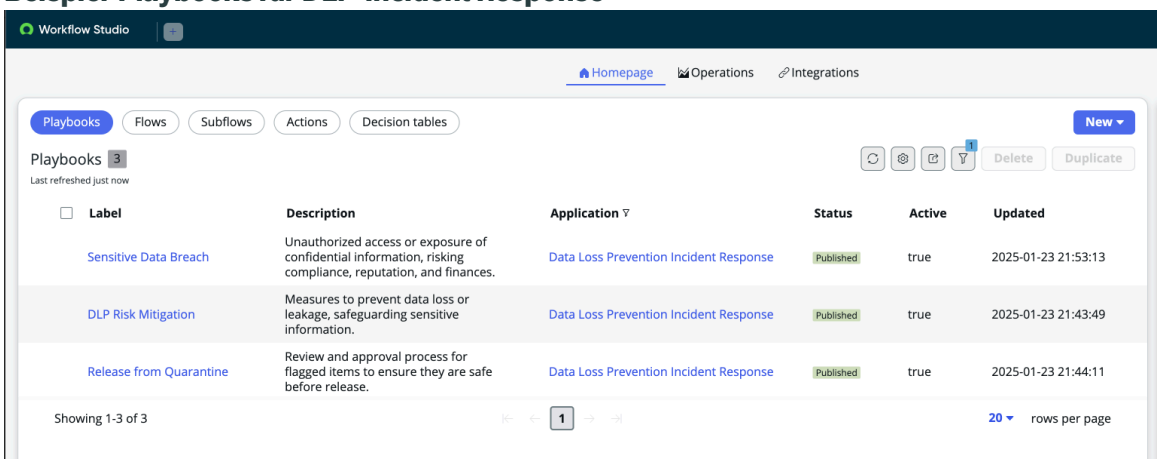
Playbook für Data Loss Prevention Incident Response

A Data Loss Prevention Incident Response Playbook ist eine Schritt-für-Schritt-Anleitung für die Behandlung und Minderung von Incidents mit Datenverlust, die nicht autorisierte Risiken, Leaks oder Verstöße gegen vertrauliche Informationen umfassen können, die die Sicherheit Ihrer Organisation gefährden können.

Die folgende Abbildung zeigt die Beispiel-Playbooks, die für DLP IR verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel-Playbooks für DLP-Incident Response



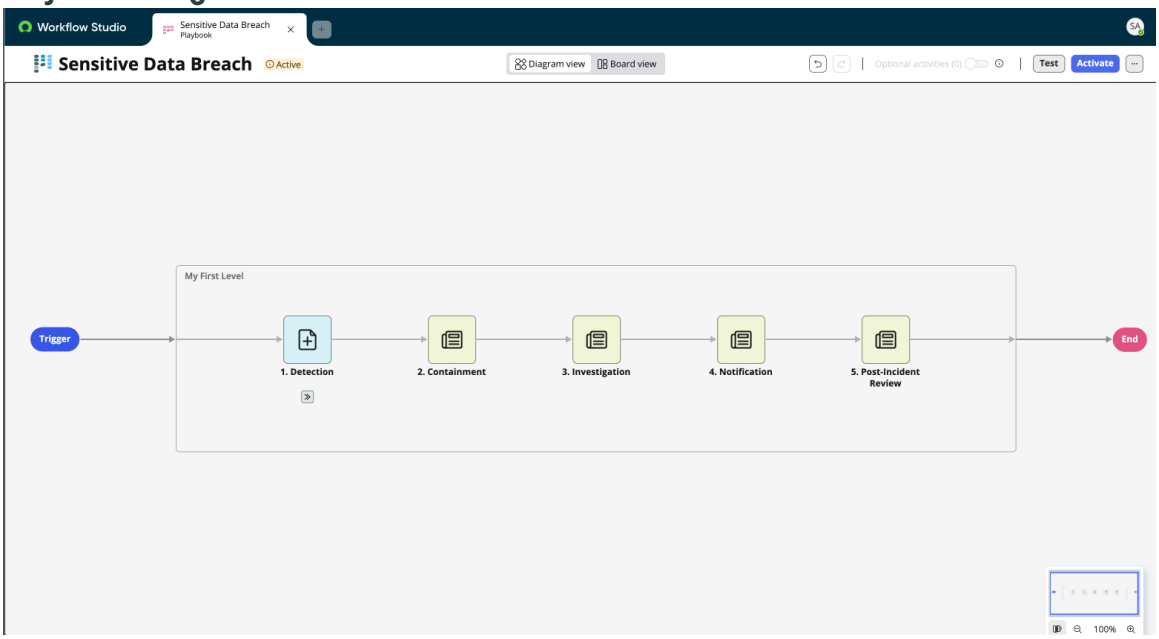
In der folgenden Tabelle sind die Aktivitäten und Phasen aufgeführt, die zum Erstellen eines DLP-Playbooks verfügbar sind. Weitere Informationen finden Sie unter Fügen Sie ein DLP-Playbook hinzu:

Aktivität	Beschreibung
Erkennung	Identifizieren und bestätigen Sie den nicht autorisierten Zugriff oder die Offenlegung vertraulicher Daten.
Aufnahme	Isolieren Sie betroffene Systeme oder Anwender, um weitere Datenverluste oder nicht autorisierten Zugriff zu verhindern.
Ermittlung	Untersuchen Sie den Verstoß, um zu verstehen, wie er aufgetreten ist, welche Daten betroffen waren und welche potenziellen Auswirkungen er hat.
Benachrichtigung	Benachrichtigen Sie interne Teams, externe Stakeholder und Aufsichtsbehörden gemäß den gesetzlichen oder richtlinienrechtlichen Anforderungen.
Korrektur	Wenden Sie Korrekturmaßnahmen an, um Schwachstellen zu beheben, Richtlinien zu aktualisieren und zukünftige Verstöße zu verhindern.
Wiederherstellung	Stellen Sie Systeme aus sicheren Sicherungen wieder her, und validieren Sie die Integrität der Daten nach dem Incident.
Überprüfung Nach Incident	Analysieren Sie den Incident, um Ursachen zu identifizieren, Sicherheitskontrollen zu verbessern und Richtlinien zu stärken.

Die folgende Abbildung zeigt den Workflow von Aktivitäten und Phasen, die an der Erstellung des Playbooks für Verstöße gegen sensible Daten beteiligt sind. Playbook-Schritte variieren je nach Workflow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Playbook-Design-Workflow



Zugehörige Informationen

Fügen Sie ein DLP-Playbook hinzu

Brechen Sie ein DLP-Playbook ab

Fügen Sie ein DLP-Playbook hinzu

Fügen Sie ein Playbook in hinzu Data Loss Prevention Incident Response Arbeitsbereich für Analysten, der als Leitfaden für die Behandlung und Minderung von Incidents mit Datenverlust fungieren kann, die die Sicherheit Ihres Unternehmens gefährden können.

Vorbereitungen

Erforderliche Rolle: sn_dlir.Analyst – fügen Sie Playbooks im DLP-Arbeitsbereich hinzu oder zeigen Sie sie an.

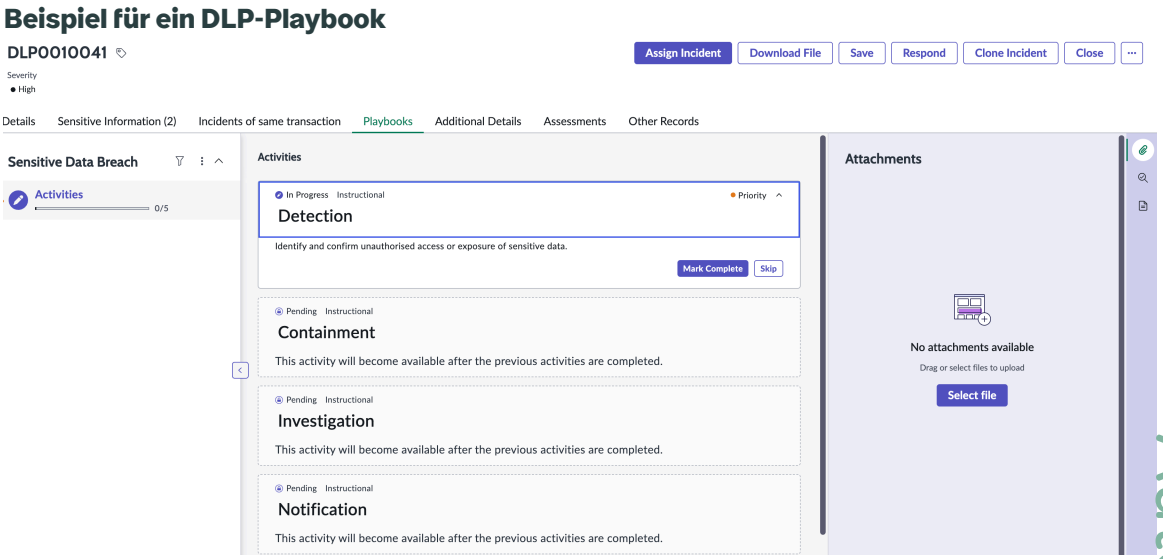
Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
2. Öffnen Sie auf der Seite „DLP-Analysten-Arbeitsbereich – meine Incidents“ einen beliebigen DLP-Incident.
3. Fügen Sie das Playbook hinzu.
   a. Navigieren Sie zu **Playbooks** Registerkarte.
   b. Wählen Sie im Menü „UI-Aktionen“ das Symbol „weitere Aktionen“ ( ) Und wählen Sie aus **Fügen Sie Playbooks Hinzu** .
   c. Wählen Sie im Dialogfeld ein Playbook aus dem Dropdown-Menü aus.
   d. Wählen Sie Aus **Fügen Sie Playbooks Hinzu** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie jede Spalte aus, um die Aufgaben zu erkunden, die dieses Playbook ausführt.



Brechen Sie ein DLP-Playbook ab

Brechen Sie einen ab Data Loss Prevention Incident Response Playbook zum Anhalten eines Business-Flows, wenn er nicht mehr gültig ist.

Vorbereitungen

Hinweis:
Playbooks werden automatisch abgebrochen, wenn der zugehörige DLP-Incident geschlossen wird.

Erforderliche Rolle: sn_dlir.admin.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
2. Öffnen Sie einen beliebigen DLP-Incident.
3. Navigieren Sie zu **Playbooks** Registerkarte.
4. Wählen Sie im Header des Playbooks, das Sie abbrechen möchten, das Symbol für Playbook-Aktionen (⋮) Und dann auswählen **Playbook Abbrechen** .
5. Geben Sie einen Grund für den Abbruch des Playbooks an.
6. Wählen Sie Aus **Playbook Abbrechen** .

Ergebnisse

Unter dem Playbook-Header wird ein Banner angezeigt, das bestätigt, dass das Playbook abgebrochen wurde.

Zeigen Sie archivierte DLP-Incidents an

Verwenden Sie den DLP-Analysten-Arbeitsbereich, um die archivierten DLP-Incidents anzuzeigen

Vorbereitungen

Erforderliche Rolle:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_dlir.Analyst: Bearbeiten und zeigen Sie DLP-Incidents an.
- sn_dlir.Analyst_read und sn_dlir.read: Zeigen Sie DLP-Incidents an.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
   Standardmäßig wird der Abschnitt „meine Incidents“ angezeigt.
2. Klicken Sie Auf **Archivierte Incidents** .
   Die Liste archivierter DLP-Incidents wird angezeigt.
3. Klicken Sie Auf **Incident-Anzahl Anzeigen** Schaltfläche zum Anzeigen der Anzahl der archivierten Incidents.

   Hinweis:

   - Standardmäßig ist die Anzahl der archivierten Incidents ausgeblendet, um die Ladezeit der Liste zu verbessern. Sie müssen auf klicken **Incident-Anzahl Anzeigen** Schaltfläche zum Anzeigen der Incident-Anzahl. Außerdem wird eine Informationsnachricht angezeigt, die die Anzahl der Incidents anzeigt.
   - Die Systemeigenschaft glide.ui.list.seismic.omit.count ist im Basissystem für die archivierten Incidents aktiviert, um die Incident-Listenanzahl auszublenden.

4. Wählen Sie einen oder mehrere DLP-Incidents aus, die Sie anzeigen möchten.
   Der DLP-Incident zeigt den Abschnitt „Incident-Details“ an.

   Hinweis:

   - Die **Andere Incidents von Endanwendern** Die Registerkarte enthält auch die archivierten Incidents.
   - **Inhalt Abgleichen** Wird für alle archivierten Incidents unterstützt (was auch in allen Integrationen unterstützt wird), aber **Datei herunterladen** Wird nur für Microsoft-Integrationen unterstützt.

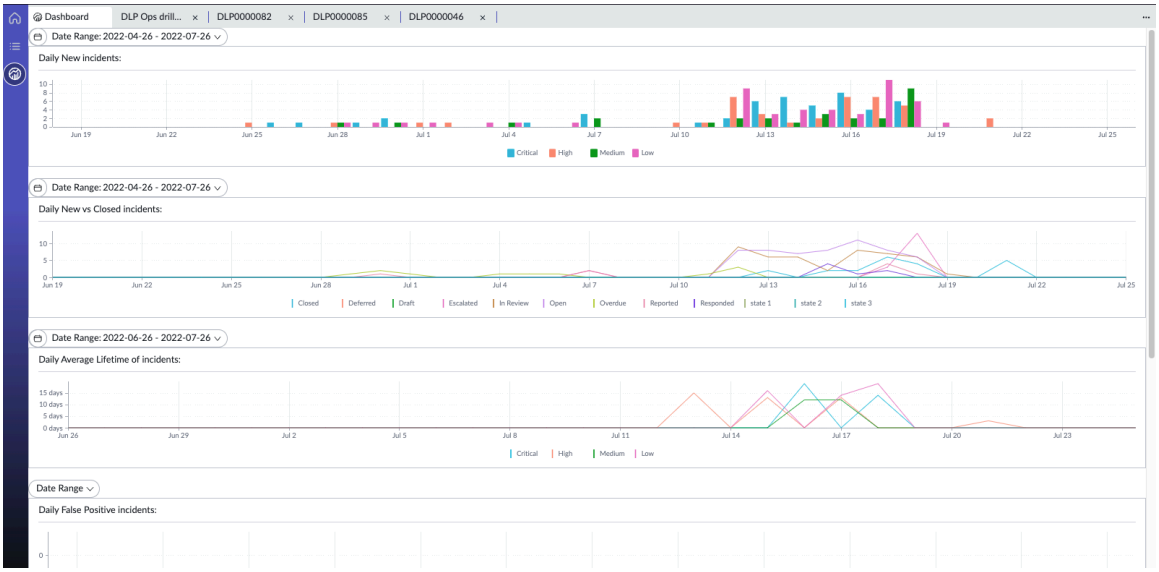
Data Loss Prevention Incident Response-Dashboard

Die Data Loss Prevention Incident Response Das Dashboard (DLP IR) bietet in Form von grafischen Diagrammen einen allgemeinen Überblick über Ihre DLP-Incidents und täglichen Incident-Trends in Ihrer Instanz. Diese Diagramme helfen Ihnen, DLP-Incidents effektiv anzuzeigen, zu verwalten und zu beheben.

Die Data Loss Prevention Incident Response Das Dashboard bietet täglich wichtige Einblicke zu Ihren DLP-Incidents. Sie können Indikatoren einrichten und regelmäßig Daten-Snapshots der Incidents erfassen, die den Bedingungen in den Indikatoreigenschaften entsprechen. Die gesammelten Daten werden dann mithilfe von Widgets im Dashboard visualisiert. Um die DLP-Incidents in verschiedenen Zeitintervallen zu analysieren, können Sie verschiedene Datumsbereiche anwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DLP-Dashboard



Analysieren Sie tägliche Incident-Trends in Ihren DLP-Incidents

Greifen Sie auf zu Data Loss Prevention Incident Response Dashboard (DLP IR), um die täglichen Trends in Ihren DLP-Incidents zu analysieren und effektiv zu beheben.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.Analyst – DLP-Incidents bearbeiten und anzeigen.
- sn_dlir.Analyst_read und sn_dlir.read: Zeigen Sie DLP-Incidents an.

Warum und wann dieser Vorgang ausgeführt wird

Sie können die täglichen Trends mithilfe von Widgets im DLP-Dashboard visualisieren. Die Daten oder Statistiken für die täglichen Trends Ihrer DLP-Incidents werden aus den Indikatoreigenschaften für tägliche Incidents erfasst, die von Ihrer Organisation definiert werden. Sie können wichtige Einblicke gewinnen, indem Sie verschiedene Datenbereiche anwenden, um DLP-Incidents in verschiedenen Zeitintervallen für die folgenden Diagramme zu analysieren:

- **Tägliche neue Incidents** : Daten der gesamten täglich erstellten DLP-Incidents unabhängig vom Status der Incidents. Die DLP-Incidents werden basierend auf den Schweregraden kategorisiert, einschließlich „Mittel“, „Kritisch“, „hoch“ und „Niedrig“. Jeder DLP-Incident-Schweregrad wird durch eine bestimmte Farbe im Diagramm dargestellt.
- **Tägliche neue vs. Geschlossene Incidents** : Die verschiedenen status der DLP-Incidents und ein Vergleich zwischen den täglichen neuen Incidents und täglich geschlossenen Incidents. Die Kategorie „täglich neu“ enthält alle DLP-Incidents in den Kategorien „Offen“, „Entwurf“, „eskaliert“, „in Überprüfung“, „überfällig“, status „gemeldet“, „beantwortet“ oder „Anwenderdefiniert“ (falls vorhanden). Die Kategorie „geschlossener Incident“ enthält die geschlossenen DLP-Incidents. Jeder DLP-Incident-Status wird durch eine bestimmte Farbe im Diagramm dargestellt.
- **Tägliche durchschnittliche Lebensdauer von Incidents** : Die Lebensdauer eines Incidents ist der Zeitraum zwischen dem Öffnen und Schließen eines bestimmten DLP-Incidents. Die tägliche durchschnittliche Lebensdauer wird nur für die geschlossenen DLP-Incidents berechnet.
- **Tägliche falsch positive Incidents** : Daten aller DLP-Incidents, die als tägliche falsch positive Ergebnisse gemeldet werden. Die täglichen falsch positiven Incidents werden basierend auf den Schweregraden kategorisiert, einschließlich „Mittel“, „Kritisch“, „hoch“

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

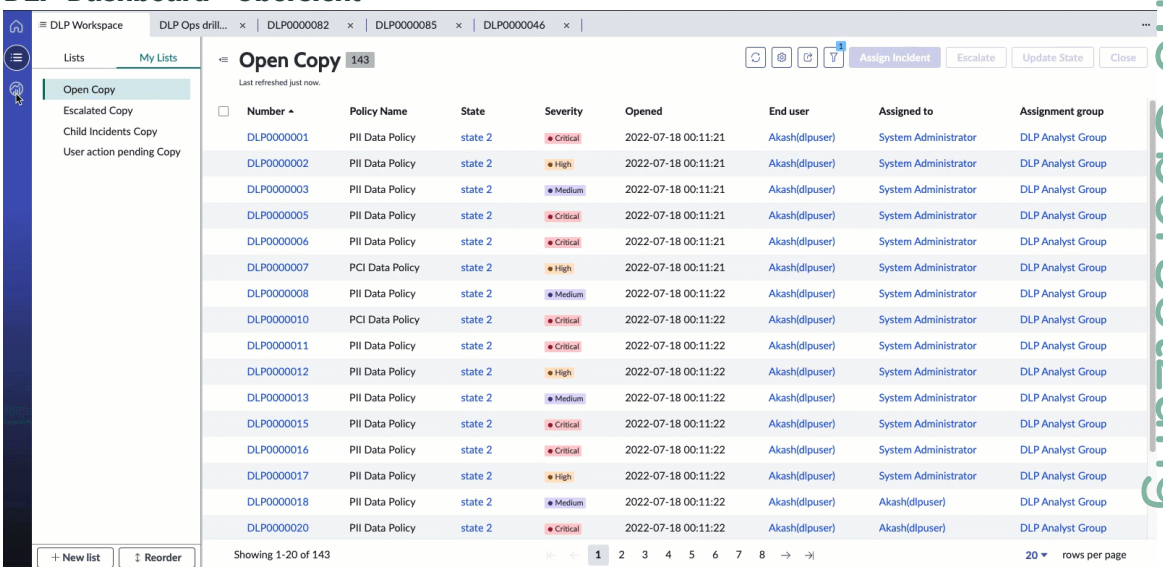
und „Niedrig“. Jeder tägliche falsch positive Incident-Schweregrad wird durch eine bestimmte Farbe im Diagramm dargestellt.

- **Alter vs. Schweregrad von Incidents** : Datenvergleich aller DLP-Incidents, kategorisiert nach Alter und konfiguriert mit dem Schweregrad der DLP-Incidents. Die Alterskategorie enthält alle DLP-Incidents unter dem von Ihrer Organisation definierten Alter. Weitere Informationen zu Altersdiagrammen finden Sie unter Erstellen Sie Altersdiagrammkonfigurationen. Der Schweregrad von Incidents umfasst alle DLP-Incidents in der Kategorie hoch oder Niedrig. Jeder Schweregrad wird durch eine bestimmte Farbe im Diagramm dargestellt.
- **Tägliche eskalierte Incidents** : Daten aller eskalierten DLP-Incidents täglich. Die täglich eskalierten Incidents werden basierend auf den Schweregraden kategorisiert, einschließlich „Mittel“, „Kritisch“, „hoch“ und „Niedrig“. Jeder tägliche eskalierte Incident-Schweregrad wird durch eine bestimmte Farbe im Diagramm dargestellt.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Dashboard**an.
   Die Seite mein DLP-Dashboard wird in einer neuen Browserregisterkarte angezeigt.
2. Wählen Sie ein Dashboard-Widget aus, für das Sie eine tägliche Trendanalyse durchführen möchten.
   Beispiel: Das Diagramm tägliche neue Incidents.
3. Überprüfen Sie die Dashboard-Widgets, um Trends zu identifizieren.
4. Klicken Sie Auf **Datumsbereich** .

DLP-Dashboard – Übersicht



5. Wählen Sie einen Datumsbereich aus dem Kalender aus, und klicken Sie auf **Anwenden** .

   Example
   Beispielsweise wird das Diagramm „tägliche neue Incidents“ für den ausgewählten Datenbereich aktualisiert.
6. Verwenden Sie die Filter unterhalb des Diagramms, um Detailinformationen anzuzeigen und eine eingehendere Analyse durchzuführen.

Eingehende Integration für Data Loss Prevention Incident Response

Erstellen Sie einzelne oder mehrere DLP-Incidents mithilfe der eingehenden REST-API.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen einzelnen DLP-Incident

Erforderliche Rolle: sn_dlir.api_Integration_user.

Um einen einzelnen DLP-Incident zu erstellen, definieren Sie nach Bedarf die folgenden Parameter:

Feld	Beschreibung
HTTP-Methode	`POST`
URL	https://{instance}/api/now/import/sn_dlir_incident_import
Anforderungs-Header	**Akzeptieren:** `application/json` **Inhaltstyp:** `application/json`
Beispielnutzlast	{ "application_window_title": "<value>", "assigned_to": "<value>", "attachments": "<value>", "data_owner_email": "<value>", "destination": "<value>", "dest_ip": "<value>", "dest_ip_port": "<value>", "detection_date": "<value>", "endpoint_on_corporate_net": "<value>", "files": "", "file_created": "", "file_created_by": "", "file_location": "", "file_modified_by": "", "file_name": "", "file_owner": "", "file_permissions": "", "ftp_user_name": "", "last_modified": "", "machine_ip": "", "machine_name": "", "match_count": "", "policy_id": "", "policy_name": "", "printer_name": "", "printer_type": "", "print_job_name": "", "recipients": "", "scanned_machine": "", "scan_source": "", "seen_before": "", "sender":"", "source":"", "source_file":"", "source_ip":"", "source_ip_port":"", "subject":"",

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung

	<pre>"url":"",
	"user_justification":""
	}</pre>

Beispielantwort	<pre>{
	"import_set": "ISET0010003",
	"staging_table": "sn_dlir_incident_import",
	"result": [
	{
	"transform_map": "",
	"table": "sn_dlir_incident",
	"display_name": "number",
	"display_value": "DLP0001012",
	"record_link":
	"https://{instance}/api/now/table/sn_dlir_incident/7cda322297c2411056a43d1e6253af1f",
	"status": "inserted",
	"sys_id": "7cda322297c2411056a43d1e6253af1f"
	}
	]
	}</pre>

Erstellen Sie mehrere DLP-Incidents

Erforderliche Rolle: sn_dlir.api_Integration_user.

Um mehrere DLP-Incidents aus derselben Anforderung zu erstellen, definieren Sie nach Bedarf die folgenden Parameter:

Feld	Beschreibung
HTTP-Methode	`POST`
URL	https://{instance}/api/now/import/sn_dlir_incident_import/insertMultiple
Anforderungs-Header	**Akzeptieren:** `application/json` **Inhaltstyp:** `application/json`

Beispielnutzlast	<pre>{
	"records": [
	{
	"file_name": "<value>",
	"file_modified_by": "<value>",
	"work_notes": "<value>",
	"url": "<value>",
	"scan_source": "<value>",
	"data_owner_email": "<value>",
	"file_created_by": "<value>",
	"file_owner": "<value>",
	"policy_name": "<value>"</pre>

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	`},{"dest_ip": "<value>","dest_ip_port": "<value>","detection_date": "<value>","endpoint_on_corporate_net": "<value>","files": "<value>","file_created": "<value>","file_created_by": "<value>","file_location": "<value>","file_modified_by": "<value>","file_name": "<value>","file_owner": "<value>"}]}`
Beispielantwort	`{"import_set_id": "a38f69229734dd1056a43d1e6253af75","multi_import_set_id": "e78f69229734dd1056a43d1e6253af75"}`

Hinweis:
Standardmäßig ist die Transformation asynchron. Um die synchrone Transformation festzulegen, erstellen Sie einen neuen Datensatz in der Tabelle „REST – Multiple einfügen“ [sys_Rest_insert_multiple], und wählen Sie die Quelltabelle als aus **sn_dlir_Incident_Import** , Und legen Sie die Transformation auf fest **Synchron** .

DLP-Integrationen

Die Data Loss Prevention Incident Response Das Basissystem enthält Integrationen in Softwarepakete zur Vermeidung von Datenverlust von Drittparteien.

Dieser Abschnitt enthält Anweisungen zum Aktivieren der Plugins und zum Konfigurieren beider ServiceNow Und Drittpartei-Integrationen. Ebenfalls enthalten sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten Integrationen, die im Basissystem enthalten sind.

Integrationskonfigurationen

Das Basissystem enthält eine Reihe von Karten für jede der Integrationsimplementierungen, die Sie aktivieren und verwenden können. Außerdem werden Karten für alle im ServiceNow Store veröffentlichten Integrationen angezeigt, die Abhängigkeiten von haben Security Operations Plugins. Die Integrationskarten können angezeigt werden, indem Sie auswählen **Security Operations** > **Integrationskonfigurationen**an.

Data Loss Prevention Incident Response Unterstützt die folgenden Softwarepakete zur Vermeidung von Datenverlust von Drittparteien:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symantec Integration für Data Loss Prevention Incident Response

Die Symantec Die DLP-Integration unterstützt die Erfassung von Data Loss Prevention Incident Response Incidents, die auf erstellt wurden Symantec Data Loss Prevention Incident Response Bereitstellung. Nach der Erfassung können Sie die Incident-Management-Funktionen verwenden, um DLP-Incidents zu beheben.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht und wichtige Funktionen

Die Symantec Die DLP-Integration hilft Unternehmen, die Nutzung und Bewegung vertraulicher Daten auf verschiedenen Plattformen nachzuverfolgen.

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Möglichkeit, mehrere Integrationsprofile für verschiedene zu erstellen Symantec API-Endpunkte.
- Geplante Erfassung von DLP-Incidents aus Symantec In Ihren ServiceNow Instanz.
- Möglichkeit, API-Filter anzuwenden, um die Incidents abzurufen, die den Filterkriterien entsprechen, und auch den Filter für anzugeben Symantec DLP-Incidents, die importiert werden müssen.
- Zuordnung der DLP-Incident-status in Ihrem ServiceNow Instanz zu DLP-Incident-status in Symantec.
- Incident-Status in automatisch aktualisieren Symantec Wenn sich der Status in ändert ServiceNow Instanz.
- Möglichkeit, die Schweregradzuordnung zwischen Symantec DLP-Incidents mit ServiceNow-Incidents anzupassen und zu definieren.

Weitere Informationen zur Integration finden Sie unter Symantec-Produktdokumentation .

Erste Schritte mit Symantec DLP-Integration für die Vermeidung von Datenverlust

Bevor Sie die Integration verwenden können, müssen Sie sie aus dem herunterladen ServiceNow® Store.

Prüfliste

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihres beginnen Symantec DLP-Integration zur Vermeidung von Datenverlust.

Prüfliste

Feld	Beschreibung
Überprüfen Sie, ob Sie die erforderlichen zugewiesen haben ServiceNow AI Platform, Anwendung zur Vermeidung von Datenverlust, MID-Anwendungsrollen.	Die folgenden Rollen werden im verwendet Symantec DLP-Integration auf dem ServiceNow AI Platform: • Der Administrator (admin) installiert die Anwendungen aus dem ServiceNow® Store Und weist den Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Feld	Beschreibung
	zur Vermeidung von Datenverlust (sn_dlir.admin) zu. • Der Benutzer mit der Rolle „sn_dlir.admin“ kann die Integration konfigurieren und die Incident-Profile einrichten. • Die Anwender mit der Rolle „sn_dlir.Analyst“ haben Leserollen in der gesamten Integration.
Weisen Sie die erforderlichen zu Symantec DLP-Anwenderrollen.	Überprüfen Sie Symantec DLP-Integrationsrollen und -Berechtigungen.
Überprüfen Sie, ob Sie verwenden Symantec DLP 15,8	Die Symantec Die DLP-Integration für die Vermeidung von Datenverlust wird mit der Version 15,8 von getestet Symantec Vermeidung Von Datenverlust. **Hinweis:** Stellen Sie sicher, dass Sie verwenden Symantec DLP 15,8
Verifizieren Sie das ServiceNow®Kernanwendung, die zur Unterstützung von erforderlich ist Symantec DLP-Integration wird installiert und aktiviert.	Überprüfen Sie, ob die folgenden allgemeinen DLP-Anwendungen und Sicherheitssupport-Anwendungen im ServiceNow Store installiert und aktiviert sind. Wenn nicht installiert, installieren Sie die Anwendung, und aktivieren Sie sie. • Security Support Common • Reaktion auf Incident zur Vermeidung von Datenverlust

Installieren und konfigurieren Sie Symantec DLP-Integration für die Vermeidung von Datenverlust

Installieren und konfigurieren Sie Symantec DLP-Integration aus dem ServiceNow® Store Auf Ihrem ServiceNow AI Platform Instanz. Beginnen Sie mit der Untersuchung von DLP-Incidents mit Symantec DLP-Incident-Daten.

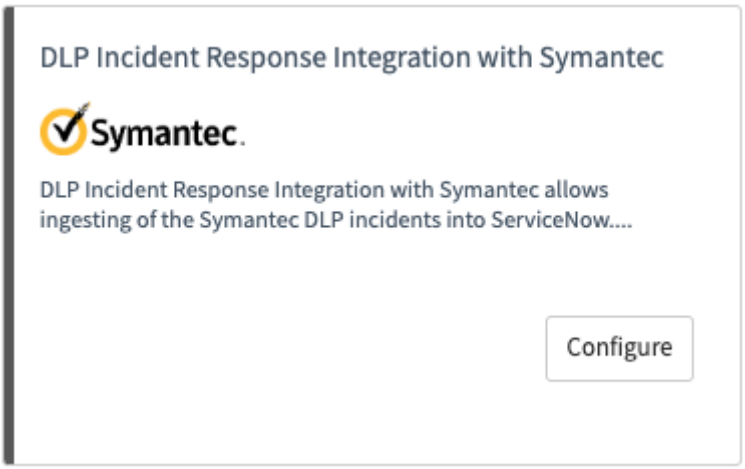
Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Prozedur

1. Laden Sie herunter Symantec DLP-Integration aus dem ServiceNow® Store Und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie#mit nach der Integration von DLP Incident ResponseSymantec Kachel und klicken Sie auf **Konfigurieren** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

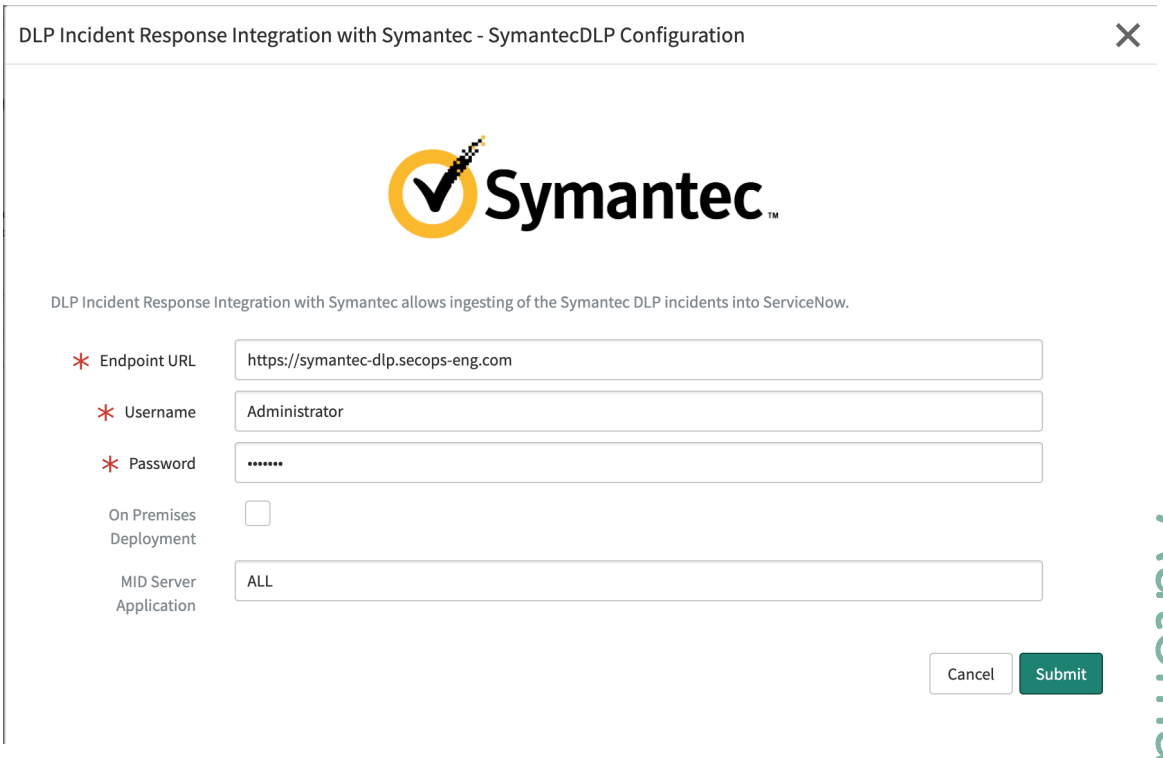


4. Füllen Sie im Formular die Felder aus.

Formular „Symantec DLP-Integrationskonfiguration“

Feld	Beschreibung
Name	Name des Symantec DLP-Integrationskonfiguration.
Endpunkt-URL	Symantec REST-API-Endpunkt.
Anwendername	Symantec Account-Name. Informationen zu den erforderlichen Rollen und Berechtigungen finden Sie unter Rollen und Berechtigungen .
Passwort	Symantec Account-Passwort.
Lokale Bereitstellung	Option, die Sie auswählen können, wenn Symantec Wird in einer lokalen Instanz bereitgestellt. Wenn Sie diese Option auswählen, müssen Sie den MID-Server verwenden, um eine Verbindung mit Symantec herzustellen.
MID-Server-Anwendung	Der Name der MID-Anwendung, der für die Kommunikation mit verwendet wird Symantec. Dieses Feld wird benötigt, wenn Sie auswählen **Lokale Bereitstellung** Option.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Absenden**.

Ergebnisse

Hinweis:
Verbinden Sie die symantec-Subprod mit der ServiceNow-Subprod. Halten Sie alle Anwendernamen und Passwörter in allen Instanzen synchron, um zu vermeiden, dass Accounts abgemeldet werden.

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird Symantec DLP-Integration wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Erstellen Sie ein Profil für Symantec DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrem ServiceNow AI Platform Instanz. Bestimmen Sie Symantec DLP-Incidents, die zum Erstellen von DLP-Incidents geeignet sind.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie ServiceNow AI Platform®Dient zum Abrufen der DLP-Incidents aus dem Symantec Endpunkt. Speichern Sie diese Incidents in ServiceNow® Instanz als DLP-Incidents.

Prozedur

1. Navigieren zu **Symantec-DLP-Integration** > **Incident-Profil**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder im Abschnitt Name aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

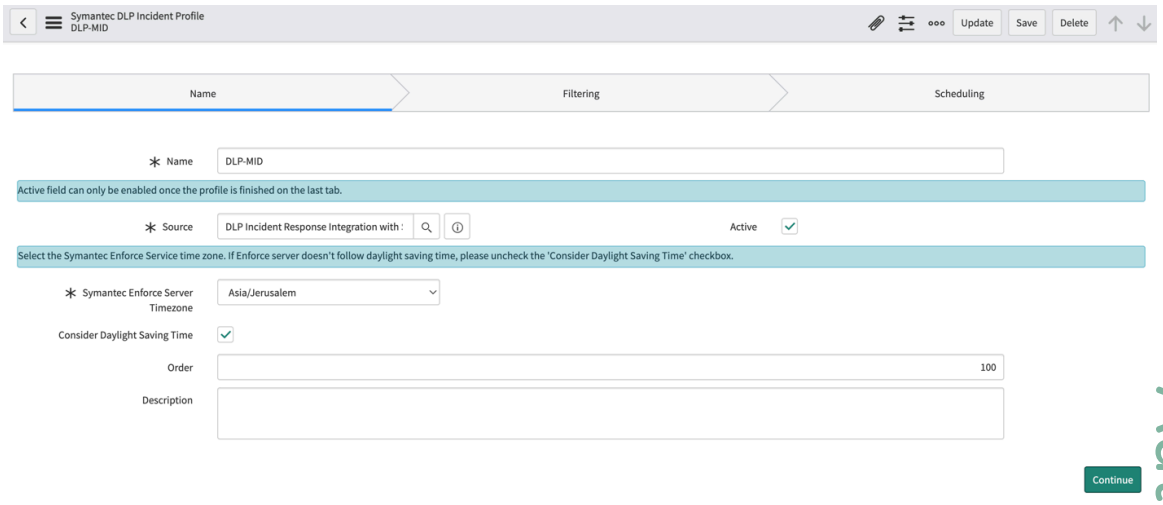
Erstellen Sie ein Profil

Feld	Beschreibung
Name	Name des Profils. Dieses Feld hilft Ihnen, das Profil zu identifizieren. **Hinweis:** De Name muss für jedes Profil eindeutig sein.
Quelle	Symantec DLP-Instanz, die Sie zum Erfassen von Incidents konfiguriert haben. Wenn Sie mehrere Instanzen konfiguriert haben, wählen Sie die entsprechende Instanz für die Incident-Typen aus, die Sie für das Profil erfassen möchten.
Aktiv	Option, um anzugeben, ob das Profil aktiv ist. Dieses Feld kann nur aktiviert werden, nachdem Sie auf geklickt haben **Beenden** Im Abschnitt Zeitplanung. Wenn das Profil aktiv ist, bedeutet dies, dass ServiceNow AI Platform Fragt aktiv ab Symantec DLP-Incidents. Die entsprechenden DLP-Incidents werden in#DLP erstellt#, wenn die Filterbedingungen basierend auf den von Ihnen angegebenen Zeitplanungsparametern erfüllt werden.
Symantec Enforce Server – Zeitzone	Wählen Sie im Profil die Zeitzone für den symantec Enforce-Server aus, damit Incidents aufgrund von Zeitzonenproblemen nicht verpasst werden.
Sommerzeit berücksichtigen	Aktivieren Sie dieses Kontrollkästchen, wenn der Enforce-Server die Sommerzeit einhält.
Reihenfolge	Reihenfolge der Profilausführung. Das Profil mit der niedrigsten Reihenfolge, das als höchste Priorität betrachtet wird. Standardmäßig ist der Wert 100.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Eindeutige Beschreibung für dieses Profil.



Nächste Maßnahme

Um zum Abschnitt Filterung zu wechseln,#klicken Sie auf **Fahren Sie Fort** .

Definieren Sie Filter, die für die Incident-Erstellung angewendet werden sollen

Definieren und legen Sie Filterbedingungen fest, um Detailinformationen für eingehende Elemente anzuzeigen Symantec DLP#-Incidents. Bestimmen Sie die Incidents, die als DLP-Incidents in erstellt werden sollen ServiceNow®.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Das Filtern hilft Ihnen, DLP-Incidents zu isolieren und die Anzahl der von Ihnen erstellten DLP-Incidents zu begrenzen. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur Incidents erstellt, die den Bedingungen entsprechen.

Prozedur

1. Wählen Sie Aus **API-basierter Filter für Incident-Erfassung** Kontrollkästchen zum Anwenden der API-Filter und Abrufen der Incidents, die den Filterkriterien entsprechen.
2. Fügen Sie die API-Filter hinzu.
   Das folgende Beispiel zeigt die API-Filter.

```
{
            "operandOne": {
               "name": "incidentStatusName"
            },
            "filterType": "string",
            "operator": "EQ",
            "operandTwoValues": [
               "incident.status.New"
            ]
         }
```

Automatische Übersetzung

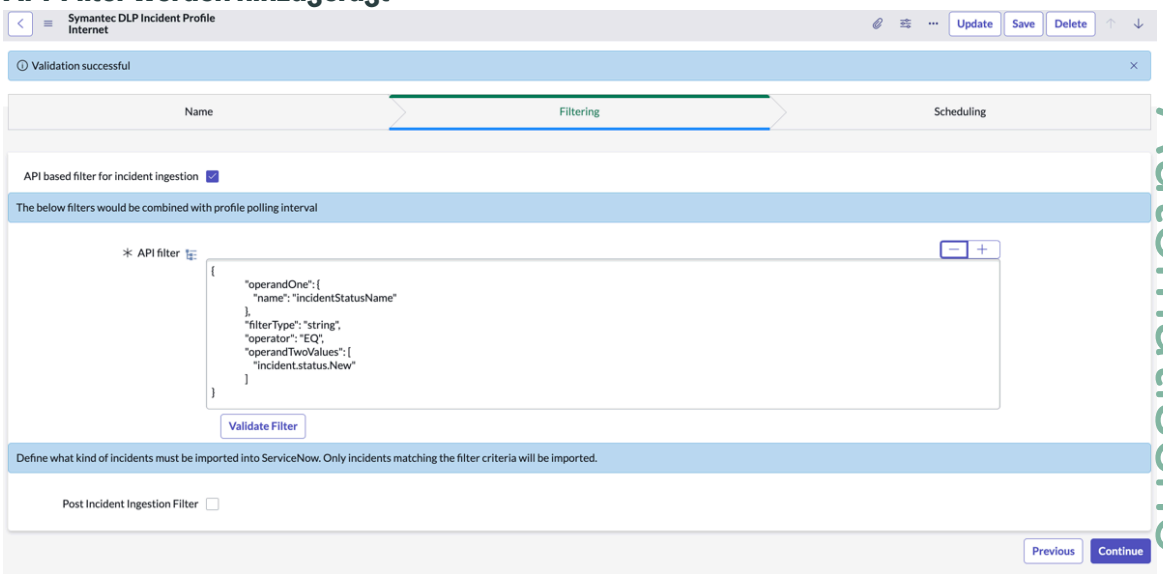
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Weitere Informationen zu den API-Filtern in der Symantec-Integration finden Sie unter Incident-Listen: Parameter: Details zum Anforderungsobjekt .

3. Klicken Sie Auf **Filter Validieren** Nachdem Sie die API-Filter angewendet haben.

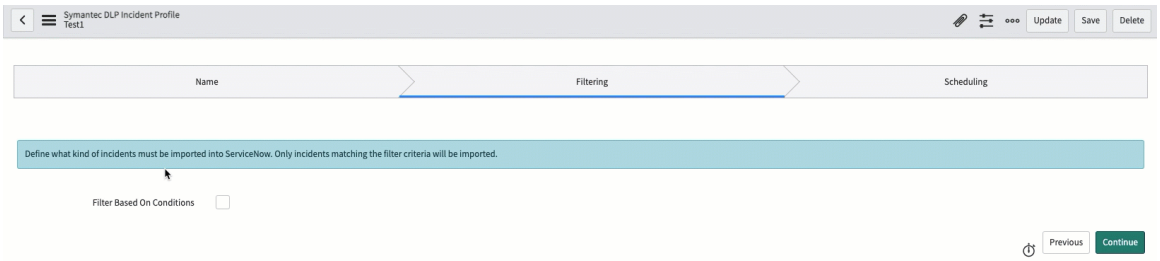
Hinweis:
Wenn die Validierung nicht erfolgreich ist, wird eine Fehlermeldung angezeigt, dass die Validierung fehlgeschlagen ist. Dies geschieht, wenn die Filter nicht ordnungsgemäß gemäß den Symantec-APIs eingegeben werden.

API-Filter werden hinzugefügt



4. Wählen Sie Aus **Filter Für Incident-Erfassung** Kontrollkästchen zum Definieren der Kriterien, die ein eingehender Symantec-DLP-Incident erfüllen muss, damit ein DLP-Incident erstellt wird.
Die Optionen im ersten Feld in den Filterbedingungen entsprechen den Feldern, die im DLP-Incident verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Überprüfen Sie, ob die von Ihnen definierten Kriterien mit den Werten des Incident übereinstimmen.
5. Legen Sie im Bedingungsgenerator die Filter in fest **Filterbedingungen** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Um weitere Bedingungen hinzuzufügen, klicken Sie auf **UND** #Oder**ODER** .
   - Wenn **UND** #Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** #Ist ausgewählt, kann eine der Bedingungen erfüllt werden.

Nächste Maßnahme
Klicken Sie auf, um den Zeitplan zu konfigurieren **Fahren Sie Fort** .

Konfigurieren Sie die Speicherung von Nachweisdateien

Konfigurieren Sie den Nachweisdateispeicher, um die Nachweisdatei für die DLP-Incidents sicher zu speichern.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Stellen Sie sicher, dass für den Symantec-Anwender, den Sie für die Integration von ServiceNow Symantec DLP konfigurieren, die Optionen „Text“, „Anhänge“ und „ursprüngliche Nachricht“ auf der Konfigurationsseite „Rollen“ im Symantec DLP-Portal aktiviert sein müssen. Weitere Informationen finden Sie im Abschnitt „Attribute anzeigen“ verfügbar unter Rollen Werden Konfiguriert Dokument für weitere Informationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können den Nachweisdateispeicher konfigurieren, um Dateien sicher zu speichern. Dies bietet eine Option für internen Speicher in der ServiceNow-Instanz, um sicherzustellen, dass Dateien mit ServiceNow gespeichert und verschlüsselt werden Feldverschlüsselung. Weitere Informationen finden Sie unter Feldverschlüsselung In NowPlatform-Dokumentation.

Wenn der DLP-Analyst die Aktion „Nachweisdateien für DLP-Incidents herunterladen“ aus dem Arbeitsbereich des Analysten ausführt, wird die Datei aus dem ausgewählten Speicher heruntergeladen, wenn die Speicheroption für Nachweisdateien aktiviert ist. Andernfalls wird die Datei direkt aus der Symantec-Quelle heruntergeladen und nicht in der ServiceNow-Instanz beibehalten.

Hinweis:

Wenn ein DLP-Analyst die Aktion „Nachweisdateien für DLP-Incidents herunterladen“ aus dem Arbeitsbereich des Analysten ausführt, wird die Datei aus dem ausgewählten Speicher heruntergeladen, wenn die Speicheroption für Nachweisdateien aktiviert ist. Andernfalls wird die Datei direkt aus der Symantec-Quelle heruntergeladen und nicht in der ServiceNow-Instanz beibehalten.

Prozedur

1. Navigieren zu **Alle** > **Symantec DLP-Integration** > **Incident-Profil**an.
2. Klicken Sie auf **Nachweisspeicher** Abschnitt im Formular „Incident-Profil“.
3. Wählen Sie Aus **Nachweisdateispeicher** Kontrollkästchen zum Aktivieren des Dateispeichers.
4. Wählen Sie den bevorzugten Speichertyp aus.
5. Klicken Sie Auf **Fahren Sie Fort** Und wechseln Sie zu **Zeitplanung** Abschnitt.

Ergebnisse

Die Nachweisdateien werden gemäß der Konfiguration gespeichert, nachdem die Incident-Erfassung abgeschlossen ist.

Laden Sie Nachweisdateien herunter

Laden Sie DLP-Incident-Nachweisdateien herunter, die gegen die DLP-Richtlinie auf Symantec verstoßen.

Vorbereitungen

Laden Sie diese Datei aus dem DLP-IR-Analyst-Arbeitsbereich und dem DLP-IR-Endanwender-Arbeitsbereich auf Ihren lokalen Computer herunter. Die Aktion „Dateien herunterladen“ ist nur für die Genehmiger im DLP IR-Endanwenderarbeitsbereich verfügbar.

Erforderliche Rolle:

- sn_dlir.Analyst
- sn_dlir.secure_file_download (jeder Genehmiger mit dieser Rolle)

Prozedur

1. Navigieren zu **Alle** > **Symantec DLP-Integration** > **Einstellung**an.
2. Aktivieren **Sollte das Herunterladen der Datei mit Verstoß des gemeldeten Incidents zulässig sein** Eigenschaft.
   Nachdem Sie diese Eigenschaft aktiviert haben, können Sie jetzt sehen **Datei Herunterladen** Aktion im DLP-Analysten-Arbeitsbereich für jeden Symantec-DLP-Incident.
3. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Öffnen Sie einen DLP-Incident-Datensatz, der aus der Symantec-Quelle erfasst wird.
5. Klicken Sie Auf **Datei Herunterladen** .

> **Hinweis:**
> Die Datei, die gegen die DLP-Richtlinie auf Symantec verstoßen hat, wird auf den lokalen Computer des Anwenders heruntergeladen.

Führen Sie die folgenden Schritte aus, damit der Genehmiger die Aktion „Datei herunterladen“ anzeigen kann:

6. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Anwenderarbeitsbereich**an.
   Die Seite „meine DLP-Incidents“ wird auf einer neuen Registerkarte angezeigt.
7. Wählen Sie Aus **Meine Genehmigungen** Modul, das unter dem Modul „meine DLP-Incidents“ verfügbar ist.
   Die Listenansicht „meine Genehmigungen“ wird angezeigt.
8. Öffnen Sie einen Genehmigungsanforderungsdatensatz, der für den Symantec DLP-Incident ausgelöst wird.
9. Klicken Sie auf das Infosymbol (i), das im Feld DLP-Incident in der Formularansicht verfügbar ist.
10. Klicken Sie Auf **Datei Herunterladen** .

Ergebnisse

Nach dem Ausführen dieser Aktion wird die Nachweisdatei entweder im ZIP-Format (wenn der Incident Verstöße in mehreren Komponenten aufweist und/oder die ursprünglichen Nachrichtendaten ebenfalls verfügbar sind) oder eine einzelne Datei (wenn der Incident Verstöße in einer einzelnen Komponente aufweist oder nur ursprüngliche Nachrichtendaten verfügbar sind) auf den lokalen Computer des Anwenders heruntergeladen.

> **Hinweis:**
> Als DLP-Administrator können Sie den Zugriff auf steuern **Datei Herunterladen** Aktion durch Deaktivieren von **Sollte das Herunterladen der Datei mit Verstoß des gemeldeten Incidents zulässig sein** Option von **Erweiterte Einstellungen** Seite. Weitere Informationen finden Sie unter Konfigurieren Sie erweiterte Einstellungen für die Reaktion auf Incidents zur Vermeidung von Datenverlust .

Vorschau der Nachweisdateien anzeigen

Vorschau Data Loss Prevention Incident Response Nachweisdateien im DLP-IR-Analyst-Arbeitsbereich.

Vorbereitungen

> **Wichtig:**
> Bei der Verwendung der Aktion „Nachweisdateien“ im DLP-Analysten-Arbeitsbereich werden die Nachweisdateien vorübergehend in der ServiceNow-Datenbank in einem unverschlüsselten Format gespeichert. Wenn Sie die Nachweisdateien nicht speichern möchten, deaktivieren Sie die Vorschaufunktion für Nachweisdateien. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Erforderliche Rolle: sn_dlir.Analyst

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
2. Öffnen Sie einen DLP-Incident-Datensatz.
3. Wählen Sie in der kontextbezogenen Sidebar das Symbol für Nachweisdateien ( ).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Auf der **Nachweisdateien** Wählen Sie die Registerkarte aus **Nachweisdatei** Karte zur Vorschau der Nachweisdateien im Dokument-Viewer.

   Die Vorschaufunktion unterscheidet sich für jeden Dateityp, wie in der folgenden Tabelle aufgeführt.

Dateiformat	Dateierweiterung
Bild	.Bmp, .gif, .ico, .JPEG, .jpg, .png, .svg und .webp. Bilddateien werden im Dokument-Viewer-Modus geöffnet.
Microsoft Office-Dateien	.Doc, .docx, .ppt, .pptx, .xls, und .xlsx Office-Dateien werden im Dokument-Viewer-Modus geöffnet.
Textdateien	.txt Textdateien werden im Texteditor-Modus geöffnet.
E-Mail-Dateien	.Eml **Hinweis:** Die Dateigröße muss weniger als 5 MB betragen. Sie müssen zuerst die Datei herunterladen, um eine Vorschau des Inhalts anzuzeigen.
PDF-Dateien	.PDF ○ Geben Sie ein Stichwort ein, um das Dokument zu durchsuchen. ○ Zoom- und Verkleinerungsfunktionen, um die Ansicht für eine bessere Lesbarkeit anzupassen. ○ Drehen Sie die Seite im Uhrzeigersinn oder gegen den Uhrzeigersinn, um den Inhalt klarer anzuzeigen.

Hinweis:

Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion „Vorschaunachweisdatei“ funktioniert auch für archivierte Incidents.

Planen Sie Symantec DLP-Incident-Abruf

Legen Sie einen Zeitplan fest, um die Incident-Daten abzurufen und zu erfassen Symantec DLP-Incidents, die den Kriterien im Profil entsprechen. Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Incidents aus abrufen Symantec.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können planen, wie oft Sie zukünftige Incidents abfragen, die der Incident-Profilkonfiguration entsprechen. Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Planung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Das Profil kann so konfiguriert werden, dass ein einmaliger Abruf mit durchgeführt wird **Einmaliger Abruf** Kontrollkästchen. Das historische Datum kann bis zu den letzten drei Monaten ab dem aktuellen Datum liegen.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die verschiedenen Abfrageintervalle können sich auf die Leistung von auswirken Symantec DLP-Incident-Integration. Planen Sie bei der Planung, dass die Systemlast gegen die Dringlichkeit eines Incident ausgeglichen wird.

Prozedur

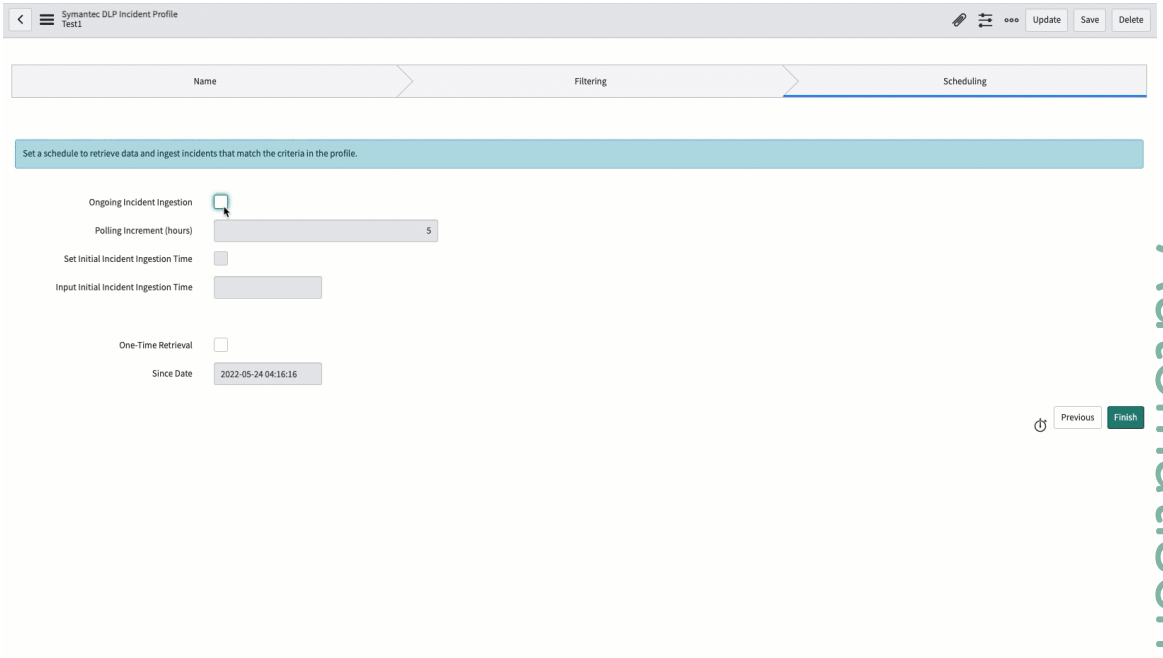
1. Legen Sie einen Zeitplan fest, um Daten abzurufen und Incidents zu erfassen, die den Kriterien im Profil entsprechen.
2. Füllen Sie die Felder im Formular aus.

Zeitplan für den DLP-Incident

Feld	Beschreibung
Laufende Incident-Erfassung	Die laufende Incident-Erfassung, die von ServiceNow AI Platform Instanz ruft aus#Symantec für neue Incidents ab. DLP-Incidents werden erstellt, wenn ausgelöste Incidents gefunden werden und die Filterkriterien für die Incident-Generierung erfüllt sind.
Abfrageschritt (Minuten)	Die Abfragehäufigkeit, die in Minuten definiert ist. Dieses Feld wird automatisch auf 300 Minuten festgelegt.
Zeitpunkt der ersten Incident-Erfassung festlegen	Option zum Definieren eines Datums und einer Uhrzeit für die anfängliche Erfassung. Nachfolgende Erfassungen basieren auf dem Abfrageintervall-Zeitraum.
Zeitpunkt der ersten Incident-Erfassung eingeben	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben.
Zeitpunkt der ersten Incident-Erfassung	Erstes Mal, wenn die Daten erfasst werden. Sie können sehen, dass Werte angezeigt werden, wenn die erste Incident-Erfassungszeit festgelegt ist.
Nächste Incident-Erfassungszeit (geschätzt)	Nächster Zeitraum für eine geschätzte Incident-Erfassung.
Einmaliger Abruf	Option zum Aktivieren des einmaligen Abrufs von Verlaufsdaten. Wenn dieses Feld ausgewählt ist, werden Verlaufsdaten gemäß dem in hinzugefügten Datum aus Symantec DLP abgerufen **Seit Datum** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Seit Datum	Datum, ab dem Daten von Symantec abgerufen werden sollen. Dieses Feld kann auf höchstens drei Monate festgelegt werden.



3. Klicken Sie auf , um die erstellte Profilkonfiguration zu speichern **Beenden** Im Popup-Fenster.
4. Um das Profil zu aktivieren, öffnen Sie das erstellte Profil.
5. Aktivieren **Aktiv** Option.
6. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Nach erfolgreicher Erstellung und Aktivierung des Profils werden die Incidents regelmäßig gemäß der im Profil festgelegten Konfiguration abgerufen und der DLP-Incident-Tabelle hinzugefügt.

Zuordnung Symantec DLP-Incident-Status mit ServiceNow Incident-Status

Synchronisieren Sie den Status der DLP-Incidents, die in erfasst wurden ServiceNow Mit den DLP-Incidents von Symantec. Ordnen Sie zu **ServiceNow-Incident-Status** Feld mit **Symantec-Incident-Status** Feld.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Der Incident-Status wird dynamisch aus abgerufen Symantec Endpunktquelle, die der Zuordnung hinzugefügt wird. Sie müssen eine eins-zu-eins-Incident-Statuszuordnung durchführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

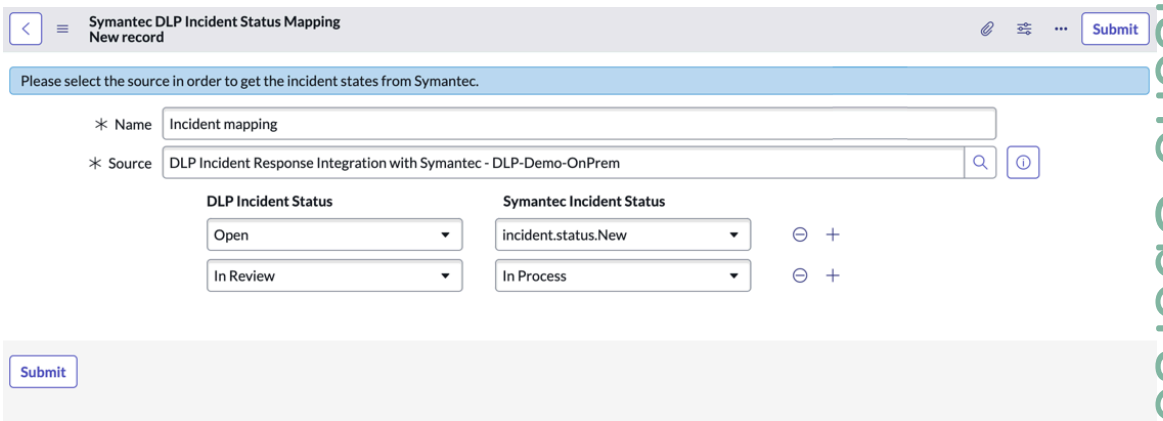
Prozedur

1. Navigieren zu **Symantec-DLP-Integration** > **Incident-Statuszuordnung**an.
2. Geben Sie ein an **Name** Um die Zuordnung zu identifizieren.
3. Wählen Sie aus **Quelle** Integration, aus der Sie den Status abrufen möchten.
4. Ordnen Sie zu **DLP-Incident-Status** Mit **Symantec-Incident-Status** .

Hinweis:
Es ist nicht erforderlich, alle status zuzuordnen. Sie können nur die erforderlichen status zuordnen.

Statuszuordnung für Symantec-DLP-Incident

Feld	Beschreibung
Name	Name des Zuordnungsdatensatzes.
Quelle	Die konfigurierte Symantec-Endpunktquelle, aus der Sie den Incident-Status abrufen möchten.
DLP-Incident-Status	Liste des Status von DLP-Incidents.
Symantec-Incident-Status	Liste des Status, der aus der Quelle abgerufen wird (Symantec-Endpunkt).



5. Klicken Sie auf **Absenden**.

Ergebnisse

Nachdem der Datensatz für die Zuordnung von Status von erfolgreich erstellt wurde ServiceNow Incidents, die ServiceNow Incident-Status wird mit synchronisiert Symantec DLP-Incident-Status.

Wenn Sie den Status eines DLP-Incidents auf Ihrem ändern ServiceNow Instanz, dann der Status von zugeordnet Symantec DLP-Incidents werden in der Quelle geändert Symantec Plattform basierend auf dem Zuordnungssatz im Datensatz.

Schweregradzuordnung zwischen Symantec-DLP-Incidents und ServiceNow-Incidents

Verwenden Sie die Schweregradzuordnungsfunktion, um die Zuordnung zwischen zu konfigurieren und zu synchronisieren Symantec Incidents und ServiceNow AI Platform® Incidents.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Mit der DLP-Schweregradzuordnung können Sie den Quellschweregrad dem DLP-Incident-Schweregrad zuordnen. Sie können den Quellschweregradwert anpassen, definieren und dem gewünschten DLP-Incident-Schweregradwert zuordnen.

Prozedur

1. Navigieren zu **Symantec-DLP-Integration** > **Incident-Schweregradzuordnung**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

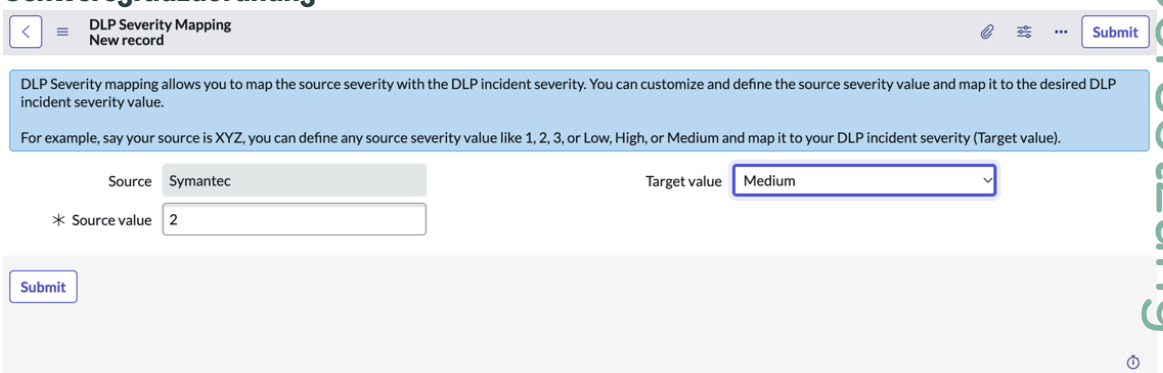
DLP-Schweregradzuordnung

Feld	Beschreibung
Quelle	Die konfigurierte Symantec-Endpunktquelle, aus der Sie den Incident abrufen möchten.
Zielwert	Der Zielwert ist die DLP-Incident-Schweregrad-ID. Die verfügbaren Werte sind „Kritisch“, „hoch“, „Mittel“, „Niedrig“ und „Info“ (wird in Symantec als Informationsschweregrad verwendet).
Quellwert	Quellwert ist der Symantec-Incident-Schweregrad.

Hinweis:
Innerhalb des Basissystems gibt es vier Schweregradzuordnungen, die an die DLP-Anwender gesendet werden.

4. Klicken Sie auf **Absenden**.

Schweregradzuordnung



Konfigurieren Sie Intelligente Antwortregeln

Konfigurieren Sie die intelligente Symantec-Antwortregel, um Antwortaktionen für die erfassten Symantec-DLP-Incidents auszuführen.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Stellen Sie sicher, dass für den Symantec-Anwender, den Sie für die Integration von ServiceNow Symantec DLP konfigurieren, diese Smart Response-Regeln unter ausgewählt sein müssen **Rollenkonfiguration** Seite. Weitere Informationen finden Sie unter **Aktionen** Abschnitt verfügbar für Rollen Werden Konfiguriert Dokument.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für die abgerufenen intelligenten Antwortregeln kann der DLP-Administrator die Zuordnungen „Incident-Antwortoptionsregel(n)“ und „Antwortoptionszuordnungen“ erstellen, um die Antwortaktion(en) zu konfigurieren, die für erfasste Symantec-DLP-Incidents ausgeführt werden soll.

Prozedur

1. Navigieren zu **Alle** > **Symantec DLP-Integration** > **Intelligente Antwortregeln**an.
   Sie können alle verfügbaren intelligenten Antwortoptionen für jede konfigurierte Integrationskonfiguration anzeigen. Weitere Informationen finden Sie unter . Installieren und konfigurieren Sie Symantec DLP-Integration für die Vermeidung von Datenverlust Und befolgen Sie das erklärte Verfahren Konfigurieren der Symantec-Integrationskonfigurationsquelle, falls nicht konfiguriert)
2. Klicken Sie auf eine der Smart Response-Regeln, um die zugehörige Formularansicht zu öffnen.

   Folgen Erstellen Sie Optionsregeln für die Reaktion auf Incidents Dient zum Erstellen von Optionsregeln für die Reaktion auf Incidents und Antwortoptionszuordnungen, um diese intelligente Antwortregel im Dialogfeld „Antworten“ des DLP-Arbeitsbereichs anzuzeigen.
3. Erstellen Sie die Genehmigungsregeln für die intelligente Antwortregel mit **Genehmigungsregeln** Registerkarte in der zugehörigen Liste oder durch das folgende Verfahren, das im Abschnitt „Genehmigungsregeln konfigurieren“ erläutert wird.
   Genehmigungsregeln für jede Smart Response-Regel sind in der zugehörigen Liste „Genehmigungsregeln“ sichtbar.
4. Nachdem Sie die Optionsregel(n) für die Reaktion auf Incidents erstellt haben, können Sie den Datensatz in der zugehörigen Liste des Datensatzes der intelligenten Antwortregel anzeigen.
5. Verwenden Sie **Aktualisieren Sie Die Intelligente Antwortregel** Schaltfläche in der Listenansicht, um die Quelle manuell zu aktualisieren.
   Die Regeln für intelligente Antworten werden jeden Tag für jede Quelle automatisch hinzugefügt, aktualisiert oder gelöscht.

Smart Response-Regeln Ausführen

Verwenden Sie diese Funktion, um intelligente Antwortregeln für Symantec DLP-Incidents auszuführen.

Vorbereitungen

Sie müssen die Smart Response-Regeln konfigurieren, indem Sie das hier in diesem Abschnitt erläuterte Verfahren ausführen: Konfigurieren Sie Intelligente Antwortregeln.

Erforderliche Rolle: sn_dlir.admin

Hinweis:

Die Antwortoptionen im Arbeitsbereich sind für Endanwender, Analyst oder Manager verfügbar, je nachdem, welche Konfiguration im Abschnitt erwähnt wird Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents.

Prozedur

1. Navigieren zu **Alle** > **DLP** > **DLP-Anwenderarbeitsbereich**an.
2. Öffnen Sie einen Symantec DLP-Incident.
3. Klicken Sie Auf **Antworten Sie** .
4. Wählen Sie die Antwortoption aus der Dropdown-Liste Antwort aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Antwortoptionen sind basierend auf der Konfiguration von sichtbar **Optionsregel Für Reaktion Auf Incidents** Und **Antwortoptionszuordnungen** .

5. Klicken Sie auf **Absenden**.

> **Hinweis:**
> Sie können auch die Genehmigungsregel(n) für die Antwortoptionen konfigurieren, indem Sie das im erläuterte Verfahren befolgen Erstellen Sie Genehmigungsregeln Abschnitt. Wenn eine Genehmigungsregel für die Smart Response-Regel konfiguriert ist, wird zuerst der Genehmigungs-Flow ausgelöst, und nach Erhalt aller Genehmigungen wird der Smart Response-Optionsflow ausgelöst. Der Status des DLP-Incidents wird gemäß dem Zielstatus der Antwortoptionszuordnung nach erfolgreicher Ausführung der Antwortoption aktualisiert.

Konfigurieren Sie Symantec DLP-#Integrationseinstellungen

Ändern Sie Symantec#Standardsystemeigenschaften der DLP-Integration.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Prozedur

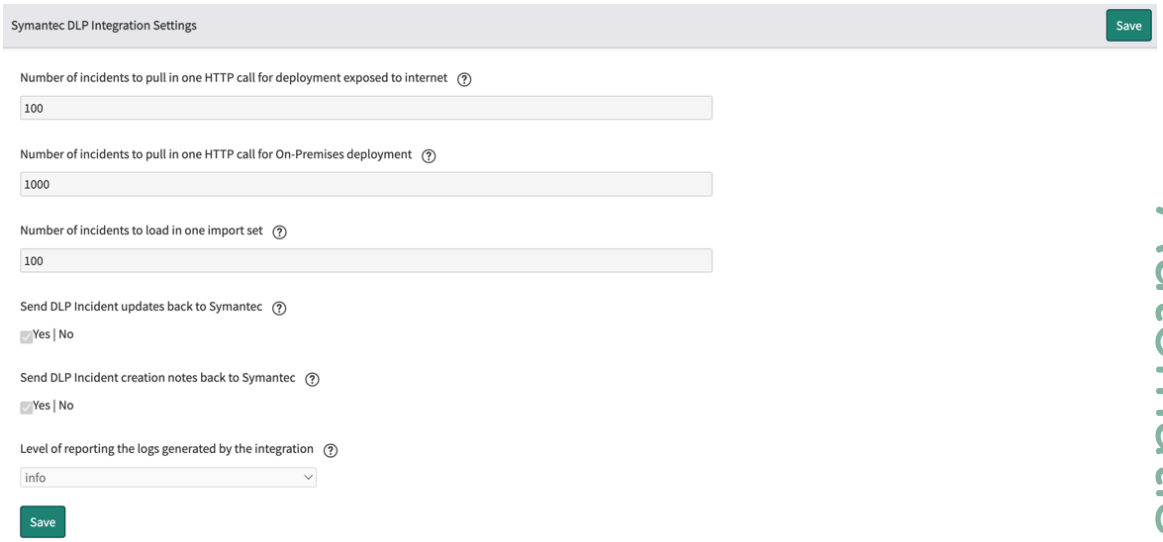
1. Navigieren zu **Symantec DLP-Integration** > **Einstellungen**an.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.

Einstellungen

Feld	Beschreibung
Erzwingen Sie ein Limit für die Anzahl der Incidents, um in einem HTTP-Aufruf für die lokale Bereitstellung sn_sym_dlp.page_size_on_prem abzurufen	Maximale Anzahl von Incidents, die in einem HTTP-Aufruf für die lokale Bereitstellung von abgerufen werden sollen Symantec. ○ Typ: Ganzzahl ○ Standardwert: 1000
Erzwingen Sie einen Grenzwert für die Anzahl der Incidents, um in einem HTTP-Aufruf für die Bereitstellung im Internet sn_sym_dlp.page_size_on_Internet abzurufen	Maximale Anzahl von Incidents, die in einem HTTP-Aufruf für abgerufen werden sollen Symantec Bereitstellung für das Internet verfügbar. ○ Typ: Ganzzahl ○ Standardwert: 100
Anzahl der Incidents, die in einem Importsatz geladen werden sollen sn_sym_dlp.incidents_per_attachment	Anzahl der Datensätze, die zur Verarbeitung in einer Anhangdatei gespeichert werden sollen. ○ Typ: Ganzzahl ○ Standardwert: 100
Senden Sie DLP-Incident-Updates zurück an Symantec sn_sym_dlp.incident_update	Mit dieser Eigenschaft können Sie die Statussynchronisierung zwischen einschränken ServiceNow Und Symantec DLP-Incidents. ○ Typ: Boolesch ○ Standardwert: **true**
Senden Sie DLP-Incident-Erstellungshinweise an Symantec sn_sym_dlp.incident_creation_notes zurück	Mit dieser Eigenschaft können Sie eine Notiz an Symantec zurücksenden, sobald ein Incident in erstellt wird ServiceNow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	○ Typ: Boolesch ○ Standardwert: **true**
Ebene der Berichterstellung der von der Integration „sn_sym_dlp.Logging.verbosity“ generierten Protokolle	Eigenschaft, die die Berichterstellung der von der Integration generierten Protokolle definiert.



3. Klicken Sie auf **Speichern**.

Domänentrennung in Symantec DLP-Integration

Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Supportstufe

Support: Standard.

Funktionsweise der Domänentrennung Symantec DLP-Integration

Führen Sie die folgenden Schritte aus, um die Domänentrennung zu erreichen:

- Erstellen Sie einen Anwender mit der erforderlichen Rolle in der jeweiligen Domäne.
- Führen Sie aus Symantec DLP-Integrationsverfahren in der entsprechenden Domäne.

Integration der Reaktion auf Incidents zur Vermeidung von Datenverlust mit Proofpoint

Die Proofpoint Die DLP-Integration unterstützt die Erfassung von Incidents zur Vermeidung von Datenverlust, die auf erstellt wurden Proofpoint Datenverlustvermeidung – Bereitstellung. Nach der Erfassung können Sie die Incident-Management-Funktionen verwenden, um DLP-Incidents zu beheben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht und wichtige Funktionen

Die Proofpoint Die DLP-Integration hilft Unternehmen, die Nutzung und Bewegung vertraulicher Daten auf verschiedenen Plattformen nachzuverfolgen.

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Erstellung mehrerer Profile für verschiedene Proofpoint Endpunkte.
- Automatisierung der Erstellung von DLP-Incidents.
- Zuordnung von Proofpoint DLP-Incident-Statusfeld zu DLP-Incident-Statusfeld.
- Filterung von Proofpoint DLP-Incidents.
- Erfassung von Incidents in Ihrem ServiceNow Instanz, sobald die Incidents am erstellt werden Proofpoint DLP-Mandant.
- Proofpoint Die DLP-Integration unterstützt sowohl Endpunkte als auch E-Mail-Typ von Incidents.
- Automatische Updates für Proofpoint DLP-Incident-Status und Kommentare für die Erstellung von DLP-Incidents sowie für Statusänderung und Abschluss am ServiceNow Seite.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
Proofpoint Produktdokumentations-Website	Proofpoint-Produktdokumentation
ServiceNow® Produktdokumentations-Website	ServiceNow-Produktdokumentationswebsite

Erste Schritte mit Proofpoint Integration zur Vermeidung von Datenverlust

Die Proofpoint Die DLP-Integration unterstützt die Erfassung von Incidents zur Vermeidung von Datenverlust, die auf erstellt wurden Proofpoint Mandant zur Vermeidung von Datenverlust. Nach der Erfassung werden die Incident-Management-Funktionen verwendet, die DLP-Incidents beheben.

Prüfliste

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihres beginnen Proofpoint DLP-Integration für die Vermeidung von Datenverlust.

Prüfliste

Feld	Beschreibung
Überprüfen Sie, ob Sie die erforderlichen zugewiesen haben ServiceNow AI Platform Und Data Loss Prevention Incident Response Anwendungsrollen.	Die folgenden Rollen werden im verwendet Proofpoint DLP-Integration auf dem ServiceNow AI Platform:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Feld	Beschreibung
	• Der Administrator (Administrator) installiert die -Anwendungen aus dem ServiceNow® Store Und weist den Administrator zur Vermeidung von Datenverlust (sn_dlir.admin) zu. • Der Anwender mit der Rolle „sn_dlir.admin“ kann die Integration konfigurieren und die Incident-Profile einrichten. • Die Anwender mit der Rolle „sn_dlir.Analyst“ verfügen über Leserollen in der gesamten Integration.
Weisen Sie die erforderlichen zu Proofpoint DLP-Anwenderrollen.	Überprüfen Sie Proofpoint DLP-Integrationsrollen und -Berechtigungen.
Überprüfen Sie, ob Sie verwenden Proofpoint DLP 1.0.1 oder höher.	Die Proofpoint Die DLP-Integration für die Vermeidung von Datenverlust wird mit getestet Proofpoint Vermeidung von Datenverlust, Version 1.0.1 oder höher.
Verifiziert, ob die Endanwender-Core-Anwendung zur Unterstützung von erforderlich ist Proofpoint DLP-Integration ist installiert und aktiviert.	Überprüfen Sie, ob die folgenden allgemeinen DLP-Anwendungen und Sicherheitssupport-Anwendungen in installiert und aktiviert werden ServiceNow Speichern. Wenn nicht installiert, installieren Sie die Anwendung, und aktivieren Sie sie. • Security Support Common • Reaktion auf Incident zur Vermeidung von Datenverlust

Installieren und konfigurieren Sie Proofpoint Integration zur Vermeidung von Datenverlust

Installieren und konfigurieren Sie Proofpoint DLP-Integration aus dem ServiceNow® Store Auf Ihrem ServiceNow AI Platform Instanz. Beginnen Sie mit der Untersuchung von DLP-Incidents mit Proofpoint DLP-Incident-Daten.

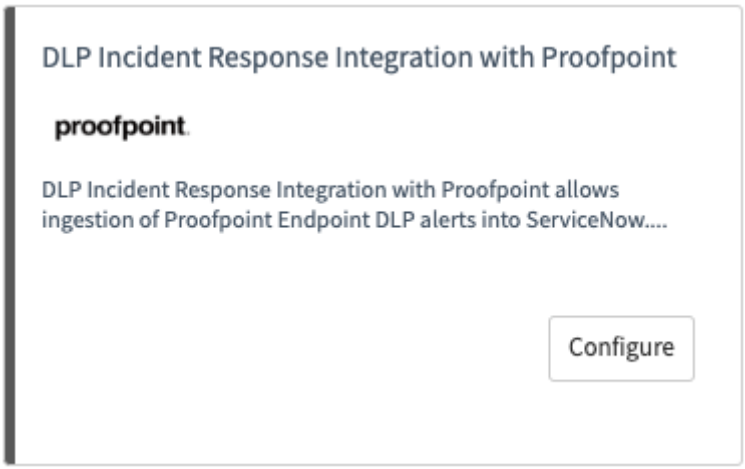
Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Prozedur

1. Laden Sie herunter Proofpoint DLP-Integration aus dem ServiceNow® Store Und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie nach Integration von DLP Incident Response mit Proofpoint Kachel und klicken Sie auf **Konfigurieren** .

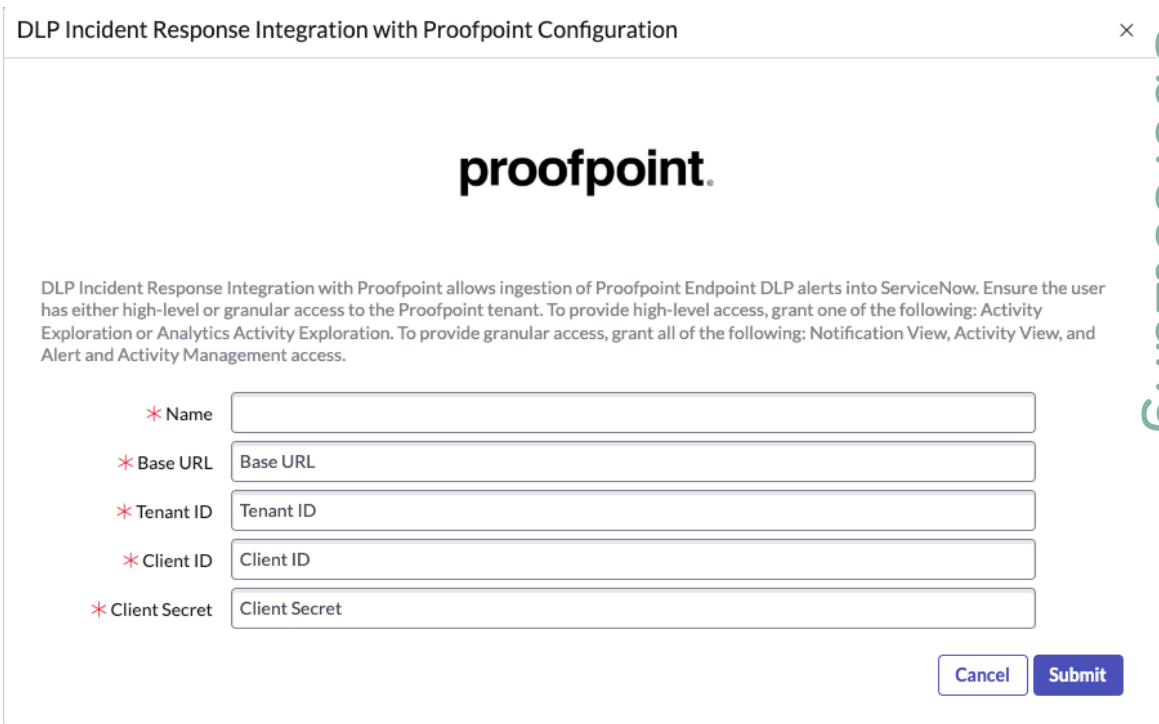
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie im Formular die Felder aus.

Proofpoint Formular „DLP-Integrationskonfiguration“

Feld	Beschreibung
Name	Name des Proofpoint DLP-Integrationskonfiguration.
Basis-URL	URL für Proofpoint Der als REST-Endpunkt dient.
Client-ID	Die ID von Proofpoint Zu verwendender Client.
Geheimer Clientschlüssel	Das für Ihren Anwenderaccount in konfigurierte Geheimnis Proofpoint.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Für Bestandskunden unterstützen wir weiterhin die Standardauthentifizierung, um sicherzustellen, dass die vorhandenen untergeordneten Kacheln, die wie erwartet eine Standardauthentifizierungsfunktion haben. Wenn ein Kunde jedoch OAuth einer untergeordneten Kachel hinzufügen möchte, darf er die vorhandenen Anmeldeinformationen für die Standardauthentifizierung (Anwendername und Passwort) nicht entfernen. Diese Werte können zwar durch Dummy-Einträge ersetzt werden, wenn die Felder jedoch leer bleiben, kann die Kachel nicht erfolgreich übermittelt werden.

5. Klicken Sie auf **Absenden**.

Ergebnisse
Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird Proofpoint DLP-Integration wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Konfigurieren Sie den Webhook auf der Proofpoint DLP-Mandant für Warnungsbenachrichtigungen an ServiceNow

Konfigurieren Sie einen Webhook auf Proofpoint Verwenden des REST-API-Endpunkts, um mit dem Abrufen der Warnungen von zu beginnen Proofpoint DLP-Mandant. Ihr ServiceNow Instanz erstellt DLP-Incidents aus diesen Warnungen. Die Proofpoint Die DLP-Integration bietet Endanwendern einen REST-API-Endpunkt zum Konfigurieren des Webhooks.

Vorbereitungen
Erforderliche Rolle: sn_PP_dlp.api_Integration_user

Prozedur

1. Melden Sie sich bei an **Proofpoint** .
2. Navigieren zu **Proofpoint-Mandant** > **Administrationsanwendung** > **Integration** > **Benachrichtigungsrichtlinien**an.
3. Erstellen Sie eine Benachrichtigungsrichtlinie mit einem entsprechenden Namen.
4. Klicken Sie auf **Benachrichtigungsrichtlinie** Und verwalten Sie die in der Benachrichtigungsrichtlinie konfigurierten Webhooks.
5. Erstellen Sie eine neue Webhook-Konfiguration, indem Sie auf klicken **Fügen Sie Webhooks Hinzu** .
6. Wählen Sie den Webhook-Typ als aus **Generisch** .
7. Geben Sie unter URL-Eingabe eine URL im folgenden Format ein: `https://<Instance_Name>.service-now.com/api/sn_pp_dlp/proofpointalertapi/getalerts` .
8. Behalten Sie die Methode als bei **VERÖFFENTLICHEN** .
9. Fügen Sie dem Webhook die folgenden Header hinzu:
   - ```
     Name: Authorization
     Value: Basic <Base64Encoded Username and Password of the ServiceNow instance user>
     ```
   - ```
     Name: Content-Type
     Value: application/json
     ```
10. D ändern Sie die anderen Werte nicht.
11. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Navigieren zu **Proofpoint-Mandant** > **Administrationsanwendung** > **Richtlinien** > **Bedingungen**an.
13. Wählen Sie im Abschnitt Aktionen die Regeln aus, für die die Webhook-Benachrichtigung generiert werden soll.
14. Fügen Sie die neu erstellten Benachrichtigungsrichtlinien hinzu, für die ein Webhook konfiguriert ist.
15. Klicken Sie auf **Speichern**.

Erstellen Sie eine Anwendung in Proofpoint Und Client-Anmeldeinformationen abrufen

Erstellen Sie eine Anwendung in Proofpoint Und konfigurieren Sie die erforderlichen Einstellungen, um Client-Anmeldeinformationen zu erhalten. Diese Anmeldeinformationen ermöglichen sicheren Zugriff auf die API von Proofpoint für eine nahtlose Integration und Automatisierung.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Melden Sie sich bei an Proofpoint Konsole.
   Greifen Sie auf zu Proofpoint Konsole mit Ihren Anmeldeinformationen.
2. Erstellen Sie eine neue Anwendung.
   a. In **Entwickler** Wählen Sie Autorisierung aus.
   b. Wählen Sie **Erstellen** aus.
   c. Geben Sie einen Anwendungsnamen ein.
   d. Fügen Sie Ihrer Anwendung unter zulässige Umfänge nach Bedarf Umfänge hinzu.
   e. Wählen Sie unter zulässige Zuschüsse die Option aus **Client-Anmeldeinformationen** .
   f. Wählen Sie **Speichern**.
   Client-ID und geheimer Client-Schlüssel werden generiert.
3. Konfigurieren Sie Anwendungsdetails.
   a. Wählen Sie die neu erstellte Anwendung aus.
   b. Wählen Sie in den Zugriffsrichtlinien die Option aus **Bearbeiten** .
   Wählen Sie entweder Zugriffsrichtlinien auf hoher Ebene oder granulare Ebene aus.
   c. Wählen Sie **Fertig**.

Ergebnisse

Verwenden Sie die generierte Client-ID und das geheime Client-Geheimnis, um die Integration in DLP zu konfigurieren Proofpoint(PPT)-Anwendung und beginnen Sie mit der Verwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Profil für Proofpoint DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrem ServiceNow AI PlatformInstanz. Bestimmen Sie Proofpoint DLP-Incidents, die zum Erstellen von DLP-Incidents geeignet sind.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie ServiceNow AI PlatformZum Ausfüllen von DLP-Warnungen von Proofpoint. Speichern Sie die Warnungen als DLP-Incidents in Ihrem ServiceNow Instanz.

Prozedur

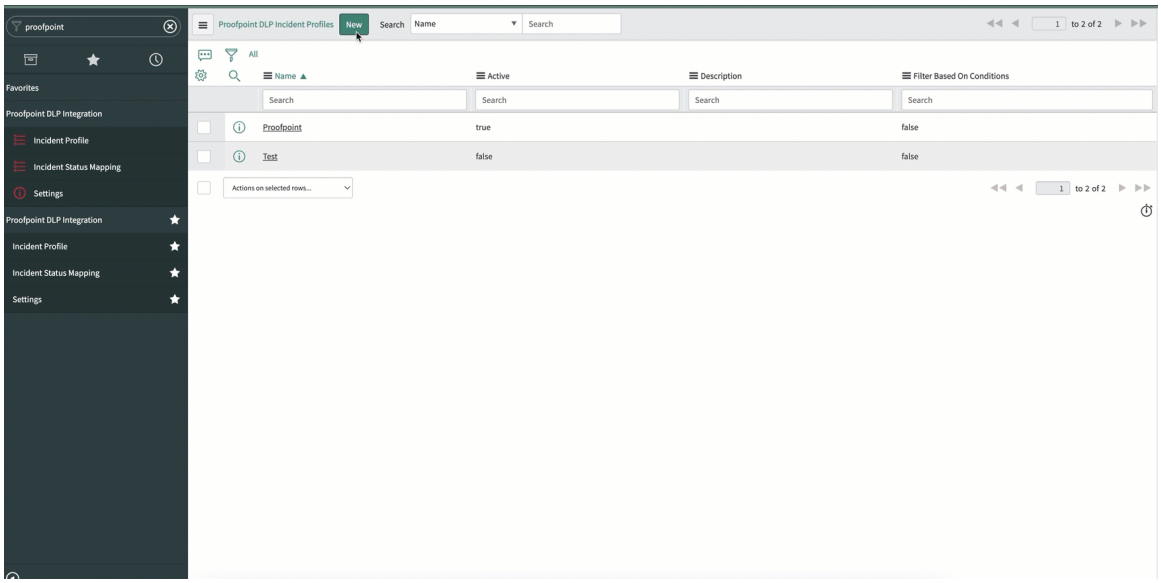
1. Navigieren zu **Proofpoint-DLP-Integration** > **Incident-Profil**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder im aus **Name** Abschnitt.

Erstellen Sie ein Profil für Proofpoint DLP-Integrationsformular

Feld	Beschreibung
Name	Name des Profils. Dieser Name hilft Ihnen, das Profil zu identifizieren. **Hinweis:** De Name muss für jedes Profil eindeutig sein.
Quelle	Die Proofpoint DLP-Instanz, die Sie zum Erfassen von Incidents konfiguriert haben. Wenn Sie mehrere Instanzen konfiguriert haben, wählen Sie die entsprechende Instanz für die Incident-Typen aus, die Sie für das Profil erfassen möchten.
Aktiv	Option zum Aktivieren des Profils. Wenn das Profil aktiv ist, ist Ihr ServiceNow AI Platform Instanz ist bereit, die Incidents von zu empfangen Proofpoint.
Beschreibung	Beschreibung, die hilft, dieses Profil von anderen Profilen zu unterscheiden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie Auf **Fahren Sie Fort** Und wechseln Sie zum Abschnitt Filterung.

Definieren Sie Filter, die für die Incident-Erstellung angewendet werden sollen

Definieren und legen Sie Filterbedingungen fest, um eingehende zu filtern Proofpoint DLP#-Incidents. Steuert, für welche DLP-Incidents erstellt werden sollen ServiceNow®.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

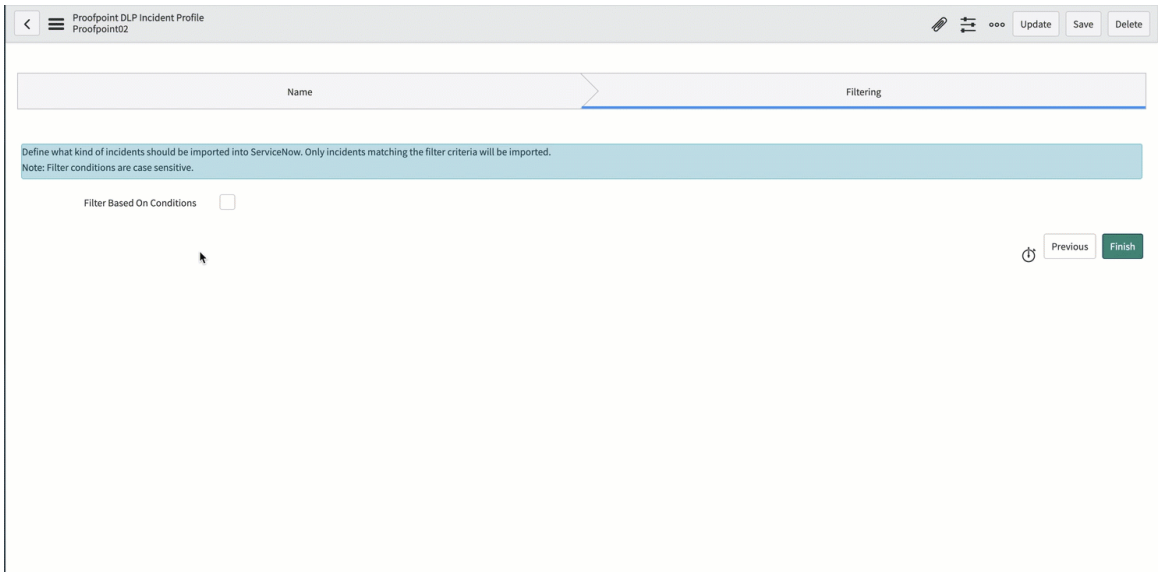
Diese Art der Filterung hilft Ihnen, DLP-Incidents zu isolieren und die Anzahl der von Ihnen erstellten DLP-Incidents zu begrenzen. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur Incidents erstellt, die den Bedingungen entsprechen.

Prozedur

1. Wählen Sie aus **Filtern Sie basierend auf Bedingungen** Option und definieren Sie die Kriterien, die ein eingehender Proofpoint DLP-Incident muss erfüllen, damit ein Security Incident erstellt wird.
2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter in fest **Filterbedingungen** Feld.

   Die Optionen im ersten Feld in **Filterbedingungen** Stimmt mit den Feldern überein, die im DLP-Incident verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Überprüfen Sie, ob die von Ihnen definierten Kriterien mit den Werten des Incident übereinstimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Fügen Sie weitere Bedingungen hinzu, indem Sie auf klicken **UND** #Oder**ODER** .
   - Wenn **UND** #Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** #Ist ausgewählt, kann eine der Bedingungen erfüllt werden.
4. Klicken Sie auf **Fertigstellen**.

Vorschau der Nachweisdateien anzeigen

Vorschau Data Loss Prevention Incident Response Nachweisdateien im DLP-IR-Analyst-Arbeitsbereich.

Vorbereitungen

Wichtig:
Bei der Verwendung der Aktion „Nachweisdateien“ im DLP-Analysten-Arbeitsbereich werden die Nachweisdateien vorübergehend in der ServiceNow-Datenbank in einem unverschlüsselten Format gespeichert. Wenn Sie die Nachweisdateien nicht speichern möchten, deaktivieren Sie die Vorschaufunktion für Nachweisdateien. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Erforderliche Rolle: sn_dlir.Analyst

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
2. Öffnen Sie einen DLP-Incident-Datensatz.
3. Wählen Sie in der kontextbezogenen Sidebar das Symbol für Nachweisdateien ( ).
4. Auf der **Nachweisdateien** Wählen Sie die Registerkarte aus **Nachweisdatei** Karte zur Vorschau der Nachweisdateien im Dokument-Viewer.

   Die Vorschaufunktion unterscheidet sich für jeden Dateityp, wie in der folgenden Tabelle aufgeführt.

Dateiformat	Dateierweiterung
Bild	.Bmp, .gif, .ico, .JPEG, .jpg, .png, .svg und .webp.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateiformat	Dateierweiterung
	Bilddateien werden im Dokument-Viewer-Modus geöffnet.
Microsoft Office-Dateien	.Doc, .docx, .ppt, .pptx, .xls, und .xlsx Office-Dateien werden im Dokument-Viewer-Modus geöffnet.
Textdateien	.txt Textdateien werden im Texteditor-Modus geöffnet.
E-Mail-Dateien	.Eml **Hinweis:** Die Dateigröße muss weniger als 5 MB betragen. Sie müssen zuerst die Datei herunterladen, um eine Vorschau des Inhalts anzuzeigen.
PDF-Dateien	.PDF ○ Geben Sie ein Stichwort ein, um das Dokument zu durchsuchen. ○ Zoom- und Verkleinerungsfunktionen, um die Ansicht für eine bessere Lesbarkeit anzupassen. ○ Drehen Sie die Seite im Uhrzeigersinn oder gegen den Uhrzeigersinn, um den Inhalt klarer anzuzeigen.

Hinweis:

Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion „Vorschaunachweisdatei“ funktioniert auch für archivierte Incidents.

Zuordnung Proofpoint DLP-Incident-Status mit ServiceNow Incident-Status

Synchronisieren Sie den Status der DLP-Incidents, die in erfasst wurden ServiceNow Instanz- und DLP-Incidents von Proofpoint. Ordnen Sie zu ServiceNow Incident-Status mit Proofpoint Incident-Status.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Prozedur

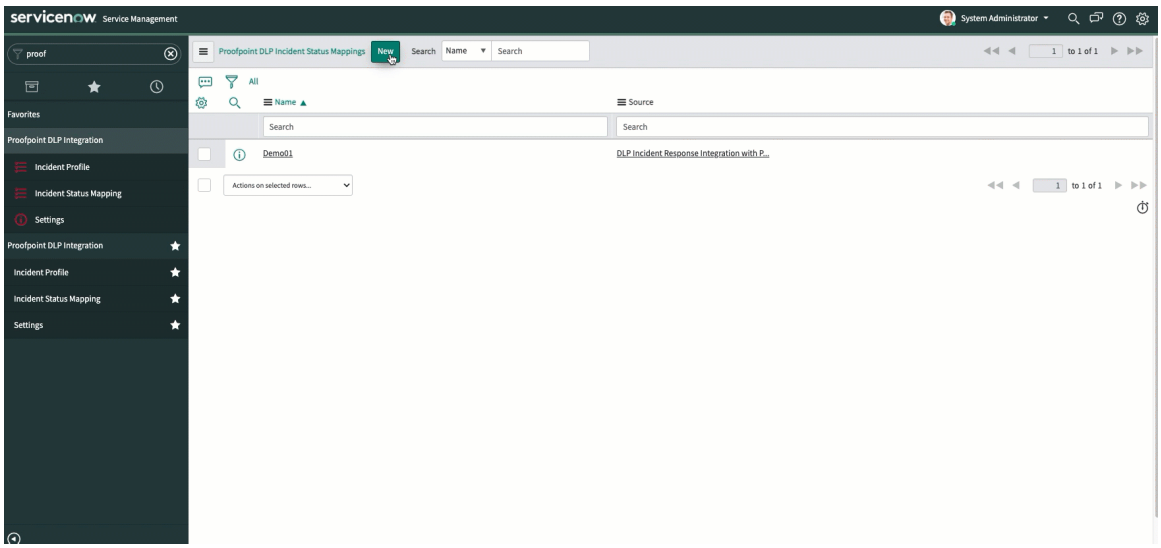
1. Navigieren zu **Proofpoint-DLP-Integration** > **Incident** > **Incident-Statuszuordnung**an.
2. Geben Sie ein an **Name** Um die Zuordnung zu identifizieren.
3. Wählen Sie aus **Quelle** Kachel (Integrationskonfiguration), für die die Statuszuordnung angewendet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Ordnen Sie zu **ServiceNow-DLP-Incident-Status** Mit **Status Des Proofpoint-Incidents** .

Ordnen Sie den Status von Proofpoint-DLP-Incidents dem ServiceNow-Incident-Statusformular zu

Feld	Beschreibung
Name	Platzhalter für den Zuordnungsdatensatz.
Quelle	Konfiguriert Proofpoint Endpunktquelle, aus der Sie den Incident-Status abrufen möchten.
ServiceNow-Incident-Status	Liste des Status von DLP-Incidents.
Status Des Proofpoint-Incidents	Standardmäßig zugeordnete Werte für standardstatus, die in DLP-Incidents verfügbar sind. Für anwenderdefinierte status der Standard Proofpoint Status ist **Neu** . Sie können die erforderlichen ändern und hinzufügen Proofpoint Status im Eingabefeld.



5. Klicken Sie auf **Absenden**.

Ergebnisse

Ein Datensatz für die Zuordnung wurde erfolgreich erstellt. Die Status von ServiceNow Incidents werden mit synchronisiert Proofpoint DLP-Incidents.

Wenn Sie den Status eines DLP-Incidents auf Ihrem ändern ServiceNow Instanz, dann der Status der zugeordneten Proofpoint DLP-Incident wird in der Quelle geändert Proofpoint Plattform gemäß dem Zuordnungssatz im Datensatz.

Konfigurieren Proofpoint DLP-Integrationseinstellungen

Ändern Sie Proofpoint#Standardsystemeigenschaften der DLP-Integration.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Proofpoint-DLP-Integration** > **Einstellungen**an.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.
3. Klicken Sie auf **Speichern**.

Ergebnisse

Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

Domänentrennung in Proofpoint DLP-Integration

Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Supportstufe

Support: Standard.

Funktionsweise der Domänentrennung Proofpoint DLP-Integration

Führen Sie die folgenden Schritte aus, um die Domänentrennung zu erreichen:

- Erstellen Sie einen Anwender mit der erforderlichen Rolle in der jeweiligen Domäne.
- Führen Sie aus Proofpoint DLP-Integrationsverfahren in der entsprechenden Domäne.

Integration der Reaktion auf Incidents zur Vermeidung von Datenverlust mit Netskope

Die Netskope Die DLP-Integration unterstützt die Erfassung von Incidents zur Vermeidung von Datenverlust, die auf erstellt wurden Netskope Datenverlustvermeidung – Bereitstellung. Netskope DLP hilft Unternehmen, die Nutzung und Bewegung vertraulicher Daten auf verschiedenen Plattformen nachzuverfolgen.

Nach der Erfassung können Sie die Incident-Management-Funktionen verwenden, um DLP-Incidents zu beheben.

Schlüsselfunktionen

Diese Integration umfasst die folgenden wichtigen Funktionen:

- Erstellung mehrerer Profile für verschiedene Netskope Mandanten.
- Automatisieren der Erstellung von ServiceNow DLP-Incidents aus Netskope DLP-Incidents.
- Filterung von Netskope DLP-Incidents.
- Geplante Erfassung von Netskope DLP-Incidents, die DLP-Incidents in ServiceNow erstellen.
- Objektstatus für automatisch aktualisieren Netskope Wenn sich der DLP-Status in Ihrer ServiceNow-Instanz ändert.
- Zeigen Sie die forensischen Details (verletzender Inhalt) des DLP-Incidents im DLP-IR-Analyst-Arbeitsbereich und im DLP-Endanwender-Arbeitsbereich an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Der verstoßende Inhalt wird in ServiceNow nicht beibehalten. Der Inhalt wird abgerufen, wenn sich der Incident im Arbeitsbereich geöffnet befindet.

- Nachweisdatei wird direkt aus heruntergeladen Netskope Bei Bedarf.

Hinweis:
Die Nachweisdatei wird in ServiceNow nicht beibehalten. Die Nachweisdatei wird abgerufen, wenn der Analyst auf klickt **Datei Herunterladen** Im Arbeitsbereich.

- Benachrichtigung per E-Mail an DLP-Administratoranwender auf Netskope Token-Ablauf.
- Eine Benachrichtigung per E-Mail wird an DLP-Administratoranwender gesendet, wenn die definierte Wiederholungsgrenze für Fehler beim API-Aufruf von Incidents überschritten wird.
- Netskope Unterstützt auch den Integrationsausführungsprozess. Weitere Informationen finden Sie unter Überwachen Sie den DLP-Integrationsausführungsprozess.

Erste Schritte mit Netskope DLP-Integration für die Vermeidung von Datenverlust

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihres beginnen Netskope DLP-Integration für die Vermeidung von Datenverlust.

Setup-Aufgabe	Beschreibung
Verifizieren Sie, dass Sie die erforderliche Now-Plattform, die Anwendung zur Vermeidung von Datenverlust, zugewiesen haben.	Die folgenden Rollen werden im verwendet Netskope DLP-Integration auf dem ServiceNow AI Platform: • Der Administrator (Administrator) installiert die -Anwendungen aus dem ServiceNow Store Und weist den Administrator zur Vermeidung von Datenverlust (sn_dlir.admin) zu. • Der Anwender mit der Rolle „sn_dlir.admin“ kann die Integration konfigurieren und die Incident-Profile einrichten. • Die Anwender mit der Rolle „sn_dlir.Analyst“ haben Leserollen in der gesamten Integration.
Weisen Sie die erforderlichen Berechtigungen für zu Netskope API v2-Token.	Die folgenden Endpunktberechtigungen werden im verwendet Netskope API v2-Tokenisierung. • Lesen Sie: /api/v2/Incidents/dlpIncidents • Lesen Sie: /api/v2/Events/dataexport/Events/Incident • Lesen + Schreiben: /api/v2/Incidents/Update
Verifiziert, ob die Endanwender-Core-Anwendung zur Unterstützung von erforderlich ist Netskope DLP-Integration ist installiert und aktiviert.	Überprüfen Sie, ob die folgenden allgemeinen DLP-Anwendungen und Sicherheitssupport-Anwendungen in installiert und aktiviert werden ServiceNow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setup-Aufgabe	Beschreibung
	Speichern. Wenn nicht installiert, installieren Sie die Anwendung, und aktivieren Sie sie. • Security Support Common • Reaktion auf Incident zur Vermeidung von Datenverlust

Installieren und konfigurieren Sie Netskope DLP-Integration für die Vermeidung von Datenverlust

Installieren und konfigurieren Sie Netskope DLP-Integration von ServiceNow StoreServiceNow AI Platform Instanz. Sie können mit der Untersuchung von DLP-Incidents beginnen Netskope DLP-Incident-Daten.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

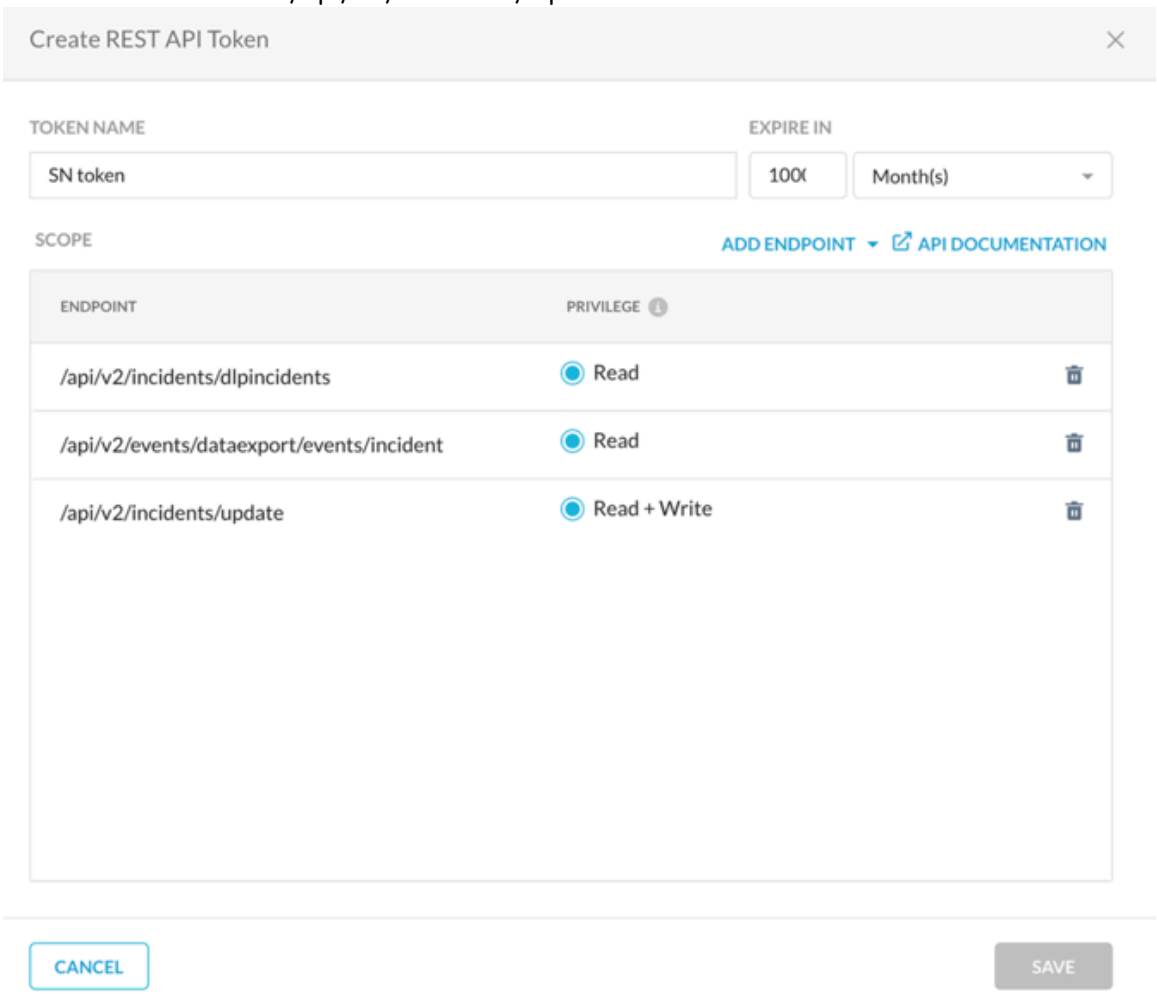
Prozedur

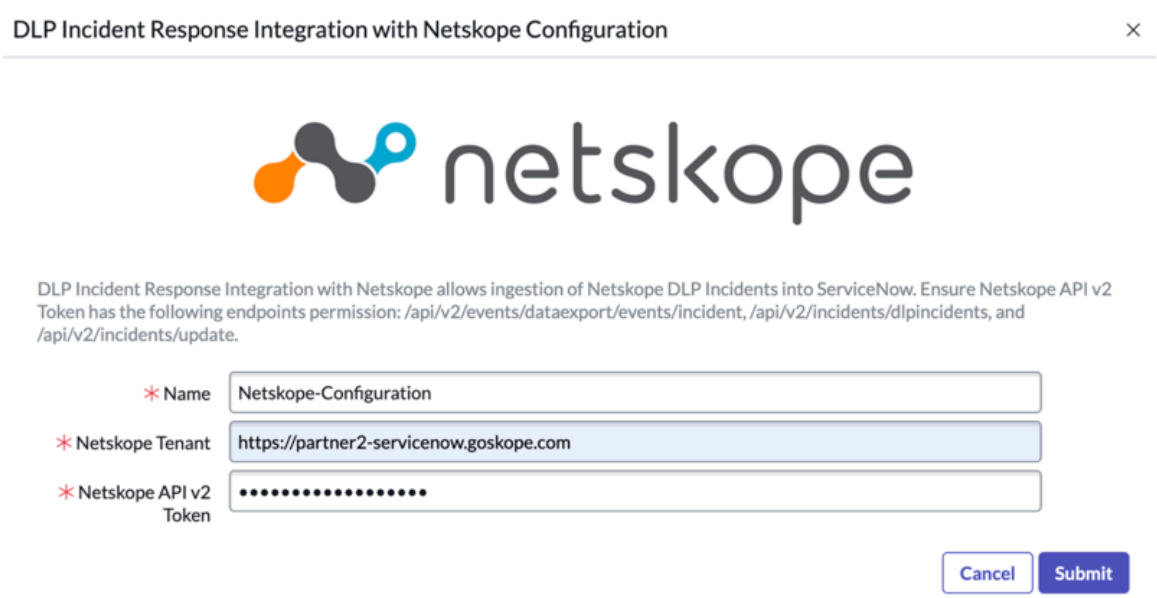
1. Laden Sie herunter Netskope DLP-Integration aus dem ServiceNow Store Und installieren Sie es.
2. Navigieren Sie zu #**Security Operations** > **Integrationen** > **Integrationskonfigurationen**
3. Suchen Sie nach Integration von DLP Incident Response mit Netskope Kachel und klicken Sie auf **Konfigurieren** .
4. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Stellen Sie sicher, dass Netskope API v2-Token verfügt über die folgenden Endpunktberechtigungen:

- Lesen Sie: /api/v2/Incidents/dlpIncidents
- Lesen Sie: /api/v2/Events/dataexport/Events/Incident
- Lesen + Schreiben: /api/v2/Incidents/Update





Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name des Netskope DLP-Integrationskonfiguration.
Netskope-Mandant	Die Netskope Basis-URL für Netskope Mandant.
Netskope-API-v2-Token	Token, das für REST API v2 in Ihrem Anwenderaccount unter konfiguriert ist Netskope.

5. Klicken Sie auf **Absenden**.

Ergebnisse

Hinweis:
Verbinden Sie die netskope-Subprod mit der ServiceNow-Subprod. Halten Sie alle Anwendernamen und Passwörter in allen Instanzen synchron, um zu vermeiden, dass Accounts abgemeldet werden.

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird Netskope DLP-Integration wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Erstellen Sie ein Profil für Netskope DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrem ServiceNow AI Platform Instanz.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren ServiceNow AI Platform Dient zum Abrufen der DLP-Incidents aus der Netskope Endpunkt. Speichern Sie die Incidents in Ihrem ServiceNow Instanz als DLP-Incidents.

Prozedur

1. Navigieren zu **Netskope-DLP-Integration** > **Incident-Profil**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder aus.

Erstellen Sie ein Profil

Feld	Beschreibung
Name	Name des Profils. De Name muss für jedes Profil eindeutig sein. Dieser Name hilft Ihnen, das Profil zu identifizieren.
Quelle	Netskope DLP-Instanz, die Sie zum Erfassen von Incidents konfiguriert haben. Wenn Sie mehrere Instanzen konfiguriert haben, wählen Sie die entsprechende Instanz für die Incident-Typen aus, die Sie für das Profil erfassen möchten. **Hinweis:** Pro Quelle ist nur ein aktives Profil zulässig.
Aktiv	Indikator, dass das Profil aktiv ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Dieses Feld ist erst verfügbar, nachdem Sie auf geklickt haben **Beenden** Im Abschnitt Letzte Planung. Wenn das Profil aktiv ist, ist Ihr ServiceNow AI Platform Instanz fragt aktiv ab Netskope DLP-Incidents. Entsprechende DLP-Incidents werden als ServiceNow-DLP-Incidents erstellt, wenn die Filterbedingungen basierend auf den von Ihnen angegebenen Zeitplanungsparametern erfüllt werden.
Reihenfolge	Reihenfolge der Profilausführung. Das Profil mit der niedrigsten Reihenfolge, das als höchste Priorität betrachtet wird. Standardmäßig ist der Wert 100.
Beschreibung	Beschreibung, die Ihnen hilft, dieses Profil von anderen Profilen zu unterscheiden.

4. Klicken Sie Auf **Fahren Sie Fort** Und wechseln Sie zum Abschnitt Filterung.

Definieren Sie Filter, die für die Incident-Erstellung angewendet werden sollen

Definieren und legen Sie Filterbedingungen fest, um eingehende zu filtern Netskope DLP#-Incidents. Steuern Sie, welche dieser Incidents als DLP-Incidents auf Ihrem erstellt werden sollen ServiceNow Instanz.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Art der Filterung hilft Ihnen, DLP-Incidents zu isolieren und die Anzahl der von Ihnen erstellten DLP-Incidents zu begrenzen. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur Incidents erstellt, die den Bedingungen entsprechen.

Prozedur

1. Wählen Sie aus **Filtern Sie basierend auf Bedingungen** Option und definieren Sie die Kriterien, die ein eingehender Netskope-DLP-Incident erfüllen muss, damit ein DLP-Incident erstellt wird.
2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter in fest **Filterbedingungen** Feld.

   Die Optionen im ersten Feld in **Filterbedingungen** Stimmen Sie die Felder ab, die in verfügbar sind **Import von Netskope-DLP-Incidents** Tabelle. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Überprüfen Sie, ob die von Ihnen definierten Kriterien mit den Werten des Incident übereinstimmen.
3. Fügen Sie weitere Bedingungen hinzu, indem Sie auf klicken **UND** #Oder**ODER** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn **UND** #Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
- Wenn **ODER** #Ist ausgewählt, kann eine der Bedingungen erfüllt werden.

4. Klicken Sie Auf **Fahren Sie Fort** Und wechseln Sie zum Abschnitt Zeitplanung.

Planen Sie Netskope Abruf von DLP-Incidents

Legen Sie einen abzurufenden Zeitplan fest Netskope DLP-Incidents, die den Kriterien im Profil entsprechen.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können planen, wie oft Sie nach Net New abfragen Netskope Incidents, die der Incident-Profilkonfiguration entsprechen. Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Planung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Das Profil kann so konfiguriert werden, dass ein einmaliger Abruf mit durchgeführt wird **Einmaliger Abruf** Kontrollkästchen. Das historische Datum kann bis zu einem Monat aus der Vergangenheit liegen.

Prozedur

1. Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Incidents aus abrufen Netskope.
2. Füllen Sie im Formular die Felder aus.

Planen Sie Netskope DLP-Incidents

Feld	Beschreibung
Laufende Incident-Erfassung	Laufende Incident-Erfassung, die Ihr ServiceNow AI Platform Instanz ruft ab Netskope Für neue Incidents. Wenn ausgelöste Incidents gefunden werden, die den Incident-Filterkriterien entsprechen, werden DLP-Incidents erstellt.
Abfrageschritt (Minuten)	Abfragehäufigkeit, die in Minuten definiert ist. Dieser Standardwert ist auf festgelegt **5** .
Zeitpunkt der ersten Incident-Erfassung festlegen	Option zum Festlegen der ersten Incident-Erfassung basierend auf dem konfigurierten Datum und der konfigurierten Uhrzeit. Sie können diese Option verwenden, um ein bestimmtes Datum und eine bestimmte Uhrzeit für die anfängliche Erfassung zu definieren. Nachfolgende Erfassungen basieren auf dem Abfrageintervall-Zeitraum.
Zeitpunkt der ersten Incident-Erfassung eingeben	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben.
Zeitpunkt der ersten Incident-Erfassung	Das erste Mal, wenn Daten erfasst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Der Wert ist nur sichtbar, wenn **Legen Sie Die Erste Incident-Erfassungszeit Fest** Option ist ausgewählt.
Nächste Incident-Erfassungszeit (geschätzt)	Die nächste geschätzte Incident-Erfassungszeit.
Einmaliger Abruf	Option zum Aktivieren des einmaligen Abrufs von Verlaufsdaten. **Hinweis:** Wenn diese Option ausgewählt ist, werden Verlaufsdaten aus abgerufen Netskope DLP gemäß dem Datum, an dem in hinzugefügt wurde **Seit Datum** .
Seit Datum	Datum, ab dem Daten abgerufen werden Netskope. **Hinweis:** Höchstens die Daten der letzten 30 Tage können aus abgerufen werden Netskope.

3. Klicken Sie auf **Fertigstellen**.
4. Speichern Sie im Popup-Fenster die erstellte Profilkonfiguration, indem Sie auf klicken **Beenden** .
5. Aktivieren Sie das Profil.
   a. Öffnen Sie das erstellte Profil.
   b. Festlegen **Aktiv** Bis **Wahr** .
   c. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Nach der erfolgreichen Aktivierung des Profils werden Incidents regelmäßig gemäß der im Profil festgelegten Konfiguration abgerufen. Die Incidents werden der Tabelle „DLP-Incidents“ hinzugefügt.

DLP-Incident-Status wird zugeordnet Netskope

Im Abschnitt „Incident-Statuszuordnung“ können Anwender Zuordnungen zwischen dem DLP-Incident-Status in ServiceNow und bereitstellen Netskope Objektstatus.

Vorbereitungen

Die Zuordnung wird verwendet, wenn DLP-Incidents von erfasst werden Netskope In ServiceNow sowie Synchronisierung von Statusänderungen von DLP-Incidents in ServiceNow zurück zu Netskope.

Synchronisieren Sie den Status der in ServiceNow erfassten DLP-Incidents mit dem DLP-Incident von Netskope. Ordnen Sie das Feld ServiceNow-Incident-Status dem zu Netskope Objektstatusfeld.

Erforderliche Rolle: sn_dlir.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen eine eins-zu-eins-Incident-Statuszuordnung von erstellen Netskope Und ServiceNow-Status.

Prozedur

1. Navigieren zu **Netskope-DLP-Integration** > **Incident-Statuszuordnung**an.
2. Geben Sie einen Namen an, um die Zuordnung zu identifizieren.
3. Wählen Sie die Quellintegration aus.
4. Ordnen Sie den DLP-Incident-Status zu zu Netskope Objektstatus (Duplikat Netskope status kann auch zugeordnet werden).
   Die Statussynchronisierung von ServiceNow zu Netskope Wird deaktiviert, wenn Sie keinen Zuordnungsdatensatz erstellen.

Wichtig:
Sie müssen alle zuordnen Netskope Objektstatus für alle ServiceNow-Status. Wählen Sie die Quelle aus, mit der der DLP-Incident-Status wieder synchronisiert werden soll Netskope Objekt.

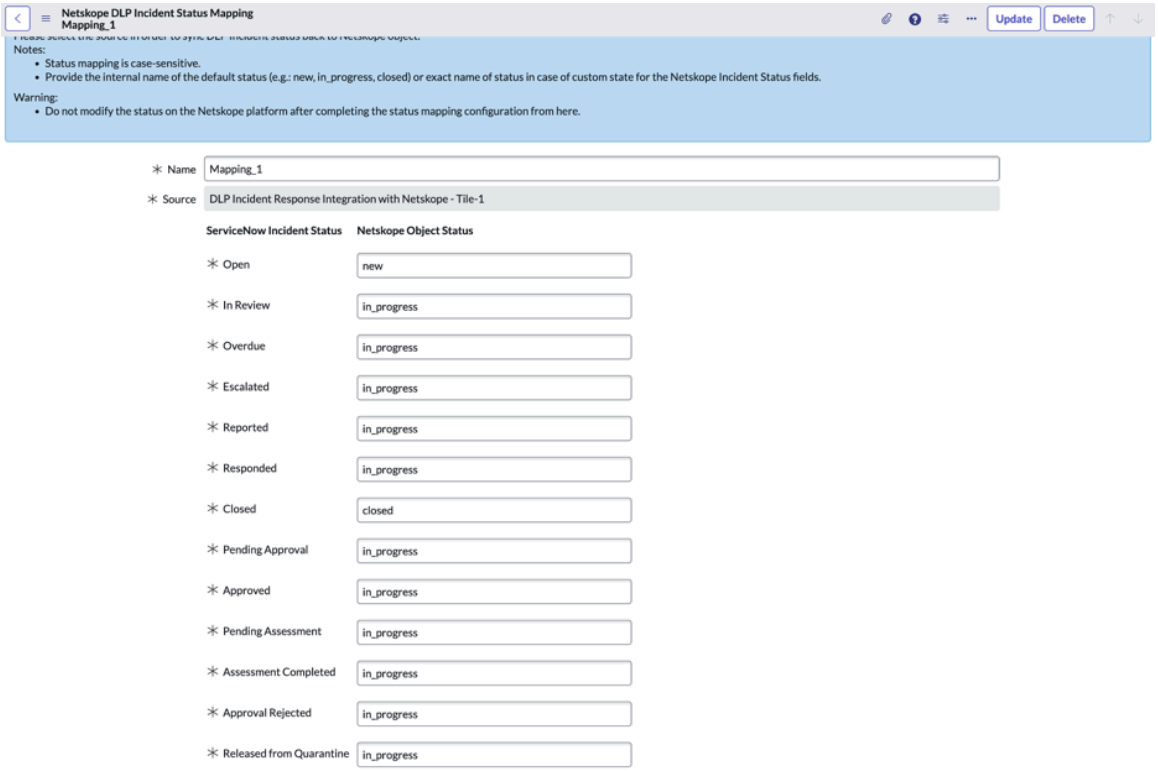
Die folgenden Informationen und Warnmeldungen werden angezeigt, wenn Sie den Incident-Status zuordnen, die Nachrichten überprüfen und fortfahren.

Hinweis:

- Bei der Statuszuordnung wird zwischen Groß- und Kleinschreibung unterschieden.
- Geben Sie den internen Namen des Standardstatus (z. B. New, in_Progress, Closed) oder den genauen Namen des Status an, falls ein anwenderdefinierter Status für vorliegt Netskope Objektstatusfelder.

Warnung:
Ändern Sie den Status nicht in Netskope Plattform nach Abschluss der Statuszuordnungskonfiguration von hier.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Netskope DLP-Incident-Statuszuordnung

Feld	Beschreibung
Name	Name des Zuordnungsdatensatzes.
Quelle	Konfiguriert Netskope Endpunktquelle, von der aus Sie den Incident-Status synchronisieren möchten.
DLP-Incident-Status	Gibt die Liste des Status von DLP-Incidents an.
Netskope Objektstatus	Gibt die Liste von an Netskope Objektstatus.

5. Klicken Sie auf **Absenden**.

Ergebnisse

Nach dem erfolgreichen Erstellen des Datensatzes für die Statuszuordnung wird der Status des ServiceNow DLP-Incidents automatisch angezeigt, wenn der Status des ServiceNow DLP-Incidents aktualisiert wird Netskope Seite gemäß Zuordnung.

Hinweis:
Wenn Sie den Status eines DLP-Incidents in ändern Netskope Mandant direkt, dann die Statussynchronisierung von SN zu Netskope Funktioniert unter Berücksichtigung der API-Einschränkungen nicht. Stellen Sie sicher, dass Sie allen DLP-Incident-Status zuordnen Netskope Objektstatus vorsichtig.

Konfigurieren Netskope DLP-Integrationseinstellungen

Ändern Sie Netskope#Standardsystemeigenschaften der DLP-Integration.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Netskope-DLP-Integration** > **Einstellungen**an.
2. Ändern Sie die folgenden Einstellungen nach Bedarf.

Konfigurieren Netskope DLP-Integrationseinstellungen

Feld	Beschreibung
Soll das Herunterladen der Datei mit Verstoß des gemeldeten Incidents zulässig sein, sn_ns_dlp.enable_file_Download.	Option, um auszuwählen, ob Sie den Download der Datei aktivieren möchten. Standardmäßig ist diese Option aktiviert.
Maximale Zeitüberschreitung für HTTP-Aufrufe, in Sekunden sn_ns_dlp.Maximum_http_time_out.	Maximale Zeitüberschreitung für HTTP-Aufrufe in Sekunden. Dieses Feld wird automatisch auf 30 festgelegt.
Maximale Anzahl von Wiederholungen, die für API-Fehler ausgeführt werden sollen. sn_ns_dlp.Maximum_retry.	Maximale Anzahl von Wiederholungen, die für API-Fehler ausgeführt werden sollen. Der Standardwert ist 3.
Ebene der Berichterstellung der von der Integration „sn_ns_dlp.Logging.verbosity“ generierten Protokolle.	Definieren Sie die Ebene der durch die Integration generierten Berichterstellungsprotokolle. Dieses Feld wird automatisch auf festgelegt **Info** .

3. Klicken Sie auf **Speichern**.

Ergebnisse
Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

Laden Sie Nachweisdateien herunter

Laden Sie Dateien herunter, die gegen die DLP-Richtlinie in verstoßen Netskope. Laden Sie diese Datei aus dem DLP-IR-Analyst-Arbeitsbereich und dem DLP-IR-Endanwender-Arbeitsbereich für Genehmiger auf Ihren lokalen Computer herunter.

Vorbereitungen
Erforderliche Rolle:

- sn_dlir.Analyst
- sn_dlir.secure_file_download (jeder Genehmiger mit dieser Rolle)

Warum und wann dieser Vorgang ausgeführt wird
Sie müssen den Dateidownload für aktivieren Netskope Bevor Sie fortfahren.

Prozedur

1. Navigieren zu **Alle** > **Netskope-DLP-Integration** > **Einstellungen**an.
2. Aktivieren Sie die Eigenschaft **Sollte das Herunterladen der Datei mit Verstoß des gemeldeten Incidents zulässig sein** .
   Sie können sehen **Datei Herunterladen** Schaltfläche im DLP IR Analyst Workspace und DLP IR Endanwenderarbeitsbereich.
3. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
4. Öffnen Sie einen DLP-Incident-Datensatz, der aus erfasst wird Netskope Quelle.
5. Klicken Sie Auf **Datei Herunterladen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Datei, die gegen die DLP-Richtlinie auf der verstößt Netskope Wird auf den lokalen Computer des Anwenders heruntergeladen.

Hinweis:
DLP-Administrator kann den Zugriff von steuern **Datei Herunterladen** Aktion für alle Integrationen durch Deaktivieren von **Sollte das Herunterladen der Datei mit Verstoß des gemeldeten Incidents zulässig sein** Option von **Erweiterte Einstellungen** Seite der DLP-Administration. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Vorschau der Nachweisdateien anzeigen

Vorschau der DLP-Incident-Nachweisdateien im DLP IR-Analyst-Arbeitsbereich anzeigen.

Vorbereitungen

- Navigieren zu **Alle** > **DLP-Administration** > **Erweiterte Einstellungen**an.
- Stellen Sie sicher, dass **sn_ns_dlp.enable_evidence_file_preview** Eigenschaft ist bereits aktiviert.

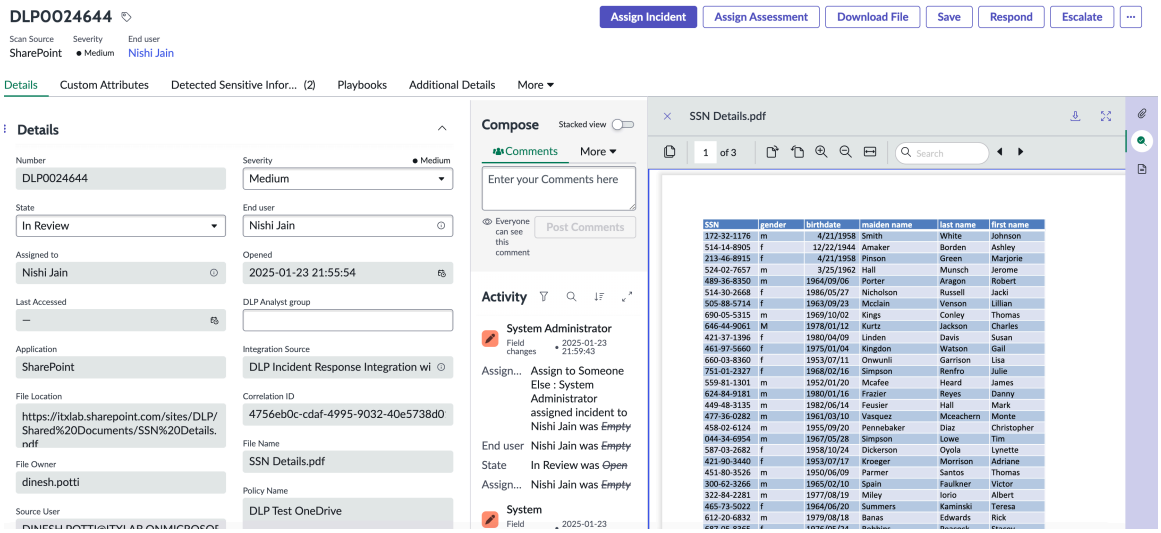
Wichtig:
Bei der Verwendung der Aktion „Nachweisdateien“ im DLP-Analysten-Arbeitsbereich werden die Nachweisdateien vorübergehend in der ServiceNow-Datenbank in einem unverschlüsselten Format für die Dauer gespeichert, die Sie mit ausgewählt haben **sn_dlir.preview_temp_files_cleanup_interval** Eigenschaft von **Erweiterte Einstellungen** Seite. Sie können deaktivieren **Nachweisdateien** Vorschaufunktion, wenn Sie keine Daten in der ServiceNow-Datenbank speichern möchten. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Erforderliche Rolle: sn_dlir.Analyst

Prozedur

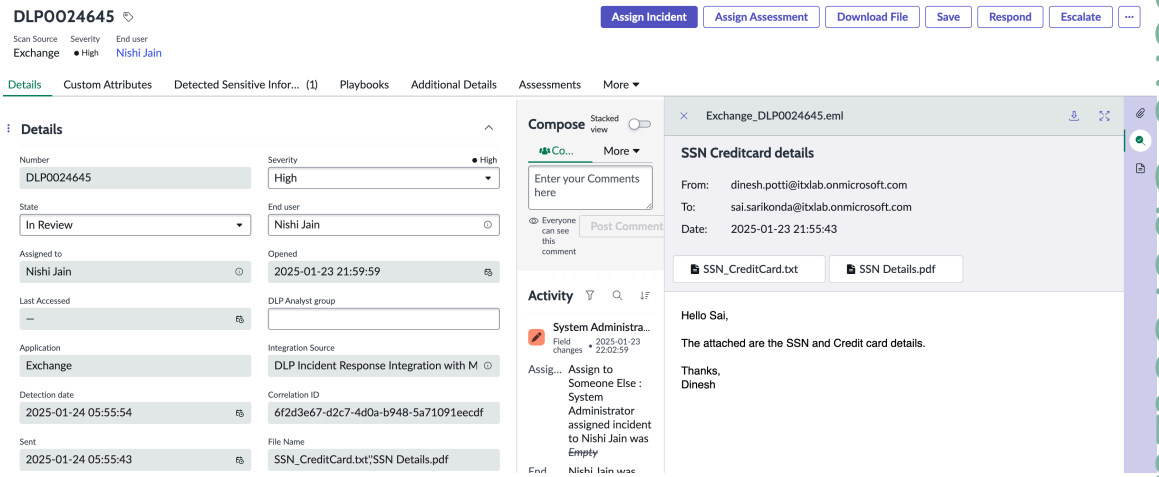
1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
2. Öffnen Sie einen DLP-Incident-Datensatz.
3. Wählen Sie aus **Nachweisdateien** Symbol, das im Kontextmenü verfügbar ist.
   Eine Registerkarte wird geöffnet, auf der alle Nachweisdateien abgerufen werden. Sobald der Download abgeschlossen ist, können Sie alle Nachweisdateien in anzeigen **Nachweisdateien** Registerkarte.
4. Wählen Sie aus **Nachweisdatei** Karte, die Sie in der Vorschau anzeigen möchten.
   Die Vorschaufunktion unterscheidet sich für jeden Dateityp.
5. Zeigen Sie eine Vorschau von PDF- und Office-Dokumenten im Dokument-Viewer an, indem Sie auswählen **Erweitern Sie** Symbol oben rechts in der Nachweisdatei, um die PDF-Datei im Vollbildmodus zu öffnen. Office-Erweiterungen, für die der Dokumentbetrachter die Nachweisdateien öffnet: Doc, docx, ppt, pptx, xls, XLSX.
   a. Suchen Sie die Suchleiste, und geben Sie das gesuchte Stichwort ein.
   b. Verwenden Sie die Funktionen zum Vergrößern und Verkleinern, um die Ansicht für eine bessere Lesbarkeit anzupassen.
   c. Drehen Sie die Seite im Uhrzeigersinn oder gegen den Uhrzeigersinn, um den Inhalt klarer anzuzeigen.
   Diese Steuerungsoptionen verbessern Ihre Fähigkeit, die Nachweisdatei umfassend zu verstehen. Nur die PDF-Datei enthält Steuerungsoptionen im Header.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Eml-Dateien in der Vorschau anzeigen.
Wählen Sie die Anhänge in der E-Mail aus, und zeigen Sie eine Vorschau an.

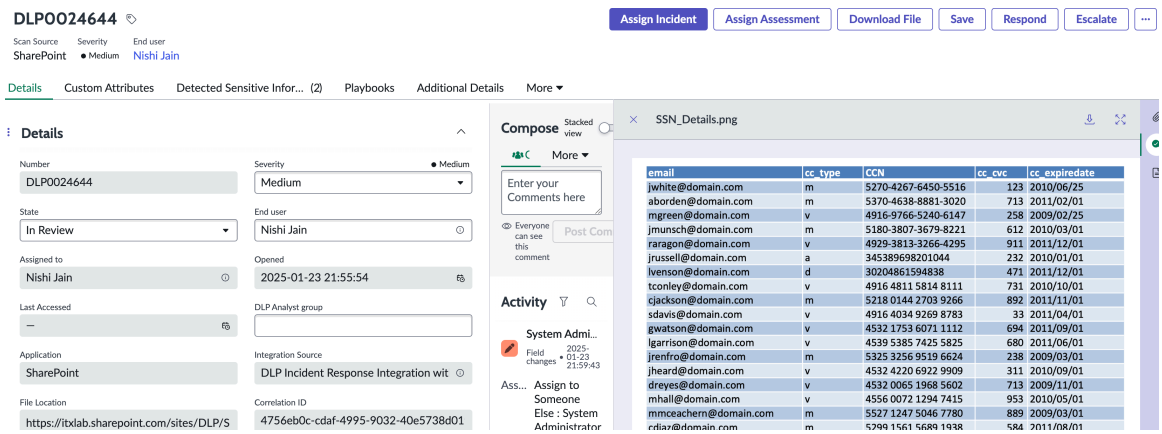
> **Hinweis:**
> Wenn die ausgewählte Nachweisdatei den Grenzwert von 5 MB überschreitet, kann sie im Arbeitsbereich des Analysten nicht in der Vorschau angezeigt werden. Sie müssen die Datei herunterladen, um eine Vorschau des Inhalts anzuzeigen. Dieser Grenzwert gilt nur für EML-Dateien.



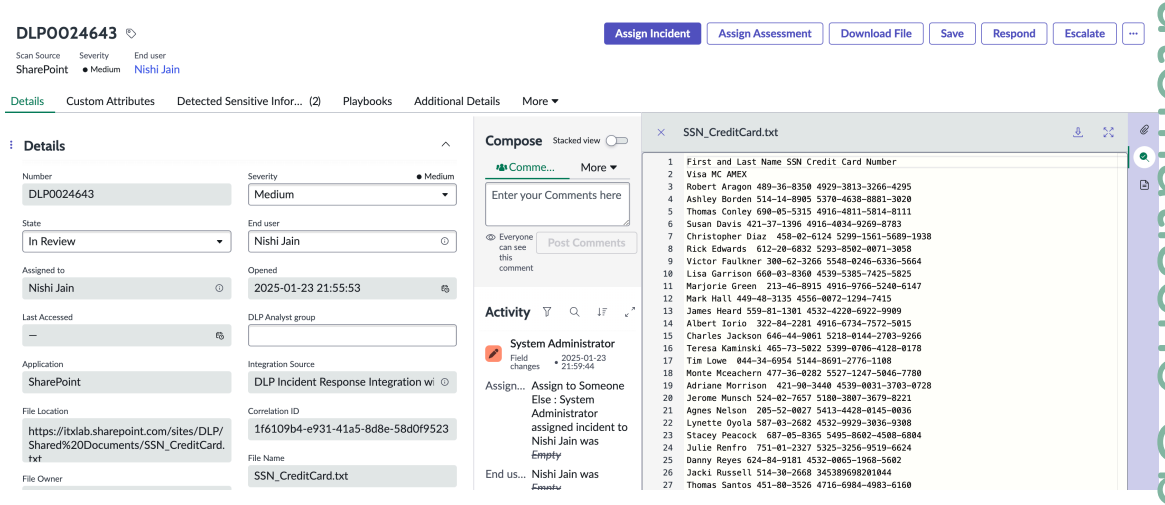
7. Zeigen Sie eine Vorschau der Bilder im DLP-Analystenbereich an.
Bilder nur mit .bmp, .gif, .ico, .JPEG, .jpg, die Erweiterungen .png, .svg und .webp werden unterstützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Zeigen Sie eine Vorschau von Textdateien im Texteditor an, indem Sie auswählen **Erweitern Sie** Symbol oben rechts in der Nachweisdatei.



Hinweis:
Nachweisdateien außer Office-Dokumenten werden EML-Dateien, Text- und Bilderweiterungen für die Vorschau nicht unterstützt. Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion „Vorschaunachweisdatei“ funktioniert auch für archivierte Incidents.

Benachrichtigungen für Anwender im Wiederholungsmechanismus

Netskope Bei der Integration wird die konfigurierte Anzahl wiederholt, wenn API-Fehler während der Erfassung von DLP-Incidents auftreten.

Sobald das maximale Wiederholungslimit überschritten wurde, Netskope Die Integration sendet eine E-Mail-Benachrichtigung an Anwender mit der DLP-Administratorrolle (sn_dlir.admin).

Nachdem Sie das Setup und die Konfiguration der Integration abgeschlossen haben, geben Sie den Anwendern die Rolle „DLP-Administrator“ (sn_dlir.admin) an, die benachrichtigt werden sollen, wenn das maximale Wiederholungslimit überschritten wird.

Sobald das maximale Wiederholungslimit überschritten wurde, überspringt das Profil die Erfassung für eine Dauer von bis zu einer Stunde. Die maximalen Wiederholungen werden mit der Eigenschaft konfiguriert: Maximale Anzahl von Wiederholungen, die für API-Fehler ausgeführt werden sollen . Weitere Informationen finden Sie unter Konfigurieren Netskope DLP-Integrationseinstellungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mail-Benachrichtigungen beim Ablauf der Anmeldeinformationen

Wenn das Token in verwendet wird ServiceNow Instanz läuft ab, Netskope Die Integration sendet eine E-Mail-Benachrichtigung an Anwender mit der DLP-Administratorrolle (sn_dlir.admin).

Nachdem das Setup der Integrationskonfiguration abgeschlossen ist, geben Sie den Anwendern die Rolle „DLP-Administrator“ (sn_dlir.admin) an, die benachrichtigt werden sollen, wenn das Token abgelaufen ist.

Wenn das Token abläuft, wird die Datenerfassung für zugehörige Profile angehalten, bis die Netskope-Integrationskonfiguration mit einem gültigen Token aktualisiert wird.

Sie müssen ein Token erstellen oder das alte auf verlängern Netskope, Und aktualisieren Sie dann das Token auf der ServiceNow Instanz. Wenn Sie das Token verlängern, indem Sie die Ablaufzeit verlängern, dann die Netskope Die Anwendung erkennt die Verlängerung automatisch und setzt die Datensammlung fort. Wenn Sie ein Token erstellen, müssen Sie das Token in der Konfiguration aktualisieren.

Domänentrennung in Netskope DLP-Integration

Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Supportstufe

Support: Standard.

Funktionsweise der Domänentrennung Netskope DLP-Integration

Führen Sie die folgenden Schritte aus, um die Domänentrennung zu erreichen:

- Erstellen Sie einen Anwender mit der erforderlichen Rolle in der jeweiligen Domäne.
- Führen Sie aus Netskope DLP-Integrationsverfahren in der entsprechenden Domäne.

ICAP-Integration (Internet Content Adaption Protocol) für DLP IR

Die DLP-Integration des Internet Content Adaption Protocol (ICAP) unterstützt die Erfassung von Data Loss Prevention Incident Response Warnungen, ermöglicht das Abrufen von Übereinstimmungsinhalten und Nachweisdateien aus Amazon S3, die auf dem unterstützten ICAP erstellt wurden Data Loss Prevention Incident Response Bereitstellung.

Nachdem die Warnungen erfasst wurden, können Sie den DLP-Arbeitsbereich verwenden, um die erforderlichen wichtigen Informationen anzuzeigen, z. B. Übereinstimmungsinhalte, Warnungsschweregrad und verschiedene Incident-Management-Funktionen, um die DLP-Incidents zu beheben.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Übersicht und wichtige Funktionen

Die ICAP-Integration (Internet Content Adaption Protocol) hilft Ihnen, die Nutzung und Bewegung vertraulicher Daten auf verschiedenen Plattformen nachzuverfolgen.

Diese Integration umfasst die folgenden wichtigen Funktionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erfassung von DLP-Warnungen: Anwender können die Erfassung von DLP-Warnungen aus angegebenen Amazon S3-Buckets konfigurieren und planen. Dies umfasst die Möglichkeit, Delta-Importe durchzuführen, um sicherzustellen, dass nur neue Daten erfasst werden.
- Erfasste Warnungen im DLP-Arbeitsbereich anzeigen: Sobald die Warnungen erfasst wurden, sollten sie im DLP-Arbeitsbereich angezeigt werden und wichtige Details zu jeder Warnung enthalten, z. B. Übereinstimmungsinhalt, Warnungsschweregrad und relevante Metadaten.
- Inhalt abgleichen: Datensätze mit vertraulichen Informationen werden während der Erfassung erstellt, Übereinstimmungsinhalte werden abgerufen, wenn der Datensatz geöffnet wird.
- Download der Nachweisdatei: Das System ermöglicht Anwendern das Herunterladen zugehöriger Nachweisdateien direkt aus dem DLP-Arbeitsbereich zur weiteren Untersuchung oder Überprüfung.
- Möglichkeit, die Schweregradzuordnung zwischen ICAP-DLP-Incidents und ServiceNow-Incidents anzupassen und zu definieren.

Erste Schritte mit der ICAP-DLP-Integration für die Vermeidung von Datenverlust

Bevor Sie die Integration verwenden können, müssen Sie sie aus dem herunterladen ServiceNow® Store

Prüfliste

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung der ICAP DLP-Integration Ihres Anbieters zur Vermeidung von Datenverlust beginnen.

Prüfliste

Feld	Beschreibung
Überprüfen Sie, ob Sie die erforderlichen zugewiesen haben ServiceNow AI Platform, Anwendungsrollen zur Vermeidung von Datenverlust.	Die folgenden Rollen werden in der ICAP-DLP-Integration auf verwendet ServiceNow AI Platform: • Der Administrator (Administrator) installiert die -Anwendungen aus dem ServiceNow® Store Und weist den Administrator zur Vermeidung von Datenverlust (sn_dlir.admin) zu. • Der Benutzer mit der Rolle „sn_dlir.admin“ kann die Integration konfigurieren und die Incident-Profile einrichten. • Die Anwender mit der Rolle „sn_dlir.Analyst“ haben Leserollen für alle Integrationskonfigurationen.
Stellen Sie sicher, dass Sie die erforderlichen Amazon S3-Bucket-Richtlinien zugewiesen haben.	Sie können die offizielle AWS-Dokumentation zum Erstellen und Verwalten von IAM-Anwendern, -Richtlinien und -Berechtigungen über die folgenden Links befolgen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Feld	Beschreibung
	• IAM-Anwender wird erstellt • IAM-Richtlinien werden erstellt • Amazon S3-Berechtigungen **Hinweis:** Über die obigen Links erfahren Sie mehr über die detaillierten Anweisungen und weiteren Optionen zum Verwalten von IAM-Anwendern und S3-Berechtigungen in AWS, zum Erstellen eines IAM-Anwenders in Ihrem AWS-Account – AWS-Identitäts- und Zugriffsmanagement – und die grundlegende Übersicht über den Prozess zum Erstellen eines IAM-Anwenders und von Anmeldeinformationen in AWS-Identitäts- und Zugriffsmanagement.
Verifizieren Sie das ServiceNow® Kernanwendungen, die zur Unterstützung der ICAP-DLP-Integration erforderlich sind, werden installiert und aktiviert.	Überprüfen Sie, ob die folgenden allgemeinen DLP-Anwendungen und Sicherheitssupport-Anwendungen im ServiceNow Store installiert und aktiviert sind. Wenn nicht installiert, installieren Sie die Anwendung, und aktivieren Sie sie. • Security Support Common • Allgemeine Sicherheitsfallmanagement-Arbeitsbereichskomponenten. • Reaktion auf Incident zur Vermeidung von Datenverlust

Installieren und konfigurieren Sie die ICAP-DLP-Integration

Installieren und konfigurieren Sie die#ICAP-DLP-Integration des Anbieters aus dem ServiceNow® Store Auf Ihrem ServiceNow AI Platform Instanz. Beginnen Sie mit der Untersuchung von DLP-Incidents mithilfe der#ICAP-DLP-Incident-Daten des Anbieters.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

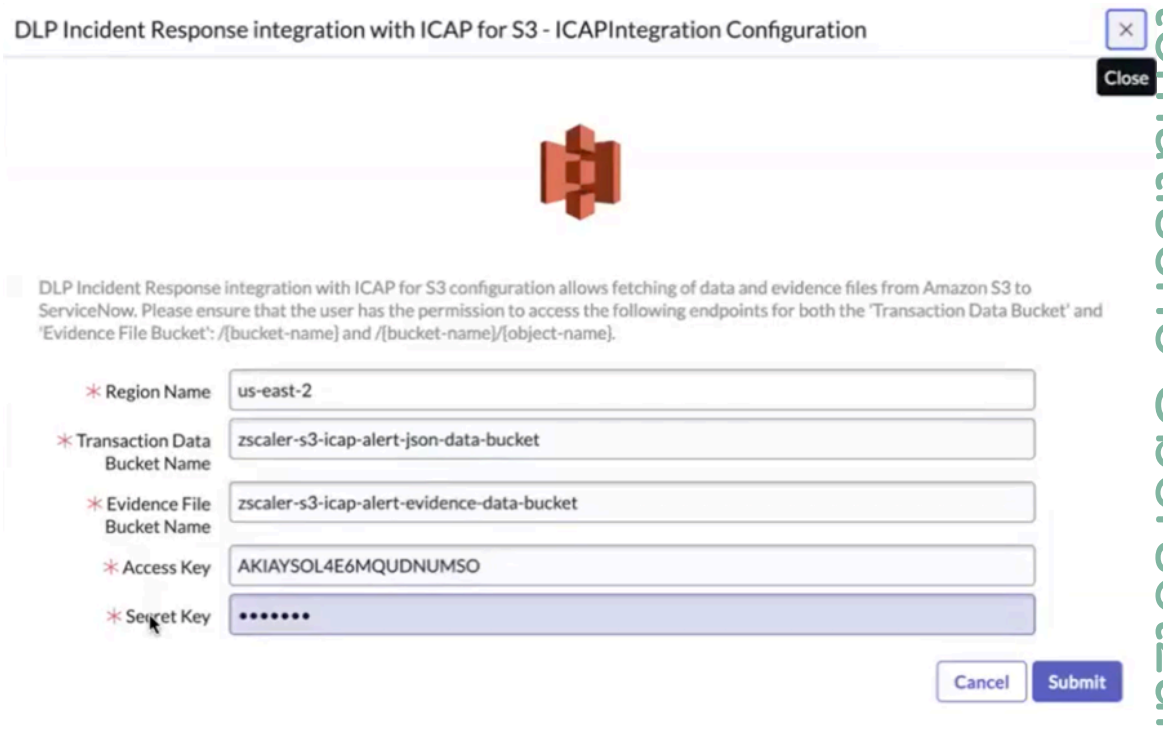
Prozedur

1. Laden Sie die#ICAP-DLP-Integration des Anbieters aus dem herunterServiceNow® Store Und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Suchen Sie nach der#Kachel „Integration von DLP-Incident Response mit ICAP“, und klicken Sie auf **Konfigurieren** .
4. Füllen Sie im Formular die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Konfiguration der ICAP-DLP-Integration“

Feld	Beschreibung
Regionsname	Regionsname des Amazon S3-Bucket-Namens.
Name des Transaktionsdaten-Buckets	Der Name des Transaktionsdaten-Buckets ist der Bucket, in dem eine DLP-Verstoßtransaktion aufgetreten ist.
Name des Nachweisdatei-Buckets	Der Bucket-Name der Nachweisdatei ist der Bucket, in dem Sie die DLP-Datei finden können, die den Verstoß verursacht hat.
Zugriffsschlüssel	AWS IAM-Zugriffsschlüssel für die ICAP-Konfiguration.
Geheimer Schlüssel	Geheimer AWS-IAM-Schlüssel für die ICAP-Konfiguration.



5. Klicken Sie auf **Absenden**.

Ergebnisse

Hinweis:
Verbinden Sie die ICAP-Subprod mit der ServiceNow-Subprod. Halten Sie alle Anwendernamen und Passwörter in allen Instanzen synchron, um zu vermeiden, dass Accounts abgemeldet werden.

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, werden die Konfigurationen der ICAP-DLP-Integration gespeichert.

Erstellen Sie ein Profil für die ICAP-DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrem ServiceNow AI Platform Instanz. Bestimmen Sie die#ICAP-DLP-Warnungen, die für die Erstellung von DLP-Incidents geeignet sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie die NowPlatform, um die DLP-Warnungen aus der Amazon S3-Konfiguration abzurufen. Speichern Sie diese Warnungen in Ihrer ServiceNow-Instanz als DLP-Incidents.

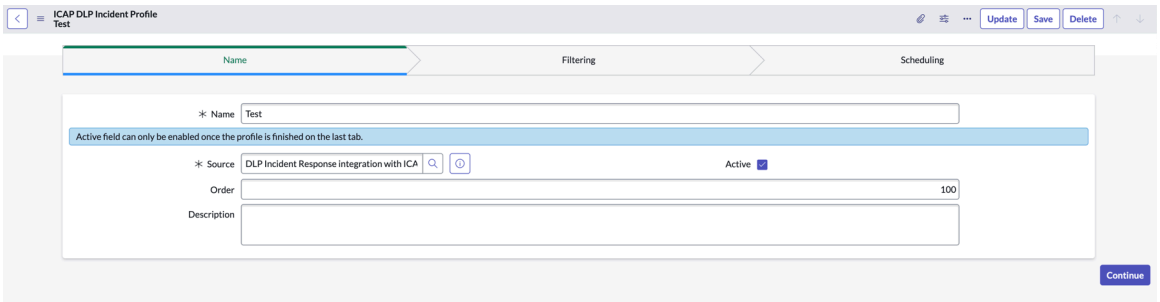
Prozedur
1. Navigieren zu **Alle** > **ICAP-DLP-Integration** > **Incident-Profil**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder im Abschnitt Name aus.

Erstellen Sie ein Profil

Feld	Beschreibung
Name	Name des Profils. Dieses Feld hilft Ihnen, das Profil zu identifizieren. **Hinweis:** De Name muss für jedes Profil eindeutig sein.
Quelle	Amazon S3-Konfiguration, die Sie zum Erfassen von Incidents konfiguriert haben. Wenn Sie mehrere Quellen konfiguriert haben, wählen Sie die entsprechende Quelle für den Incident-Typ aus, den Sie für das Profil erfassen möchten. **Hinweis:** Für das aktive Profil ist nur eine einzelne Quelle zulässig.
Aktiv	Option, um anzugeben, ob das Profil aktiv ist. Dieses Feld kann nur aktiviert werden, nachdem Sie auf geklickt haben **Beenden** Im Abschnitt Zeitplanung. Wenn das Profil aktiv ist, bedeutet dies, dass ServiceNow AI Platform Fragt aktiv ICAP-DLP-Warnungen ab. Die entsprechenden DLP-Warnungen werden in#DLP erstellt#, wenn die Filterbedingungen basierend auf den von Ihnen angegebenen Zeitplanungsparametern erfüllt werden.
Reihenfolge	Reihenfolge der Profilausführung. Das Profil mit der niedrigsten Reihenfolge, das als höchste Priorität betrachtet wird. Standardmäßig ist der Wert 100.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Beschreibung für dieses Profil.



Nächste Maßnahme

Um zum Abschnitt Filterung zu wechseln,#klicken Sie auf **Fahren Sie Fort** .

Definieren Sie Filter, die für die Incident-Erstellung angewendet werden sollen

Definieren und legen Sie Filterbedingungen fest, um die eingehenden#DLP-#Warnungen zu filtern. Bestimmen Sie die Warnungen, die als DLP-Incidents in ServiceNow erstellt werden sollen.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Das Filtern hilft Ihnen, DLP-Warnungen zu isolieren und die Anzahl der von Ihnen erstellten DLP-Warnungen zu begrenzen. Wenn zusätzliche Filterkriterien festgelegt sind, werden nur Warnungen erstellt, die den Bedingungen entsprechen.

Prozedur

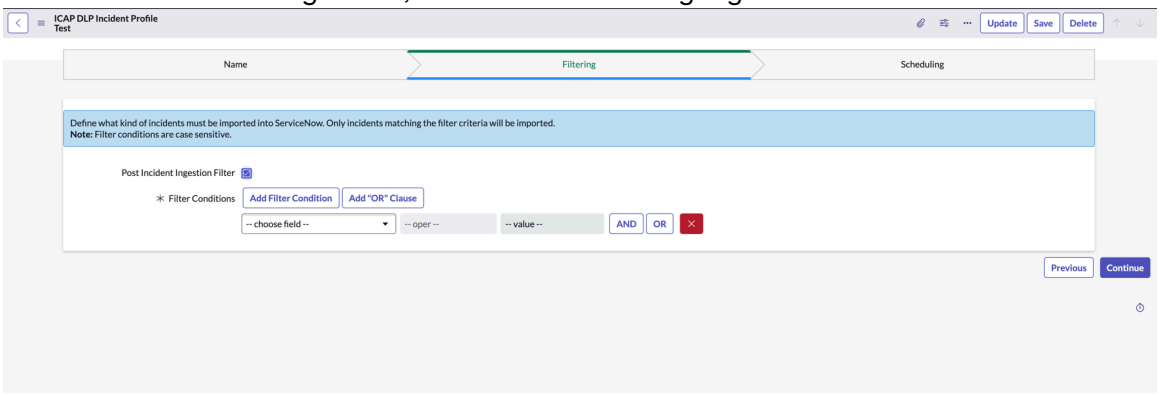
1. Wählen Sie Aus **Filter Für Incident-Erfassung** Kontrollkästchen zum Anwenden der Filter für die Erfassung nach Incidents und zum Abrufen der Incidents, die den Filterkriterien entsprechen.
2. Wählen Sie aus **Filtern Sie basierend auf Bedingungen** Option und definieren Sie die Kriterien, die ein eingehender ICAP-DLP-Incident erfüllen muss, damit ein DLP-Incident erstellt wird.
3. Legen Sie die Filter in fest **Filterbedingungen** Feld.

   Die Optionen in der Dropdown-Liste **Filterbedingungen** Stimmen Sie die Felder ab, die in verfügbar sind **Import von ICAP-DLP-Incidents** Tabelle. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Überprüfen Sie, ob die von Ihnen definierten Kriterien mit den Werten des Incident übereinstimmen.
4. Fügen Sie weitere Bedingungen hinzu, indem Sie auf klicken **UND** #Oder**ODER** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn **UND** #Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
- Wenn **ODER** #Ist ausgewählt, kann eine der Bedingungen erfüllt werden.



Nächste Maßnahme

Klicken Sie auf, um den Zeitplan zu konfigurieren **Fahren Sie Fort** .

Planen Sie den Abruf von ICAP-DLP-Incidents

Legen Sie einen Zeitplan fest, um ICAP-DLP-Warnungen abzurufen, die den Kriterien im Profil entsprechen.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können planen, wie oft Sie Netto-neue ICAP-Incidents abfragen, die der Incident-Profilkonfiguration entsprechen. Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Planung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Das Profil kann so konfiguriert werden, dass ein einmaliger Abruf mit durchgeführt wird **Einmaliger Abruf** Kontrollkästchen.

Prozedur

1. Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Incidents aus ICAP abrufen.
2. Füllen Sie im Formular die Felder aus.

Planen Sie die ICAP-DLP-Incidents

Feld	Beschreibung
Laufende Incident-Erfassung	Laufende Incident-Erfassung, die Ihr ServiceNow AI Platform Instanz ruft aus#ICAP für neue Incidents ab. Wenn ausgelöste Incidents gefunden werden, die den Incident-Filterkriterien entsprechen, werden DLP-Incidents erstellt.
Abfrageschritt (Minuten)	Abfragehäufigkeit, die in Minuten definiert ist. Dieser Standardwert ist auf festgelegt **5** .
Zeitpunkt der ersten Incident-Erfassung festlegen	Option zum Festlegen der ersten Incident-Erfassung basierend auf dem konfigurierten Datum und der konfigurierten Uhrzeit.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie können diese Option verwenden, um ein bestimmtes Datum und eine bestimmte Uhrzeit für die anfängliche Erfassung zu definieren. Nachfolgende Erfassungen basieren auf dem Abfrageintervall-Zeitraum.
Zeitpunkt der ersten Incident-Erfassung eingeben	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben.
Zeitpunkt der ersten Incident-Erfassung	Das erste Mal, wenn Daten erfasst werden. **Hinweis:** Der Wert ist nur sichtbar, wenn **Legen Sie Die Erste Incident-Erfassungszeit Fest** Option ist ausgewählt.
Nächste Incident-Erfassungszeit (geschätzt)	Die nächste geschätzte Incident-Erfassungszeit.
Einmaliger Abruf	Option zum Aktivieren des einmaligen Abrufs von Verlaufsdaten. **Hinweis:** Wenn diese Option ausgewählt ist, werden Verlaufsdaten gemäß dem in hinzugefügten Datum aus ICAP-DLP abgerufen **Seit Datum** .
Ordnername	Name des Ordners, aus dem Sie die Daten abrufen möchten. Alle Ordner, deren Namen lexikografisch größer als der angegebene Ordnername sind, werden beim einmaligen Abruf erfasst.

3. Klicken Sie auf **Fertigstellen**.
4. Speichern Sie im Popup-Fenster die erstellte Profilkonfiguration, indem Sie auf klicken **Beenden** .
5. Aktivieren Sie das Profil.
   a. Öffnen Sie das erstellte Profil.
   b. Festlegen **Aktiv** Bis **Wahr** .
   c. Klicken Sie auf **Aktualisieren**.

Ergebnisse
Nach der erfolgreichen Aktivierung des Profils werden Incidents regelmäßig gemäß der im Profil festgelegten Konfiguration abgerufen. Die Warnungen werden der DLP-Incident-Tabelle hinzugefügt.

Zeigen Sie vertrauliche Informationen für DLP-Warnungen an

Zeigen Sie die erkannten sensiblen Informationen für DLP-Warnungen an.

Vorbereitungen
In der jeweiligen Integration sind bestimmte Regeln und Richtlinien konfiguriert. Wenn Sie jedes Mal gegen die definierten Richtlinien verstoßen, wird ein DLP-Incident erstellt,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

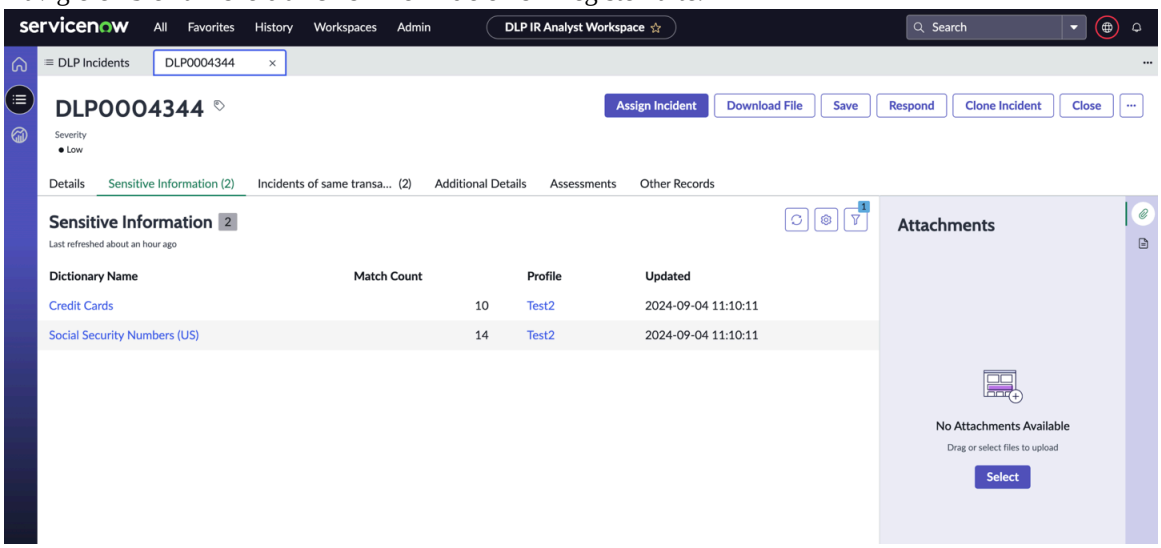
und der Abgleichinhalt zeigt im Abschnitt „sensible Informationen“ dieses DLP-Incident-Datensatzes Informationen an, die verletzt wurden.

Erforderliche Rolle: sn_dlir.Analyst

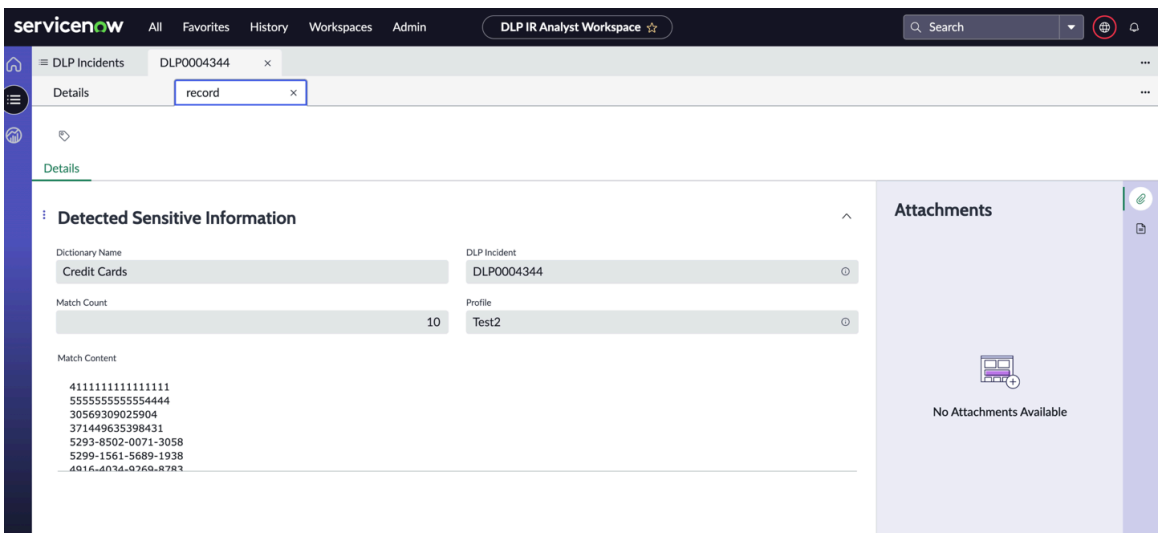
Hinweis:
Endanwender können die vertraulichen Informationen auch anzeigen, indem sie sich beim DLP-Anwenderarbeitsbereich anmelden.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
   Die Seite „DLP-Arbeitsbereich – meine Incidents“ wird im DLP-Arbeitsbereich für Analysten angezeigt.
2. Öffnen Sie einen beliebigen DLP-Incident.
3. Navigieren Sie zu **Vertrauliche Informationen** Registerkarte.



4. Klicken Sie auf den Datensatz mit Verletzungen.
5. Zeigen Sie die Informationen zum Übereinstimmungsinhalt an, und ergreifen Sie die entsprechenden Maßnahmen nach Bedarf.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Laden Sie Nachweisdateien für DLP-Warnungen herunter

Laden Sie Dateien herunter, die gegen die DLP-Richtlinie für Anbieter verstoßen, der ICAP unterstützt. Laden Sie diese Datei aus dem DLP-IR-Analyst-Arbeitsbereich und dem DLP-IR-Endanwender-Arbeitsbereich für Genehmiger auf Ihren lokalen Computer herunter.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.Analyst und Genehmiger können herunterladen

Warum und wann dieser Vorgang ausgeführt wird

Sie müssen den Dateidownload für ICAP aktivieren, bevor Sie fortfahren.

Prozedur

1. Navigieren zu **Alle** > **ICAP-DLP-Integration** > **Einstellungen**an.
2. Aktivieren Sie die Eigenschaft sn_icap_dlp.enable_file_Download **Durch Aktivieren dieser Eigenschaft kann die Nachweisdatei des gemeldeten ICAP-Incidents heruntergeladen werden** .
   Sie können sehen **Datei Herunterladen** Schaltfläche im DLP IR Analyst Workspace und DLP IR-Endanwenderarbeitsbereich.
3. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
4. Öffnen Sie einen DLP-Incident-Datensatz, der aus der ICAP-Anbieterquelle erfasst wird.
5. Klicken Sie Auf **Datei Herunterladen** .

Hinweis:
DLP-Administrator kann den Zugriff von steuern **Datei Herunterladen** Aktion für alle Integrationen durch Deaktivieren von **Sollte das Herunterladen der Datei mit Verstoß des gemeldeten Incidents zulässig sein** Option von **Erweiterte Einstellungen** Seite der DLP-Administration. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Zeigen Sie eine Vorschau der Nachweisdateien für ICAP an

Vorschau der DLP-Incident-Nachweisdateien im DLP IR-Analyst-Arbeitsbereich anzeigen.

Vorbereitungen

- Navigieren zu **Alle** > **DLP-Administration** > **Erweiterte Einstellungen**an.
- Stellen Sie sicher, dass **sn_icap_dlp.enable_evidence_file_preview** Eigenschaft ist bereits aktiviert.

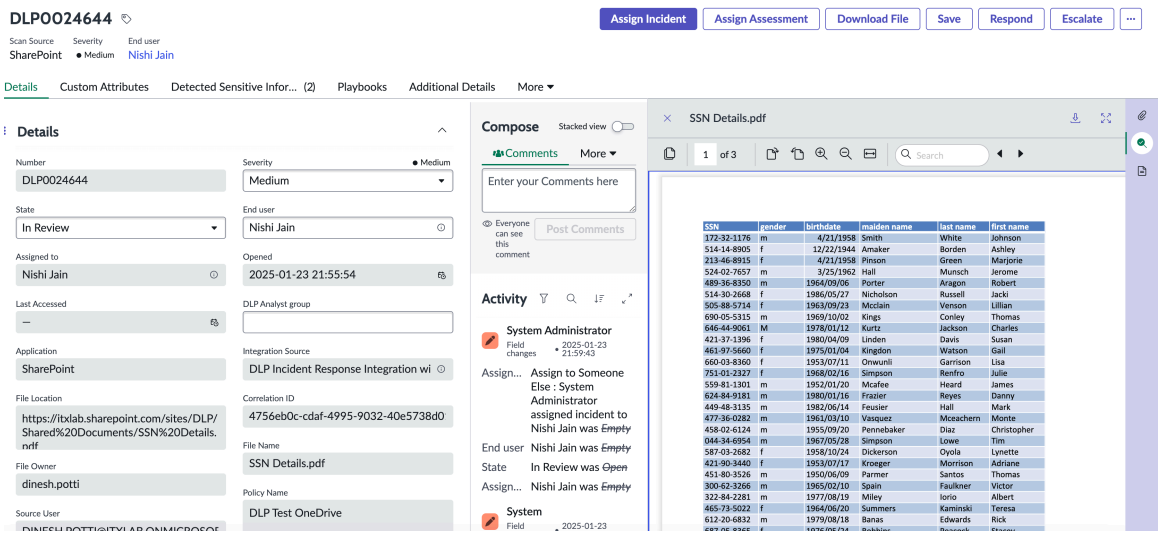
Wichtig:
Bei der Verwendung der Aktion „Nachweisdateien“ im DLP-Analysten-Arbeitsbereich werden die Nachweisdateien vorübergehend in der ServiceNow-Datenbank in einem unverschlüsselten Format für die Dauer gespeichert, die Sie mit ausgewählt haben **sn_dlir.preview_temp_files_cleanup_interval** Eigenschaft von **Erweiterte Einstellungen** Seite. Sie können deaktivieren **Nachweisdateien** Vorschaufunktion, wenn Sie keine Daten in der ServiceNow-Datenbank speichern möchten. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Erforderliche Rolle: sn_dlir.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
2. Öffnen Sie einen DLP-Incident-Datensatz.
3. Wählen Sie aus **Nachweisdateien** Symbol, das im Kontextmenü verfügbar ist.
   Eine Registerkarte wird geöffnet, auf der alle Nachweisdateien abgerufen werden. Sobald der Download abgeschlossen ist, können Sie alle Nachweisdateien in anzeigen **Nachweisdateien** Registerkarte.
4. Wählen Sie aus **Nachweisdatei** Karte, die Sie in der Vorschau anzeigen möchten.
   Die Vorschaufunktion unterscheidet sich für jeden Dateityp.
5. Zeigen Sie eine Vorschau von PDF- und Office-Dokumenten im Dokument-Viewer an, indem Sie auswählen **Erweitern Sie** Symbol oben rechts in der Nachweisdatei, um die PDF-Datei im Vollbildmodus zu öffnen. Office-Erweiterungen, für die der Dokumentbetrachter die Nachweisdateien öffnet: Doc, docx, ppt, pptx, xls, XLSX.
   a. Suchen Sie die Suchleiste, und geben Sie das gesuchte Stichwort ein.
   b. Verwenden Sie die Funktionen zum Vergrößern und Verkleinern, um die Ansicht für eine bessere Lesbarkeit anzupassen.
   c. Drehen Sie die Seite im Uhrzeigersinn oder gegen den Uhrzeigersinn, um den Inhalt klarer anzuzeigen.
   Diese Steuerungsoptionen verbessern Ihre Fähigkeit, die Nachweisdatei umfassend zu verstehen. Nur die PDF-Datei enthält Steuerungsoptionen im Header.



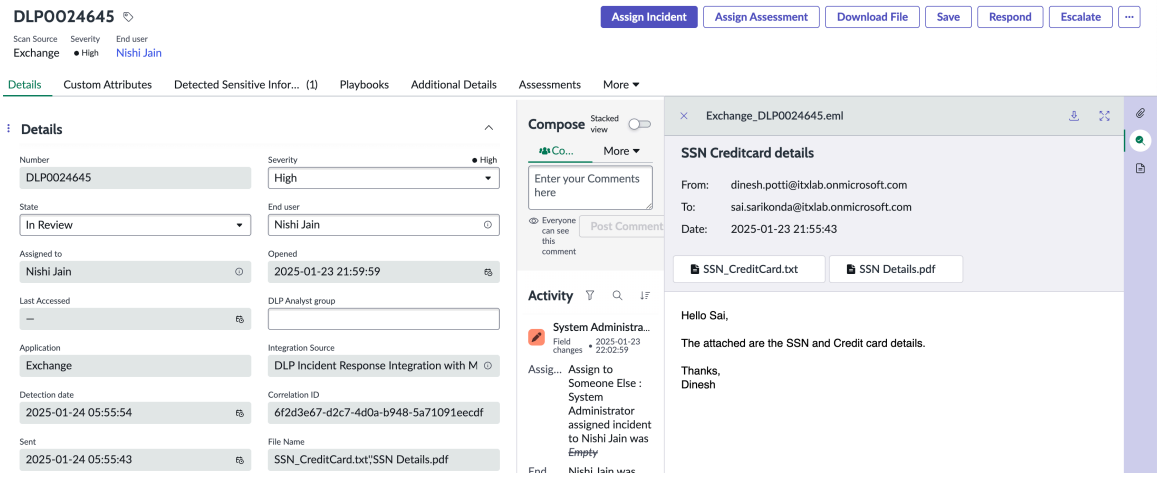
6. Eml-Dateien in der Vorschau anzeigen.
   Wählen Sie die Anhänge in der E-Mail aus, und zeigen Sie eine Vorschau an.

Hinweis:

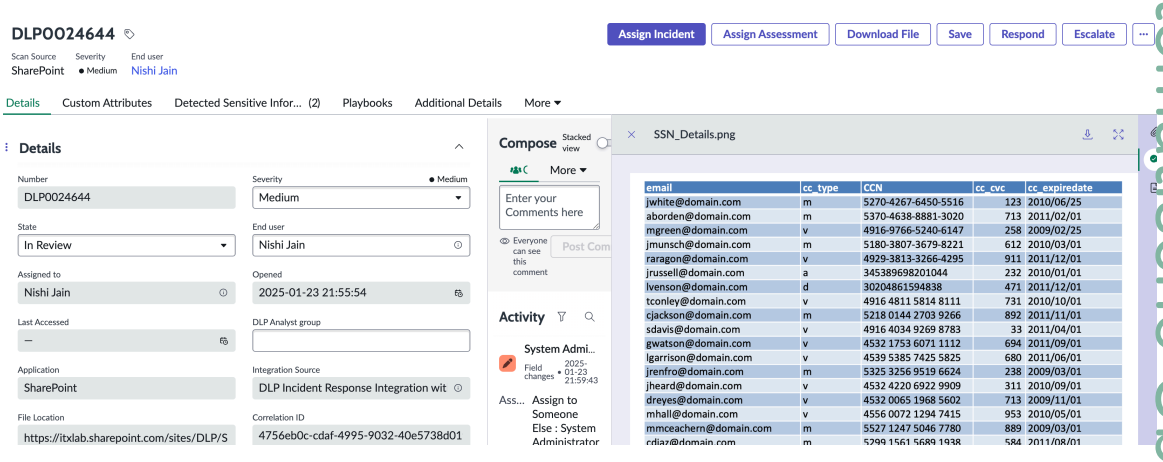
Wenn die ausgewählte Nachweisdatei den Grenzwert von 5 MB überschreitet, kann sie im Arbeitsbereich des Analysten nicht in der Vorschau angezeigt werden. Sie müssen die Datei herunterladen, um eine Vorschau des Inhalts anzuzeigen. Dieser Grenzwert gilt nur für EML-Dateien.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



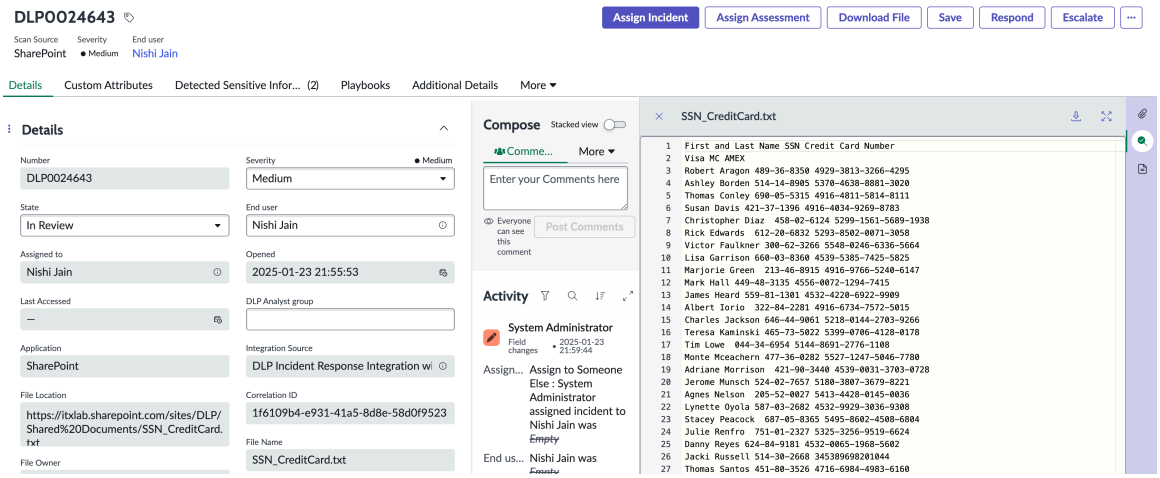
7. Zeigen Sie eine Vorschau der Bilder im DLP-Analystenbereich an.
Bilder nur mit .bmp, .gif, .ico, .JPEG, .jpg, die Erweiterungen .png, .svg und .webp werden unterstützt.



8. Zeigen Sie eine Vorschau von Textdateien im Texteditor an, indem Sie auswählen **Erweitern Sie** Symbol oben rechts in der Nachweisdatei.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Nachweisdateien außer Office-Dokumenten werden EML-Dateien, Text- und Bilderweiterungen für die Vorschau nicht unterstützt. Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion „Vorschaunachweisdatei“ funktioniert auch für archivierte Incidents.

Überprüfen Sie die Einstellungen für die ICAP-DLP-Integration

Überprüfen Sie die Einstellungen der ICAP DLP-Integration des Anbieters, und ändern Sie die Standardsystemeigenschaften entsprechend Ihrer Umgebung.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin

Prozedur

1. Navigieren zu **Alle** > **ICAP-DLP-Integration** > **Einstellungen**an.
2. Überprüfen und ändern Sie die Einstellungen.

Data Loss Prevention Incident Response mit Microsoft

Die Data Loss Prevention Incident Response Mit Microsoft Bietet ein Core-Framework zum Importieren von DLP-Incidents (Data Loss Prevention) aus mehreren Quellen, z. B. Microsoft Vorschau der Apps anzeigen (Microsoft Teams, Exchange Online, SharePoint Online, OneDrive for Business) und andere Ereignistypen. Endpunktgeräte ermöglichen einen Korrektur-Workflow mit Endanwendern, Managern und#DLP-#Betriebsteams mit automatisierter Incident-Zuweisung und -Eskalationen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Schlüsselfunktionen

Verwenden Sie die wichtigsten Funktionen dieser Integration, um die folgenden Aktionen auszuführen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie mehrere Profile für verschiedene Accounts.
- Automatisieren Sie die Erstellung von DLP IR Incidents.
- Ordnen Sie zu Microsoft DLP IR Ereignisfelder bis DLP IR Incident-Felder.
- Filter Microsoft DLP IR Ereignisse.
- Planen Sie die Erfassung von DLP IR Ereignisse, die erstellen DLP IR Incidents regelmäßig.
- Speichern Sie den passenden Inhalt jedes Microsoft DLP-Ereignisses im externen Cloud-Speicher.
- Löschen Sie übereinstimmende Inhalte im externen Cloud-Speicher nach dem Löschen von DLP IR Incident in ServiceNow.
- Dateien für herunterladen DLP IR Incidents vom Typ Exchange, OneDrive und SharePoint.

Weitere Informationen zu dieser Integration

Dokumentbezeichner	Dokumententitel
Microsoft Produktdokumentations-Website	Microsoft-Produktdokumentations-Website
ServiceNow Produktdokumentations-Website	ServiceNow-Produktdokumentationswebsite

Erste Schritte mit Microsoft DLP IR Integration zur Vermeidung von Datenverlust

Überprüfen Sie die folgenden Informationen, bevor Sie mit der Einrichtung Ihres beginnen Microsoft DLP IR Integration zur Vermeidung von Datenverlust.

Prüfliste

Setupaufgabe	Beschreibung
Rufen Sie die Anmeldeinformationen für Microsoft Purview ab, um die Ereignisdaten abzurufen, und AWS/Azure Storage-Account-Anmeldeinformationen, um den Übereinstimmungsinhalt zu speichern Registrieren Sie eine Anwendung bei der Microsoft Identity Platform	Registrieren Sie eine Anwendung auf der Microsoft Azure-Plattform aus Hier Zum Abrufen der Client-ID, des geheimen Clientschlüssels und der Mandanten-ID. Informationen zu den zum Erstellen einer Anwendung erforderlichen Rollen finden Sie unter Voraussetzungen . Informationen zu den API-Berechtigungen/-Rollen, die in einer Microsoft Azure-Anwendung erforderlich sind, um sie für zu konfigurieren ServiceNow Microsoft DLP-Integration finden Sie in der folgenden Tabelle.
Berechtigungen, die für den Azure-Anwender erforderlich sind, um den Zugriff auf Lese-/Schreib-/Löschblob in Azure Storage zu erhalten	Der Azure-Anwender muss über die Rolle verfügen **Speicher-Blob-Datenbeitragender** Zum Lesen, Schreiben und Löschen von Blobs in Azure Storage.
Berechtigungen, die für den AWS-Anwender erforderlich sind, um Zugriff auf Lese-/Schreib-/Löschobjekte in AWS Storage zu erhalten	Es sollte eine Richtlinie erstellt werden, die Listen-, Lese-, Schreib- und Löschzugriff für das Objekt in AWS S3 Storage gewährt.
Weisen Sie die erforderlichen Rollen zu, und überprüfen Sie sie, ob Sie über die erforderlichen Rollen für verfügen ServiceNow AI Platform Und Administrationsrollen für Datenverlust.	Die folgenden Rollen sind für die Konfiguration und Verifizierung der erwarteten Ergebnisse erforderlich:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfliste (Fortsetzung)

Setupaufgabe	Beschreibung

	• Die Administratorrolle installiert die Integration aus dem ServiceNow Store Und weist die Rolle sn_dlir.admin zu.
	• Die Rolle „sn_dlir.admin“ führt die folgenden Aufgaben aus:
	  ○ Konfiguriert die Integration.
	  ○ Richtet die Incident-Profile ein.

Überprüfen Sie, ob ServiceNow Kernanwendungen, die zur Unterstützung von Microsoft erforderlich sind DLP IR Die Integration wird installiert und aktiviert, bevor Sie diese Integration konfigurieren.	Überprüfen Sie Folgendes DLP IR Allgemeine Anwendungen und Sicherheitssupport werden über installiert und aktiviert ServiceNow Speichern. Wenn nicht installiert, installieren Sie die Anwendung, und aktivieren Sie sie. • Security Support Common • Reaktion auf Incident zur Vermeidung von Datenverlust

Erforderliche API-Berechtigungen/-Rollen in einer Microsoft Azure-Anwendung

Sie benötigen die folgenden API-Berechtigungen/-Rollen in einer Microsoft Azure-Anwendung, um sie für zu konfigurieren* ServiceNow *Microsoft DLP-Integration.

API	Berechtigungsnam	Typ	Beschreibun	Erforderlich für welche ServiceNow-Funktionalität?	Ist Administrator erforderlich?
Office 365-Management-API	AktivitätenFeed.Read	Anwendung	Lesen Sie DLP-Richtlinienereignisse, einschließlich erkannter sensibler Daten.	Dient zum Erfassen der DLP-Ereignisse aus dem MSFT-Bereich in ServiceNow. **Hinweis:** Diese Berechtigung ist ein muss, um die MSFT-Daten in abzurufen ServiceNow.	Ja
Microsoft Graph-API	Dateien.Lesen.Alle	Anwendung	Lesen Sie Dateien in allen Websitesammlungen, auf die Sie zugreifen können.	Datei herunterladen: Zum Herunterladen des Anhangs auf die ServiceNow-Instanz, der das DLP-Ereignis von OneDrive oder SharePoint verursacht hat	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche API-Berechtigungen/-Rollen in einer Microsoft Azure-Anwendung
Sie benötigen die folgenden API-Berechtigungen/-Rollen in einer Microsoft Azure-Anwendung, um sie für zu konfigurieren **ServiceNow** *Microsoft DLP-Integration.*

(Fortsetzung)

API	Berechtigungsnam	Typ	Beschreibun	Erforderlich für welche ServiceNow-Funktionalität?	Ist Administrator erforderlich?
				Hinweis: Dies ist optional. Sie können diese API-Berechtigung überspringen, wenn Sie den Analysten nicht erlauben möchten, den Anhang herunterzuladen, der das DLP-Ereignis verursacht hat.	
	E-Mail.Lesen	Anwendung	E-Mails in allen Postfächern lesen.	Datei herunterladen: Zum Herunterladen des E-Mail-Inhalts (Text und Anhang) auf die ServiceNow-Instanz, die das DLP-Ereignis von Exchange verursacht hat. **Hinweis:** Dies ist optional. Sie können diese API-Berechtigung überspringen, wenn Sie den Analysten nicht erlauben möchten, den E-Mail-Inhalt (Text, Anhang) herunterzuladen, der das DLP-Ereignis verursacht hat.	Ja
	Anwender.Lesen	Delegiert	Melden Sie sich an, und lesen Sie das Anwenderprofil.	Dies ist die Standardberechtigung, die für alle neuen Anwendungen verfügbar ist.	Nein

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkannte Vertrauliche Informationen (Optional)

Der Übereinstimmungsinhalt wird extern in Azure Blob Storage oder Amazon S3-Bucket gespeichert und aus dem externen Speicher abgerufen, wenn der Anwender einen Incident anzeigt.

Eine der folgenden Berechtigungen ist erforderlich, wenn die Anwender übereinstimmende Inhalte/erkannte vertrauliche Informationen in der DLP Core-Anwendung anzeigen möchten:

1. Wenn Sie ein sind Microsoft Azure Anwender, benötigen Sie die Rolle Storage Blob Data Contributor, um Blobs in Azure Storage zu lesen, zu schreiben und zu löschen.
2. Wenn Sie ein Amazon S3-Anwender sind, müssen Sie eine Richtlinie erstellen, die Listen-, Lese-, Schreib- und Löschzugriff für das Objekt in Amazon S3 Storage gewährt.

Installieren und konfigurieren Sie die Microsoft DLP-Integration

Installieren und konfigurieren Sie die#Integration von DLP Incident Response mit Microsoft DLP aus dem ServiceNow® Store Auf Ihrem ServiceNow AI Platform Instanz. Beginnen Sie mit der Untersuchung von DLP-Incidents mit Microsoft DLP-Ereignisdaten.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Prozedur

1. Laden Sie herunter Microsoft DLP-Integration aus dem ServiceNow® Store Und installieren Sie es.
2. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen**an.
3. Konfigurieren Sie Microsoft DLP-Integration.

   a. Suchen Sie nach **Integration von DLP Incident Response mit Microsoft** Kachel und klicken Sie auf **Konfigurieren** .

   b. Füllen Sie im Formular die Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Microsoft DLP-Integrationskonfiguration“

Feld	Beschreibung
Name	Name des Microsoft DLP-Integrationskonfiguration.
Client-ID	Client-ID der im Microsoft Azure-Portal erstellten App.
Geheimer Clientschlüssel	Client-Geheimnis der App, die im Microsoft Azure-Portal erstellt wurde.
Mandanten-ID	Mandanten-ID des Anwenders.

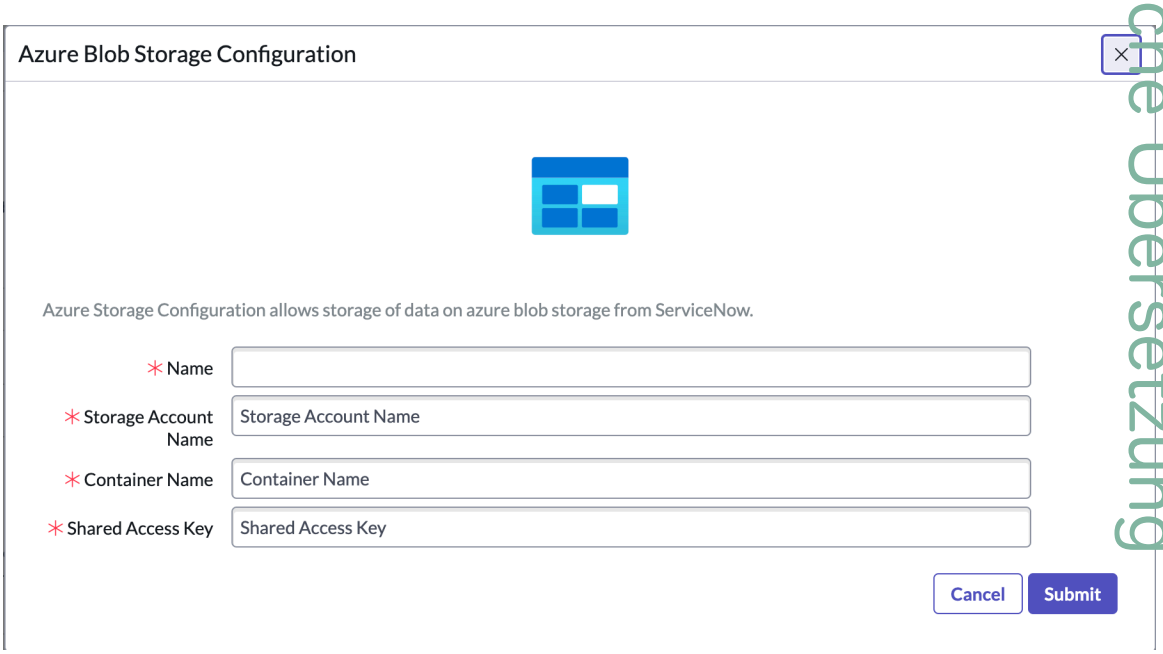
c. Klicken Sie auf **Absenden**.

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird Microsoft DLP-Integration wird auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

4. Aktualisieren Sie die Azure-Speicherkonfiguration.

a. Suchen Sie auf der Seite „Sicherheitsintegrationen“ nach **Azure-Speicherkonfiguration** Kachel.

b. Klicken Sie in der Kachel Azure Storage Configuration (Azure-Speicherkonfiguration) auf **Aktualisieren**.



c. Füllen Sie im Formular die Felder aus.

Formular „Azure-Speicherkonfiguration“

Feld	Beschreibung
Name	Name der Azure Storage-Konfiguration.
Name des Speicher-Accounts	Speicher-Account-Name, der im Azure-Portal erstellt wurde

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Containername	Containername, der im Speicher-Account im Azure-Portal erstellt wurde.
Freigegebener Zugriffsschlüssel	Freigegebener Zugriffsschlüssel für den Speicher-Account.

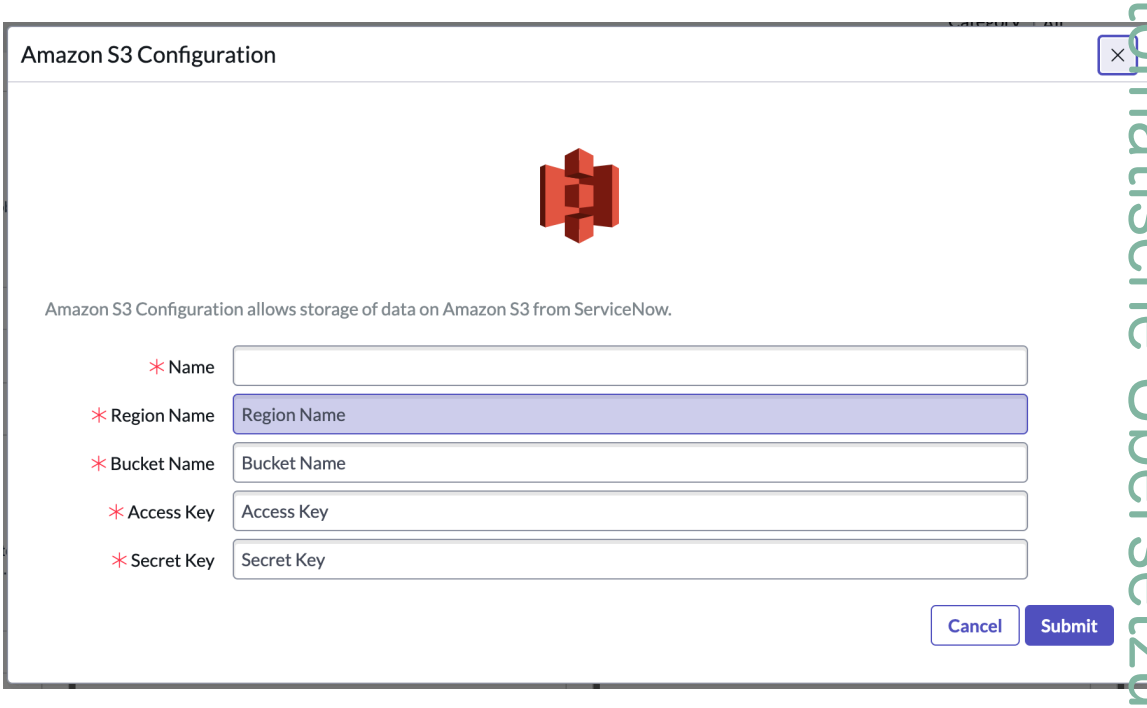
d. Klicken Sie auf **Absenden**.

Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die Azure-Speicherkonfiguration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

5. Aktualisieren Sie die AWS-Speicherkonfiguration.

a. Suchen Sie auf der Seite „Sicherheitsintegrationen“ nach **AWS-Speicherkonfiguration** Kachel.

b. Klicken Sie in der Kachel „AWS-Speicherkonfiguration“ auf **Aktualisieren** .



c. Füllen Sie im Formular die Felder aus.

Formular „AWS-Speicherkonfiguration“

Feld	Beschreibung
Name	Name der AWS-Speicherkonfiguration.
Regionsname	Regionsname des AWS Storage-Accounts.
Bucket-Name	Bucket-Name, der im AWS-Portal erstellt wurde.
Zugriffsschlüssel	Zugriffsschlüssel mit Lese-, Schreib- und Löschzugriff.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Geheimer Schlüssel	Freigegebener Schlüssel mit Lese-, Schreib- und Löschzugriff

d. Klicken Sie auf **Absenden**.

Ergebnisse
Nachdem Sie die Konfiguration erfolgreich validiert und übermittelt haben, wird die AWS S3-Konfiguration auf der Seite „Sicherheitsintegrationen“ als Kachel gespeichert.

Erstellen Sie ein neues Incident-Profil für Microsoft DLP-Integration

Erstellen Sie ein Incident-Profil in Ihrem ServiceNow AI Platform Instanz zum Abrufen der Daten aus dem Microsoft-Bereich und Hinzufügen der Daten zu ServiceNow DLP IR Incident-Tabelle.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin(Erstellen, bearbeiten und löschen)

sn_dlir.Analyst – Ansicht (schreibgeschützt)

Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie ServiceNow AI Platform®Zum Abrufen der Ereignisse aus dem Microsoft Geltungsbereich. Speichern Sie diese Ereignisse im DLP IR Incident-Tabelle in Ihrem ServiceNow® Instanz.

Prozedur
1. Navigieren zu **Microsoft DLP-Integration** > **Incident-Profil**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie im Formular die Felder im Abschnitt Name aus.

Erstellen Sie ein Profilformular

Feld	Beschreibung
Name	Name des Profils. Dieses Feld hilft Ihnen, das Profil zu identifizieren. **Hinweis:** De Name muss für jedes Profil eindeutig sein.
Quelle	Die Microsoft DLP IR Instanz, die Sie zum Erfassen von Incidents konfiguriert haben. Wenn Sie mehrere Integrationskonfigurationen haben, wählen Sie den entsprechenden Integrationskonfigurationsdatensatz für die Incident-Typen aus, die Sie für das Profil erfassen möchten.
Aktiv	Option, um anzugeben, ob das Profil aktiv ist. Dieses Feld kann nur aktiviert werden, nachdem Sie auf geklickt haben **Beenden** Feld im Abschnitt „Zeitplanung“. Wenn das Profil aktiv ist, bedeutet dies, dass ServiceNow AI Platform Fragt aktiv ab

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Microsoft DLP IR Ereignisse basierend auf der im Profil definierten Konfiguration.
Reihenfolge	Reihenfolge der Profilausführung. Das Profil mit der niedrigsten Reihenfolge, das als höchste Priorität betrachtet wird. Standardmäßig ist der Wert 100.
Beschreibung	Eindeutige Beschreibung für das Profil.

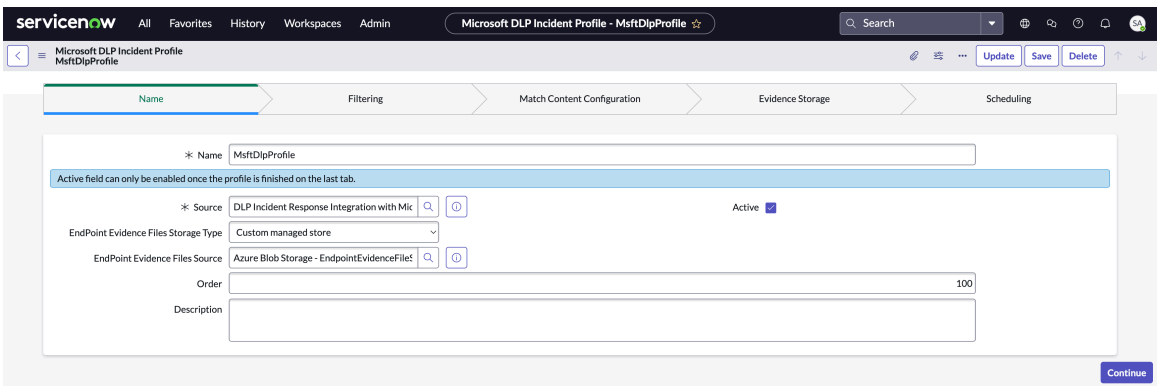
Nächste Maßnahme
Um zum Abschnitt Filterung zu wechseln,#klicken Sie auf **Fahren Sie Fort** .

Microsoft Purview-Endpunktspeicherkonfiguration

Die Speicherkonfiguration für Microsoft Purview-Endpunktnachweisdateien gibt Ihnen an, wo die Endpunktnachweisdateien von der Purview gespeichert werden – anwenderdefinierter verwalteter Speicher oder von Microsoft verwaltete Speicherumgebungen.

Im Fall eines von Microsoft verwalteten Stores speichert Microsoft die Nachweisdateien selbst an einem bestimmten Ort, und für den anwenderdefinierten verwalteten Store müssen Sie den Container angeben, in dem die Nachweisdateien von der Purview gespeichert werden, wenn eine Warnung generiert wird.

Wählen Sie einen der beiden Speichertypen basierend auf dem aus, was am Bereichsende für das System konfiguriert wird, um die Nachweisdateien der entsprechenden Endpunkt-DLP-Incidents abzurufen.



Hinweis:
Wir empfehlen die Verwendung von **Anwenderdefinierter Verwalteter Store** Da Microsoft derzeit keine APIs zum Abrufen von Nachweisdateien aus bereitstellt **Microsoft Managed Store** . Daher wird die Vorschau- und Download-Funktionalität für Nachweise, die im Microsoft Managed Store gespeichert sind, nicht unterstützt. Wir haben einen Fall bezüglich dieser Einschränkung bei Microsoft gemeldet.

Definieren Sie Filter, die für die Incident-Erstellung angewendet werden sollen

Definieren und legen Sie Filterbedingungen fest, um die eingehenden#Microsoft DLP-#Ereignisse zu filtern. Steuern Sie, als welche dieser Ereignisse erstellt werden sollen DLP IR Incidents auf Ihrem ServiceNow Instanz.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin(Erstellen, bearbeiten und löschen)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sn_dlir.Analyst – Ansicht (schreibgeschützt)

Warum und wann dieser Vorgang ausgeführt wird

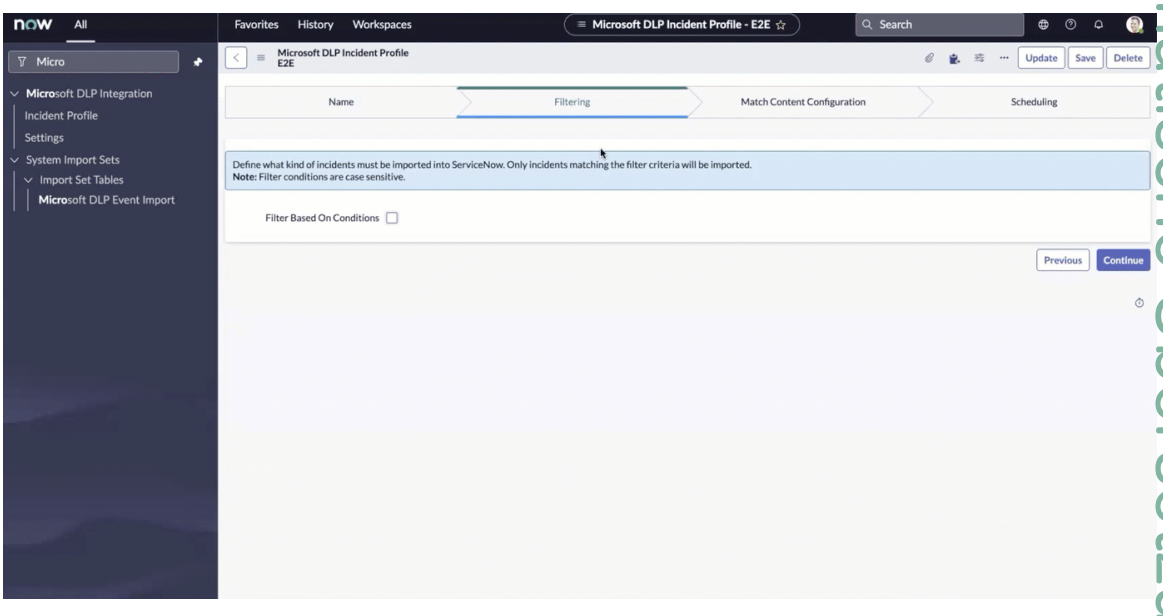
Diese Art der Filterung hilft Ihnen, Microsoft DLP-#Ereignisse zu isolieren, um die Anzahl von zu beschränken DLP IR Incidents, die Sie erstellen. Wenn die Filterkriterien festgelegt sind, werden nur Ereignisse, die den Bedingungen entsprechen, als DLP-Incidents erstellt.

Prozedur

1. Wählen Sie aus **Filtern Sie basierend auf Bedingungen** Option.
2. Legen Sie mithilfe der Listen und Felder des Bedingungsgenerators die Filter in fest **Filterbedingungen** Feld.

   Definieren Sie die Kriterien, die eingehend sind Microsoft DLP-Ereignis muss erfüllen, damit ein DLP-Incident erstellt wird.

   Die Optionen im ersten Feld in **Filterbedingungen** Stimmen Sie die Felder ab, die im Microsoft DLP-Ereignis verfügbar sind. Bei den von Ihnen eingegebenen Kriterien wird zwischen Groß- und Kleinschreibung unterschieden. Überprüfen Sie, ob die von Ihnen definierten Kriterien mit den Werten des Ereignisses übereinstimmen.



3. Fügen Sie weitere Bedingungen hinzu, indem Sie auf klicken **UND** #Oder**ODER** .
   - Wenn **UND** #Ist ausgewählt, müssen alle Bedingungen erfüllt sein.
   - Wenn **ODER** #Ist ausgewählt, kann eine der Bedingungen erfüllt werden.
4. Klicken Sie Auf **Fahren Sie Fort** Und wechseln Sie zum Abschnitt „Inhaltskonfiguration abgleichen“. Zuvor wurde „UserID“ nur dem Feld „Quellanwender“ zugeordnet, das Feld „UserID“ ist jedoch derzeit als Suchattribut für alle Purview-Ereignisse verfügbar, einschließlich Endpunktereignisse.

Konfigurieren Sie den Übereinstimmungsinhalt für den Incident

Geben Sie die Konfiguration an, um vertrauliche Informationen im externen Cloud-Speicher zu speichern, z. B. Azure Storage oder AWS S3-Bucket, um diesen Inhalt während des Zugriffs auf den DLP-IR-Incident abzurufen.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin(Erstellen, bearbeiten und löschen)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sn_dlir.Analyst – Ansicht (schreibgeschützt)

Prozedur

1. Klicken Sie in der Fortschrittsleiste auf **Passen Sie Die Inhaltskonfiguration Ab** Schritt.
2. Füllen Sie im Formular die Felder aus.

Inhaltskonfiguration abgleichen

Feld	Beschreibung
Abgleichsinhalt speichern	Option zum Speichern des übereinstimmenden Inhalts im Cloud-Speicher. **Wichtig:** Wenn diese Option nicht ausgewählt ist, kann der Inhalt der Richtlinienübereinstimmung für DLP-Incidents im DLP-Arbeitsbereich nicht angezeigt werden. Durch Aktivieren dieser Option wird sichergestellt, dass in den DLP-Incidents zurückgegebene Übereinstimmungsinhalte im externen Cloud-Speicher gespeichert werden (z. B. Azure, AWS). Sie können den Übereinstimmungsinhalt auch abrufen und anzeigen, wenn ein DLP-Incident im Arbeitsbereich geöffnet wird. Informationen zur Konfiguration des externen Cloud-Speichers finden Sie unter Installieren und konfigurieren Sie die Microsoft DLP-Integration.
Übereinstimmungsinhalt bei Incident-Löschung löschen	Option zum Löschen des Inhalts von Incident-Übereinstimmungen aus dem externen Cloud-Speicher. Diese Option ist nur sichtbar, wenn **Abgleichsinhalt Speichern** Feld ist ausgewählt.
Externe Cloud-Anmeldeinformationen	Der externe Cloud-Speicher, in dem der Übereinstimmungsinhalt gespeichert wird. Sie können die für die Speicherkonfiguration hinzugefügten externen Cloud-Anmeldeinformationen lesen. Diese Option ist nur sichtbar, wenn **Abgleichsinhalt Speichern** Feld ist ausgewählt.

3. Klicken Sie Auf **Fahren Sie Fort** Und wechseln Sie zum Abschnitt Zeitplanung.

Planen Sie DLP IR Microsoft-Incident-Abruf

Legen Sie einen Zeitplan fest, um die Incident-Daten abzurufen und zu erfassen Microsoft DLP IR Incidents, die den Kriterien im Profil entsprechen. Konfigurieren Sie den Zeitplan, um zu definieren, wie und wann Sie Incidents aus abrufen Microsoft.

Vorbereitungen

Erforderliche Rolle: sn_dlir.admin(Erstellen, bearbeiten und löschen)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sn_dlir.Analyst – Ansicht (schreibgeschützt)

Warum und wann dieser Vorgang ausgeführt wird

Sie können planen, wie oft Sie zukünftige Incidents abfragen, die der Incident-Profilkonfiguration entsprechen. Um die automatisierte Incident-Erfassung zu aktivieren, müssen Sie die Planung und den Incident-Abruf konfigurieren, bevor Sie das Profil aktivieren. Das Profil kann so konfiguriert werden, dass ein einmaliger Abruf mit durchgeführt wird **Einmaliger Abruf** Kontrollkästchen. Das historische Datum kann bis zu den letzten drei Monaten ab dem aktuellen Datum liegen.

Das Abfrageintervall wird für jedes Profil einzeln konfiguriert. Die verschiedenen Abfrageintervalle können sich auf die Leistung von auswirken Microsoft DLP IR Incident-Integration. Planen Sie bei der Planung, dass die Systemlast gegen die Dringlichkeit eines Incident ausgeglichen wird.

Prozedur

1. Legen Sie einen Zeitplan fest, um Daten abzurufen und Incidents zu erfassen, die den Kriterien im Profil entsprechen.
2. Füllen Sie im Formular die Felder aus.

Zeitplan für das DLP-Incident-Formular

Feld	Beschreibung
Laufende Incident-Erfassung	Die laufende Incident-Erfassung, die von ServiceNow AI Platform Instanz ruft aus Microsoft für neue Incidents ab. DLP IR Incidents werden erstellt, wenn ausgelöste Incidents gefunden werden und die Filterkriterien für die Incident-Generierung erfüllt sind.
Abfrageschritt (Minuten)	Die Abfragehäufigkeit von Microsoft. Dieses Feld wird automatisch auf 300 Minuten festgelegt.
Zeitpunkt der ersten Incident-Erfassung festlegen	Option zum Definieren eines Datums und einer Uhrzeit für die anfängliche Erfassung. Nachfolgende Erfassungen basieren auf dem Abfrageintervall-Zeitraum. Diese Option ist nur sichtbar, wenn **Laufende Incident-Erfassung** Feld ist ausgewählt.
Zeitpunkt der ersten Incident-Erfassung eingeben	Datum und Uhrzeit, die Sie für die Incident-Erfassung angeben. ○ Wenn der Wert festgelegt ist, beginnt der Datenabruf von Microsoft ab dem hinzugefügten zukünftigen Datum. ○ Dieses Feld ist nur sichtbar, wenn **Legen Sie die Zeit der ersten Erfassung fest** Ist ausgewählt.
Zeitpunkt der ersten Incident-Erfassung	Erstes Mal, wenn die Daten erfasst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie können sehen, dass Werte angezeigt werden, wenn die erste Incident-Erfassungszeit festgelegt ist.
Nächste Incident-Erfassungszeit (geschätzt)	Der nächste Zeitraum für eine geschätzte Incident-Erfassung.
Einmaliger Abruf	Option zum Aktivieren einmaliger Abrufe von Verlaufsdaten. Wenn dieses Feld ausgewählt ist, werden Verlaufsdaten aus Microsoft abgerufen DLP IR Entsprechend dem Datum, das in hinzugefügt wurde **Seit Datum** Feld.
Seit Datum	Datum, ab dem Daten von Microsoft abgerufen werden sollen. Dieses Feld kann auf maximal 7 Tage festgelegt werden.

3. Speichern Sie die erstellte Profilkonfiguration, indem Sie auf klicken **Beenden** Im Popup-Fenster.
4. Aktivieren Sie das Profil.
   a. Öffnen Sie das erstellte Profil.
   b. Aktivieren Sie **Aktiv** Option.
   c. Klicken Sie auf **Aktualisieren**.

Ergebnisse
Nach der erfolgreichen Erstellung und Aktivierung des Profils werden die Incidents regelmäßig gemäß der im Profil festgelegten Konfiguration abgerufen und der Tabelle „DLP-Incidents“ hinzugefügt.

Konfigurieren Sie Microsoft DLP IR Integrationseinstellungen

Ändern Sie Microsoft DLP IR#Standardsystemeigenschaften der Integration.

Vorbereitungen
Erforderliche Rolle: sn_dlir.admin

Prozedur
1. Navigieren zu **Microsoft-DLP-Integration** > **Einstellungen**an.
2. Ändern Sie die folgenden Eigenschaften nach Bedarf.

Microsoft DLP-Integrationseinstellungen

Feld	Beschreibung
Maximale Zeitüberschreitung für HTTP-Aufrufe (sn_PP_dlp.Maximum_http_time_out)	Maximale Zeitüberschreitung für HTTP-Aufrufe (in Sekunden). ○ Typ: Ganzzahl ○ Standardwert: 30

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ebene der Berichterstellung der von der Integration generierten Protokolle (sn_PP_dlp.Logging.verbosity)	Die Ebene der durch die Integration generierten Berichterstellungsprotokolle, d. h. der Name des Informationstyps. Sie können den Wert auch auf die folgenden Optionen aktualisieren: ○ **Fehler** ○ **warnen** ○ **Info** ○ **debuggen** ○ **Aus** Standardmäßig ist der Wert **Info** .
Ziel der Berichterstellung der von der Integration generierten Protokolle (sn_pp_dlp.logging.destination)	Das Ziel für die Protokolle, die von der Integration generiert werden. Sie können den Wert auch auf die folgenden Optionen aktualisieren: ○ **DB** ○ **Datei** ○ **Keine** Standardmäßig ist der Wert **DB** .

3. Klicken Sie auf **Speichern**.

Ergebnisse

Ihre geänderten Integrationseinstellungen werden im nächsten Abfrageintervall angewendet, wie im Profil definiert.

Release-E-Mail aus Quarantäne anfordern

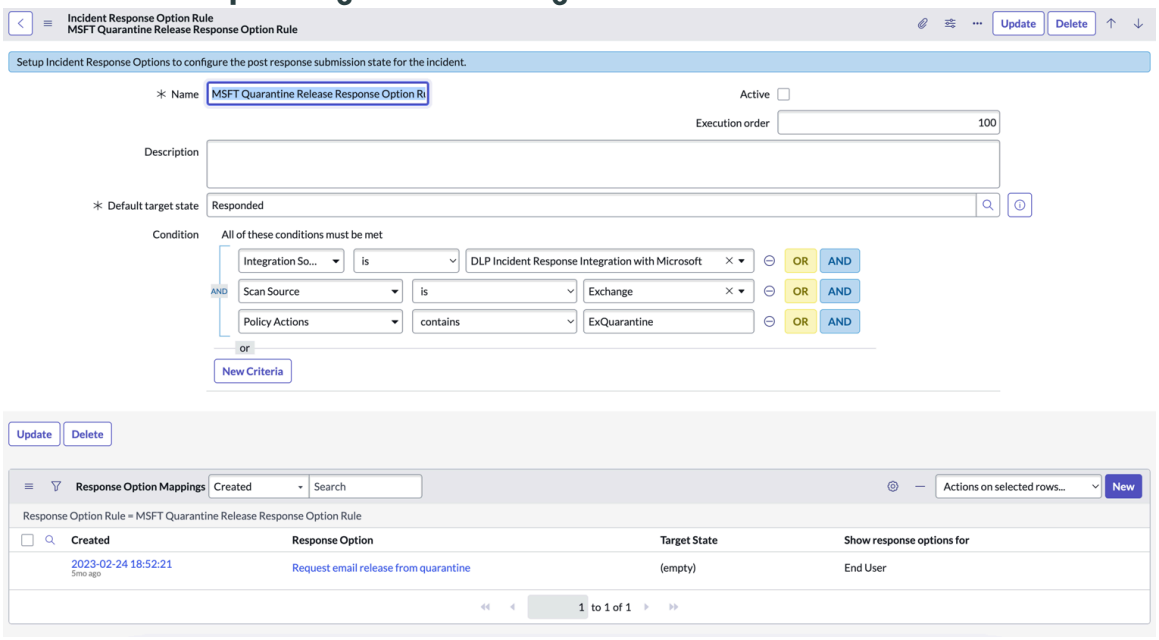
Verwenden Sie diese Funktion, um die E-Mail freizugeben, die im Microsoft Purview Compliance-Portal unter Quarantäne gestellt wird.

Vorbereitungen

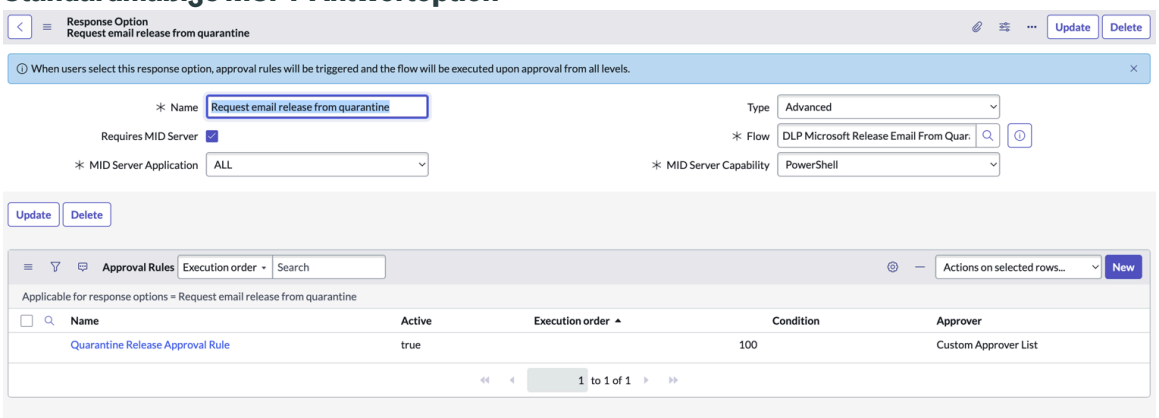
Standardmäßig stellt das -Basissystem bereit **E-Mail-Freigabe aus Quarantäne anfordern** Antwortoption und **Optionsregel für MSFT-Quarantänefreigabe** Um die E-Mail aus der Quarantäne freizugeben. Dieser Standarddatensatz hat auch **Genehmigungsregel Für Quarantänefreigabe** Mit konfiguriert, um die Genehmigungsfunktion für diese Aktion zu nutzen. Weitere Informationen finden Sie unter Erstellen Sie Optionsregeln für die Reaktion auf Incidents, Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents und Erstellen Sie Genehmigungsregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MSFT – Antwortoptionsregel für Entlassung aus Quarantäne



Standardmäßige MSFT-Antwortoption



Voraussetzungen :

1. Das Exchange Online PowerShell-Modul muss auf dem MID-Server installiert sein. Weitere Informationen finden Sie unter Installieren und verwalten Sie Exchange Online PowerShell .
2. Der MID-Server muss mit dem Exchange-Server kommunizieren, der auch ein Cloud-Service ist. Daher erfordert der MID-Server kontinuierlichen Internetzugang.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie diese Antwortoption verwenden, stellen Sie sicher, dass der MID-Server mit PowerShell-Fähigkeit ausgeführt wird. Wenn ein MID-Server nicht ausgeführt wird und nicht über PowerShell-Fähigkeit verfügt, kann der Endanwender nicht auswählen **E-Mail-Freigabe aus Quarantäne anfordern** Aktion aus dem DLP-Anwenderarbeitsbereich. Weitere Informationen finden Sie unter Erstellen Sie Optionsregeln für die Reaktion auf Incidents und Konfigurieren Sie die Antwortoption für Ihre DLP-Incidents.

- Wenn Sie einen bestimmten MID-Server aus der Liste haben möchten, müssen Sie die MID-App konfigurieren und in der Liste sichtbar machen. Dann sollte mindestens ein konfigurierter MID-Server aus den ausgewählten MID-Anwendungen ausgeführt werden und über die Power Shell-Fähigkeit verfügen.
- Damit Sie die Option aus Quarantäne freigeben verwenden können, benötigen Sie API-Berechtigungen. Überprüfen Sie auf der Seite mit Microsoft API-Berechtigungen **Office 365 Exchange Online** > **Exchange.ManageAsApp** Ist aufgeführt und enthält die folgenden Werte:
  - **Typ** : **Anwendung** .
  - **Administratoreinwilligung erforderlich** : **Ja** .
  - **Status** : Der aktuelle falsche Wert ist **Nicht gewährt für <Organization>** Für **Office 365 Exchange Online** > **Exchange.ManageAsApp** Geben Sie den Statuswert ein, und ändern Sie ihn. Weitere Schritte zu den API-Berechtigungen finden Sie unter Weisen Sie der Anwendung API-Berechtigungen zu Auf der Microsoft-Dokumentationswebsite.

    Hinweis:
    Dieser Schritt ist erforderlich, um eine Online-Verbindung mit Exchange über das Serviceprinzip herzustellen.

- Sie sollten auch benötigen **Sicherheitsadministrator** Rolle im Serviceprinzip,
  - Suchen Sie nach **Microsoft Entra ID-Rollen und -Administratoren** Fügen Sie im Microsoft Azure-Portal der registrierten App eine Zuweisung hinzu (Serviceprinzip), und befolgen Sie dann das in der Microsoft-Dokumentation erläuterte Verfahren Weisen Sie eine Rolle zu .
- Diese Option gilt nur für Microsoft Exchange-Incidents mit **Richtlinienaktion** Option als **Quarantäne** In der Incident-Formularansicht.

Erforderliche Rolle: Endanwender

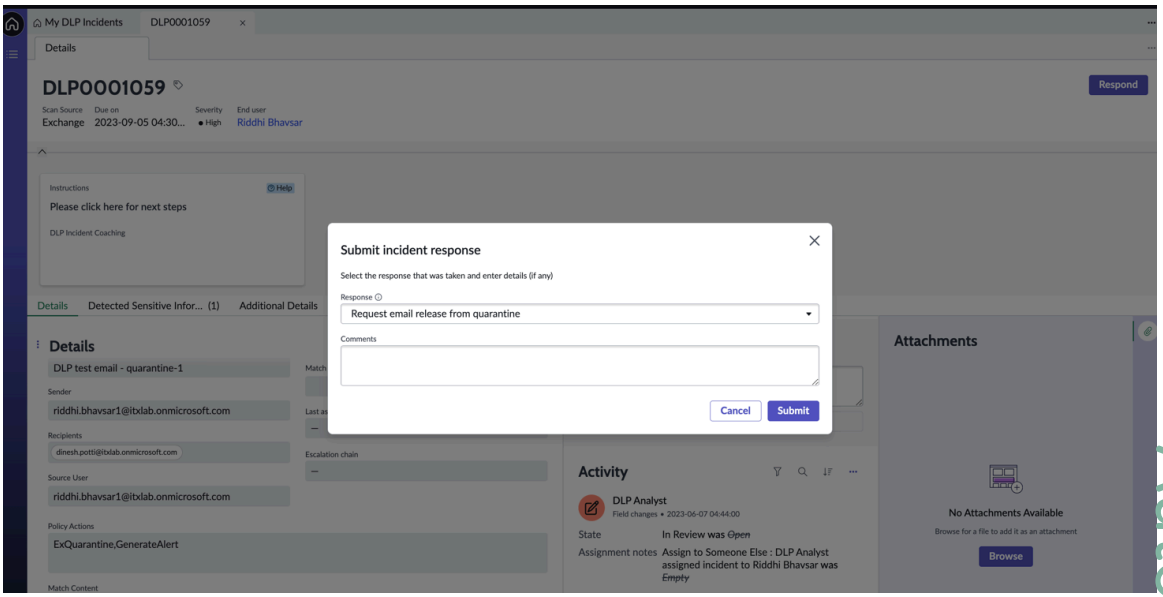
Im folgenden Verfahren wird erläutert, wie diese Aktion über den DLP-Anwenderarbeitsbereich übermittelt wird.

Prozedur

1. Navigieren zu **DLP** > **DLP-Anwenderarbeitsbereich**an.
2. Öffnen Sie einen beliebigen Microsoft Exchange DLP-Incident.
   Überprüfen Sie, ob der Incident vorliegt **Richtlinienaktion** Ist auf Quarantäne festgelegt.
3. Klicken Sie Auf **Antworten Sie** .
4. Wählen Sie Aus **Release-E-Mail aus Quarantäne anfordern** Option aus der Dropdown-Liste Antwort.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Incident-Antwort übermitteln – Option „E-Mail-Freigabe aus Quarantäne anfordern“



5. Klicken Sie auf **Absenden**.

> **Hinweis:**
> Wenn für diese Aktion eine Genehmigungsregel konfiguriert ist, wird zuerst der Genehmigungs-Flow ausgelöst, und nach Erhalt aller Genehmigungen wird der Flow „E-Mail-Freigabe aus Quarantäne anfordern“ ausgelöst, und die E-Mail wird aus der Quarantäne freigegeben. Der Status des DLP-Incidents wird auf aktualisiert **Aus Quarantäne freigegeben** Nach erfolgreichem Release.

Laden Sie Dateien für DLP-Incidents vom Typ Exchange Online, OneDrive und SharePoint herunter

Laden Sie Dateien oder E-Mails herunter, die gegen die DLP-Richtlinie für Microsoft-Zwecke verstoßen. Laden Sie diese Datei oder E-Mail von auf Ihren lokalen Computer von herunter DLP IR Incident-Ansicht. Sie können die Dateien für herunterladen DLP IR Incidents vom Typ Scan-Quelle Exchange Online, OneDrive und SharePoint.

Vorbereitungen

Erforderliche Rolle:

- sn_dlir.admin, sn_dlir.Analyst
- Beliebiger gültiger Genehmiger

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
2. Öffnen Sie einen DLP-Incident-Datensatz vom Typ Scan-Quelle Exchange Online, OneDrive oder SharePoint, der aus der Microsoft-Quelle erfasst wird.
3. Klicken Sie Auf **Datei Herunterladen** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Datei oder E-Mail, die bzw. die gegen die DLP-Richtlinie auf der Microsoft-Berechtigungsseite verstoßen hat, wird auf den lokalen Computer des Anwenders heruntergeladen.

Hinweis:
DLP-Administrator kann den Zugriff von steuern **Datei Herunterladen** Aktion durch Deaktivieren von **Sollte das Herunterladen der Datei mit Verstoß des gemeldeten Incidents zulässig sein** Einstellung auf der Seite „Erweiterte Einstellungen“. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Zeigen Sie eine Vorschau der Nachweisdateien für DLP-Incidents vom Typ Exchange Online, OneDrive und SharePoint an

Vorschau Data Loss Prevention Incident Response Nachweisdateien im DLP-IR-Analyst-Arbeitsbereich.

Vorbereitungen

Wichtig:
Bei der Verwendung der Aktion „Nachweisdateien“ im DLP-Analysten-Arbeitsbereich werden die Nachweisdateien vorübergehend in der ServiceNow-Datenbank in einem unverschlüsselten Format gespeichert. Wenn Sie die Nachweisdateien nicht speichern möchten, deaktivieren Sie die Vorschaufunktion für Nachweisdateien. Weitere Informationen finden Sie unter Erweiterte Einstellungen konfigurieren.

Erforderliche Rolle: sn_dlir.Analyst

Prozedur

1. Navigieren zu **Alle** > **DLP-Incident-Management** > **DLP-Arbeitsbereich für Analysten**an.
2. Öffnen Sie einen DLP-Incident-Datensatz.
3. Wählen Sie in der kontextbezogenen Sidebar das Symbol für Nachweisdateien ( ).
4. Auf der **Nachweisdateien** Wählen Sie die Registerkarte aus **Nachweisdatei** Karte zur Vorschau der Nachweisdateien im Dokument-Viewer.

   Die Vorschaufunktion unterscheidet sich für jeden Dateityp, wie in der folgenden Tabelle aufgeführt.

Dateiformat	Dateierweiterung
Bild	.Bmp, .gif, .ico, .JPEG, .jpg, .png, .svg und .webp. Bilddateien werden im Dokument-Viewer-Modus geöffnet.
Microsoft Office-Dateien	.Doc, .docx, .ppt, .pptx, .xls, und .xlsx Office-Dateien werden im Dokument-Viewer-Modus geöffnet.
Textdateien	.txt Textdateien werden im Texteditor-Modus geöffnet.
E-Mail-Dateien	.Eml

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateiformat	Dateierweiterung
	Hinweis: Die Dateigröße muss weniger als 5 MB betragen. Sie müssen zuerst die Datei herunterladen, um eine Vorschau des Inhalts anzuzeigen.
PDF-Dateien	.PDF ○ Geben Sie ein Stichwort ein, um das Dokument zu durchsuchen. ○ Zoom- und Verkleinerungsfunktionen, um die Ansicht für eine bessere Lesbarkeit anzupassen. ○ Drehen Sie die Seite im Uhrzeigersinn oder gegen den Uhrzeigersinn, um den Inhalt klarer anzuzeigen.

Hinweis:

Binärdateien werden nicht gerendert und müssen heruntergeladen werden, um eine Vorschau ihres Inhalts anzuzeigen. Die Funktion „Vorschaunachweisdatei“ funktioniert auch für archivierte Incidents.

Domänentrennung in Microsoft DLP-Integration

Mit der Domänentrennung können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können dann verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten anzeigen und darauf zugreifen können.

Supportstufe

Support: Standard.

Funktionsweise der Domänentrennung Microsoft DLP-Integration

Führen Sie die folgenden Schritte aus, um die Domänentrennung zu erreichen:

- Erstellen Sie einen Anwender mit Erforderliche Rolle In der jeweiligen Domäne.
- Führen Sie aus Microsoft DLP-Integrationsverfahren in der entsprechenden Domäne.

Security Operations Allgemeine Funktionalität

Wann immer eines der Plugins für den Main Security Operations Anwendungen (Security Incident Response, Vulnerability Response, Threat Intelligence, Oder Konfigurations-Compliance) aktiviert sind, Security Support Common Plugin ist aktiviert. Dieses Plugin lädt verschiedene Module, die Funktionen bereitstellen, die in allen Bereichen gemeinsam sind Security Operations Anwendungen.

Hinweis:

Nur Anwender mit [sn_sec_cmn.admin] können anzeigen und verwenden Security Operations Modul. Diese Rolle wird geerbt, wenn Ihnen in einer der Administratorrollen zugewiesen wird Security Operations Anwendungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations-Module

Funktion	Beschreibung
Referenzen zur Integration mit Security Operations, Threat Intelligence-Integrationen, Vulnerability Response-Integrationen	Mehrere Integrationen sind in enthalten Security Operations Anwendungen (Security Incident Response, Threat Intelligence, Und Vulnerability Response). Dieser Abschnitt enthält Anweisungen zum Aktivieren der Plugins und zum Konfigurieren beider ServiceNow Und Drittpartei-Integrationen. Ebenfalls enthalten sind einige grundlegende Richtlinien für die Entwicklung eigener Integrationen sowie Details zu bestimmten Integrationen, die im Basissystem enthalten sind.
Security Operations E-Mail-Verarbeitung	Mit können Sie die Integration von Informationen aus externen Erkennungssystemen einrichten, Granularität bei der Verarbeitung von Sicherheitsvorgangsdatensätzen bereitstellen, nicht abgeglichene E-Mails verarbeiten und Doppelungen von Datensätzen verhindern E-Mail-Verarbeitung.
Gruppen	• **Filtergruppen** Erstellen und verwenden Sie Filtergruppen, um Datensätze aus einer beliebigen Tabelle in Ihrer Instanz zu finden. Sie können beispielsweise eine Gruppe aller Computer desselben Herstellers erstellen. Sie können auch Konfigurationselemente (Configuration Items, CIs) filtern, die ähnliche Schwachstellen aufweisen oder in einen bestimmten Subnetz-IP-Adressbereich fallen. • **Eskalationen** Sie können einen Eskalationspfad für Security Incidents für Probleme erstellen, die mehr Aufmerksamkeit oder Fachwissen erfordern. Sobald eine Eskalationsgruppe vorhanden ist, wird bei jedem Security Incident in dieser Gruppe eine Schaltfläche angezeigt.
Sicherheits-Tags	**Tags** : Sicherheits-Tag-Regeln filtern den Zugriff auf Sicherheits-Tag.
Workflows	• **Sicherheitsworkflows anzeigen** Sie können die vielen Workflows anzeigen, die in den Security Operations-Anwendungen enthalten sind. Sie können Workflows aus Vorlagen und im Workflow-Editor erstellen. • **Workflow-Auslöser**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktion	Beschreibung
	Security Operations Workflow-Auslöser enthalten eine Bedingung für eine Tabelle. Alle an den Workflow-Auslöserdatensatz angehängten Workflows werden ausgeführt, wenn die Bedingung erfüllt ist.
Dienstprogramme	• **Ergänzungsdatenzuordnung** ErgänzungsdatenzuordnungWandelt Daten aus XML, JSON oder um EigenschaftenDateien in ServiceNow Datensätze. Security Operations Workflows verwenden Ergänzungsdatenzuordnungen und stellen Ausgabedaten für Security Incidents bereit. • **Feldwertumwandlungen** Wandelt eindeutige Kundenfeldwerte in von erkannte Feldwerte um Security Operations E-Mail-Analyse, Datenanreicherung oder Tabellen mithilfe von Feldzuordnungen. Unterstützt Auswahlfelder und Referenzen und richtet externe Daten an der Standardterminologie und dem Standardformat für Ihren neuen Datensatz aus. • **Feldzuordnung** Security Operations Tabellen können anderen Tabellen und aus anderen Tabellen zugeordnet werden, indem ein Security Incident mit einem Kundenservicefall oder ein Problem mit anderen Teilen von verknüpft wird Security Operations System. Sie können beispielsweise ein Plugin in einen integrieren Security Incident Response Aufgabe. • **Orchestration bei Bedarf** Während Security Incident Response Analyse, kann ein Sicherheitsanalyst eine Aufgabe ausführen, die von einem Security Incident-Workflow gesteuert wird. Führen Sie beispielsweise einen Prozess-Dump für ein bestimmtes CI aus. Dies kann mit Orchestration bei Bedarf erreicht werden. • **Betriebssystemgruppen** N/V

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktion	Beschreibung
	• **SecOps-Applikationsregistrierung** N/V
CMDB	**CI-Bezeichnerregeln** : CI-Bezeichner sind Regeln, die zum Suchen eines Konfigurationselements (Configuration Item, CI) in der CMDB verwendet werden, das übereinstimmende Informationen aus einer Drittpartei-Integration enthält. Diese Regeln definieren die Felder, die übereinstimmende Daten enthalten, und die Reihenfolge, nach der sie ausgewertet werden. Der niedrigste **Reihenfolge** Wert wird zuerst ausgewertet.

Erstellen und definieren Sie Filtergruppen in Security Operations

Erstellen und verwenden Sie Filtergruppen, um Datensätze aus einer beliebigen Tabelle in Ihrer Instanz zu finden. Sie können beispielsweise eine Gruppe aller Computer desselben Herstellers erstellen. Sie können auch Konfigurationselemente (Configuration Items, CIs) filtern, die ähnliche Schwachstellen aufweisen oder in einen bestimmten Subnetz-IP-Adressbereich fallen.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.write

Warum und wann dieser Vorgang ausgeführt wird

Filtergruppen können dynamisch aktualisierte Datensätze, eine Reihe statischer Datensätze, die nicht anhand von Bedingungen gefiltert werden, oder eine Kombination aus dynamisch aktualisierten und statischen Datensätzen enthalten. Einige Filtergruppen sind im Basissystem enthalten, z. B. CI-Ausschlüsse.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Gruppen** > **Filtergruppen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name der Filtergruppe.
Aktiv	Feld zum Aktivieren der Gruppe.
Beschreibung	Beschreibung für die Filtergruppe.
IP-Adresse für Netzwerk	Die Netzwerk-IP-Adresse, die die IP-Adressen der CIs enthält, die Sie der Gruppe hinzufügen möchten. Dieses Feld wird nur angezeigt, wenn Sie Konfigurationselement [cmdb_ci] oder eine Tabelle ausgewählt haben, die das Konfigurationselement in erweitert **Tabelle** Feld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Subnetzmaske	Das Subnetz, das die IP-Adressen der CIs enthält, die Sie der Gruppe hinzufügen möchten, z. B. 255.255.255.0. Dieses Feld wird nur angezeigt, wenn Sie Konfigurationselement [cmdb_ci] oder eine Tabelle ausgewählt haben, die das Konfigurationselement in erweitert **Tabelle** Feld.
Tabelle	Die Tabelle, nach der gefiltert werden soll.
Bedingung	Verwenden Sie Bedingungsgenerator Zum Definieren der zu filternden Kriterien.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Ein **Erweiterte Bedingungen** Die Registerkarte wird angezeigt.

   Je nach Typ der Tabelle, die Sie in angegeben haben, werden weitere Registerkarten angezeigt **Tabelle** Feld wie folgt:

Tabelle	Registerkarten Angezeigt
Konfigurationselement [cmdb_ci] oder eine Tabelle, die die Konfigurationselementtabelle erweitert	**Manuell hinzugefügte CIs** Und **Übereinstimmende CIs**
Aufgabe [Aufgabe] oder eine Tabelle, die die Aufgabentabelle erweitert	**Manuell Hinzugefügte Aufgaben** Und **Übereinstimmende Aufgaben**
Eine Tabelle, die nicht zu einem CI oder einer Aufgabe gehört	**Manuell hinzugefügter Datensatz**

5. So definieren Sie weitere Bedingungen für Ihre Filtergruppe:

   a. Klicken Sie Auf **Erweiterte Bedingungen** .

   b. Fügen Sie eine neue Zeile in ein **Zusätzliche Filtergruppenbedingungen** Eingebettete Liste, um andere vorgefertigte Filtergruppen auszuwählen, die Sie mit der zu aktualisierenden Filtergruppe kombinieren möchten.
   Wenn die ausgewählte Filtergruppe Datensätze basierend auf einem Referenzfeld filtern soll, wird beim Speichern des aktuellen Datensatzes automatisch ein zugeordnetes Feld ausgewählt.

   Hinweis:
   Die **Zugeordnetes Feld** Wert kann nicht aus bearbeitet werden **Zusätzliche Filtergruppenbedingungen** Eingebettete Liste. Klicken Sie auf das Informationssymbol, um das Feld zu ändern Zum Öffnen des Datensatzes.

   c. Klicken Sie auf **Aktualisieren**.

6. So fügen Sie der Filtergruppe manuell weitere CIs oder Aufgaben hinzu:

   a. Klicken Sie auf **Manuell hinzugefügte CIs** Oder **Manuell Hinzugefügte Aufgaben** Registerkarte.

   b. Klicken Sie auf **Bearbeiten**.

   c. Wählen Sie die CIs oder Aufgaben aus, die Sie hinzufügen möchten.

   d. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. So zeigen Sie die CIs oder Aufgaben an, die Ihren Auswahlkriterien entsprechen:
   a. Klicken Sie auf **Übereinstimmende CIs** Oder **Übereinstimmende Aufgaben** Registerkarte.
   b. Wenn Sie die Kriterien geändert haben, aktualisieren Sie die Liste, indem Sie mit der rechten Maustaste in den Formularheader klicken und auswählen **Aktualisieren Sie Die Liste** .

Transformation freigegebener Daten

Die Security Incident Response, Vulnerability Response, Und Threat Intelligence Plugins nutzen gemeinsame Funktionen für Beziehungsdaten und Duplizierungsregeln, die zum Importieren externer und interner Informationen in verwendet werden Security Operations.

E-Mail-Analyse, Duplizierungsregeln, Und FeldzuordnungVerwenden Sie Eingabedaten (E-Mail, JSON- oder XML-Datei oder Datensatz), und wandeln Sie diese Daten in das richtige Format um, um einen neuen Datensatz zu erstellen. Jede dieser Funktionen ruft Daten auf ihre eigene Weise ab, sie werden jedoch mithilfe vieler derselben Prozesse in den neuen Datensatz umgewandelt.

Beziehungsdaten

Wenn Sie einer zugehörigen Liste Informationen hinzufügen (z. B. ein zugehöriges erkennbares Element in einem Security Incident), können Sie einen Beziehungsdatensatz erstellen, der aus einer m2m-Tabelle besteht. Manchmal gibt es zusätzliche Daten für diesen Beziehungsdatensatz, die festgelegt werden sollen. Beispiel: Ein erkennbares Element ist eine Quell-IP (im Gegensatz zu einer Ziel-IP). Diese Informationen werden in eingegeben **Beziehungsdaten** Feld in **Feldtransformation** Formular verwendet von **E-Mail-Analyse** Oder ein **Feldzuordnungsfelder** Zugehörige Liste in **Feldzuordnung** Formular.

Die **Beziehungsdaten** Feld ist normalerweise leer. Wird am häufigsten für IP-Adressen für erkennbare Elemente in verwendet **E-Mail-Analyse** .

Sie können Daten von jedem transformieren ServiceNow Datensatz für beliebige andere ServiceNow Datensatz mit **Feldzuordnungsfelder** In **Feldzuordnung** Funktion. Zum Beispiel, um Daten von einem Incident in einen Security Incident oder von einem Security Incident in ein PRB umzuwandeln.

Security Operations-Duplizierungsregeln

Verwenden DuplizierungsregelnZur Verarbeitung doppelter Datensätze für Sicherheit, Schwachstelle, IoCs usw.

Duplizierungsregeln haben zwei Zwecke. Sie verhindern, dass zu viele doppelte Datensätze erstellt werden, und wenn ein Duplikat erkannt wird, geben sie an, welche Felder im Datensatz aktualisiert werden. Es werden nur aktive Duplikate gesucht. Wenn der Datensatz nicht aktiv ist, z. B. wenn der Incident geschlossen wird, wird jedes neue identische Problem zu einem neuen Incident.

Duplizierungsregeln werden von verwendet **E-Mail-Analyse** , **Feldzuordnung** , Und **Ergänzungsdatenzuordnung** .

Zugehörige Informationen

Erstellen Sie E-Mail-Parser in Security Operations

Ordnen Sie Tabellen mit der Feldzuordnung „Security Operations“ zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Duplizierungsregeln in Security Operations

Sie können verwenden DuplizierungsregelnUm neue E-Mails, Ergänzungsdaten oder Feldzuordnungen mit aktiven doppelten Datensätzen zu identifizieren und entsprechend zu verarbeiten.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.write

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Duplizierungsregeln**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular entsprechend aus:

Duplizierungsregel

Feld	Beschreibung
Name	Der Name der Duplizierungsregel.
Tabelle	Tabelle, in der Datensätze erstellt und zur Bestimmung der Duplizierung verwendet werden.
Identifizierende Felder	Wählen Sie eine Reihe von Feldern aus, die einen doppelten Security Incident, ein erkennbares Element, eine Schwachstelle usw. anzeigen, wenn die Werte in diesen Feldern identisch sind.
Duplikataktion	Steuert, wie doppelte E-Mails behandelt werden. Die Auswahlmöglichkeiten lauten wie folgt: **Als untergeordnet erstellen** Erstellt einen Datensatz als untergeordnetes Element des Originals. Das Feld, das das untergeordnete Element mit dem übergeordneten Element verknüpft, ist **Übergeordnet** Feld. **Datensätze nicht erstellen oder aktualisieren** (Standard) führt nichts aus. Ignoriert Duplikate. **Duplizierten Datensatz aktualisieren** Aktualisiert die Felder im vorhandenen Datensatz wie in angegeben **Duplizierungsaktionen.** **Hinweis:** Wenn Sie wählen **Doppelten Datensatz aktualisieren** , **Duplizierungsaktionen** Zugehörige Liste wird angezeigt.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Regel zu aktivieren.
Beschreibung	Beschreibt den Zweck und die Anwendung dieser Duplizierungsregel; wann sie verwendet werden soll, z. B. eine Regel für IP-basierte erkennbare Elemente oder Security Incidents aus der Firewall.

4. Klicken Sie mit der rechten Maustaste in den Datensatzheader, und wählen Sie aus **Speichern** Oder klicken Sie auf **Aktualisieren** .
5. Zum Festlegen von Duplizierungsaktionen, wenn Sie ausgewählt haben **Doppelten Datensatz aktualisieren** , Klicken Sie auf **Neu** Um Duplikationsaktionen für jedes Feld zu erstellen, das Sie im Incident aktualisieren möchten.

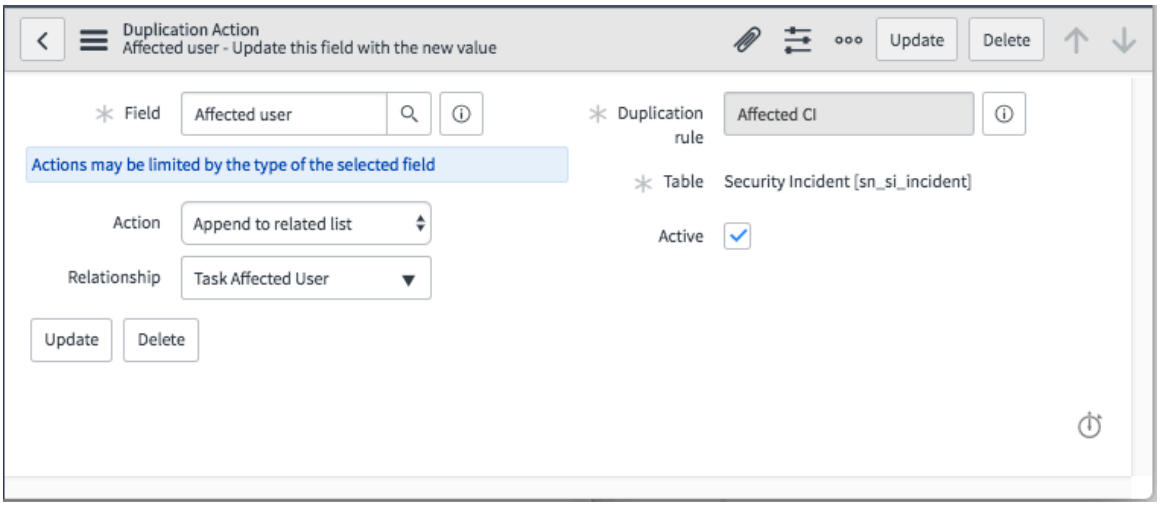
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Füllen Sie die Felder im Formular aus, oder bearbeiten Sie sie, um zu beschreiben, wie das Feld aktualisiert wird:

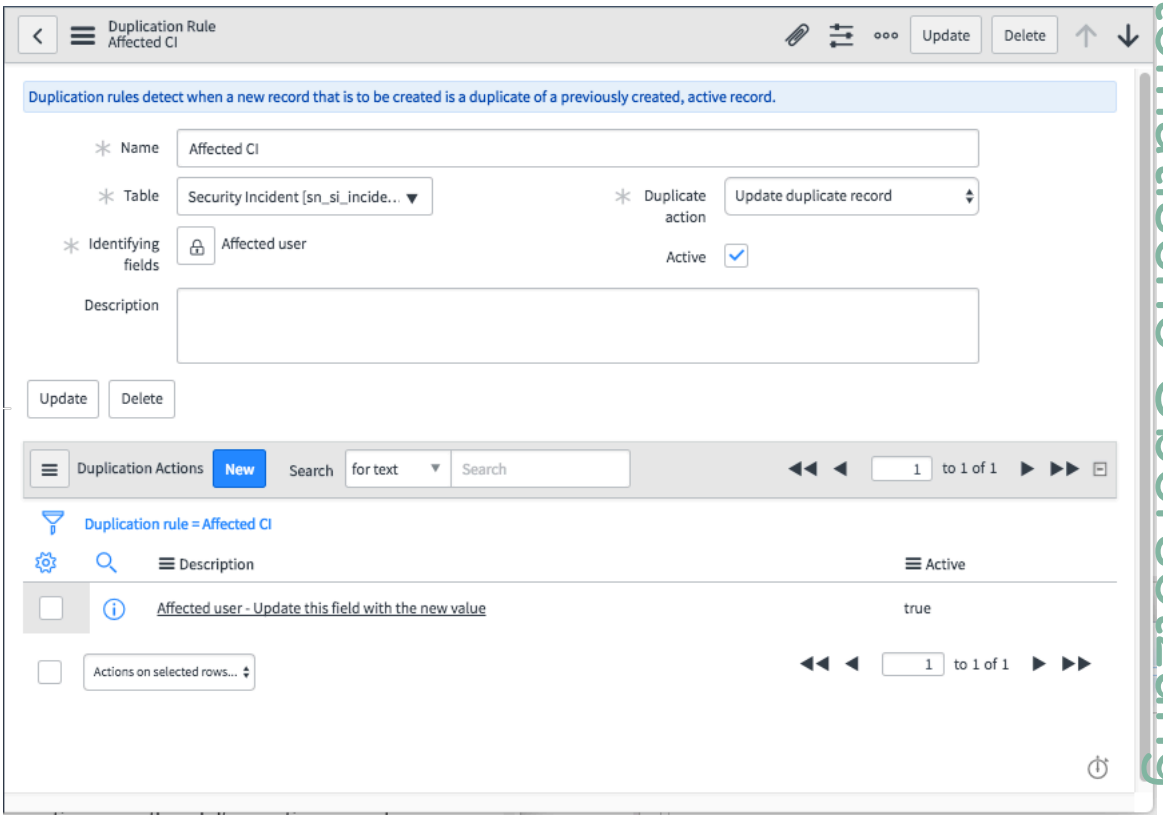
Duplizierungsaktionen

Feld	Beschreibung
Feld	Der Name des Felds, das für die Duplizierungsaktion verwendet werden soll.
Aktion	Die unterstützten Aktionen variieren je nach Feldtyp. Die Auswahlmöglichkeiten lauten wie folgt: **Dieses Feld mit dem neuen Wert aktualisieren** Ersetzt den vorherigen Wert im vorhandenen Datensatz durch diesen Wert. **Neuen Wert an eine kommagetrennte Liste anhängen, falls einzigartig** Behandelt den Wert als Eintrag in einer durch Kommas getrennten Liste und fügt die neuen Daten (falls vorhanden) als neuen Eintrag in diese Liste hinzu. Wenn sich die Daten bereits in der Liste befinden, werden sie nicht zweimal hinzugefügt. **Neuen Wert an dieses Feld anhängen** Fügt den neuen Wert an das Ende des vorhandenen Texts im Feld an. **Einmal zu einem Zählerfeld hinzufügen** Fügt dem numerischen Feld eine hinzu. **Feld auf heute einstellen** Legt das Feld auf das aktuelle Datum und die aktuelle Uhrzeit fest. **An zugehörige Liste anhängen** Fügt den zugehörigen Datensatz mit diesem Wert der zugehörigen Liste des aktuellen Datensatzes hinzu. Wird angezeigt, wenn eine viele-zu-viele-Tabelle mit einer Spalte desselben Typs mit der zu aktualisierenden Tabelle verknüpft ist. Beispiel: **Betroffenes CI** Oder **Betroffener Anwender** .
Beziehung	[Optional] dieses Feld wird nur angezeigt, wenn **An zugehörige Liste anhängen** Aktion ist ausgewählt. Dies ist der Name der zugehörigen Liste, die Sie dieser Regel zuordnen möchten.
Duplizierungsregel	Regel, zu der diese Aktion gehört.
Tabelle	Tabelle, in der Datensätze erstellt werden. Wird nur als Information angezeigt.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Aktion zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Absenden**.



Automatische Übersetzung

Security Operations E-Mail-Verarbeitung

Mit können Sie die Integration von Informationen aus externen Erkennungssystemen einrichten, Granularität bei der Verarbeitung von Sicherheitsvorgangsdatensätzen bereitstellen, nicht abgeglichene E-Mails verarbeiten und Doppelungen von Datensätzen verhindern E-Mail-Verarbeitung.

E-Mail-Verarbeitung Besteht aus diesen Funktionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktion	Beschreibung
E-Mail-Analyse	Generieren Sie neu Security Operations Datensätze aus externen System-E-Mails.
Duplizierungsregeln	Identifiziert neue E-Mails mit bekannten Incidents und verarbeitet sie entsprechend.
Eigenschaften	Gibt Accounts an, die als Eingabe in verwendet werden E-Mail-AnalyseFür Sicherheit, Schwachstellen und IoCs. Bietet Granularität bei der Verarbeitung Security Operations Datensätze.
Nicht übereinstimmende E-Mails	Listet E-Mails auf, die keinen entsprechen Security Operations Datensatz.

E-Mail-Eigenschaften für Security Operations

E-Mail EigenschaftenGeben Sie an, welche Posteingänge als Eingabe in verwendet werden E-Mail-AnalyseDient zum Importieren von Informationen aus externen Erkennungssystemen, um Datensätze für Sicherheit, Schwachstellen und IoCs zu erstellen. Sie können einen allgemeinen Account für alle externen Erkennungssysteme oder einzelne E-Mail-Accounts für einrichten Security Incident Response, Threat Intelligence, Oder Vulnerability Response.

Erstellen Security Operations E-Mail-Eigenschaften

Sie können E-Mail-Adressen für Berichte angeben und das automatische E-Mail-Verhalten per E-Mail steuern Eigenschaften.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Richten Sie externe Erkennungstools ein, um E-Mails an Ihren E-Mail-Analyseeingang zu senden.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Verarbeitung** > **Eigenschaften**an.
2. Geben Sie Ihre Empfänger-Postfächer entsprechend ein:
   Dies sind eingehende E-Mail-Adressen, von denen verarbeitet werden soll **E-Mail-Analyse** , Anstatt **Eingehende Aktionen** .

Eigenschaften der E-Mail-Analyse

Feld	Beschreibung
Posteingang für Security Operations Tools	Vollständige E-Mail-Adresse für Security Operations. Beispiel: secops_support@yourcompany.com.
Postfach für Security Incident-Tools	Vollständige E-Mail-Adresse für Security Incident Response. Beispiel: sir_support@your.company.com.
Posteingang für Vulnerability Response Tools	Vollständige E-Mail-Adresse für Vulnerability Response. Beispiel: vuln_resp@yourcompany.com.
Posteingang für Threat Intelligence Tools	Vollständige E-Mail-Adresse für Threat Intelligence. Beispiel: threat_intel@yourcompany.com.

3. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations E-Mail-Analyse

Generieren Sie neu Security Operations Datensätze aus externen Erkennungssystemen mit E-Mail-Analyse. Diese Funktion bietet eine Methode zum Integrieren von Informationen aus externen Tools wie Malware-Erkennung, Schwachstellenerkennung, Firewalls, Threat Intelligence und mehr.

Wie E-Mails analysiert werden

Jedes System, das eine E-Mail senden kann, kann erstellen Security Operations Datensätze, z. B. Security Incidents, Anforderungen, angreifbare Elemente, Schwachstellen, erkennbare Security Incident-Elemente, Angriffsmethoden und mehr.

Alle Security Operations Plugins (Security Incident Response, Threat Intelligence, Und Vulnerability Response) Haben eine Eigenschaft (**E-Mail_an**), die die E-Mail-Adresse definiert, an die externe Integrationen E-Mails senden sollen, die von den E-Mail-Parsern analysiert werden sollen. Siehe **E-Mail-Verarbeitung** > **Eigenschaften** Weitere Informationen finden Sie unter .

E-Mail an einen der gesendet Security Operations E-Mail-Adressen werden in einer E-Mail-Ereignistabelle gespeichert. Diese E-Mails werden verarbeitet, um festzustellen, ob sie mit einem E-Mail-Parser übereinstimmen.

E-Mails, die eine Übereinstimmung aufweisen, werden gekennzeichnet, und die Transformations- und Duplizierungsregeln erstellen oder aktualisieren einen Security Operations Datensatz. Die E-Mail ist mit diesem Datensatz verknüpft und als gekennzeichnet Übereinstimmend .

E-Mails, die nicht übereinstimmen, werden in aufgeführt Nicht übereinstimmende E-MailsAls Security Operations Datensatz. Sie können überprüft werden, um E-Mail-Parser zur Verarbeitung dieser E-Mails zu erstellen. Mit der Aktion „erneut verarbeiten“ können Sie die nicht abgeglichene E-Mail erneut über die Parser ausführen. Das ursprüngliche E-Mail-Protokoll ist mit diesem Datensatz verknüpft.

Die Duplizierungsregeln für die E-Mail-Transformation verwalten mehrere E-Mails im Zusammenhang mit demselben Problem. Diese Regeln definieren, was zu einem doppelten Datensatz führt, und können verhindern, dass doppelte Datensätze erstellt werden. Wenn ein Duplikat erkannt wird, gibt die Regel an, welche Aktion ausgeführt werden soll: Keine Aktion (keinen neuen Datensatz erstellen), neuen Datensatz als untergeordneten Datensatz des vorhandenen Datensatzes erstellen oder den vorhandenen Datensatz aktualisieren. Beim Aktualisieren gibt die Duplikatregel an, welche Felder im vorhandenen Datensatz aktualisiert werden.

Hinweis:
A Security Operations E-Mail-Parser funktioniert in Verbindung mit eingehenden Plattformaktionen und ersetzt sie nicht. Das Festlegen von Werten für indirekte Felder wird nicht unterstützt, z. B. **sys_Journal_field** Einträge.

Standardmäßig werden E-Mail-Ereignisse nach 30 Tagen gelöscht.

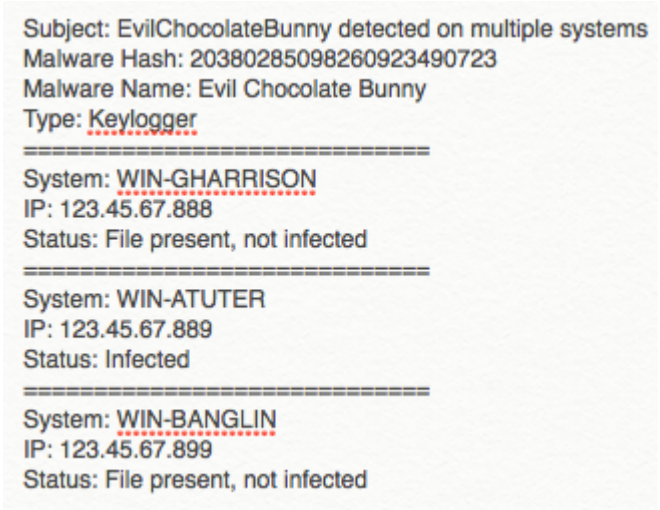
Mehrere Datensätze

Externe Erkennungssysteme (Malware-Erkennung, Schwachstelle usw.) können E-Mails senden, die mehrere Elemente gleichzeitig melden. Der E-Mail-Parser unterstützt Trennzeichen innerhalb der E-Mail.

Beispielsweise könnte Ihnen ein Malware-Detektor einen E-Mail-Bericht über alle Systeme in Ihrem Netzwerk senden, die von einer bestimmten Malware infiziert sind, und zuerst Informationen zur Malware, gefolgt von einer Liste der betroffenen Systeme.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für schädliche E-Mails



In diesem Beispiel, wenn **Datensatztrennzeichen** Ist in festgelegt **E-Mail-Transformation** Als **==========** , Teilt die E-Mail in vier Abschnitte auf, die separat ausgewertet werden. Dadurch wird für jedes der drei betroffenen Systeme ein Security Incident erstellt.

Hinweis:
Der Header-Abschnitt wird erkannt, weist jedoch keine betroffenen Systeme auf. Daher wird er in allen drei Datensätzen verwendet und erstellt keinen vierten Datensatz.

Feldtransformationen Rufen Sie Daten aus jedem Abschnitt ab. Wenn etwas in der Header- oder Fußzeile der E-Mail für alle Datensätze gilt, z. B. Malware-Hash, Malware-Name und Typ in diesem Beispiel, sollte die Feldtransformation für sie festgelegt werden **Suchen Sie nach Wert** Zu einem Wert, der entweder innerhalb des E-Mail-Texts sucht **Am Anfang einer Zeile im E-Mail-Text** Oder **An beliebiger Stelle im E-Mail-Text** .

Feldtransformation S müssen für die Suche festgelegt werden **Am Anfang einer Zeile im Datensatzabschnitt** Oder **Sek** Für Daten, die in jedem Abschnitt definiert sind, z. B. System, IP-Adresse oder Status. Die Optionen für den Datensatzabschnitt sind nur verfügbar, wenn in der E-Mail-Transformation ein Datensatztrennzeichen definiert ist.

Beim Analysieren einer E-Mail mit einem definierten Trennzeichen werden Datensätze nur für Abschnitte mit mindestens einem Stück abschnittsspezifischer Daten erstellt.

In diesem Beispiel werden drei Datensätze erstellt, obwohl vier Abschnitte definiert sind. Der erste Abschnitt ist ein Header, und es fehlt alles, was für nur ein System spezifisch ist. Wenn eines der Felder im ersten Abschnitt ausgefüllt wurde (System, IP oder Status), wird auch für diesen Abschnitt ein Datensatz erstellt.

Zugehörige Informationen

- Erstellen Sie E-Mail-Parser in Security Operations
- Security Operations Ergänzungsdatenzuordnung
- Security Operations Feldzuordnung

Erstellen Sie E-Mail-Parser in Security Operations

E-Mail-AnalyseErstellt Security Operations Datensätze aus Ihrer E-Mail für Sicherheit, Schwachstellen und erkennbare Elemente, um die Reaktion auf Bedrohungen und die Korrektur zu beschleunigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Richten Sie externe Erkennungstools ein, um E-Mails an eine zentrale E-Mail-Adresse zu senden.
- Legen Sie die E-Mail-Adresse in Security Operations-Eigenschaften fest. Weitere Informationen finden Sie unter Erstellen Security Operations E-Mail-Eigenschaften.
- Weisen Sie dieser E-Mail-Adresse einen Anwenderaccount zu, und weisen Sie diesem Anwender Sicherheitszugriffssteuerungen zu, um die E-Mail-Ereignisdatensätze zu erstellen und zu aktualisieren.
- Halten Sie eine Kopie der relevanten E-Mail aus Ihrem externen Erkennungstool vor sich.
- Entscheiden Sie, welche Art von Datensatz Sie erstellen möchten, einen Security Incident, einen Schwachstellendatensatz, eine Aufgabe usw. Diese Auswahl bestimmt die von Ihnen ausgewählte Tabelle.

Erforderliche Rolle: sn_sec_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Analyse**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Hinweis:
Wenn mehr als ein Feld angegeben ist, müssen alle Felder mit der E-Mail übereinstimmen, um einen Datensatz zu erstellen.

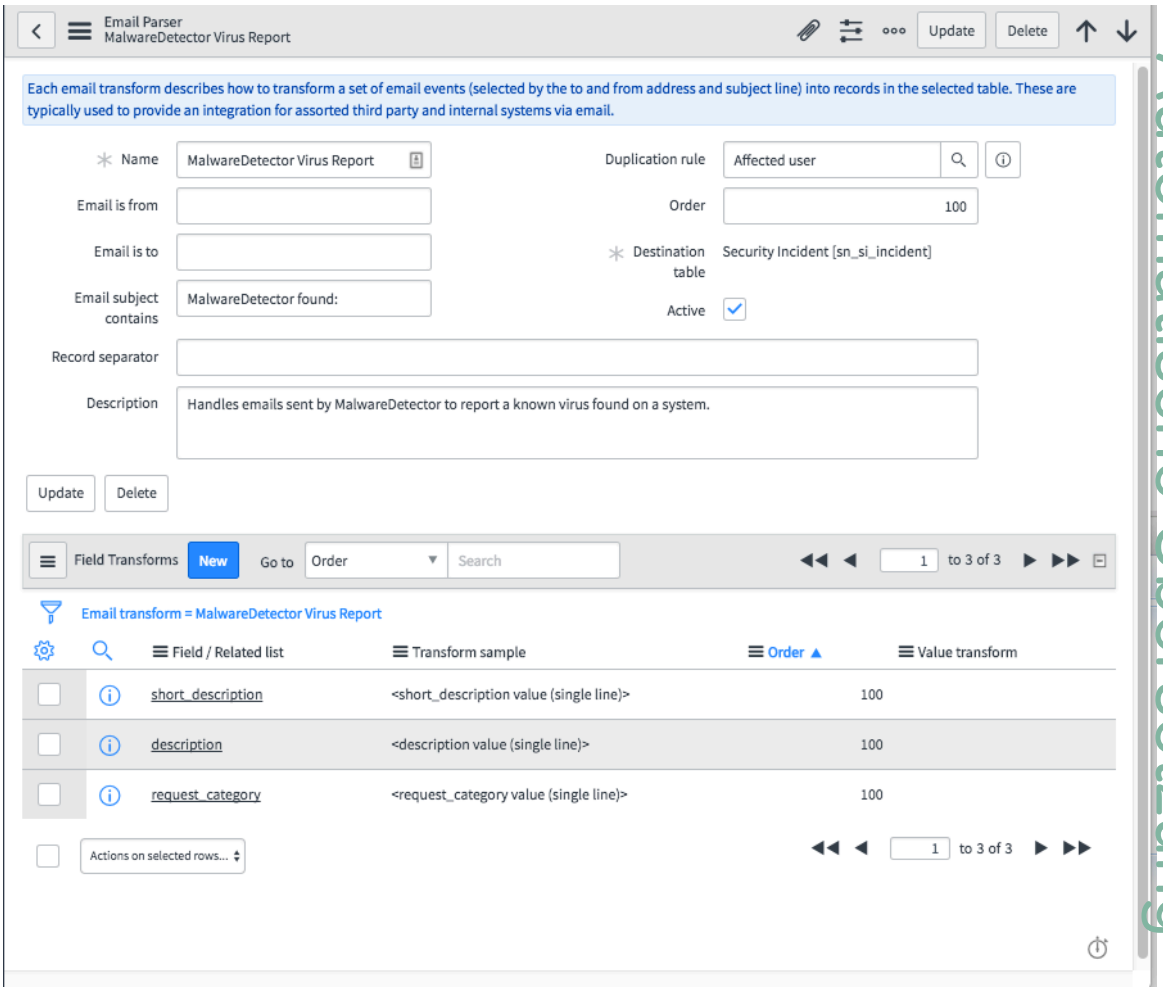
E-Mail-Parser

Feld	Beschreibung
Name	Der Name des E-Mail-Parsers.
E-Mail ist von	Wenn ausgefüllt, werden nur E-Mails von dieser Adresse von diesem E-Mail-Parser umgewandelt.
E-Mail an	Wenn ausgefüllt, werden nur E-Mails von dieser Adresse von diesem E-Mail-Parser umgewandelt.
E-Mail Betreff enthält	Wenn ausgefüllt, werden nur E-Mails, in denen der Betreff diesen Ausdruck enthält, von diesem E-Mail-Parser umgewandelt.
Duplizierungsregel	Steuert, wie doppelte E-Mails für alle E-Mails behandelt werden, die diese Transformation verarbeitet. Weitere Informationen finden Sie unter Transformation freigegebener Daten.
Reihenfolge	In welcher Reihenfolge die Transformationen berücksichtigt werden sollen. Die erste übereinstimmende E-Mail-Transformation wird verwendet. Normalerweise möchten Sie die spezifischsten E-Mail-Parser in den niedrigeren Zahlen mit einem Fallback einrichten. Geben Sie Catchall-E-Mail-Parser höher an **Reihenfolge** Nummern, damit sie ausgeführt werden, wenn nichts anderes übereinstimmt. Der Standardwert ist 100. Wenn alles übereinstimmt, stimmt der spezifischste E-Mail-Parser (stimmt überein **Von** , **Bis** , Und **Betreff**) Wird verwendet.
Zieltabelle	Die Tabelle, in der Sie Datensätze erstellen möchten.
Aktiv	Gibt an, ob diese Transformation aktiv, in Gebrauch oder nicht aktiv ist. Wenn diese Option deaktiviert ist, werden keine E-Mails mit diesem Code umgewandelt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Datensatztrennzeichen	Wenn E-Mails, die von diesem E-Mail-Parser verarbeitet werden, mehrere Datensätze erstellen, enthält dieses Feld das Trennzeichen zwischen den Informationen für diese Datensätze. Weitere Informationen finden Sie unter Security Operations E-Mail-Analyse.
Beschreibung	Beschreibung dieses E-Mail-Parsers, mit welchem Tool er arbeitet, der Zweck usw.

4. Wenn Sie Ihre Einträge abgeschlossen haben, klicken Sie mit der rechten Maustaste in den Formularheader, und wählen Sie aus **Speichern** .
   A **Feldtransformationen** Die Registerkarte wird angezeigt. Diese Registerkarte zeigt, wie einzelne Felder in der Zieltabelle basierend auf dem E-Mail-Inhalt festgelegt werden.



5. Zum Hinzufügen **Feldtransformationen** , Führen Sie diese Schritte aus.
   a. In **Feldtransformationen** Klicken Sie auf die Registerkarte **Neu** .
   b. Füllen Sie die entsprechenden Felder im Formular aus.

Option	Bezeichnung
Feld	**Beschreibung**
Wert in einem Feld oder einer zugehörigen Liste speichern	Wählen Sie aus, wo der Wert gefunden werden soll. Zur Auswahl stehen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	○ Speichern Sie den Wert in einem Feld im neuen Datensatz ○ Verknüpfung mit diesem Wert in einer zugehörigen Liste erstellen ○ Verknüpfung mit diesem Wert erstellen und neuen Datensatz erstellen, wenn kein übereinstimmender Datensatz vorhanden ist **Hinweis:** Wenn die Zieltabelle keine zugehörigen Listen enthält, wird dieses Feld nicht angezeigt.
Feld	Wählen Sie das Feld aus, das mit diesem Wert ausgefüllt werden soll. **Hinweis:** Für Auswahlfelder werden Übereinstimmungen mit vorhandenen Auswahlmöglichkeiten mithilfe der zugrunde liegenden Auswahlbezeichnung oder des zugrunde liegenden Werts getroffen. Wenn keine Übereinstimmung gefunden wird, wird das Feld festgelegt, der Auswahlliste wird jedoch kein neuer Eintrag hinzugefügt. Weitere Informationen finden Sie unter Auswahllisten . Für Referenzfelder wird ein Eintrag nur festgelegt, wenn ein Wert dem Anzeigenamen des Datensatzes entspricht oder ein gültiger Wert vorliegt `sys_ID` Wurde gefunden. Weitere Informationen finden Sie unter Referenzfelder .
Zugehörige Liste	Wenn **Speichern Sie den Wert in einem Feld oder einer zugehörigen Liste** Ist auf festgelegt **Link zu diesem Wert in einer zugehörigen Liste** Oder **Link zu diesem Wert, um einen neuen Datensatz zu erstellen, wenn kein übereinstimmender Datensatz vorhanden ist** , Dieses Feld gibt die zugehörige Liste an, zu der Informationen hinzugefügt werden sollen.
Wertfeld	Wenn **Speichern Sie den Wert in einem Feld oder einer zugehörigen Liste** Ist auf festgelegt **Link zu diesem Wert in einer zugehörigen Liste** Oder **Link zu diesem Wert, um**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	einen neuen Datensatz zu erstellen, wenn kein übereinstimmender Datensatz vorhan den ist , Dieses Feld gibt das Feld innerhalb der Tabelle an, das in der zugehörigen Lis–te angezeigt wird. Wird verwendet, um ei–nen vorhandenen Datensatz zu suchen und zu finden. Beispiel: Wenn Ihre zugehöri–ge Liste lautet **Betroffene CIs** , Dieses Feld kann enthalten **Name** Oder **Vollqualifizier ter Domänenname** , Oder ein anderes Feld im CI-Datensatz, das zum Suchen des CI verwendet werden soll, das zu hinzugefügt wurde **Betroffene CIs** Liste.
Beziehungsdaten	Wenn **Speichern Sie den Wert in einem Feld oder einer zugehörigen Liste** Ist auf festge–legt **Link zu diesem Wert in einer zugehöri gen Liste** , Wird ein Datensatz erstellt, um diesen Datensatz (z. B. einen Security Inci–dent) mit dem Wert (CI, erkennbares Ele–ment usw.) zu verknüpfen. Dieses Feld gibt alle zusätzlichen Informationen (Feld- und Wertpaare) an, die dem Verknüpfungsda–tensatz hinzugefügt werden sollen. Geben Sie beispielsweise beim Hinzufügen eines erkennbaren Elements für eine Quell-IP an, dass diese IP die Quell- und nicht die Ziel-IP ist. Verwenden Sie für mehrere Wer–te ein ^-Trennzeichen, z. B. TYPE= Quell-IP^Active=true.
Neue Datensatzdaten	Wenn **Speichern Sie den Wert in einem Feld oder einer zugehörigen Liste** Ist auf festge–legt **Link zu diesem Wert, um einen neuen Datensatz zu erstellen, wenn kein überein stimmender Datensatz vorhanden ist** Wenn kein zugehöriger Datensatz gefunden wird, der dem analysierten Wert entspricht, wird ein Datensatz erstellt. Dieses Feld gibt die statischen Daten an, die diesem Datensatz hinzugefügt werden sollen. Für **Betroffenes CI** S: Wenn keine übereinstimmenden CIs gefunden werden, wird ein CI-Datensatz erstellt). Wenn dies geschieht, wird der in der E-Mail gefundene Wert auf festgelegt **Wert** Feld im CI-Datensatz. Sie können zu–sätzliche Daten festlegen – eine Notiz, die angibt, warum das CI erstellt wurde, eini–ge Informationen darüber, mit welcher Art von CIs Sie arbeiten usw. Ein Beispiel wäre: Description=Created by Malware Scanner Email Parser^type=autodetect.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Suche nach Wert	Wählen Sie den zu suchenden Standort in der E-Mail aus. Zur Auswahl stehen: ○ **Am Anfang einer Zeile im E-Mail-Text** ○ **Irgendwo im E-Mail-Text** ○ **In der E-Mail-Betreffzeile** ○ **Immer der statistische Wert** Wenn Sie eine definiert haben **Datensatz trennzeichen** , Weitere Optionen (**An belie biger Stelle im Datensatzabschnitt** Und **Am Anfang einer Zeile im Datensatzabschnitt)** Ermöglichen Sie es Ihnen, nur innerhalb des aktuellen Abschnitts und nicht im gesamten E-Mail-Text zu suchen (siehe Security Operations E-Mail-Analyse Weitere Informationen finden Sie unter . Informationen, die sich in einer Kopf- oder Fußzeile befinden und für alle Datensät–ze gelten, werden im gesamten E-Mail-Text gesucht. Die Informationen, die sich zwi–schen Datensätzen unterscheiden, werden nur innerhalb des Abschnitts gesucht.
Werttrennzeichen	Wenn **Speichern Sie den Wert in einem Feld oder einer zugehörigen Liste** Ist auf festge–legt **Link zu diesem Wert in einer zugehöri gen Liste** Oder **Link zu diesem Wert, um ei nen neuen Datensatz zu erstellen, wenn kein übereinstimmender Datensatz vorhanden ist** , Dieses Feld gibt das Trennzeichen an, das für Listen von Elementen verwendet werden soll. Zum Beispiel ein Komma oder Semikolon, wenn die Daten aus der E-Mail eine Liste von IP-Adressen sind.
Wertepräfix	Der Text, der immer dem Wert vorangeht, der in diesem zu extrahierenden Feld plat–ziert wird.
Ende des Werts	Wählen Sie aus, was das Ende des Werts angibt. Auswahlmöglichkeiten: **Zeilenende** , **Ende der E-Mail** (Bringt den gesamten ver–bleibenden Text in die E-Mail ein), oder **Bis** (Wird angehalten, wenn der angegebene Text gefunden wird), oder **Bis** (Wird ange–halten, wenn der angegebene Text gefun–den wird).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Wertesuffix	Wenn **Ende des Werts** Ist auf festgelegt **Bis** , Dieses Feld gibt an, welcher Text immer dem Wert folgt, der in diesem Feld platziert wird. Beispielsweise wird nach einem Wert ge–sucht, der nach „der betroffene Computer ist“ und vor „“ steht. Analysiert „AB123“ aus „der dementierte Bunny-Virus wur–de gefunden. Der betroffene Computer ist AB123. Die geschätzte Infektionszeit be–trug 45 Uhr in einer E-Mail.
Wertumwandlung	Wählen Sie den anzuwendenden Feldtransformati-onseintrag aus. Konvertiert den in der E-Mail gefun-denen Wert in einen anderen Wert, der zum Ausfül-len von Auswahlfeldern, gelegentlich als Referenz und anderen Feldern verwendet wird .
Reihenfolge	Die Reihenfolge, in der die Feldtransformationen ausgeführt werden, vom niedrigsten zum höchsten. Eine Feldtransformation mit einem Reihenfolgeein-trag von 100 wird zuerst versucht. Nur wenn die-se Feldtransformation keinen Wert findet, wird eine Feldtransformation mit einer höheren Reihenfolge (200) im selben Feld ausgeführt.
E-Mail-Transformation	Die Transformation, zu der diese Feldtransformation gehört.
Zieltabelle	Zieltabelle der E-Mail-Transformation. Enthält Infor-mationsdaten aus der E-Mail-Transformation.
Aktiv	Der Standardwert ist aktiviert. Wenn diese Option aktiviert ist, wird die Feldtransformation aktiviert. Deaktivieren Sie dieses Kontrollkästchen, um die Feldtransformation zu deaktivieren.

a. Klicken Sie auf **Absenden**.
Der neue Datensatz wird verwendet, um die Informationen in der E-Mail in einen neuen Datensatz zu analysieren.

Zugehörige Informationen

Erstellen Sie Duplizierungsregeln in Security Operations

Erstellen Security Operations Feldwerttransformationen

Definieren Vulnerability ResponseE-Mail-Benachrichtigungen

Bearbeiten Sie E-Mail-Datensätze in Security Operations

Fügen Sie Ihren vorhandenen E-Mail-Ereignisdatensätzen Transformationen hinzu, oder erstellen Sie sie.

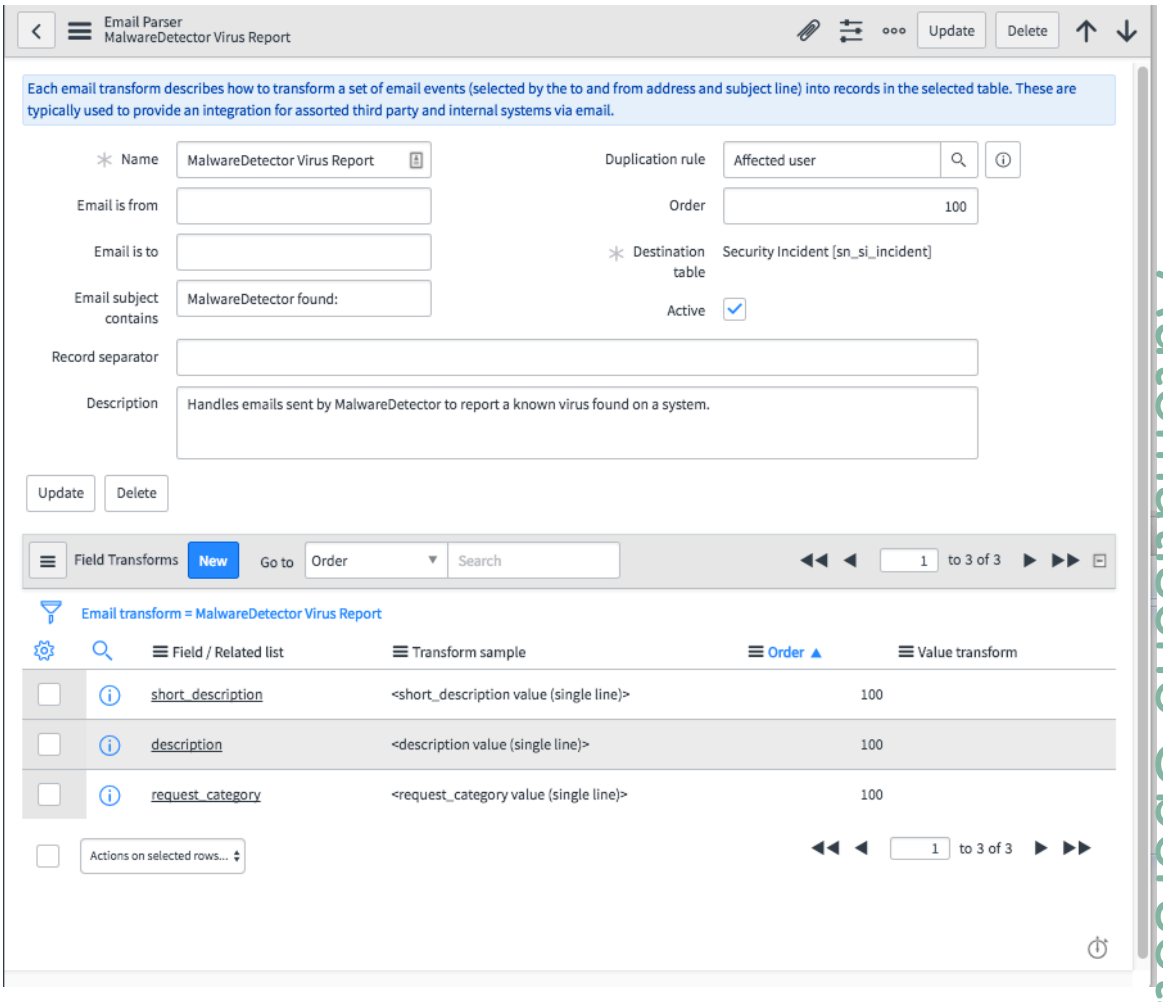
Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **E-Mail-Analyse**an.
2. Klicken Sie zum Bearbeiten auf den E-Mail-Parser.
   Wenn der Datensatz schreibgeschützt ist, klicken Sie auf Hier Link in der Header-Nachricht.
   Sie gelangen zum bearbeitbaren Formular der Transformation.



3. Bearbeiten Sie Felder nach Bedarf.
4. Zum Bearbeiten **Feldtransformationen** , Klicken Sie in das Feld, und ändern Sie es entsprechend.
5. Klicken Sie auf **Aktualisieren.**

Nicht Abgeglichen Security Operations E-Mail-Ereignisse

Für E-Mail-Ereignisse, die keinem E-Mail-Parser entsprechen, ist die Kennzeichnung „abgeglichen“ deaktiviert. Sie können diese E-Mail-Ereignisdatensätze über anzeigen Nicht übereinstimmende E-MailsListe, um externe Erkennungssysteme anzuzeigen, deren E-Mails noch nicht analysiert wurden.

Während Sie E-Mail-Parser erstellen, können Sie versuchen, das E-Mail-Ereignis (aus dem Formular oder der Liste) erneut zu verarbeiten, um einen neuen E-Mail-Parser zu validieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie nicht abgeglichene Security Operations-E-Mails an, und verarbeiten Sie sie erneut

Sie können überprüfen Nicht übereinstimmende E-MailsFür eingestellte Filter oder als Kandidaten für einen neuen Filter, um die Rate beizubehalten oder zu verbessern, mit der Sie E-Mail-Bedrohungen erkennen.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.read

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Nicht übereinstimmende E-Mails**an.
   Wenn nicht übereinstimmende E-Mails gefunden wurden, werden sie aufgelistet.
2. Die Felder im Formular lauten wie folgt:

Sicherheits-E-Mail-Ereignisse

Feld	Beschreibung
Von	E-Mail-Adresse des Absenders.
An	E-Mail-Adresse der Empfänger.
Betreff	Betreffzeile in der E-Mail.
Textkörper	Inhalt des Textkörpers der E-Mail.
Abgleich	Gibt an, ob dieses E-Mail-Ereignis abgeglichen wurde.

3. Um diese E-Mail erneut zu verarbeiten, erstellen Sie einen E-Mail-Datensatz, oder bearbeiten Sie einen vorhandenen E-Mail-Datensatz, um den Informationen in dieser E-Mail zu entsprechen.
   Weitere Informationen finden Sie unter Erstellen Sie E-Mail-Parser in Security Operations.
4. Navigieren Sie zurück zu **Security Operations** > **Nicht übereinstimmende E-Mails**an.
5. Klicken Sie Auf **E-Mail-Ereignis Erneut Verarbeiten** Um zu versuchen, diese E-Mail zu verarbeiten. Sie kehren zu zurück Nicht übereinstimmende E-MailsHauptliste. Wenn der neue E-Mail-Datensatz übereinstimmt, befindet sich das E-Mail-Ereignis nicht mehr in der Liste. Eine Nachricht gibt an, ob sie abgeglichen wurde oder nicht.

Security Operations Feldzuordnung

Security Operations Tabellen können anderen Tabellen und aus anderen Tabellen zugeordnet werden, indem ein Security Incident mit einem Kundenservicefall oder ein Problem mit anderen Teilen von verknüpft wird Security Operations System.

Feldzuordnung Definiert die Zuordnung, die verwendet wird, wenn ein Datensatz aus der Quelltabelle zum Erstellen eines neuen Datensatzes in der Zieltabelle verwendet wird. Diese Karten werden normalerweise verwendet, um einen Security Incident aus einem anderen Datensatz zu erstellen. Sie definieren, welche Felder in einem Security Incident in ein neues Problem eingefügt werden oder welche Felder aus einem vorhandenen Kunden-Incident einen neuen Security Incident ausfüllen.

Ordnen Sie Tabellen mit der Feldzuordnung „Security Operations“ zu

Security Operations Bietet Ihnen eine feinere Feldzuordnungsgranularität, damit Sie eine zuordnen können Security Operations Tabelle zu einer anderen Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Sec_cmn.write

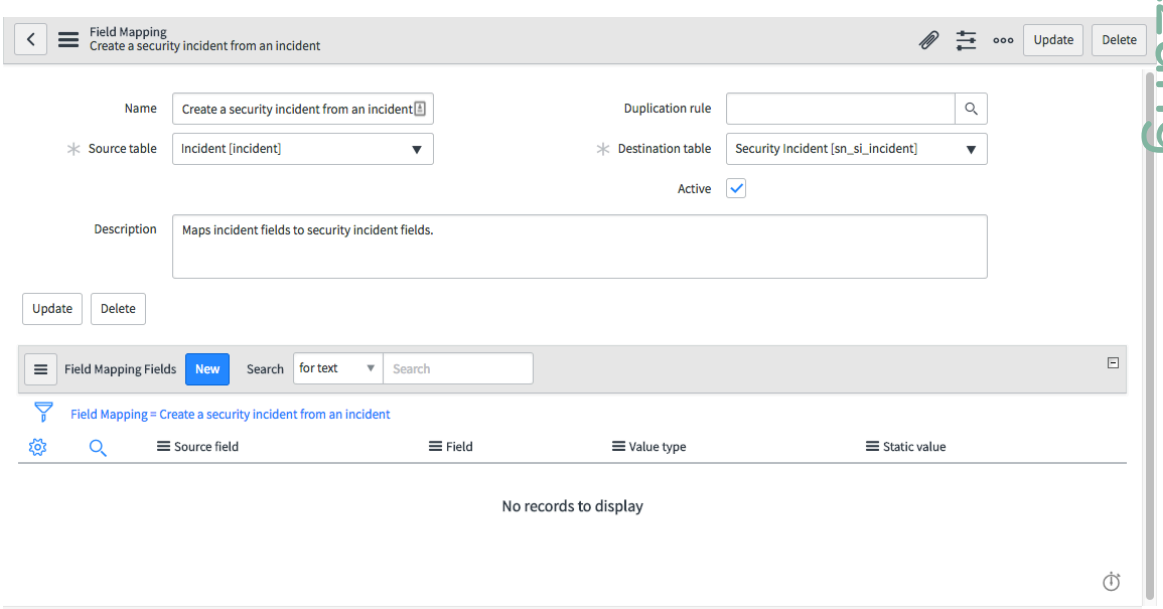
Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Feldzuordnung**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feldzuordnung

Feld	Beschreibung
Name	Der Name der Feldzuordnung.
Quelltabelle	Die Tabelle, die die Daten bereitstellt, die zum Erstellen eines Datensatzes in der Zieltabelle verwendet werden sollen.
Duplizierungsregel	Steuert, wie Quelldatensätze behandelt werden, die einen doppelten Datensatz generieren würden. Weitere Informationen finden Sie unter Transformation freigegebener Daten.
Zieltabelle	Die Tabelle, in der neue Datensätze erstellt werden.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Zuordnung zu aktivieren. **Hinweis:** Es kann jeweils nur eine Zuordnung zwischen Tabellen aktiv sein. Wenn zwei Karten dieselben Tabellen enthalten, wird die ältere Version automatisch deaktiviert.
Beschreibung	Beschreibung für die Feldzuordnung.

4. Wenn Sie Ihre Einträge abgeschlossen haben, klicken Sie mit der rechten Maustaste in den Formularheader, und wählen Sie aus **Speichern** .
Feldzuordnungsfelder Die Registerkarte wird angezeigt. Dieser Datensatz definiert, welche Daten im Zielfeld in Datensätzen platziert werden, die von dieser Feldtransformation erstellt wurden.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Neu**.
6. Füllen Sie die entsprechenden Felder im Formular aus.

Option	Bezeichnung
Feld	**Beschreibung**
Wert in einem Feld oder einer zugehörigen Liste speichern	Wählen Sie aus, wo der Wert gefunden werden soll. Zur Auswahl stehen: ○ Neuen Wert in einem Feld im Datensatz hinzufügen ○ Verknüpfung mit diesem Wert in einer zugehörigen Liste erstellen ○ Link zu diesem Wert, um einen Datensatz zu erstellen, wenn kein übereinstimmender Datensatz vorhanden ist **Hinweis:** Wenn die Zieltabelle keine zugehörigen Listen enthält, wird dieses Feld nicht angezeigt.
Feld	Wenn **Speichern Sie den Wert in einem Feld oder einer zugehörigen Liste** Ist auf festgelegt **Fügen Sie einem Feld im Datensatz einen neuen Wert hinzu** Dieses Feld gibt das auszufüllende Feld an. **Hinweis:** Für Auswahlfelder werden Übereinstimmungen mit vorhandenen Auswahlmöglichkeiten mithilfe der zugrunde liegenden Auswahlbezeichnung oder des zugrunde liegenden Werts getroffen. Wenn keine Übereinstimmung gefunden wird, wird das Feld festgelegt, der Auswahlliste wird jedoch kein neuer Eintrag hinzugefügt. Weitere Informationen finden Sie unter Auswahllisten . Für Referenzfelder wird ein Eintrag nur festgelegt, wenn ein Wert dem Anzeigenamen des Datensatzes entspricht oder gültig ist `sys_ID` Wurde gefunden. Weitere Informationen finden Sie unter Referenzfelder .
Zugehörige Liste	Wenn **Speichern Sie den Wert in einem Feld oder einer zugehörigen Liste** Ist auf festgelegt **Link zu diesem Wert in einer zugehörigen Liste** Oder **Link zu diesem Wert, um einen neuen Datensatz zu erstellen, wenn kein übereinstimmender Datensatz vorhanden**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	ist , Dieses Feld gibt die zugehörige Liste an, zu der Informationen hinzugefügt werden sollen.
Wertfeld	Wenn **Speichern Sie den Wert in einem Feld oder einer zugehörigen Liste** Ist auf festgelegt **Link zu diesem Wert in einer zugehörigen Liste** Oder **Link zu diesem Wert, um einen neuen Datensatz zu erstellen, wenn kein übereinstimmender Datensatz vorhanden ist** , Dieses Feld gibt das Feld in der Tabelle an, das in der zugehörigen Liste angezeigt wird, das zum Suchen und Suchen eines vorhandenen Datensatzes verwendet wird. Beispiel: Wenn Ihre zugehörige Liste lautet **Betroffene CIs** , Dieses Feld kann enthalten **Name** Oder **Vollqualifizierter Domänenname** , Oder ein anderes Feld im CI-Datensatz, das zum Suchen des CI verwendet werden soll, wird dem hinzugefügt **Betroffene CIs** Liste.
Beziehungsdaten	Wenn **Speichern Sie den Wert in einem Feld oder einer zugehörigen Liste** Ist auf festgelegt **Link zu diesem Wert in einer zugehörigen Liste** , Wird ein neuer Datensatz erstellt, um diesen Datensatz (z. B. einen Security Incident) mit dem Wert (CI, erkennbares Element usw.) zu verknüpfen. Dieses Feld gibt alle zusätzlichen Informationen (Feld- und Wertpaare) an, die diesem Verknüpfungsdatensatz hinzugefügt werden sollen. Wenn Sie beispielsweise ein erkennbares Element für eine Quell-IP hinzufügen, können Sie angeben, dass diese IP die Quell- und nicht die Ziel-IP ist. Verwenden Sie für mehrere Werte ein ^-Trennzeichen, z. B. TYPE= Quell-IP^Active=true.
Neue Datensatzdaten	**Wenn Wert in einem Feld oder einer zugehörigen Liste gespeichert wird** Ist auf festgelegt **Link zu diesem Wert, um einen neuen Datensatz zu erstellen, wenn kein übereinstimmender Datensatz vorhanden ist** Wenn kein zugehöriger Datensatz gefunden wird, der dem analysierten Wert entspricht, wird ein neuer Datensatz erstellt. Dieses Feld gibt die statischen Daten an, die diesem Datensatz hinzugefügt werden sollen. Beispiel: Für **Betroffene CIs** , Wenn wir das CI nicht finden können, gibt diese Einstellung an, dass ein neues CI erstellt wird.) Der im Quelldatensatz gefundene Wert wird auf festgelegt **Wert** Feld im CI-Datensatz. Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	können zusätzliche Daten festlegen – ein Hinweis, der angibt, warum dieses CI erstellt wurde, einige Informationen darüber, mit welcher Art von CIs Sie arbeiten. Ein Beispiel wäre: `Description=erstellt von Malware-Incident-Bericht^type=autoDetect`
Werttrennzeichen	Wenn **Speichern Sie den Wert in einem Feld oder einer zugehörigen Liste** Ist auf festgelegt **Link zu diesem Wert in einer zugehörigen Liste** Oder **Link zu diesem Wert, um einen neuen Datensatz zu erstellen, wenn kein übereinstimmender Datensatz vorhanden ist** , Dieses Feld gibt das Trennzeichen an, das für Listen von Elementen verwendet werden soll, normalerweise ein Komma oder Semikolon.
Werttyp	Wenn **Speichern Sie den Wert in einem Feld oder einer zugehörigen Liste** Ist auf festgelegt **Fügen Sie einem Feld im Datensatz einen neuen Wert hinzu** Dieses Feld gibt den Typ des Werts an. Zur Auswahl stehen: ○ **Quellfelddatensatz** ○ **Dem Feld als neue Zeile anfügen** ○ **Statischer Wert** ○ **Statischer Wert plus Quelldatensatz-Feldwert**
Quellenfeld	Wählen Sie das Quellfeld aus, das den Wert enthält, der im Zielfeld oder in der ausgewählten zugehörigen Liste platziert werden soll.
Statisches Feld	Statischer Wert für das Feld.
Wertumwandlung	Wählen Sie den anzuwendenden Feldwert-Transformationseintrag aus. Es wird verwendet, um Auswahlfelder zwischen Datensätzen zuzuordnen, z. B. um den Satz von zu konvertieren **Kategorie** Auswahlmöglichkeiten für einen Security Incident in die entsprechende **Typ** Feld für eine Change-Anforderung.
Zieltabelle	Wird automatisch mit der Zieltabelle ausgefüllt.
Feldzuordnung	Wird automatisch mit der übergeordneten Feldzuordnung ausgefüllt.
Quelltabelle	Wird automatisch mit der Quelltabelle ausgefüllt.

7. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations Feldwerttransformationen

Wandelt eindeutige Kundenfeldwerte in von erkannte Feldwerte um Security Operations E-Mail-Analyse, Datenanreicherung oder Tabellen mithilfe von Feldzuordnungen. Unterstützt Auswahlfelder und Referenzen und richtet externe Daten an der Standardterminologie und dem Standardformat für Ihren neuen Datensatz aus.

Sie können Daten für Felder wie Kategorie, Status oder Zuweisungsgruppe den Werten zuordnen, die in der Tabelle „Security Operations“ verwendet werden. Ordnen Sie beispielsweise „in Analyse“ zu „in Arbeit“ zu.

Erstellen Security Operations Feldwerttransformationen

Feldwerttransformationen Definiert eine Transformation zwischen bereitgestellten Quelldaten und dem zu verwendenden Ersatzwert.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.Basic oder sn_si.Basic

Warum und wann dieser Vorgang ausgeführt wird

Definieren Sie jeden Transformationseintrag, der angewendet werden soll, wenn eine Übereinstimmung mit dem Suchwert vorliegt, wenn der Suchwert in den bereitgestellten Quelldaten enthalten ist oder wenn keine Übereinstimmungen gefunden werden. Legen Sie einen Standardwert für fest, wenn keine Übereinstimmung gefunden wird. Wenn kein Standardwert festgelegt ist und keine Übereinstimmungen gefunden werden, werden die ursprünglichen Quelldaten verwendet.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Feldwertumwandlungen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feldwerttransformationen

Feld	Beschreibung
Name	Der Name der Feldwerttransformation.
Beschreibung	Beschreibung für die Feldzuordnung.
Feldwert-Umwandlungseinträge	Die Tabellenliste der Einträge. **a.** Unter **Ersetzen Sie Daten** , Doppelklicken Sie auf „neue Zeile einfügen“. **b.** Wählen Sie eine der folgenden Optionen: Wenn das Datum für dieses Feld übereinstimmt Wenn die Daten für dieses Feld Folgendes enthalten Wenn kein anderer Transform-Eintrag mit den Daten (Standard) übereinstimmt **c.** Klicken Sie auf das grüne Häkchen. **d.** Doppelklicken Sie unter **Suchwert** , Fügen Sie Ihren Suchwert hinzu. **e.** Klicken Sie auf das grüne Häkchen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	f. Doppelklicken Sie unter **Ersatzwert** Fügen Sie hinzu ServiceNow Entsprechender Wert. g. Wiederholen Sie dies bei Bedarf.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Transformation zu aktivieren.
Anwendung	Umfang der Anwendung.

4. Klicken Sie auf **Absenden**.

Security Operations Ergänzungsdatenzuordnung

ErgänzungsdatenzuordnungWandelt Daten aus XML, JSON oder um EigenschaftenDateien in ServiceNow Datensätze. Security Operations Workflows verwenden Ergänzungsdatenzuordnungen und stellen Ausgabedaten für Security Incidents bereit.

Security Operations Enthält mehrere Ergänzungsdatenzuordnungen, ausgelöst durch verschiedene Workflows, z. B. Security Operations-Integrationen – Flow „Netzwerkstatistiken abrufen“ Und Integration von Security Operations-Systembefehlen: Flow „laufende Prozesse abrufen“. Ausgabe der Ergänzungsdatenzuordnung von Security Operations Workflows werden in angezeigt **Ergänzungsdaten** Registerkarte im Security Incident-Formular.

Erstellen Sie einen Security Operations Ergänzungsdatenzuordnung

Transformieren Sie Daten aus JSON, XML oder EigenschaftenDateiformat bis ServiceNow Datensätze mit Ergänzungsdatenzuordnungen.

Vorbereitungen
Erforderliche Rolle: sn_sec_cmn.write

Warum und wann dieser Vorgang ausgeführt wird
Vorhandene Ergänzungsdatenzuordnungen werden von Workflows verwendet, die in bereitgestellt werden Security Operations. Sie können die Liste unter anzeigen **Ergänzungsdatenzuordnung** . Zur Verwendung einer Zuordnung benötigen Sie einen Auslöser, entweder eine Business-Regel oder einen Workflow.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Ergänzungsdatenzuordnung**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

Erstellen einer Ergänzungsdatenzuordnung

Feld	Beschreibung
Name	Name dieser Ergänzungsdatenzuordnung.
Eingabeformat	Wählen Sie ein Format aus der Liste aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	JSON (Standard) XML Dateiformat der Eigenschaften

Präfixschlüssel	Verwenden Sie , um den Eingabedatensatz auf einen angegebenen Schlüssel zu beschränken. Der Stamm des Eingabedatensatzes ist auf diesen Schlüssel festgelegt. Wenn Sie in diesem Beispiel file_info eingegeben haben, werden die Eingabewerte auf diese Werte in file_info beschränkt.
	`<?xml version="1.0" encoding="UTF-8"?>`
	`<malware>`
	`<version>2.0</version>`
	`<file_info>`
	`<malware>yes</malware>`
	`<sha1>24c051142583e10451a53893fed3aa5d80bfb1f6</sha1>`
	`<filetype>PE</filetype>`
	`<sha256>be9bd96808173e2d967feef8c8c5b8c4d73b621584fb11eb68434da1e6a0a930</sha256>`
	`<md5>ee8c91751b3010e38c479cf9ab09827a</md5>`
	`<size>546304</size>`
	`</file_info>`
	`</malware>`

Anwendung	Umfang der Anwendung.
Duplizierungsregel	Regel, die definiert, wann ein Datensatz als Duplikat betrachtet wird und welche Aktionen mit doppelten Datensätzen ausgeführt werden sollen.
Zieltabelle	Wählen Sie eine Tabelle aus der Liste aus.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Karte zu aktivieren.
Beschreibung	Geben Sie eine Beschreibung der Ergänzungsdatenzuordnung ein.

4. Klicken Sie auf **Absenden**.
   Die Registerkarte Ergänzungsdatenzuordnungsfelder wird angezeigt.
5. Klicken Sie auf **Neu**.
6. Füllen Sie die entsprechenden Felder im Formular aus.

Zuordnungsfelder für Ergänzungsdaten

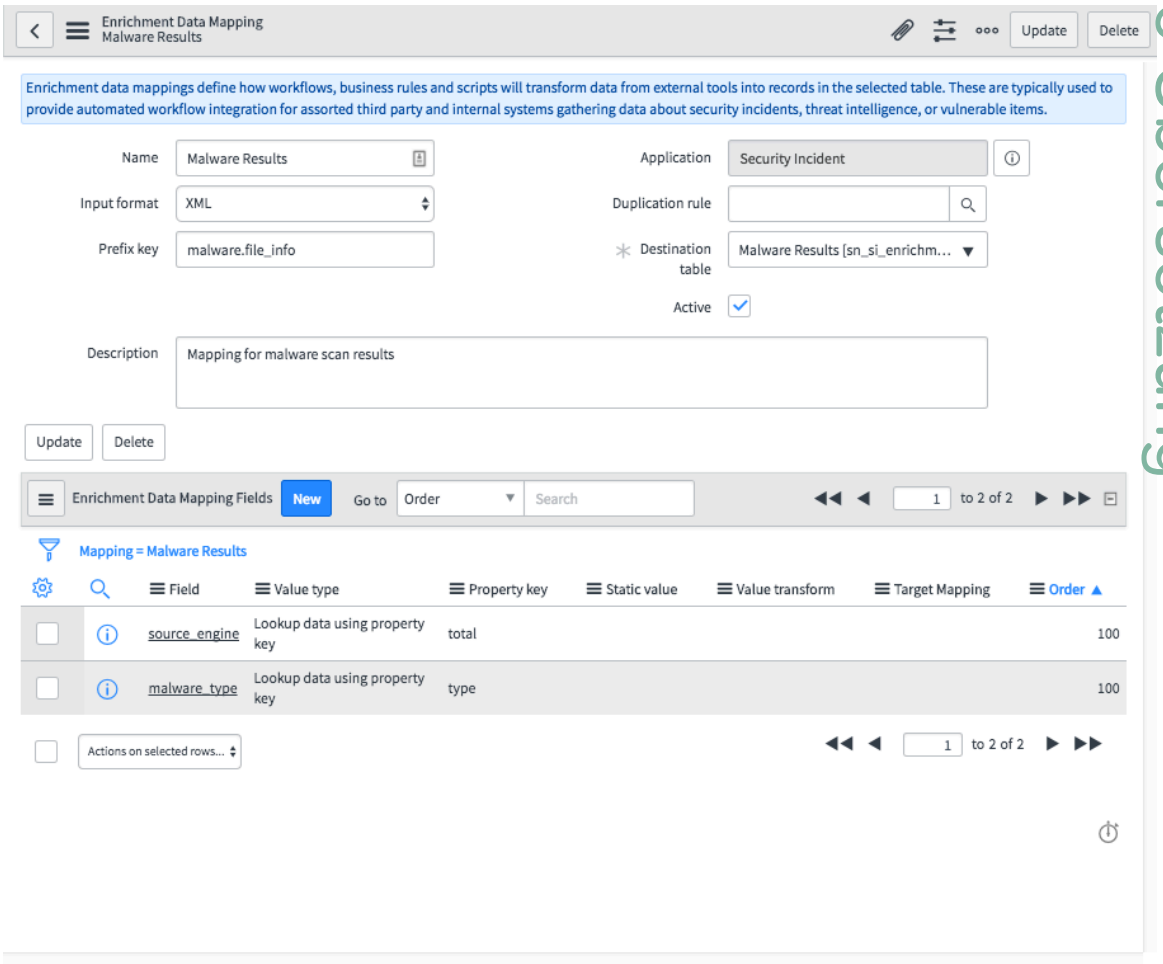
Feld	Beschreibung
Feld	Name der Ergänzungsdatenzuordnung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Werttyp	Wählen Sie aus der Liste: Suchdaten, die einen Eigenschaftsschlüssel verwenden Statischer Wert Statischer Wert plus Daten aus dem Eigenschaftsschlüssel Feld ist ein Array oder Objekt (Verschachtelung von Rohdaten) Jede Auswahl hat verschiedene Einträge. Feldwerte und Arrays oder Objekte erfordern einen Eigenschaftsschlüssel.
Eigenschaftsschlüssel	Bestimmt den Schlüssel für die Eingabedatensuche und den Wert, der in das Zielfeld geschrieben wird.
Wertumwandlung	Die Feldwerttransformation, die einen Wert einem anderen zuordnet.
Anwendung	Umfang der Anwendung.
Reihenfolge	In welcher Reihenfolge die Zuordnung berücksichtigt werden soll. Die erste Übereinstimmung wird verwendet. Der Standardwert ist 100.
Zuordnung	Name der Ergänzungsdatenzuordnung.
Zieltabelle	Die Tabelle, zu der die zuzuordnenden Felder gehören.

7. Klicken Sie auf **Absenden**.
Im Folgenden finden Sie ein Beispiel für eine Ergänzungsdatenzuordnung.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations Anwenderdefinierte Eskalation

Sie können einen Eskalationspfad für Security Incidents für Probleme erstellen, die mehr Aufmerksamkeit oder Fachwissen erfordern. Sobald eine Eskalationsgruppe vorhanden ist, wird bei jedem Security Incident in dieser Gruppe eine Schaltfläche angezeigt.

Erstellen Sie einen Security Operations Anwenderdefinierte Eskalationsgruppe

Eskalieren Sie einen Security Incident mithilfe von Eskalationen an eine beliebige Gruppe, die dem Incident zugeordnet ist.

Vorbereitungen

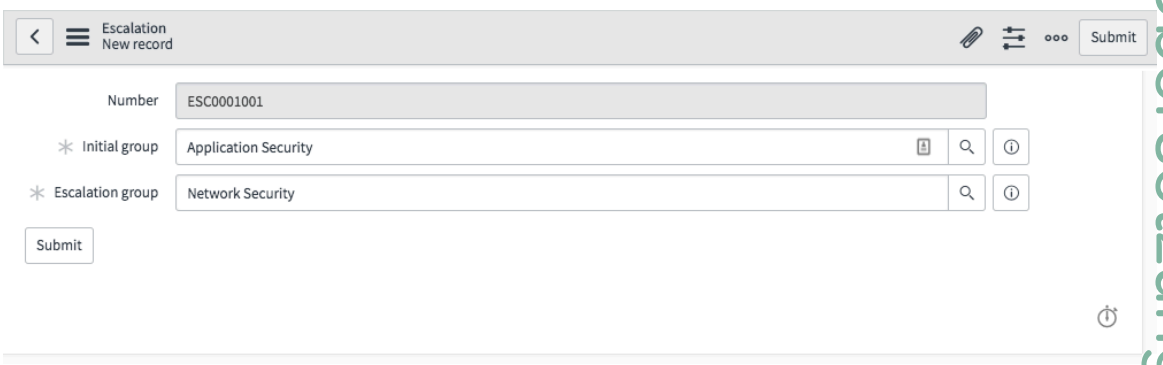
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Gruppen** > **Eskalationen**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Eskalationen

Feld	Beschreibung
Anzahl	Nummer des Eskalations-Incidents (Feld wird automatisch generiert).
Ursprungsgruppe	Wählen Sie die Gruppe aus, zu der dieser Security Incident gehört.
Eskalationsgruppe	Wählen Sie die Gruppe aus, an die der Security Incident eskaliert werden soll.

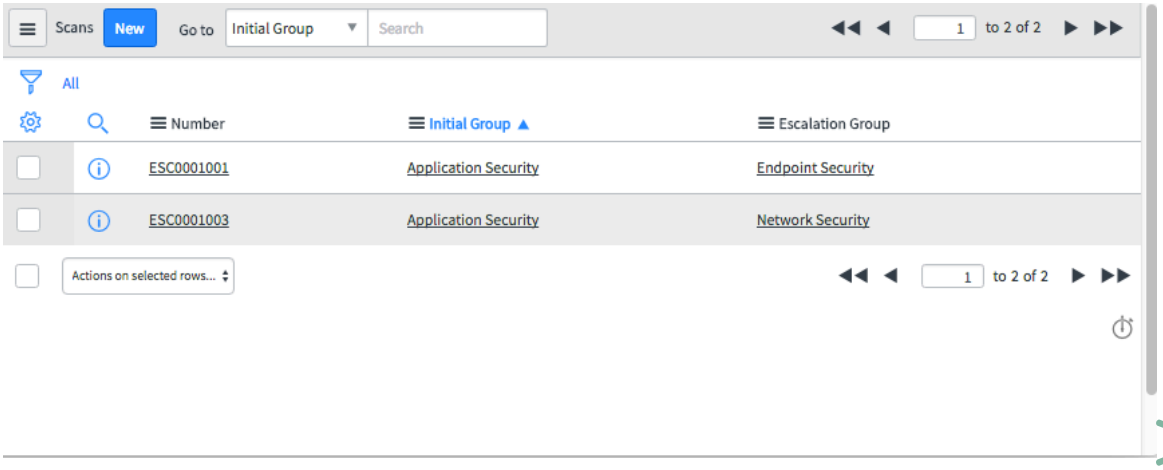


4. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Eskalationsgruppe ist für alle Security Incidents in der ursprünglichen Gruppe verfügbar. Sie können mehrere Gruppen erstellen.



Erstellen Sie domänengetrennte Eigenschaftsüberschreibungen

Wenn Sie Domänentrennung verwenden, können Sie Überschreibungen für vorhandene Security Operations-Eigenschaften erstellen, mit denen Sie die Funktionen der Anwendungen in jeder Ihrer Domänen anpassen können.

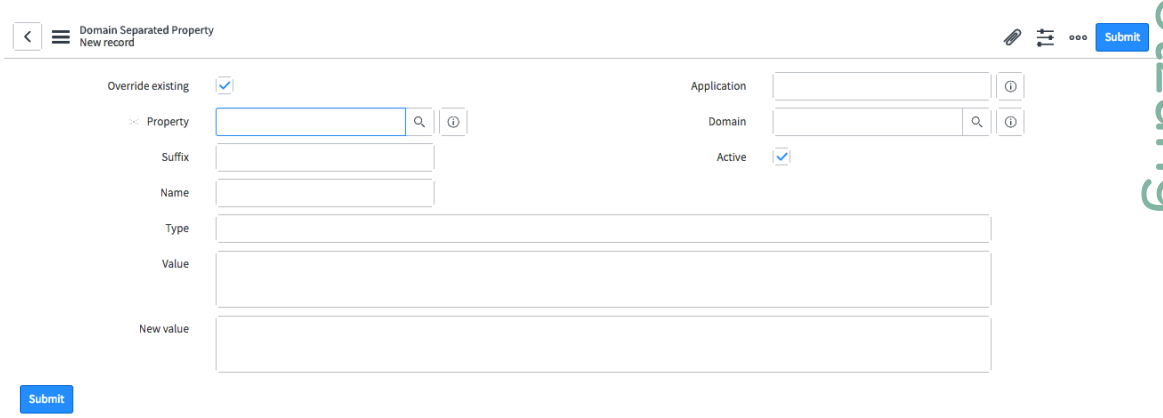
Vorbereitungen

Erfordert das Domänensupport: Domänenerweiterungen Aktiviert sein. Sie können auch mehr über erfahren Viewer Für Domänenüberschreibung .

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Nach Domäne getrennte Eigenschaften**an.
2. Klicken Sie auf **Neu**.



3. Füllen Sie im Formular die Felder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Domänentrennungseigenschaft“

Feld	Beschreibung
Vorhandene überschreiben	Aktivieren Sie dieses Kontrollkästchen, um einen domänenspezifischen Wert für eine vorhandene Eigenschaft zu erstellen.
Anwendung	Wählen Sie die Anwendung aus, die die Eigenschaft enthält, die Sie überschreiben möchten.
Eigenschaft	Wählen Sie die Eigenschaft für die ausgewählte Anwendung aus, für die Sie eine domänenspezifische Überschreibung erstellen möchten.
Domäne	Wählen Sie die Domäne aus, für die Sie diese Eigenschaftsüberschreibung erstellen.
Aktiv	Aktivieren oder deaktivieren Sie die Überschreibung.
Suffix	Zeigt das Eigenschaftssuffix an.
Name	Zeigt den Eigenschaftsnamen an.
Typ	Zeigt den Eigenschaftstyp an.
Wert	Zeigt den aktuellen Wert für die Eigenschaft an.
Neuer Wert	Geben Sie einen neuen Wert für die Eigenschaft ein, die auf diese Domäne angewendet werden soll.

4. Klicken Sie auf **Absenden**.
   Die Eigenschaftsüberschreibung wird auf die ausgewählte Eigenschaft in der angegebenen Domäne angewendet. Wenn die Logik für diese Eigenschaft ausgelöst wird, überprüft das System auf Überschreibungen durch Domänen getrennter Eigenschaften. Wenn eine Überschreibung für die Domäne gefunden wird, wird der neue Wert verwendet. Andernfalls wird der Wert für die Standarddomäne verwendet.

Zugehörige Informationen

Domänentrennung verstehen

Erstellen Sie eine Betriebssystemgruppe

Betriebssystemgruppen werden verwendet, um ein Betriebssystem bestimmten Prozesstypen und Skripts in zuzuordnen Security Incident Response Workflows. Die Skripts definieren, wie laufende Prozesse für die definierten Betriebssystemgruppen abgerufen werden. Neue Betriebssysteme können nach Bedarf hinzugefügt werden.

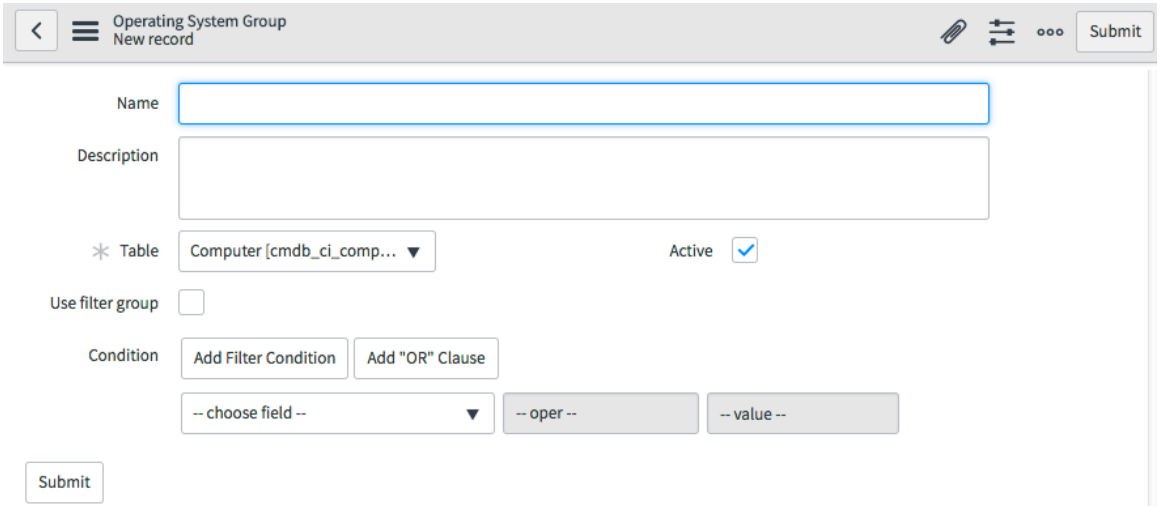
Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Betriebssystemgruppen**an.
   Das Basissystem enthält Skripts für drei Betriebssysteme:
   - BSD-basiertes Betriebssystem
   - POSIX-basiertes Betriebssystem
   - Betriebssystem Windows
2. Klicken Sie auf **Neu**.

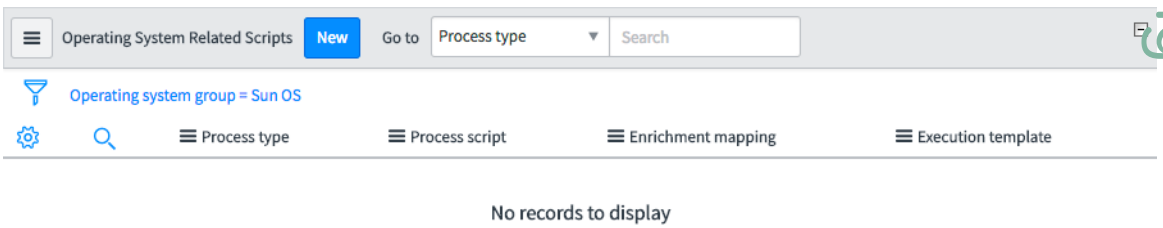
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Füllen Sie die Felder nach Bedarf aus.

Feld	Beschreibung
Name	Der Name der Betriebssystemgruppe.
Beschreibung	Eine Beschreibung für die Betriebssystemgruppe.
Tabelle	Die betroffene Tabelle.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Betriebssystemgruppe zu aktivieren.
Filtergruppe verwenden	Aktivieren Sie dieses Kontrollkästchen, um eine Filtergruppe zum Suchen übereinstimmender Datensätze in der ausgewählten Tabelle zu verwenden.
Filtergruppe	Wählen Sie die Filtergruppe für die Suche nach übereinstimmenden Datensätzen in der ausgewählten Tabelle aus. Dieses Feld wird nur angezeigt, wenn Sie ausgewählt haben **Verwenden Sie die Filtergruppe** Kontrollkästchen.
Bedingung	Die zugehörigen Listen namens Bedingungsgenerator Felder werden nur angezeigt, wenn Sie nicht ausgewählt haben **Verwenden Sie die Filtergruppe** Kontrollkästchen.

4. Klicken Sie mit der rechten Maustaste in die Formularkopfzeile, und wählen Sie **Speichern** aus.
Die zugehörige Liste „Betriebssystembezogene Skripts“ wird geöffnet.



5. Klicken Sie auf **Neu**.
6. Wählen Sie Skripts aus, die den Workflows entsprechen, die Sie verwenden, um laufende Prozesse, Services und/oder Netzwerkstatistiken abzurufen.
7. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Hängen Sie eine Skriptdatei an einen synchronisierten MID-Server an

Richten Sie Sicherheits-Tag-Gruppen und -Tags ein

Sie können Security Incidents, Antwortaufgaben, angreifbaren Elementen, erkennbaren Elementen, IoCs, Tags zuweisen. und Sicherheitsfälle, um Metadaten im Antwortdatensatz zu erstellen und zu definieren, wer Zugriff auf bestimmte Arten von Sicherheitsinhalten haben soll. Die Tags können Sicherheitsgruppen hinzugefügt werden, um sie zu organisieren.

Vorbereitungen

Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Sicherheits-Tags** > **Gruppen**an.
   Drei Standardklassifizierungsgruppen sind im Basissystem enthalten.
   - **Liste der Ergänzungsberechtigungen/Ablehnungen** : Diese Gruppe definiert, ob ein Datensatz als Allow-Listen- oder Deny-Listendatensatz behandelt werden soll. Allow-Listendatensätze haben im Allgemeinen weniger Bedeutung, daher können sie ignoriert werden. Datensätze der Deny-Liste sind im Allgemeinen von höherem Interesse.
   - **Metatag** : Diese Gruppe wird als Demodaten bereitgestellt. Sie können damit anwenderdefinierte Klassifizierungs-Tags erstellen, die von Security Operations-Anwendungen verwendet werden.
   - **Ampelprotokoll** : Diese Gruppe wird verwendet, um sicherzustellen, dass vertrauliche Informationen an die richtige Zielgruppe weitergegeben werden. Es werden vier Farben (weiß, Grün, Gelb und Rot) verwendet, um verschiedene Empfindlichkeitsgrade anzuzeigen. Für jede Farbe können Sie die entsprechenden Lese-/Schreibzugriffsrollen zuweisen. Wenn erkennbare Elemente für einen vertrauenswürdigen Sicherheitskreis freigegeben werden, bestimmt das dem vertrauenswürdigen Sicherheitskreisprofil zugewiesene Tag, welche erkennbaren Elemente mit TLP-Tags für den Kreis freigegeben werden können, wie folgt:
     - **TLP: WEISS:** Nur erkennbare Elemente mit TLP: WEISS können für ein TLP: WHITE-Profil freigegeben werden.
     - **TLP: GRÜN:** Erkennbare Elemente mit TLP: GRÜN und TLP: WEISS können für ein TLP: GRÜNES Profil freigegeben werden.
     - **TLP: GELB:** Erkennbare Elemente mit TLP: GELB, TLP: GRÜN und TLP: WEISS können für ein TLP: GELB-Profil freigegeben werden.
     - **TLP: ROT:** Alle erkennbaren Elemente können unabhängig von ihrem TLP-Tag für ein TLP: RED-Profil freigegeben werden, da TLP: ROT das TLP-Tag mit dem höchsten Rang ist.

   Hinweis:
   Sie können andere TLP-Farben hinzufügen, aber zusätzlich zu den vier enthaltenen Farben werden vom Forum für Incident Response- und Sicherheitsteams (ZUERST).

2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie den Namen der Sicherheitsgruppe ein.
Mehrfachauswahl zulassen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie einem Datensatz, der eine Gruppe teilt, mehrere Sicherheits-Tags zuweisen möchten.
Aktiv	Aktivieren oder deaktivieren Sie die Gruppe.
Beschreibung	Geben Sie eine Beschreibung dieser Gruppe ein.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die zugehörige Liste Sicherheits-Tags wird angezeigt.
5. Klicken Sie in der zugehörigen Liste Sicherheits-Tags auf **Neu** .
6. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name des Klassifizierungs-Tags.
Sicherheits-Tag-Gruppe	Ob das Tag mit erstellt wurde **Neu** Schaltfläche in der zugehörigen Gruppenliste. Dieses Feld ist standardmäßig auf die aktuelle Gruppe festgelegt. Bei Bedarf können Sie das Tag einer anderen Gruppe hinzufügen. Dies ist jedoch optional.
Reihenfolge	Geben Sie die Reihenfolge an, in der das Tag in Formularen oder in einer Liste angezeigt wird.
Farbe	Wählen Sie die Farbe für dieses Tag aus.
Eingeschränkten Zugriff erzwingen	Aktivieren Sie dieses Kontrollkästchen, um Lese- und/oder Schreibrollen zuzuweisen, die Anwender zum Lesen oder Schreiben in Datensätzen benötigen, die dieses Sicherheits-Tag haben.
Aktiv	Aktivieren oder deaktivieren Sie das Tag.
Beschreibung	Eine Beschreibung dieses Tags.
Rollen (Lesezugriff)	Um einem Sicherheits-Tag Lesezugriff zuzuweisen, klicken Sie auf das Schlosssymbol, wählen Sie die entsprechenden Zugriffsrollen aus, und klicken Sie erneut auf das Schlosssymbol. Dieses Feld wird nur angezeigt, wenn Sie ausgewählt haben **Eingeschränkten Zugriff erzwingen** Kontrollkästchen.
Rollen (Schreibzugriff)	Um einem Sicherheits-Tag Schreibzugriff zuzuweisen, klicken Sie auf das Schlosssymbol, wählen Sie die entsprechenden Zugriffsrollen aus, und klicken Sie erneut auf das Schlosssymbol. Dieses Feld wird nur angezeigt, wenn Sie ausgewählt haben **Eingeschränkten Zugriff erzwingen** Kontrollkästchen.

7. Wiederholen Sie den Vorgang nach Bedarf, um weitere Sicherheits-Tags zu erstellen.
8. Klicken Sie auf **Aktualisieren**.

Hinweis:
Sie können auch neue Tags erstellen, indem Sie zu navigieren **Security Operations** > **Sicherheits-Tags** > **Tags**an. Das Verfahren ist identisch.

Erstellen Sie Sicherheits-Tag-Regeln

Sicherheits-Tag-Regeln bieten Filterung für den Zugriff auf Sicherheits-Tag.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Sicherheits-Tags** > **Tags**an.
2. Wählen Sie oder aus Erstellen Sie ein Sicherheits-Tag .
3. In **Sicherheits-Tag-Regeln** Zugehörige Registerkarte klicken Sie auf **Neu** .
4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name der Sicherheits-Tag-Regel.
Sicherheits-Tag	Das Sicherheits-Tag, das an die Regel angehängt werden soll.
Aktiv	Aktivieren oder deaktivieren Sie das Sicherheits-Tag.
Beschreibung	Eine Beschreibung dieser Regel.

5. Bestimmen **Datensatzfilterung.**
6. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Filtergruppe verwenden	Ordnet der Regel eine Filtergruppe zu.
Tabelle	Die Tabelle, die die Regel enthalten soll.
Bedingung	Fügen Sie eine oder mehrere Filterbedingungen hinzu.

7. Klicken Sie auf **Absenden**.

Sicherheits-Tag-Regeln importieren

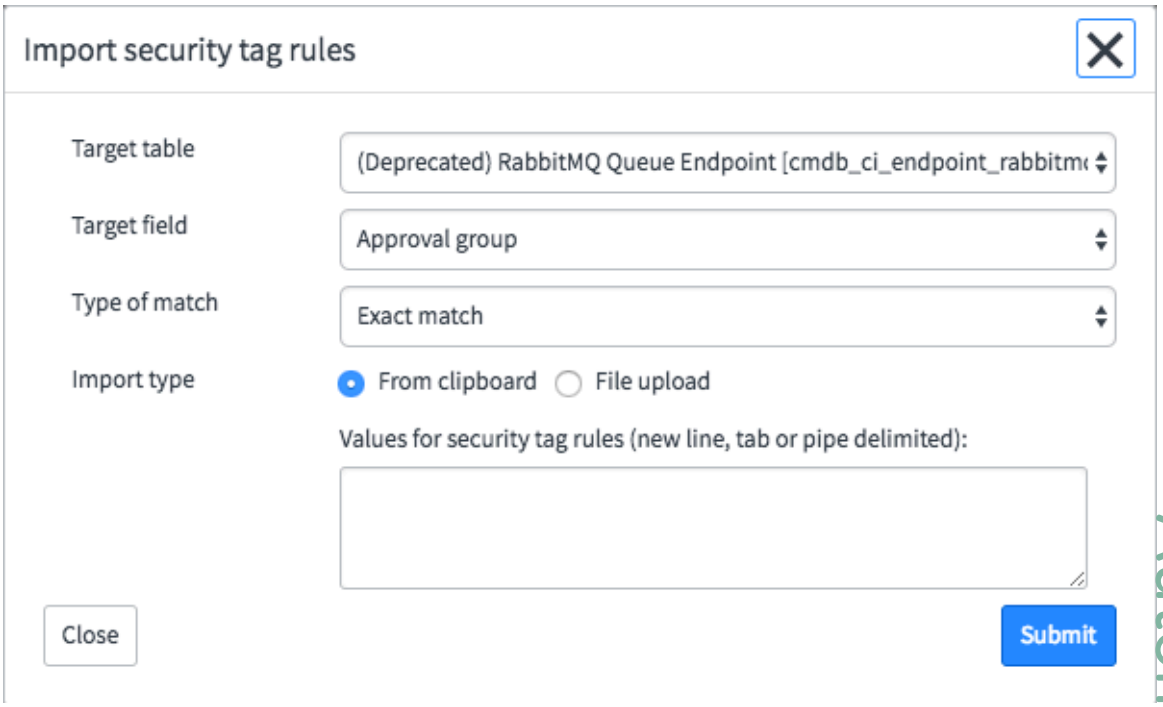
Sie können Sicherheits-Tag-Regeln aus anderen Tabellen in Ihrer Bereitstellung importieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Sicherheits-Tags** > **Tags**an.
2. Wählen Sie oder aus Erstellen Sie ein Sicherheits-Tag .
3. Klicken Sie auf **Importieren Sie Sicherheits-Tag-Regeln** Zugehöriger Link.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Zieltabelle	Wählen Sie die Tabelle aus, die zum Importieren von Regeln verwendet werden soll.
Zielfeld	Wählen Sie das Feld aus, das zum Importieren von Regeln verwendet werden soll.
Typ der Übereinstimmung	Wählen Sie aus, wie die importierten Regeln zugeordnet werden sollen **Sicherheits-Tags** Von: Genaue Übereinstimmung (Standard) Enthält Beginnt mit Endet mit Regulärer Ausdruck
Importtyp	Wählen Sie: **Aus Zwischenablage** Kopieren Sie eine Liste von getrennten Werten in den Textbereich. Die Werte werden in Sicherheits-Tags analysiert. **Aus Datei-Upload** Laden Sie eine Datei mit getrennten Werten hoch. Die Werte werden in Sicherheits-Tags analysiert. Fügen Sie Werte für die Sicherheits-Tag-Regeln mit neuen Linien- oder Pipe-Trennzeichen hinzu.

5. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsanmerkungen

Eine Sicherheitsanmerkung ist eine Erklärung oder ein Kommentar, die einem Konfigurationselement oder erkennbarem Element hinzugefügt oder für einen Security Incident verwendet wird.

Mehrere Sicherheitsanmerkungen sind für Anwender und erkennbare Elemente verfügbar (erfordert Threat Intelligence Plugin). Berichte zu Sicherheitsanmerkungen sind ebenfalls verfügbar.

Erstellen Sie Sicherheitsanmerkungen für CIs

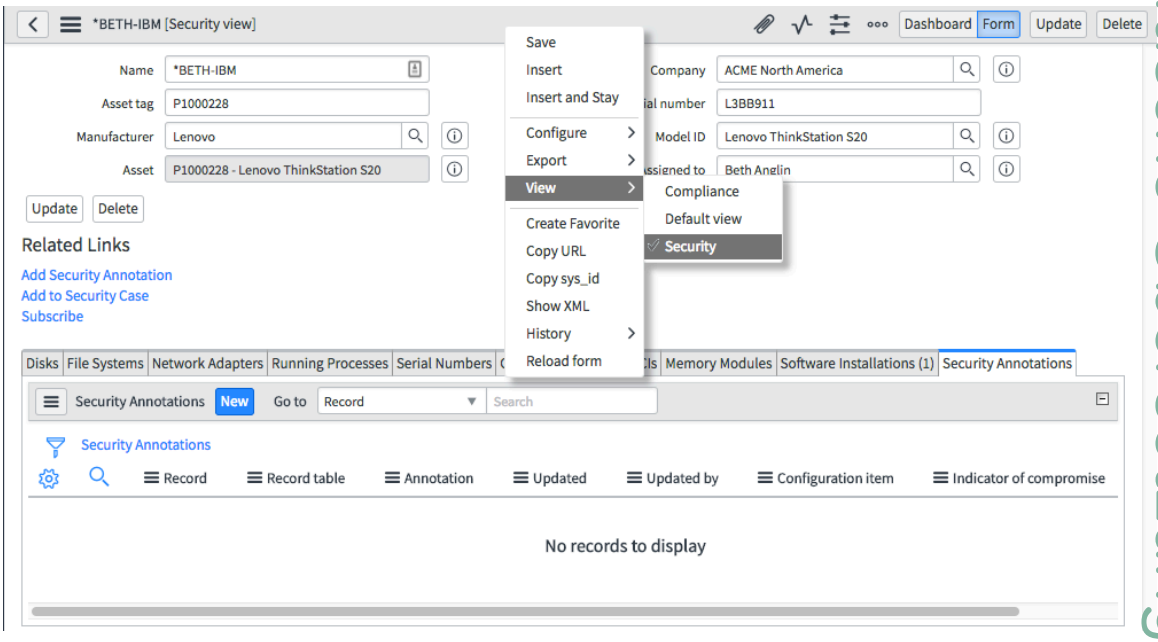
Mit Anmerkungen zu CIs können Sie Aktivitäten über Incidents hinweg nachverfolgen. Sie können einem oder mehreren CIs Anmerkungen hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie in einem Security Incident oder in der Konfigurationselementtabelle ein CI.
2. Klicken Sie mit der rechten Maustaste in den Header, und wählen Sie aus **Ansicht** > **Sicherheit**an.



3. In **Sicherheitsanmerkungen** Registerkarte „zugehörige Liste“ klicken Sie auf **Neu** .
4. Geben Sie eine Anmerkung ein.
   Anmerkungen können in einem beliebigen Textformat vorliegen.
5. Klicken Sie auf **Absenden**.

Hinweis:
Sie können mehrere CIs dieselbe Anmerkung hinzufügen, indem Sie CIs in der Liste auswählen und wählen **Fügen Sie eine Sicherheitsanmerkung hinzu** Geben Sie eine Anmerkung in einem beliebigen Textformat ein, und klicken Sie auf **Übermitteln** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie Sicherheitsanmerkungen für erkennbare Elemente

Sie können ein oder mehrere erkennbare Elemente auswählen und mit Sicherheitsanmerkungen darauf anwenden **Aktionen für ausgewählte Zeilen** Auswahlmenü.

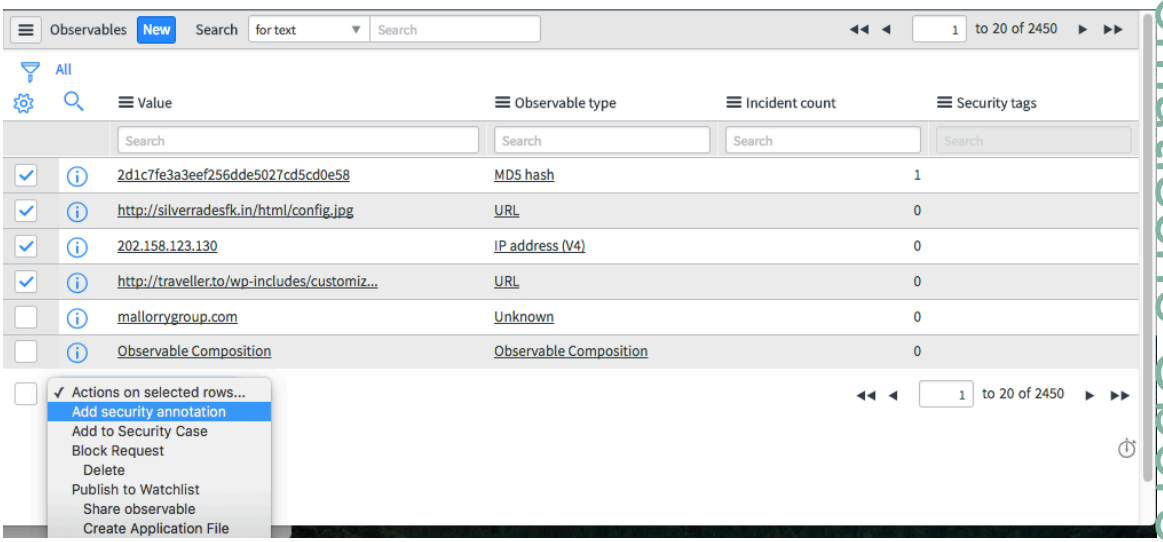
Vorbereitungen

- Erfordert Threat Intelligence Plugin und Aktivierung. Das Threat Intelligence-Plugin ist als separates Abonnement verfügbar.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Threat Intelligence** > **Erkennbare Elemente**
2. Wählen Sie ein oder mehrere erkennbare Elemente in der Liste aus.
3. Von **Aktionen für ausgewählte Zeilen** Dropdown-Menü auswählen **Fügen Sie eine Sicherheitsanmerkung hinzu** .



4. Geben Sie eine Anmerkung ein.
   Anmerkungen können in einem beliebigen Textformat vorliegen.
5. Klicken Sie auf **Absenden**.

Erstellen Sie Sicherheitsanmerkungen für Anwender

Sie können einen einzelnen oder mehrere Anwender auswählen und mit Sicherheitsanmerkungen darauf anwenden **Aktionen für ausgewählte Zeilen** Auswahlmenü.

Vorbereitungen

Erfordert Threat Intelligence Plugin und Aktivierung. Das Threat Intelligence-Plugin ist als separates Abonnement verfügbar.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Anwenderadministration** > **Anwender**
2. Wählen Sie einen oder mehrere Anwender in der Liste aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Von **Aktionen für ausgewählte Zeilen** Dropdown-Menü auswählen **Fügen Sie eine Sicherheitsanmerkung hinzu** .
4. Geben Sie eine Anmerkung ein.
   Anmerkungen können in einem beliebigen Textformat vorliegen.
5. Klicken Sie auf **Absenden**.

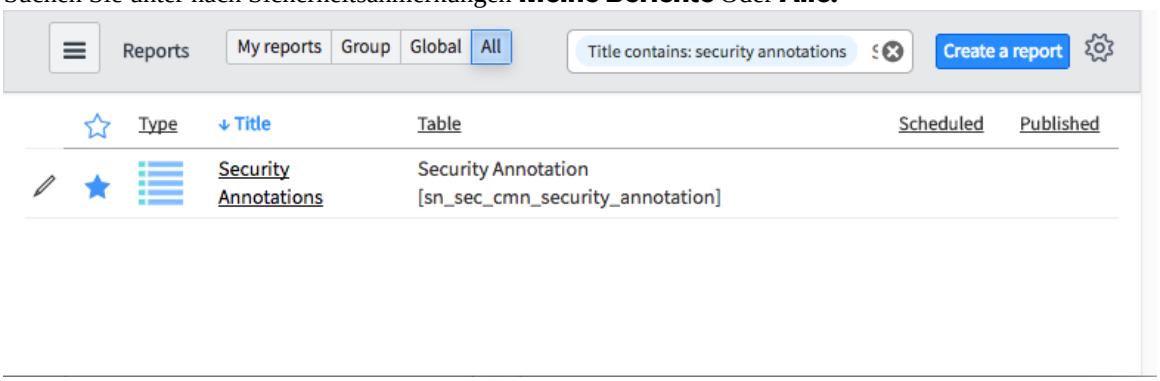
Zeigen Sie Berichte zu Sicherheitsanmerkungen an

Der Bericht „Sicherheitsanmerkungen“ enthält Details, die in der Tabelle „Sicherheitsanmerkungen“ [sn_sec_cmn_Security_annotations] gespeichert sind. Sie können die Spalten im Bericht anpassen und die Daten nach Ihren Wünschen gruppieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Berichte** > **Anzeigen/Ausführen**an.
2. Suchen Sie unter nach Sicherheitsanmerkungen **Meine Berichte** Oder **Alle.**



Zugehörige Informationen

Liste „Berichte“ anzeigen

Mit Security Support Common installierte Komponenten

Mit Security Support Common werden verschiedene Arten von Komponenten installiert. Sie bieten allgemeine Funktionen für die Verwendung in den verschiedenen Sicherheitsanwendungen, z. B. Security Incident Response.

Installierte Komponenten werden gesucht und angezeigt

Siehe Zeigen Sie mit installierte Komponenten an Security Support Common Weitere Informationen zum Suchen und Anzeigen installierter Komponenten.

Zeigen Sie mit installierte Komponenten an Security Support Common

Beim Aktivieren von werden verschiedene Arten von Komponenten installiert Security Support Common Plugin, einschließlich, aber nicht beschränkt auf Tabellen, Anwenderrollen und Module.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten werden gesucht

Hinweis:
In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Wenn Sie die Liste der installierten Komponenten auf Rollen, geplante Aufgaben und Tabellen für die Anwendung „Security Support Common“ beschränken möchten, führen Sie die folgenden Schritte aus:

Zeigen Sie gefilterte Listen für Komponenten an, die mit einer Anwendung installiert wurden

Filtern Sie die Tabelle „Anwendungsdateien“ so, dass nur die Rollen, geplanten Aufgaben und Tabellen angezeigt werden, die mit einer Anwendung installiert werden. Die Anwendung, für die Sie diese Komponenten anzeigen möchten, sollte installiert werden, damit ihre Dateien in die Instanz und in die Metadatentabelle geladen werden. Führen Sie die folgenden Schritte aus, um gefilterte Listen aus der Tabelle „Anwendungsdateien“ anzuzeigen.

1. Geben Sie im Filternavigator ein **sys_metadata.list** Um zur Metadatentabelle zu navigieren.
2. Wählen Sie den Bedingungsgenerator (Filtersymbol) aus, und wählen Sie, **Anwendung** > **ist** Gefolgt vom Namen Ihrer Anwendung.
3. Klicken Sie im Bedingungsgenerator auf, um einen zweiten Filter hinzuzufügen **UND** , Und wählen Sie dann aus, **Klasse** > **ist ein** Und wählen Sie eine der folgenden Klassen aus der Liste aus: **Rolle** , **Geplante Aufgabe** , Oder **Tabelle** .
4. Wählen Sie **Ausführen**.

Die Ergebnisse für die von Ihnen ausgewählte Klasse werden in einer gefilterten Liste angezeigt.

[store-future: BEGIN review]

Modulzugriff nach Rolle für Security Operations-Anwendungen

Für jede Anwendung finden Sie die Menüelemente, auf die eine bestimmte Rolle zugreifen kann.

[End]
[store-future: BEGIN review]

Modulzugriff nach Rolle für Konfigurations-Compliance

Informationen zur Konfigurations-Compliance finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

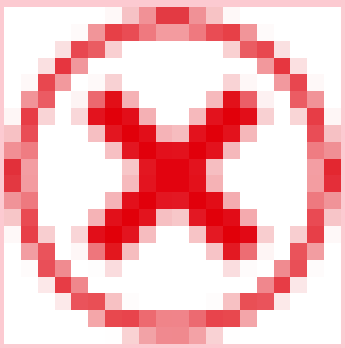
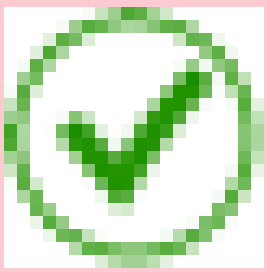
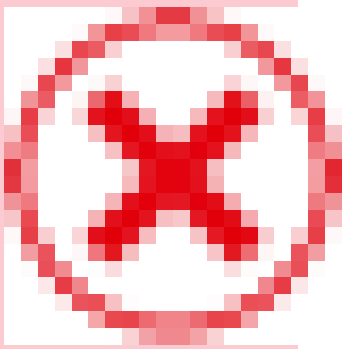
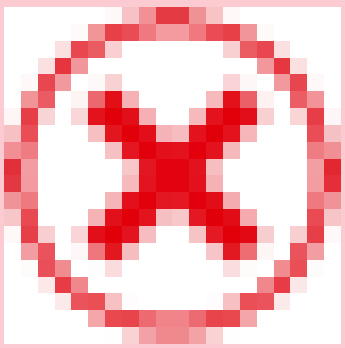
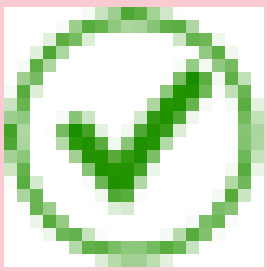
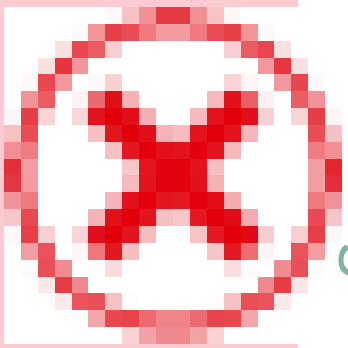
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
(Haupt-App-Gruppe)				
Übersicht				
Richtlinien				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

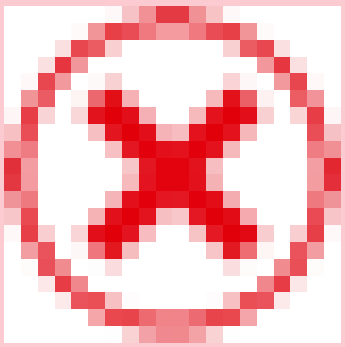
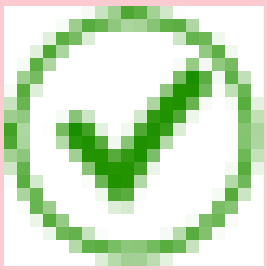
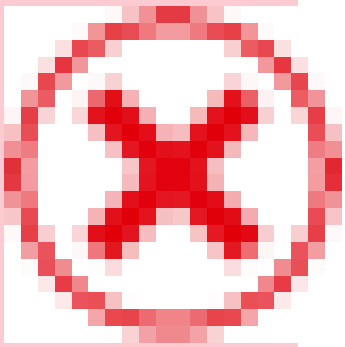
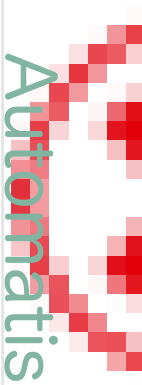
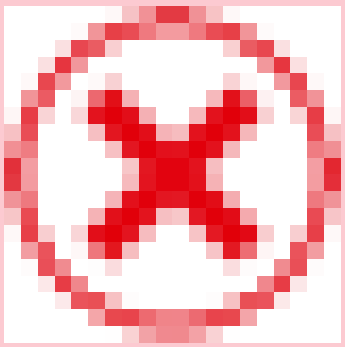
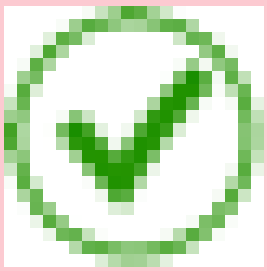
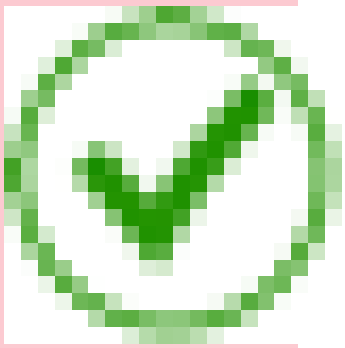
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Tests				
Meine Genehmigungen				
Testergebnisse				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

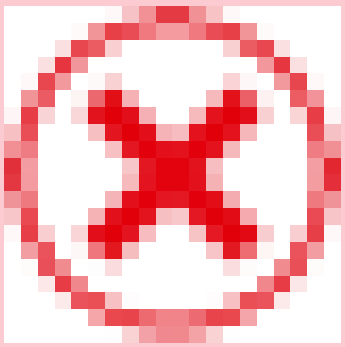
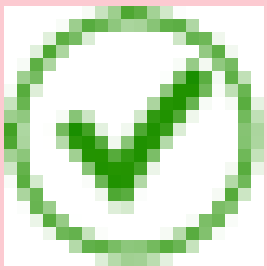
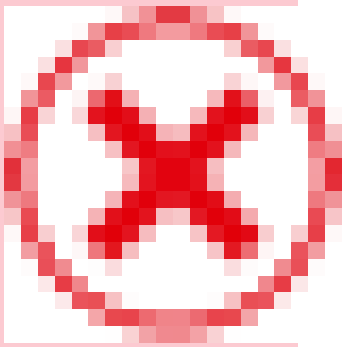
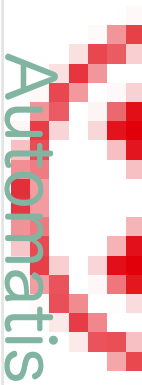
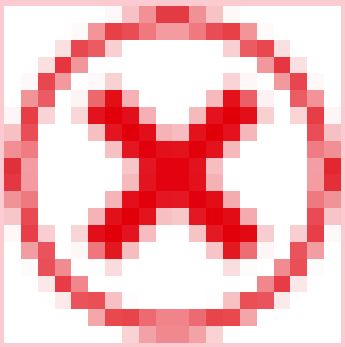
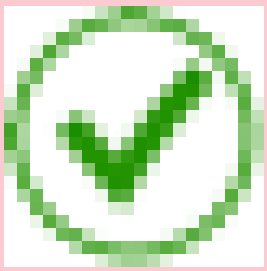
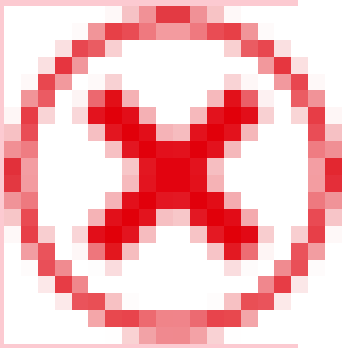
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Nicht selektierte Testergebnisse				
Meine offenen Testergebnisse				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

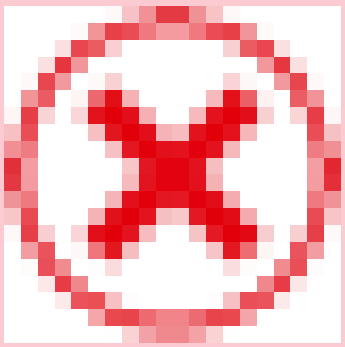
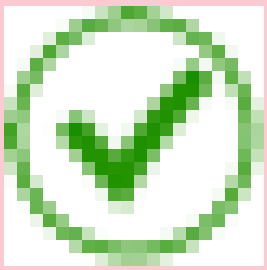
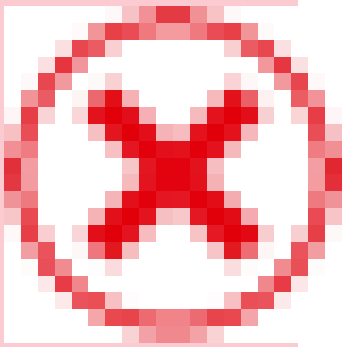
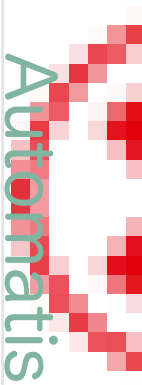
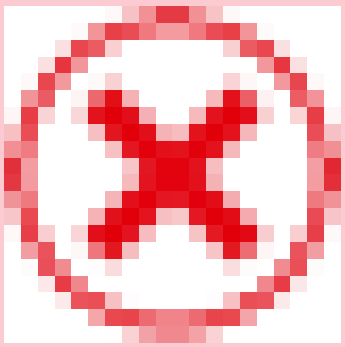
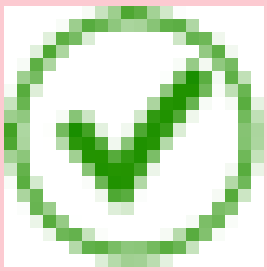
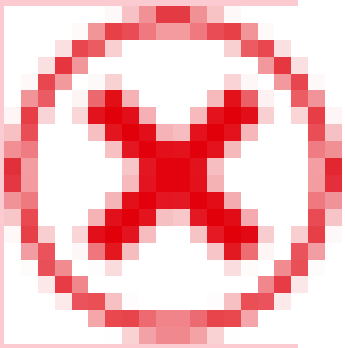
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Offene Testergebnisse				
Ziel rückt näher				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

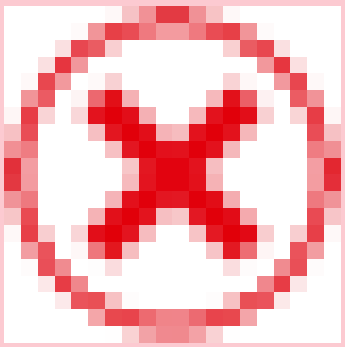
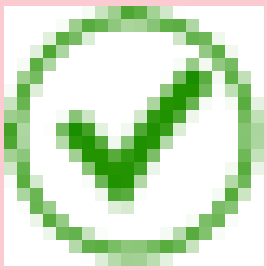
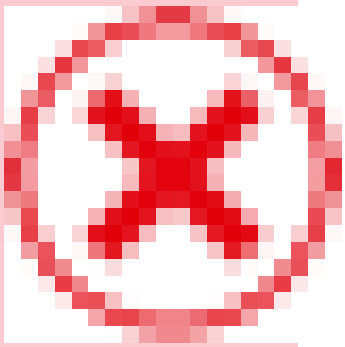
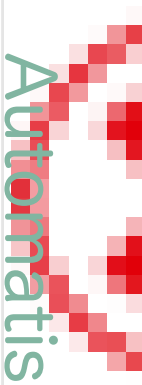
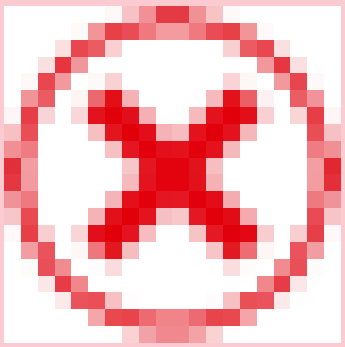
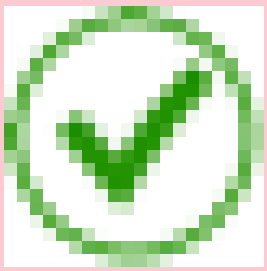
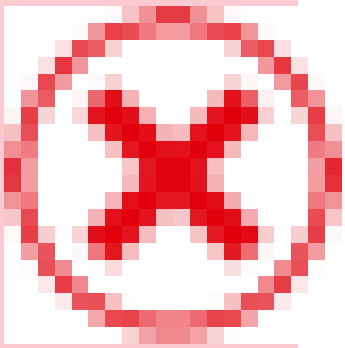
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Verfehltes Ziel				
Nicht zugewiesen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

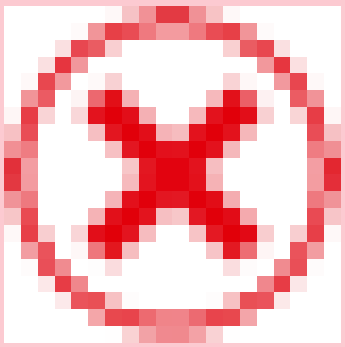
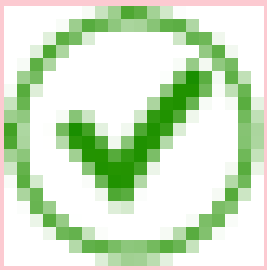
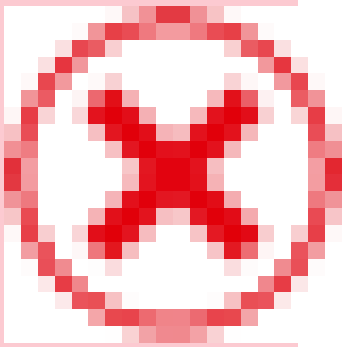
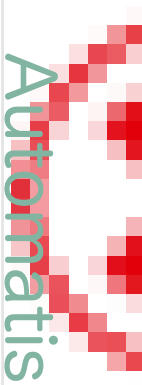
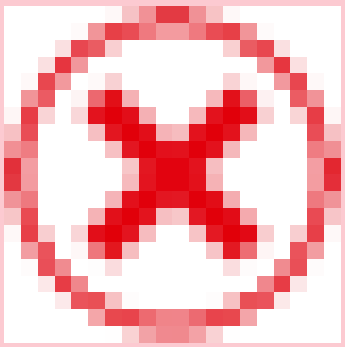
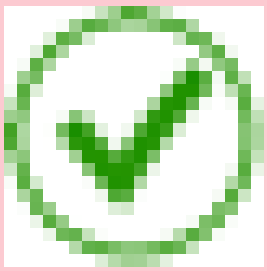
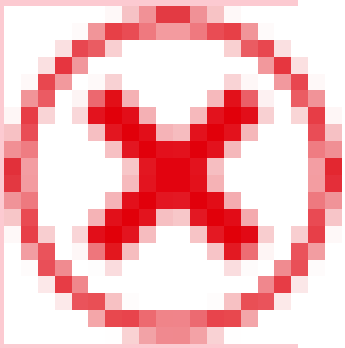
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Mehrere Zurückstellungen				
Alle				
Testergebnisgruppen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

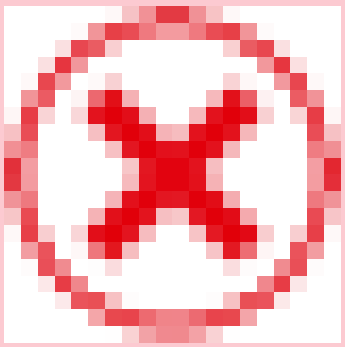
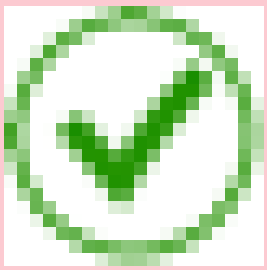
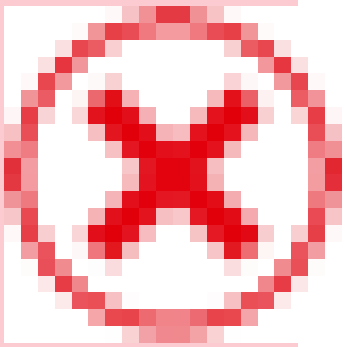
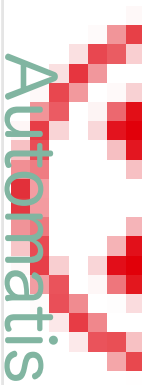
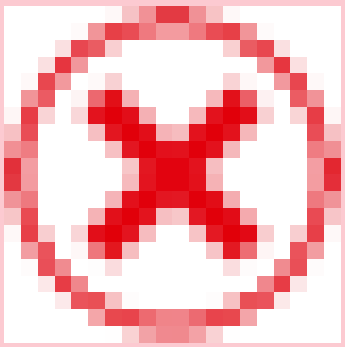
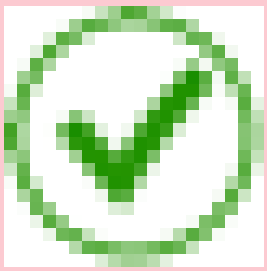
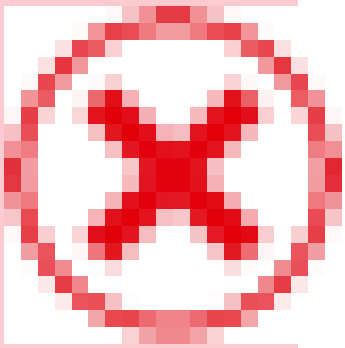
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Meine Offenen Gruppen				
Alle Offenen Gruppen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

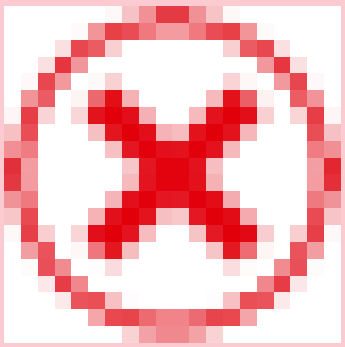
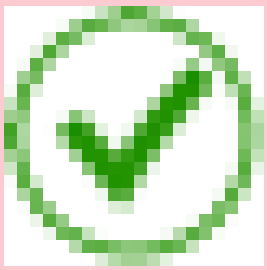
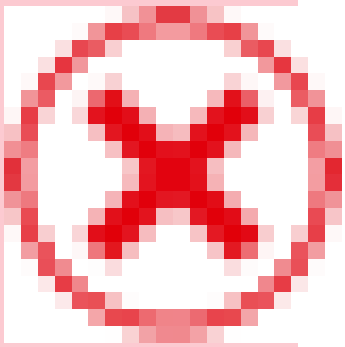
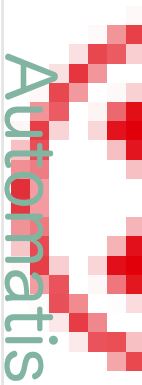
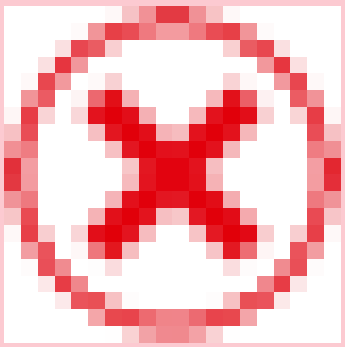
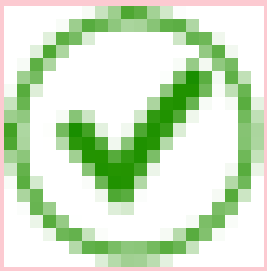
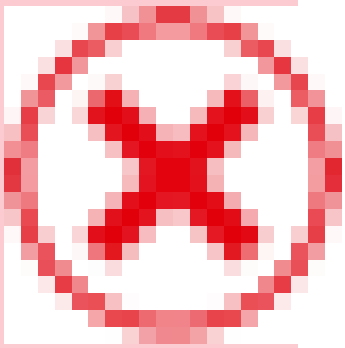
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Mehrere Zurückstellungen				
Alle Gruppen				
Unterstützungsdaten				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

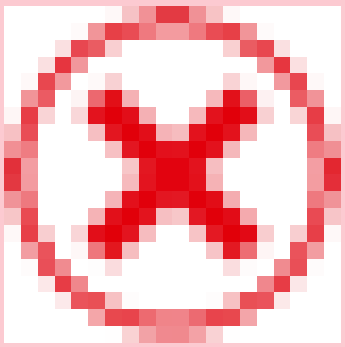
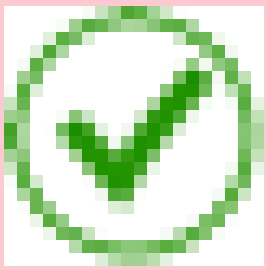
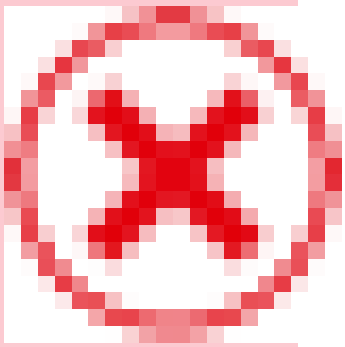
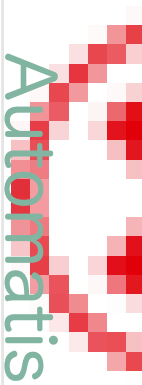
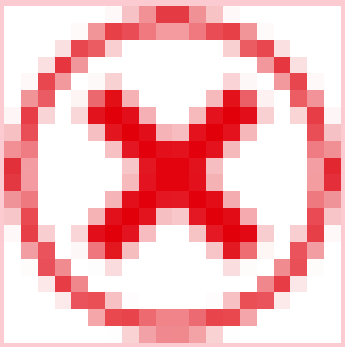
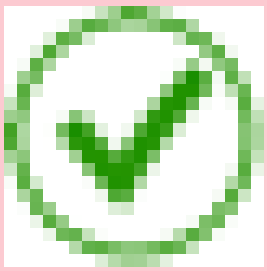
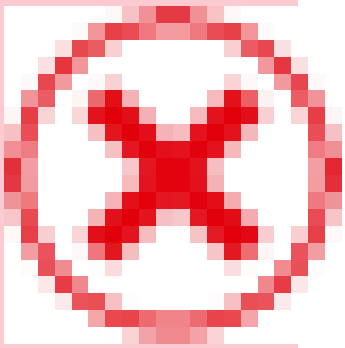
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Autoritative Quellen				
Technologien				
Administration				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

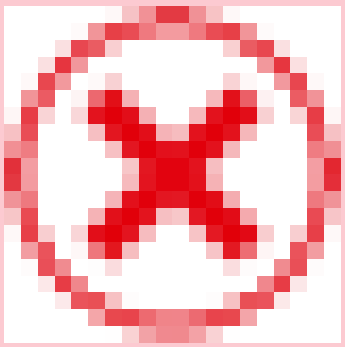
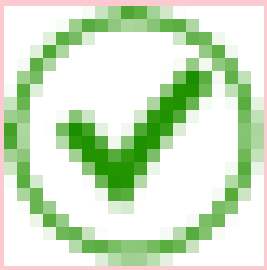
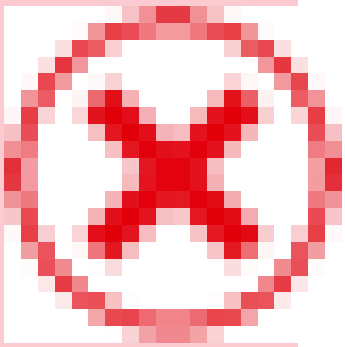
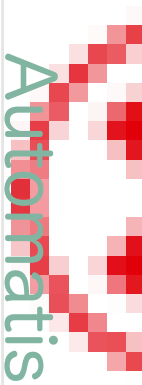
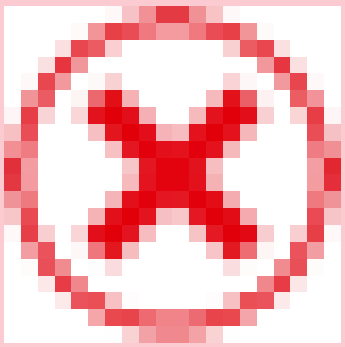
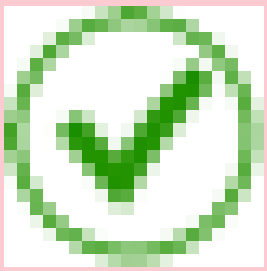
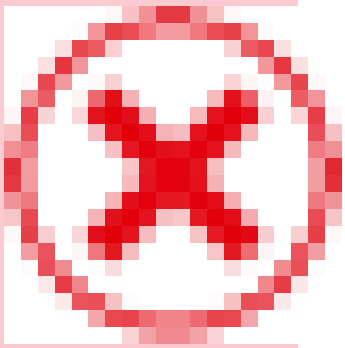
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Zuweisungsregeln				
Veraltete Testergebnisse automatisch schließen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

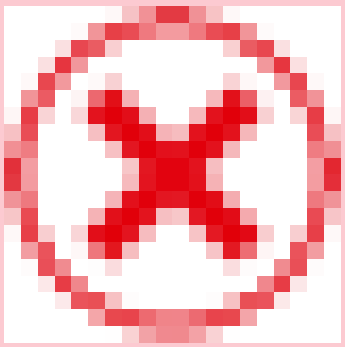
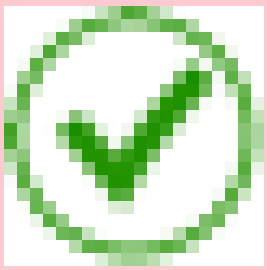
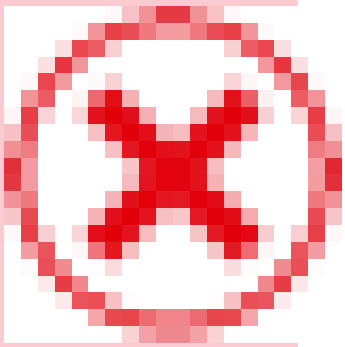
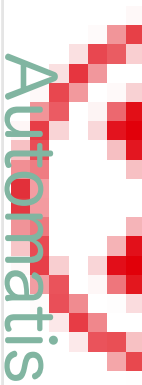
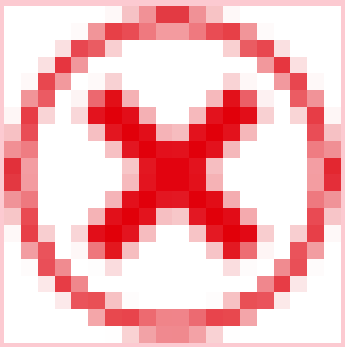
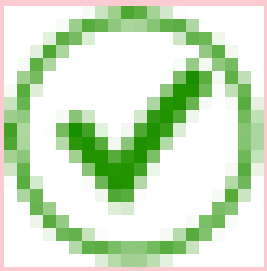
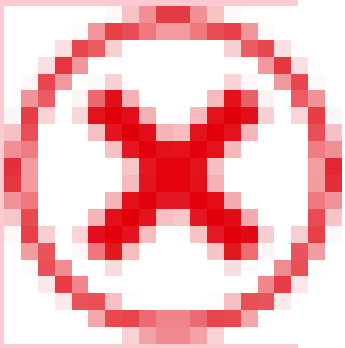
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Gruppenregeln				
Automatische Ausnahmeregel				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

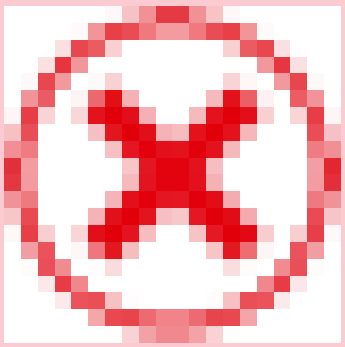
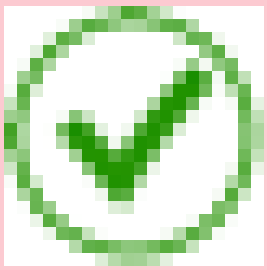
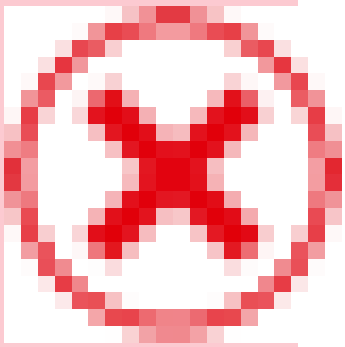
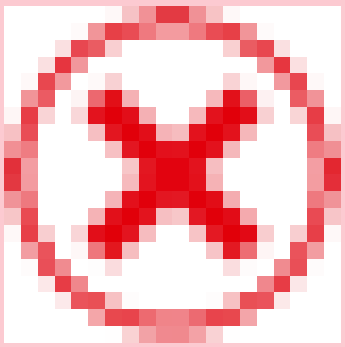
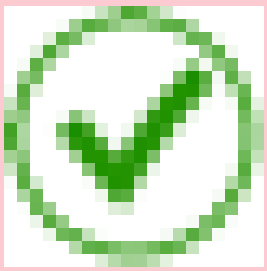
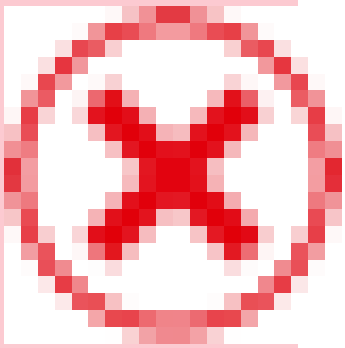
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Genehmigungsregeln				
Risikorechner				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

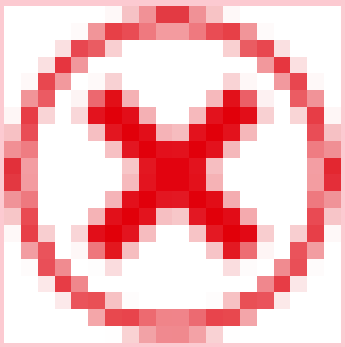
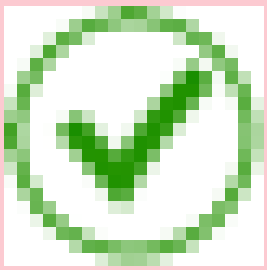
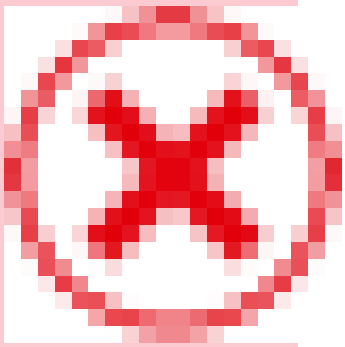
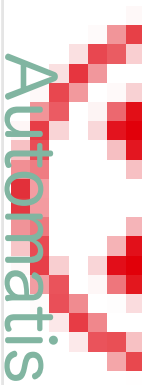
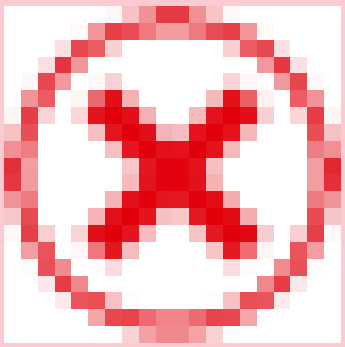
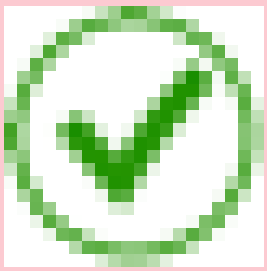
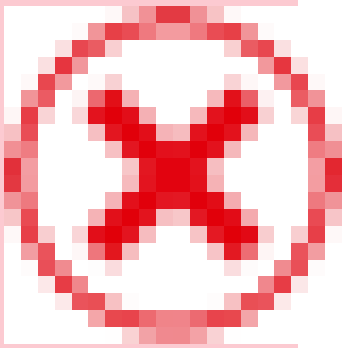
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Rollup-Rechner für Risikopunktzahl				
Korrekturzielregeln				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

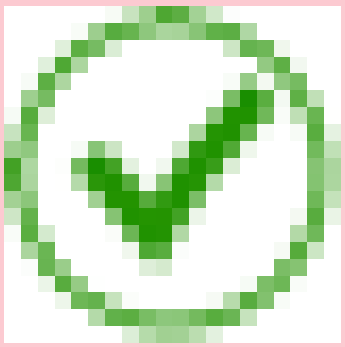
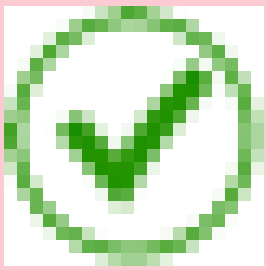
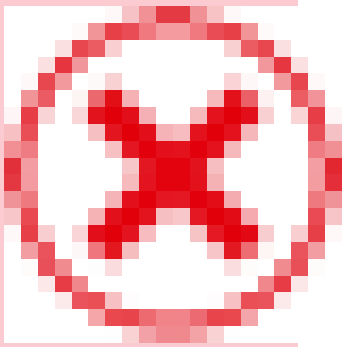
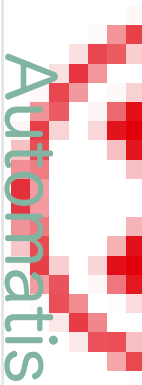
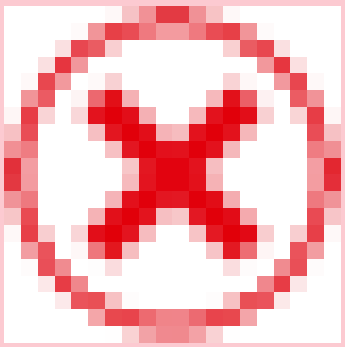
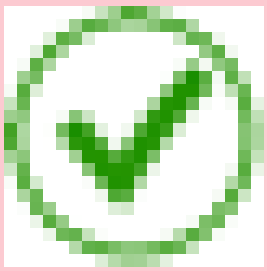
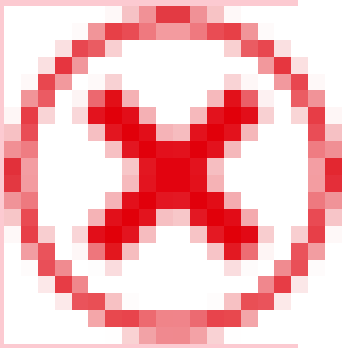
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Relevanz-Zuordnung				
Benachrichtigungen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

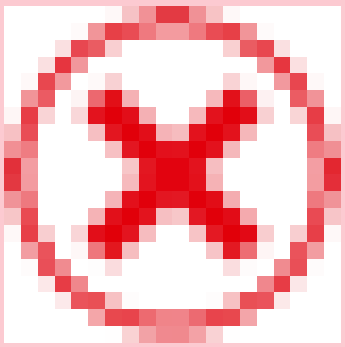
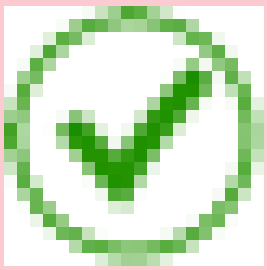
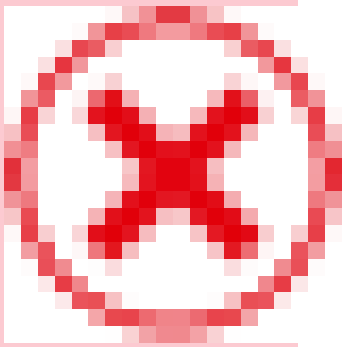
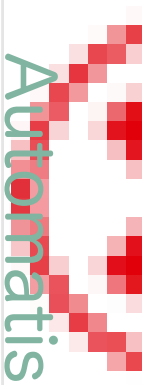
Modulzugriff für: sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

Informationen für andere Rollen:

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vul_qualys. Administrator	sn_vulc. Administrator	sn_vulc. Exception_Approver	sn_vulc. Ma
Ausnahmenverwaltung				

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn
(Haupt-App-Gruppe)				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Übersicht	✗	✗	✓	
Richtlinien	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Tests	✗	✗	✓	
Meine Genehmigungen	✗	✗	✗	
Testergebnisse				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Nicht selektierte Testergebnisse	✗	✗	✓	
Meine offenen Testergebnisse	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Offene Testergebnisse	✗	✗	✓	
Ziel rückt näher	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Verfehltes Ziel	✗	✗	✓	
Nicht zugewiesen	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Mehrere Zurückstellungen	✗	✗	✓	
Alle	✗	✗	✓	
Testergebnisgruppen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

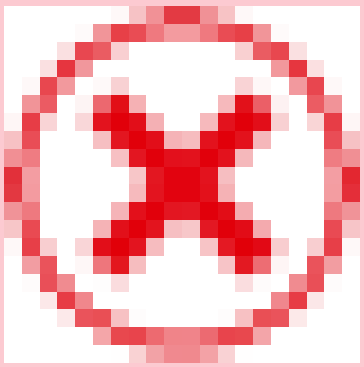
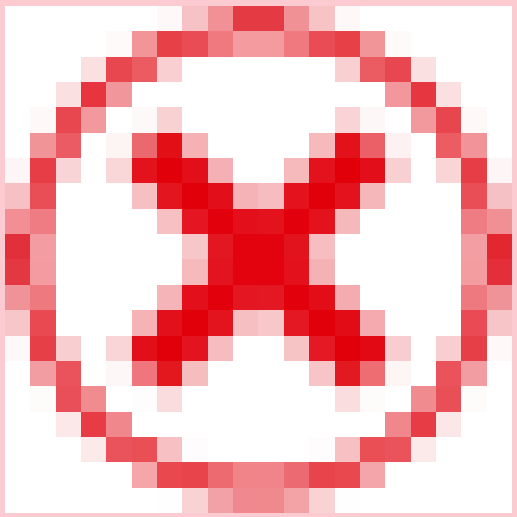
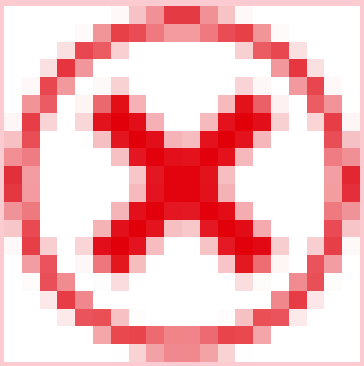
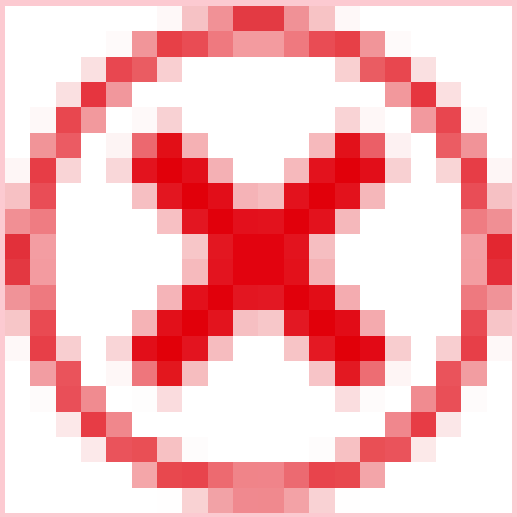
Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Meine Offenen Gruppen				
Alle Offenen Gruppen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

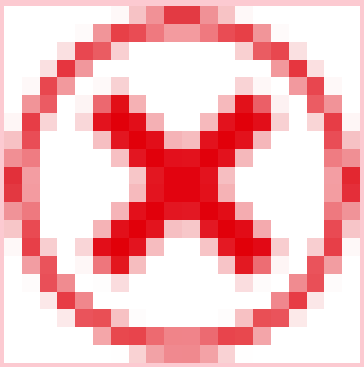
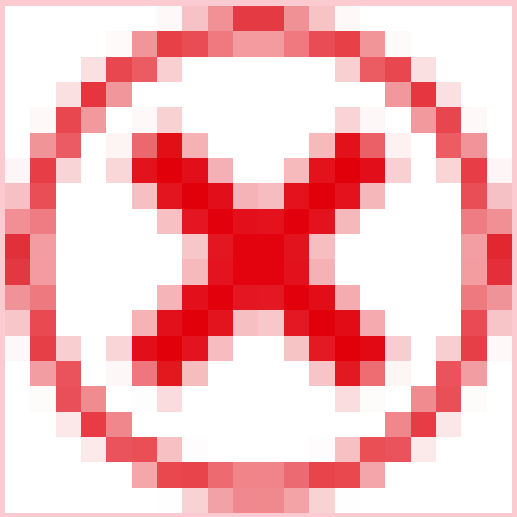
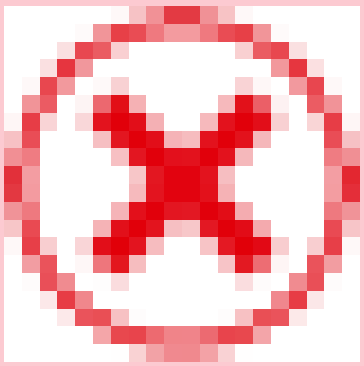
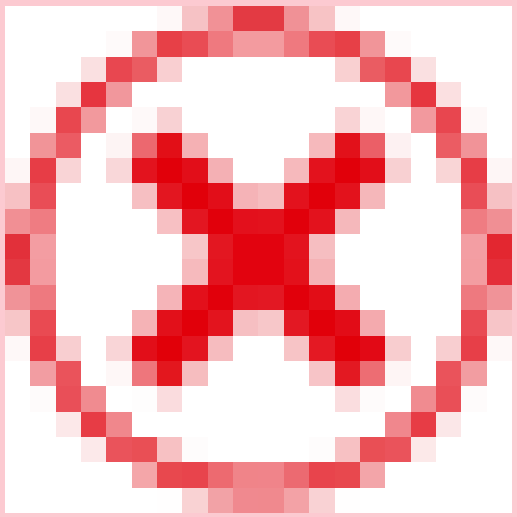
Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Mehrere Zurückstellungen				
Alle Gruppen				
Unterstützungsdaten				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Autoritative Quellen	✗	✗	✓	
Technologien	✗	✗	✓	
Administration				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Zuweisungsregeln	✗	✗	✗	
Veraltete Testergebnisse automatisch schließen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

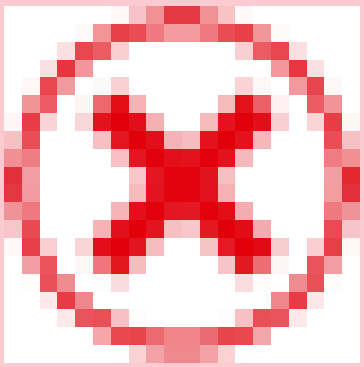
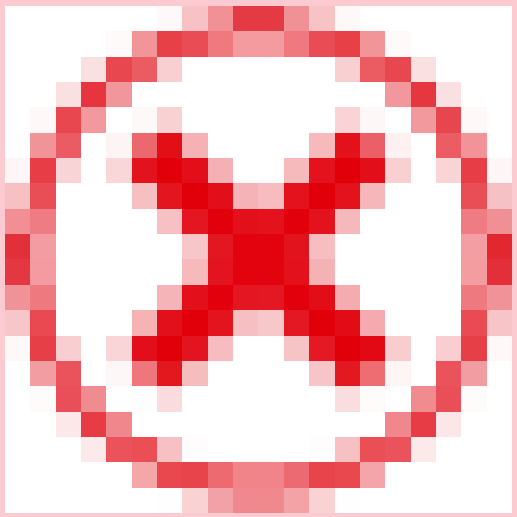
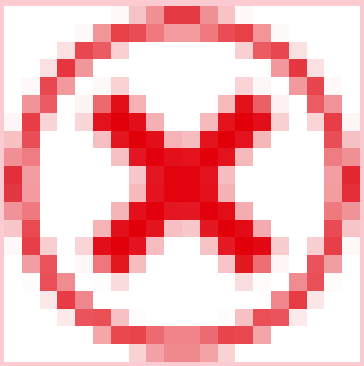
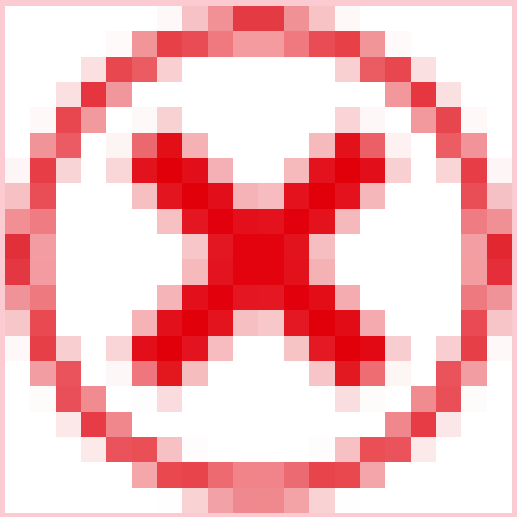
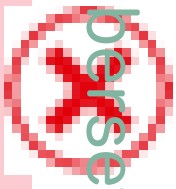
Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Gruppenregeln				
Automatische Ausnahmeregel				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Genehmigungsregeln	✗	✗	✗	
Risikorechner	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Rollup-Rechner für Risikopunktzahl	✗	✗	✗	
Korrekturzielregeln	✗	✓	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

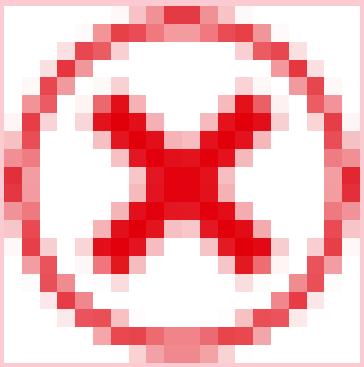
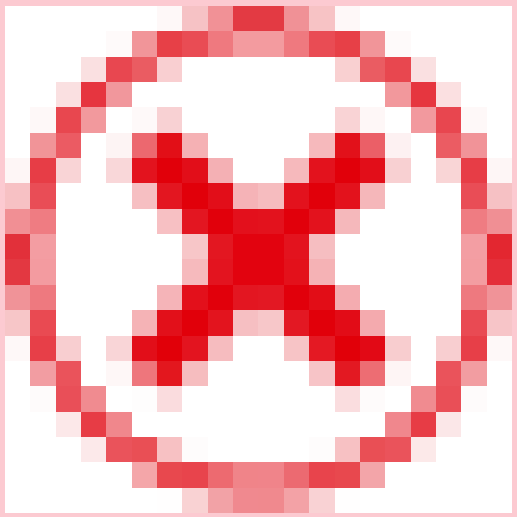
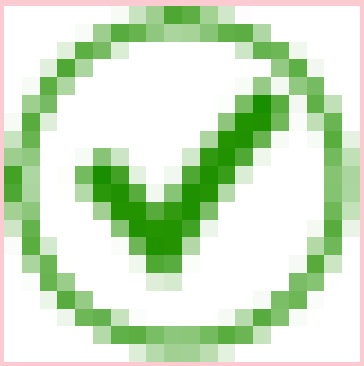
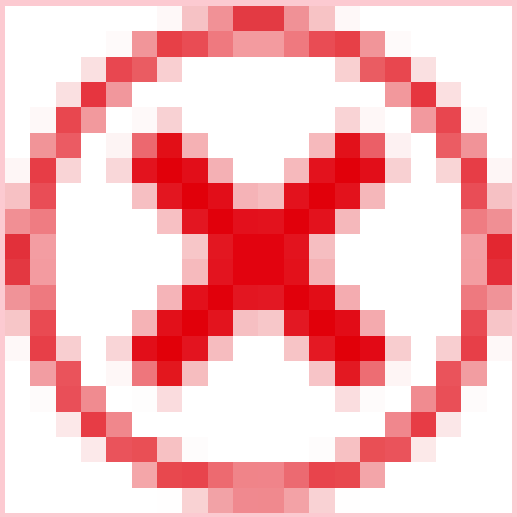
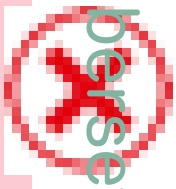
Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Relevanz-Zuordnung				
Benachrichtigungen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

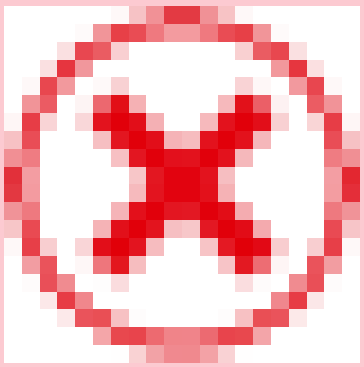
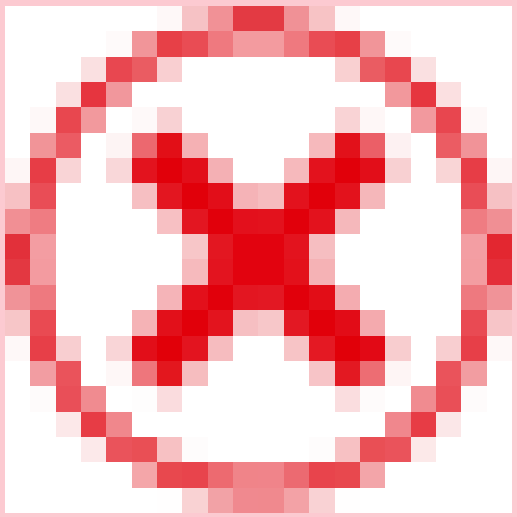
Modulzugriff für: sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Remediation_owner

(Fortsetzung)

Modul	sn_vulc. Manage_Notifications	sn_vulc. Manage_Remediation_target_rules	sn_vulc. Lesen	sn_
Ausnahmenverwaltung				

Modulzugriff für: sn_vulc.Remediation_owner

Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

Modul	sn_vulc. Remediation_owner
(Haupt-App-Gruppe)	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

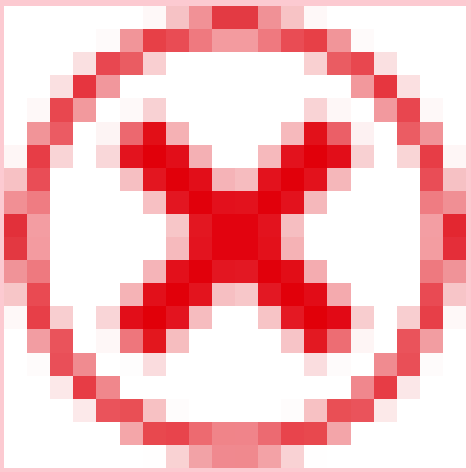
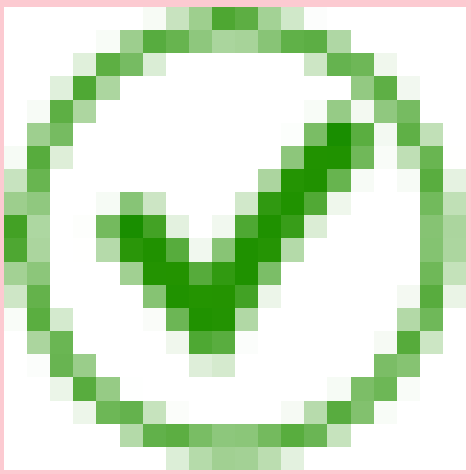
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Übersicht	
Richtlinien	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

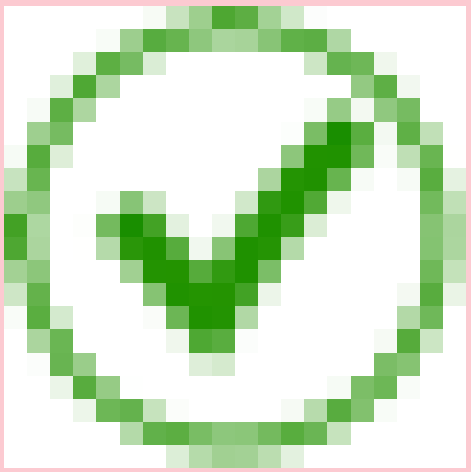
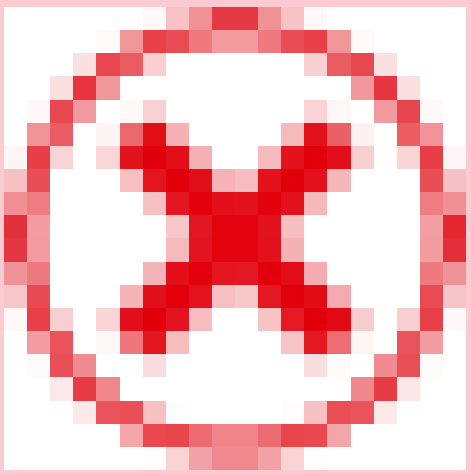
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Tests	
Meine Genehmigungen	
Testergebnisse	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

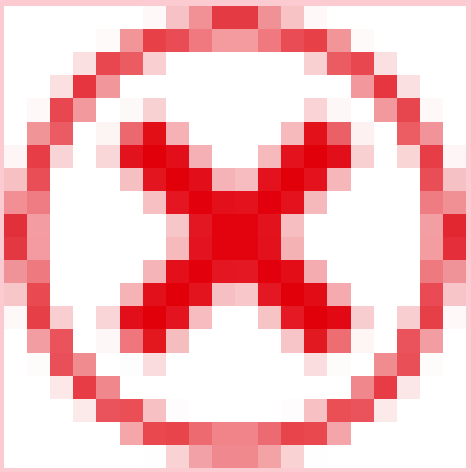
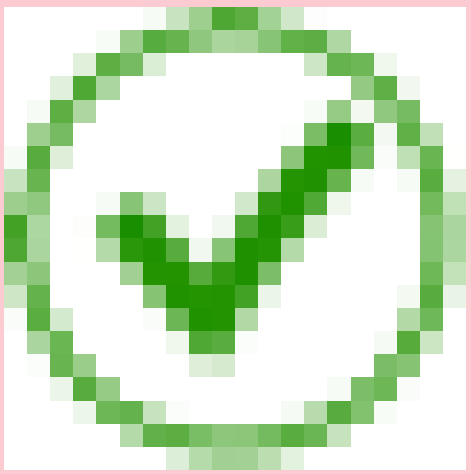
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Nicht selektierte Testergebnisse	
Meine offenen Testergebnisse	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

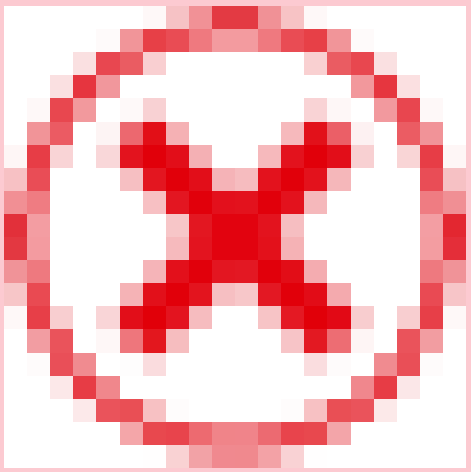
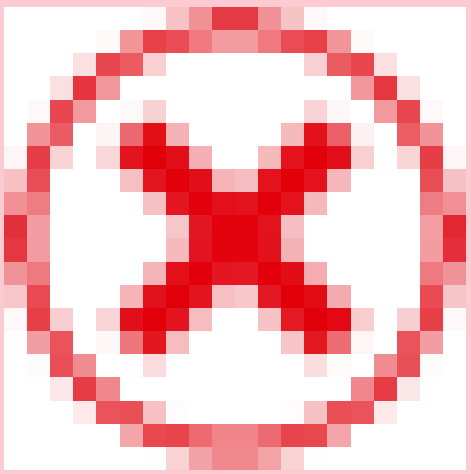
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Offene Testergebnisse	
Ziel rückt näher	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

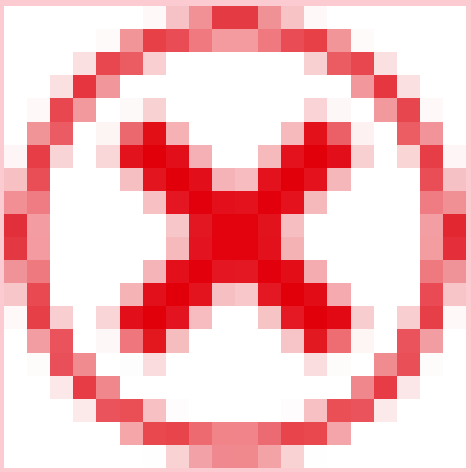
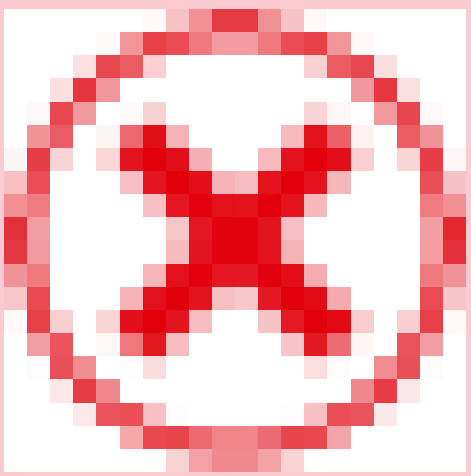
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Verfehltes Ziel	
Nicht zugewiesen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

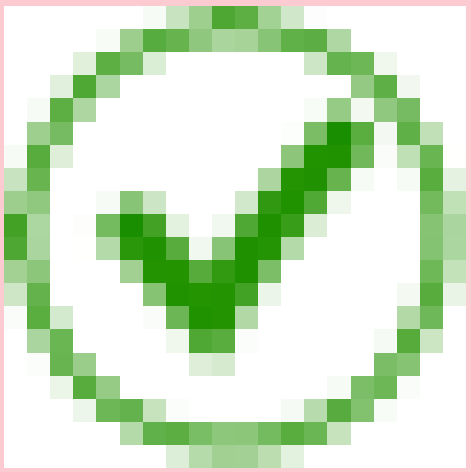
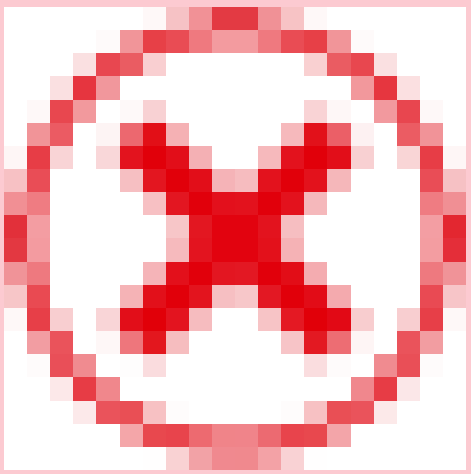
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Mehrere Zurückstellungen	
Alle	
Testergebnisgruppen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

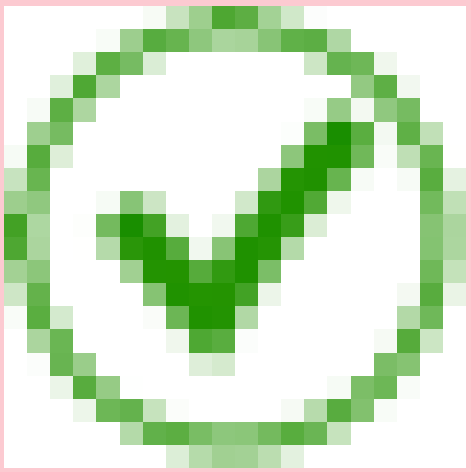
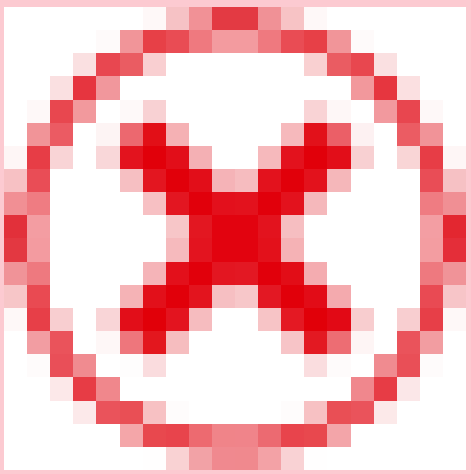
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Meine Offenen Gruppen	
Alle Offenen Gruppen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

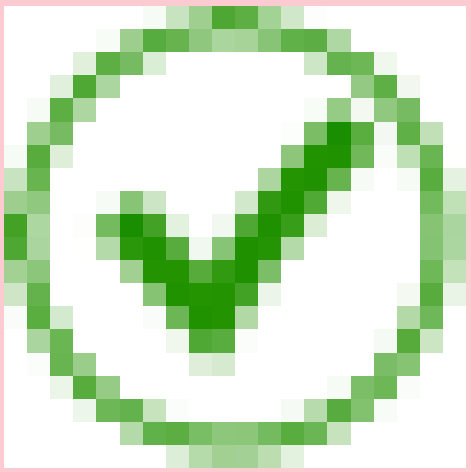
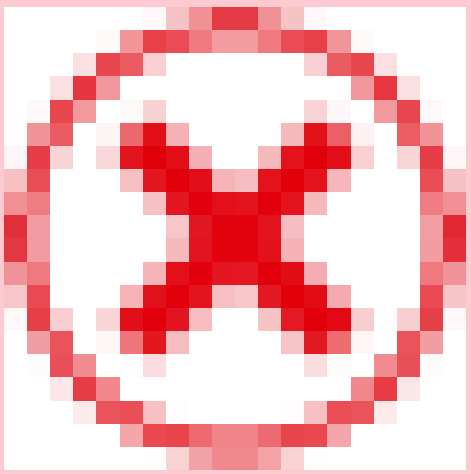
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Mehrere Zurückstellungen	
Alle Gruppen	
Unterstützungsdaten	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

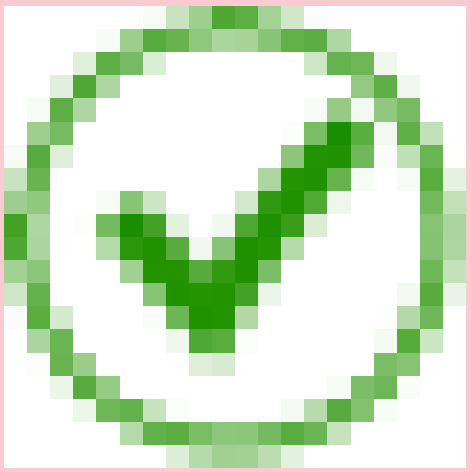
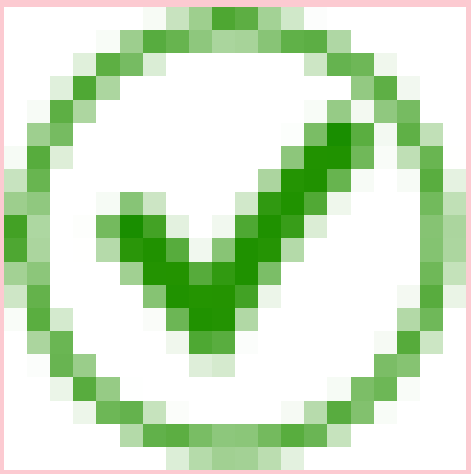
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Autoritative Quellen	
Technologien	
Administration	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

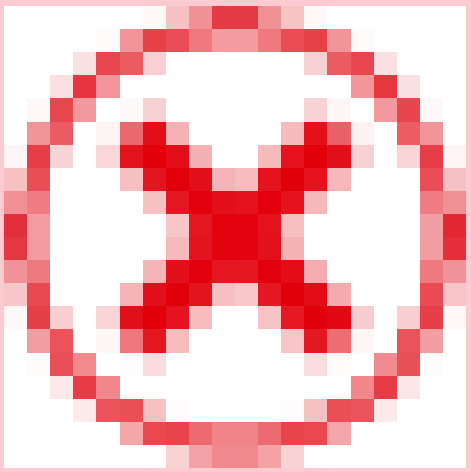
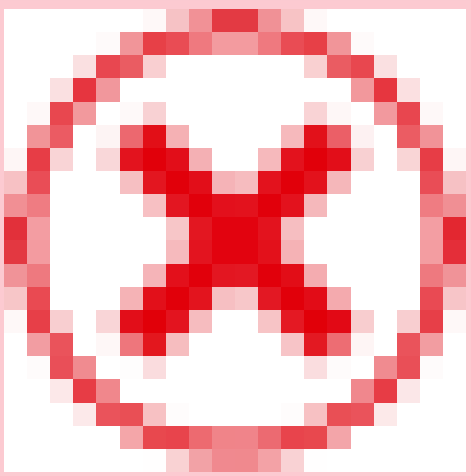
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Zuweisungsregeln	
Veraltete Testergebnisse automatisch schließen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

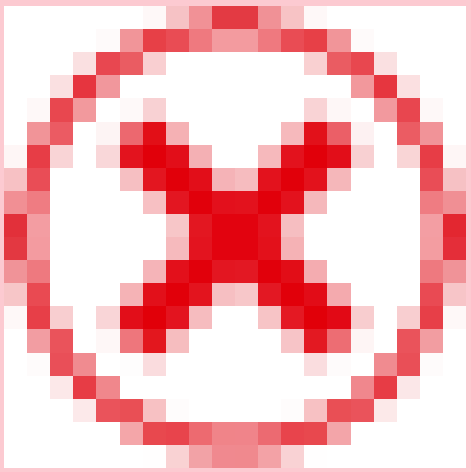
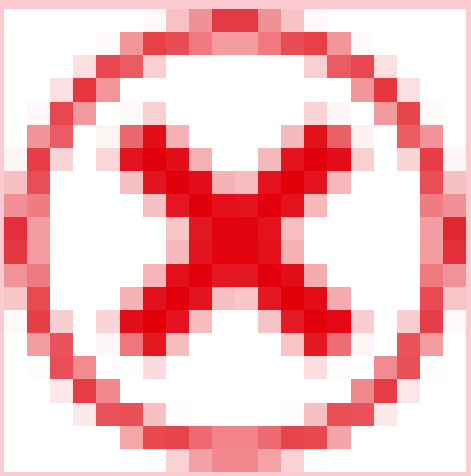
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Gruppenregeln	
Automatische Ausnahmeregel	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

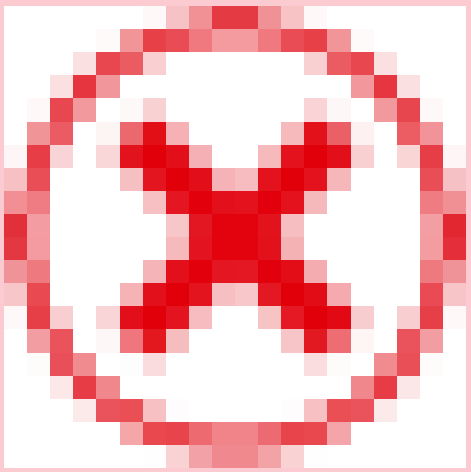
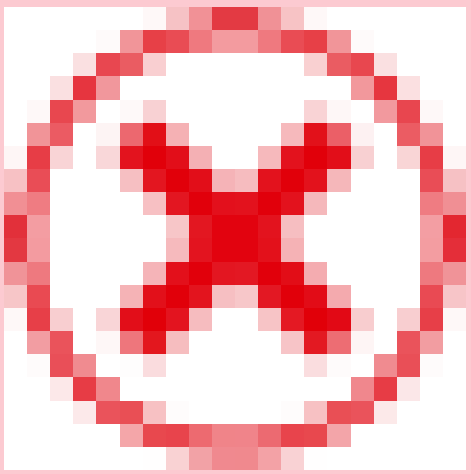
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Genehmigungsregeln	
Risikorechner	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

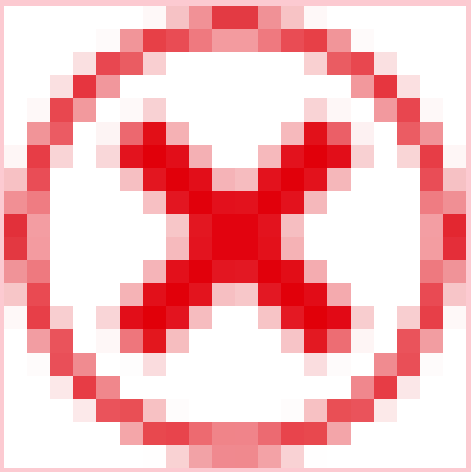
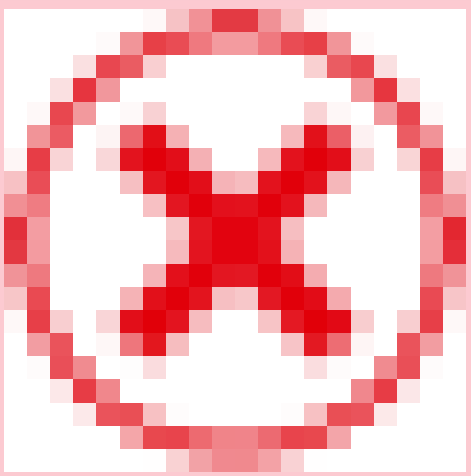
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Rollup-Rechner für Risikopunktzahl	
Korrekturzielregeln	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

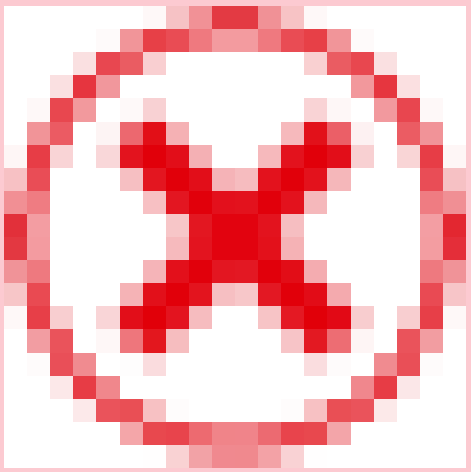
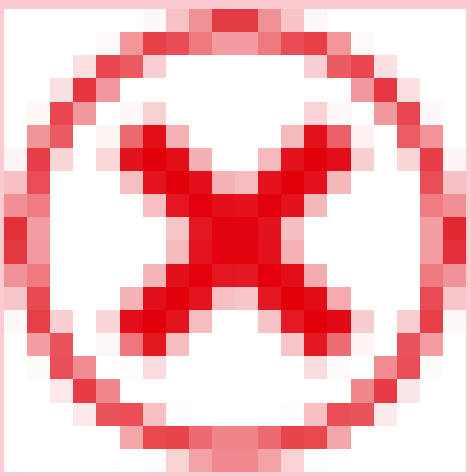
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Relevanz-Zuordnung	
Benachrichtigungen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

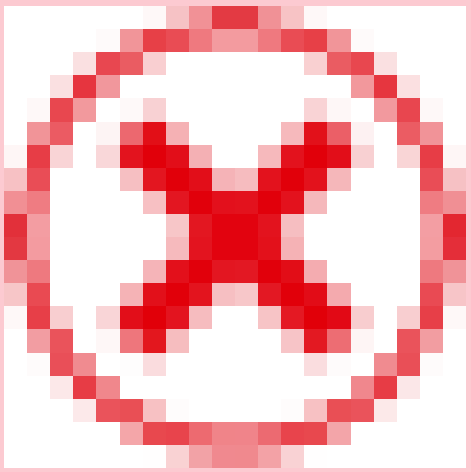
Modulzugriff für: sn_vulc.Remediation_owner

Informationen für andere Rollen:

sn_vul_qualys.admin, sn_vulc.admin, sn_vulc.Exception_Approver, sn_vulc.Manage_Approval_rules, sn_vulc.Manage_Auto_Exception_rule

sn_vulc.Manage_Notifications, sn_vulc.Manage_Remediation_target_rules, sn_vulc.read, sn_vulc.read_Remediation_target_rules

(Fortsetzung)

Modul	sn_vulc. Remediation_owner
Ausnahmenverwaltung	

[End]

[store-future: BEGIN review]

Modulzugriff nach Rolle für Container Vulnerability Response

Informationen zu Container Vulnerability Response finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

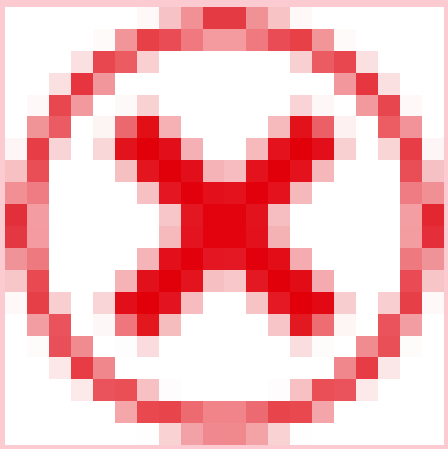
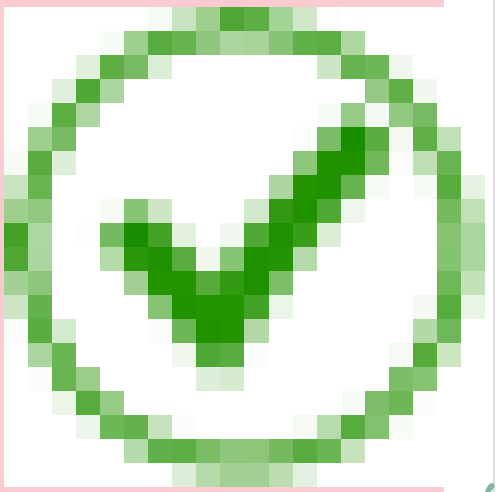
Informationen für andere Rollen:

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul_Container. Configure_Integrations	sn_vul_Con
(Haupt-App-Gruppe)			
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

Informationen für andere Rollen:

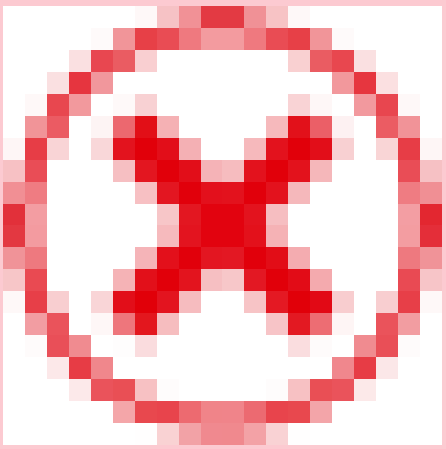
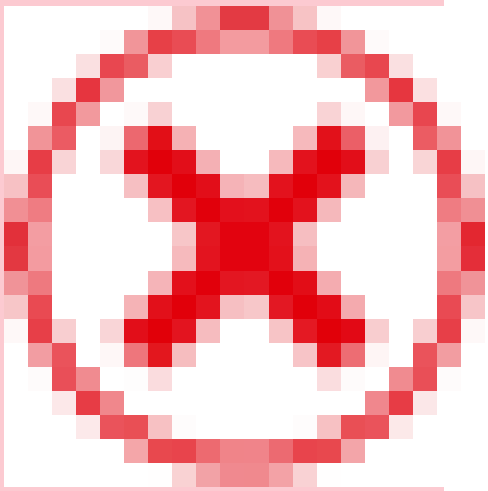
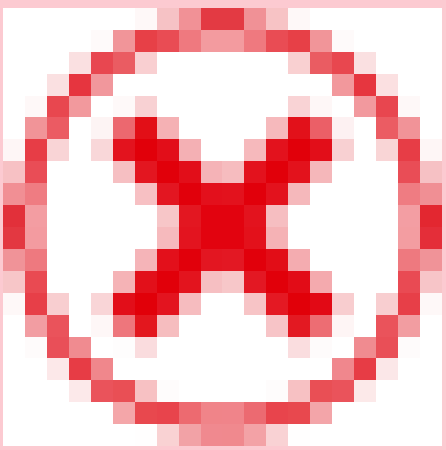
sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul_Container. Configure_Integrations	sn_vul_Con
Meine Genehmigungen			
Angreifbare Container-Elemente			
Mir zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

Informationen für andere Rollen:

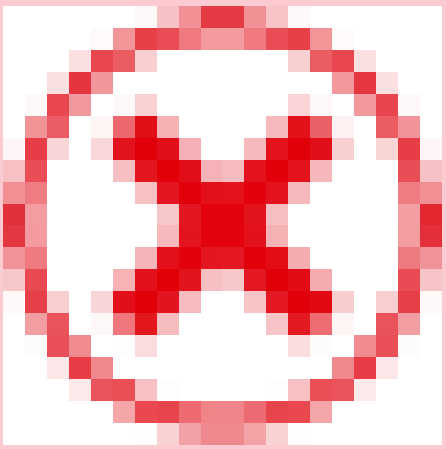
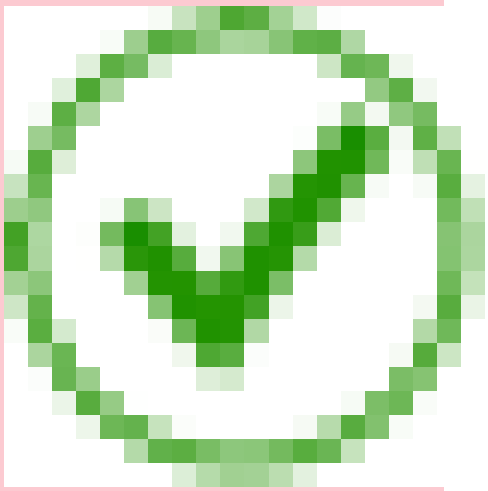
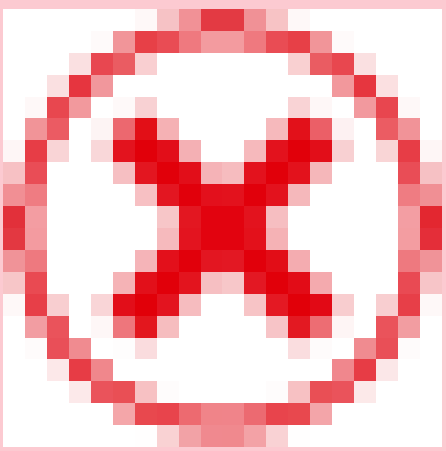
sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul_Container. Configure_Integrations	sn_vul_Con
Meinen Gruppen zugewiesen			
Kritisches und hohes Risiko			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

Informationen für andere Rollen:

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul_Container. Configure_Integrations	sn_vul_Con
Nutzbar	✗	✓	
Ziel rückt näher	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

Informationen für andere Rollen:

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul_Container. Configure_Integrations	sn_vul_Con
Verfehltes Ziel	✗	✓	
Alle	✗	✓	
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

Informationen für andere Rollen:

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul_Container. Configure_Integrations	sn_vul_Con
NVD	✗	✓	
Drittpartei	✗	✓	
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

Informationen für andere Rollen:

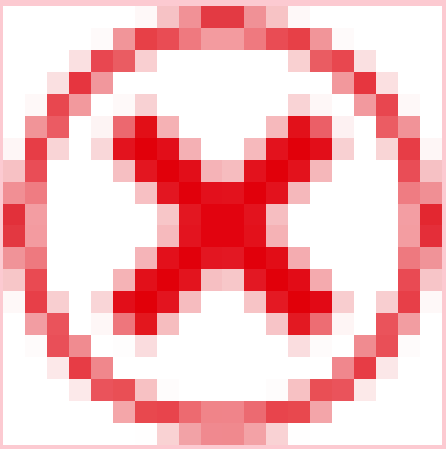
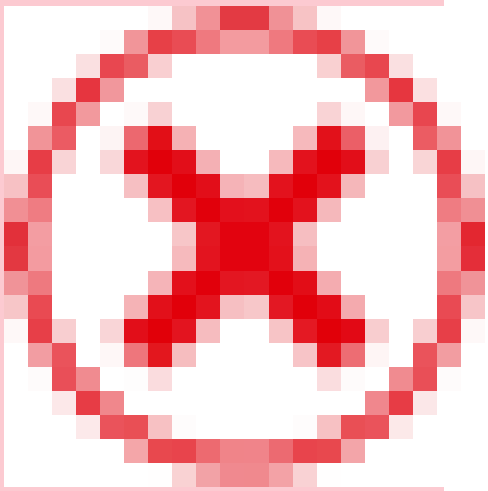
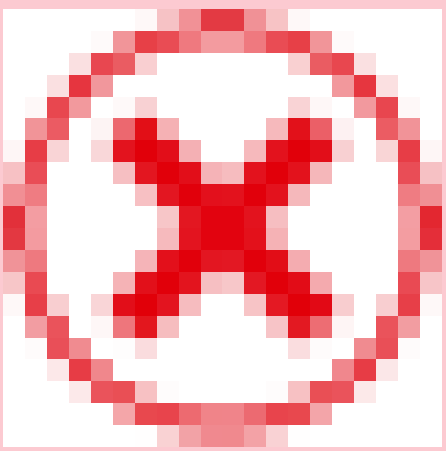
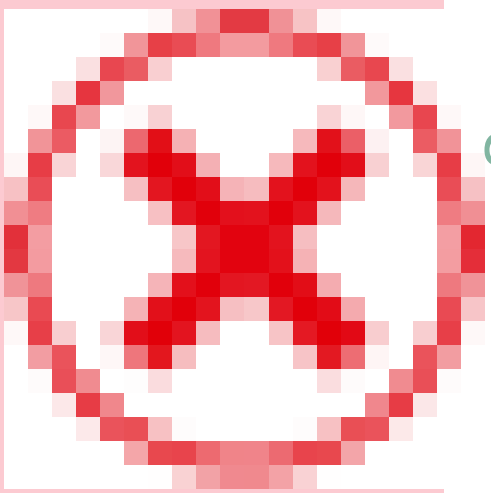
sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul_Container. Configure_Integrations	sn_vul_Con
Zuweisungsregeln			
Schwachstellen-Rechner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

Informationen für andere Rollen:

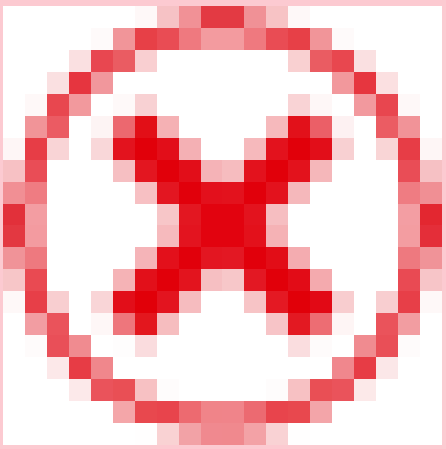
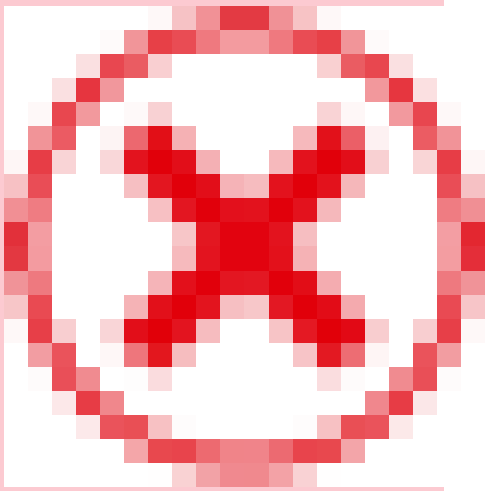
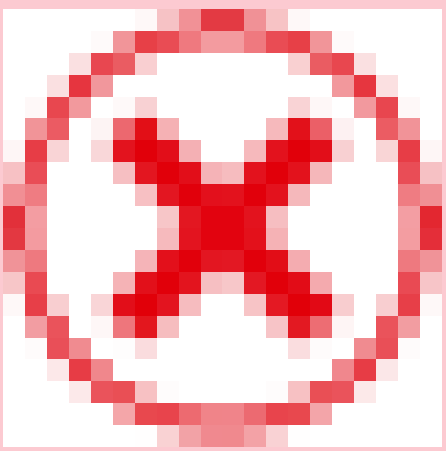
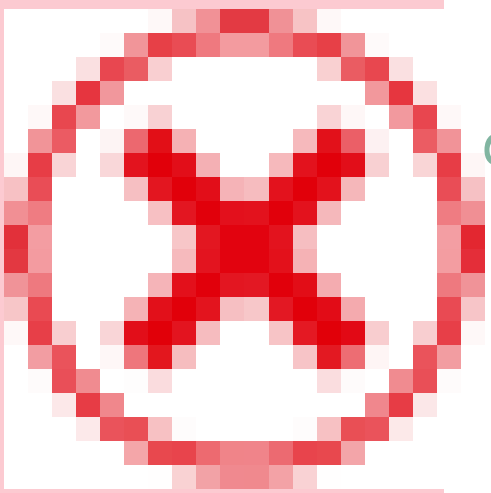
sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul_Container. Configure_Integrations	sn_vul_Con
Korrekturzielregeln			
VI-Granularität konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

Informationen für andere Rollen:

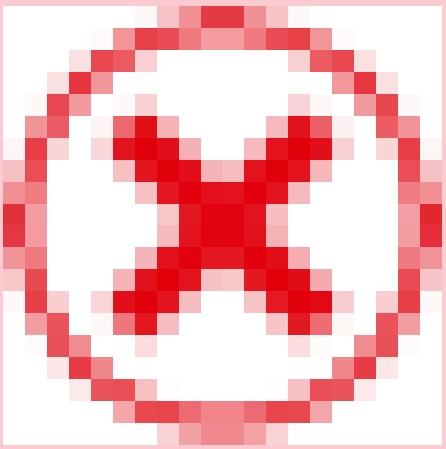
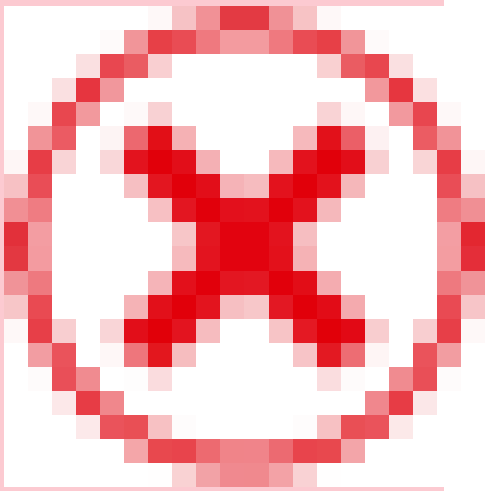
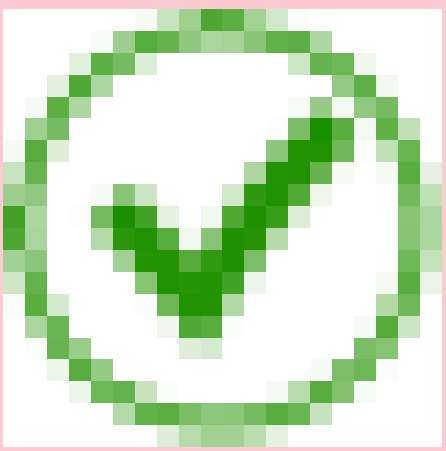
sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul_Container. Configure_Integrations	sn_vul_Con
Ausnahmeregeln			
Genehmigungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

Informationen für andere Rollen:

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul_Container. Configure_Integrations	sn_vul_Con
Container-Sicherheitsintegrationen	✗	✓	
Angreifbare Elemente automatisch schließen	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

Informationen für andere Rollen:

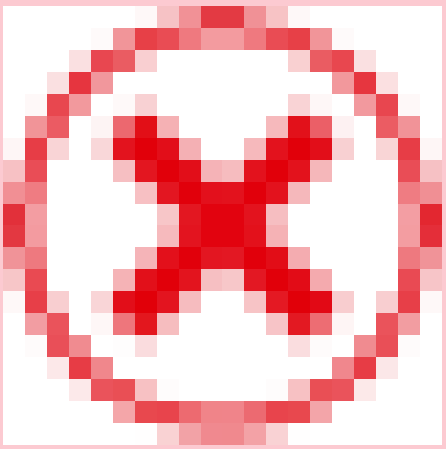
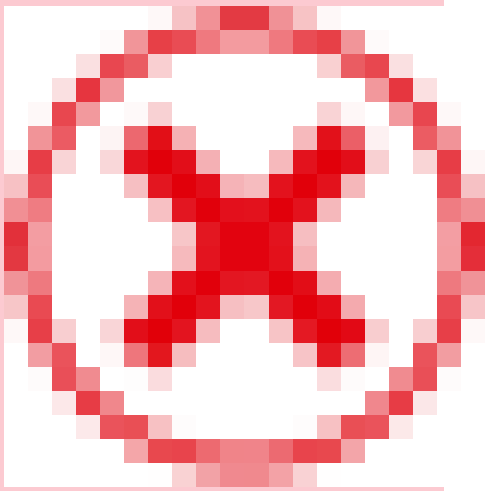
sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul_Container. Configure_Integrations	sn_vul_Con
Normalisierte Schweregradzuordnungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
(Haupt-App-Gruppe)			
Übersicht	✓	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

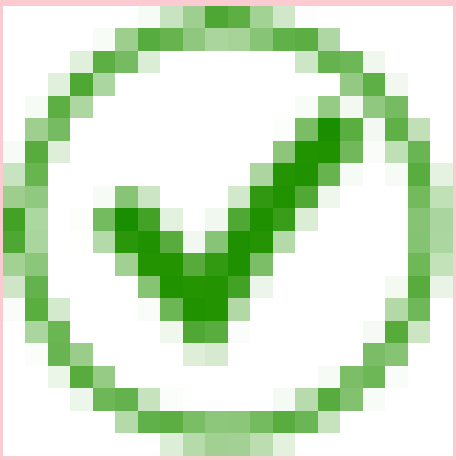
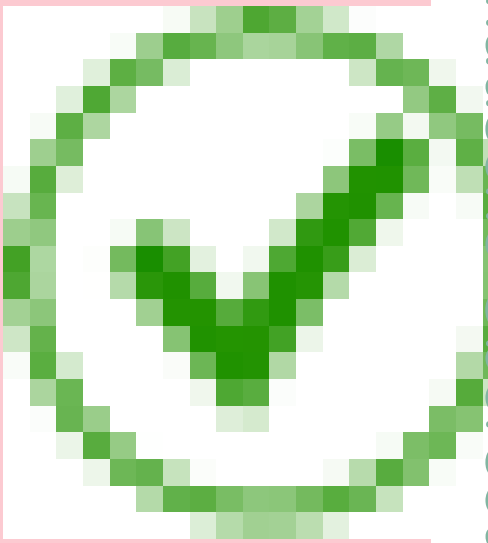
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Meine Genehmigungen			
Angreifbare Container-Elemente			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

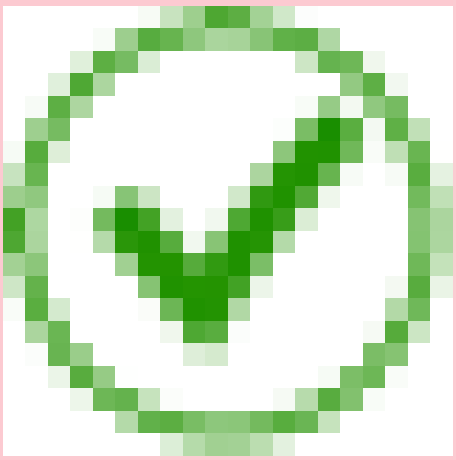
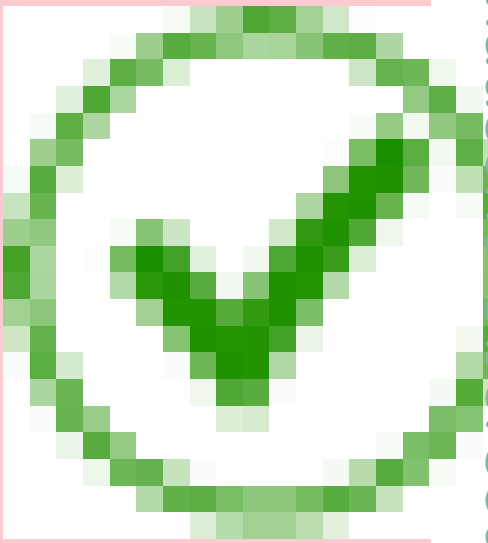
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Mir zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

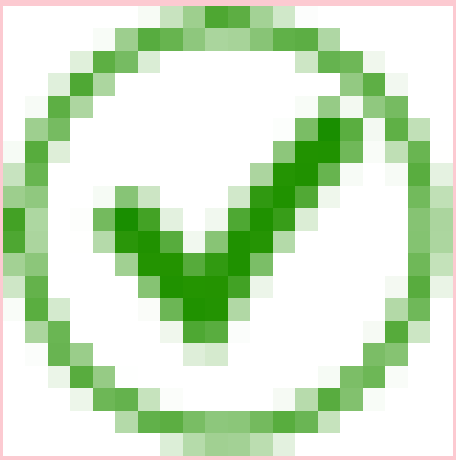
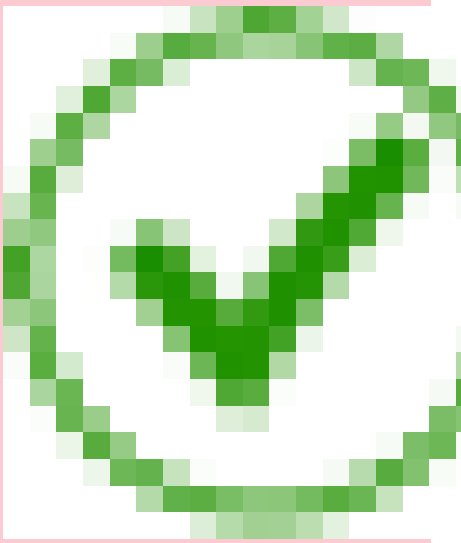
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Meinen Gruppen zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

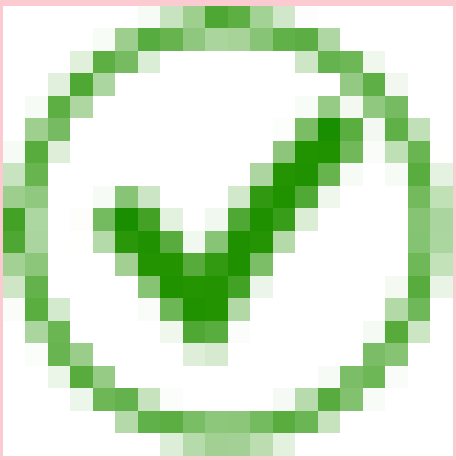
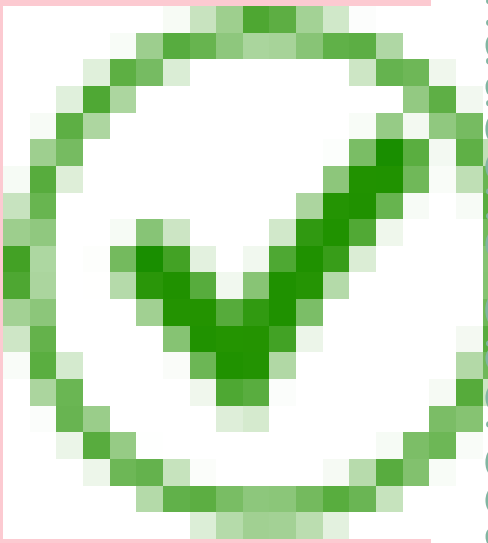
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Kritisches und hohes Risiko			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

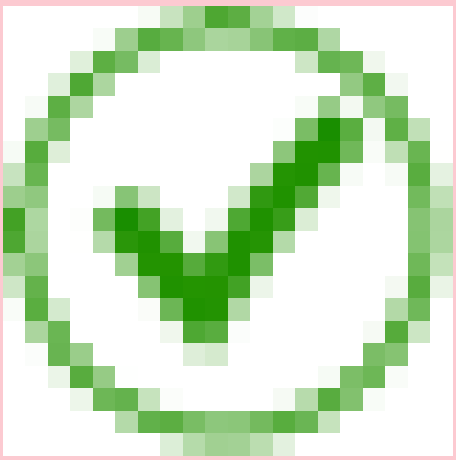
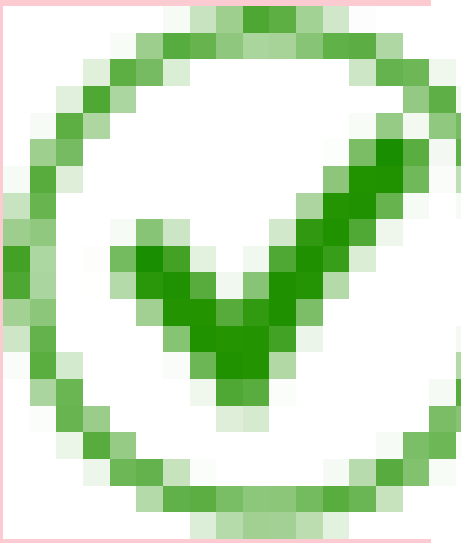
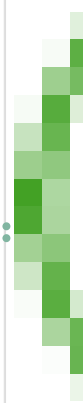
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Nutzbar			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

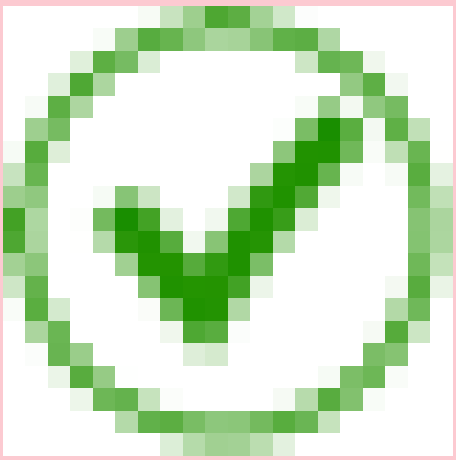
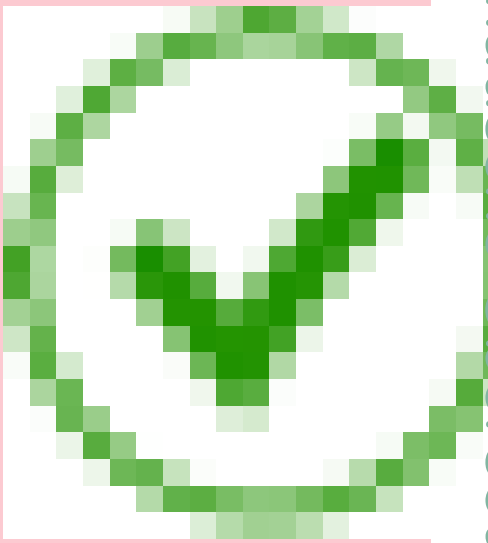
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Ziel rückt näher			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

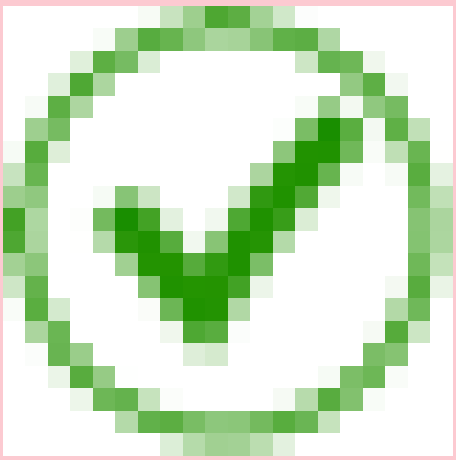
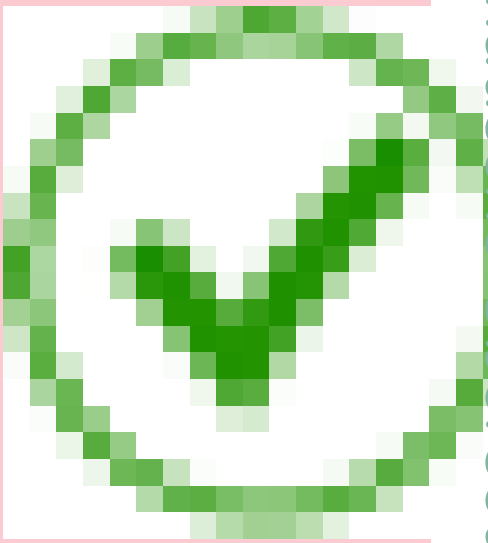
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Verfehltes Ziel			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

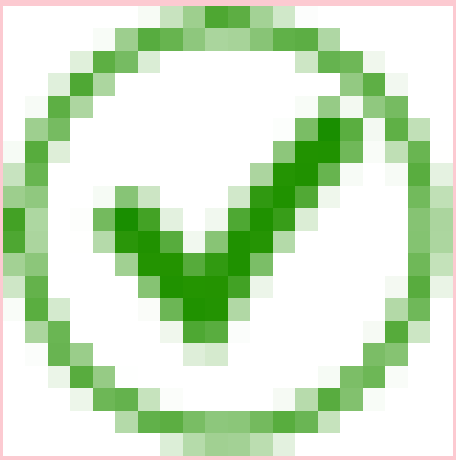
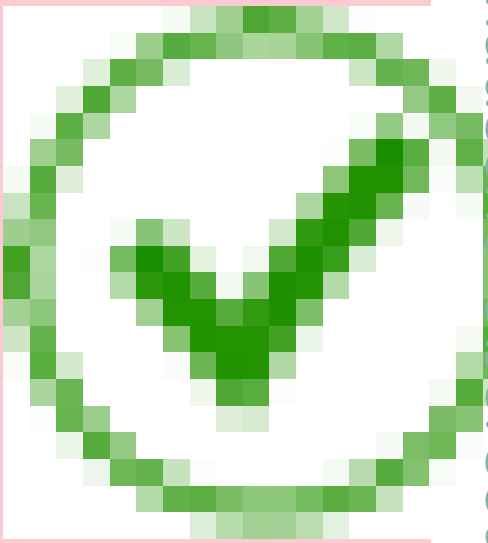
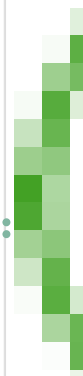
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Alle			
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

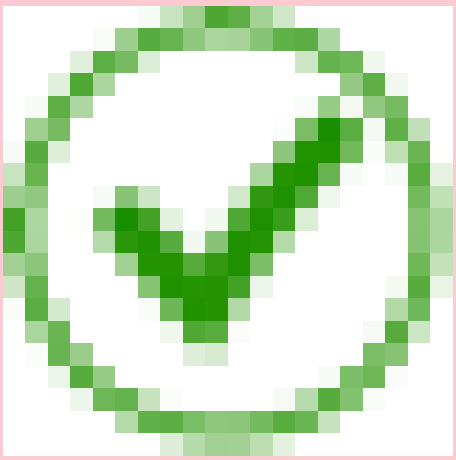
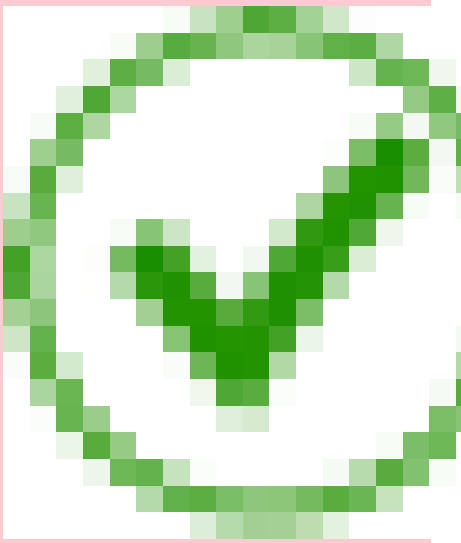
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
NVD			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

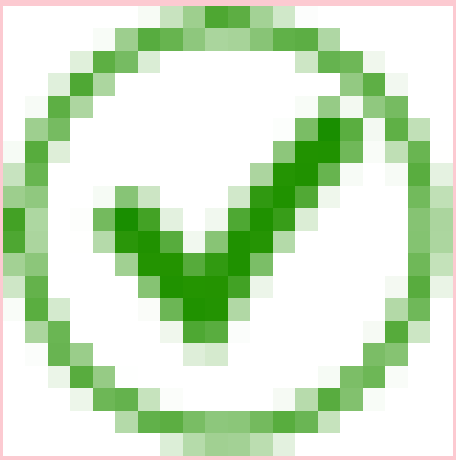
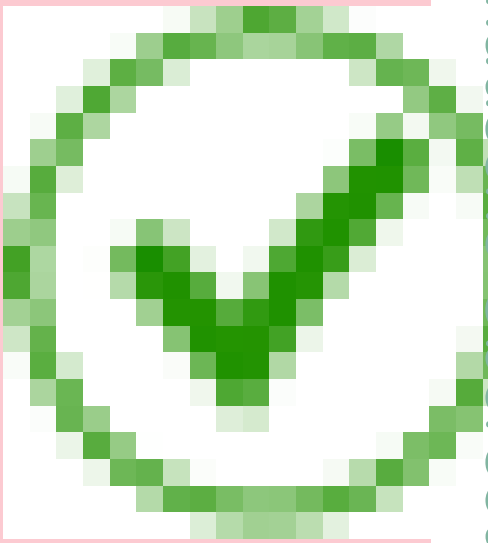
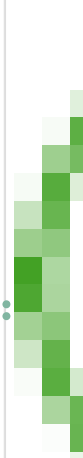
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Drittpartei			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

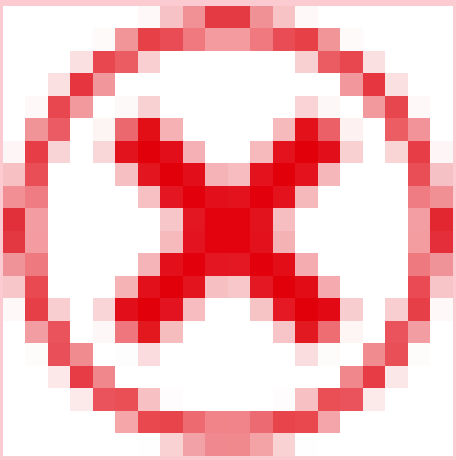
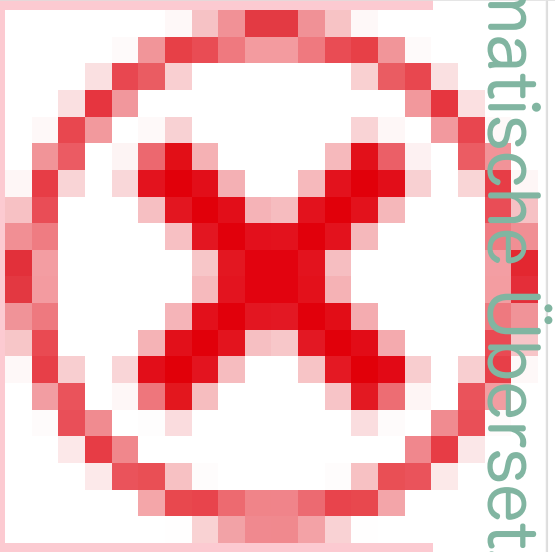
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Zuweisungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

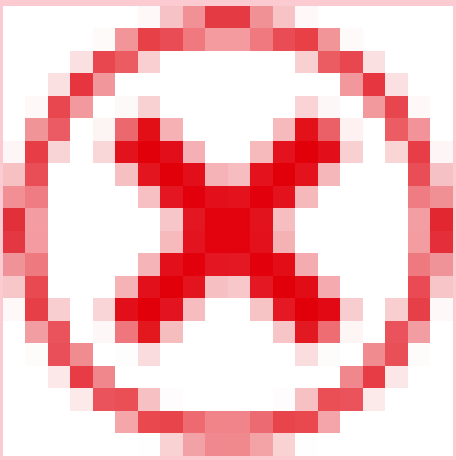
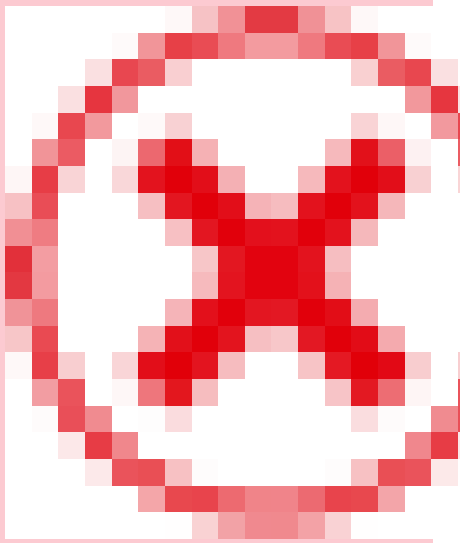
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Schwachstellen-Rechner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

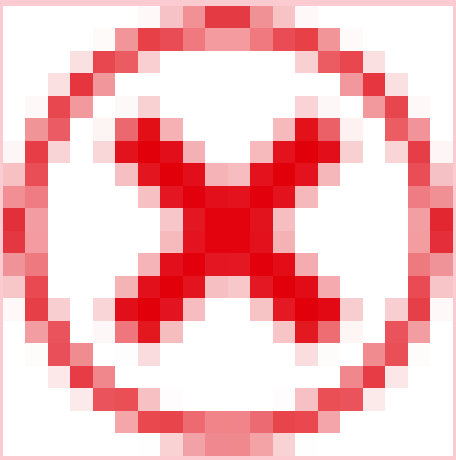
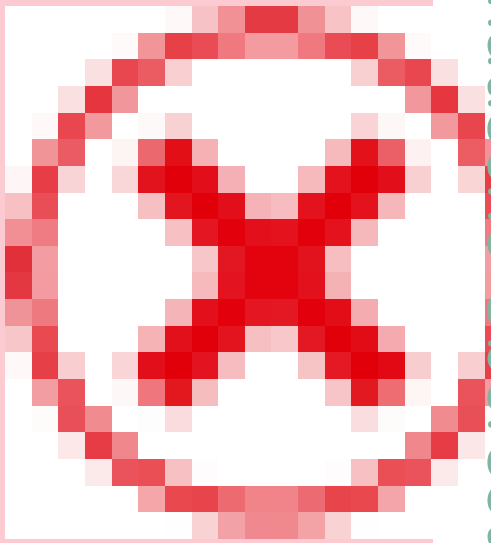
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Korrekturzielregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

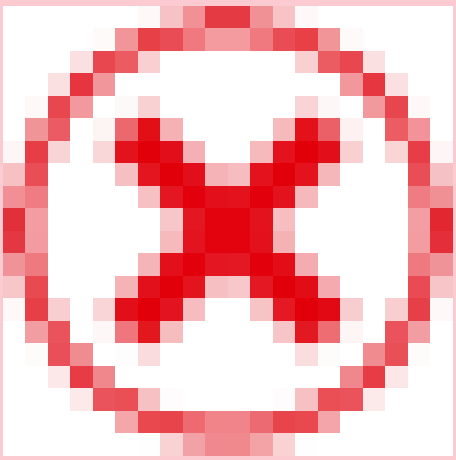
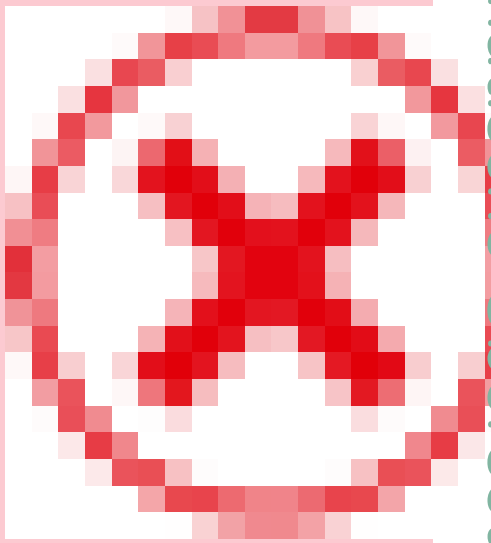
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
VI-Granularität konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

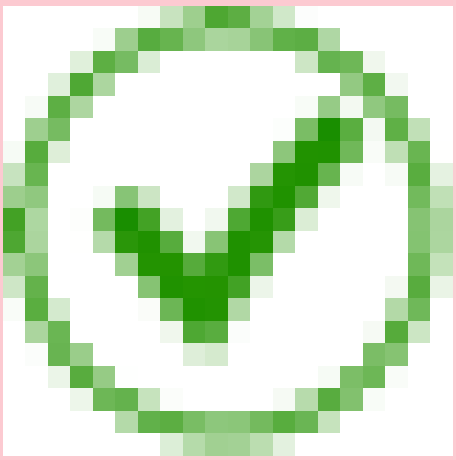
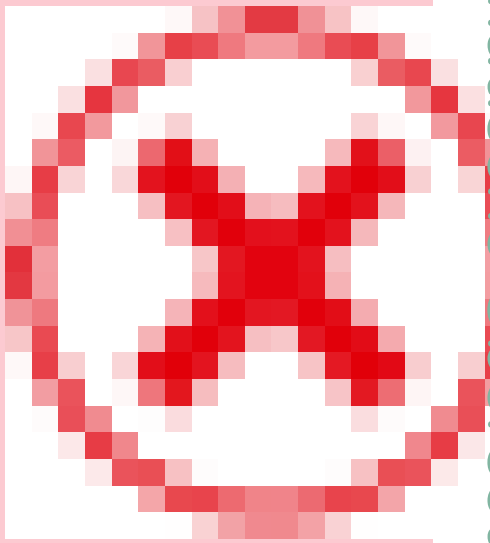
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Ausnahmeregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

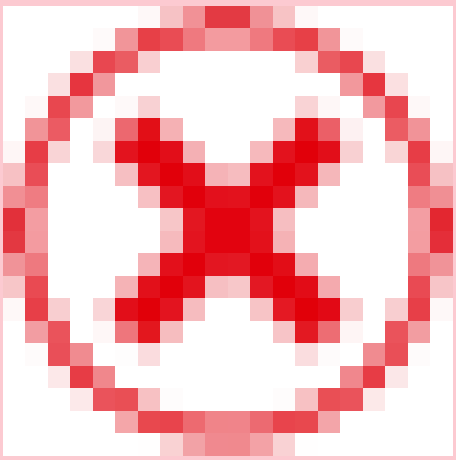
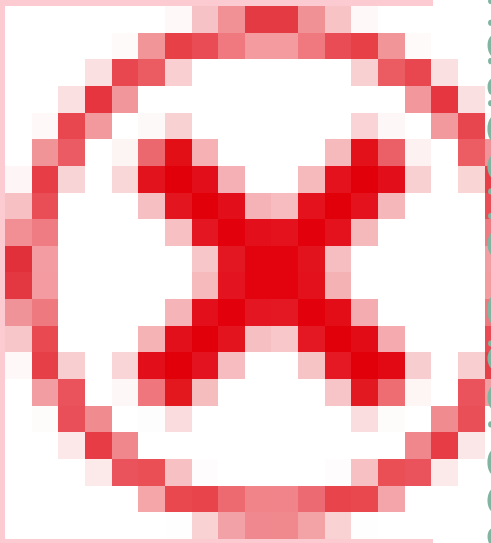
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Genehmigungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

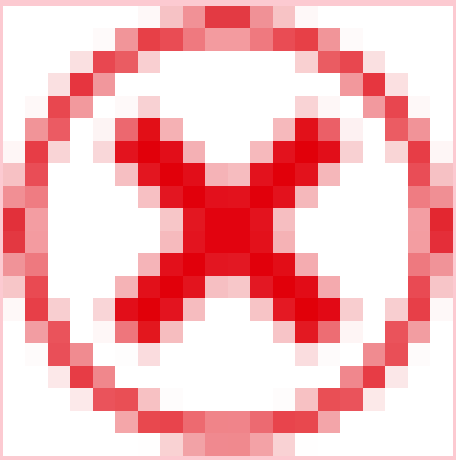
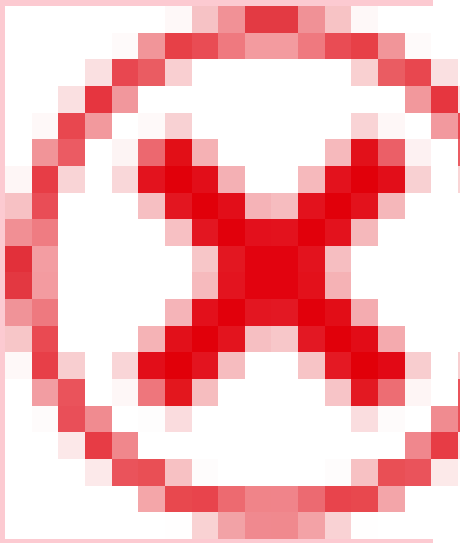
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Container-Sicherheitsintegrationen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

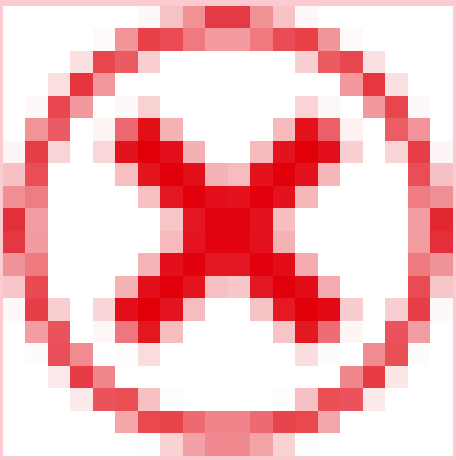
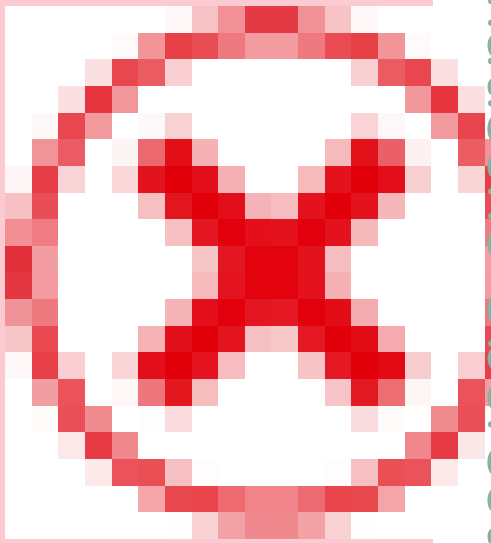
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Angreifbare Elemente automatisch schließen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

Informationen für andere Rollen:

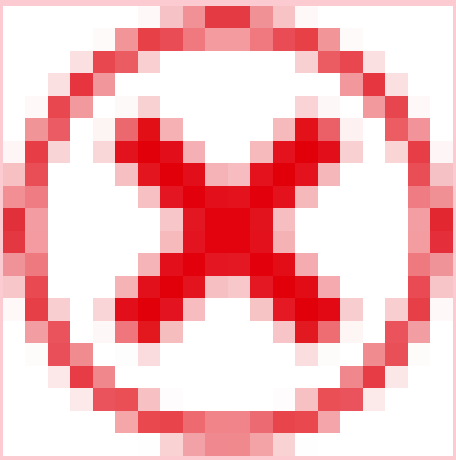
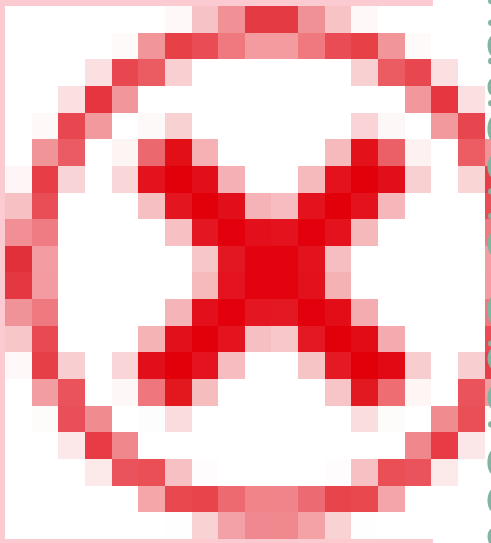
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Exception_Approver	sn_vul_Container. Falsch_positiv_Genehmiger	sn_vu
Normalisierte Schweregradzuordnungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

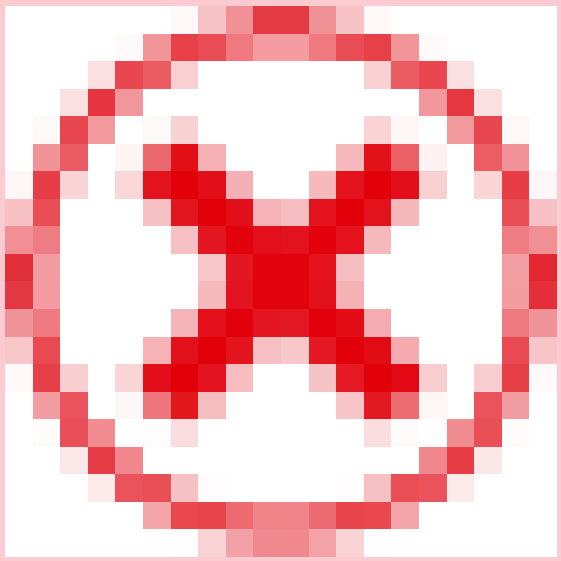
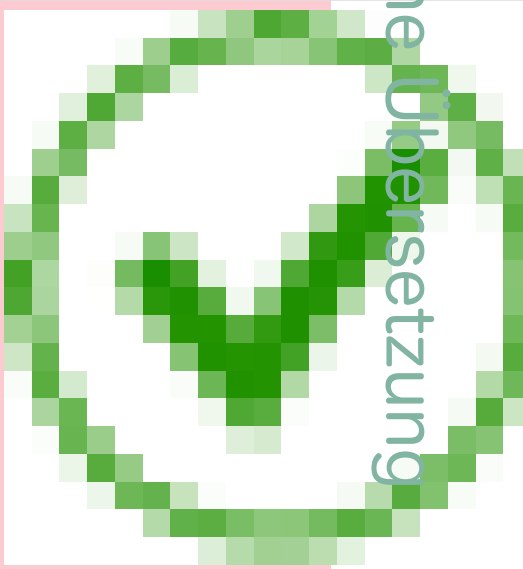
Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
(Haupt-App-Gruppe)		
Übersicht		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

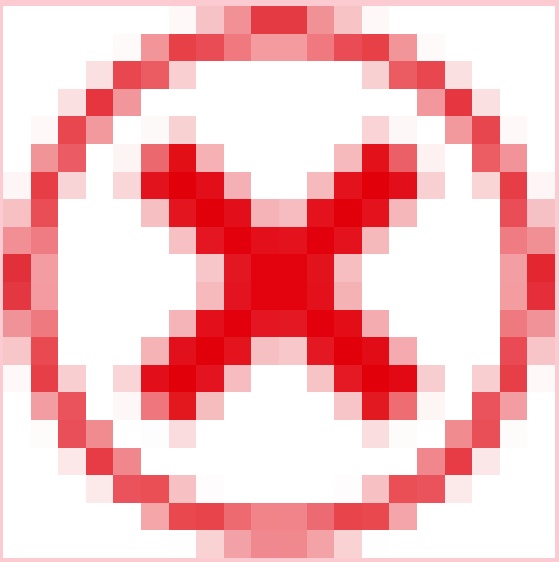
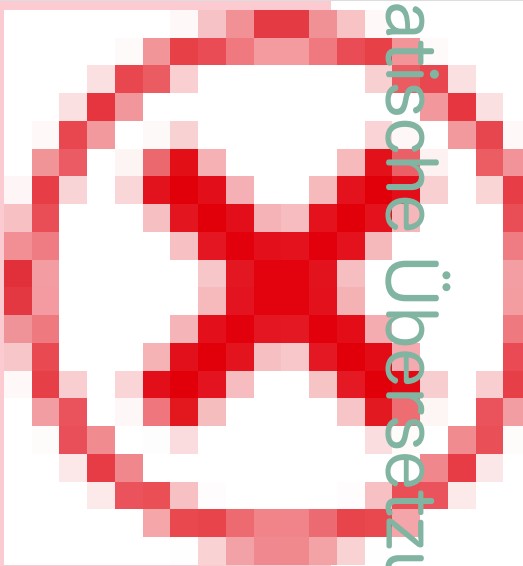
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Meine Genehmigungen		
Angreifbare Container-Elemente		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

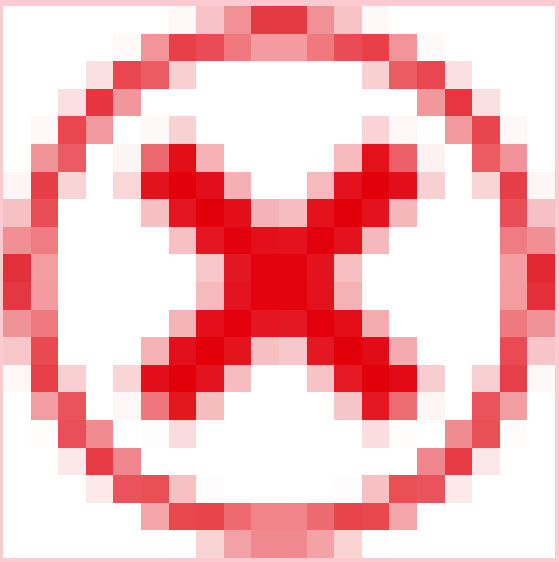
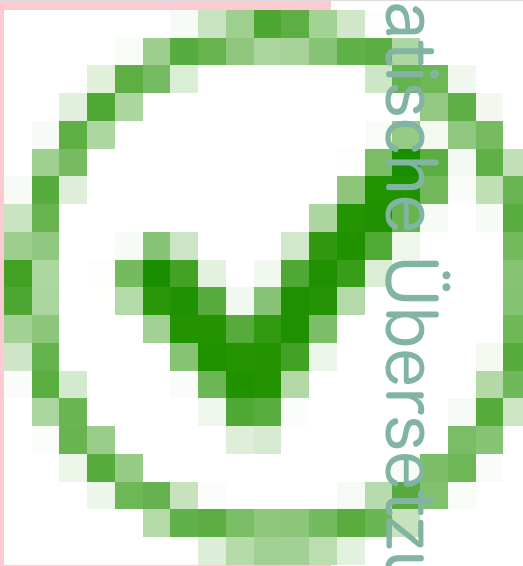
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Mir zugewiesen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

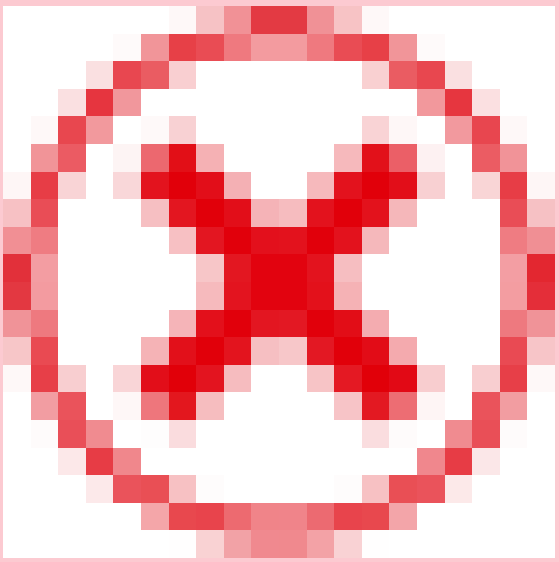
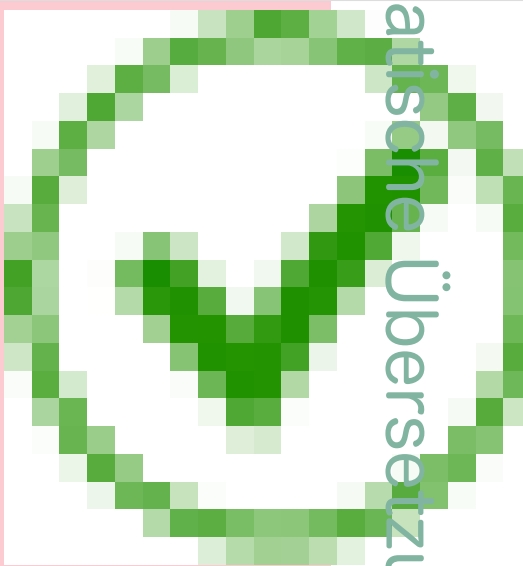
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Meinen Gruppen zugewiesen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

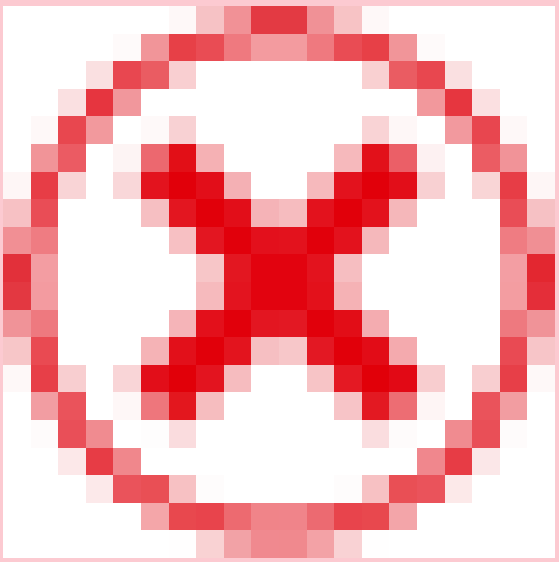
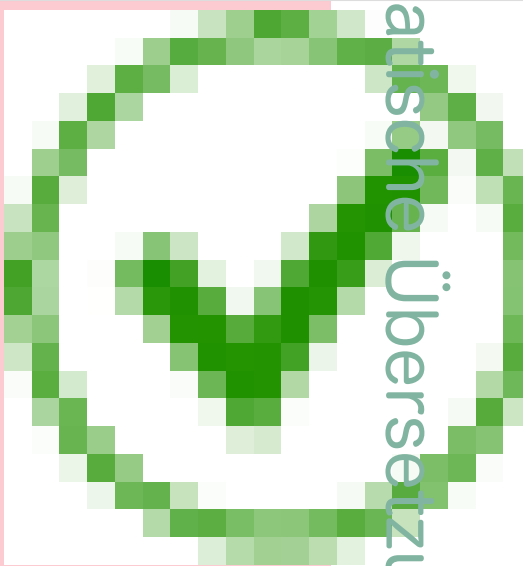
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Kritisches und hohes Risiko		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

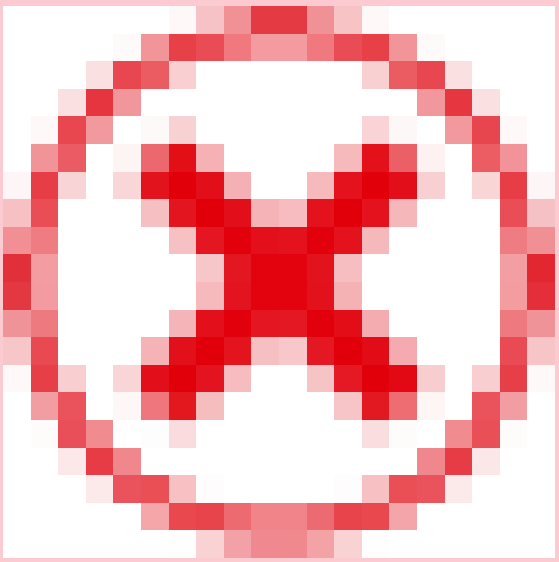
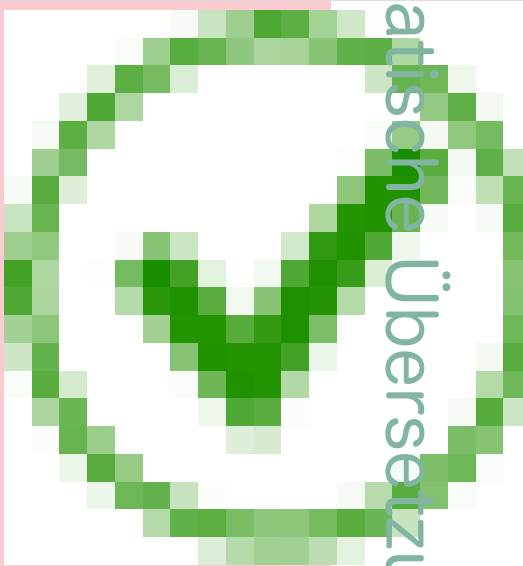
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Nutzbar		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

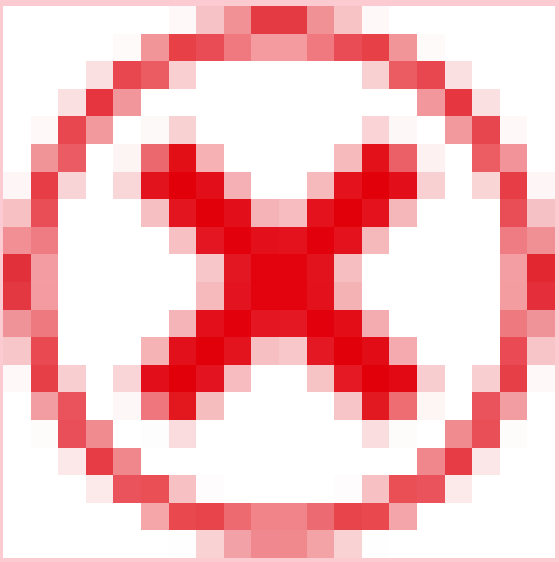
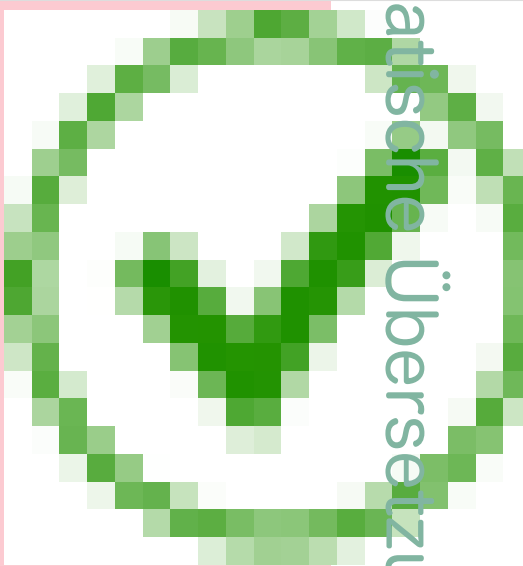
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Ziel rückt näher		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

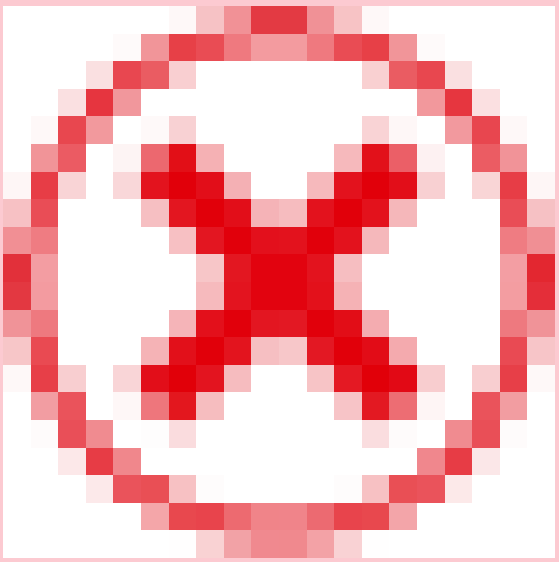
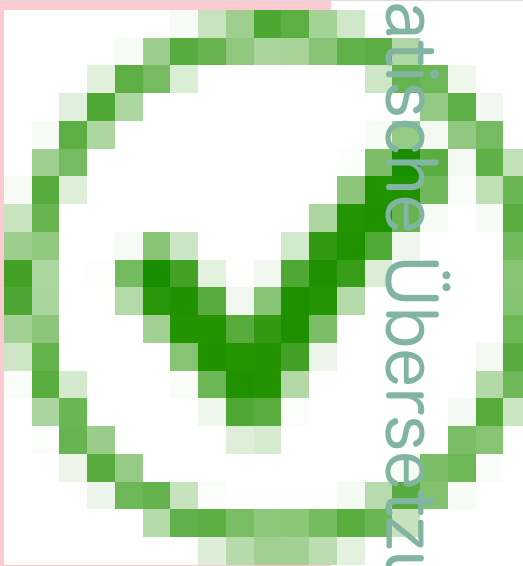
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Verfehltes Ziel		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

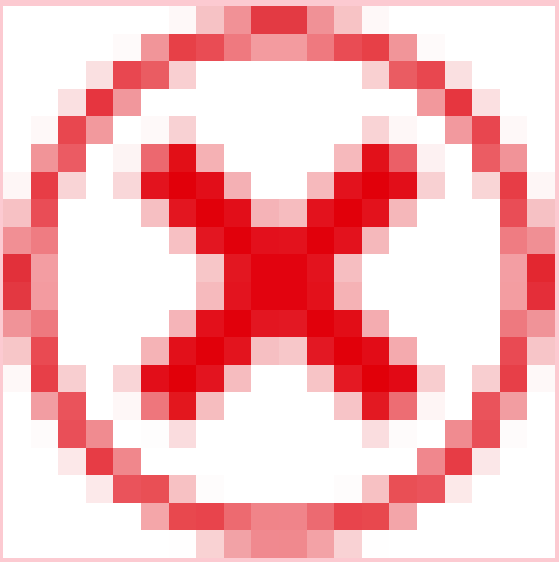
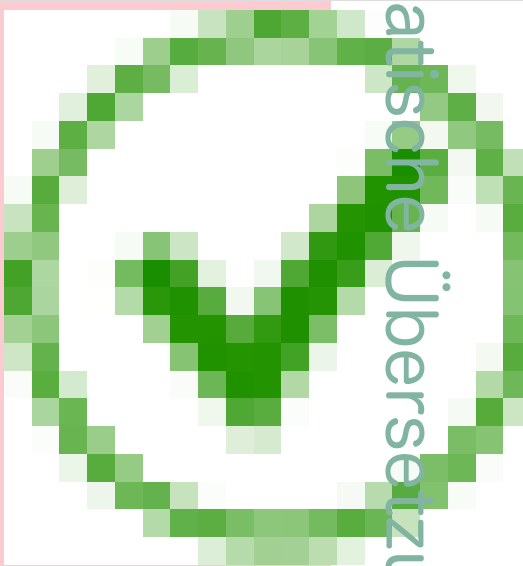
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Alle		
Bibliotheken		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

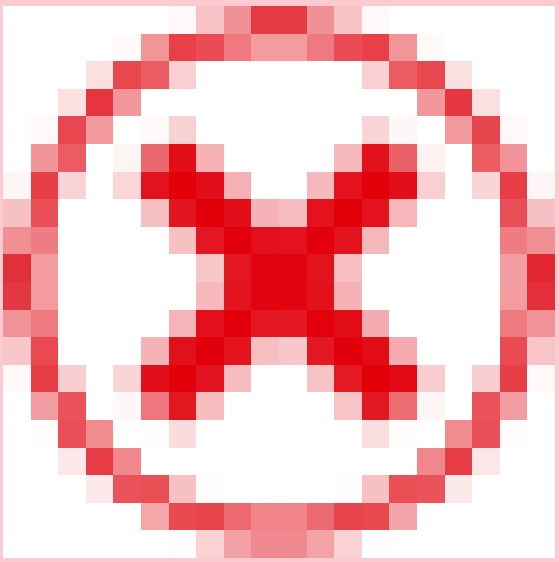
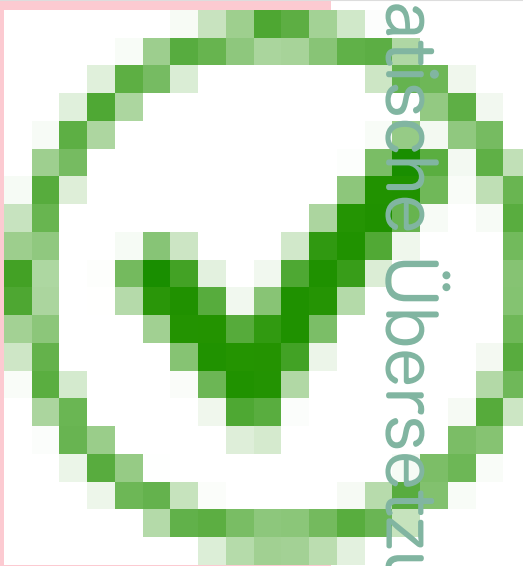
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
NVD		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

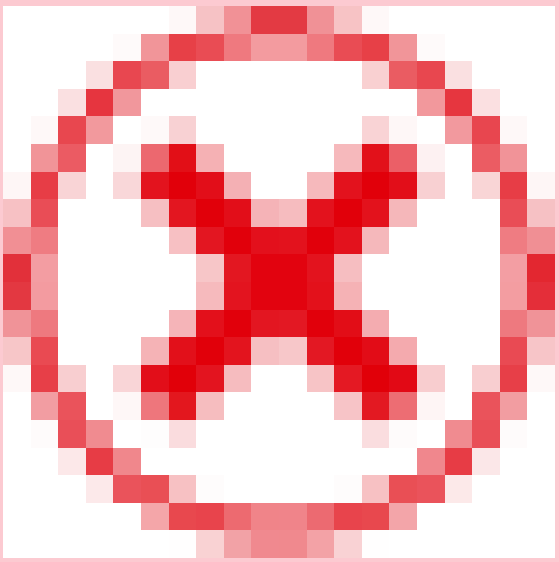
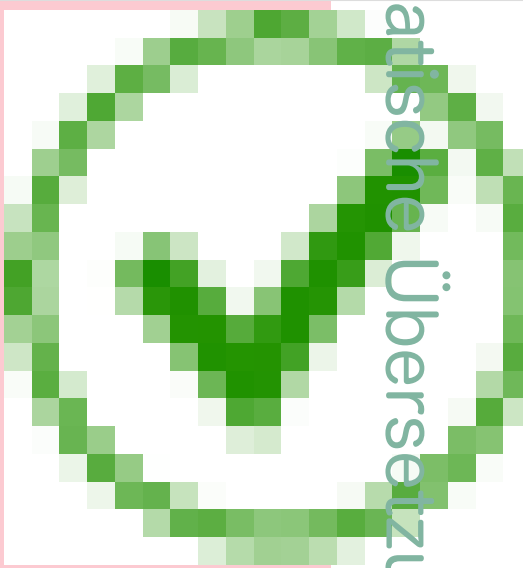
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Drittpartei		
Administration		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

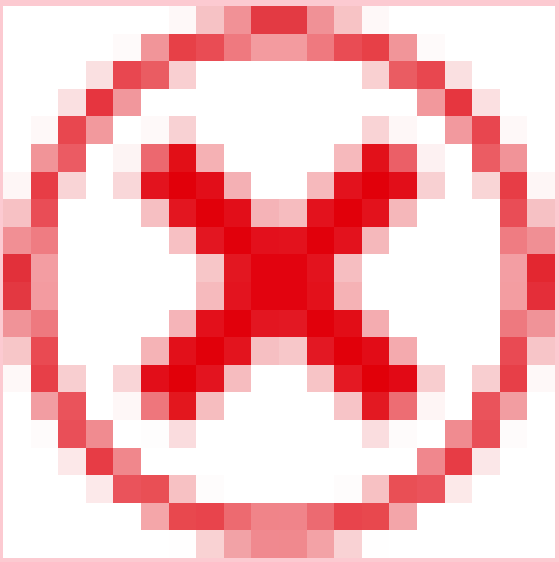
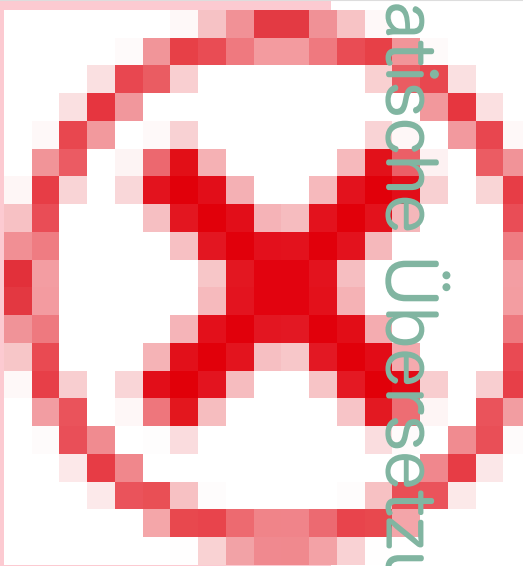
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Zuweisungsregeln		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

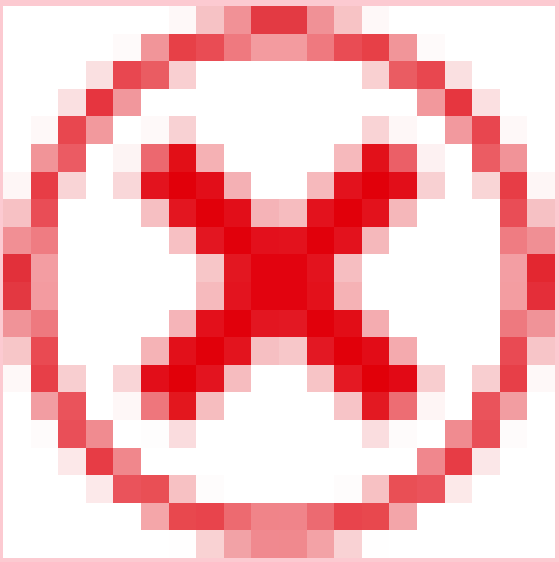
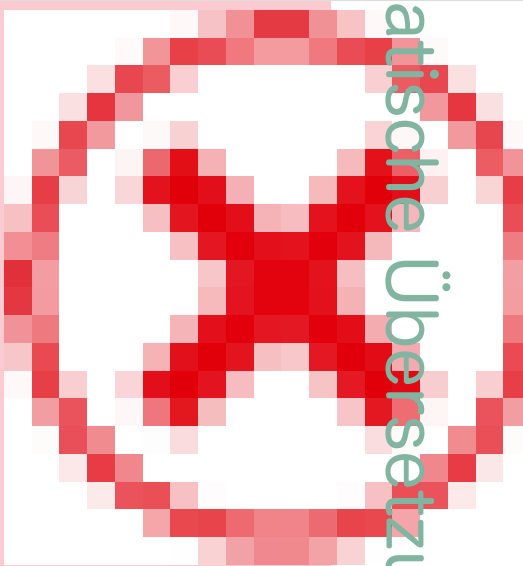
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Schwachstellen-Rechner		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

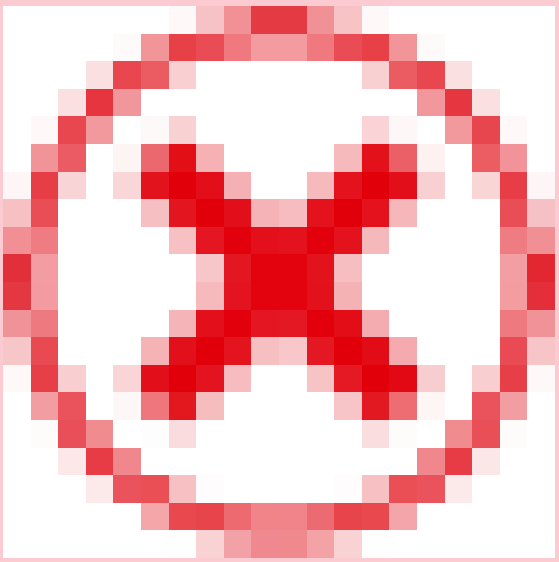
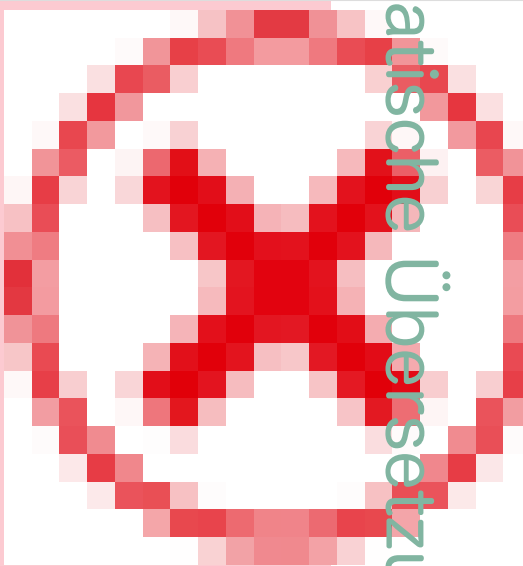
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Korrekturzielregeln		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

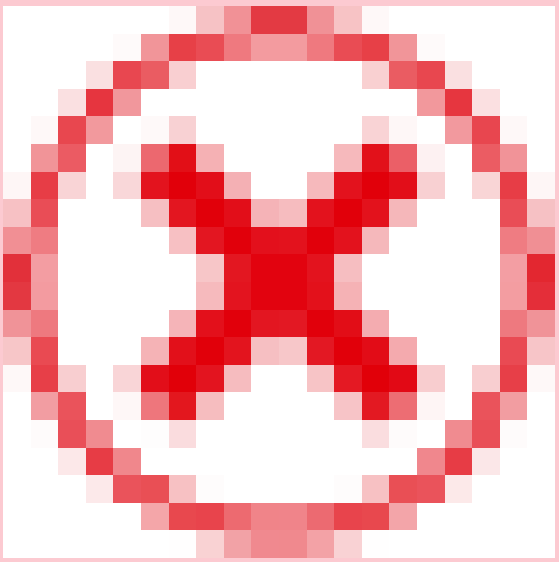
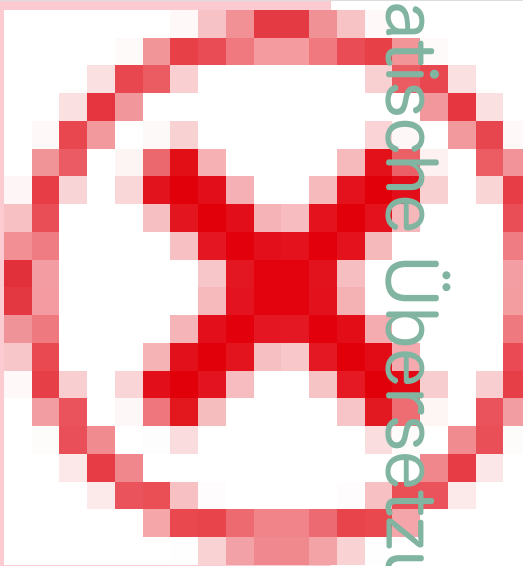
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
VI-Granularität konfigurieren		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

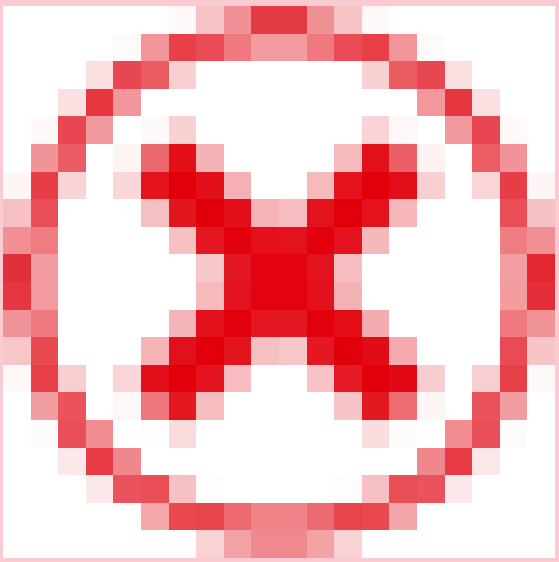
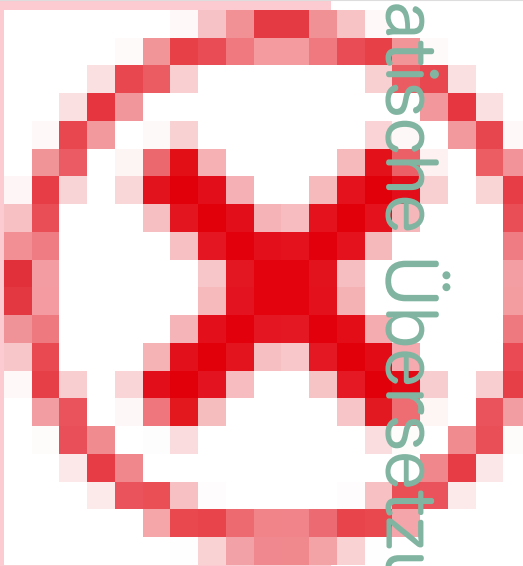
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Ausnahmeregeln		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

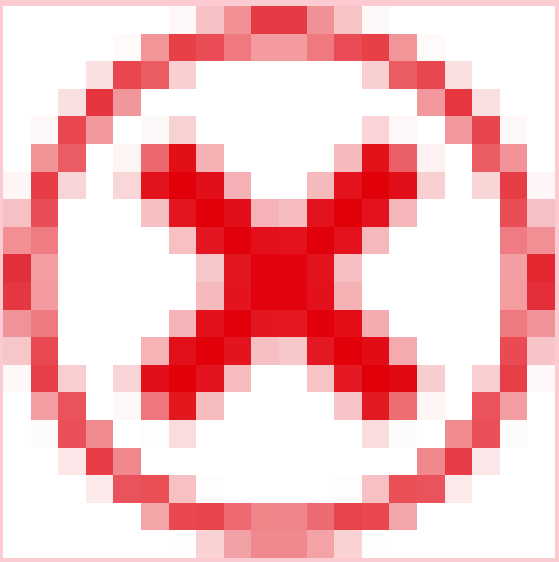
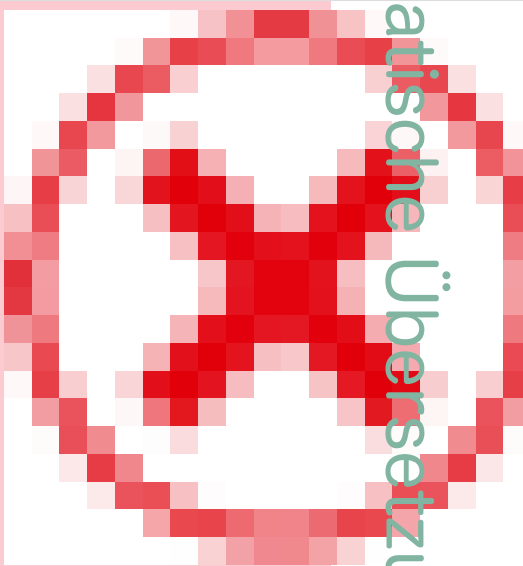
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Genehmigungsregeln		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

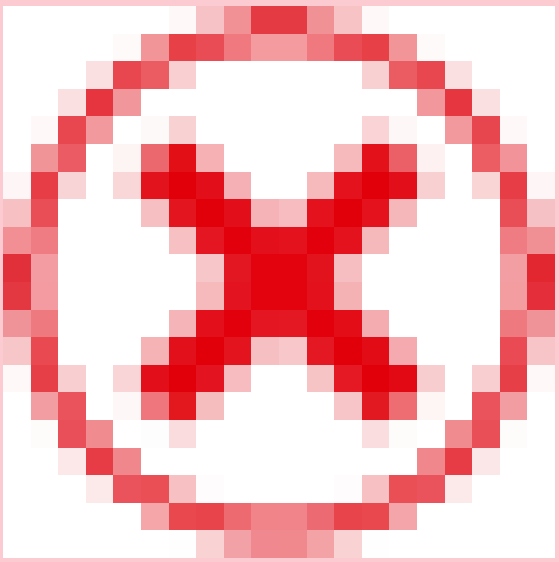
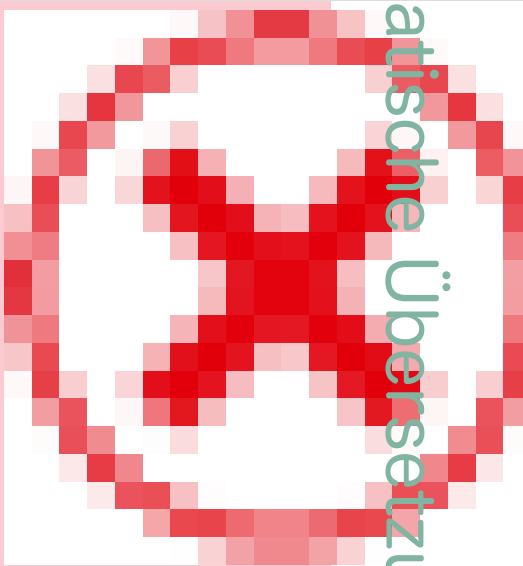
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Container-Sicherheitsintegrationen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

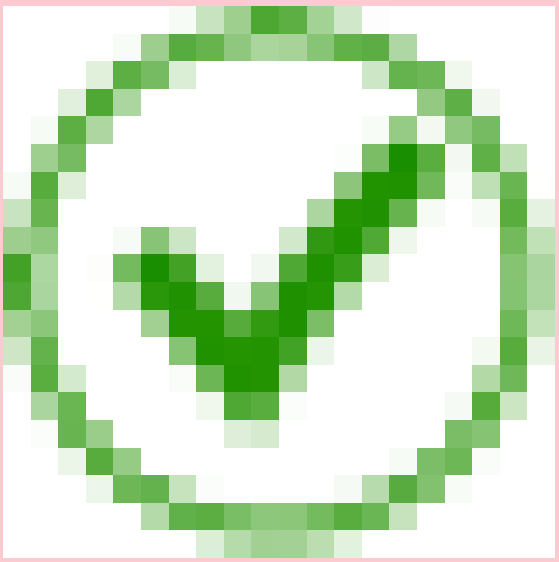
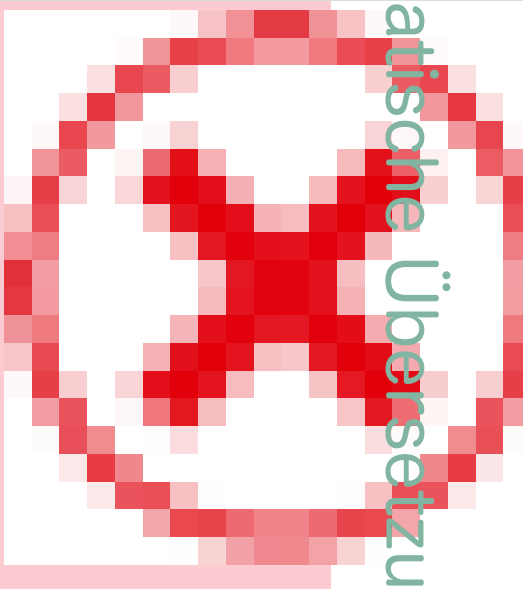
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Angreifbare Elemente automatisch schließen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

Informationen für andere Rollen:

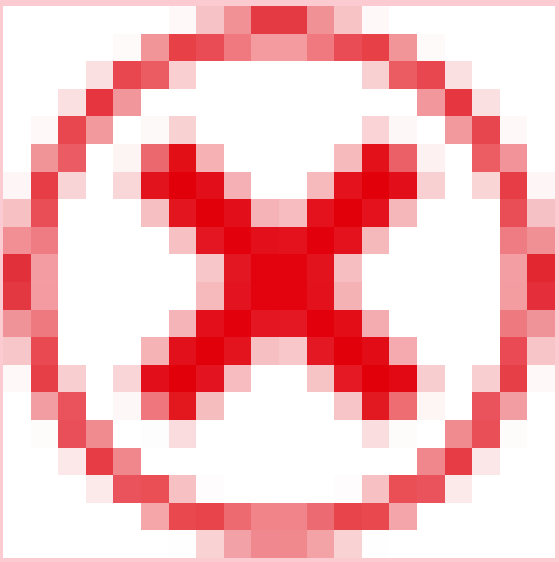
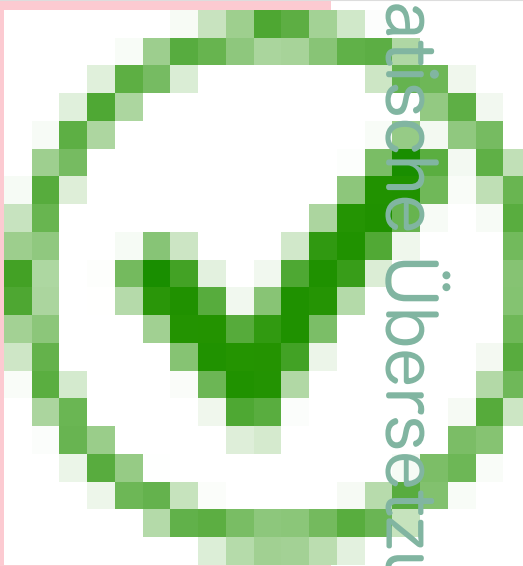
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Auto_close_stale_VI	sn_vul_Container. Manage_normalized_sever
Normalisierte Schweregradzuordnungen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

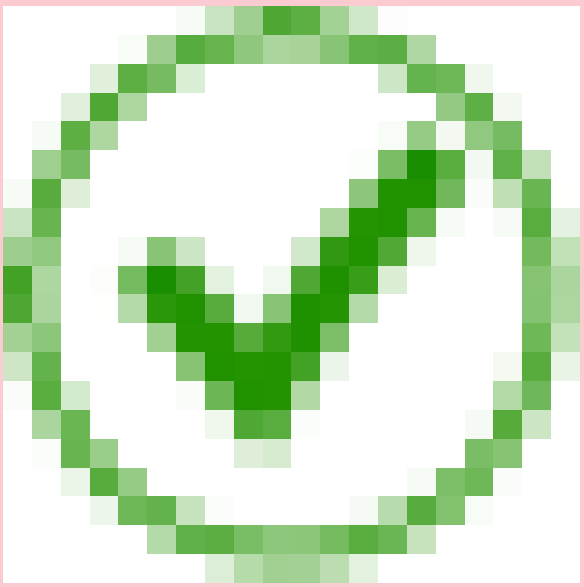
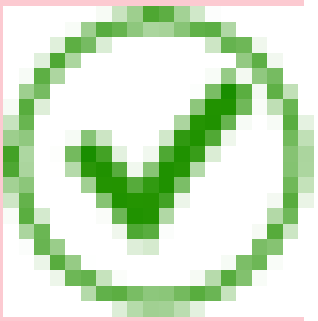
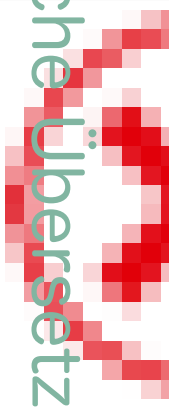
Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
(Haupt-App-Gruppe)			
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Meine Genehmigungen	✗	✗	✗
Angreifbare Container-Elemente			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Mir zugewiesen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Meinen Gruppen zugewiesen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Kritisches und hohes Risiko	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

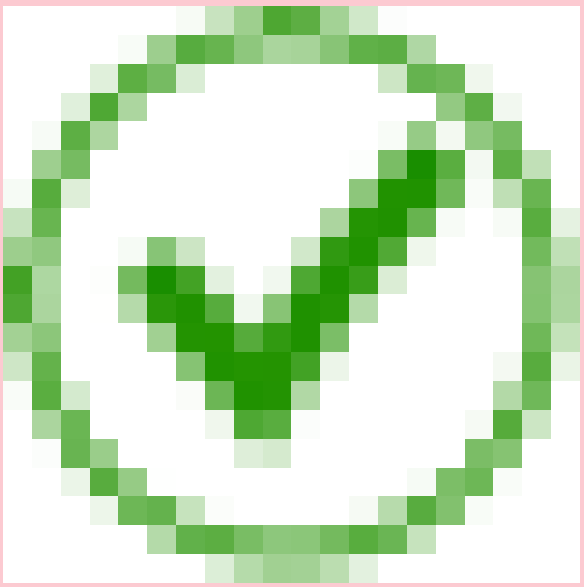
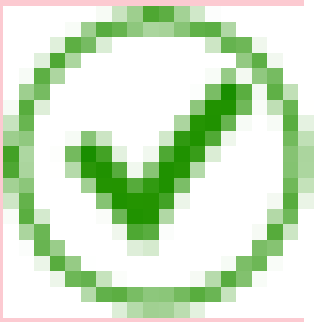
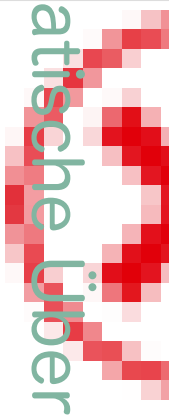
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Nutzbar			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

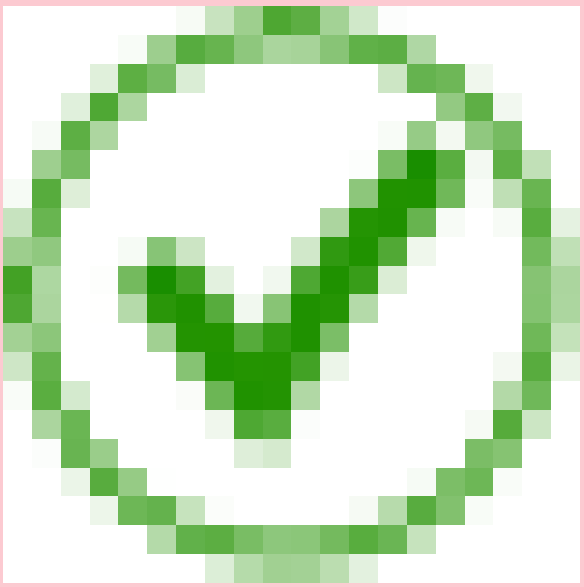
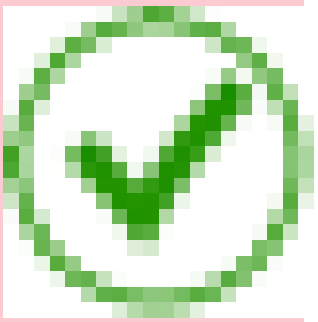
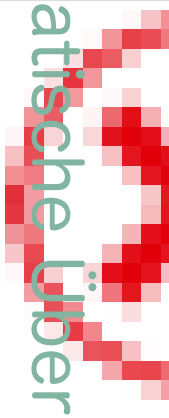
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Ziel rückt näher			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

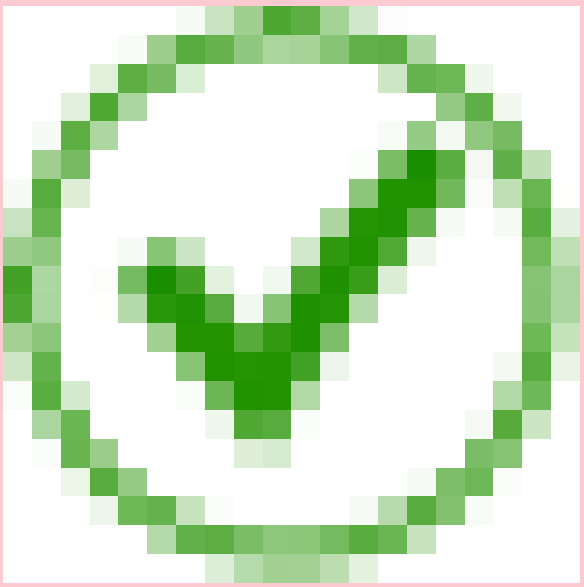
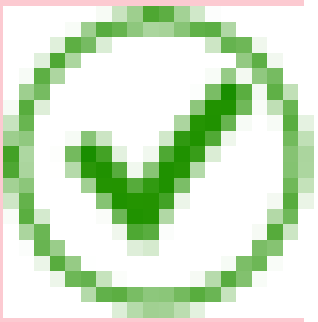
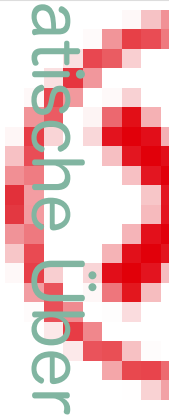
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Verfehltes Ziel			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

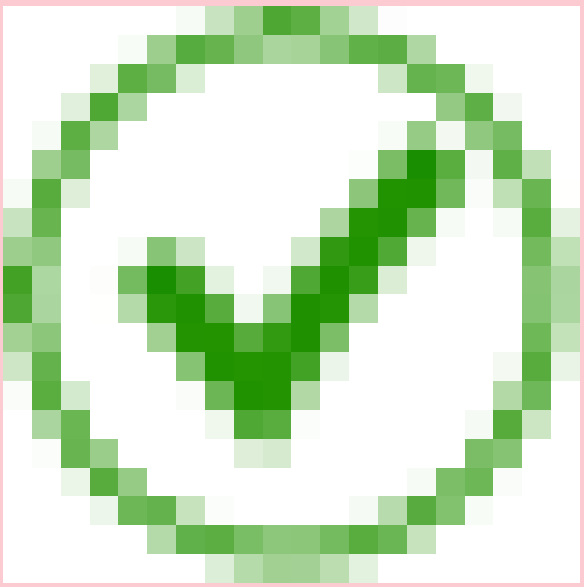
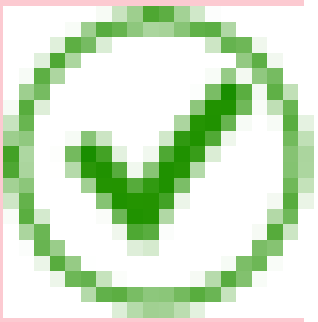
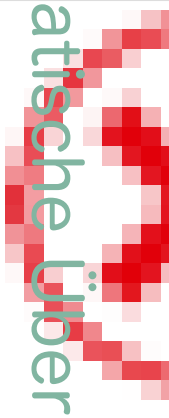
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Alle			
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

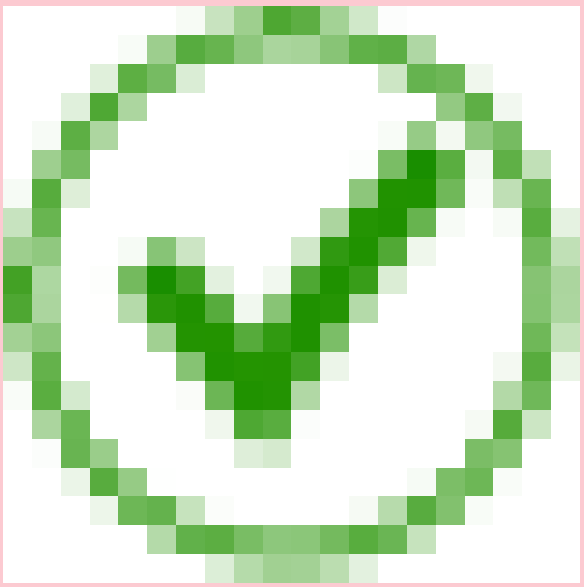
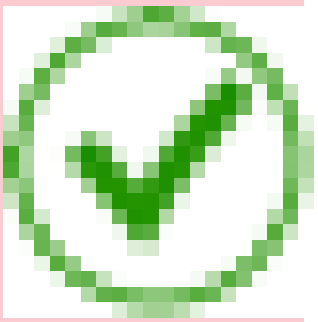
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
NVD			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

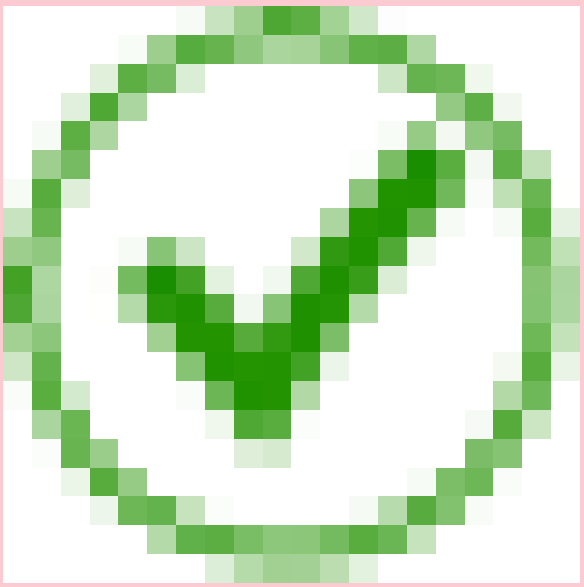
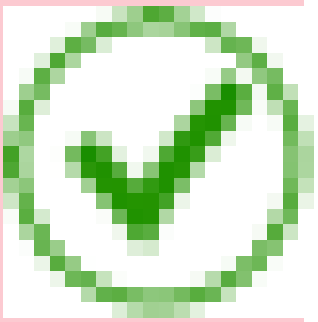
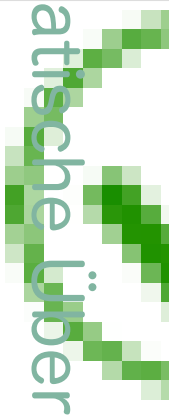
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Drittpartei			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Zuweisungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

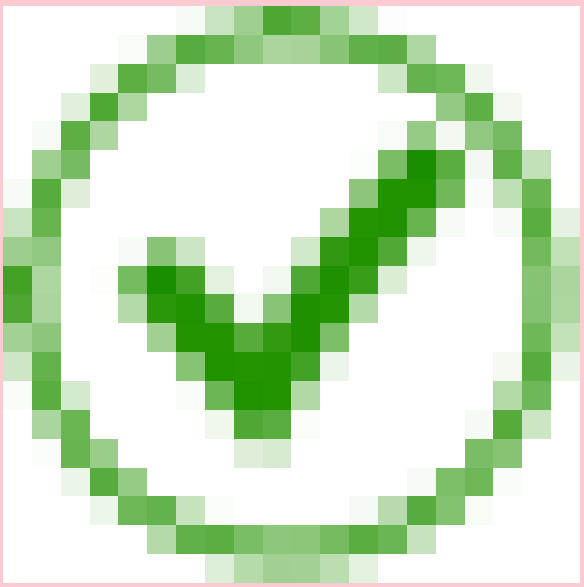
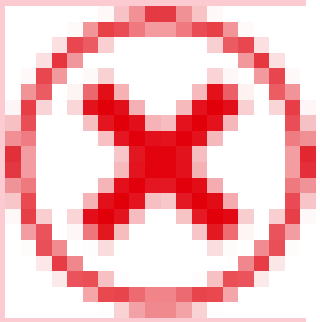
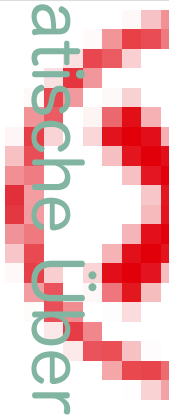
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Schwachstellen-Rechner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Korrekturzielregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

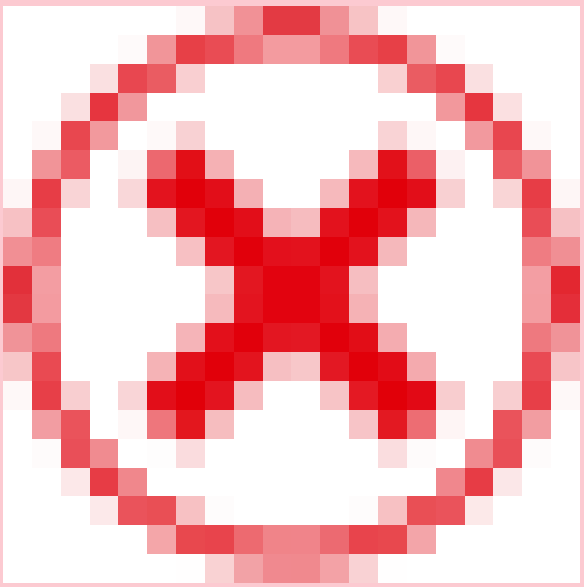
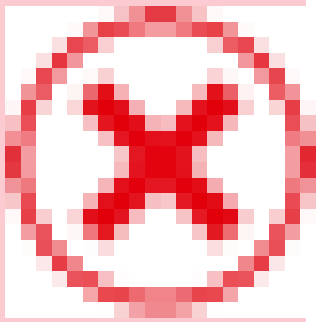
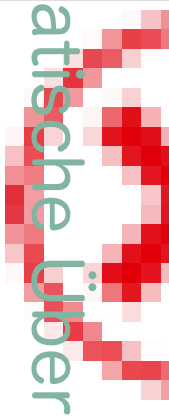
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
VI-Granularität konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

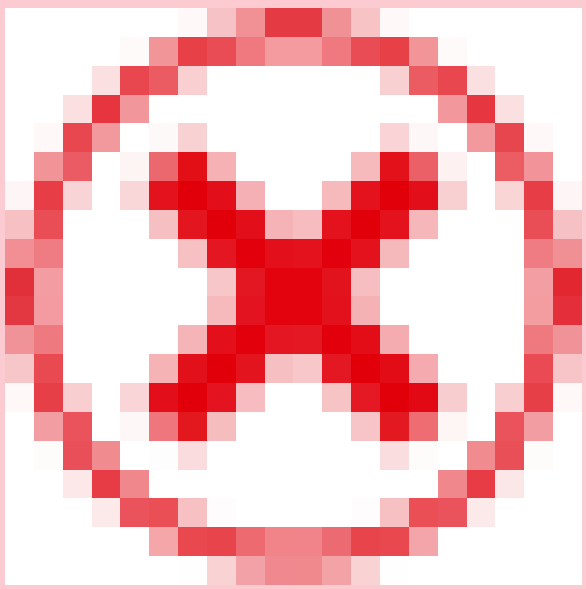
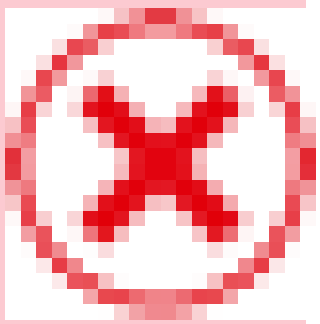
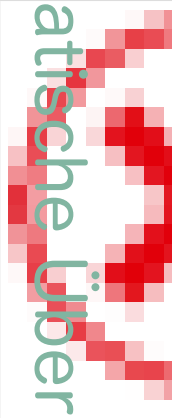
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Ausnahmeregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

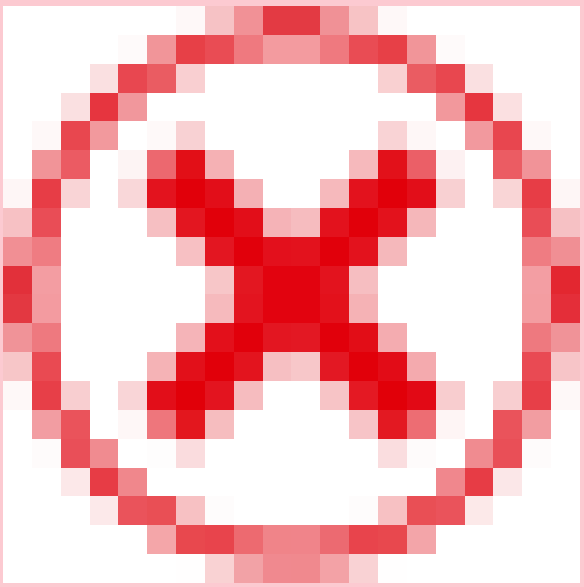
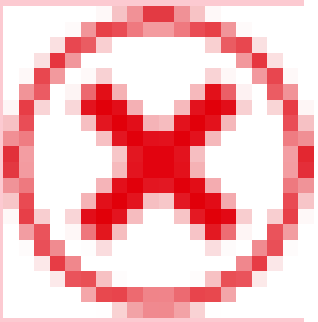
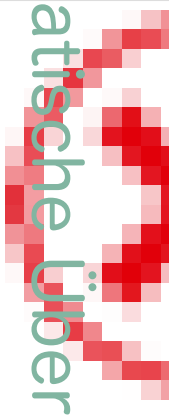
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Genehmigungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

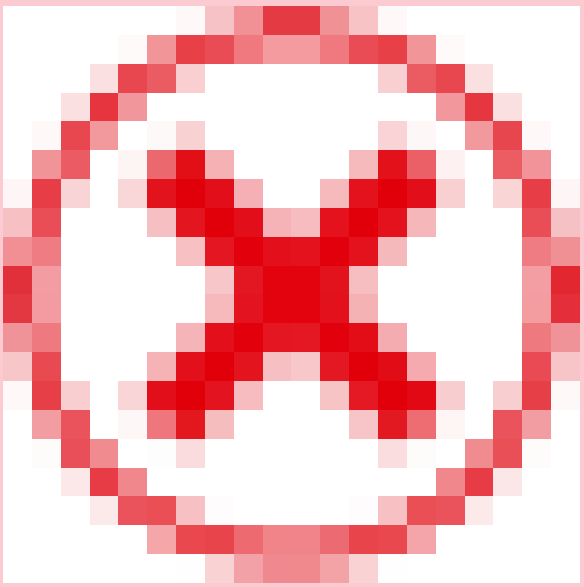
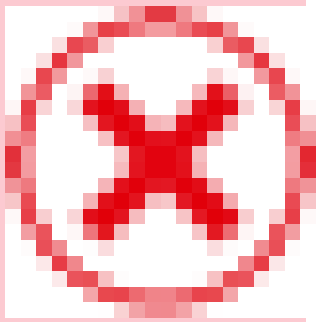
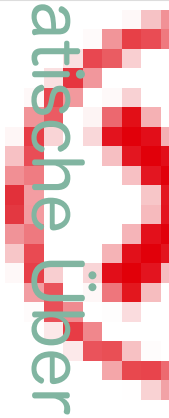
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Container-Sicherheitsintegrationen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

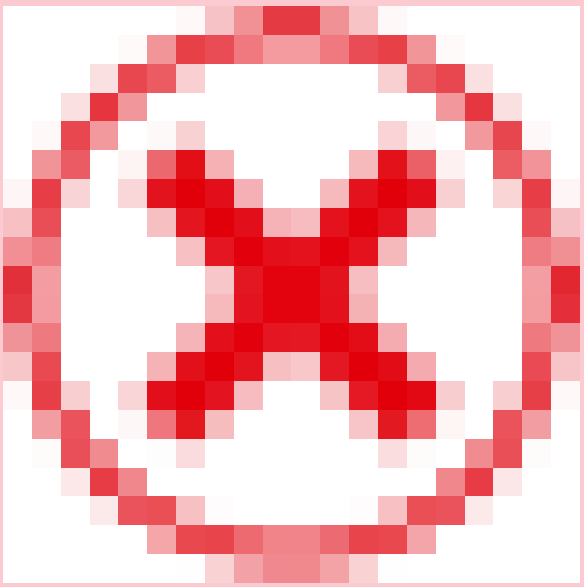
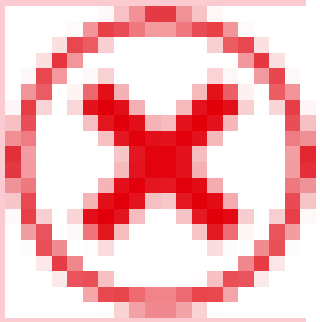
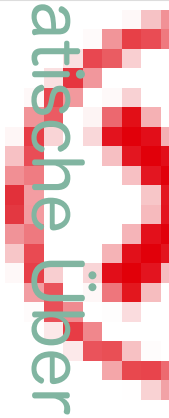
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Angreifbare Elemente automatisch schließen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Informationen für andere Rollen:

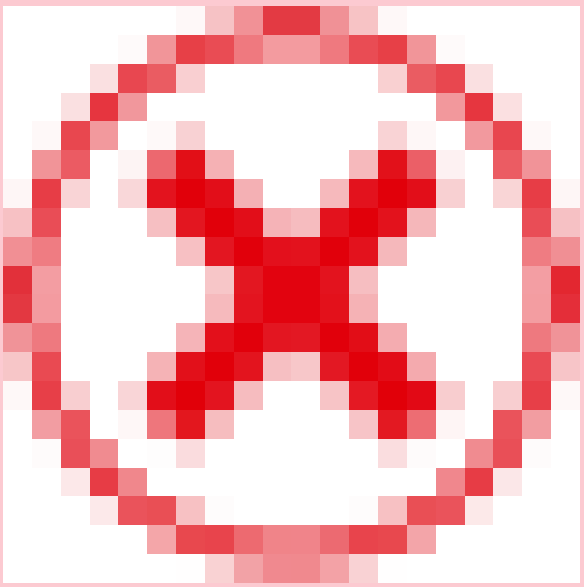
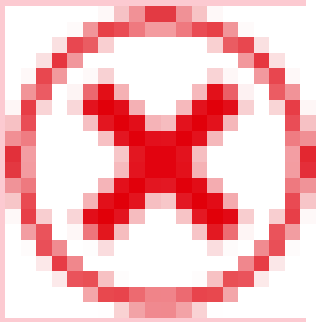
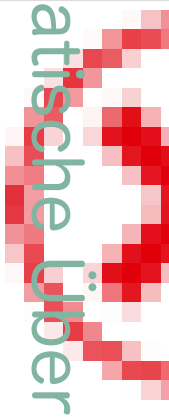
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.read_Auto_Exception_rule

(Fortsetzung)

Modul	sn_vul_Container. Manage_Risk_Score_Configuration	sn_vul_Container. Read_all	sn_vul_Contai
Normalisierte Schweregradzuordnungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

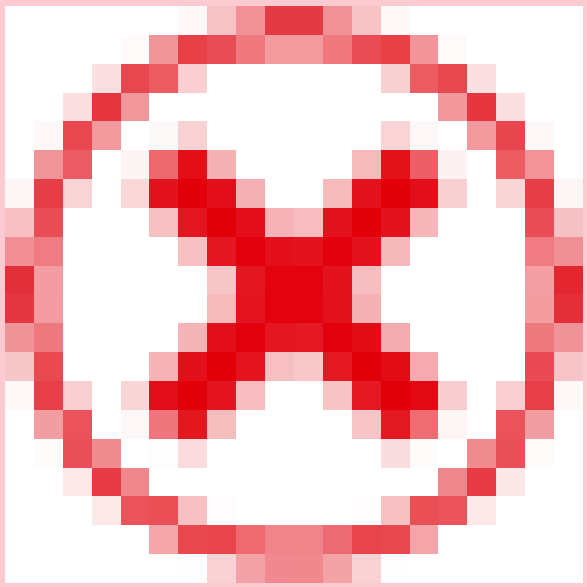
Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

Modul	sn_vul_Container. Read_Auto_Exception_rule
(Haupt-App-Gruppe)	
Übersicht	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

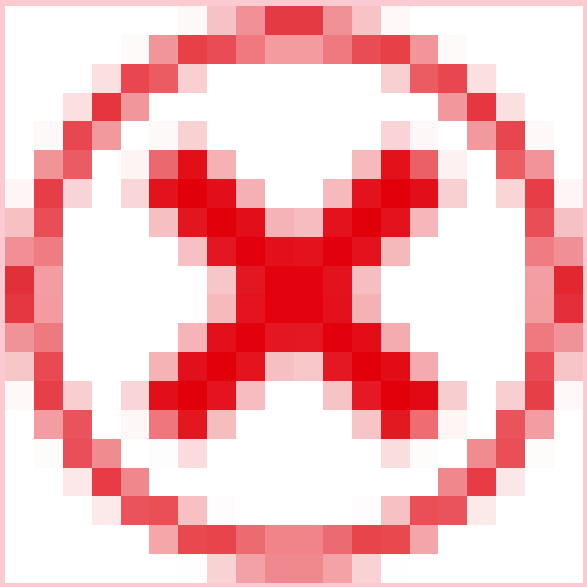
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Meine Genehmigungen	
Angreifbare Container-Elemente	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

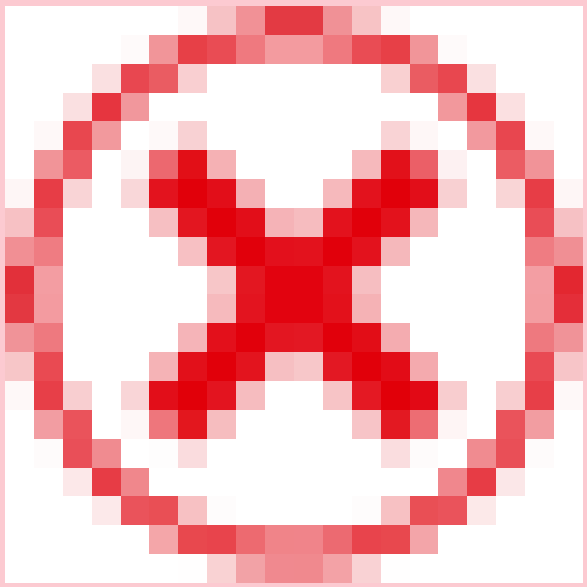
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Mir zugewiesen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

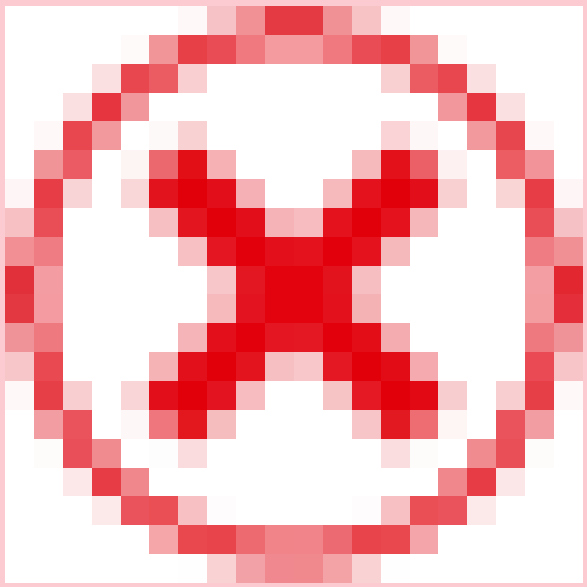
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Meinen Gruppen zugewiesen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

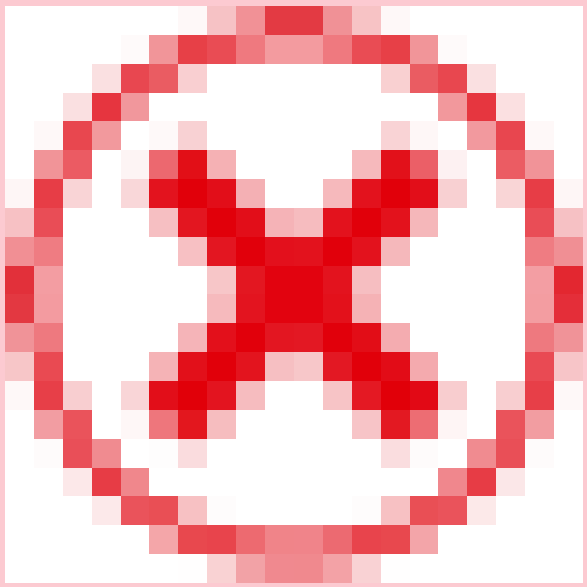
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Kritisches und hohes Risiko	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

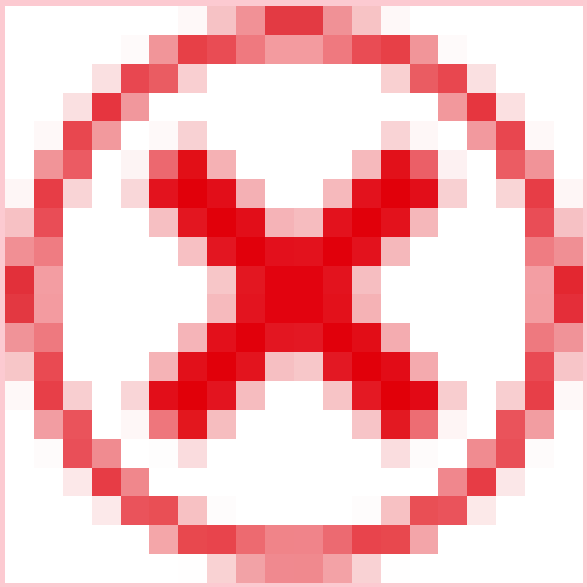
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Nutzbar	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

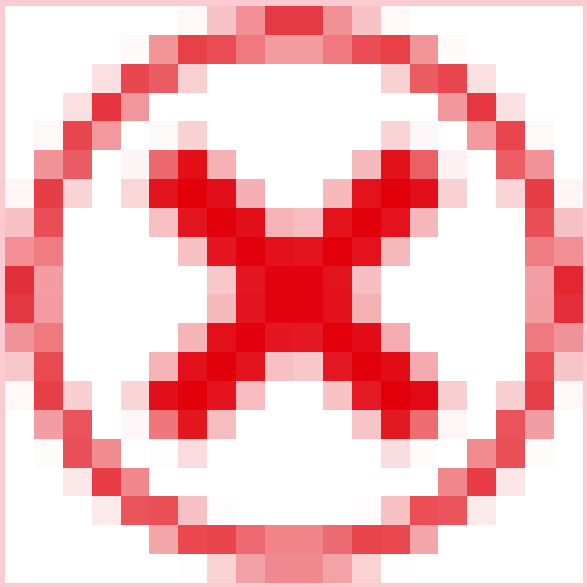
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Ziel rückt näher	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

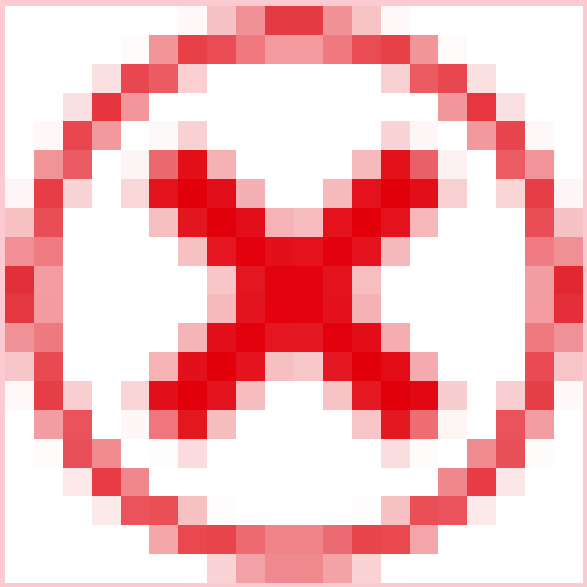
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Verfehltes Ziel	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

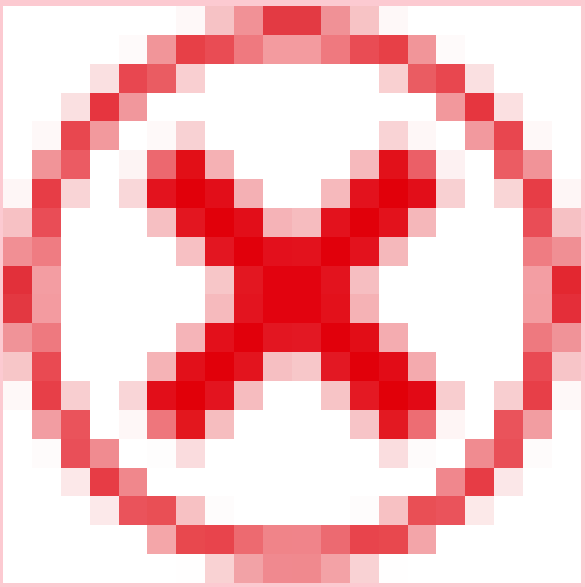
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Alle	
Bibliotheken	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

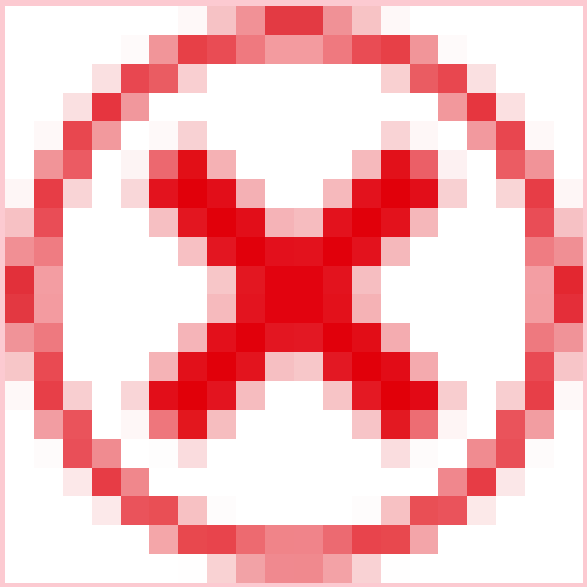
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
NVD	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

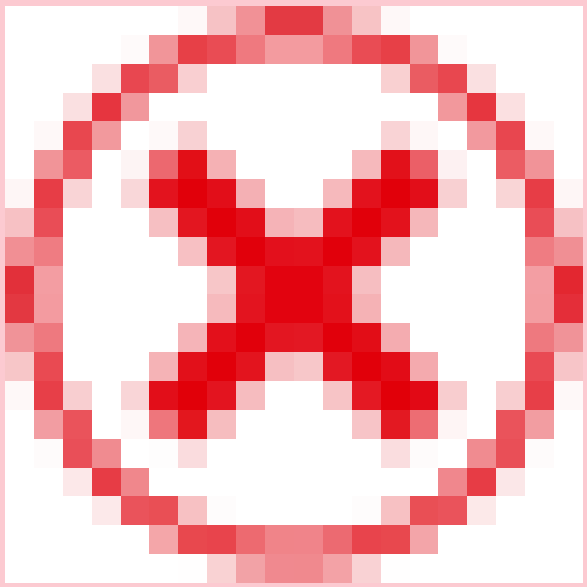
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Drittpartei	
Administration	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

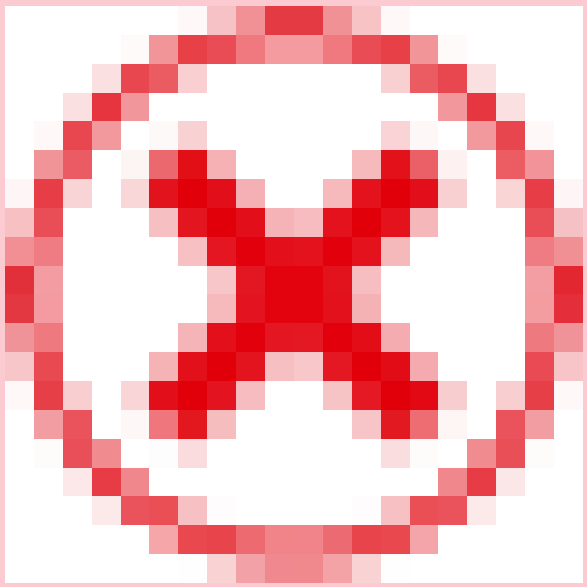
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Zuweisungsregeln	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

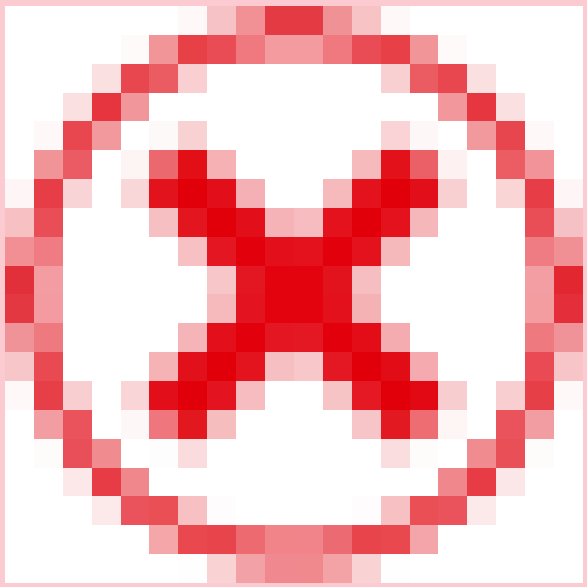
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Schwachstellen-Rechner	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

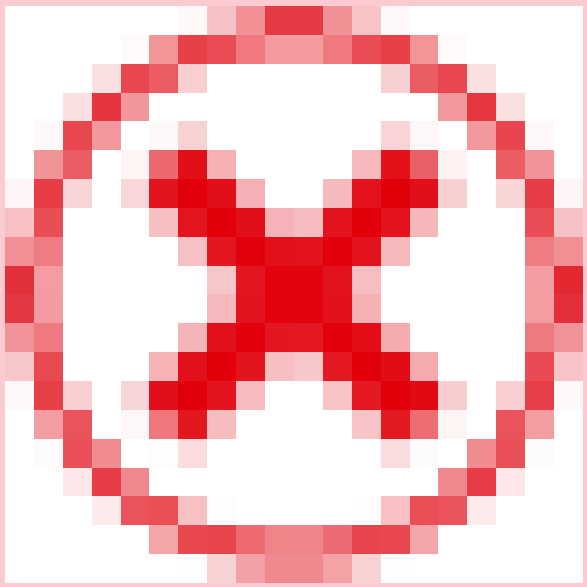
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Korrekturzielregeln	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

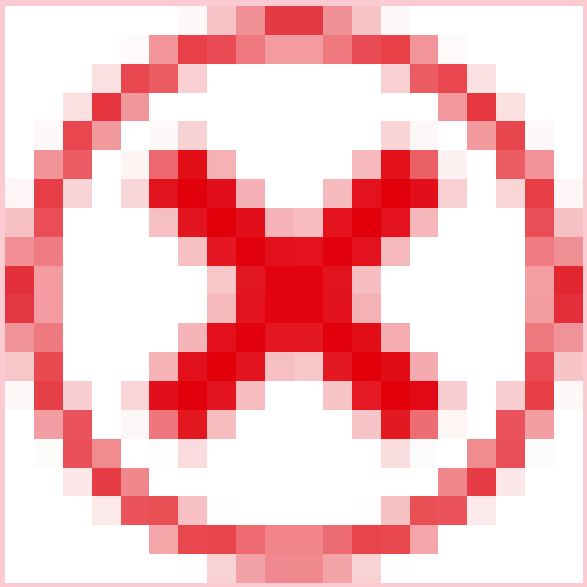
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
VI-Granularität konfigurieren	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Ausnahmeregeln	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

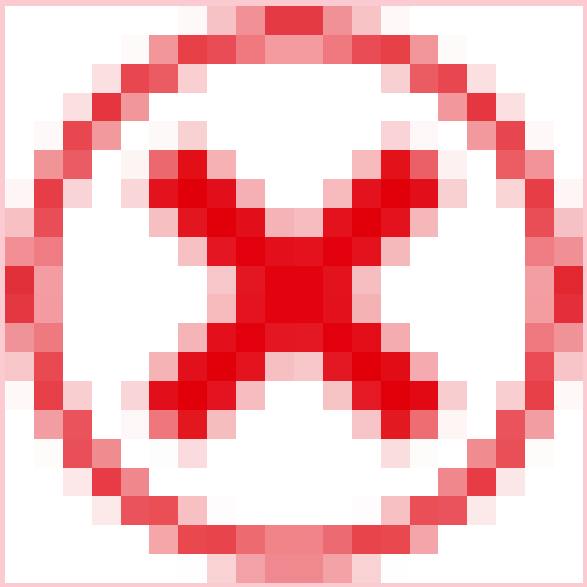
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Genehmigungsregeln	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

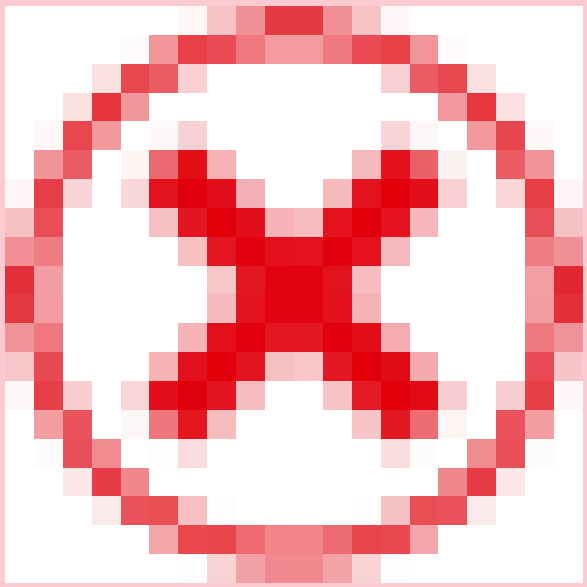
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Container-Sicherheitsintegrationen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

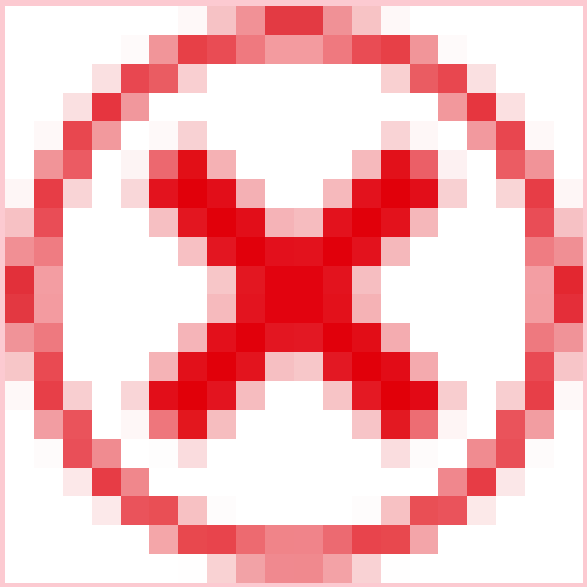
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Angreifbare Elemente automatisch schließen	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul_Container.read_Auto_Exception_rule

Informationen für andere Rollen:

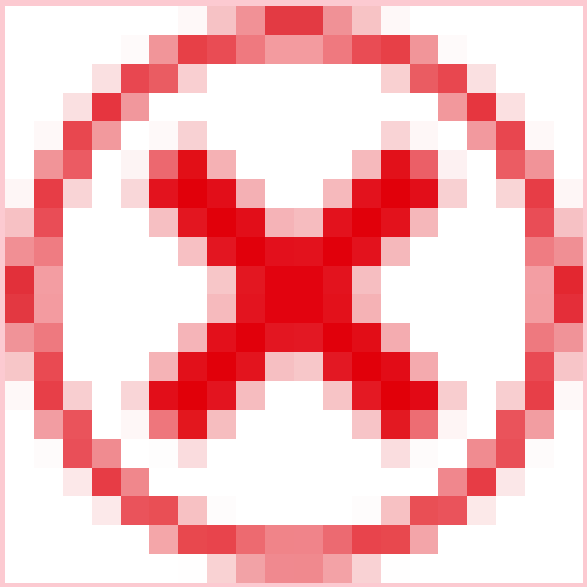
sn_sec_cmn.Manage_Approval_rules, sn_vul_Container.configure_Integrations, sn_vul_Container.configure_VI_granularity

sn_vul_Container.Exception_Approver, sn_vul_Container.false_positive_Approver, sn_vul_Container.Manage_assignment_rules

sn_vul_Container.Manage_Auto_close_stale_VI, sn_vul_Container.Manage_normalized_severity, sn_vul_Container.Manage_Remediation_target_rules

sn_vul_Container.Manage_Risk_Score_Configuration, sn_vul_Container.read_all, sn_vul_Container.read_assigned

(Fortsetzung)

Modul	sn_vul_Container. Read_Auto_Exception_rule
Normalisierte Schweregradzuordnungen	

[End]

[store-future: BEGIN review]

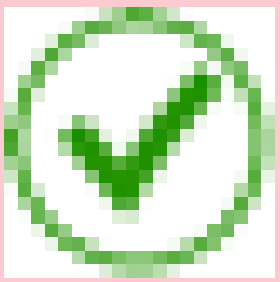
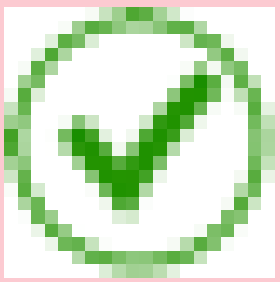
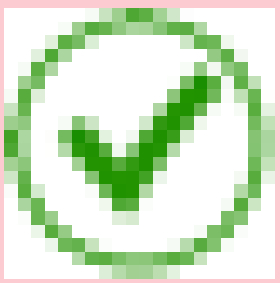
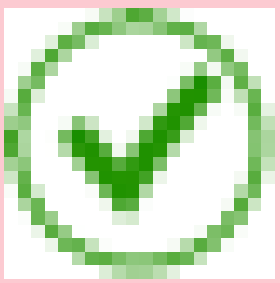
Modulzugriff nach Rolle für DLP-Administration

Informationen zur DLP-Administration finden Sie in den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

Modul	sn_dlir. Analyst
(Haupt-App-Gruppe)	

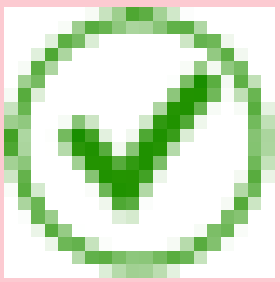
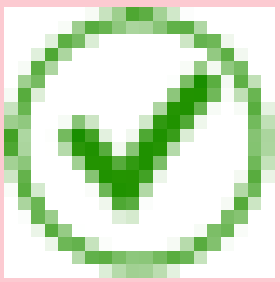
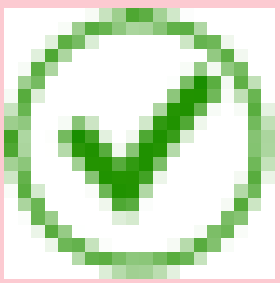
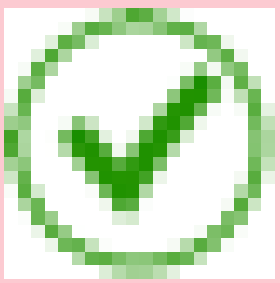
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_dlir. Analyst
Standardkonfiguration	
Zuweisungsregeln	
Regeln für Fälligkeitsdatum der Antwort	
E-Mail-Vorlagen	
Bewertungen	
Optionen für die Reaktion auf Incidents	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_dlir. Analyst
Konfiguration des Altersdiagramms	
Delegierten-Konfiguration	
Anwenderdefinierte Status	
Regeln zur Identifizierung von Wiederholungsvergehen	
Anwenderdefinierte Felder	
Erweiterte Einstellungen	
Incident-Zugriffsbeschränkungen	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

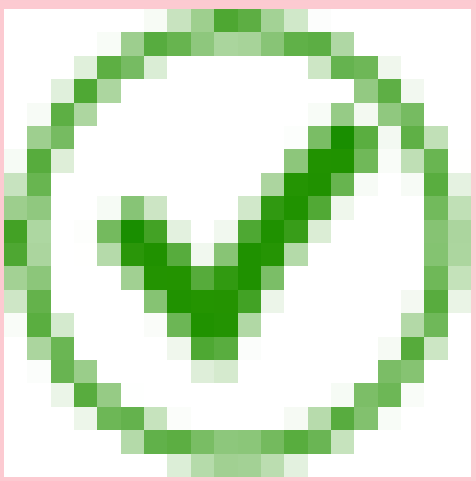
Modul	sn_dlir. Analyst
Einschränkungen auf Datensatzebene	
Einschränkungen auf Feldebene	

[End]

[store-future: BEGIN review]

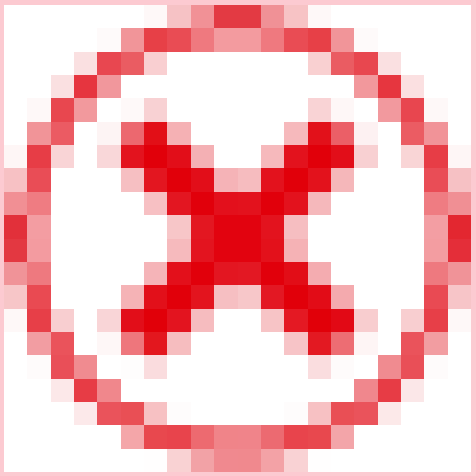
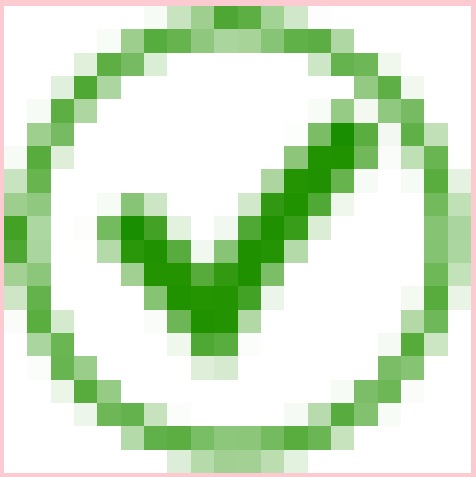
Modulzugriff nach Rolle für DLP-Incident-Management

Informationen zum DLP-Incident-Management finden Sie in den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

Modul	sn_dlir. Analyst
(Haupt-App-Gruppe)	
DLP-Ops-Portal	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_dlir. Analyst
DLP-Endanwenderportal	
DLP-Dashboard	

[End]

[store-future: BEGIN review]

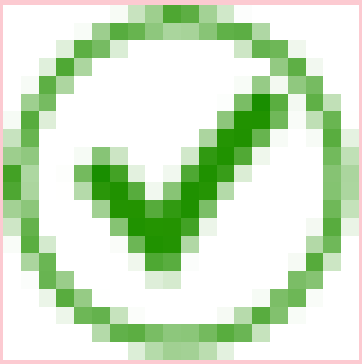
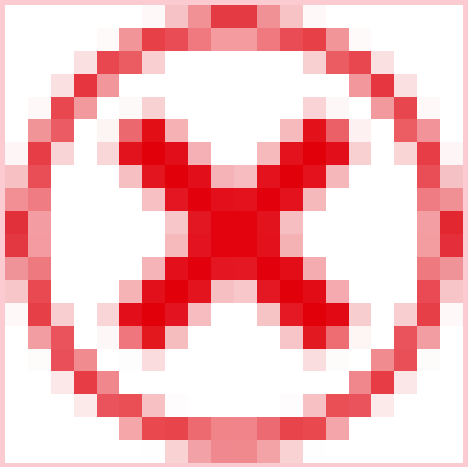
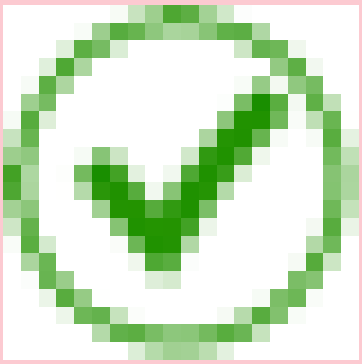
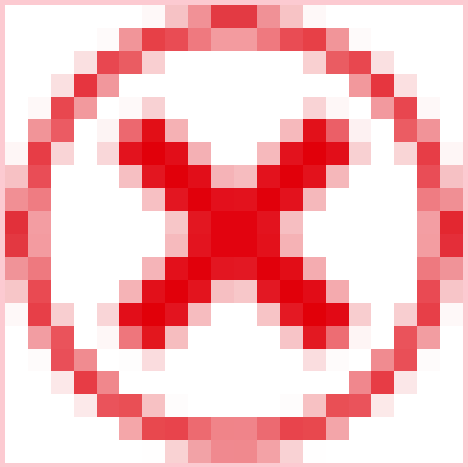
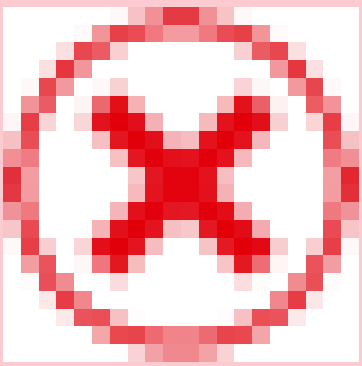
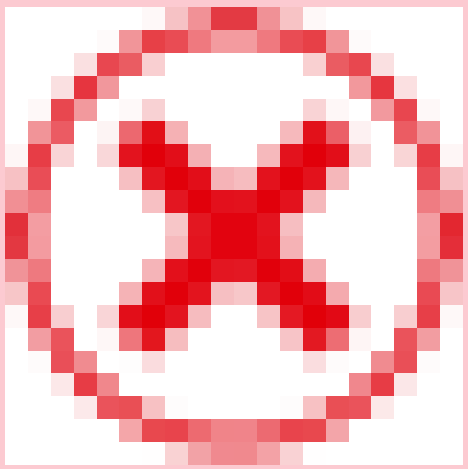
Modulzugriff nach Rolle für Datenzertifizierung

Informationen zur Datenzertifizierung finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modul	certification_admin	certification_filter_admin
(Haupt-App-Gruppe)		

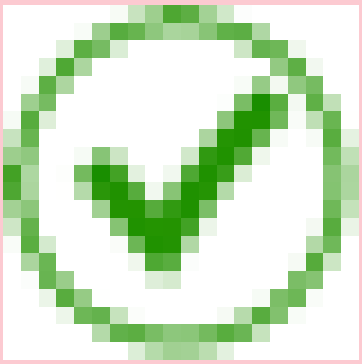
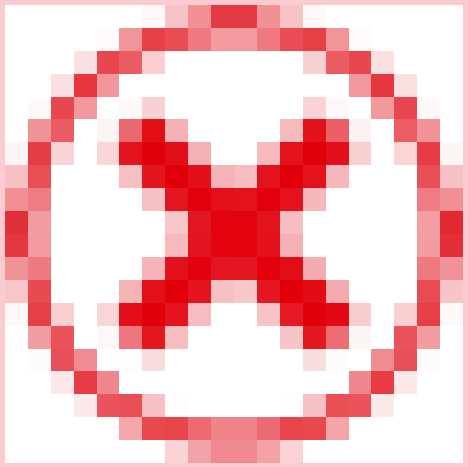
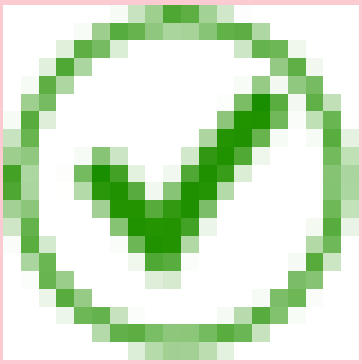
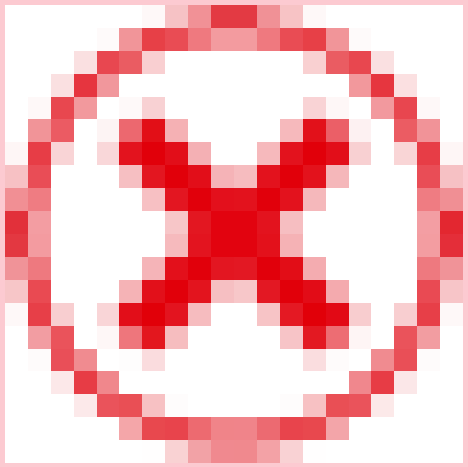
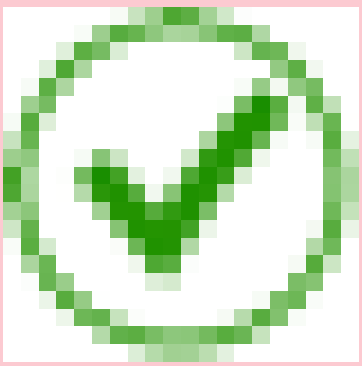
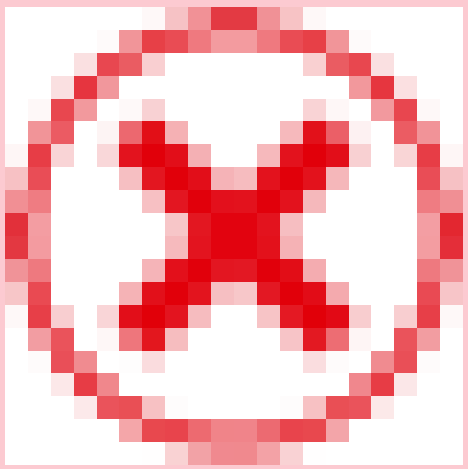
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	certification_admin	certification_filter_admin
Übersicht		
Erste Schritte		
Aufgaben		
Meine Aufgaben		

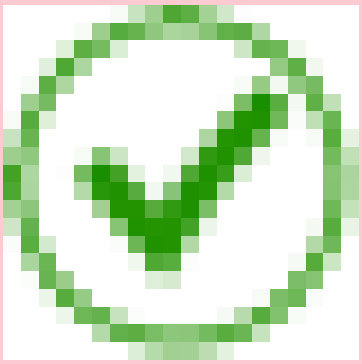
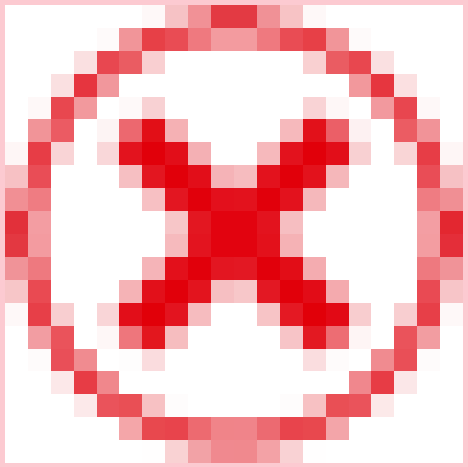
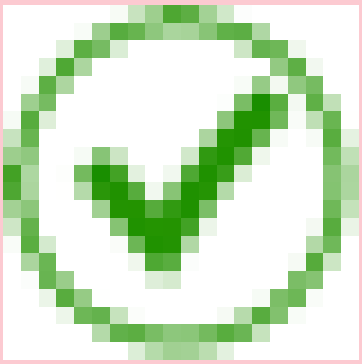
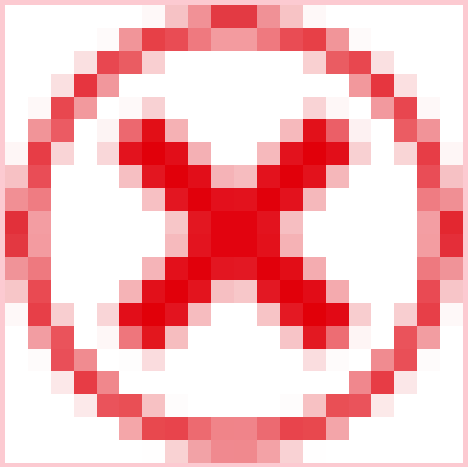
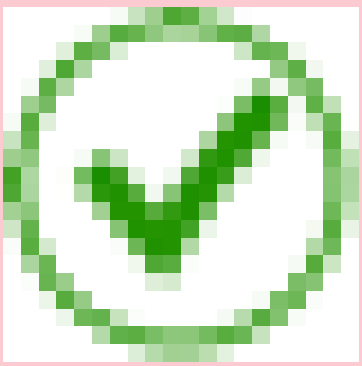
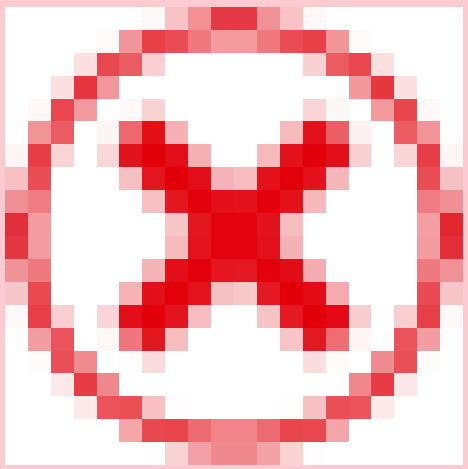
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	certification_admin	certification_filter_admin
Öffnen		
Alle Aufgaben		
Zertifizierungen		
Zertifiziert		

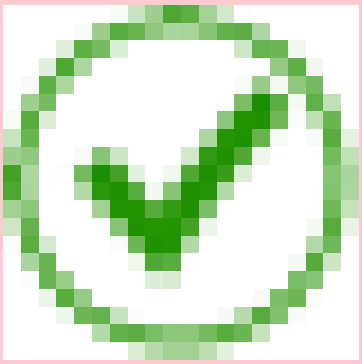
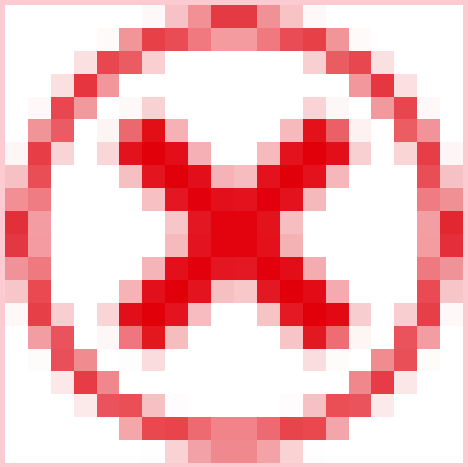
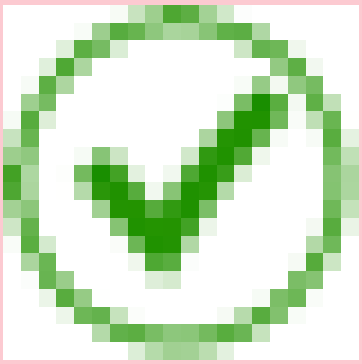
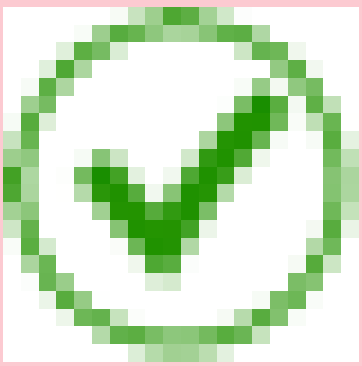
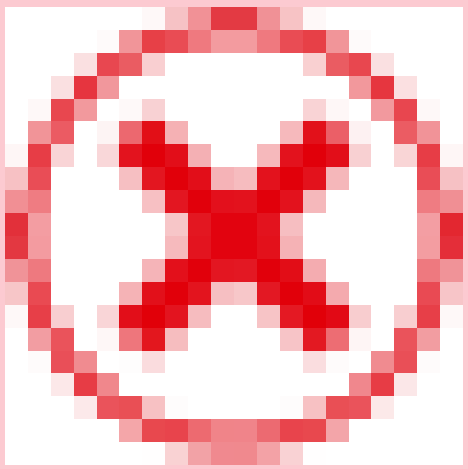
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	certification_admin	certification_filter_admin
Ausstehend		
Alle		
Zeitpläne		
Neu erstellen		

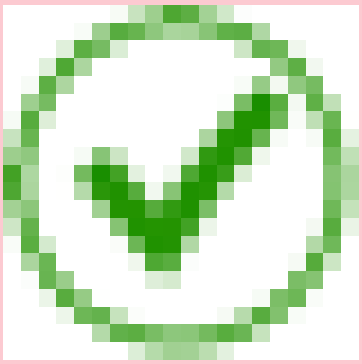
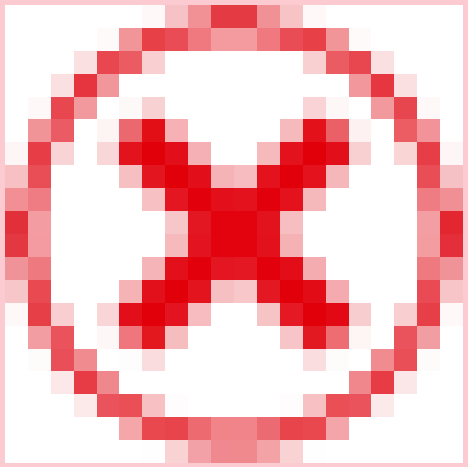
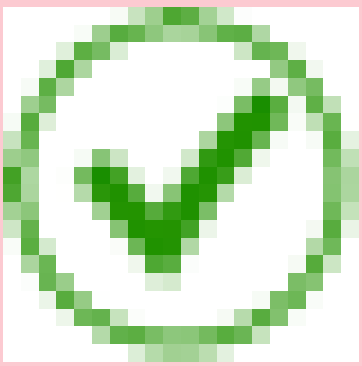
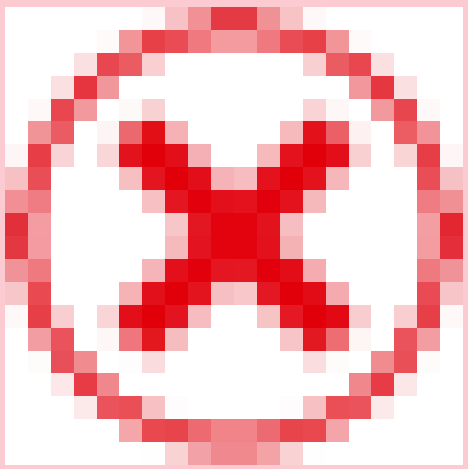
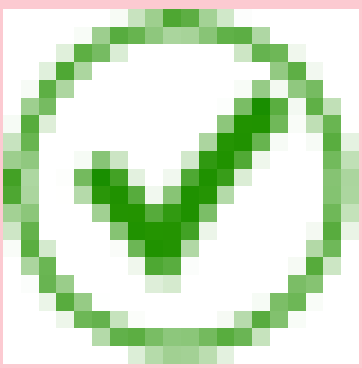
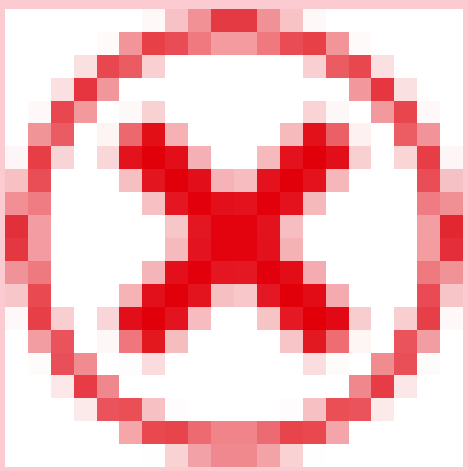
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	certification_admin	certification_filter_admin
Plandefinitionen		
Zertifizierungsfilter		
Instanzen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	certification_admin	certification_filter_admin
Audit-Ergebnisse		
Audits		
Auditdefinitionen		
Auditinstanzen		

[End]

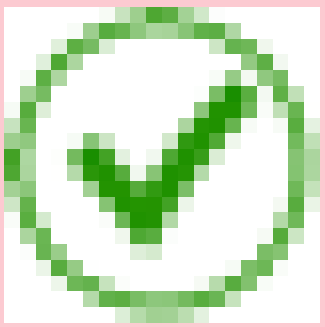
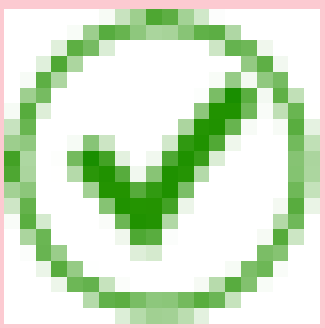
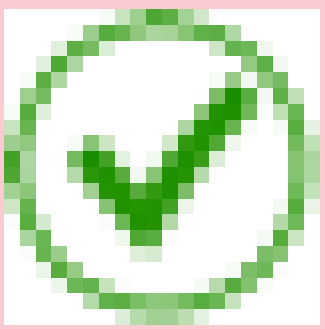
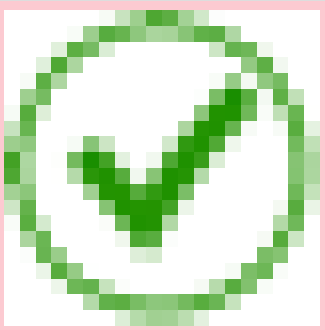
[store-future: BEGIN review]

Modulzugriff nach Rolle für IBM QRadar-Integration

Informationen zur IBM QRadar-Integration finden Sie in den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si.analyst
(Haupt-App-Gruppe)	
IBM QRadar-Profil	
Import von IBM QRadar-Vergehen	
IBM QRadar – Verstoß gegen Aufgabe	
IBM QRadar-Feldübersetzung	
IBM QRadar-Integrationseinstellungen	

Automatische Übersetzung

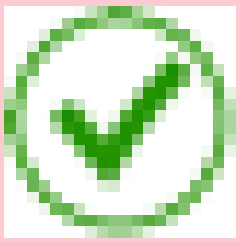
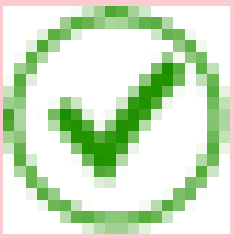
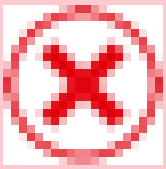
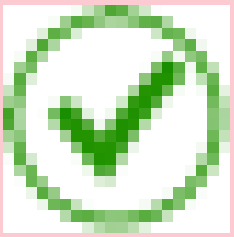
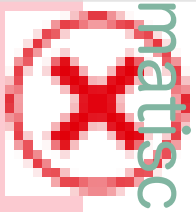
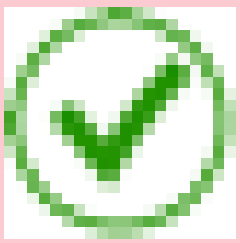
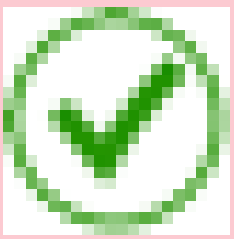
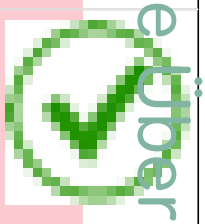
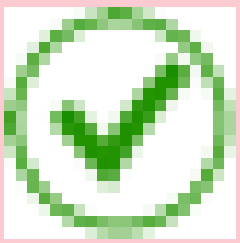
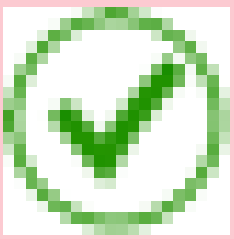
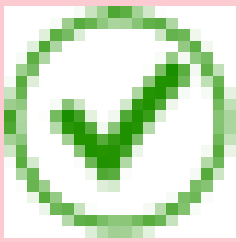
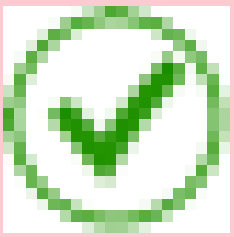
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[End]

[store-future: BEGIN review]

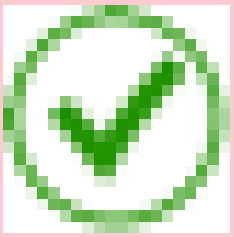
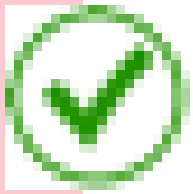
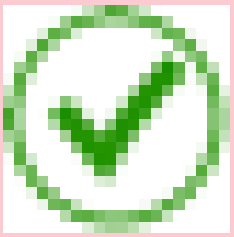
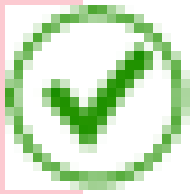
Modulzugriff nach Rolle für MISP-Integration

Informationen zur MISP-Integration finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modul	sn_si. Administrator	sn_si. Analyst	sn_ti. Administrator	sn_ti. Lesen	sn_ti. Schreiben
(Haupt-App-Gruppe)					
Integrationseinstellungen					
Sichtungssuche: Konfiguration					
Profile für die automatische Erstellung von Ereignissen					
Warteschlange für automatische Ereigniserstellung					
MISP-Ereignis-Daten					

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

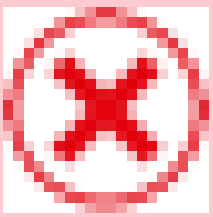
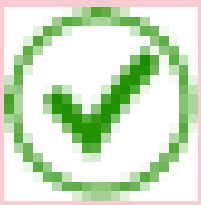
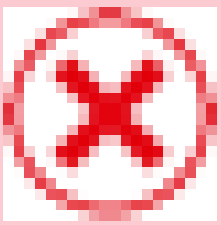
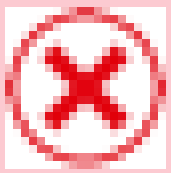
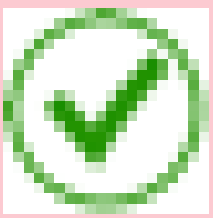
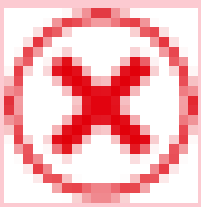
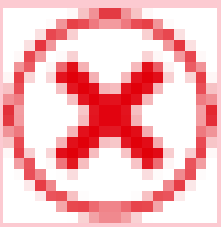
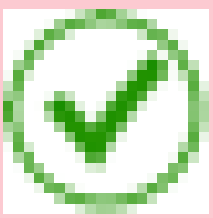
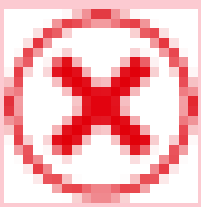
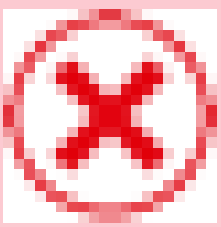
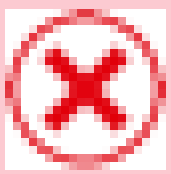
Modul	sn_si. Administrator	sn_si. Analyst	sn_ti. Administrator	sn_ti. Lesen	sn_ti. Schreiben
Zugeordnete MISP-Ereignisse					
MISP-Anwenderinformationen					

[End]

[store-future: BEGIN review]

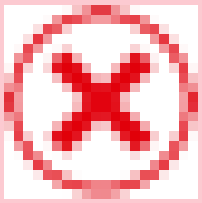
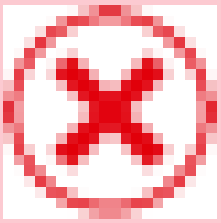
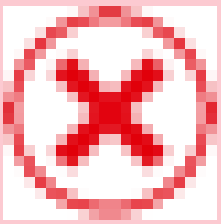
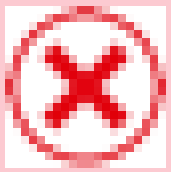
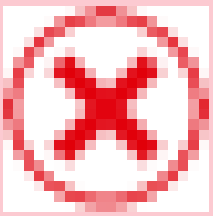
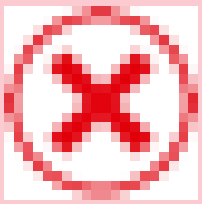
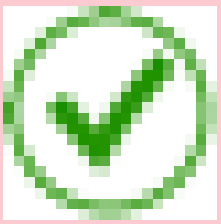
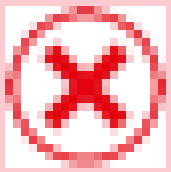
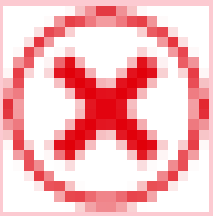
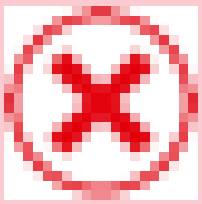
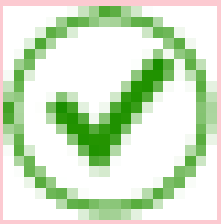
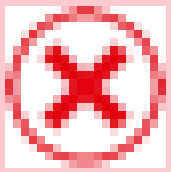
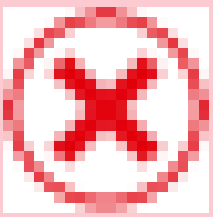
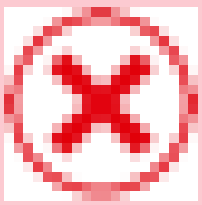
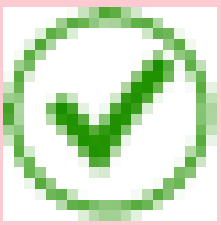
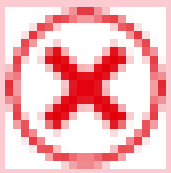
Modulzugriff nach Rolle für Microsoft Azure Defender for IoT

Informationen zu Microsoft Azure Defender for IoT finden Sie in den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

Modul	cmdb_inst_admin	cmdb_OT_admin	connection_admin	import_admin
(Haupt-App-Gruppe)				
Setup				
Datenquellen				
IntegrationHub ETL				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	cmdb_inst_admin	cmdb_OT_admin	connection_admin	import_admin
Zeitpläne importieren				
Eigenschaften				
Verbindungen und Anmeldeinformationen				
Aliasse Für Verbindungs-Anmeldeinformationen				
Anmeldeinformationen				
Verbindungen				

[End]

[store-future: BEGIN review]

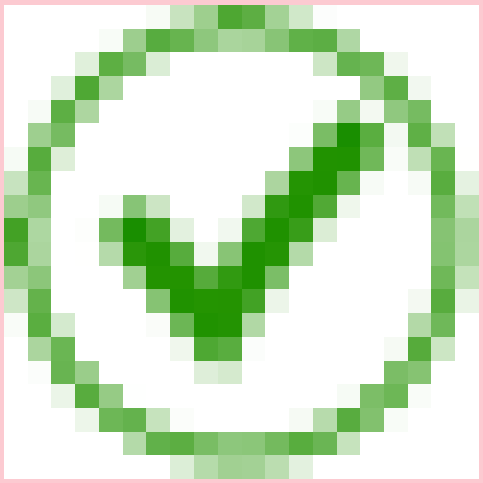
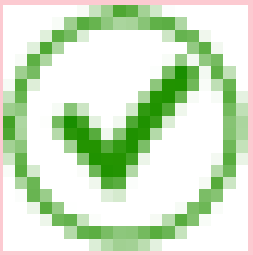
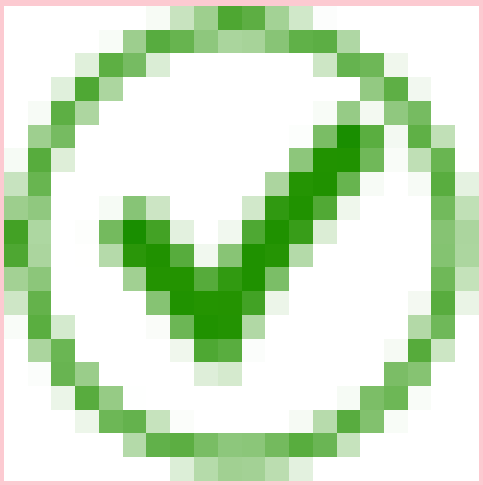
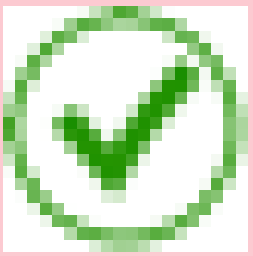
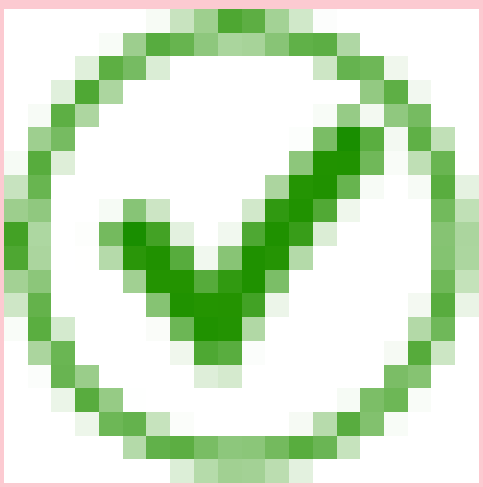
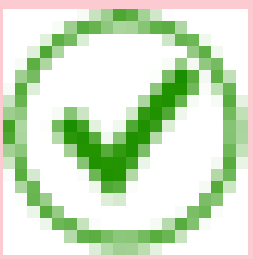
Modulzugriff nach Rolle für Qualys Vulnerability Integration

Informationen zur Qualys Vulnerability Integration finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modul	sn_vul. Konfigurieren_qualys_Integration	sn_vul_qualys. Lesen
(Haupt-App-Gruppe)		

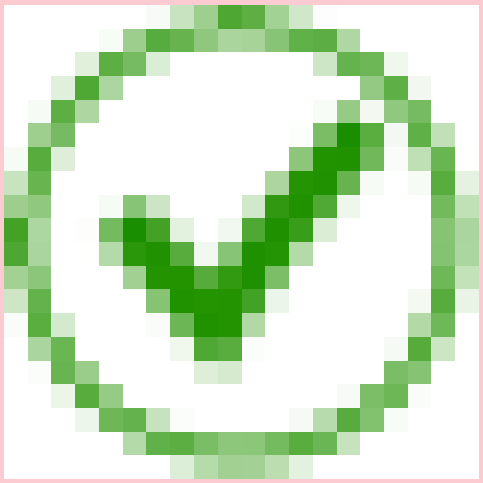
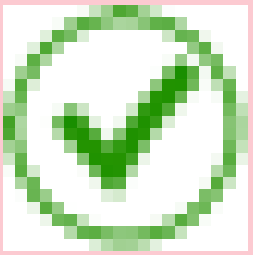
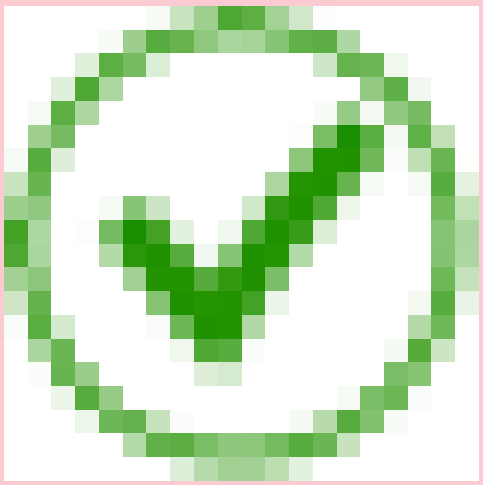
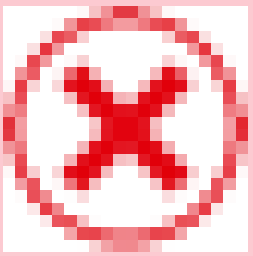
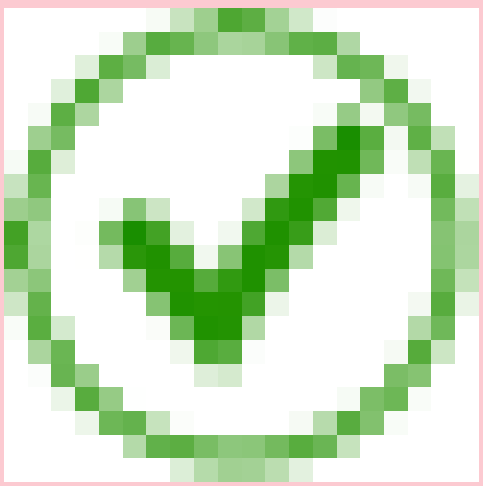
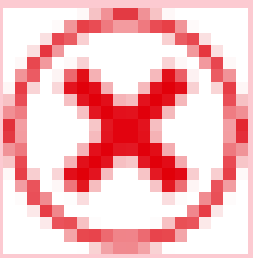
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul. Konfigurieren_qualys_Integration	sn_vul_qualys. Lesen
Übersicht		
Status der Integrationsausführung		
Scannergeräte		

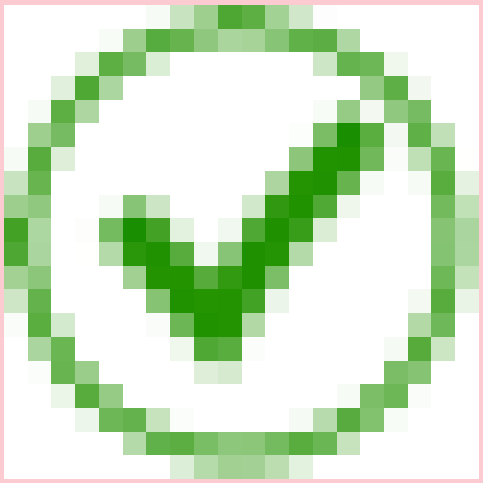
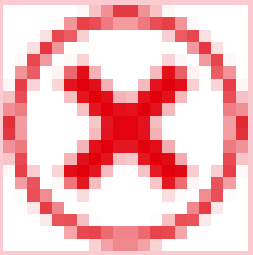
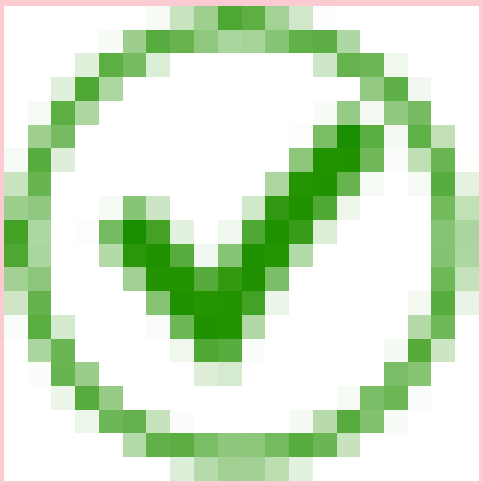
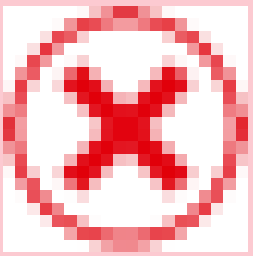
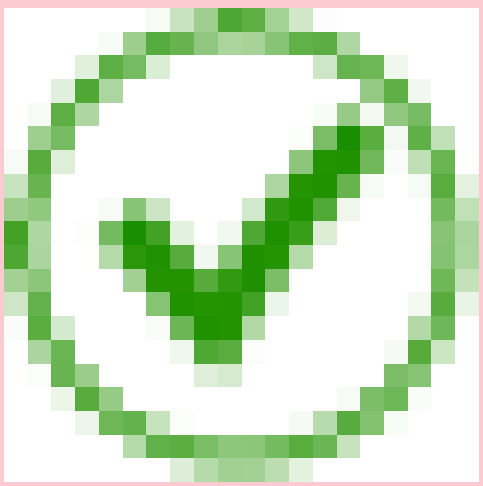
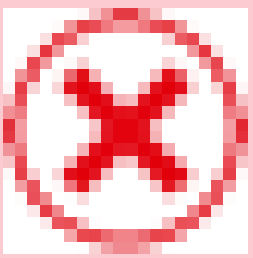
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul. Konfigurieren_qualys_Integration	sn_vul_qualys. Lesen
Suchlisten		
Administration		
Integrationsinstanzen		
Primäre Integrationen		

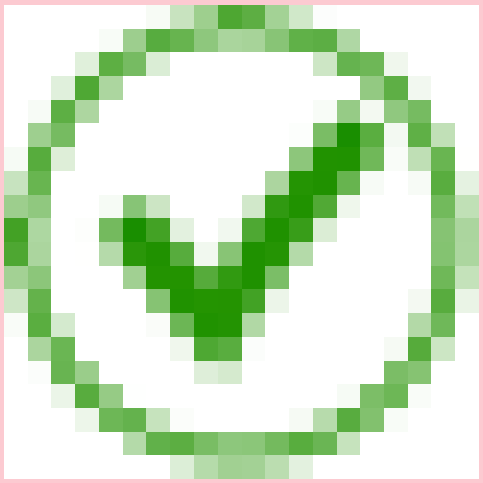
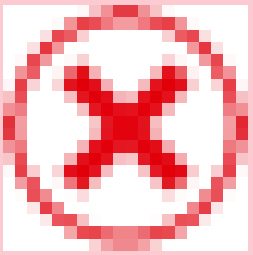
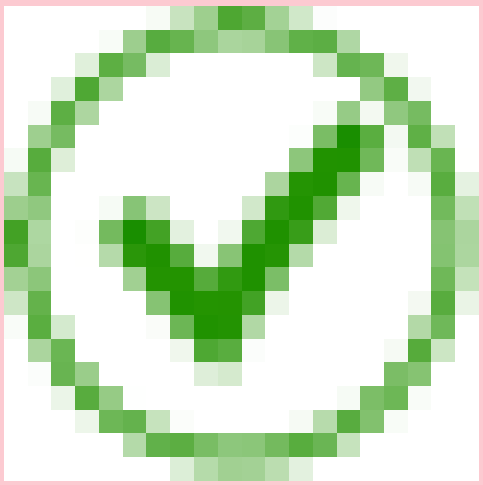
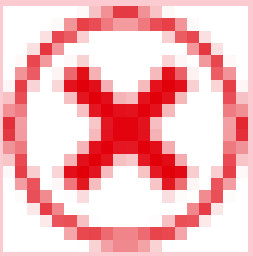
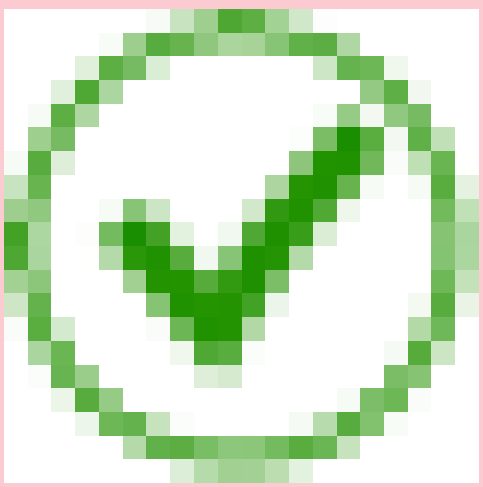
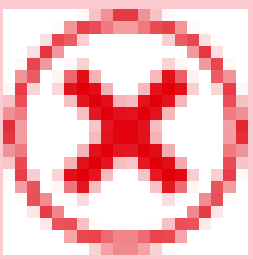
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul. Konfigurieren_qualys_Integration	sn_vul_qualys. Lesen
Unterstützende Integrationen		
Importsatztabellen		
Host-Import		
Import der Host-Erkennungsliste		

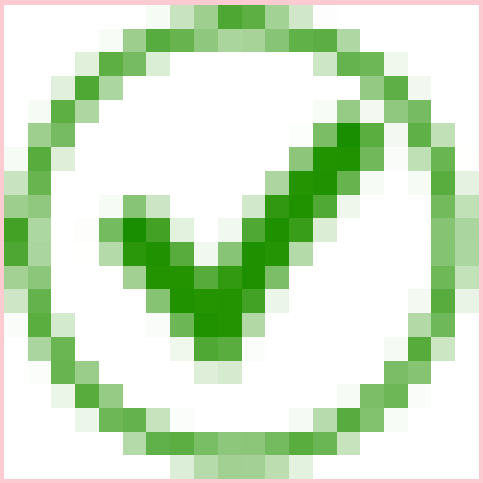
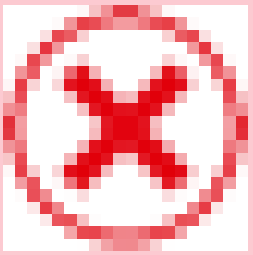
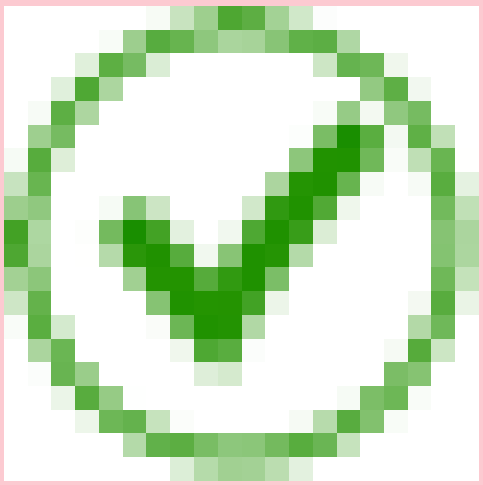
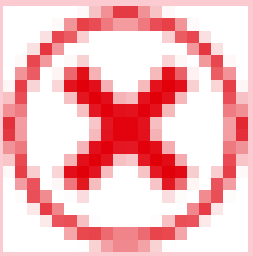
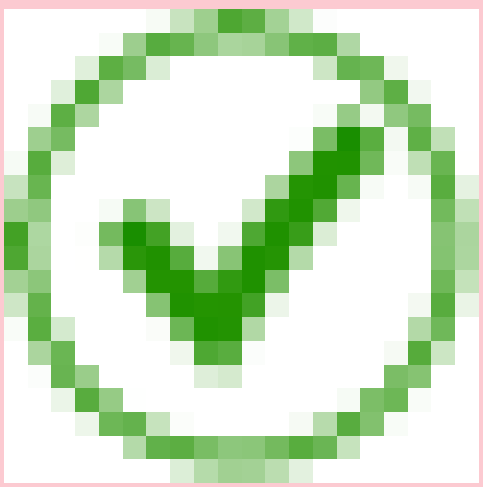
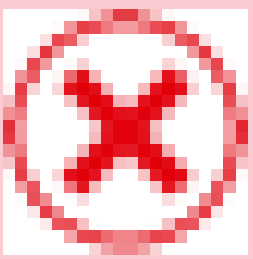
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul. Konfigurieren_qualys_Integration	sn_vul_qualys. Lesen
Wissensdatenbankimport		
Ticket-Listenimport		
Import dynamische Suchliste		

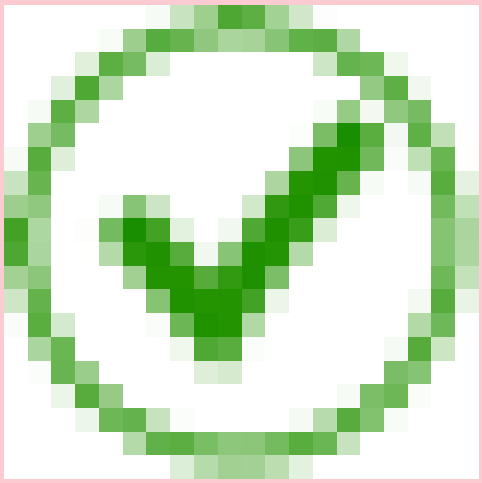
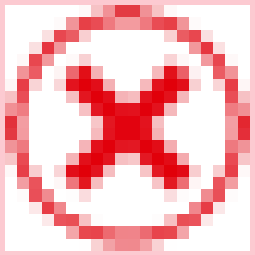
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul. Konfigurieren_qualys_Integration	sn_vul_qualys. Lesen
Import statische Suchliste		
Assetgruppenimport		
Appliance-Import		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

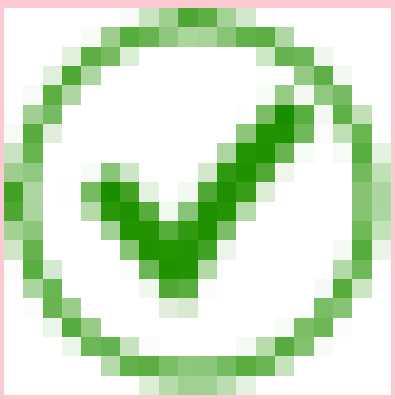
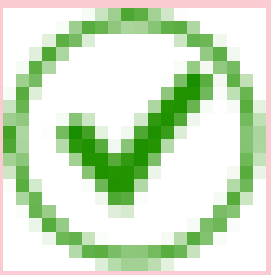
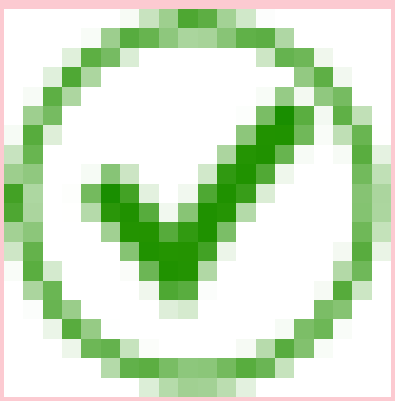
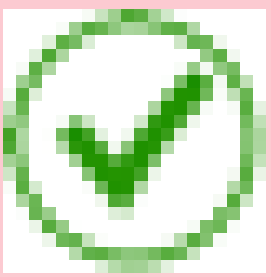
Modul	sn_vul. Konfigurieren_qualys_Integration	sn_vul_qualys. Lesen
Import der Host-Erkennungspaginierung		

[End]

[store-future: BEGIN review]

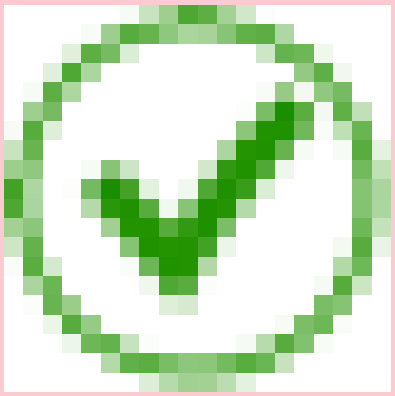
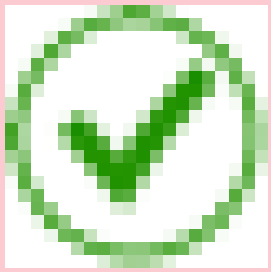
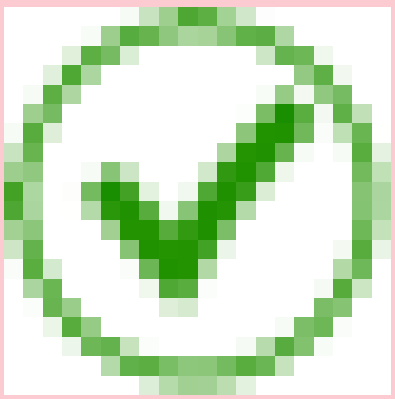
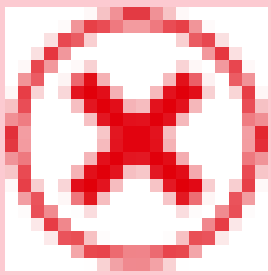
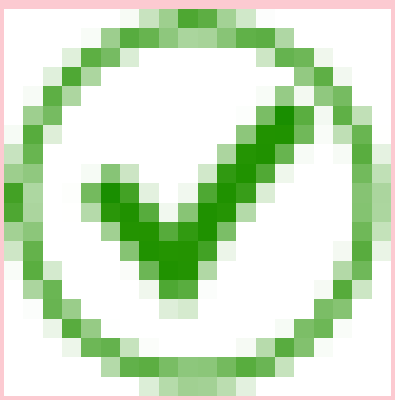
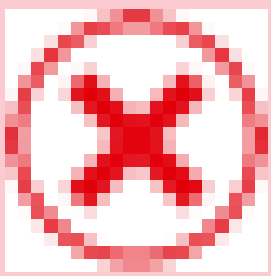
Modulzugriff nach Rolle für Rapid7 Vulnerability Integration

Informationen zur Rapid7 Vulnerability Integration finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modul	sn_vul_r7. Administrator	sn_vul_r7. Lesen
(Haupt-App-Gruppe)		
Status der Integrationsausführung		
Standorte		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_vul_r7. Administrator	sn_vul_r7. Lesen
Lösungen		
Administration		
Integrationen		
Konfiguration		

[End]

[store-future: BEGIN review]

Modulzugriff nach Rolle für Security Incident

Informationen zu Security Incidents finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Automatische Übersetzung

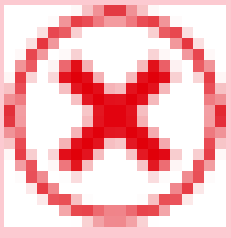
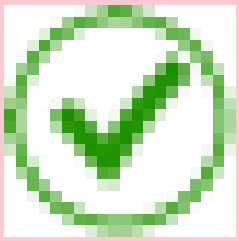
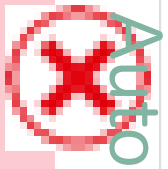
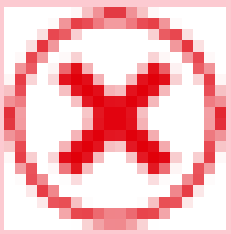
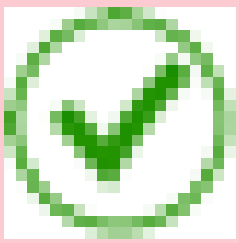
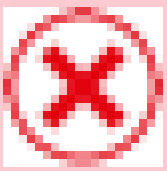
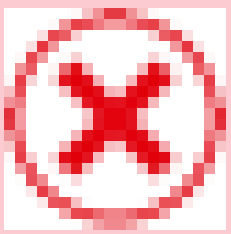
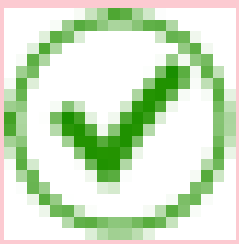
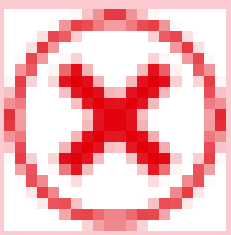
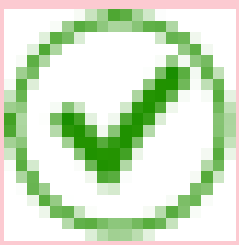
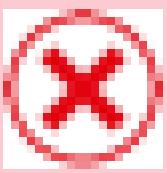
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
(Haupt-App-Gruppe)						
Incidents – neue UI						
Serviceeinfluss						
Übersicht						
Echtzeit						
Incidents						

Automatische Übersetzung

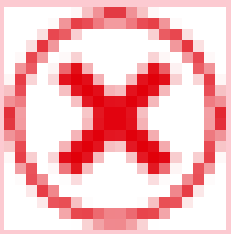
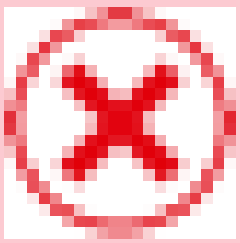
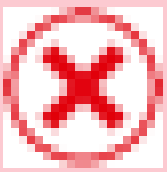
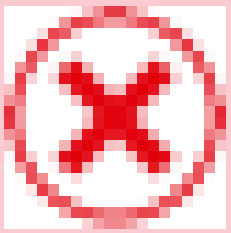
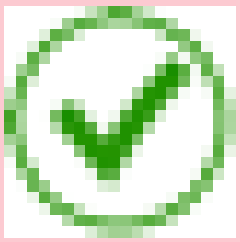
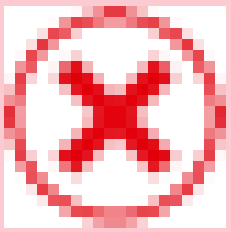
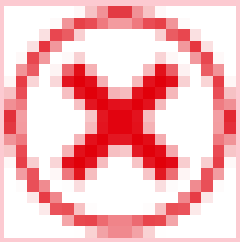
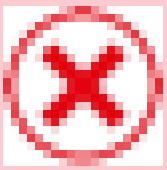
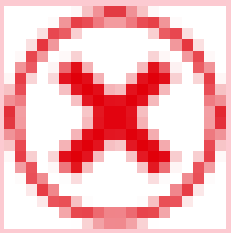
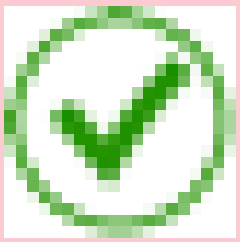
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Für mich sichtbar						
Mir zugewiesen						
Meine Arbeit						
Dem Team zugewiesen						

Automatische Übersetzung

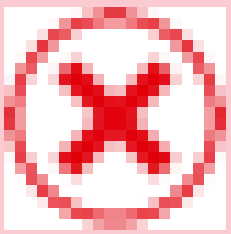
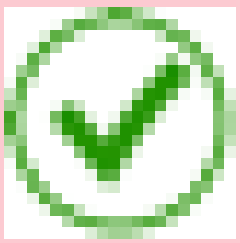
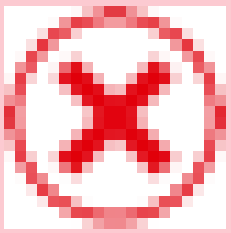
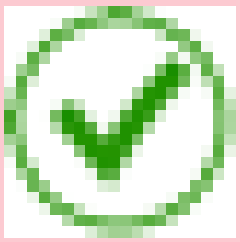
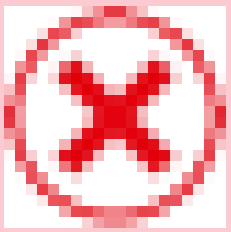
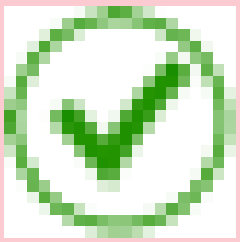
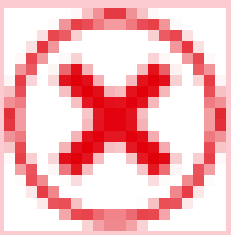
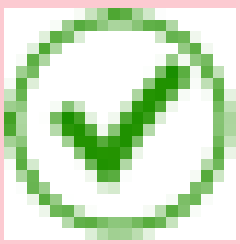
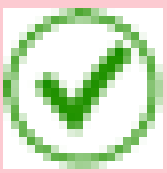
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Offene Incidents anzeigen						
Alle Incidents anzeigen						
Nicht zugewiesene Incidents						
Antwortaufgaben						
Mir zugewiesen						

Automatische Übersetzung

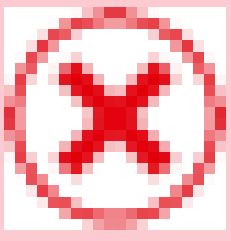
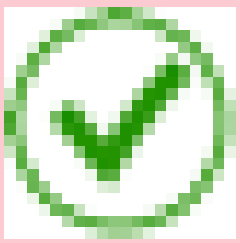
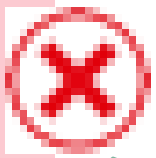
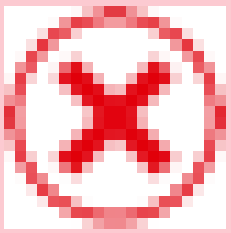
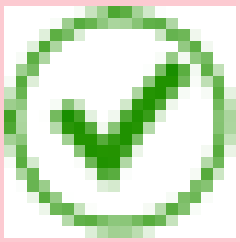
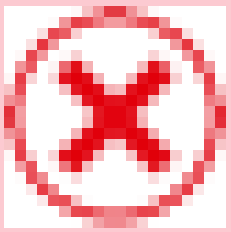
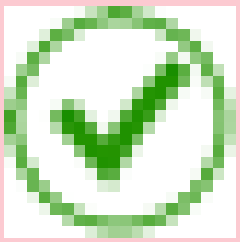
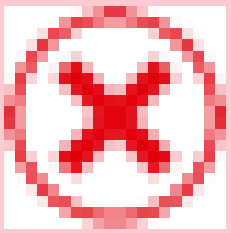
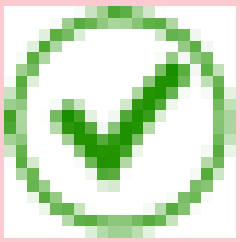
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Dem Team zugewiesen						
Offene Aufgaben anzeigen						
Alle Aufgaben anzeigen						
Nicht zugewiesene Aufgaben						
Eingehende Anfragen						

Automatische Übersetzung

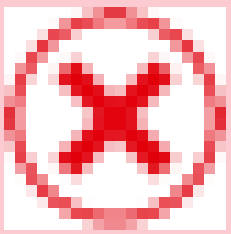
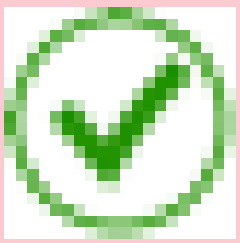
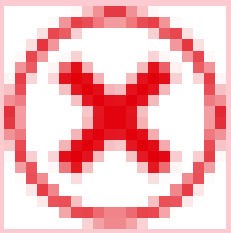
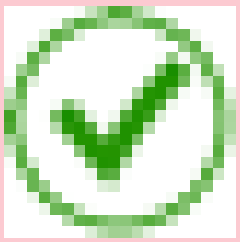
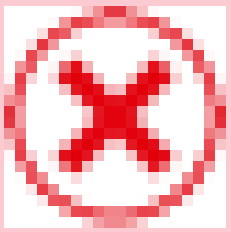
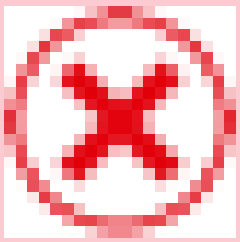
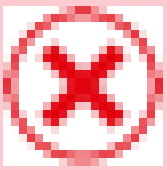
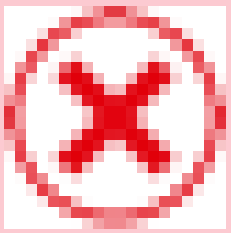
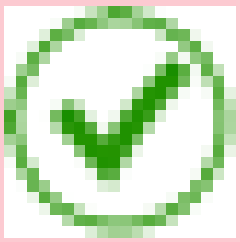
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Mir zugewiesen						
Dem Team zugewiesen						
Meine Genehmigungen						
Offene Anfragen anzeigen						

Automatische Übersetzung

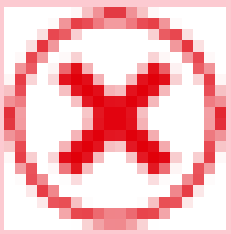
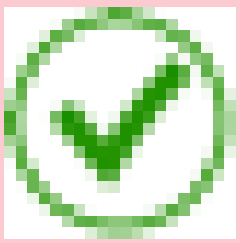
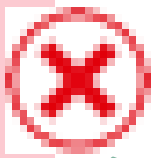
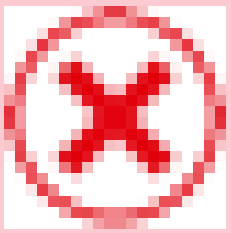
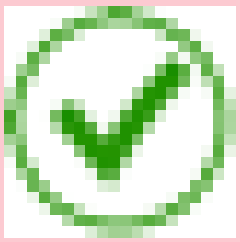
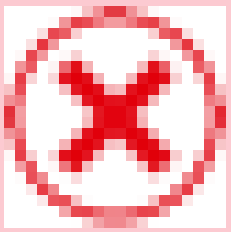
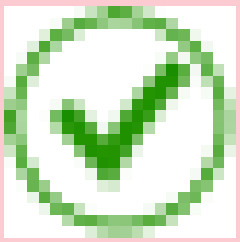
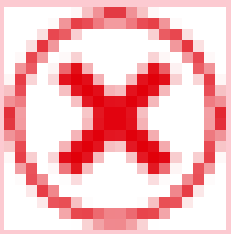
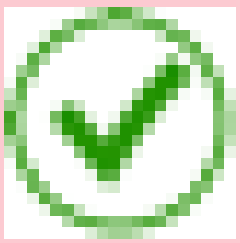
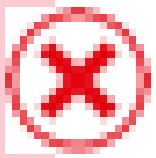
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Alle Anforderungen anzeigen						
Nicht zugewiesene Anfragen						
Meine Karte						
Warnungen und Ereignisse						
Überprüfung nach Incident						
Meine ausstehenden Überprüfungen						

Automatische Übersetzung

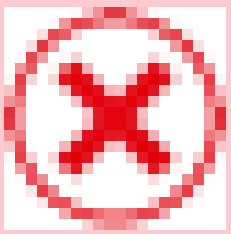
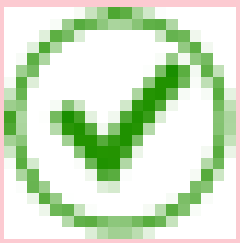
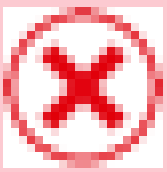
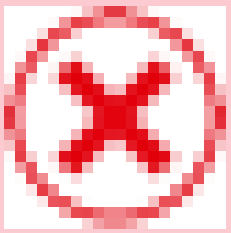
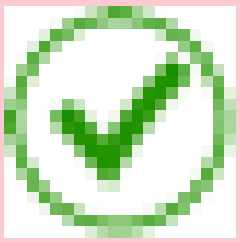
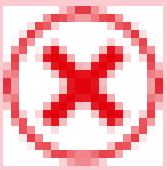
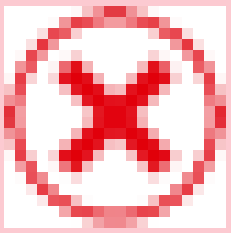
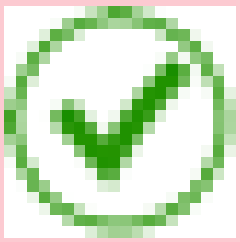
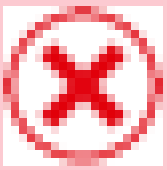
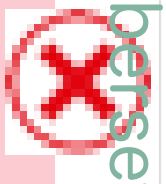
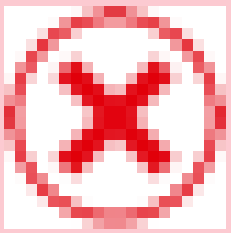
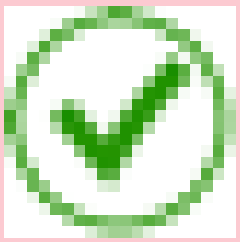
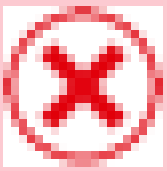
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Ausstehende Überprüfungen des Teams						
Alle unvollständigen Überprüfungen						
Setup						
Security Incident-Rechnergruppen						
Schweregradrechner						

Automatische Übersetzung

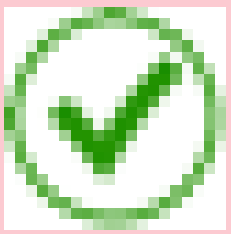
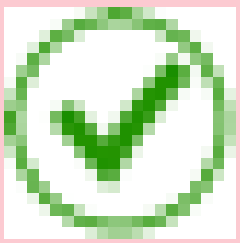
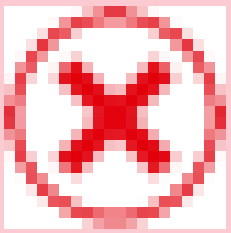
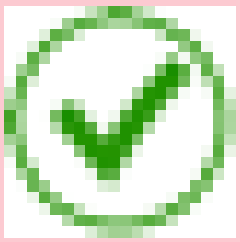
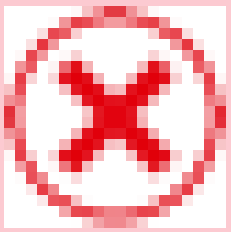
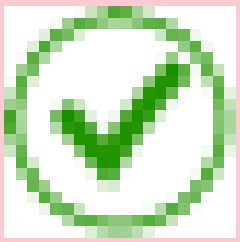
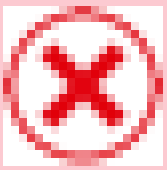
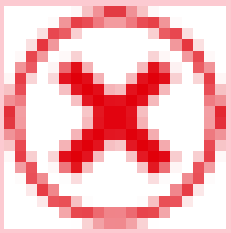
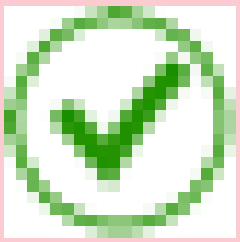
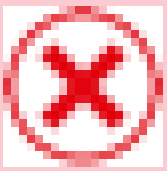
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Risikopunktzahlkonfiguration						
Nachrichtenfeed-Konfiguration						
Gruppen						
Rollen						

Automatische Übersetzung

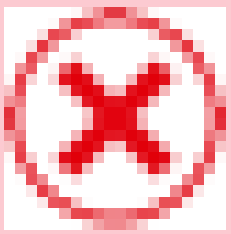
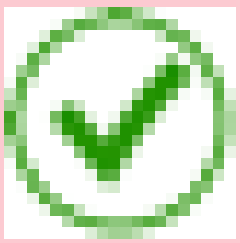
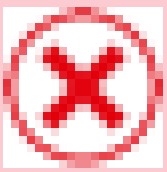
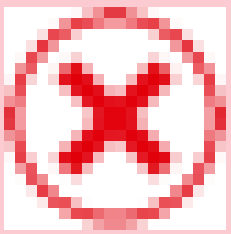
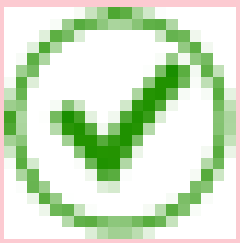
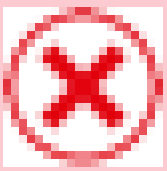
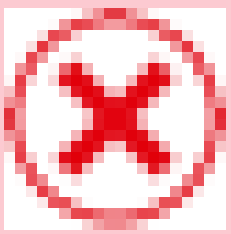
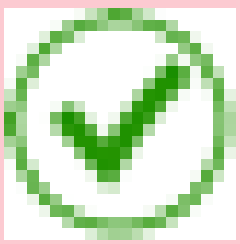
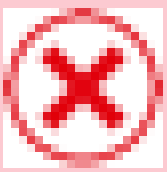
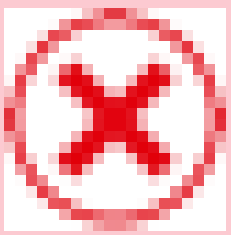
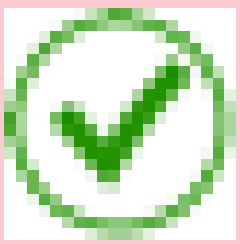
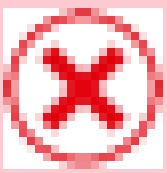
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
SLAs						
Setup des Analysten-Arbeitsbereichs (neue UI)						
Setup-Assistent						
Zielseiten-Filterkonfiguration						
Formular-UI-Aktionen						

Automatische Übersetzung

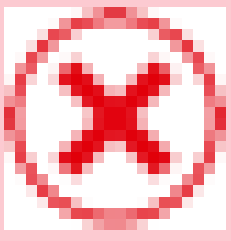
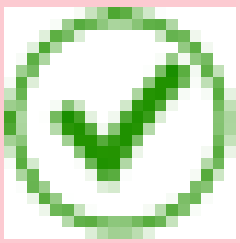
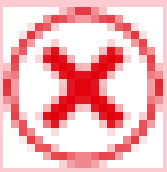
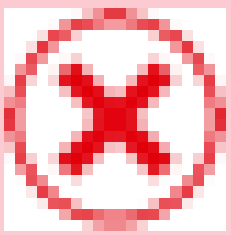
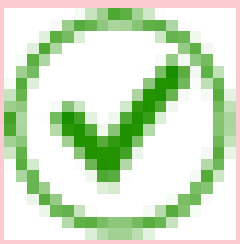
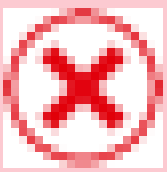
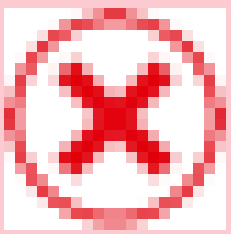
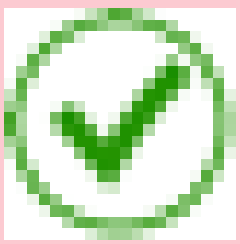
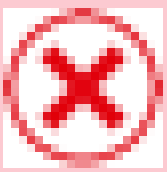
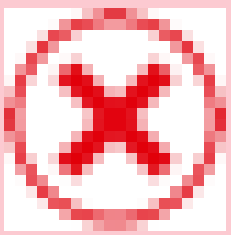
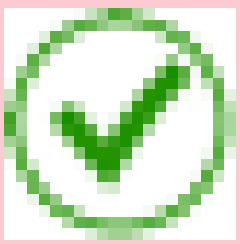
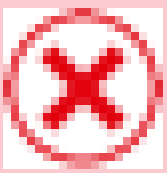
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Konfigurationen Der Zugehörigen Liste						
Eigenschaften Des Analysten-Arbeitsbereichs						
Katalog & Wissen						
Vorlagen für Security Incidents						
Katalogelemente pflegen						

Automatische Übersetzung

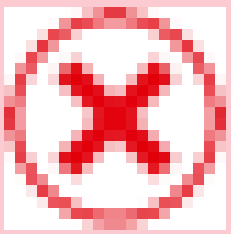
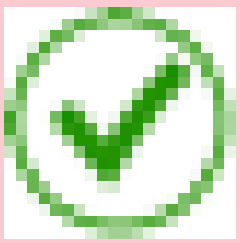
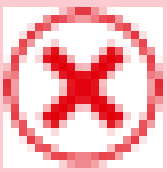
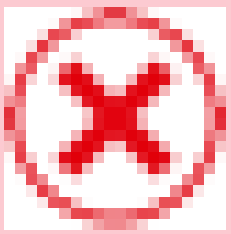
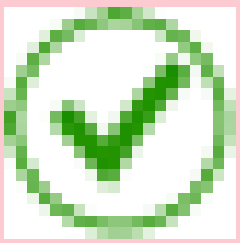
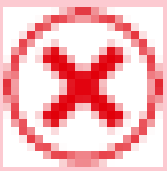
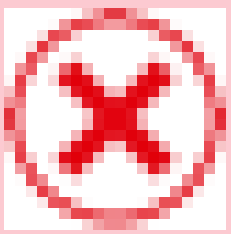
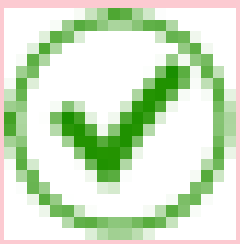
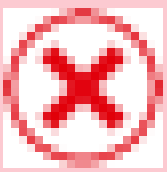
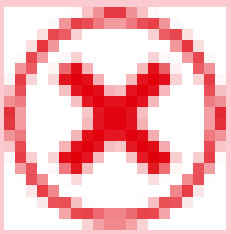
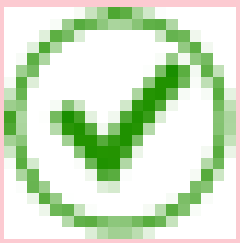
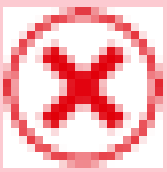
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Wissen						
Manuelles Runbook						
Neues Runbook erstellen						
Runbook-Dokumente anzeigen						
Administration						
Eigenschaften						

Automatische Übersetzung

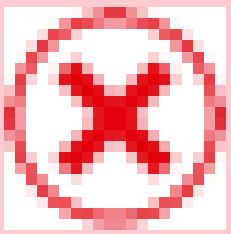
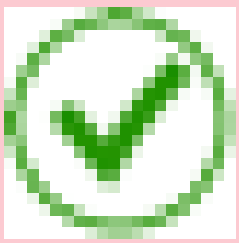
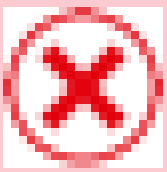
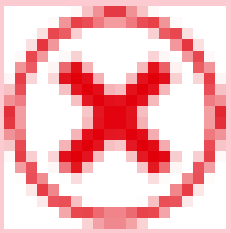
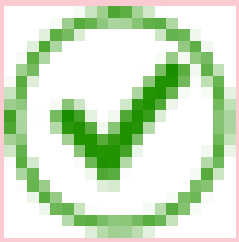
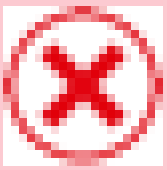
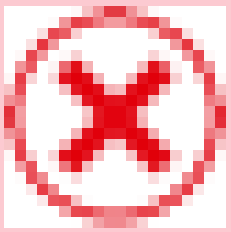
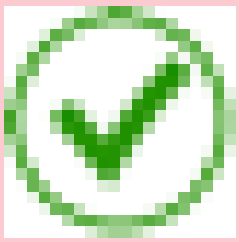
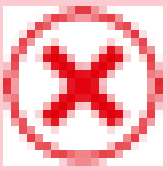
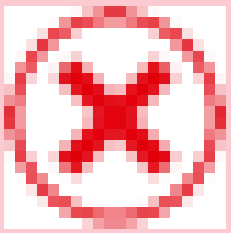
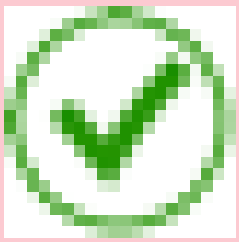
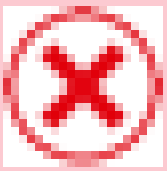
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Konfiguration						
Benachrichtigungen						
Servicerelevanz-Reportingdefinition						
Servicerelevanzdefinition						

Automatische Übersetzung

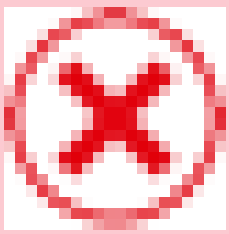
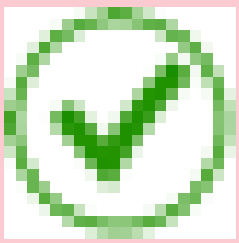
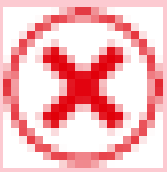
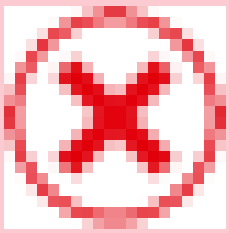
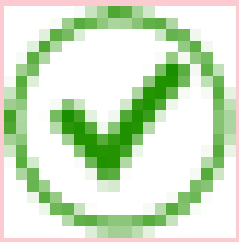
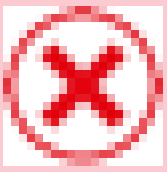
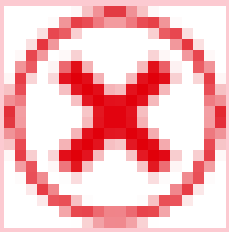
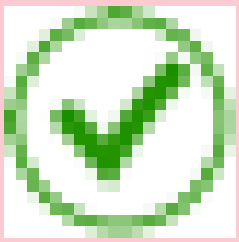
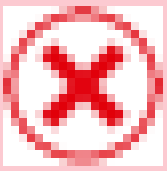
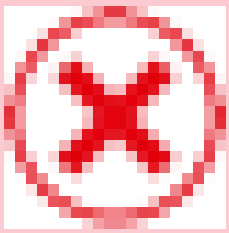
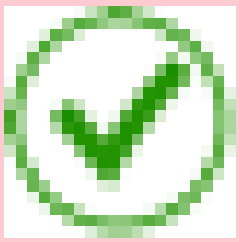
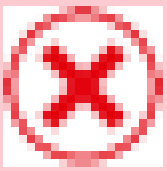
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Serviceeinfluss-Definitionen						
Setup Der Bewertungen Der Überprüfung Nach Incident						
Setup Des Berichts Zur Überprüfung Nach Incident						
Echtzeitdefinition						

Automatische Übersetzung

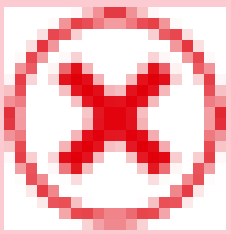
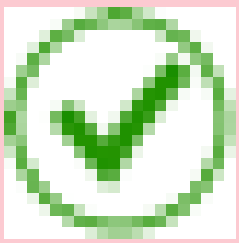
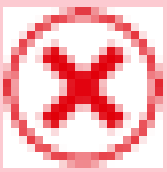
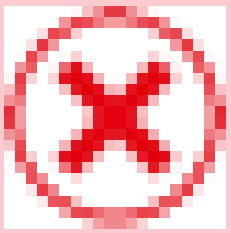
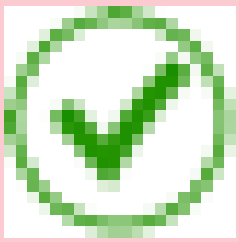
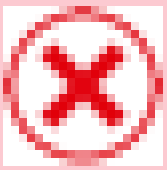
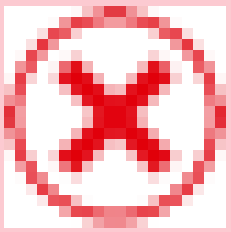
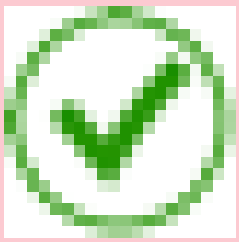
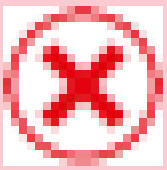
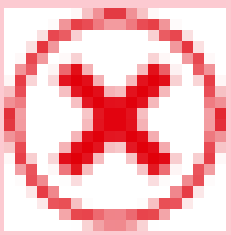
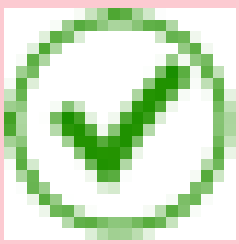
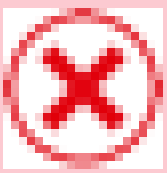
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Prozessauswahl						
Prozessdefinitionen						
Vorlagenworkflow – Ergebnisauswertung						
Phishing-E-Mails						
Lizenzverwaltung						

Automatische Übersetzung

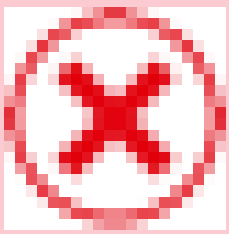
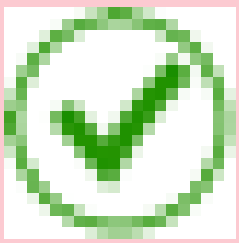
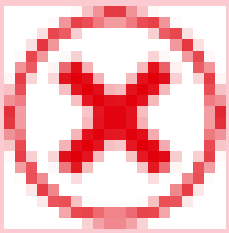
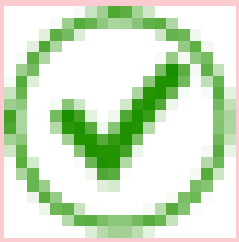
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Informationen für andere Rollen:

sn_si.special_Access, sn_si_Approver_user

(Fortsetzung)

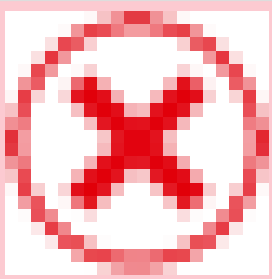
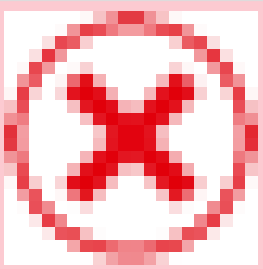
Modul	sn_sec_cmn. Lesen	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Extern	sn_si.
Phishing-E-Mail melden						
Alle Phishing-E-Mails anzeigen						

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

Modul	sn_si. Special_Access	sn_si_Approver_user
(Haupt-App-Gruppe)		
Incidents – neue UI		

Automatische Übersetzung

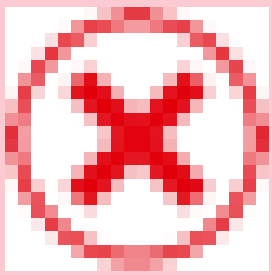
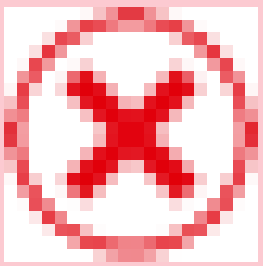
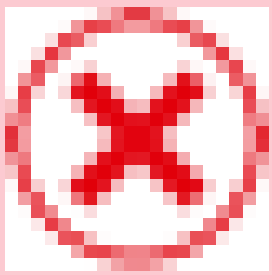
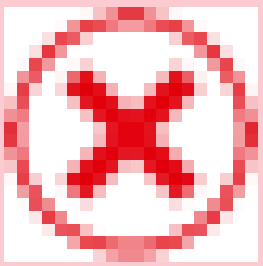
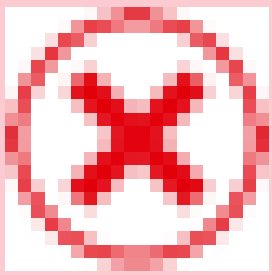
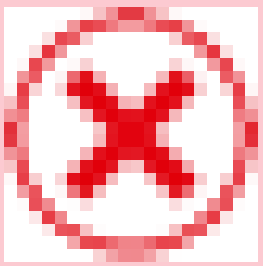
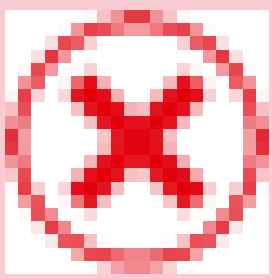
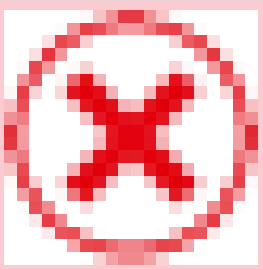
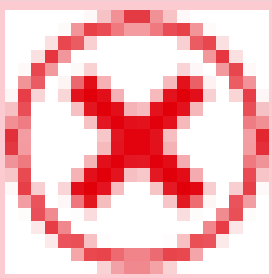
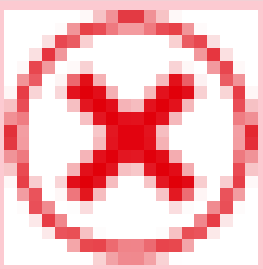
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Serviceeinfluss		
Übersicht		
Echtzeit		
Incidents		
Für mich sichtbar		
Mir zugewiesen		

Automatische Übersetzung

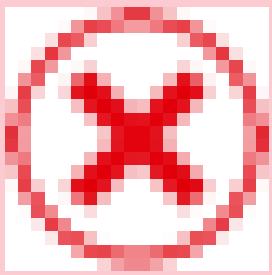
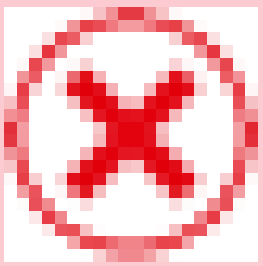
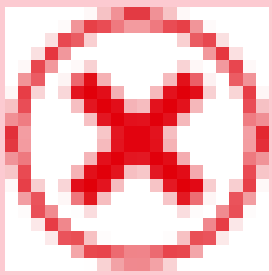
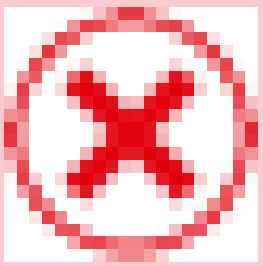
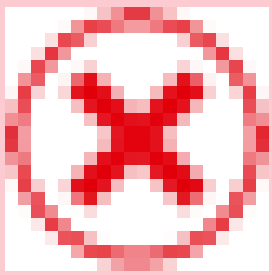
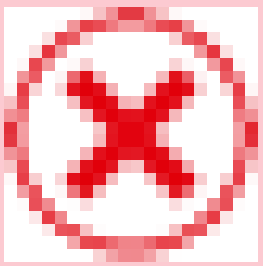
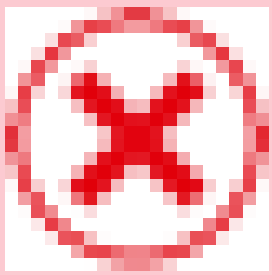
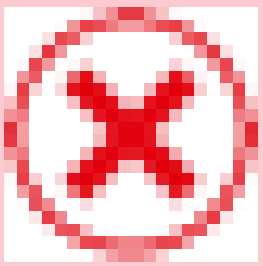
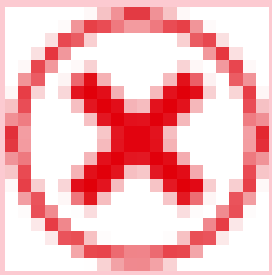
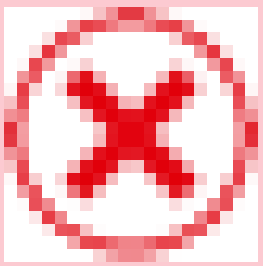
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Meine Arbeit		
Dem Team zugewiesen		
Offene Incidents anzeigen		
Alle Incidents anzeigen		
Nicht zugewiesene Incidents		
Antwortaufgaben		

Automatische Übersetzung

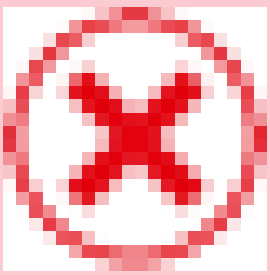
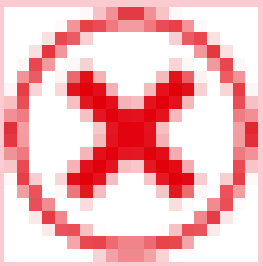
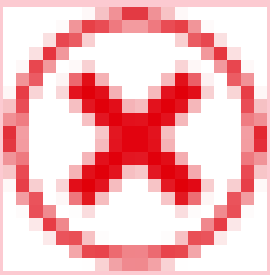
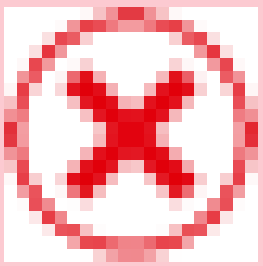
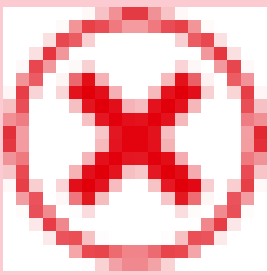
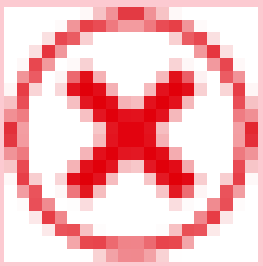
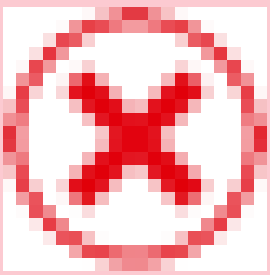
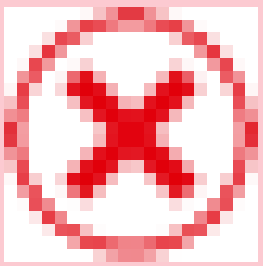
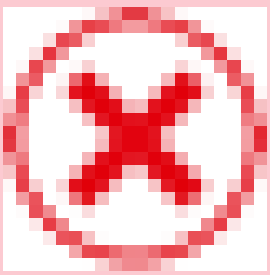
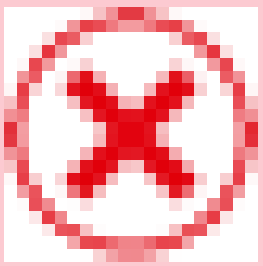
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Mir zugewiesen		
Dem Team zugewiesen		
Offene Aufgaben anzeigen		
Alle Aufgaben anzeigen		
Nicht zugewiesene Aufgaben		
Eingehende Anfragen		

Automatische Übersetzung

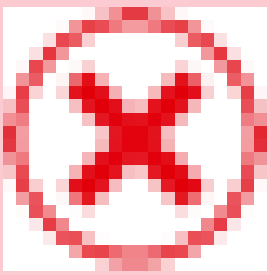
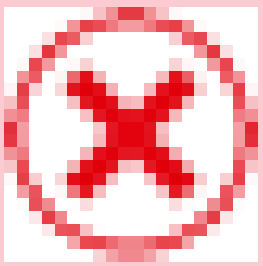
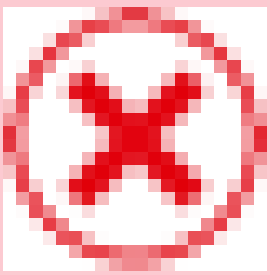
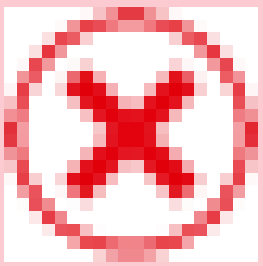
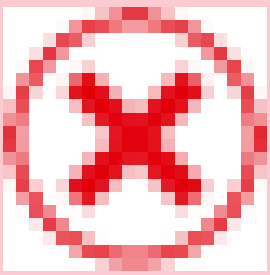
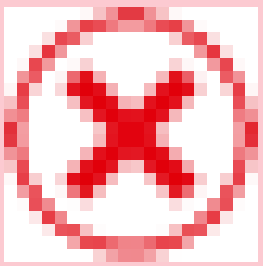
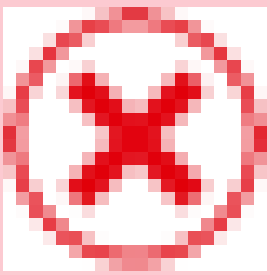
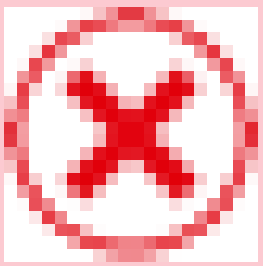
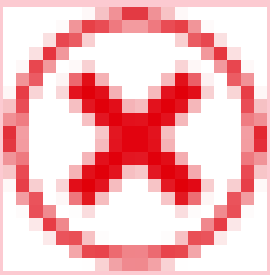
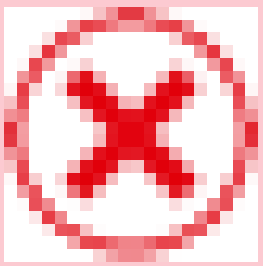
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Mir zugewiesen		
Dem Team zugewiesen		
Meine Genehmigungen		
Offene Anfragen anzeigen		
Alle Anforderungen anzeigen		

Automatische Übersetzung

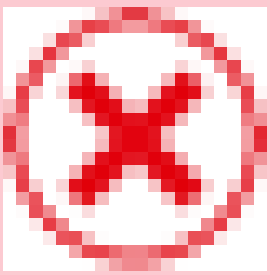
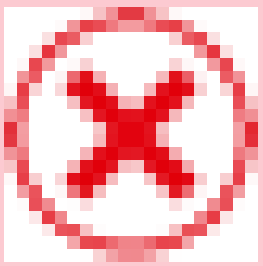
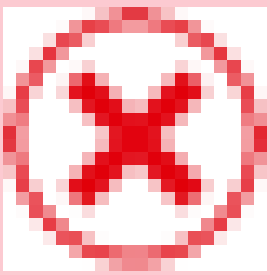
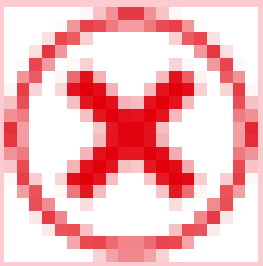
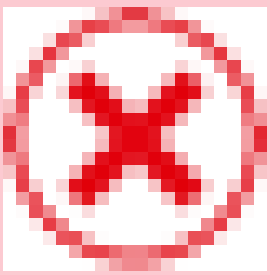
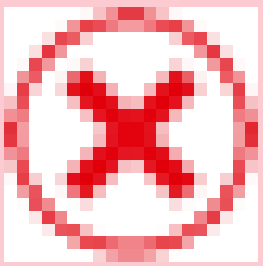
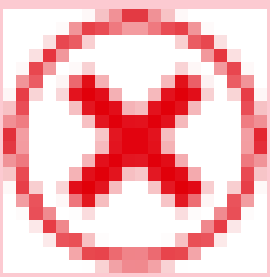
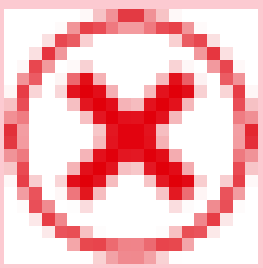
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Nicht zugewiesene Anfragen		
Meine Karte		
Warnungen und Ereignisse		
Überprüfung nach Incident		
Meine ausstehenden Überprüfungen		
Ausstehende Überprüfungen des Teams		

Automatische Übersetzung

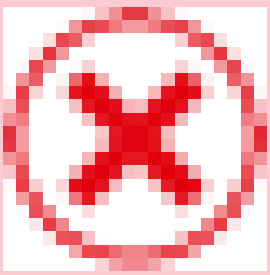
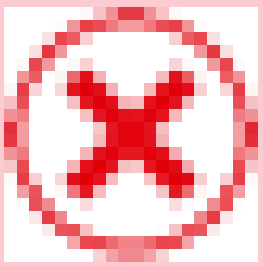
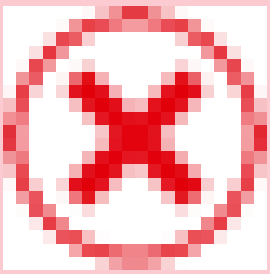
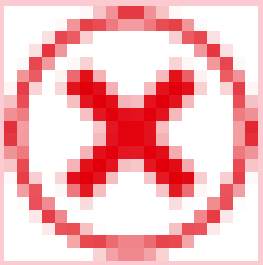
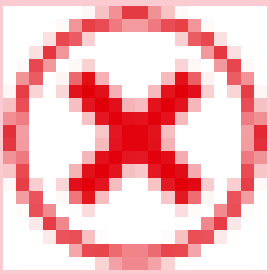
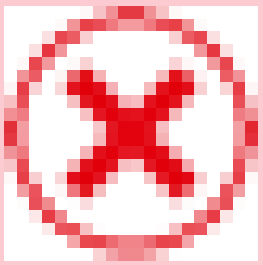
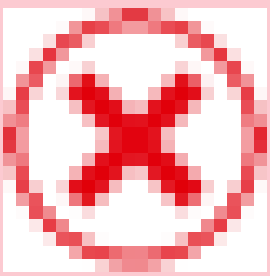
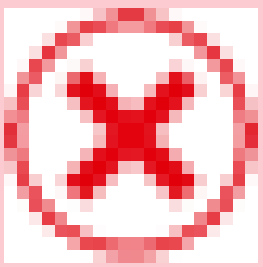
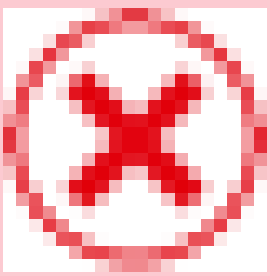
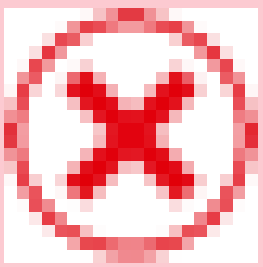
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Alle unvollständigen Überprüfungen		
Setup		
Security Incident-Rechnergruppen		
Schweregradrechner		
Risikopunktzahlkonfiguration		
Nachrichtenfeed-Konfiguration		

Automatische Übersetzung

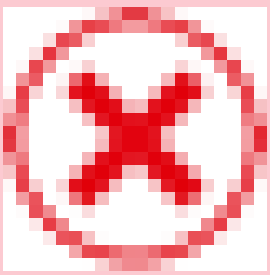
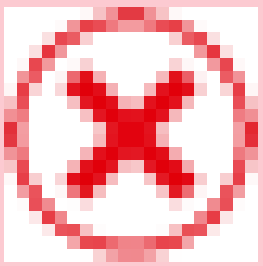
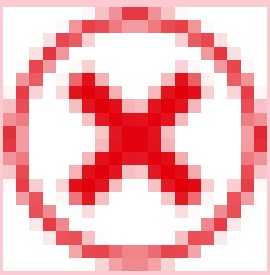
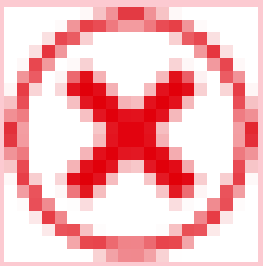
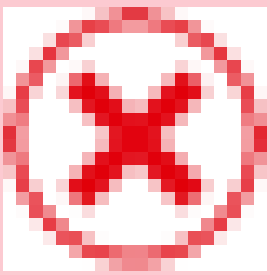
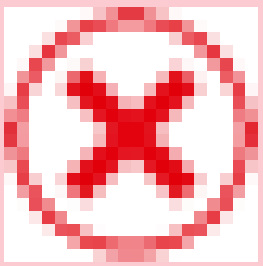
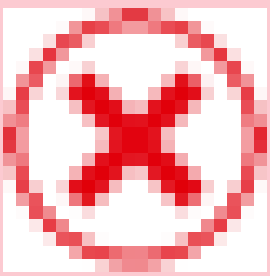
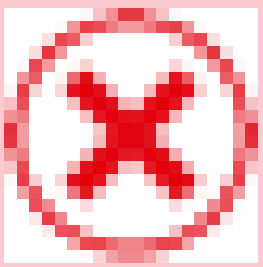
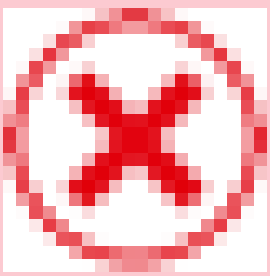
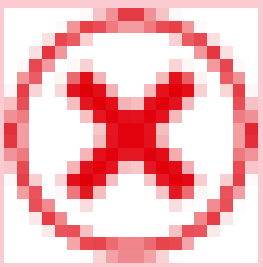
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Gruppen		
Rollen		
SLAs		
Setup des Analysten-Arbeitsbereichs (neue UI)		
Setup-Assistent		
Zielseiten-Filterkonfiguration		

Automatische Übersetzung

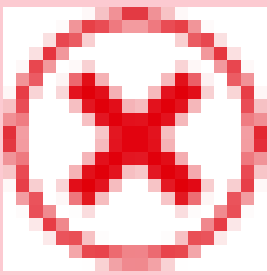
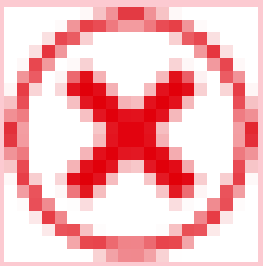
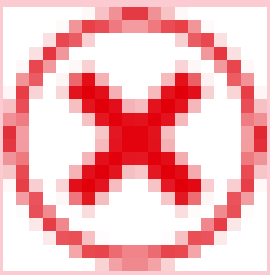
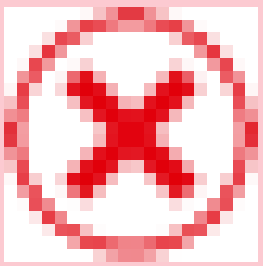
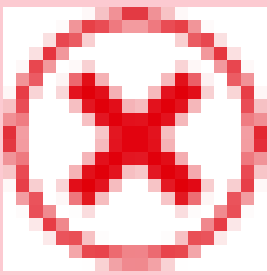
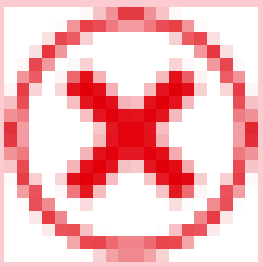
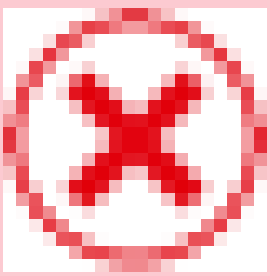
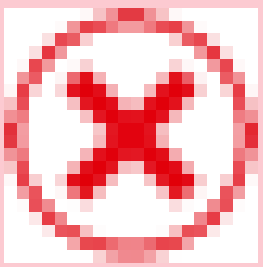
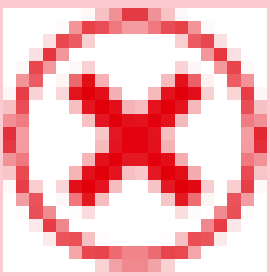
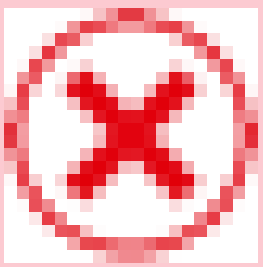
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Formular-UI-Aktionen		
Konfigurationen Der Zugehörigen Liste		
Eigenschaften Des Analysten-Arbeitsbereichs		
Katalog & Wissen		
Vorlagen für Security Incidents		
Katalogelemente pflegen		

Automatische Übersetzung

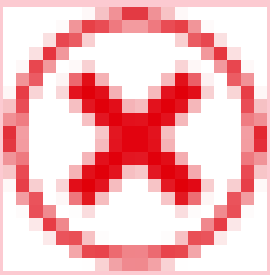
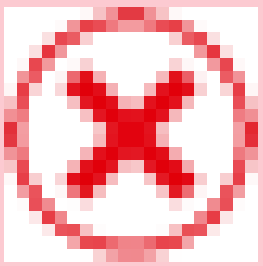
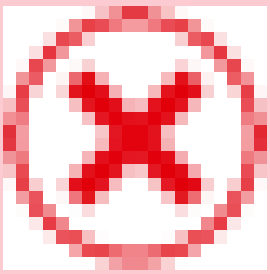
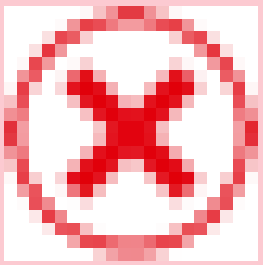
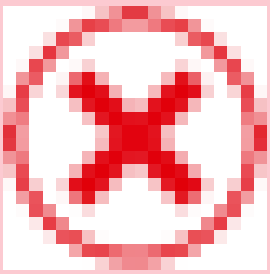
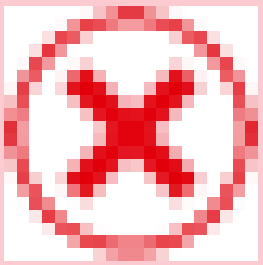
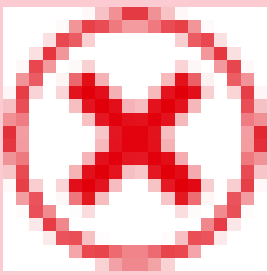
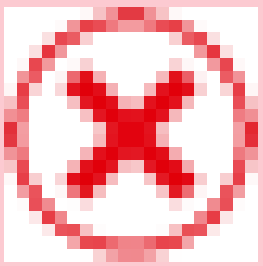
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Wissen		
Manuelles Runbook		
Neues Runbook erstellen		
Runbook-Dokumente anzeigen		
Administration		
Eigenschaften		

Automatische Übersetzung

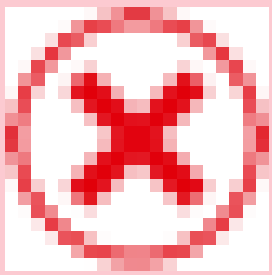
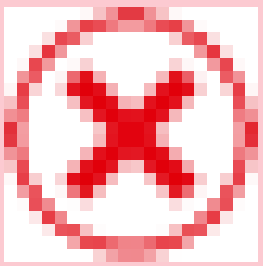
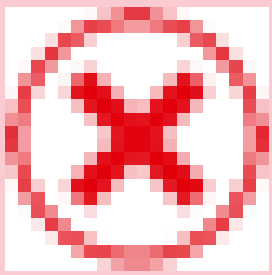
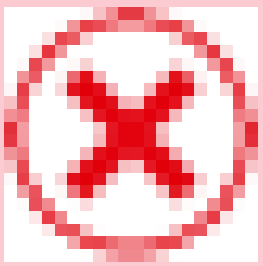
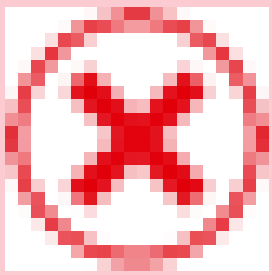
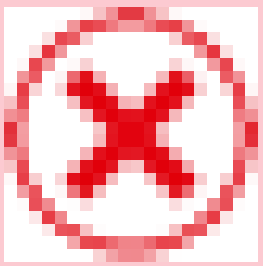
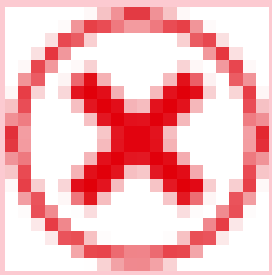
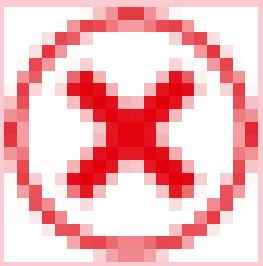
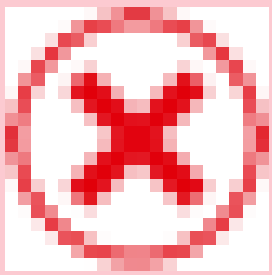
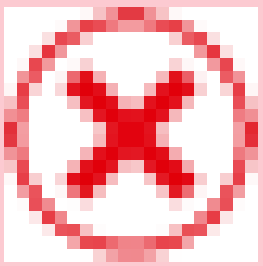
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Konfiguration		
Benachrichtigungen		
Servicerelevanz-Reportingdefinition		
Servicerelevanzdefinition		
Serviceeinfluss-Definitionen		

Automatische Übersetzung

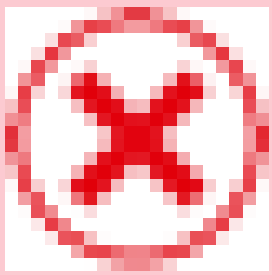
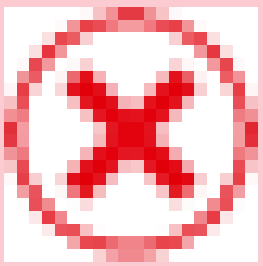
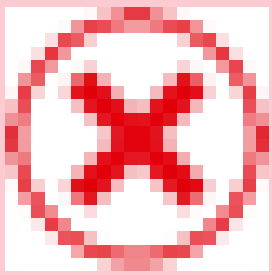
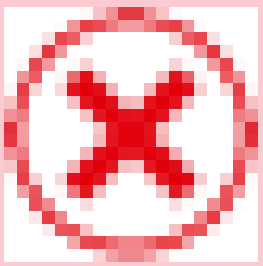
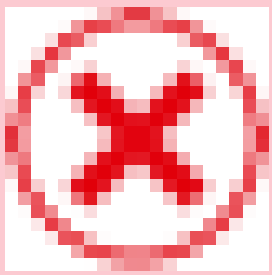
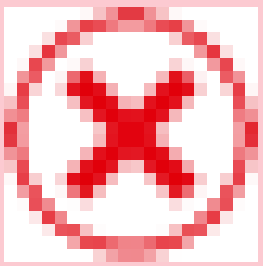
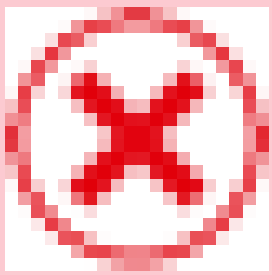
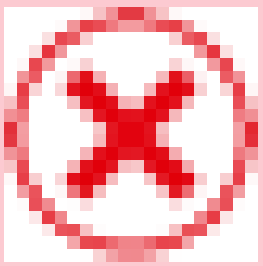
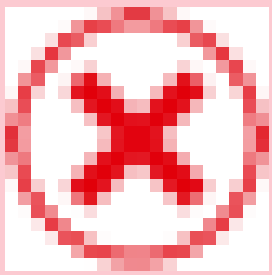
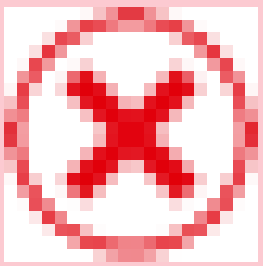
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Setup Der Bewertungen Der Überprüfung Nach Incident		
Setup Des Berichts Zur Überprüfung Nach Incident		
Echtzeitdefinition		
Prozessauswahl		
Prozessdefinitionen		

Automatische Übersetzung

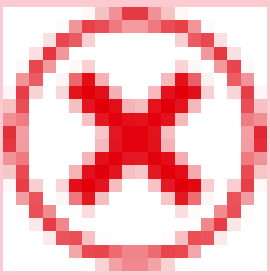
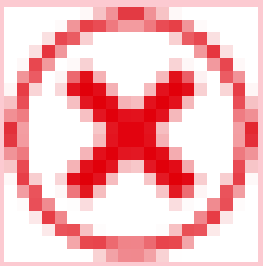
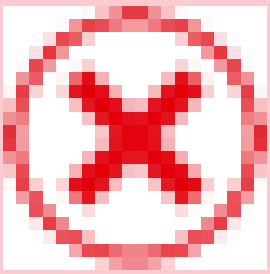
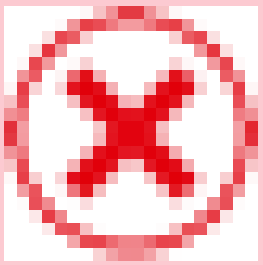
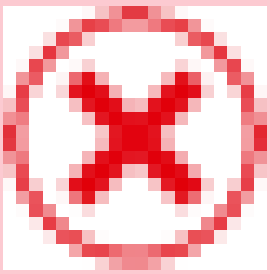
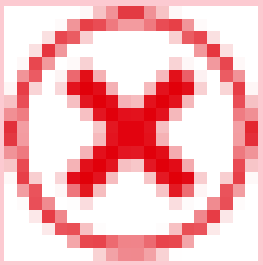
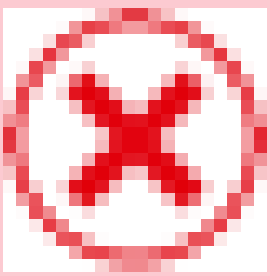
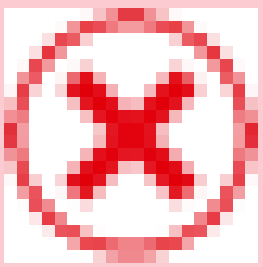
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_si.special_Access, sn_si_Approver_user

Informationen für andere Rollen:

sn_sec_cmn.read, sn_si.admin, sn_si.Analyst, sn_si.ciso, sn_si.external, sn_si.Knowledge_admin, sn_si.Manager, sn_si.read

(Fortsetzung)

Modul	sn_si. Special_Access	sn_si_Approver_user
Vorlagenworkflow – Ergebnisauswertung		
Phishing-E-Mails		
Lizenzverwaltung		
Phishing-E-Mail melden		
Alle Phishing-E-Mails anzeigen		

[End]

[store-future: BEGIN review]

Modulzugriff nach Rolle für Security Operations

Informationen zu Security Operations finden Sie in den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
(Haupt-App-Gruppe)				
Integrationen	✓	✓	✗	✗
Integrationsfähigkeiten-Flows	✓	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Fähigkeitsausführungen	✓	✗	✗	✗
Ratenbegrenzung für Fähigkeitsimplementierungen	✓	✗	✗	✗
Integrationskonfigurationen	✓	✓	✗	✗

Automatische Übersetzung

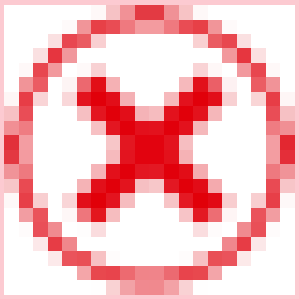
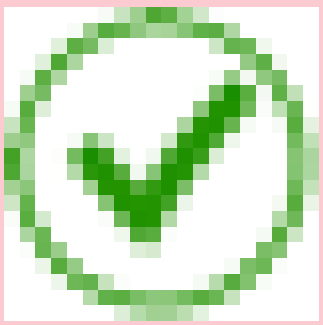
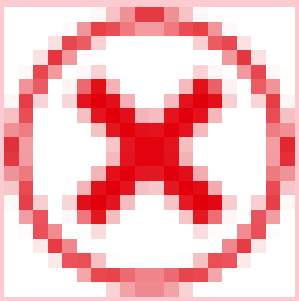
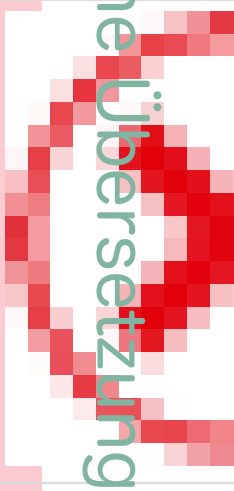
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Sichtungssuche – Konfiguration				
Integrationsfunktionen				
Integrationen				

Automatische Übersetzung

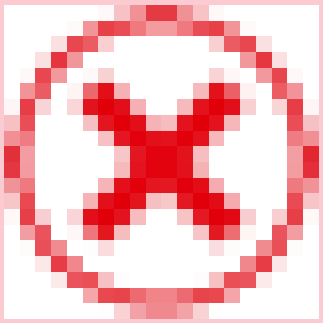
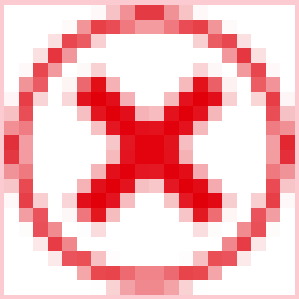
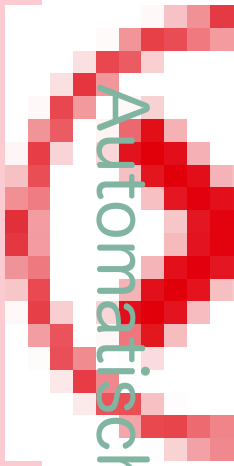
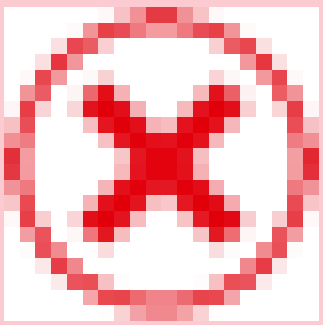
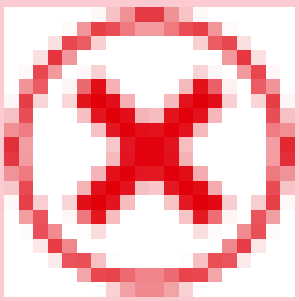
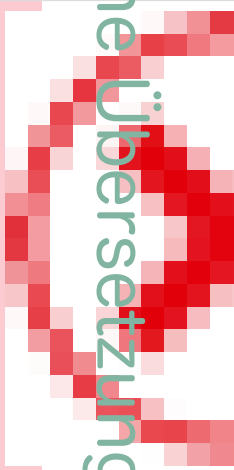
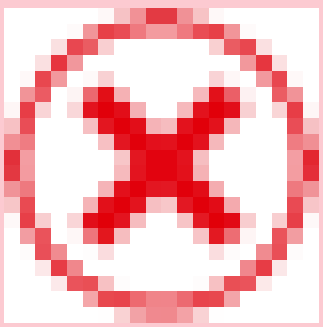
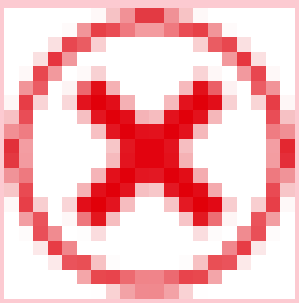
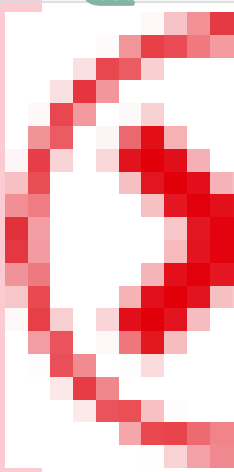
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Integrationsfähigkeiten-Flows				
Fähigkeitsausführungen				
Ratenbegrenzung für Fähigkeitsimplementierungen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Integrationskonfigurationen	✓	✓	✗	✗
Sichtungssuche – Konfiguration	✓	✓	✗	✗
Integrationsfunktionen	✓	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
E-Mail-Verarbeitung				
E-Mail-Analyse	✓	✓	✗	✗
Duplizierungsregeln	✓	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Eigenschaften	✓	✓	✗	✗
Nicht übereinstimmende E-Mails	✓	✓	✗	✗
Erfassungsregeln – Anwender Hat Phishing Gemeldet	✗	✗	✗	✗

Automatische Übersetzung

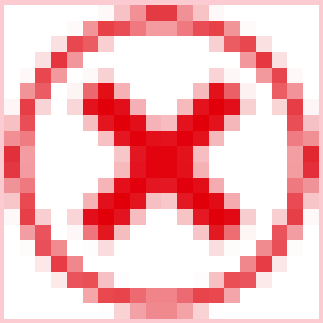
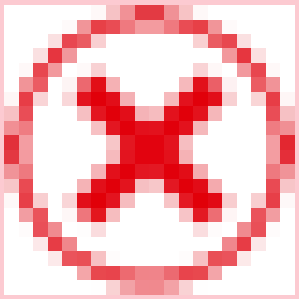
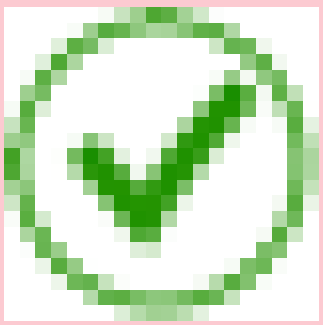
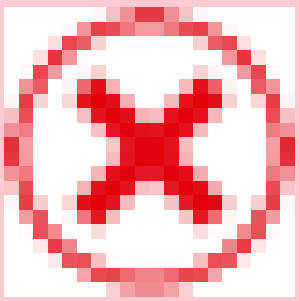
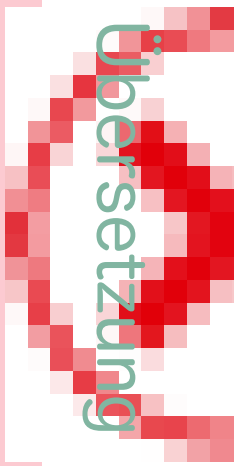
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Eigenschaften des vom Anwender gemeldeten Phishing				
Gruppen				
Filtergruppen				

Automatische Übersetzung

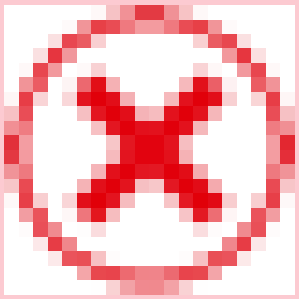
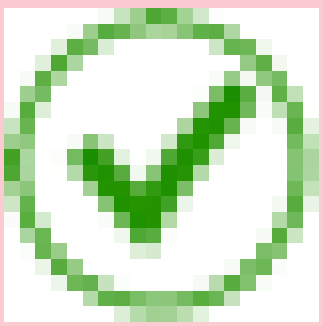
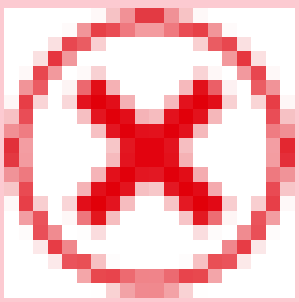
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Eskalationen				
Datenergänzungen				
Sicherheits-Tags				
Gruppen				

Automatische Übersetzung

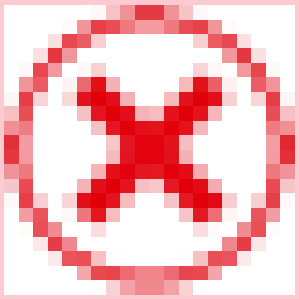
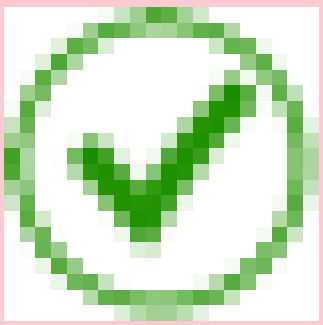
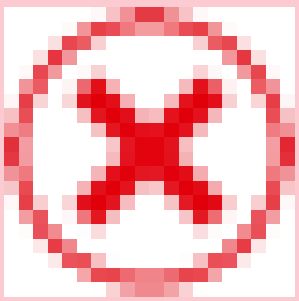
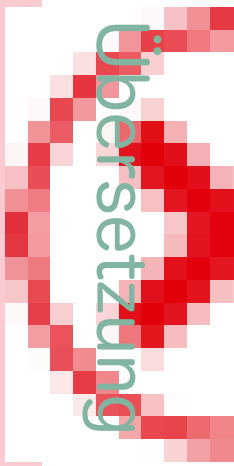
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Tags				
Workflows				
Ausführungsverfolgung				

Automatische Übersetzung

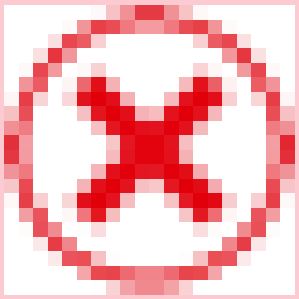
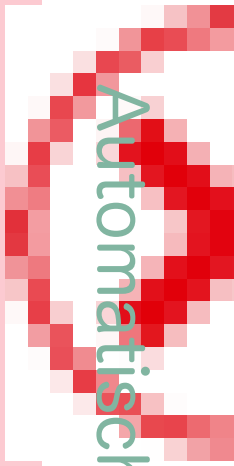
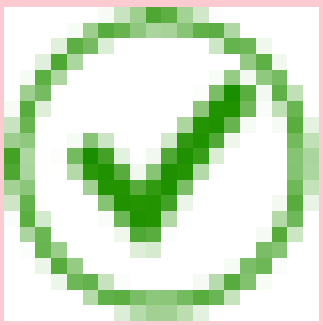
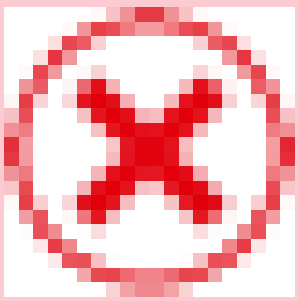
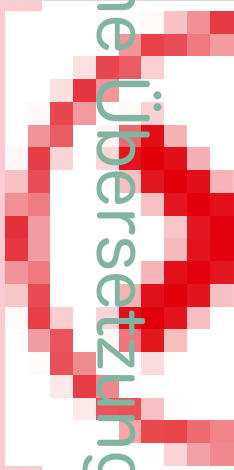
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Sicherheitsworkflows anzeigen				
Workflow-Auslöser				
Dienstprogramme				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Ergänzungsdatenzuordnung	✓	✓	✗	✗
Feldwertumwandlungen	✓	✓	✗	✗
Feldzuordnung	✓	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
OnDemand-Orchestration	✓	✗	✗	✗
Betriebssystemgruppen	✓	✓	✗	✗
SecOps-Applikationsregistrierung	✓	✗	✗	✗

Automatische Übersetzung

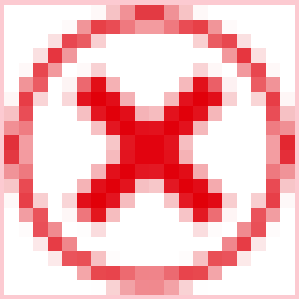
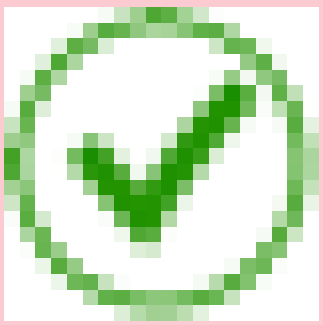
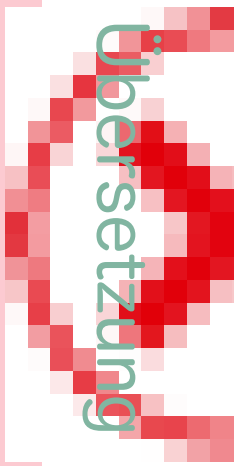
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Hintergrundauftrags-Konfiguration				
CMDB				
CI-Suchregeln				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
Erkannte Elemente	✓	✓	✓	✗
Nicht übereinstimmende erkannte Elemente abstimmen	✓	✓	✗	✗
Erkannte Container-Images	✓	✓	✗	✗

Automatische Übersetzung

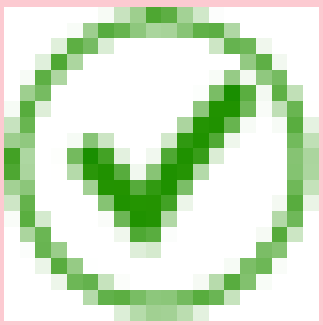
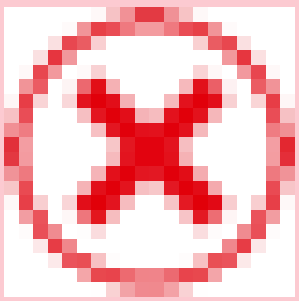
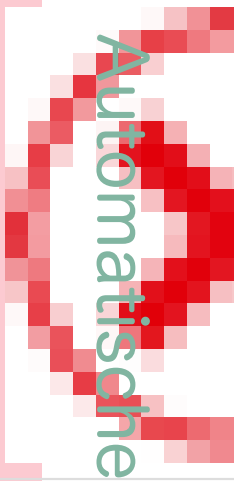
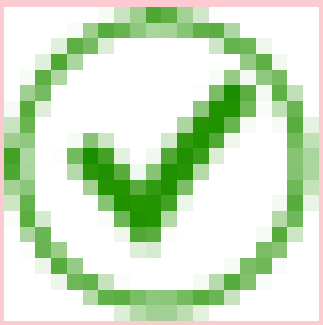
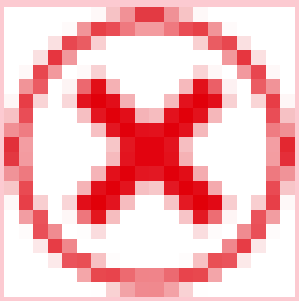
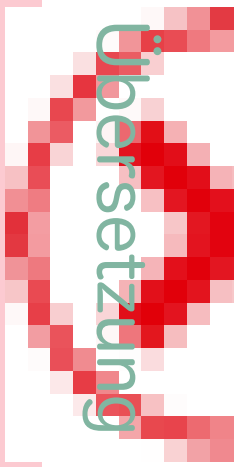
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: admin, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Informationen für andere Rollen:

sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

(Fortsetzung)

Modul	Administrator	sn_sec_cmn. Administrator	sn_sec_cmn. ci_Manager	sn_sec_cmn. Manag
WatchDog				
Konfiguration				
Übersicht				

Automatische Übersetzung

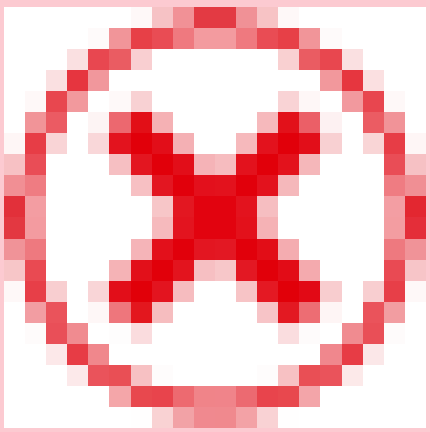
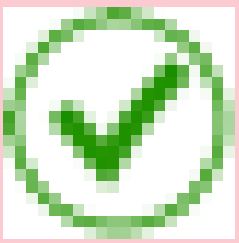
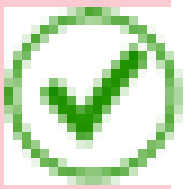
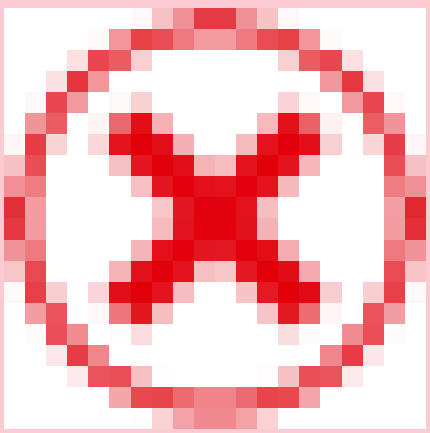
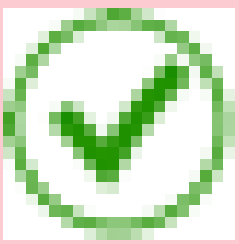
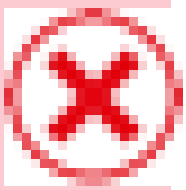
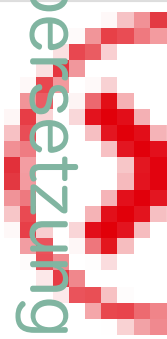
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
(Haupt-App-Gruppe)				
Integrationen				
Integrationsfähigkeiten-Flows				

Automatische Übersetzung

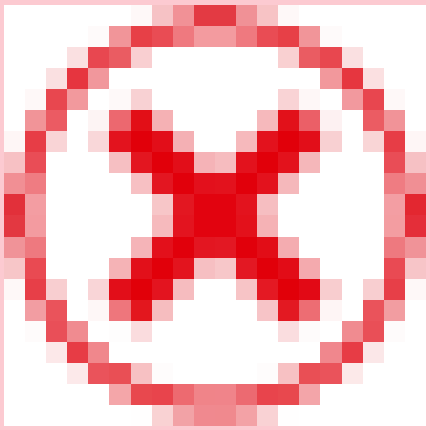
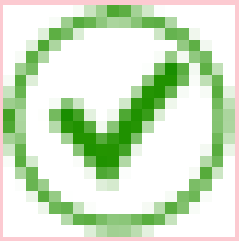
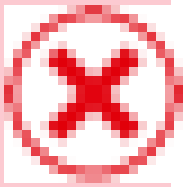
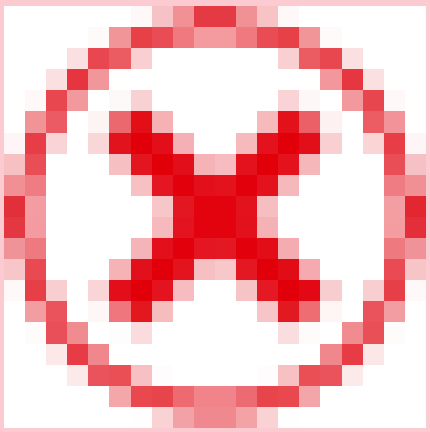
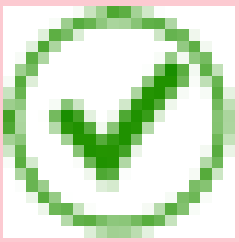
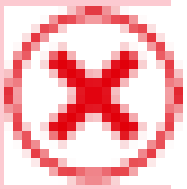
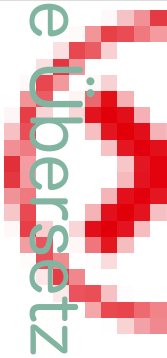
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Fähigkeitsausführungen				
Ratenbegrenzung für Fähigkeitsimplementierungen				

Automatische Übersetzung

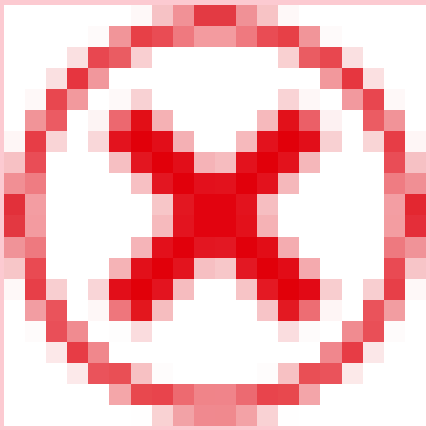
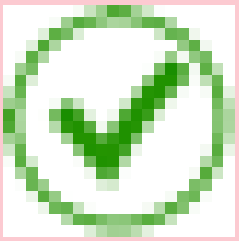
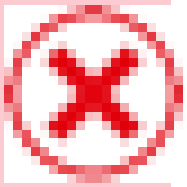
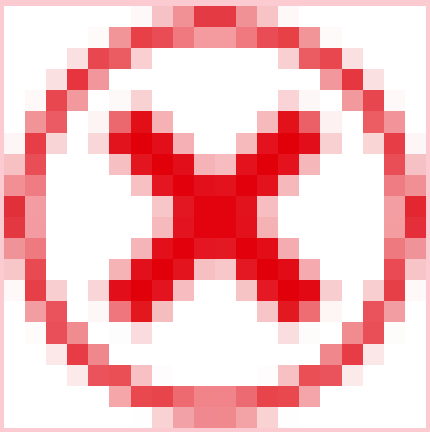
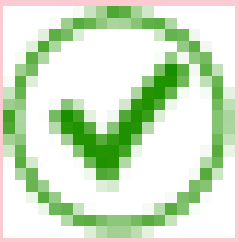
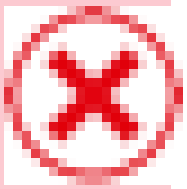
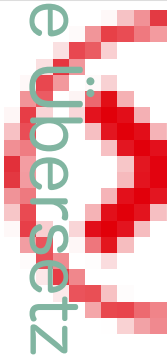
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Integrationskonfigurationen				
Sichtungssuche – Konfiguration				

Automatische Übersetzung

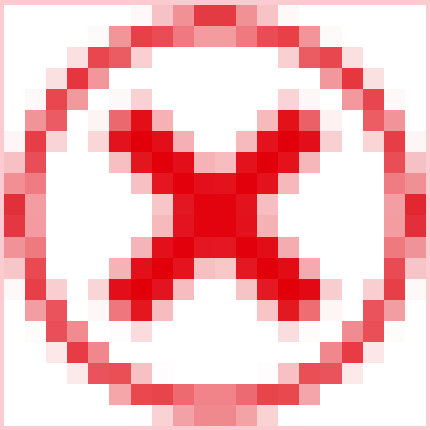
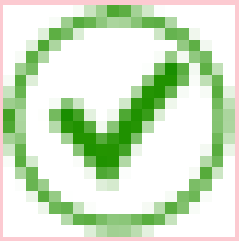
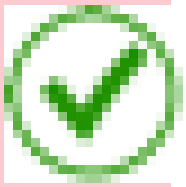
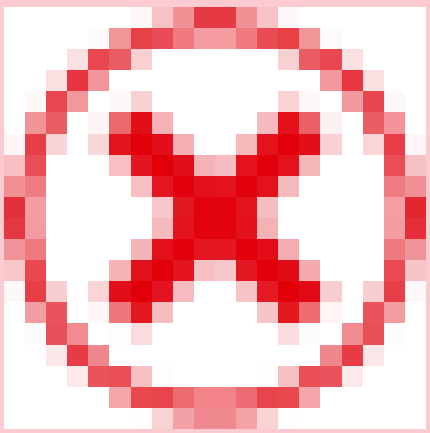
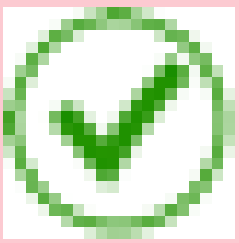
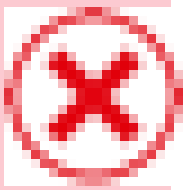
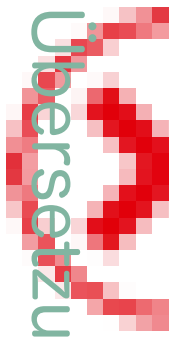
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Integrationsfunktionen				
Integrationen				
Integrationsfähigkeiten-Flows				

Automatische Übersetzung

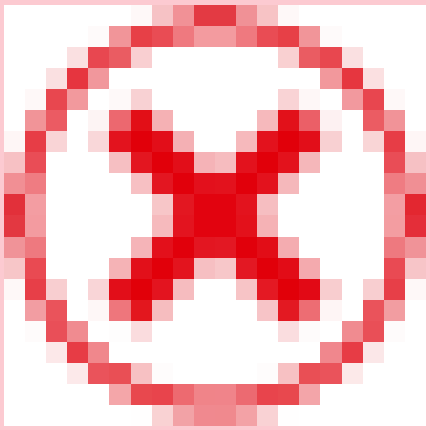
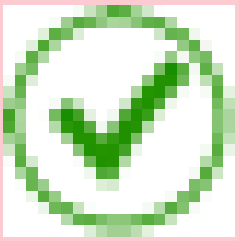
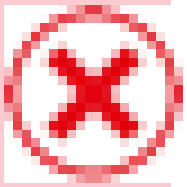
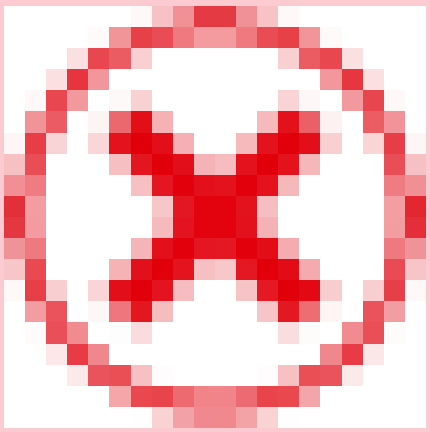
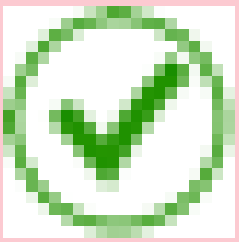
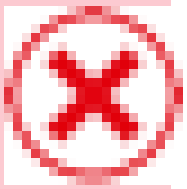
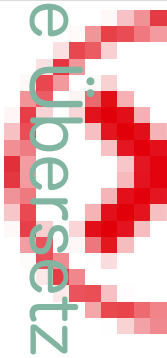
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Fähigkeitsausführungen				
Ratenbegrenzung für Fähigkeitsimplementierungen				

Automatische Übersetzung

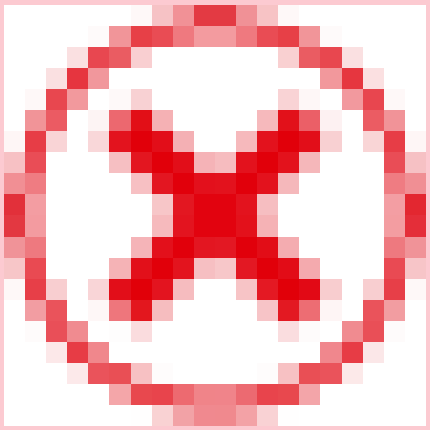
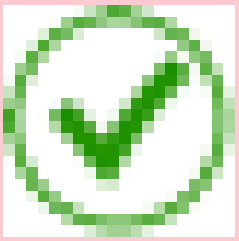
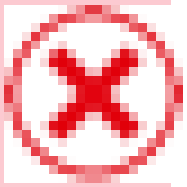
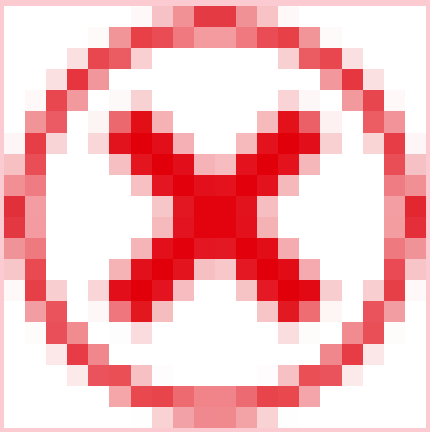
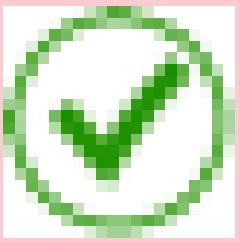
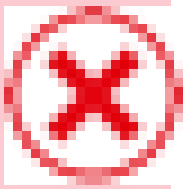
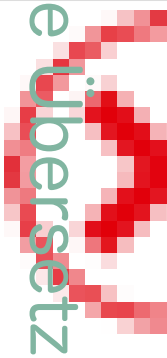
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Integrationskonfigurationen				
Sichtungssuche – Konfiguration				

Automatische Übersetzung

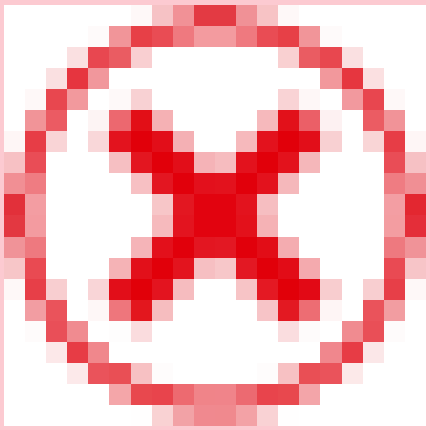
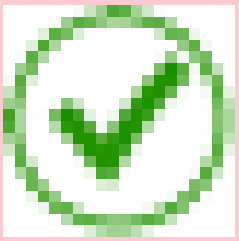
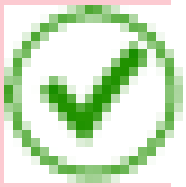
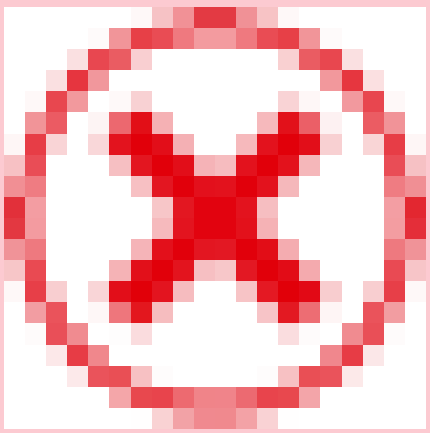
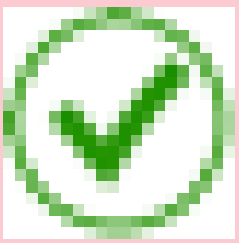
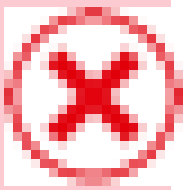
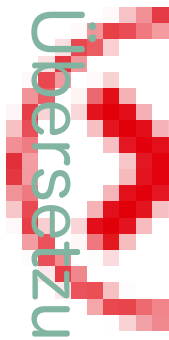
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Integrationsfunktionen				
E-Mail-Verarbeitung				
E-Mail-Analyse				

Automatische Übersetzung

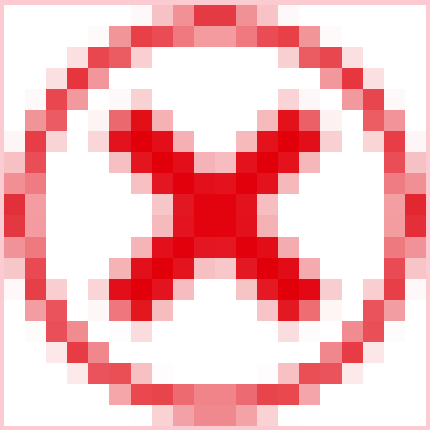
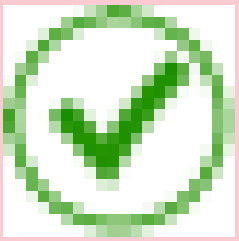
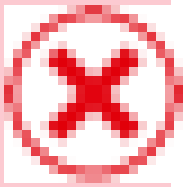
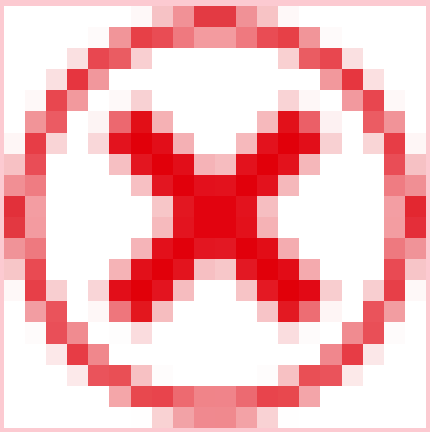
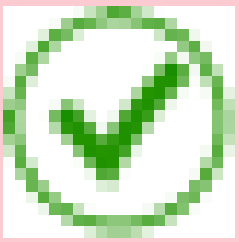
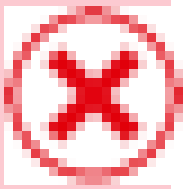
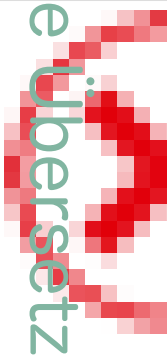
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Duplizierungsregeln				
Eigenschaften				

Automatische Übersetzung

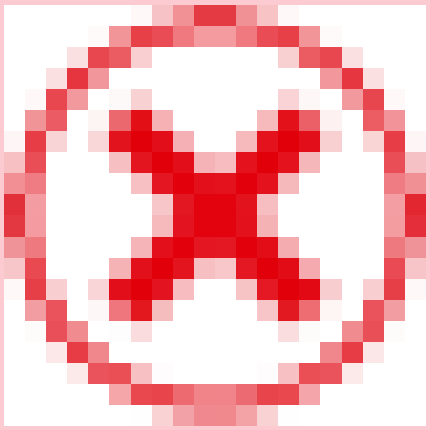
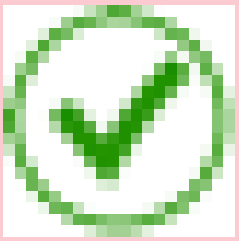
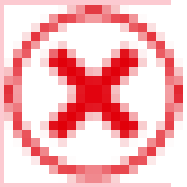
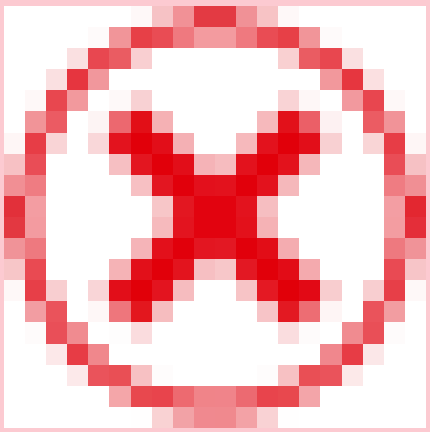
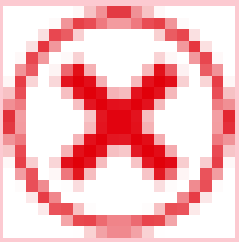
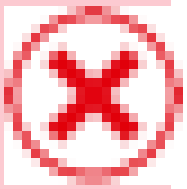
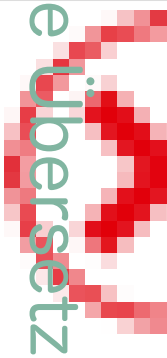
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Nicht übereinstimmende E-Mails				
Erfassungsregeln – Anwender Hat Phishing Gemeldet				

Automatische Übersetzung

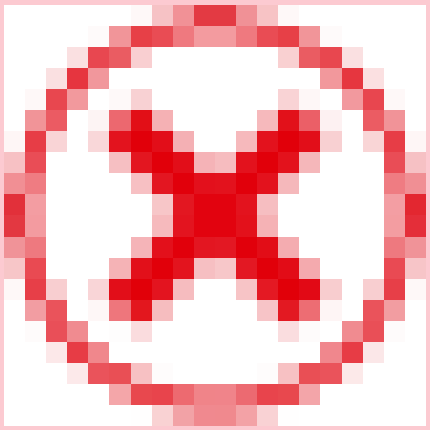
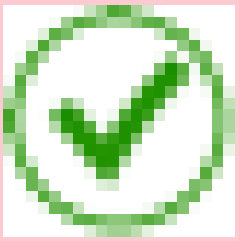
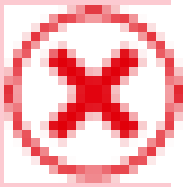
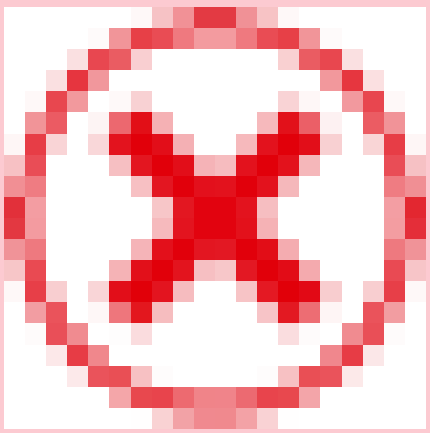
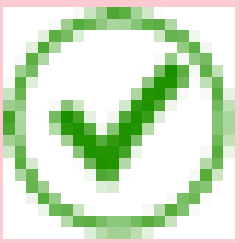
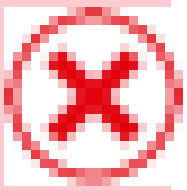
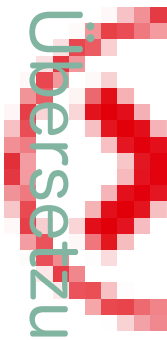
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Eigenschaften des vom Anwender gemeldeten Phishing				
Gruppen				
Filtergruppen				

Automatische Übersetzung

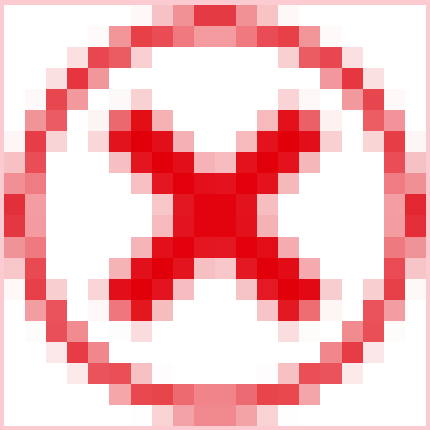
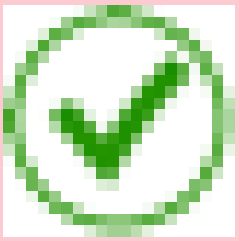
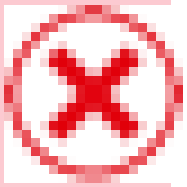
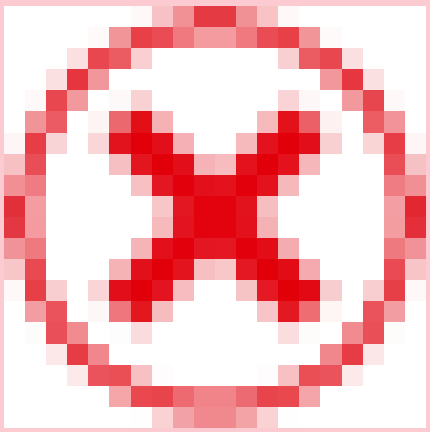
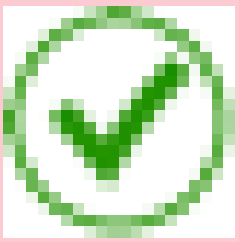
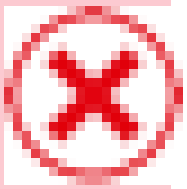
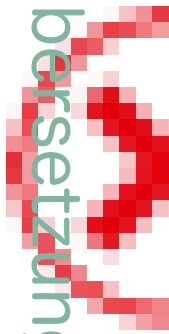
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Eskalationen				
Datenergänzungen				
Sicherheits-Tags				
Gruppen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Tags	✗	✓	✗	✗
Workflows				
Ausführungsverfolgung	✗	✓	✗	✗

Automatische Übersetzung

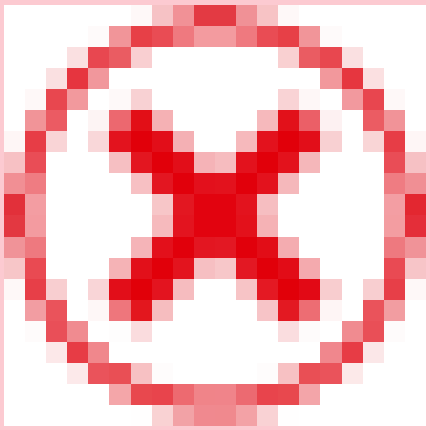
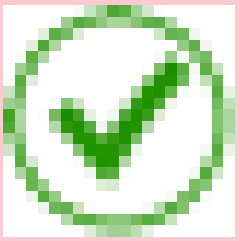
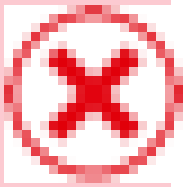
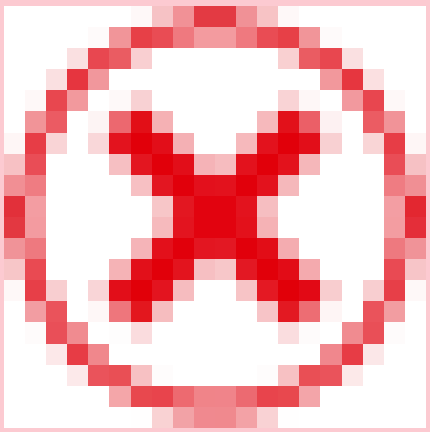
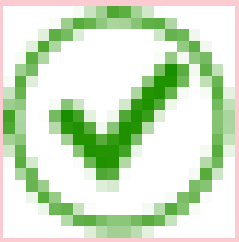
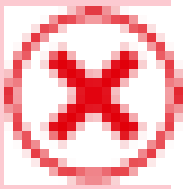
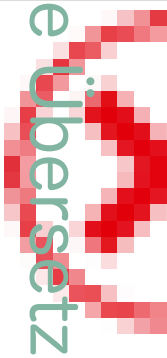
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Sicherheitsworkflows anzeigen				
Workflow-Auslöser				
Dienstprogramme				

Automatische Übersetzung

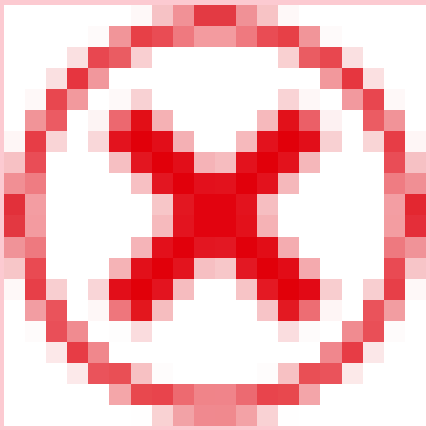
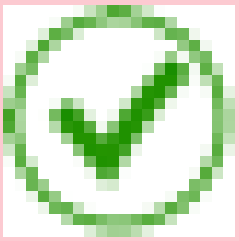
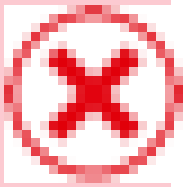
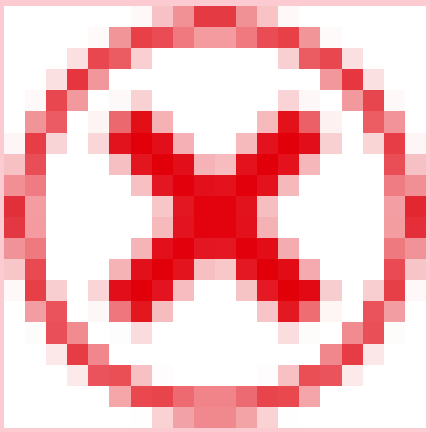
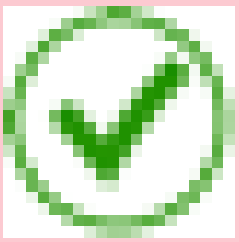
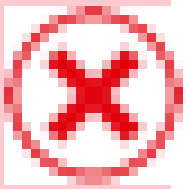
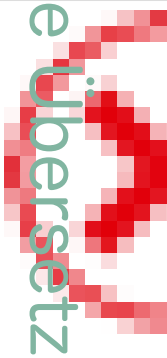
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Ergänzungsdatenzuordnung				
Feldwertumwandlungen				

Automatische Übersetzung

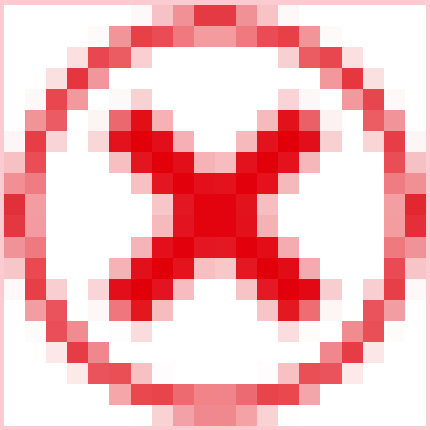
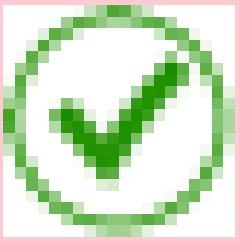
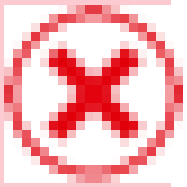
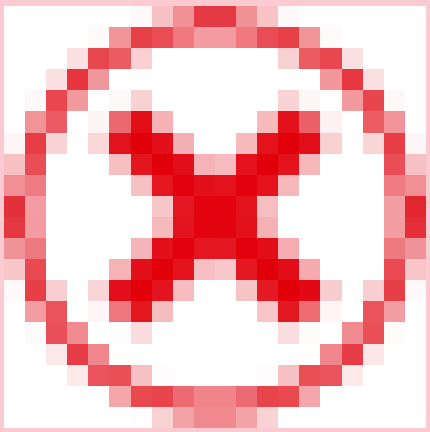
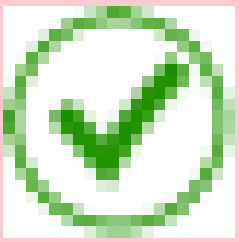
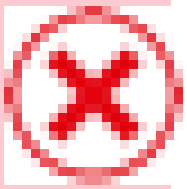
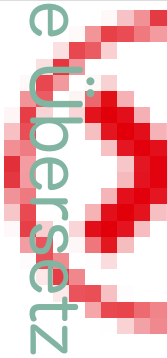
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Feldzuordnung				
OnDemand-Orchestration				

Automatische Übersetzung

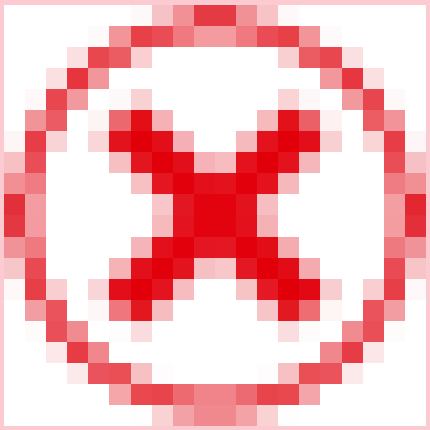
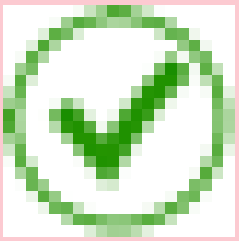
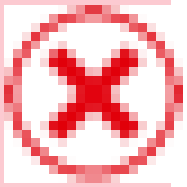
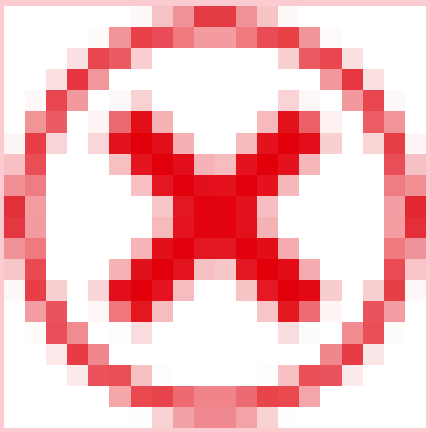
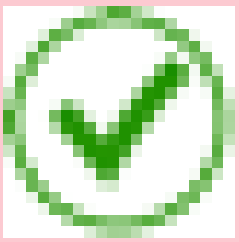
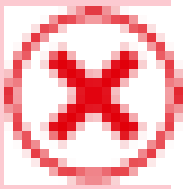
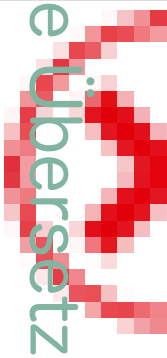
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Betriebssystemgruppen				
SecOps-Applikationsregistrierung				

Automatische Übersetzung

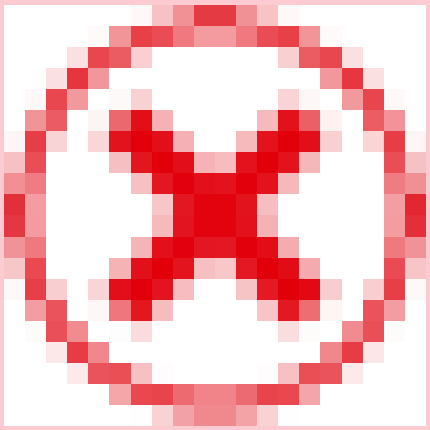
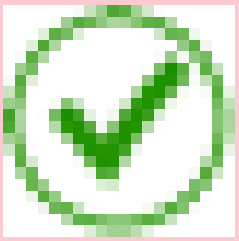
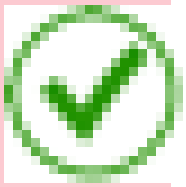
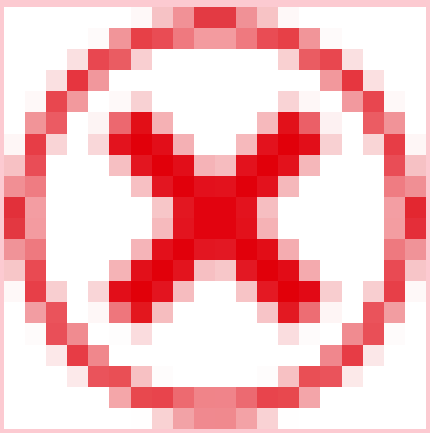
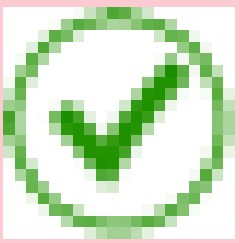
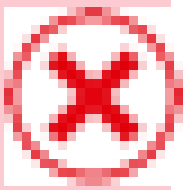
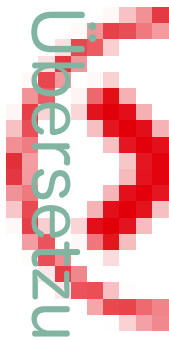
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Hintergrundauftrags-Konfiguration				
CMDB				
CI-Suchregeln				

Automatische Übersetzung

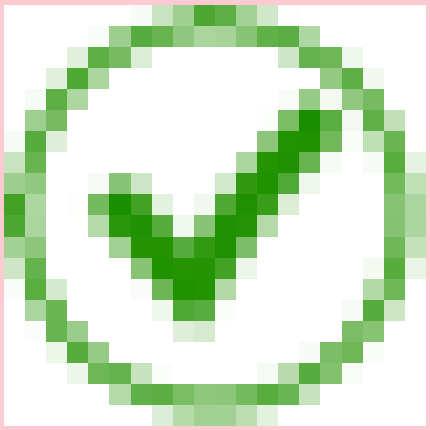
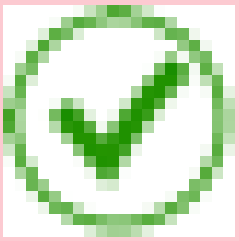
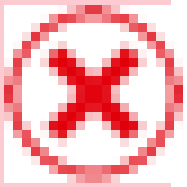
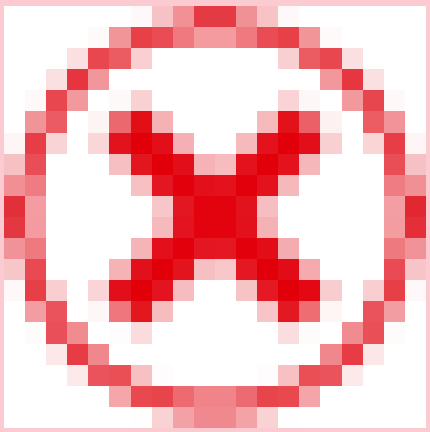
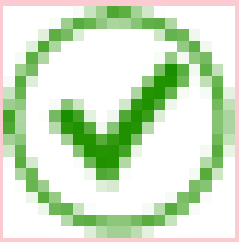
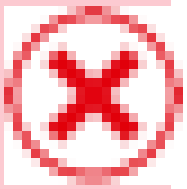
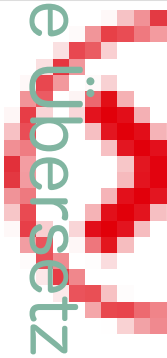
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Erkannte Elemente				
Nicht übereinstimmende erkannte Elemente abstimmen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Erkannte Container-Images	✗	✓	✗	✗
WatchDog				
Konfiguration	✗	✓	✓	✗

Automatische Übersetzung

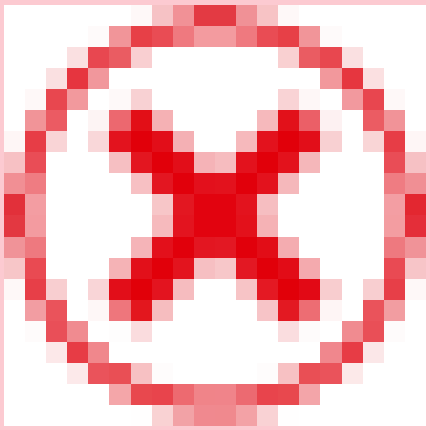
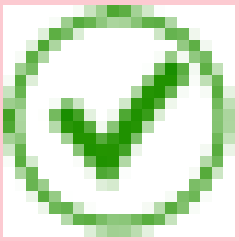
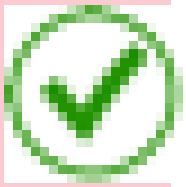
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.reclassify_unmatch_ci, sn_si.admin, sn_si.Basic, sn_vul.read_discovered_item, sn_vul_Container.read_discovered_image

Informationen für andere Rollen:

administrator, sn_sec_cmn.admin, sn_sec_cmn.ci_Manager, sn_sec_cmn.Manage_background_Job, sn_sec_cmn.read, sn_sec_cmn.read_background_Job

(Fortsetzung)

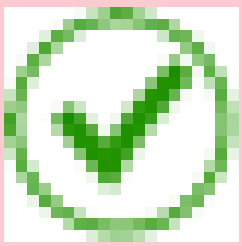
Modul	sn_sec_cmn. Reklassify_Unmatch_ci	sn_si. Administrator	sn_si. Standard	sn_vul. Read_
Übersicht				

[End]

[store-future: BEGIN review]

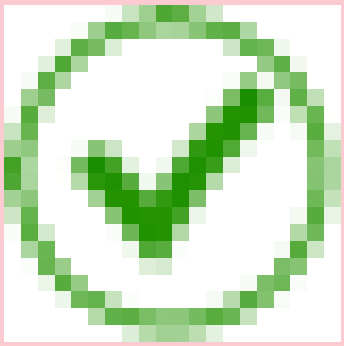
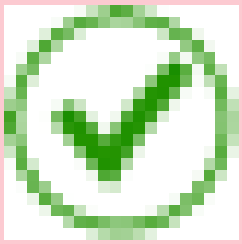
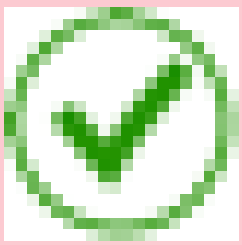
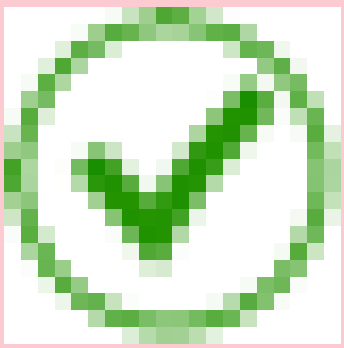
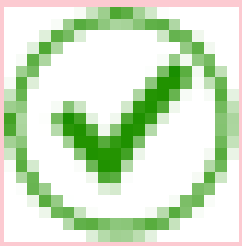
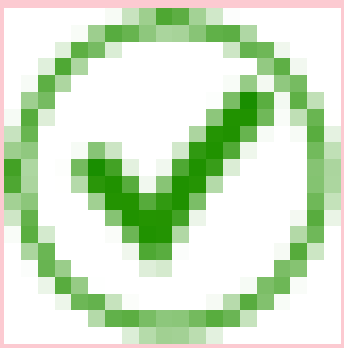
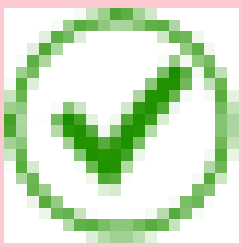
Modulzugriff nach Rolle für Splunk-Integration

Informationen zur Splunk-Integration finden Sie in den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

Modul	sn_si. Administrator	sn_si. Analyst
(Haupt-App-Gruppe)		
Splunk-Ereignisprofile		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst
Splunk-Feld-Übersetzungen		
Splunk-Ereignis zu Aufgaben		
Splunk-Ereignisimport		
Einstellungen von Splunk Integration		

[End]

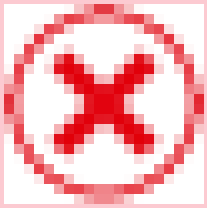
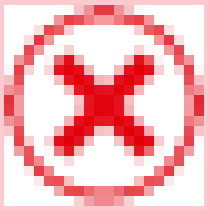
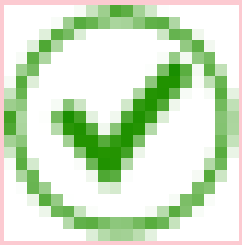
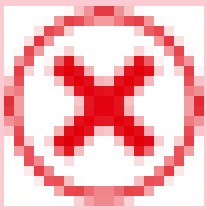
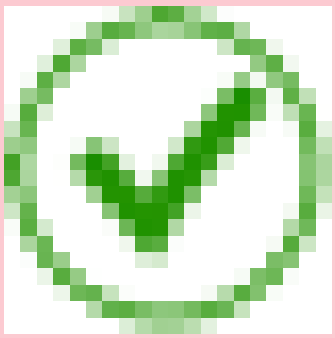
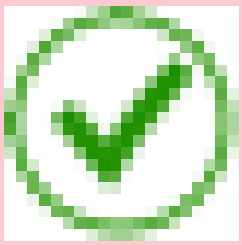
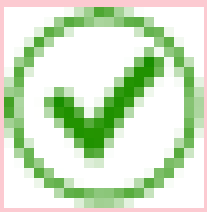
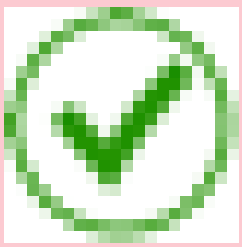
[store-future: BEGIN review]

Modulzugriff nach Rolle für Symantec DLP-Integration

Informationen zur Symantec DLP-Integration finden Sie in den Menüelementen, auf die eine bestimmte Rolle zugreifen kann.

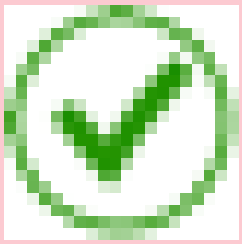
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	agent_admin	sn_dlir. Administrator	sn_dlir. Analyst
(Haupt-App-Gruppe)			
Incident-Profil			
Incident-Statuszuordnung			
Einstellungen			
MID-Anwendung			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

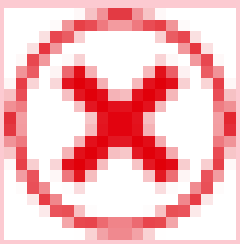
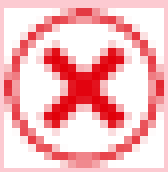
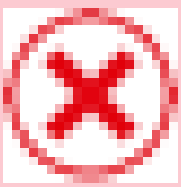
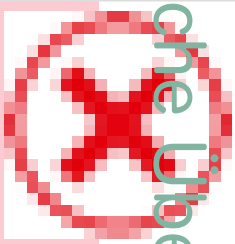
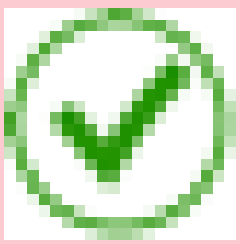
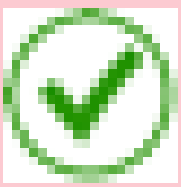
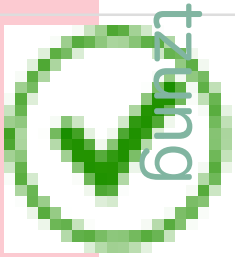
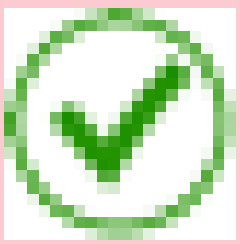
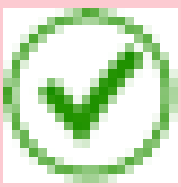
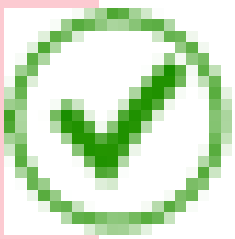
Modul	agent_admin	sn_dlir. Administrator	sn_dlir. Analyst
MID-Server			

[End]

[store-future: BEGIN review]

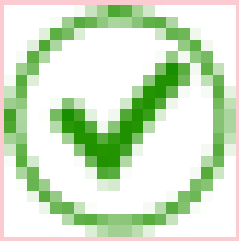
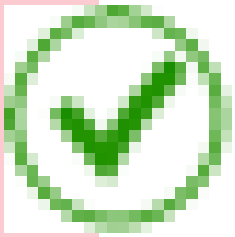
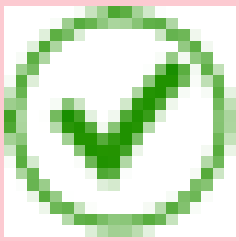
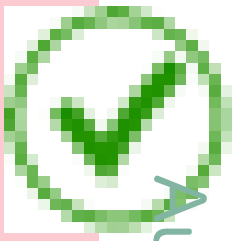
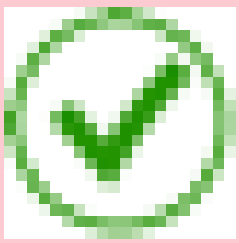
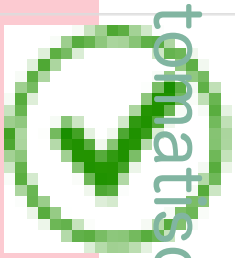
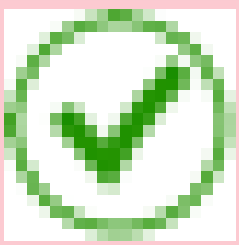
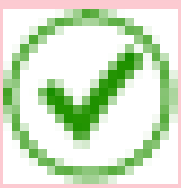
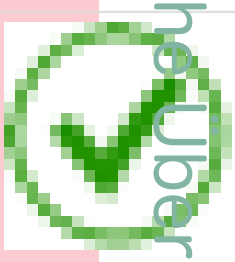
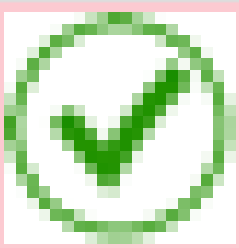
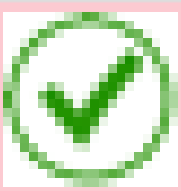
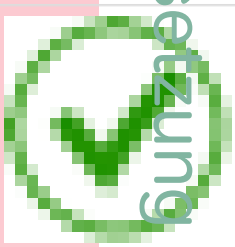
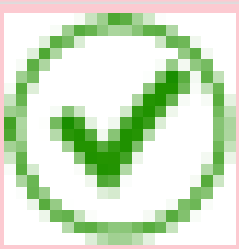
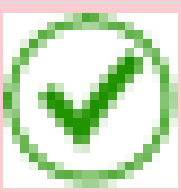
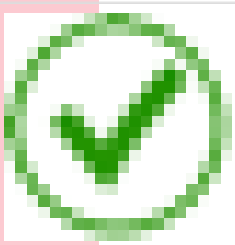
Modulzugriff nach Rolle für Threat Intelligence

Informationen zu Threat Intelligence finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
(Haupt-App-Gruppe)						
Objekte						
Objekte						
IoC-Repository						
AngriffsmodusMethods						
Indikatoren						

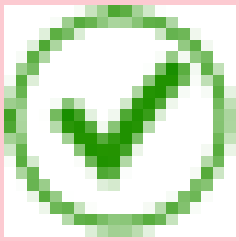
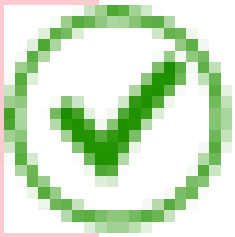
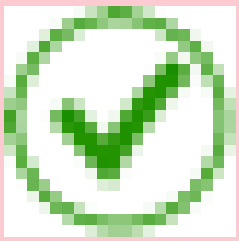
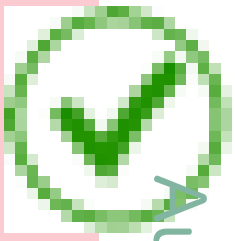
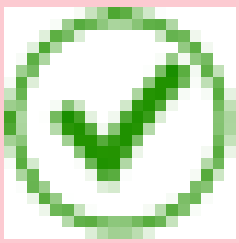
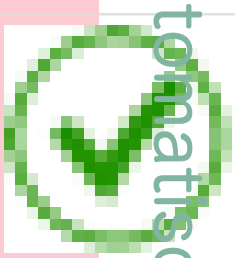
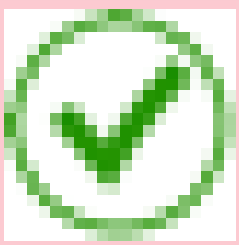
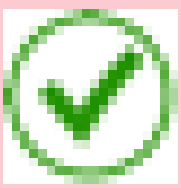
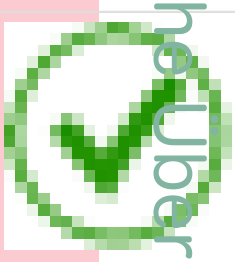
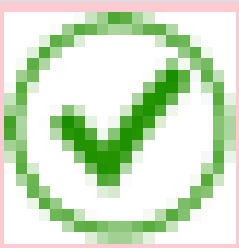
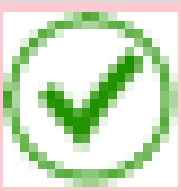
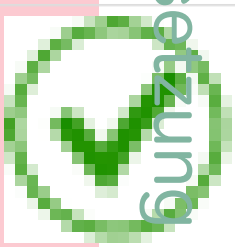
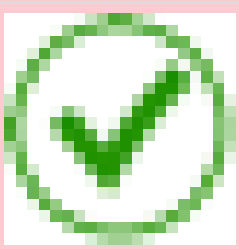
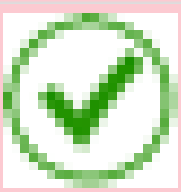
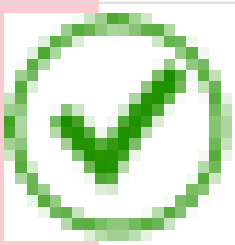
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Erkennbare Elemente						
Angriffsmuster						
Kampagnen						
Vorgehensweisen						
Identitäten						
Infrastruktur						

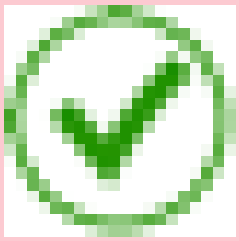
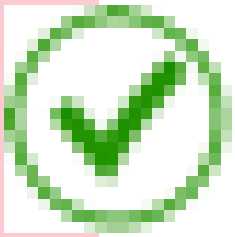
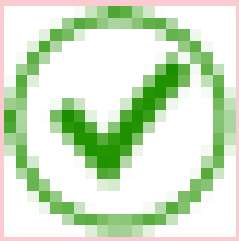
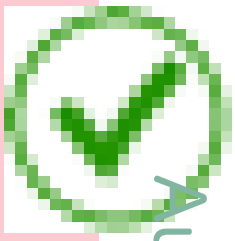
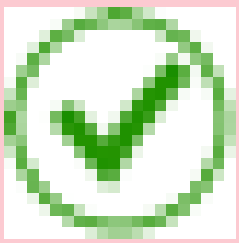
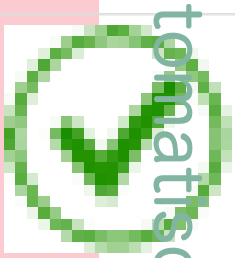
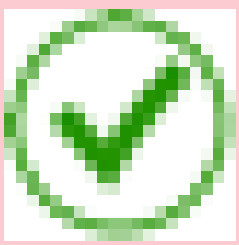
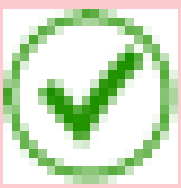
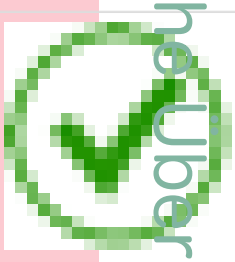
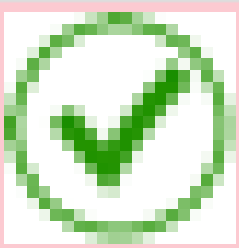
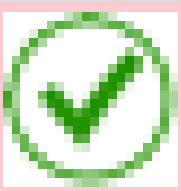
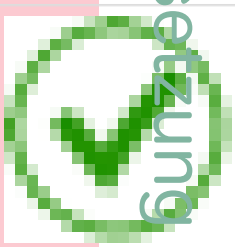
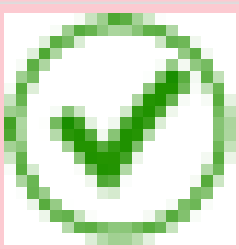
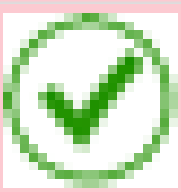
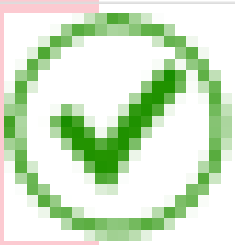
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Standorte						
Malware						
Angriffssatz						
Bedrohungsakteure						
Malware-Analyse						
Beobachtete Daten						

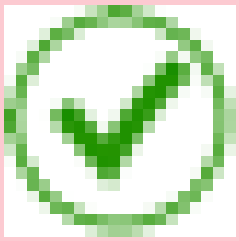
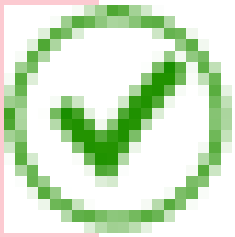
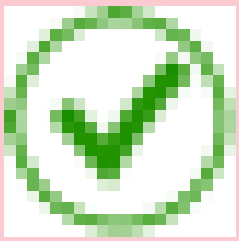
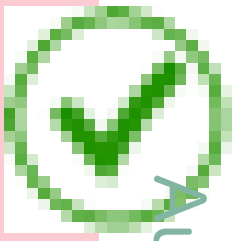
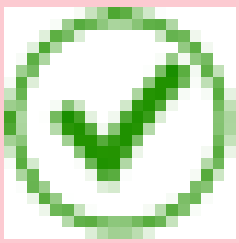
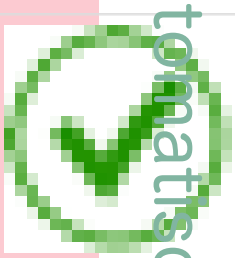
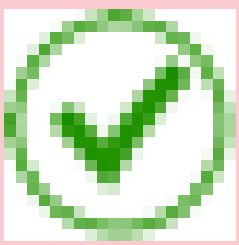
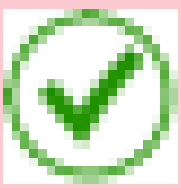
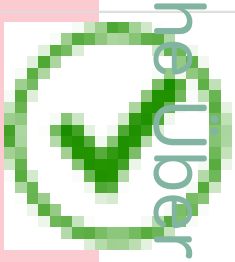
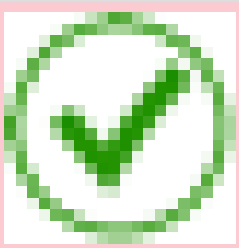
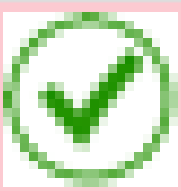
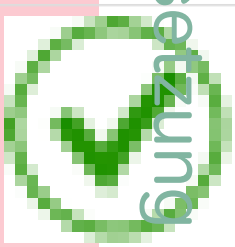
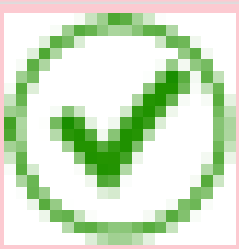
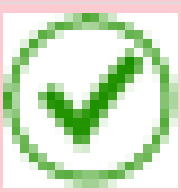
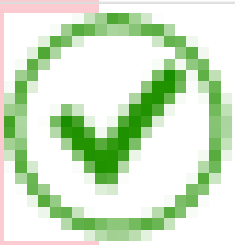
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Bedrohungsgruppierungen						
Markierungsdefinitionen						
Bedrohungshinweise						
Bedrohungsmeinungen						
Bedrohungsberichte						
Indikatorsichtungen						

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Objektsichtungen						
Schwachstellen						
Tools						
ObjectObject-Beziehungen						
ObjectIndicator-Beziehungen						
ObjectObservable-Beziehungen						
Quellen						

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Bedrohungsquellen	✗	✗	✗	✗	✓	
TAXII-Profile	✗	✗	✗	✗	✓	
Externe Intelligenz						
Datenschutzverletzung – Bibliothek	✓	✓	✓	✓	✓	
WHOIS-Bibliothek	✓	✓	✓	✓	✓	
Administration						
Eigenschaften	✗	✗	✗	✗	✓	
Angriffsmechanismen	✗	✗	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Angriffsmotivationen	✗	✗	✗	✗	✓	
Discovery-Methoden	✗	✗	✗	✗	✓	
Feeds	✗	✗	✗	✗	✓	
Indikatortypen	✗	✗	✗	✗	✓	
Infrastrukturtypen	✗	✗	✗	✗	✓	
Beabsichtigte Wirkungen	✗	✗	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Malware-Fähigkeiten	✗	✗	✗	✗	✓	
Schadsoftwaretypen	✗	✗	✗	✗	✓	
Benachrichtigungen	✗	✗	✗	✗	✓	
Erkennbare Typen	✗	✗	✗	✗	✓	
Quotengrenzdefinitionen	✗	✗	✗	✗	✓	
Berichtstypen	✗	✗	✗	✗	✓	

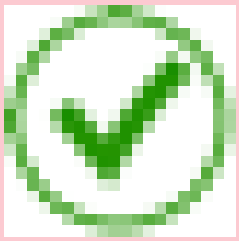
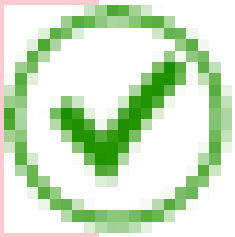
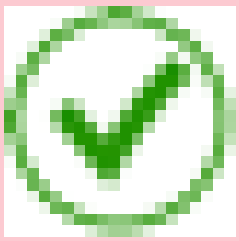
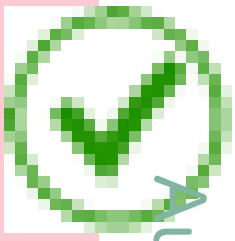
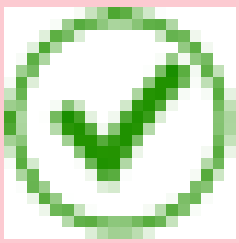
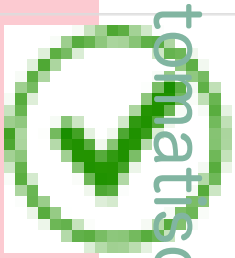
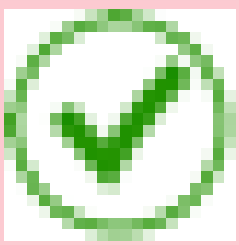
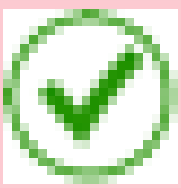
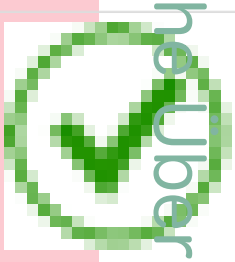
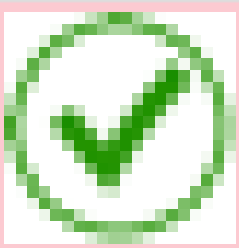
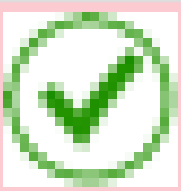
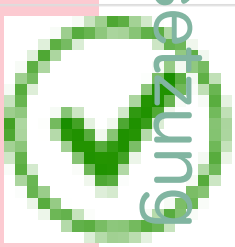
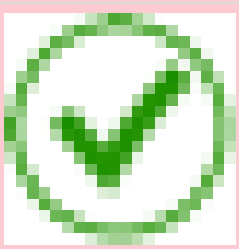
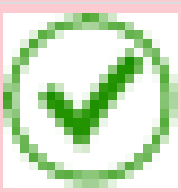
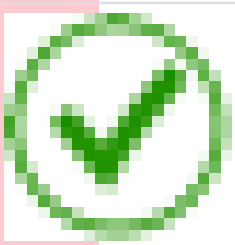
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Bedrohungsakteurrollen	✗	✗	✗	✗	✓	
Bedrohungsakteurtypen	✗	✗	✗	✗	✓	
Tooltypen	✗	✗	✗	✗	✓	
Fallmanagement						
Alle Fälle	✗	✗	✗	✗	✗	
Offene Fälle	✗	✗	✗	✗	✗	
Meine Fälle	✗	✗	✗	✗	✗	
MITRE ATT&CK-Repository						

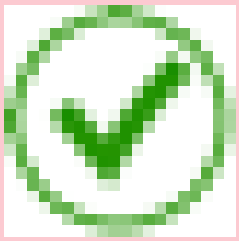
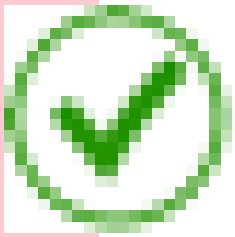
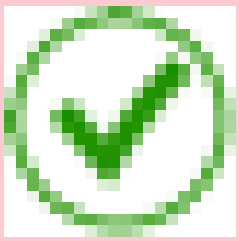
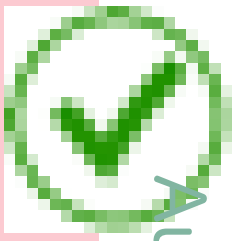
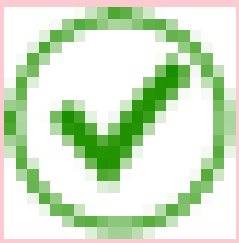
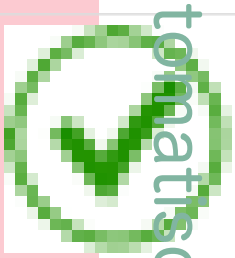
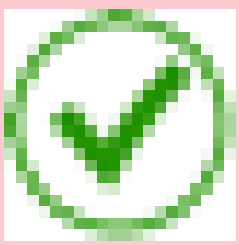
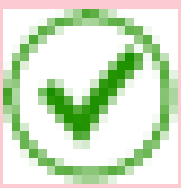
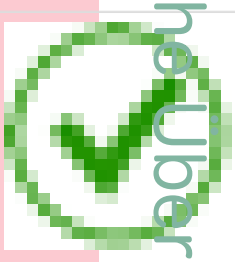
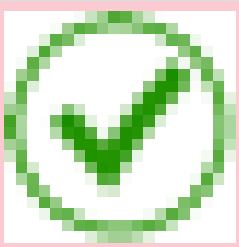
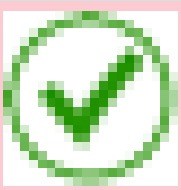
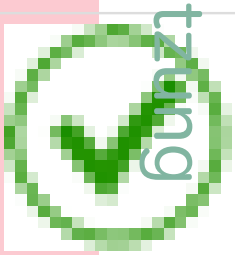
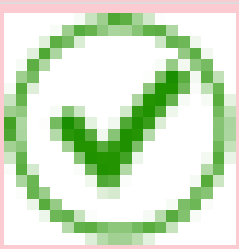
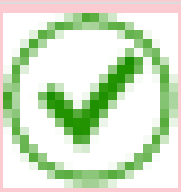
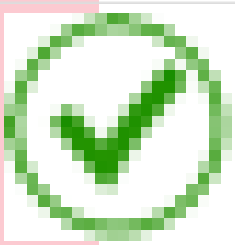
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Übersicht						
Matrizen						
Techniken						
Mitigationen						
Gruppen						
Malware						

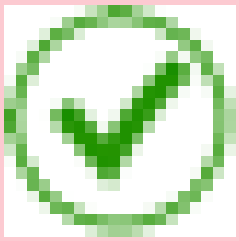
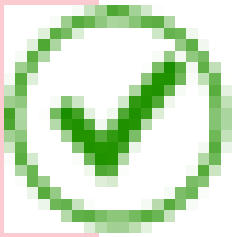
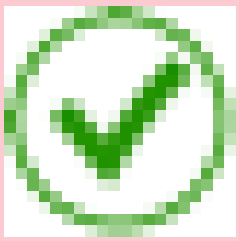
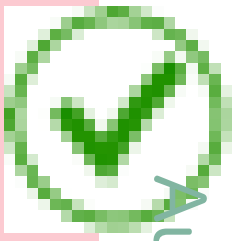
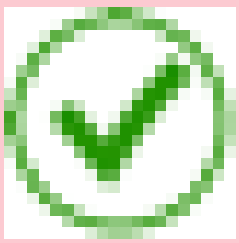
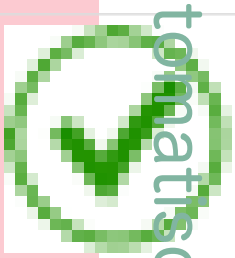
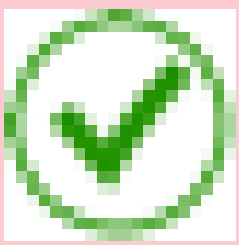
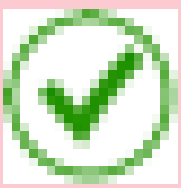
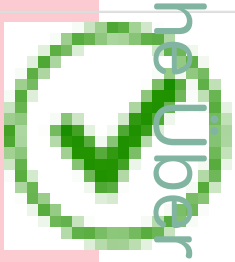
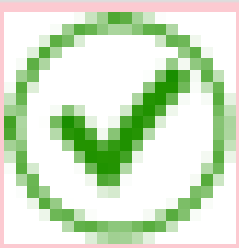
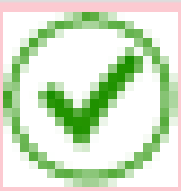
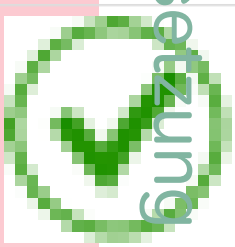
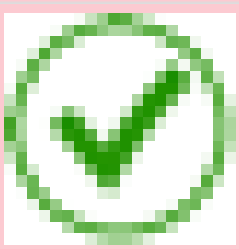
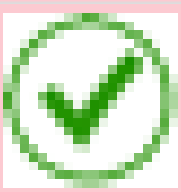
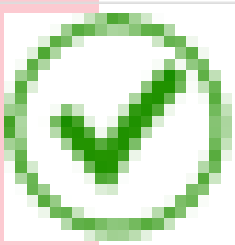
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Tools						
MITRE-Beziehungen						
Heatmap und Navigator						
CVE-Technikzuordnung						
MITRE ATT&CK-Administration						
Datenquellenzuordnung						
Datenkomponentenzuordnung						

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Definition der Erkennungsabdeckung						
Zuordnung der Abdeckung durch Erkennung						
Definition der Abdeckung durch Risikominderung						
Rechner für Abdeckung durch Risikominderung						
Zuordnung der Abdeckung durch Risikominderung						
Extraktionsregel für Technik						

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modul	sn_si. Administrator	sn_si. Analyst	sn_si. ciso	sn_si. Manager	sn_ti. Administrator	sn_
Erkennungsregeln MITRE ATTCK-Zuordnung	✓	✓	✓	✓	✓	
Heatmap-Definition für Threat GroupTechnique	✓	✓	✓	✓	✓	
Zuordnung der Threat GroupMITRE ATTCK-Technik	✓	✓	✓	✓	✓	
Eigenschaften	✓	✗	✗	✗	✓	

[End]

[store-future: BEGIN review]

Modulzugriff nach Rolle für Vulnerability Response

Informationen zu Vulnerability Response finden Sie in den Menüelementen, auf die von einer bestimmten Rolle zugegriffen werden kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

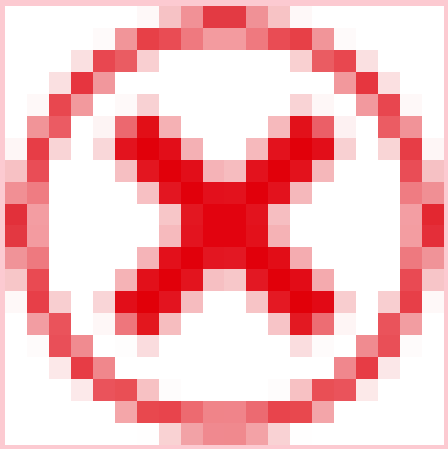
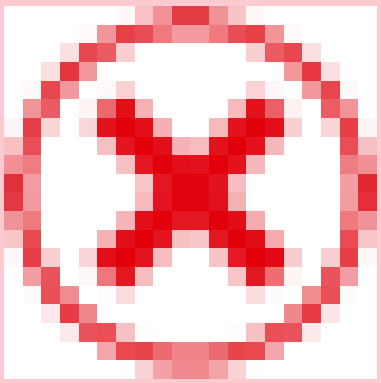
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
(Haupt-App-Gruppe)				
CISO-Dashboard				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

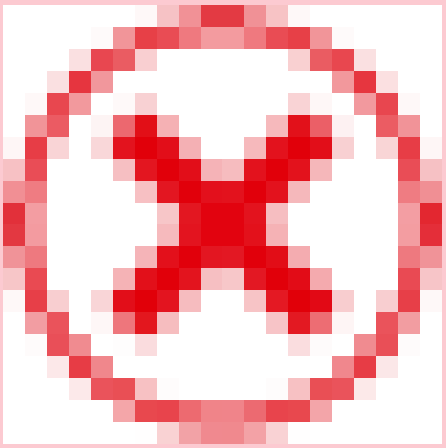
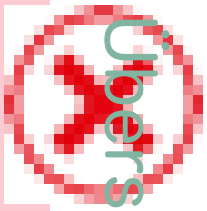
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Korrekturübersicht				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Arbeitsbereich des Schwachstellenmanagers	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

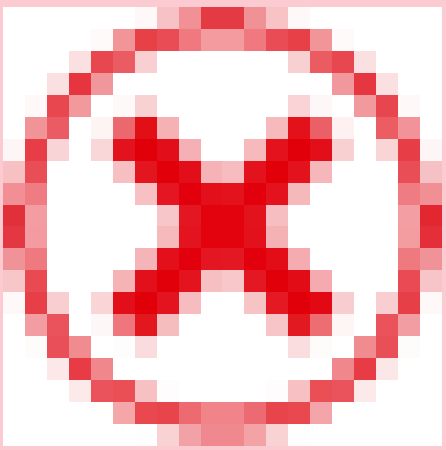
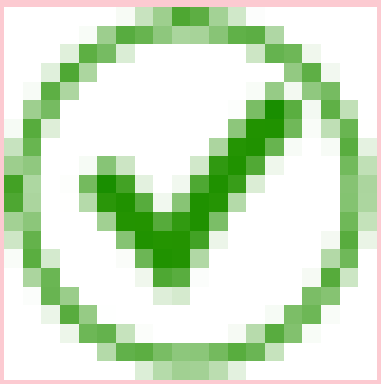
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Übersicht				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

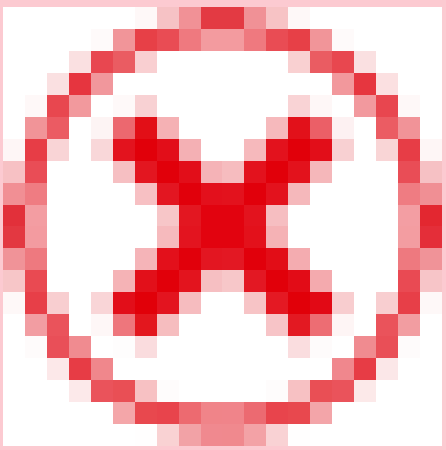
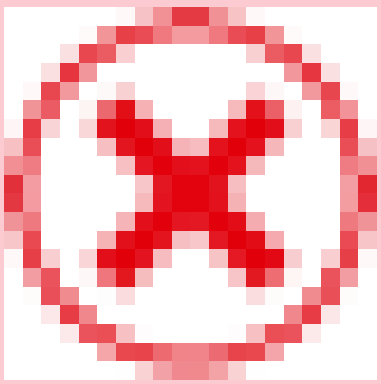
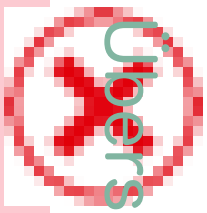
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Arbeitsbereich für IT-Korrekturen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

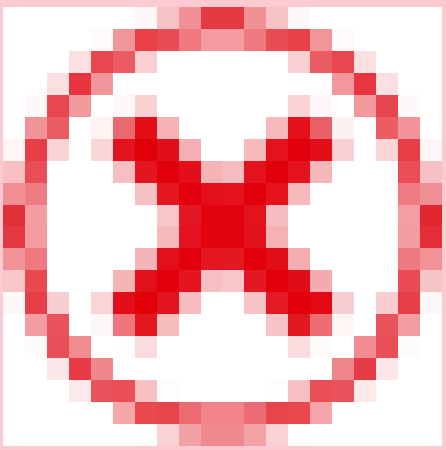
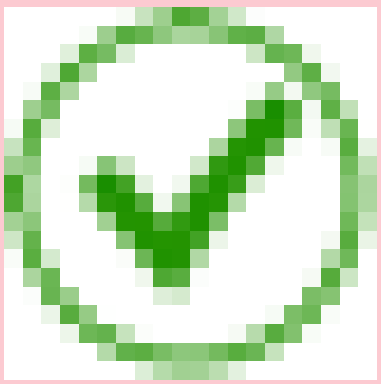
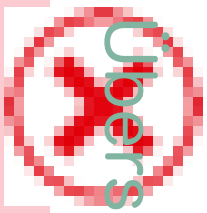
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Genehmiger-Übersicht				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

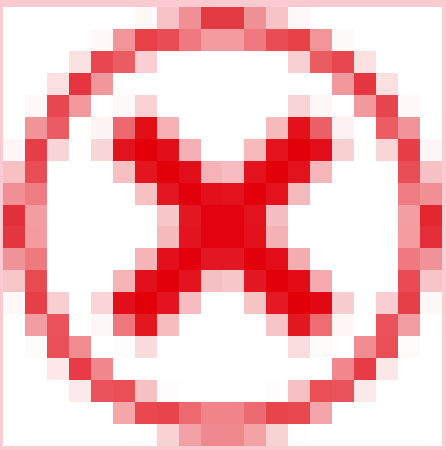
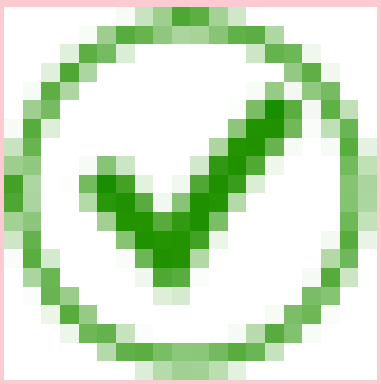
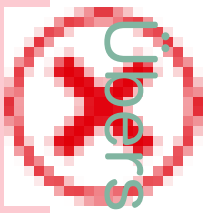
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Übersicht				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

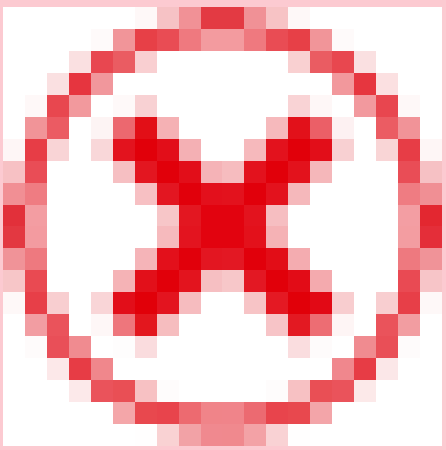
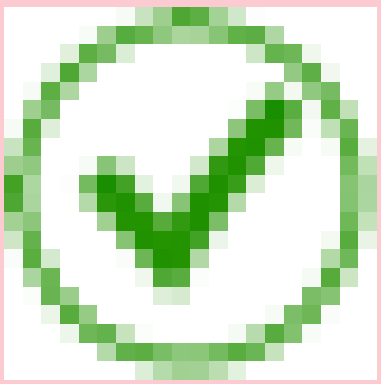
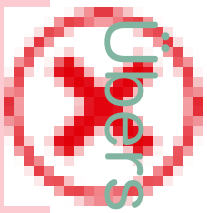
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Meine Genehmigungen				
Korrekturaufgaben				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

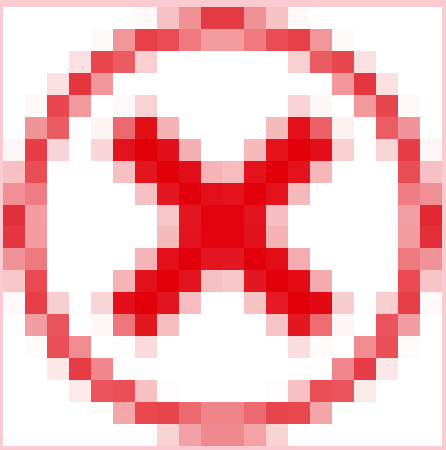
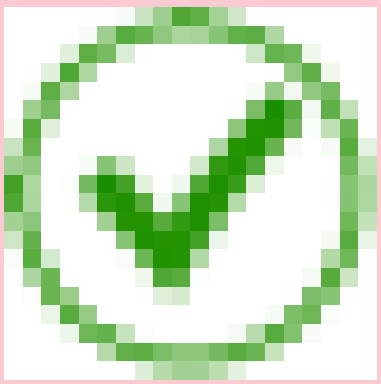
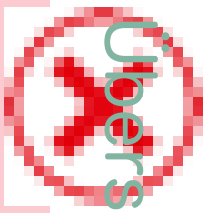
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Aktiv				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

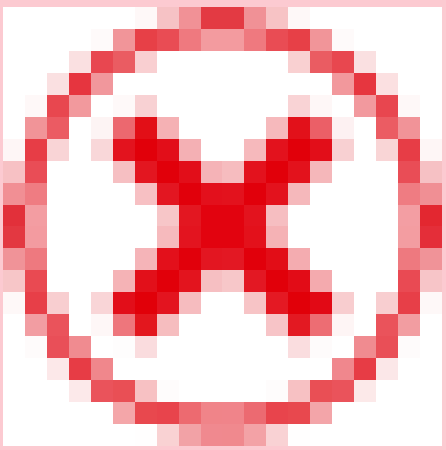
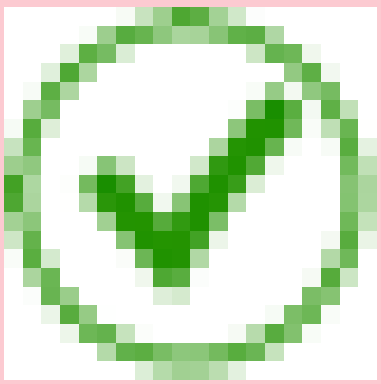
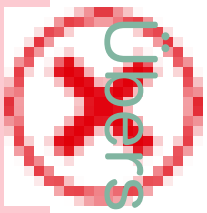
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Mir zugewiesen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

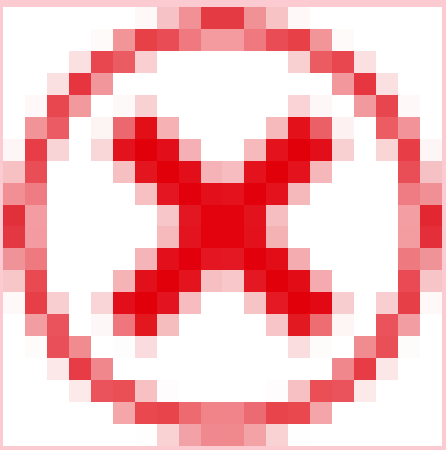
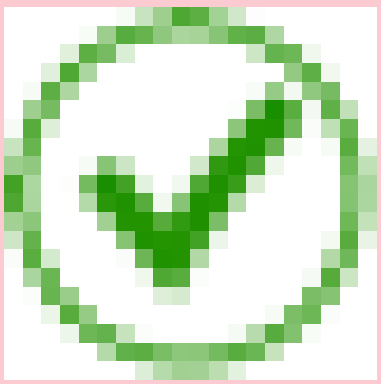
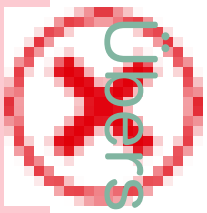
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Meinen Gruppen zugewiesen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

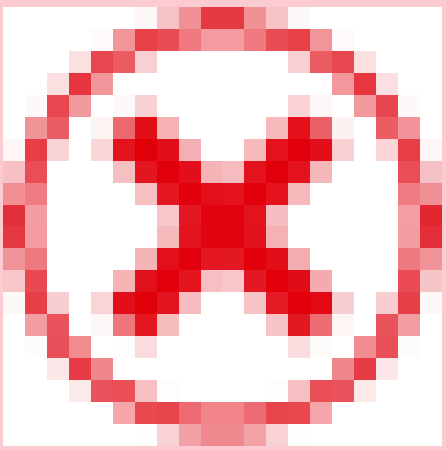
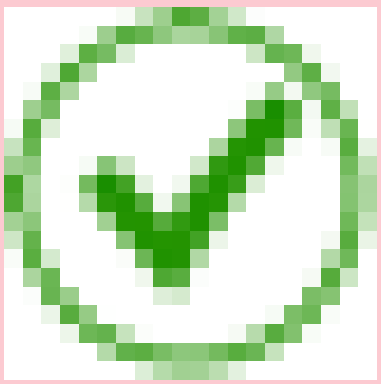
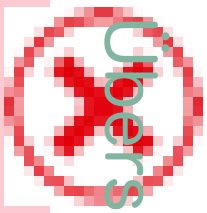
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Alle				
Angreifbare Elemente				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

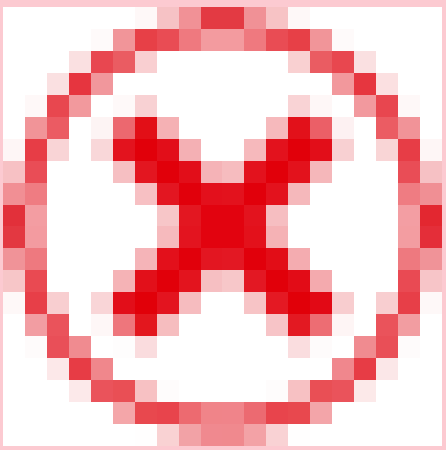
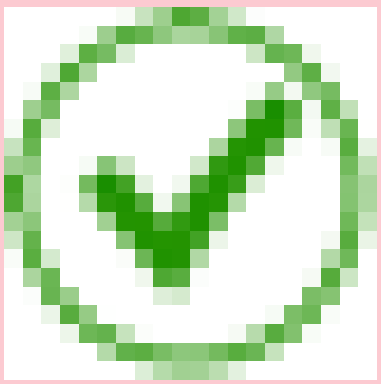
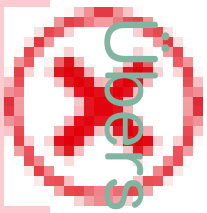
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Kritisches Risiko				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

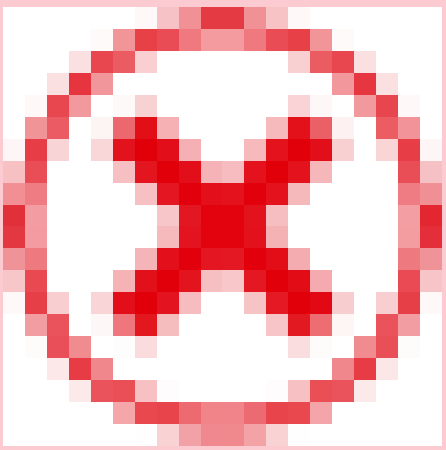
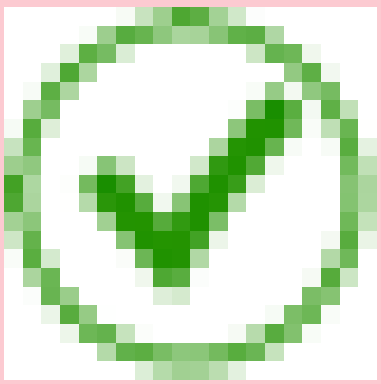
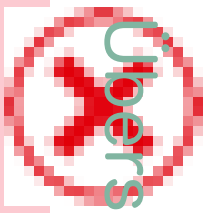
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Hohes Risiko				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Nutzbar	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

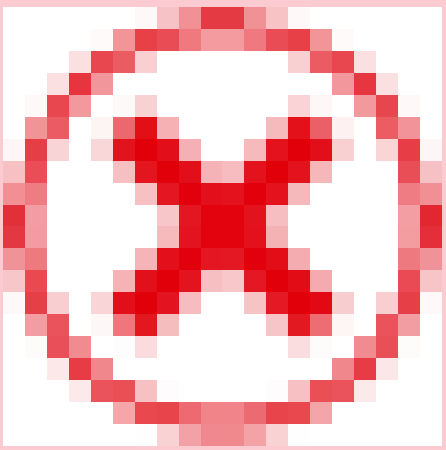
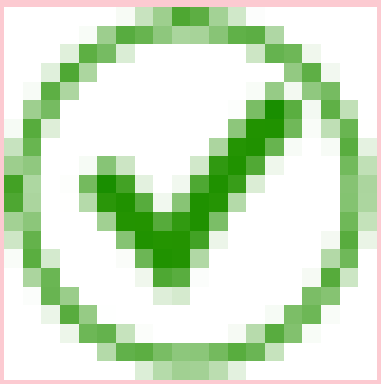
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Ziel rückt näher				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

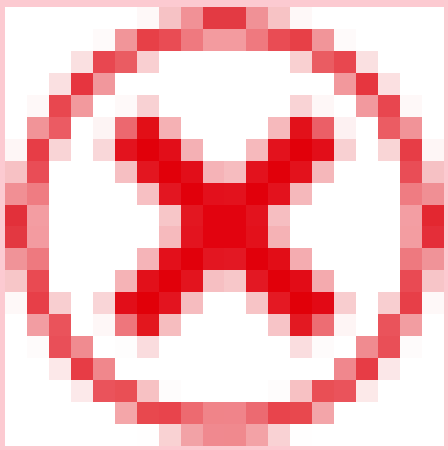
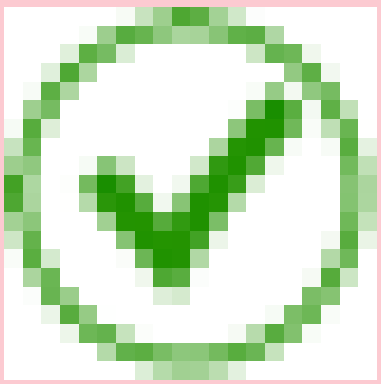
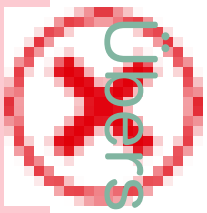
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Verfehltes Ziel				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Innerhalb der letzten 90 Tage	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

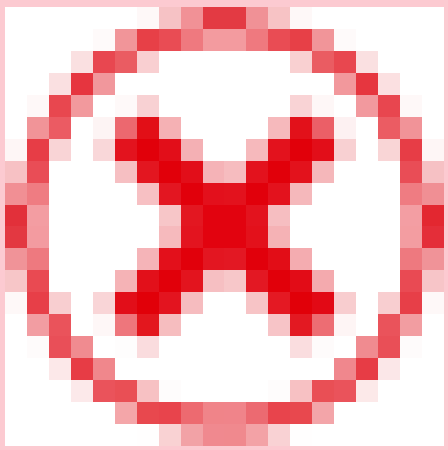
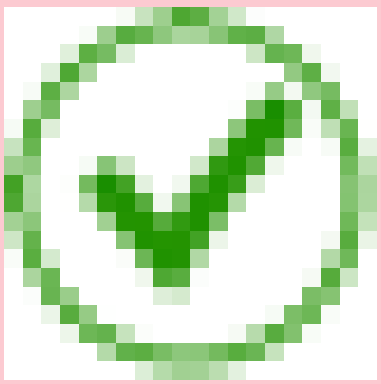
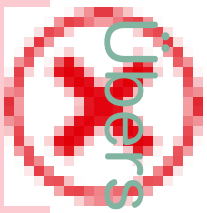
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Älter als 90 Tage				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

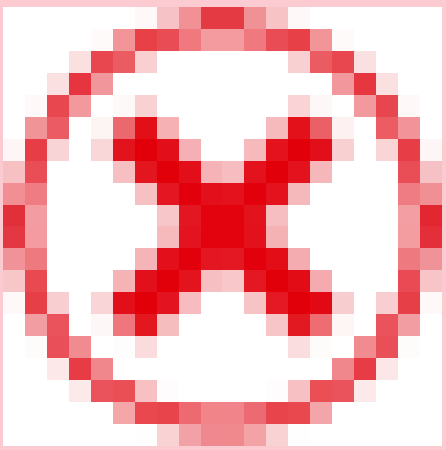
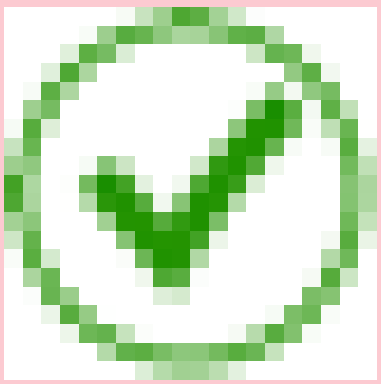
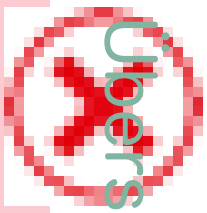
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Nicht zugewiesen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

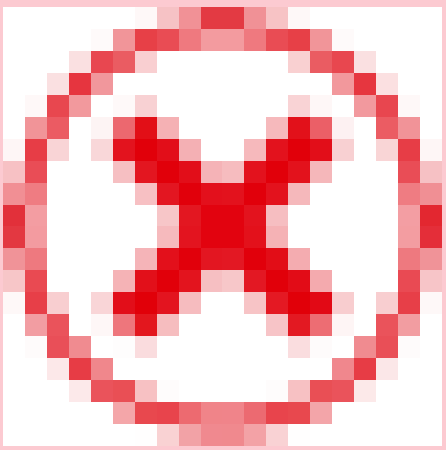
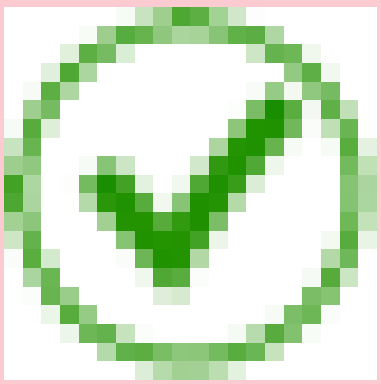
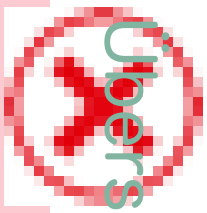
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Nicht gruppiert				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

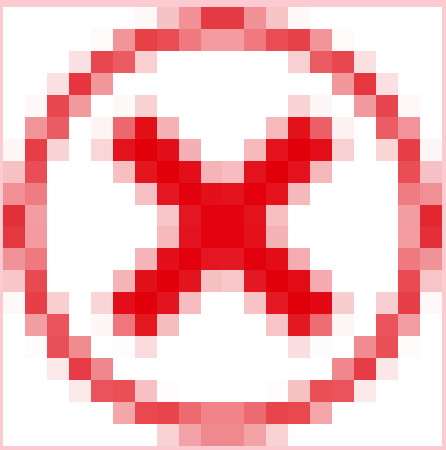
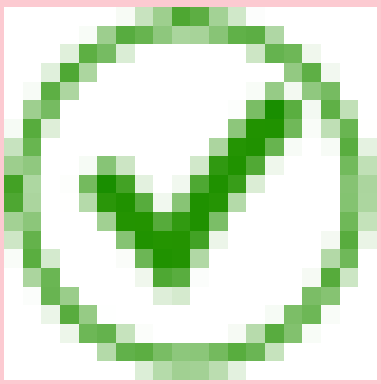
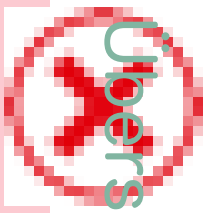
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Außer Betrieb genommen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

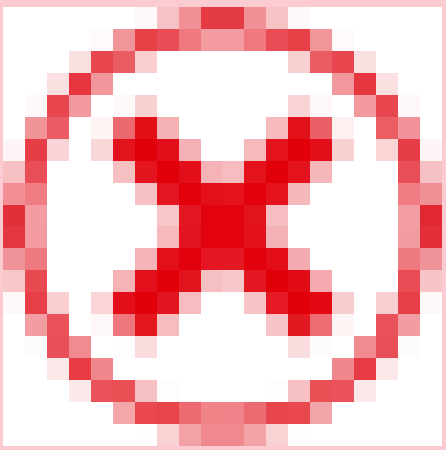
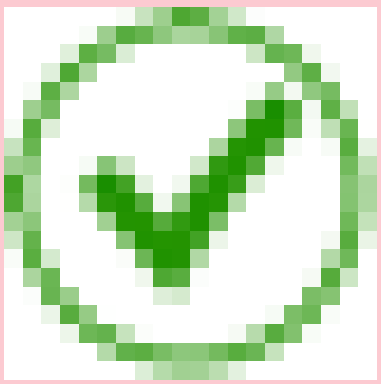
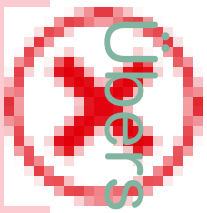
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Mehrere Zurückstellungen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

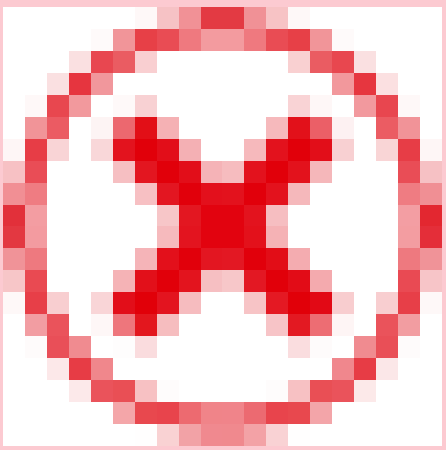
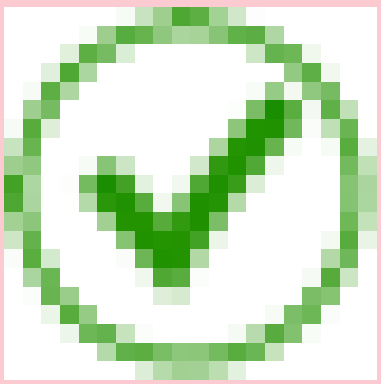
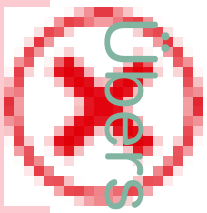
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Alle				
Lösungen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

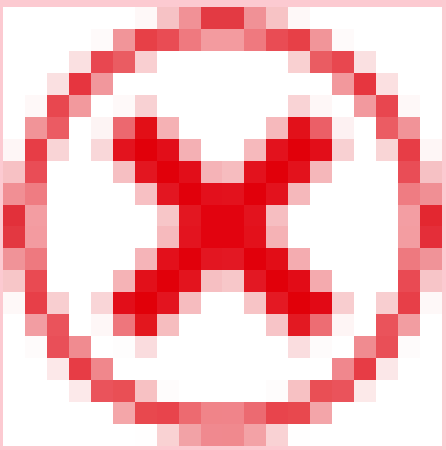
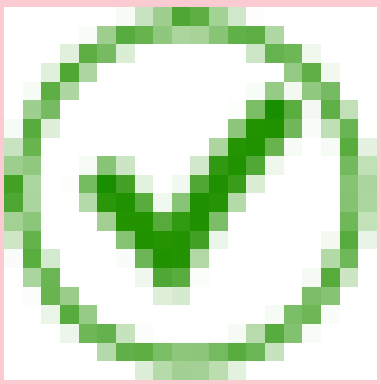
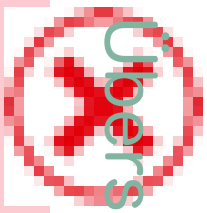
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Alle				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

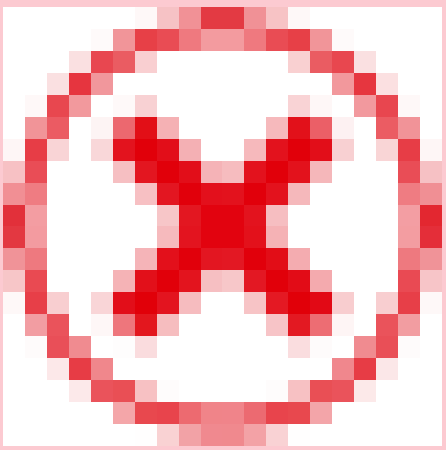
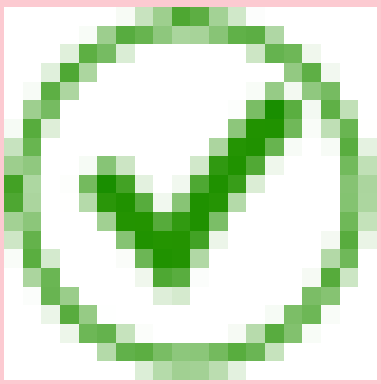
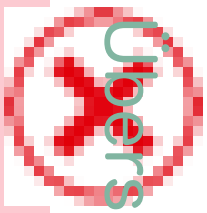
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Ersetzung mit höchster Priorität				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

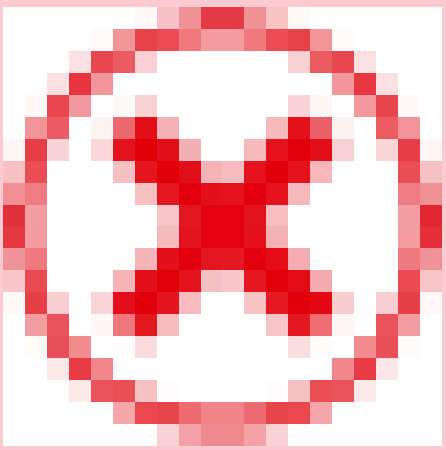
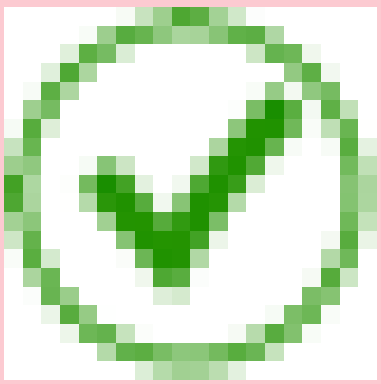
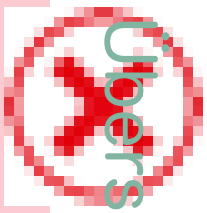
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Mit angreifbaren Elementen				
Bibliotheken				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

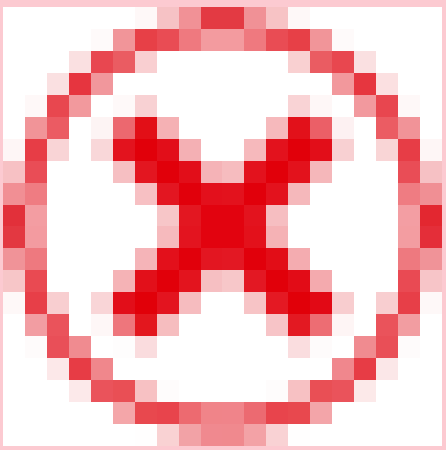
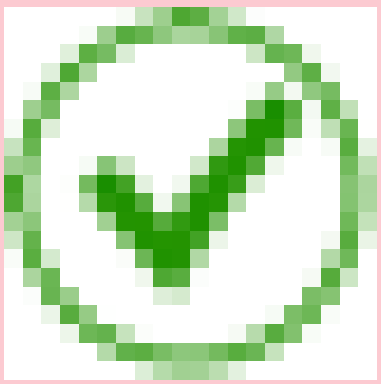
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
NVD				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

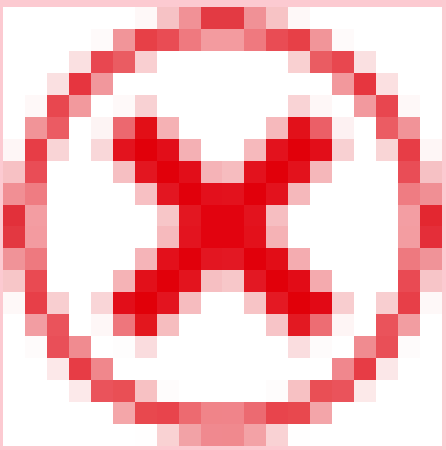
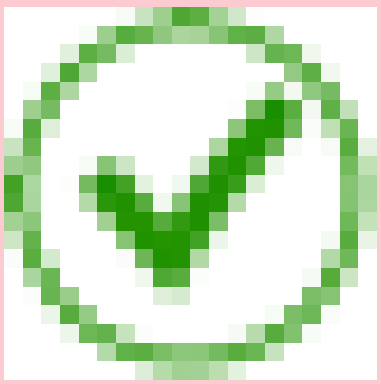
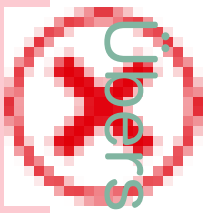
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
CWE				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

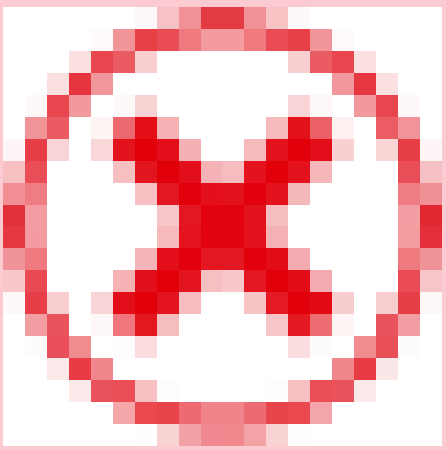
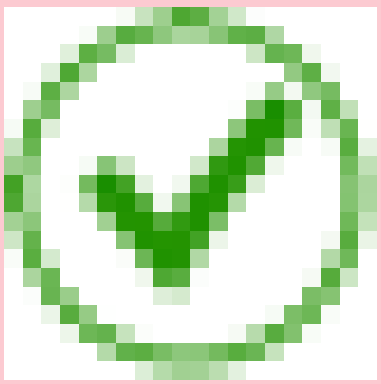
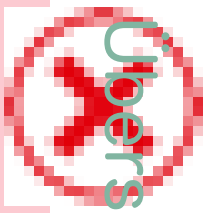
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Drittpartei				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

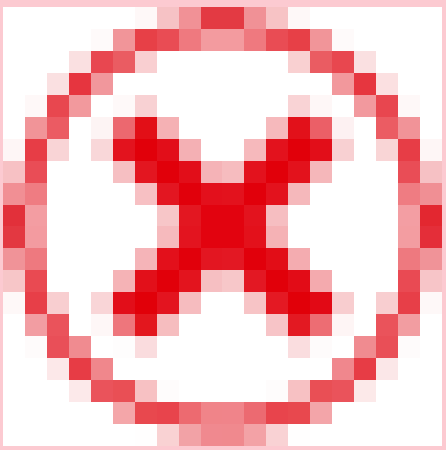
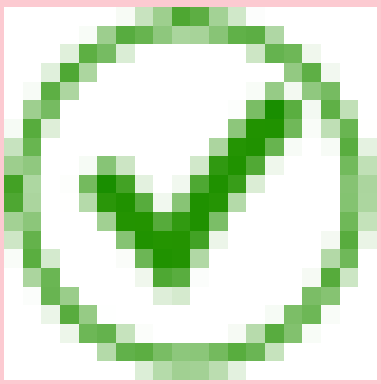
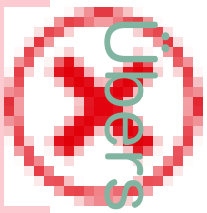
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Software mit Schwachstellen				
Schwachstellenscan				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

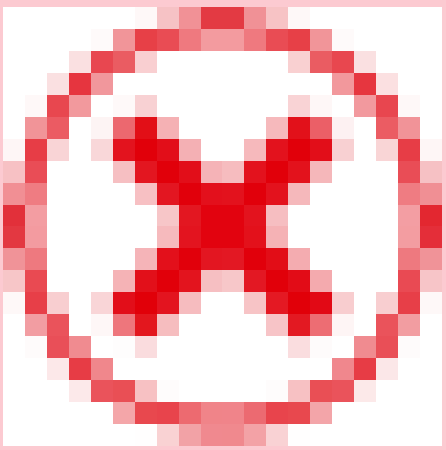
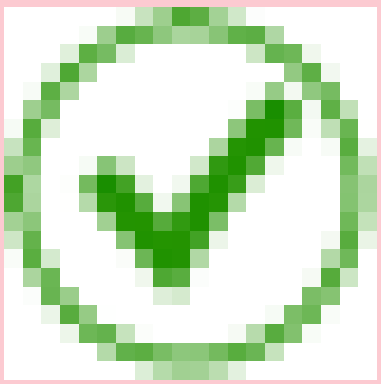
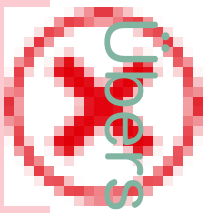
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Bewertung des Gefahrenpotenzials				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

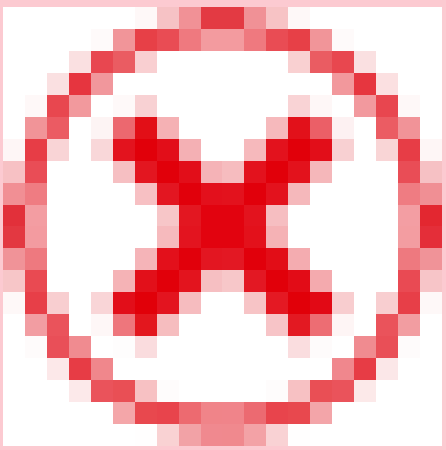
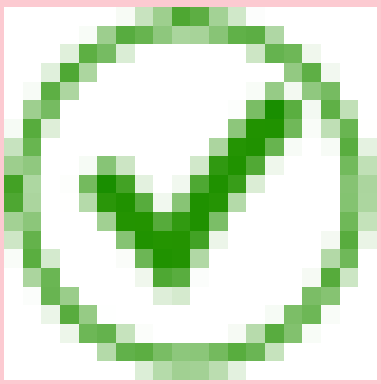
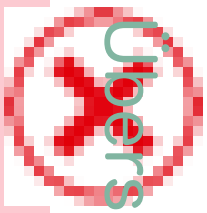
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Scans				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Scanner	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

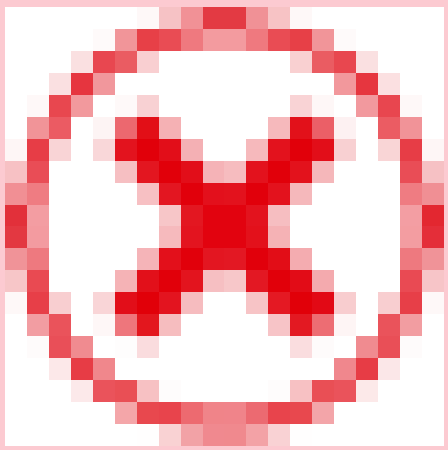
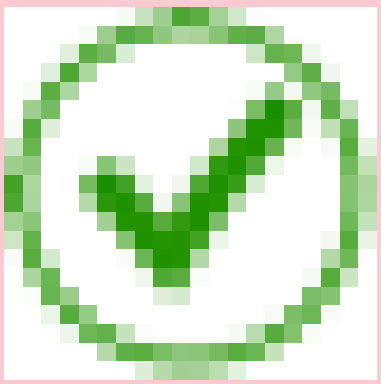
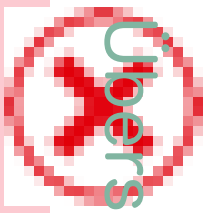
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Scan-Warteschlange				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

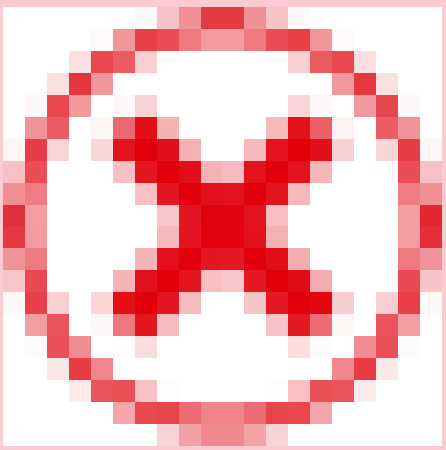
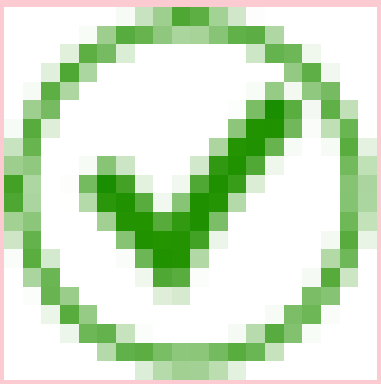
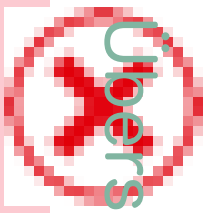
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Scannerquotengrenzen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

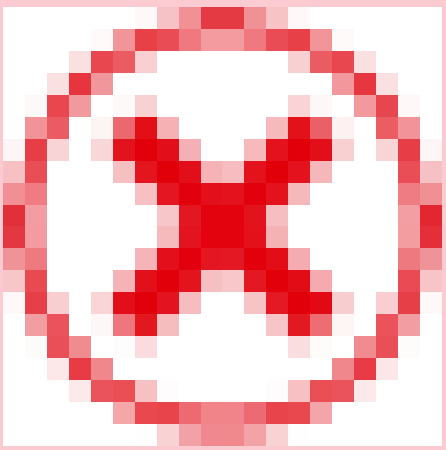
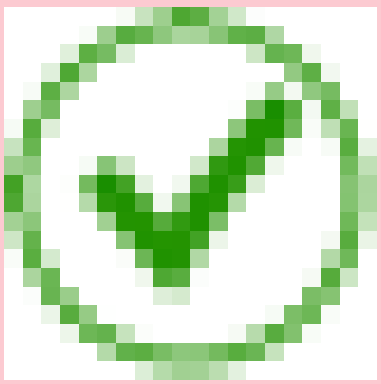
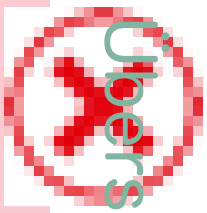
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Quotengrenzdefinitionen				
Administration				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

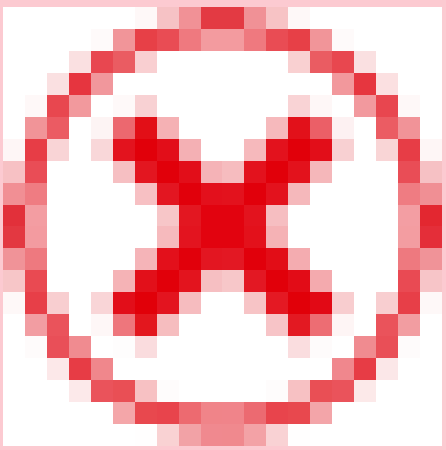
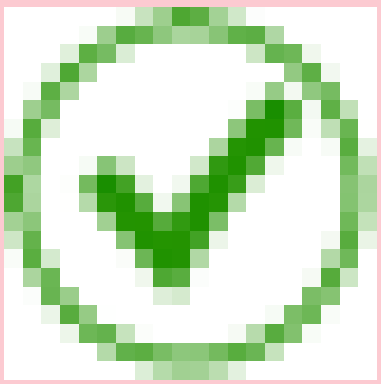
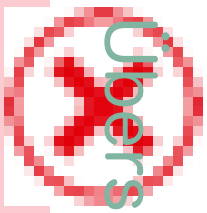
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Setup-Assistent				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

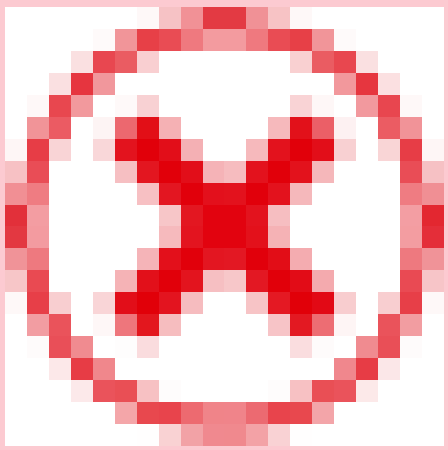
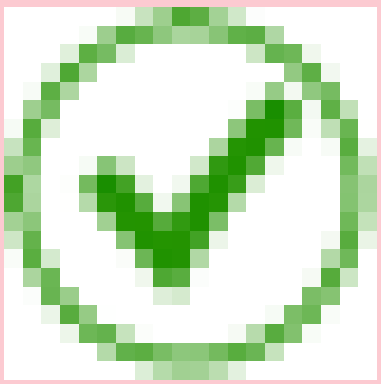
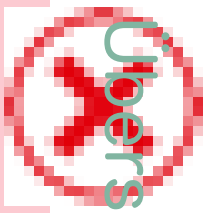
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Überwachungsthemen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Zuweisungsregeln	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Regeln für Korrekturaufgaben	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Zuweisungsempfehlungen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

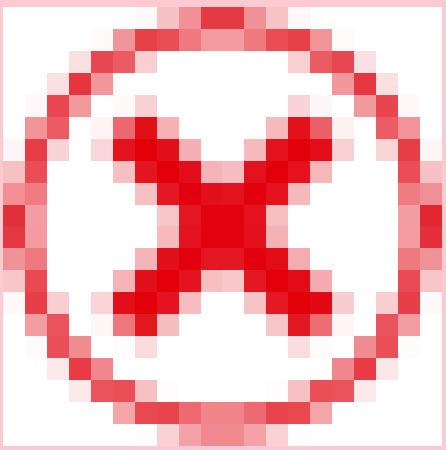
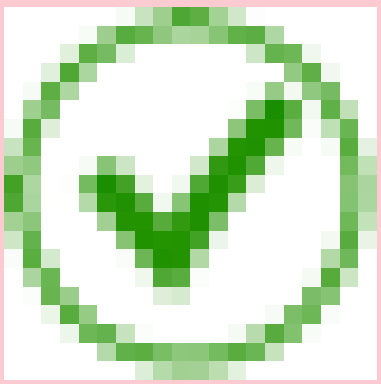
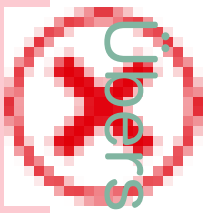
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Schwachstellen-Rechner				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Rechner für Schwachstellen-Rollup	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

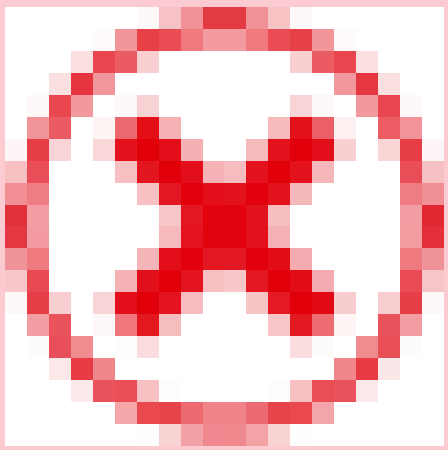
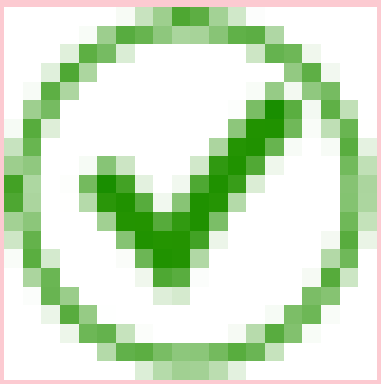
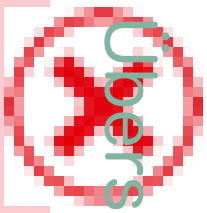
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Korrekturzielregeln				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

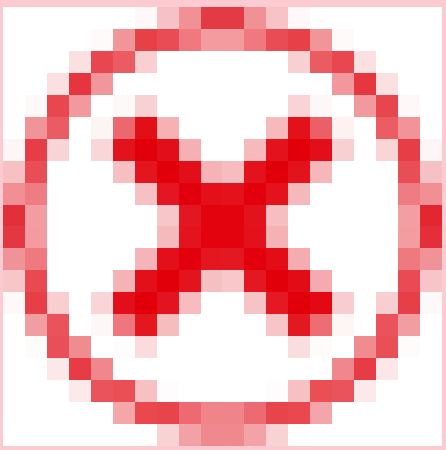
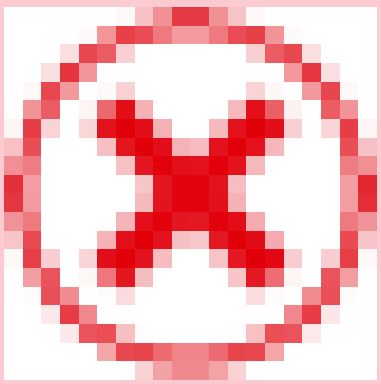
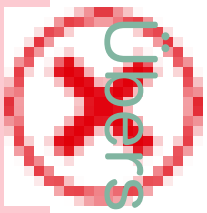
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Konfiguration automatisch schließen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Regeln für automatisches Löschen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Ausnahmeregeln	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Genehmigungsregeln	✓	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

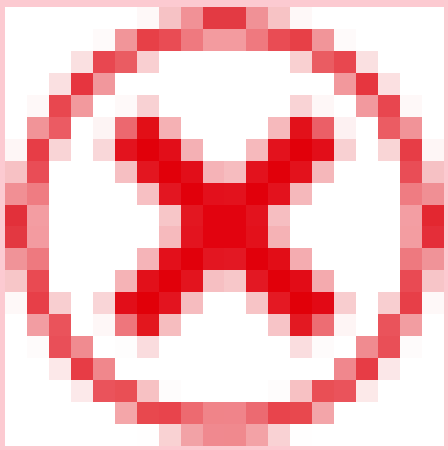
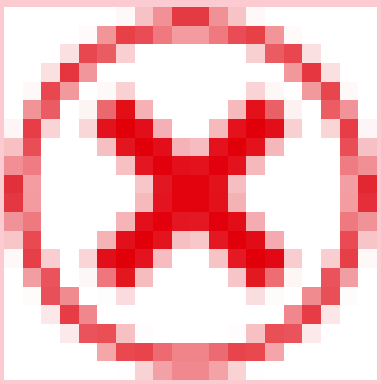
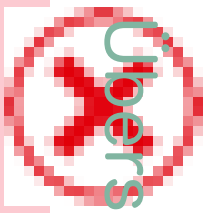
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Klassifizierungsregeln				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

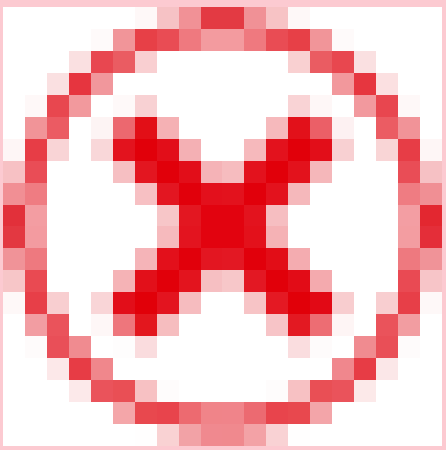
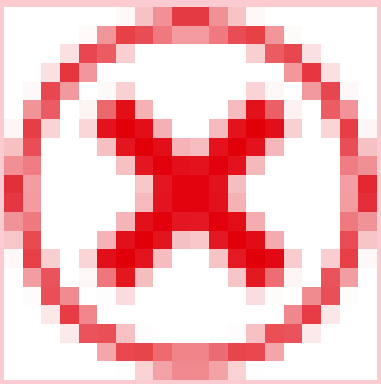
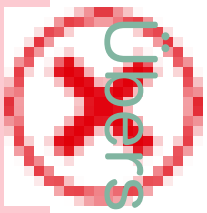
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Leistungskonfiguration				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

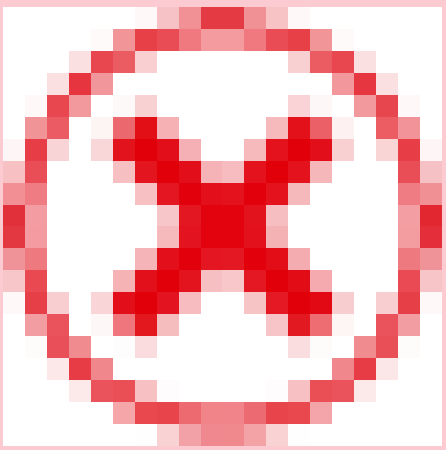
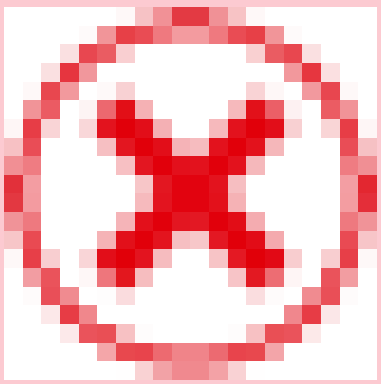
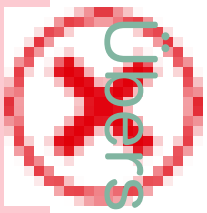
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
VI-Granularität konfigurieren				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Benachrichtigungen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

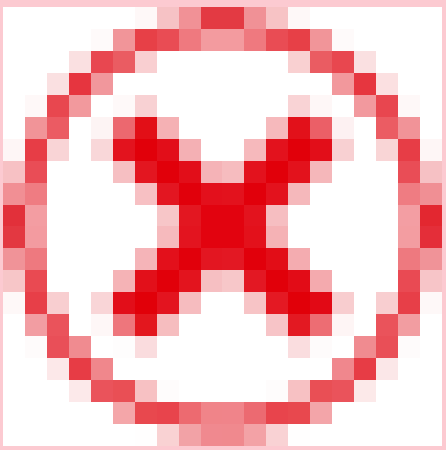
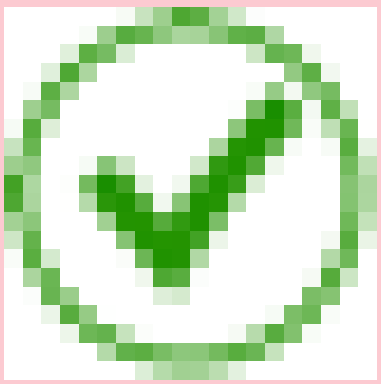
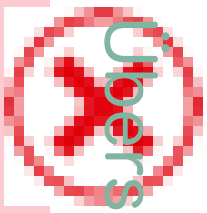
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
E-Mail-Vorlagen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

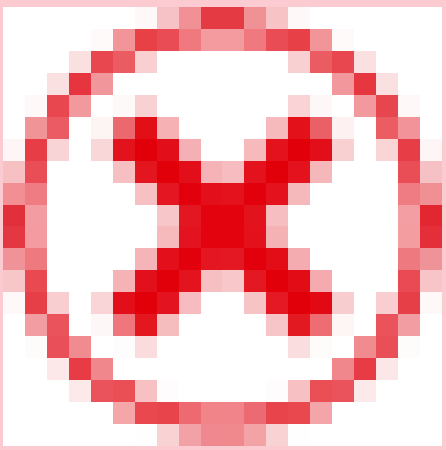
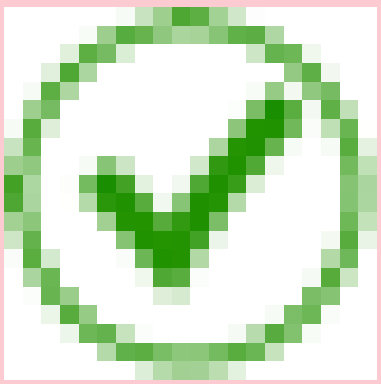
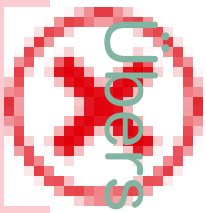
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Warteschlange importieren				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

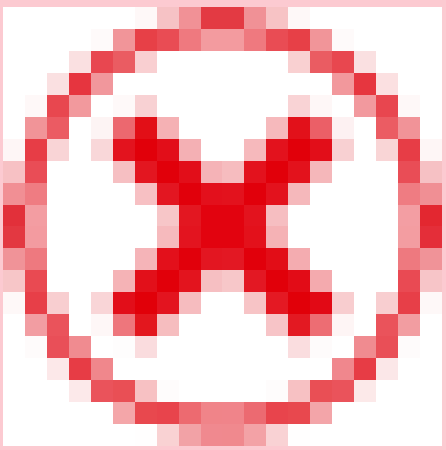
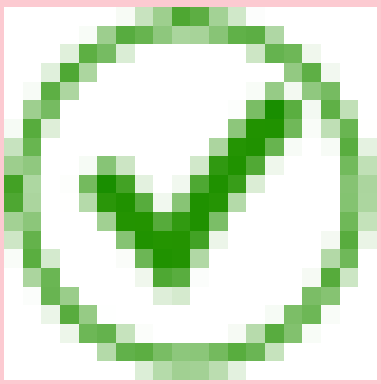
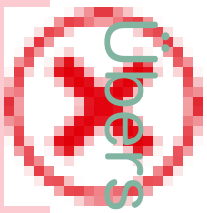
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Integrationen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

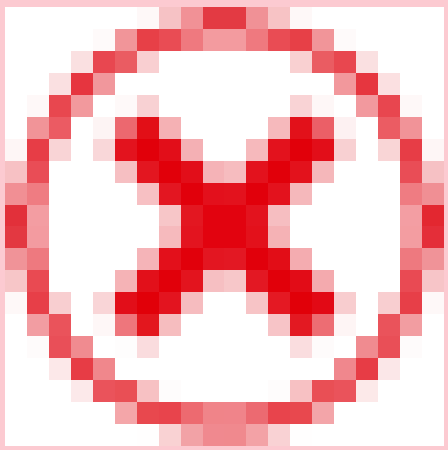
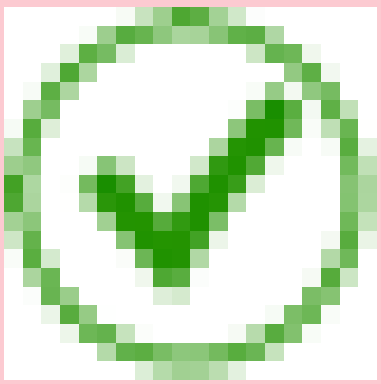
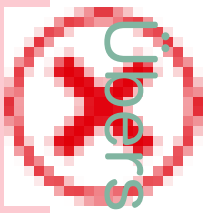
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
SLA-Definitionen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

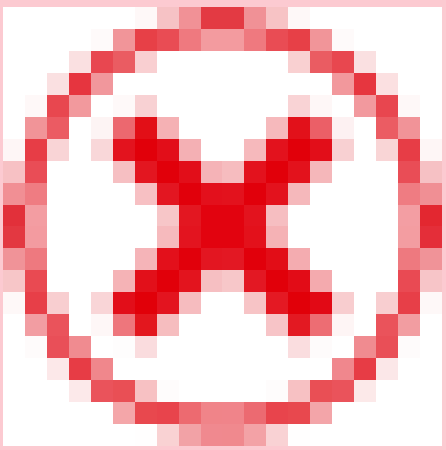
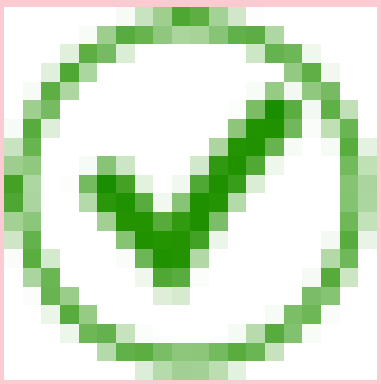
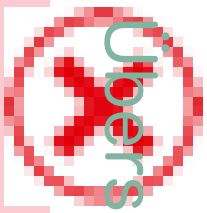
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
SAM-NVD konfigurieren				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

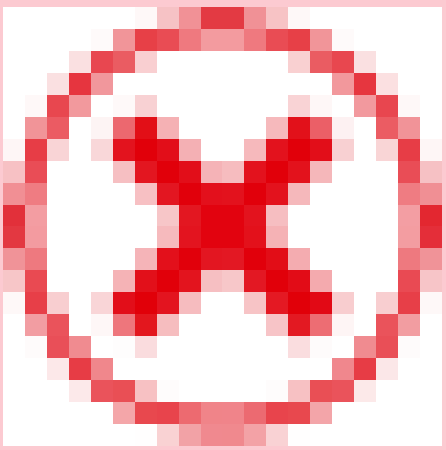
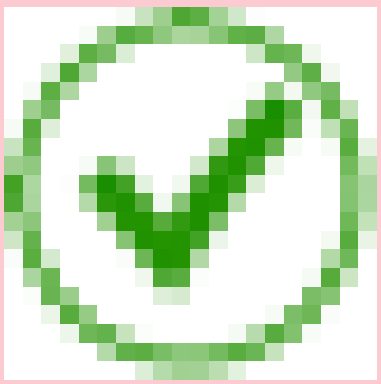
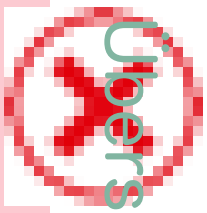
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Normalisierte Schweregradzuordnungen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

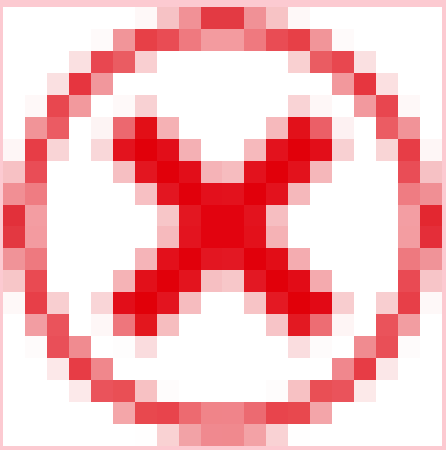
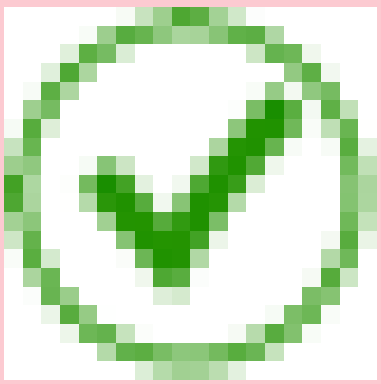
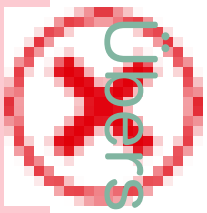
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Konfiguration der Scan-Abdeckung				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

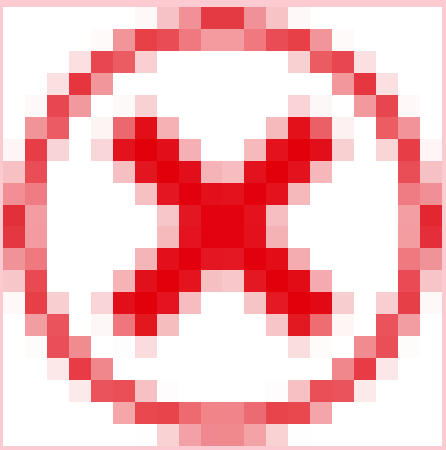
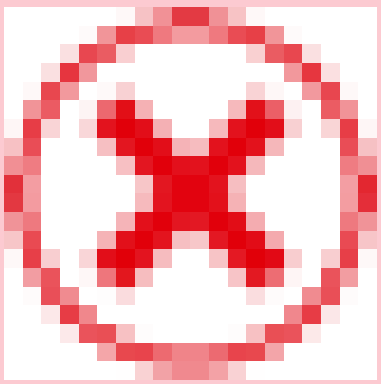
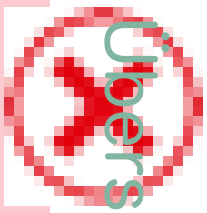
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Ausnahmenverwaltung				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Verwendungsbericht				
Diagnosen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

Informationen für andere Rollen:

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_sec_cmn. Manage_Approval_rules	sn_vul. Access_Setup_Assistant	sn_vul. ciso_read	sn
Überprüfungen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

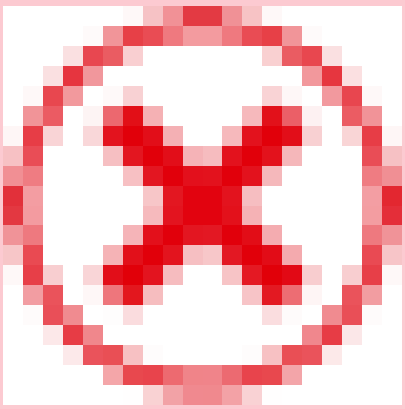
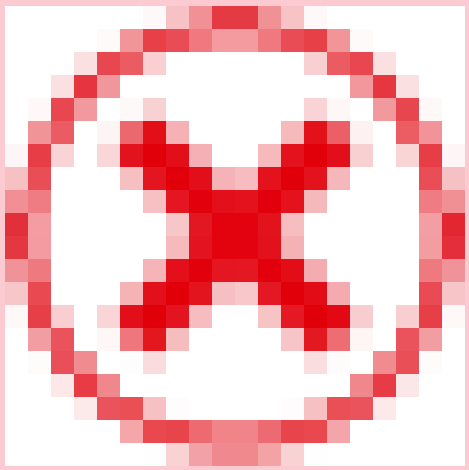
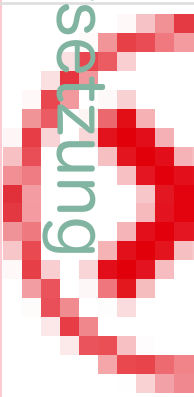
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
(Haupt-App-Gruppe)			
CISO-Dashboard			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Korrekturübersicht	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Arbeitsbereich des Schwachstellenmanagers	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Übersicht	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Arbeitsbereich für IT-Korrekturen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Genehmiger-Übersicht	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Übersicht	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Meine Genehmigungen	✗	✗	✗
Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Aktiv	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Mir zugewiesen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Meinen Gruppen zugewiesen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Alle			
Angreifbare Elemente			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Kritisches Risiko	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Hohes Risiko	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Nutzbar	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Ziel rückt näher	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Verfehltes Ziel			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Innerhalb der letzten 90 Tage	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Älter als 90 Tage	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Nicht zugewiesen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Nicht gruppiert	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Außer Betrieb genommen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Mehrere Zurückstellungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Alle			
Lösungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Alle	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Ersetzung mit höchster Priorität			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Mit angreifbaren Elementen			
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
NVD	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
CWE	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Drittpartei	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Software mit Schwachstellen	✗	✗	✗
Schwachstellenscan			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Bewertung des Gefahrenpotenzials	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Scans	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Scanner	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Scan-Warteschlange	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Scannerquotengrenzen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Quotengrenzdefinitionen			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Setup-Assistent	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Überwachungsthemen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Zuweisungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Regeln für Korrekturaufgaben	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Zuweisungsempfehlungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Schwachstellen-Rechner	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Rechner für Schwachstellen-Rollup	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Korrekturzielregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Konfiguration automatisch schließen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Regeln für automatisches Löschen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Ausnahmeregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Genehmigungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Klassifizierungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Leistungskonfiguration	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
VI-Granularität konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Benachrichtigungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
E-Mail-Vorlagen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Warteschlange importieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Integrationen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
SLA-Definitionen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

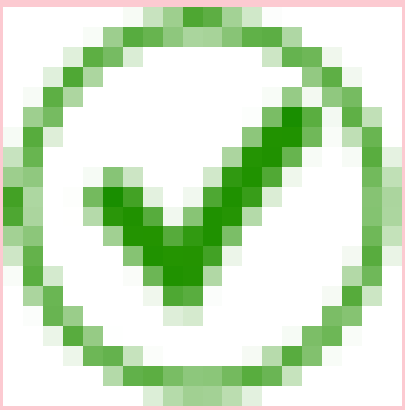
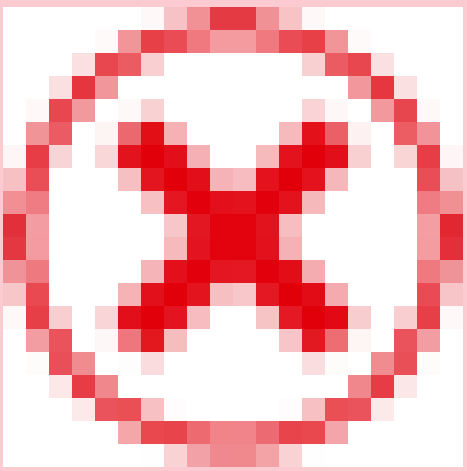
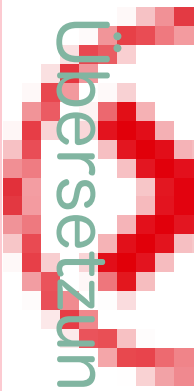
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
SAM-NVD konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Normalisierte Schweregradzuordnungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

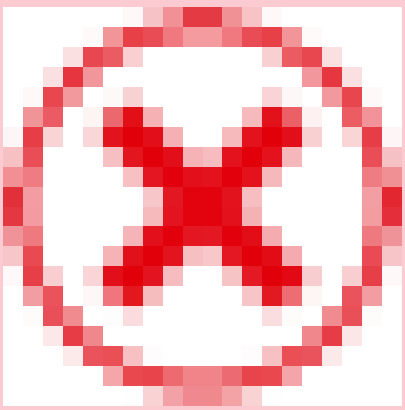
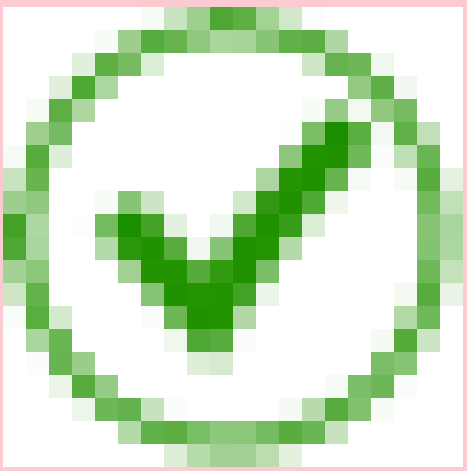
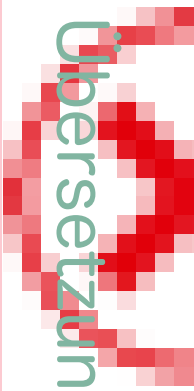
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Konfiguration der Scan-Abdeckung			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Ausnahmenverwaltung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Verwendungsbericht			
Diagnosen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Configure_nvd_Integration	sn_vul. Configure_Scan_Coverage_read	sn_vul. Configur
Überprüfungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
(Haupt-App-Gruppe)			
CISO-Dashboard	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

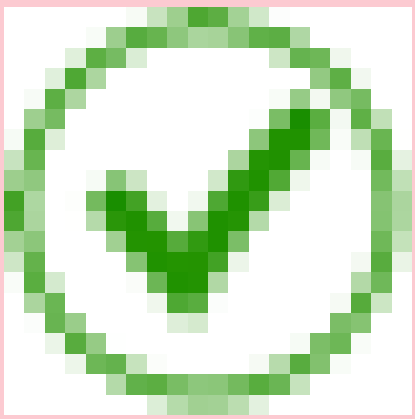
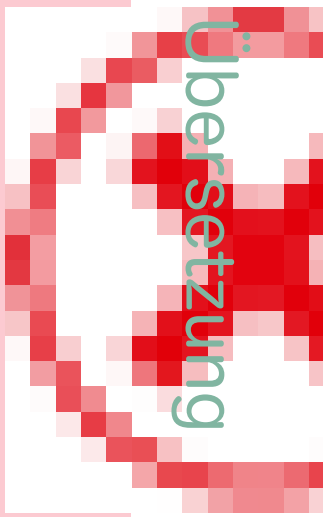
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Korrekturübersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

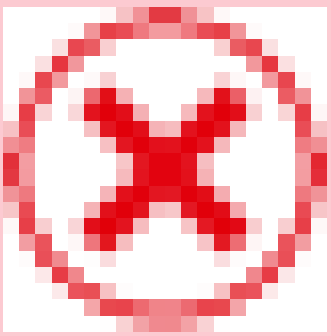
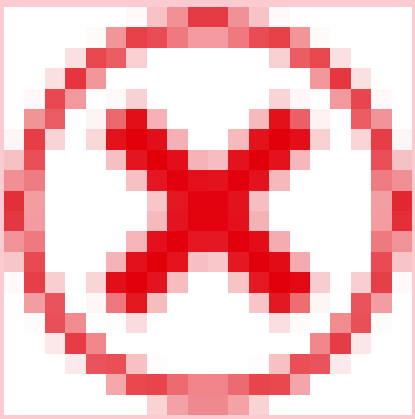
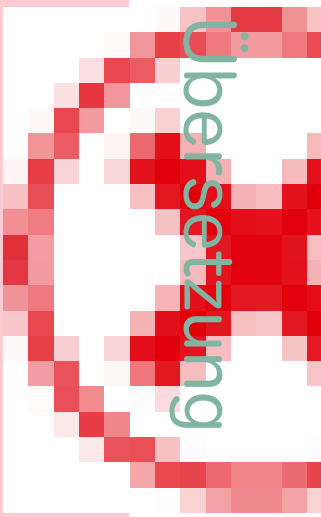
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Arbeitsbereich des Schwachstellenmanagers			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

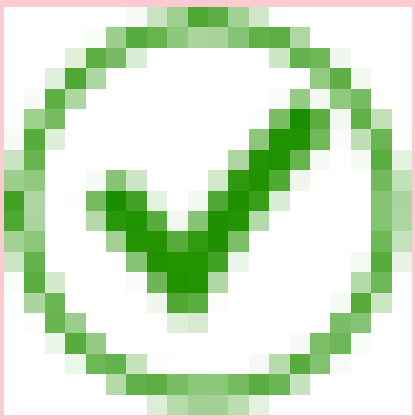
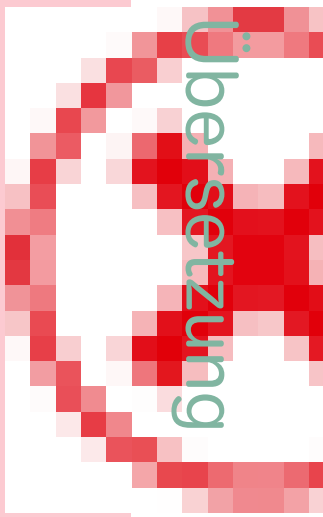
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Arbeitsbereich für IT-Korrekturen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

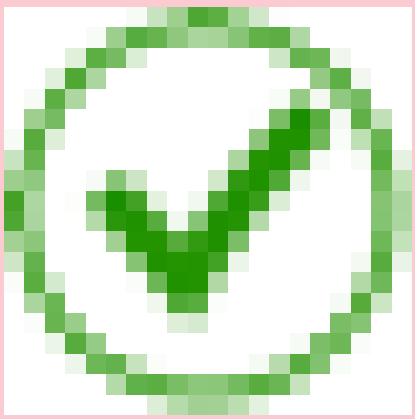
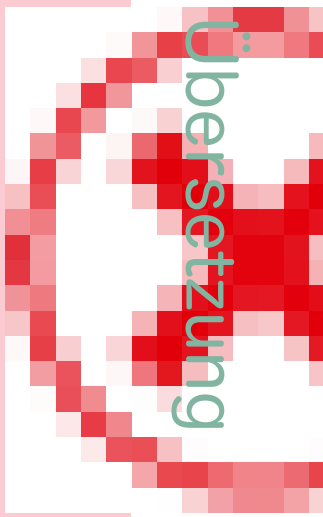
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Genehmiger-Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

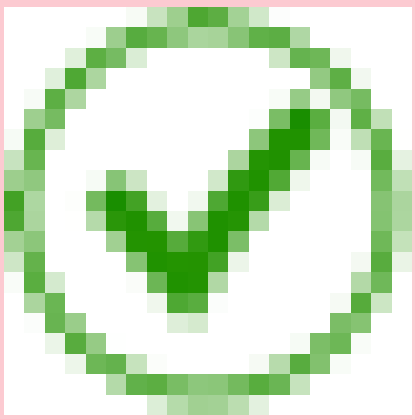
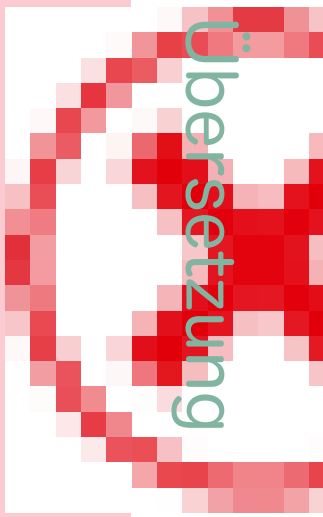
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

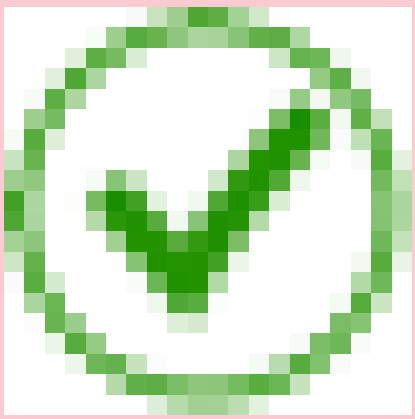
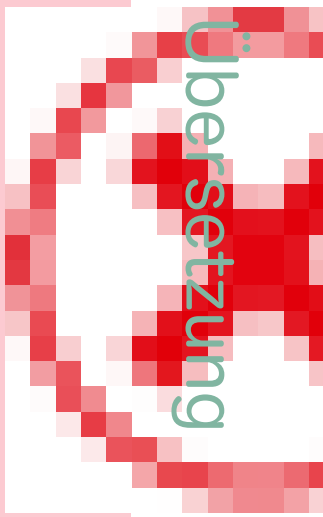
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Meine Genehmigungen			
Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

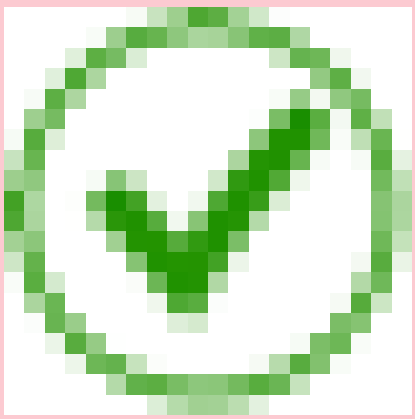
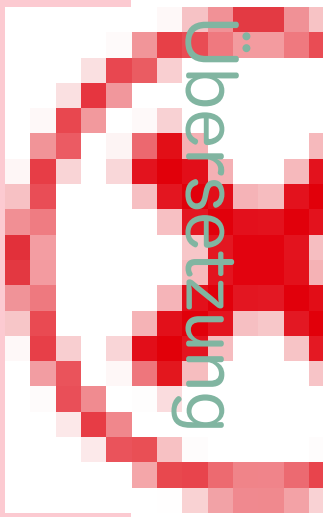
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Aktiv			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

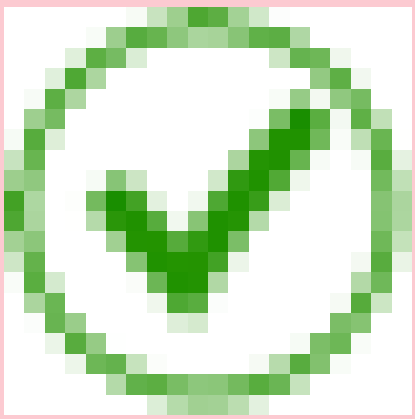
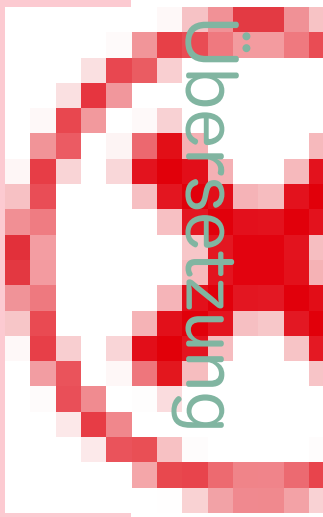
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Mir zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

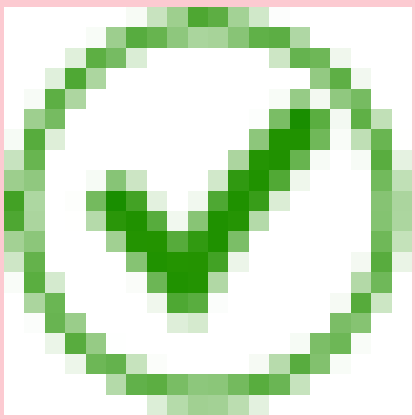
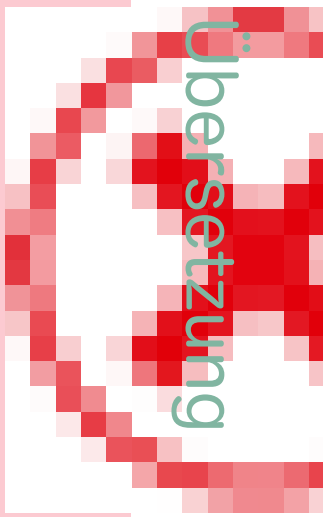
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Meinen Gruppen zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

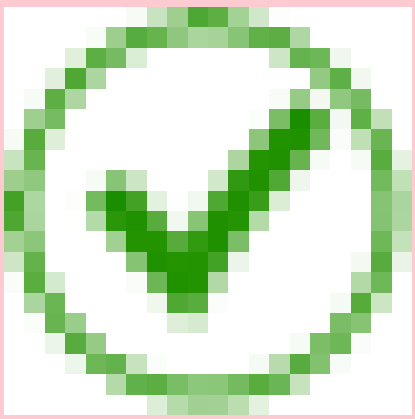
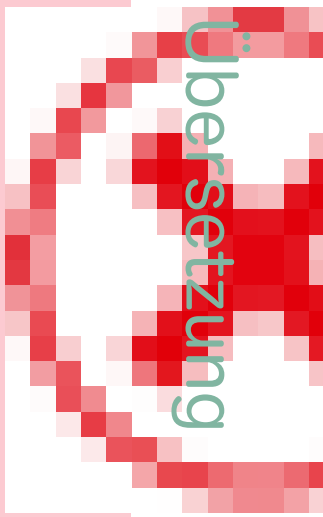
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Alle			

Angreifbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

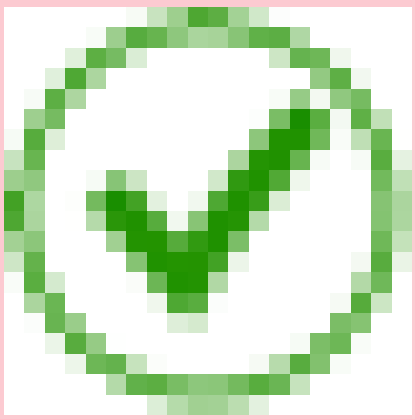
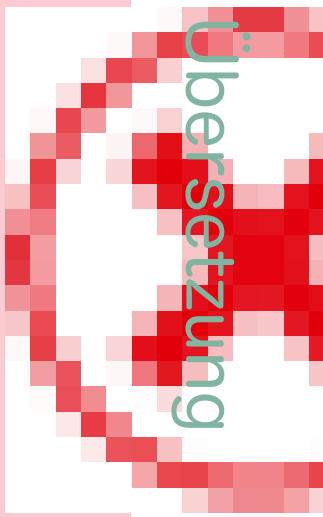
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Kritisches Risiko			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Hohes Risiko	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

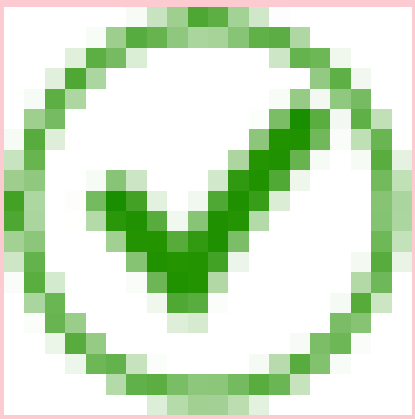
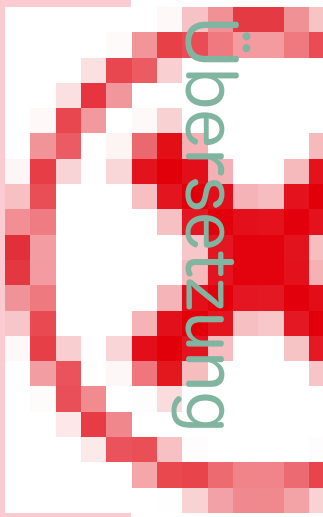
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Nutzbar			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

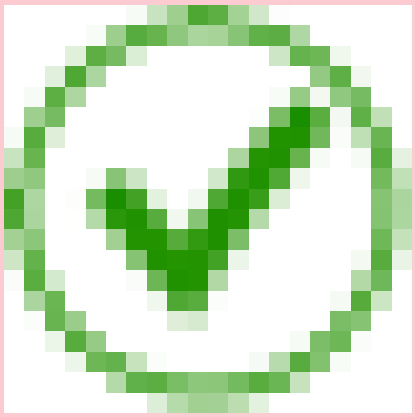
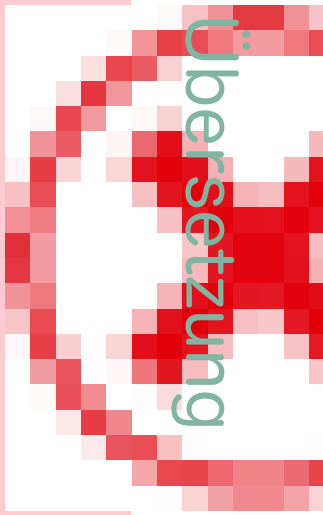
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Ziel rückt näher			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

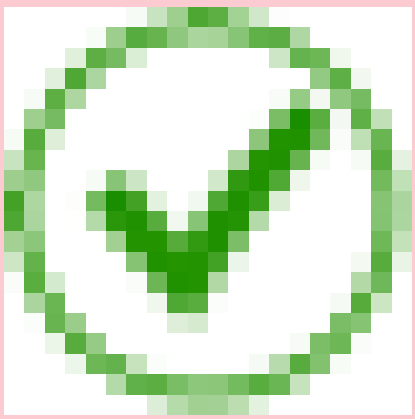
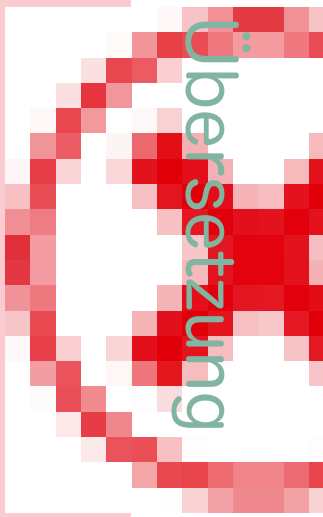
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Verfehltes Ziel			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

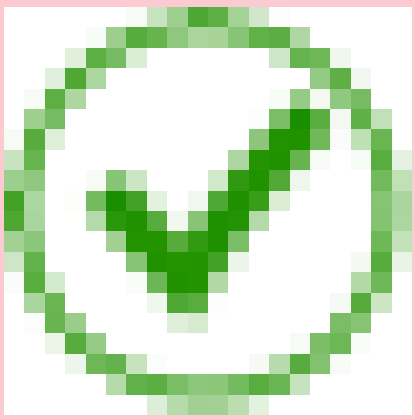
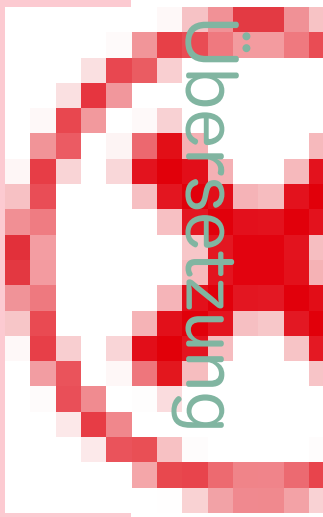
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Innerhalb der letzten 90 Tage			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

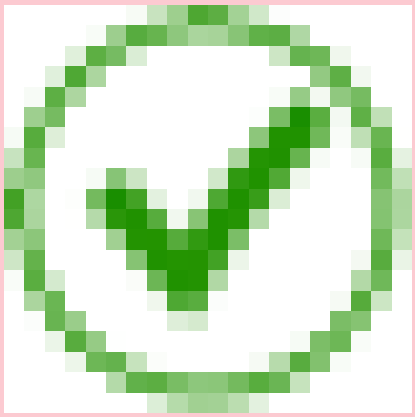
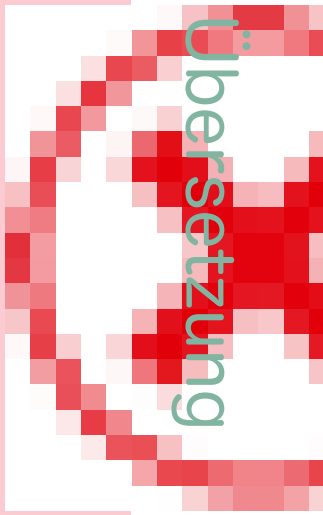
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Älter als 90 Tage			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

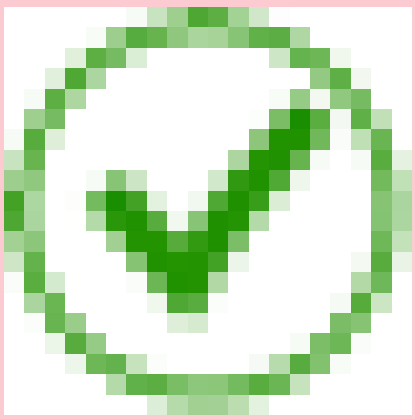
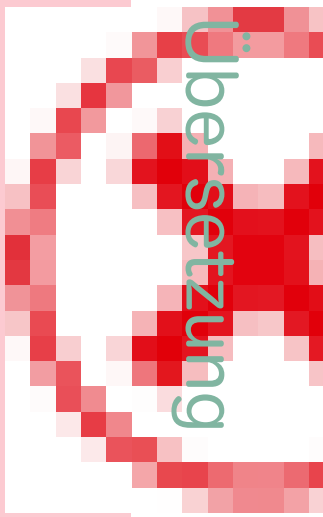
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Nicht zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

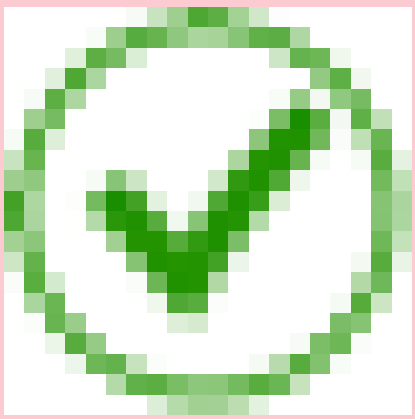
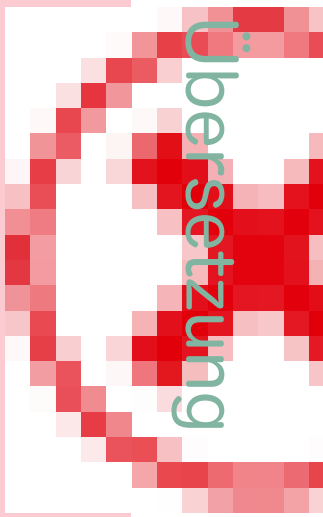
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Nicht gruppiert			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Außer Betrieb genommen	✓	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

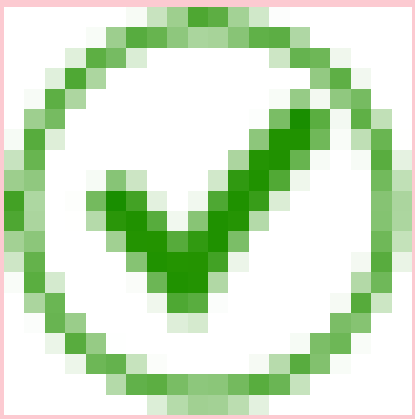
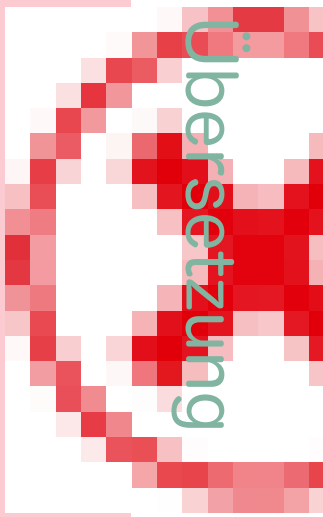
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Mehrere Zurückstellungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

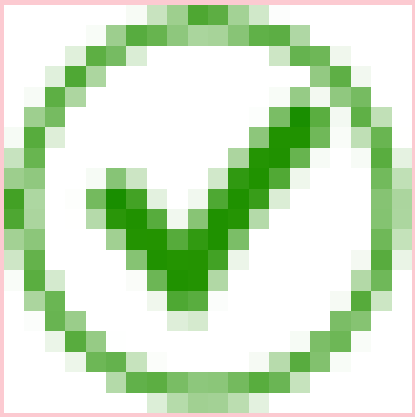
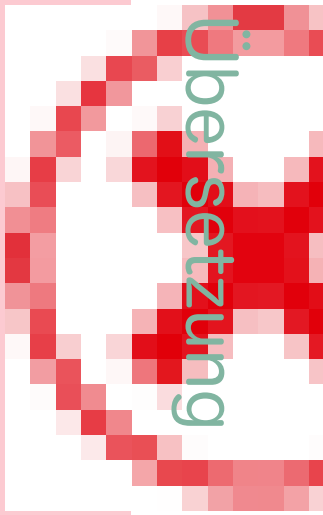
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Alle			
Lösungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

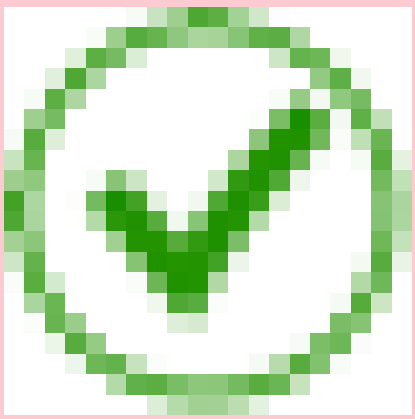
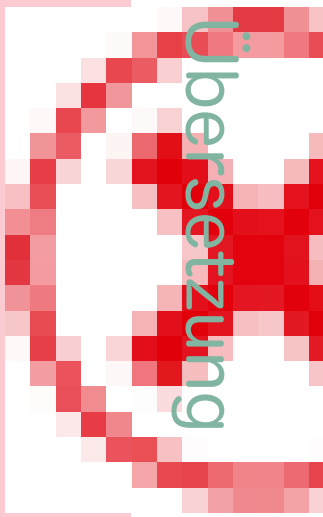
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Alle			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

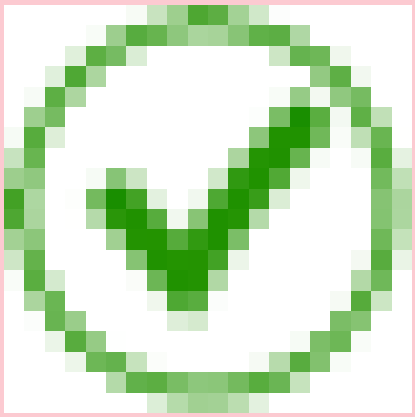
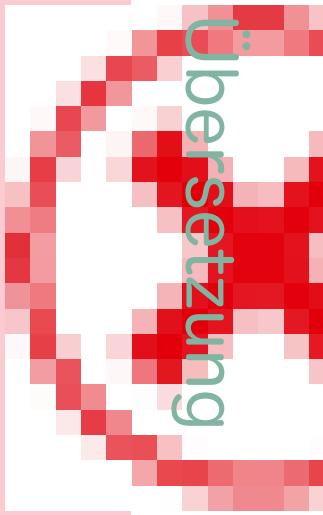
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Ersetzung mit höchster Priorität			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

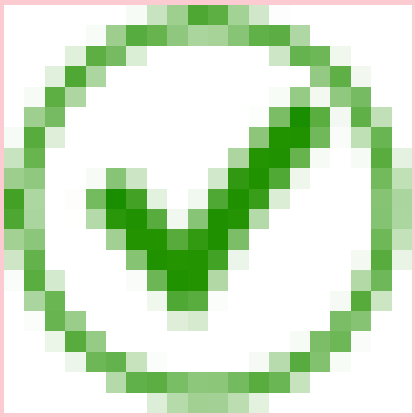
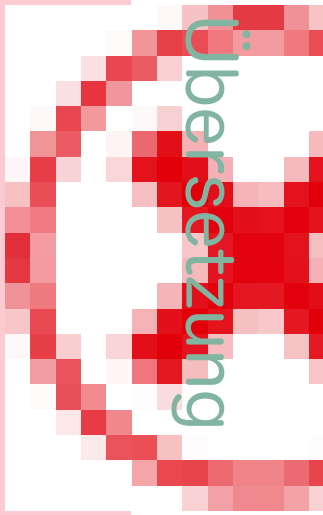
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Mit angreifbaren Elementen			
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

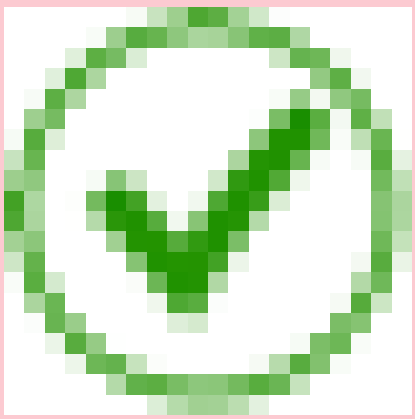
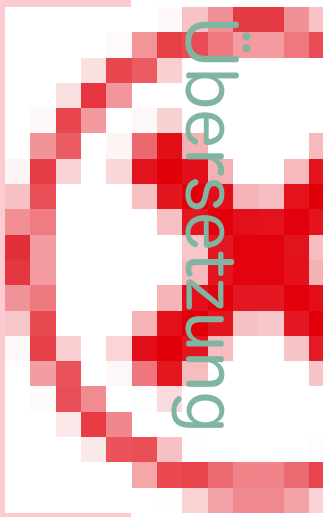
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
NVD			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

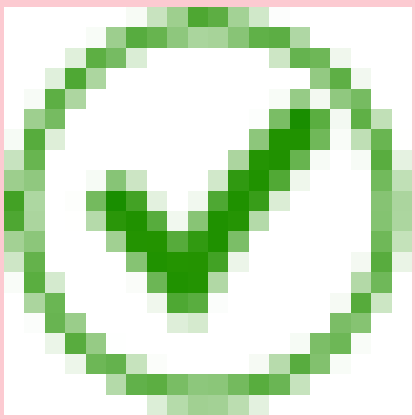
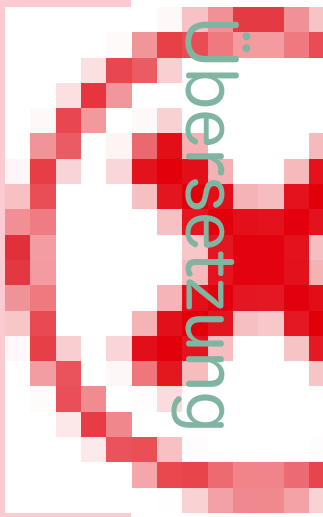
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
CWE			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

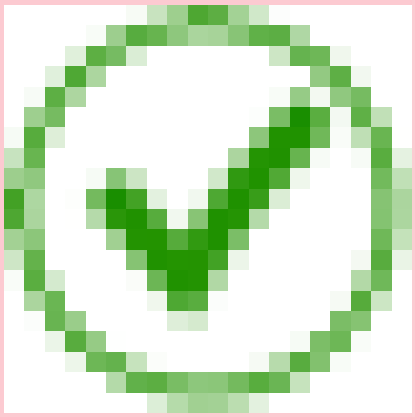
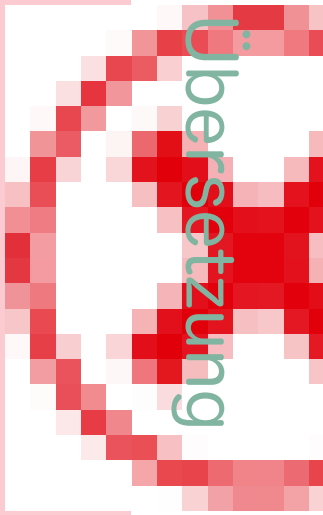
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Drittpartei			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

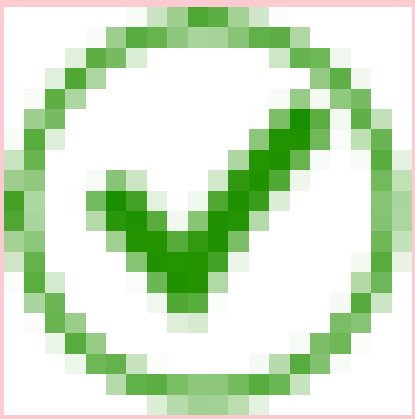
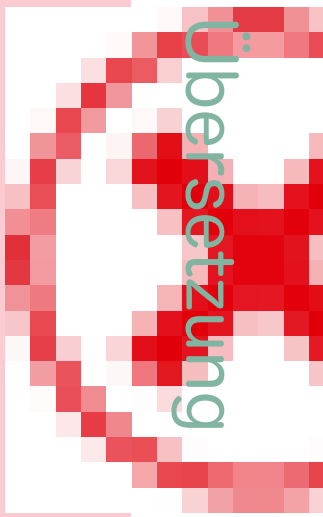
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Software mit Schwachstellen			
Schwachstellenscan			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Bewertung des Gefahrenpotenzials	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

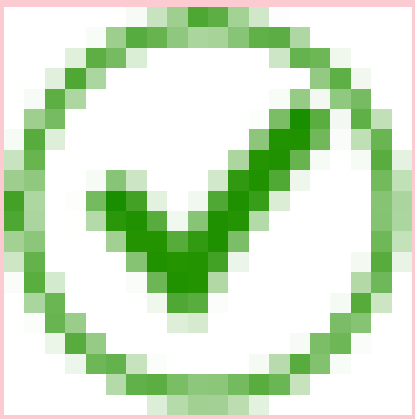
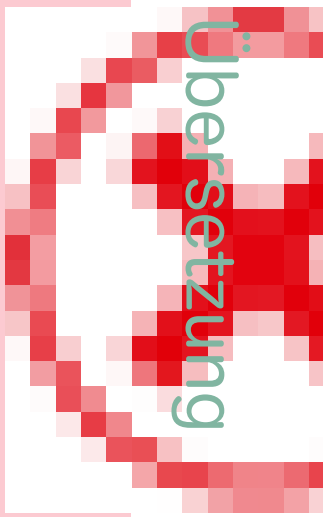
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Scans			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

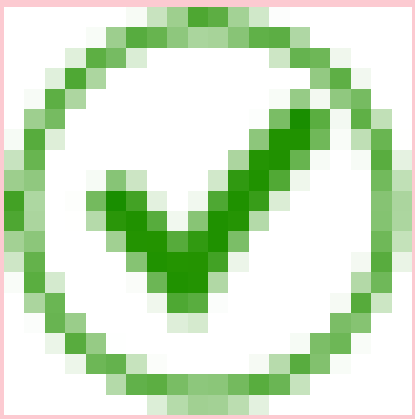
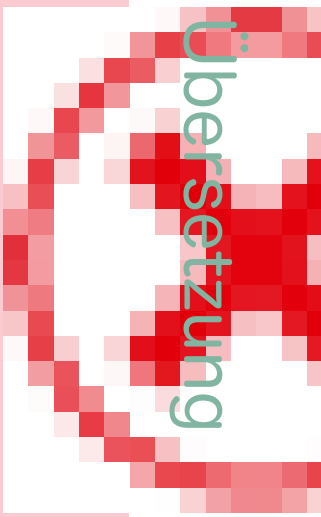
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Scanner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

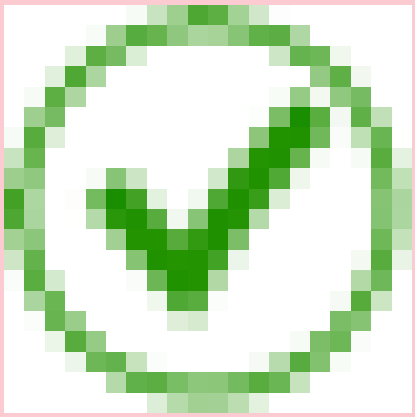
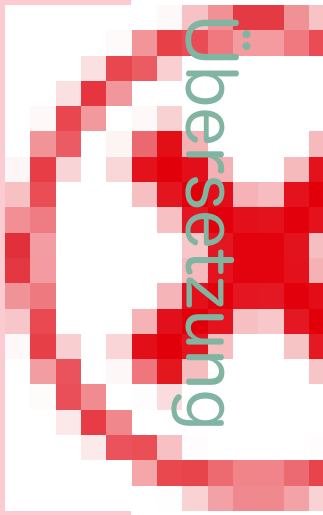
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Scan-Warteschlange			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

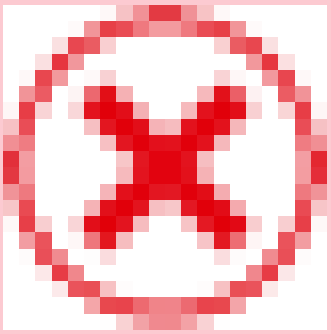
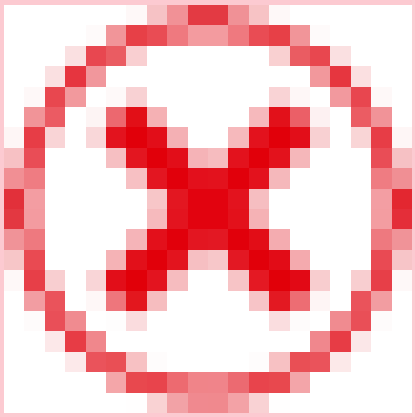
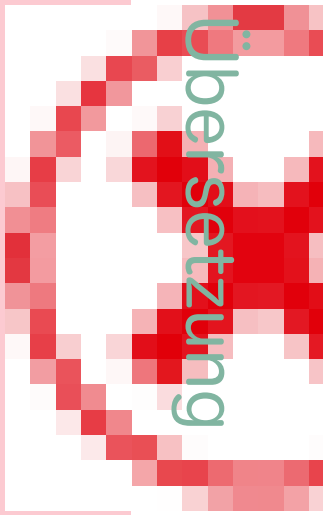
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Scannerquotengrenzen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

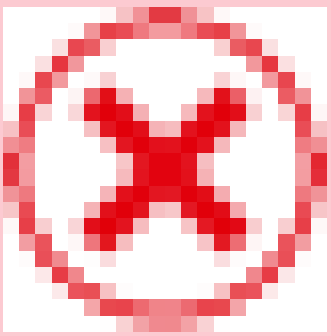
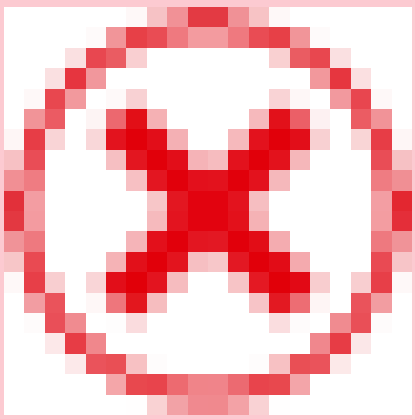
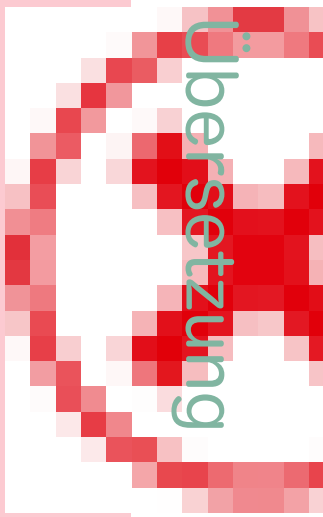
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Quotengrenzdefinitionen			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

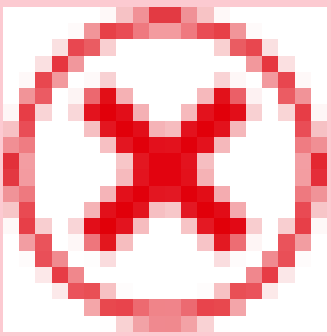
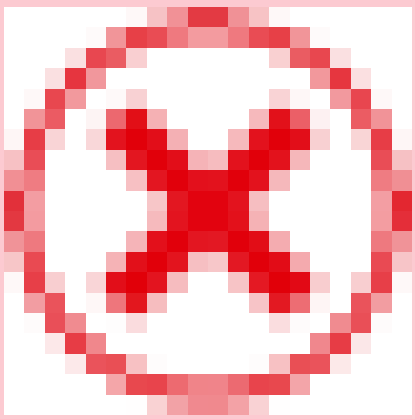
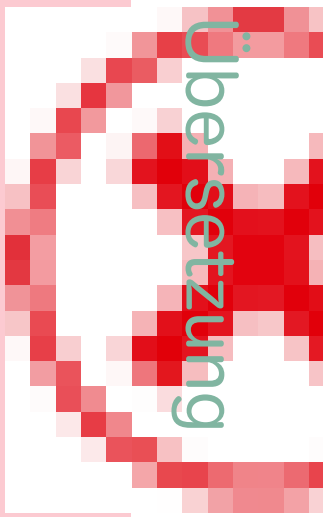
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Setup-Assistent			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

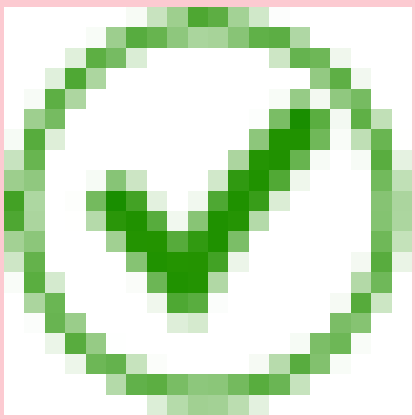
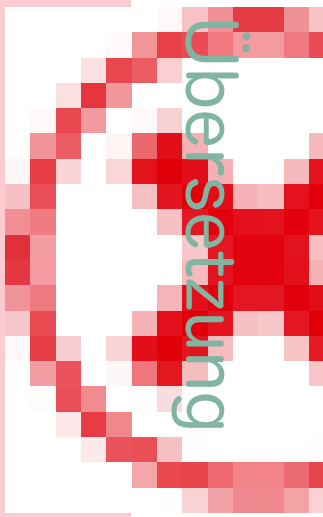
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Überwachungsthemen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

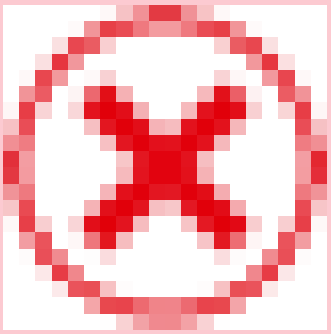
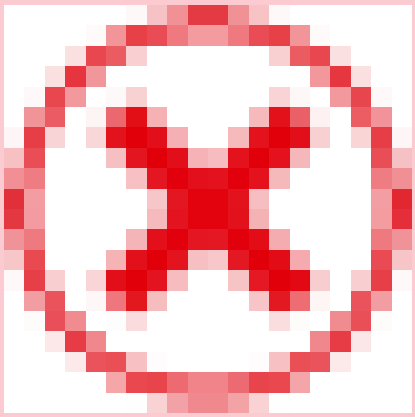
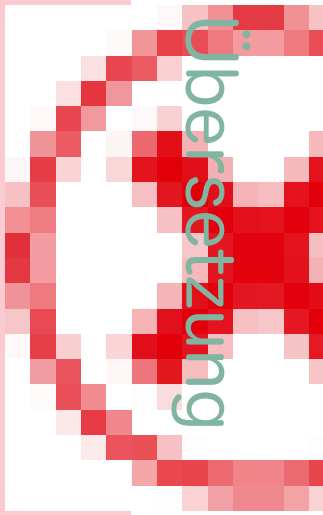
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Zuweisungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

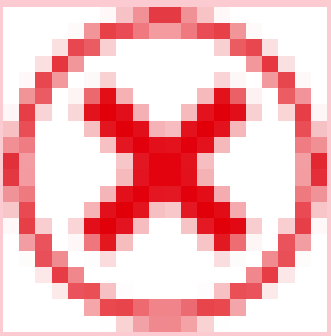
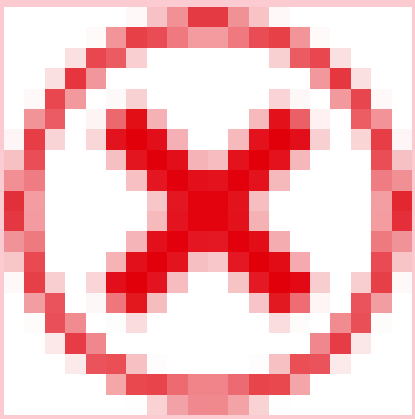
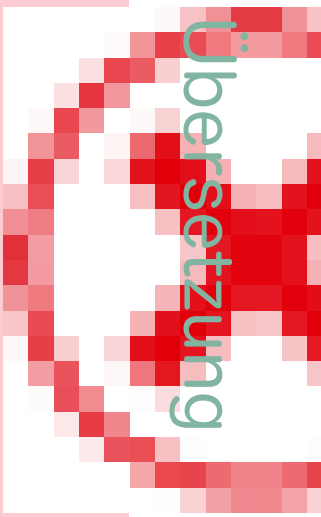
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Regeln für Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

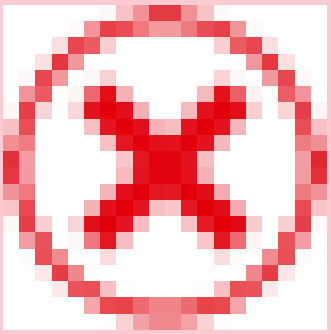
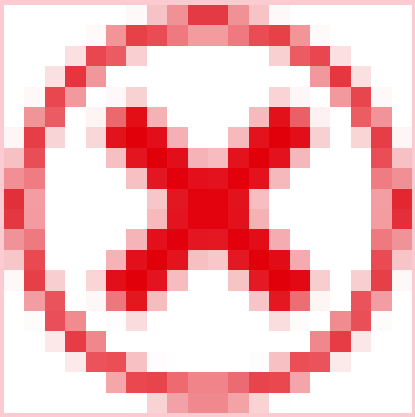
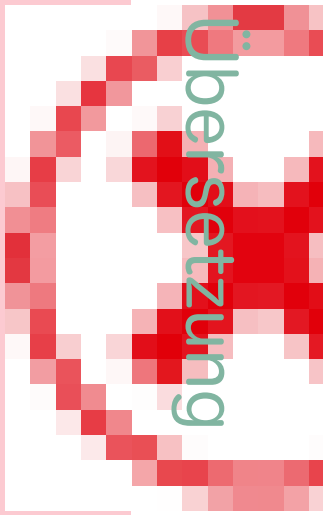
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Zuweisungsempfehlungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

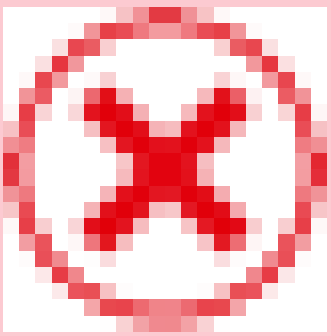
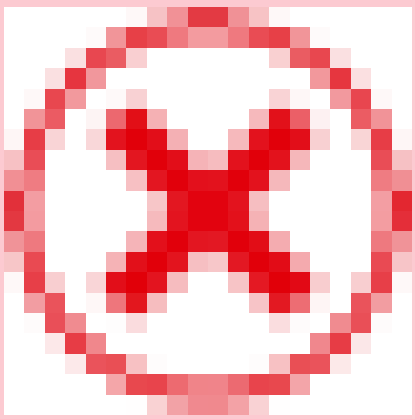
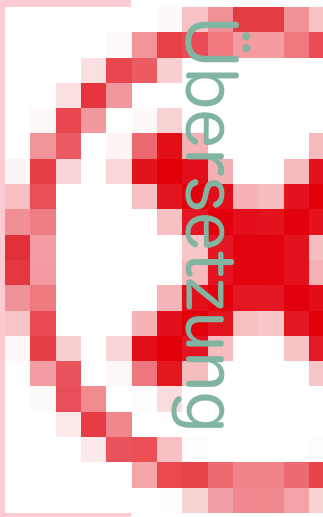
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Schwachstellen-Rechner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

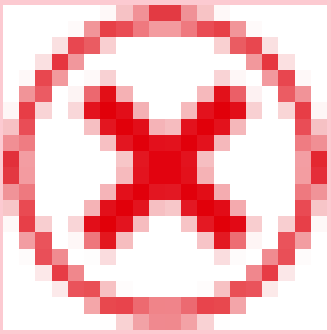
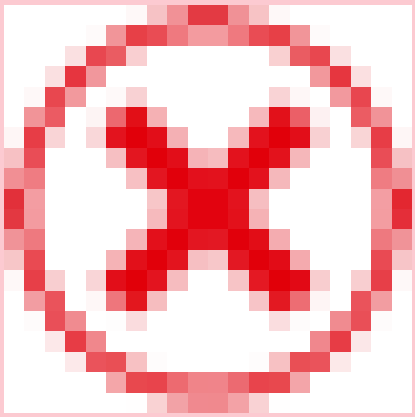
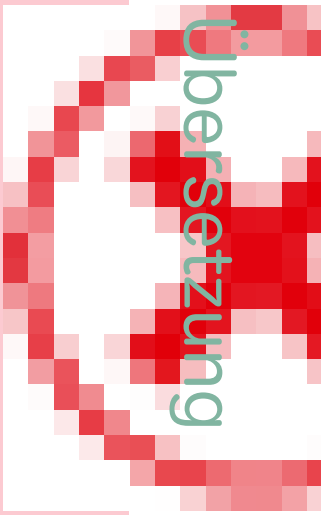
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Rechner für Schwachstellen-Rollup			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

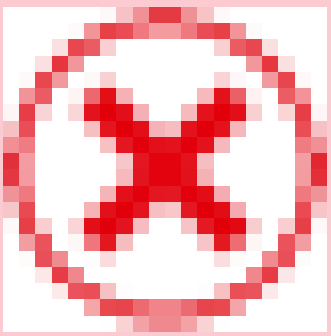
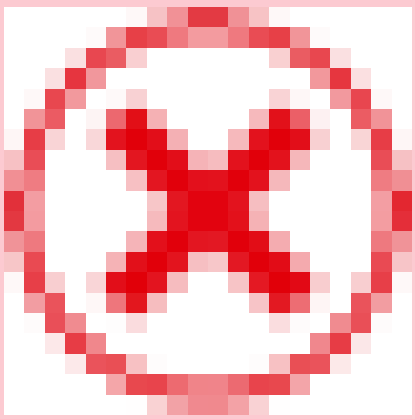
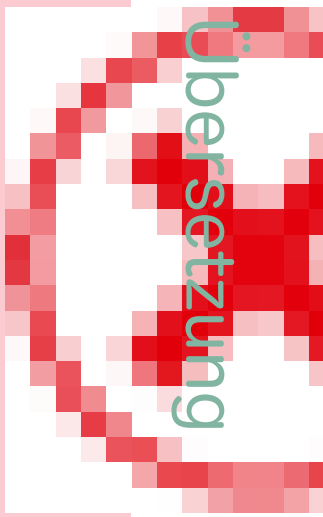
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Korrekturzielregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

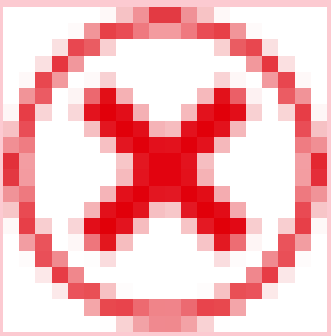
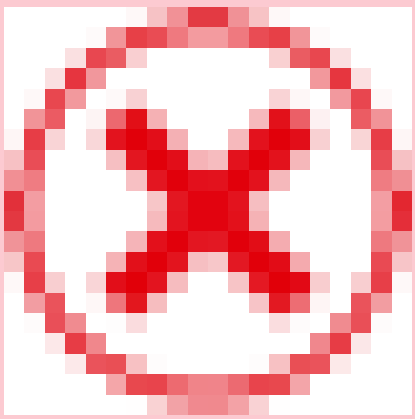
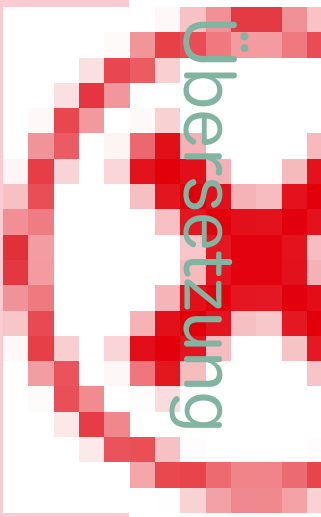
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Konfiguration automatisch schließen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

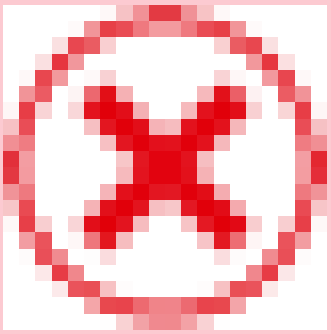
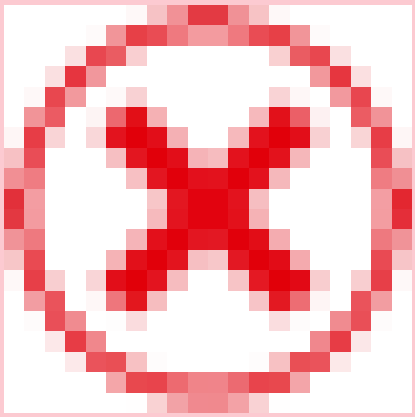
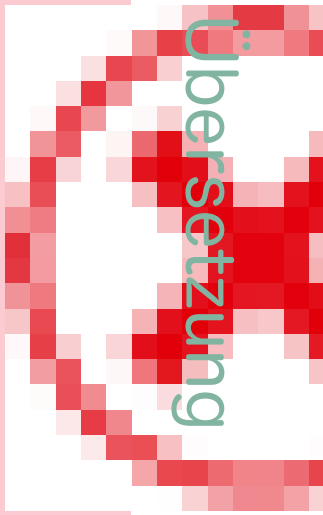
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Regeln für automatisches Löschen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

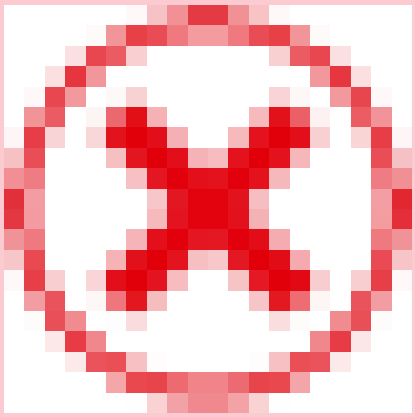
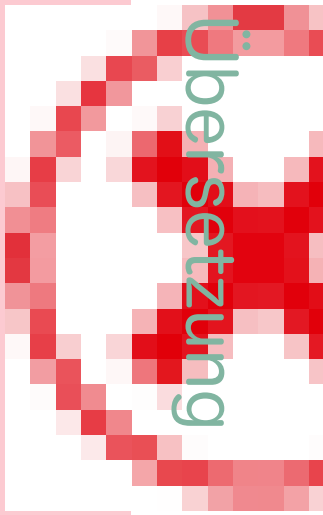
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Ausnahmeregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

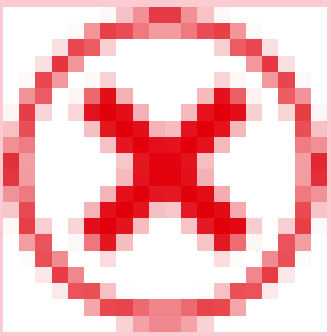
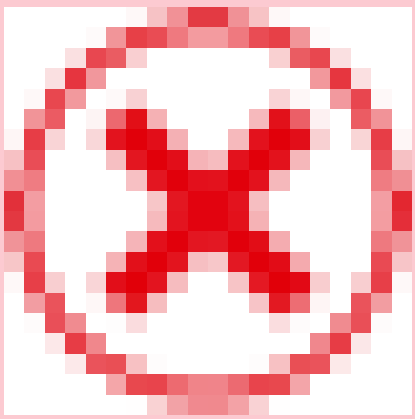
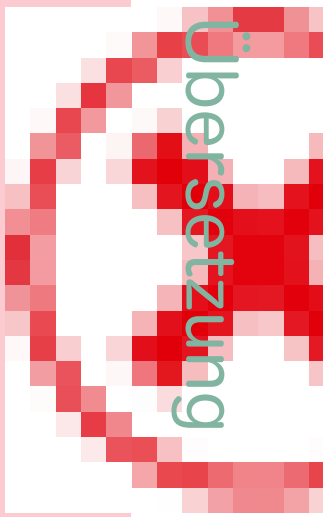
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Genehmigungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

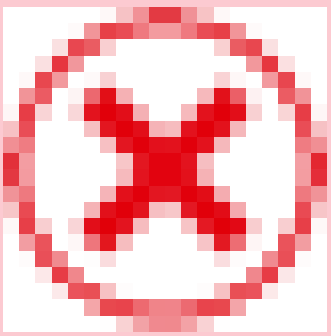
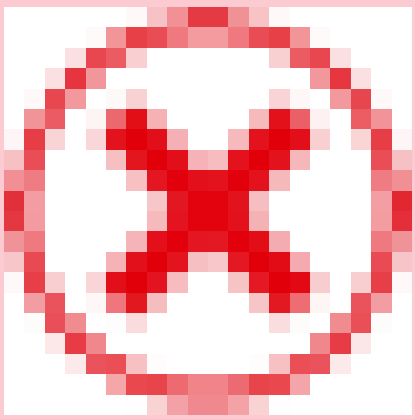
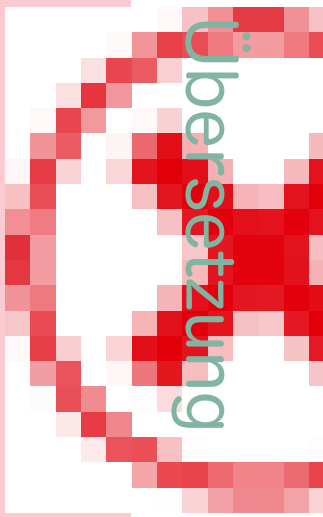
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Klassifizierungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

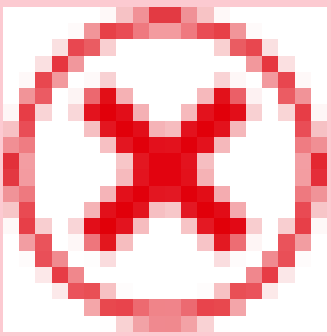
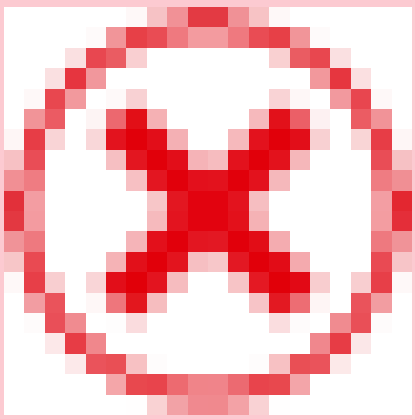
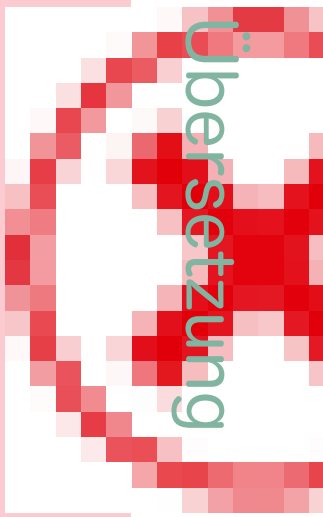
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Leistungskonfiguration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

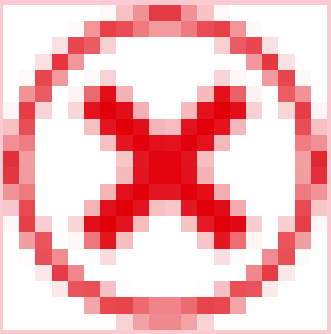
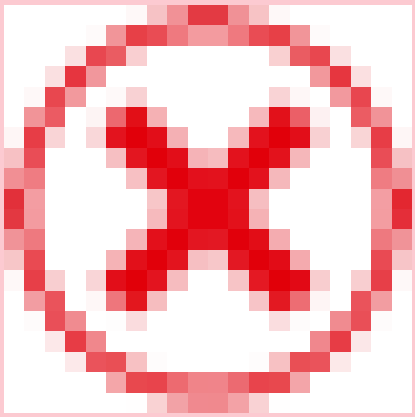
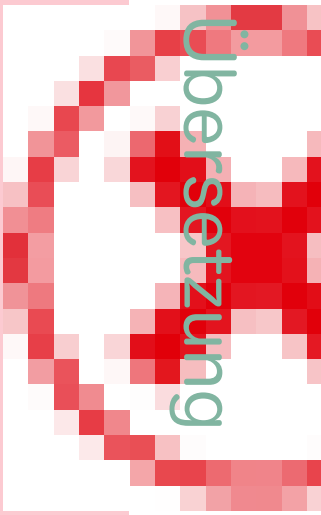
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
VI-Granularität konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

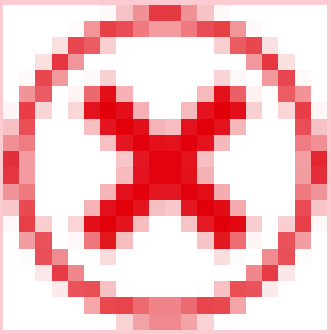
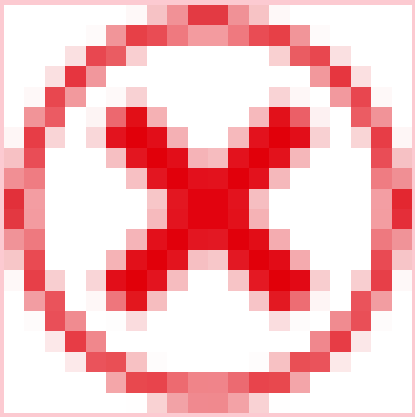
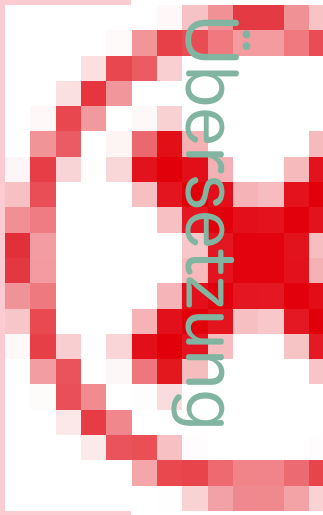
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Benachrichtigungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

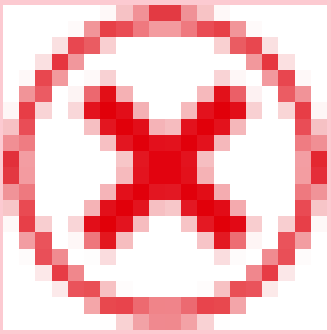
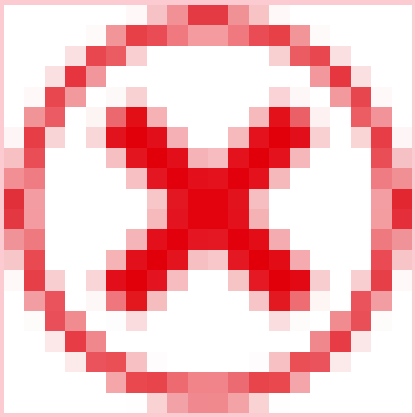
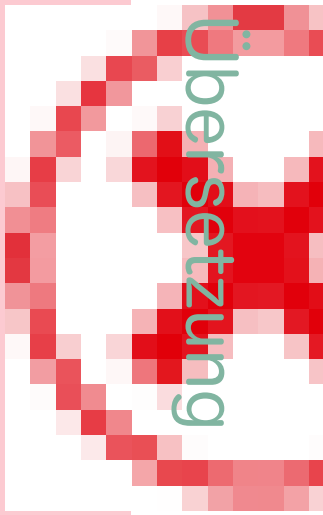
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
E-Mail-Vorlagen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

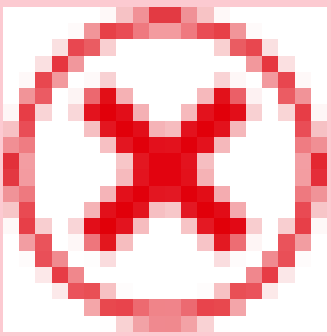
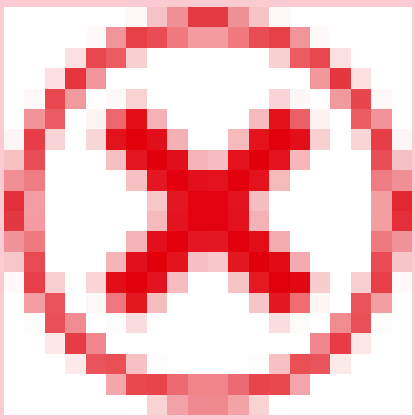
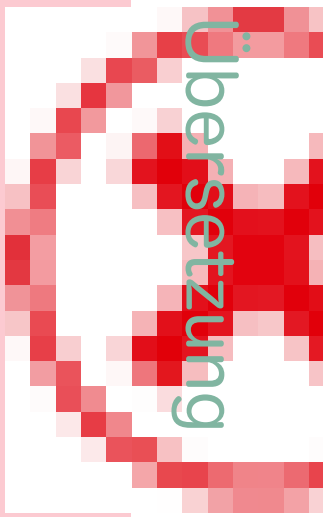
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Warteschlange importieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Integrationen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

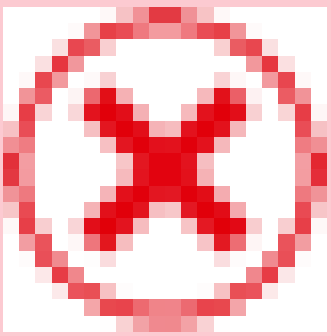
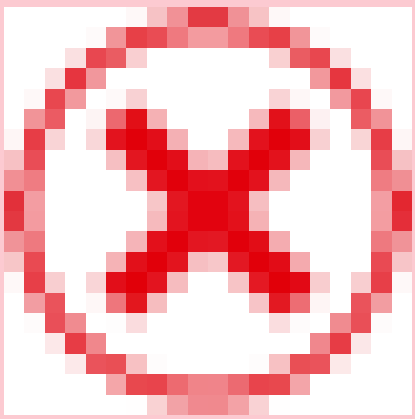
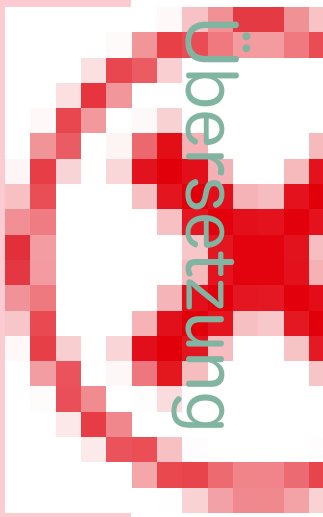
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
SLA-Definitionen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

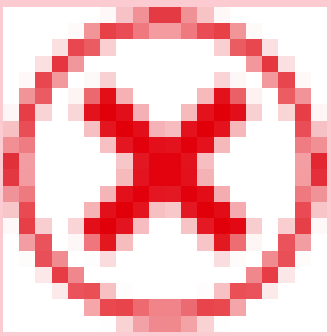
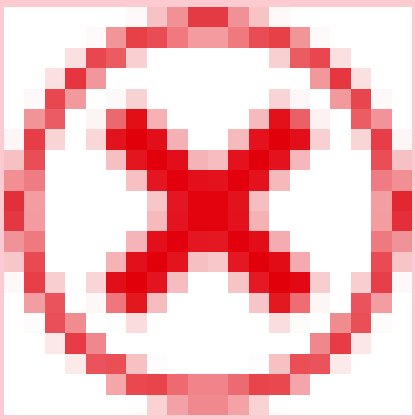
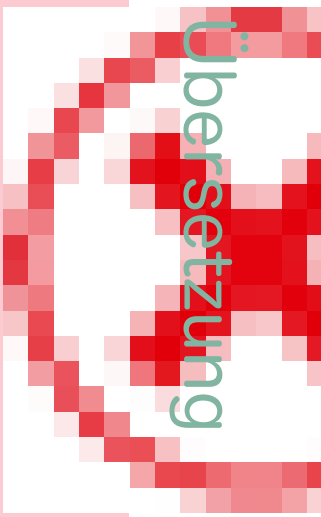
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
SAM-NVD konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

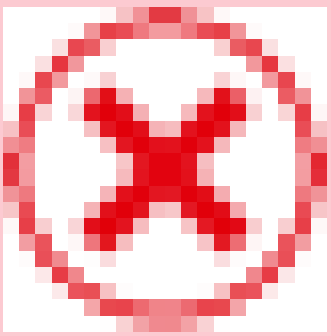
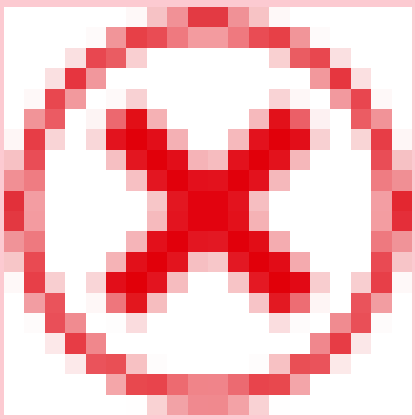
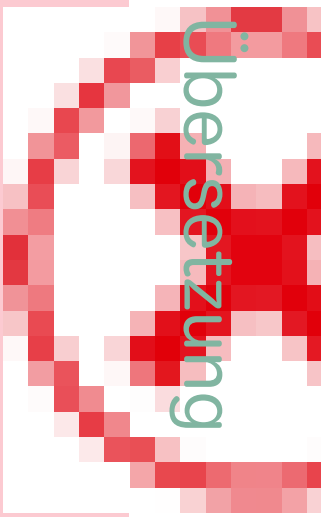
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Normalisierte Schweregradzuordnungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

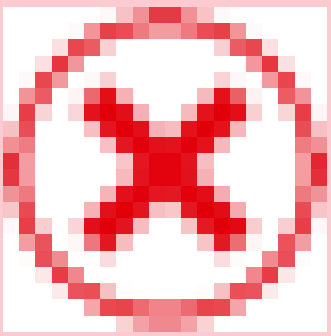
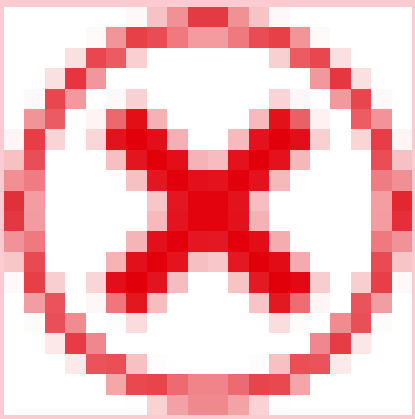
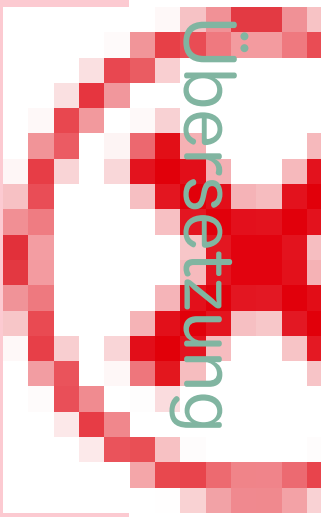
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Konfiguration der Scan-Abdeckung			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

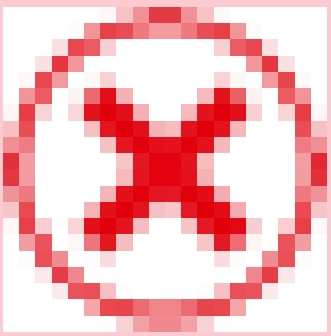
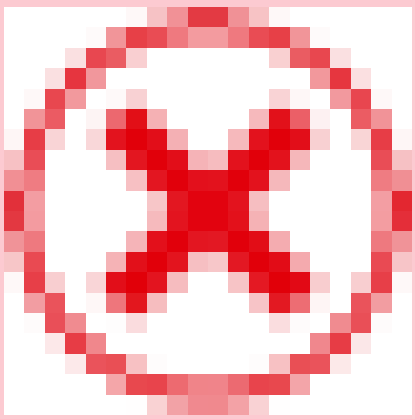
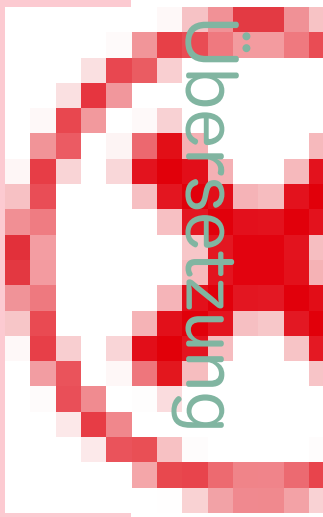
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Ausnahmenverwaltung			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

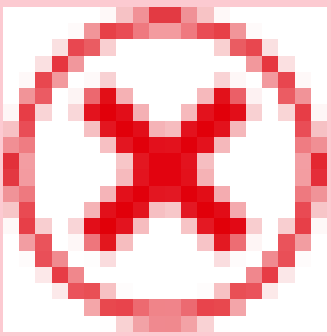
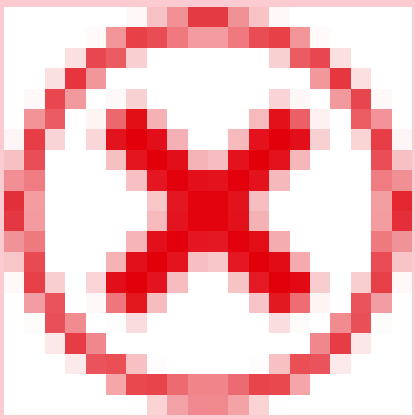
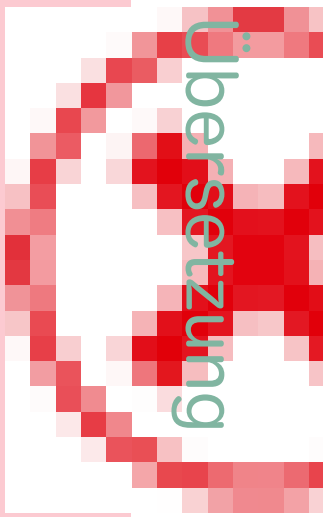
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Verwendungsbericht			
Diagnosen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

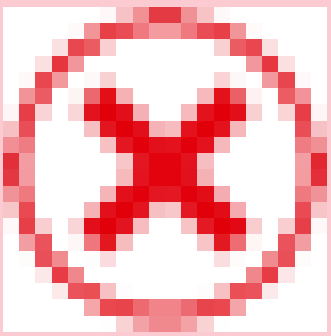
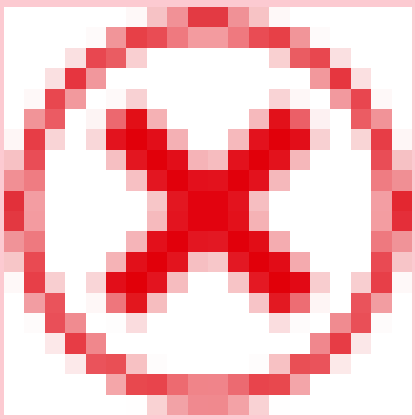
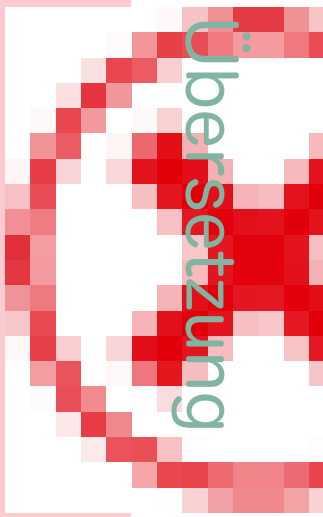
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Exception_Approver	sn_vul. Falsch_positiv_Genehmiger	sn_vul. Manage_assignmen
Überprüfungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
(Haupt-App-Gruppe)			
CISO-Dashboard	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

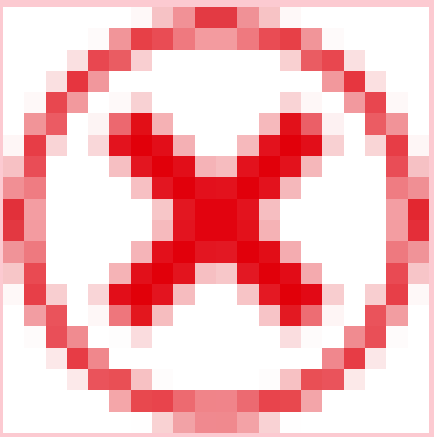
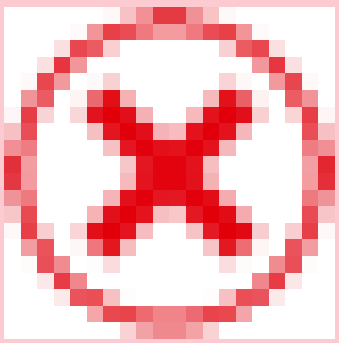
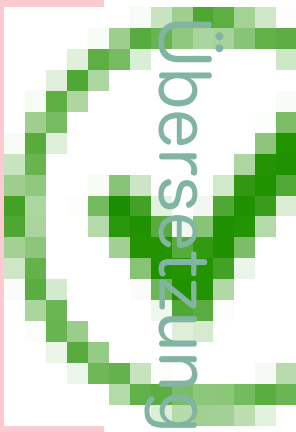
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Korrekturübersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Arbeitsbereich des Schwachstellenmanagers	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Übersicht	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Arbeitsbereich für IT-Korrekturen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Genehmiger-Übersicht	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Übersicht	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Meine Genehmigungen	✗	✗	✗
Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Aktiv	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Mir zugewiesen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Meinen Gruppen zugewiesen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Alle	✗	✗	✓
Angreifbare Elemente			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Kritisches Risiko	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Hohes Risiko	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Nutzbar	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Ziel rückt näher	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Verfehltes Ziel	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Innerhalb der letzten 90 Tage	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Älter als 90 Tage	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Nicht zugewiesen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Nicht gruppiert	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Außer Betrieb genommen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Mehrere Zurückstellungen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Alle	✗	✗	✓
Lösungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Alle	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

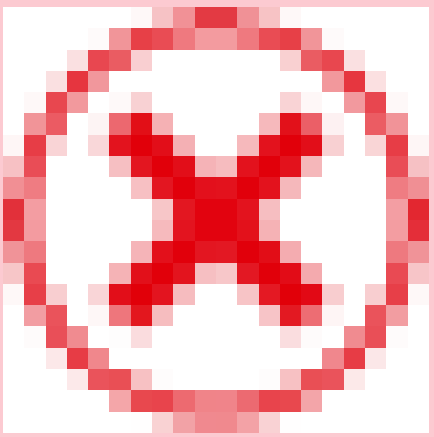
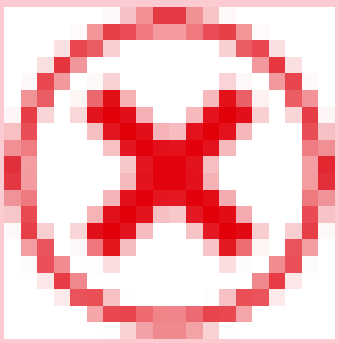
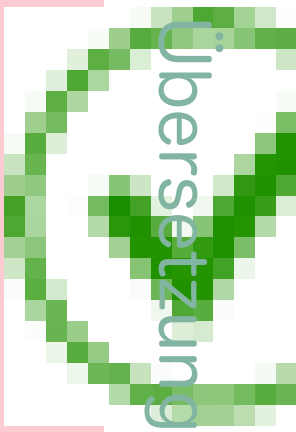
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Ersetzung mit höchster Priorität			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

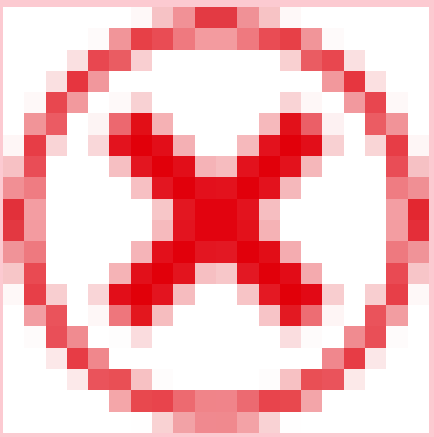
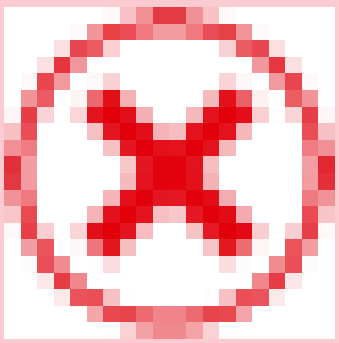
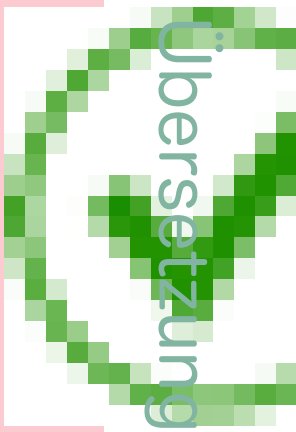
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Mit angreifbaren Elementen			
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
NVD	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
CWE	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Drittpartei	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Software mit Schwachstellen	✗	✗	✓
Schwachstellenscan			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Bewertung des Gefahrenpotenzials	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Scans	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Scanner	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Scan-Warteschlange	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Scannerquotengrenzen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

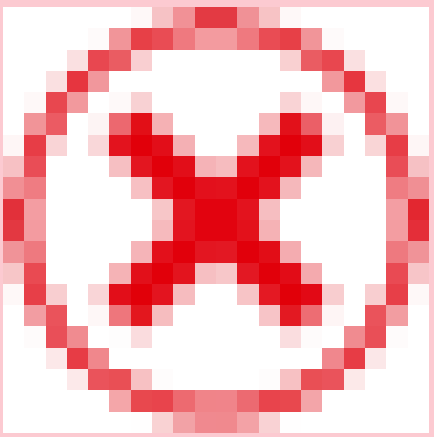
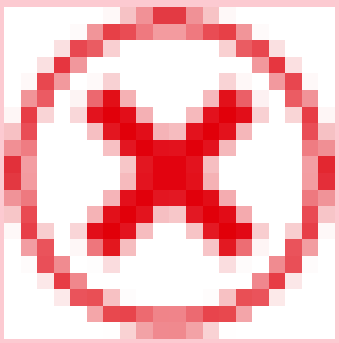
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Quotengrenzdefinitionen			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Setup-Assistent	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Überwachungsthemen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Zuweisungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Regeln für Korrekturaufgaben	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Zuweisungsempfehlungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Schwachstellen-Rechner	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Rechner für Schwachstellen-Rollup	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Korrekturzielregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Konfiguration automatisch schließen	✓	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Regeln für automatisches Löschen	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Ausnahmeregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Genehmigungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Klassifizierungsregeln	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

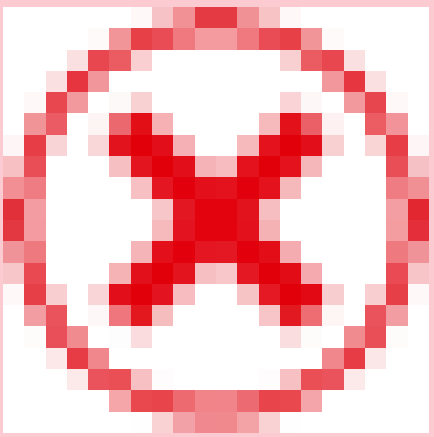
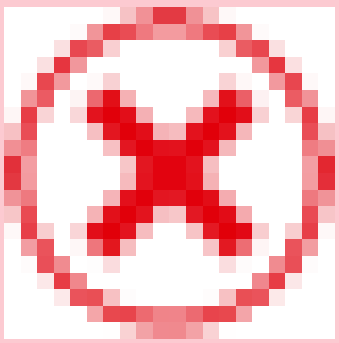
sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Leistungskonfiguration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
VI-Granularität konfigurieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Benachrichtigungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
E-Mail-Vorlagen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Warteschlange importieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Integrationen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
SLA-Definitionen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
SAM-NVD konfigurieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Normalisierte Schweregradzuordnungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Konfiguration der Scan-Abdeckung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Ausnahmenverwaltung	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Verwendungsbericht	✗	✗	✗
Diagnosen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Auto_close_stale_VI	sn_vul. Manage_Auto_delete	sn_vul. Manage_classific
Überprüfungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

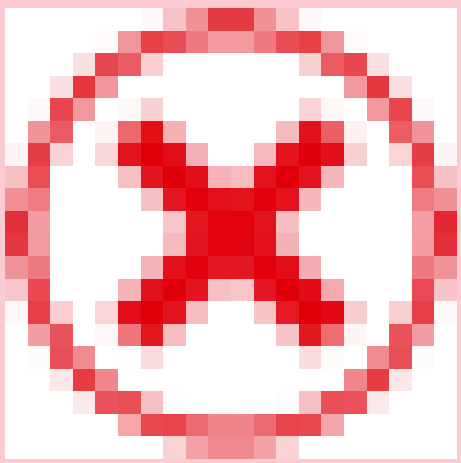
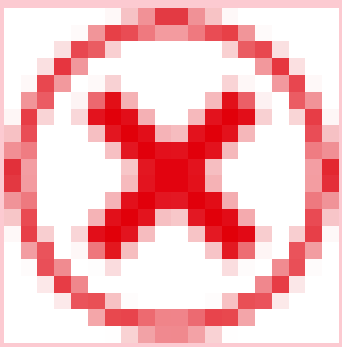
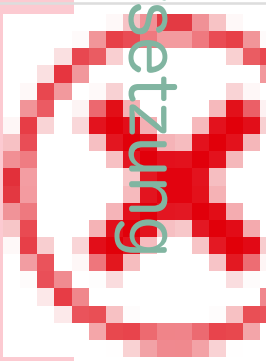
sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
(Haupt-App-Gruppe)			
CISO-Dashboard			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Korrekturübersicht	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

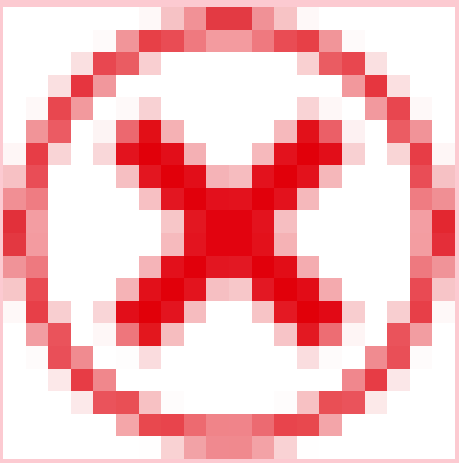
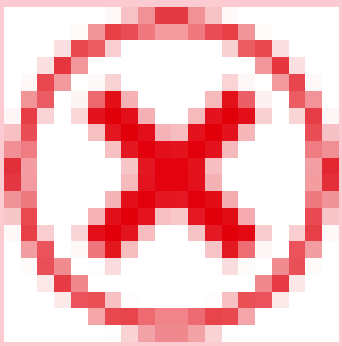
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Arbeitsbereich des Schwachstellenmanagers			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Übersicht	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Arbeitsbereich für IT-Korrekturen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Genehmiger-Übersicht	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Übersicht	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

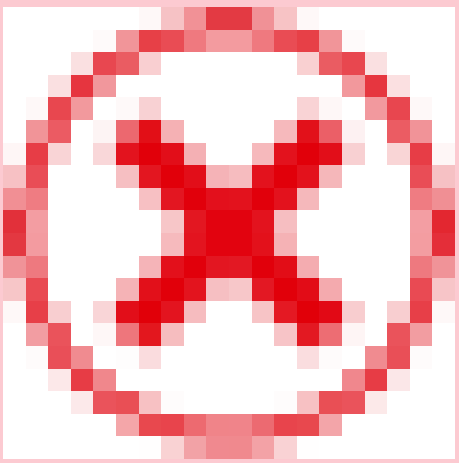
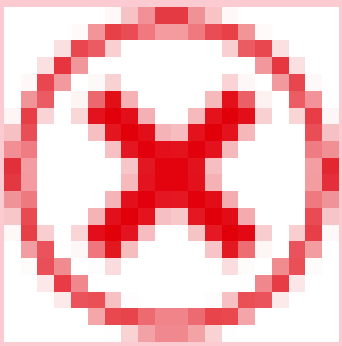
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Meine Genehmigungen			
Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Aktiv	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Mir zugewiesen	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Meinen Gruppen zugewiesen	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Alle	✗	✓	✗
Angreifbare Elemente			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Kritisches Risiko	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Hohes Risiko	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

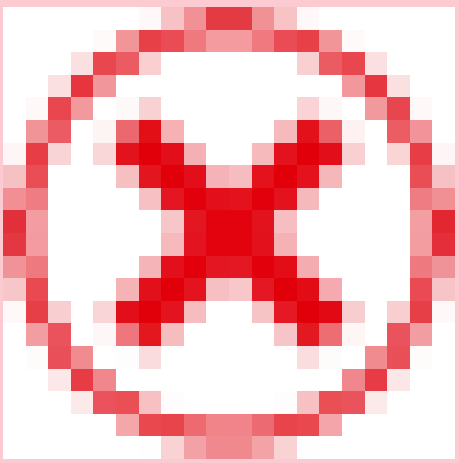
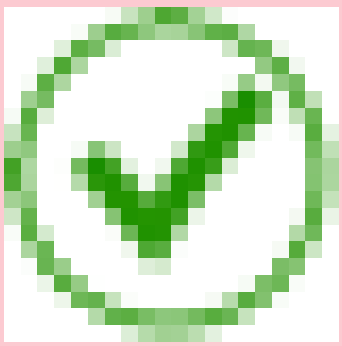
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Nutzbar			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Ziel rückt näher	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

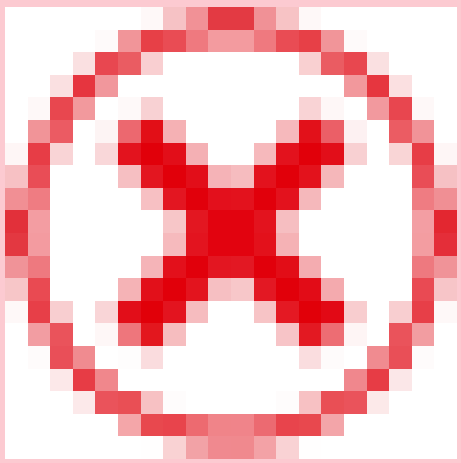
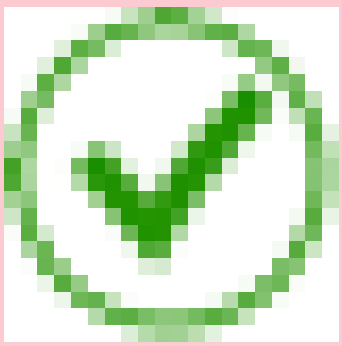
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Verfehltes Ziel			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

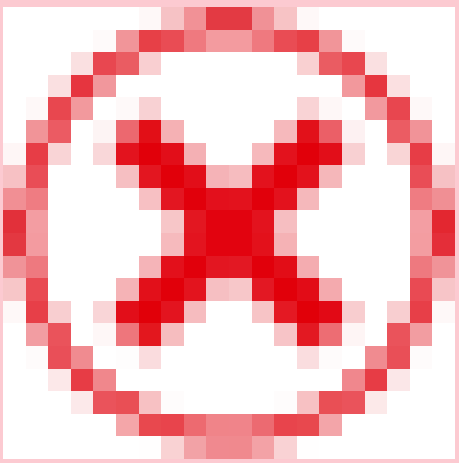
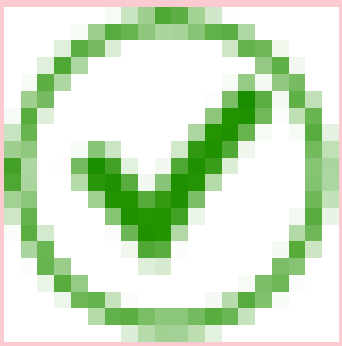
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Innerhalb der letzten 90 Tage			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

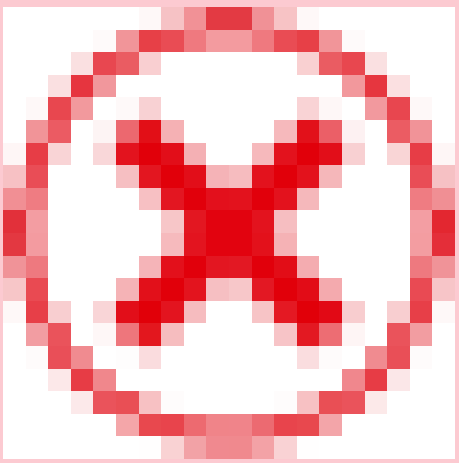
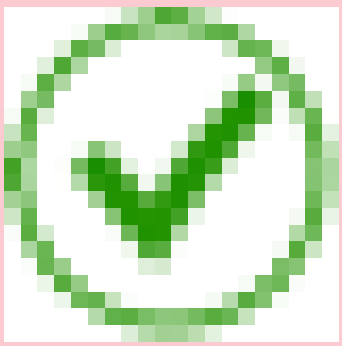
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Älter als 90 Tage			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Nicht zugewiesen	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Nicht gruppiert	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Außer Betrieb genommen	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Mehrere Zurückstellungen	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Alle	✗	✓	✗
Lösungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Alle	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

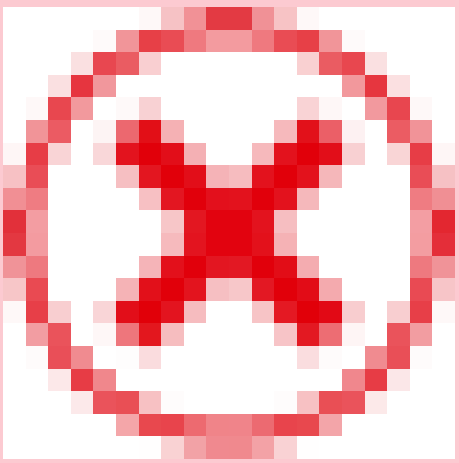
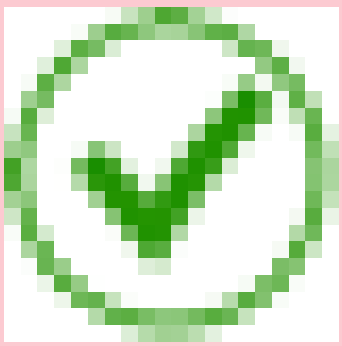
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Ersetzung mit höchster Priorität			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Mit angreifbaren Elementen	✗	✓	✗
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
NVD	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
CWE	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Drittpartei	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Software mit Schwachstellen	✗	✓	✗
Schwachstellenscan			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

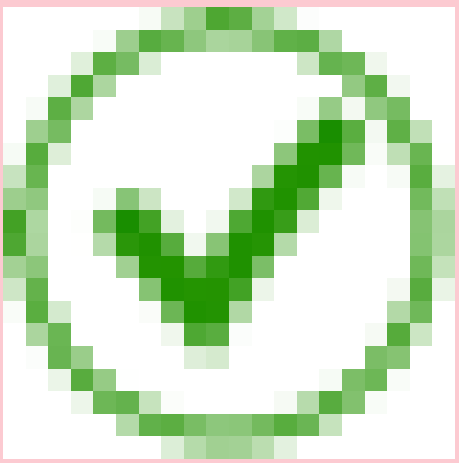
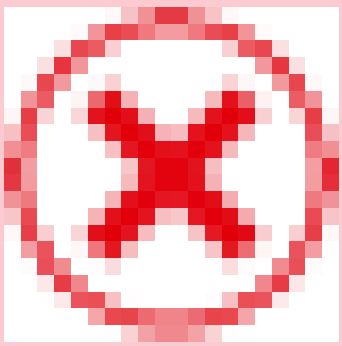
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Bewertung des Gefahrenpotenzials			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Scans	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Scanner	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Scan-Warteschlange	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Scannerquotengrenzen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Quotengrenzdefinitionen	✗	✗	✗
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Setup-Assistent	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Überwachungsthemen	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Zuweisungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Regeln für Korrekturaufgaben	✗	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Zuweisungsempfehlungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Schwachstellen-Rechner	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Rechner für Schwachstellen-Rollup	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Korrekturzielregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Konfiguration automatisch schließen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Regeln für automatisches Löschen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

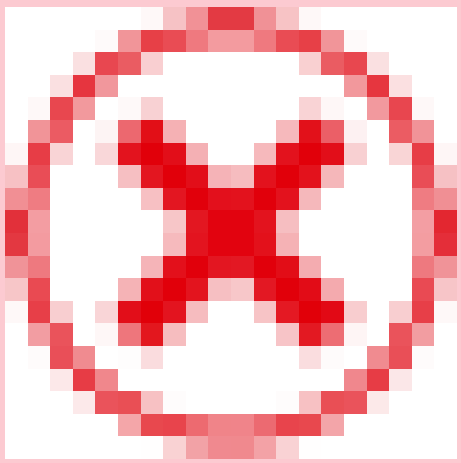
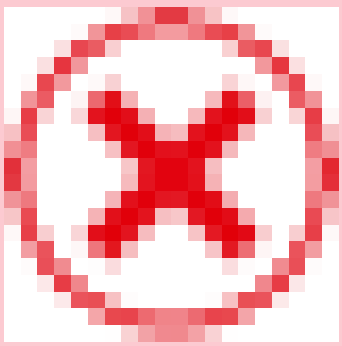
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Ausnahmeregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

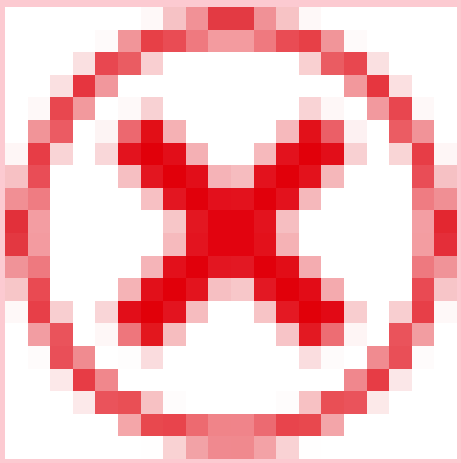
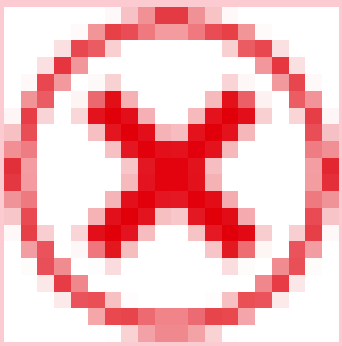
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Genehmigungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Klassifizierungsregeln	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Leistungskonfiguration	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
VI-Granularität konfigurieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Benachrichtigungen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
E-Mail-Vorlagen	✗	✗	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Warteschlange importieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Integrationen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
SLA-Definitionen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
SAM-NVD konfigurieren	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Normalisierte Schweregradzuordnungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

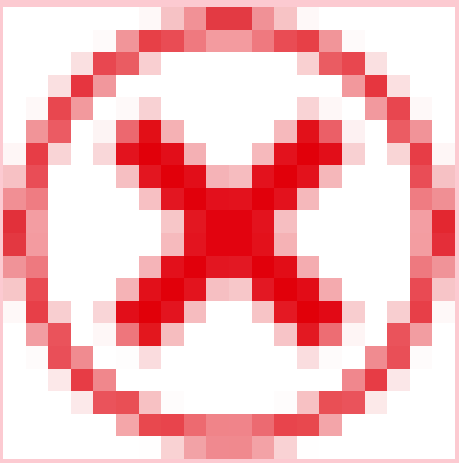
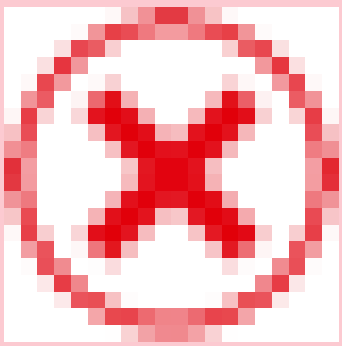
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Konfiguration der Scan-Abdeckung			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

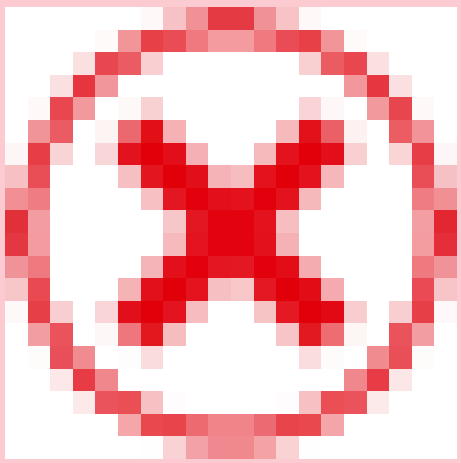
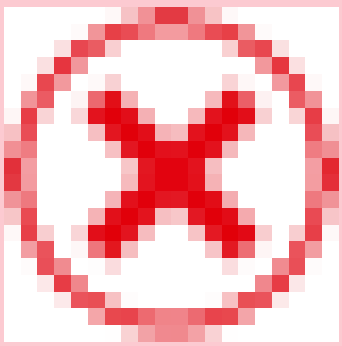
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Ausnahmenverwaltung			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Verwendungsbericht	✗	✗	✗
Diagnosen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.manage_exposure_assessment, sn_vul.manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.manage_permissions

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_exposure_assessment	sn_vul. Manage_Group_rules	sn_vul. Manage_Notifi
Überprüfungen	✗	✗	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

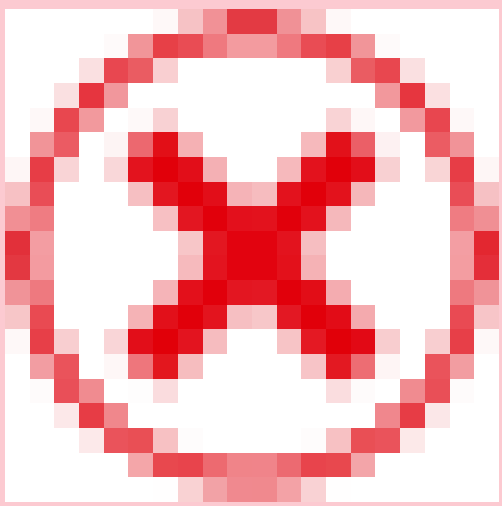
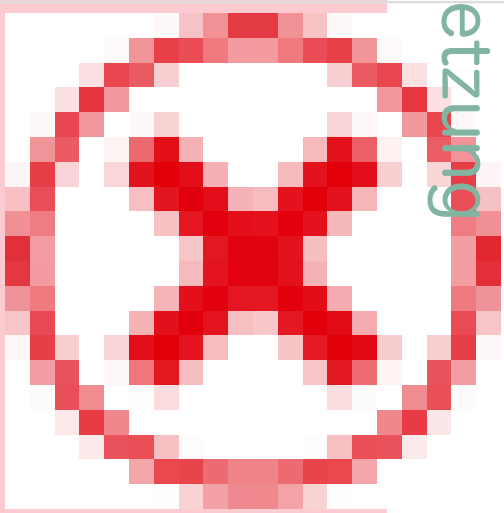
sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
(Haupt-App-Gruppe)			
CISO-Dashboard			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

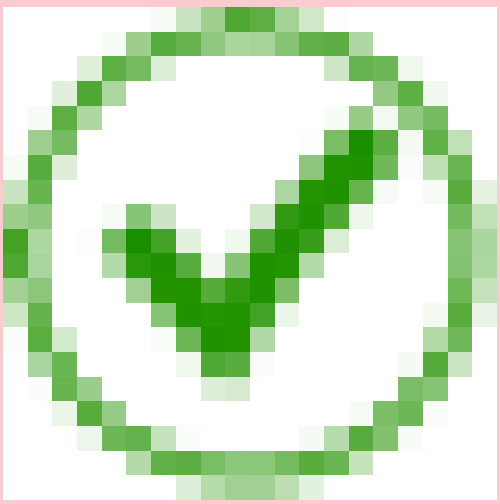
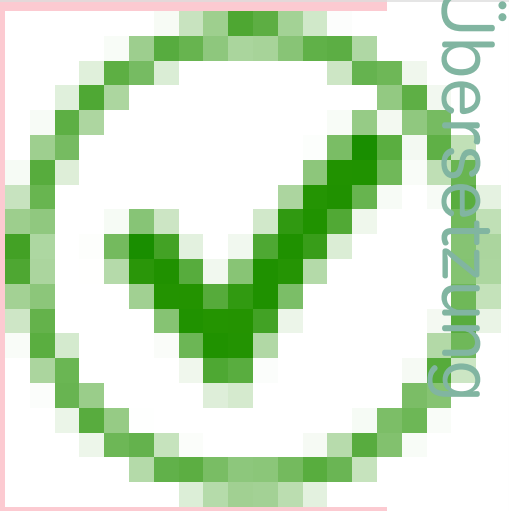
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Korrekturübersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Arbeitsbereich des Schwachstellenmanagers			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Übersicht	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

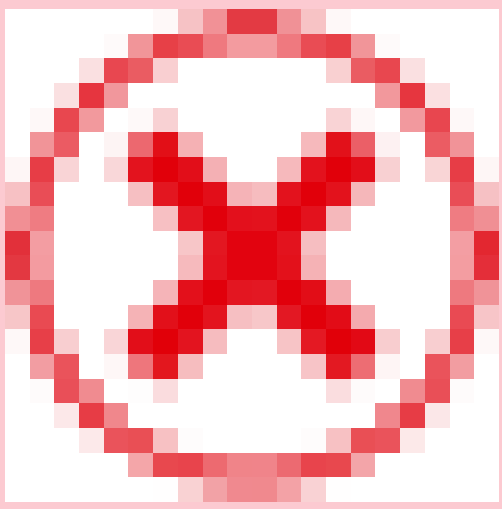
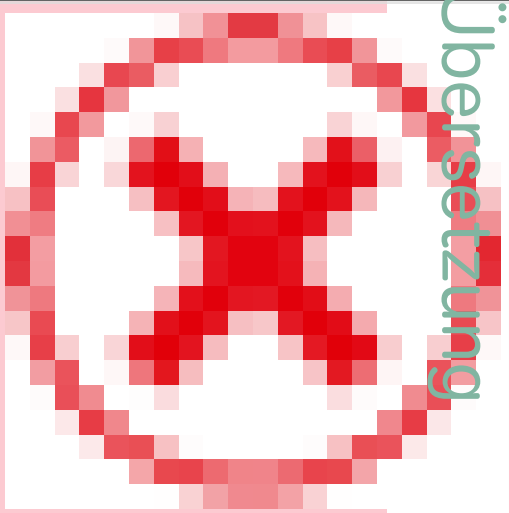
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Arbeitsbereich für IT-Korrekturen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Genehmiger-Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

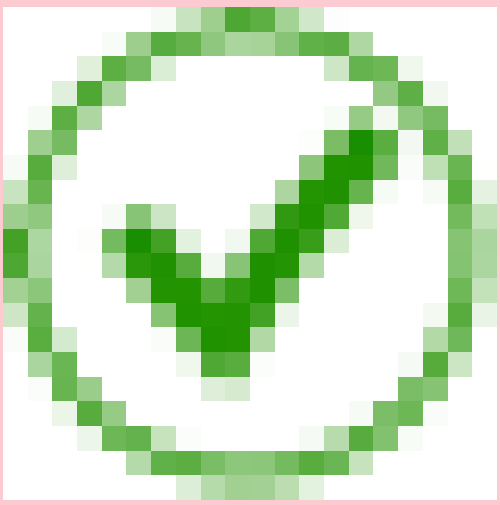
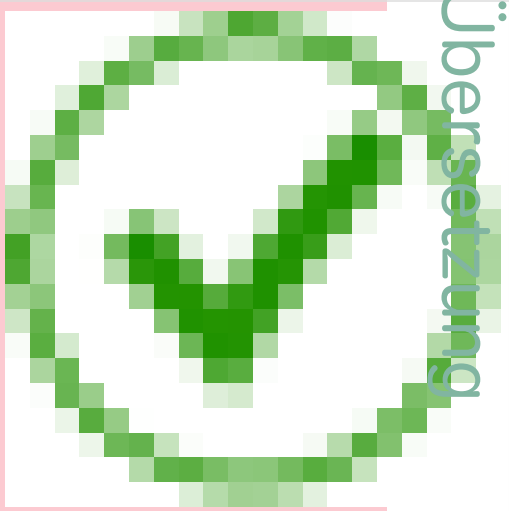
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Übersicht			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Meine Genehmigungen			
Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

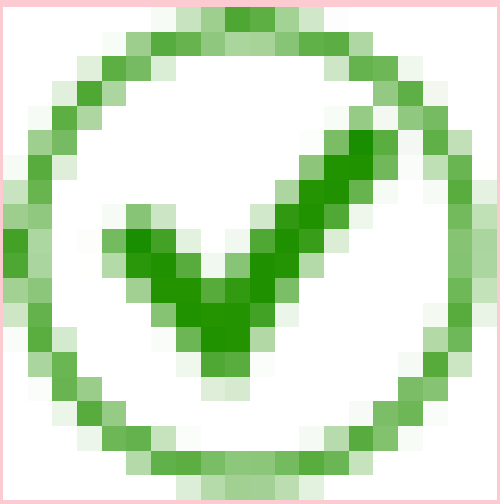
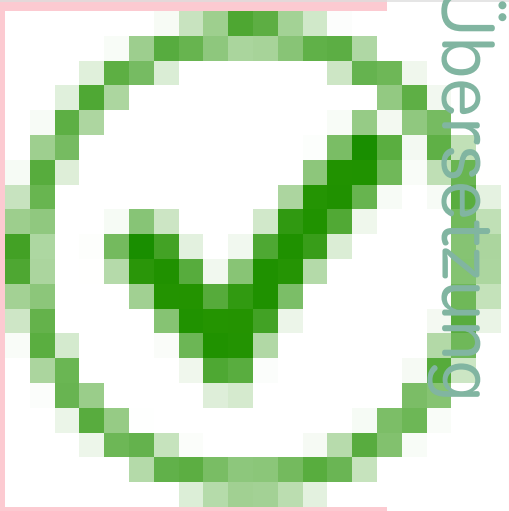
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Aktiv			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Mir zugewiesen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Meinen Gruppen zugewiesen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Alle	✓	✓	✓
Angreifbare Elemente			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

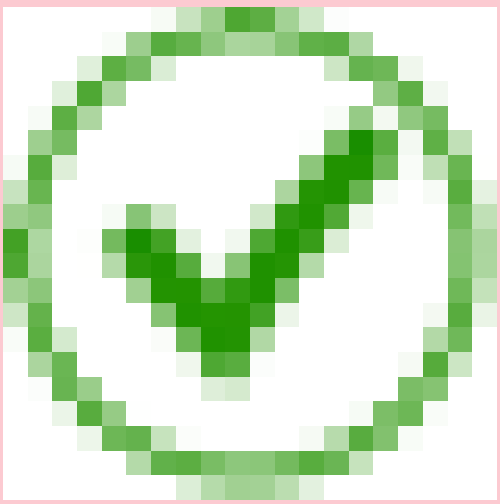
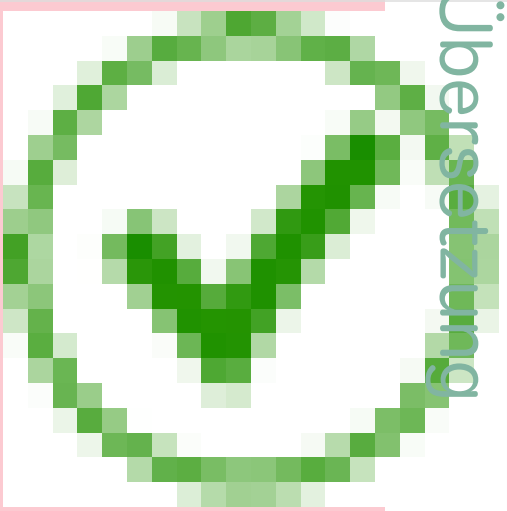
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Kritisches Risiko			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Hohes Risiko	✓	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Nutzbar	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Ziel rückt näher	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

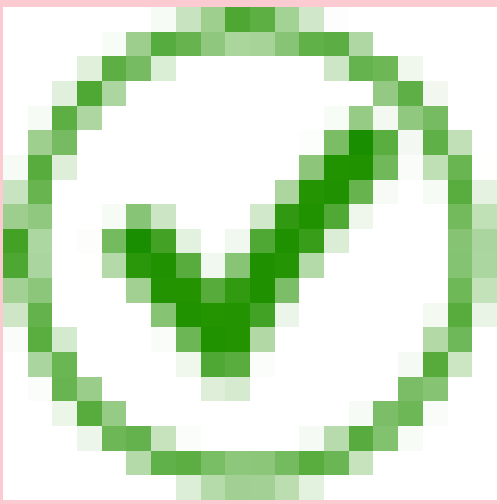
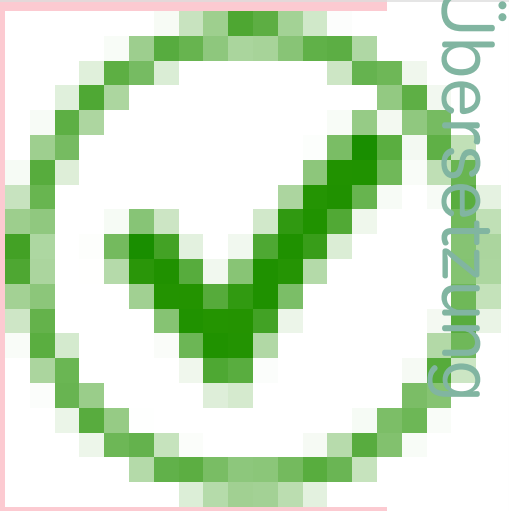
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Verfehltes Ziel			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Innerhalb der letzten 90 Tage	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

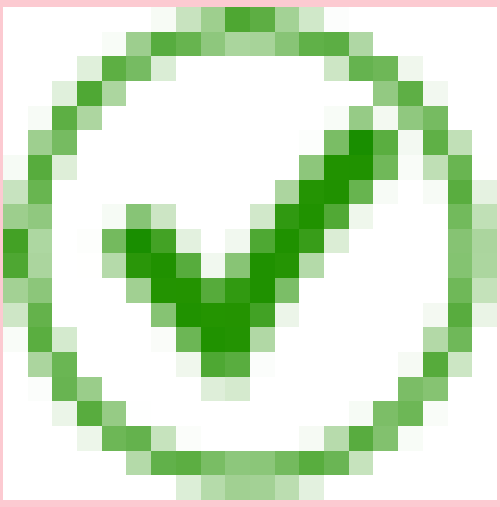
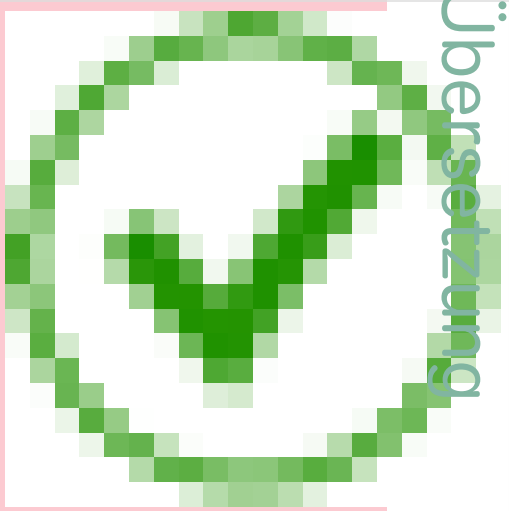
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Älter als 90 Tage			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

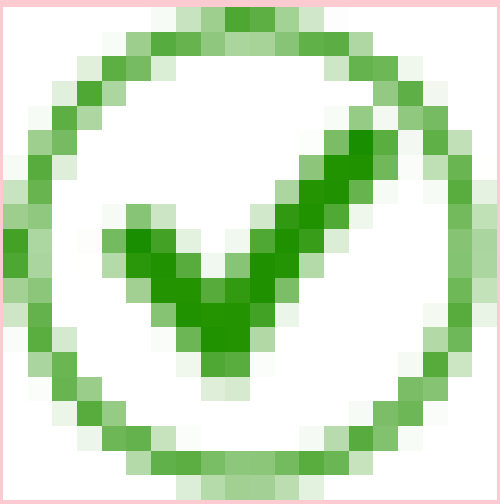
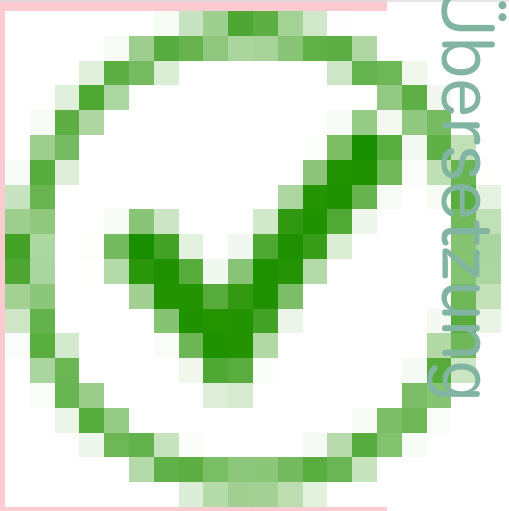
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Nicht zugewiesen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

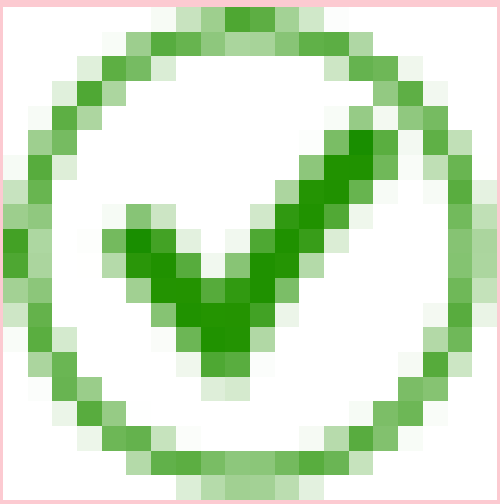
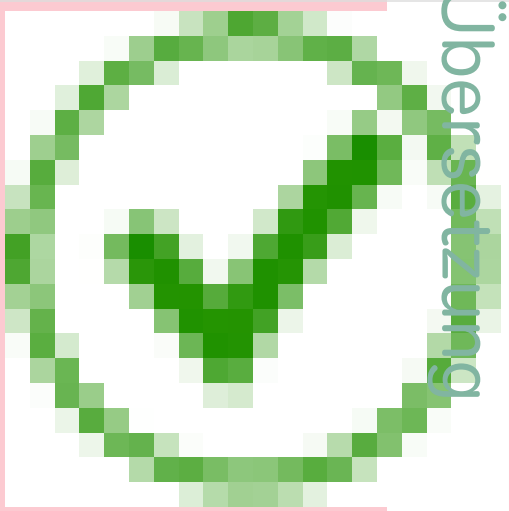
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Nicht gruppiert			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Außer Betrieb genommen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Mehrere Zurückstellungen	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

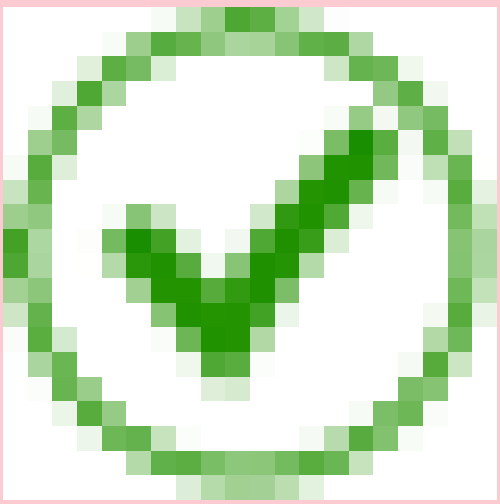
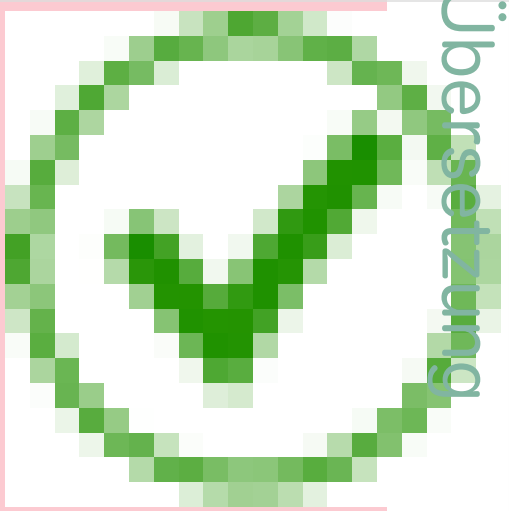
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Alle			
Lösungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

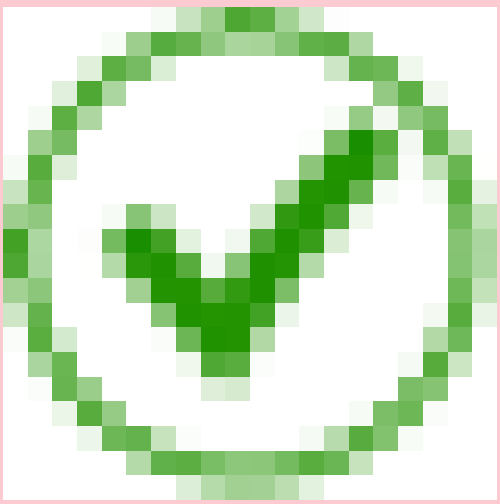
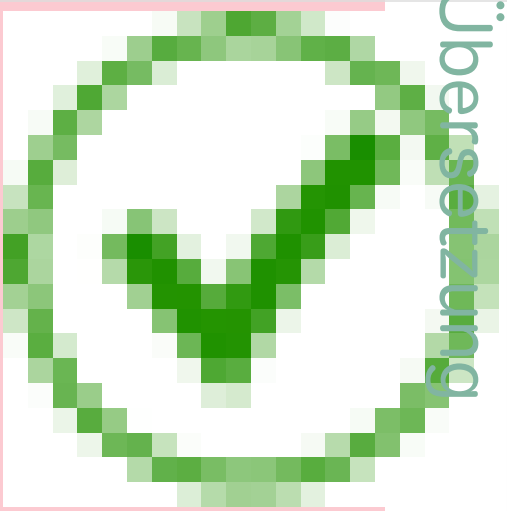
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Alle			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

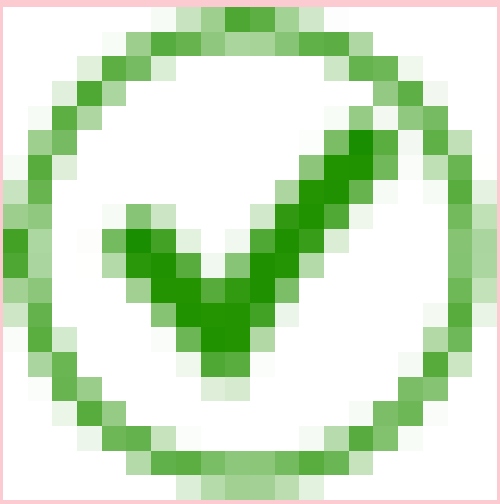
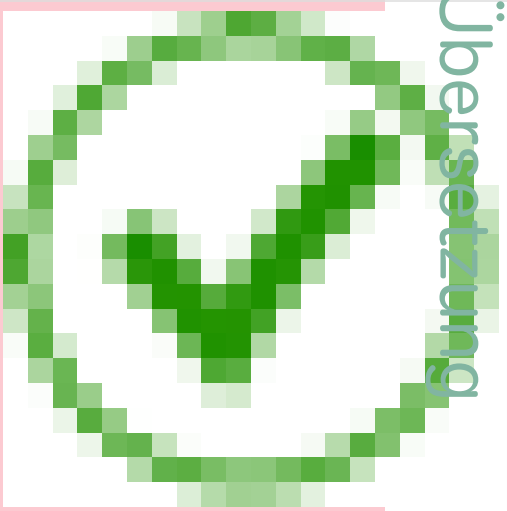
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Ersetzung mit höchster Priorität			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Mit angreifbaren Elementen	✓	✓	
Bibliotheken			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

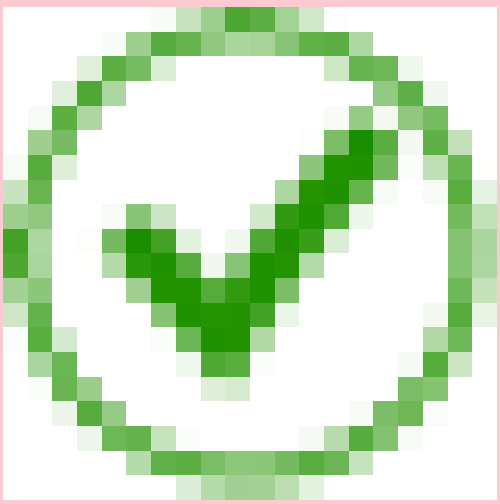
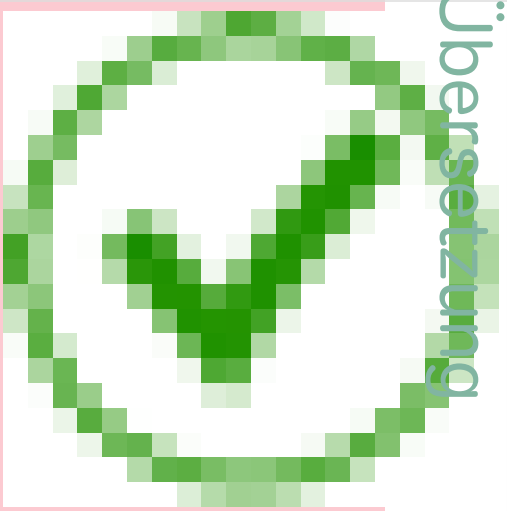
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
NVD			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

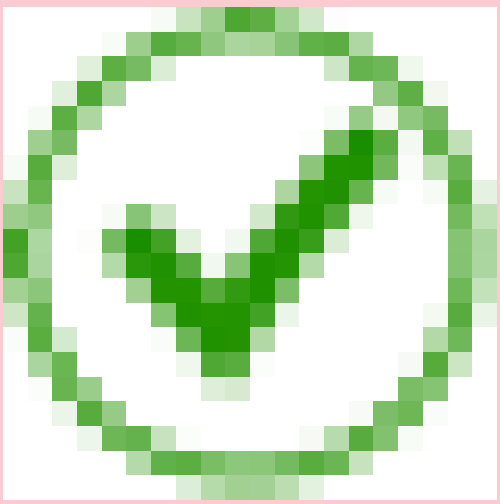
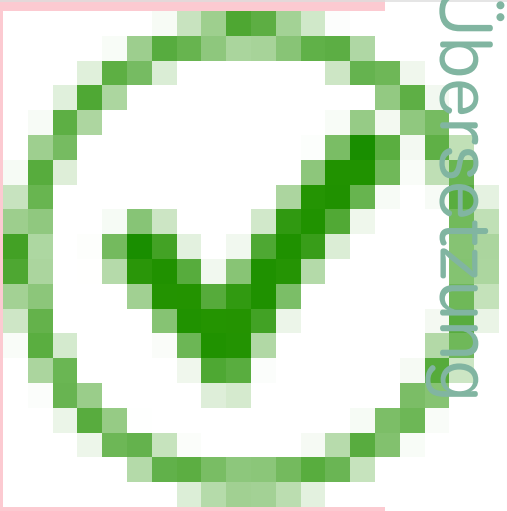
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
CWE			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Drittpartei	✓	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Software mit Schwachstellen	✓	✓	
Schwachstellenscan			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

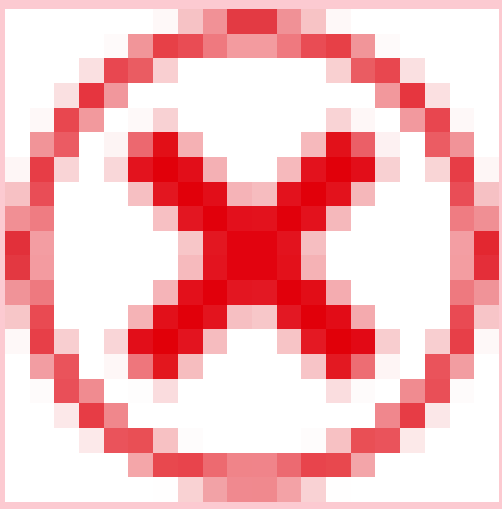
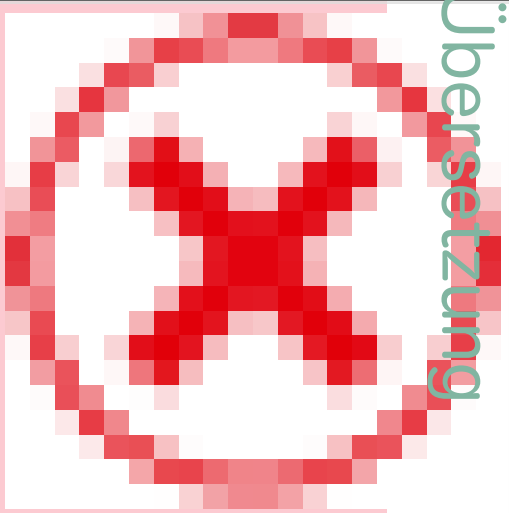
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Bewertung des Gefahrenpotenzials			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Scans	✓	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

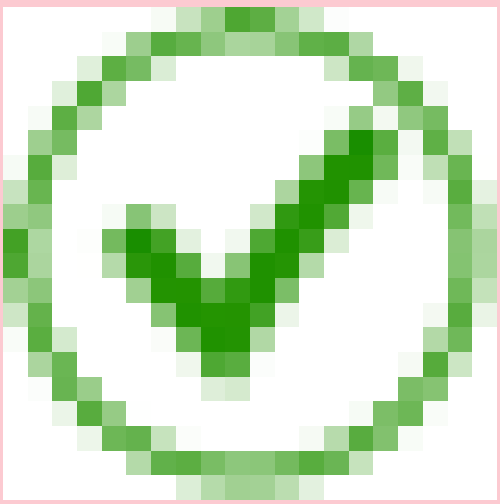
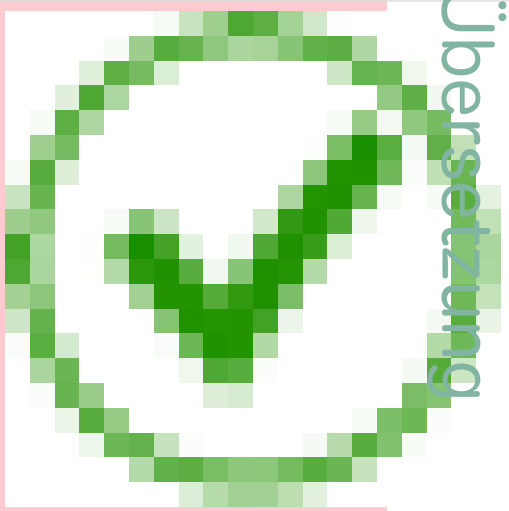
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Scanner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Scan-Warteschlange	✓	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Scannerquotengrenzen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

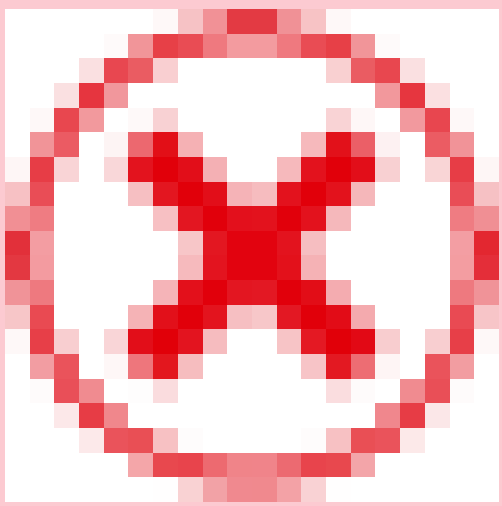
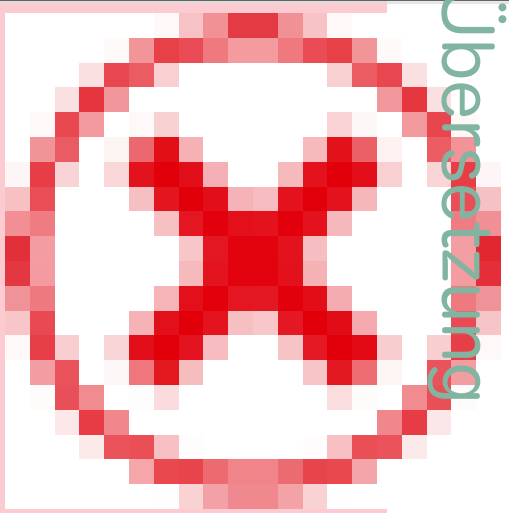
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Quotengrenzdefinitionen			
Administration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

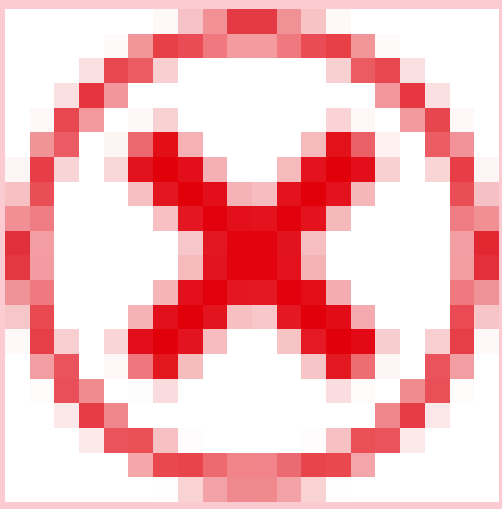
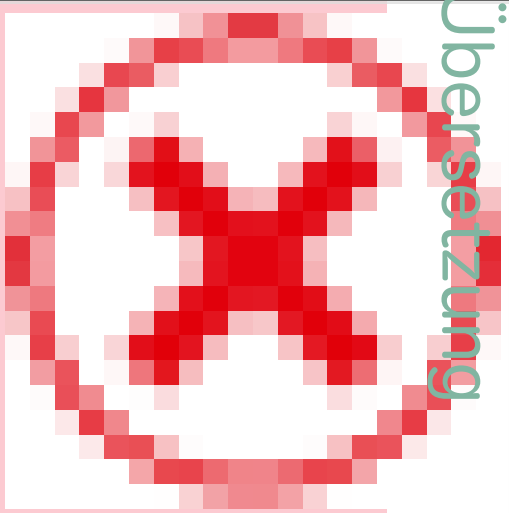
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Setup-Assistent			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Überwachungsthemen	✓	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Zuweisungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Regeln für Korrekturaufgaben			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

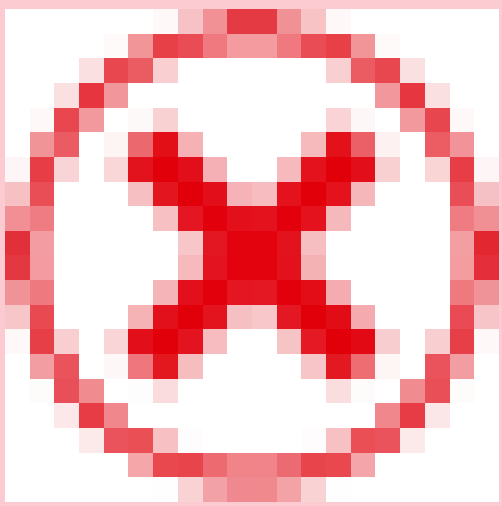
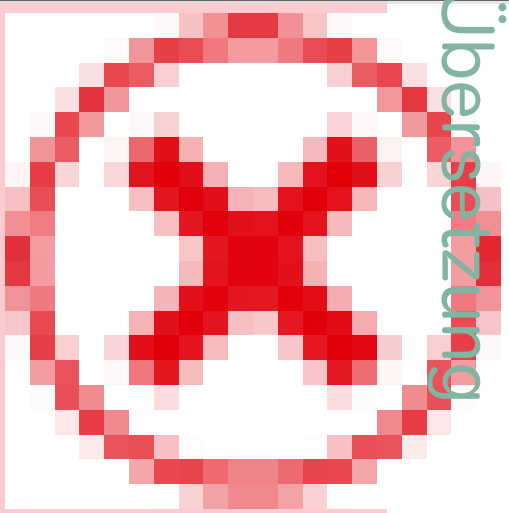
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Zuweisungsempfehlungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

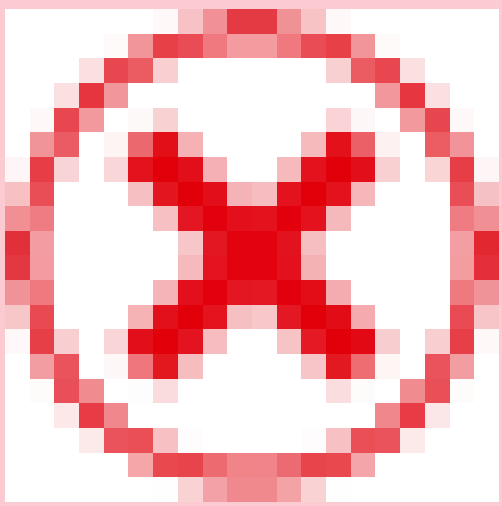
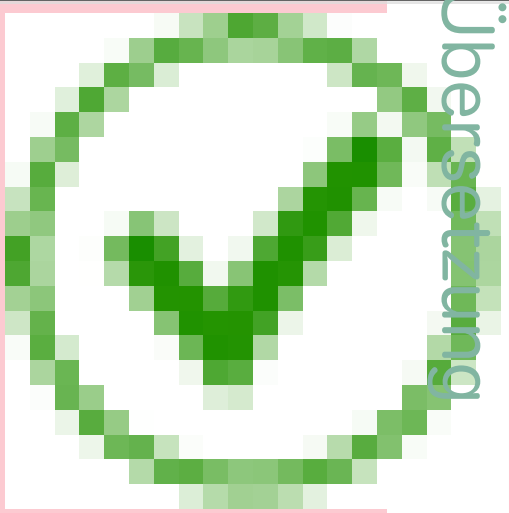
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Schwachstellen-Rechner			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

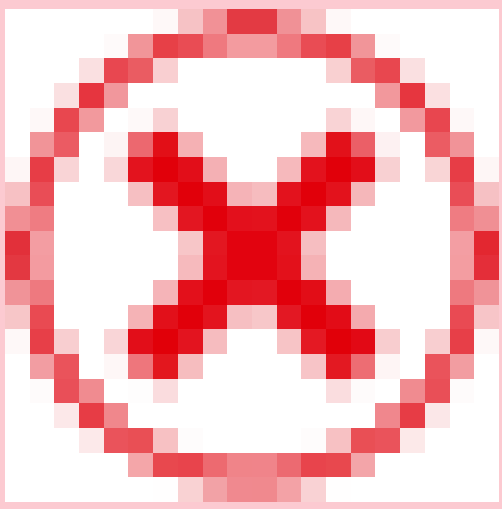
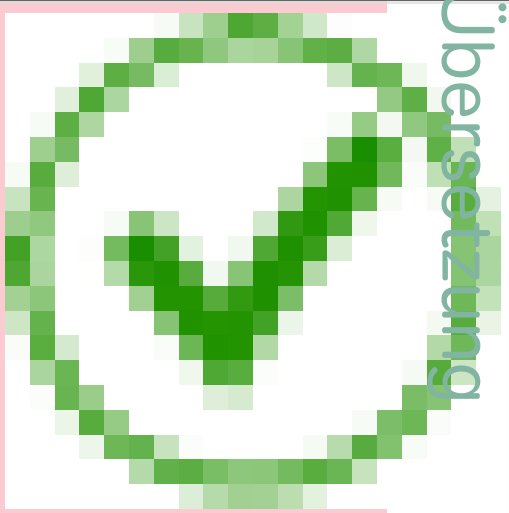
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Rechner für Schwachstellen-Rollup			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

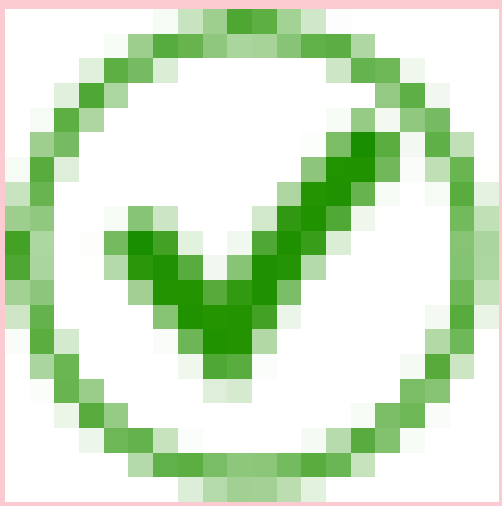
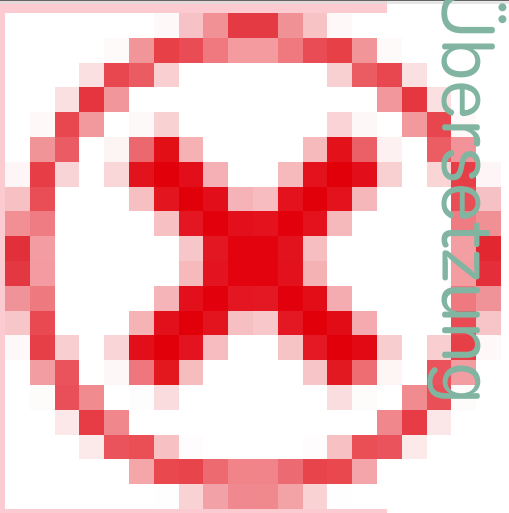
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Korrekturzielregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Konfiguration automatisch schließen	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Regeln für automatisches Löschen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Ausnahmeregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Genehmigungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Klassifizierungsregeln			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Leistungskonfiguration			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

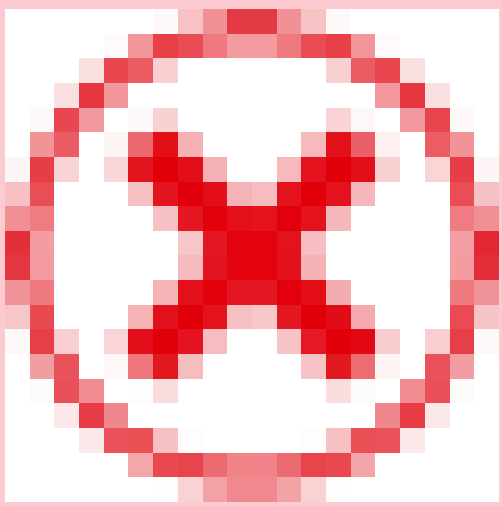
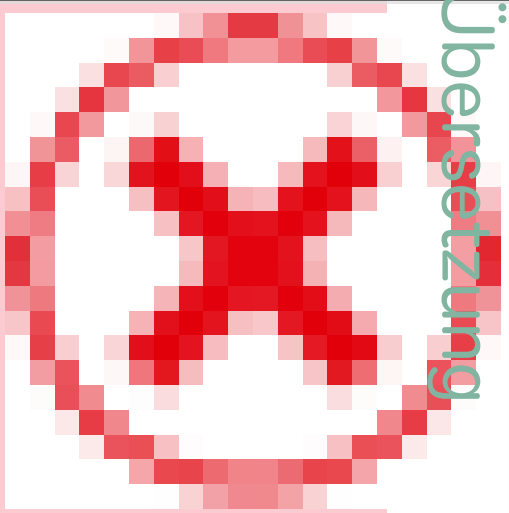
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
VI-Granularität konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

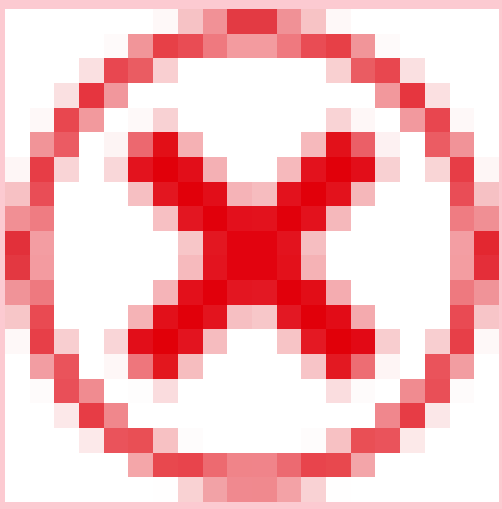
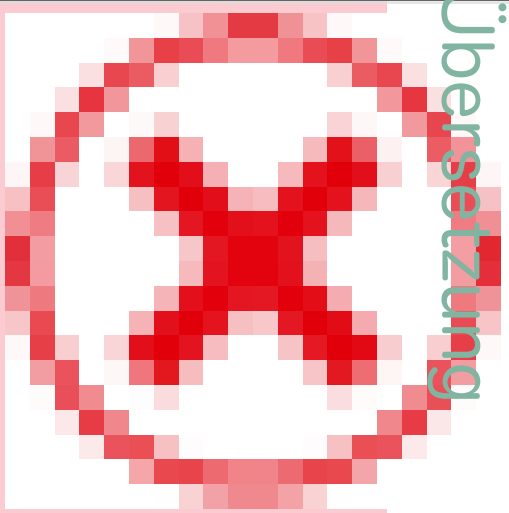
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Benachrichtigungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

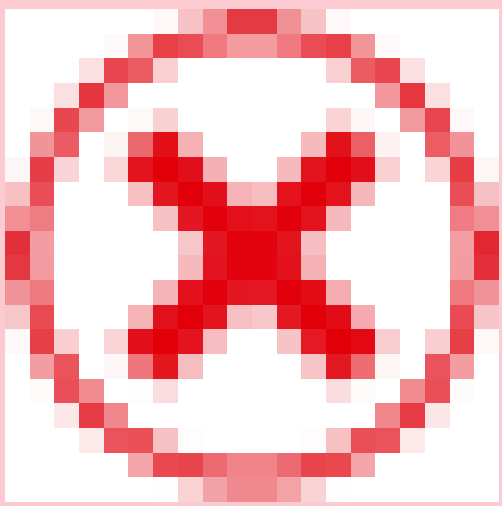
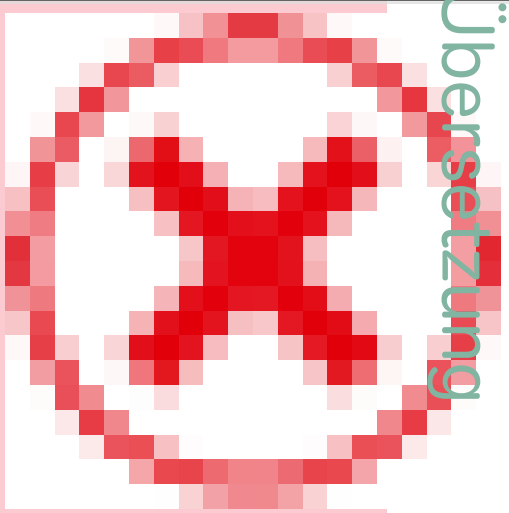
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
E-Mail-Vorlagen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Warteschlange importieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

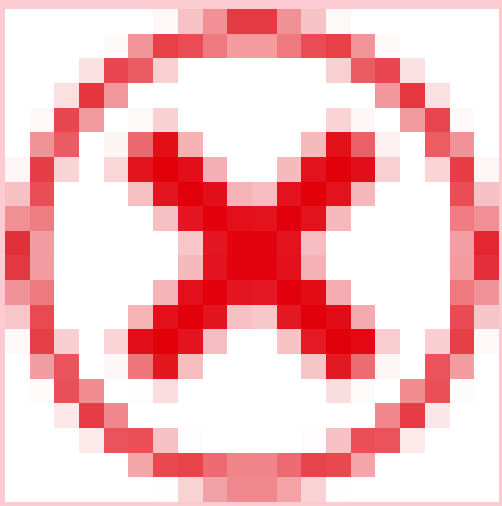
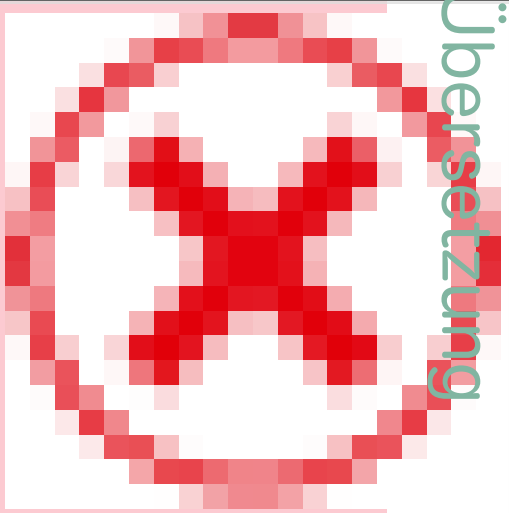
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Integrationen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

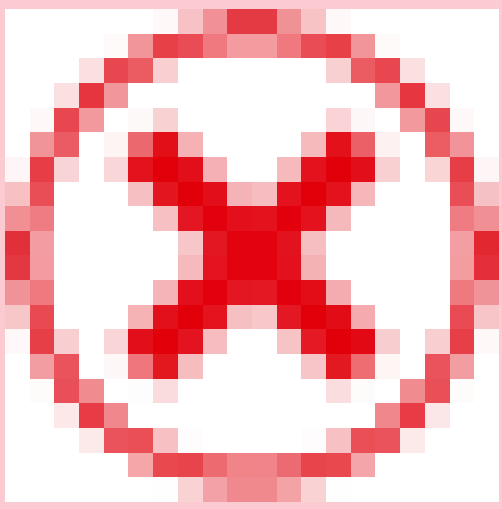
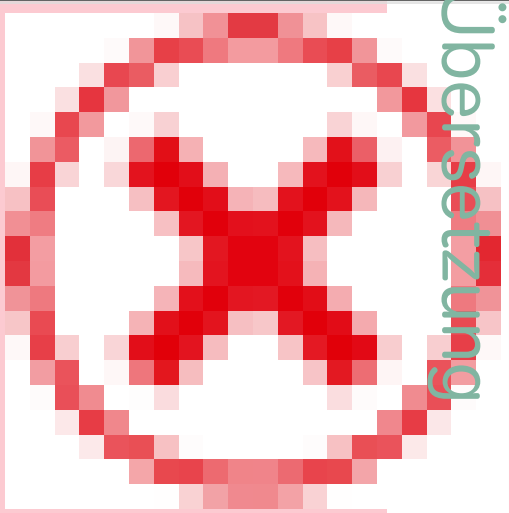
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
SLA-Definitionen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
SAM-NVD konfigurieren			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Normalisierte Schweregradzuordnungen	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

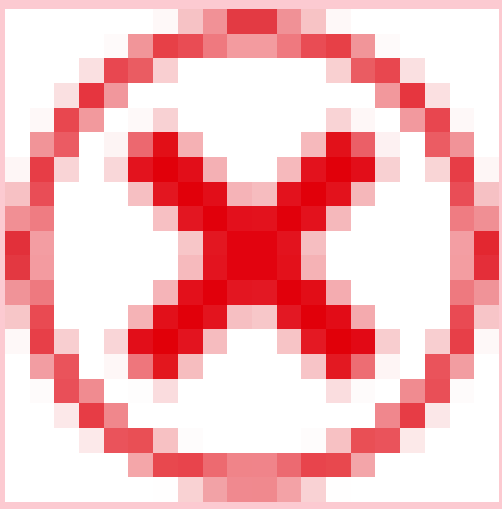
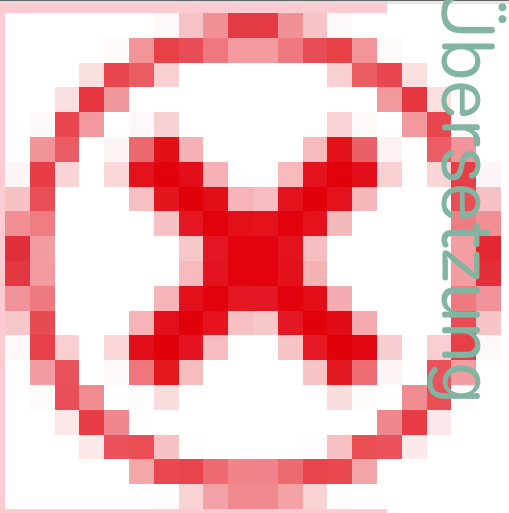
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Konfiguration der Scan-Abdeckung			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

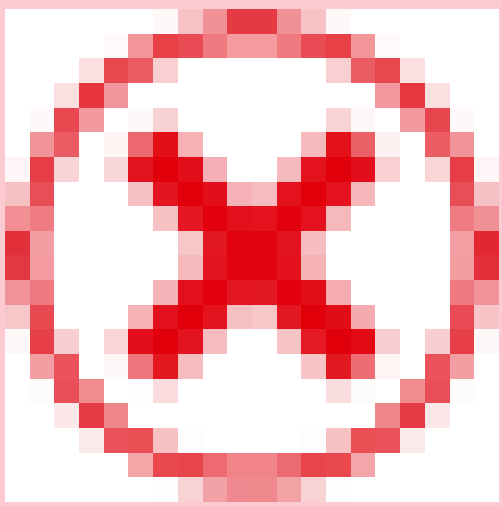
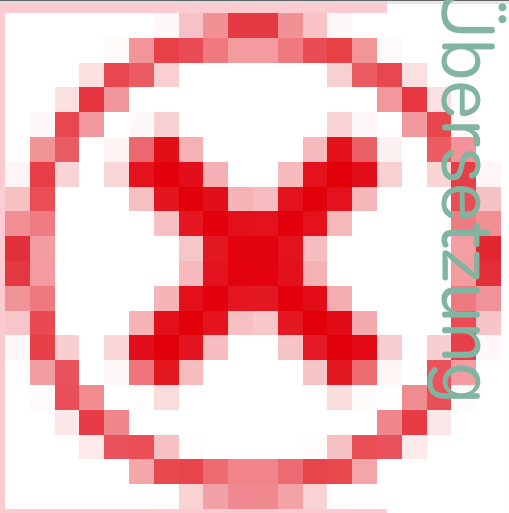
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Ausnahmenverwaltung			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

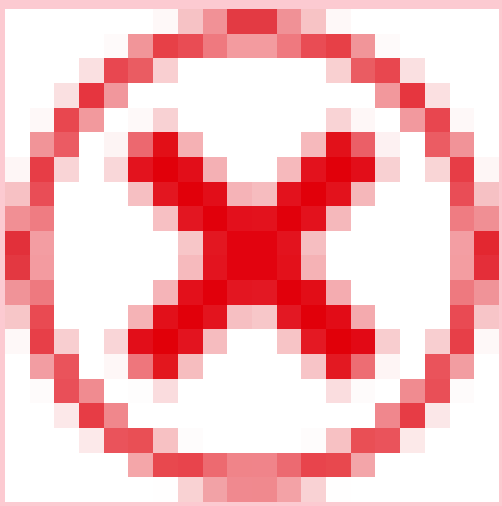
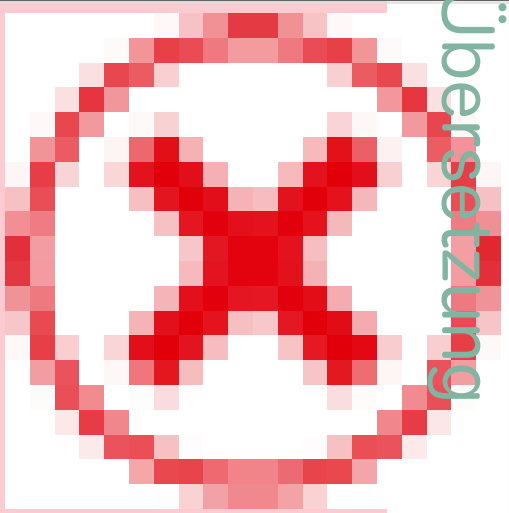
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Verwendungsbericht			
Diagnosen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Manage_Remediation_target_rules	sn_vul. Manage_Risk_Score_Configuration	sn_vu
Überprüfungen			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

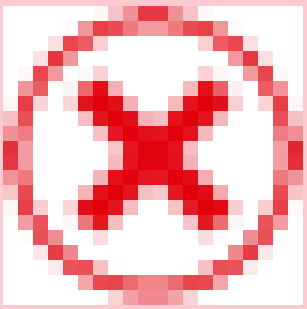
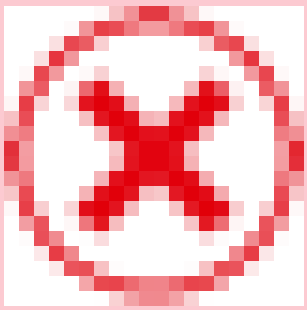
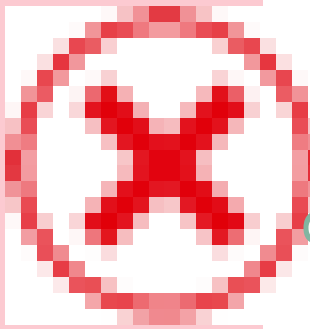
sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
(Haupt-App-Gruppe)				
CISO-Dashboard				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Korrekturübersicht	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Arbeitsbereich des Schwachstellenmanagers	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Übersicht	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Arbeitsbereich für IT-Korrekturen	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Genehmiger-Übersicht	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Übersicht	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Meine Genehmigungen	✗	✗	✗	
Korrekturaufgaben				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Aktiv	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Mir zugewiesen	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

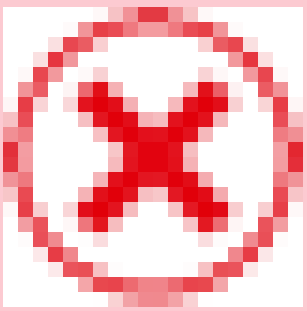
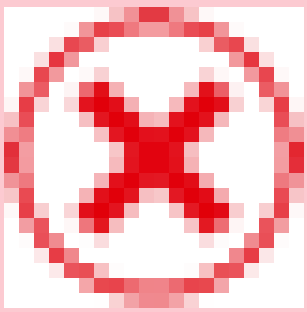
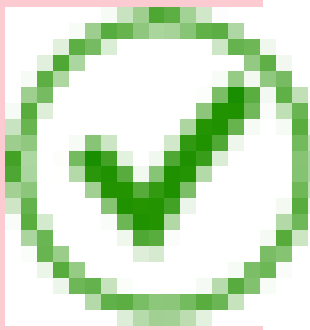
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Meinen Gruppen zugewiesen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Alle	✗	✗	✗	

Angreifbare Elemente

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Kritisches Risiko	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Hohes Risiko	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Nutzbar	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Ziel rückt näher	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Verfehltes Ziel	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Innerhalb der letzten 90 Tage	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Älter als 90 Tage	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Nicht zugewiesen	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Nicht gruppiert	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Außer Betrieb genommen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Mehrere Zurückstellungen	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Alle	✗	✗	✗	
Lösungen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Alle	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

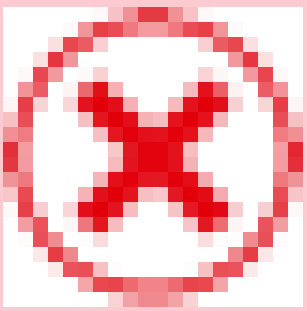
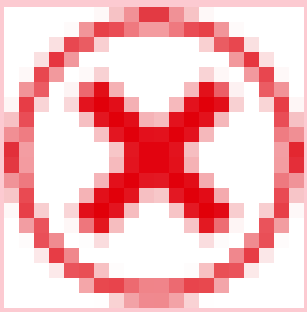
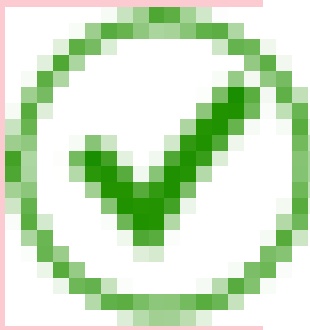
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Ersetzung mit höchster Priorität				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Mit angreifbaren Elementen	✗	✗	✗	
Bibliotheken				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
NVD	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
CWE	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Drittpartei	✗	✗	✓	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Software mit Schwachstellen	✗	✗	✗	
Schwachstellenscan				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Bewertung des Gefahrenpotenzials	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Scans	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Scanner	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

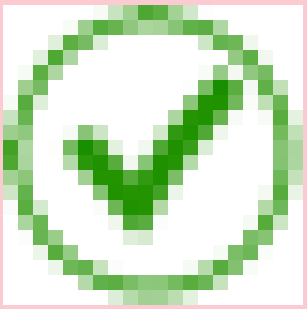
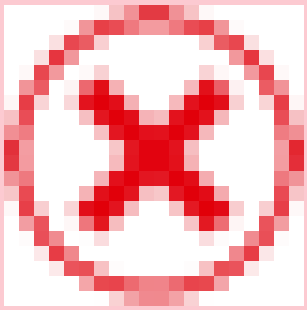
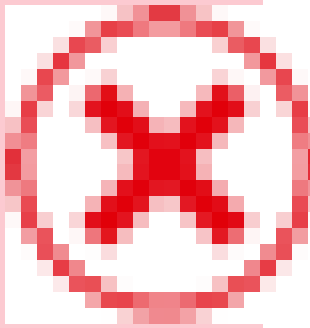
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Scan-Warteschlange				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Scannerquotengrenzen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Quotengrenzdefinitionen	✗	✗	✗	
Administration				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Setup-Assistent	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Überwachungsthemen	✗	✓	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Zuweisungsregeln	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Regeln für Korrekturaufgaben	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Zuweisungsempfehlungen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Schwachstellen-Rechner	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Rechner für Schwachstellen-Rollup	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Korrekturzielregeln	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Konfiguration automatisch schließen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Regeln für automatisches Löschen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Ausnahmeregeln	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Genehmigungsregeln	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Klassifizierungsregeln	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Leistungskonfiguration	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
VI-Granularität konfigurieren	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Benachrichtigungen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
E-Mail-Vorlagen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Warteschlange importieren	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Integrationen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
SLA-Definitionen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
SAM-NVD konfigurieren	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Normalisierte Schweregradzuordnungen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Konfiguration der Scan-Abdeckung	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Ausnahmenverwaltung	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Verwendungsbericht	✗	✗	✗	
Diagnosen				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

(Fortsetzung)

Modul	sn_vul. Read_Integrations	sn_vul. Read_watch_topic	sn_vul. Remediation_owner	sn_vul. Un
Überprüfungen	✗	✗	✗	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

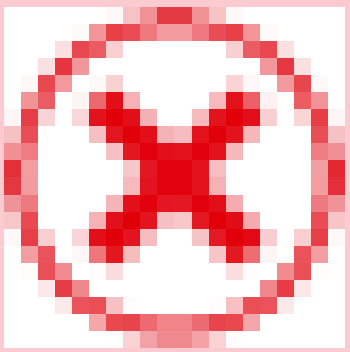
sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
(Haupt-App-Gruppe)		
CISO-Dashboard		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Korrekturübersicht	✓	✓
Arbeitsbereich des Schwachstellenmanagers	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

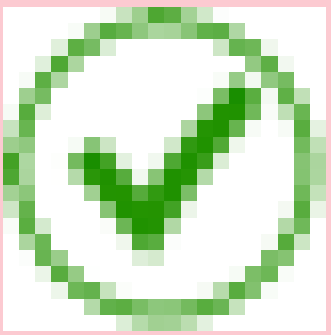
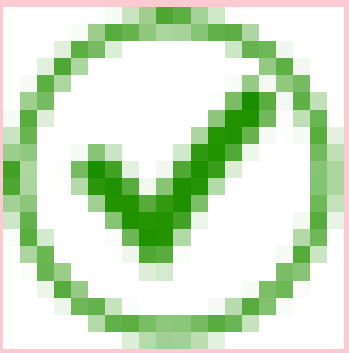
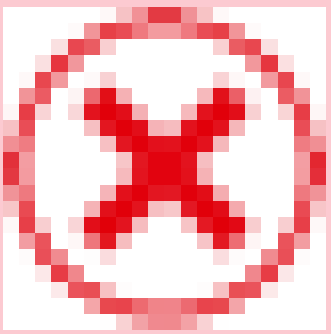
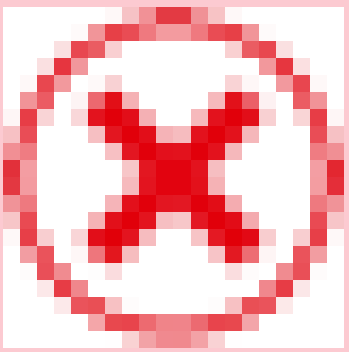
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Übersicht		
Arbeitsbereich für IT-Korrekturen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

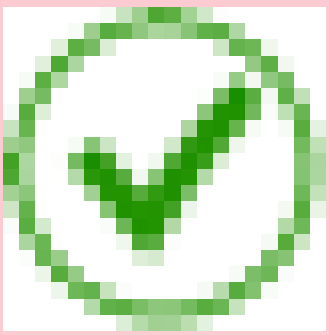
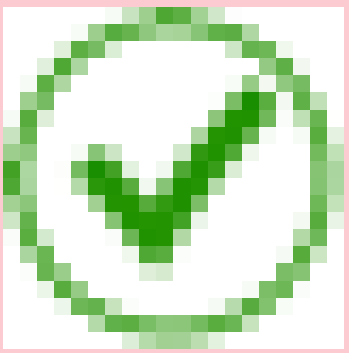
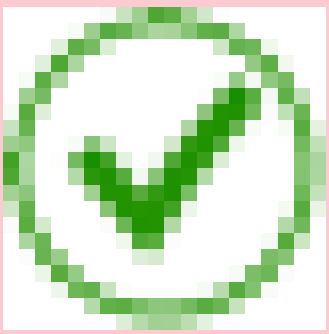
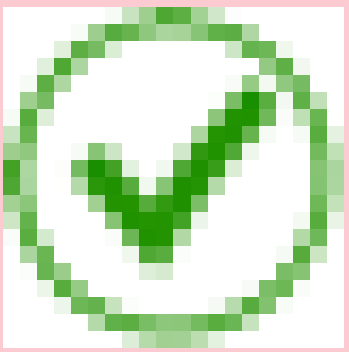
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Genehmiger-Übersicht		
Übersicht		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

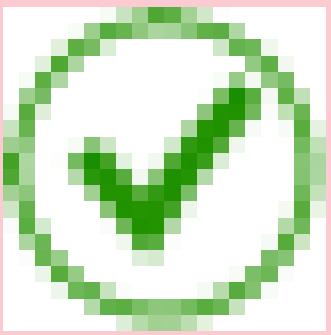
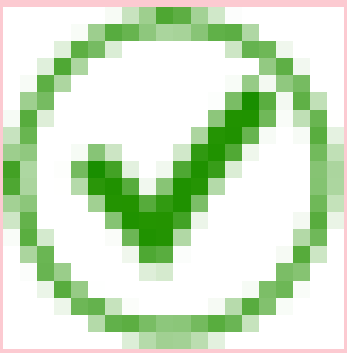
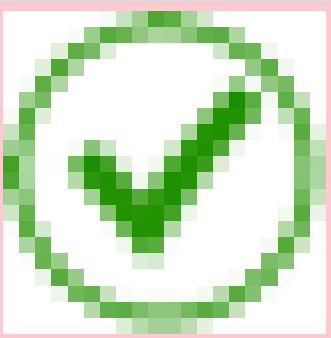
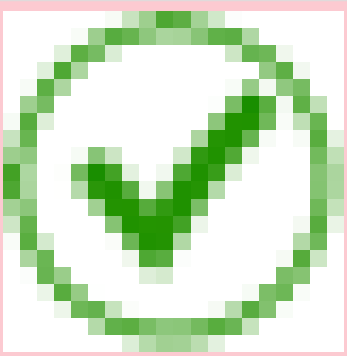
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Meine Genehmigungen		
Korrekturaufgaben		
Aktiv		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

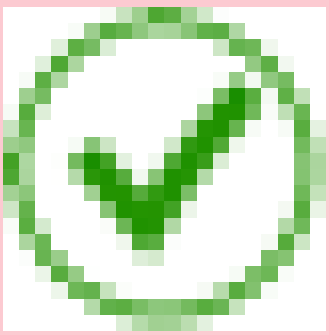
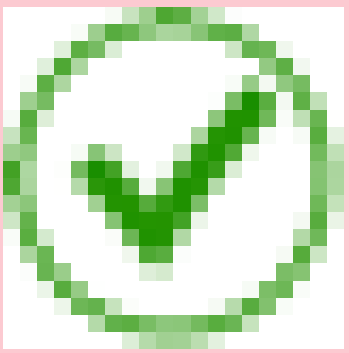
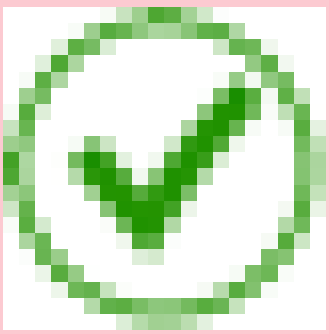
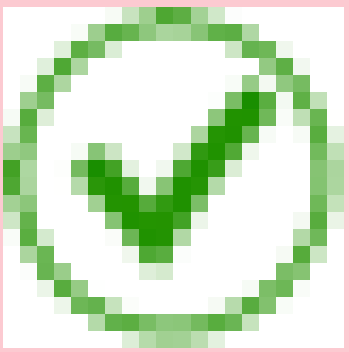
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Mir zugewiesen		
Meinen Gruppen zugewiesen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

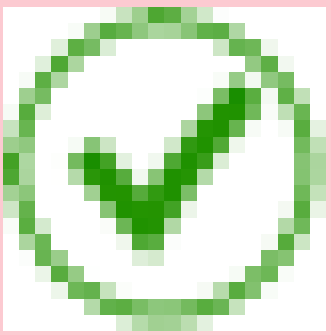
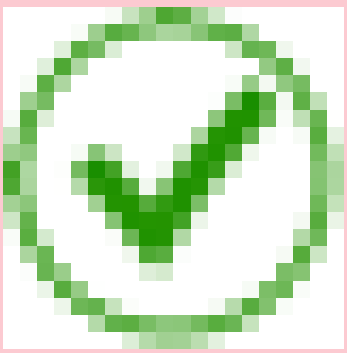
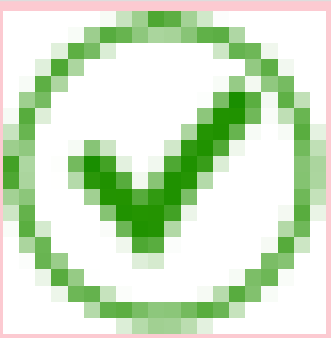
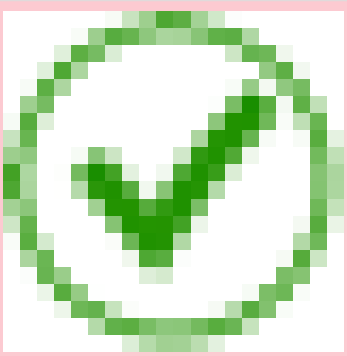
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Alle		
Angreifbare Elemente		
Kritisches Risiko		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Hohes Risiko	✓	✓
Nutzbar	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

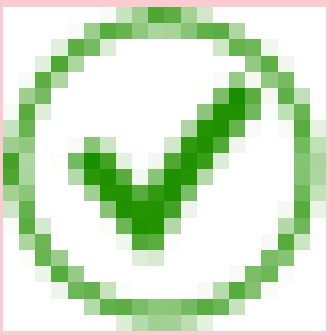
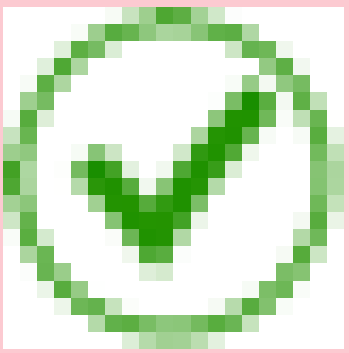
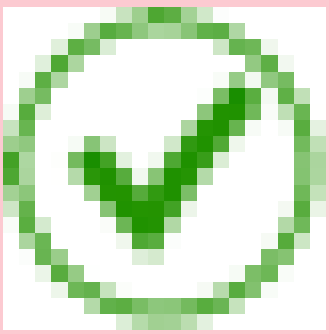
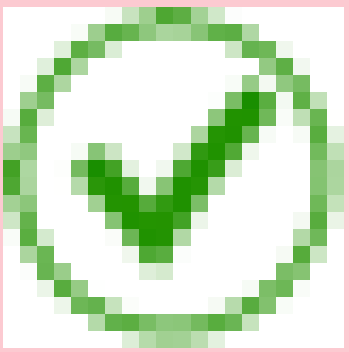
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Ziel rückt näher		
Verfehltes Ziel		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

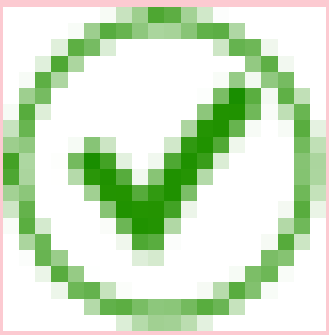
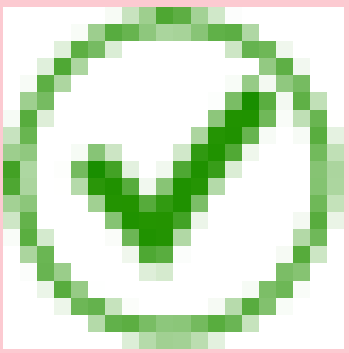
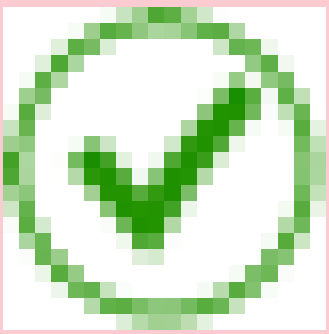
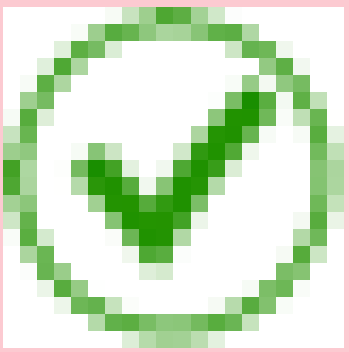
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Innerhalb der letzten 90 Tage		
Älter als 90 Tage		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

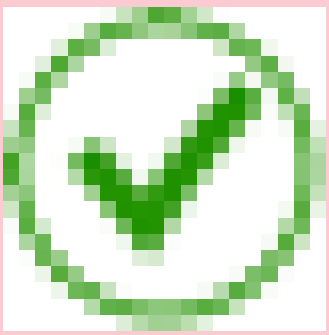
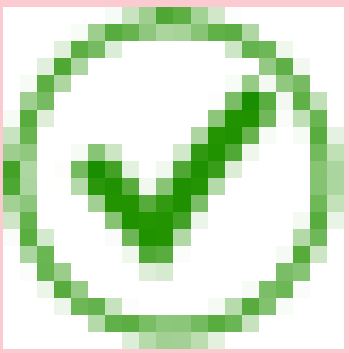
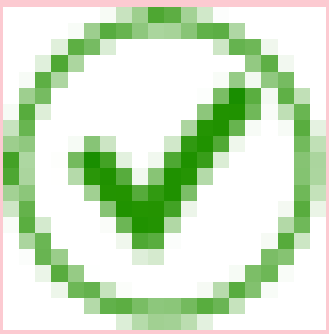
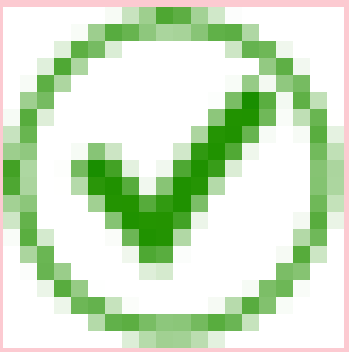
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Nicht zugewiesen		
Nicht gruppiert		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Außer Betrieb genommen	✓	✓
Mehrere Zurückstellungen	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

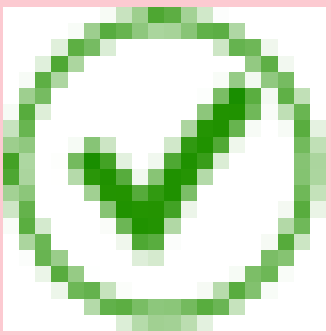
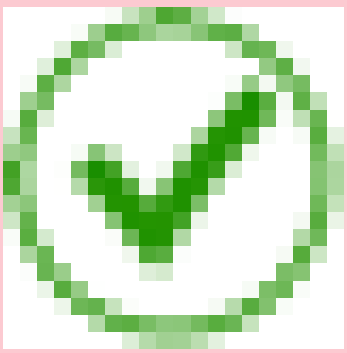
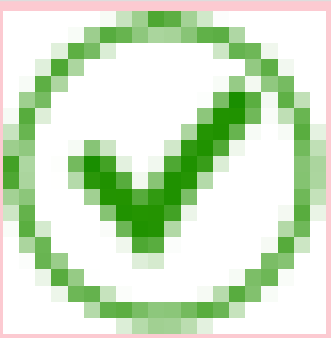
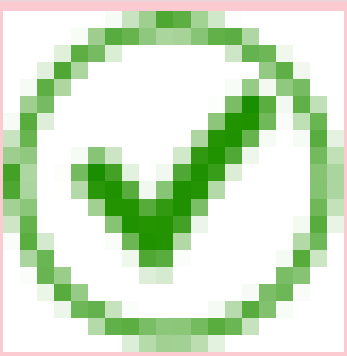
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Alle		
Lösungen		
Alle		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

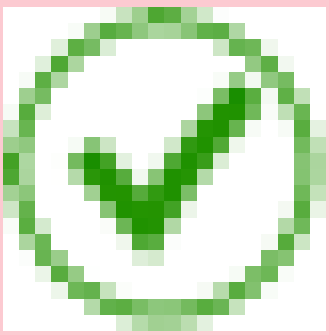
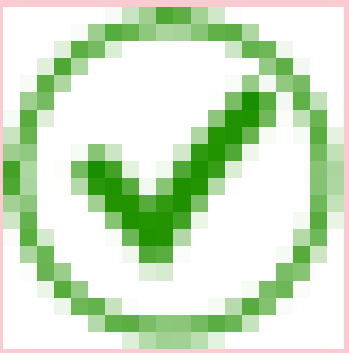
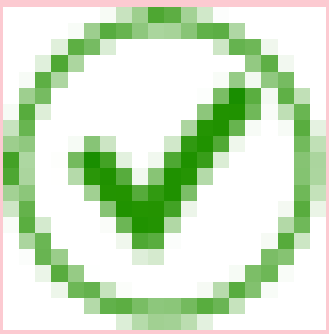
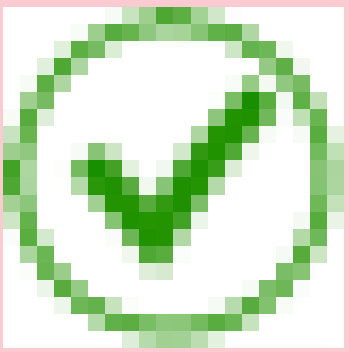
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Ersetzung mit höchster Priorität		
Mit angreifbaren Elementen		
Bibliotheken		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
NVD	✓	✓
CWE	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

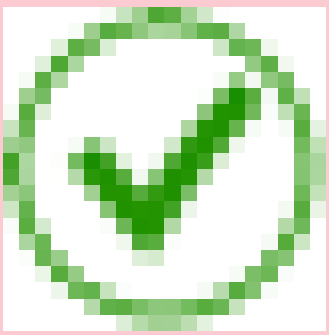
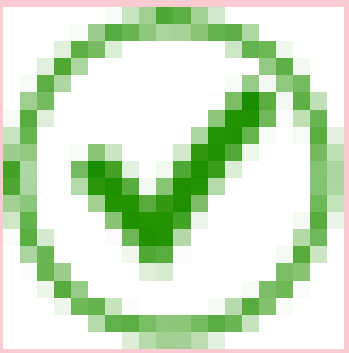
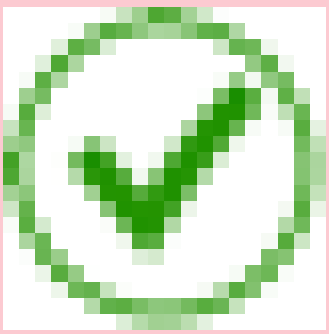
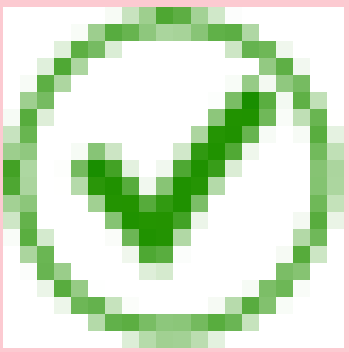
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Drittpartei		
Software mit Schwachstellen		
Schwachstellenscan		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

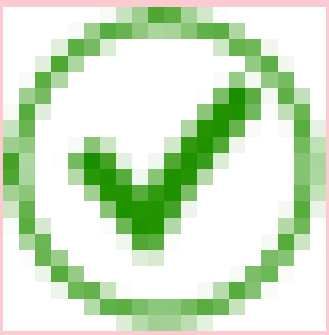
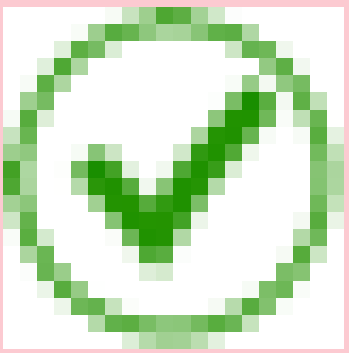
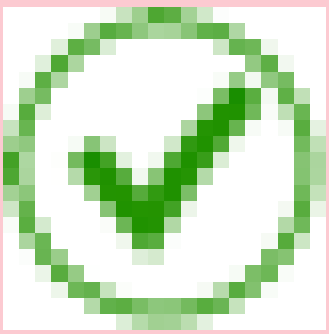
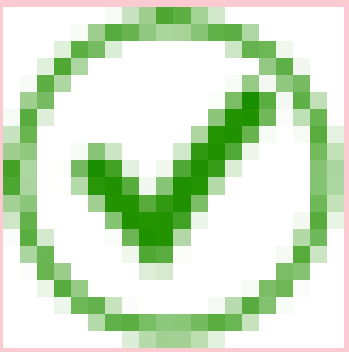
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Bewertung des Gefahrenpotenzials		
Scans		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Scanner	✓	✓
Scan-Warteschlange	✓	✓

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

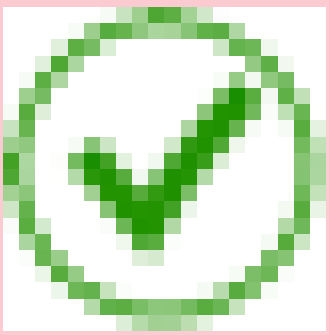
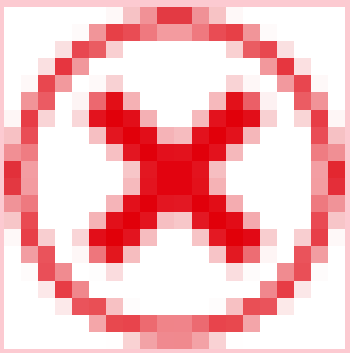
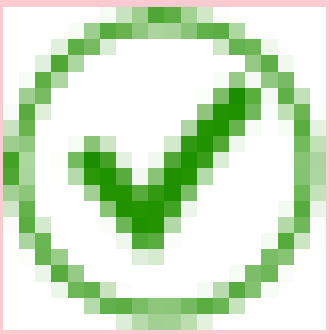
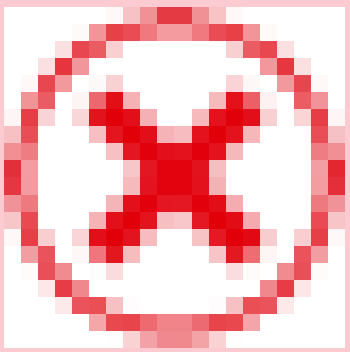
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Scannerquotengrenzen		
Quotengrenzdefinitionen		
Administration		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

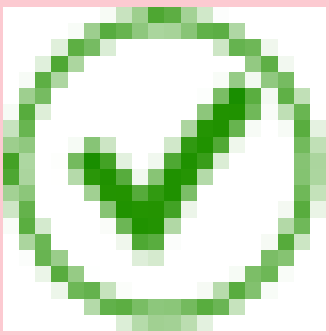
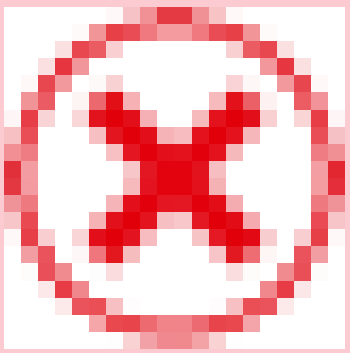
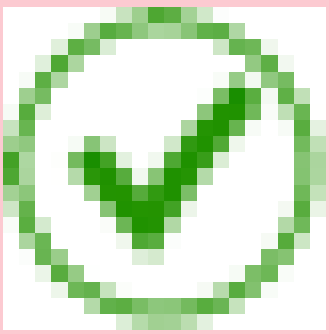
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Setup-Assistent		
Überwachungsthemen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

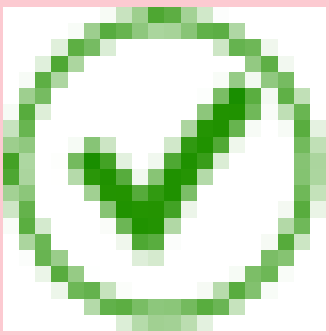
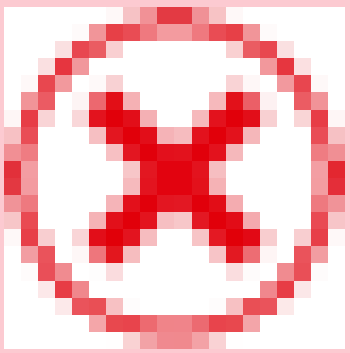
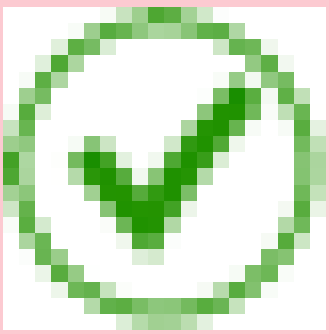
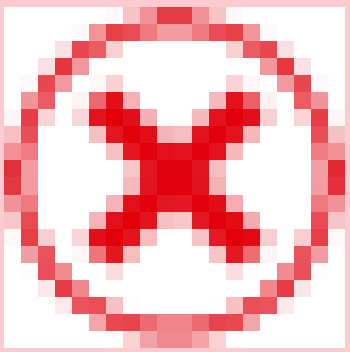
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Zuweisungsregeln		
Regeln für Korrekturaufgaben		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Zuweisungsempfehlungen	✗	✗
Schwachstellen-Rechner	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Rechner für Schwachstellen-Rollup	✓	✗
Korrekturzielregeln	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

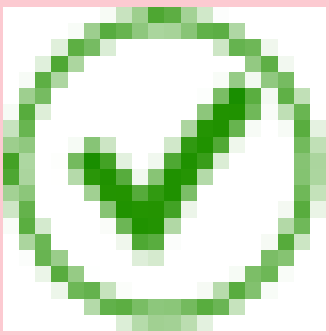
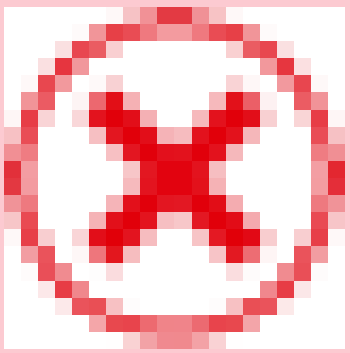
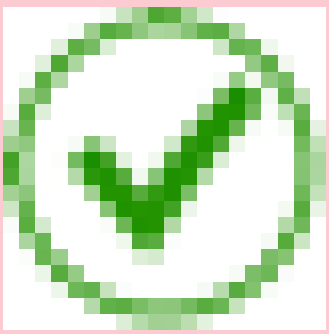
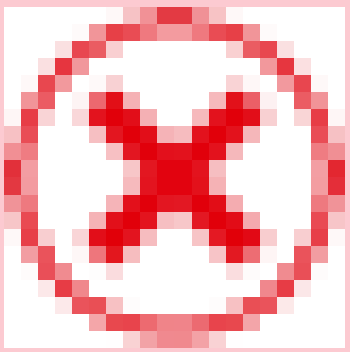
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Konfiguration automatisch schließen		
Regeln für automatisches Löschen		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

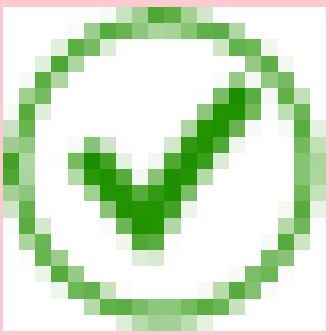
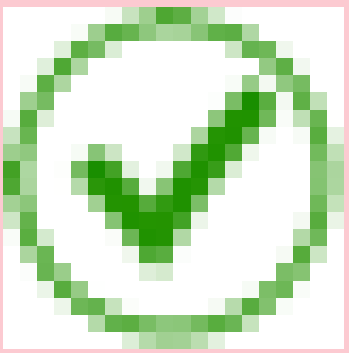
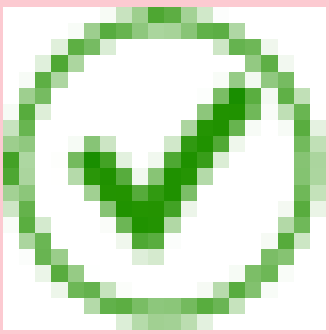
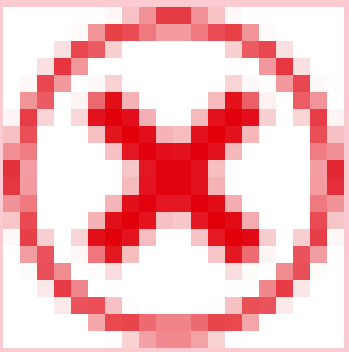
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Ausnahmeregeln		
Genehmigungsregeln		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Klassifizierungsregeln	✓	✗
Leistungskonfiguration	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

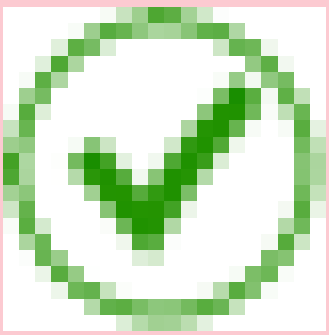
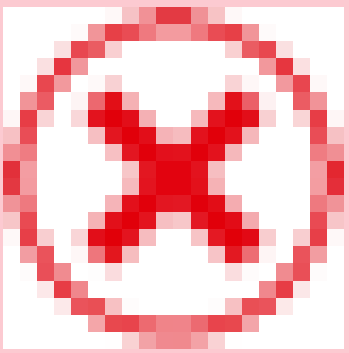
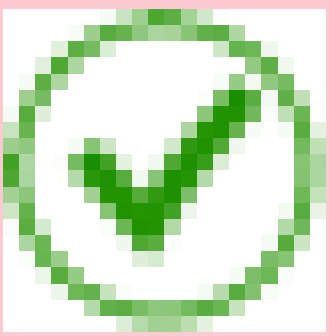
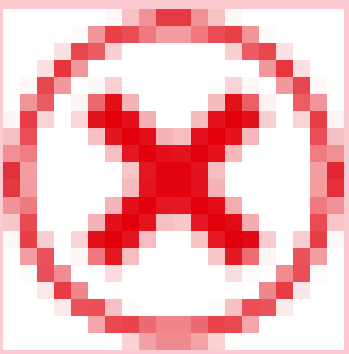
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
VI-Granularität konfigurieren		
Benachrichtigungen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

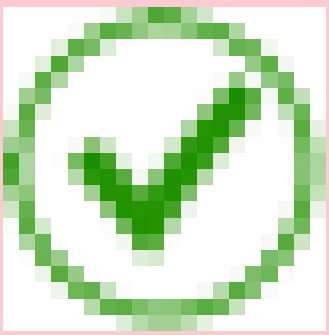
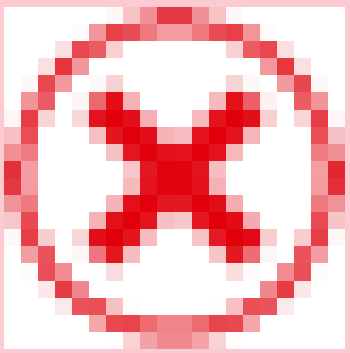
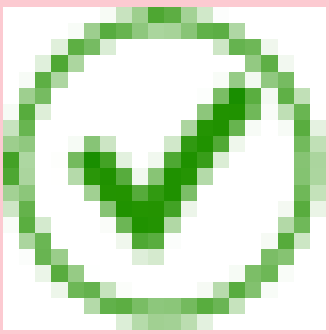
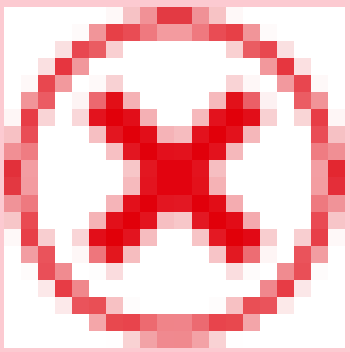
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
E-Mail-Vorlagen		
Warteschlange importieren		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

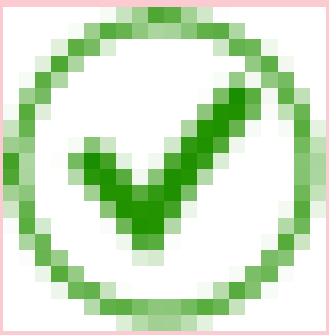
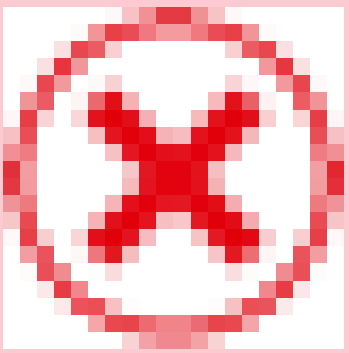
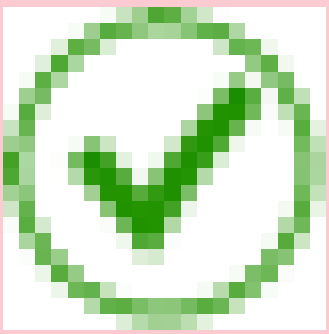
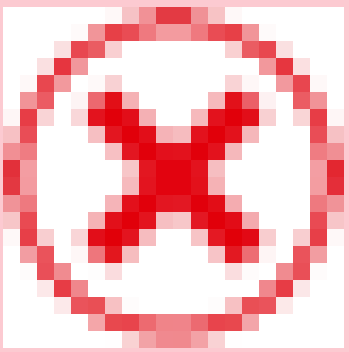
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Integrationen		
SLA-Definitionen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
SAM-NVD konfigurieren	✓	✗
Normalisierte Schweregradzuordnungen	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Konfiguration der Scan-Abdeckung	✓	✓
Ausnahmenverwaltung	✓	✗

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Modulzugriff für: sn_vul.Vulnerability_admin, sn_vul.Vulnerability_Analyst

Informationen für andere Rollen:

sn_sec_cmn.Manage_Approval_rules, sn_vul.Access_Setup_Assistant, sn_vul.ciso_read, sn_vul.configure_Integrations

sn_vul.configure_nvd_Integration, sn_vul.configure_Scan_Coverage_read, sn_vul.configure_VI_granularity, sn_vul.configure_vr_Performance

sn_vul.Exception_Approver, sn_vul.false_positive_Approver, sn_vul.Manage_assignment_Recom_config, sn_vul.Manage_assignment_rules

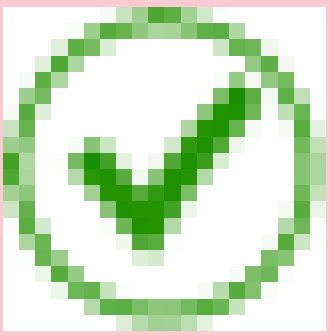
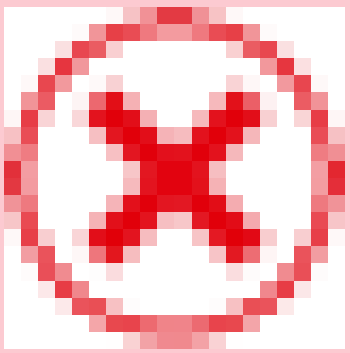
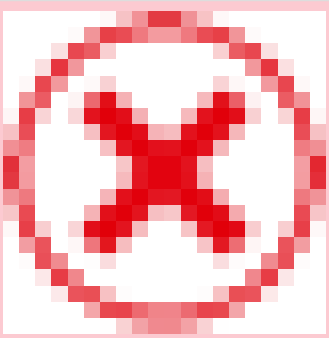
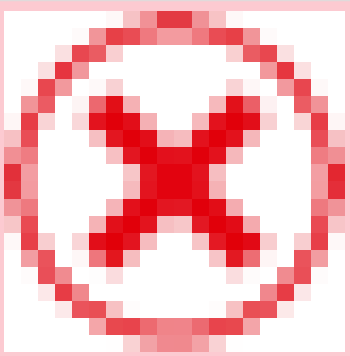
sn_vul.Manage_Auto_close_stale_VI, sn_vul.Manage_Auto_delete, sn_vul.Manage_classification_rules, sn_vul.Manage_Exception_Configuration

sn_vul.Manage_exposure_assessment, sn_vul.Manage_Group_rules, sn_vul.Manage_Notifications, sn_vul.Manage_permissions

sn_vul.Manage_Remediation_target_rules, sn_vul.Manage_Risk_Score_Configuration, sn_vul.read_all, sn_vul.read_assigned, sn_vul.read_Auto_Exception_rule

sn_vul.read_Integrations, sn_vul.read_watch_topic, sn_vul.Remediation_owner, sn_vul.unassign_Approver, sn_vul.View_Enterprise_Wide_stats

(Fortsetzung)

Modul	sn_vul. Vulnerability_admin	sn_vul. Vulnerability_Analyst
Verwendungsbericht		
Diagnosen		
Überprüfungen		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

[End]

Security Operations durchsuchen

Sie können Informationen schnell in jedem finden Security Operations Anwendung über das Suchsymbol im Bildschirm-Header. Zing ist die Textindizierungs- und Suchmaschine, die alle Textsuchen in Ihrer Instanz durchführt.

Vorbereitungen

Erforderliche Rolle: sn_si.read oder höher

Prozedur

1. Klicken Sie auf das Suchsymbol ( ) In der oberen rechten Ecke des Bildschirms.
2. Geben Sie die Kriterien ein, nach denen Sie suchen möchten, und drücken Sie **Geben Sie Ein** .
   Wenn Sie haben Security Incident Response Plugin aktiviert. Die von Ihnen eingegebenen Suchkriterien enthalten übereinstimmende Kurzbeschreibungstexte, CIs, IP-Adressen oder URLs in Ihren Security Incidents. Security Incident Response Aufgaben oder Sicherheitsanforderungen. Wenn Sie haben Vulnerability Response Oder Threat Intelligence Plugins aktiviert. Die Suchergebnisse umfassen Schwachstellen, angreifbare Elemente, Einträge angreifbarer Elemente, erkennbare Elemente, IoCs, und Angriffsmodus/-Methoden.

Zugehörige Informationen

Einführung in die Suche

Zing-Textsuche

Referenzen zur Integration mit Security Operations

Entwickler und ServiceNow-Partner können die Informationen in diesem Abschnitt verwenden, um ein Verständnis der unterirdischen Funktionalität von Drittpartei-Integrationen zu erhalten, einschließlich Entwicklungsrichtlinien, Integrationsfähigkeiten und Workflows.

ServiceNow Security Operations Richtlinien für die Integrationsentwicklung

Die ServiceNow Die Plattform bietet mehrere Mechanismen für die Entwicklung von Integrationen mit externen Systemen. Die ServiceNow Security Operations Die Produktsuite fügt Integrationsfunktionen hinzu, die den Prozess der Integration mit sicherheitsorientierten externen Systemen optimieren sollen.

Die meisten Konzepte in diesem Leitfaden gehen von einer gewissen Vertrautheit mit dem Standard aus ServiceNow Funktionalität. Zur Integration mit Security Operations suite mindestens Kenntnisse über Folgendes ServiceNow Konzepte sind erforderlich:

- Skripteinbindungen
- Eingehende/ausgehende Webservices
- Datenquellen
- Importsätze
- Transformationszuordnungen

Technologie-Partnerprogramm

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Anforderungen für die Anwendungszertifizierung oder Richtlinien in der Literatur zum Technologiepartnerprogramm ersetzen alle Informationen in diesem Leitfaden. Dieser Leitfaden ist kein Ersatz für die Literatur zum Technologie-Partnerprogramm und dient nur als Ergänzung zur vorhandenen Dokumentation.

Weitere Informationen finden Sie unter Blog-Post zum Schulungskurs des Technologiepartnerprogramms .

Typen von ServiceNow Integrationen bereitgestellt

Die Security Operations Anwendungen (Security Incident Response, Threat Intelligence, Und Vulnerability Response) Kann nahtlos in andere integriert werden ServiceNow Anwendungen zur Verbesserung ihrer Funktionalität.

Die folgenden Integrationen werden in bereitgestellt Security Operations Basissystem.

Security Incident Response: Integration des Ereignismanagements

Die Fähigkeiten von Ereignismanagement Anwendung wurde auf Support erweitert Security Incident Response. Die Security Incident Response Ereignismanagement Das Support-Plugin analysiert automatisch den Inhalt von Ereignissen in Ereignismanagement Zum Ausfüllen von Feldern in Security Incidents.

Abgedeckter Anwendungsfall:

Erstellung von Sicherheitsereignissen in Ereignismanagement System aus Sicherheitsinformationen und Ereignismanagement(SIEM)-Tools

Nützliche Fähigkeiten bereitgestellt:

- Ereignismanagement-Funktionalität: Ereigniskorrelation, Ereignisregeln und Warnungsregeln
- Automatische Zuordnung von Additional_Information-Werten zu resultierendem Security Incident

Ressourcen:

Dokumentation zur Unterstützung des Security Incident-Ereignismanagements

Ereignismanagement-Dokumentation

Security Incident Response: Integration der Importsatz-API

Zusätzlich zur Verwendung Ereignismanagement Um sicherheitsbezogene Ereignisse zu veröffentlichen, die Security Incident Response Die Anwendung stellt eine Importsatz-API bereit, die die direkte Erstellung von Security Incidents ermöglicht. Der REST-Endpunkt für den Security Incident-Importsatz ist http://localhost:8080/api/now/import/sn_si_incident_import.

Diese Integrationstechnik ist nützlich, wenn a) Ereignismanagement Ist nicht installiert, oder b) es ist wünschenswert, einfach Security Incidents zu erstellen, ohne den Flow „Ereignis > Warnung > Security Incident“ durchlaufen zu müssen, der bei Verwendung erforderlich ist Ereignismanagement.

Abgedeckter Anwendungsfall:

Erstellung von Security Incidents direkt aus SIEM-Tools.

Nützliche Fähigkeiten bereitgestellt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatischer CI-Abgleich bei Erstellung von Security Incidents basierend auf IP, NetBIOS oder vollqualifiziertem Domänennamen.

Ressourcen:

Dokumentation zur Plattform-Importsatz-API

Security Incident Webservice-Importsatz-Dokumentation

Threat Intelligence: Integration der Suchquelle

Suchquellen bieten die Möglichkeit, Daten an externe Suchquellen zu senden, um festzustellen, ob diese Daten schädlich sind. Im Allgemeinen handelt es sich bei diesen Daten um eine IP-Adresse, URL, Datei oder Datei-Hash.

Abgedeckter Anwendungsfall:

Suchen Sie mit einem externen Suchservice nach einer IP-Adresse, URL, Datei oder Hash.

Nützliche Fähigkeiten bereitgestellt:

- Konsistente Methode zum anfordern von Suchen nach Katalogelementen und Security Incidents.
- Ratenbegrenzungs- und Drosselungsfähigkeiten mit wenig/keiner Codierung bereitgestellt.
- Automatische Erstellung von Einträgen erkennbarer Elemente (Indicators of Commission, IOC) für alle Probleme, die von Suchquellen gefunden werden.

Threat Intelligence: Integration der Bedrohungsquelle

Bedrohungsquellen bieten die Möglichkeit, Daten aus externen Threat Intelligence-Repositorys abzurufen. Diese Daten werden dann in die verschiedenen Indikatoren von Kompromisstabellen importiert, die im System vorhanden sind. TAXII-Sammlungen und einfache Blocklisten werden nativ unterstützt. Um neue TAXII-Sammlungen (oder Profile basierend auf einer Discovery oder einem Sammlungsverwaltungsservice) hinzuzufügen, müssen Sie einfach einen Eintrag hinzufügen. Ebenso besteht das Hinzufügen einer neuen einfachen einspaltigen Blockliste darin, einen neuen Datensatz einzugeben und die URL der Blockliste anzugeben. Für kompliziertere Datensätze kann eine anwenderdefinierte Integration bereitgestellt werden, um eine URL aufzurufen und die Antwort zu analysieren.

Abgedeckter Anwendungsfall:

Ruft Daten aus einer Threat Intelligence-Quelle ab, um sie in IOC-Tabellen zu laden.

Nützliche Fähigkeiten bereitgestellt:

- Unterstützung für einfache Blocklisten und TAXII-Sammlungen ohne Codierung.
- Einfacher Mechanismus zum Ausführen von REST-Nachrichten zum Abrufen von Daten.
- Entkoppelter Datenabruf/-Verarbeitung für Wiederverwendbarkeit der Integrationskomponente.
- Native Unterstützung für die Verarbeitung der Übergabe von Daten, die an Datenquellen (und Importsätze/Transformationszuordnungen) zurückgegeben werden.
- Unterstützt mehrere Datenanforderungen pro Integration (für paginierte Anrufe) mit der Möglichkeit, Kontext an nachfolgende Anrufe zu übergeben

Ressourcen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie eine Bedrohungsquelle

Vulnerability Response: Integration des Scanneraufrufs

Der Aufruf von Schwachstellen-Scannern ist ein leichter Integrationseinstiegspunkt, der das Aufrufen von Schwachstellen-Scans aus der Instanz unterstützt. Ein Schwachstellen-Scanner von Drittanbietern wird asynchron aufgerufen, um einen Scan nach Konfigurationselementen oder IP-Adressen zu planen.

Abgedeckter Anwendungsfall:

Anforderung an einen Drittpartei-Scanner senden, um ein CI (mithilfe von Host-Informationen, die von CI abgeleitet wurden) oder eine IP-Adresse/IP-Adressen zu scannen.

Nützliche Fähigkeiten bereitgestellt:

- Einfaches Framework zum Definieren von Scanner-Implementierungen.
- Konsistente Möglichkeit, Scans von Katalogelementen, Security Incidents und angreifbaren Elementen anzufordern.
- Automatische Aktualisierung von Aufgaben mit Ergebnis des Scan-Aufrufs.

Vulnerability Response: Datenintegration

Integrationen von Schwachstellendaten dienen dazu, Schwachstellendaten aus Schwachstellensystemen von Drittanbietern abzurufen. Die erwarteten Ausgaben dieser Integrationen sind Schwachstelleneinträge und angreifbare Elemente. Diese Integration ermöglicht es Drittanbieter-Schwachstellen-Scannern, unabhängig zu funktionieren, mit der Erwartung, dass Schwachstellen innerhalb der Instanz bearbeitet und nachverfolgt werden können.

Abgedeckte Anwendungsfälle:

- Rufen Sie Schwachstellen-Bibliotheken ab
- Rufen Sie Schwachstellen-/CI-Paarungen ab
- Synchronisieren Sie CIs mit dem Schwachstellen-Management-System

Nützliche Fähigkeiten bereitgestellt:

- Entkoppelter Datenabruf/-Verarbeitung für Wiederverwendbarkeit der Integrationskomponente.
- Native Unterstützung für die Verarbeitung der Übergabe von Daten, die an Datenquellen (und Importsätze/Transformationszuordnungen) zurückgegeben werden.
- Unterstützt mehrere Datenanforderungen pro Integration (für paginierte Anrufe) mit der Möglichkeit, Kontext an nachfolgende Anrufe zu übergeben.

Ressourcen:

Dokumentation zur Integration von Schwachstellendaten

Security Operations Integrationskonfigurationen

Viele der im Basissystem enthaltenen Integrationen erfordern wenig oder kein Setup und funktionieren auf dieselbe Weise. Bestimmte Integrationen, z. B. Qualys Cloud Platform, Erfordern jedoch separate Schritte zum Einrichten der Integration. Andere unterstützen verschiedene Sätze von Scan- und Suchtypen und verschiedene Quotengrenzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Abschnitt werden die Unterschiede zwischen den unterstützten Integrationen beschrieben und Sie nach Bedarf auf weitere Dokumentation verwiesen.

- Integration mit Carbon Black: Ermöglicht es Ihnen, Security Incidents zu untersuchen und darauf zu reagieren, indem Sie die Carbon Black APIs verwenden, um Endpunkte abzufragen und mit diesen zu interagieren, die Security Incidents zugeordnet sind.
- Integration mit Check Point Anti-Bot - Email Parser: Verwendet einen E-Mail-Parser, der E-Mail-Benachrichtigungen vom Check Point Anti-Bot verwendet, um Security Incidents zu erstellen.
- Elasticsearch – Incident-Anreicherung – Integration: Durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- Have I Been Pwned?-Integration: Ermöglicht das schnelle Durchsuchen der Liste der Accounts mit Verstößen (E-Mail-Adressen und Anwendernamen) über einen RESTful-Service.
- HPE Security ArcSight ESM – E-Mail-Parser-Integration: Verwendet einen E-Mail-Parser, der E-Mail-Benachrichtigungen von HPE ArcSight ESM verwendet, um Security Incidents zu erstellen.
- HPE ArcSight Logger – Integration der Incident-Anreicherung: Durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- IBM QRadar – Integration der Incident-Anreicherung: Durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- McAfee ESM: E-Mail-Parser-Integration: Verwendet einen E-Mail-Parser, der E-Mail-Benachrichtigungen von McAfee ESM verwendet, um Security Incidents zu erstellen.
- McAfee ESM: Incident-Anreicherungsintegration: Durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- Integrationsüberblick OPSWAT Metadefender: Ermöglicht das Herunterladen von Bedrohungsdaten, die vom Metadefender-Scanner der Drittpartei erkannt wurden, in den Threat Intelligence Anwendung für Nachverfolgung, Priorisierung und Lösung.
- Palo Alto Networks – AutoFocus-Integration: Der Palo Alto Networks-Autofokus, ein Threat Intelligence-Cloud-Service, ermöglicht Ihnen die Suche nach Sitzungsinformationen im Zusammenhang mit erkennbaren Security Incident-Elementen.
- Palo Alto Networks – Firewall-Integration: Mit der Palo Alto Networks-Firewall können Sie Firewalls einrichten und verwalten, um bekannte und unbekannte Bedrohungen im Netzwerk, in der Cloud und in Endpunkten zu verhindern.
- Palo Alto Networks – WildFire-Integration: Mit der Wildfire-Integration können Sie Analyseaufträge in Wildfire programmgesteuert abfragen und historische Ergebnisse über eine einfache XML-API-Schnittstelle abrufen.
- Qualys Vulnerability Integration verstehen: Qualys Cloud Platform Wird in verwendet Vulnerability Response.
- Integration mit Splunk - Incident Enrichment: Durchsucht Ihre Protokolle und fügt Ihren Security Incidents relevante Sichtungsinformationen hinzu.
- Integration mit VirusTotal: Verwendet in Threat Intelligence. Um diese Suchquelle zu verwenden, müssen Sie Aktivieren Sie das Plugin VirusTotal Integration .
- Setup der WhoisXML-API-Integration: Stellt konsistente, gut strukturierte Daten aus einer Whois-Suche bereit. Hält genaue Whois-Daten rund um die Uhr zugänglich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren und konfigurieren Sie Drittpartei-Integrationen

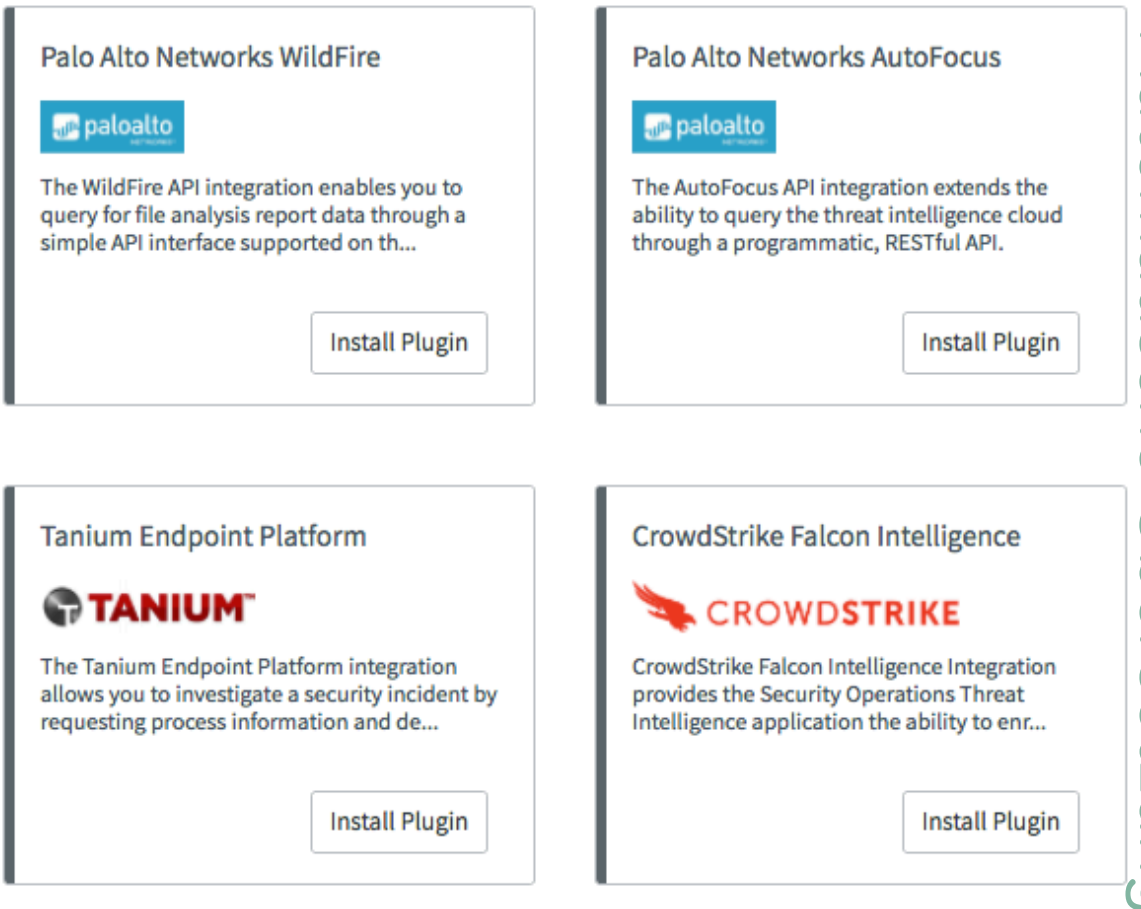
Sie können die Plugins für Integrationen von Drittparteien aktivieren und sie für die Verwendung über denselben Bildschirm konfigurieren.

Vorbereitungen

Erforderliche Rolle: sn_sec_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationskonfiguration**an.
   Die verfügbaren Sicherheitsintegrationen werden als eine Reihe von Karten angezeigt, ähnlich der folgenden Kartengruppe. Sie können auf eine beliebige Karte verweisen, um eine Beschreibung der Integration zu erhalten.



2. Klicken Sie auf , um das Plugin für eine bestimmte Integration zu installieren **Installieren Sie Das Plugin** .

   a. Überprüfen Sie im Formular System-Plugin die Plugin-Details, und klicken Sie auf **Aktivieren/ Upgrade Durchführen** Zugehöriger Link.

   b. Klicken Sie auf **Aktivieren**.
   Wenn die Aktivierung abgeschlossen ist, wird der Bildschirm „Sicherheitsintegration“ erneut geöffnet, und die Schaltfläche für die von Ihnen aktivierte Integration wird mit gekennzeichnet **Konfigurieren** .

3. Klicken Sie auf **Konfigurieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn Sie konfigurieren Qualys Vulnerability Integration, Siehe Installation von Vulnerability Response Und unterstützte Anwendungen.

4. Geben Sie ein **API-Schlüssel** .
5. Klicken Sie auf **Absenden**.

Erstellen Sie eine Integration

Sie können eine Integration erstellen und die zugehörige Integrationskarte dem Bildschirm „Sicherheitsintegrationen“ hinzufügen. Dieses Verfahren ist für Partner vorgesehen, die Drittpartei-Integrationen erstellen.

Vorbereitungen
Erforderliche Rolle: sn_sec_cmn.admin

Zielgruppe: Partner, die Drittpartei-Integrationen erstellen.

Prozedur

1. Geben Sie im Navigationsfilter sn_sec_Core_Integration_item.list ein, und drücken Sie **Geben Sie Ein** Schlüssel.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

Feld	Beschreibung
Name	Der Name der Integration.
Plugin-ID	Das Plugin, das aktiviert werden muss, um die Integration zu verwenden.
Reihenfolge	Gibt die Reihenfolge an, in der diese Integrationskarte angezeigt wird.
Bannertext	Klicken Sie auf den Link, wählen Sie ein Bild oder ein Logo aus, das auf der Integrationskarte angezeigt werden soll, und klicken Sie auf **OK** .
Installiert	Schreibgeschütztes Feld, das angibt, ob das Plugin bereits installiert wurde.
Konfigurierbar	Gibt an, ob Sie die Integration konfigurieren können.
Kategorien	Wird zum Filtern der Integrationskarten verwendet.
Kurzbeschreibung	Eine Beschreibung der Integration, die im Tooltip-Tipp für die Karte angezeigt wird.
Beschreibung	Eine längere Beschreibung der Integration.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die **Integration und Konfigurationen** Zugehörige Liste wird angezeigt. Sie können diese zugehörige Liste verwenden, um Konfigurationsoptionen für die Integration zu definieren. Diese Optionen werden angezeigt, wenn Sie auf klicken **Konfiguration** Schaltfläche auf der zugehörigen Integrationskarte.
5. Klicken Sie auf **Neu**.
6. Füllen Sie die entsprechenden Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Bezeichnung	Der Name des Integrationselements.
Name	Das Plugin, das aktiviert werden muss, um die Integration zu verwenden.
Integration	Zeigt die Integration an, für die Sie Integrationselemente definieren
Reihenfolge	Gibt die Reihenfolge an, in der dieses Integrationselement angezeigt wird.
Typ	Wählen Sie in der Liste den Typ des Felds aus: ○ Zeichenfolge ○ Ganzzahl ○ Dezimal ○ Datum ○ Boolean ○ Passwort ○ IPv4 ○ IPv6 ○ URL
Wert	Geben Sie den Wert ein, der dem zugeordnet ist **Typ** Ausgewählt. Wenn ein Wert für den ausgewählten ungültig ist **Typ** Wird eingegeben, werden keine Datensätze abgerufen, wenn die Integration ausgeführt wird. Wenn Sie beispielsweise den URL-Typ auswählen und einen Wert von 12.32.23.10 eingeben, werden keine Datensätze abgerufen.

7. Klicken Sie auf **Absenden**.

Tipps zum Schreiben von Integrationen

Vermeiden Sie einige der Fallstricke, die Sie beim Schreiben Ihrer eigenen Integrationen sehen können, indem Sie diese Richtlinien befolgen.

Verwenden Sie nach Möglichkeit die Funktionalität der ServiceNow-Plattform

Hauptsächlich die in integrierten Integrationsfunktionen Security Operations Anwendungen (Security Incident Response, Threat Intelligence, Und Vulnerability Response) Dienen dazu, vorhandene zu verbessern oder zu optimieren ServiceNow Plattformintegrationsfunktion. Achten Sie beim Schreiben von Integrationen immer darauf, die Plattformfunktionalität zu verwenden, wenn sie vorhanden ist. Hier sind einige gängige ServiceNow Funktionalitäten, die anstelle von „Rolling-your-own“ verwendet werden können.

- Ausgehende Webservices: Bei den meisten Interaktionen mit Systemen von Drittparteien erfolgt die Kommunikation über Webservices. Verwenden Sie in diesen Fällen ausgehende Webservices der Plattform (REST und SOAP werden unterstützt).
- Eine Datenquellen-/Importsätze-/Transformationszuordnung – zum Verarbeiten von Daten und zum Einfügen in ServiceNow Tabellen, der bevorzugte Mechanismus ist die Verwendung von Datenquellen und zugehörigen Komponenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie nach Möglichkeit Security Operations-Integrations-Frameworks

Weil Security Operations Integrationsmechanismen haben viele häufige Probleme gelöst. Grundlegende Funktionen müssen nicht für jede Integration neu eingeführt werden. Beispielsweise unterstützen die Frameworks für Schwachstellendaten und Bedrohungsquellen die Verarbeitung mehrerer Seiten und die Weitergabe dieser Daten an Datenquellen/Transformationen/Importsätze. Ebenso bietet das Quell-Framework für Scan- oder Suchvorgänge konfigurierbare Ratenbegrenzungsfunktionen. Überprüfen Sie bei der Implementierung einer Funktion oder einer Reihe von Funktionen in der Regel, ob vorhanden ist Security Operations Das Integrations-Framework deckt Ihren Anwendungsfall ab. Wenn ja, verwenden Sie dieses Framework.

Erweitern Sie die vorhandenen Security Operations-Integrations-Frameworks nach Bedarf

Die meisten von verwendeten Tabellen und Skripts Security Operations Integrations-Frameworks sollten erweitert werden, um zukünftige Anforderungen zu erfüllen. Wenn beim Schreiben einer Integration ein Anwendungsfall auftritt, erweitern Sie eine Integrationstabelle oder ein -Skript, um diesen Anwendungsfall besser anzupassen.

Geben Sie ServiceNow Feedback zu Problemen, die während der Integration aufgetreten sind

Wenn eine Integration entwickelt oder getestet wird, geben Sie Feedback, wenn Probleme auftreten. Auch wenn eine Problemumgehung erforderlich ist, Kundenservice und Support Mitarbeiter können in zukünftigen Releases eine Verbesserung bieten, die das Problem für zukünftige Integrationen lindern könnte.

Testen Sie unter angemessener Last

Ein häufiges Problem bei Integrationen besteht darin, dass sie nicht für realistische Lasten ausgestattet sind. Da jede Integration eine bereichsbezogene Anwendung ist, gibt es weitere Einschränkungen, die von der Plattform auferlegt werden, um die Systemstabilität sicherzustellen. Diese Einschränkungen können dazu führen, dass Aufträge mit langer Ausführungszeit oder API-Aufrufe beendet werden. Sie können sicherstellen, dass lange laufende Prozesse oder Prozesse, die viele Daten verarbeiten, ordnungsgemäß behandelt werden, indem Sie die Zeit reduzieren, die jeder Aufruf oder Prozess benötigt (normalerweise indem Sie eine Möglichkeit zum Paginieren von API-Anforderungen bereitstellen oder große Datensätze blockieren).

Problembehandlung bei der Integration

Diese Vorschläge zur Problembehandlung können Ihnen helfen, häufige Probleme zu lösen, die beim Einrichten oder Ausführen von Integrationen auftreten können.

Ersetzen Sie ein nicht vertrauenswürdiges oder abgelaufenes SSL-Zertifikat einer Drittpartei

Wenn in einer Integration eine SSL-Verbindung erforderlich ist, gibt es Umstände, in denen das vom Drittanbieter bereitgestellte Zertifikat entweder noch nicht vertrauenswürdig ist ServiceNow Oder ist abgelaufen. Sie können es ersetzen oder ein neues Zertifikat hinzufügen.

Vorbereitungen
Erforderliche Rolle: sn_ti.write

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erwerben Sie das SSL-Zertifikat vom Drittanbieter.
   Sie können beispielsweise ein X.509-Zertifikat (PEM) von einem SSL-Endpunkt im Firefox-Browser wie folgt importieren.

   a. Geben Sie die Endpunkt-URL in die Adressleiste des Browsers ein.
   Beispiel: `https://<3rdparty>/` .

   b. Klicken Sie auf das Schlosssymbol in der Adresszeile.

   c. Klicken Sie Auf **Weitere Informationen** Und klicken Sie auf **Sicherheit** Registerkarte.

   d. Klicken Sie Auf **Zeigen Sie Das Zertifikat An** Und klicken Sie auf **Detail** Registerkarte.

   e. Klicken Sie Auf **Exportieren** Um das PEM in Ihrem lokalen Dateisystem zu speichern.

   f. Öffnen Sie die gespeicherte Datei in einem beliebigen Texteditor-Tool, und kopieren Sie den Inhalt in die Zwischenablage.
   Sie muss mit beginnen `----- ZERTIFIKAT BEGINNEN------` Und enden mit `----- ENDZERTIFIKAT-----` .

2. Navigieren zu **Systemdefinition** > **Zertifikate**an.
3. Klicken Sie Auf **Neu** Und Erstellen Sie einen neuen Datensatz Für die Integration.
4. In **PEM-Zertifikat** , Fügen Sie das Zertifikat ein, das Sie zuvor heruntergeladen und in die Zwischenablage kopiert haben.
5. Klicken Sie auf **Speichern**.
   Die anderen Felder im Datensatz werden automatisch generiert.

Integrationsfähigkeits-Framework 2,0

Das neue Framework für Integrationsfähigkeiten 2,0 wurde überarbeitet, um die Implementierung von Integrationen auf einfache und konsistente Weise zu ermöglichen. Dies stellt eine konsistente Experience für ähnliche Integrationstypen sicher (z. B. Reputationssuche erkennbarer Elemente).

Das neue Framework verfügt über Fähigkeiten, die mit implementiert wurden Flows .

Vorteile der erweiterten Framework-Implementierung:

- Die Fähigkeits-Flows, die nur Komponenten auf Geschäftsebene ohne implementierungsspezifische Logik enthalten.
- Die Fähigkeits-Flows akzeptieren jetzt ein breites Spektrum von Eingaben und Formaten, um maximale Flexibilität zu gewährleisten (z. B. Referenzen erkennbarer Elemente, CI-Referenzen, Aufgaben, beliebige Tabellen- oder sys_ID-Kombinationen).
- Quotenbegrenzung oder Drosselung bei Integrationsausführungen sind jetzt einfach zu konfigurieren (ohne dass dies mithilfe von anwenderdefiniertem Code oder Änderungen an Implementierungs-Workflows erfolgen muss).
- Verbesserte Auditing- und Ausführungsnachverfolgungsfunktionen ermöglichen jetzt bessere Berichterstellung und einfachere Problembehandlung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Robuste Fehlerbehandlungsfunktionen sind in die Fähigkeits-Flows integriert, um zu vermeiden, dass Implementierungsroutinen dupliziert werden.
- Möglichkeit, die bedingte Auslösung der Fähigkeiten oder Integrationen zu konfigurieren. Dies bietet Flexibilität, Automatisierungen basierend auf der Incident-Kategorie automatisch zu starten.
- Eine Standardfilterbedingung wurde für alle Fähigkeiten eingeführt, um „Zulassen gelisteter erkennbarer Elemente zulassen“ zu filtern, bevor Eingaben für die Integrationen bereitgestellt werden.

Hinweis:
Dieses neue Fähigkeits-Framework führt kein Upgrade des aktuellen Fähigkeits-Frameworks durch. Beide Frameworks können parallel arbeiten. Anweisungen zur Nutzung des neuen Fähigkeits-Frameworks finden Sie unter Verwenden des neuen Fähigkeits-Frameworks mit einer installierten Integration Und Verwenden des neuen Fähigkeits-Frameworks mit einem Flow.

Unterstützte Integrationen und Komponenten

Das Plugin „Security Incident Response“ enthält alle in Integration Capabilities Framework 2,0 aufgeführten Fähigkeits-Flows und allgemeine Standardfilter, die Sie je nach Anforderung aktivieren oder deaktivieren können.

Hinweis:
Wenn Sie das neue Fähigkeits-Integrations-Framework mit dem New York-Release verwenden möchten, müssen Sie das Plugin ServiceNow IntegrationHub Starter Pack Installer installieren. Wenden Sie sich an den Kundensupport, um Hilfe bei der Installation zu erhalten.

Unterstützte Anwendungsversionen

Ab Security Incident Response 10.0 werden die folgenden Integrationen unterstützt:

Anwendung	Mindestversion erforderlich
Integration Von Security Operations Hybrid Analysis	10.0.0
PhishTank-Integration für Security Operations	10.0.0
ThreatCrowd-Integration für Security Operations	10.0.0
CrowdStrike Intelligence-Integration für Security Operations	10.0.0
Security Operations „wurde ich verpönt?“ Integration	10.0.0
Security Operations-Metadefender-Integration	10.0.0
Security Operations – Aufgezeichnete Zukünftige Integration	10.0.0
Security Operations VirusTotal-Integration	10.0.0
Security Operations – WHOIS-Integration umkehren	10.0.0

Ab Security Incident Response 10.4 werden die folgenden Integrationen unterstützt:

Anwendung	Mindestversion erforderlich
Security Operations RiskIQ-Integration	10.0.0

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung	Mindestversion erforderlich
Security Operations-Shodan-Integration	10.0.0
Security Operations WHOIS-Integration	10.0.0
Security Operations Carbon Black-Integration	10.3.1
Integration Der Splunk-Suche Für Security Operations	10.3.0
Integration von Security Operations ArcSight Logger	10.3.0
Security Operations McAfee ESM-Integration	10.3.0
Security Operations Elasticsearch-Integration	10.3.0
Security Operations: IBM QRadar-Integration	10.3.1
CrowdStrike Falcon-Host für Security Operations	10.3.0

Enthaltene Komponenten

Das neue Fähigkeits-Integrations-Framework enthält die folgenden Komponenten:

- **Fähigkeiten** : Alle folgenden Funktionen, die heute im Produkt als Workflows vorhanden sind, wurden mit neu gestaltet Flows :
  - **Anforderung Blockieren** : Bietet eine Möglichkeit zum Blockieren erkennbarer Elemente, die einem Security Incident zugeordnet sind, an einer Firewall, einem Web-Proxy oder einem anderen Kontrollpunkt. Diese Fähigkeit wird bei der Reaktion auf Incidents für Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.
  - **E-Mail suchen und löschen** : Bietet eine Möglichkeit, einen E-Mail-Server während einer Sicherheitsuntersuchung zu durchsuchen und bei Bedarf E-Mails vom Server zu löschen.
  - **Bereichern Sie Das Konfigurationselement** : Bietet eine allgemeine Möglichkeit, Konfigurationselemente mit zusätzlichen Informationen aus einer Vielzahl von Quellen zu ergänzen. Diese Fähigkeit wird bei Untersuchungen zur Reaktion auf Incidents verwendet, um Daten anzureichern, die einem Security Incident zugeordnet sind.
  - **Reichern Sie Erkennbares Element An** : Bietet eine allgemeine Möglichkeit, erkennbare Elemente mit zusätzlichen Informationen aus einer Vielzahl von Quellen zu ergänzen. Diese Fähigkeit wird bei der Reaktion auf Incidents für Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.
  - **Ereigniserfassung** : Bietet eine allgemeine Möglichkeit, einen Security Incident zu erstellen, indem Ereignisse aus einer Integrationsquelle einem Security Incident zugeordnet werden.
  - **Rufen Sie Netzwerkstatistiken Ab** : Ruft eine Liste aktiver Netzwerkverbindungen von einem Endpunkt oder Host ab. Diese Funktion wird bei Untersuchungen zur Ergänzung von Incidents verwendet.
  - **Laufende Prozesse Abrufen** : Ruft eine Liste der laufenden Prozesse von einem Endpunkt oder Host ab. Diese Funktion wird bei Untersuchungen zur Ergänzung von Incidents verwendet.
  - **Host Isolieren** : Bietet eine Möglichkeit, einen Endpunkt oder einen Host zu isolieren, der einem Security Incident zugeordnet ist. „Host isolieren“ wird für ein Konfigurationselement (CI) ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **In Beobachtungsliste veröffentlichen** : Bietet eine Möglichkeit, erkennbare Elemente, die einem Security Incident zugeordnet sind, einer Beobachtungsliste hinzuzufügen, die Sicherheitsereignisse überwacht und Warnungen generiert. Diese Fähigkeit wird als Teil der Reaktion auf Incidents während Untersuchungen verwendet.
- **Sichtungssuche** : Durchsucht verschiedene SIEMs oder andere Protokollspeicher nach Instanzen von erkennbaren Elementen. Diese Fähigkeit wird verwendet, um das Vorhandensein schädlicher IoCs in Ihrer Umgebung zu bestimmen.
- **Bedrohungssuche** : Führt Threat Intelligence-Suchen durch, um zu bestimmen, ob ein bestimmtes erkennbares Element einer bekannten Sicherheitsbedrohung zugeordnet ist. Diese Fähigkeit wird als Teil der Reaktion auf Incidents während Untersuchungen verwendet.

- **Neue Tabellen** :
  - sn_sec_cmn_Capability: Fähigkeit und Flow, die die Fähigkeit implementieren.
  - sn_sec_cmn_Capability_Implementation: Der tatsächliche Implementierungs-Flow, der die Services der Fähigkeit bereitstellt.
  - sn_sec_cmn_Capability_Execution: Der Ausführungsdatensatz für eine Fähigkeit zur Laufzeit.
  - sn_sec_cmn_Capability_Implementation_Execution: Der Ausführungsdatensatz für eine Fähigkeitsimplementierung zur Laufzeit.
  - sn_sec_cmn_Filter_condition: Die Filterbedingungen, die zur Laufzeit auf die Fähigkeit oder eine Fähigkeitsimplementierung angewendet werden können.
- **Skript einschließen** : CapabilityProcessor: Verarbeitet den gesamten Verarbeitungscode für das Framework.
- **Quotenlimit** : Maximale gleichzeitige Anforderung der Fähigkeit pro Zeitraum: Definiert, wie viele Integrationen parallel ausgeführt werden können.
- **Implementierung der Prozessfähigkeit für geplante Aufgaben** : Wird alle 15 Sekunden ausgeführt und kann auf der Seite „Eigenschaften der Sicherheitsadministration“ (. Deaktiviert werden**Security Incident** > **Administration** > **Eigenschaften**an.
  - Aktiviert oder deaktiviert die geplante Aufgabe, Prozessfähigkeitsimplementierungen: Dieser Auftrag plant und verwaltet automatisch die Ausführungs-Flows der Fähigkeitsimplementierung.
  - Aktiviert oder deaktiviert automatisierte Suchen oder Ergänzungen: Einstellung, die die geplante Aufgabe aktiviert oder deaktiviert, die eine automatisierte Bedrohungssuche oder Ergänzung erkennbarer Elemente durchführt, wenn erkennbare Elemente Security Incidents im aktuellen Fähigkeits-Framework hinzugefügt werden.
  - Aktiviert oder deaktiviert die geplante Aufgabe „erkennbare Security Incident-Elemente suchen“: Dieser Auftrag plant automatisch einen Auftrag zur Bedrohungssuche oder zum Anreichern erkennbarer Elemente, wenn erkennbare Elemente zu einem Security Incident hinzugefügt werden.

Konfigurationen im neuen Fähigkeits-Framework

In diesem Abschnitt werden die im neuen Framework verfügbaren Konfigurationen beschrieben.

Vorbereitungen

Erforderliche Rolle: sn_si.admin, Flow_Designer, action_Designer

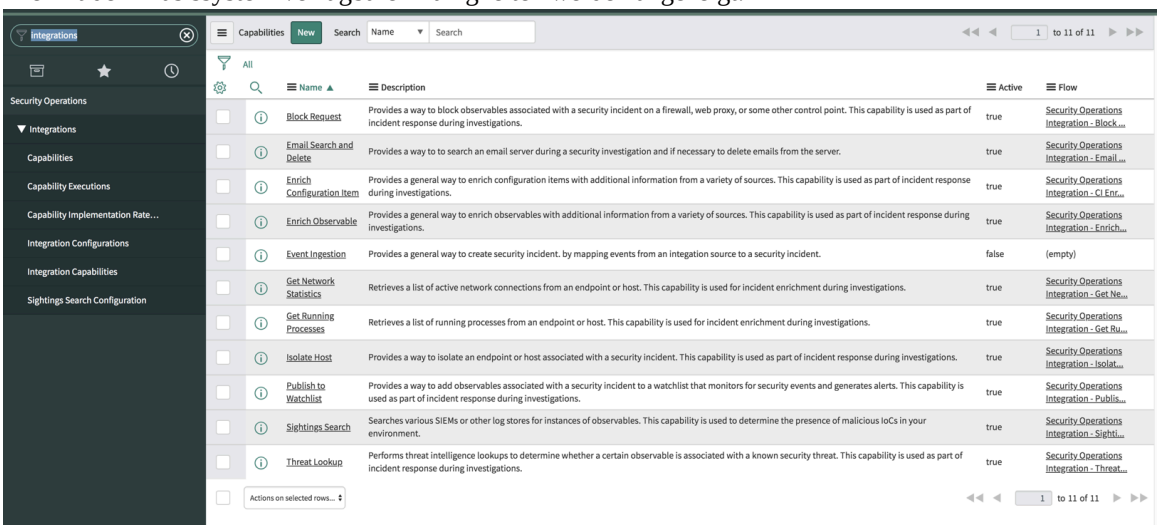
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Fähigkeiten**an.

   Hinweis:
   Version 10.4: Ab Security Incident Response 10.4, dem Menünamen **Fähigkeiten** Wurde in geändert **Integrationsfähigkeiten (Flows)** .

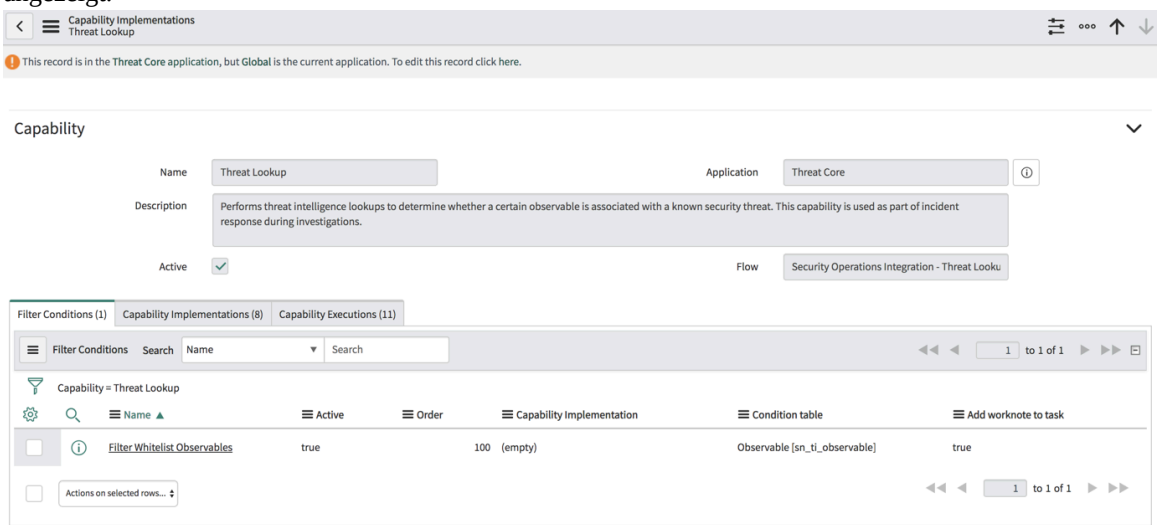
2. Die mit dem Basissystem verfügbaren Fähigkeiten werden angezeigt.



   Hinweis:

   Dies sind die Fähigkeiten, die mit dem Basissystem bereitgestellt werden. Sie können die Fähigkeiten verwenden oder sie nach Bedarf anpassen. Die folgenden Schritte beschreiben, wie eine Fähigkeit konfiguriert wird, und die für die Fähigkeit implementierten Integrationen.

3. Klicken Sie auf den Link in der Spalte Name, um eine Fähigkeit zu konfigurieren.
   Der Name, die Anwendung, die Beschreibung und der Flow, den die Fähigkeit implementiert, werden angezeigt.



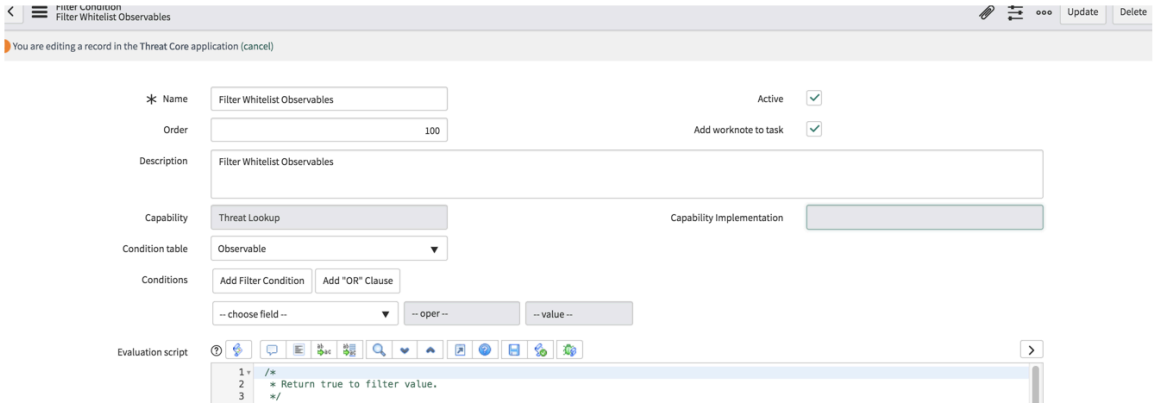
4. Wählen Sie aus **Aktiv** Kontrollkästchen zum Aktivieren der Fähigkeit.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Filterbedingungen auf Fähigkeitsebene** : Wenn eine Integrationsfähigkeit einen Flow implementiert, werden die dem Flow zugeordneten Filterbedingungen ausgeführt, bevor der Fähigkeits-Flow gestartet wird. Beispielsweise enthält die Funktion „Bedrohungssuche“ die Bedingung „Allowlist für erkennbare Elemente filtern“, wie oben gezeigt. Klicken Sie auf den Namenslink, um die Filterbedingung zu bearbeiten.

  Hinweis:
  Wählen Sie aus **Arbeitsnotiz zu Aufgabe hinzufügen** Kontrollkästchen zum Hinzufügen von Arbeitsnotizen, um Informationen zu den verwendeten Filterbedingungen einzubeziehen.



  Sie können entweder Filterbedingungen oder ein Skript oder eine Kombination aus beiden definieren. Im obigen Beispiel wird ein Skript verwendet, um die Filterbedingungen zu definieren. Wenn der Fähigkeits-Flow ausgeführt wird, sucht das Skript nach zulässigen erkennbaren Elementen und entfernt sie aus der Tabelle.

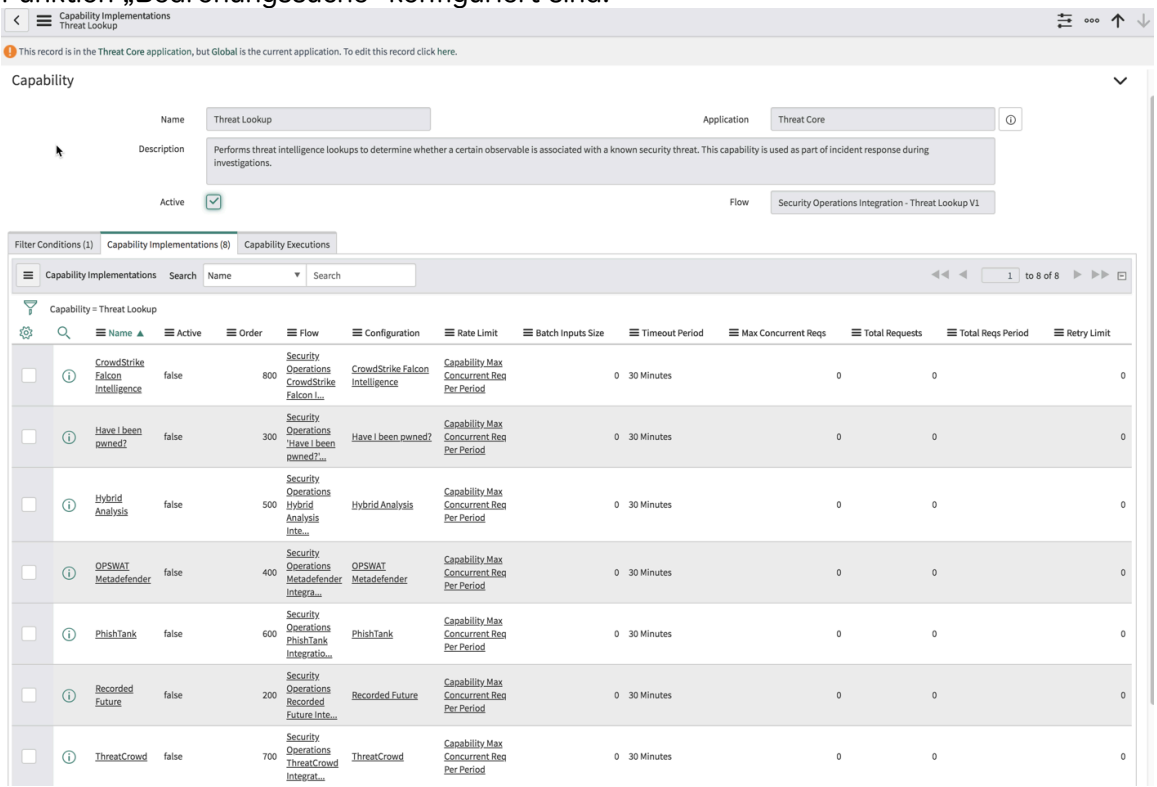
  Hinweis:
  Die hier festgelegten Filterbedingungen gelten für alle aktiven Integrationen, die in definiert sind **Fähigkeitsimplementierungen** Registerkarte.

- **Fähigkeitsimplementierungen** : Klicken Sie auf **Fähigkeitsimplementierungen** Registerkarte. Die Implementierungen (Integrationen), die für die Fähigkeit konfiguriert

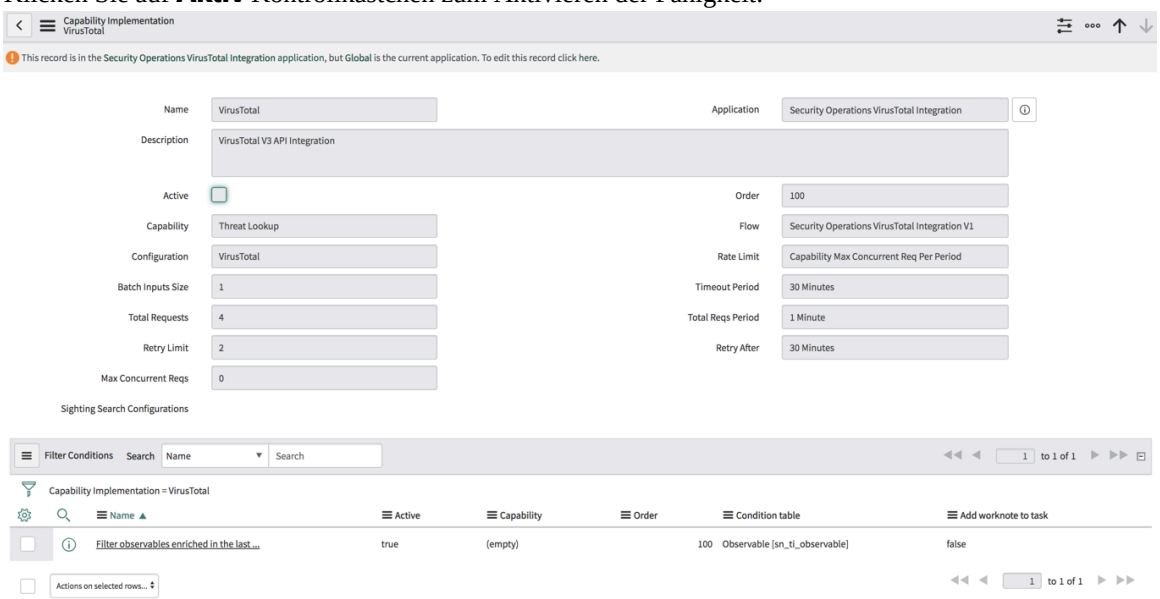
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wurden, werden angezeigt. Das folgende Beispiel zeigt die Integrationen, die für die Funktion „Bedrohungssuche“ konfiguriert sind:



5. Klicken Sie auf den Namenslink, um die Fähigkeitsimplementierung anzuzeigen.
   Der Name, die Anwendung, die Beschreibung und der Flow, den die Fähigkeit implementiert, werden angezeigt.
6. Klicken Sie auf **Aktiv** Kontrollkästchen zum Aktivieren der Fähigkeit.



Sie können die folgenden Details angeben:

Feldname	Beschreibung
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diese Integration zu deaktivieren.

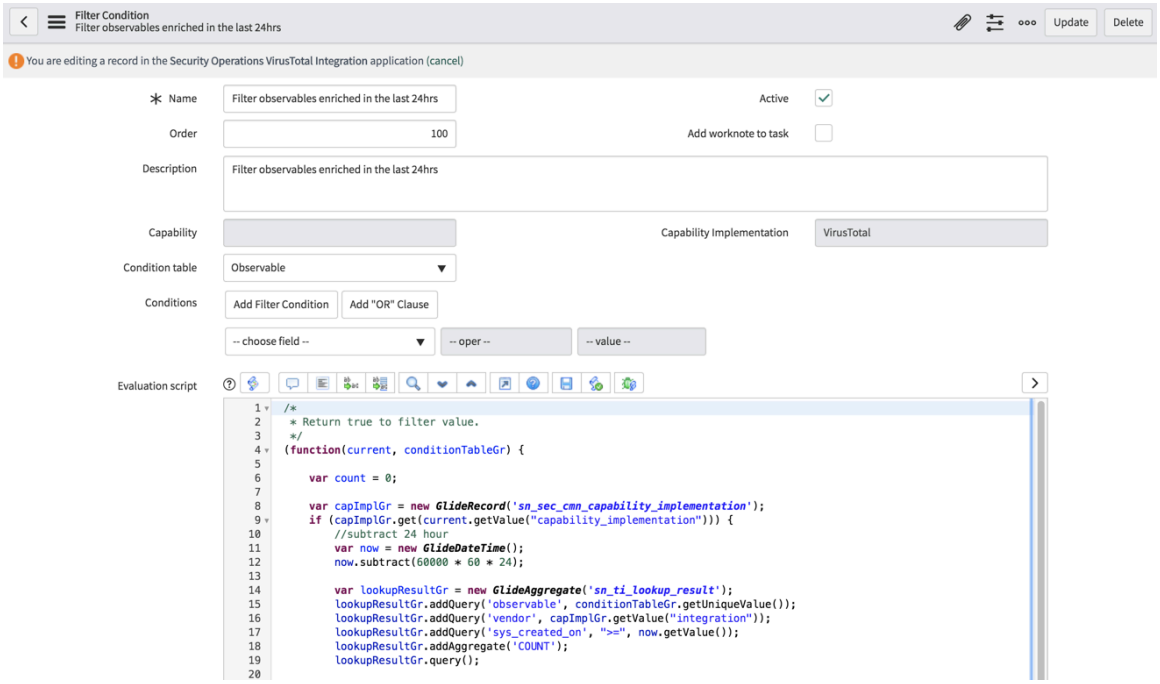
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldname	Beschreibung
	Hinweis: Wenn Sie diese Integration mithilfe der Integrationskachel in konfigurieren **Security Operations** > **Integrationen** > **Integrationskonfigurationen**Seite, auf die diese Kennzeichnung automatisch festgelegt ist **Aktiv** .
Reihenfolge	Gibt die Reihenfolge an, in der die Integrationen ausgeführt werden.
Fähigkeit	Die von dieser Integration implementierte Fähigkeit.
Flow	Der Subflow, der die Fähigkeit implementiert.
Konfiguration	Die Integrationskonfiguration für diese Fähigkeit. **Hinweis:** Dies wird anfänglich auf die Standardkonfiguration festgelegt, die mit dem Basissystem bereitgestellt wird. Wenn eine Integration mit der Integrationskachel in konfiguriert wird **Integrationskonfigurationen** Seite, wird dieser Wert automatisch auf die neu erstellte Konfiguration zurückgesetzt.
Quotengrenze	Gibt die Anzahl der Integrationen an, die zur Laufzeit ausgeführt werden können (parallel oder pro Zeiteinheit).
Batch-Eingabegröße	Die Batch-Eingabegröße für jede Ausführung. Für eine Sichtungssuchintegration können Sie beispielsweise die erkennbaren Elemente in Batches von 50 gruppieren, damit die generierten Abfragen nicht zu groß werden. 0 gibt an, dass kein Grenzwert vorhanden ist.
Zeitüberschreitungszeitraum	Die maximale Dauer, bis der Fähigkeitsimplementierungs-Flow abgebrochen wird. 0 gibt an, dass kein Zeitüberschreitungszeitraum vorhanden ist.
Anforderungen insgesamt	Die Gesamtzahl der Implementierungsausführungsanforderungen. Dieses Feld kann in Verbindung mit dem Feld Gesamtanforderungszeitraum verwendet werden, um die Anzahl der Anforderungen für den Service zu begrenzen. Sie können die Anzahl beispielsweise auf 4 Anforderungen pro Minute beschränken.
Anforderungen insgesamt im Zeitraum	Die Gesamtzahl der pro Zeitraum zulässigen Ausführungsanforderungen.
Wiederholungsbegrenzung	Die Anzahl der Wiederholungen, die für eine fehlgeschlagene Ausführungsanforderung zulässig sind. Dieser Grenzwert gilt, wenn **Wiederholen Sie Den Vorgang** Die Kennzeichnung ist in Ihrer Integration so festgelegt, dass eine Ausführungsanforderung wiederholt wird, wenn eine Bedingung erfüllt ist. Beispielsweise wird eine Wiederholungsanforderung gestellt, wenn Sie Ihr Lizenzlimit für diesen Service für einen Zeitraum überschritten haben oder der Service ausgefallen ist.
Wiederholen nach	Der Zeitraum, nach dem versucht wird, eine fehlgeschlagene Ausführungsanforderung erneut zu versuchen.
Max. gleichzeitige Anforderungen	Die maximale Anzahl gleichzeitiger Implementierungsausführungsanforderungen. 0 gibt keinen Grenzwert an.
Sichtungssuchkonfigurationen	Die standardmäßigen Sichtungssuchabfragen, die ausgeführt werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie im Abschnitt Filterbedingungen auf den Link Name, um die für die Implementierung definierten Bedingungen zu konfigurieren. Fügen Sie Filterbedingungen hinzu, oder löschen Sie sie, ändern Sie das Skript bei Bedarf, und aktualisieren Sie den Datensatz.



Verwenden des neuen Fähigkeits-Frameworks mit einer installierten Integration

In diesem Abschnitt wird beschrieben, wie das neue Fähigkeits-Framework für eine vorhandene Integration verwendet wird.

Führen Sie die folgenden Schritte aus, um eine bereits installierte und konfigurierte Integration zu aktivieren (siehe unterstützte Liste der Integrationen in Unterstützte Integrationen und Komponenten), um das neue Fähigkeits-Framework zu verwenden.

Hinweis:
Integration Capability Framework 2,0, das mit Security Incident Response 10.0.2 verfügbar ist, unterstützt Implementierungen für **Bedrohungssuche** Und **Reichern Sie Erkennbares Element An** Fähigkeiten. Implementierungen für andere Fähigkeiten werden in einem zukünftigen Release verfügbar gemacht.

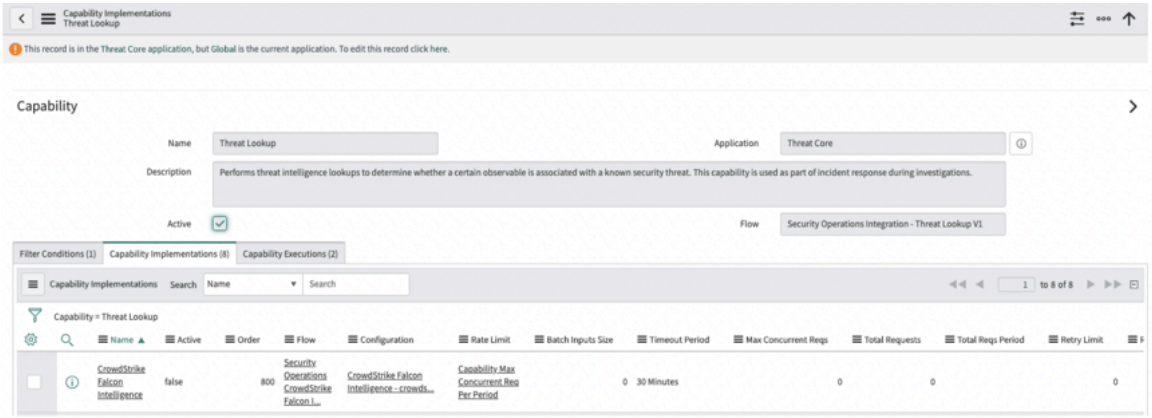
Bevor Sie beginnen

- Erforderliche Rolle: sn_si.admin
- Security Incident Response 10.0.2

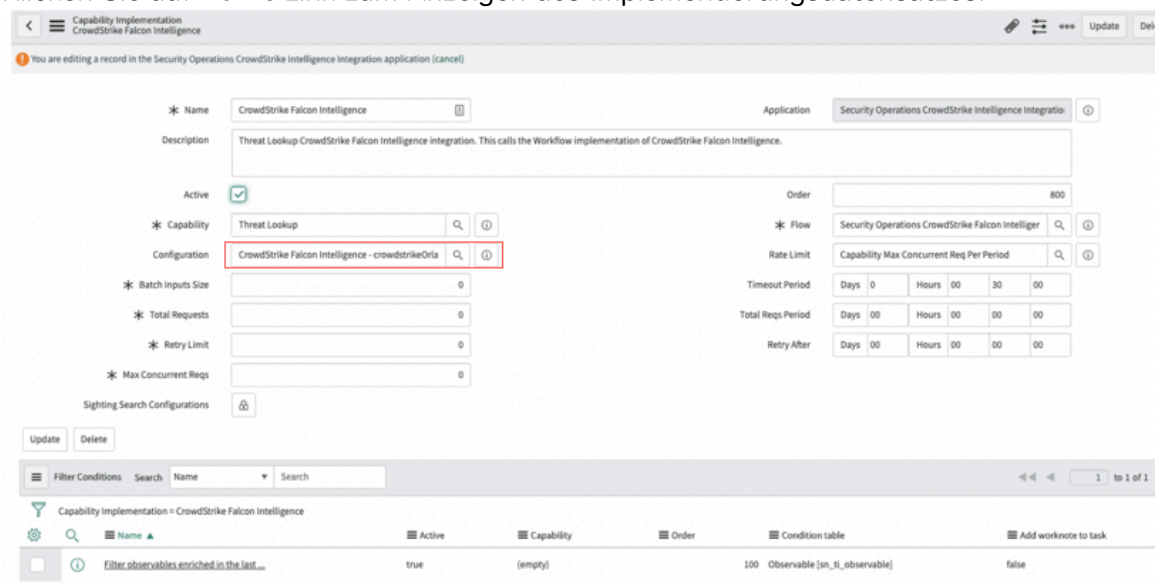
1. Navigieren zu **Security Operations** > **Integrationen** > **Fähigkeiten**an.
2. Klicken Sie auf **Bedrohungssuche** Fähigkeit.
3. Klicken Sie auf die Registerkarte Fähigkeitsimplementierung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

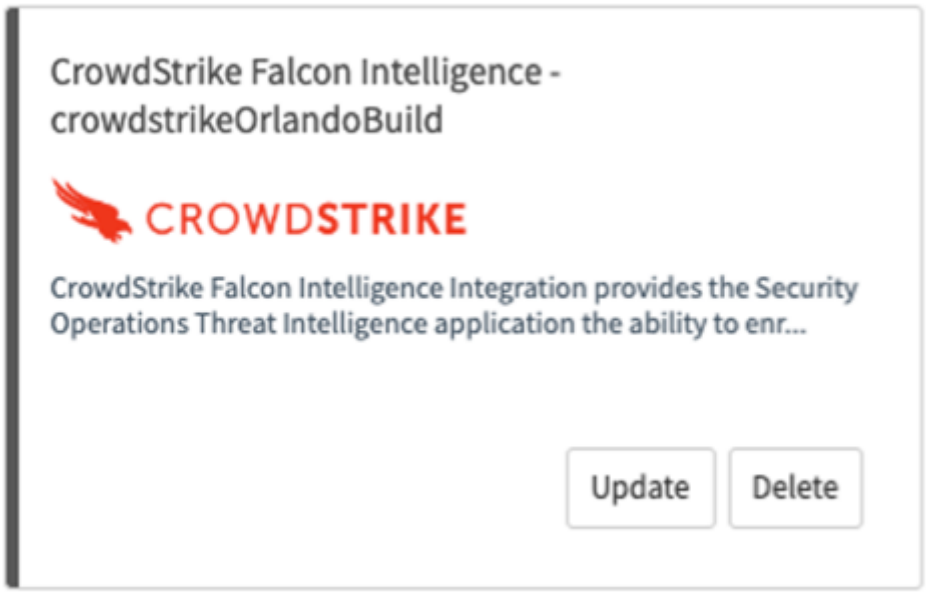


4. 4. Zeigen Sie den Fähigkeitsimplementierungsdatensatz für die Integration von Interesse an (Beispiel: CrowdStrike Falcon Intelligence). Die **Aktiv** Die Spalte muss den Wert haben **Falsch** .
5. Klicken Sie auf **Name** Link zum Anzeigen des Implementierungsdatensatzes.



6. Aktivieren Sie die Checkbox **Aktiv**.
7. Stellen Sie sicher, dass der Implementierungsdatensatz auf den richtigen Konfigurationsdatensatz (den Kachelnamen für die Integration in) verweist **Integrationskonfigurationen** > **Konfigurationen Anzeigen (Ja)**) an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Die Implementierung ist für die Verwendung mit dem neuen Framework aktiviert.

Hinweis:
Alle unterstützten Integrationen, wenn sie mit Security Incident Response 10.0.2 installiert werden, werden automatisch unter dem neuen Framework für Integrationsfähigkeiten aktiviert.

Verwenden des neuen Fähigkeits-Frameworks mit einem Flow

Führen Sie die folgenden Schritte aus, um einen Flow zu erstellen und den Subflow aufzurufen, der vom neuen Fähigkeits-Framework bereitgestellt wird.

Vorbereitungen

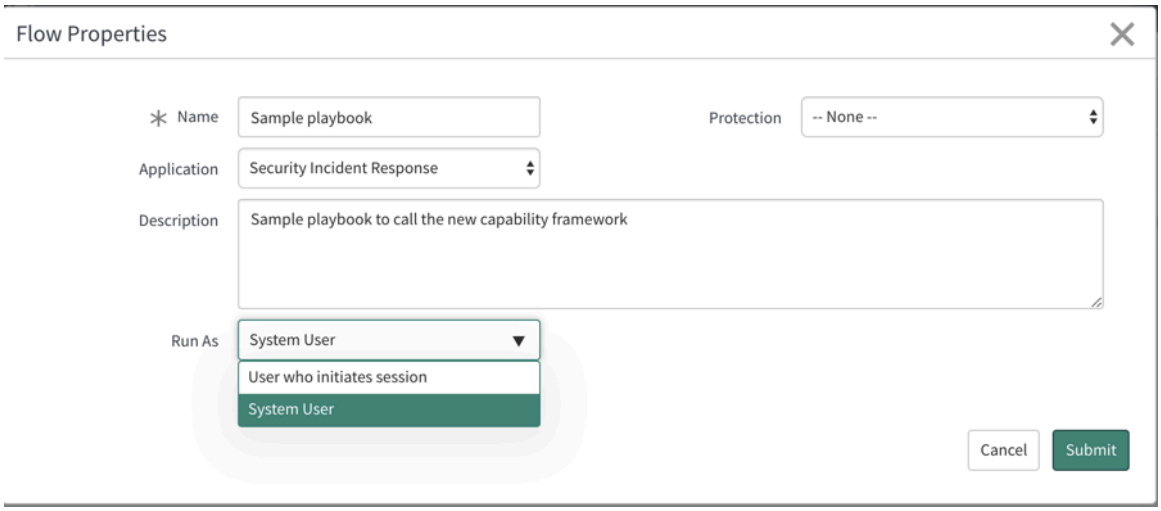
- Erforderliche Rolle: sn_si.admin, Flow_Designer, action_Designer
- Installieren Sie eine der unterstützten Integrationen (siehe Unterstützte Integrationen und Komponenten)

Die folgenden Schritte beschreiben, wie Sie einen Beispiel-Flow erstellen und einen der Subflows aufrufen, die mit dem neuen Fähigkeits-Framework bereitgestellt werden.

Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Designer**an.
2. Klicken Sie Auf **Neu** Um einen neuen Flow zu erstellen und die erforderlichen Informationen für die Eigenschaften bereitzustellen.

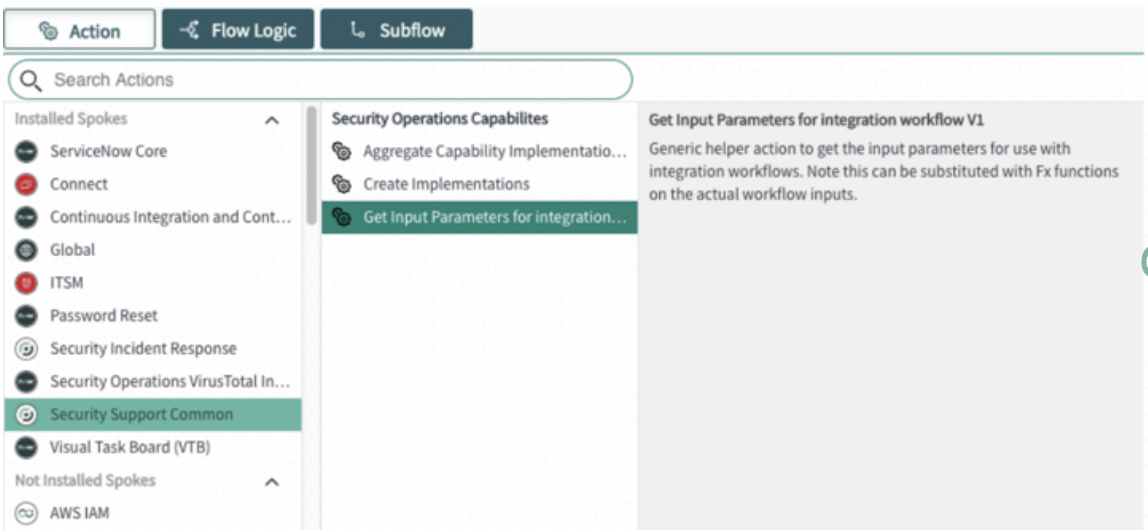
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis:
Wählen Sie Aus **Systemanwender** In der Auswahlliste Ausführen als, wie in der obigen Abbildung gezeigt.

3. Wählen Sie eine Auslöserbedingung für den Flow aus (ein allgemeiner Auslöser ist die Erstellung eines Security Incident-Datensatzes für eine bestimmte Incident-Kategorie).

4. Wählen Sie in Schritt 1 des Flows eine Aktion aus, um Eingaben aus dem Security Incident abzurufen (z. B. erkennbare Elemente).
Sie können eine Aktion aus den Aktionen auswählen, die im Basissystem mit der Common Spoke für Security Support bereitgestellt werden.

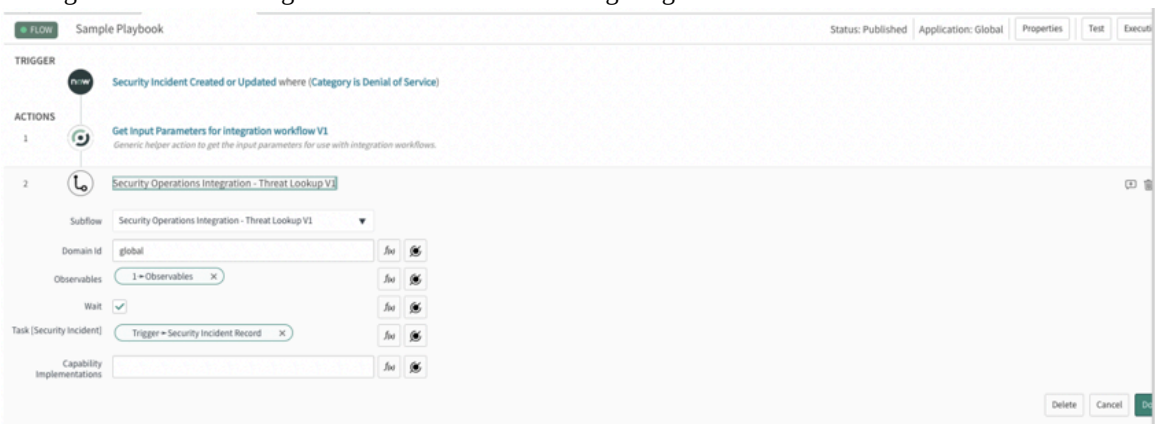


5. Wählen Sie in Schritt 2 einen Subflow aus (z. B. Bedrohungssuche).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Konfigurieren Sie den ausgewählten Subflow wie unten gezeigt:



7. Speichern und veröffentlichen Sie den Flow.

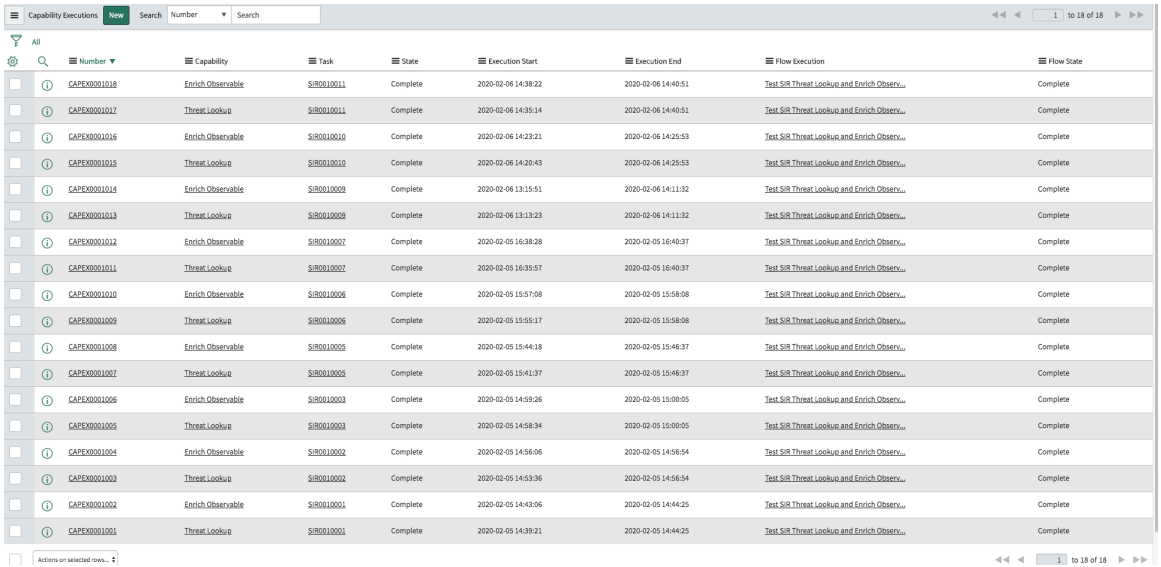
Problembehandlung für Integrationsfähigkeits-Flows

Die Option Fähigkeitsausführungen enthält detaillierte Informationen zu jeder ausgeführten Fähigkeit.

Hinweis:
Abgeschlossene Ausführungen werden nach 30 Tagen archiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Security Operations** > **Integrationen** > **Fähigkeitsausführungen.**an.



2. Klicken Sie auf den Link Fähigkeitsausführungen, um zusätzliche Details anzuzeigen.

`Security Incident-Datensatz-Arbeitsnotizen`

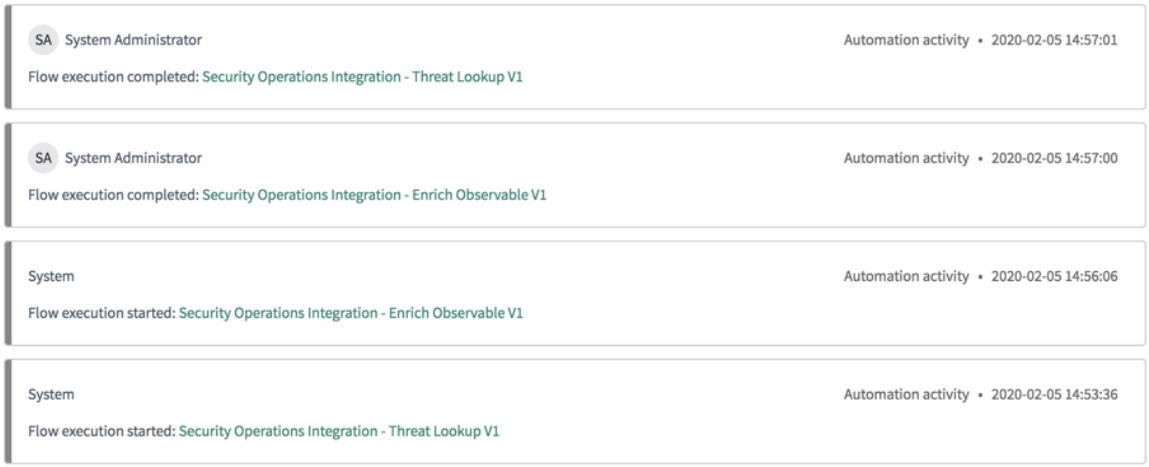
Wenn erkennbare Elemente einem Security Incident hinzugefügt wurden und die Auslöserbedingung für den Flow erfüllt ist, werden die Subflows „Bedrohungssuche“ und „erkennbare Elemente anreichern“ initiiert, und dem Security Incident werden die folgenden Arbeitsnotizen hinzugefügt:

- Flow-Ausführung gestartet: Integration von Security Operations – erkennbares Element anreichern V1
- Flow-Ausführung abgeschlossen: Integration von Security Operations – erkennbares Element anreichern V1
- Flow-Ausführung gestartet: Integration von Security Operations – Bedrohungssuche V1
- Flow-Ausführung abgeschlossen: Integration von Security Operations – Bedrohungssuche V1

Um diese Arbeitsnotizen anzuzeigen, melden Sie sich als Anwender mit an *`sn_si.admin`* Oder *`sn_si.Analyst`* , Und *`Flow_Designer`* , Und *`Action_Designer`* Rollen.

Navigieren Sie zur Datensatzseite für Security Incidents, und klicken Sie auf diese Arbeitsnotizen, um die Flow-Ausführungsdetails anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



REST APIs für die Integration von Drittparteien mit Security Operations

Die Security Operations Das Basissystem enthält eine Reihe von geskripteten REST-APIs, mit denen Kunden und Partner die einfache Integration in eine vorhandene ermöglichen Security Operations Bereitstellung. Mit den APIs können Sie Daten von außerhalb Ihres Systems erfassen (z. B. wird ein Python-Skript verwendet, um Daten von VirusTotal zu empfangen) und an Ihre Instanz zurücksenden.

Skripts, die in fast jeder Sprache geschrieben wurden (z. B. Python), können mit den APIs verwendet werden, um kundenspezifische Prozesse auszuführen. Die Skripts müssen in einer Sprache geschrieben werden, die einen HTTP Post-Aufruf nach außen durchführen kann. Wenn Sie beispielsweise eine Java-Anwendung haben, müssen Sie eine Bibliothek wie verwenden `java.net.HttpUrlConnection` Paket, um einen HTTP-Aufruf zu erstellen und eine JSON-Zeichenfolge als Text für die Nachricht zu übergeben.

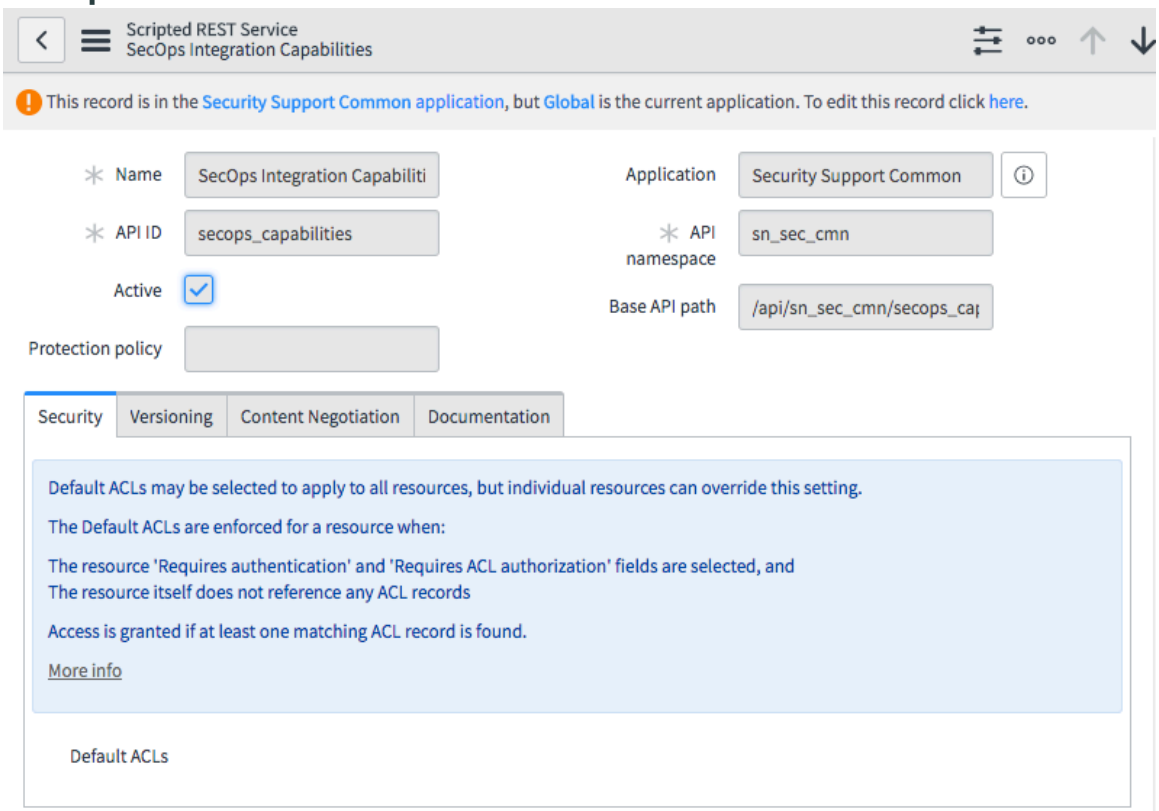
Die API wird ausschließlich verwendet, um Daten hinzuzufügen, die außerhalb unseres Systems erfasst wurden. Wenn Sie beispielsweise das VT-Python-Skript eingegeben und Daten von VT erhalten haben, können Sie diese Daten an die SN-Instanz zurücksenden.

Authentifizierung

Alle Vorgänge innerhalb der API-Definitionen verwenden die Plattformauthentifizierung, die von bereitgestellt wird Geskriptete REST-APIs Vorgangsfunktion. Um auf zuzugreifen, navigieren Sie zu **System-Webservices** > **Scripted Web Services** > **Scripted REST APIs** Und suchen Sie **SecOps-Integrationsfähigkeiten** API.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geskripteter REST-Service



Der Anwender und die Domäne des Anwenders sind im Kontext der API leicht verfügbar. Datensätze können an einen Anwender gebunden, ein Audit-Pfad eingerichtet und Domänentrennung durchgeführt werden. Da Sie als bestimmter Anwender authentifiziert sind, können Sie auch verwenden Mit GlideRecordSecure Um nicht autorisierten Zugriff auf Daten zu verhindern.

Autorisierung

Dient zum Schutz des Datensatzerstellungsprozesses vor Anwendern außerhalb des Security Operations-Anwendung benötigen Sie sn_sec_cmn.api_write Rolle. Nur Anwender mit dieser Rolle können auf die APIs zugreifen.

Parameter der Konfigurationsanforderung

Die folgenden Anforderungsparameter sind verfügbar.

Name	Standard	Beschreibung
Ignorieren_obligatorisch_fields	falsch	Bei „wahr“ wird der Datensatz beibehalten, auch wenn keine Pflichtfelder ausgefüllt sind.
Include_wrap	falsch	Bei „wahr“ enthält die Antwort den von der Instanz bereitgestellten Standard-Wrapper für geskriptete REST-APIs.
Simple_response	falsch	Bei „wahr“ enthält die Antwort nur, ob der Vorgang erfolgreich war.

Fehlerantworten

Die folgenden Fehlerantworten können auftreten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlermeldung	Wann tritt es auf?	Lösung
Ungenügender Zugriff	Anwender hat nicht die Rolle sn_sec_cmn.api_write.	Fügen Sie dem Anwender die Rolle hinzu.
Ungültiger Beitragstext	Anforderungstext ist leer oder ein leeres Objekt.	Entsprechen Sie der API-Definition.
Keine Felder angegeben	Datenfelder, die beibehalten werden sollen, sind leer.	Entsprechen Sie der API-Definition.
Pflichtfelder fehlen: X,y,z	Pflichtfelder fehlen.	Entsprechen Sie der Tabellendefinition der Zieltabelle oder des Zielsatzes **Ignorieren_obligatorisch_fields** Auf „wahr“.
Datensatz kann nicht beibehalten werden	Der analysierte Datensatz kann nicht beibehalten werden.	GlideRecord – Einfügen() fehlgeschlagen, weitere Analyse ist erforderlich.
Unbekannter Fehler.	Tritt auf, wenn kein Known Error-Pfad befolgt wurde.	Weitere Analysen sind erforderlich.

Anwendungsfall „CI-Ergänzung“

Mit Ihren Drittanbieterskripts können Sie in die Tabelle „Konfigurationselementanreicherung“ [sn_sec_cmn_ci_Enrichment_result] für die CI-Anreicherung schreiben. Die Ergänzungsdatensätze basieren auf vorhandenen Fähigkeiten, die detaillierte Informationen zu einem Datensatz aus einer Drittparteiquelle bereitstellen.

Beispielanforderung und -Antworten für den Anwendungsfall „CI-Ergänzung“ werden hier angezeigt.

Erstellen – Anforderung für CI-Ergänzung

```
{
   "ignore_mandatory_fields": true,
   "payload": [
      {
         "configuration_item_id": "2dfd7c8437201000deeabfc8bcbe5d56",
         "data": [
             {
               "external_link": "http://www.servicenow.com",
               "vendor": "aafbf46ad72212007a6de294de6103a2",
               "data_type": null,
               "source": null,
               "name": null,
               "parent": null,
               "summary": "Found 1000 open vulnerabilities on the specified
               configuration item",
               "retrieval_date": "2017-09-05 08:56:28"
             }
          ]
      }
   ]
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Create-Response für CI-Ergänzung


```
{
   "success": true,
   "status": "success",
   "payload": {
        "results": [
            {
                "sys_id": "2dfd7c8437201000deeabfc8bcbe5d56",
                "reference_url":
                "http://10.0.214.15:8080/nav_to.do?uri=cmdb_ci.do?sys_id=2dfd7c8437201000
                deeabfc8bcbe5d56",
                    "results": [
                        {
                            "sys_id": "4a8b92fb0b410300263a089b37673a33",
                            "reference_url":
                            "http://10.0.214.15:8080/nav_to.do?uri=sn_sec_cmn_ci_
                        enrichment_result.do?sys_id=4a8b92fb0b410300263a089b37673a33"}
                    ]
                }
            ],
            "domain": "global",
            "configuration_item_ids": [
            "2dfd7c8437201000deeabfc8bcbe5d56"
        ]
    }
}
```


Anwendungsfall zur Ergänzung erkennbarer Elemente

Mit Ihren Drittanbieterskripts können Sie in das Ergebnis der Anreicherung erkennbarer Elemente schreiben [sn_ti_observable_Enrichment_result] Tabelle für Ergänzung erkennbarer Elemente. Die Ergänzungsdatensätze basieren auf vorhandenen Fähigkeiten, die detaillierte Informationen zu einem Datensatz aus einer Drittparteiquelle bereitstellen.

Beispielanforderung und -Antworten für den Anwendungsfall zur Ergänzung erkennbarer Elemente werden hier angezeigt.

Erstellen – Anforderung für Ergänzung erkennbarer Elemente


```
"ignore_mandatory_fields": true,
  "payload": [
    {
      "observable_value": "http://www.google.com",
      "security_incident_ids": [
        "9424d4e10b110300263a089b37673a21"
      ],
      "enrichment_mapping_id": "9fa7d4590b622200263a089b37673a1d",
      "data": [{
        "vendor": "f15a46140b622200263a089b37673a7e",
        "summary": "Registrar:MarkMonitor, Inc., Registration Date:1997-09-15,
            Expiration Date:2020-09-14, Registrant country:UNITED STATES",
        "data_type": "json",
        "retrieval_date": "2017-08-30 10:35:02",
        "raw_data": "{\"WhoisRecord\":{\"administrativeContact\":{\"city\":
            \"Mountain View\",\"country\":\"UNITED STATES\",\"email\":
            \"dns-admin@google.com\",\"fax\":\"16506188571\",\"name\":
            \"DNS Admin\",\"organization\":\"Google Inc.\"}"
      }]
    }
  ]
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Create-Response für Ergänzung erkennbarer Elemente


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "43bd3f210b510300263a089b37673ac6",
                "reference_url": "http://10.0.65.185:8080/sn_ti_observable.do?
                    sys_id=43bd3f210b510300263a089b37673ac6&sys_target=&XML",
                "results": [
                    {
                        "sys_id": "0bbd3f210b510300263a089b37673acc",
                        "reference_url": "http://10.0.65.185:8080/sn_ti_observable_
                            enrichment_result.do?sys_id=0bbd3f210b510300263a089b37673acc
                                &sys_target=&XML"
                    }
                ]
            }
        ],
        "domain": "global",
        "observable_ids": [
            "43bd3f210b510300263a089b37673ac6"
        ]
    }
}
```


Hinweis:
Sie können nicht nur vorhandene Datensätze anreichern, sondern auch verwenden Security Operations Ergänzungsdatenzuordnung Dient zum Hinzufügen neuer Datensätze zu Tabellen durch Übergabe von **Anreicherung_Mapping_ID** Für eine vorhandene Ergänzungszuordnung und eine entsprechende **Rohdaten** Zeichenfolge, die vom Zuordnungsprozess analysiert werden kann.

Anwendungsfall für Bedrohungssuche

Mit Ihren Drittanbieterskripts können Sie in die Tabelle „Bedrohungssuchergebnis“ [sn_ti_LOOKUP_result] für Ergebnisse der Bedrohungssuche schreiben. Die Suchdatensätze basieren auf vorhandenen Fähigkeiten, die detaillierte Informationen zu einem Datensatz aus einer Drittparteiquelle bereitstellen.

Beispielanforderung und -Antworten für den Anwendungsfall „Bedrohungssuche“ werden hier angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen – Anforderung für Bedrohungssuchen


```
{
"simple_response": false,
"include_wrapper": true,
  "ignore_mandatory_fields": false,
  "payload": [
    {
      "request_element_correlation_id": "1",
      "observable_value": "128.214.67.80",
      "data": [
        {
          "request_element_correlation_id": "2",
          "finding": "Malicious6",
          "source_engine": "VirusTotal API",
          "vendor": "aafbf46ad72212007a6de294de6103a2",
          "data_type": null,
          "source": null,
          "name": null,
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        },
        {
          "finding": "Malicious8",
          "source_engine": "VirusTotal API",
          "source_engine_version": "v2",
          "first_found": "2000-09-05 15:56:28",
          "parent": null,
          "retrieval_date": "2017-09-05 08:56:28",
          "external_link": "https://www.virustotal.com/en/ip-address/41.79.173.47/
            information/"
        }
      ]
    }
  ]
}
```


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Create-Response für Bedrohungssuchen


```
{
    "success": true,
    "status": "success",
    "payload": {
        "results": [
            {
                "sys_id": "a0bddafb0b410300263a089b37673a93",
                "reference_url":
                    http://10.0.214.15:8080/nav_to.do?uri=sn_ti_observable.do?sys_id=
                        a0bddafb0b410300263a089b37673a93,
                    "request_element_correlation_id": "1",
                    "results": [
                        {
                            "sys_id": "24bddafb0b410300263a089b37673a95",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?sys
                            _id=24bddafb0b410300263a089b37673a95,
                    "request_element_correlation_id": "2",
                },
                {
                    "sys_id": "e8bddafb0b410300263a089b37673a96",
                    "reference_url":
                        http://10.0.214.15:8080/nav_to.do?uri=sn_ti_lookup_result.do?
                            sys_id=e8bddafb0b410300263a089b37673a96
                            }
                        ]
                    }        ],
                "domain": "global",
                "observable_ids": [
                    "a0bddafb0b410300263a089b37673a93"        ]
    }
}
```


Integrationsfunktionen

Die IntegrationsfunktionenDas Framework bietet eine konsistente Architektur zur Unterstützung der Interoperabilität mit Drittpartei-Integrationen. Diese abstrahierte Schnittstelle und dieses Datenmodell isoliert Integrationen von Änderungen an der Kernanwendung und stellt eine konsistente Experience für ähnliche Integrationstypen sicher.

Jede Integrationsfähigkeit bleibt in der Integrationsfähigkeit erhalten [sn_sec_cmn_Integration_Capability] Tabelle. Integrationsfähigkeits-Flows können nicht allein ausgeführt werden und erfordern den Start eines Implementierungs-Flows. Jedes Plugin, das eine Implementierung der Fähigkeit bereitstellt, fügt ihre Implementierung der untergeordneten Tabelle hinzu: Implementierung der Integrationsfähigkeit [sn_sec_cmn_Integration_Capability_implementation] .

Die Implementierung gibt den auszuführenden Flow, die zugehörige Integration (Plugin-ID) und die Fähigkeit an, die sie implementiert. Diese Flows können mit dem parallelen Flow-Startprogramm parallel ausgeführt werden. Die sequenzielle Ausführung ist jedoch der Standard im Basissystem. Bei Bedarf können Sie dies tun Ändern Sie die Reihenfolge der Ausführung .

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Integration von Security Operations: Fähigkeit zum Blockieren von Anforderungen

Die Blockierungsfunktion blockiert erkennbare Elemente, die einem Security Incident zugeordnet sind, auf einer Firewall, einem Webproxy oder einem anderen Kontrollpunkt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mithilfe von Implementierungs-Flows. Diese Fähigkeit wird bei der Reaktion auf Incidents für Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.

Die Funktion „Anforderung blockieren“ hat einen Flow, Integration Von Security Operations: Block-Anforderungs-Flow, Der die Anforderung zum Blockieren ausführt. Dieser Flow akzeptiert eine Liste erkennbarer Elemente, sucht nach Implementierungsfähigkeiten und führt die Anforderung basierend auf dem konfigurierten Flow aus.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Blockierungsanforderung ausführen

Blockiert die Kommunikation mit erkennbaren Elementen, die einem Security Incident zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

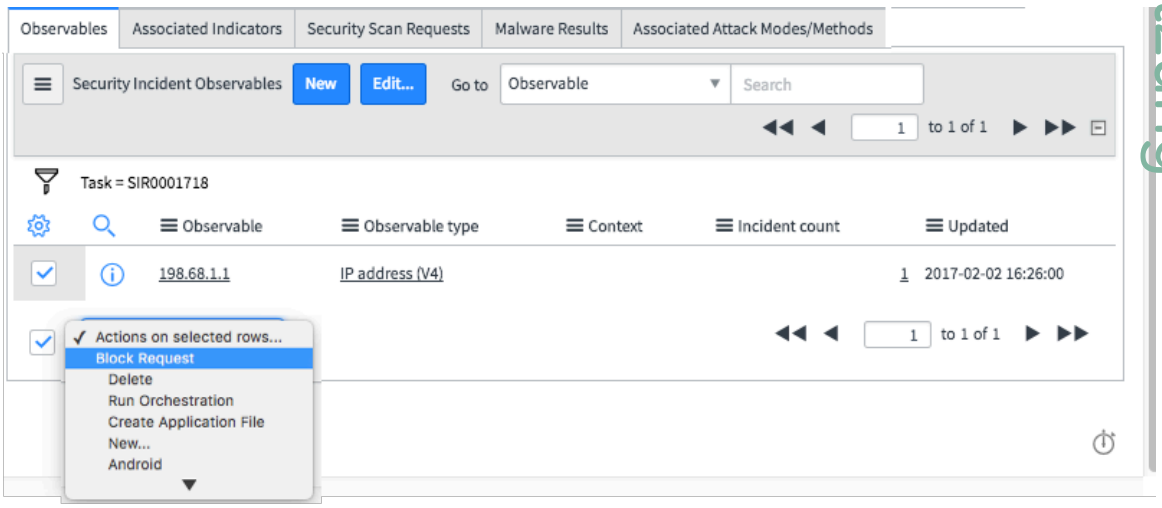
Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Die **Integration Von Security Operations – Anforderung Blockieren** Flow kann über ein Formular für erkennbare Elemente oder über ausgelöst werden **Erkennbare Security Incident-Elemente** Zugehörige Liste zu einem Security Incident.

Dieses Beispiel zeigt eine Blockierungsanforderung aus einem Security Incident.

Prozedur

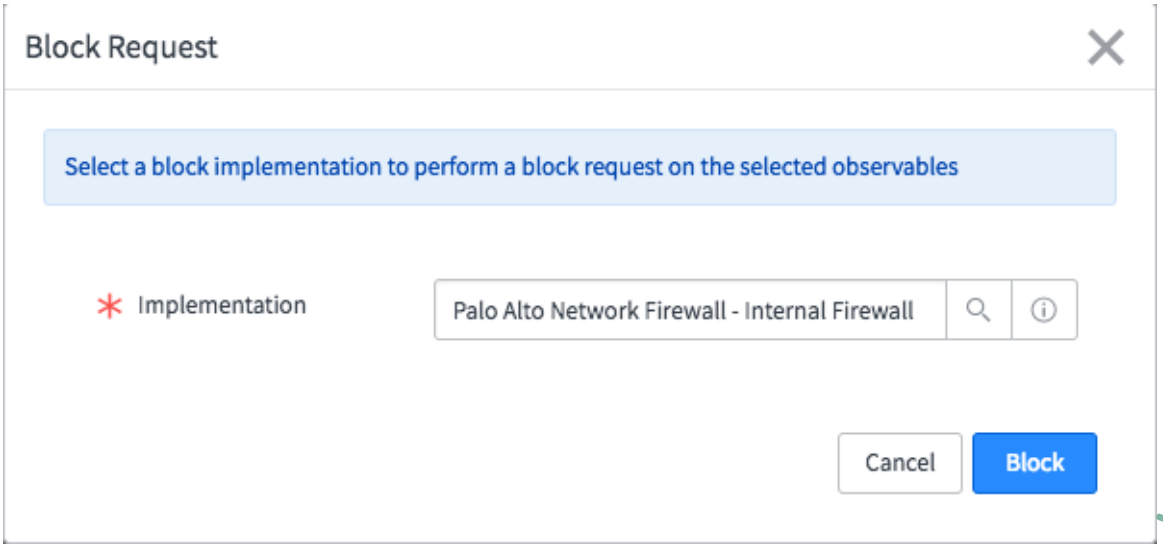
1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie erkennbare Elemente aus dem aus **Zugehörige Liste** Registerkarte.
3. Klicken Sie Auf **Anforderung Blockieren** In **Aktionen für ausgewählte Zeilen...** Dropdown-Menü.



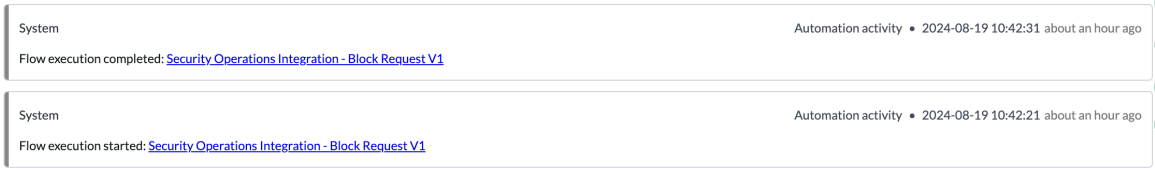
Das Dialogfeld wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Implementierung aus.
5. Klicken Sie Auf **Blockieren** .
   Das Audit der Flow-Ausführung wird im Abschnitt „Arbeitsnotizen“ angezeigt.



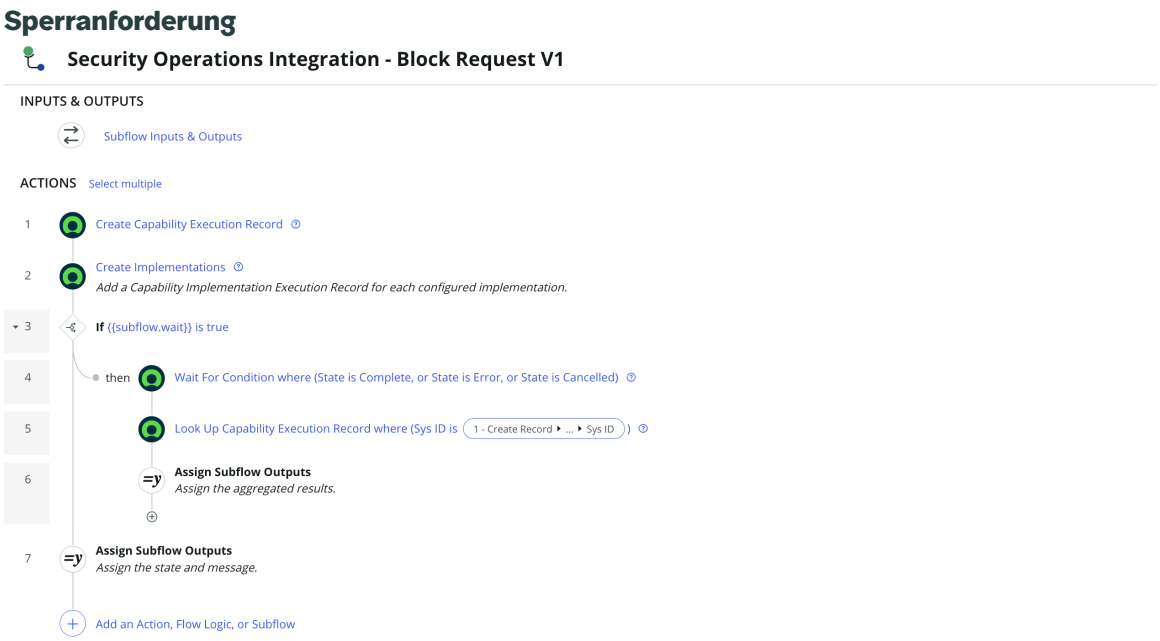
Integration Von Security Operations: Block-Anforderungs-Flow

Der Flow „Security Operations-Integration – Blockanforderung“ ist ein allgemeiner Flow, der unabhängig von Integrationen ist. Blockiert erkennbare Elemente, die einem Security Incident zugeordnet sind. Verwenden Sie es, um eine Integration wie auszuführen Palo Alto Networks – Firewall.

Die **Integration Von Security Operations – Anforderung Blockieren** Flow kann auf einem Formular für erkennbare Elemente oder über ausgelöst werden **Erkennbare Security Incident-Elemente** Zugehörige Liste zu einem Security Incident. In einer Liste befindet sie sich im Dropdown-Aktionsmenü. In einem Formular ist dies ein zugehöriger Link. Das Blockieren einer Anforderung ist nur verfügbar, wenn Sie eine Implementierung für die Funktion zum Blockieren von Anforderungen installiert haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Aktionen, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Integration von Security Operations: Funktion „E-Mail suchen und löschen“

Die Funktion „E-Mail suchen und löschen“ gibt die Anzahl der Bedrohungs-E-Mails aus einer E-Mail-Serversuche zurück und gibt optional Details für jede gefundene E-Mail zurück. Nachdem die E-Mail-Suche abgeschlossen ist, können Sie die E-Mails löschen.

Die Funktion „E-Mail suchen und löschen“ verfügt über einen Flow, der die Prozesse „E-Mail suchen und löschen“ ausführt.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt. Darüber hinaus, wenn keiner von den ist **E-Mail suchen und löschen** Fähigkeitsimplementierungen sind aktiv, die **E-Mail-Suche** Der zugehörige Link zu einem Security Incident wird nicht angezeigt.

Integration von Security Operations – Flow für E-Mail-Suche und -Löschung

Der Flow „Integration von Security Operations – E-Mail-Suche und -Löschung“ gibt die Anzahl der Bedrohungs-E-Mails aus einer E-Mail-Serversuche zurück und gibt optional Details für jede gefundene E-Mail zurück. Nachdem die E-Mail-Suche abgeschlossen ist, können Sie die E-Mails löschen.

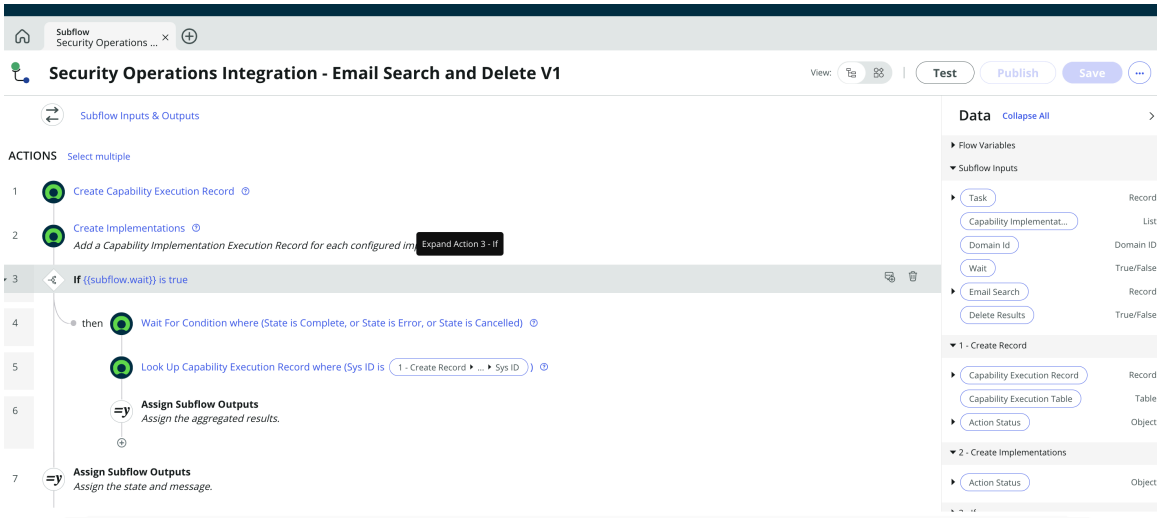
Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Die Suchabfrage kann einige Zeit in Anspruch nehmen. Nachdem die Anzahl empfangen wurde, ist eine Genehmigung erforderlich, um E-Mails von einem E-Mail-Server zu löschen.

Dieser Flow wird durch ausgelöst **Aus E-Mail-Server(n) löschen** Und **E-Mail-Server suchen** Schaltflächen im **E-Mail-Suche** Formular in einem Security Incident. Weitere Informationen finden Sie unter Suchen und löschen Sie Phishing-E-Mails.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

E-Mails suchen und löschen



Aktivitäten, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Die Flow-Prozessaktivitäten umfassen:

Aktion „Beginn der Ausführungsnachverfolgung“ (E-Mail-Suche)

Die Ausführungsaktion „Ausführungsnachverfolgung – Beginnen (E-Mail-Suche)“ erstellt einen Ausführungsnachverfolgungsdatensatz und markiert den Datensatzstatus als gestartet. Diese Aktion wird von allen Fähigkeits- und Implementierungs-Flows verwendet, um ihren Status nachzuverfolgen.

Ergebnisse

Mögliche Ergebnisse für diese Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Ausführungsnachverfolgungsdatensatz wurde erstellt.
Fehler	Ausführungsnachverfolgungsdatensatz konnte nicht erstellt werden.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
capabilityId	Systembezeichner der auszuführenden Integrationsfähigkeit.
Implementierungs-ID	Systembezeichner der Implementierung der Integrationsfähigkeit, die ausgeführt wird.
Aufgaben-ID	Systembezeichner für jede Aufgabe, die dem Flow zugeordnet ist.
flowContextId	Systembezeichner des zugehörigen Flow-Kontextdatensatzes. Vom System bereitgestellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
FlowName	Name des Flows. Vom System bereitgestellt.
ParentCapabilityExcutionId	Systembezeichner des Audit-Datensatzes, der den Implementierungs-Flow gestartet hat. Nur für Implementierungs-Flows der Integrationsfähigkeit erforderlich, z. B. Splunk, Elasticsearch.
E-Mail-Suche-ID	Die sysid des E-Mail-Suchdatensatzes in der Tabelle „E-Mail-Suche“ [sn_sec_cmn_email_search].

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
CapabilityExecutionId	Systembezeichner des Ausführungsnachverfolgungsdatensatzes.

- Aktion „unterstützte Sicherheitsfähigkeiten abrufen“
- Nachverfolgung der Fähigkeitsausführung: Keine Impls-Aktion

Security Operations-Integration: Bereichern Sie die CI-Fähigkeit

Mit der Funktion „CI anreichern“ können Sie Daten für Konfigurationselemente anreichern, die einem Security Incident zugeordnet sind.

Die **Bereichern Sie das CI** Fähigkeit hat einen Flow, Security Operations-Integration – CI-Anreicherungs-Flow. Wenn der Fähigkeits-Flow ausgeführt wird, werden zusätzliche Flows für die aktivierten Implementierungen ausgeführt. Sie können eine Implementierung angeben, die zum Durchführen der Ergänzung der ausgewählten CIs verwendet werden soll, oder Sie können die Ergänzung mit allen Implementierungen durchführen.

Hinweis:
Diese angereicherten Daten sind nicht die Art von Daten, die Sie in Ihrer CMDB speichern möchten, da es sich um forensische Daten handelt, die spezifisch für eine bestimmte Untersuchung sind – z. B. das Durchführen eines Memdumps von einem CI. Stattdessen werden die Daten in der Tabelle „Konfigurationselementanreicherung“ [sn_sec_cmn_ci_Enrichment_result] gespeichert.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Security Operations-Integration – CI-Anreicherungs-Flow

Mit dem Flow „Integration von Security Operations – CI-Anreicherung“ können Sie Daten in Konfigurationselementen (CI) anreichern, die einem Security Incident zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

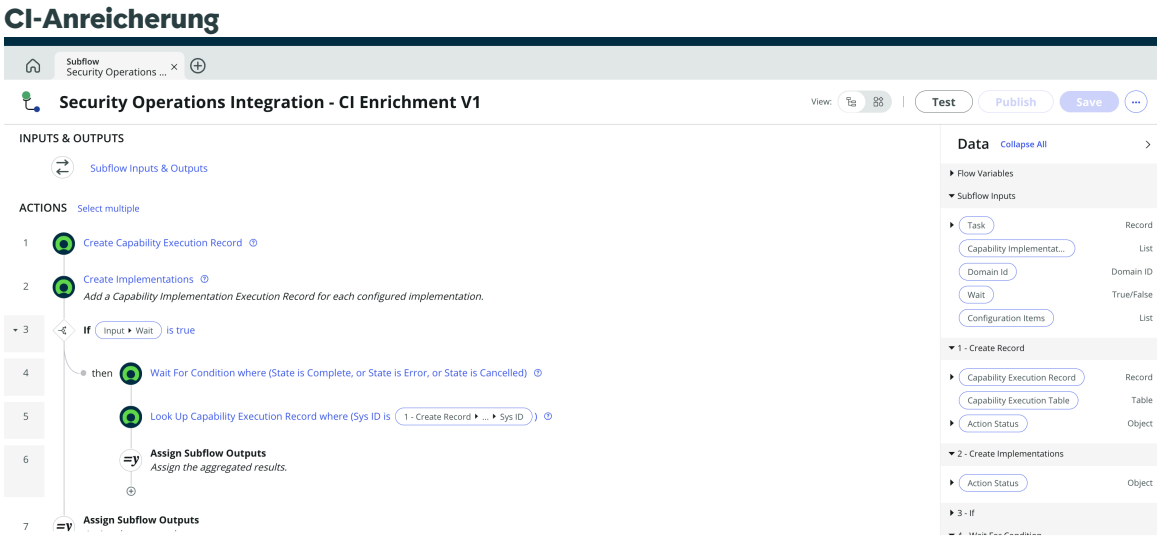
Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird von ausgelöst Security Incident Response Auf zwei Arten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Indem Sie mindestens ein CIs aus dem auswählen **Konfigurationselemente** Registerkarte (unter **Betroffene Elemente** Zugehöriger Link) und auswählen **CI-Ergänzung ausführen** Von **Aktionen für ausgewählte Zeilen** Auswahlliste.
- Indem Sie einen CI-Datensatz öffnen und auf klicken **CI-Ergänzung ausführen** Zugehöriger Link.

Mit beiden Methoden können Sie dann angeben, welche Implementierungen zum Anreichern der ausgewählten CIs verwendet werden sollen. Die zugehörigen Implementierungs-Flows werden ausgeführt, um die Ergänzung durchzuführen.

Hinweis:
Das Basissystem enthält keinen Implementierungs-Flow für diese Fähigkeit. Zum Anreichern von CIs müssen Sie eine eigene Implementierung erstellen Flow .



Aktionen, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Die Flow-Prozessaktionen umfassen:

- Ausführungsnachverfolgung: Flow-Aktion Starten
- Security Operations-Integration – CI-Anreicherungs-Flow
- Nachverfolgung der Fähigkeitsausführung: Keine Impls-Aktion
- Aktion „unterstützte Sicherheitsfähigkeiten abrufen“

Integration von Security Operations: Bereichern Sie die Fähigkeit erkennbarer Elemente

Mit der Fähigkeit „erkennbare Elemente anreichern“ können Sie erkennbare Elemente mithilfe von Implementierungs-Flows mit zusätzlichen Informationen aus einer Vielzahl von Quellen anreichern. Diese Fähigkeit wird bei der Reaktion auf Incidents für Untersuchungen verwendet, um eine identifizierte Bedrohung einzudämmen.

Die Fähigkeit „erkennbares Element anreichern“ hat einen Flow, Integration von Security Operations – Flow für erkennbare Elemente anreichern. Wenn der Fähigkeits-Flow ausgeführt wird, werden zusätzliche Flows für die aktivierten Implementierungen ausgeführt. Sie können eine Implementierung angeben, die verwendet werden soll, um die ausgewählten erkennbaren Elemente zu ergänzen, oder Sie können die Ergänzung mit allen Implementierungen durchführen, die den unterstützten erkennbaren Elementen entsprechen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Integration von Security Operations – Flow für erkennbare Elemente anreichern

Mit dem Subflow „Security Operations-Integration – erkennbare Elemente anreichern“ können Sie erkennbare Elemente mit dem Implementierungs-Flow Designer mit zusätzlichen Informationen aus einer Vielzahl von Quellen anreichern.

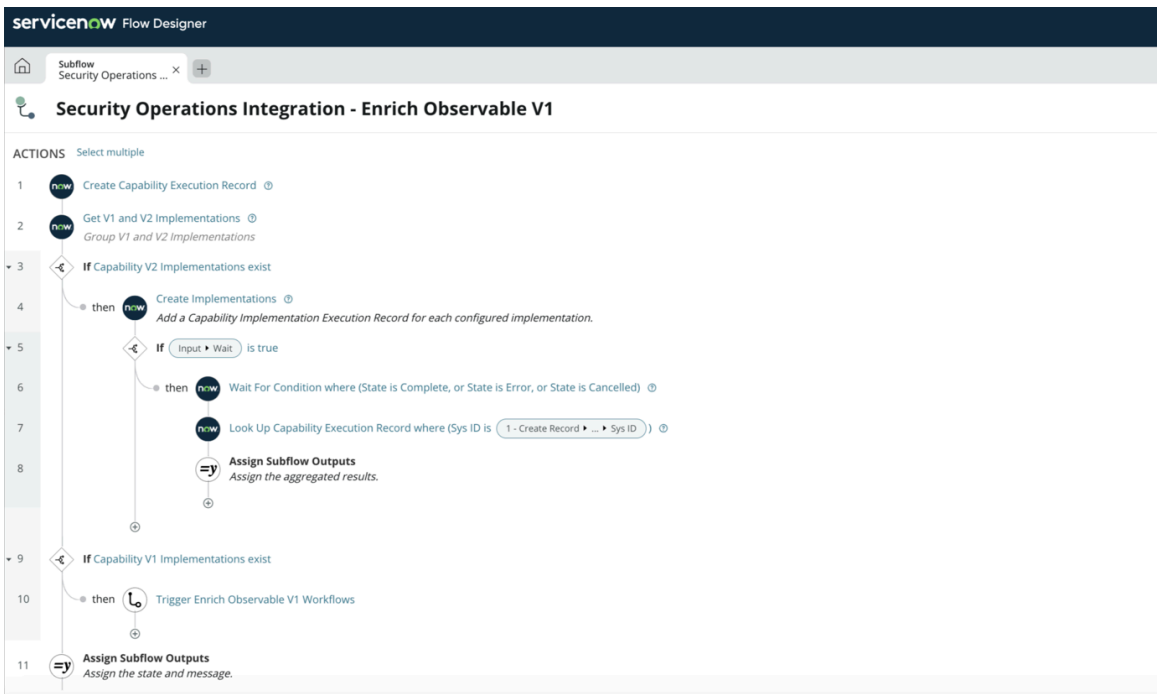
Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow kann von beiden ausgelöst werden Security Incident Response Oder Threat Intelligence Auf zwei Arten.

- Indem Sie ein oder mehrere erkennbare Elemente aus der Liste erkennbarer Elemente auswählen und auswählen **Ergänzung erkennbarer Elemente ausführen** Von **Aktionen für ausgewählte Zeilen** Auswahlliste.
- Indem Sie einen Datensatz eines erkennbaren Elements öffnen und auf klicken **Ergänzung erkennbarer Elemente ausführen** Zugehöriger Link.

Mit beiden Methoden können Sie dann angeben, welche Implementierungen zum Anreichern der ausgewählten erkennbaren Elemente verwendet werden sollen. Die zugehörigen Implementierungs-Flows werden ausgeführt, um die Ergänzung durchzuführen.

Erkennbares Element ergänzen



Aktionen, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Die Flow-Prozessaktionen umfassen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Nachverfolgung der Fähigkeitsausführung: Keine Impls-Aktion
- Aktion „unterstützte Sicherheitsfähigkeiten abrufen“Nachverfolgung der Fähigkeitsausführung: Keine Impls-Aktion

Integration von Security Operations: Fähigkeit zum Abrufen von Netzwerkstatistiken

Die Funktion „Netzwerkstatistiken abrufen“ ruft eine Liste aktiver Netzwerkverbindungen von einem Host oder Endpunkt ab. Sie kann für die Ergänzung von Incidents während Untersuchungen verwendet werden. Diese Fähigkeit wird automatisch ausgelöst, wenn einem Security Incident ein Konfigurationselement hinzugefügt wird.

Die **Rufen Sie Netzwerkstatistiken Ab** Fähigkeit hat einen Flow, Security Operations-Integrationen – Flow „Netzwerkstatistiken abrufen“ Die ein oder mehrere CIs und Aufgaben akzeptiert. Der Flow iteriert über jede Implementierung und jedes CI und ruft den Implementierungs-Flow erneut auf.

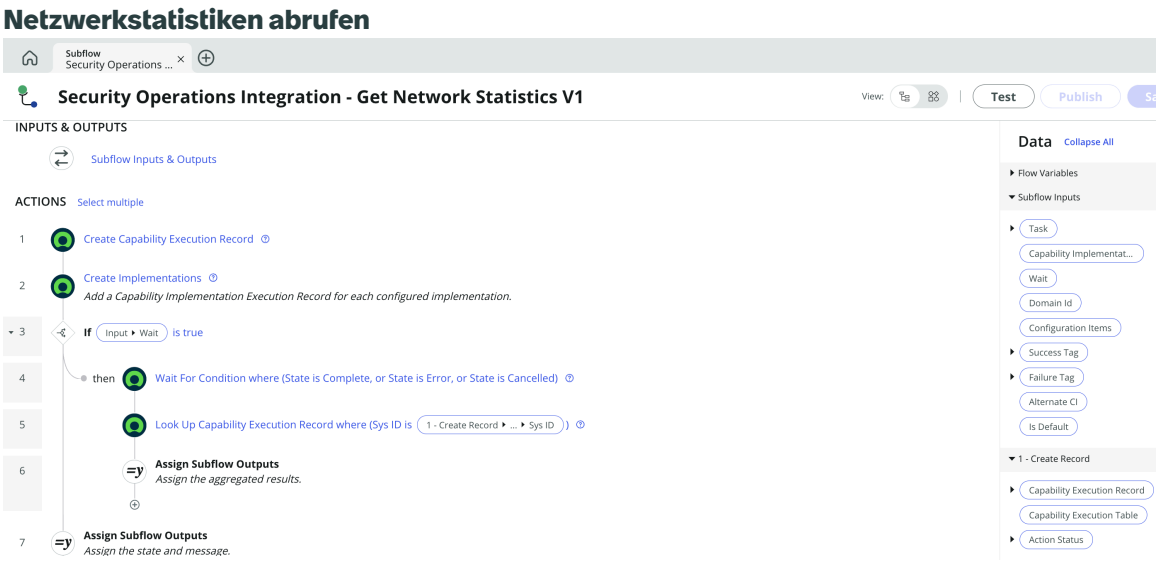
Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Security Operations-Integrationen – Flow „Netzwerkstatistiken abrufen“

Der Flow „Security Operations Integrations – Netzwerkstatistiken abrufen“ ruft eine Liste aktiver Netzwerkverbindungen von einem Host oder Endpunkt ab.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird automatisch ausgeführt, wenn einem Security Incident ein Konfigurationselement hinzugefügt wird.



Aktionen, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Die Flow-Aktionen umfassen:

- Fähigkeit: CIs-Aktivität bestimmen
-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

an.

Ausführungsnachverfolgung – Begin (CIs) Flow-Aktion

Die **Ausführungsnachverfolgung – Begin (CIs)** Flow-Aktion startet den Auditprozess für einen Security Operations Integrations-Flow, der für Konfigurationselemente (Configuration Items, CIs) ausgeführt wird.

Die **Ausführungsnachverfolgung – Begin (CIs)** Die Flow-Aktion kann mit jedem CI-Flow verwendet werden, um mit der Aufzeichnung des Fortschritts des Flows in einem Audit zu beginnen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Ein Audit-Datensatz wird erstellt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
capabilityId	Systembezeichner der auszuführenden Integrationsfähigkeit.
IsImpl	Kennzeichnung, die angibt, ob ein Audit für einen Integrationsfähigkeits-Flow oder einen Implementierungs-Flow für Integrationsfähigkeiten durchgeführt wird. Mögliche Werte: • Falsch: Bezeichnet Audits für einen abstrakten Integrationsfähigkeits-Flow, z. B. Sichtungssuche. (Standard.) • „Wahr“: Bezeichnet das Auditing eines Implementierungs-Flows der Integrationsfähigkeit. Zum Beispiel Splunk oder Elasticsearch.
Aufgaben-ID	Systembezeichner für jede Aufgabe, die dem Flow zugeordnet ist.

CiList	Ein oder mehrere Konfigurationselemente (Configuration Items, CI), für die die gewünschte Aktion ausgeführt werden soll, im folgenden Format:
	`["sysId", "sysId"]`
	oder
	`"sysId"`
	Wird als Flow-Eingabe verwendet.

flowContextId	Systembezeichner des zugehörigen Flow-Kontextdatensatzes. Vom System bereitgestellt.
FlowName	Name des Flows. Vom System bereitgestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
ParentCapabilityExcutionId	Systembezeichner des Audit-Datensatzes, der den Implementierungs-Flow gestartet hat. Nur erforderlich für Implementierungs-Flows der Integrationsfähigkeit wie Splunk, Elasticsearch.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
CapabilityExecutionId	Systembezeichner des Audit-Datensatzes.

Die Flow-Prozessaktionen umfassen:

- Aktion „unterstützte Sicherheitsfähigkeiten abrufen“
- Nachverfolgung der Fähigkeitsausführung: Keine Impls-Aktion

Security Incident Response: Flow „Netzwerkstatistiken abrufen“

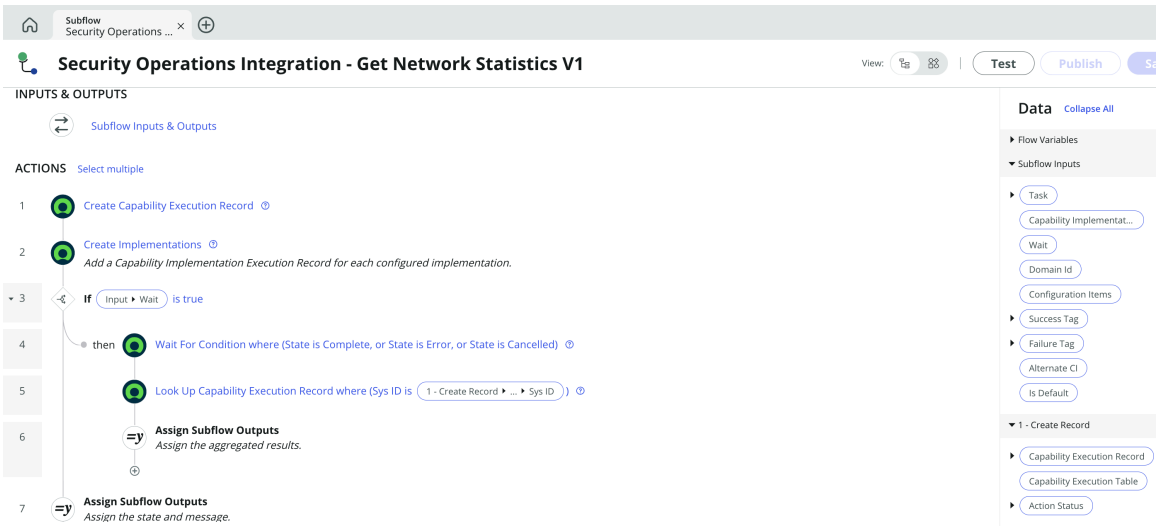
Die zugehörigen Listen namens **Security Incident Response** > **Netzwerkstatistiken abrufen** Flow ruft die Netzwerkstatistiken für eine betroffene Windows-basierte Ressource ab, wenn sie einem Security Incident in hinzugefügt wird **Analyse** status.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Bei neuen Security Incidents, die Konfigurationselemente enthalten, wird der Flow automatisch ausgeführt, wenn sich der Status in ändert **Analyse** .

Vorhandene Security Incidents werden automatisch aktualisiert, wenn Sie sich in befinden **Analyse** status, und Sie fügen ein neues Konfigurationselement hinzu.

Netzwerkstatistiken abrufen



Die Flow-Prozessaktionen umfassen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

FQDN-Flow-Aktion für Konfigurationselement abrufen

Shell-Skript nach Betriebssystem bestimmen

Wenn-Anweisung von Powershell ausgeführt wird

Ausführungsnachverfolgung: Flow-Aktion Starten

Rufen Sie Netzwerkstatistiken über die netstat-Flow-Aktion ab

Nachverfolgung Der Fähigkeitsausführung: Fehler-Flow-Aktion

Flow-Aktion „Ergänzungsdatensätze erstellen“

Nachverfolgung Der Fähigkeitsausführung: Fehler-Flow-Aktion – Gibt die Ergänzungs-ID zurück.

Nachverfolgung Der Fähigkeitsausführung: Flow-Aktion Abschließen

Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie **Status** Bis **Analyse** , Falls erforderlich.
3. Fügen Sie ein Konfigurationselement (Computer, Server oder Ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response Orchestration Stellt Informationen zur Netzwerkstatistik in bereit **Zugehörige Links** > **Anreicherungen Von Security Incidents** Registerkarte Weitere Informationen finden Sie unter Security Operations Ergänzungsdatenzuordnung.

Aktionen, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Integration von Security Operations: Fähigkeit zum Abrufen laufender Prozesse

Mit der Fähigkeit „Laufende Prozesse abrufen“ wird eine Liste der laufenden Prozesse für ein Configuration Item (CI) von einem Host oder Endpunkt abgerufen. Diese Funktion wird bei Untersuchungen zur Ergänzung von Incidents verwendet.

Die Fähigkeit „laufende Prozesse abrufen“ hat zwei Implementierung Flows:

- Security Operations Carbon Black-Integration – Flow Für Laufende Prozesse Abrufen
- Integration von Security Operations-Systembefehlen: Flow „laufende Prozesse abrufen“

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Aktionen, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

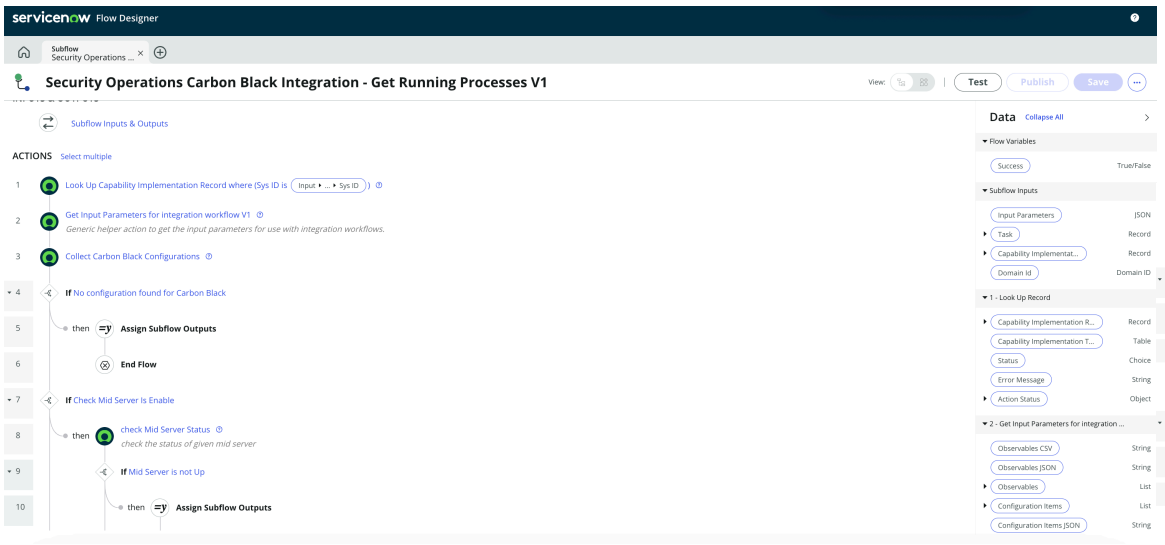
Security Operations Carbon Black-Integration – Flow Für Laufende Prozesse Abrufen

Die Carbon Black-Integration von Security Operations – laufende Prozesse abrufen ist die Implementierung für die Carbon Black-Integration, die vom Flow „Security Operations Integration – laufenden Prozess abrufen“ gestartet wird.

Erforderliche Rolle: sn_si.Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Carbon Black – Laufende Prozesse Abrufen



Aktionen, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Flow-Aktion „Carbon Black-Konfigurationen Erfassen“

Die Flow-Aktion Carbon Black-Konfigurationen erfassen erfasst Konfigurationsinformationen, die im Flow verwendet werden sollen.

Die Flow-Aktion Carbon Black-Konfigurationen erfassen erfasst Carbon Black-Konfigurationsinformationen, die im Flow verwendet werden sollen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Konfiguration erfolgreich.
Fehler	Beim Versuch, die Konfiguration zu verifizieren, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Für diese Flow-Aktion sind keine Eingabevariablen vorhanden.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
endpoint_base	Basis-URL der Drittanbieter-Integrations-API.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen (Fortsetzung)

Variable	Beschreibung
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.
api_token	API-Schlüssel für Drittpartei-Integration.

Überprüfen Sie den MID-Server-Status

Bestimmt, ob der MID-Server in identifiziert wurde **MID-Server-Host** Das Feld der Konfiguration der Integration ist gestartet und wird ausgeführt. Wenn das Feld auf festgelegt ist **Beliebig** , Die Flow-Aktion überprüft, ob ein MID-Server aktiv ist und ausgeführt wird.

Die Flow-Aktion „MID-Serverstatus überprüfen“ kann mit jedem Flow verwendet werden, um zu überprüfen, ob ein laufender MID-Server im Flow vorhanden ist.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sitzungsstatus zurückgegeben.
Fehler	Sitzungsstatusfehler. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
CapabilityExecutionId	Die ID der ausgeführten Fähigkeit.
FlowName	Der Name des ausgeführten Flows.
Mid_Server_Host	Der in der Konfiguration i der Integration identifizierte MID-Server

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Mid_Server_Live	Gibt an, ob der MID-Server in identifiziert wurde **MID-Server-Host** Das Feld der Konfiguration der Integration ist gestartet und wird ausgeführt. Wenn das Feld auf festgelegt ist **Beliebig** , Die Flow-Aktion überprüft, ob ein MID-Server aktiv ist und ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flow-Aktion für Sensor-ID abrufen

Die Flow-Aktion „Sensor-ID abrufen“ erfasst Sensorbezeichner, die im Flow verwendet werden sollen.

Die Flow-Aktion „Sensor-ID abrufen“ kann mit jedem Flow verwendet werden, um Sensorinformationen zur Verwendung im Flow zu sammeln.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sensorbezeichner gefunden.
Fehler	Keine Sensoren gefunden. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.
endpoint_base	Basis-URL der Carbon Black-API.
ci_ip_address	IP-Adresse des Konfigurationselements.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Bestimmt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt.
Array-Elementtyp	API-Variablen.
sensor_detail	Beschreibung des Carbon Black-Sensors im JSON-Format.

Flow-Aktion Für Sitzung Erstellen

Die Flow-Aktion Sitzung erstellen richtet eine Carbon Black-Sitzung ein, die im Flow verwendet werden soll.

Die Flow-Aktion Sitzung erstellen kann mit jedem Flow verwendet werden, um eine Carbon Black-Sitzung innerhalb des Flows zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sitzung erstellt.
Fehler	Sitzung nicht erstellt. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
endpoint_base	Basis-URL der Carbon Black-API.
sensor_id	Sensorbezeichner.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Bestimmt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt.
Ausgabe	API-Variablen

Flow-Aktion „Sitzungsstatus Überprüfen“

Bestimmt den Status einer Carbon Black-Sitzung innerhalb des Flows.

Die Flow-Aktion Sitzungsstatus überprüfen kann mit jedem Flow verwendet werden, um den Carbon Black-Sitzungsstatus innerhalb des Flows zu überprüfen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sitzungsstatus zurückgegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse (Fortsetzung)

Ergebnis	Beschreibung
Fehler	Sitzungsstatusfehler. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
endpoint_base	Basis-URL der Carbon Black-API.
session_id	Sitzungsbezeichner.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Bestimmt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt.
Ausgabe	Informationen zu laufenden Carbon Black-Prozessen.

Flow-Aktion Für Befehlsprozess Erstellen

Mit der Flow-Aktion Befehlsprozess erstellen wird ein Carbon Black-Befehlsprozess erstellt, der im Flow verwendet werden soll.

Die Flow-Aktion „Befehlsprozess erstellen“ kann mit jedem Flow verwendet werden, um einen Carbon Black-Befehlsprozess innerhalb des Flows zu erstellen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Befehlsprozess erstellt.
Fehler	Befehlsprozess nicht erstellt. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
endpoint_base	Basis-URL der Carbon Black-API.
session_id	Sitzungsbezeichner.
command_id	Befehlsbezeichner.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Bestimmt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt.
Ausgabe	API-Variablen

Überprüfen Sie den Befehlsstatus, und rufen Sie die Prozess-Flow-Aktion ab

Überprüft den Carbon Black-Befehlsstatus und ruft Prozesse ab, die im Flow verwendet werden sollen.

Die Aktion „Befehlsstatus überprüfen“ und „Prozess-Flow abrufen“ können mit jedem Flow verwendet werden, um einen Carbon Black-Befehlsstatus zu überprüfen und Prozesse innerhalb des Flows abzurufen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Befehlsstatus zurückgegeben und Prozesse erstellt.
Fehler	Befehlsstatus- oder Prozessfehler. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
endpoint_base	Basis-URL der Carbon Black-API.
session_id	Sitzungsbezeichner.
command_id	Befehlsbezeichner.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Bestimmt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt.
Ausgabe	API-Variablen

Datenflussaktion „Prozesse Zuordnen“

Die Flow-Aktion „Prozessdaten zuordnen“ ordnet Carbon Black-Prozessdaten innerhalb des Flows zu.

Die Flow-Aktion Prozesse zuordnen kann mit jedem Flow verwendet werden, um Carbon Black-Prozesse zuzuordnen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Prozesse zugeordnet
Fehler	Prozesse nicht zugeordnet. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
Betroffen_ci	Betroffenes Konfigurationselement.
Implementierungs-ID	Implementierungsbezeichner.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ausgabe	Formatierte Rückgabedaten für laufende Prozesse, die vom abstrakten Workflow verwendet werden.
Prozesse	Liste der Prozesse in einem Array.

Nachverfolgung Der Fähigkeitsausführung: Flow-Aktion Abschließen

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Abschließen“ aktualisiert den Audit-Datensatz, wenn der Flow abgeschlossen ist.

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Abgeschlossen“ kann mit jedem Flow verwendet werden, um den Abschluss des Flows aufzuzeichnen.

Hinweis:
Die **Rückgabewert** Array aus dem **Paralleler Startprogramm** Die Core-Flow-Aktion enthält ein Array von Ergebnissen aller ausgeführten Integrations-Flows und fordert den erfolgreichen Abschluss der Ausführungsnachverfolgung auf.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Der Status des Audit-Datensatzes wird auf aktualisiert **Abgeschlossen** .

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
CapabilityExecutionId	Systembezeichner für den Audit-Datensatz. Dieses Feld war die Ausgabe einer der Aktivitäten zum Starten des Audits.
FlowName	Name des Flows. Vom System bereitgestellt.
Nachricht	Abschlussnachricht.

Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

Flow-Aktion „Sitzung Schließen“

Schließt eine Carbon Black-Sitzung innerhalb des Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Aktivität „Sitzung schließen“ kann mit jedem Flow verwendet werden, um eine Carbon Black-Sitzung zu schließen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sitzung geschlossen.
Fehler	Sitzung nicht geschlossen. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
endpoint_base	Basis-URL der Carbon Black-API.
session_id	Sitzungsbezeichner.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Bestimmt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt.
Ausgabe	API-Variablen

Integration von Security Operations-Systembefehlen: Flow „laufende Prozesse abrufen“

Der Flow „Integration von Security Operations-Systembefehlen – laufende Prozesse abrufen“ ruft die laufenden Prozesse eines Konfigurationselements ab, wenn er einem Windows- oder Unix-basierten Security Incident in hinzugefügt oder aktualisiert wird **Analyse** status.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Bei neuen Security Incidents wird der Flow automatisch ausgeführt, wenn Sie den Incident mit einem ausgewählten Konfigurationselement übermitteln, wenn sich der Status

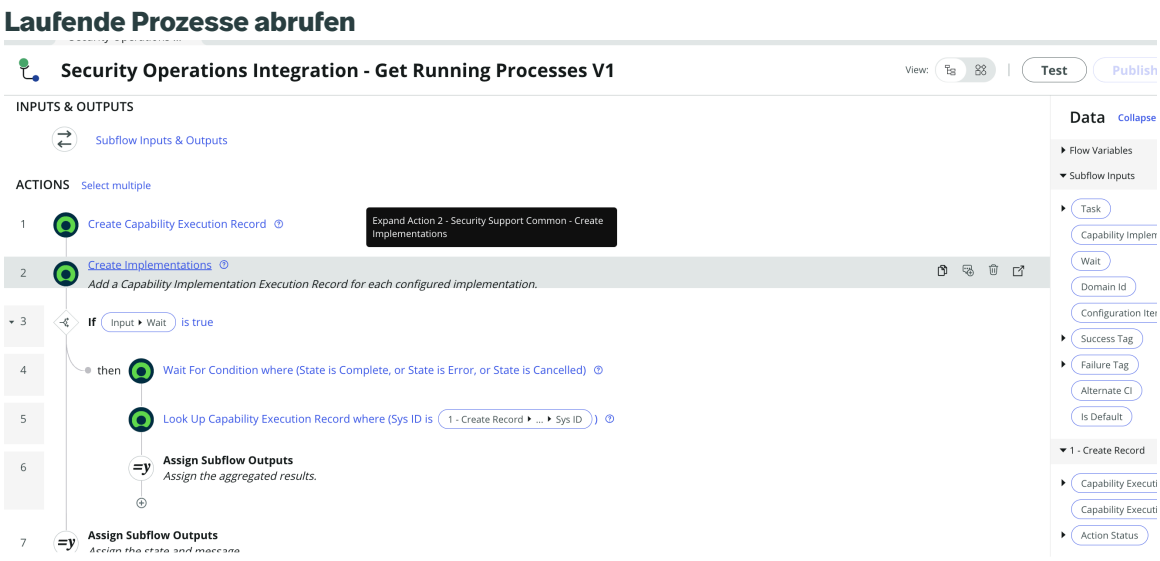
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

automatisch in ändert **Analyse** . Wenn es in verbleibt **Entwurf** status, dann wird er nicht ausgeführt.

Vorhandene Security Incidents werden automatisch aktualisiert, wenn Sie sich in befinden **Analyse** status, und Sie fügen ein neues Konfigurationselement hinzu.

Die Flow-Prozessaktionen umfassen:

- FQDN-Flow-Aktion für Konfigurationselement abrufen
- Bestimmen Sie das Shell-Skript nach BS-Aktivität
- Ausführungsnachverfolgung: Flow-Aktion Starten
- Laufende Prozesse über PowerShell abrufen
- Shell-Skriptaktivität ausführen
- Nachverfolgung Der Fähigkeitsausführung: Fehler-Flow-Aktion
- Shell-Skript aus MID-Skriptaktivität extrahieren
- Ergebnisse Kombinieren Und geben Werte in einem Array zurück
- Flow-Aktion „Ergänzungsdatensätze erstellen“
- Nachverfolgung Der Fähigkeitsausführung: Flow-Aktion Abschließen



Prozedur

1. Öffnen Sie einen Security Incident.
2. Aktualisieren Sie **Status** Bis **Analyse** , Falls erforderlich.
3. Fügen Sie ein Konfigurationselement (Computer, Server oder Ähnliches) hinzu.
4. Klicken Sie auf **Aktualisieren**.
   Security Incident Response Orchestration Stellt Informationen zum laufenden Prozess in bereit **Zugehöriger Link** > **Anreicherungen Von Security Incidents**Registerkarte Weitere Informationen finden Sie unter Security Operations Ergänzungsdatenzuordnung.

   Aktionen, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisaktivität kombinieren

Die Workflow-Aktivität „Ergebnisse kombinieren“ führt die Ergebnisse aus Drittpartei-Integrationen zusammen, um sie im Workflow zu verwenden.

Die Aktivität „Ergebnisse kombinieren“ kann mit jedem Workflow verwendet werden, um ein MID-Server-Shell-Skript im Workflow auszuführen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Ergebnisse kombiniert.
Fehler	Kombination fehlgeschlagen. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
Eingabe A	Ergebnissatz A
Eingabe B	Ergebnissatz B
Implementierungs-ID	Implementierungsbezeichner.
Betroffen_ci	Konfigurationselement

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ergebnis	Ergebnissatz A oder Ergebnissatz B, basierend auf dem einer ausgefüllt wird.

Shell-Skriptaktivität ausführen

Die Workflow-Aktivität „Shell-Skript ausführen“ führt ein MID-Server-Shell-Skript innerhalb des Workflows aus.

Die Aktivität „Shell-Skript ausführen“ kann mit jedem Workflow verwendet werden, um ein MID-Server-Shell-Skript im Workflow auszuführen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Shell-Skript gefunden
Fehler	Kein Shell-Skript gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
Ziel	IP oder vollqualifizierter Domänenname (FQDN) des Ziel-CI.
ScriptValue	Skript als Zeichenfolgenwert, das auf einem Unix-System ausgeführt wird.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response	Rohausgabe. Daten laufender Prozesse.

Shell-Skript aus MID-Skriptaktivität extrahieren

Die Workflow-Aktivität „Shell-Skript aus MID-Skript extrahieren“ ruft ein MID-Server-Shell-Skript ab, das im Workflow verwendet werden soll.

Die Aktivität Shell-Skript aus MID-Skript extrahieren kann mit jedem Workflow verwendet werden, um ein MID-Server-Shell-Skript zu extrahieren, das in den Workflow aufgenommen werden soll.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Shell-Skript gefunden
Fehler	Kein Shell-Skript gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
sysId	Systembezeichner

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
ScriptValue	Skript als Zeichenfolgenwert, das auf einem Unix-System ausgeführt wird.

Ruft laufende Prozesse über PowerShell-Aktivität ab

Die Workflow-Aktivität „Sensor-ID abrufen“ erfasst laufende Prozesse mit PowerShell zur Verwendung im Workflow.

Die Workflow-Aktivität „laufende Prozesse über PowerShell abrufen“ kann mit jedem Workflow verwendet werden, um Prozesse abzurufen, die in den Workflow aufgenommen werden sollen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Prozesse gefunden
Fehler	Keine Prozesse gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
Ziel	IP oder vollqualifizierter Domänenname (FQDN) des Ziel-CI.
ProcessingScript	ECC-Skript wird auf einem Windows-basierten System ausgeführt.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response	Rohausgabe. Daten laufender Prozesse.

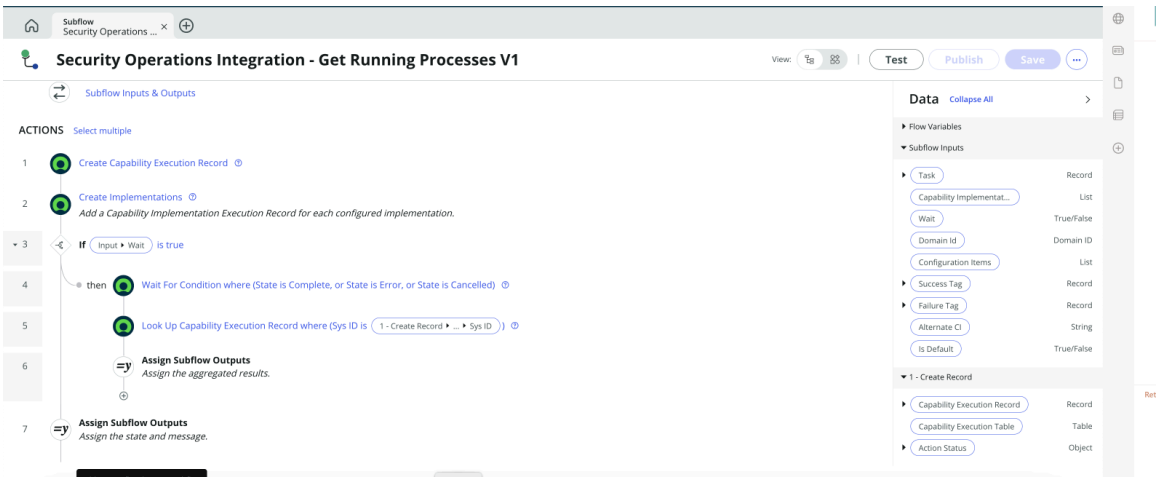
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Security Operations – Flow „Laufende Prozesse Abrufen“

Der Flow „Security Operations – laufende Prozesse abrufen“ ist ein allgemeiner Flow, der unabhängig von Integrationen ist. Ruft eine Liste der laufenden Prozesse für ein Konfigurationselement (Configuration Item, CI) von einem Host ab. Verwenden Sie es, um eine Integration wie Carbon Black oder für einen Windows-basierten Security Incident auszuführen.

Erforderliche Rolle: sn_si.Analyst

Laufende Prozesse abrufen



Aktivitäten, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Integration von Security Operations: Fähigkeit zum Isolieren des Hosts

Die **Host Isolieren** Die Fähigkeit schränkt Systemverbindungen zu anderen Geräten ein. „Host isolieren“ wird für ein Konfigurationselement (CI) ausgeführt.

Die **Host Isolieren** Fähigkeit hat einen Flow, Sicherheitsvorgänge: Host-Flow Isolieren Die ein oder mehrere CIs und optional eine Implementierung akzeptiert. Sie können eine Implementierung angeben, die zum Isolieren des Hosts verwendet werden soll, oder für den Flow, um zu versuchen, den Host mit allen Implementierungen zu isolieren.

Hinweis:
Obwohl nicht in eine Fähigkeit integriert, ein Flow, Security Operations Carbon Black-Integration: Flow Zum Entfernen Der Host-Isolation Ist für Orchestration verfügbar, um die Kommunikation mit einem isolierten Host wiederherzustellen.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Führen Sie „Host Isolieren“ Aus

Host Isolieren Schränkt Systemverbindungen zu anderen Geräten ein.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

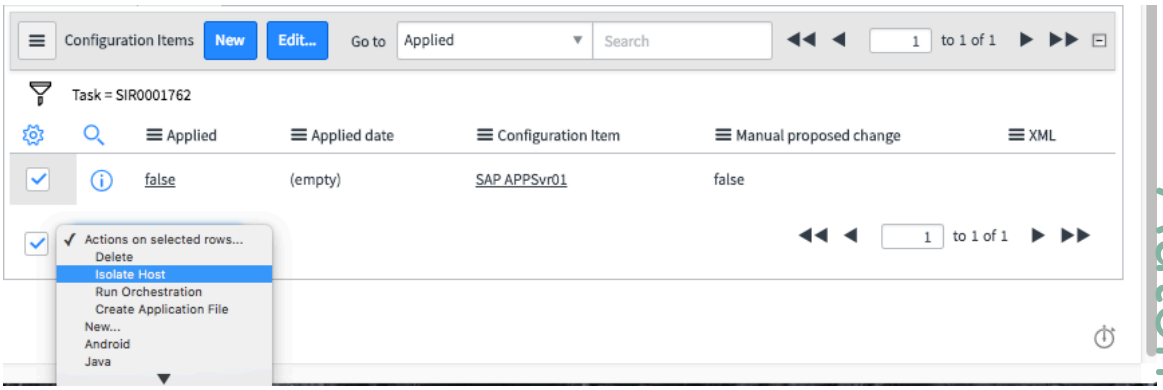
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

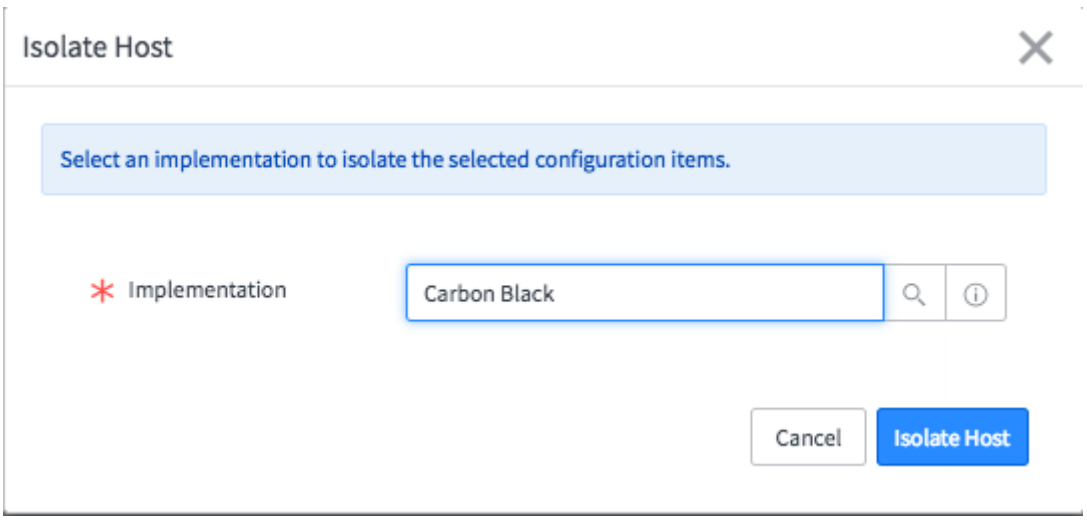
Die **Integration von Security Operations: Host oder Endpunkt isolieren** Flow kann über die zugehörige Liste eines Security Incidents ausgelöst werden.

Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie Aus **Konfigurationselemente** Von **Zugehörige Liste** Registerkarte.
3. Klicken Sie Auf **Host Isolieren** In **Aktionen für ausgewählte Zeilen...** Dropdown-Menü.



Das Dialogfeld wird angezeigt.



4. Wählen Sie die Implementierung aus.
5. Klicken Sie Auf **Host Isolieren** .
   Das Audit der Flow-Ausführung wird im Abschnitt „Arbeitsnotizen“ angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

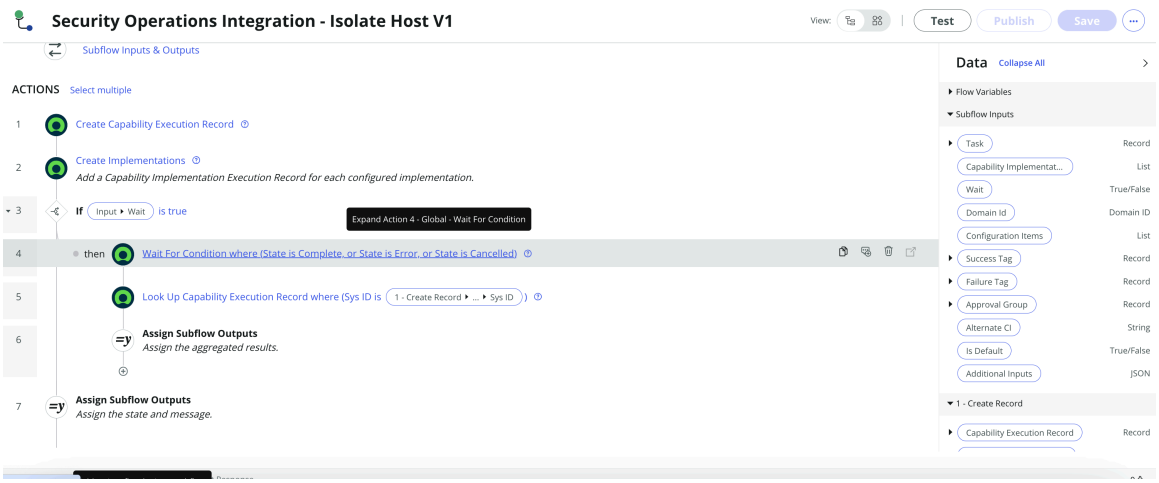
Sicherheitsvorgänge: Host-Flow Isolieren

Die **Sicherheitsvorgänge: Host Isolieren** Flow ist ein allgemeiner Flow, der unabhängig von Integrationen ist. Es verwendet die konfigurierten Abfragen, um nach einer Reihe von Konfigurationselementen zu suchen. Verwenden Sie es, um eine Integration wie Carbon Black zu erfüllen.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow wird von ausgelöst **Konfigurationselemente** Registerkarte in einer zugehörigen Liste „Security Incident“.

Host isolieren



Aktivitäten, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Security Operations Carbon Black-Integration – Host-Flow Isolieren

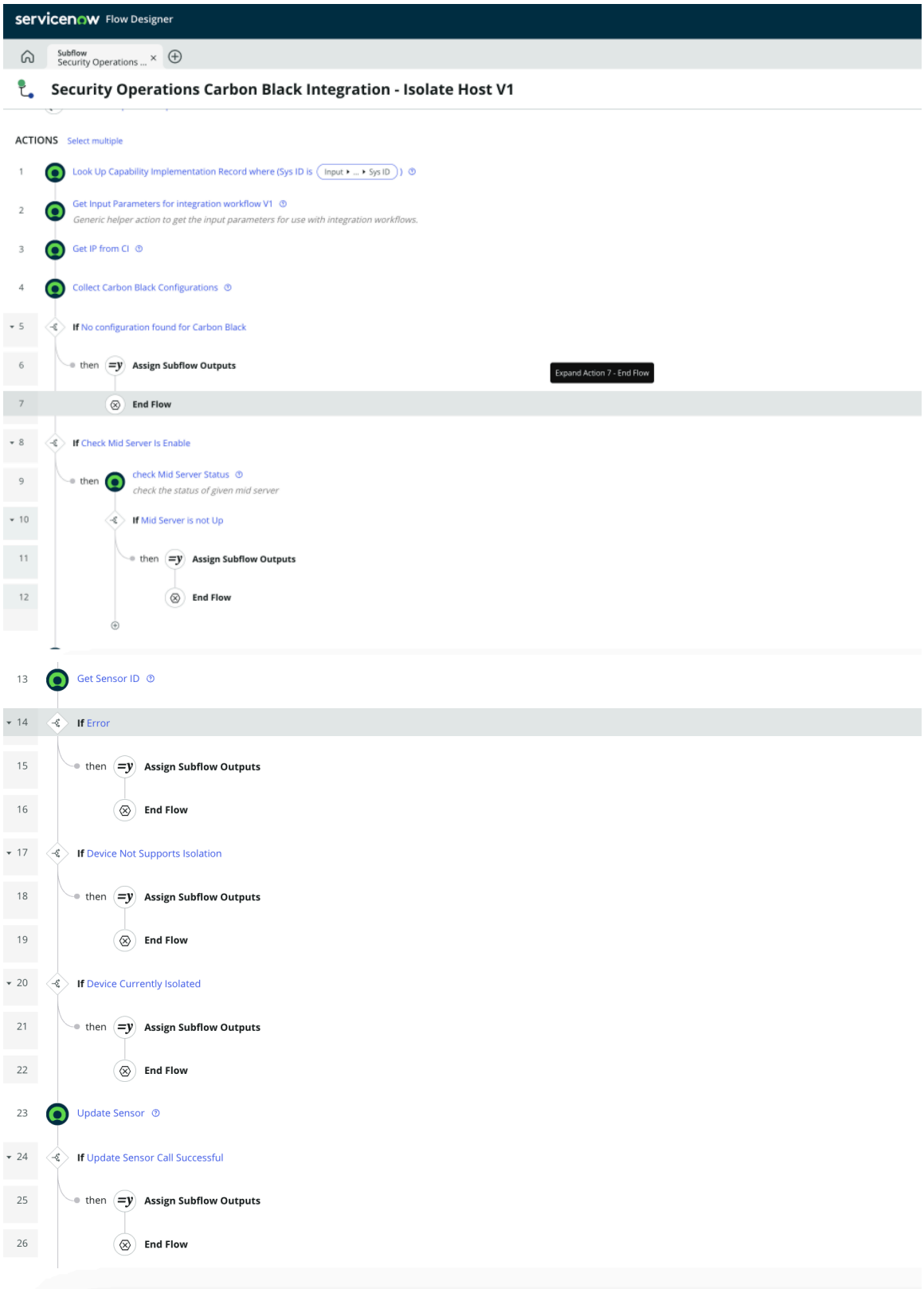
Die Carbon Black-Integration von Security Operations – Host isolieren ist die Implementierung für die Carbon Black-Integration, die vom Flow Security Operations Integration – Host isolieren gestartet wird.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Die Flow-Prozessaktivitäten umfassen:

- Ausführungsnachverfolgung – Begin (CIs) Flow-Aktion
- IP von CI abrufen
- Sammeln Sie Carbon Black-Konfigurationen
- Nachverfolgung Der Fähigkeitsausführung: Fehler-Flow-Aktion
- Sensor-ID abrufen
- Legen Sie die Aktivität „Netzwerkisolierung aktiviert“ fest
- Aktualisieren Sie Den Sensor – Gibt das Ergebnis „Host isolieren“ zurück.
- Nachverfolgung Der Fähigkeitsausführung: Flow-Aktion Abschließen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Aktivitäten, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Flow-Aktion für Sensor-ID abrufen

Die Flow-Aktion „Sensor-ID abrufen“ erfasst Sensorbezeichner, die im Flow verwendet werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Flow-Aktion „Sensor-ID abrufen“ kann mit jedem Flow verwendet werden, um Sensorinformationen zur Verwendung im Flow zu sammeln.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sensorbezeichner gefunden.
Fehler	Keine Sensoren gefunden. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.
endpoint_base	Basis-URL der Carbon Black-API.
ci_ip_address	IP-Adresse des Konfigurationselements.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Bestimmt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt.
Array-Elementtyp	API-Variablen.
sensor_detail	Beschreibung des Carbon Black-Sensors im JSON-Format.

Legen Sie die Aktivität „Netzwerkisolierung aktiviert“ fest

Die Workflow-Aktivität „Netzwerkisolierung aktivieren“ aktiviert die Netzwerkisolierung.

Die Aktivität „Netzwerkisolierung aktivieren“ kann mit jedem Workflow verwendet werden, um die Netzwerkisolierung zu aktivieren.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Netzwerkisolierung aktiviert.
Fehler	Netzwerkisolierung kann nicht aktiviert werden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
sensor_detail	Beschreibung des Carbon Black-Sensors im JSON-Format.
Deaktivieren	Bestimmt, ob der Host isoliert ist oder die Host-Isolierung entfernt. Wahr = Isolation deaktivieren Falsch = Isolierung bleibt aktiviert

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
sensor_detail	Beschreibung des Carbon Black-Sensors im JSON-Format.

Aktualisieren Sie die Sensoraktivität

Die Workflow-Aktivität „Sensor aktualisieren“ aktualisiert den Sensor, um Hosts oder Endpunkte zu isolieren.

Die Aktivität „Sensor aktualisieren“ kann mit jedem Workflow verwendet werden, um Hosts oder Endpunkte zu isolieren.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Sensor aktualisiert.
Fehler	Sensor kann nicht aktualisiert werden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
api_token	Carbon Black-API-Schlüssel.
use_mid_server	Bestimmt, ob die REST-Aktivität den MID-Server für die Interaktion mit Carbon Black verwendet oder nicht.
endpoint_base	Basis-URL der Carbon Black-API.
sensor_id	Sensorbezeichner.
sensor_detail	Beschreibung des Carbon Black-Sensors im JSON-Format.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
status_code	Bestimmt, ob die Anforderung erfolgreich war. Wenn nicht, werden ein HTTP-Fehlercode und eine Meldung angezeigt.

Security Operations Carbon Black-Integration: Flow Zum Entfernen Der Host-Isolation

Die **Security Operations Carbon Black-Integration – Hostisolierung Entfernen** Flow hebt die Kommunikation mit einem angegebenen Host oder Endpunkt in einem Carbon Black-System auf.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

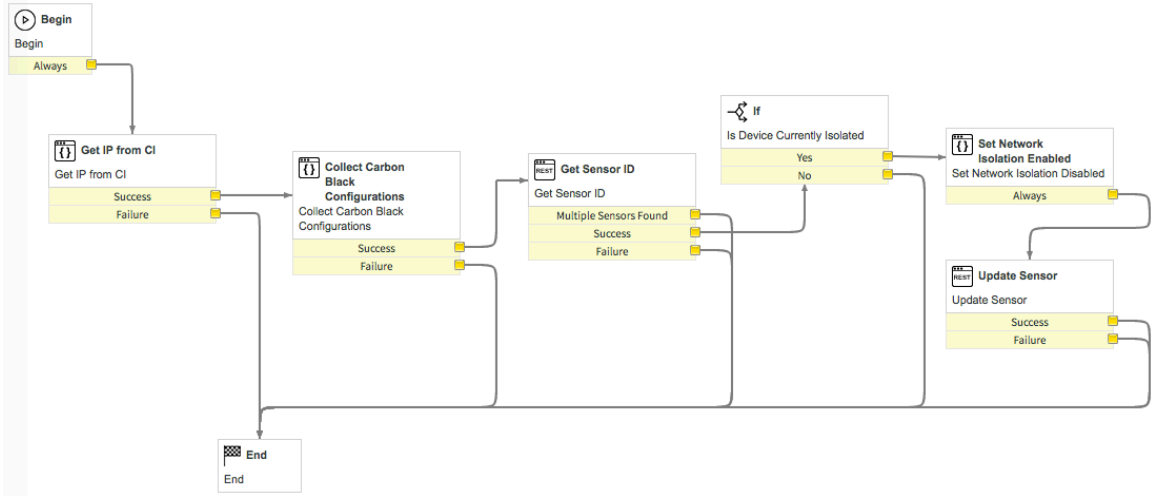
Dieser Flow ist nicht Teil einer Fähigkeit und benötigt eine anwenderdefinierte Orchestration, um ausgeführt zu werden.

Die Flow-Prozessaktivitäten umfassen:

- IP aus CI-Aktivität abrufen
- Wenn erfolgreich: Flow-Aktion „Carbon Black-Konfigurationen Erfassen“
- Flow-Aktion für Sensor-ID abrufenSensor-ID abrufen
- Wenn – Gerät die Isolierung unterstützt und das Gerät nicht isoliert ist Zu deaktiviert.
- Aktualisieren Sie die Sensoraktivität– Gibt das Ergebnis „Host isolieren“ zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Carbon Black-Integration: Hostisolierung Entfernen



Integration von Security Operations: Funktion „in Beobachtungsliste veröffentlichen“

Die In Beobachtungsliste veröffentlichen Die Fähigkeit fügt einer Beobachtungsliste von Drittparteien erkennbare Elemente und Indikatoren hinzu, die einem Security Incident zugeordnet sind und auf Sicherheitsereignisse überwachen und Warnungen generieren. Diese Fähigkeit wird als Teil der Reaktion auf Incidents während Untersuchungen verwendet.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Integration von Security Operations: Flow „in Beobachtungsliste veröffentlichen“

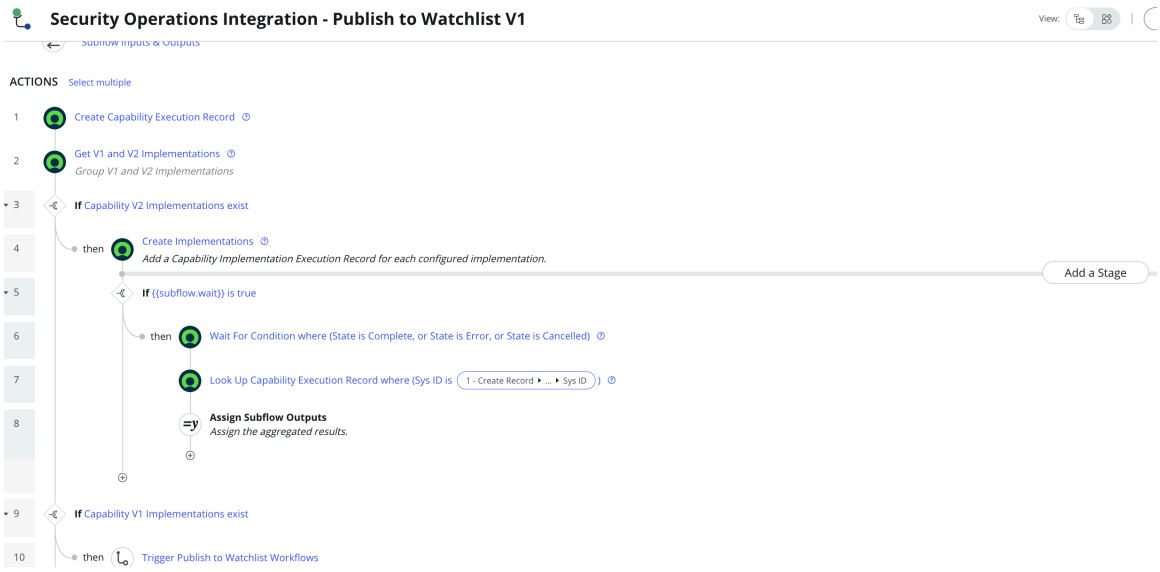
Die **Security Operations-Integrationen: In Beobachtungsliste veröffentlichen** Flow ist ein allgemeiner Flow, der unabhängig von Integrationen ist. Er fügt der Beobachtungsliste von Drittparteien erkennbare Elemente hinzu, die die Fähigkeit unterstützen. Verwenden Sie es, um eine Integration zu erfüllen.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow ist sichtbar und wird nur ausgeführt, wenn eine Integration verfügbar ist. Wird von ausgelöst **Erkennbare Elemente** Oder **Zugeordnete Indikatoren** Registerkarte für einen Security Incident.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In Beobachtungsliste veröffentlichen



Aktivitäten, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Integration von Security Operations: Sichtungssuchfunktion

Die **Sichtungssuche** Die Fähigkeit akzeptiert eine Reihe erkennbarer Elemente, sucht nach Integrationen, die eine Sichtungssuche unterstützen, und führt diese Suchen aus.

Die Sichtungssuche verfügt über einen Workflow, Integration Von Security Operations: Sichtungssuche-Flow, Der die Sichtungssuche ausführt. Dieser Workflow akzeptiert eine Liste erkennbarer Elemente, findet alle Implementierungsfähigkeiten, erstellt die Abfragen basierend auf Sichtungssuchkonfigurationen und führt die Suchen basierend auf dem konfigurierten Workflow aus. Sobald die Suche abgeschlossen ist, wird den Arbeitsnotizen für Incidents eine Notiz hinzugefügt, die angibt, ob und wenn ja, wie viele Sichtungen gefunden wurden.

Um Sichtungssuchkonfigurationen anzuzeigen, navigieren Sie zu **Security Operations** > **Integrationen** > **Sichtungssuche – Konfigurationen**an.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Erstellen Sie Konfigurationsdatensätze für Sichtungssuche

Erstellen Sie mehrere Sichtungssuchkonfigurationsdatensätze, und verwenden Sie sie, wenn Sie mehrere Protokollspeicher abfragen oder die Suchparameter ändern.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

- Das CIM-Add-on muss auf der Splunk-Instanz installiert sein.
- Gespeicherte Suchen und Inplace-Abfragen werden nur für Splunk-Integration unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch Konfigurationsdatensätze für Sichtungssuche erstellen, um sie aufzurufen Gespeicherte Suchen Im Splunk Enterprise-Protokollspeicher.

Hinweis:
Die Suchkonfigurationsabfragen basieren auf Splunk-Protokolldaten, um Splunk Common Information Model (CIM)-konform zu sein.

Mit gespeicherten Suchkonfigurationen können Sie:

- Erstellen Sie anwenderdefinierte Suchen, die mehrere Ereignisdatensätze kombinieren.
- Designeffiziente und effektive Suchen.
- Verwenden Sie parametrisierte Eingaben in der gespeicherten Splunk-Suche.

Das Basissystem enthält die Beispielkonfigurationen, wie in dieser Abbildung gezeigt:

Gespeicherte Suchkonfigurationen

Name	Observable type	Search	Is saved search
Search	Search	Search	Search
Default Proofpoint Inplace Search-Emails	Email	tag=email [| search tag="email" AND (sub...	false
Default Saved Search - Emails	Email	args.email.subject=${email.subject}&args...	true
Default PAN Inplace Search - URLs	URL	tag=network url=${observable} | table us...	false

Die gespeicherten Such- und Inplace-Konfigurationsabfragen sind Beispielabfragen und können durch entsprechende Parameter für Ihre Umgebung ersetzt werden. Erstellen Sie nach Bedarf zusätzliche gespeicherte Suchkonfigurationen. Wenn Sie eine gespeicherte Suchkonfiguration definieren, müssen der Name und die Parameter in der Suchabfrage mit der gespeicherten Konfiguration übereinstimmen, die in Ihrer Splunk-Instanz definiert ist. Wenn der Name und die Parameter nicht identisch sind, werden bei einer Sichtungssuche möglicherweise keine genauen Ergebnisse angezeigt.

Hinweis:
Navigieren Sie in Ihrer Splunk-Instanz zur Seite Suchen, Berichte und Warnungen, und suchen Sie Ihre gespeicherte Suchabfrage. Klicken Sie auf **Berechtigungen** Link, um zur Seite „Berechtigungen“ zu navigieren. Wählen Sie aus **Alle Apps** Optionsschaltfläche und aktivieren Sie **Leseberechtigung** Option für **Alle** . Dadurch wird der Wert der Spalte „Freigeben“ für Ihre gespeicherte Suchabfrage von „Privat“ in „App“ geändert. Wenn dies nicht festgelegt ist, gibt die gespeicherte Suchabfrage möglicherweise keine Ergebnisse zurück.

So überprüfen Sie, ob die gespeicherte Suchkonfiguration mit der in Ihrer Splunk-Instanz definierten Konfiguration übereinstimmt:

1. Navigieren zu **Einstellungen** > **Suchen, Berichte und Warnungen**an.
2. Ändern **App-Kontext** Bis **Alle** .

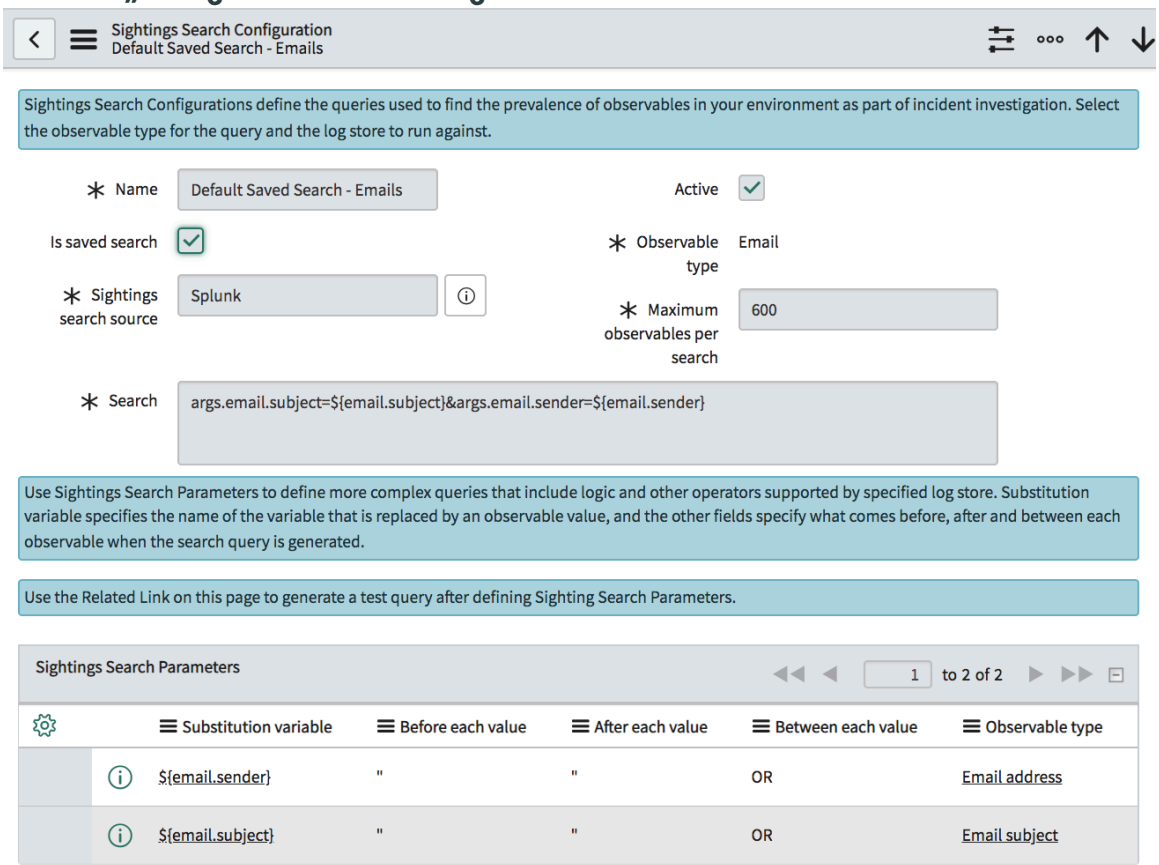
   Eine Liste der Suchberichte wird angezeigt.
3. Bestätigen Sie, dass die gespeicherte Suchabfrage in der Liste vorhanden ist.

Beispielsweise enthält das Formular „Sichtungssuchkonfiguration“ die E-Mail-Adresse und den E-Mail-Absender als Suchparameter:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Konfiguration der Sichtungssuche“



Definieren Sie in Ihrer Splunk-Instanz die gespeicherte Suche mit dem gleichen Namen, der standardmäßig gespeicherten Suche – E-Mails und den gleichen Suchparametern für die E-Mail-Adresse und den E-Mail-Betreff. Wenn Name und Suchparameter nicht identisch sind, wird bei der Sichtungssuche kein genaues Ergebnis generiert.

Prozedur

1. Navigieren zu **Security Operations** > **Integrationen** > **Sichtungssuche – Konfiguration** Und erstellen Sie einen neuen Datensatz (Feldbeschreibungen finden Sie in der Tabelle).

Formular „Konfiguration der Sichtungssuche“

Feld	Beschreibung
Name	Name der Konfiguration
Ist gespeicherte Suche	Wenn Sie diese Option auswählen, wird eine gespeicherte Suchkonfiguration erstellt.
Sichtungssuchquelle	Die Quelle für die Sichtungssuche. Wählen Sie den Splunk-Protokollspeicher als Quelle aus.
Aktiv	Option für den gespeicherten Suchstatus. Nur aktive Suchkonfigurationen können verwendet werden, um eine Sichtungssuche durchzuführen.
Typ des erkennbaren Elements	Der Typ des erkennbaren Elements kann ein beliebiger Typ des erkennbaren Elements sein, z. B. IP, Hash-Wert, URL, Domänenname usw.
Maximale erkennbare Elemente pro Suche	Maximale Anzahl erkennbarer Elemente, die von der Suche zurückgegeben werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Suchen	Die Standardsuchzeichenfolge ist `$(erkennbares Element)` , Sie können jedoch Ihre eigene Suchabfrage definieren, indem Sie Parameter angeben, die vom Splunk-Protokollspeicher unterstützt werden.

2. Klicken Sie auf **Absenden**.

Ergebnisse
Sie haben einen Konfigurationsdatensatz für die Sichtungssuche erstellt.

Nächste Maßnahme
Klicken Sie nach dem Definieren der Suchabfrage auf **Testabfrage Für Sichtungssuche Generieren** , Und geben Sie eine Liste erkennbarer Werte an, um eine Testabfrage basierend auf dieser gespeicherten Suchkonfiguration zu generieren.

Führen Sie eine Sichtungssuche aus

Bestimmen Sie die Verbreitung einer Bedrohung im Zeitverlauf, oder testen Sie Korrekturmaßnahmen oder Beseitigungsmaßnahmen. Sie können einzelne oder mehrere erkennbare Elemente und den Datumsbereich für Ihre Suche aus einem Security Incident auswählen. Ergebnisse sind in enthalten **Erkennbare Security Incident-Elemente** Zugehörige Liste.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

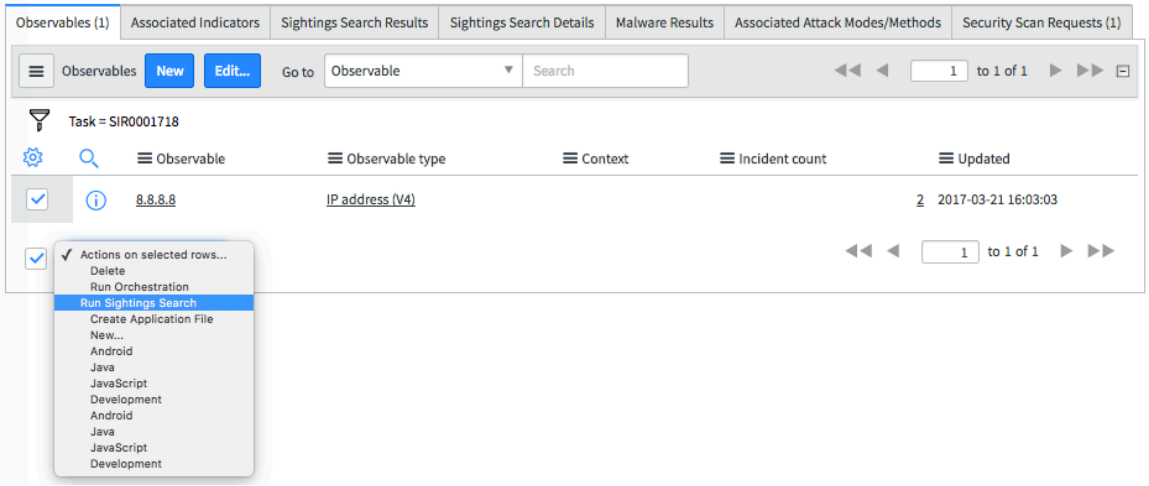
Warum und wann dieser Vorgang ausgeführt wird
Die Sichtungssuche verfügt über einen Flow, Integration Von Security Operations: Sichtungssuche-Flow, Der die Sichtungssuche ausführt. Dieser Flow akzeptiert eine Liste erkennbarer Elemente, findet alle Implementierungsfähigkeiten, erstellt die Abfragen basierend auf Sichtungssuchkonfigurationen und führt die Suchen basierend auf dem konfigurierten Flow aus.

Hinweis:
Eine aktive Implementierung muss konfiguriert werden. Die Sichtungssuche unterstützt Elasticsearch, Splunk, McAfee ESM, HPE ArcSight Logger und QRadar-Incident-Anreicherung. Wenn keine Implementierungen verfügbar sind, Fähigkeitsaktionen, z. B. **Sichtungssuche Ausführen** , Werden nicht in Produktmenüs angezeigt.

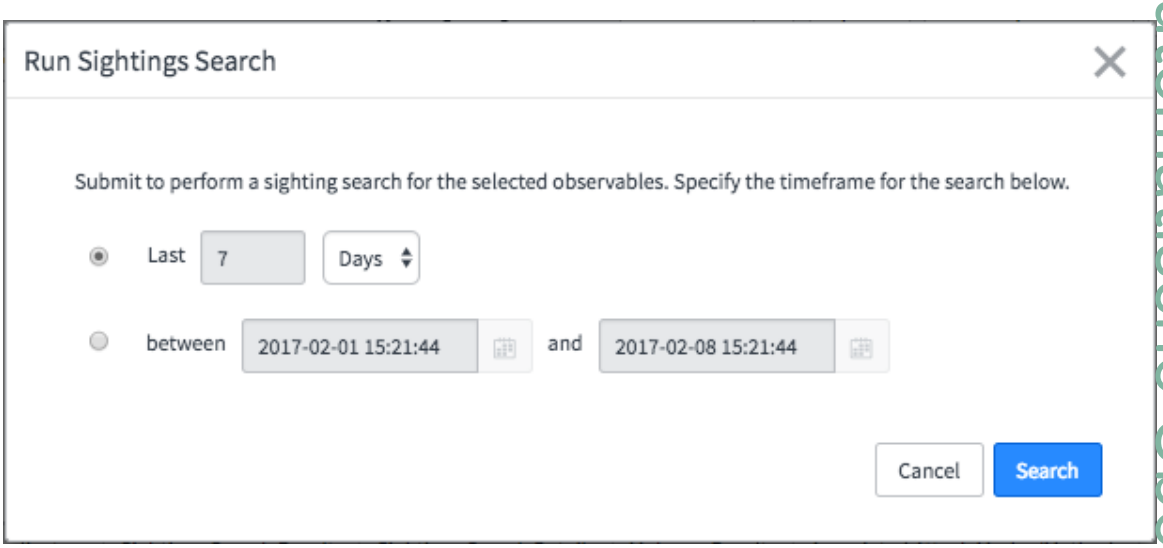
Prozedur
1. Navigieren Sie zu einem Security Incident.
2. Klicken Sie auf **IOC anzeigen** Zugehöriger Link.
3. Wählen Sie Aus **Erkennbare Elemente** Auf der Registerkarte zugehörige Liste.
4. Wählen Sie die erkennbaren Elemente aus, für die Sie eine Sichtungssuche durchführen möchten.
5. Klicken Sie Auf **Sichtungssuche Ausführen** In **Aktionen für ausgewählte Zeilen...** Dropdown-Menü.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Dialogfeld Sichtungssuche ausführen wird geöffnet.



Hinweis:
Werte, die im Dialogfeld eingegeben werden, überschreiben die Konfigurationswerte der Fähigkeit für diese Ausführung.

6. Wählen Sie die Anzahl der Tage oder einen Datumsbereich aus, um nach Daten zu suchen.

Option	Bezeichnung
Letzte	Die Anzahl der Stunden oder Tage vor der Erstellung des zu suchenden Incident. Der Standardwert ist 7 Tage. Der Grenzwert beträgt 99 Stunden oder Tage.
zwischen	Bereich der zu suchenden Daten. Standarddaten sind: Datum und Uhrzeit der Eröffnung des Incident. Datum und Uhrzeit sieben Tage vor der Eröffnung des Incident.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:
Zuletzt Ist die Anzahl der Stunden oder Tage vor der Erstellung des zu suchenden Incident. Der Standardwert ist 7 Tage. Der Grenzwert beträgt 99 Stunden oder Tage.

7. Klicken Sie auf **Suche**.
Ein Sichtungssuchdatensatz wird erstellt. Aggregat- und zugehörige Sichtungsdaten werden im Security Incident unter angezeigt **Sichtungssuchergebnisse** Und **Sichtungssuchdetails** Registerkarten.

Hinweis:
Sichtungssuchergebnisdaten können für freigegeben werden Trusted Security Circle, Mit Ausnahme von Rohdaten im Fall von Implementierungen, die so konfiguriert sind, dass Rohdaten eingeschlossen werden.

Ergebnisse der Sichtungssuche

Ergebnis	Beschreibung
Anzahl	Der Bezeichner für die Sichtungssuche.
Anzahl der erkennbaren Elemente	Anzahl der erkennbaren Elemente, die nach Abfrage gesucht werden.
Interne Sichtungen	Anzahl der internen Sichtungen.
Externe Sichtungen	Anzahl der externen Sichtungen. (Erhalten von Bedrohungsfreigabe.)
Übereinstimmende Konfigurationselemente	Anzahl der Konfigurationselemente, die einem vorhandenen Datensatz in Ihrer cmdb für jedes in Ihrer Umgebung gefundene erkennbare Element entsprechen.
Startdatumsbereich	Zeit, um mit der Suche nach Sichtungen zu beginnen.
Enddatumsbereich	Zeit, um die Suche nach Sichtungen zu beenden.
Aktualisiert	Datum und Uhrzeit der letzten Änderung.

Hinweis: Wenn die für die Sichtungssuche verwendete Implementierung so konfiguriert ist, dass Rohdaten eingeschlossen werden, und mindestens eine Sichtung gefunden wird, wird oben im Security Incident ein Anhang mit Rohdatenbeispielen angezeigt.

Details der Sichtungssuche

Detail	Beschreibung
Sichtungssuche	Der Bezeichner für die Sichtungssuche.
Erkennbares Element	Erkennbares Element, nach dem nach Abfrage gesucht wird.
Typ des erkennbaren Elements	Typ des erkennbaren Elements, nach dem nach Abfrage gesucht wird.
Interne Sichtungen	Zusammengefasste Anzahl der internen Sichtungen.
Externe Sichtungen	Zusammengefasste Anzahl der externen Sichtungen. (Erhalten von Bedrohungsfreigabe.)
Aktualisiert	Datum und Uhrzeit der letzten Änderung.

Integration Von Security Operations: Sichtungssuche-Flow

Security Operations-Integration – Sichtungssuche Flow ist ein allgemeiner Flow, der unabhängig von Integrationen ist. Es verwendet die konfigurierten Abfragen, um basierend

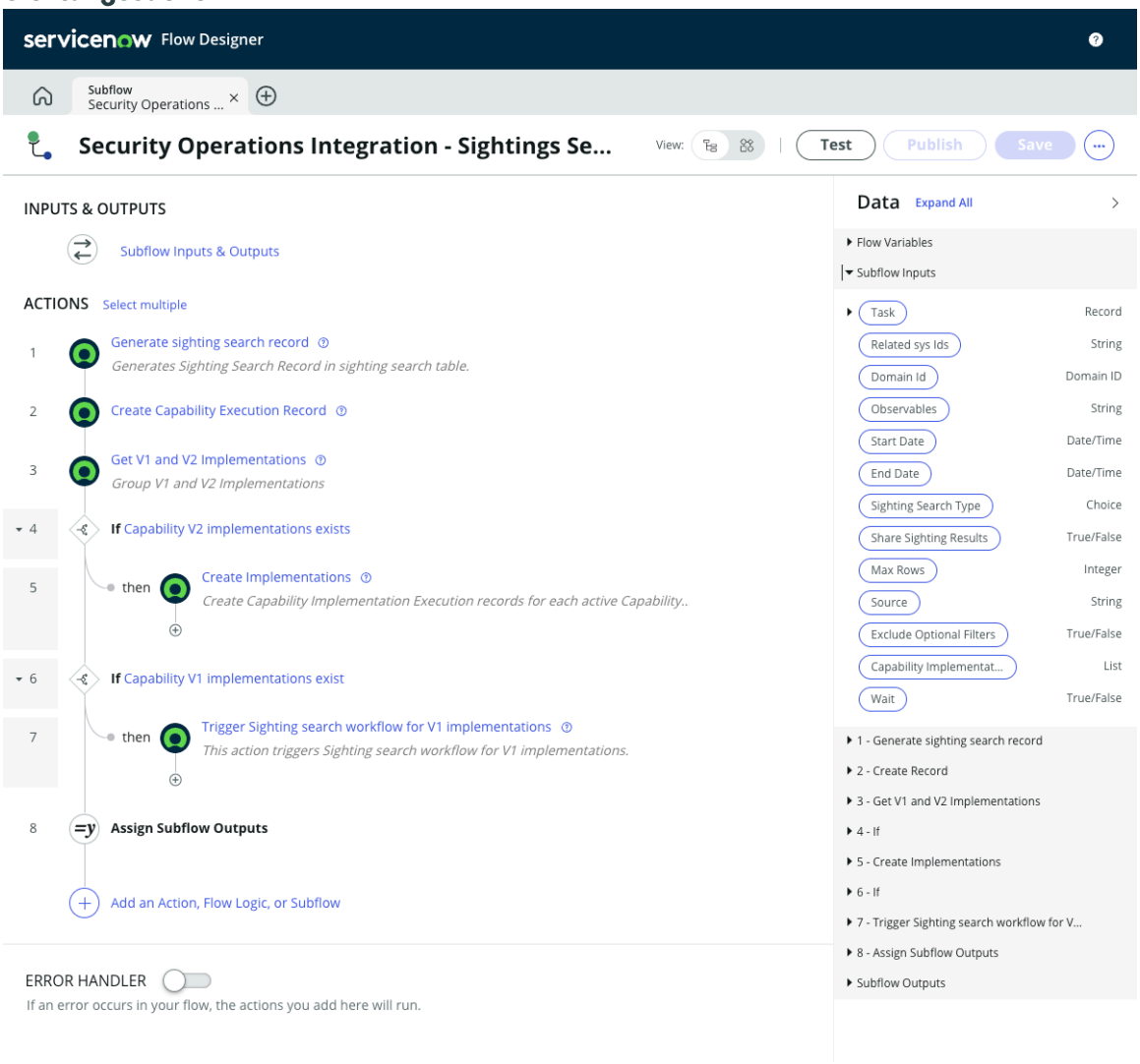
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auf den konfigurierten Integrationen, die die Fähigkeit unterstützen, nach einer Reihe erkennbarer Elemente zu suchen. Verwenden Sie es, um eine Integration wie Splunk oder Elasticsearch zu erfüllen.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
Wenn an einen Security Incident ein erkennbares Element angehängt ist, wird dieser Flow ausgelöst, wenn Sie auf klicken **Sichtungssuche Ausführen** In **Aktionen für ausgewählte Zeilen...** Dropdown-Menü in **Erkennbare Security Incident-Elemente** Registerkarte.

Sichtungssuche



Aktivitäten, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Sichtungssuche: Aktivität erkennbarer Elemente bestimmen

Die **Sichtungssuche: Bestimmen Sie Erkennbare Elemente** Die Workflow-Aktivität bestimmt, welche erkennbaren Elemente in den Workflow aufgenommen werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die **Sichtungssuche: Bestimmen Sie Erkennbare Elemente** Aktivität kann mit jedem Workflow verwendet werden, um zu bestimmen, welche erkennbaren Elemente in den Workflow aufgenommen werden sollen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Erkennbare Elemente gefunden
Fehler	Keine erkennbaren Elemente gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
task_sys_id	Aufgabenbezeichner (ordnet Security Incident erkennbaren Elementen zu).
Erkennbare Elemente	IP-Adressen, Hash, URLs, Domänennamen.
Workflow_current_sys_ID	Systembezeichner des aktuellen Datensatzes. (Wird nur verwendet, wenn `Aufgabe_sys_ID` , Eingaben für erkennbare Elemente sind nicht verfügbar.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Erkennbare Elemente	Gefilterte erkennbare Elemente

Sichtungsaktivität für persistente erkennbare Elemente

Die **Sichtungen Persistenter Erkennbarer Elemente** Workflow-Aktivität ruft erkennbare Elemente aus der Drittpartei-Integration ab.

Die **Sichtungen Persistenter Erkennbarer Elemente** Aktivität kann mit jedem Workflow verwendet werden, um erkennbare Elemente in der Drittpartei-Integration aufzuzeichnen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Erkennbare Elemente abgerufen.
Fehler	Beim Versuch, erkennbare Elemente zu erfassen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
sightingsResponse	
Aufgaben-ID	Aufgabenbezeichner.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response	

Ruft die Aktivität „Sichtungsabfragen erkennbarer Elemente“ ab

Die **Rufen Sie Sichtungsabfragen Erkennbarer Elemente Ab** Workflow-Aktivität ruft Abfragen aus der Integrationskonfiguration ab.

Die **Rufen Sie Sichtungsabfragen Erkennbarer Elemente Ab** Die Aktivität kann mit jedem Workflow verwendet werden, um Abfragen abzurufen, die mit an die angegebene Implementierung gesendet werden sollen **Paralleler Flow-Startprogramm** .

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Abfragen gefunden.
Fehler	Beim Versuch, Abfragen abzurufen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
Erkennbare Elemente	Liste der gefilterten erkennbaren Elemente.
capabilities	Liste der unterstützten Fähigkeiten.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
queries	Suchzeichenfolge.
QueryCount	Anzahl der auszuführenden Abfragen.

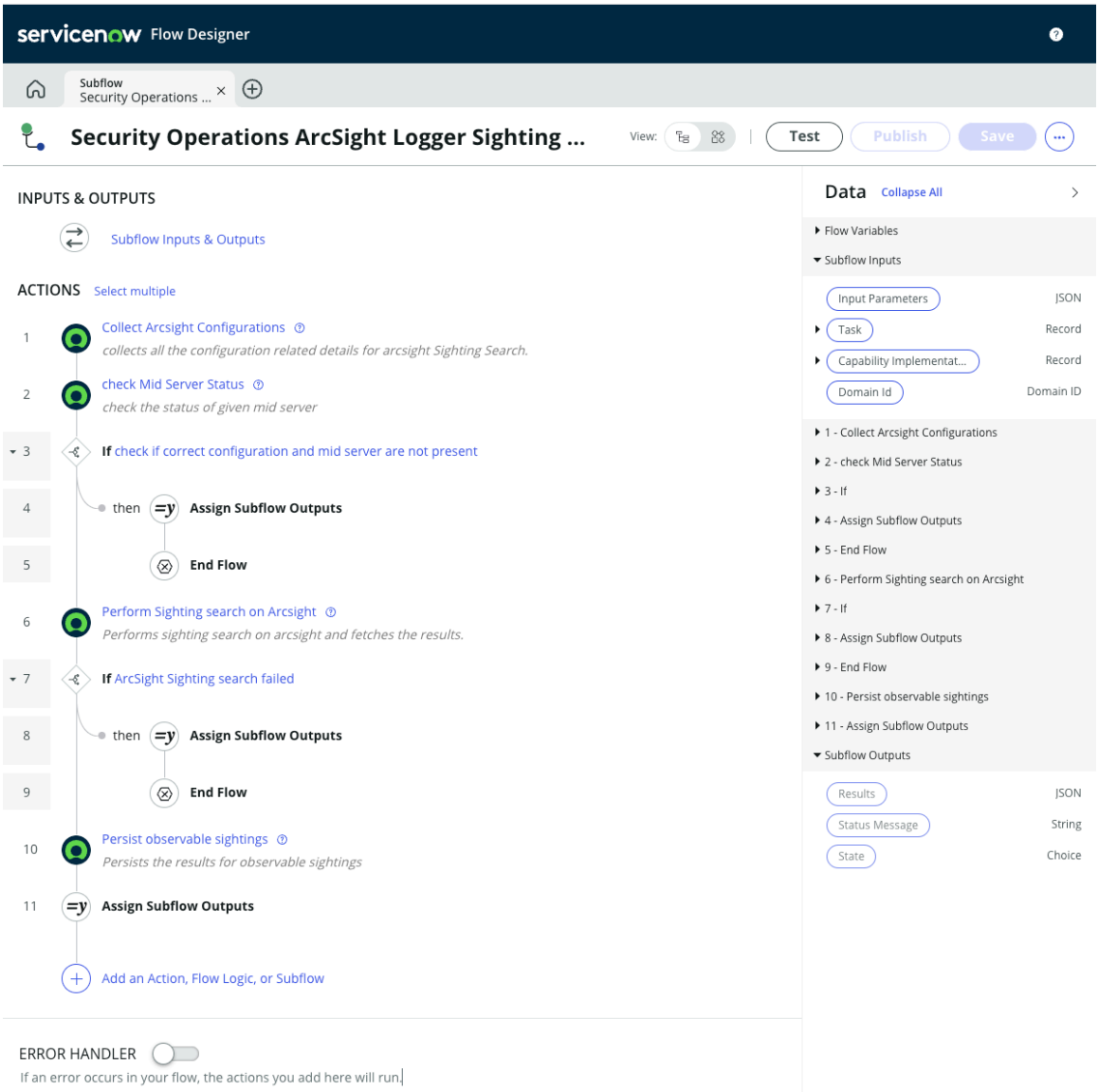
Security Operations – Suchflow Für Arcsight Logger-Sichtungen

Security Operations – Sichtungssuche für ArcSight Logger Flow ist die Implementierung für die Splunk-Integration, die von gestartet wurde **Integration Von Security Operations: Sichtungssuche-Flow** .

Erforderliche Rolle: sn_si_Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arcsight Logger – Sichtungssuche



Aktivitäten, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Security Operations: Elasticsearch-Sichtungssuche-Flow

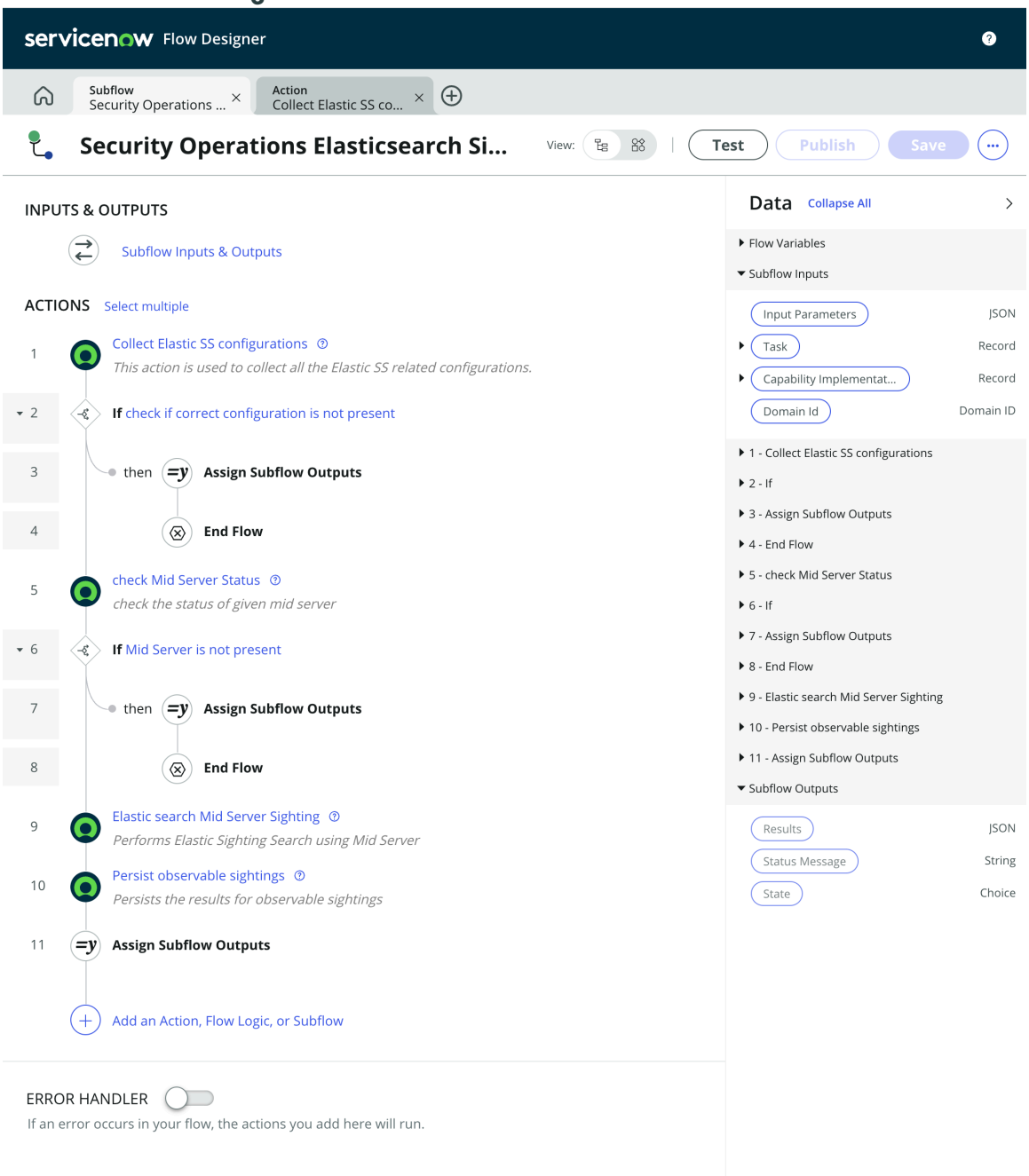
Security Operations: Elasticsearch-Sichtungssuche Flow ist die Elasticsearch-Implementierung, die von gestartet wurde **Security Operations-Integration – Sichtungssuche** Flow.

Erforderliche Rolle: sn_si.Analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Elasticsearch Sichtungssuche



Automatische Übersetzung

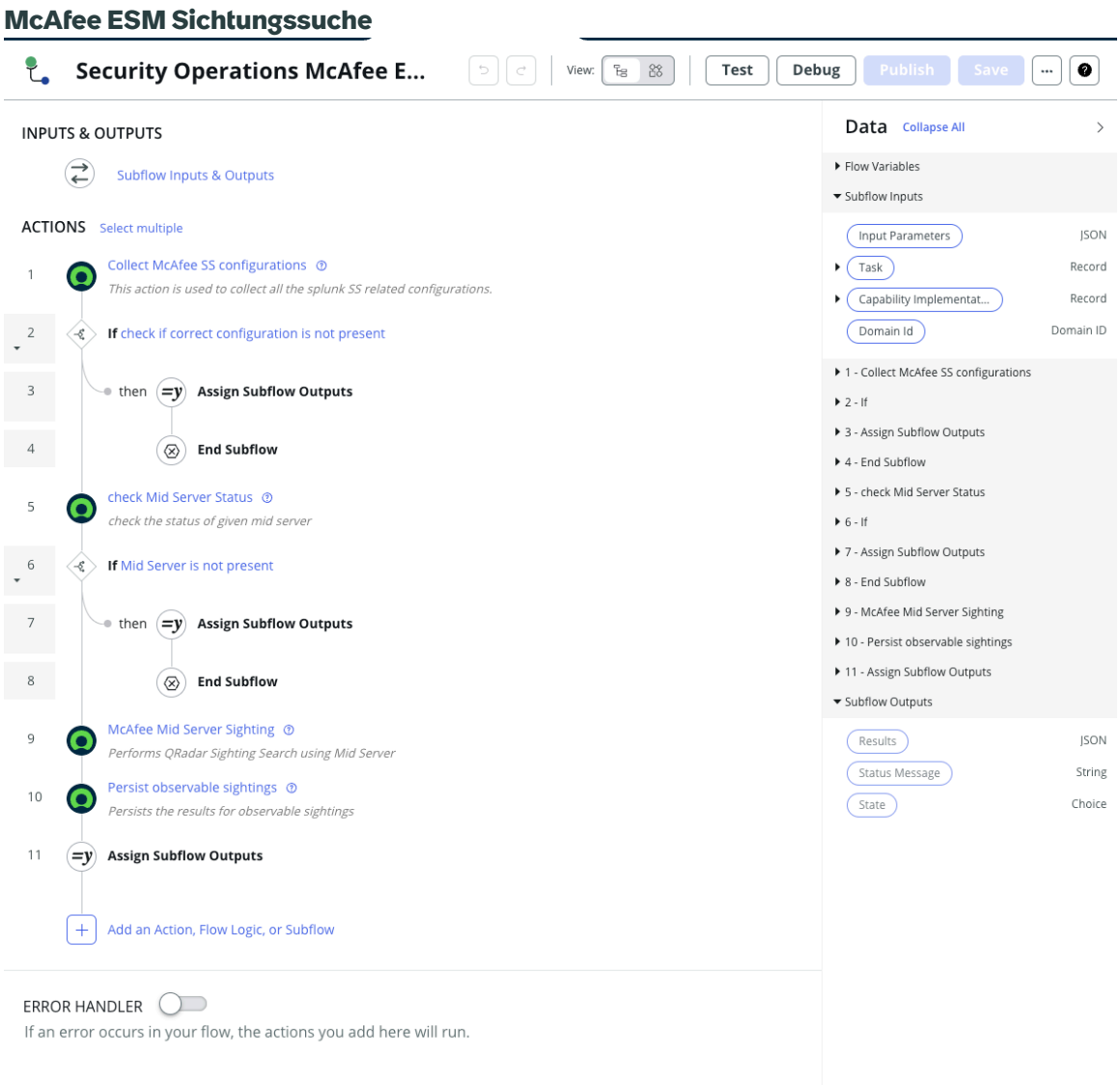
Aktivitäten, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Security Operations – Suchflow für McAfee ESM-Sichtungen

Security Operations – McAfee ESM Sichtungssuche Flow ist die Implementierung für die McAfee-Sichtungssuche-Implementierung, die von gestartet wurde **Integration Von Security Operations: Sichtungssuche-Flow** .

Erforderliche Rolle: sn_si_Analyst

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Aktivitäten, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Security Operations – QRadar-Sichtungssuche-Flow

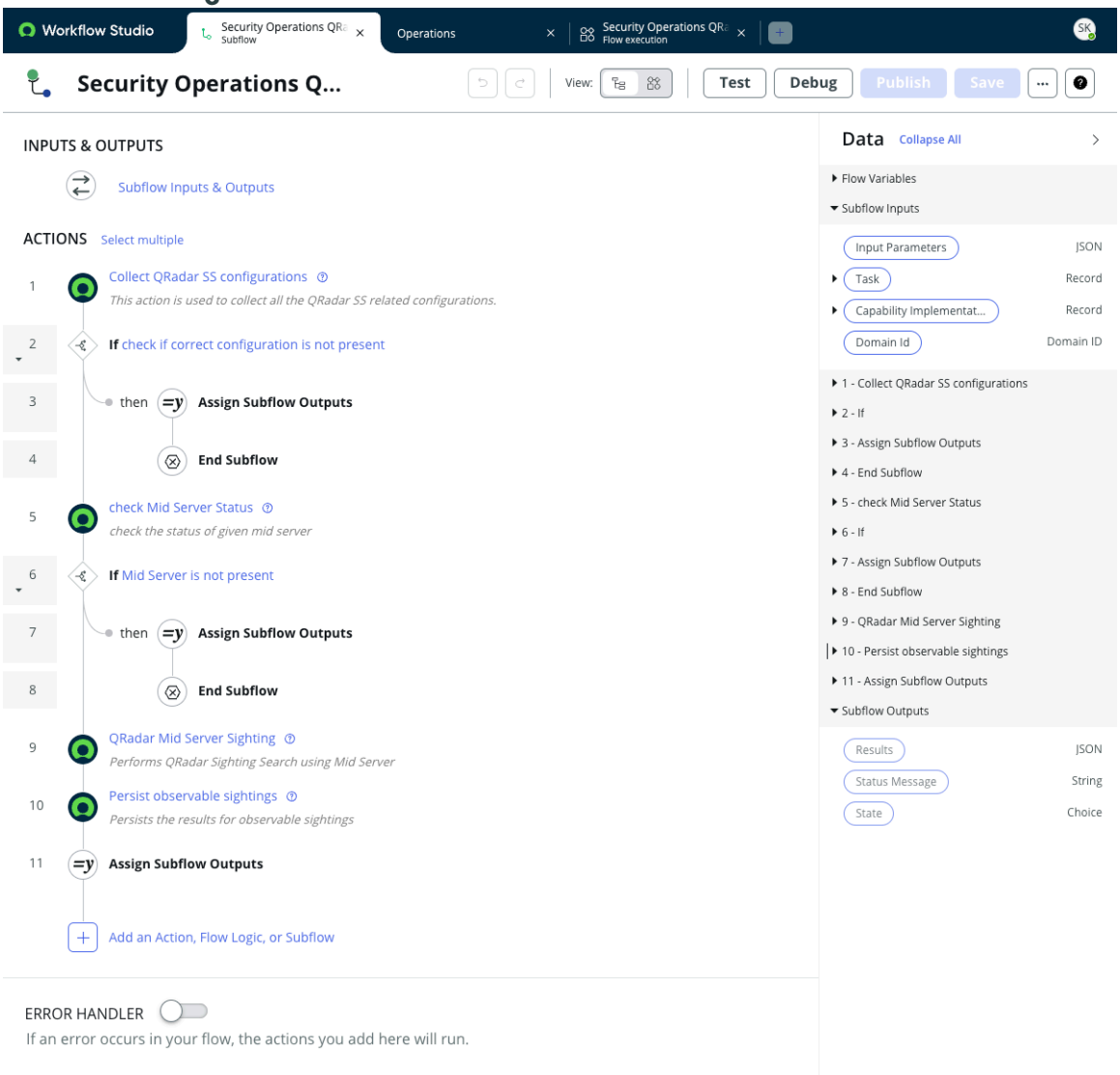
Sicherheitsvorgänge: QRadar-Sichtungssuche Flow ist die Implementierung für die IBM QRadar-Integration, die von gestartet wurde **Integration von Security Operations – Sichtungssuche-Flow** .

Erforderliche Rolle: sn_si_Analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

QRadar-Sichtungssuche



Aktivitäten, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Integration Von Security Operations – Suchflow Für Splunk-Sichtungen

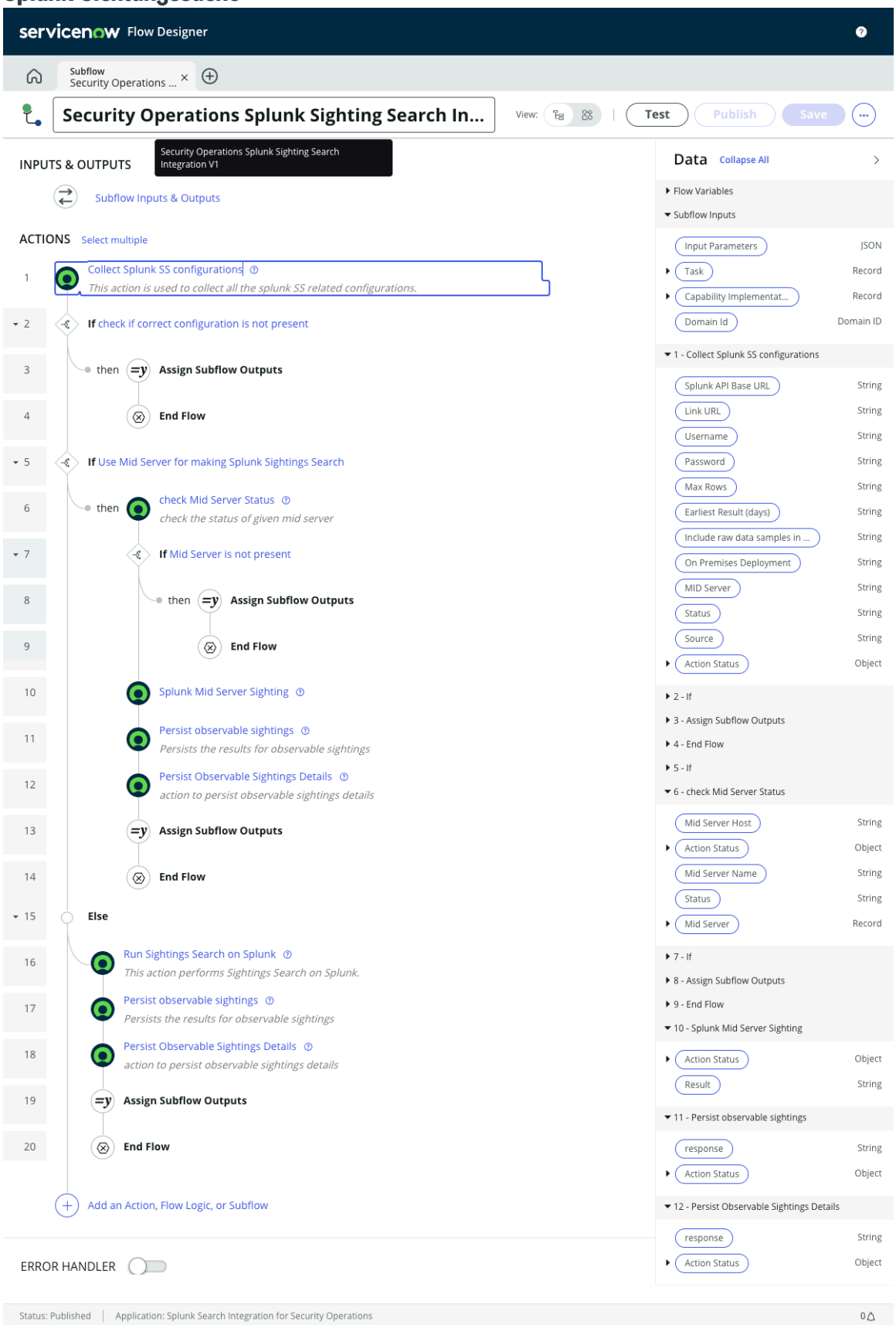
Security Operations – Splunk-Sichtungssuche Flow ist die Implementierung für die Splunk-Integration, die von gestartet wurde **Integration von Security Operations – Sichtungssuche-Flow** .

Erforderliche Rolle: sn_si_Analyst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Splunk-Sichtungssuche



Automatische Übersetzung

Aktivitäten, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktivitäten finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie Die Ergebnisse Der Sichtungssuche An

Sie können die Ergebnisse der Sichtungssuche auf interne und externe Indikatoren für schädliche Auswirkungen überprüfen.

Vorbereitungen

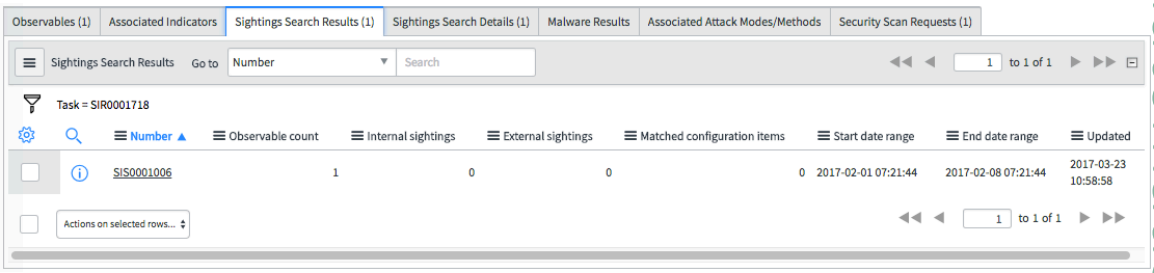
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

an.

Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie aus **Sichtungssuchergebnisse** Registerkarte von **IOC anzeigen** Gruppe „zugehörige Liste“ zum Anzeigen der Liste der Sichtungssuchen.



Hinweis:
Diese Daten können für freigegeben werden Trusted Security Circle.

Ergebnisse der Sichtungssuche

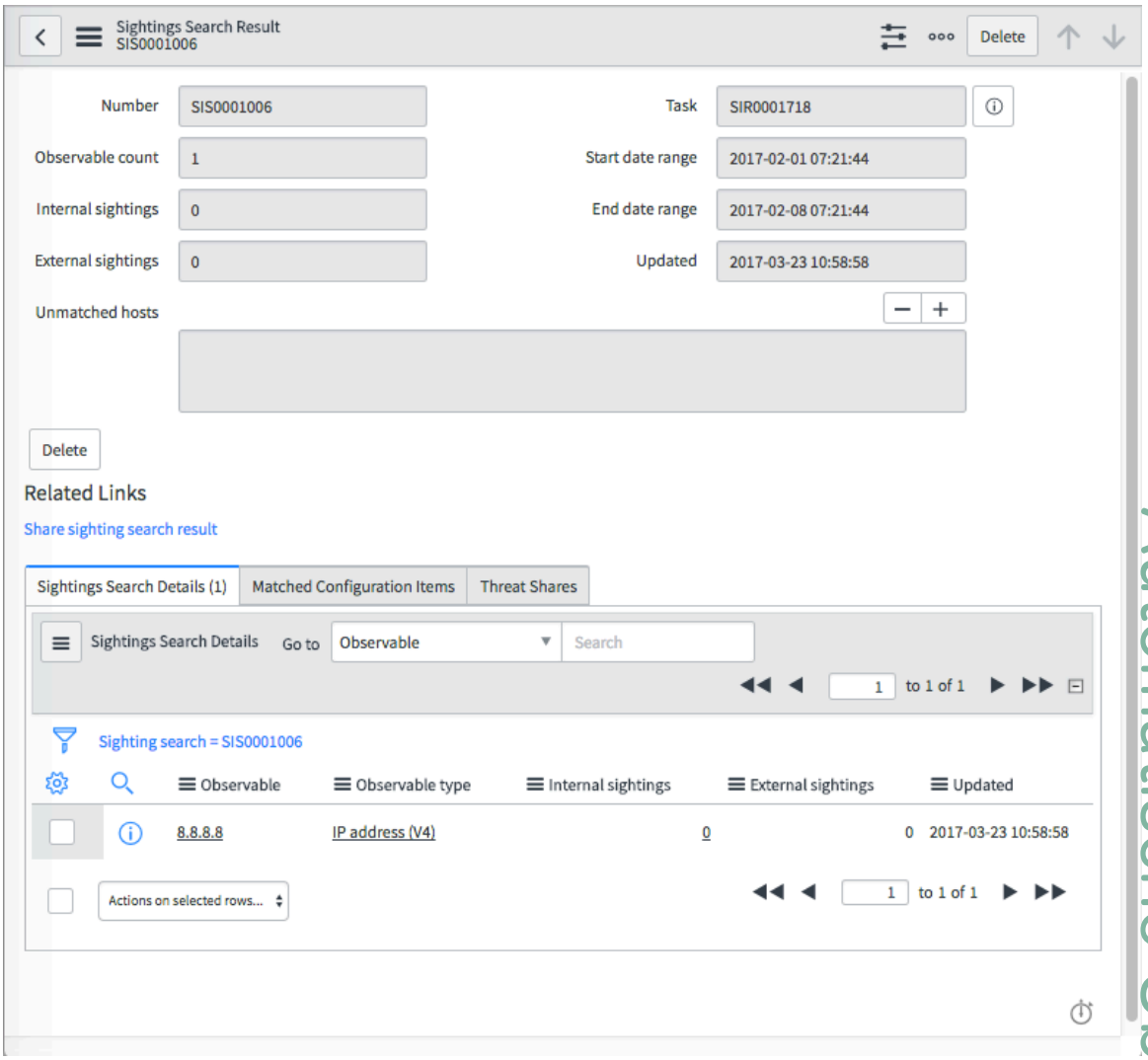
Ergebnis	Beschreibung
Anzahl	Sichtungssuchbezeichner.
Anzahl der erkennbaren Elemente	Anzahl der gesuchten erkennbaren Elemente.
Interne Sichtungen	Zusammengefasste Anzahl der internen Sichtungen.
Externe Sichtungen	Zusammengefasste Anzahl der externen Sichtungen. (Erhalten von Bedrohungsfreigabe.)
Übereinstimmende Konfigurationselemente	Zusammengefasste Anzahl der Konfigurationselemente, die einem vorhandenen Datensatz in entsprechen `cmdb` .
Startdatumsbereich	Zeit, um mit der Suche nach Sichtungen zu beginnen.
Enddatumsbereich	Zeit, um die Suche nach Sichtungen zu beenden.
Aktualisiert	Datum und Uhrzeit der letzten Änderung.

So zeigen Sie die Details einer einzelnen Suche an:

3. Klicken Sie im auf eine Sichtungssuche **Sichtungssuchergebnisse** Liste.
Das Formular Sichtungssuchergebnis wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Formular „Sichtungssuchergebnisse“

Detail	Beschreibung
Anzahl	Interner Sichtungssuchbezeichner.
Anzahl der erkennbaren Elemente	Anzahl der erkennbaren Elemente, die von dieser Abfrage gesucht werden.
Interne Sichtungen	Anzahl der internen Sichtungen für diese Suche.
Externe Sichtungen	Anzahl der externen Sichtungen für diese Suche. (Erhalten von Trusted Security Circle.)
Nicht übereinstimmende Hosts	Liste der potenziellen Konfigurationselemente für diese Suche, die mit keinen Datensätzen in Ihrem abgeglichen wurden `cmdb` .
Aufgabe	Bezeichner der Security Incident-Aufgabe.
Startdatumsbereich	Zeitpunkt, zu dem die Sichtungssuche gestartet wurde.
Enddatumsbereich	Zeitpunkt, zu dem die Sichtungssuche beendet wurde.
Aktualisiert	Datum und Uhrzeit der letzten Änderung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Detail	Beschreibung
Details einer Sichtungssuche	Typ, Anzahl der Sichtungen und Änderungsdatum.
Zugeordnete Konfigurationselemente	Anzahl der Konfigurationselemente, die mit einem vorhandenen Datensatz in übereinstimmen `cmdb` . Listet das CI und die Sichtung auf.
Bedrohungsfreigaben	Liste der für freigegebenen Bedrohungen Trusted Security Circle.

Geben Sie Sichtungssuchergebnisse frei

Sie können lokale Sichtungsdetails oder Ergebnisse, die einer bestimmten Suche zugeordnet sind, für Ihren vertrauenswürdigen Sicherheitskreis freigeben.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird

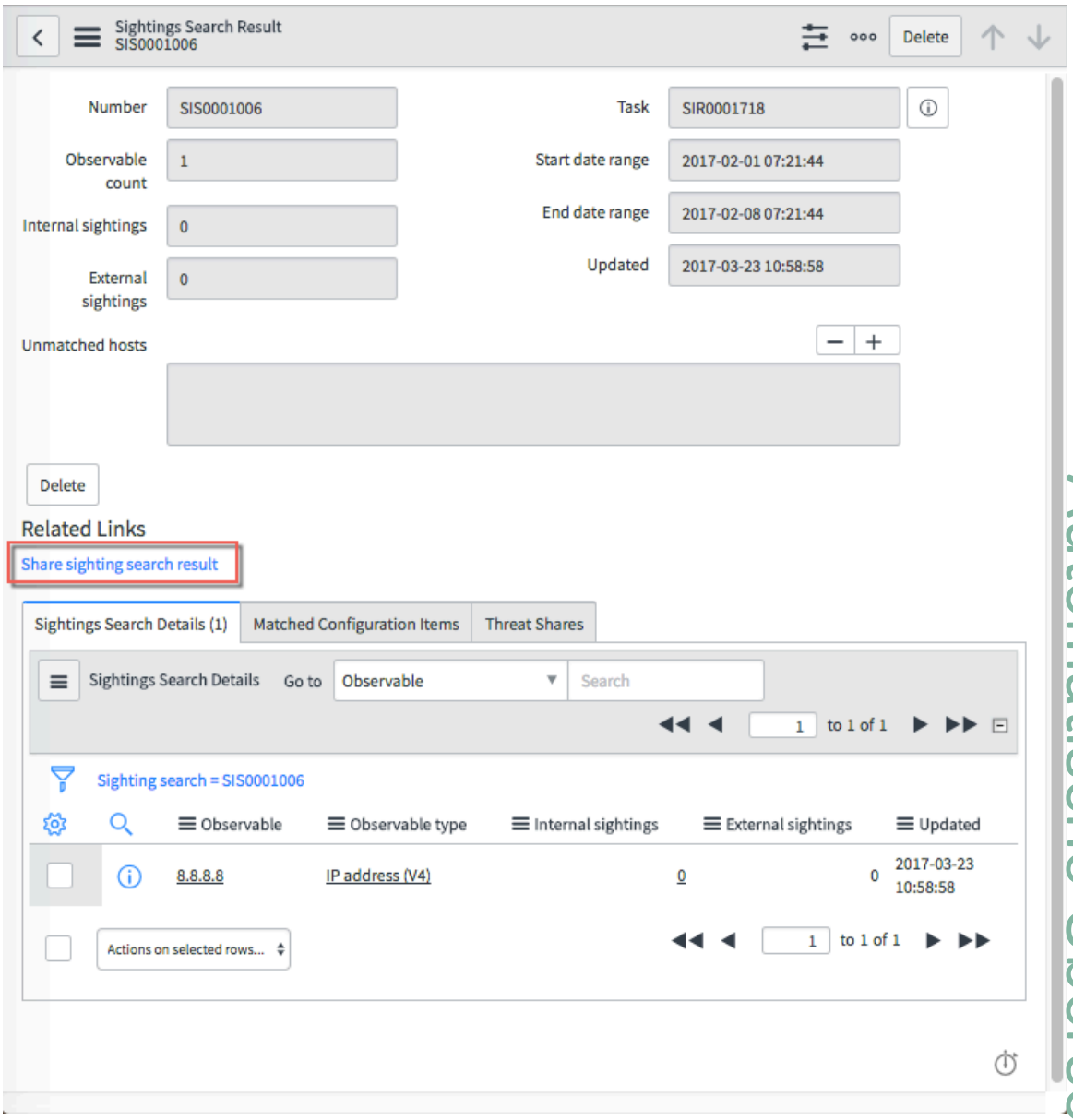
Die Freigabe kann mithilfe der folgenden Security Incident Response automatisiert werden **Eigenschaften** .

- Geben Sie die Ergebnisse einer Sichtungssuche automatisch für den standardmäßigen vertrauenswürdigen ServiceNow-Kreis frei
- Schließen Sie erkennbare Elemente ohne lokale Sichtungen ein, wenn Sie Sichtungssuchergebnisse automatisch freigeben
- Reagieren Sie mit lokalen Sichtungen, wenn eine Bedrohungsfreigabe von einem vertrauenswürdigen Kreis empfangen wird

Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Klicken Sie auf **IOC anzeigen** Zugehörige Liste, und wählen Sie aus **Sichtungssuchergebnisse** Registerkarte zum Anzeigen der Liste der Sichtungssuchen.
3. Klicken Sie auf ein Sichtungssuchergebnis.

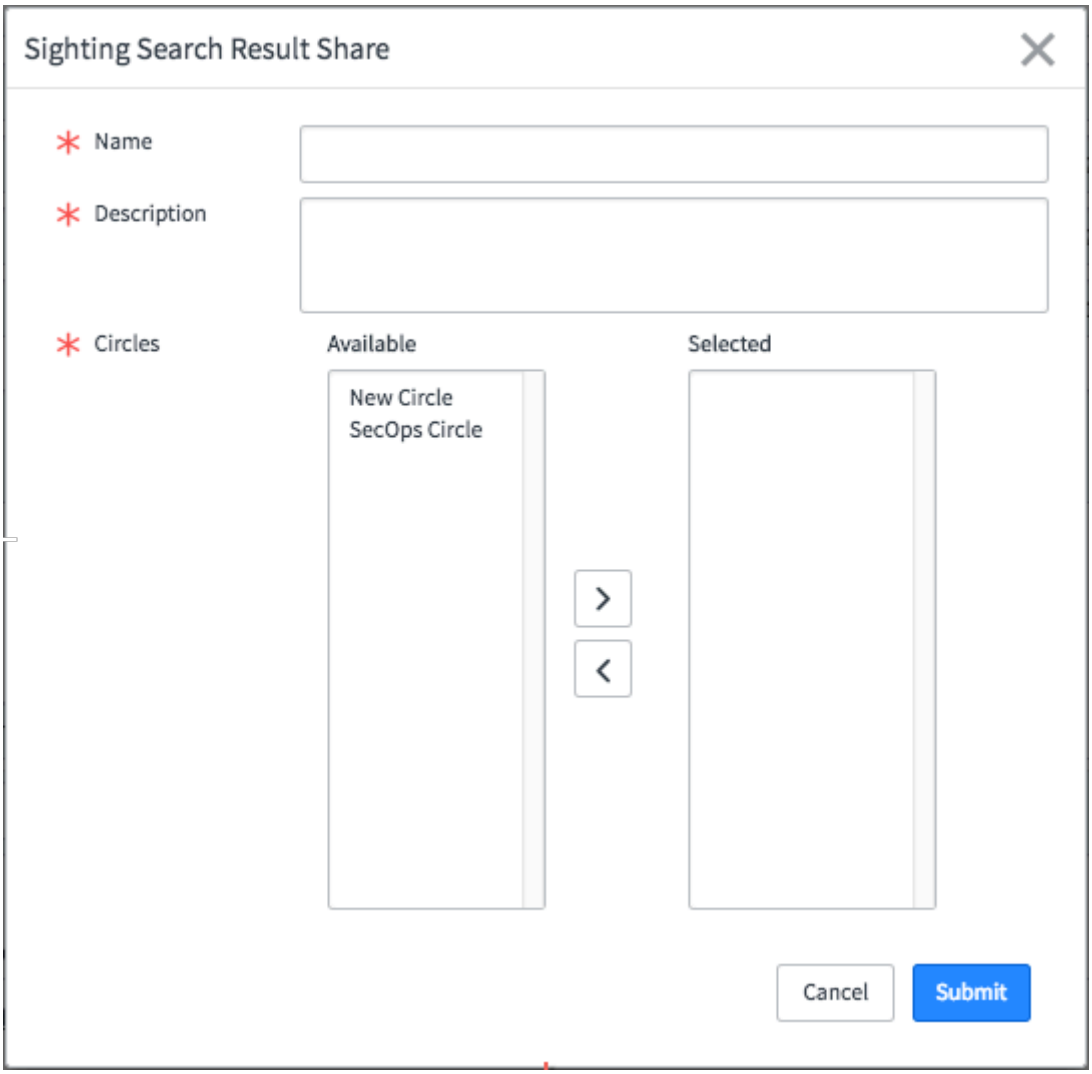
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Auf der **Sichtungssuchergebnis** Klicken Sie auf das Formular **Geben Sie das Sichtungssuchergebnis frei** Zugehöriger Link.
   Das Dialogfeld „Sichtungssuchergebnis freigeben“ wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Geben Sie ein **Name** Für diesen freigegebenen Datensatz des erkennbaren Elements.
6. Geben Sie ein **Beschreibung** Der freizugebenden erkennbaren Elemente.
7. Wählen Sie Aus **Kreise** Um die erkennbaren Elemente für freizugeben.
8. Klicken Sie auf **Absenden**.
   Die erkennbaren Elemente werden für den angegebenen vertrauenswürdigen Kreis freigegeben.

Geben Sie erkennbare Elemente aus einem Security Incident frei

Erkennbare Elemente können von einem Security Incident in freigegeben werden Security Incident Response An Mitglieder in Ihrem vertrauenswürdigen Kreis.

Vorbereitungen

Erforderliche Rolle: sn_si.Analyst

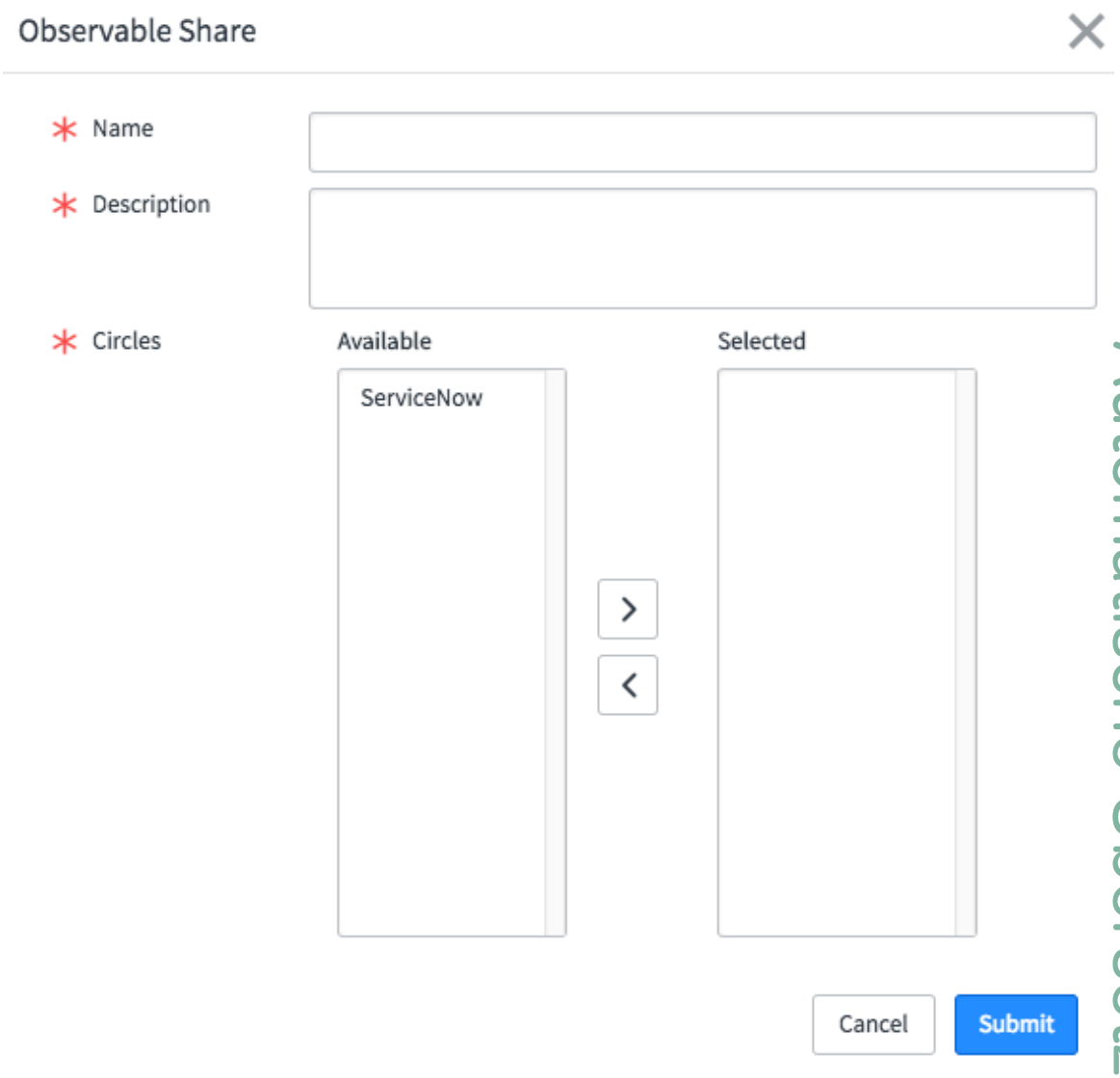
Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie aus **Erkennbare Elemente** Registerkarte von **IOC anzeigen** Zugehörige Listengruppe.
3. Klicken Sie auf ein erkennbares Element.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Auf der **Erkennbares Element** Formular Klicken Sie auf **Erkennbares Element freigeben** Zugehöriger Link.
   Das Dialogfeld „Freigabe erkennbarer Elemente“ wird angezeigt.



5. Geben Sie ein **Name** Für diesen Bedrohungsfreigabedatensatz.
6. Geben Sie ein **Beschreibung** Der ausgewählten erkennbaren Elemente.
7. Wählen Sie Aus **Kreise** Um die erkennbaren Elemente für freizugeben.
8. Klicken Sie auf **Absenden**.
   Die erkennbaren Elemente werden für den angegebenen vertrauenswürdigen Kreis freigegeben.
9. Sie können die Datensätze der Bedrohungsfreigabe anzeigen, indem Sie auf klicken **Bedrohungsfreigaben** Registerkarte.
10. Wenn eines der freigegebenen erkennbaren Elemente Sichtungen enthält, werden die Sichtungen auch freigegeben und können durch Klicken auf angezeigt werden **Sichtungen** Registerkarte.

Sichtungssuchdetails Anzeigen

Überprüfen Sie die Aggregatdetails aller Sichtungssuchen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Warum und wann dieser Vorgang ausgeführt wird
an.

Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie aus **Sichtungssuchdetails** Registerkarte von **IOC anzeigen** Gruppe „zugehörige Liste“ zum Anzeigen der Liste der Sichtungssuchen.

Hinweis:
Diese Daten können für freigegeben werden Trusted Security Circle.

Details einer Sichtungssuche

Detail	Beschreibung
Erkennbares Element	Liste aller erkennbaren Elemente, nach denen nach Abfrage gesucht wird.
Typ des erkennbaren Elements	
Interne Sichtungen	Anzahl der internen Sichtungen für alle Suchen.
Externe Sichtungen	Anzahl der externen Sichtungen für alle Suchen. (Erhalten von Bedrohungsfreigabe.)
Sichtungssuche	Sichtungssuchbezeichner.
Aktualisiert	Datum und Uhrzeit der letzten Änderung.

Sichtungssuchdaten Anzeigen

Überprüfen Sie die aggregierten Daten aller Sichtungssuchen.

Vorbereitungen
Erforderliche Rolle: sn_si.Analyst

Prozedur

1. Navigieren Sie zu einem Security Incident.
2. Wählen Sie aus **Sichtungssuchdaten** Registerkarte von **Alle Zugehörigen Listen Anzeigen** Gruppe „zugehörige Liste“ zum Anzeigen der Liste der Sichtungssuchen.

Hinweis:
Diese Daten können für freigegeben werden Trusted Security Circle.

Sichtungssuchdaten

Ergebnis	Beschreibung
Enddatumsbereich	Zeit, um die Suche nach Sichtungen zu beenden.
Externe Sichtungen	Zusammengefasste Anzahl der externen Sichtungen. (Erhalten von Bedrohungsfreigabe.)
Interne Sichtungen	Zusammengefasste Anzahl der internen Sichtungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis	Beschreibung
Ist lokal	Gibt an, ob die Sichtungen aus der aktuellen oder einer gemeinsam genutzten Umgebung stammen.
Erkennbares Element	Liste aller erkennbaren Elemente, nach denen nach Abfrage gesucht wird.
Sichtungsanzahl	Anzahl der gesuchten Sichtungen.
Sichtungssuche	Sichtungssuchbezeichner.
Detail der Sichtungssuche	Aggregierte Details der Sichtungssuche.
Sichtungssuchlink	Link, der auf das Sichtungssuchportal verweist. Die Suchabfrage wird automatisch angewendet, wenn Sie auf den Sichtungssuchlink klicken.
Sichtungssuchabfrage	Abfrage zur Identifizierung der Instanz. 172.10.0.171 ist ersetzbar und wird im ausgewählten erkennbaren Element ersetzt. (Suche 172.10.0.171 | Head 10) **Hinweis:** Die Auswahl von Tagen gilt nicht für die gespeicherte Suche.

Integration von Security Operations: Fähigkeit zur Bedrohungssuche

Die **Bedrohungssuchen** Die Fähigkeit führt Threat Intelligence-Suchen durch, um festzustellen, ob ein oder mehrere erkennbare Elemente bekannten Sicherheitsbedrohungen zugeordnet sind.

Die **Bedrohungssuchen** Fähigkeit hat einen Workflow, Integration Von Security Operations: Flow Für Bedrohungssuche. Wenn der Fähigkeits-Workflow ausgeführt wird, werden zusätzliche Workflows für die aktivierten Implementierungen ausgeführt. Sie können eine Implementierung angeben, die zum Durchführen einer Suche nach den ausgewählten erkennbaren Elementen verwendet werden soll, oder Sie können die Suche mit allen Implementierungen durchführen.

Hinweis:
Wenn keine Implementierungen verfügbar sind, werden Fähigkeitsaktionen nicht in Produktmenüs angezeigt.

Integration Von Security Operations: Flow Für Bedrohungssuche

Die **Integration Von Security Operations: Bedrohungssuche** Der Fähigkeits-Flow greift auf verfügbare Implementierungen der Bedrohungssuche zu und führt die Implementierungs-Flows aus, die jedem zugeordnet sind, um Bedrohungssuchen ausgewählter erkennbarer Elemente durchzuführen.

Vorbereitungen
Erforderliche Rolle: sn_ti.write

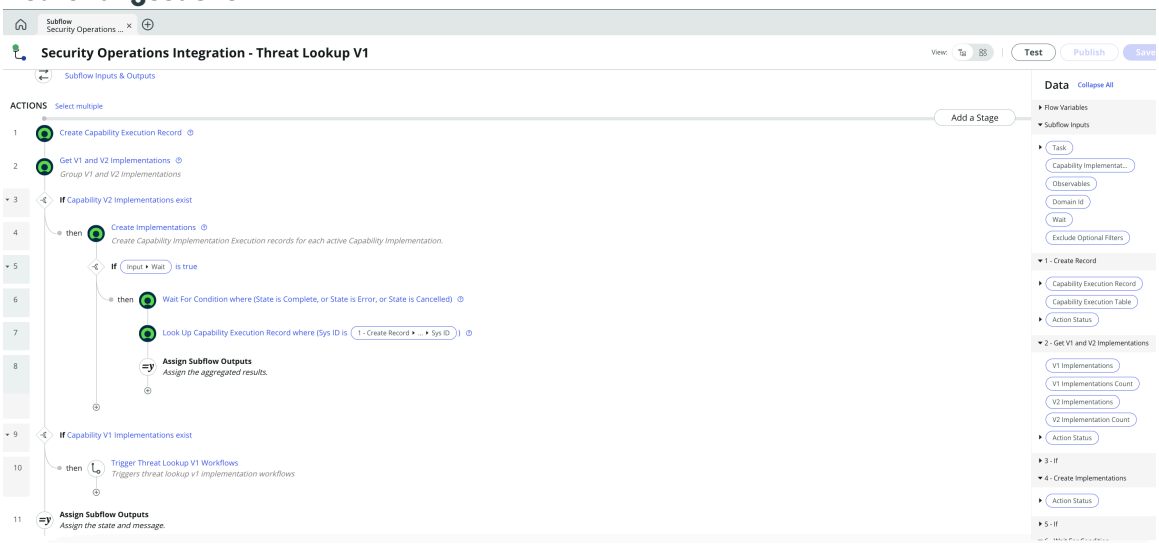
Warum und wann dieser Vorgang ausgeführt wird
Dieser Flow kann auf diese Weise ausgelöst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Indem Sie ein oder mehrere erkennbare Elemente aus der Liste erkennbarer Elemente auswählen und auswählen **Bedrohungssuche ausführen** Von **Aktionen für ausgewählte Zeilen** Auswahlliste.
- Indem Sie einen Datensatz eines erkennbaren Elements öffnen und auf klicken **Bedrohungssuche ausführen** Zugehöriger Link.
- Aus der zugehörigen Liste erkennbarer Elemente in einem Security Incident.

Mit jeder Methode können Sie dann angeben, welche Suchanwendungsimplementierungen zum Scannen der ausgewählten erkennbaren Elemente verwendet werden sollen. Die zugehörigen Implementierungs-Flows werden ausgeführt, um die Suchvorgänge durchzuführen.

Bedrohungssuche



Aktionen, die für diesen Flow spezifisch sind, werden hier beschrieben. Weitere Informationen zu anderen Aktionen finden Sie unter Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten.

Die Flow-Prozessaktionen umfassen:

- Aktion „unterstützte Sicherheitsfähigkeiten abrufen“
- Nachverfolgung der Fähigkeitsausführung: Keine Impls-Aktion

Ändern Sie die Reihenfolge der Flow-Ausführung

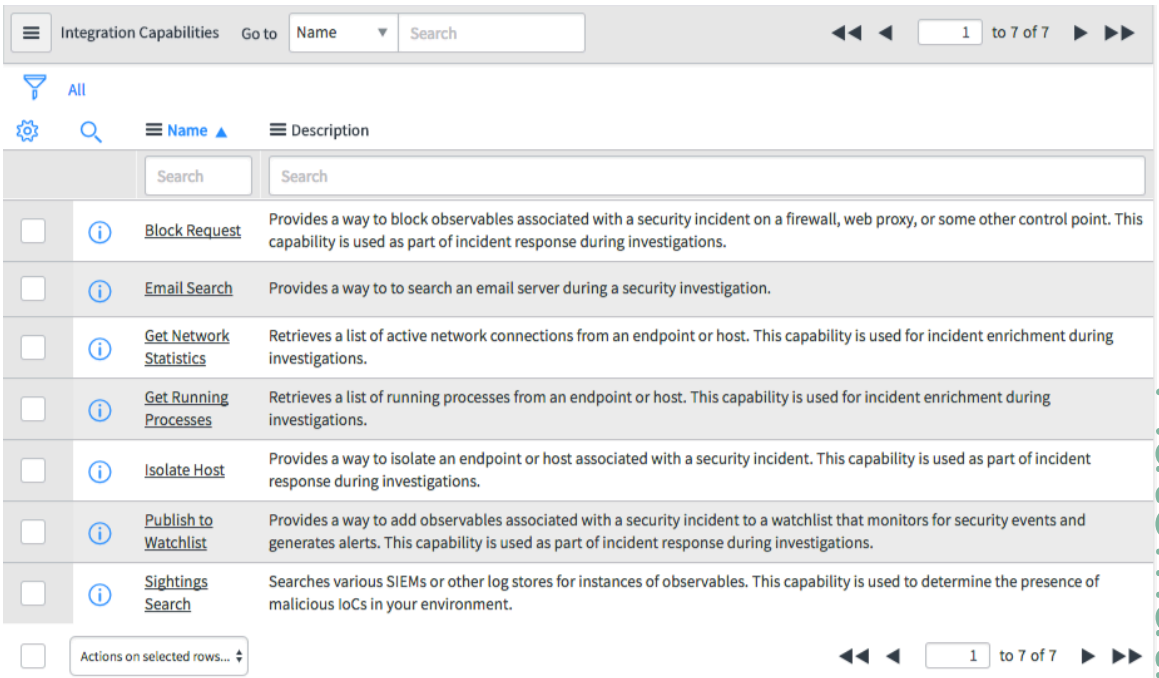
Implementierungen der Integrationsfähigkeit geben den auszuführenden Flow an. Im Basissystem werden Flows sequenziell in der in der Implementierung angegebenen Reihenfolge ausgeführt. Sie können die Reihenfolge nach Bedarf ändern.

Vorbereitungen
Erforderliche Rolle: sn_sec_cmn.write

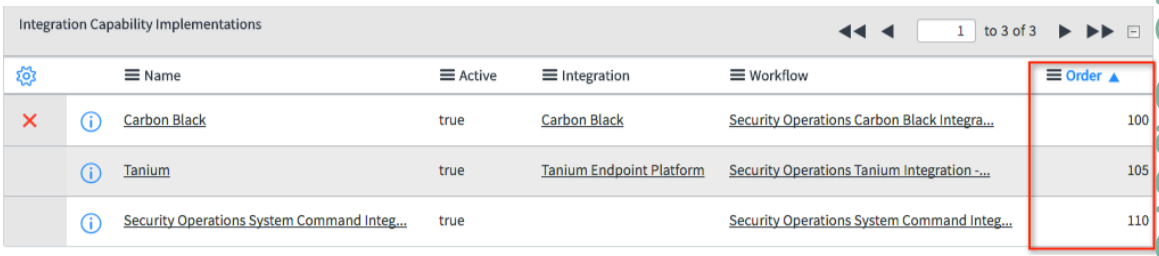
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

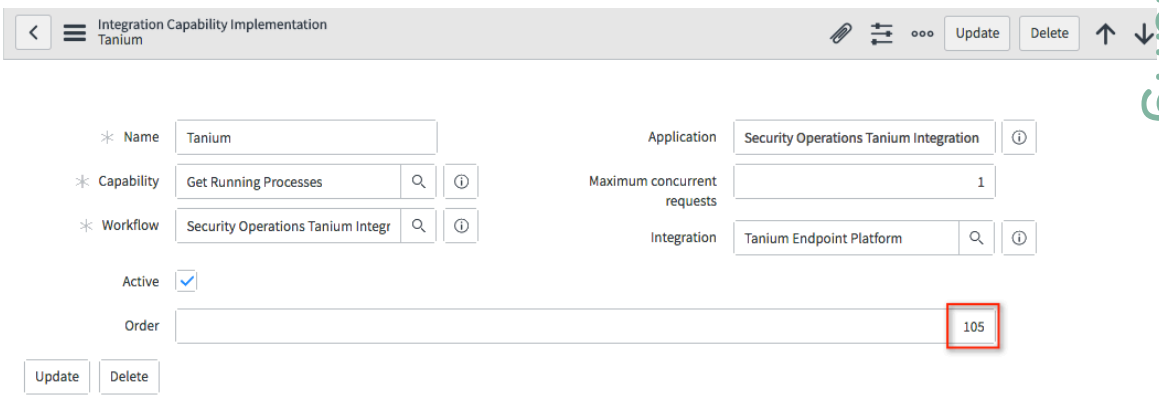
1. Navigieren zu **Alle** > **Security Operations** > **Integrationen** > **Integrationsfunktionen**an.



2. Wählen Sie die Integrationsfähigkeit aus, für die Sie die Ausführungsreihenfolge ändern möchten.



3. Wählen Sie die Implementierung aus, die Sie ändern möchten.



4. Ändern Sie **Reihenfolge** Auf eine höhere oder niedrigere Zahl.
   Niedrigere Zahlen haben eine höhere Ausführungspriorität.

5. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Security Operations-Integrations-Flows und Orchestration-Aktivitäten

Viele der Flows, die Drittpartei-Integrationen zugeordnet sind, enthalten dieselben Aktivitäten. Zum Beispiel Aktivitäten zum Starten und Abschließen der Verarbeitung.

Ausführungsnachverfolgung: Flow-Aktion Starten

Die Flow-Aktion „Ausführungsnachverfolgung – Beginnen“ startet den Auditprozess für einen Security Operations Integrations-Flow, der für erkennbare Elemente funktioniert.

Die Flow-Aktion „Ausführungsnachverfolgung – Beginn“ kann mit jedem Flow verwendet werden, um mit der Aufzeichnung des Fortschritts des Flows in einem Audit zu beginnen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Ein Audit-Datensatz wird erstellt.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
capabilityId	Systembezeichner der auszuführenden Integrationsfähigkeit.
IsImpl	Kennzeichnung, die angibt, ob ein Audit für einen Integrationsfähigkeits-Flow oder einen Implementierungs-Flow für Integrationsfähigkeiten durchgeführt wird. Mögliche Werte: • Falsch: Bezeichnet Audits für einen abstrakten Integrationsfähigkeits-Flow, z. B. Sichtungssuche. (Standard.) • „Wahr“: Bezeichnet das Auditing eines Implementierungs-Flows der Integrationsfähigkeit. Zum Beispiel Splunk oder Elasticsearch.
Aufgaben-ID	Systembezeichner für jede Aufgabe, die dem Flow zugeordnet ist.
Erkennbare Liste	Eine oder mehrere SysIDs des erkennbaren Elements, um die gewünschte Aktion auszuführen. Wird als Flow-Eingabe verwendet.
flowContextId	Systembezeichner des zugehörigen Flow-Kontextdatensatzes. Vom System bereitgestellt.
FlowName	Name des Flows. Vom System bereitgestellt.
ParentCapabilityExcutionId	Systembezeichner des Audit-Datensatzes, der den Implementierungs-Flow gestartet hat. Nur erforderlich für Implementierungs-Flows der Integrationsfähigkeit wie Splunk, Elasticsearch und VirusTotal.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
CapabilityExecutionId	Systembezeichner des Audit-Datensatzes.

- Aktion „unterstützte Sicherheitsfähigkeiten abrufen“
- Nachverfolgung der Fähigkeitsausführung: Keine Impls-Aktion

Nachverfolgung Der Fähigkeitsausführung: Flow-Aktion Abschließen

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Abschließen“ aktualisiert den Audit-Datensatz, wenn der Flow abgeschlossen ist.

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Abgeschlossen“ kann mit jedem Flow verwendet werden, um den Abschluss des Flows aufzuzeichnen.

Hinweis:
Die **Rückgabewert** Array aus dem **Paralleler Startprogramm** Die Core-Flow-Aktion enthält ein Array von Ergebnissen aller ausgeführten Integrations-Flows und fordert den erfolgreichen Abschluss der Ausführungsnachverfolgung auf.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Der Status des Audit-Datensatzes wird auf aktualisiert **Abgeschlossen** .

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
CapabilityExecutionId	Systembezeichner für den Audit-Datensatz. Dieses Feld war die Ausgabe einer der Aktivitäten zum Starten des Audits.
FlowName	Name des Flows. Vom System bereitgestellt.
Nachricht	Abschlussnachricht.

Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachverfolgung Der Fähigkeitsausführung: Fehler-Flow-Aktion

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Fehler“ zeichnet einen Fehler im Audit-Datensatz auf.

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – Fehler“ kann mit jedem Flow verwendet werden, um eine Fehlerbedingung aufzuzeichnen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Der Status des Audit-Datensatzes ist auf festgelegt **Fehler** Und eine Meldung, die angibt, dass der Fehler aufgezeichnet wurde.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
CapabilityExecutionId	Systembezeichner für den Audit-Datensatz. Dies ist die Ausgabe einer der Aktivitäten „Auditing beginnen“.
errorMessage	Meldung, die den Grund für den Fehler angibt.
FlowName	Name des Flows. Vom System bereitgestellt.

Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

Fähigkeit: CIs-Aktivität bestimmen

Die Workflow-Aktivität „Fähigkeit – CIs bestimmen“ bestimmt, welche Konfigurationselemente (Configuration Items, CIs) in den Workflow aufgenommen werden sollen.

Die Aktivität „Fähigkeit – CIs bestimmen“ kann mit jedem Workflow verwendet werden, um zu bestimmen, welche CIs in den Workflow aufgenommen werden sollen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Konfigurationselemente gefunden.
Fehler	Keine CIs gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
task_sys_id	Aufgabenbezeichner (ordnet Security Incident CIs zu).
cis_betroffen	Konfigurationselemente.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
cis_betroffen	Gefilterte CIs
task_sys_id	Aufgabenbezeichner (ordnet Security Incident CIs zu).

Flow-Aktion „Ergänzungsdatensätze erstellen“

Die **Erstellen Sie Ergänzungsdatensätze** Flow-Aktion erstellt oder aktualisiert Ergänzungsdatensätze zur Verwendung im Flow.

Die **Erstellen Sie Ergänzungsdatensätze** Die Flow-Aktion kann mit jedem Flow verwendet werden, um Ergänzungsdatensätze im Flow zu aktualisieren.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Ergänzungsdatensatz aktualisiert.
Fehler	Ergänzungsdatensatz nicht aktualisiert. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Variable	Beschreibung
task_id	Aufgabenbezeichner.
Content	Rohinhalt (Daten laufender Prozesse).
enrichment_mapping_id	Bezeichner der Ergänzungszuordnung.
ci_id	Konfigurationselement-Bezeichner.
Reference_value	Nicht Verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ergebnis	GlideRecords, die mit dem Skript „enrichmentUtils“ erstellt wurden.

FQDN-Flow-Aktion für Konfigurationselement abrufen

Die zugehörigen Listen namens **Allgemeine Sicherheits-Orchestration** > **Konfigurationselement-FQDN abrufen** Flow-Aktion ruft den vollqualifizierten Domänennamen (FQDN) eines Konfigurationselements ab. Diese Flow-Aktion kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Flow-Aktion „Konfigurationselement-FQDN abrufen“ kann mit jedem Flow verwendet werden, um den vollqualifizierten Domänennamen (FQDN) eines Konfigurationselements abzurufen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Flow-Aktion.

Eingabevariablen

Variable	Beschreibung
cmdb_ci.ID [Zeichenfolge]	Der Systembezeichner (sys_ID) eines Konfigurationselementdatensatzes.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
fqdn [Zeichenfolge]	Der vollqualifizierte Domänenname (FQDN) des Konfigurationselements.

Zusätzliche Hinweise

Das fqdn-Feld im Konfigurationselement muss ausgefüllt werden.

Bestimmen Sie die Aktivität erkennbarer Elemente

Die **Bestimmen Sie Erkennbare Elemente** Die Workflow-Aktivität bestimmt, welches erkennbare Element in den Workflow aufgenommen werden soll

Die **Bestimmen Sie Erkennbare Elemente** Aktivität kann mit jedem Workflow verwendet werden, um zu bestimmen, welche erkennbaren Elemente in den Workflow aufgenommen werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Erkennbare Elemente gefunden
Fehler	Keine erkennbaren Elemente gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
task_sys_id	Aufgabenbezeichner (ordnet Security Incident erkennbaren Elementen zu).
Erkennbare Elemente	IP-Adressen, Hash, URLs, Domänennamen.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Erkennbare Elemente	Gefilterte erkennbare Elemente

Aktion „unterstützte Sicherheitsfähigkeiten abrufen“

Die Flow-Aktion „unterstützte Fähigkeiten abrufen“ ruft den Namen und die Anzahl der Integrationen ab, die aktiv sind und die angeforderte Fähigkeit unterstützen.

Die Aktion „unterstützte Fähigkeiten abrufen“ kann mit jedem Flow verwendet werden, um zu bestimmen, welche Fähigkeiten unterstützt werden.

Ergebnisse

Mögliche Ergebnisse für diese Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Integration, die die gefundene Fähigkeit unterstützt.
Fehler	Beim Versuch, eine aktive Integration zu finden, die die Fähigkeit unterstützt, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktionsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
capabilityName	Name der Fähigkeit.
Aufgaben-ID	Systembezeichner für jede Aufgabe, die dem Flow zugeordnet ist.
domainId	Systembezeichner für eine beliebige Domäne, die dem Flow zugeordnet ist.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Unterstützte Fähigkeiten	Liste der Integrationen, die die Fähigkeit unterstützen.
CapabilityCount	Anzahl der Integrationen, die die Fähigkeit unterstützen.

Nachverfolgung der Fähigkeitsausführung: Keine Impls-Aktion

Die Flow-Aktion „Nachverfolgung der Fähigkeitsausführung – keine Verbesserungen“ erstellt einen Fehlerdatensatz, wenn keine Implementierung der Integrationsfähigkeit gefunden wird.

Die Aktion Nachverfolgung der Fähigkeitsausführung – keine Verbesserungen kann mit jedem abstrakten Integrationsfähigkeits-Flow verwendet werden, um die Fehlerbedingung zu behandeln, wenn keine konfigurierte Fähigkeitsimplementierung verfügbar ist.

Ergebnisse

Mögliche Ergebnisse für diese Aktion:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Der Status des Ausführungsnachverfolgungsdatensatzes ist auf festgelegt **Fehler** Und eine Meldung, die angibt, dass der Fehler aufgezeichnet wurde.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
CapabilityExecutionId	Systembezeichner für den Audit-Datensatz. Ausgabe der Aktion, die zum Starten der Ausführungsnachverfolgung verwendet wird.
FlowName	Name des Flows. Vom System bereitgestellt.

Ausgabevariablen

Es sind keine Ausgabevariablen vorhanden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Compliance-Suchaktion Erstellen

Die Aktion Compliance-Suche erstellen erstellt eine Compliance-Suche nach E-Mails auf den angegebenen Exchange-Servern mithilfe der definierten Suchabfragen und gibt den Namen der erstellten Compliance-Suche zurück.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
search_query	Obligatorische Suchabfrage, die verwendet wird, um E-Mails in Exchange Server über alle Postfächer hinweg zu finden.
Austauschstandort	Obligatorisches Standortfeld, das für die Suche nach einem definierten Standort verwendet wird. Werte sind: • Alle • Name des bestimmten Postfachs
targetId	Obligatorisches Feld für Zielhost-Bezeichner, in dem sich der Exchange Server befindet.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response	Name der erstellten Compliance-Suche.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

Austrittsbedingungen

Variable	Beschreibung
Fehler Beim Erstellen Der Suche	Wenn die Sucherstellung aufgrund einer Ausnahme in Exchange Server fehlschlägt.
Suche Erfolgreich Erstellt	Wenn die Sucherstellung erfolgreich ist.
Fehler beim Erstellen der Suche aufgrund eines Analysefehlers	Wenn die Sucherstellung aufgrund eines Analyseproblems fehlschlägt.
Fehler	Wenn in der Flow-Aktion eine Ausnahme auftritt.

IP aus CI-Aktivität abrufen

Diese Workflow-Aktivität bestimmt die IPV4-Adresse, die einem Konfigurationselement (Configuration Item, CI) zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die **IP von CI abrufen** Aktivität kann mit jedem Workflow verwendet werden, um die IPv4-Adresse eines CI abzurufen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
ci_sys_ID [Zeichenfolge]	Systembezeichner des Konfigurationselements

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
ip_addr [Zeichenfolge]	IPv4-Adresse. Wenn die IP-Adresse nicht bestimmt werden kann, ist dieser Wert leer.

Austrittsbedingungen

Mögliche Ergebnisse für diese Aktivität:

Bedingungen

Bedingung	Beschreibung
Erfolg	Eine IPv4-Adresse wurde zurückgegeben.
Fehler	Eine IPv4-Adresse konnte nicht bestimmt werden.

Rufen Sie Netzwerkstatistiken über die netstat-Flow-Aktion ab

Die Flow-Aktion „Allgemeine Sicherheitsorchestration – Netzwerkstatistiken über netstat abrufen“ ruft die Netzwerkstatistiken für eine betroffene Ressource auf einem Windows-basierten System ab. Diese Flow-Aktion kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Flow-Aktion „Netzwerkstatistiken über netstat abrufen“ kann mit jedem Flow verwendet werden, um Netzwerkstatistiken aus einem Windows-basierten System abzurufen. Der Computer wird mit abgefragt **Netstat** Befehl einschließlich **-A** Und **-O** Parameter. So verbessern Sie die Ausgabedaten: **Get-Process** Befehl wird ebenfalls aufgerufen.

Ergebnisse

Mögliche Ergebnisse für diese Flow-Aktion:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Netzwerkstatistiken wurden im JSON-Format abgerufen.
Fehler	Beim Versuch, Netzwerkstatistiken abzurufen, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Ausgabefehler der Flow-Aktion verfügbar.

Eingabevariablen

Variable	Beschreibung
Ziel [Zeichenfolge]	Der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse des Zielsystems.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Antwort [Zeichenfolge]	Eine JSON-Zeichenfolge, die die aktuell laufenden Prozesse auf dem Zielcomputer darstellt. JSON-Daten umfassen: **pid** Prozessbezeichner **Lokaler _Port** Lokaler Port für die Netzwerktransaktion **Status** Status der TCP-Verbindung. **Hinweis:** Dieses Feld ist für UDP-Verbindungen null. **Local_address** Lokaler vollqualifizierter Domänenname (FQDN) oder IP-Adresse **Remote_address** Vollqualifizierter Remote-Domänenname (FQDN) oder IP-Adresse **protocol** TCP oder UDP **Remote_Port** Remote-Port der Netzwerktransaktion **path** Der Dateipfad der ausführbaren Prozessdatei **Hash**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen (Fortsetzung)

Variable	Beschreibung
	Der Hash-Wert der ausführbaren Prozessdatei. Der Hash befindet sich in SHA-256 für PowerShell V4 oder höher. Andernfalls befindet sich der Hash in MD5.

Beschränkungen

Der MID-Server muss unterstützen PowerShell .

SHA-256-Hash erfordert PowerShell V4.

Rufen Sie laufende Prozesse über die WMI-Aktivität ab

Die **Laufende Prozesse Abrufen** Workflow-Aktivität ruft die laufenden Prozesse eines Konfigurationselements auf einem Windows-basierten System ab. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die **Rufen Sie laufende Prozesse über WMI ab** Aktivität kann mit jedem Workflow verwendet werden, um laufende Prozesse auf einem Windows-basierten System abzurufen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Ziel [Zeichenfolge]	Der vollqualifizierte Domänenname (FQDN) oder die IP-Adresse des Zielsystems.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Antwort [Zeichenfolge]	Eine JSON-Zeichenfolge, die die aktuell laufenden Prozesse auf dem Zielsystem darstellt. JSON-Daten umfassen: **pid** Der Prozessbezeichner **name** Der Name des Prozesses Außerdem, falls verfügbar: **Besitzer** Der Name des Prozessbesitzers

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausgabevariablen (Fortsetzung)

Variable	Beschreibung
	Owner_sid Der Systembezeichner des Prozessbesitzers **Owner_Domain** Die Domäne des Prozessbesitzers **path** Der Dateipfad der ausführbaren Prozessdatei **Hash** Der Hash-Wert der ausführbaren Prozessdatei. Der Hash befindet sich in SHA-256 für PowerShell V4 oder höher. Andernfalls befindet sich der Hash in MD5.

Beschränkungen

Der MID-Server muss unterstützen **PowerShell** .

SHA-256-Hash erfordert PowerShell V4.

Aktion „Compliance-Suchstatus Überprüfen“

Mit der Aktion Compliance-Suchstatus überprüfen wird der Status der erstellten Compliance-Suche auf dem Exchange-Server überprüft. Wenn der Status „Abgeschlossen“ lautet, werden die Informationen zur E-Mail-Suche zurückgegeben, die für die Compliance-Suche gefunden wurden.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktion.

Variable	Beschreibung
targetId	Obligatorisches Feld für Zielhost-Bezeichner, in dem sich der Exchange Server befindet.
SearchName	Obligatorischer Name der Compliance-Suche, die auf dem Exchange-Server erstellt wurde.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktionen verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
response	Enthält den Status der Compliance-Suche und die Anzahl der E-Mails, die auf dem Exchange-Server für die Compliance-Suche gefunden wurden.

Austrittsbedingungen

Mögliche Austrittsbedingungen für diese Aktion sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Austrittsbedingungen

Variable	Beschreibung
Suche Wird Ausgeführt	Wenn der Status der Compliance-Suche „in Bearbeitung“ lautet.
Suche Abgeschlossen: Keine Bedrohungs-E-Mails Gefunden	Wenn der Status der Compliance-Suche abgeschlossen ist und keine E-Mails als Teil der Compliance-Suche gefunden werden.
Suche Abgeschlossen: Bedrohungs-E-Mails Gefunden	Wenn der Status der Compliance-Suche abgeschlossen ist und E-Mails als Teil der Compliance-Suche gefunden werden.
Fehler Beim Überprüfen Des Status	Wenn die Statusüberprüfung aufgrund einer Ausnahme im Exchange-Server fehlschlägt.
Fehler	Wenn in der Flow-Aktion eine Ausnahme auftritt.

Aktivität „Aufgabenarbeitsnotizen“ aktualisieren

Die **Allgemeine Sicherheitsorchestration: Aufgabenarbeitsnotizen Aktualisieren** Die Workflow-Aktivität aktualisiert den **Aktivität** Abschnitt (Arbeitsnotizen) eines Aufgabendatensatzes. Dies ist nützlich für die Protokollierung von Informationen.

Die **Aktualisieren Sie Aufgabenarbeitsnotizen** Aktivität kann mit jedem Workflow verwendet werden, um die Arbeitsnotizen eines beliebigen Aufgabendatensatzes zu aktualisieren.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Task_ID [Zeichenfolge]	Der Systembezeichner (sys_ID) eines Aufgabendatensatzes.
Inhalt [Zeichenfolge]	Die Daten, die in die Arbeitsnotizen einer Aufgabe geschrieben wurden.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ergebnis [Zeichenfolge]	Gibt an, ob die Aktualisierung erfolgreich war.

Rollup der Suchinformationen zur Security Incident-Aktivität

Die **Rollup der Suchinformationen zu Security Incident** Aktivität kann mit jedem Workflow verwendet werden, um Informationen aus einer Bedrohungssuche zu sammeln und eine Zusammenfassung des Inhalts sowie die ID des ursprünglichen Security Incident in den Arbeitsnotizen der Aufgabe auszugeben.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Zusammenfassung des Suchberichts für Security Incident zusammengefasst.
Fehler	Ursprungsaufgabe und Suchzusammenfassungsbericht sind leer.

Eingabevariablen

Variable	Beschreibung
Scan-ID[Zeichenfolge]	Suchbezeichner.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
SiId[Zeichenfolge]	Security Incident-Bezeichner.
Antwort [Zeichenfolge]	Zusammenfassung der Suchergebnisse, einschließlich IOC-Wert, Ergebnis, Fehlergrund, Suchreferenz usw.

Aktualisieren Sie den Security Incident mit dem Workflow für Suchergebnisse

Die **Aktualisieren Sie Security Incident mit Suchergebnissen** Workflow aktualisiert vorhandene Security Incidents mit Suchergebnissen.

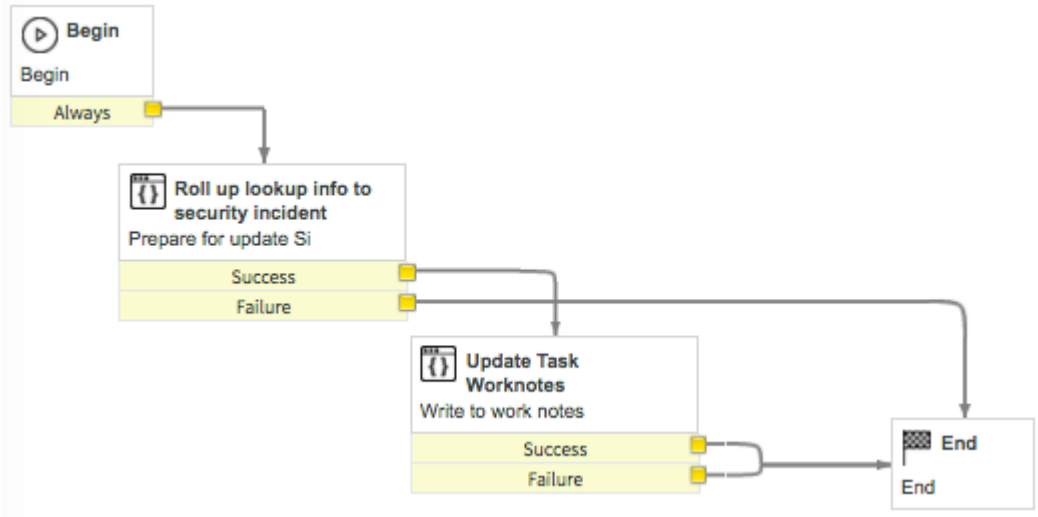
Vorbereitungen
Erforderliche Rolle: sn_si.Basic

Warum und wann dieser Vorgang ausgeführt wird
Dieser Workflow wird durch eine Business-Regel in der Suchtabelle ausgelöst, die überwacht, wann der verwendet wird **Ergebnis** Feld ändert sich in „Fehlgeschlagen“.

Workflow-Prozessaktivitäten umfassen:

- Rollup der Suchinformationen zur Security Incident-Aktivität
- Aktivität „Aufgabenarbeitsnotizen“ aktualisieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Filtern Sie die Aktivität der auf der Liste aufgeführten erkennbaren Elemente

Die Workflow-Aktivität „gefilterte Allow List erkennbare Elemente“ entfernt erkennbare Elemente, die aus der Liste der erkennbaren Elemente ignoriert werden können. Diese Aktivität kann den Untersuchungs- und Korrekturprozess beschleunigen.

Die Aktivität „Allow list erkennbare Elemente filtern“ kann mit jedem Workflow verwendet werden, um erkennbare Elemente zu filtern, bevor eine Aktion ausgeführt wird.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	Filterliste erstellt.
Fehler	Beim Versuch, die erkennbaren Elemente zu filtern, ist ein Fehler aufgetreten. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
Erkennbare Elemente	Liste der verfügbaren erkennbaren Elemente.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
GefiltertObservables	Gefilterte erkennbare Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schreiben Sie Inhalt als Anhangsaktivität in den Datensatz

Diese Aktivität schreibt den aus einer Eingabe übergebenen Inhalt und erstellt einen festgelegten Anhang für einen bestimmten Datensatz.

Die **Schreiben Sie den Inhalt als Anhang in den Datensatz** Aktivität kann mit jedem Workflow verwendet werden, um Inhalte zu schreiben und an einen Datensatz anzuhängen.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Eingabevariablen

Variable	Beschreibung
Tabellenname [Zeichenfolge]	Der Tabellenname für den Datensatz. Dieses Eingabefeld ist ein Pflichtfeld.
Sysid [Zeichenfolge]	Der Systembezeichner (sys_ID) eines Aufgabendatensatzes. Dieses Eingabefeld ist ein Pflichtfeld.
Nutzlast	Der nur-Text-Inhalt, der als Anhang geschrieben werden soll. Dieses Eingabefeld ist ein Pflichtfeld.
filename	Der Name der Anhangsdatei.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
Ergebnis [Zeichenfolge]	Gibt an, ob die Aktualisierung erfolgreich war.

IP aus CI-Aktivität abrufen

Die Flow-Aktivität „IP aus CI abrufen“ erfasst die IP-Adresse aus Configuration Items (CIs), die im Flow verwendet werden sollen.

Die Aktivität „IP aus CI abrufen“ kann mit jedem Flow verwendet werden, um CI-IP-Adressen (Configuration Item) zu erfassen, die im Flow verwendet werden sollen.

Ergebnisse

Mögliche Ergebnisse für diese Aktivität:

Ergebnisse

Ergebnis	Beschreibung
Erfolg	IP-Adressen gefunden.
Fehler	Keine IP-Adressen gefunden. Weitere Fehlerinformationen sind im Aktivitätsausgabefehler verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabevariablen

Eingabevariablen bestimmen das anfängliche Verhalten der Aktivität.

Variable	Beschreibung
ci_sys_id	Konfigurationselement-Bezeichner.

Ausgabevariablen

Die Ausgabevariablen enthalten Daten, die in nachfolgenden Aktivitäten verwendet werden können.

Ausgabevariablen

Variable	Beschreibung
ip_addr	IP-Adressen.

Security Operations Workflow-Auslöser

Security Operations Workflow-Auslöser enthalten eine Bedingung für eine Tabelle. Alle an den Workflow-Auslöserdatensatz angehängten Workflows werden ausgeführt, wenn die Bedingung erfüllt ist.

Erstellen Security Operations Workflow-Auslöser

Erstellen Sie einen Workflow-Auslöser, der eine Bedingung für eine Tabelle enthält.

Vorbereitungen

Security Operations Enthält mehrere Workflow-Auslöser im Basissystem:

Konfigurationselement ändert sich bei einem aktiven Security Incident

Verwendet die Integration, um CI-bezogene Daten anzureichern, wenn sich Konfigurationselemente ändern.

Angreifbare Gruppe erneut scannen

Scannt eine angreifbare Gruppe mit erneut Scan-Schwachstellen-Workflow, Wenn Sie **Schließen/Ignorieren** Die Gruppe.

Angreifbares Element erneut scannen

Scannt ein angreifbares Element mit erneut Scan-Workflow für Schwachstellenelement Wenn Sie **Schließen/Ignorieren** Das Element.

Erforderliche Rollen:

- Zu lesen: sn_sec_cmn.read
- So erstellen oder aktualisieren Sie: sn_sec_cmn.write
- Zum Löschen: sn_sec_cmn.admin

Prozedur

1. Navigieren zu **Alle** > **Security Operations** > **Dienstprogramme** > **Workflow-Auslöser**an.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die entsprechenden Felder im Formular aus.

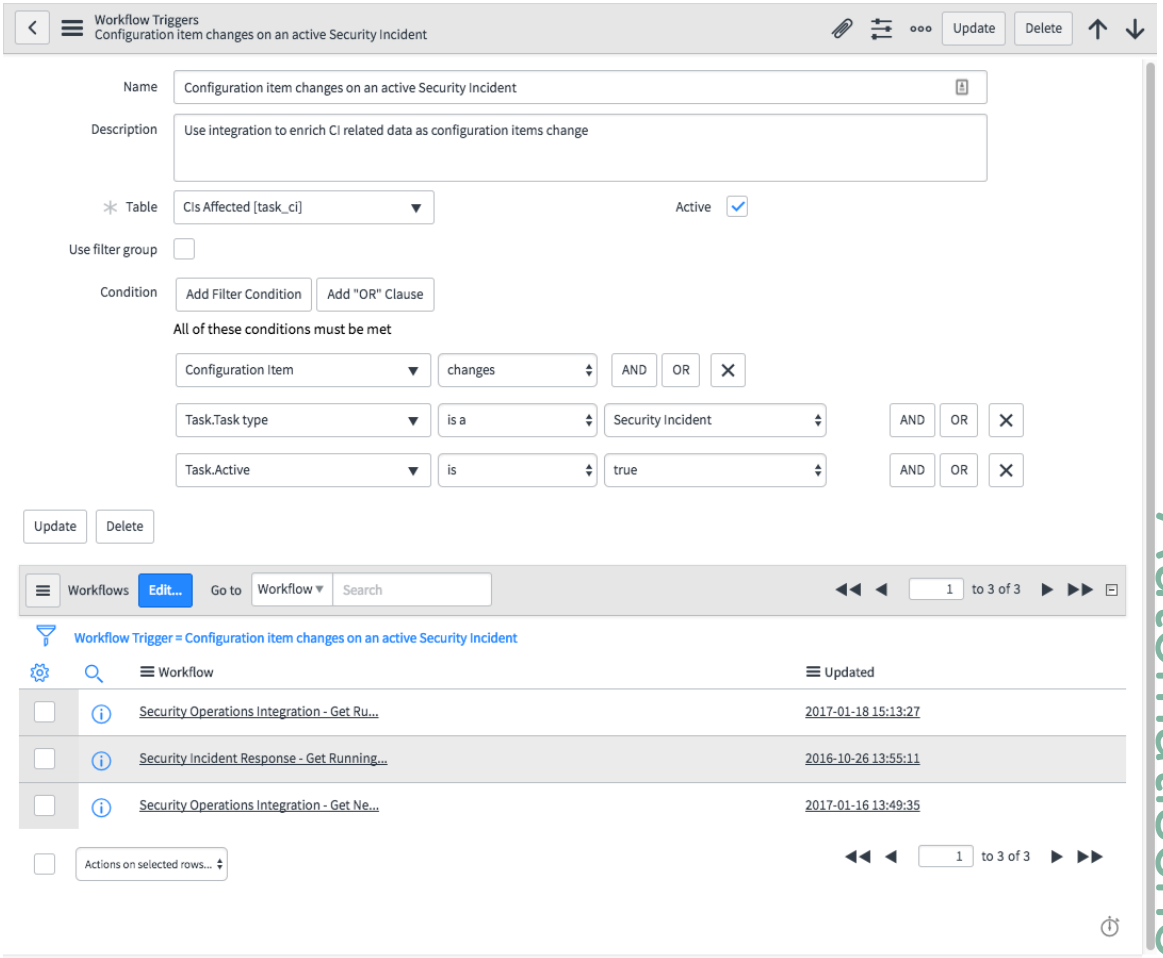
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow-Auslöser

Feld	Beschreibung
Name	Der Name des Workflow-Auslösers.
Beschreibung	Geben Sie eine Beschreibung für den Workflow-Auslöser ein.
Tabelle	Die Tabelle, die den Workflow-Auslöser enthält. Wenn Sie ausgewählt haben **Verwenden Sie die Filtergruppe** Kontrollkästchen und eine Filtergruppe ausgewählt. Dieses Feld wird standardmäßig auf die Tabelle gesetzt, die der ausgewählten Filtergruppe zugeordnet ist.
Bedingung	Verwenden Sie den Bedingungsgenerator Zum Definieren der Kriterien für den Workflow-Auslöser. Wenn Sie ausgewählt haben **Verwenden Sie die Filtergruppe** Aktivieren Sie das Kontrollkästchen, und wählen Sie eine Filtergruppe aus, die **Bedingung** Felder werden nicht angezeigt.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um den Workflow-Auslöser zu aktivieren.
Filtergruppe verwenden	Aktivieren Sie dieses Kontrollkästchen, um eine vordefinierte Filtergruppe oder zu verwenden Erstellen Sie eine neue Filtergruppe Zum Definieren der Workflow-Auslöserkriterien.
Filtergruppe	Wählen Sie die Filtergruppe aus, die zum Definieren von Workflow-Auslösern verwendet werden soll. Dieses Feld wird nur angezeigt, wenn **Verwenden Sie Filtergruppen** Das Kontrollkästchen ist aktiviert.

4. Wenn Sie Ihre Einträge abgeschlossen haben, klicken Sie mit der rechten Maustaste in den Formularheader, und wählen Sie aus **Speichern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die **Workflows** Die Registerkarte wird angezeigt. Enthält Workflows, die ausgeführt werden, wenn alle Filterbedingungen oder Filtergruppenbedingungen erfüllt sind.

5. Führen Sie diese Schritte aus, um Workflows hinzuzufügen.
   a. In **Workflows** Klicken Sie auf die Registerkarte **Bearbeiten** .
   b. Verwenden Sie bei Bedarf den Bedingungsgenerator, um die Workflows zu suchen, die Sie auswählen möchten, oder verwenden Sie den Slushbucket, um Workflows auszuwählen und in die Workflows-Liste zu verschieben.
   c. Klicken Sie auf **Speichern**.
   Die ausgewählten Workflows werden hinzugefügt.
6. Klicken Sie auf **Aktualisieren**.

Orchestration für Security Operations

Benutzer können mithilfe von Aktivitätspaketen und -Workflows in mit Windows- oder UNIX-basierten Systemen und -Umgebungen interagieren und Daten aus diesen abrufen Security Operations Orchestration.

Security Operations Orchestration Zeitersparnis durch die Eliminierung manueller Prozesse und das Abrufen kontextbezogener Informationen zur Behebung von Incidents. Die Security Operations Produkte verfügen über Standard-Aktivitätspakete und -Workflows, die in jedem der Plugins enthalten und aktiviert sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um zusätzliche Orchestration-Aktivitäten zu erstellen und darauf zuzugreifen, die mit dem Standardangebot nicht verfügbar sind Security Operations Produkte erwerben Sie eine vollständige Orchestration-Lizenz.

- Security Incident Response Orchestration Workflows:
  - Security Incident Response: Flow „Netzwerkstatistiken abrufen“
  - Integration von Security Operations-Systembefehlen: Flow „laufende Prozesse abrufen“
  - Erstellen Sie einen Suchanforderung für IOC-Changes-Workflow
  - Integration von Security Operations – Flow für E-Mail-Suche und -Löschung
- Threat Intelligence Orchestration Workflows:
  - Threat Intelligence – Workflow für IOC-Suche ausführen
  - Aktualisieren Sie den Security Incident mit dem Workflow für Suchergebnisse
- Vulnerability Response Orchestration Workflows:
  - Scan-Schwachstellen-Workflow
  - Scan-Workflow für Schwachstellenelement

[store-future: BEGIN review]

Security Operations Szenarien und Beispiele

Die ServiceNow® Security Operations Produkte können leicht verstanden werden, indem Sie sich einige Szenarien ansehen. Diese Szenarien stellen Funktionen dar, die Sie bei der Verwendung der Produkte verwenden können. Sie sollen Sie über die Leistung und Flexibilität dieser Produkte informieren.

[End]
[store-future: BEGIN review]

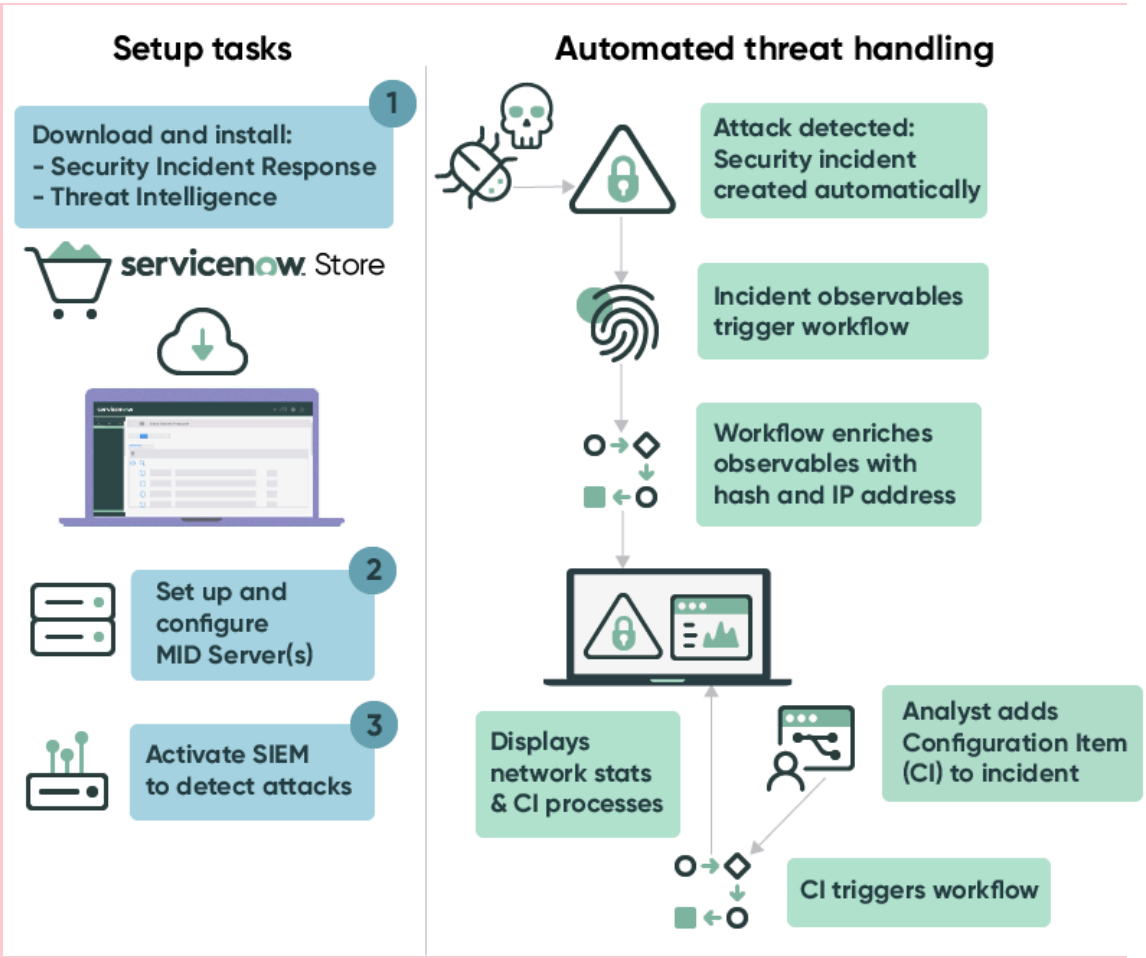
Reduzieren Sie die Zeit für die Bedrohungsanalyse durch Automatisierung

Die Selektierung und Analyse von Security Incidents sind erforderliche Schritte, um während des Bedrohungsreaktionsprozesses falsch positive Ergebnisse auszugleichen und zu bestimmen, wie Sie Sicherheitsbedrohungen am besten identifizieren, eindämmen und beseitigen können.

Selektierung kann manuelle Schritte umfassen, um die Ursachen und Auswirkungen von Bedrohungen aufzudecken. Durch die Automatisierung vieler Schritte können Sie den Zeit- und Arbeitsaufwand für die Analyse und Eindämmung von Bedrohungen erheblich reduzieren. Nachdem Sie die Automatisierung in eingerichtet haben ServiceNow® Security Operations Software können Sie verschiedene Automatisierungstypen ausführen. Sie können beispielsweise Daten erkennbarer Elemente automatisch anreichern, wenn einem Security Incident ein erkennbares Element hinzugefügt wird. Oder Sie können laufende Prozesse anzeigen oder Netzwerkstatistiken abrufen, wenn ein CI in Ihrer CMDB einem Security Incident hinzugefügt wird. Diese unten dargestellten Prozesse können Ihnen wertvolle Zeit während der Bedrohungsanalyse sparen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



In diesem Szenario wurde eine schädliche Datei vom SIEM-Tool (Security Information and Event Management) erkannt, das Ihr Unternehmen für die Bedrohungserkennung verwendet. Die Security Operations Die Integration mit SIEM bewirkt, dass basierend auf dem Typ der aufgetretenen Bedrohung automatisch ein Security Incident erstellt wird. Wenn die schädliche Datei bereits erkennbare Elemente enthielt oder der Sicherheitsanalysten neue, nicht abgelaufene erkennbare Elemente hinzugefügt hat, wird automatisch ein Workflow ausgelöst, der die Datensätze erkennbarer Elemente ergänzt. Der Workflow bewirkt, dass die erkennbaren Elemente gescannt werden, und der Hash und die IP-Adresse der Partei, die die Datei gesendet hat, werden dem Security Incident hinzugefügt.

Während der Selektierung kann der Analyst feststellen, dass Konfigurationselemente (CI), die in der CMDB des Unternehmens enthalten sind, von dem Angriff betroffen waren. Der Analyst fügt daher die CIs dem Security Incident hinzu. Wenn der Security Incident gespeichert wird, werden zwei weitere Workflows ausgeführt, und Netzwerkstatistiken und laufende Prozesse im Zusammenhang mit den CIs werden dem Security Incident sofort hinzugefügt.

[End]

Bereiten Sie sich auf vor Threat Intelligence Automatisierung

Vor Threat Intelligence Automatisierung kann im Bedrohungsreaktionsprozess verwendet werden. Sie müssen einige vorläufige Setup-Schritte ausführen. Wenn das Setup abgeschlossen ist, werden die Workflows automatisch mit wenig oder ohne Anwenderunterstützung ausgeführt.

Vorbereitungen

Erforderliche Rolle: Administrator

Automatische Übersetzung

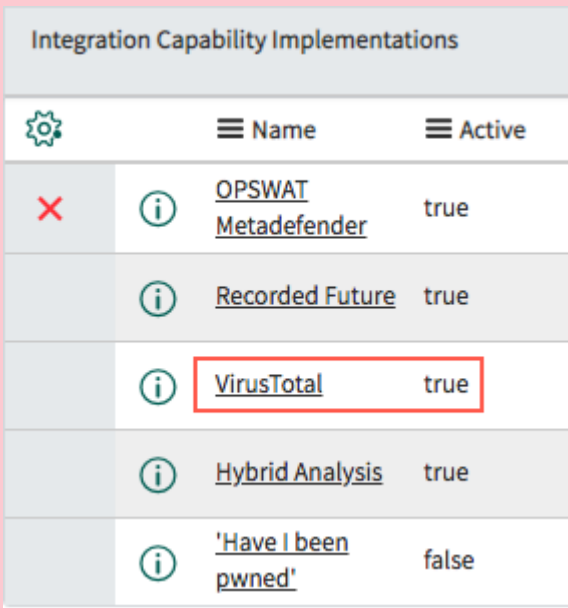
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Laden Sie herunter Security Incident Response und Threat Intelligence Anwendungen aus dem ServiceNow Storean.
2. Installieren Sie einen oder mehrere MID-Server , Und Konfigurieren Sie Service-Anmeldeinformationen für jeden von ihnen .
3. Wenn die MID-Server ausgeführt werden, stellen Sie sicher, dass die von Ihnen verwendete Integrationsfähigkeitsimplementierung (z. B. VirusTotal) für die Bedrohungssuchfunktion aktiv ist. Die Funktion „Bedrohungssuche“ führt Suchen durch, um festzustellen, ob ein oder mehrere erkennbare Elemente bekannten Sicherheitsbedrohungen zugeordnet sind.

   a. Navigieren zu **Security Operations** > **Integrationen** > **Integrationsfunktionen**an.

   b. Klicken Sie Auf **Bedrohungssuche** Und scrollen Sie nach unten zur zugehörigen Liste Implementierung der Integrationsfähigkeit.



   c. Suchen Sie die Implementierung, die Sie verwenden möchten, und überprüfen Sie, ob die -Implementierung **Aktiv** Spalte wird angezeigt **Wahr** .

   d. Wenn die Implementierung nicht aktiv ist, klicken Sie auf die Implementierung **Name** , Klicken Sie, um auszuwählen **Aktiv** Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Aktualisieren** .

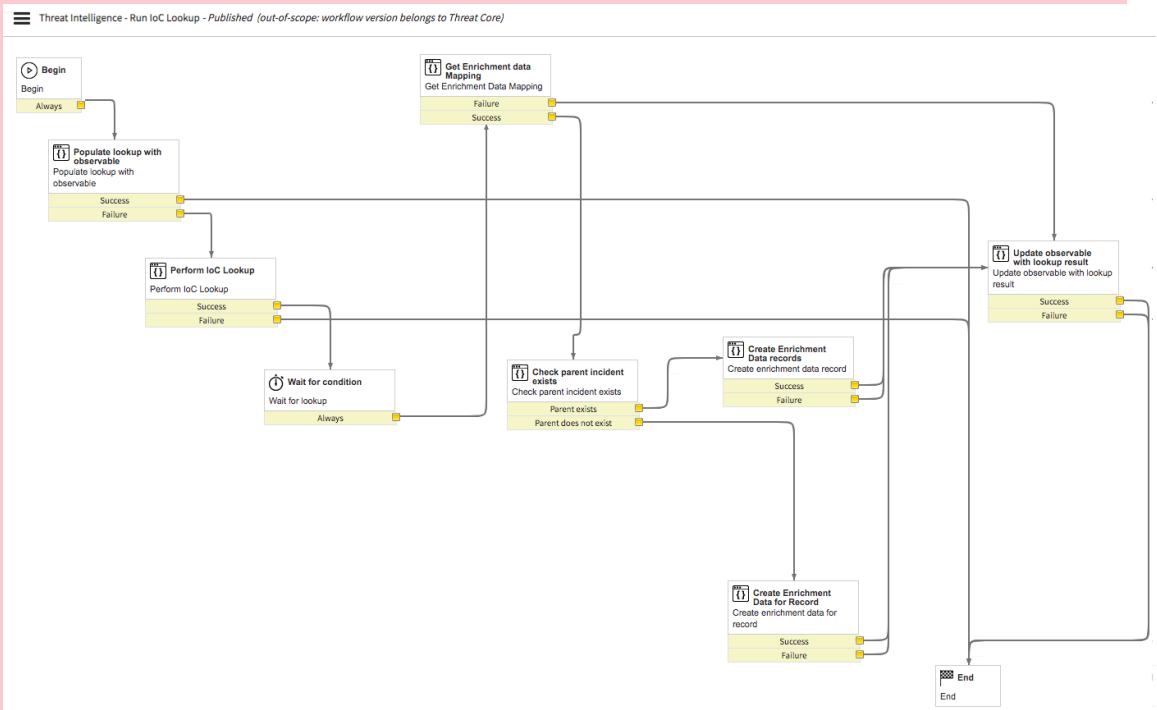
Daten erkennbarer Elemente automatisch anreichern

Nachdem Sie sich auf vorbereitet haben Threat Intelligence Automatisierung und Hinzufügen neuer oder nicht abgelaufener Indikatoren für Kompromittierung (Indicators of Commitment, IOC) zu einem Security Incident wird automatisch der Workflow Threat Intelligence – IOC-Suche ausführen ausgeführt.

Die Workflow-Aktivitäten extrahieren ohne Anwendereingriff Informationen aus den IoCs, einschließlich des Hash der verdächtigen Datei und der ursprünglichen IP-Adresse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten erkennbarer Elemente automatisch anreichern



Hinweis:
Sie können die Suche auch manuell ausführen, indem Sie mindestens ein erkennbares Element auswählen, das bereits an den Security Incident angehängt ist, und wählen **Bedrohungssuche Ausführen** Von **Aktionen für ausgewählte Zeilen** Auswahlliste.

Der Workflow führt die folgenden Aktivitäten aus:

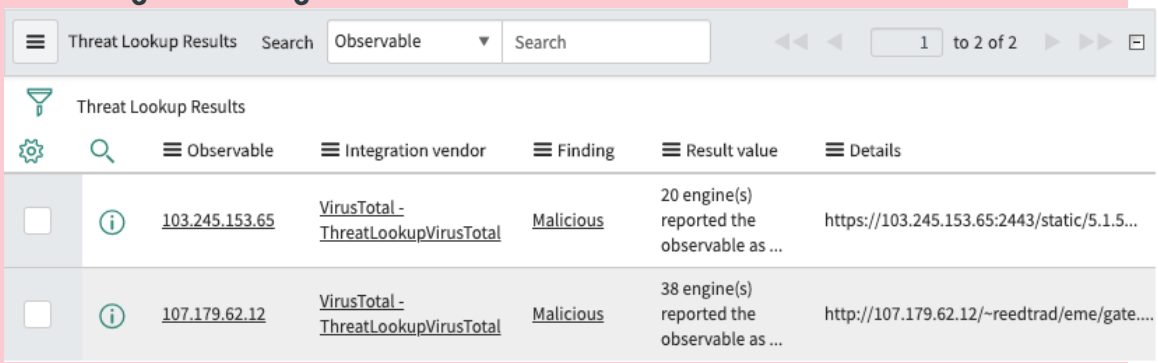
1. Die **Füllen Sie die Suche mit erkennbarem Element aus** Aktivität versucht, ein vorhandenes erkennbares Element für eine Suche zu finden, das dem Wert und Typ der Suche entspricht, die der Aktivität als Eingabe bereitgestellt werden.
   a. Wenn ein erkennbares Element gefunden wird, das den Eingaben entspricht, wird **IOC-Suche durchführen** Die Aktivität bewirkt, dass eine Suche nach der ScanID des Datensatzes durchgeführt wird.
   b. Wenn ein erkennbares Element gefunden wird und nicht abgelaufen ist, wird die Suche nicht durchgeführt, und die Suchergebnisse im Security Incident werden mit Informationen aus dem erkennbaren Element aktualisiert. Weitere Informationen finden Sie unter Füllen Sie die Suche mit Aktivität des erkennbaren Elements aus.
2. Wenn eine IOC-Suche durchgeführt wird, rufen die folgenden vier Aktivitäten zuerst Informationen aus der Ergänzungsdatenzuordnung ab. Ergänzungsdatenzuordnung Wandelt Daten aus XML-, JSON- oder Eigenschaftsdateien in ServiceNow-Datensätze um. Als Nächstes überprüfen sie, ob ein übergeordneter Security Incident vorhanden ist. Wenn dies der Fall ist, wird ein erkennbares Element erstellt und ergänzt. Wenn nicht, wird das vorhandene erkennbare Element ergänzt. Weitere Informationen finden Sie unter Aktualisieren Sie das erkennbare Element mit der Aktivität „Suchergebnis“.
   - **Ergänzungsdatenzuordnung abrufen**
   - **Überprüft, ob der übergeordnete Incident vorhanden ist**
   - **Ergänzungsdatensätze erstellen**
   - **Ergänzungsdaten für Datensatz erstellen**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Nachdem die Datenanreicherung abgeschlossen ist, wird **Aktualisieren Sie das erkennbare Element mit Suchergebnissen** Aktivität aktualisiert die erkennbaren Elemente im Security Incident und schreibt die Ergebnisse in die **Ergebnisse Der Bedrohungssuche** Zugehörige Liste.

Bedrohungssuche – Ergebnisse



Ruft automatisch Netzwerkstatistiken und laufende Prozesse ab

Wenn Sie einem Security Incident ein Konfigurationselement (CI) mit einem vollqualifizierten Windows-Domänennamen (FQDM) hinzufügen, das sich in der CMDB befindet, werden zusätzliche Workflows ausgeführt, um Netzwerkstatistiken und laufende Prozesse bereitzustellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

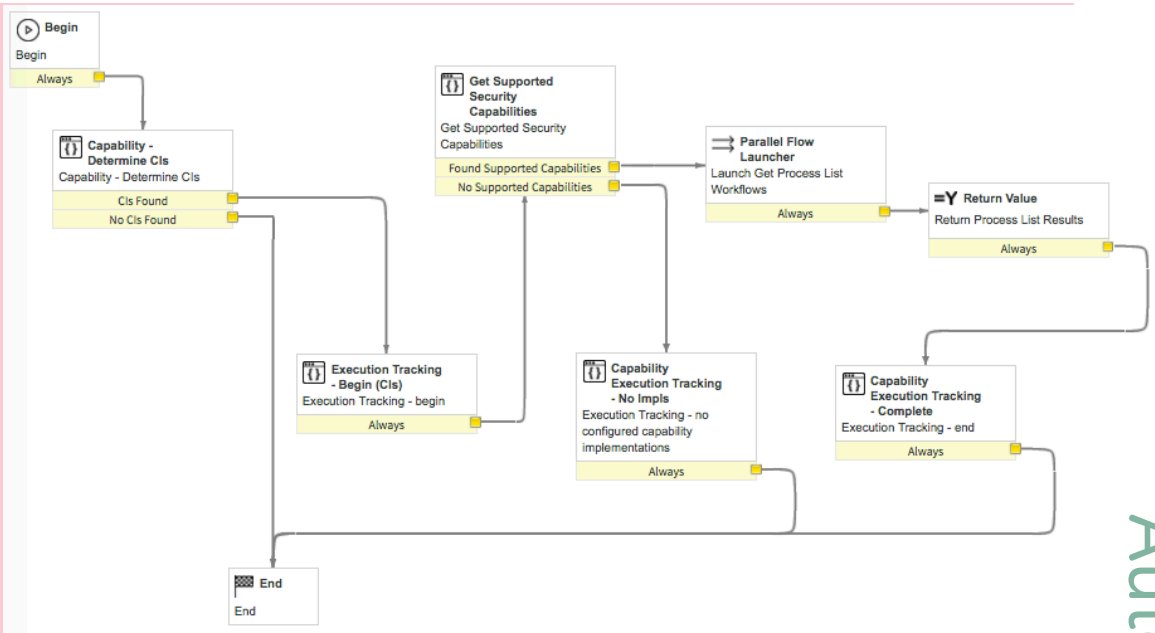
1. Mit Discovery Modul, füllen Sie die CMDB mit Windows-Domänennamen aus.

> **Hinweis:**
> Wenn Sie nicht abonnieren ServiceNow Discovery Modul müssen Sie Ihre CMDB manuell ausfüllen oder ein Discovery-Produkt eines Drittanbieters verwenden.

2. Fügen Sie dem Security Incident ein CI hinzu.
   Die folgenden beiden Workflows werden parallel ausgeführt.
   - Security Operations – Flow „Laufende Prozesse Abrufen“: Dieser Workflow ruft eine Liste der laufenden Prozesse für ein Konfigurationselement (Configuration Item, CI) von einem Host ab. Verwenden Sie es, um eine Integration wie Carbon Black oder für einen Windows-basierten Security Incident auszuführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn der Workflow abgeschlossen ist, werden laufende Prozesse in angezeigt **Laufende Prozesse** Zugehörige Liste im Security Incident.

Laufende Prozesse

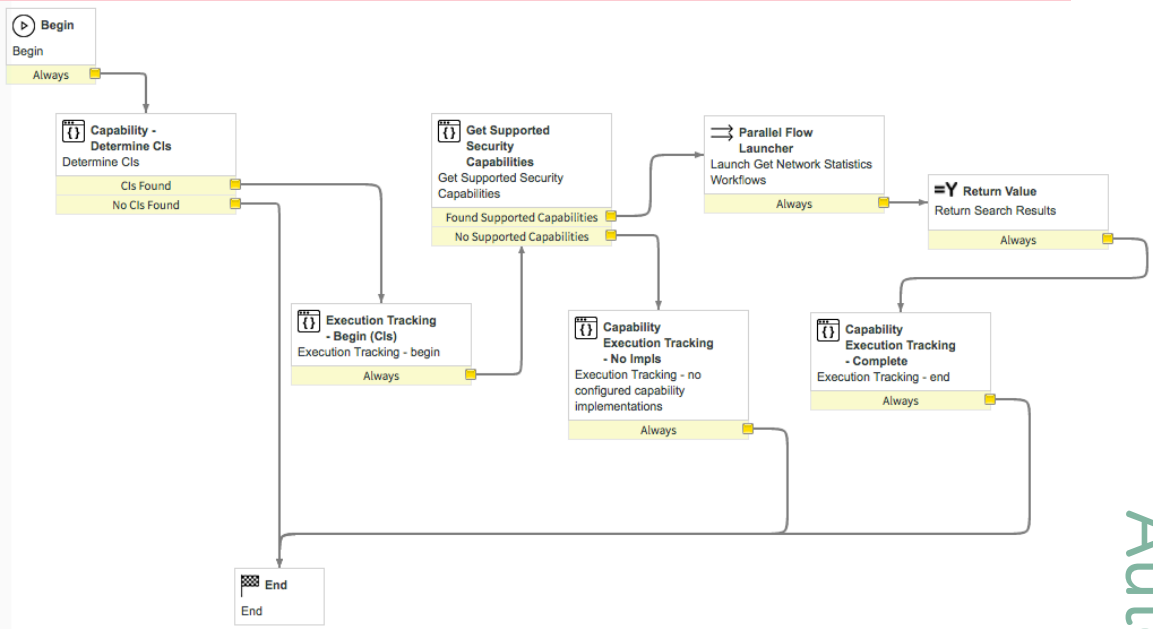
Running Processes

Path	Command ...	Owner	PID	Parent PID	Security Tags
C:\Windows\syste...	C:\Windows\syste...	SYSTEM	456	368	UNKNOWN
C:\Windows\syste...	C:\Windows\syste...	LOCAL SERVICE	856	456	UNKNOWN
C:\Windows\syste...	\??\C:\Windows\sy...	SYSTEM	1748	320	UNKNOWN
C:\Windows\Syste...	C:\Windows\Syste...	NETWORK SERVICE	3676	456	UNKNOWN
C:\Windows\syste...	\	Administrator	2400	1056	UNKNOWN
C:\demo\agent\jre\...	\	SYSTEM	6932	2540	UNKNOWN
C:\Windows\syste...	\	SYSTEM	6720	2968	UNKNOWN
		SYSTEM	4	0	UNKNOWN
C:\Windows\syste...	C:\Windows\syste...	SYSTEM	472	368	UNKNOWN
C:\Windows\syste...	C:\Windows\syste...	NETWORK SERVICE	964	456	UNKNOWN

1 to 10 of 50

- Security Operations-Integrationen – Flow „Netzwerkstatistiken abrufen“: Dieser Workflow ruft eine Liste aktiver Netzwerkverbindungen von einem Host oder Endpunkt ab. Wann

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn der Workflow abgeschlossen ist, werden Netzwerkstatistiken in angezeigt **Netzwerkstatistiken** Zugehörige Liste im Security Incident.

Netzwerkstatistiken

Workflow Activity History | Search | Started | Search | 1 to 8 of 8

Context = Security Operations Integration - Get Network Statistics

Started	Activity	State	Ended	Result	Fault Description
2019-05-13 13:28:38	Execution Tracking - begin	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:38	Get Supported Security Capabilities	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:39	Execution Tracking - end	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:39	End	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:39	Return Search Results	Finished	2019-05-13 13:28:39		
2019-05-13 13:28:38	Determine CIs	Finished	2019-05-13 13:28:38		
2019-05-13 13:28:38	Launch Get Network Statistics Workflows	Finished	2019-05-13 13:28:39	success	
2019-05-13 13:28:38	Begin	Finished	2019-05-13 13:28:38		

Priorisieren Sie wichtige Schwachstellen

Wenn Ihr Netzwerk angegriffen wird, werden häufig folgende Fragen gestellt: „Wie bestimmen wir unser Risikorisiko?“ Und noch wichtiger: „Wie bestimmen wir, welche Systeme zuerst behandelt werden sollen?“

Anfang 2018 wurden zwei kritische Schwachstellen freigesetzt: **Kernschmelze** Und **Spectre** .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Priorisieren Sie wichtige Schwachstellen

Meltdown exposes cached data in personal computers, mobile devices, and cloud servers to attack.

Spectre allows an attacker to trick error-free apps, which follow best practices, into leaking their secrets. The safety checks inherent in those best practices actually make the apps more susceptible to Spectre.

Schädliche Programme können Meltdown und Spectre ausnutzen, um Zugriff auf Geheimnisse zu erhalten, die im Speicher anderer ausgeführter Programme gespeichert sind. Fast drei Milliarden Systeme weltweit waren potenziell von den Schwachstellen betroffen, da sowohl Hardware- als auch Software-Anbieter versuchten, Patches in die Hände ihrer Kunden zu bekommen.

Rangfolge von Bedrohungen mit gescannten Daten in Vulnerability Response

Mit Security Operations Vulnerability Response Anwendung sind zahlreiche Methoden für die Ausführung verfügbar Schwachstellen-Scans . Wenn Security Incident Response Anwendung ist aktiviert, Sie können auch Initiieren Sie Scans aus dem Security Incident-Katalog, einem Security Incident-Datensatz oder einer Security Scan-Anforderung .

Abhängig von Integration von Drittparteien Sie verwenden, werden Schwachstellendaten gescannt und in importiert Vulnerability Response Anwendung mit APIs. Es wird dann mit Ihren Assets in abgeglichen ServiceNow Configuration Management Database (CMDB). Die resultierenden angreifbaren Elemente werden zugewiesen Risikopunktzahl Basierend auf mehreren Faktoren, einschließlich des Schweregrads der Schwachstelle und der Wichtigkeit des betroffenen Assets.

Risikopunktzahl

All Open Incidents

Search all incident columns

Create Incident

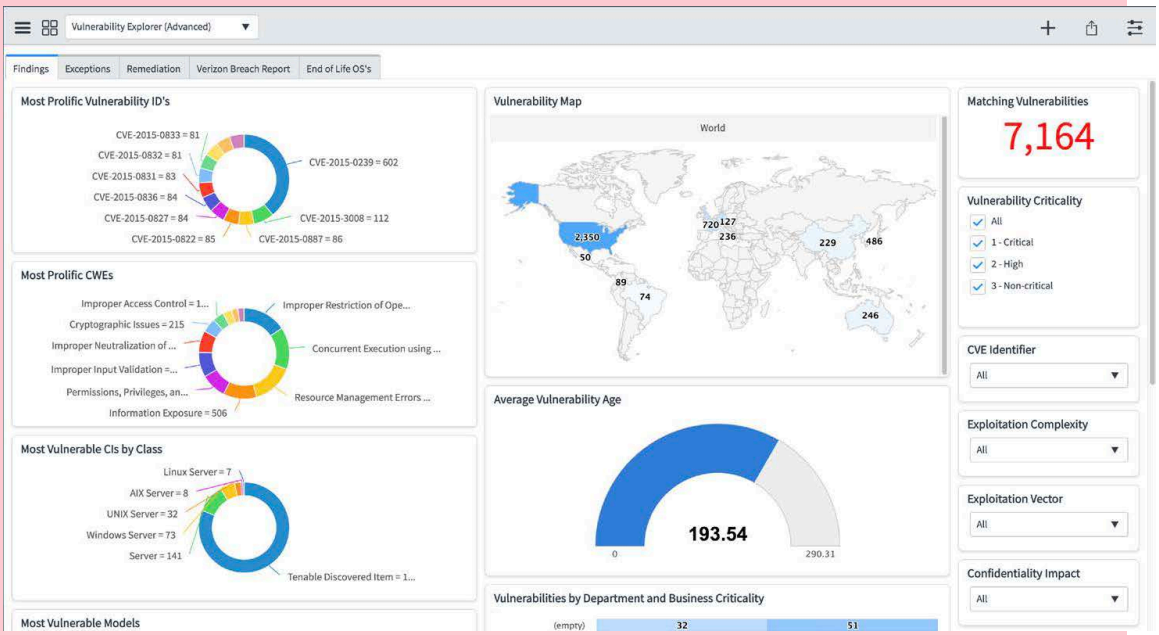
Number	Risk Score	Short Description	Category	Source
SIR0001774	89	DNS attack: zone transfer	Unauthorized access	Phone
SIR0001756	89	online gambling (policy breach)	Policy violation	Phone
SIR0001736	89	Email Malware in HQ	Malicious code act…	Alert
SIR0001742	82	USB drive found in server port	Criminal activity/i…	Email
SIR0001784	82	DNS redirect	Unauthorized access	Phone
SIR0001770	72	Database moved	Unauthorized access	Phone
SIR0001776	69	Sensitive data exposure (breach)	Unauthorized access	Phone
SIR0001761	65	email open relay	Unauthorized access	Phone

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Risikopunktzahl ist konfigurierbar und bietet eine schnelle Priorisierung. Alle Informationen über die Schwachstelle (z. B. was sie ist, wie sie ausgenutzt wurde und wie die Bedrohung behoben werden kann) werden automatisch abgerufen Vulnerability Response Aus der National Vulnerability Database (NVD), wodurch manuelle Forschung überflüssig wird. Die konfigurierbaren Dashboards der Lösung zeigen sofort das Gesamtrisiko Ihrer Organisation an.

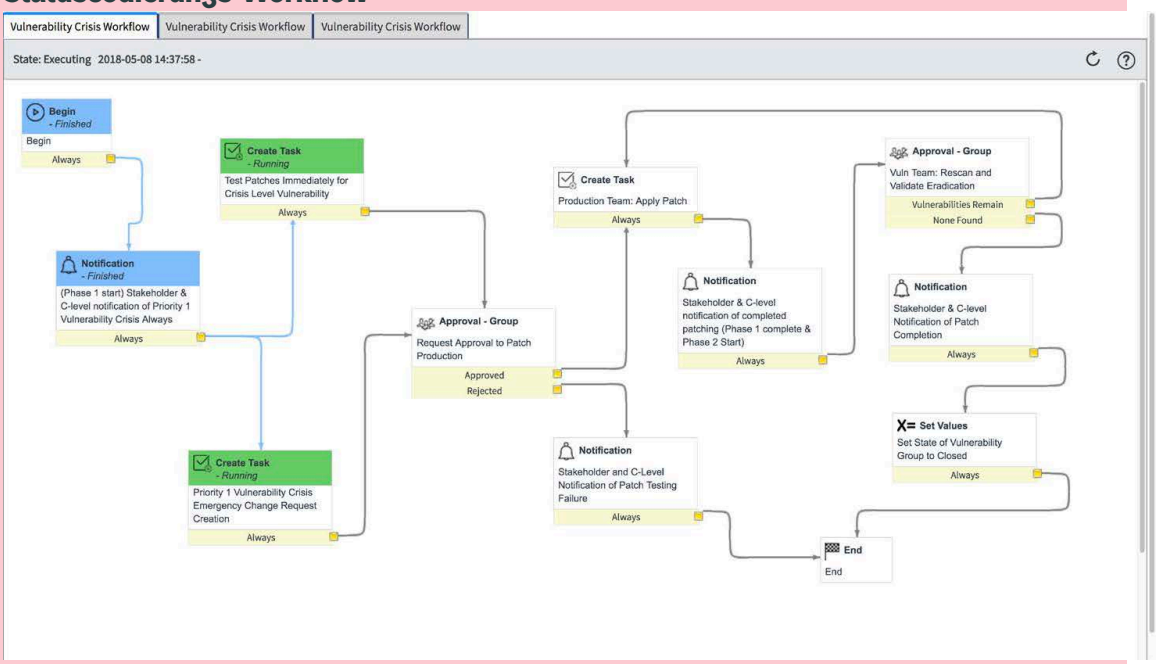
VR-Dashboard



Die nächsten Schritte werden automatisiert

Nachdem Sie die kritischsten angreifbaren Elemente identifiziert und priorisiert haben, Security Operations Workflows automatisieren mehrere der nächsten Schritte.

Statuscodierungs-Workflow



Für geschäftskritische angreifbare Elemente werden Anforderungen zur Genehmigung des automatischen Patches gesendet, und die entsprechenden Besitzer werden benachrichtigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dadurch ist es nicht mehr erforderlich, nach dem Bereitschaftsanalysten zu suchen oder manuell zu entscheiden, welche Elemente als „Kritisch“ gelten.

Nach Genehmigung und Abschluss des Patches wird automatisch ein zweiter Scan ausgeführt, um die Korrektur zu verifizieren. Mithilfe von Priorisierung, Workflows und Automatisierung werden die kritischsten Elemente zuerst behandelt.

Security Operations Und ServiceNow Store

Beginnend mit Madrid, Alle Security Operations Anwendungen und unterstützte Integrationen können über heruntergeladen werden ServiceNow Store. Dadurch können Sie schneller neue und aktualisierte Funktionen erhalten. Bevor Sie verwenden können Security Operations Anwendungen müssen Sie überprüfen, ob Sie Berechtigungen für sie haben (d. h. Sie haben gültige Lizenzen für die Verwendung), und sie aus dem herunterladen ServiceNow Store, Und aktivieren Sie sie.

Die ständig wachsende Liste von Security Operations Zum Herunterladen verfügbare Anwendungen:

- Security Incident Response (Und unterstützte Integrationen)
- Vulnerability Response (Und unterstützte Integrationen)
- Threat Intelligence (Und unterstützte Integrationen)
- Konfigurations-Compliance
- Trusted Security Circle
- Data Loss Prevention Incident Response

Sehen Sie sich dieses fünfminütige Video an, um mehr über das Herunterladen von Security Operations- und GRC-Anwendungen aus dem zu erfahren ServiceNow Store. In diesem 5-minütigen Video wird beschrieben, wie Security Operations- und GRC-Anwendungen aus dem ServiceNow Store heruntergeladen werden

Der Prozess, den Sie zum Abrufen verwenden Security Operations Anwendungen und Integrationen hängen davon ab, ob Sie eine Anwendung zum ersten Mal herunterladen und eine Anwendung aktualisieren, die Sie zuvor von heruntergeladen haben ServiceNow Store, Oder Upgrade von einem Familien-Release auf das nächste.

Laden Sie eine Anwendung aus dem herunter ServiceNow Store Zum ersten Mal

Lädt eine Anwendung aus dem herunter ServiceNow Store Zum ersten Mal umfasst es eine Reihe einfacher Schritte. Einige der Schritte werden für ausgeführt ServiceNow Store Und einige in Ihrer Instanz.

Die ServiceNow Store Ermöglicht das Herunterladen von Kernprodukten und -Anwendungen. Ein Produkt enthält eine oder mehrere Anwendungen, die als Gruppe lizenziert sind. Beispiel: Security Incident Response Ist ein Produkt. Der Prozess umfasst die folgenden Schritte:

Erforderliche Rolle: admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- In ServiceNow Store, Sie müssen sicherstellen, dass Sie über Berechtigungen (oder Lizenzen) für die Anwendung und ihre abhängigen Anwendungen verfügen.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in nicht-Produktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

- Schließlich können Sie die Anwendung aktivieren und auf Ihrer Instanz ausführen.

Hinweis:
Beginnend mit vorherigen Versionen von Rome Und spätere Releases werden Abhängigkeits-Plugins automatisch aktiviert, wenn Sie eine Kernanwendung aktivieren. Beispiel: Wenn Sie aktivieren Vulnerability Response Anwendung, die Vulnerability Response Das Plugin „Abhängigkeiten“ ist ebenfalls aktiviert. Weitere Informationen finden Sie unter Aktivieren Sie einen ServiceNow Store Anwendung.

Berechtigung für abrufen Security Operations Produkt oder Anwendung

Der erste Schritt bei der Installation von Security Operations Die Anwendung dient dazu, sicherzustellen, dass die Anwendung oder das Produkt und die zugehörigen Anwendungen gültig sind ServiceNow Berechtigungen.

Vorbereitungen

Erforderliche Rolle: Administrator

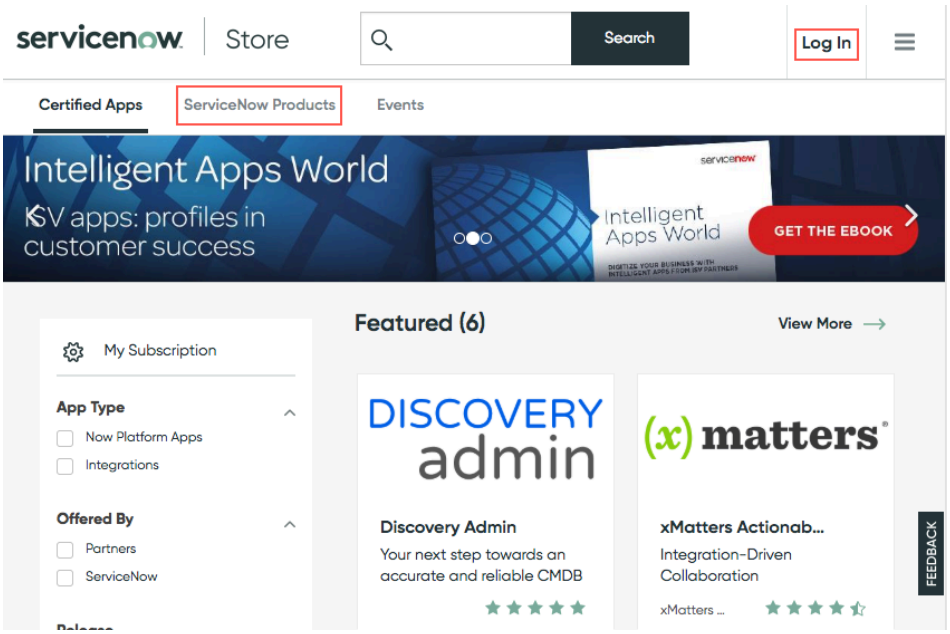
Personen, die eine Berechtigung ausführen, müssen über einen verfügen Now Support Account und Berechtigung zum anfordern von Anwendungen für die betreffenden Instanzen.

Hinweis:
Dieser Prozess gilt nur für Anwendungen, die in Produktionsinstanzen heruntergeladen werden. Wenn Sie Anwendungen in Unterproduktions- oder Entwicklungsinstanzen herunterladen, müssen Sie keine Berechtigungen abrufen. Fahren Sie mit fort Aktivieren Sie einen ServiceNow Store Anwendung.

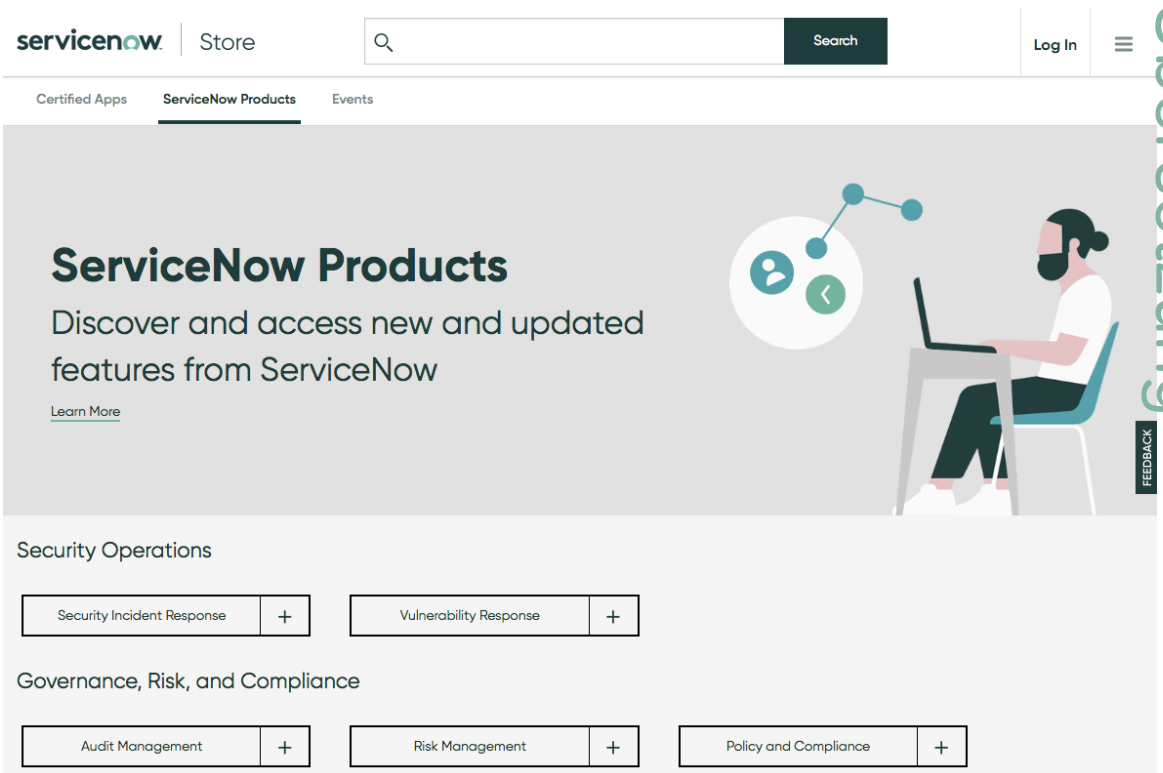
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zu ServiceNow Store an.



2. Klicken Sie Auf **Melden Sie Sich An** Und melden Sie sich mit an HI Anmeldeinformationen.
3. Klicken Sie auf **ServiceNow-Produkte** Registerkarte zum Anzeigen aller verfügbaren Elemente ServiceNow Produkte.
   Integrationen und andere Inhaltstypen werden im angezeigt **Zertifizierte Apps** Registerkarte.



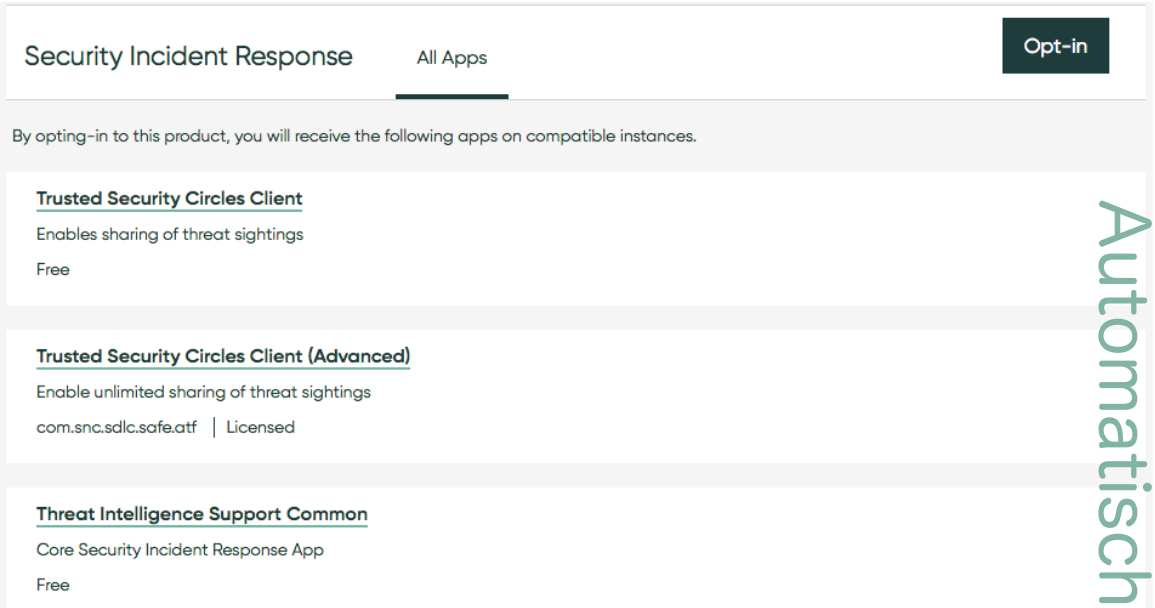
Hinweis:
Nehmen Sie für dieses Beispiel an, dass Sie eine Berechtigung für erwerben Security Incident Response Produkt.

Automatische Übersetzung

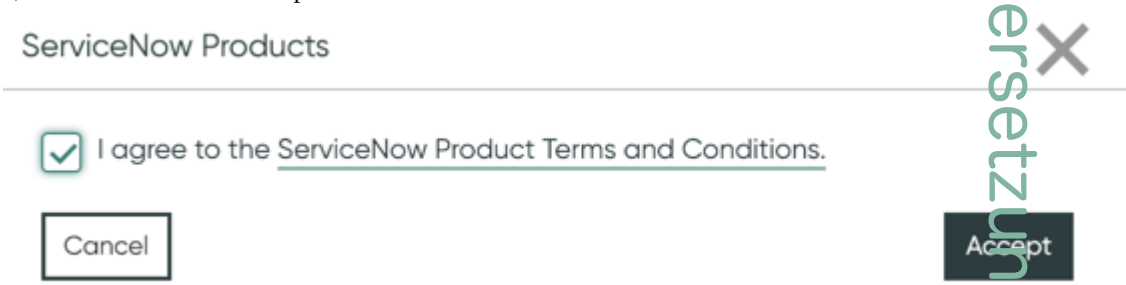
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf das Pluszeichen (+) neben dem Produktnamen, für den Sie eine Berechtigung erhalten. Alle Anwendungen, die dem Produkt zugeordnet sind, für das Sie eine Berechtigung haben, werden aufgelistet. Wenn Sie die Berechtigung für das Kernprodukt erhalten haben, sind auch die darin aufgeführten Anwendungen berechtigt.

   Hinweis:
   Sie können auch auf den Produktnamen klicken, um weitere Informationen zum Produkt und den zugehörigen Anwendungen anzuzeigen.



5. Klicken Sie Auf **Aktivieren** Um sicherzustellen, dass Sie Berechtigungen für das Produkt und die aufgeführten Anwendungen haben.
   Sie werden aufgefordert, den zu lesen und zu akzeptieren ServiceNow



   Nutzungsbedingungen.

6. Aktivieren Sie das Kontrollkästchen, und klicken Sie auf **Akzeptieren** .

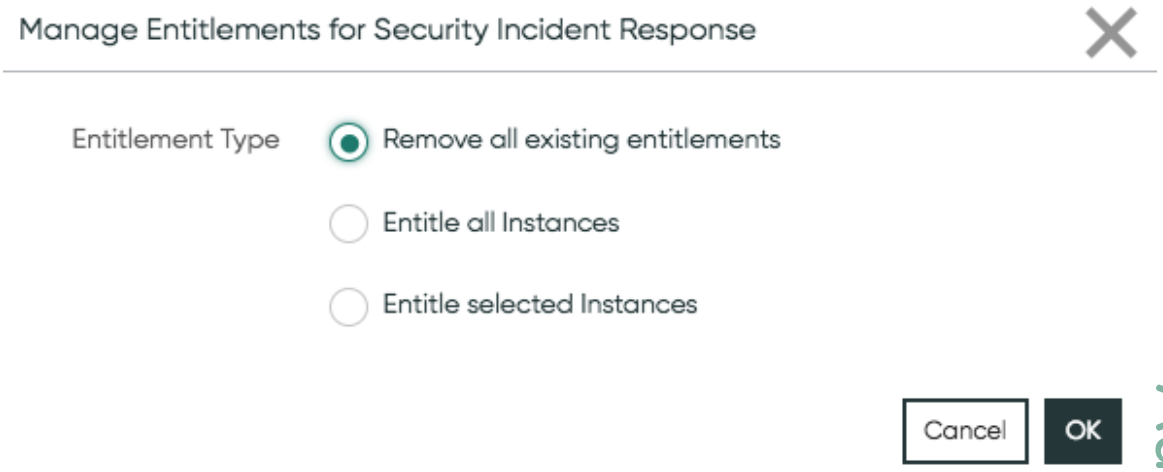
7. Beachten Sie, dass neben dem Produktnamen ein Häkchen angezeigt wird und die Schaltfläche Berechtigungen verwalten angezeigt wird.

   Das Häkchen gibt an, dass Sie das Produkt und die zugehörigen Anwendungen abonniert haben. Es ist an der Zeit, Ihre Berechtigungen zu verwalten. Dies ist ein einmaliger Prozess für dieses Produkt und alle anderen Produkte, die Sie in der Zukunft installieren möchten.

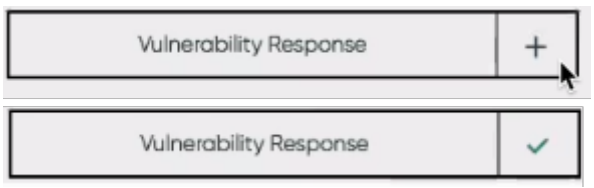
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. **Wahlweise:** Sie können auf klicken **Verwalten Sie Berechtigungen** Zum Ändern der Instanzen, die von den Anwendungen betroffen sind, für die Sie berechtigt sind.



9. Nachdem Sie dem zugestimmt haben ServiceNow Nutzungsbedingungen und verwaltete Berechtigungen können Sie mit einem einzigen Klick andere Produkte berechtigen.



Hinweis:
Sie sind bereit, das Produkt zu aktivieren.

Aktivieren Sie einen ServiceNow Store Anwendung

Nachdem eine Anwendung berechtigt wurde, müssen Sie das Plugin „Abhängigkeiten“ aktivieren und die Anwendung aktivieren. Dieser Prozess gilt auch für Anwendungen, die in Subproduktionsinstanzen heruntergeladen werden.

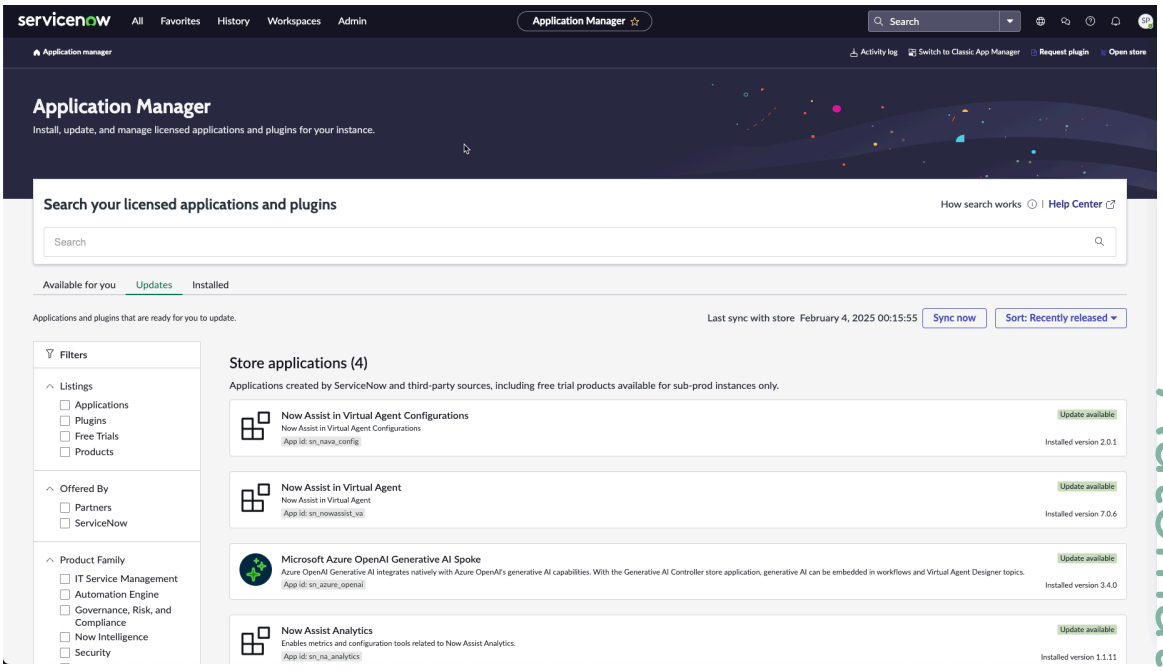
Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

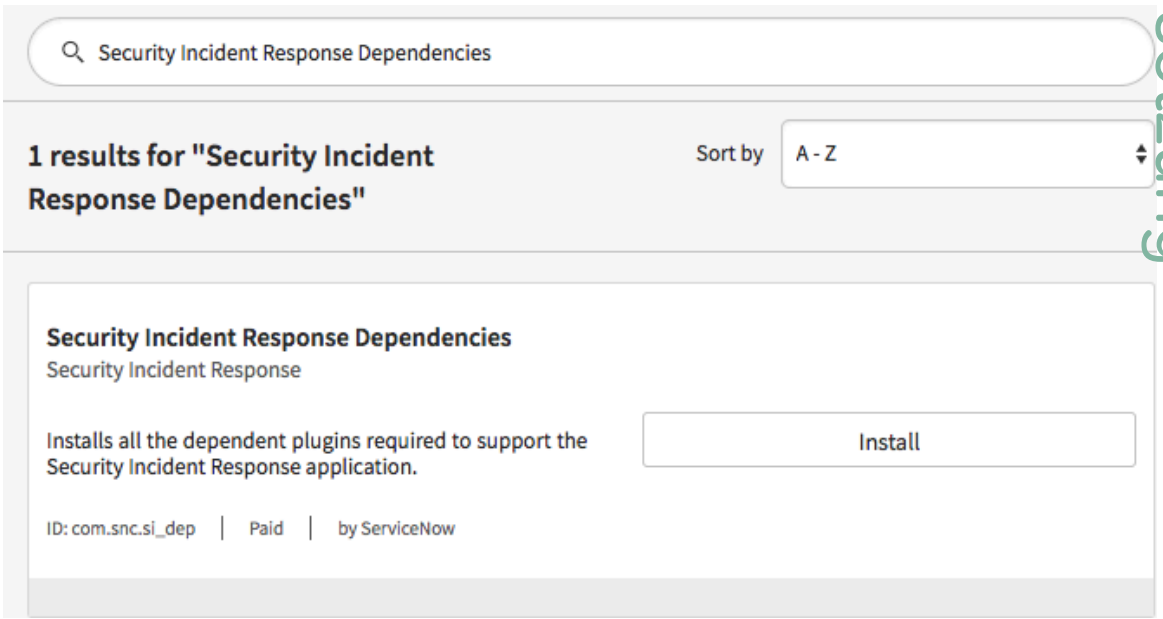
Prozedur

1. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.



Hinweis:
Ab Orlando werden Abhängigkeits-Plugins automatisch aktiviert, wenn Sie eine Kernanwendung aktivieren. Beispiel: Wenn Sie aktivieren Vulnerability Response Anwendung, die Vulnerability Response Das Plugin „Abhängigkeiten“ ist ebenfalls aktiviert. Daher sind die Schritte 2 bis 5 optional.

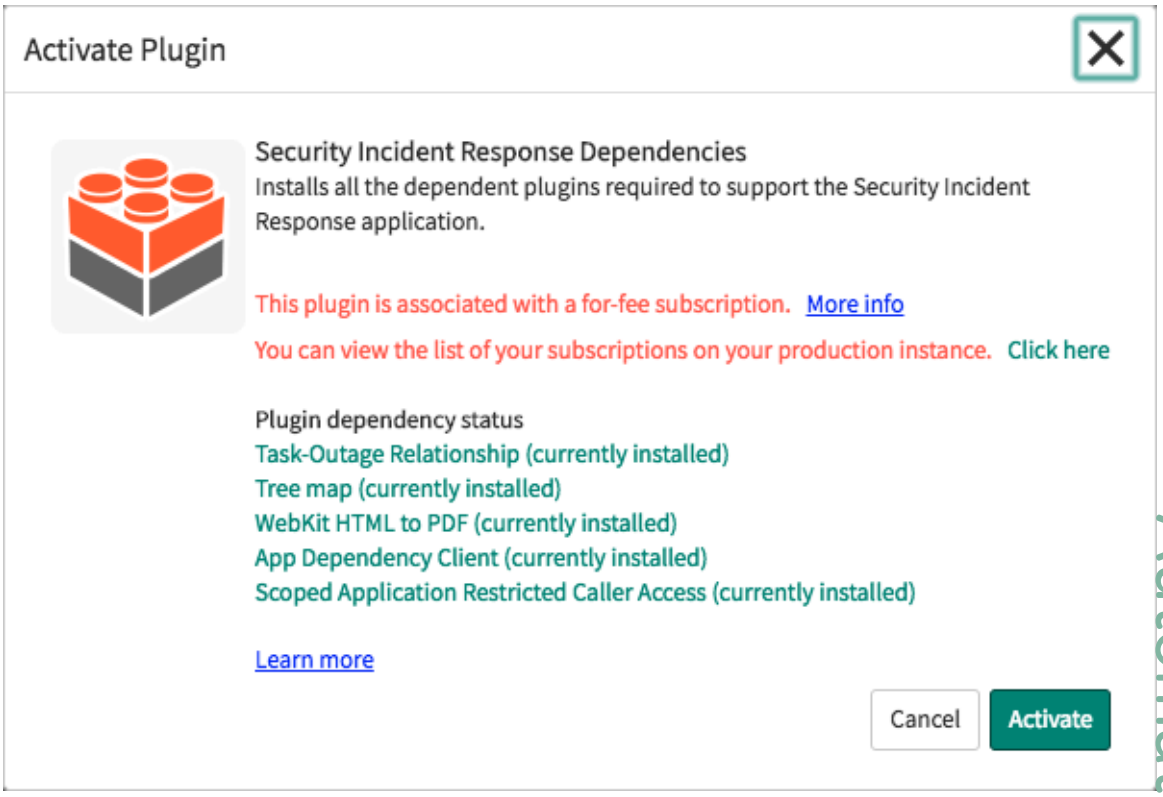
2. Suchen Sie nach dem Abhängigkeiten-Plugin für die Anwendung, die Sie aktivieren möchten.
Beispiel: Wenn Sie aktivieren Security Incident Response, Suchen Sie nach Security Incident Response Plugin „Abhängigkeiten“.



3. Klicken Sie auf **Installieren**.
Das Dialogfeld Plugin aktivieren wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. In **Aktivieren Sie Das Plugin** Klicken Sie auf das Dialogfeld **Aktivieren** .
5. Wenn die Aktivierung abgeschlossen ist, klicken Sie auf **Formular Schließen Und Neu Laden** .
6. Suchen Sie nun das Kernprodukt, das Sie aktivieren, und klicken Sie auf **Mit Demodaten installieren** Aktivieren Sie das Kontrollkästchen, wenn Sie Demodaten laden möchten, und klicken Sie auf **Installieren** . Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Hinweis:
Wenn Sie nicht auswählen **Mit Demodaten installieren** Kontrollkästchen, Demodaten sind nicht verfügbar, um von zu installieren **Anwendungsmanager** Später. Informationen zur Installation oder Neuinstallation von Demodaten nach der Erstinstallation finden Sie unter Problemumgehung zum Installieren von Demodaten, wenn die Anwendung bereits installiert ist [KB0722909] artikel in HI Knowledge Base.

Installieren Sie ein Security Operations Integration

Alle ServiceNow Integrationen sind auf verfügbar ServiceNow Store. Kernanwendungen, z. B. Security Incident Response, sind in sichtbar **ServiceNow-Produkte** Registerkarte im Store. Integrations-Add-ons sind in sichtbar **Zertifizierte Apps** Registerkarte.

Vorbereitungen

Erforderliche Rolle: Administrator

Store-Installationen erfordern einen Now Support Account und Berechtigung zum anfordern von Anwendungen für die betroffenen Instanzen.

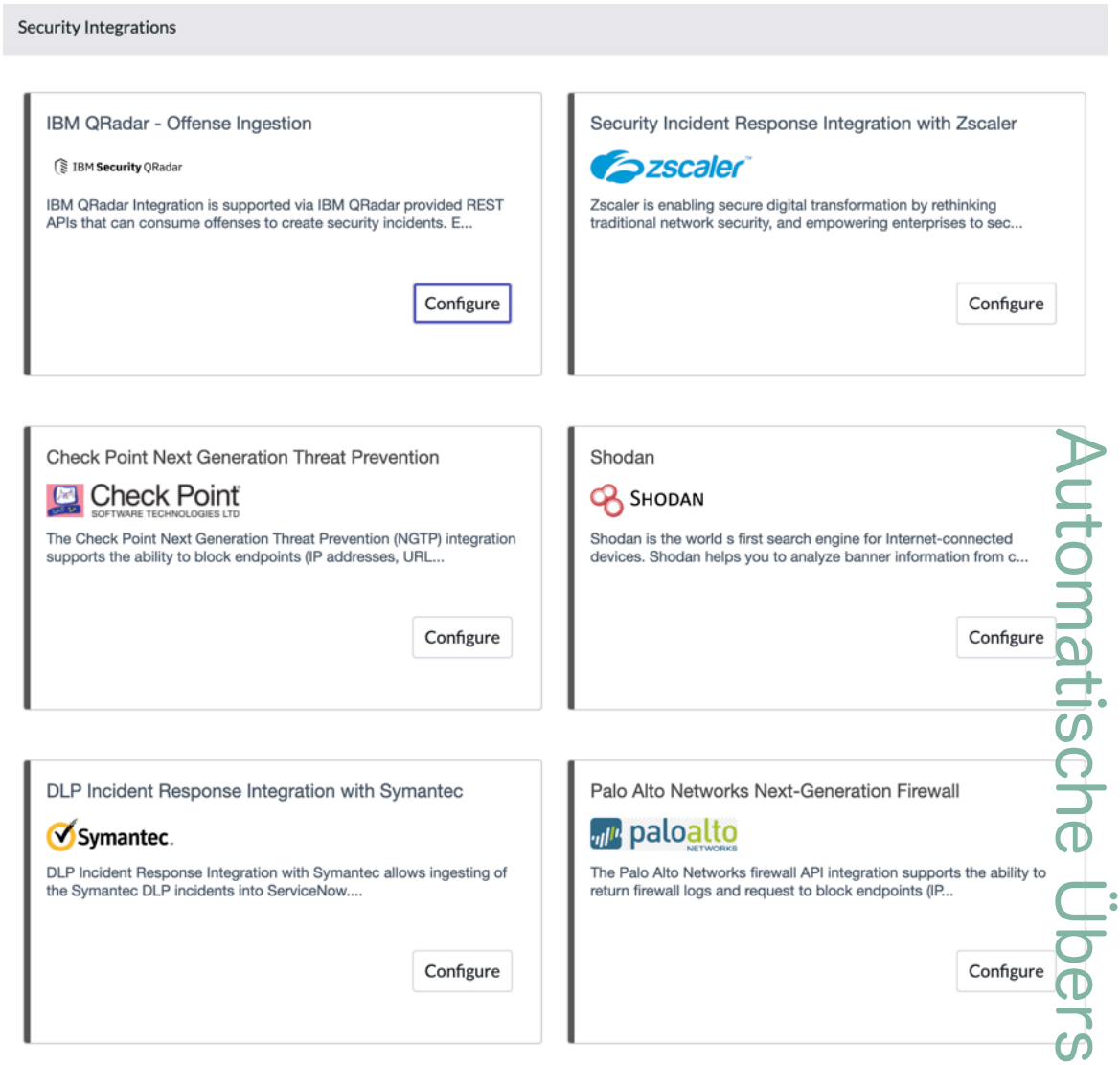
Prozedur

1. Navigieren zu **Security Operations** > **Integrationen** > **Integrationskonfigurationen** Nachdem Sie die Anwendung aus dem ServiceNow Store installiert haben.
   Konfigurationskacheln für die Integrationen werden angezeigt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

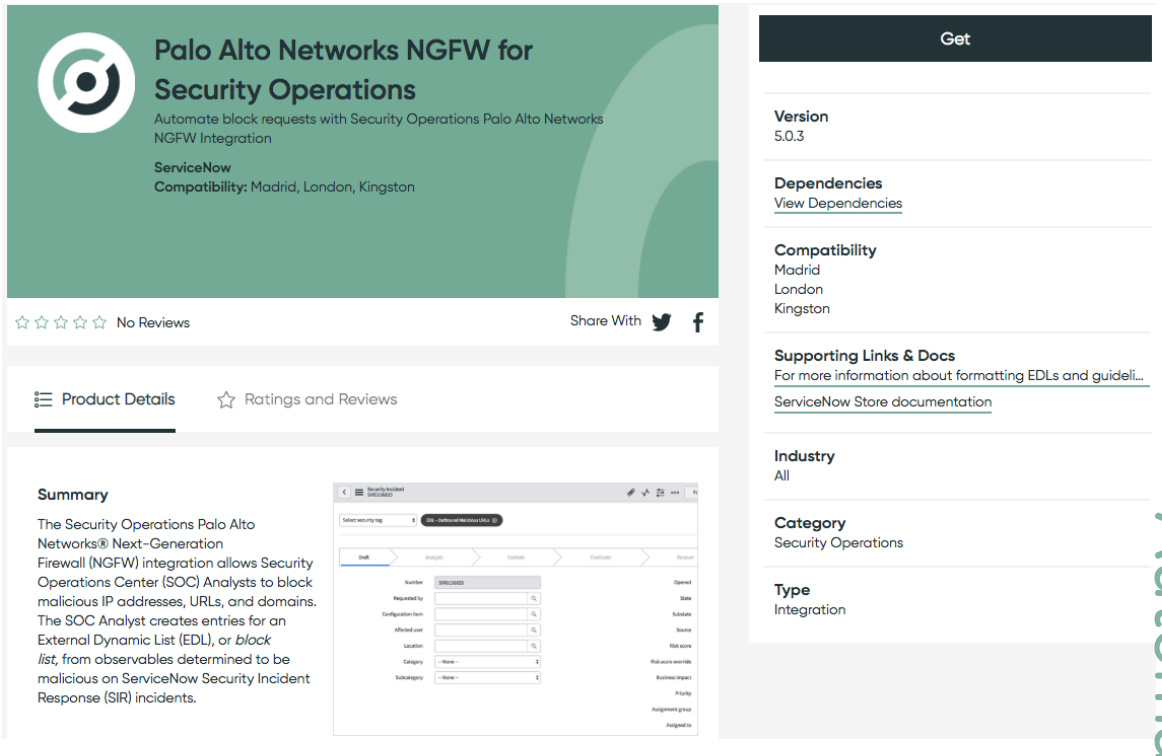
Hinweis:



2. Suchen Sie die Integration, die Sie installieren möchten, und klicken Sie auf **Konfigurieren** .
   Die ausgewählte Integration wird in angezeigt ServiceNow Store

Automatische Übersetzung

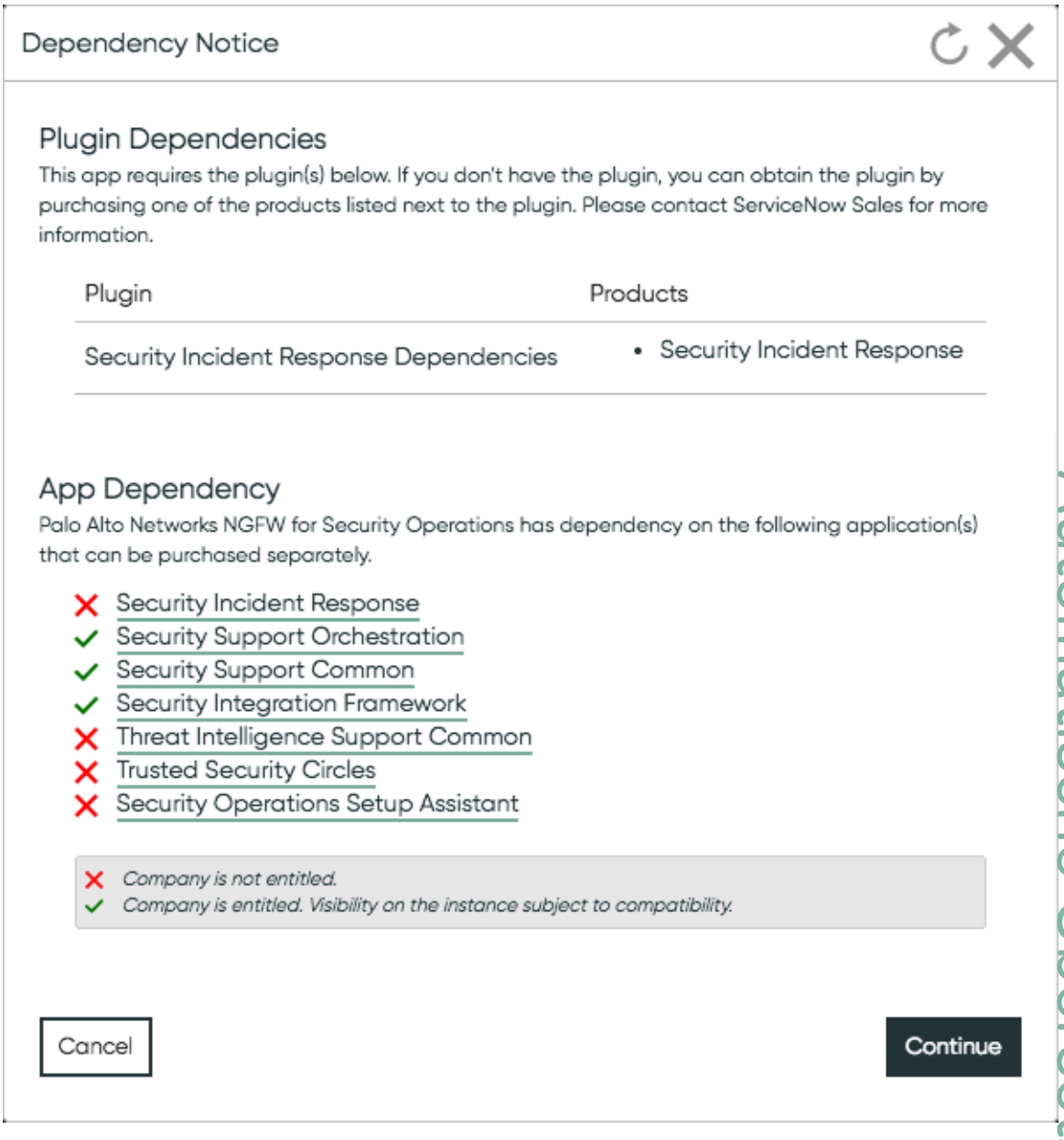
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie Auf **Zeigen Sie Abhängigkeiten An** Und überprüfen Sie die aufgeführten App-Abhängigkeiten.

Automatische Übersetzung

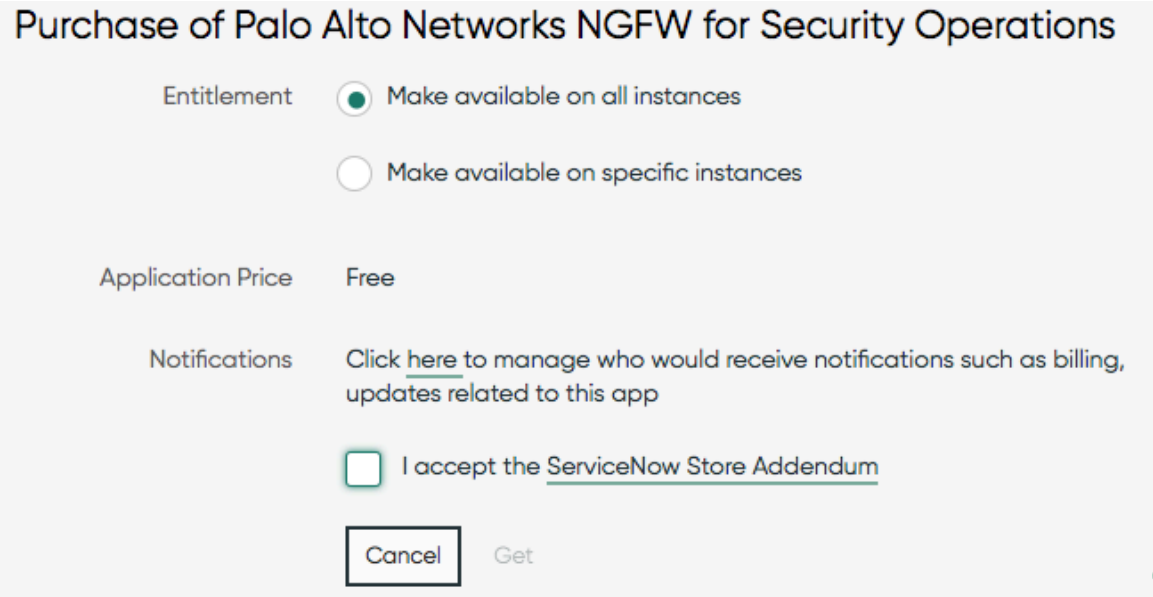
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wenn die Integration Kernanwendungsabhängigkeiten aufweist, z. B. Security Incident Response, Für die Ihr Unternehmen noch nicht berechtigt ist:
   a. Befolgen Sie diese Anweisungen, um Berechtigungen abzurufen, Abhängigkeits-Plugins herunterzuladen und die Anwendungen zu aktivieren .
   b. Kehren Sie zu diesem Verfahren zurück.
   c. Klicken Sie auf **Fortsetzen**.
5. Klicken Sie auf **Abrufen**.
   Die ServiceNow-Nutzungsbedingungen werden angezeigt.
6. Klicken Sie auf **Fortsetzen**.
   Ein Kaufbildschirm ähnlich dem folgenden wird geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Identifizieren Sie, in welchen Instanzen die Integration verfügbar sein soll, verwalten Sie Ihre Benachrichtigungen, und wählen Sie aus **ServiceNow Store-Nachtrag** Kontrollkästchen.
8. Klicken Sie auf **Abrufen**.

> **Hinweis:**
> Wenn Sie eine Anwendung zum Kauf herunterladen, klicken Sie auf **Kaufen** . Wenn Sie eine Anwendung herunterladen, für die Sie eine vorherige Genehmigung vom Lieferanten einholen müssen, klicken Sie auf **App Anfordern** .

9. Geben Sie den Instanznamen und einen Grund für die Anforderung ein, und klicken Sie dann auf **Anforderung** .
   Sie erhalten eine E-Mail mit detaillierten Installationsanweisungen.
10. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.
    Eine Liste der Anwendungen, die für die Installation verfügbar sind, wird angezeigt.
11. Suchen Sie nach der Anwendung, wählen Sie sie aus und klicken Sie auf **Installieren**.
    Ihre Integration wird automatisch auf Ihrer Instanz installiert.

Aktualisieren Sie eine Anwendung, die zuvor aus dem heruntergeladen wurde ServiceNow Store

Wenn Sie zuvor eine Anwendung aus heruntergeladen haben ServiceNow Store Und eine neue Version ist verfügbar. Sie können sie in Ihrer Instanz aktualisieren.

Vorbereitungen

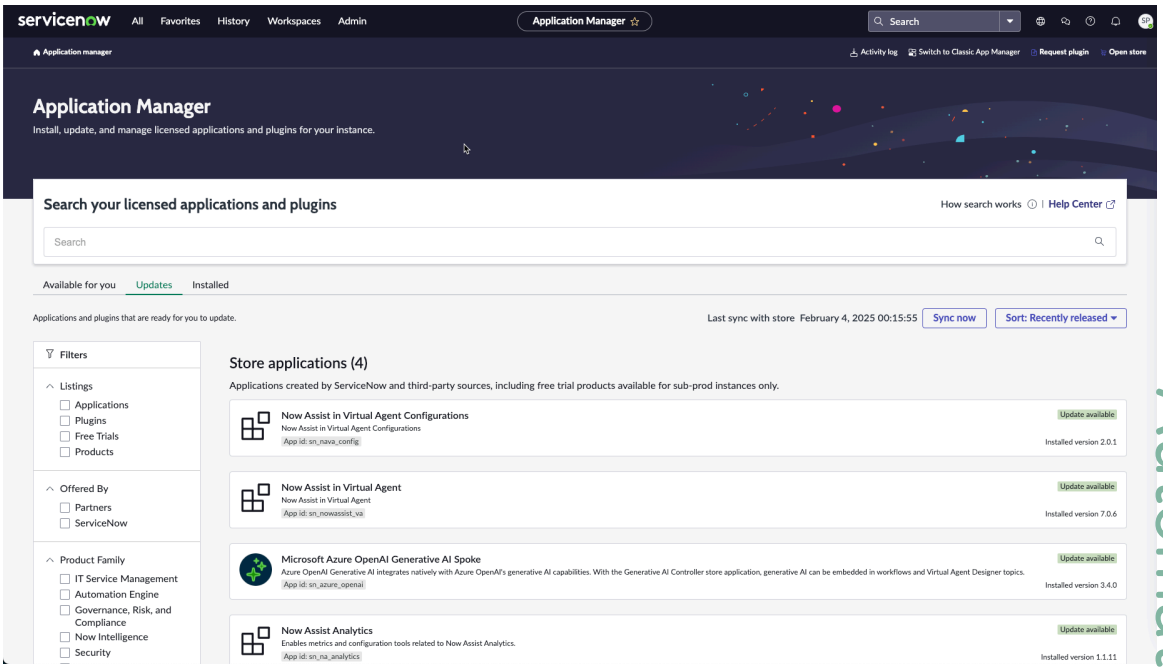
Erforderliche Rolle: admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**an.



2. Suchen Sie nach der Anwendung, die Sie aktualisieren möchten.
3. Wählen Sie die Version aus, auf die Sie ein Upgrade durchführen möchten, und klicken Sie auf **Aktualisieren** .
   Ihre Anwendung wird automatisch auf Ihrer Instanz installiert.

Führen Sie ein Upgrade Ihrer Instanz auf das nächste Familien-Release durch

Wenn Sie derzeit ein Familien-Release ausführen und ein Upgrade auf das nächste Release durchführen möchten, müssen Sie die Anwendungen nicht von beziehen ServiceNow Store. Die Anwendung wird automatisch aktualisiert, wenn die Plattform auf die erforderliche Mindestversion aktualisiert wird.

Erforderliche Rolle: Administrator

Weitere Informationen finden Sie unter Using the release notes Um zu erfahren, wie Sie in den überarbeiteten Versionshinweisen navigieren und die gesuchten Informationen und finden Learn about the Zurich release Für neue Funktionen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.